

# Bitdefender®

## GravityZone

API DOCUMENTATION

## Bitdefender Control Center API Documentation

Publication date 2017.01.25

Copyright© 2017 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	15
2.1.5. configureNotificationsSettings	17
2.1.6. getNotificationsSettings	20
2.1.7. Objects	23
2.2. Companies	29
2.2.1. createCompany	29
2.2.2. deleteCompany	31
2.2.3. updateCompanyDetails	32
2.2.4. getCompanyDetails	34
2.2.5. getCompanyDetailsByUser	35
2.2.6. findCompaniesByName	37
2.2.7. suspendCompany	39
2.2.8. activateCompany	40
2.3. Licensing	40
2.3.1. getLicenseInfo	41
2.3.2. setMonthlySubscription	42
2.3.3. setLicenseKey	43
2.3.4. getMonthlyUsage	44
2.4. Network	46
2.4.1. getCompaniesList	47
2.4.2. getCompanyFoldersList	48
2.4.3. createCompanyFolder	49
2.4.4. deleteCompanyFolder	50
2.4.5. moveCompanyOrCompanyFolder	51
2.4.6. getEndpointsList	52
2.4.7. getManagedEndpointDetails	54
2.4.8. createCustomGroup	58
2.4.9. deleteCustomGroup	59
2.4.10. getCustomGroupsList	60
2.4.11. moveEndpoints	61
2.4.12. deleteEndpoint	62
2.4.13. moveCustomGroup	63
2.4.14. getRootContainers	64
2.4.15. createScanTask	66

2.4.16. getScanTasksList .....	67
2.5. Packages .....	69
2.5.1. getInstallationLinks .....	69
2.5.2. createPackage .....	71
2.5.3. getPackagesList .....	74
2.6. Policies .....	76
2.6.1. getPoliciesList .....	76
2.6.2. getPolicyDetails .....	78
2.7. Integrations .....	80
2.7.1. getHourlyUsageForAmazonEC2Instances .....	80
2.7.2. configureAmazonEC2Integration .....	82
2.7.3. disableAmazonEC2Integration .....	83
2.7.4. getCompanyDetailsByAWSAccountId .....	84
2.8. Reports .....	85
2.8.1. createReport .....	86
2.8.2. getReportsList .....	103
2.8.3. getDownloadLinks .....	106
2.8.4. deleteReport .....	109
3. API Usage Examples .....	111
3.1. C# Example .....	111
3.2. curl Example .....	112
3.3. Python Example .....	113
3.4. Node.js example .....	114

## 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 creating a company inside Bitdefender Control Center:

```
{
  "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
  "jsonrpc": "2.0",
  "method": "createCompany",
  "params": {
    "type": 0,
    "name": "My Company"
  }
}
```

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

```
{
  "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
  "jsonrpc": "2.0",
  "result": "5493dcd2b1a43df00b7b23c6"
}
```

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/](https://cloud.gravityzone.bitdefender.com/api/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:	<a href="https://cloud.gravityzone.bitdefender.com/api">https://cloud.gravityzone.bitdefender.com/api</a>

Currently, the following APIs are being exposed:

1. **Companies**, with the API URL:  
[CONTROL\\_CENTER\\_APIs\\_ACCESS\\_URL/v1.0/jsonrpc/companies](https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/companies).
2. **Licensing**, with the API URL:  
[CONTROL\\_CENTER\\_APIs\\_ACCESS\\_URL/v1.0/jsonrpc/licensing](https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/licensing).
3. **Accounts**, with the API URL:  
[CONTROL\\_CENTER\\_APIs\\_ACCESS\\_URL/v1.0/jsonrpc/accounts](https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/accounts).
4. **Network**, with the API URL:  
[CONTROL\\_CENTER\\_APIs\\_ACCESS\\_URL/v1.0/jsonrpc/network](https://cloud.gravityzone.bitdefender.com/api/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.`

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

**Note**

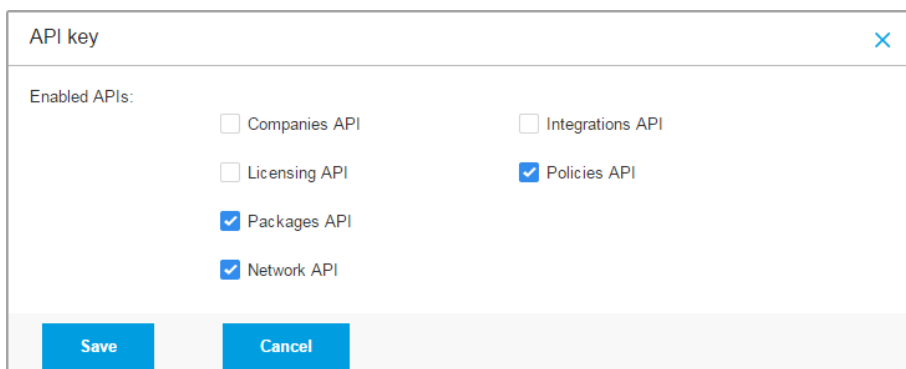
Batch requests and notifications are not currently supported by Bitdefender Control Center.

## 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 partner 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:

- ☐ Companies API
- ☐ Integrations API
- ☐ Licensing API
- ☒ Policies API
- ☒ Packages API
- ☒ Network API

**Save** **Cancel**

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



+ Add - Delete Refresh		
<input type="checkbox"/>	Key	Created
<input type="checkbox"/>		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 licenses and customers inventory. Please do not share or distribute your own generated API keys, in order to prevent the leaking of sensitive information!

Bitdefender Control Center also allows partners to delete the previously generated API keys if they are no longer needed.

## 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

HTTP status	Description
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](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
<code>companyId</code>	String	Yes	When set, this method will list only the user accounts belonging to the company identified with the given ID.
<code>page</code>	Number	Yes	The results page number. The default value is 1.

