Table of Contents

Symantec™ Endpoint Protection Manager REST API Reference

3.32. Get the details of a command status
3.33. Cancel an existing command by creating a new cancel command for clients for which the command is still pending
3.34. Get the information about the computers in a specified domain
3.35. Check for and move a client to the specified group
3.36. Delete the list of existing computers
3.37. Update the device ID and encrypted device password for a specified computer
3.38. Get the status of the enrollment job
3.39. Delete an existing computer
3.40. Get the latest revision information for antivirus definitions from Symantec Security Response
3.41. Create a new Symantec Endpoint Protection Manager domain
3.42. Get a list of all accessible Symantec Endpoint Protection Manager domains
3.43. Get the domain name for the specified Symantec Endpoint Protection Manager domain ID
3.44. Update the status of a specified Symantec Endpoint Protection Manager domain as enabled or disabled
3.45. Get the details for a specified Symantec Endpoint Protection Manager domain
3.46. Update an existing Symantec Endpoint Protection Manager domain's information
3.47. Delete a specified Symantec Endpoint Protection Manager domain
3.48. Acknowledge a specified event for a given event ID
3.49. Get information related to critical events
3.50. Post an external notification
3.51. Delete a group or groups
3.52. Add or update groups
3.53. Change the group node type back to its default value
3.54. Get cloud external communication settings for the given group
3.55. Update low-bandwidth external communication settings for a given group
3.56. Withdraw a cloud setting from a group
3.57. Get a cloud policy from a group
3.58. Assign a cloud policy to a group
3.59. Withdraw a cloud policy from a group
3.60. Get a cloud policy from a group
3.61. Assign a cloud policy with a sub-type to a group
3.62. Withdraw a cloud policy with a sub-type from a group
3.63. Get the 'My Company' group details
3.64. Get the group information from its cloud policy group ID
3.65. Get a group list
3.66. Create a group
3.67. Get SEPM group details
3.68. Delete a specific group
3.69. Update group configuration
3.70. Get the information about the computers in a specified domain and group
3.71. Get the external communication settings of a location in the given group
3.72. Add or replace external communication settings to a given group
3.73. Modify the external communication settings for a given group
3.74. Get Symantec Endpoint Protection Manager location information for a specific group
3.75. Get the external communication settings of a location in the given group
3.76. Update the external communication settings to a location in the given group
3.77. Modify the external communication settings to a location in the given group
3.78. Get a list of policy types that are supported by Symantec Endpoint Protection Manager for the specific group
3.79. Get the ID of a specific policy type that is assigned to the specific location in a specific group
3.80. Get a list of quarantine policy types that are supported by Symantec Endpoint Protection Manager for group locations
3.81. Get a list of quarantine policy types that are assigned to the specific location in specific group
3.82. Assign a policy to a given location with in a group
3.83. Assign a location-independent policy to a group
3.84. Assign a fingerprint list to a group for system lockdown
3.85. Get a list of group update providers (GUPs)
3.86. Authenticate and return an access token for a valid user
3.87. Log off the user that is associated with a specified token

3.88. Retrieve all license-related information
3.89. Import a license file into SEPM
3.90. Get the license configuration
3.91. Retrieve specified licenses from the licensing server, given a list of serial numbers
3.92. Get information about the license type and the expiration state
3.93. Create a new exceptions policy
3.94. Get the exceptions policy for a specified policy ID
3.95. Modify existing policy values
3.96. Delete an existing Exceptions policy
3.97. Update exceptions policies
3.98. Creates a new HID policy
3.99. Get the HID policy payload for a specified policy ID
3.100. Modify existing HID policy values
3.101. Delete an existing HID policy
3.102. Update an HID policy
3.103. Create a new licensing setting
3.104. Get the LiveUpdate settings policy for specified policy ID
3.105. Create a new MEM policy
3.106. Get the MEM Policy payload for a specified policy ID
3.107. Modify existing MEM policy values
3.108. Delete an existing MEM policy
3.109. Update a MEM policy
3.110. Get the policy summary for a specified policy type
3.111. Get the policy summary for specified policy type; get the list of groups to which the policies are assigned
3.112. Create a new TDAD policy
3.113. Get the TDAD policy payload for a specified policy ID
3.114. Modify existing TDAD policy values
3.115. Delete an existing TDAD policy
3.116. Update TDAD policies by patch
3.117. Add a blacklist as a file fingerprint list to SEPM
3.118. Get the file fingerprint list for a specified name as a set of hash values
3.119. Update an existing blacklist
3.120. Get the file fingerprint list for a specified ID as a set of hash values
3.121. Delete an existing blacklist, and remove it from a group to which it applies
3.122. Check whether a site has a replication partner
3.123. Initiate replication for the specified replication partner
3.124. Get the replication status
3.125. Authenticate and return a PHP session token for a valid user
3.126. Get the current user token object
3.127. Get a list of threats that were automatically resolved
3.128. Get a list of clients for a group by content version
3.129. Get a list and count of client groups by content download sources
3.130. Get a list and count of infected clients for a specified time range
3.131. Get a list for a specified time range of clients reporting malware events
3.132. Get a list and count of the online and offline clients
3.133. Get a list for a specified time range the risk distribution by protection technology information for the given time range
3.134. Get a list and count of clients by client product version
3.135. Get the current threat statistics
3.136. Create a new TDAD global policy
3.137. Get all TDAD policies
3.138. Update an existing TDAD policy.
3.139. Delete all TDAD data
3.140. Update an existing TDAD policy
3.141. Get a TDAD policy for the specified Active Directory domain UID and policy UID
3.142. Deletes the TDAD data for the specified Active Directory domain UID and policy UID.
3.143. Get the current version of Symantec Endpoint Protection Manager

4. Definitions
    4.1. AdDomainPolicies
    4.2. AddAdminEntry
    4.3. AdminEntry
    4.4. AdminSummaryDetails
    4.5. AutoResolvedAttacks
    4.6. AutoResolvedAttacksResponse
    4.7. BinaryFile
    4.8. BlacklistPayload
    4.9. BufferedReader
    4.10. CASServerConfig
    4.11. CASVersionResult
    4.12. ClientDefStatus
    4.13. ClientDefStatusResponse
    4.14. ClientVersion
    4.15. ClientVersionResponse
    4.16. ClientsOnlineStats
    4.17. ClientsOnlineStatsResponse
    4.18. CloudModeCommandData
    4.19. CloudServerCertificate
    4.20. CommandTargets
    4.21. Computer
    4.22. ComputerPayload
    4.23. ContentDownloadSource
    4.24. ContentDownloadSourceResponse
    4.25. ContentThreshold
    4.26. Cookie
    4.27. CriticalEventsInfo
    4.28. CriticalEventsResponse
    4.29. DirectoryServerIntegrationConfiguration
    4.30. DomainAddEditTO
    4.31. DomainEntry
    4.32. DomainSummary
    4.33. EPMPUserCredential
    4.34. EnrollmentStatus
    4.35. Enumeration
    4.36. ExceptionThreat
    4.37. ExceptionsApplicationToMonitor
    4.38. ExceptionsConfiguration
    4.39. ExceptionsFile
    4.40. ExceptionsFingerprint
    4.41. ExceptionsLinuxConfiguration
    4.42. ExceptionsLockedOptions
    4.43. ExceptionsMacConfiguration
    4.44. ExceptionsRuleApplication
    4.45. ExceptionsRuleBlacklist
    4.46. ExceptionsRuleCertificate
    4.47. ExceptionsRuleDirectory
    4.48. ExceptionsRuleDnsHostBlacklist
    4.49. ExceptionsRuleDomain
    4.50. ExceptionsRuleExtensionList
    4.51. ExceptionsRuleFile
    4.52. ExceptionsRuleKnownRisk
    4.53. ExceptionsRuleLinuxDirectory
    4.54. ExceptionsRuleMacFile
    4.55. ExceptionsRuleState

4.56. ExternalCommunicationSettings
4.57. FingerPrintList
4.58. FingerprintlistPayload
4.59. Group
4.60. GroupPayload
4.61. GroupSummary
4.62. HidConfiguration
4.63. HttpServletRequest
4.64. HttpServletResponse
4.65. HttpSession
4.66. HttpSessionContext
4.67. InfectedClientStats
4.68. InfectedClientStatsResponse
4.69. InputStream
4.70. LatestRevisionInfo
4.71. LicenseEntitlements
4.72. LicenseSummary
4.73. LicensingPolicyPayload
4.74. Locale
4.75. LowBandwidthConfiguration
4.76. MalwareClientStats
4.77. MalwareClientStatsResponse
4.78. MemConfiguration
4.79. MemLockedOptions
4.80. MetadataAttributes
4.81. MultipartFile
4.82. Notification
4.83. Page
4.84. PepExceptionElement
4.85. PepThreatRuleElement
4.86. Policy
4.87. PolicyExceptionsConfigurationExceptionsLockedOptions
4.88. PolicyHidConfigurationObject
4.89. PolicyMemConfigurationMemLockedOptions
4.90. PolicyTdadConfigurationObject
4.91. Principal
4.92. PrintWriter
4.93. PrivateCloudConfiguration
4.94. PrivateCloudServer
4.95. PrivateCloudServerGroup
4.96. RepDiscoveredRule
4.97. RepPrevalenceRule
4.98. ReplicationAllStatus
4.99. ReplicationPartnerStatus
4.100. ReplicationStatus
4.101. ReplicationStatusResponse
4.102. ReportingInfo
4.103. RiskDistributionStats
4.104. RiskDistributionStatsResponse
4.105. Server
4.106. ServletContext
4.107. ServletInputStream
4.108. ServletOutputStream
4.109. Settings
4.110. SettingsExternalCommunicationSettingsObject
4.111. Sort

Symantec™ Endpoint Protection Manager

Symantec™ Endpoint Protection Manager REST API Reference

1. Overview

1.1. 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) and Symantec Web Gateway (SWG). You use the APIs if you do not have access to Symantec Endpoint Protection Manager.

If you use the Symantec Endpoint Protection cloud portal, REST APIs are supported only for those functions that the cloud portal does not manage.

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.

1.1.1. 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.

1.2. Required command components

You must have Symantec Endpoint Protection Manager System Administrator privileges to use REST API commands.

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.

Component	Description
URI	The base Uniform Resource Identifier (URI), which is as follows: • Host: https://*SEPM_IP*:8446 • Base path: /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.

1.3. 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.

1.3.1. 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.

1.3.2. 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": "AF3C39A10A3208010000000DBF200C60A",
  "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.

1.3.3. 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": "AF3C39A10A3208010000000DBF200C60A",
      "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": "AF3C39A10A3208010000000DBF200C60A",
      "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
}
```


1.3.4. 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": []
}
```

