

# Privilege Management Cloud 23.1 API Guide - Version 2



# **Table of Contents**

Privilers Management Claud ADI Version 2	44
Privilege Management Cloud API - Version 2	
Authenticate to the PM Cloud API	
Methods	13
AcceptedDomains	15
ActivityAudits	21
AuthorizationRequestAudits	37
Computers	42
Events	60
File	114
Groups	115
Policies	131
Roles	145
ScimResourceTypes	148
ScimSchemas	151
ScimServiceProviderConfig	155
ScimUsers	157
Tasks	166
Users	167
Models	181
AcceptedDomainDetailModel	187
AcceptedDomainListItemModel	188
Activex	189
ActivityAuditDetailModel	189
ActivityAuditDetailModelPagedResponse	191
ActivityAuditListItemModel	192
ActivityAuditListItemModelPagedResponse	193
ActivityAuditRoleNameModel	193
ActivtyAuditRoleResourceModel	194
Agent	
AgentBuild	
AgentHostType	



ApiClientDataAuditingDetailModel	196
Application	197
Applicationgroup	197
As	198
AsOrganization	198
AssignComputersToGroupRequest	198
AssignPolicyRevisionToGroupRequest	199
AssignUserToRolesRequest	199
Attribute	199
Authentication	201
Authorization	201
AuthorizationRequestAuditDetailModel	201
AuthorizationRequestAuditDetailModelPagedResponse	203
AuthorizationRequestAuditListItemModel	203
AuthorizationRequestAuditListItemModelPagedResponse	205
Authorizationrequest	205
Authorizinguser	206
AutoAssignPolicyRevisionToGroupRequest	207
Bundle	207
CertificateInformationModel	208
ChangedBy	208
Client	209
ClientNat	210
Cloud	211
CloudAccount	212
CloudInstance	212
CloudMachine	213
CloudOrigin	213
CloudProject	214
CloudService	214
CloudTarget	214
CodeSignature	215
Com	217



ComputerDataAuditingDetailModel	217
ComputerDetailModel	218
ComputerFilterModel	221
ComputerListItemModel	223
ComputerListItemModelPagedResponse	226
ComputerLogModel	227
ComputerRenewCertificateRequest	227
ComputerRetrieveLogsRequest	227
ComputerRetrieveStatusInfoRequest	228
ComputersAuthoriseRequest	228
ComputersDeactivateRequest	229
ComputersRejectRequest	229
ComputersRemoveRequest	230
Configuration	230
Container	232
ContainerCpu	234
ContainerDisk	234
ContainerDiskRead	234
ContainerDiskWrite	234
ContainerImage	235
ContainerImageHash	235
ContainerMemory	235
ContainerNetwork	236
ContainerNetworkEgress	236
ContainerNetworkIngress	236
Content	236
Contentgroup	237
CountRange	237
CreateAcceptedDomainRequest	238
CreateGroupRequest	238
DataStream	238
DateFilterModel	239
DateSelectionMode	239



Destination	.240
DestinationNat	. 241
DII	. 242
Dns	. 242
DnsQuestion	.243
Ecs	.244
Elf	. 244
ElfHeader	246
ElfSections	.247
ElfSegments	.248
Email	. 248
EmailAttachments	.250
EmailAttachmentsFile	. 250
EmailBcc	. 251
EmailCc	.251
EmailFrom	251
EmailReplyTo	. 251
EmailSender	.252
EmailTo	.252
EndpointInformationModel	252
EpmEcsEvent	. 255
EpmEcsEventResponseModel	.260
EpmEcsEventSpan	. 261
EpmEcsEventTrace	.261
EpmEcsEventTransaction	.261
Epmwinmac	.261
Error	.263
Event	.264
Faas	.264
FaasTrigger	.265
File	.265
Geo	.269
GeoPoint	271



Gpo	271
Group	272
GroupDataAuditingDetailModel	272
GroupListItemModel	273
GroupListItemModelPagedResponse	275
Hash	276
Host	277
HostBoot	279
HostCpu	279
HostDisk	280
HostDiskRead	280
HostDiskWrite	280
HostNetwork	280
HostNetworkEgress	281
HostNetworkIngress	281
Http	281
HttpRequest	282
HttpRequestBody	283
HttpResponse	283
HttpResponseBody	284
InstallationKeyDataAuditingDetailModel	284
Installer	285
ListItemErrorInfoModel	285
Log	286
LogFile	286
LogOrigin	287
LogOriginFile	287
Message	287
ModifyAcceptedDomainRequest	288
ModifyGroupRequest	289
ModifyPolicyRequest	289
ModifyUserPreferencesRequest	289
ModifyUserRequest	290



Network	290
OS	292
Observer	292
OperationValue	294
Operator	295
Orchestrator	295
OrchestratorCluster	296
OrchestratorResource	296
OrchestratorResourceParent	297
Organization	297
Os	298
Owner	299
Package	299
Pe	301
PolicyDataAudtingDetailModel	302
PolicyGroupsListItemModel	302
PolicyListItemModel	303
PolicyListItemModelPagedResponse	306
PolicyRevisionDataAuditingDetailModel	306
PolicyRevisionModel	307
PolicyRevisionState	308
Privilegedgroup	308
ProblemDetails	308
Process	309
ProcessEntryLeader	313
ProcessEntryMeta	317
ProcessGroupLeader	318
ProcessParent	321
ProcessPrevious	325
ProcessSessionLeader	329
ProcessThread	333
Registry	333
RegistryData	