Parameter	Type	Optional	Description
perPage	Number	Yes	The number of items displayed in a page. The upper limit is 30 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, 4 - Partner, 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.
  - **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,  
    "companyId": "58541613aaed7090058b4567"  
  }  
}
```

## 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
    },
    "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.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.



Parameter	Type	Optional	Description
companyId	String	Yes	The company ID used for linking the user account to a specific company. If not specified, the account will be linked to the company that holds the API key.
role	Number	Yes	<p>The role of the new account. The default value is 1 - Company Administrator. These are the available roles:</p> <ul style="list-style-type: none"> <li>1 - Company Administrator.</li> <li>2 - Network Administrator.</li> <li>3 - Reporter.</li> <li>4 - Partner.</li> <li>5 - Custom. For this role, rights must be specified.</li> </ul>
rights	Object	Yes	<p>An object containing the rights of a user account. This object should be set only when <code>role</code> parameter has the value 5 - Custom. When set for other roles, the values will be ignored and replaced with the rights specific to that role. The available rights are:</p> <ul style="list-style-type: none"> <li><code>manageCompanies</code></li> <li><code>manageNetworks</code> Setting this to true implies <code>manageReports</code> right to true</li> <li><code>manageUsers</code></li> <li><code>manageReports</code></li> <li><code>companyManager</code></li> </ul> <p>Each option has two possible values: true, where the user is granted the right, or false otherwise. Omitted values from the request are automatically set to false.</p>
targetIds	Array	Yes	A list of IDs representing the targets to be managed by the user account. For more

Parameter	Type	Optional	Description
			information, refer to the <a href="#">relation between companyId and targetIds</a> .

## 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
    },
    "companyId": "58541613aaed7090058b4567",
    "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.
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	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.
role	Number	Yes	The new role of the user. These are the available roles: <ul style="list-style-type: none"><li>● 1 - Company Administrator.</li><li>● 2 - Network Administrator.</li><li>● 3 - Reporter.</li><li>● 4 - Partner.</li><li>● 5 - Custom. For this role, rights must be specified.</li></ul>
rights	Object	Yes	An object containing the rights of a user account. This object should be set only when <code>role</code> parameter has the value 5 - Custom. When set for

Parameter	Type	Optional	Description
			<p>other roles, the values will be ignored and replaced with the rights specific to that role. The available rights are:</p> <ul style="list-style-type: none"> <li>• manageCompanies</li> <li>• manageNetworks</li> <li>• manageUsers</li> <li>• manageReports</li> <li>• companyManager</li> </ul> <p>Setting this to True implies manageReports right to true</p> <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 Boolean: True when the user account has been successfully updated.

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "updateAccount",
  "params": {
    "accountId" : "585d3d3faaed70970e8b45ed",
    "email": "client@bitdefender.com",
    "profile": {
      "fullName": "Bitdefender User",
      "language": "en_US",
      "timezone": "Europe/Bucharest"
    }
  }
}
```

```
    },
    "password": "P@s4w0rd",
    "role": 5,
    "rights": {
      "manageNetworks": true,
      "manageReports": true,
      "manageUsers": false
    },
    "companyId": "58541613aaed7090058b4567",
    "targetIds": [
      "585d2dc9aaed70820e8b45b4",
      "585d2dd5aaed70b8048b45ca"
    ]
  }
}
```

### Response :

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

## 2.1.5. configureNotificationsSettings

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



### Note

This method may be accessed using an API key generated only by `Partner` and `Company Administrator` user accounts.

### Parameters

Parameter	Type	Optional	Description
accountId	String	Yes	The ID of the account for which the notification settings are

Parameter	Type	Optional	Description
			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 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> .
notificationsSettings	Array	Yes	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

Parameter	Type	Optional	Description
			<p>should have the following structure:</p> <ul style="list-style-type: none"><li>• type, the notification type,</li><li>• enabled, True if the notification is enabled, False otherwise,</li><li>• visibilitySettings, an object containing the visibility settings. For more information, refer to <a href="#">Notifications Visibility Options</a>,</li><li>• configurationSettings, notification specific configurations. This field depends on the notification type. For more information, refer to <a href="#">Relation Between Notification Type and configurationSettings</a>.</li></ul>

## Return value

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

## Example

### Request :

```
{
  "params": {
    "accountId": "55896b87b7894d0f367b23c8",
    "deleteAfter": 17,
    "includeDeviceName": true,
```

```
"includeDeviceFQDN": true,
"emailAddresses": ["example1@example.com"],
"notificationsSettings": [
  {
    "type" : 1,
    "enabled" : true,
    "visibilitySettings" : {
      "sendPerEmail" : true,
      "showInConsole" : true,
      "useCustomEmailDistribution": false
      "emails" : ["example2@example.com"]
    },
    "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.



### Note

This method may be accessed using an API key generated only by Partner and Company Administrator user accounts.



## 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

Relation between the company ID and the target IDs

This table shows possible combinations between `companyId` and `targetIds` default values, and how they affect creation of new user accounts.

companyId value	targetIds value	Result
Not set	Not set	The new account is linked to the same company and targets as the user who created the API key.
Not set	Valid IDs	The new account is linked to the same company as the user who created the API key, but it is able to access only the targets with the IDs specified in the <code>targetIds</code> parameter. Validations occur on targets.
Valid ID	Not set	The new account is linked to the company with the ID specified in the request. The target will be automatically set to the root of that company.
Valid ID	Valid IDs	The new account is linked to the company with the specified ID and it is able to access only the targets with the specified IDs. Validations occur on both company ID and target IDs.

## 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	<code>True</code> to display this notification in Control Center, <code>False</code> otherwise. If no value is specified it will be set to its previous value or <code>False</code> if a previous value was not set.
<code>sendPerEmail</code>	Yes	<p><code>True</code> to send this notification by email, <code>False</code> otherwise. If no value is specified it will be set to its previous value or <code>False</code> if a previous value was not set.</p> <p>This option will take effect only if a SMTP server is configured in the <b>Configuration</b> page of Bitdefender Control Center.</p>
<code>useCustomEmailDistribution</code>	Yes	<p><code>True</code> to send email notification to a custom emailing list, <code>False</code> otherwise. The notification will be sent by email to the distribution list only.</p> <p>If this option is set to <code>True</code> the <code>sendPerEmail</code> parameter must be specified and set to <code>True</code>.</p> <p>If no value is specified it will be set to its previous value or <code>False</code> if a previous value was not set.</p>
<code>emails</code>	Yes	A list of email addresses to receive the notification via email. When set, only these email addresses receive

Visibility option	Optional	Value
		the notification. When <code>useCustomEmailDistribution</code> is set to <code>True</code> , this list must contain at least one valid email address.



### 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"><li>• <code>useThreshold</code>, <b>boolean</b>, <code>True</code> to trigger this notification when the number of infected managed network objects exceeds a custom threshold, <code>False</code> otherwise</li><li>• <code>threshold</code>, <b>integer</b>, the percentage of managed network objects infected by the same malware. Valid values are between 1 and 100</li></ul>
2 - License Expires	<ul style="list-style-type: none"><li>• <code>receiveForChildCompany</code>, <b>boolean</b>, <code>True</code> to receive the notification for a child company, <code>False</code> otherwise</li></ul>
3 - License Usage Limit Has Been Reached	<ul style="list-style-type: none"><li>• <code>receiveForChildCompany</code>, <b>boolean</b>, <code>True</code> to receive the notification for a child company, <code>False</code> otherwise</li></ul>

Notification type	Available configurationSettings items with their type and possible values
4 - License Limit Is About To Be Reached	<ul style="list-style-type: none"> <li>● <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
5 - Update Available	<ul style="list-style-type: none"> <li>● <code>showConsoleUpdate</code>, <b>boolean</b>, <b>True</b> to receive the notification for console updates, <b>False</b> otherwise</li> <li>● <code>showPackageUpdate</code>, <b>boolean</b>, <b>True</b> to receive the notification for package updates, <b>False</b> otherwise</li> <li>● <code>showProductUpdate</code>, <b>boolean</b>, <b>True</b> to receive the notification for product updates, <b>False</b> otherwise</li> </ul>
9 - Exchange License Usage Limit Has Been Reached	<ul style="list-style-type: none"> <li>● <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
10 - Invalid Exchange User Credentials	<ul style="list-style-type: none"> <li>● <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
11 - Upgrade Status	The <code>configurationSettings</code> parameter should not be set for this notification.
13 - Authentication Audit	<ul style="list-style-type: none"> <li>● <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
17 - Antipshising Event	<ul style="list-style-type: none"> <li>● <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>

Notification type	Available configurationSettings items with their type and possible values
18 - Firewall Event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> </ul>
19 - ATC/IDS event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> </ul>
20 - User Control Event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> </ul>
21 - Data Protection Event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> </ul>
22 - Product Modules Event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> </ul>
23 - Security Server Status Event	<ul style="list-style-type: none"> <li>receiveForChildCompany, boolean, True to receive the notification for a child company, False otherwise</li> <li>notUpdated, boolean, True to receive the notification when the Security Server is outdated, False otherwise</li> <li>reboot, boolean, True to receive the notification when the Security Server needs a reboot, False otherwise</li> <li>stopped, boolean, True to receive the notification when the Security Server was powered off, False otherwise</li> </ul>

Notification type	Available configurationSettings items with their type and possible values
24 - Product Registration Event	<ul style="list-style-type: none"> <li>• <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
25 - Overloaded Security Server Event	<ul style="list-style-type: none"> <li>• <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> <li>• <code>useThreshold</code>, <b>boolean</b>, <b>True</b> to receive the notification when the scan load exceeds a custom threshold, <b>False</b> otherwise</li> <li>• <code>threshold</code>, <b>integer</b>, the minimum scan load necessary to issue this notification. Valid values are between 1 and 100</li> </ul>
26 - Task Status	<ul style="list-style-type: none"> <li>• <code>statusThreshold</code>, <b>integer</b>, the task status which triggers this notification. Set to 2 for any status, 3 for failed tasks</li> </ul>
27 - Outdated Update Server	<ul style="list-style-type: none"> <li>• <code>receiveForChildCompany</code>, <b>boolean</b>, <b>True</b> to receive the notification for a child company, <b>False</b> otherwise</li> </ul>
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.



**Note**

Notification types 32, 33, 34, 35 and 36 require an active Amazon EC2 integration with Bitdefender Control Center.

## 2.2. Companies

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

- `createCompany` : adds a new company.
- `deleteCompany` : deletes a company.
- `updateCompanyDetails` : updates company information, such as name or type.
- `getCompanyDetails` : retrieves the details of a company.
- `getCompanyDetailsByUser` : retrieves the details of the company linked to the specified user account.
- `findCompaniesByName` : retrieves all managed companies containing the specified string in their name.
- `suspendCompany` : disables access to Control Center for all user accounts of a company.
- `activateCompany` : activates a previously suspended company.

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

### 2.2.1. createCompany

This method creates a customer or partner company account.

The license type for the created company is TRIAL. 'Licensing' api can be used to change the license for the new company.

#### Parameters

Parameter	Type	Optional	Description
type	Number	No	The company type. Available values:

Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> <li>0 for Partner companies,</li> <li>1 for Customer companies.</li> </ul>
name	String	No	The company name. Must be unique.
parentId	String	Yes	The ID of the parent partner company.
address	String	Yes	The company's physical address.
phone	String	Yes	The company's phone number.
canBeManagedByAbove	Boolean	Yes	An option defining if the security of the new company can be managed by its Partner company. Available values: <code>true</code> or <code>false</code> . The default value is <code>true</code> .
accountEmail	String	Yes	The email for the new user account to be linked to the new company. If the parameter <code>canBeManagedByAbove</code> is set to <code>false</code> , the <code>accountEmail</code> parameter must be passed.
accountFullName	String	Yes	The full name of the new user account to be linked to the new company. This parameter is required when <code>canBeManagedByAbove</code> is set to <code>false</code> .
accountTimezone	String	Yes	The timezone of the new user account to be linked to the new company. The default value is <code>GMT (UTC)</code> .
accountLanguage	String	Yes	The user interface language for the new user account to be linked to the

Parameter	Type	Optional	Description
			new company. The default value is en_US.

## Return value

This method returns a String: the ID of the newly-created company.

## Example

### Request :