1.3.5. 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.
```

1.4. Where to get more information

1.4.1. REST API documentation

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

- From the following website:
- https://apidocs.symantec.com/home/saep (https://apidocs.symantec.com/home/saep)
- From a web address, which is hosted on and viewable from 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 (http://entced.symantec.com/sep/14/restapidocs)
- Download the .zip archive, extract all to a folder, and then view the HTML file with a web browser.

2. Symantec Endpoint Protection Incident Response Use Cases

2.1. Authentication

Most Symantec Endpoint Protection Manager REST API commands require that you first authenticate.

2.1.1. /api/v1/identity/authenticate

The ***authenticate*** API authenticates and returns an access token for a valid user.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/identity/authenticate

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	yes	The credentials used to log on to Symantec Endpoint Protection Manager.		UserCredential (https://apidocs.symantec.com/home/saep#_usercredential)
getBanner	query	no	Displays a logon banner, if configured. The possible values are TRUE or FALSE.		string
appName	query	no	Specify an application name to receive a token unique for that app.		string
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The service successfully processed the web request and returned a result.	UserToken (https://apidocs.symantec.com/home/saep#_usertoken)
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.2. Create, delete, or update groups

The following commands allow you to create, delete, or update groups, or get information about groups.

2.2.1. /api/v1/groups

Gets a listing of groups.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/groups

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
domain	query	no			string
pageIndex	query	no	The index page used for returned results. The default page index is 1.		integer (int32)
pageSize	query	no	The number of results to include on each page. The default is 25.		integer (int32)
sort	query	no	The column by which the results are sorted. The default is by name.		string
order	query	no	Specifies whether the results are in ascending order (ASC) or descending order (DESC).		string
mode	query	no	The presentation mode for the results, as a list (default) or as a tree.		string
fullPathName	query	no	The full path name of the group.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.2.2. /api/v1/groups/{groupId}

Create a group using POST.

GET information for a specific group.

DELETE a specific group.

Update group information using PATCH.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/groups/{groupId}

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
groupid	path	yes	The ID of the parent group.		string
domainId	query	no	The ID of the group's domain.		string
body	body	yes	The group configuration to be created.		GroupPayload (https://apidocs.symantec.com/home/saep#_grouppayload)
body	body	no			HttpServletResponse (https://apidocs.symantec.com/home/saep#_httpservletresponse)

Response Codes

Status Code	Reason	Response Model
201		

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
groupid	path	yes	The ID of the group from which to query group detail.		string
domainId	query	no	The ID of the group's domain.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Group
400	The parameters are invalid.	

401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
410	Cannot find the specified object.	
500	The web service encountered an error while processing the web request.	

HTTP Method

DELETE

Parameters

Name	Located in	Required	Description	Default	Schema
groupid	path	yes	The ID of the group to be deleted.		string
domainId	query	no	The ID of the group's domain.		string

Response Codes

Status Code	Reason	Response Model
204		

HTTP Method

PATCH

Parameters

Name	Located in	Required	Description	Default	Schema
groupid	path	yes	The ID of the group.		string
domainId	query	no	The ID of the group's domain.		string
body	body	yes	The group configurations to be updated.		GroupPayload (https://apidocs.symantec.com/home/saep#_grouppayload)

Response Codes

Status Code	Reason	Response Model
200		

2.3. Move a client to a different group

Use this command when you want to move a client to a different group.

2.3.1. /api/v1/computers

Checks and moves a client to the specified group.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/computers

HTTP Method

PATCH

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	yes	Information of a computer.		Array[Computer]

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Array[]
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
409	The request could not be completed due to a conflict with the current state of the source or target group.	
410	Cannot find the specified object.	
500	The web service encountered an error while processing the web request.	

2.4. Get information about a policy

You can get information about different kinds of policies using these commands.

2.4.1. /api/v1/policies/summary/exceptions

Get a list of exception policies that includes the policy ID and and policy name.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/summary/exceptions

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
domainId	query	no	If present, get the policies from this domain. Otherwise, get the policies from the logged-on domain.		string

Response Codes

Status Code	Reason	Response Model

200	The web service successfully processed the web request and returned a result.	

2.4.2. /api/v1/policies/exceptions/{id}

Get policy information for a specific exception policy.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/exceptions/{id}

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
id	path	yes	The ID of the exceptions policy to get.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Policy (https://apidocs.symantec.com/home/saep#_policy)

2.4.3. /api/v1/policies/summary/lu

Get a list of LiveUpdate (lu) policies that includes their ids and names.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/summary/lu

Parameters

Name	Located in	Required	Description	Default	Schema
domainId	query	no	If present, get the policies from this domain. Otherwise, get the policies from the logged-on domain.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	

2.4.4. /api/v1/policies/lu/{id}

Get policy information for a specific LiveUpdate policy.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/policies/lu/{id}

Parameters

Name	Located in	Required	Description	Default	Schema
id	path	yes	The ID of the LiveUpdate policy to get.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Policy (https://apidocs.symantec.com/home/saep#_policy)

2.5. Create and manage an exceptions policy

These commands let you create, manage, delete, and update exception policies.

2.5.1. /api/v1/policies/exceptions

Creates a new exceptions policy.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/policies/exceptions

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	no			PolicyExceptionsConfigurationExceptionsLockedOptions (https://apidocs.symantec.com/home/saep#_policyexceptionsconfigurationexceptionslockedo
body	body	no			HttpServletResponse (https://apidocs.symantec.com/home/saep#_httpservletresponse)

Response Codes

Status Code	Reason	Response Model
201		

2.5.2. /api/v1/policies/exceptions/{id}

GET the exceptions policy by policy id.

Modify an existing exceptions policy values with PUT request.

DELETE an existing exceptions policy.

Update an exceptions policies by using PATCH.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/exceptions/{id}

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
id	path	yes	The ID of the exceptions policy to get.		string

Response Codes

Status Code	Reason	Response Model
200	The operation completed.	Policy

HTTP Method

PUT

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	no			PolicyExceptionsConfigurationExceptionsLockedOptions (https://apidocs.symantec.com/home/saep#_policyexceptionsconfigurationexceptionslockedo
id	path	yes	The ID of the exceptions policy to edit.		string

Response Codes

Status Code	Reason	Response Model
200	The operation completed.	

HTTP Method

DELETE

Parameters

Name	Located in	Required	Description	Default	Schema
id	path	yes	The ID of the exceptions policy to delete.		string

Response Codes

Status Code	Reason	Response Model
200	The operation completed.	

HTTP Method

PATCH

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	no			PolicyExceptionsConfigurationExceptionsLockedOptions (https://apidocs.symantec.com/home/saep#_policyexceptionsconfigurationexceptionslockedo
id	path	yes	The ID of the exceptions policy to update.		string

Response Codes

Status Code	Reason	Response Model
200	The operation completed.	

2.6. Apply a policy to a group based on location

These commands let you get a list of groups, a list of locations for a specific group, or assign a policy to a group location.

2.6.1. /api/v1/groups

Gets a list of groups.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/groups

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
domain	query	no			string
pageIndex	query	no	The index page used for returned results. The default page index is 1.		integer (int32)
pageSize	query	no	The number of results to include on each page. The default is 25.		integer (int32)
sort	query	no	The column by which the results are sorted. The default is by name.		string
order	query	no	Specifies whether the results are in ascending order (ASC) or descending order (DESC).		string
mode	query	no	The presentation mode for the results, as a list (default) or as a tree.		string

fullPathName	query	no	The full path name of the group.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Group (https://apidocs.symantec.com/home/saep#_group)
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The resource requested was not found	
500	The web service encountered an error while processing the web request.	

2.6.2. /api/v1/groups/{groupId}/locations

Get information about Symantec Endpoint Protection Manager locations for a specific group.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/groups/{groupId}/locations

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
groupid	path	yes	The ID of the group from which to query locations.		string
domainId	query	no	The ID of the group's domain.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Group (https://apidocs.symantec.com/home/saep#_group)
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
410	Cannot find the specified object.	
500	The web service encountered an error while processing the web request.	

2.6.3. /api/v1/groups/{group_id}/locations/{location_id}/policies/{policy_type}

Assign a policy to a given location within a group.

NOTE | Only location-specific policies can be assigned to a location.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/groups/{group_id}/locations/{location_id}/policies/{policy_type}

HTTP Method

PUT

Parameters

Name	Located in	Required	Description	Default	Schema
group_id	path	yes	The ID of the group to which the policy is being assigned.		string
location_id	path	yes	The ID of the location to which the policy is being assigned. To assign policy to default location, default can also be used instead of location ID.		string
policy_type	path	yes	The type of the Policy to assign.		string
body	body	yes	JSON object containing ID of the policy to be assigned. e.g. {"id":"some GUID"}		MetadataAttributes (https://apidocs.symantec.com/home/saep#_metadataattributes)

Response Codes

Status Code	Reason	Response Model
200		

2.7. Assign a Firewall or IPS policy to a group

These commands let you get a list of Firewall or IPS policies, and then assign those policies to a specified group.

2.7.1. /api/v1/policies/summary/fw

Gets a list of Firewall policies that includes the policy IDs and the policy names.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/summary/fw

Parameters

Name	Located in	Required	Description	Default	Schema
domainId	query	no	If present, get the policies from this domain. Otherwise, get the policies from the logged-on domain.		string

Response Codes

Status Code	Reason	Response Model
200		

2.7.2. /api/v1/policies/summary/ips

Get a list of IPS policies that includes the policy IDs and the policy names.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/policies/summary/ips

Parameters

Name	Located in	Required	Description	Default	Schema
domainId	query	no	If present, get the policies from this domain. Otherwise, get the policies from the logged-on domain.		string

Response Codes

Status Code	Reason	Response Model
200		

2.7.3. /api/v1/groups/{group_id}/policies/{policy_type}

Assign a policy to a group.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/{group_id}/policies/{policy_type}

Name	Located in	Required	Description	Default	Schema
group_id	path	yes	The ID of the group to which the policy is being assigned.		string
policy_type	path	yes	The type of the Policy to assign.		string
body	body	yes	JSON object containing ID of the policy to be assigned. e.g. {"id":"some GUID"}.		MetadataAttributes (https://apidocs.symantec.com/home/saep#_metadataattributes)

Response Codes

Status Code	Reason	Response Model
200		

2.8. Generate an alert when a specified file appears

These commands let you create a new exception policy to define which file (or files) to monitor, get information related to the alerts generated by that exceptions policy, and then to acknowledge that specific event.

2.8.1. /api/v1/policies/exceptions

Creates a new exception policy.

https:// `SEPM_IP` :8446/sepm/api/v1/policies/exceptions

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
body	body	no			PolicyExceptionsConfigurationExceptionsLockedOptions (https://apidocs.symantec.com/home/saep#_policyexceptionsconfigurationexceptionslockedo
body	body	no			HttpServletResponse (https://apidocs.symantec.com/home/saep#_httpservletresponse)

Response Codes

Status Code	Reason	Response Model
201		

2.8.2. /api/v1/events/critical

Gets information related to critical events.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/events/critical

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
source	query	no	The source from which to get information. Not currently used.		string
pageIndex	query	no	The index page used for returned results. Not currently used.		integer (int32)

pageSize	query	no	The number of results returned for each page. Not currently used.		integer (int32)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	CriticalEventsResponse (https://apidocs.symantec.com/home/saep#_criticaleventsresponse)
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.8.3. /api/v1/events/acknowledge/{eventID}

Acknowledges a specified event for a given event ID.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/events/acknowledge/{eventID}

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
eventID	path	yes	The event ID to acknowledge.		string

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.9. Add or remove network quarantine status

You can add to or remove endpoints from the network quarantine with this command.

2.9.1. /api/v1/command-queue/quarantine

Sends a command from Symantec Endpoint Protection Manager to add Symantec Endpoint Protection endpoints to (or remove them from) network quarantine.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/command-queue/quarantine

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
group_ids	query	yes	The list of groups on which to run the command.		string
computer_ids	query	yes	The list of computers on which to run the command.		string
undo	query	no	If set to true, will undo quarantine.		boolean
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.10. Run a scan on Symantec Endpoint Protection endpoints

This command allows you to start an Evidence of Compromise (EOC) scan on managed Symantec Endpoint Protection endpoints. Requires Advanced Threat Protection.

2.10.1. /api/v1/command-queue/eoc

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection endpoints to request an Evidence of Compromise scan on the endpoint.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/command-queue/eoc

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
group_ids	query	yes	The list of groups on which to run the command.		string
computer_ids	query	yes	The list of computers on which to run the command.		string
body	body	yes	The evidence of compromise command in XML. See eoc.xsd in the Remote Management and Monitoring documentation for the proper format.		
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Array[]
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.11. Retrieve a file from Symantec Endpoint Protection Manager

This command lets you retrieve a file from the server on which you run Symantec Endpoint Protection Manager.

2.11.1. /api/v1/command-queue/file/{file_id}/content

Gets the binary file content for a given file ID.

URL

https:// SEPM_IP :8446/sepm/api/v1/command-queue/file/{file_id}/content

HTTP Method

GET

Parameters

Name	Located in	Required	Description	Default	Schema
file_id	path	yes	The file ID from which to get the binary content.		string
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
410	Cannot find the specified object.	
500	The web service encountered an error while processing the web request.	

2.12. Send a suspicious file to Symantec Endpoint Protection Manager

You use this command to request that a managed Symantec Endpoint Protection endpoint send a suspicious file back to Symantec Endpoint Protection Manager.

2.12.1. /api/v1/command-queue/files

Sends a command to request that the Symantec Endpoint Protection endpoint uploads a suspicious file back to Symantec Endpoint Protection Manager.

URL

https:// SEPM_IP :8446/sepm/api/v1/command-queue/files

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema

file_path	query	yes	The file path of the suspicious file.		string
computer_ids	query	yes	The list of computers on which to search for the suspicious file.		string
sha256	query	no	The SHA256 hash value of the suspicious file.		string
md5	query	no	The MD5 hash value of the suspicious file.		string
sha1	query	no	The SHA1 hash value of the suspicious file.		string
source	query	no	The file source from where to search for the suspicious file. Possible values are: FILESYSTEM (default), QUARANTINE, or BOTH. 12.1.x clients only use FILESYSTEM.		string
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	Array[]
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

2.13. LiveUpdate management

This command tells Symantec Endpoint Protection endpoints to run LiveUpdate to update their content.

2.13.1. /api/v1/command-queue/updatecontent

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection endpoints to update content.

URL

https:// `SEPM_IP` :8446/sepm/api/v1/command-queue/updatecontent

HTTP Method

POST

Parameters

Name	Located in	Required	Description	Default	Schema
group_ids	query	yes	The list of groups on which to run the command.		string
computer_ids	query	yes	The list of computers on which to run the command.		string
body	body	no			HttpServletRequest (https://apidocs.symantec.com/home/saep#_httpservletrequest)

Response Codes

Status Code	Reason	Response Model
200	The web service successfully processed the web request and returned a result.	
400	The parameters are invalid.	
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	
404	The requested resource was not found.	
500	The web service encountered an error while processing the web request.	

3. API Listing

3.1. Create a new administrator with the details that are provided.

```
POST /api/v1/admin-users
```

3.1.1. Parameters

Type	Name	Description	Schema
Query	**domainid** *optional*	The domain in which to create the administrator.	string
Body	**body** *required*	The information used to create the administrator.	AddAdminEntry

3.1.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	AdminSummaryDetails
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.1.3. Tags

- Allows you to view, modify, and create administrators.

3.2. Get the list of administrators for a particular domain

```
GET /api/v1/admin-users
```

3.2.1. Parameters

Type	Name	Description	Schema
Query	**domain** *optional*	The domain in which to look for administrators.	string

3.2.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content

HTTP Code	Description	Schema
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.2.3. Tags

- Allows you to view, modify, and create administrators.

3.3. Get the details of a single administrator

```
GET /api/v1/admin-users/{id}
```

3.3.1. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The administrator's ID.	string
Query	**domainId** *optional*	The domain in which to look for the administrator.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.3.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	AdminSummaryDetails
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.3.3. Tags

- Allows you to view, modify, and create administrators.

3.4. Update the details for a specified administrator

```
PUT /api/v1/admin-users/{id}
```

3.4.1. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The administrator's ID.	string

Type	Name	Description	Schema
Query	**domainid** *optional*	The administrator's domain.	string
Body	**body** *optional*	The updated details for the administrator.	AdminEntry

3.4.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	AdminEntry
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.4.3. Tags

- Allows you to view, modify, and create administrators.

3.5. Get the list of servers present in SEPM

```
GET /api/v1/admin/servers
```

3.5.1. Description

Gets the list of servers present in Symantec Endpoint Protection Manager. A system administrator account is required for this REST API.

3.5.2. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.5.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.5.4. Tags

- Allows you to view, modify administrative servers.

3.6. Update servers

```
PATCH /api/v1/admin/servers/{id}
```

3.6.1. Description

Updates servers. A system administrator account is required for this REST API.

3.6.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the server to update.	string
Body	**body** *required*	The server payload.	Server
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.6.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.6.4. Tags

- Allows you to view or modify administrative servers.

3.7. Update TDAD server information

```
POST /api/v1/admin/tdadserver
```

3.7.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	Object containing TDAD server details.	TdadServerDetails
Body	**body** *optional*		HttpServletRequest

3.7.2. Responses

HTTP Code	Schema

HTTP Code	Schema
200	No Content

3.7.3. Tags

- Allows you to view, modify administrative servers.

3.8. Retrieve TDAD server information

```
GET /api/v1/admin/tdadserver
```

3.8.1. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.8.2. Responses

HTTP Code	Schema
200	No Content

3.8.3. Tags

- Allows you to view, modify administrative servers.

3.9. Delete TDAD server information

```
DELETE /api/v1/admin/tdadserver
```

3.9.1. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.9.2. Responses

HTTP Code	Description	Schema
204	Deleted the TDAD server information. If the resource did not exist prior to the call, 204 is still returned.	No Content

3.9.3. Tags

- Allows you to view, modify administrative servers.

3.10. Delete an existing content analysis server API key

```
DELETE /api/v1/cas/key
```

3.10.1. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
204	Deleted the content analysis server API key. If the resource did not exist prior to the call, 204 is still returned.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
500	The web service encountered an error processing the web request.	No Content

3.10.2. Tags

- production

3.11. Validate support for the content analysis server version by Symantec Endpoint Protection Manager

```
POST /api/v1/cas/version
```

3.11.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The content analysis server configuration to check for the version.	CASServerConfig

3.11.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	CASVersionResult
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.11.3. Tags

- production

3.12. Retrieve the cloud console's domain enrollment status

```
GET /api/v1/cloud/epmp/cloud_enrollment
```

3.12.1. Description

Retrieves the cloud console's domain enrollment status. A system administrator account is required for this REST API.

3.12.2. Parameters

Type	Name	Description	Schema	Default

Type	Name	Description	Schema	Default
Header	**x-epmp-client-id** *required*	EPMP Client ID	string	""
Header	**x-epmp-client-secret** *required*	EPMP Client Secret	string	""
Header	**x-epmp-customer-id** *required*	EPMP Customer ID	string	""
Header	**x-epmp-domain-id** *required*	EPMP Domain ID	string	""

3.12.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.12.4. Tags

- Allows you to enroll into the cloud console per domain

3.13. Enrolls the SEPM Bridge with the cloud portal

```
POST /api/v1/cloud/epmp/enroll
```

3.13.1. Parameters

Type	Name	Description	Schema
Query	**domainid** *required*	The ID of the Symantec Endpoint Protection Manager domain that you want to enroll.	string
Body	**body** *required*	The enrollment details to register in the cloud console.	EPMPUserCredential
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.13.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	< string, object > map

3.13.3. Tags

- Allows you to enroll into the cloud portal by domain

3.14. Get the cloud portal enrollment status

```
GET /api/v1/cloud/epmp/enroll
```

3.14.1. Parameters

Type	Name	Description	Schema
Query	**domainid** *required*	The ID of the domain for which you want to check the enrollment status.	string

3.14.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	EnrollmentStatus

3.14.3. Tags

- Allows you to enroll into the cloud portal by domain

3.15. Unenroll SEPM Bridge from the cloud portal

```
DELETE /api/v1/cloud/epmp/enroll
```

3.15.1. Description

Unenrolls Symantec Endpoint Protection Manager Bridge from the cloud portal. A system administrator account is required for this REST API.

3.15.2. Parameters

Type	Name	Description	Schema
Query	**domainid** *required*	The Symantec Endpoint Protection Manager domain to unenroll.	string

3.15.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.15.4. Tags

- Allows you to enroll into the cloud by domain

3.16. Get the reporting hub's status

```
GET /api/v1/cloud/epmp/hubstatus
```

3.16.1. Responses

HTTP Code	Schema
200	No Content

3.16.2. Tags

- Allows you to enroll into the cloud by domain

3.17. Check if the hub on the specified server is the reporting hub

```
GET /api/v1/cloud/epmp/isEnrolled
```

3.17.1. Parameters

Type	Name	Description	Schema
Query	**domainid** *required*	The domain ID.	string

3.17.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	boolean
400	Invalid parameters	No Content
401	The current logged in user does not have sufficient rights to execute the web method or user is unauthorized	No Content
404	The resource reguested was not found	No Content
500	The web service encountered an error processing the web request	No Content

3.17.3. Tags

- Allows you to enroll into the cloud by domain

3.18. Send a command from SEPM to SEP clients to request an active scan

```
POST /api/v1/command-queue/activescan
```

3.18.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request an active scan on the client computer. A system administrator account is required for this REST API.

3.18.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string
Query	**group_ids** *required*	The list of groups on which to run the command.	string
Body	**body** *optional*		HttpServletRequest

3.18.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content

HTTP Code	Description	Schema
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.18.4. Tags

- Lists all of the Symantec Endpoint Protection Manager suspicious file-related command operations.

3.19. Send a command from SEPM to SEP clients to request a suspicious file submission to a CAS/MAA, and send the score back to SEPM

```
POST /api/v1/command-queue/analyze
```

3.19.1. Description

Send a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request a suspicious file submission to a content analysis server (or a malware analysis appliance) and to send the score back to Symantec Endpoint Protection Manager. * Note that while sha256, md5, or sha1 are not required parameters, you must include at least one of these to invoke this API.

3.19.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers to search for the suspicious file.	string
Query	**file_path** *required*	The file path of the suspicious file.	string
Query	**hardware_ids** *optional*	The list of computers to search, by hardware keys.	string
Query	**md5** *optional*	The MD5 hash value of the suspicious file.	string
Query	**sha1** *optional*	The SHA1 hash value of the suspicious file.	string
Query	**sha256** *optional*	The SHA256 hash value of the suspicious file.	string
Query	**source** *optional*	The file source to search for the suspicious file. Possible values are: FILESYSTEM (default), QUARANTINE, or BOTH. 12.1.x clients only use FILESYSTEM.	string
Body	**body** *optional*		HttpServletRequest

3.19.3. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.19.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.20. Send a command from SEPM to SEP clients to request that baseline application information be uploaded back to SEPM

```
POST /api/v1/command-queue/baseline
```

3.20.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request that baseline application information be uploaded back to Symantec Endpoint Protection Manager. A system administrator account is required for this REST API.

3.20.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computer IDs from which to request the baseline information.	string
Query	**group_ids** *required*	The list of group IDs from which to request the baseline information.	string
Body	**body** *optional*		HttpServletRequest

3.20.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.20.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.21. Sends a command from SEPM to SEP clients to request that those clients communicate directly with the cloud

```
POST /api/v1/command-queue/cloudmanaged
```

3.21.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request that those clients communicate directly with the cloud instead of Symantec Endpoint Protection Manager. A system administrator account is required for this REST API.

3.21.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The target groups or computers to which this command should be applied.	CloudModeCommandData
Body	**body** *optional*		HttpServletRequest

3.21.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.21.4. Tags

- Lists all of the Symantec Endpoint Protection Manager suspicious file-related command operations.

3.22. Sends a command from SEPM to SEP clients to request an "Evidence of Compromise" scan

```
POST /api/v1/command-queue/eoc
```

3.22.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request an "Evidence of Compromise" scan on the client computer. A system administrator account is required for this REST API.

3.22.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string
Query	**group_ids** *required*	The list of groups on which to run the command.	string

Type	Name	Description	Schema
Body	**body** *required*	The evidence of compromise command in XML. See eoc.xsd in the Remote Management and Monitoring documentation for the proper format.	string
Body	**body** *optional*		HttpServletRequest

3.22.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.22.4. Tags

- Lists all of the Symantec Endpoint Protection Manager suspicious file-related command operations.

3.23. Get the binary file content for a given file ID

