Symantec™ Endpoint Protection Manager 14 REST API Reference

Legal notice

Product version: 14

Documentation version: 14

This document was last updated on: March 02, 2017

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

REST API Reference

This document includes the following topics:

About Symantec Endpoint Protection Manager REST APIs

Symantec Endpoint Protection Manager includes a set of REST APIs that connect to and perform Symantec Endpoint Protection Manager (SEPM) operations from a remote application, such as Symantec Advanced Threat Protection (ATP). You use the APIs if you do not have access to Symantec Endpoint Protection Manager.

This document is intended for developers who want to write applications that interact with Symantec Endpoint Protection Manager. It explains the basic concepts of Symantec Endpoint Protection Manager production APIs. It also provides an overview of the different functions that the API supports.

Version information

The Symantec Endpoint Protection Manager API version is 1.

API content is versioned separately from Symantec Endpoint Protection. This version of the Symantec Endpoint Protection Manager API supports Symantec Endpoint Protection 14.

Required command components

To customize a REST API call, you use the following required components with a tool such as SoapUI or with a programming language such as PowerShell or Java.

Table 1-1 Required components for using a REST API command

Component	Description
URI	The base Uniform Resource Identifier (URI), which is as follows: https://*SEPM_IP*:8446/sepm/api/v1/ *SEPM_IP* represents the IP address or the host name of the Symantec Endpoint Protection Manager server. All APIs exposed by Symantec Endpoint Protection Manager carry authentication tokens and other privileged data. To ensure the confidentiality of the data, the REST APIs are only available over a secure connection.
Method	The method that you use to make the call to the command. Which method you use depends on the command and what you want to accomplish with the command. Methods include GET, PUT, POST, and DELETE.
Headers	Symantec Endpoint Protection Manager REST API commands require the following HTTP headers: ■ Authorization: Bearer *UserToken* *UserToken* represents the token response that the authenticate command returns. The authenticate command itself does not require this header. ■ Content-Type: application/json
Request parameters	The request parameters that are appropriate for the command that you want to use.

Symantec Endpoint Protection Manager API usage examples

You can use the following examples to familiarize yourself with using APIs with Symantec Endpoint Protection Manager.

- Verify the version of Symantec Endpoint Protection
- Authenticate to Symantec Endpoint Protection Manager

- Get a list of Symantec Endpoint Protection Manager groups
- Get fingerprint lists
- Assign a fingerprint list to a group for system lockdown

Note: You can send Symantec Endpoint Protection Manager API commands in many different ways. The examples to follow are presented in a raw HTTP format.

Verify the version of Symantec Endpoint Protection

To verify the version of Symantec Endpoint Protection, enter:

```
GET /sepm/api/v1/version
```

The response should be similar to the following:

```
{"API_SEQUENCE":"161014002","API_VERSION":"1.0.0",
     "version":"14.0.1904.0000"}
```

As a sanity check, you can also enter the following into a web browser, and then compare the results:

https://*SEPM_IP*:8446/sepm/api/v1/version

Note: The version command is an unauthenticated call.

Authenticate to Symantec Endpoint Protection Manager

Once you authenticate to Symantec Endpoint Protection Manager, you can perform authenticated calls, such as getting a list of Symantec Endpoint Protection Manager groups.

To authenticate to Symantec Endpoint Protection Manager, enter the command as an HTTP request:

```
POST /sepm/api/v1/identity/authenticate HTTP/1.1
Content-Type: application/json

{
"username" : "admin",
"password" : "password",
"domain" : ""
}
```

In this example, *admin* and *password* are the user name and password that you use to authenticate to Symantec Endpoint Protection Manager.

You should get a response similar to the following:


```
{
  "domain": "Default",
  "refreshToken": "cab16df1-58a2-4b8a-ad70-7b023db34025",
  "refreshTokenExpiration": 43199,
  "role": {
    "bitMask": 8,
    "title": "sysadmin"
  },
  "adminId": "AF3C39A10A320801000000DBF200C60A",
  "clientId": "4767c33a-99be-4ef9-b41f-e8db00da10ee",
  "clientSecret": "b65a52eb-c153-43f5-b9bd-6d2f0b43394f",
  "bannerTitle": "",
  "bannerText": "",
  "username": "admin",
  "fullname": null,
  "token": "c34692c5-201d-4d94-b0f8-61ed03383337",
  "tokenExpiration": 43199,
  "permissionSet": {
    "reportingRights": true,
    "groupRights": true,
    "siteRights": true,
    "remoteCommandRights": true,
    "policyRights": true
  },
  "domainid": "FC1716470A931BA765167FEC6FDA9A5C"
}
```


Copy the string that appears next to `token`. In this example, that string is `c34692c5-201d-4d94-b0f8-61ed03383337`.