```
{
  "params": {
    "type": 1,
    "name": "Customer LTD",
    "parentId": "5518f5f3b1a43d357e7b23c6",
    "address": "Str Example No 1",
    "phone": "0040740000000",
    "canBeManagedByAbove": true,
    "accountEmail": "customer@example.com",
    "accountFullName": "Customer account"
  },
  "jsonrpc": "2.0",
  "method": "createCompany",
  "id": "e249c22c-0ada-4772-a9f1-ee1cbb322588"
}
```

### Response :

```
{
  "id": "e249c22c-0ada-4772-a9f1-ee1cbb322588",
  "jsonrpc": "2.0",
  "result": "5493dcd2b1a43df00b7b23c6"
}
```

## 2.2.2. deleteCompany

This method deletes a company.

## Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company to be deleted

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "companyId": "54a295d8b1a43d7c4a7b23c6",
  },
  "jsonrpc": "2.0",
  "method": "deleteCompany",
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0"
}
```

### Response :

```
{
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.2.3. updateCompanyDetails

This method updates the details of a partner or customer company.

## Parameters

Parameter	Type	Optional	Description
id	String	No	The ID of the company to be updated.
type	Number	Yes	The company type. Available values: <ul style="list-style-type: none"><li>0 for Partner companies,</li><li>1 for Customer companies.</li></ul> If not set, the company type will not be changed.
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.

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "id" : "5493dcd2b1a43df00b7b23c6",
    "type": 0,
    "name": "Customer to Partner 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
}
```

## 2.2.4. getCompanyDetails

This method retrieves the details of a company.

### Parameters

Parameter	Type	Optional	Description
companyId	String	Yes	The company's ID. The default value is the ID of the company linked to the user who generated the API key.

### Return value

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

- `type` - the company type: 0 for Partner, 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
- `isSuspended` - company account status: `true`, if the company is suspended

### Example

**Request :**

```
{
  "params": {
    "companyId" : "5493dcd2b1a43df00b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "getCompanyDetails",
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810"
}
```

### Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": {
    "type": 0,
    "name": "Customer to Partner LTD",
    "id": "54aeab40b1a43dc0467b23e9",
    "address": "Str Example No 1",
    "phone": "0040740000001",
    "canBeManagedByAbove": true,
    "isSuspended": false
  }
}
```

## 2.2.5. getCompanyDetailsByUser

This method retrieves the details of a company linked to an account identified through the given username and password.

### Parameters

Parameter	Type	Optional	Description
username	String	No	The username linked to the referred company.
password	String	No	The password linked to the referred company.

## Return value

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

- `type` - the company type: 0 for Partner, 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
- `isSuspended` - company account status: true, if the company is suspended

## Example

### Request :

```
{
  "params": {
    "username": "partner@bitdefender.com",
    "password": "password"
  },
  "jsonrpc": "2.0",
  "method": "getCompanyDetailsByUser",
  "id": "6435c228-73b0-4e72-9a2a-8716cc58c883"
}
```

### Response :

```
{
  "id": "6435c228-73b0-4e72-9a2a-8716cc58c883",
  "jsonrpc": "2.0",
  "result": {
    "type": 0,
    "name": "Test partner",
    "id": "550ac840b1a43da64d7b23c6",
  }
}
```



```
    "address": "Str Example No 1",  
    "phone": "0040740000001",  
    "canBeManagedByAbove": true,  
    "isSuspended": false  
  }  
}
```

## 2.2.6. findCompaniesByName

This method searches for all managed companies containing the specified string in their name.

### Parameters

Parameter	Type	Optional	Description
nameFilter	String	No	The string to be searched in the company 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.

### Return value

This method returns an Array containing company objects whose names contain the given search criteria. The size of the returned array is limited to 25 entries. Each entry in the array has the following structure:

- `type` - the company type: 0 for Partner, 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

- `isSuspended` - company account status: true, if the company is suspended

## Example

### Request :