```
GET /api/v1/command-queue/file/{file_id}/content
```

3.23.1. Description

Gets the binary file content for a given file ID. A system administrator account is required for this REST API.

3.23.2. Parameters

Type	Name	Description	Schema
Path	**file_id** *required*	The file ID from which to get the binary content.	string
Body	**body** *optional*		HttpServletResponse

3.23.3. Responses

HTTP Code	Description	Schema
200	The web service successfully processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content

HTTP Code	Description	Schema
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.23.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.24. Get the details of a binary file, such as the checksum and the file size

```
GET /api/v1/command-queue/file/{file_id}/details
```

3.24.1. Description

Gets the details of a binary file, such as the checksum and the file size. A system administrator account is required for this REST API.

3.24.2. Parameters

Type	Name	Description	Schema
Path	**file_id** *required*	The file ID from which to get detailed information.	string

3.24.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	BinaryFile
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.24.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.25. Send a command from SEPM to SEP clients to request a suspicious file be uploaded back to SEPM

```
POST /api/v1/command-queue/files
```

3.25.1. Description

Sends a command from SEPM to SEP clients to request a suspicious file be uploaded back to SEPM. A system administrator account is required for this REST API.

3.25.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to search for the suspicious file.	string
Query	**file_path** *required*	The file path of the suspicious file.	string
Query	**md5** *optional*	The MD5 hash value of the suspicious file.	string
Query	**sha1** *optional*	The SHA1 hash value of the suspicious file.	string
Query	**sha256** *optional*	The SHA256 hash value of the suspicious file.	string
Query	**source** *optional*	The file source to search for the suspicious file. Possible values are: FILESYSTEM (default), QUARANTINE, or BOTH. 12.1.x clients only use FILESYSTEM.	string
Body	**body** *optional*		HttpServletRequest

3.25.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.25.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.26. Send a command from SEPM to SEP clients to request a full scan

```
POST /api/v1/command-queue/fullscan
```

3.26.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to request a full scan on the client computer. A system administrator account is required for this REST API.

3.26.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string

Type	Name	Description	Schema
Query	**group_ids** *required*	The list of groups on which to run the command.	string
Body	**body** *optional*		HttpServletRequest

3.26.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.26.4. Tags

- Lists all of the Symantec Endpoint Protection Manager suspicious file-related command operations.

3.27. Send a command from SEPM to SEP clients to invalidate IRON cache entries on the endpoint

```
POST /api/v1/command-queue/ironcache
```

3.27.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to invalidate IRON cache entries on the client computer. A system administrator account is required for this REST API.

3.27.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string
Query	**group_ids** *required*	The list of groups on which to run the command.	string
Body	**body** *required*	The hash type and hash list to be applied to client computers.	FingerprintlistPayload
Body	**body** *optional*		HttpServletRequest

3.27.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map

HTTP Code	Description	Schema
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.27.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.28. Send a command from SEPM to SEP clients to override the default license policy

```
POST /api/v1/command-queue/license/override
```

3.28.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to override the default license policy. A system administrator account is required for this REST API.

3.28.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	the license policy to apply to the selected groups or computers.	LicenseEntitlements
Body	**body** *optional*		HttpServletRequest

3.28.3. Responses

HTTP Code	Schema
200	No Content

3.28.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.29. Send a command from SEPM to SEP clients to reset license policy to the default instance

```
POST /api/v1/command-queue/license/resetoverride
```

3.29.1. Description

Send a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to reset license policy to the default instance. A system administrator account is required for this REST API.

3.29.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	the target groups or computers to which this command should be applied.	CommandTargets

Type	Name	Description	Schema
Body	**body** *optional*		HttpServletRequest

3.29.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content

3.29.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.30. Send a command from SEPM to add SEP clients to (or remove them from) network quarantine

```
POST /api/v1/command-queue/quarantine
```

3.30.1. Description

Sends a command from Symantec Endpoint Protection Manager to add Symantec Endpoint Protection clients to (or remove them from) network quarantine. A system administrator account is required for this REST API.

3.30.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string
Query	**group_ids** *required*	The list of groups on which to run the command.	string
Query	**hardware_ids** *required*	The list of computer hardware keys	string
Query	**undo** *optional*	If set to true, it undoes the network quarantine status.	boolean
Body	**body** *optional*		HttpServletRequest

3.30.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.30.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.31. Send a command from SEPM to SEP clients to update their content

```
POST /api/v1/command-queue/updatecontent
```

3.31.1. Description

Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection clients to update their content. A system administrator account is required for this REST API.

3.31.2. Parameters

Type	Name	Description	Schema
Query	**computer_ids** *required*	The list of computers on which to run the command.	string
Query	**group_ids** *required*	The list of groups on which to run the command.	string
Body	**body** *optional*		HttpServletRequest

3.31.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.31.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.32. Get the details of a command status

```
GET /api/v1/command-queue/{command_id}
```

3.32.1. Description

Gets the details of a command status. A system administrator account is required for this REST API.

3.32.2. Parameters

Type	Name	Description	Schema
Path	**command_id** *required*	The command ID for which details are needed.	string
Query	**order** *optional*	Specifies whether the results are in ascending order (ASC) or descending order (DESC).	string

Type	Name	Description	Schema
Query	**pageIndex** *optional*	The index page for returned results. The default page index is 1.	integer (int32)
Query	**pageSize** *optional*	The number of results to include on each page. The default is 20.	integer (int32)
Query	**sort** *optional*	The column by which the results are sorted. The default is by command's start time.	string
Body	**body** *optional*		HttpServletResponse

3.32.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Page
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.32.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.33. Cancel an existing command by creating a new cancel command for clients for which the command is still pending

```
POST /api/v1/command-queue/{command_id}/cancel
```

3.33.1. Description

Cancels an existing command by creating a new cancel command for clients for which the command is still pending. A system administrator account is required for this REST API.

3.33.2. Parameters

Type	Name	Description	Schema
Path	**command_id** *required*	The command ID to be canceled.	string
Body	**body** *optional*		HttpServletRequest

3.33.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map

HTTP Code	Description	Schema
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.33.4. Tags

- Lists all of the Symantec Endpoint Protection Manager's suspicious file-related command operations.

3.34. Get the information about the computers in a specified domain

```
GET /api/v1/computers
```

3.34.1. Description

Gets the information about the computers in a specified domain. A system administrator account is required for this REST API.

3.34.2. Parameters

Type	Name	Description	Schema
Query	**computerName** *optional*	The host name of computer. Wild card is supported as '*'.	string
Query	**domain** *optional*	The domain from which to get computer information.	string
Query	**feature** *optional*	List of features to return opstate information in reduced mode.Possible values are av, mem, fw, ips, tdad	< string > array(csv)
Query	**lastUpdate** *optional*	Indicates when a computer last updated its status. The default value of 0 gets all the results.	integer (int64)
Query	**mac** *optional*	The MAC address of computer. Wild card is supported as '*'.	string
Query	**order** *optional*	Specifies whether the results are in ascending order (ASC) or descending order (DESC).	string

Type	Name	Description	Schema
Query	**os** *optional*	The list of OS to filter. Possible values are CentOs, Debian, Fedora, MacOSX, Oracle, OSX, RedHat, SUSE, Ubuntu, Win10, Win2K, Win7, Win8, Win81, WinEmb7, WinEmb8, WinEmb81, WinFundamental, WinNT, Win2K3, Win2K8, Win2K8R2, Win2K12, Win2K12R2, Win2K16, WinVista, WinXP, WinXPEmb, WinXPProf64	< enum (CentOs, Debian, Fedora, MacOSX, Oracle, OSX, RedHat, SUSE, Ubuntu, Win10, Win2K, Win7, Win8, Win81, WinEmb7, WinEmb8, WinEmb81, WinFundamental, WinNT, Win2K3, Win2K8, Win2K8R2, Win2K12, Win2K12R2, Win2K16, WinVista, WinXP, WinXPEmb, WinXPProf64) > array(csv)
Query	**pageIndex** *optional*	The index page that is used for the returned results. The default page index is 1.	integer (int32)
Query	**pageSize** *optional*	The number of results to include on each page. The default is 20.	integer (int32)
Query	**sort** *optional*	The column by which the results are sorted. Possible values are COMPUTER_NAME (Default value), COMPUTER_ID, COMPUTER_DOMAIN_NAME, or DOMAIN_ID.	string
Query	**verbose** *optional*	Returns a reduced set of computer information, if true.	boolean

3.34.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Page
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.34.4. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.35. Check for and move a client to the specified group

```
PATCH /api/v1/computers
```

3.35.1. Description

Check for and move a client to the specified group. A system administrator account is required for this REST API.

3.35.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	Information about the computer.	< Computer > array

3.35.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
409	The request could not be completed due to a conflict with the current state of the source or target group.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.35.4. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.36. Delete the list of existing computers

```
POST /api/v1/computers/delete
```

3.36.1. Description

Deletes the list of existing computers. A system administrator account is required for this REST API.

3.36.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	Information about the computer.	< Computer > array
Body	**body** *optional*		HttpServletRequest

3.36.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	< object > array
207		No Content

3.36.4. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.37. Update the device ID and encrypted device password for a specified computer

```
POST /api/v1/computers/enroll
```

3.37.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The device ID and encrypted device password to upload to Symantec Endpoint Protection Manager for enrollment.	< ComputerPayload > array

3.37.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.37.3. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.38. Get the status of the enrollment job

```
GET /api/v1/computers/enroll/{id}
```

3.38.1. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The enrollment job for which the status is needed.	string

3.38.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.38.3. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.39. Delete an existing computer

```
DELETE /api/v1/computers/{id}
```

3.39.1. Description

Deletes an existing computer. A system administrator account is required for this REST API.

3.39.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the computer to delete.	string
Body	**body** *optional*		HttpServletRequest

3.39.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.39.4. Tags

- All Symantec Endpoint Protection Manager computer operations.

3.40. Get the latest revision information for antivirus definitions from Symantec Security Response

```
GET /api/v1/content/avdef/latest
```

3.40.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	LatestRevisionInfo
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.40.2. Tags

- Symantec Endpoint Protection Manager content information operations.

3.41. Create a new Symantec Endpoint Protection Manager domain

```
POST /api/v1/domains
```

3.41.1. Parameters

Type	Name	Schema
Body	**body** *optional*	DomainEntry
Body	**body** *optional*	HttpServletRequest

3.41.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	DomainAddEditTO

3.41.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.42. Get a list of all accessible Symantec Endpoint Protection Manager domains

```
GET /api/v1/domains
```

3.42.1. Responses

HTTP Code	Description	Schema
200	The operation completed.	< object > array

3.42.2. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.43. Get the domain name for the specified Symantec Endpoint Protection Manager domain ID

```
GET /api/v1/domains/name/{id}
```

3.43.1. Parameters

Type	Name	Schema
Path	**id** *required*	string
Body	**body** *optional*	HttpServletRequest

3.43.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	< object > array

3.43.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.44. Update the status of a specified Symantec Endpoint Protection Manager domain as enabled or disabled

```
POST /api/v1/domains/{id}
```

3.44.1. Parameters

Type	Name	Schema
Path	**id** *required*	string
Query	**action** *required*	string

3.44.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.44.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.45. Get the details for a specified Symantec Endpoint Protection Manager domain

```
GET /api/v1/domains/{id}
```

3.45.1. Parameters

Type	Name	Schema
Path	**id** *required*	string
Body	**body** *optional*	HttpServletRequest

3.45.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	DomainAddEditTO

3.45.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.46. Update an existing Symantec Endpoint Protection Manager domain's information

```
PUT /api/v1/domains/{id}
```

3.46.1. Parameters

Type	Name	Schema

Type	Name	Schema
Path	**id** *required*	string
Body	**body** *optional*	DomainEntry

3.46.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	DomainAddEditTO

3.46.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.47. Delete a specified Symantec Endpoint Protection Manager domain

```
DELETE /api/v1/domains/{id}
```

3.47.1. Parameters

Type	Name	Schema
Path	**id** *required*	string
Body	**body** *optional*	HttpServletRequest

3.47.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.47.3. Tags

- Lists, adds, modifies, or deletes Symantec Endpoint Protection Manager domains.

3.48. Acknowledge a specified event for a given event ID

```
POST /api/v1/events/acknowledge/{eventID}
```

3.48.1. Parameters

Type	Name	Description	Schema
Path	**eventID** *required*	The event ID to acknowledge.	string

3.48.2. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.48.3. Tags

- Symantec Endpoint Protection Manager events information operations.

3.49. Get information related to critical events

```
GET /api/v1/events/critical
```

3.49.1. Parameters

Type	Name	Description	Schema
Query	**pageIndex** *optional*	The index page that is used for returned results. Not currently used.	integer (int32)
Query	**pageSize** *optional*	The number of results returned for each page. Not currently used.	integer (int32)
Query	**source** *optional*	The source from which to get information. Not currently used.	string

3.49.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	CriticalEventsResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.49.3. Tags

- Symantec Endpoint Protection Manager events information operations.

3.50. Post an external notification

```
POST /api/v1/events/notifications
```

3.50.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The external Notificaiton to be added.	Notification
Body	**body** *optional*		HttpServletRequest

3.50.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.50.3. Tags

- Symantec Endpoint Protection Manager events Notifications operations.

3.51. Delete a group or groups

```
POST /api/v1/ext/groups/syncdelete
```

3.51.1. Description

Delete a group or groups. A system administrator account is required for this REST API.

3.51.2. Parameters

Type	Name	Description	Schema
Query	**domainId** *optional*	The id of the domain for which the groups needs to be deleted.	string
Body	**body** *required*	Group details	Group

3.51.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.51.4. Tags

- production

3.52. Add or update groups

```
POST /api/v1/ext/groups/synchronization
```

3.52.1. Description

Adds or updates groups. A system administrator account is required for this REST API.

3.52.2. Parameters

Type	Name	Description	Schema
Query	**domainId** *optional*	The ID of the domain for which the group needs to be created or updated.	string
Body	**body** *required*	Group details	Group

3.52.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.52.4. Tags

- production

3.53. Change the group node type back to its default value

```
DELETE /api/v1/ext/groups/synchronization
```

3.53.1. Description

Changes the group node to native for all the groups and temporary for default group, and then changes the external Reference ID back to null.

3.53.2. Parameters

Type	Name	Schema
Query	**domainId** *optional*	string

3.53.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.53.4. Tags

- production

3.54. Get cloud external communication settings for the given group

```
GET /api/v1/ext/groups/{group_id}/policies/external-communication
```

3.54.1. Parameters

Type	Name	Schema
Path	**group_id** *required*	string

3.54.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.54.3. Tags

- production

3.55. Update low-bandwidth external communication settings for a given group

```
PUT /api/v1/ext/groups/{group_id}/policies/external-communication
```

3.55.1. Description

Updates low-bandwidth external communication settings for a given group. The values that are not specified are set to defaults.

3.55.2. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group.	string
Body	**body** *required*	The Settings to be used.	SettingsExternalCommunicationSettingsObject
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.55.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.55.4. Tags

- production

3.56. Withdraw a cloud setting from a group

```
DELETE /api/v1/ext/groups/{group_id}/policies/external-communication
```

3.56.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group from which the Symantec Endpoint Protection Manager setting needs to be withdrawn.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.56.2. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The operation completed.	string
204	The resource was deleted. If the resource did not exist prior to the call, 204 is still returned.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.56.3. Tags

- production

3.57. Get a cloud policy from a group

```
GET /api/v1/ext/groups/{group_id}/policies/{policy_type}
```

3.57.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**policy_type** *required*	The type of policy to get.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.57.2. Responses

HTTP Code	Schema
200	No Content

3.57.3. Tags

- production

3.58. Assign a cloud policy to a group

```
PUT /api/v1/ext/groups/{group_id}/policies/{policy_type}
```

3.58.1. Parameters

Type	Name	Description	Schema

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**policy_type** *required*	The type of policy to assign.	string
Body	**body** *required*	JSON object containing ID of the policy to be assigned. e.g. {"id":"Policy ID"}	MetadataAttributes
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.58.2. Responses

HTTP Code	Schema
200	No Content

3.58.3. Tags

- production

3.59. Withdraw a cloud policy from a group

```
DELETE /api/v1/ext/groups/{group_id}/policies/{policy_type}
```

3.59.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group from which the policy needs to be withdrawn.	string
Path	**policy_type** *required*	The type of policy to withdraw.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.59.2. Responses

HTTP Code	Description	Schema
200	The operation completed	string

3.59.3. Tags

- production

3.60. Get a cloud policy from a group

```
GET /api/v1/ext/groups/{group_id}/policies/{policy_type}/{sub_type}
```

3.60.1. Parameters

Type	Name	Description	Schema

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**policy_type** *required*	The type of the policy to get.	string
Path	**sub_type** *required*	The type of sub-policy to get.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.60.2. Responses

HTTP Code	Schema
200	No Content

3.60.3. Tags

- production

3.61. Assign a cloud policy with a sub-type to a group

```
PUT /api/v1/ext/groups/{group_id}/policies/{policy_type}/{sub_type}
```

3.61.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**policy_type** *required*	The type of the policy to assign.	string
Path	**sub_type** *required*	The type of the sub policy to assign.	string
Body	**body** *required*	JSON object containing ID of the policy to be assigned. e.g. {"id":"Policy ID"}	MetadataAttributes
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.61.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.61.3. Tags

- production

3.62. Withdraw a cloud policy with a sub-type from a group