You must provide this token for subsequent authenticated calls. The value of `token` is different for every logon.

Get a list of Symantec Endpoint Protection Manager groups

Getting a list of groups is an authenticated call, so you must use the token you previously copied in the authorization header. Enter the following HTTP request:

```
GET /sepm/api/v1/groups HTTP/1.1
Authorization: Bearer c34692c5-201d-4d94-b0f8-61ed03383337
```

You should get back a list of groups:


```
{
  "content": [
    {
      "id": "EF9C029A0A931BA7246C99C00F39133C",
      "name": "Default Group",
      "description": "",
      "fullPathName": "My Company\\Default Group",
      "numberOfPhysicalComputers": 1,
      "numberOfRegisteredUsers": 1,
      "createdBy": "AF3C39A10A320801000000DBF200C60A",
      "created": 1477983046292,
      "lastModified": 1477983046292,
      "policySerialNumber": "EF9C-11/08/2016 12:21:22 652",
      "policyDate": 1478607682652,
      "customIpsNumber": "",
      "childGroups": null,
      "domain": {
        "id": "FC1716470A931BA765167FEC6FDA9A5C",
        "name": "Default"
      },
      "policyInheritanceEnabled": false
    },
    {
      "id": "4541012E0A931BA7085259C3220013FB",
      "name": "My Company",
      "description": "",
      "fullPathName": "My Company",
      "numberOfPhysicalComputers": 0,
      "numberOfRegisteredUsers": 0,
      "createdBy": "AF3C39A10A320801000000DBF200C60A",
      "created": 1477983046292,
      "lastModified": 1477983046292,
      "policySerialNumber": "4541-11/08/2016 12:21:22 652",
      "policyDate": 1478607682652,
      "customIpsNumber": "",
      "childGroups": null,
      "domain": {
        "id": "FC1716470A931BA765167FEC6FDA9A5C",
        "name": "Default"
      },
      "policyInheritanceEnabled": false
```

```
    }
  ],
  "size": 25,
  "number": 0,
  "totalPages": 1,
  "lastPage": true,
  "firstPage": true,
  "sort": [
    {
      "direction": "ASC",
      "property": "NAME",
      "ascending": true
    }
  ],
  "totalElements": 2,
  "numberOfElements": 2
}
```


Get fingerprint lists

To send a command to get the file fingerprint list for a specified whitelist name as a set of hash values, enter the following HTTP request:

```
GET /api/v1/policy-objects/fingerprints
Authorization: Bearer c34692c5-201d-4d94-b0f8-61ed03383337
Content-Type: application/json
{
"name" : "Whitelist"
}
```

The command response would look similar to the following:


```
{
  "id": "20F543E30ADA144447A5FAAA370633DF",
  "name": "Whitelist",
  "hashType": null,
  "source": null,
  "description": "",
  "data": [
    "1F1DB67B07175194CE17ACAADC1B6AF5",
    "2B026E4B17034FE53BF3E660A61666FC",
    "3D5FFCC5C2709DF095D1F1CC8AE9747F",
    "570D47645E35D68B3985098BB98A357B",
    "A1E419B82CD4C6B60C1A5A0B7336DB3A",
```

```
    "BE13A88AE7196C1FE69314F328583162",
    "C2854A94987062EF750D72DC5525F0D8",
    "C9524B84BE07A1FF9DCF6BA12F76C4E4",
    "D17449D456CD8A3CBCB318C86B2B5156",
    "E0758A56E04D50EBEDB6DEB35D035855",
    "F4C9381A3B265EC5F1CEF1DEC638E0E9"
  ],
  "groupIds": []
}
```

Assign a fingerprint list to a group for system lockdown

To assign a fingerprint list to a group for system lockdown, use the following HTTP request:

```
PUT /api/v1/groups/{group_id}/system-lockdown/fingerprints/{fingerprint_id}
Authorization: Bearer c34692c5-201d-4d94-b0f8-61ed03383337
Content-Type: application/json
{
"group_id" : "EF9C029A0A931BA7246C99C00F39133C",
"fingerprint_id" : "20F543E30ADA144447A5FAAA370633DF"
}
```

Substitute actual group ID and fingerprint ID values instead of the examples that are provided for group_id and fingerprint_id.

If the request is successful, the HTTP OK code 200 is returned.

Where to get more information

REST API documentation

You can obtain the complete list of Symantec Endpoint Protection Manager APIs in the following ways:

- From a web address, which is hosted on the Symantec Endpoint Protection Manager server:
  https://*SEPM_IP*:8446/sepm/restapidocs.html
- From the Symantec support site:
  Symantec Endpoint Protection Manager 14 REST API Reference
  Download the .zip archive, extract all to a folder, and then view the HTML file with a web browser.