```
{
  "params": {
    "nameFilter": "Test"
  },
  "jsonrpc": "2.0",
  "method": "findCompaniesByName",
  "id": "ae037403-7947-4f2b-b0b2-af190a8b44eb"
}
```

### Response :

```
{
  "id": "ae037403-7947-4f2b-b0b2-af190a8b44eb",
  "jsonrpc": "2.0",
  "result": [{
    "type": 1,
    "name": "Test customer",
    "id": "55191c7ab1a43d1f107b23c7",
    "address": "Str Example No 1",
    "phone": "0040740000001",
    "canBeManagedByAbove": true,
    "isSuspended": false
  },
  {
    "type": 0,
    "name": "Test partner",
    "id": "55191c5fb1a43da8107b23c6",
    "address": "Str Example No 2",
    "phone": "0040740000002",
    "canBeManagedByAbove": true,
    "isSuspended": false
  }
]
```

## 2.2.7. suspendCompany

This method suspends an active company account, with the following implications:

- The company's users will no longer be able to log in to GravityZone Control Center.
- The agents on endpoints directly managed by the suspended company will expire.

### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company to be suspended.

### Return value

This method does not return any value.

### Example

#### Request :

```
{
  "params": {
    "companyId" : "5493dcd2b1a43df00b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "suspendCompany",
  "id": "8f6748b9-d201-4b63-b17f-4ecbebbece24a9"
}
```

#### Response :

```
{
  "id": "8f6748b9-d201-4b63-b17f-4ecbebbece24a9",
  "jsonrpc": "2.0",
  "result": null
}
```

### 2.2.8. activateCompany

This method activates a suspended company.

#### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company to be activated.

#### Return value

This method does not return any value.

#### Example

##### Request :

```
{
  "params": {
    "companyId" : "5493dcd2b1a43df00b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "activateCompany",
  "id": "c67860e2-36cc-43bd-bc0f-f1061c180b52"
}
```

##### Response :

```
{
  "id": "c67860e2-36cc-43bd-bc0f-f1061c180b52",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.3. Licensing

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

- `getLicenseInfo` : retrieves the license information for a company.
- `setMonthlySubscription` : enables the monthly subscription 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.

API url: [CONTROL\\_CENTER\\_APIS\\_ACCESS\\_URL/v1.0/jsonrpc/licensing](CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/licensing)

### 2.3.1. getLicenseInfo

This method retrieves the license information for a company.

#### Parameters

Parameter	Type	Optional	Description
<code>companyId</code>	String	Yes	The ID of the company for which the license information is retrieved. The default value is the ID of the user's company.

#### 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 inherited monthly 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 licensed subscription.
- `manageExchange` - True if the company is allowed to manage exchange, false otherwise

## Example

### Request :

```
{
  "params": {
    "companyId": "5493dcd2b1a43df00b7b23c6"
  },
  "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
  }
}
```

## 2.3.2. setMonthlySubscription

This method enables monthly subscription for a company.

### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company that will inherit license seats from the parent company.
reservedSlots	Number	Yes	The number of seats to be reserved from the parent's company total amount of seats. If no value is passed, the number of

Parameter	Type	Optional	Description
			reserved seats is not restricted unless a number of seats was previously reserved.
manageExchange	Boolean	Yes	True for allowing the company to manage Exchange, false otherwise. If no value is passed, the default value is true.

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "companyId" : "5493dcd2b1a43df00b7b23c6",
    "reservedSlots" : 12,
    "manageExchange": false
  },
  "jsonrpc": "2.0",
  "method": "setMonthlySubscription",
  "id": "d4d50719-3215-455a-a329-086fe77f6d72"
}
```

### Response :

```
{
  "id": "2b5f52d8-5f6f-466c-b952-61b5c87c3182",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.3.3. setLicenseKey

This method sets the license key for a company.

## Parameters

Parameter	Type	Optional	Description
licenseKey	String	No	The license key to be set.
companyId	String	Yes	The ID of the company whose license will be set. If no value is passed, the user's company will be selected.

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "licenseKey" : "TNB3AAA",
    "companyId" : "5493dcd2b1a43df00b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "setLicenseKey",
  "id": "48daf1bc-4078-411c-bf44-4f293e68f501"
}
```

### Response :

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

## 2.3.4. getMonthlyUsage

This method exposes the monthly usage for a company in a target month.



## Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company
targetMonth	String	No	The month for which the usage is returned. It should have the following format: mm/yyyy

## Return value

This method returns an Object containing the number of license seats used by the target company in a specified month:

- `endpointMonthlyUsage` - the monthly usage for endpoints. The method returns an error if the queried company does not have a monthly license.
- `exchangeMonthlyUsage` - the monthly usage for mail boxes. The method returns an error if the queried company does not have a monthly license.

## Example

### Request :

```
{
  "params": {
    "targetMonth": "03/2015",
    "companyId": "55115935b1a43dcc4a7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "getMonthlyUsage",
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4"
}
```

### Response :

```
{
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
  "jsonrpc": "2.0",
  "result": {
    "endpointMonthlyUsage": 101,
  }
}
```

```
        "exchangeMonthlyUsage": 15
    }
}
```

## 2.4. Network

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

- `getCompaniesList` : returns the list of companies under a parent company or from a company folder.
- `getCompanyFoldersList` : returns the list of company folders under a company or under a company folder.
- `createCompanyFolder` : creates a new folder under an existing folder or company.
- `deleteCompanyFolder` : deletes a company folder.
- `moveCompanyOrCompanyFolder` : moves a company or company folder under a parent company or company folder.
- `getEndpointsList` : returns the list of endpoints under the specified company or group.
- `getManagedEndpointDetails` : returns the properties of the specified endpoint.
- `createCustomGroup` : creates a new group under an existing one or under a company's **Computers and Groups**.
- `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.
- `getRootContainers` : returns the root containers for a company. Available root containers include **Companies, Network, Computers and Groups, Deleted**.

- `createScanTask` : launches a scan task on the specified endpoints or groups. The available scan types are: Quick Scan, Full Scan and Memory Scan.
- `getScanTasksList` : returns the list of scan tasks.

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

### 2.4.1. getCompaniesList

This method returns the list of companies under a parent company or from a company folder.

#### Parameters

Parameter	Type	Optional	Description
parentId	String	Yes	The parent company's ID or the company folder's ID. The default value is the ID of the parent company.

#### Return value

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

- `id` - the ID of the company
- `name` - the name of the company

#### Example

##### Request :

```
{
  "params": {
    "parentId" : "54a28b41b1a43d89367b23fd"
  },
  "jsonrpc": "2.0",
  "method": "getCompaniesList",
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a"
}
```

##### Response :

```
{
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a",
  "jsonrpc": "2.0",
  "result": [
    {
      "id": "54a295eeb1a43d8b497b23c6",
      "name": "Customer Company"
    },
    {
      "id": "54a295d8b1a43d7c4a7b23c6",
      "name": "Partner Company"
    }
  ]
}
```

### 2.4.2. getCompanyFoldersList

This method returns the list of company folders under a company or under a company folder.

#### Parameters

Parameter	Type	Optional	Description
parentId	String	Yes	The parent company's ID or the parent folder's ID. The default value is the ID of the parent company.

#### Return value

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

- `id` - the ID of the folder
- `name` - the name of the folder

#### Example

##### Request :