```
DELETE /api/v1/ext/groups/{group_id}/policies/{policy_type}/{sub_type}
```

3.62.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group from which the policy needs to be withdrawn.	string
Path	**policy_type** *required*	The type of policy to withdraw.	string
Path	**sub_type** *required*	The type of sub-policy to withdraw.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.62.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.62.3. Tags

- production

3.63. Get the 'My Company' group details

```
GET /api/v1/ext/{source}/groups/mycompany
```

3.63.1. Parameters

Type	Name	Description	Schema
Path	**source** *required*	The external source.	string
Query	**domainId** *optional*		string

3.63.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.63.3. Tags

- production

3.64. Get the group information from its cloud policy group ID

```
GET /api/v1/ext/{source}/groups/{groupId}
```

3.64.1. Description

Gets the group information from its cloud policy group ID; this is the equivalent of /api/v1/groups/{groupId}, but takes an external source's group ID.

3.64.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The external source's group ID.	string
Path	**source** *required*	The name of the external source.	string
Query	**domainId** *optional*		string

3.64.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.64.4. Tags

- production

3.65. Get a group list

```
GET /api/v1/groups
```

3.65.1. Description

Gets a group list. A system administrator account is required for this REST API.

3.65.2. Parameters

Type	Name	Description	Schema
Query	**domain** *optional*		string
Query	**fullPathName** *optional*	The full path name of the group.	string
Query	**mode** *optional*	The presentation mode for the results, as a list (default) or as a tree.	string
Query	**order** *optional*	Specifies whether the results are in ascending order (ASC) or descending order (DESC).	string
Query	**pageIndex** *optional*	The index page that is used for returned results. The default page index is 1.	integer (int32)
Query	**pageSize** *optional*	The number of results to include on each page. The default is 25.	integer (int32)
Query	**sort** *optional*	The column by which the results are sorted. The default is by name.	string

3.65.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Page
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.65.4. Tags

- production

3.66. Create a group

```
POST /api/v1/groups/{groupId}
```

3.66.1. Description

Creates a group. A system administrator account is required for this REST API.

3.66.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the parent group.	string
Query	**domainId** *optional*	The ID of the group's domain	string
Body	**body** *required*	The group configuration to be created.	GroupPayload
Body	**body** *optional*		HttpServletResponse

3.66.3. Responses

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content

3.66.4. Tags

- production

3.67. Get SEPM group details

```
GET /api/v1/groups/{groupId}
```

3.67.1. Parameters

Type	Name	Description	Schema

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query group details.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.67.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Group
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.67.3. Tags

- production

3.68. Delete a specific group

```
DELETE /api/v1/groups/{groupId}
```

3.68.1. Description

Deletes a specific group. A system administrator account is required for this REST API.

3.68.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group to be deleted.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.68.3. Responses

HTTP Code	Description	Schema
204	The resource was deleted. If the resource did not exist prior to the call, 204 is still returned.	No Content

3.68.4. Tags

- production

3.69. Update group configuration

```
PATCH /api/v1/groups/{groupId}
```

3.69.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string
Query	**domainId** *optional*	The ID of the group's domain.	string
Body	**body** *required*	The group configurations to be updated.	GroupPayload

3.69.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.69.3. Tags

- production

3.70. Get the information about the computers in a specified domain and group

```
GET /api/v1/groups/{groupId}/computers
```

3.70.1. Description

Gets the information about the computers in a specified domain and group. A system administrator account is required for this REST API.

3.70.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group where the clients are communicating	string
Query	**domain** *optional*	The domain from which to get computer information.	string
Query	**feature** *optional*	List of features to return opstate information in reduced mode.Possible values are av, mem, fw, ips, tdad	< string > array(csv)
Query	**lastUpdate** *optional*	Indicates when a computer last updated its status. The default value of 0 gets all the results.	integer (int64)
Query	**order** *optional*	Specifies whether the results are in ascending order (ASC) or descending order (DESC).	string

Type	Name	Description	Schema
Query	**os** *optional*	The list of OS to filter. Possible values are CentOs, Debian, Fedora, MacOSX, Oracle, OSX, RedHat, SUSE, Ubuntu, Win10, Win2K, Win7, Win8, WinEmb7, WinEmb8, WinEmb81, WinFundamental, WinNT, Win2K3, Win2K8, Win2K8R2, WinVista, WinXP, WinXPEmb, WinXPProf64	< enum (CentOs, Debian, Fedora, MacOSX, Oracle, OSX, RedHat, SUSE, Ubuntu, Win10, Win2K, Win7, Win8, Win81, WinEmb7, WinEmb8, WinEmb81, WinFundamental, WinNT, Win2K3, Win2K8, Win2K8R2, Win2K12, Win2K12R2, Win2K16, WinVista, WinXP, WinXPEmb, WinXPProf64) > array(csv)
Query	**pageIndex** *optional*	The index page that is used for returned results. The default page index is 1.	integer (int32)
Query	**pageSize** *optional*	The number of results to include on each page. The default is 20.	integer (int32)
Query	**sort** *optional*	The column by which the results are sorted. Possible values are COMPUTER_NAME (Default value), COMPUTER_ID, COMPUTER_DOMAIN_NAME, or DOMAIN_ID.	string
Query	**verbose** *optional*	Returns a reduced set of computer information if true.	boolean

3.70.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	Page

3.70.4. Tags

- production

3.71. Get the external communication settings of a location in the given group

```
GET /api/v1/groups/{groupId}/external-communication
```

3.71.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string

3.71.2. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Settings
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.71.3. Tags

- production

3.72. Add or replace external communication settings to a given group

```
PUT /api/v1/groups/{groupId}/external-communication
```

3.72.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string
Body	**body** *required*	The settings to use.	SettingsExternalCommunicationSettingsObject
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.72.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.72.3. Tags

- production

3.73. Modify the external communication settings for a given group

```
PATCH /api/v1/groups/{groupId}/external-communication
```

3.73.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string
Body	**body** *required*	The settings to use.	SettingsExternalCommunicationSettingsObject
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.73.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.73.3. Tags

- production

3.74. Get Symantec Endpoint Protection Manager location information for a specific group

```
GET /api/v1/groups/{groupId}/locations
```

3.74.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query locations.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.74.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.74.3. Tags

- production

3.75. Get the external communication settings of a location in the given group

```
GET /api/v1/groups/{groupId}/locations/{locationId}/external-communication
```

3.75.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string
Path	**locationId** *required*	The ID of the location to which the policy is being retrieved.	string

3.75.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Settings
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.75.3. Tags

- production

3.76. Update the external communication settings to a location in the given group

```
PUT /api/v1/groups/{groupId}/locations/{locationId}/external-communication
```

3.76.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group.	string
Path	**locationId** *required*	The ID of the location to which the policy is being updated.	string
Body	**body** *required*	The settings to use.	SettingsExternalCommunicationSettingsObject
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.76.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.76.3. Tags

- production

3.77. Modify the external communication settings to a location in the given group

```
PATCH /api/v1/groups/{groupId}/locations/{locationId}/external-communication
```

3.77.1. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group	string
Path	**locationId** *required*	The ID of the location to which the policy is being updated.	string
Body	**body** *required*	The settings to use.	SettingsExternalCommunicationSettingsObject
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.77.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.77.3. Tags

- production

3.78. Get a list of policy types that are supported by Symantec Endpoint Protection Manager for the specific group

```
GET /api/v1/groups/{groupId}/locations/{locationId}/policies
```

3.78.1. Description

Gets a list of policy types that are supported by SEPM for the specific group. This command currently returns av, fw, lu, hi, hid adc, ips, or exceptions.

3.78.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query locations.	string
Path	**locationId** *required*	The ID of the location from which to query policy types; returns av, fw, lu, hi, hid adc, ips, and exception policies.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.78.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.78.4. Tags

- production

3.79. Get the ID of a specific policy type that is assigned to the specific location in a specific group

```
GET /api/v1/groups/{groupId}/locations/{locationId}/policies/{policyType}
```

3.79.1. Description

Gets the ID of a specific policy type that is assigned to the specific location in a specific group. The policy type can be av, fw, ips, adc, hi, hid, mem, lu, or exceptions.

3.79.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query locations.	string
Path	**locationId** *required*	The ID of the location from which to query the policy ID.	string
Path	**policyType** *required*	The policy types, which can be av, fw, ips, adc, hi, hid, mem, lu, or exceptions.	string

Type	Name	Description	Schema
Query	**domainId** *optional*	The ID of the group's domain.	string

3.79.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.79.4. Tags

- production

3.80. Get a list of quarantine policy types that are supported by Symantec Endpoint Protection Manager for group locations

```
GET /api/v1/groups/{groupId}/locations/{locationId}/quarantine
```

3.80.1. Description

Gets a list of quarantine policy types that are supported by SEPM for group locations. This command currently returns av, fw, lu, hi, hid adc, ips, or exceptions.

3.80.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query locations.	string
Path	**locationId** *required*	The ID of the location from which to query policy types.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.80.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content

HTTP Code	Description	Schema
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.80.4. Tags

- production

3.81. Get a list of quarantine policy types that are assigned to the specific location in specific group

```
GET /api/v1/groups/{groupId}/locations/{locationId}/quarantine/{policyType}
```

3.81.1. Description

Gets a list of quarantine policy types that are assigned to the specific location in specific group. The policy type can be av, fw, ips, adc, hid, lu, or exceptions.

3.81.2. Parameters

Type	Name	Description	Schema
Path	**groupId** *required*	The ID of the group from which to query locations.	string
Path	**locationId** *required*	The ID of the location from which to query policy types	string
Path	**policyType** *required*	The policy types, which can be av, fw, ips, adc, hi, lu, or exception.	string
Query	**domainId** *optional*	The ID of the group's domain.	string

3.81.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.81.4. Tags

- production

3.82. Assign a policy to a given location with in a group

```
PUT /api/v1/groups/{group_id}/locations/{location_id}/policies/{policy_type}
```

3.82.1. Description

Assigns a policy to a given location with in a group. Only location-specific policies can be assigned to a location.

3.82.2. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**location_id** *required*	The ID of the location to which the policy is being assigned. To assign policy to default location, 'default' can also be used instead of location ID.	string
Path	**policy_type** *required*	The type of the Policy to assign.	string
Body	**body** *required*	JSON object containing ID of the policy to be assigned. e.g. {"id":"some GUID"}	MetadataAttributes

3.82.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.82.4. Tags

- production

3.83. Assign a location-independent policy to a group

```
PUT /api/v1/groups/{group_id}/policies/{policy_type}
```

3.83.1. Parameters

Type	Name	Description	Schema
Path	**group_id** *required*	The ID of the group to which the policy is being assigned.	string
Path	**policy_type** *required*	The type of policy to assign.	string
Body	**body** *required*	JSON object containing ID of the policy to be assigned. e.g. {"id":"some GUID"}	MetadataAttributes

3.83.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	No Content

3.83.3. Tags

- production

3.84. Assign a fingerprint list to a group for system lockdown

```
PUT /api/v1/groups/{group_id}/system-lockdown/fingerprints/{fingerprint_id}
```

3.84.1. Description

Assigns a fingerprint list to a group for system lockdown. A system administrator account is required for this REST API.

3.84.2. Parameters

Type	Name	Description	Schema
Path	**fingerprint_id** *required*	The ID of the fingerprint list to assign.	string
Path	**group_id** *required*	The ID of the group to which a fingerprint list is being assigned.	string

3.84.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
409	The requested settings conflict with the current settings.	No Content
410	Cannot find the specified object.	No Content
422	Unable to process the request because system lockdown is currently disabled, or some file fingerprint lists or file names were already assigned.	No Content
423	The resource to update is locked and cannot be updated.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.84.4. Tags

- production

3.85. Get a list of group update providers (GUPs)

```
GET /api/v1/gup/status
```

3.85.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content

HTTP Code	Description	Schema
500	The web service encountered an error while processing the web request.	No Content

3.85.2. Tags

- Symantec Endpoint Protection Manager Group Update Provider-related operations.

3.86. Authenticate and return an access token for a valid user

```
POST /api/v1/identity/authenticate
```

3.86.1. Parameters

Type	Name	Description	Schema
Query	**appName** *optional*	Specify an application name to receive a token that is unique to that application.	string
Query	**getBanner** *optional*	Displays a logon banner, if configured. The possible values are TRUE or FALSE.	string
Body	**body** *required*	The credentials used to log on to Symantec Endpoint Protection Manager.	UserCredential
Body	**body** *optional*		HttpServletRequest

3.86.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	UserToken
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.86.3. Tags

- production

3.87. Log off the user that is associated with a specified token

```
POST /api/v1/identity/logout
```

3.87.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The user token to log off.	UserToken

Type	Name	Description	Schema
Body	**body** *optional*		HttpServletRequest

3.87.2. Responses

HTTP Code	Description	Schema
204	The requested user was logged off.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.87.3. Tags

- production

3.88. Retrieve all license-related information

```
GET /api/v1/licenses
```

3.88.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.88.2. Tags

- All of the Symantec Endpoint Protection Manager-related license operations.

3.89. Import a license file into SEPM

```
POST /api/v1/licenses/add
```

3.89.1. Description

Imports a license file into Symantec Endpoint Protection Manager. A system administrator account is required for this REST API.

3.89.2. Parameters

Type	Name	Description	Schema

Type	Name	Description	Schema
Body	**body** *required*	The license file to import into Symantec Endpoint Protection Manager.	MultipartFile
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.89.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.89.4. Tags

- All of the Symantec Endpoint Protection Manager-related license operations.

3.90. Get the license configuration

```
GET /api/v1/licenses/config
```

3.90.1. Description

Gets the license configuration. A system administrator account is required for this REST API.

3.90.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.90.3. Tags

- All of the Symantec Endpoint Protection Manager-related license operations.

3.91. Retrieve specified licenses from the licensing server, given a list of serial numbers

```
GET /api/v1/licenses/entitlements
```

3.91.1. Description

Retrieves specified licenses from the licensing server, given a list of serial numbers. A system administrator account is required for this REST API.

3.91.2. Parameters

Type	Name	Description	Schema
Query	**serialNumbers** *required*	The serial numbers used to retrieve the licenses.	< string > array(csv)
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.91.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< object > array
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.91.4. Tags

- All of the Symantec Endpoint Protection Manager-related license operations.

3.92. Get information about the license type and the expiration state

```
GET /api/v1/licenses/summary
```

3.92.1. Description

Gets information about the license type and the expiration state. A system administrator account is required for this REST API.

3.92.2. Parameters

Type	Name	Schema
Query	**domainId** *optional*	string

3.92.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	LicenseSummary
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content

HTTP Code	Description	Schema
500	The web service encountered an error while processing the web request.	No Content

3.92.4. Tags

- All of the Symantec Endpoint Protection Manager-related license operations.

3.93. Create a new exceptions policy

```
POST /api/v1/policies/exceptions
```

3.93.1. Description

Creates a new exceptions policy. A system administrator account is required for this REST API

3.93.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The exceptions policy to create.	PolicyExceptionsConfigurationExceptionsLockedOptions
Body	**body** *optional*		HttpServletResponse

3.93.3. Responses

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content

3.93.4. Tags

- production

3.94. Get the exceptions policy for a specified policy ID

```
GET /api/v1/policies/exceptions/{id}
```

3.94.1. Description

Gets the exceptions policy for a specified policy ID. A system administrator account is required for this REST API.

3.94.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the exceptions policy to get.	string

3.94.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	Policy

3.94.4. Tags

- production

3.95. Modify existing policy values

```
PUT /api/v1/policies/exceptions/{id}
```

3.95.1. Description

Modify existing policy values with a PUT request. A system administrator account is required for this REST API.

3.95.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the exceptions policy to edit.	string
Body	**body** *required*	The exceptions policy to modify.	PolicyExceptionsConfigurationExceptionsLockedOptions

3.95.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.95.4. Tags

- production

3.96. Delete an existing Exceptions policy

```
DELETE /api/v1/policies/exceptions/{id}
```

3.96.1. Description

Deletes an existing Exceptions policy. A system administrator account is required for this REST API.

3.96.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the Exceptions policy to delete.	string

3.96.3. Responses

HTTP Code	Description	Schema
204	Deleted the resource. If the resource did not exist prior to the call, 204 is still returned.	No Content

3.96.4. Tags

- production

3.97. Update exceptions policies

```
PATCH /api/v1/policies/exceptions/{id}
```

3.97.1. Description

Updates exceptions policies by PATCH. A system administrator account is required for this REST API.

3.97.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the exceptions policy to update.	string
Body	**body** *required*	The exceptions policy to modify.	PolicyExceptionsConfigurationExceptionsLockedOptions

3.97.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.97.4. Tags

- production

3.98. Creates a new HID policy

```
POST /api/v1/policies/hid
```

3.98.1. Description

Creates a new High Intensity Detection (HID) policy. A system administrator account is required for this REST API.

3.98.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The HID policy to create.	PolicyHidConfigurationObject
Body	**body** *optional*		HttpServletResponse

3.98.3. Responses

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content

3.98.4. Tags

- production

3.99. Get the HID policy payload for a specified policy ID

```
GET /api/v1/policies/hid/{id}
```

3.99.1. Description

Get the HID policy payload for a specified policy ID. A system administrator account is required for this REST API.

3.99.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the HID policy to get.	string

3.99.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	Policy

3.99.4. Tags

- production

3.100. Modify existing HID policy values

```
PUT /api/v1/policies/hid/{id}
```

3.100.1. Description

Modifies existing HID policy values. A system administrator account is required for this REST API.

3.100.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the HID policy to edit.	string
Body	**body** *required*	The HID policy to be modified.	PolicyHidConfigurationObject

3.100.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.100.4. Tags

- production

3.101. Delete an existing HID policy

```
DELETE /api/v1/policies/hid/{id}
```

3.101.1. Description

Deletes an existing HID policy. A system administrator account is required for this REST API.

3.101.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the HID policy to delete.	string

3.101.3. Responses

HTTP Code	Description	Schema
204	Deleted the resource. If the resource did not exist prior to the call, 204 is still returned.	No Content

3.101.4. Tags

- production

3.102. Update an HID policy

```
PATCH /api/v1/policies/hid/{id}
```

3.102.1. Description

Updates an HID policy by PATCH. A system administrator account is required for this REST API.

3.102.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the HID policy to update.	string
Body	**body** *required*	The HID policy to be modified.	PolicyHidConfigurationObject

3.102.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.102.4. Tags

- production

3.103. Create a new licensing setting

```
POST /api/v1/policies/licensing
```

3.103.1. Description

Creates a new licensing setting. A system administrator account is required for this REST API.

3.103.2. Parameters

Type	Name	Schema
Body	**body** *optional*	LicensingPolicyPayload
Body	**body** *optional*	HttpServletResponse

3.103.3. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content

3.103.4. Tags

- production

3.104. Get the LiveUpdate settings policy for specified policy ID

```
GET /api/v1/policies/lu/{id}
```

3.104.1. Description

Gets the LiveUpdate settings policy for specified policy ID. A system administrator account is required for this REST API.

3.104.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the LiveUpdate settings policy to get.	string

3.104.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	Policy

3.104.4. Tags

- production

3.105. Create a new MEM policy

```
POST /api/v1/policies/mem
```

3.105.1. Description

Creates a new Memory Exploit Mitigation (MEM) policy. A system administrator account is required for this REST API.

3.105.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The MEM policy to be created.	PolicyMemConfigurationMemLockedOptions
Body	**body** *optional*		HttpServletResponse

3.105.3. Responses

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content
400	The parameters are invalid.	No Content

HTTP Code	Description	Schema
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.105.4. Tags

- production

3.106. Get the MEM Policy payload for a specified policy ID

```
GET /api/v1/policies/mem/{id}
```

3.106.1. Description

Gets the MEM Policy payload for a specified policy ID. A system administrator account is required for this REST API.

3.106.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the MEM policy to get.	string

3.106.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	Policy
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.106.4. Tags

- production

3.107. Modify existing MEM policy values

```
PUT /api/v1/policies/mem/{id}
```

3.107.1. Description

Modifies existing MEM policy values. A system administrator account is required for this REST API.

3.107.2. Parameters

Type	Name	Description	Schema

Type	Name	Description	Schema
Path	**id** *required*	The ID of the MEM policy to edit.	string
Body	**body** *required*	The MEM policy to modify.	PolicyMemConfigurationMemLockedOptions

3.107.3. Responses

HTTP Code	Description	Schema
200	The web service processed and updated the policy.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.107.4. Tags

- production

3.108. Delete an existing MEM policy

```
DELETE /api/v1/policies/mem/{id}
```

3.108.1. Description

Deletes an existing MEM policy. A system administrator account is required for this REST API.

3.108.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the MEM policy to delete.	string

3.108.3. Responses

HTTP Code	Description	Schema
204	The resource was deleted. If the resource did not exist prior to the call, 204 is still returned.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.108.4. Tags

- production

3.109. Update a MEM policy

```
PATCH /api/v1/policies/mem/{id}
```

3.109.1. Description

Updates a MEM policy by PATCH. A system administrator account is required for this REST API.

3.109.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the MEM policy to update.	string
Body	**body** *required*	The MEM policy to modify.	PolicyMemConfigurationMemLockedOptions

3.109.3. Responses

HTTP Code	Description	Schema
200	The web service processed and updated the policy.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.109.4. Tags

- production

3.110. Get the policy summary for a specified policy type

```
GET /api/v1/policies/summary
```

3.110.1. Description

Gets the policy summary for a specified policy type. Also gets the list of groups to which the policies are assigned.

3.110.2. Parameters

Type	Name	Description	Schema
Query	**domainId** *optional*	If present, get policies from this domain. Otherwise, get policies from the logged-on domain.	string

3.110.3. Responses

HTTP Code	Schema
200	No Content

3.110.4. Tags

- production

3.111. Get the policy summary for specified policy type; get the list of groups to which the policies are assigned

```
GET /api/v1/policies/summary/{policy_type}
```

3.111.1. Parameters

Type	Name	Description	Schema
Path	**policy_type** *required*	Gets a summary for all the policies of this type.	string
Query	**domainId** *optional*	If present, get policies from this domain. Otherwise, get policies from the logged-on domain.	string

3.111.2. Responses

HTTP Code	Schema
200	No Content

3.111.3. Tags

- production

3.112. Create a new TDAD policy

```
POST /api/v1/policies/tdad
```

3.112.1. Description

Creates a new Threat Defense for Active Directory (TDAD) policy. A system administrator account is required for this REST API.

3.112.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The TDAD policy to create.	PolicyTdadConfigurationObject
Body	**body** *optional*		HttpServletRequest
Body	**body** *optional*		HttpServletResponse

3.112.3. Responses

HTTP Code	Description	Schema
201	The web service processed and the resource was created.	No Content

3.112.4. Tags

- production

3.113. Get the TDAD policy payload for a specified policy ID

```
GET /api/v1/policies/tdad/{id}
```

3.113.1. Description

Gets the TDAD policy payload for a specified policy OD. A system administrator account is required for this REST API.

3.113.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the TDAD policy to get.	string
Body	**body** *optional*		HttpServletRequest

3.113.3. Responses

HTTP Code	Description	Schema
200	The operation completed	Policy

3.113.4. Tags

- production

3.114. Modify existing TDAD policy values

```
PUT /api/v1/policies/tdad/{id}
```

3.114.1. Description

Modifies existing TDAD policy values. A system administrator account is required for this REST API.

3.114.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the TDAD policy to modify.	string
Body	**body** *required*	The TDAD policy to modify.	PolicyTdadConfigurationObject
Body	**body** *optional*		HttpServletRequest

3.114.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.114.4. Tags

- production

3.115. Delete an existing TDAD policy

```
DELETE /api/v1/policies/tdad/{id}
```

3.115.1. Description

Deletes an existing TDAD policy. A system administrator account is required for this REST API.

3.115.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the TDAD policy to delete.	string
Body	**body** *optional*		HttpServletRequest

3.115.3. Responses

HTTP Code	Description	Schema
204	Deleted the existing TDAD policy. If the resource did not exist prior to the call, 204 is still returned.	No Content

3.115.4. Tags

- production

3.116. Update TDAD policies by patch

```
PATCH /api/v1/policies/tdad/{id}
```

3.116.1. Description

Update TDAD policies by patch. A system administrator account is required for this REST API.

3.116.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the TDAD policy to update.	string
Body	**body** *required*	The TDAD policy to modify.	PolicyTdadConfigurationObject
Body	**body** *optional*		HttpServletRequest

3.116.3. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.116.4. Tags

- production

3.117. Add a blacklist as a file fingerprint list to SEPM

```
POST /api/v1/policy-objects/fingerprints
```

3.117.1. Description

Adds a blacklist as a file fingerprint list to Symantec Endpoint Protection Manager. A system administrator account is required for this REST API.

3.117.2. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The blacklist to be added.	BlacklistPayload

3.117.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	No Content
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
409	The request could not be completed due to a conflict with the current state of the target resource. The file fingerprint already exists.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.117.4. Tags

- production

3.118. Get the file fingerprint list for a specified name as a set of hash values

```
GET /api/v1/policy-objects/fingerprints
```

3.118.1. Description

Gets the file fingerprint list for a specified name as a set of hash values. A system administrator account is required for this REST API.

3.118.2. Parameters

Type	Name	Description	Schema
Query	**domainId** *optional*	The domain for the file fingerprint list.	string
Query	**name** *required*	The name of the file fingerprint list.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.118.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	FingerPrintList
400	The parameters are invalid.	No Content

HTTP Code	Description	Schema
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.118.4. Tags

- production

3.119. Update an existing blacklist

```
POST /api/v1/policy-objects/fingerprints/{id}
```

3.119.1. Description

Updates an existing blacklist. A system administrator account is required for this REST API.

3.119.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the file fingerprint list to update.	string
Body	**body** *required*	The fingerprint list to update.	BlacklistPayload

3.119.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
410	Cannot find the specified object.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.119.4. Tags

- production

3.120. Get the file fingerprint list for a specified ID as a set of hash values

```
GET /api/v1/policy-objects/fingerprints/{id}
```

3.120.1. Description

Gets the file fingerprint list for a specified ID as a set of hash values. A system administrator account is required for this REST API.

3.120.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the file fingerprint list.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.120.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	FingerPrintList
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.120.4. Tags

- production

3.121. Delete an existing blacklist, and remove it from a group to which it applies

```
DELETE /api/v1/policy-objects/fingerprints/{id}
```

3.121.1. Description

Deletes an existing blacklist, and removes it from a group to which it applies. A system administrator account is required for this REST API.

3.121.2. Parameters

Type	Name	Description	Schema
Path	**id** *required*	The ID of the file fingerprint list to delete.	string

3.121.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	string
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
410	Cannot find the specified object.	No Content

HTTP Code	Description	Schema
500	The web service encountered an error while processing the web request.	No Content

3.121.4. Tags

- production

3.122. Check whether a site has a replication partner

```
GET /api/v1/replication/is_replicated
```

3.122.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	boolean
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.122.2. Tags

- Symantec Endpoint Protection Manager data replication-related operations.

3.123. Initiate replication for the specified replication partner

```
POST /api/v1/replication/replicatenow
```

3.123.1. Description

Initiates replication for the specified replication partner. A system administrator account is required for this REST API.

3.123.2. Parameters

Type	Name	Description	Schema
Query	**content** *required*	Replicate Content And Packages.	boolean
Query	**logs** *required*	Replicate Logs	boolean
Query	**partnerSiteName** *required*	Replication partner site name.	string
Body	**body** *optional*	Only used internally.	HttpServletRequest

3.123.3. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ReplicationAllStatus
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.123.4. Tags

- Symantec Endpoint Protection Manager data replication-related operations.

3.124. Get the replication status

```
GET /api/v1/replication/status
```

3.124.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ReplicationStatusResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.124.2. Tags

- Symantec Endpoint Protection Manager data replication-related operations.

3.125. Authenticate and return a PHP session token for a valid user

```
POST /api/v1/reporting/authenticate
```

3.125.1. Parameters

Type	Name	Description	Schema
Body	**body** *required*	The credentials used to log on to Symantec Endpoint Protection Manager.	UserCredential
Body	**body** *required*	Provided by default.	HttpServletRequest

3.125.2. Responses

HTTP Code	Description	Schema

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ReportingInfo
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.125.3. Tags

- Symantec Endpoint Protection Manager authentication-related reporting operations.

3.126. Get the current user token object

```
GET /api/v1/sessions/currentuser
```

3.126.1. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.126.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	UserToken

3.126.3. Tags

- Allows you to get current user session object

3.127. Get a list of threats that were automatically resolved

```
GET /api/v1/stats/autoresolved/{reportType}/{startTime}/to/{endTime}
```

3.127.1. Description

Gets a list of threats that were automatically resolved. Threats include viruses, spyware, and risks.

3.127.2. Parameters

Type	Name	Description	Schema
Path	**endTime** *required*	The end time for gathering these statistics.	integer (int64)
Path	**reportType** *required*	The format of the report for the display of the statistics that you request. Report types are Hour, Day, Week, and Month.	string
Path	**startTime** *required*	The start time for gathering these statistics.	integer (int64)

Type	Name	Description	Schema
Query	**timeZone** *optional*	The time zone of the returned events. The default is UTC.	string

3.127.3. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	AutoResolvedAttacksResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.127.4. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.128. Get a list of clients for a group by content version

```
GET /api/v1/stats/client/content
```

3.128.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ClientDefStatusResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.128.2. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.129. Get a list and count of client groups by content download sources

```
GET /api/v1/stats/client/content/sources
```

3.129.1. Parameters

Type	Name	Description	Schema
Query	**locale** *optional*	The locale specified and the language in which to return results. The default is en-US.	string

3.129.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ContentDownloadSourceResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.129.3. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.130. Get a list and count of infected clients for a specified time range

```
GET /api/v1/stats/client/infection/{reportType}/{startTime}/to/{endTime}
```

3.130.1. Parameters

Type	Name	Description	Schema
Path	**endTime** *required*	The end time for gathering these statistics.	integer (int64)
Path	**reportType** *required*	The type of report. Report types are Hour, Day, Week, and Month.	string
Path	**startTime** *required*	The start time for gathering these statistics.	integer (int64)
Query	**timeZone** *optional*	The time zone of the returned events. The default is UTC.	string

3.130.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	InfectedClientStatsResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.130.3. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.131. Get a list for a specified time range of clients reporting malware events

```
GET /api/v1/stats/client/malware/{reportType}/{startTime}/to/{endTime}
```

3.131.1. Parameters

Type	Name	Description	Schema
Path	**endTime** *required*	The end time for gathering these statistics.	integer (int64)
Path	**reportType** *required*	The type of report. Report types are Hour, Day, Week, and Month.	string
Path	**startTime** *required*	The start time for gathering these statistics.	integer (int64)
Query	**timeZone** *optional*	The time zone of the returned events. The default is UTC.	string

3.131.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	MalwareClientStatsResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.131.3. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.132. Get a list and count of the online and offline clients

```
GET /api/v1/stats/client/onlinestatus
```

3.132.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ClientsOnlineStatsResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.132.2. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.133. Get a list for a specified time range the risk distribution by protection technology information for the given time range

```
GET /api/v1/stats/client/risk/{startTime}/to/{endTime}
```

3.133.1. Parameters

Type	Name	Description	Schema
Path	**endTime** *required*	The end time for gathering these statistics.	integer (int64)
Path	**startTime** *required*	The start time for gathering these statistics.	integer (int64)
Query	**timeZone** *optional*	The time zone of the returned events. The default is UTC.	string

3.133.2. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	RiskDistributionStatsResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.133.3. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.134. Get a list and count of clients by client product version

```
GET /api/v1/stats/client/version
```

3.134.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	ClientVersionResponse
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.134.2. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.135. Get the current threat statistics

```
GET /api/v1/stats/threat
```

3.135.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.135.2. Tags

- Symantec Endpoint Protection Manager reporting statistic information.

3.136. Create a new TDAD global policy

```
POST /api/v1/tdad
```

3.136.1. Parameters

Type	Name	Schema
Body	**body** *optional*	AdDomainPolicies
Body	**body** *optional*	HttpServletRequest

3.136.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.136.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.137. Get all TDAD policies

```
GET /api/v1/tdad
```

3.137.1. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.137.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.137.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.138. Update an existing TDAD policy.

```
PUT /api/v1/tdad
```

3.138.1. Parameters

Type	Name	Schema
Body	**body** *optional*	AdDomainPolicies
Body	**body** *optional*	HttpServletRequest

3.138.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.138.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.139. Delete all TDAD data

```
DELETE /api/v1/tdad
```

3.139.1. Parameters

Type	Name	Schema
Body	**body** *optional*	HttpServletRequest

3.139.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.139.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.140. Update an existing TDAD policy

```
PATCH /api/v1/tdad
```

3.140.1. Parameters

Type	Name	Schema
Body	**body** *optional*	AdDomainPolicies
Body	**body** *optional*	HttpServletRequest

3.140.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.140.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.141. Get a TDAD policy for the specified Active Directory domain UID and policy UID

```
GET /api/v1/tdad/{adDomainUid}/{policyUid}
```

3.141.1. Parameters

Type	Name	Description	Schema
Path	**adDomainUid** *required*	The Active Directory domain UID.	string
Path	**policyUid** *required*	The policy UID for the given AD domain	string
Body	**body** *optional*		HttpServletRequest

3.141.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.141.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.142. Deletes the TDAD data for the specified Active Directory domain UID and policy UID.