```
{
  "params": {
    "parentId" : "54a295d8b1a43d7c4a7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "getCompanyFoldersList",
  "id": "8edf135b-f7cb-41f2-8b67-98054694f61e"
}
```

### Response :

```
{
  "id": "8edf135b-f7cb-41f2-8b67-98054694f61e",
  "jsonrpc": "2.0",
  "result": [
    {
      "id" : "54a29726b1a43d8a497b23c6",
      "name" : "Company folder 1"
    },
    {
      "id" : "54a29746b1a43d0f4c7b23c6",
      "name" : "Company folder 2"
    }
  ]
}
```

### 2.4.3. createCompanyFolder

This method creates a new folder under an existing folder or company.

#### Parameters

Parameter	Type	Optional	Description
folderName	String	No	The name for the new folder.
parentId	String	Yes	The ID of the parent company or folder (if the case). The default value is the ID of the parent company.

## Return value

This method returns a String: the ID of the newly-created folder.

## Example

### Request :

```
{
  "params": {
    "parentId": "54a295d8b1a43d7c4a7b23c6",
    "folderName" : "Company folder 3"
  },
  "jsonrpc": "2.0",
  "method": "createCompanyFolder",
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0"
}
```

### Response :

```
{
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0",
  "jsonrpc": "2.0",
  "result": "54a298c5b1a43d0c4c7b23c7"
}
```

## 2.4.4. deleteCompanyFolder

This method deletes a company folder.

### Parameters

Parameter	Type	Optional	Description
folderId	String	No	The ID of the company folder to be deleted

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "folderId": "54a295d8b1a43d7c4a7b23c6",
  },
  "jsonrpc": "2.0",
  "method": "deleteCompanyFolder",
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0"
}
```

### Response :

```
{
  "id": "f5911ea2-9f14-4046-96eb-5fa24cca98f0",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.4.5. moveCompanyOrCompanyFolder

This method moves a company or company folder under a parent company or company folder.

### Parameters

Parameter	Type	Optional	Description
id	String	No	The ID of the company or company folder to be moved
newParentId	String	No	The ID of the new parent company of company folder.

### Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "newParentId" : "54a29746b1a43d0f4c7b23c6",
    "id" : "54a298c5b1a43d0c4c7b23c7"
  },
  "jsonrpc": "2.0",
  "method": "moveCompanyOrCompanyFolder",
  "id": "7d2864e9-c67b-48a2-9ba3-0a11d47e83c8"
}
```

### Response :

```
{
  "id": "7d2864e9-c67b-48a2-9ba3-0a11d47e83c8",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.4.6. getEndpointsList

This method returns the list of endpoints.

### Parameters

Parameter	Type	Optional	Description
parentId	String	Yes	The ID of the target company or group. If not specified, the method returns the endpoints under <b>Computers and Groups</b> .
isManaged	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.



Parameter	Type	Optional	Description
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 30 items per page. Default value: 30 items per page.

## 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,
  - `machineType`, the type of the machine: (1 - computer, 2 - virtual machine, 3 - EC2 Instance, 0 - Other)

## Example

### Request :

```
{
  "params": {
    "parentId": "23b19c39b1a43d89367b32ce",
    "page": 2,
    "perPage": 5
  },
  "jsonrpc": "2.0",
  "method": "getEndpointsList",
  "id": "301f7b05-ec02-481b-9ed6-c07b97de2b7b"
```

```
}
```

**Response :**

```
{
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a",
  "jsonrpc": "2.0",
  "result": {
    page: 2,
    pageCount: 11,
    perPage: 5,
    total: 54
    items[
      {
        "id" : "21a295eeb1a43d8b497b23b7",
        "name" : "Endpoint 1",
        "machineType": 1,
      },
      {
        "id" : "23a295d8b1a43d7c4a7b23c9",
        "name" : "Endpoint 2",
        "machineType": 2,
      }
    ]
  }
}
```

### 2.4.7. getManagedEndpointDetails

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

#### Parameters

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

## Return value

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

- `id` - the ID of managed endpoint
- `name` - the name of the endpoint
- `operatingSystem` - the Operating System of the endpoint
- `state` - the power state of the machine: 1 - online, 2 - offline, 3 - suspended; 0 - unknown.
- `ip` - the IP of the endpoint
- `lastSeen` - the date of the last synchronization with Control Center
- `machineType` - the type of the machine: 1 - computer, 2 - virtual machine, 3 - EC2 Instance, 0 - Other
- `agent` - an object with the agent information installed on the endpoint.

### Object description:

- `engineVersion`, the version of the engine
- `primaryEngine`, can be 1 (for Central Scanning (Security Server)), 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)); 0 Unknown
- `fallbackEngine`, can be 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)); 0 Unknown
- `lastUpdate`, the last update of the signatures
- `licensed`, the status of the license: 0 - pending authentication, 1 - active license, 2 - expired license, 6 - there is no license or not applicable
- `productOutdated`, specifies if the product is outdated
- `productUpdateDisabled`, specifies if product updates are disabled
- `productVersion`, the version of the product
- `signatureOutdated`, specifies if the signatures of the endpoint are outdated

- `signatureUpdateDisabled`, specifies if the signature updates are disabled
- `type`, the type of the endpoint. It can be:
  - 1 - Endpoint Security,
  - 2 - Bitdefender Tools,
  - 3 - BEST.
- `group` - an object that indicates the group which the endpoint is part of, containing the following information:
  - `id`, the id of the group
  - `name`, the name of the group
- `malwareStatus` - information about the malware detected on the endpoint, containing:
  - `detection`, if there is any malware detection on the endpoint,
  - `infected`, if the endpoint is infected
- `policy` - object, information about the active policy on the endpoint. The object contains:
  - `id`, the ID of the active policy,
  - `name`, the name of the policy,
  - `applied`, true if the policy is applied
- `modules` - object, the modules and their status; Possible keys are: `advancedThreatControl`, `antimalware`, `contentControl`, `deviceControl`, `firewall`, `powerUser`. The values are true, if the module is enabled or false, if the module is not enabled.

## Example

### Request :

```
{
  "params": {
    "endpointId" : "54a28b41b1a43d89367b23fd"
  },
}
```

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

## Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": {
    'id': '54a28b41b1a43d89367b23fd',
    'name': 'WIN-TGQDU499RS4',
    'operatingSystem': 'Windows Server 2008 R2 Datacenter',
    'state': 1,
    'ip': '10.10.24.154',
    'lastSeen': '2015-06-22T13:46:59',
    'machineType': 1,
    'agent': {
      'engineVersion': '7.61184',
      'primaryEngine': 1,
      'fallbackEngine': 2,
      'lastUpdate': '2015-06-22T13:40:06',
      'licensed': 1,
      'productOutdated': False,
      'productUpdateDisabled': False,
      'productVersion': '6.2.3.569',
      'signatureOutdated': False,
      'signatureUpdateDisabled': False,
      'type': 3
    },
    'group': {
      'id': '5575a235d2172c65038b456d',
      'name': 'Custom Groups'
    },
    'malwareStatus': {
      'detection': False,
      'infected': False
    },
    'modules': {
```

```
        'advancedThreatControl': False,
        'antimalware': True,
        'contentControl': False,
        'deviceControl': False,
        'firewall': False,
        'powerUser': False
    },
    'policy': {
        'id': '5121da426803fa2d0e000017',
        'applied': True,
        'name': 'Default policy'
    }
}
```

## 2.4.8. 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 group or parent company. If the parentId refers to a company, the new group is created under the 'Computers and Groups' group of that company. The user's company is automatically selected if no value is passed for this parameter.