```
DELETE /api/v1/tdad/{adDomainUid}/{policyUid}
```

3.142.1. Parameters

Type	Name	Description	Schema
Path	**adDomainUid** *required*	The Active Directory domain UID.	string

Type	Name	Description	Schema
Path	**policyUid** *required*	The policy UID for the given AD domain.	string
Body	**body** *optional*		HttpServletRequest

3.142.2. Responses

HTTP Code	Description	Schema
200	The operation completed.	string

3.142.3. Tags

- Symantec Endpoint Protection Manager Threat Defense for Active Directory related operations.

3.143. Get the current version of Symantec Endpoint Protection Manager

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

3.143.1. Responses

HTTP Code	Description	Schema
200	The web service processed the web request and returned a result.	< string, object > map
400	The parameters are invalid.	No Content
401	The user that is currently logged on has insufficient rights to execute the web method, or the user is unauthorized.	No Content
404	The requested resource was not found.	No Content
500	The web service encountered an error while processing the web request.	No Content

3.143.2. Tags

- production

4. Definitions

4.1. AdDomainPolicies

Name	Schema
ad_domain_policies *optional*	< Policy > array

4.2. AddAdminEntry

Name	Description	Schema
adminType *required*	The type of administrator. Possible values are 1 for system administrator, 2 for domain administrator, and 3 for limited administrator. **Minimum value** : `1` **Maximum value** : `3`	integer (int32)
authenticationMethod *required*	The administrator's authentication method. Possible values are 0 for Symantec Endpoint Protection Manager Authentication, 1 for RSA SecurID Authentication, and 2 for Directory Authentication. **Minimum value** : `0` **Maximum value** : `2`	integer (int32)
emailAddress *required*	The administrator's email address.	string
fullName *optional*	The administrator's full name. **Length** : `0 - 50`	string
id *optional*	The administrator's ID.	string
isReportingRights *optional*	**Default** : `false`	boolean
lockAccount *optional*	Indicates whether the administrator's account is configured to lock after a specified number of logon failures. **Default** : `false`	boolean
lockTimeThreshold *required*	The amount of time the administrator's account is locked after a logon failure. **Minimum value** : `1` **Maximum value** : `60`	integer (int32)
loginAttemptThreshold *required*	The number of logon failures allowed before the administrator's account is locked. **Minimum value** : `1` **Maximum value** : `10`	integer (int32)
loginName *required*	The administrator's logon name. **Length** : `1 - 20`	string
notifyAdminOfLockedState *optional*	Indicates whether to notify the administrator that the account is locked due to logon failures. **Default** : `false`	boolean

Name	Description	Schema
password *required*	The administrator's password. **Length** : `6 - 256`	string
reportingRights *optional*	The administrator's reporting rights. Not currently used. **Default** : `false`	boolean

4.3. AdminEntry

Name	Description	Schema
emailAddress *required*	The administrator's email address.	string
fullName *optional*	The administrator's full name. **Length** : `0 - 50`	string
lockAccount *optional*	Indicates whether the administrator's account is configured to lock after a specified number of logon failures. **Default** : `false`	boolean
lockTimeThreshold *required*	The amount of time the administrator's account is locked after a logon failure. **Minimum value** : `1` **Maximum value** : `60`	integer (int32)
loginAttemptThreshold *required*	The number of logon failures allowed before the administrator's account is locked. **Minimum value** : `1` **Maximum value** : `10`	integer (int32)
notifyAdminOfLockedState *optional*	Indicates whether to notify the administrator that the account is locked due to logon failures. **Default** : `false`	boolean

4.4. AdminSummaryDetails

Name	Description	Schema
adminType *required*	The type of administrator. Possible values are 1 for system administrator, 2 for domain administrator, and 3 for limited administrator.	integer (int32)
attemptThreshold *required*	The number of logon failures allowed before the administrator's account is locked.	string
authenticationMethod *required*	The administrator's authentication method. Possible values are 0 for Symantec Endpoint Protection Manager Authentication, 1 for RSA SecurID Authentication, and 2 for Directory Authentication.	integer (int32)
companyName *required*	The administrator's company name.	string
creationTime *required*	Indicates when the administrator account was created.	integer (int64)

Name	Description	Schema
email *required*	The administrator's email address.	string
enabled *required*	Indicates whether the administrator is enabled. **Default** : `false`	boolean
failedLoginCount *required*	The number of times the administrator's logon has failed.	integer (int32)
fullName *optional*	The administrator's full name.	string
id *optional*	The administrator's ID.	string
lastLoginTime *required*	The administrator's last logon time.	integer (int64)
lastLogonIP *required*	The administrator's last logon IP address.	string
lastPasswordChanged *required*	Indicates when the administrator's password was last changed.	integer (int64)
lockAccount *optional*	Indicates whether the administrator's account is configured to lock after a specified number of logon failures. **Default** : `false`	boolean
lockStatus *required*	Indicates whether the administrator is locked. **Default** : `false`	boolean
lockTimeThreshold *required*	The amount of time the administrator's account is locked after a logon failure.	integer (int32)
loginName *required*	The administrator's logon name.	string
notifyAdminOfLockedState *optional*	Indicates whether to notify the administrator that the account is locked due to logon failures. **Default** : `false`	boolean
onlineStatus *required*	Indicates whether the administrator is online or offline. **Default** : `false`	boolean
passwordExpiresIn *required*	Indicates when the administrator's password expires.	integer (int64)

4.5. AutoResolvedAttacks

Name	Description	Schema
autoResolvedAttacksCount *required*	The number of attacks that were automatically resolved during a specified time period.	integer (int32)
epochTime *required*	The time at the end of the specified time period during which attacks were automatically resolved.	integer (int64)

4.6. AutoResolvedAttacksResponse

Name	Description	Schema
getautoResolvedAttacks *required*	A list of attacks that were automatically resolved. Each item on the list contains a count of attacks during a specified time period.	< AutoResolvedAttacks > array
lastUpdated *required*	The last time the client responded to a request to update the last time an attack was automatically resolved.	integer (int64)

4.7. BinaryFile

Name	Description	Schema
checksum *required*	A binary file's checksum value.	string
fileSize *required*	A binary file's size.	integer (int32)
id *required*	A binary file's ID.	string

4.8. BlacklistPayload

Name	Description	Schema
data *required*	The blacklist file's data.	< string > array
description *required*	The blacklist file's description.	string
domainId *required*	The domain ID to which the blacklist file is applied.	string
hashType *required*	The blacklist file's hash type. Possible values are MD5 or SHA256.	string
name *required*	The blacklist file's ID. This field is not required at the blacklist file's creation, but when the blacklist file is updated, this field is required.	string

4.9. BufferedReader

Type : object

4.10. CASServerConfig

Name	Description	Schema
password *optional*		string
url *optional*		string
username *optional*		string

Name	Description	Schema
verifyCertificate *optional*	**Default** : `false`	boolean

4.11. CASVersionResult

Name	Description	Schema
cas_minimum_version_supported *optional*		string
cas_server_valid *optional*	**Default** : `false`	boolean
cas_server_version *optional*		string
ssl_handshake_failed *optional*	**Default** : `false`	boolean

4.12. ClientDefStatus

Name	Description	Schema
clientsCount *required*	The number of clients that use this definition revision number.	integer (int32)
version *required*	The client's definition revision number.	string

4.13. ClientDefStatusResponse

Name	Description	Schema
clientDefStatusList *required*	The list of client definition revision numbers.	< ClientDefStatus > array
lastUpdated *required*	The last time the client updated its definition revision number.	integer (int64)

4.14. ClientVersion

Name	Description	Schema
clientsCount *required*	The number of clients on each product version.	integer (int32)
formattedVersion *required*	The formatted product version number. For example, 14.0.1.1 (14.0.1 MP1) build 3876.	string
version *required*	The client's product version number.	string

4.15. ClientVersionResponse

Name	Description	Schema

Name	Description	Schema
clientVersionList *required*	The list of client versions.	< ClientVersion > array
lastUpdated *required*	The last time the client updated its client version.	integer (int64)

4.16. ClientsOnlineStats

Name	Description	Schema
clientsCount *required*	The number of clients.	integer (int32)
status *required*	The client's online status. Possible values are online or offline.	string

4.17. ClientsOnlineStatsResponse

Name	Description	Schema
clientCountStatsList *required*	A list of the online or offline status of the clients.	< ClientsOnlineStats > array
lastUpdated *required*	The last time the client updated its online status.	integer (int64)

4.18. CloudModeCommandData

Name	Description	Schema
cloud_customer_id *optional*		string
cloud_domain_id *optional*		string
computer_ids *optional*	The list of computer GUIDs to which to apply the license entitlement.	< string > array
connect_token *optional*		string
group_ids *optional*	The list of group IDs to which to apply the license entitlement.	< string > array
hardware_ids *optional*		< string > array
targets *required*		CommandTargets

4.19. CloudServerCertificate

Name	Description	Schema

Name	Description	Schema
content *optional*	The certificate's contents.	string
name *optional*	The certificate name.	string

4.20. CommandTargets

Name	Description	Schema
computer_ids *optional*	The list of computer GUIDs to which to apply the license entitlement.	< string > array
group_ids *optional*	The list of group IDs to which to apply the license entitlement.	< string > array
hardware_ids *optional*		< string > array

4.21. Computer

Name	Description	Schema
agentId *optional*		string
agentTimeStamp *optional*		integer (int64)
agentType *optional*		string
agentUsn *optional*		integer (int64)
agentVersion *optional*		string
apOnOff *optional*		integer (int32)
atpDeviceId *optional*		string
atpServer *optional*		string
attributeExtension *optional*		string
avEngineOnOff *optional*		integer (int32)
bashStatus *optional*		integer (int32)

Name	Description	Schema
biosVersion *optional*		string
bwf *optional*		integer (int32)
cidsBrowserFfOnOff *optional*		integer (int32)
cidsBrowserIeOnOff *optional*		integer (int32)
cidsDefsetVersion *optional*		string
cidsDrvMulfCode *optional*		integer (int32)
cidsDrvOnOff *optional*		integer (int32)
cidsEngineVersion *optional*		string
cidsSilentMode *optional*		integer (int32)
computerDescription *optional*		string
computerName *optional*		string
computerTimeStamp *optional*		integer (int64)
computerUsn *optional*		integer (int64)
contentUpdate *optional*		integer (int64)
creationTime *optional*		integer (int64)
currentClientId *optional*		string
daOnOff *optional*		integer (int32)
deleted *optional*		integer (int32)
department *optional*		string

Name	Description	Schema
deploymentMessage *optional*		string
deploymentPreVersion *optional*		string
deploymentRunningVersion *optional*		string
deploymentStatus *optional*		string
deploymentTargetVersion *optional*		string
description *optional*		string
dhcpServer *optional*		string
diskDrive *optional*		string
dnsServers *optional*		< string > array
domainOrWorkgroup *optional*		string
edrStatus *optional*		integer (int32)
elamOnOff *optional*		integer (int32)
email *optional*		string
employeeNumber *optional*		string
employeeStatus *optional*		string
encryptedDevicePassword *optional*		string
fbwf *optional*		integer (int32)
firewallOnOff *optional*		integer (int32)
freeDisk *optional*		integer (int64)

Name	Description	Schema
freeMem *optional*		integer (int64)
fullName *optional*		string
gateways *optional*		< string > array
group *optional*		GroupSummary
groupUpdateProvider *optional*	**Default** : `false`	boolean
hardwareKey *optional*		string
homePhone *optional*		string
hypervisorVendorId *optional*		string
idsChecksum *optional*		string
idsSerialNo *optional*		string
idsVersion *optional*		string
infected *optional*		integer (int32)
installType *optional*		string
ipAddresses *optional*		< string > array
isGrace *optional*		integer (int32)
isNpvdiClient *optional*		integer (int32)
jobTitle *optional*		string
kernel *optional*		string
lastConnectedIpAddr *optional*		string

Name	Description	Schema
lastDeploymentTime *optional*		integer (int64)
lastDownloadTime *optional*		integer (int64)
lastHeuristicThreatTime *optional*		integer (int64)
lastScanTime *optional*		integer (int64)
lastServerId *optional*		string
lastServerName *optional*		string
lastSiteId *optional*		string
lastSiteName *optional*		string
lastUpdateTime *optional*		integer (int64)
lastVirusTime *optional*		integer (int64)
licenseExpiry *optional*		integer (int64)
licenseId *optional*		string
licenseStatus *optional*		integer (int32)
logicalCpus *optional*		integer (int32)
loginDomain *optional*		string
logonUserName *optional*		string
macAddresses *optional*		< string > array
majorVersion *optional*		integer (int32)
memory *optional*		integer (int64)

Name	Description	Schema
minorVersion *optional*		integer (int32)
mobilePhone *optional*		string
officePhone *optional*		string
onlineStatus *optional*		integer (int32)
operatingSystem *optional*		string
osBitness *optional*		string
osElamStatus *optional*		integer (int32)
osFlavorNumber *optional*		integer (int32)
osFunction *optional*		enum (Unknown, Workstation, DomainController, Server)
osLanguage *optional*		string
osMajor *optional*		integer (int32)
osMinor *optional*		integer (int32)
osName *optional*		string
osServicePack *optional*		string
osVersion *optional*		string
osbitness *optional*		string
osflavorNumber *optional*		integer (int32)
osfunction *optional*		enum (Unknown, Workstation, DomainController, Server)

Name	Description	Schema
oslanguage *optional*		string
osmajor *optional*		integer (int32)
osminor *optional*		integer (int32)
osname *optional*		string
osservicePack *optional*		string
osversion *optional*		string
patternIdx *optional*		string
pepOnOff *optional*		integer (int32)
physicalCpus *optional*		integer (int32)
processorClock *optional*		integer (int64)
processorType *optional*		string
profileChecksum *optional*		string
profileSerialNo *optional*		string
profileVersion *optional*		string
ptpOnOff *optional*		integer (int32)
publicKey *optional*		string
quarantineDesc *optional*		string
rebootReason *optional*		string
rebootRequired *optional*		integer (int32)

Name	Description	Schema
securityVirtualAppliance *optional*		string
serialNumber *optional*		string
snacLicenseId *optional*		string
subnetMasks *optional*		< string > array
svaId *optional*		string
tamperOnOff *optional*		integer (int32)
tdadGlobalDataDownloadTime *optional*		integer (int64)
tdadOnOff *optional*		integer (int32)
tdadStatusId *optional*		integer (int32)
telemetryHwid *optional*		string
telemetryMid *optional*		string
timeZone *optional*		integer (int32)
tmpDevice *optional*		string
totalDiskSpace *optional*		integer (int64)
tpmDevice *optional*		string
uniqueId *optional*		string
uuid *optional*		string
uwf *optional*		integer (int32)
virtualizationPlatform *optional*		string

Name	Description	Schema
vsicStatus *optional*		integer (int32)
winServers *optional*		< string > array
worstInfectionIdx *optional*		string
writeFiltersStatus *optional*		string

4.22. ComputerPayload

Name	Description	Schema
deviceId *required*	The computer's device ID, generated by Symantec Advanced Threat Protection. **Length** : `1 - 36`	string
devicePassword *required*	The computer's password, generated by Symantec Advanced Threat Protection. **Length** : `1 - 1024`	string
hardwareKey *required*	The computer's hardware key.	string
objectValid *optional*	For internal use by Symantec Endpoint Protection Manager. **Default** : `false`	boolean
publicKey *required*	The computer's public key. **Length** : `1 - 512`	string

4.23. ContentDownloadSource

Name	Description	Schema
clientCount *required*	A count of clients by content download source.	integer (int32)
sourceKey *required*	The key that identifies the content download source. Possible values are SEPM, GUP, PUBLIC_LU, INTERNAL_LUA, or OTHER.	string
sourceName *required*	The name of the content download source. Possible values are Symantec Endpoint Protection Manager, Group Update Provider, LiveUpdate, Internal LiveUpdate, or Other.	string

4.24. ContentDownloadSourceResponse

Name	Description	Schema
downloadSources *required*	A list of the available client download sources.	< ContentDownloadSource > array

Name	Description	Schema
lastUpdated *required*	The last time the client updated this information.	integer (int64)

4.25. ContentThreshold

Name	Description	Schema
minimumagedays *optional*	The content's minimum age, in days.	string
moniker *optional*	The content's moniker.	string

4.26. Cookie

Name	Description	Schema
comment *optional*		string
domain *optional*		string
maxAge *optional*		integer (int32)
name *optional*		string
path *optional*		string
secure *optional*	**Default** : `false`	boolean
value *optional*		string
version *optional*		integer (int32)

4.27. CriticalEventsInfo

Name	Description	Schema
acknowledged *required*	Specifies whether the notification has been acknowledged.	integer (int32)
eventDateTime *required*	The notification's time.	string
eventId *required*	The notification's ID.	string
message *required*	The notification's message.	string

Name	Description	Schema
subject *required*	The notification's subject.	string

4.28. CriticalEventsResponse

Name	Description	Schema
criticalEventsInfoList *required*	The list of unacknowledged notifications.	< CriticalEventsInfo > array
lastUpdated *required*	The last time the client updated its critical event status.	integer (int64)
totalUnacknowledgedMessages *required*	The number of unacknowledged notifications.	integer (int32)

4.29. DirectoryServerIntegrationConfiguration

Name	Description	Schema
enable *optional*	Specify whether directory server integration sync is enabled. Possible values are true and false. **Default** : `false`	boolean

4.30. DomainAddEditTO

Name	Description	Schema
administratorCount *optional*		integer (int32)
allowNeverExpiresPasswords *required*	Specifies whether to allow passwords in the Symantec Endpoint Protection Manager domain to never expire. **Default** : `false`	boolean
allowUsersToSaveCredentials *required*	Specifies whether to allow the user to save credentials when logging on to Symantec Endpoint Protection Manager. **Default** : `false`	boolean
bannerText *optional*	The banner's message.	string
bannerTitle *optional*	The banner's title.	string
companyName *optional*		string
contactInfo *optional*		string
createdTime *optional*		integer (int64)

Name	Description	Schema