### 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"
}
```

## 2.4.9. 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
}
```

## 2.4.10. 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 or a company ID.

### 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"
    }
  ]
}
```

## 2.4.11. 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

Parameter	Type	Optional	Description
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
}
```

## 2.4.12. 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
}
```

## 2.4.13. 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
}
```

## 2.4.14. getRootContainers

This method returns the root containers for a company. A root container refers to special groups, such as: **Companies, Network, Computers and Groups**

## Parameters

Parameter	Type	Optional	Description
companyId	String	Yes	The ID of the company for which the method will return the root containers. If null, the id of company linked to the API access key will be considered.

## Return value

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

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

## Example

### Request :

```
{
  "params": {
    "companyId": "559bd17ab1a43d241b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "getRootContainers",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

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

```

```
        "id" : "5582d3b3b1a43d897f7b23c8",  
        "name" : "Network"  
    }  
]  
}
```

## 2.4.15. 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
name	String	Yes	The name of the task. If the parameter is not passed, the name will be automatically generated.

### Return value

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

### Example

#### Request :

```
{  
  "params": {  
    "targetIds": ["559bd17ab1a43d241b7b23c6",  
                  "559bd17ab1a43d241b7b23c7"],  
    "type": 1,  
    "name": "my scan"  
  },  
  "jsonrpc": "2.0",  
}
```

```
"method": "createScanTask",  
"id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"  
}
```

**Response :**

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

## 2.4.16. 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 30 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,
```



```
    pageCount: 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'
      },
    ]
  }
}
```

## 2.5. Packages

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

- `getInstallationLinks` : returns the installation links available for managed companies.
- `createPackage` : creates a new package and returns its ID.
- `getPackagesList` : returns the list of available packages.

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

### 2.5.1. getInstallationLinks

This method returns the installation links available for managed companies.

## Parameters

Parameter	Type	Optional	Description
companyId	String	Yes	The ID of the managed company. If no value is passed, the installation links available for all managed companies will be returned.
packageName	String	Yes	The name of the package. If no value is passed, all packages will be listed.

## Return value

This method returns an Array containing the list of installation links for each available package. Each entry in the list has the following fields:

- `packageName` - the name of the package
- `companyName` - the name of the company the package belongs to
- `companyId` - the ID of the company the package belongs to
- `installLinkWindows` - the installation link for Windows operating systems
- `installLinkMac` - the installation link for MAC operating systems
- `installLinkLinux` - the installation link for Linux operating systems

## Example

### Request :

```
{
  "params": {
    "companyId": "54a1a1d3b1a43d2b347b23c1",
    "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/EPC/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"
  }]
}
```

## 2.5.2. createPackage

This method creates an installation package.

### Parameters

Parameter	Type	Optional	Description
packageName	String	No	The name of the package.
companyId	String	No	The ID of the company.
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.
modules	Object	Yes	An object with the modules to be enabled/disabled. The keys can be: atc, firewall, contentControl, deviceControl, powerUser. The values can be 1 (enabled) or 0

Parameter	Type	Optional	Description
			(disabled). If the module is not sent, it will be considered disabled.
scanMode	Object	Yes	<p>An object with the scan mode settings.</p> <p>Object description:</p> <ul style="list-style-type: none"> <li>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).</li> <li>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>.</li> <li>The values for <code>main</code> can be 1 (for Central Scanning (Security Server)), 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)).</li> <li>The values for <code>fallback</code> can be 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)). If the value for <code>main</code> option is 2 or 3, the value of <code>fallback</code> will not be considered.</li> <li>The <code>main</code> option for <code>ec2</code> can be only 1 (for Central Scanning (Security Server)).</li> <li>If this parameter is not sent, the values for automatic mode are saved.</li> </ul>
settings	Object	Yes	<p>An object with other settings of the package. The values can be <code>scanBeforeInstall</code>, <code>uninstallPassword</code>, and <code>customInstallationPath</code>. The value for <code>scanBeforeInstall</code> can be 1 (enabled) or 0</p>

Parameter	Type	Optional	Description
			(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). All the values are optional.

## Return value

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

## Example

### Request :

```
{
  "params": {
    "packageName": "a unique name",
    "companyId": "54a1a1d3b1a43d2b347b23c1",
    "description": "package description",
    "language": "en_EN",
    "modules": {
      "atc": 1,
      "firewall": 0,
      "contentControl": 1,
      "deviceControl": 0,
      "powerUser": 0
    },
    "scanMode": {
      "type": 2,
      "computers": {"main": 1, "fallback": 2},
      "vms": {"main": 2},
      "ec2": {"main": 1, "fallback": 2}
    }
  },
}
```

```
"settings": {
  "uninstallPassword": "mys3cre3tP@assword",
  "scanBeforeInstall": 0,
  "customInstallationPath": "c:\\mypath\\bitdefender"
},
"jsonrpc": "2.0",
"method": "getInstallationLinks",
"id": "426db9bb-e92a-4824-a21b-bba6b62d0a18"
}
```

### Response :

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

### 2.5.3. getPackagesList

Returns the list of available packages.

#### Parameters

Parameter	Type	Optional	Description
companyId	String	Yes	The ID of the company for which the packages list is retrieved. The default value is the company of the user who has generated the API key. If not passed, the packages available to the company are returned.

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 30 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
      }
    ]
  }
}
```

## 2.6. Policies

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

- `getPoliciesList` : retrieves the list of available security policies related to a company.
- `getPolicyDetails` : retrieves the settings of a security policy.

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

### 2.6.1. getPoliciesList

This method retrieves the list of policies available for a company.



## Parameters

Parameter	Type	Optional	Description
companyId	String	Yes	The ID of the company for which the policies are retrieved. The default value is the company of the user who has generated the API key. If not passed, the policies available to the company are returned.
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 30 items per page. Default value: 30 items per page.

## Return value

This method returns an Array containing policy objects with the policies available to the specified company. 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 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": {
    "companyId": "55896b87b7894d0f367b23c6",
    "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.), for a specified company and month.
- [configureAmazonEC2Integration](#) : configures the Amazon EC2 integration for a company, using the provided access keys.
- [disableAmazonEC2Integration](#) : disables the previously configured Amazon EC2 integration.
- [getCompanyDetailsByAWSAccountId](#) : retrieves information regarding the managed companies that have configured the Amazon EC2 integration with a specific AWS account.

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.), for a specified company and month.

#### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company

Parameter	Type	Optional	Description
targetMonth	String	No	The month for which the usage is returned. The month will be provided in the following format: mm/yyyy

## Return value

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

## Example

### Request :

```
{
  "params": {
    "targetMonth": "03/2015",
    "companyId": "55115935b1a43dcc4a7b23c6"
  },
  "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. configureAmazonEC2Integration

This method configures the Amazon EC2 integration for a company, using the provided access keys.

### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the target company
keyId	String	No	The key ID
keySecret	String	No	The secret key

### Return value

This method does not return any value.

### Example

#### Request :

```
{
  "params": {
    "keyId": "AKIAIHEBSE2JFZ6CAAAA",
    "keySecret": "rTEuYBJXA9Wnm6I6CQKBJ30DqVUOz4NiVbeDRg2O",
    "companyId": "55115935b1a43dcc4a7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "configureAmazonEC2Integration",
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46"
}
```

#### Response :

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

```
}
```

### 2.7.3. disableAmazonEC2Integration

This method disables the previously configured Amazon EC2 integration.

#### Parameters

Parameter	Type	Optional	Description
companyId	String	No	The ID of the company

#### Return value

This method does not return any value.

#### Example

##### Request :

```
{
  "params": {
    "companyId": "55115935b1a43dcc4a7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "disableAmazonEC2Integration",
  "id": "97114e95-f36b-4206-bca0-6fb41bb47575"
}
```

##### Response :

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

### 2.7.4. getCompanyDetailsByAWSAccountId

This method retrieves information regarding the managed companies that have configured the Amazon EC2 integration with a specific AWS account.

#### Parameters

Parameter	Type	Optional	Description
accountId	String	No	The ID of the AWS account

#### Return value

This method returns an Array containing the companies that have the AWS integration configured with the specified AWS account. The size of the returned list is limited to 25 entries. Each entry has the following structure:

- `type` - company type: 0 for Partner, 1 for Customer
- `name` - the name of the company
- `id` - the ID of the company
- `address` - the physical 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
- `isSuspended` - company account status: `true`, if the company is suspended

#### Example

##### Request :

```
{
  "params": {
    "accountId": "123456789012"
  },
  "jsonrpc": "2.0",
  "method": "getCompanyDetailsByAWSAccountId",
  "id": "ae037403-7947-4f2b-b0b2-af190a8b44eb"
```



```
}
```

**Response :**

```
{
  "id": "ae037403-7947-4f2b-b0b2-af190a8b44eb",
  "jsonrpc": "2.0",
  "result": [{
    "type": 1,
    "name": "Test customer",
    "id": "55191c7ab1a43d1f107b23c7",
    "address": "Str Example No 1",
    "phone": "0040740000001",
    "canBeManagedByAbove": true,
    "isSuspended": false
  },
  {
    "type": 0,
    "name": "Test partner",
    "id": "55191c5fb1a43da8107b23c6",
    "address": "Str Example No 2",
    "phone": "0040740000002",
    "canBeManagedByAbove": true,
    "isSuspended": false
  }
]
```

## 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](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	<p>The type of report. One of the following values can be passed:</p> <ul style="list-style-type: none"><li>• 1 - Antiphishing Activity</li><li>• 2 - Blocked Applications</li><li>• 3 - Blocked Websites</li><li>• 4 - Customer Status Overview</li><li>• 5 - Data Protection</li><li>• 6 - Device Control Activity</li><li>• 7 - Endpoint Modules Status</li><li>• 8 - Endpoint Protection Status</li><li>• 9 - Firewall Activity</li><li>• 10 - License Status</li><li>• 11 - Malware Activity</li><li>• 12 - Malware Status</li><li>• 13 - Monthly License Usage</li><li>• 14 - Network Status</li><li>• 15 - On demand scanning</li></ul>

Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> <li>• 16 - Policy Compliance</li> <li>• 17 - Security Audit</li> <li>• 18 - Security Server Status</li> <li>• 19 - Top 10 Detected Malware</li> <li>• 20 - Top 10 Infected Companies</li> <li>• 21 - Top 10 Infected Endpoints</li> <li>• 22 - Update Status</li> <li>• 23 - Upgrade Status</li> <li>• 24 - AWS Monthly Usage</li> </ul>
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 can be only the ID of the user's company or IDs of child companies:</p> <ul style="list-style-type: none"> <li>• Customer Status Overview</li> <li>• License Status</li> <li>• Monthly License Usage</li> <li>• AWS Monthly Usage</li> <li>• Top 10 Infected Companies</li> </ul> <p>For the other report types, the target ID can be of any type: group, company, 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 <a href="#">scheduledInfo</a> object.</p>

Parameter	Type	Optional	Description
<code>options</code>	Object	Yes	<p>The object that defines the options for creating the report. For these reports, the <code>options</code> object should not be set:</p> <ul style="list-style-type: none"> <li>• Endpoint Modules Status</li> <li>• License Status</li> <li>• Policy Compliance</li> <li>• Security Server Status</li> <li>• Upgrade Status</li> </ul> <p>For more information, please check the details of the <a href="#">options</a> object.</p>
<code>emailsList</code>	Array	Yes	<p>A list of emails where to deliver the report. <code>emailsList</code> should not be set for an instant report.</p>

## Objects

### `scheduledInfo`

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

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

Name	Type	Description
<code>occurrence</code>	integer	<p>The member is mandatory.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>– 1 - for an instant report</li> <li>– 2 - for hourly report</li> <li>– 3 - for daily report</li> <li>– 4 - for weekly report</li> <li>– 5 - for monthly report</li> </ul>

Name	Type	Description
		<ul style="list-style-type: none"> <li>– 6 - for yearly report</li> </ul> <p>For 13 - Monthly License Usage and 24 - AWS Monthly 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 occurrence has the value 2.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>– Any integer between 1 and 24, representing the interval (in hours) at which the report will run.</li> </ul>
startHour	integer	<p>The member should be set only if occurrence has the value 3, 4 or 5.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>– Any integer between 0 and 23.</li> </ul>
startMinute	integer	<p>The member should be set only if occurrence has the value 3, 4 or 5.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>– Any integer between 0 and 59.</li> </ul>
days	array	<p>The member should be set only if occurrence has the value 4.</p> <p>Possible values of the array elements:</p> <ul style="list-style-type: none"> <li>– Integers between 0 and 6, representing the days of the week, from 0 - Sunday to 6 - Saturday.</li> </ul>
day	integer	<p>The member should be set only if occurrence has the value 5 or 6.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>– An integer between 1 and 31, representing the day of the month.</li> </ul>

Name	Type	Description
month	integer	<p>The member should be set only if <code>occurrence</code> has the value 6.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>– An integer between 1 and 12, representing the month of the year.</li></ul>

## options

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

- **Antiphishing Activity**

The object must contain these members:

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

- **Blocked Applications**

The object must contain these members:

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

- **Blocked Websites**

The object must contain these members:

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

- **Customer Status Overview**

The object must contain these members:

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

- **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 <a href="#">Relation between reporting interval and recurrence</a>

Name	Type	Description
filterType	integer	The member is mandatory. Possible values: <ul style="list-style-type: none"><li>– 0 - All endpoints</li><li>– 1 - Only managed computers with blocked threats</li></ul>
blockedEmails	boolean	The member should be set only if filterType has the value 1. Possible values: <ul style="list-style-type: none"><li>– True</li><li>– False</li></ul>
blockedWebsites	boolean	The member should be set only if filterType has the value 1. Possible values: <ul style="list-style-type: none"><li>– True</li><li>– False</li></ul>

- **Device Control Activity**

The object must contain these members:

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

- **Endpoint Protection Status**

The object must contain these members:



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

- **Firewall Activity**

The object must contain these members:

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

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

## ● Malware Activity

The object must contain these members:

Name	Type	Description
reportingInterval	integer	This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a>
filterType	integer	The member is mandatory. Possible values: – 0 - All endpoints – 1 - Only endpoints with unresolved malware

### ● Malware Status

The object must contain these members:

Name	Type	Description
reportingInterval	integer	The member is mandatory. This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a>
filterType	integer	The member is mandatory. Possible values: – 0 - All endpoints – 1 - Only endpoints still infected

### ● 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 <a href="#">Relation between reporting interval and recurrence</a>

- **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 <a href="#">Relation between reporting interval and recurrence</a>

- **Network Status**

The object must contain these members:

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

- **On demand scanning**

The object must contain these members:

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

- **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 <a href="#">Relation between reporting interval and recurrence</a>

- **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 <a href="#">Relation between reporting interval and recurrence</a>

- **Top 10 Infected Companies**

The object must contain these members:

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

- **Top 10 Infected Endpoints**

The object must contain these members:

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

## ● Update Status

The object must contain these members:

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

## ● VM Network Protection Status

The object must contain these members:

Name	Type	Description
filterType	integer	The member is mandatory.

Name	Type	Description
		Possible values: <ul style="list-style-type: none"><li>– 0 - All endpoints</li><li>– 1 - Only protected endpoints</li></ul>

**Important**

The object should not be set for these reports:

- **Endpoint Modules Status**
- **License Status**
- **Upgrade Status**
- **Policy Compliance**
- **Security Server Status**

## Relation between reporting interval and recurrence

occurrence	reportingInterval
2 - Hourly report	Possible values: <ul style="list-style-type: none"><li>– 0 - Today</li></ul>
3 - Daily report	Possible values: <ul style="list-style-type: none"><li>– 0 - Today</li><li>– 1 - Last day</li><li>– 2 - This Week</li></ul>
4 - Weekly report	Possible values: <ul style="list-style-type: none"><li>– 0 - Today</li><li>– 1 - Last day</li><li>– 2 - This Week</li><li>– 3 - Last Week</li></ul>



occurrence	reportingInterval
	<ul style="list-style-type: none"> <li>– 4 - This Month</li> </ul> <p>For 13 - Monthly License Usage and 24 - AWS Monthly Usage reports the possible value is only 4 - This Month.</p>
5 - Monthly report	<p>Possible values:</p> <ul style="list-style-type: none"> <li>– 0 - Today</li> <li>– 1 - Last day</li> <li>– 2 - This week</li> <li>– 3 - Last week</li> <li>– 4 - This month</li> <li>– 5 - Last month</li> <li>– 6 - Last 2 months</li> <li>– 7 - Last 3 months</li> <li>– 8 - This year</li> </ul> <p>For 13 - Monthly License Usage and 24 - AWS Monthly 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"> <li>– 8 - This year</li> <li>– 9 - Last year</li> </ul>

## 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"><li>• 1 - Antiphishing Activity</li><li>• 2 - Blocked Applications</li><li>• 3 - Blocked Websites</li><li>• 4 - Customer Status Overview</li><li>• 5 - Data Protection</li><li>• 6 - Device Control Activity</li><li>• 7 - Endpoint Modules Status</li><li>• 8 - Endpoint Protection Status</li></ul>

Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> <li>9 - Firewall Activity</li> <li>10 - License Status</li> <li>11 - Malware Activity</li> <li>12 - Malware Status</li> <li>13 - Monthly License Usage</li> <li>14 - Network Status</li> <li>15 - On demand scanning</li> <li>16 - Policy Compliance</li> <li>17 - Security Audit</li> <li>18 - Security Server Status</li> <li>19 - Top 10 Detected Malware</li> <li>20 - Top 10 Infected Companies</li> <li>21 - Top 10 Infected Endpoints</li> <li>22 - Update Status</li> <li>23 - Upgrade Status</li> <li>24 - AWS Monthly Usage</li> </ul>
page	Number	Yes	The results page number. Default page number is 1.
perPage	Number	Yes	The number of items displayed in a page. The upper limit is 30 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 a an empty string. For more information, refer to [1.3 Authentication](#) section for details.

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



### Note

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

## Example

### Request :

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

**Response :**

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

## 3. API USAGE EXAMPLES

The following API usage examples make use of the following generated API key: "UjlMS+0m1l9IUZjppjWyJG8gbnv2Mta4T".

### 3.1. C# Example

In the following example, we will create a company using C#.

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

String apiURL =
    "https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/";

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

String apiKey = "UjlMS+0m1l9IUZjppjWyJG8gbnv2Mta4T";
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["type"] = 1;
parameters["name"] = "Test Company";
parameters["address"] = @"23rd Fictional Street,
    Hidden Town, Invisible Land";
parameters["phone"] = "+990000000000";
parameters["canBeManagedByAbove"] = true;

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

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

```
if (response.Result != null) {  
    JToken result = response.Result;  
    Console.WriteLine(response.ToString());  
}  
  
// Output:  
// 54b646a0b1a43dbd197b23c6
```

## 3.2. curl Example

In the following example, we get information about all our managed companies using curl.

```
curl -i \  
-H "Authorization: \  
Basic VWpsTVMrMG0xbDlJVVPqcGpXeUpHOGdibnYyTXRhNFQ6" \  
-H "Content-Type: application/json" \  
-d '{"id": "123456789", "jsonrpc": "2.0",  
"method": "getCompaniesList", "params": []}' \  
-X POST \  
https://cloud.gravityzone.bitdefender.com/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": "54b646a0b1a43dbd197b23c6",  
      "name": "Test Company"  
    }  
  ]  
}
```

### 3.3. Python Example

Now, we will query the details of a company with Python.

```
import base64
import pyjsonrpc
import requests
import simplejson

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

json = pyjsonrpc.create_request_json("getCompanyDetails",
    companyId="54b646a0b1a43dbd197b23c6")
result = requests.post(
    "https://cloud.gravityzone.bitdefender.com/ \
    api/v1.0/jsonrpc/companies",
    json,
    verify=False,
    headers = {
        "Content-Type": "application/json",
        "Authorization": authorizationHeader
    })

jsonResult = simplejson.loads(result.content)

print jsonResult
```

Output:

```
{u'jsonrpc': u'2.0',
u'id': u'28ffa0ca-a6bf-4153-b8e3-1ccb3443047d',
u'result': {u'name': u'Test Company', u'isSuspended': False,
u'phone': u'+99000000000',
u'address': u'23rd Fictional Street, Fantasy City, Dream land',
u'canBeManagedByAbove': True, u'type': 1,
u'id': u'54b646a0b1a43dbd197b23c6'}}
```

## 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://cloud.gravityzone.bitdefender.com/ \
    api/v1.0/jsonrpc/network",
  method: "POST",
  headers: {
    'Authorization':
      "Basic VWpsTVMrMG0xbDlJVVpqcGpXeUpHOGdibnYyTXRhNFQ6"
  },
  json: {
    "id": "123456789",
    "jsonrpc": "2.0",
    "method": "getCompaniesList",
    "params": []
  }
}, function(response, body) {
  console.log(body);
});

// Output:

// { id: '123456789', jsonrpc: '2.0',
//   result: [ { id: '54b646a0b1a43dbd197b23c6',
//     name: 'Test Company' } ] }
```