deleteOldClients *required*	Specifies whether to delete clients that have not been connected to Symantec Endpoint Protection Manager for a given number of days. **Default** : `false`	boolean
deleteOldClientsDays *required*	The number of days after which Symantec Endpoint Protection Manager deletes clients that have not connected.	integer (int32)
deleteOldVDIClients *required*	Specifies whether to delete virtual desktop infrastructure (VDI) clients that have not been connected to Symantec Endpoint Protection Manager for a given number of days. **Default** : `false`	boolean
deleteOldVDIClientsDays *required*	The number of days after which Symantec Endpoint Protection Manager deletes virtual desktop infrastructure (VDI) clients that have not connected.	integer (int32)
description *optional*		string
enable *optional*	**Default** : `false`	boolean
id *optional*		string
name *optional*		string
showBanner *required*	Specifies whether to show a logon banner when an administrator logs on to this domain. **Default** : `false`	boolean

4.31. DomainEntry

Name	Description	Schema
allowNeverExpiringPasswords *required*	Specifies whether to allow passwords in the Symantec Endpoint Protection Manager domain to never expire. **Default** : `false`	boolean
allowSavingCredentials *required*	Specifies whether to allow the user to save credentials when logging on to Symantec Endpoint Protection Manager. **Default** : `false`	boolean
companyName *optional*	The Symantec Endpoint Protection Manager domain's company name. **Length** : `0 - 1024`	string
contactList *optional*	The contact list for the Symantec Endpoint Protection Manager domain. This list can include the phone number, name, or email. **Length** : `0 - 2048`	string

Name	Description	Schema
deleteIdleClients *required*	Specifies whether to delete clients that have not connected to Symantec Endpoint Protection Manager for a specified number of days. **Default** : `false`	boolean
deleteIdleNpvdiClients *required*	Specifies whether to delete virtual desktop infrastructure (VDI) clients that have not connected to Symantec Endpoint Protection Manager for a specified number of days. **Default** : `false`	boolean
displayLogonBanner *required*	Specifies whether to show a logon banner when an administrator logs on to this domain. **Default** : `false`	boolean
domainId *required*	The Symantec Endpoint Protection Manager domain's ID, which is a GUID.	string
domainName *required*	The Symantec Endpoint Protection Manager domain's name. **Length** : `1 - 256`	string
logonBannerText *optional*	The banner's message. **Length** : `0 - 2048`	string
logonBannerTitle *optional*	The banner's title. **Length** : `0 - 256`	string
maxClientIdleTimeInDays *required*	The number of days after which Symantec Endpoint Protection Manager deletes clients that have not connected. **Minimum value** : `1`	integer (int32)
maxNpvdiClientIdleTimeInDays *required*	The number of days after which Symantec Endpoint Protection Manager deletes virtual desktop infrastructure (VDI) clients that have not connected. **Minimum value** : `1`	integer (int32)

4.32. DomainSummary

Name	Schema
id *optional*	string
name *optional*	string

4.33. EPMPUserCredential

Name	Description	Schema
clientID *required*	For internal use. Email ID.	string
clientId *required*		string

Name	Description	Schema
clientSecret *required*	For internal use. Encrypted password.	string
epmpCustomerId *required*	For internal use. Customer ID. **Length** : `1 - 256`	string
epmpDomainId *required*	For internal use. SEPM domain ID. **Length** : `1 - 256`	string
masterSiteId *optional*		string

4.34. EnrollmentStatus

Name	Description	Schema
enrollment_state *optional*	The enrollment status of Symantec Endpoint Protection Manager to the Symantec Endpoint Protection cloud portal. Possible values are: 0: Unenrolled, 1: Enrolled, 2: Unenrollment Failed	integer (int32)
enrollment_time *optional*		integer (int64)
epmp_customer_id *optional*		string
epmp_domain_id *optional*		string
is_master *optional*	**Default** : `false`	boolean
is_master_site *optional*	**Default** : `false`	boolean
masterSite *optional*	**Default** : `false`	boolean
master_site_id *optional*		string

4.35. Enumeration

Type : object

4.36. ExceptionThreat

Name	Description	Schema
id *required*	The ID of the threat.	string
name *required*	The threat name.	string

4.37. ExceptionsApplicationToMonitor

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
name *required*	The process to detect.	string
rulestate *optional*	The options for the rule.	ExceptionsRuleState

4.38. ExceptionsConfiguration

Name	Description	Schema
applications *optional*	Applications that are indicated in the Exceptions policy.	< ExceptionsRuleApplication > array
applications_to_monitor *optional*	Monitored applications that are indicated in the Exceptions policy.	< ExceptionsApplicationToMonitor > array
blacklistrules *optional*	Blacklists that are indicated in the Exceptions policy.	< ExceptionsRuleBlacklist > array
certificates *optional*	Certificates that are indicated in the Exceptions policy.	< ExceptionsRuleCertificate > array
directories *optional*	Directories on Windows platforms that are indicated in the exceptions policy.	< ExceptionsRuleDirectory > array
dns_and_host_applications *optional*	DNS and host applications that are indicated in the Exceptions policy.	< ExceptionsRuleApplication > array
dns_and_host_blacklistrules *optional*	DNS and host blacklists that are indicated in the Exceptions policy.	< ExceptionsRuleDnsHostBlacklist > array
extension_list *optional*	Extensions on Windows platforms that are indicated in the Exceptions policy.	ExceptionsRuleExtensionList
files *optional*	Files on Windows platforms that are indicated in the exceptions policy.	< ExceptionsRuleFile > array
knownrisks *optional*	Known risks that are indicated in the Exceptions policy.	< ExceptionsRuleKnownRisk > array
linux *optional*	Linux configuration information that is indicated in the Exceptions policy.	ExceptionsLinuxConfiguration
mac *optional*	Mac files that are indicated in the Exceptions policy.	ExceptionsMacConfiguration
tamper_files *optional*	Tamper-protected files that are indicated in the Exceptions policy.	< ExceptionsRuleFile > array
webdomains *optional*	Trusted web domains that are indicated in the Exceptions policy.	< ExceptionsRuleDomain > array

4.39. ExceptionsFile

Name	Description	Schema
company *optional*	An optional attribute that indicates the name of the company that published the object.	string
directory *optional*	An optional attribute that indicates the directory where the object was originally found.	string
name *optional*	An optional attribute that indicates the name of the file object; for example, iexplore.exe.	string
sha2 *required*	The SHA-256, SHA-1, or MD5 checksum of the object content.	string
size *optional*	An optional attribute indicates the size of the object, in bytes; for example, 69472. **Minimum value** : `0` **Maximum value** : `9223372036854776000`	integer (int64)

4.40. ExceptionsFingerprint

Name	Description	Schema
algorithm *required*	The algorithm used to create the fingerprint. Only SHA-1 is supported for a certificate thumbprint for Symantec Endpoint Protection.	enum (SHA1)
value *required*	The hash value of the object content.	string

4.41. ExceptionsLinuxConfiguration

Name	Description	Schema
directories *optional*	Directories on Linux platforms that are indicated in the Exceptions policy.	< ExceptionsRuleLinuxDirectory > array
extension_list *optional*	Extensions on Linux platforms that are indicated in the Exceptions policy.	ExceptionsRuleExtensionList

4.42. ExceptionsLockedOptions

Name	Description	Schema
application *optional*	**Default** : `false`	boolean
certificate *optional*	**Default** : `false`	boolean
dnshostfile *optional*	**Default** : `false`	boolean
domain *optional*	**Default** : `false`	boolean

Name	Description	Schema
extension *optional*	**Default** : `false`	boolean
file *optional*	**Default** : `false`	boolean
knownrisk *optional*	**Default** : `false`	boolean
securityrisk *optional*	**Default** : `false`	boolean
sonar *optional*	**Default** : `false`	boolean

4.43. ExceptionsMacConfiguration

Name	Description	Schema
files *optional*	Files on Mac platforms that are indicated in the Exceptions policy.	< ExceptionsRuleMacFile > array

4.44. ExceptionsRuleApplication

Name	Description	Schema
action *optional*	The action of the threat in the Exceptions policy.	enum (IGNORE, LOG_ONLY)
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
processfile *required*	The process to ignore.	ExceptionsFile
rulestate *optional*	The options for the rule.	ExceptionsRuleState

4.45. ExceptionsRuleBlacklist

Name	Description	Schema
action *required*	The action to take on the process.	enum (BLOCK, QUARANTINE, DELETE)
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
processfile *required*	The process to block, delete, or quarantine.	ExceptionsFile
rulestate *optional*	The options for the rule.	ExceptionsRuleState

4.46. ExceptionsRuleCertificate

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
rulestate *optional*	The options for the rule.	ExceptionsRuleState
signature_company_name *optional*	The name of the company on the certificate.	string
signature_fingerprint *required*	The hash value of the digital certificate	ExceptionsFingerprint
signature_issuer *optional*	The issuer of the signature for the certificate.	string

4.47. ExceptionsRuleDirectory

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
directory *required*	The name of the folder.	string
pathvariable *required*	A prefix variable that indicates a well-known Windows folder.	enum (NONE, COMMON_APPDATA, COMMON_DESKTOPDIRECTORY, COMMON_DOCUMENTS, COMMON_PROGRAMS, COMMON_STARTUP, PROGRAM_FILES, PROGRAM_FILES_COMMON, SYSTEM, SYSTEM_DRIVE, USER_PROFILE, WINDOWS)
recursive *optional*	Indicates whether subfolders are also excluded. **Default** : `false`	boolean
rulestate *optional*	The options for the rule.	ExceptionsRuleState
scancategory *optional*	The type of security risk scan.	enum (GESC_AP, GESC_MANUAL, GESC_ALL)
scantype *optional*	The type of scan that excludes the folder.	enum (GEPT_RISK, GEPT_SECURITY_RISK, GEPT_HPP, GEPT_ADC, ALL)

4.48. ExceptionsRuleDnsHostBlacklist

Name	Description	Schema
action *required*	The action to take on the process.	enum (BLOCK, PROMPT)

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
processfile *required*	Indicates the process to block or prompt.	ExceptionsFile
rulestate *optional*	The options for the rule.	ExceptionsRuleState

4.49. ExceptionsRuleDomain

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
domain *required*	The URL domain extracted from the URL; for example, www.files.com or an ip address. Domain names can include wildcards.	string
rulestate *optional*	Rule options	ExceptionsRuleState

4.50. ExceptionsRuleExtensionList

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
extensions *required*	The extensions.	< string > array
rulestate *optional*	The options for the rule.	ExceptionsRuleState
scancategory *optional*	The scan category.	enum (GESC_AP, GESC_MANUAL, GESC_ALL)

4.51. ExceptionsRuleFile

Name	Description	Schema
SONAR *optional*	**Default** : `false`	boolean
applicationcontrol *optional*	Indicates whether to exclude this file from application control. **Default** : `false`	boolean
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
path *required*	The path to the object. The path is relative if pathvariable is defined. The path is full if pathvariable is [NONE] or not specified.	string

Name	Description	Schema
pathvariable *required*	A prefix variable that indicates a well-known Windows folder.	enum (NONE, COMMON_APPDATA, COMMON_DESKTOPDIRECTORY, COMMON_DOCUMENTS, COMMON_PROGRAMS, COMMON_STARTUP, PROGRAM_FILES, PROGRAM_FILES_COMMON, SYSTEM, SYSTEM_DRIVE, USER_PROFILE, WINDOWS)
recursive *optional*	Indicates whether to exclude child processes. **Default** : `false`	boolean
rulestate *optional*	The options for the rule.	ExceptionsRuleState
scancategory *optional*	The type of security risk scan.	enum (GESC_AP, GESC_MANUAL, GESC_ALL)
securityrisk *optional*	Indicates whether to exclude this file from a security risk. **Default** : `false`	boolean
sonar *optional*	Exclude this file from SONAR **Default** : `false`	boolean

4.52. ExceptionsRuleKnownRisk

Name	Description	Schema
action *optional*	The action to take on the threat, as defined in the exceptions policy.	enum (IGNORE, LOG_ONLY)
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
rulestate *optional*	The options for the rule.	ExceptionsRuleState
threat *required*	The threat defined in the exceptions policy.	ExceptionThreat

4.53. ExceptionsRuleLinuxDirectory

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
directory *required*	The name of the folder.	string
pathvariable *required*	A prefix variable that indicates a well-known Linux folder.	enum (NONE, HOME, ROOT, BIN, ETC, USR, OPT)

Name	Description	Schema
recursive *optional*	Indicates whether sub-folders are also excluded. **Default** : `false`	boolean
rulestate *optional*	The options for the rule.	ExceptionsRuleState
scancategory *optional*	The type of security risk scan.	enum (GESC_AP, GESC_MANUAL, GESC_ALL)

4.54. ExceptionsRuleMacFile

Name	Description	Schema
deleted *optional*	Indicates that the rule needs to be deleted when modified. **Default** : `false`	boolean
path *required*	The path to the object. The path is relative if pathvariable is defined. The path is full if pathvariable is [NONE] or not specified.	string
pathvariable *required*	A prefix variable that indicates a well-known Mac folder.	enum (NONE, HOME, APPLICATION, LIBRARY)
rulestate *optional*	The options for the rule.	ExceptionsRuleState

4.55. ExceptionsRuleState

Name	Description	Schema
enabled *optional*	Indicates the ability to disable a rule temporarily from enforcement without deleting it. **Default** : `false`	boolean
source *required*	Indicates which third-party management system was the source of the rule; for example, SEP or EDR.	string

4.56. ExternalCommunicationSettings

Name	Description	Schema
lowbandwidth *optional*	Gets the low-bandwidth object.	LowBandwidthConfiguration
privatecloud *optional*	Gets the private cloud object.	PrivateCloudConfiguration

4.57. FingerPrintList

Name	Description	Schema
data *required*	The fingerprint list data.	< string > array

Name	Description	Schema
description *required*	The fingerprint list description.	string
groupIds *required*	A list of groups that use this fingerprint list.	< string > array
hashType *required*	The fingerprint list hash type. Possible values are MD5 or SHA256.	string
id *required*	The fingerprint list ID.	string
name *required*	The fingerprint list name.	string
source *required*	The fingerprint list source. Possible values are CONSOLE, COMMAND, DELTATOOL, and WEBSERVICE.	string

4.58. FingerprintlistPayload

Name	Schema
data *optional*	< string > array
hashType *optional*	string

4.59. Group

Name	Description	Schema
childGroups *optional*	Lists the child groups of this group.	< object > array
created *optional*	Indicates when this group was created. It is not user-configurable.	integer (int64)
createdBy *optional*	The ID of the administrator who created this group. It is not user-configurable.	string
customIpsNumber *optional*	The custom IPS policy number for this group. Not currently used.	string
defaultLocationId *optional*	The default location ID for the group. If this group inherits from its parent, it is its non-inherited parent's default location.	string
description *optional*	The description of the group, if any.	string
domain *optional*	The Symantec Endpoint Protection Manager domain to which this group belongs.	DomainSummary
externalReferenceId *optional*	The external reference ID for this group. **Length** : `1 - 50`	string

Name	Description	Schema
fullPathName *optional*	The full path of the group including the root group, which SEPM sets. It is not user-configurable.	string
id *optional*	The group ID, which SEPM sets. It is not user-configurable.	string
lastModified *optional*	Indicates when this group was last modified. It is not user-configurable.	integer (int64)
name *required*	The name of the group.	string
numberOfPhysicalComputers *optional*	The number of computers in this group. It is not user-configurable.	integer (int32)
numberOfRegisteredUsers *optional*	The number of users in this group. It is not user-configurable.	integer (int32)
policyDate *optional*		integer (int64)
policyInheritanceEnabled *optional*	Indicates whether this group's policy is inherited from its parent. **Default** : `false`	boolean
policySerialNumber *optional*	The policy serial number for the group, which SEPM sets. It is not user-configurable.	string

4.60. GroupPayload

Name	Description	Schema
description *optional*	The description of the group. **Length** : `1 - 1024`	string
inherits *optional*	Enables the group inheritance. **Default** : `false`	boolean
name *required*	The name of the group. **Length** : `1 - 256`	string

4.61. GroupSummary

Name	Schema
domain *optional*	DomainSummary
externalReferenceId *optional*	string
fullPathName *optional*	string
id *optional*	string

Name	Schema
name *optional*	string
source *optional*	string

4.62. HidConfiguration

Name	Description	Schema
enabled *optional*	**Default** : `false`	boolean
rep_discovered_rule *optional*		RepDiscoveredRule
rep_prevalence_rule *optional*		RepPrevalenceRule
risk_id_level *optional*	**Minimum value** : `100` **Maximum value** : `500`	integer (int32)
suspicious_risk_id_limit *optional*	**Minimum value** : `100` **Maximum value** : `500`	integer (int32)
trust_intranet *optional*	**Default** : `false`	boolean

4.63. HttpServletRequest

Name	Description	Schema
attributeNames *optional*		Enumeration
authType *optional*		string
characterEncoding *optional*		string
contentLength *optional*		integer (int32)
contentType *optional*		string
contextPath *optional*		string
cookies *optional*		< Cookie > array
headerNames *optional*		Enumeration

Name	Description	Schema
inputStream *optional*		ServletInputStream
localAddr *optional*		string
localName *optional*		string
localPort *optional*		integer (int32)
locale *optional*		Locale
locales *optional*		Enumeration
method *optional*		string
parameterMap *optional*		< string, object > map
parameterNames *optional*		Enumeration
pathInfo *optional*		string
pathTranslated *optional*		string
protocol *optional*		string
queryString *optional*		string
reader *optional*		BufferedReader
remoteAddr *optional*		string
remoteHost *optional*		string
remotePort *optional*		integer (int32)
remoteUser *optional*		string
requestURI *optional*		string

Name	Description	Schema
requestURL *optional*		StringBuffer
requestedSessionId *optional*		string
requestedSessionIdFromCookie *optional*	**Default** : `false`	boolean
requestedSessionIdFromURL *optional*	**Default** : `false`	boolean
requestedSessionIdValid *optional*	**Default** : `false`	boolean
scheme *optional*		string
secure *optional*	**Default** : `false`	boolean
serverName *optional*		string
serverPort *optional*		integer (int32)
servletPath *optional*		string
session *optional*		HttpSession
userPrincipal *optional*		Principal

4.64. HttpServletResponse

Name	Description	Schema
bufferSize *optional*		integer (int32)
characterEncoding *optional*		string
committed *optional*	**Default** : `false`	boolean
contentType *optional*		string
locale *optional*		Locale
outputStream *optional*		ServletOutputStream

Name	Description	Schema
writer *optional*		PrintWriter

4.65. HttpSession

Name	Description	Schema
attributeNames *optional*		Enumeration
creationTime *optional*		integer (int64)
id *optional*		string
lastAccessedTime *optional*		integer (int64)
maxInactiveInterval *optional*		integer (int32)
new *optional*	**Default** : `false`	boolean
servletContext *optional*		ServletContext
sessionContext *optional*		HttpSessionContext
valueNames *optional*		< string > array

4.66. HttpSessionContext

Name	Schema
ids *optional*	Enumeration

4.67. InfectedClientStats

Name	Schema
clientsCount *optional*	integer (int32)
epochTime *optional*	integer (int64)

4.68. InfectedClientStatsResponse

Name	Schema

Name	Schema
infectedClientStats *optional*	< InfectedClientStats > array
lastUpdated *optional*	integer (int64)

4.69. InputStream

Type : object

4.70. LatestRevisionInfo

Name	Description	Schema
contentName *required*	Refers to Virus and Spyware Protection definitions.	string
publishedBySEPM *required*	The latest Virus and Spyware Protection definition revision version available from Symantec Endpoint Protection Manager.	string
publishedBySymantec *required*	The latest Virus and Spyware Protection definition revision version available from Symantec.	string

4.71. LicenseEntitlements

Name	Description	Schema
certificate *required*	The signed licensing certificate.	string
computer_ids *optional*	Lists the computer GUIDs for which a license entitlement applies.	< string > array
group_ids *optional*	Lists the group IDs for which a license entitlement applies.	< string > array
hardware_ids *optional*		< string > array
signed_payload *required*	The signed licensing policy content.	string

4.72. LicenseSummary

Name	Description	Schema
ended *optional*	**Default** : `false`	boolean
license_type *optional*		enum (PAID, TRIAL, UPGRADE, UNKNOWN)
ordered_quantity *optional*		integer (int32)

Name	Description	Schema
serial_number *optional*		string
service_end_date *optional*		integer (int64)
service_expiration_date *optional*		integer (int64)
unexpired_seats *optional*		integer (int32)

4.73. LicensingPolicyPayload

Name	Description	Schema
certificate *required*	The signed licensing certificate.	string
signed_payload *required*	The signed licensing policy content.	string

4.74. Locale

Name	Schema
country *optional*	string
displayCountry *optional*	string
displayLanguage *optional*	string
displayName *optional*	string
displayScript *optional*	string
displayVariant *optional*	string
extensionKeys *optional*	< string > array
iso3Country *optional*	string
iso3Language *optional*	string
language *optional*	string

Name	Schema
script *optional*	string
unicodeLocaleAttributes *optional*	< string > array
unicodeLocaleKeys *optional*	< string > array
variant *optional*	string

4.75. LowBandwidthConfiguration

Name	Description	Schema
contentthresholds *optional*	Gets content thresholds.	< ContentThreshold > array
enablelowbandwidth *optional*	Enable low-bandwidth mode **Default** : `false`	boolean
enablelowconnectivity *optional*	Indicates whether low-bandwidth mode is enabled. **Default** : `false`	boolean
enablelowconnectivityclient *optional*	Indicates whether low-bandwidth mode is enabled for the client. **Default** : `false`	boolean
networkWeeklyBandwidthLimitKb *optional*	Network bandwidth, in kilobytes (KB), allotted to the protection technologies.	integer (int32)

4.76. MalwareClientStats

Name	Description	Schema
clientsCount *required*	The number of affected clients.	integer (int32)
epochTime *required*	The time at the end of the specified time period during which malware against clients was found.	integer (int64)

4.77. MalwareClientStatsResponse

Name	Description	Schema
lastUpdated *required*	The last time the client updated its malware client count.	integer (int64)
malwareClientStats *required*	The list of clients that report malware.	< MalwareClientStats > array

4.78. MemConfiguration

Name	Description	Schema

Name	Description	Schema
customrules *optional*	Administrator defined application to protect. If an application is listed here without techniques, it is added to the coverage using the global technique state.	< PepExceptionElement > array
defaultruleoverrides *optional*	Overrides to the default rules. If an application is listed here without technique, it is completely disabled.	< PepExceptionElement > array
disabledefaultrules *optional*	Disables all default rules. **Default** : `false`	boolean
enableadvanced *optional*	Enables the advanced policy in addition to the basic one for Memory Exploit Mitigation. **Default** : `false`	boolean
enabled *optional*	Enables the basic policy for Memory Exploit Mitigation. **Default** : `false`	boolean
enablejavaprotection *optional*	Enable Java Security Manager Protection. **Default** : `false`	boolean
globalauditmodeoverride *optional*	Puts all techniques into audit mode, even techniques that are added later. **Default** : `false`	boolean
globaltechniqueoverrides *optional*	Global setting for the technique.	< PepThreatRuleElement > array

4.79. MemLockedOptions

Name	Description	Schema
enabled *optional*	**Default** : `false`	boolean

4.80. MetadataAttributes

Name	Description	Schema
id *required* *read-only*	Returns the ID of the object.	string
name *required* *read-only*	Returns the name of the object.	string

4.81. MultipartFile

Name	Description	Schema
bytes *optional*		< string (byte) > array
contentType *optional*		string

Name	Description	Schema
empty *optional*	**Default** : `false`	boolean
inputStream *optional*		InputStream
name *optional*		string
originalFilename *optional*		string
size *optional*		integer (int64)

4.82. Notification

Name	Description	Schema
hyperlink *required*	The event notification's link. **Length** : `1 - 512`	string
message *required*	The event notification's message. **Length** : `1 - 32767`	string
name *required*	The event notification's name. **Length** : `1 - 255`	string
subject *required*	The event notification's subject. **Length** : `1 - 255`	string

4.83. Page

Name	Description	Schema
content *optional*		< object > array
firstPage *optional*	**Default** : `false`	boolean
lastPage *optional*	**Default** : `false`	boolean
number *optional*		integer (int32)
numberOfElements *optional*		integer (int32)
size *optional*		integer (int32)
sort *optional*		Sort

Name	Description	Schema
totalElements *optional*		integer (int64)
totalPages *optional*		integer (int32)

4.84. PepExceptionElement

Name	Description	Schema
path *required*	The path of the process to protect. Wildcards are permitted. **Length** : `2 - 512`	string
techniqueoverrides *optional*	Technique override for a specific path.	< PepThreatRuleElement > array

4.85. PepThreatRuleElement

Name	Description	Schema
action *optional*	The action to take when the rule is enabled.	enum (ALLOW, BLOCK)
id *required*	The signature ID for the technique.	integer (int32)
log_action *optional*	The log action to take when the rule is enabled. **Minimum value** : `0` **Maximum value** : `1`	integer (int32)
name *required*	The name of the threat, as identified by the specific definition engine. **Length** : `1 - 50`	string
state *optional*	Indicates whether the technique is enabled. **Minimum value** : `0` **Maximum value** : `2`	integer (int32)

4.86. Policy

Name	Description	Schema
configuration *optional*	The policy configuration information.	object
desc *optional*	The policy description. **Length** : `1 - 1024`	string
enabled *optional*	Indicates whether the policy is enabled. **Default** : `false`	boolean
lockedoptions *optional*	The options to lock.	object
name *optional*	The policy name. **Length** : `1 - 256`	string

Name	Description	Schema
sources *optional*	A list of data objects provided by the policy source, which includes the ID, the name and the version.	< Sources > array

4.87. PolicyExceptionsConfigurationExceptionsLockedOptions

Name	Description	Schema
configuration *optional*	The Exceptions policy configuration information.	ExceptionsConfiguration
desc *optional*	The policy description. **Length** : `1 - 1024`	string
enabled *optional*	Indicates whether the policy is enabled. **Default** : `false`	boolean
lockedoptions *optional*	The options to lock.	ExceptionsLockedOptions
name *optional*	The policy name. **Length** : `1 - 256`	string
sources *optional*	A list of data objects provided by the policy source, which includes the ID, the name, and the version.	< Sources > array

4.88. PolicyHidConfigurationObject

Name	Description	Schema
configuration *optional*	The HID policy configuration information.	HidConfiguration
desc *optional*	The policy description. **Length** : `1 - 1024`	string
enabled *optional*	Indicates whether the policy is enabled. **Default** : `false`	boolean
lockedoptions *optional*	The options to lock.	object
name *optional*	The policy name. **Length** : `1 - 256`	string
sources *optional*	A list of data objects provided by the policy source, which includes the ID, the name and the version.	< Sources > array

4.89. PolicyMemConfigurationMemLockedOptions

Name	Description	Schema
configuration *optional*	The MEM policy configuration information.	MemConfiguration
desc *optional*	The policy description. **Length** : `1 - 1024`	string

Name	Description	Schema
enabled *optional*	Indicates whether the policy is enabled. **Default** : `false`	boolean
lockedoptions *optional*	The options to lock.	MemLockedOptions
name *optional*	The policy name. **Length** : `1 - 256`	string
sources *optional*	A list of data objects provided by the policy source, which includes the ID, the name, and the version.	< Sources > array

4.90. PolicyTdadConfigurationObject

Name	Description	Schema
configuration *optional*	Configuration	TdadConfiguration
desc *optional*	The policy description. **Length** : `1 - 1024`	string
enabled *optional*	Indicates whether the policy is enabled. **Default** : `false`	boolean
lockedoptions *optional*	Option names to be locked	object
name *optional*	The policy name. **Length** : `1 - 256`	string
sources *optional*	A list of data objects provided by the policy source, which includes the ID, the name, and the version.	< Sources > array

4.91. Principal

Name	Schema
name *optional*	string

4.92. PrintWriter

Type : object

4.93. PrivateCloudConfiguration

Name	Description	Schema
enableservers *optional*	Enables private Insight servers. **Default** : `false`	boolean
failover *optional*	Indicates whether to failover to the Symantec servers if the private Insight servers are not available. **Default** : `false`	boolean

Name	Description	Schema
groups *optional*	The private cloud groups.	< PrivateCloudServerGroup > array
servertype *optional*	The type of private Insight server. The type can be ATP or INSIGHT.	string

4.94. PrivateCloudServer

Name	Description	Schema
address *optional*	The address of the server.	string
certificates *optional*	The list of server certificates.	< CloudServerCertificate > array
description *optional*	A description of the server.	string
enable *optional*	Indicates whether the server is enabled. **Default** : `false`	boolean
legacyclientsupport *optional*	Indicates the state of the server for legacy client support. **Default** : `false`	boolean
name *optional*	The name of the server.	string
port *optional*	Indicates the server port.	integer (int32)
protocol *optional*	The protocol that the server uses.	string

4.95. PrivateCloudServerGroup

Name	Schema
serverCount *optional*	integer (int32)
servers *optional*	< PrivateCloudServer > array

4.96. RepDiscoveredRule

Name	Description	Schema
enabled *optional*	Indicates whether this rule is enabled. **Default** : `false`	boolean
rep_discovered_days *optional*	Indicates that a downloaded file is convicted if its first-seen number of days is equal to or less than this number. **Minimum value** : `1` **Maximum value** : `999`	integer (int32)

4.97. RepPrevalenceRule

Name	Description	Schema
enabled *optional*	Indicates whether this rule is enabled. **Default** : `false`	boolean
rep_prevalence_band *optional*	Indicates that a downloaded file is convicted if its prevalence band is equal to or lower than this level.	enum (FEWER5, FEWER50, FEWER100, HUNDREDS, THOUSANDS, TEN_THOUSANDS, HUN_THOUSANDS, MILLIONS)

4.98. ReplicationAllStatus

Name	Description	Schema
code *required*	The replication all status.	integer (int32)

4.99. ReplicationPartnerStatus

Name	Description	Schema
id *required*	Replication partner id	string
lastRunTime *required*	The last time that the replication ran.	integer (int64)
lastSuccessfulRunTime *required*	The last time that the replication ran and succeeded.	integer (int64)
location *required*	The geographical location of the replication site. Currently, this always displays NA.	string
name *required*	The replication partner status information.	string
nextRunTime *required*	The next time that the replication is scheduled to run.	integer (int64)
status_code *required*	The replication status. Possible values include SUCCEEDED, CONNECTING, AUTHENTICATING, SUBMITTING, PROCESSING, CANCELED, NEVER_REPLICATED, and FAILED_CONNECT.	string

4.100. ReplicationStatus

Name	Description	Schema
id *required*	The local site ID of the replication partner.	string
replicationPartnerStatusList *required*	List of statuses for all replication partners.	< ReplicationPartnerStatus > array

Name	Description	Schema
siteLocation *required*	The geographical location of the local replication site. Currently, this always displays NA.	string
siteName *required*	The local site name of the replication partner.	string

4.101. ReplicationStatusResponse

Name	Schema
replicationStatus *optional*	ReplicationStatus

4.102. ReportingInfo

Name	Schema
phpSessionId *optional*	string
reportingPort *optional*	integer (int32)
serverIp *optional*	string

4.103. RiskDistributionStats

Name	Description	Schema
protectionEnabledClientCount *required*	A list of how many clients have a specific protection technology enabled.	integer (int32)
protectionName *required*	The name of the protection technology that detected the risk. Possible values are Antivirus, SONAR, Download Insight, or CIDS.	string
riskCount *required*	The list of the number of risks sorted by the protection technology that detected them.	integer (int32)

4.104. RiskDistributionStatsResponse

Name	Description	Schema
riskDistributionStats *required*	The list of risk distribution statistics.	< RiskDistributionStats > array

4.105. Server

Name	Schema
directory_server_integration *optional*	DirectoryServerIntegrationConfiguration
id *optional*	string

4.106. ServletContext

Name	Schema
attributeNames *optional*	Enumeration
contextPath *optional*	string
initParameterNames *optional*	Enumeration
majorVersion *optional*	integer (int32)
minorVersion *optional*	integer (int32)
serverInfo *optional*	string
servletContextName *optional*	string
servletNames *optional*	Enumeration
servlets *optional*	Enumeration

4.107. ServletInputStream

Type : object

4.108. ServletOutputStream

Type : object

4.109. Settings

Name	Description	Schema
configuration *optional*	Configuration settings.	object
lockedoptions *optional*	The options to lock.	object

4.110. SettingsExternalCommunicationSettingsObject

Name	Description	Schema
configuration *optional*	Configuration settings for external communications.	ExternalCommunicationSettings
lockedoptions *optional*	The options to lock.	object

4.111. Sort

Type : object

4.112. Sources

Name	Description	Schema
exclusiveedit *optional*	Indicates whether the ExclusiveEdit flag provided by the source is set. **Default** : `false`	boolean
id *optional*	Gets the source ID of the policy.	string
name *optional*	Gets the source name from where the policy originated.	string
version *optional*	Gets the source version of the policy.	integer (int32)

4.113. StringBuffer

Type : object

4.114. TdadConfiguration

Name	Description	Schema
ad_domains *optional*		< TdadElement > array
enabled *optional*	**Default** : `false`	boolean

4.115. TdadElement

Name	Schema
ad_domain_uid *optional*	string
domain_name *optional*	string
policy_uid *optional*	string
policy_version *optional*	string
sid *optional*	string

4.116. TdadServerCertificate

Name	Description	Schema
content *optional*	The certificate's contents.	string

Name	Description	Schema
name *optional*	The certificate name.	string

4.117. TdadServerDetails

Name	Description	Schema
address *optional*	The server's address.	string
certificates *optional*	The server certificates list.	< TdadServerCertificate > array
description *optional*	The server's description.	string
httpsverifyca *optional*	Indicates whether to use HTTPS to verify CA. **Default** : `false`	boolean
name *optional*	The server's name.	string
password *optional*	The encrypted password to use with the TDAD username.	string
port *optional*	The server's port.	integer (int32)
protocol *optional*	The server's protocol.	string
username *optional*	The username used to log on to TDAD.	string

4.118. User

Name	Schema
logon_name *optional*	string
password *optional*	< string > array

4.119. UserCredential

Name	Description	Schema
domain *required*	The Symantec Endpoint Protection Manager domain to which the username logs on.	string
password *required*	The encrypted password to use with the Symantec Endpoint Protection Manager username.	string
username *required*	The username used to log on to Symantec Endpoint Protection Manager.	string

4.120. UserPermission

Name	Description	Schema
groupRights *optional*	Specifies whether the user has group rights. **Default** : `false`	boolean
policyRights *optional*	Specifies whether the user has policy rights. **Default** : `false`	boolean
remoteCommandRights *optional*	Specifies whether the user has the rights to send commands to clients. **Default** : `false`	boolean
reportingRights *optional*	Specifies whether the user has reporting rights. **Default** : `false`	boolean
siteRights *optional*	Specifies whether the user has site rights. **Default** : `false`	boolean

4.121. UserRole

The user role model for the webUI logon.

Name	Description	Schema
bitMask *required*	The user role mask for the web user interface. Possible values are 8 for system administrator, 4 for domain administrator, and 2 for limited administrator.	integer (int32)
title *required*	The user's title.	string

4.122. UserToken

Name	Description	Schema
adminId *required*	The user's Id.	string
bannerText *optional*	The banner text associated with the domain.	string
bannerTitle *optional*	The banner title associated with the domain.	string
clientId *optional*	The client id associated with the application.	string
clientSecret *optional*	The client secret associated with the application.	string
domain *optional*	The Symantec Endpoint Protection Manager domain to which the username logs on.	string
domainid *optional*	The Id of the domain.	string
getfullName *optional*	The user's fullname.	string

Name	Description	Schema
permissionSet *optional*	The user permission object.	UserPermission
refreshToken *optional*	The user's refresh token.	string
refreshTokenExpiration *optional*	Refresh token expiration value in seconds.	integer (int64)
role *optional*	The user role object.	UserRole
serverTime *optional*	The time on the server.	integer (int64)
token *required*	The access token associated with the user.	string
tokenExpiration *optional*	The access token expiration value in seconds.	integer (int64)
username *optional*	The username used to log on to Symantec Endpoint Protection Manager.	string

Last updated 2019-08-07 00:45:01 +05:30