Related	334
Remotepowershell	335
RoleElement	335
RoleItemModel	335
RoleListItemModel	336
RoleModel	337
RolePermissionModel	337
RoleResourceModel	337
Rule	338
Rulescript	338
RulescriptOutcome	339
SCIMEmail	340
SCIMUserName	340
ScimAuthenticationSchemes	340
ScimBulk	341
ScimOperation	342
ScimResourceMeta	342
ScimResourceResponse	342
ScimResourceResponseScimListResponse	343
ScimSchemaResponse	344
ScimSchemaResponseScimListResponse	345
ScimServiceProviderConfigResponse	345
ScimSupported	346
ScimUserMetaModel	347
ScimUserModel	347
ScimUserModelScimListResponse	349
ScimUserPatchRequest	350
Server	350
ServerNat	352
Service	352
ServiceNode	353
ServiceOrigin	354
ServiceTarget	355



Servicecontrol	356
ServicecontrolService	356
Session	356
SettingDataAuditingDetailModel	357
SortDirection	358
SortModel	358
Source	358
SourceNat	360
Storeapp	360
SubAttribute	361
TaskDetailModel	362
Threat	363
ThreatEnrichments	364
ThreatEnrichmentsMatched	365
ThreatFeed	366
ThreatGroup	366
ThreatIndicator	367
ThreatIndicatorEmail	369
ThreatIndicatorMarking	369
ThreatSoftware	370
ThreatTactic	370
ThreatTechnique	371
ThreatTechniqueSubtechnique	371
Tls	372
TIsClient	373
TlsClientHash	374
TlsServer	375
TlsServerHash	376
Token	376
Trustedapplication	377
UnassignComputersToGroupRequest	377
Url	378
User	379



UserAgent	381
UserAgentDevice	382
UserChanges	382
UserDataAuditing	384
UserDetailModel	385
UserEffective	. 387
UserListItemModel	. 389
UserListItemModelPagedResponse	. 390
UserRoleResourceItemModel	. 391
UserTarget	392
V2CreateUserRequest	. 393
Vlan	395
Vulnerability	395
VulnerabilityScanner	396
VulnerabilityScore	396
Workstyle	397
X509	397
X509Issuer	399
X509Subject	.400
_event	401
_rule	.404
id_AssignComputersByCsv_body	.405
id_Upload_body	. 405
v2_Policies_body	405



# **Privilege Management Cloud API - Version 2**

Use the PM Cloud Management API to configure and customize PM Cloud components to interact with external systems and software.

Use this guide as a resource to get started with the PM Cloud API.

This resource is intended for readers with knowledge of HTTPS request and response processing, web development, and JSON notation.

## Authenticate to the PM Cloud API

API requests are executed by sending an HTTP request to PM Cloud. Send the request using any HTTPS-capable socket library or scripting language module, URL fetcher such as cURL, or an OAuth library specific to your platform. BeyondTrust's web APIs use OAuth as the authentication method.

To authenticate to the API, you must create an API account on the **Configuration > Settings > API Settings** page. The account must have permission to access the necessary APIs. API requests require a token to be first created and then submitted with each API request.



For more information about creating an API account, please see <u>Configure Access to the Management API</u> in the Privilege Management Cloud Administration Guide.

#### Create a Token

Create a token by POSTing to the URL of your BeyondTrust site followed by /oauth/connect/token:

```
https://example-services.pm.beyondtrustcloud.com/oauth/connect/token
```

Replace "example" with your production sub-domain name, as shown:

```
https://[yourProductionSub-domainName]-services.pm.beyondtrustcloud.com/oauth/connect/token
```

The OAuth client ID and client secret associated with the API account should be included in the POST body:

```
grant_type=client_credentials&client_id=[yourClientId]&client_secret=[yourGeneratedClientSecret]
```

If the request is processed without error, you will get an access token JSON response:

```
"access_token":"<token>",
   "token_type":"Bearer",
   "expires_in":3600,
   "scope":"urn:management:api"
}
```





**Note:** The client secret cannot be modified, but it can be regenerated on the **Configuration > Settings > API Settings** page. Regenerating a client secret and then saving the account immediately invalidates any OAuth tokens associated with the account. Any API calls using those tokens will be unable to access the API. A new token must be generated using the new client secret.

## Request an API Resource

Now that you have an access token, you can make GET/POST requests via HTTPS to the web API:

https://example-services.pm.beyondtrustcloud.com/management-api/v1/Groups

The obtained token is used for HTTP authentication and must be included in an HTTP authorization header with each request:

Authorization: Bearer <token>

If the token is valid, you gain access to the requested URL.

#### **Authentication Errors**

Requests made to the web API with expired or invalid tokens result in a "HTTP 401 Unauthorized" response.

#### Access PM Cloud API Documentation

The management API is written according to OpenAPI standards. You can view documentation for the API using your preferred OpenAPI tool, such as Swagger, Postman, or RediDoc.

A preconfigured Swagger UI is available as part of the solution (<a href="https://example-services.pm.beyondtrustcloud.com/management-api>/swagger">https://example-services.pm.beyondtrustcloud.com/management-api>/swagger</a>). The API documentation includes a complete list of methods, models, and usage descriptions and examples. You can try out and test examples using the Swagger UI.

Alternatively, download the JSON file from the preconfigured Swagger UI and use a tool of your choice to view the documentation.



For more information on Swagger, please see Swagger UI at https://swagger.io/tools/swagger-ui/.



## **Methods**

[Jump to Models]

## **Table of Contents**

## **AcceptedDomains**

- get /v2/AcceptedDomains
- delete /v2/AcceptedDomains/{id}
- get /v2/AcceptedDomains/{id}
- put /v2/AcceptedDomains/{id}
- post /v2/AcceptedDomains

## **ActivityAudits**

- get /v2/ActivityAudits/Details
- get /v2/ActivityAudits
- get /v2/ActivityAudits/{id}

#### **AuthorizationRequestAudits**

- get /v2/AuthorizationRequestAudits
- get /v2/AuthorizationRequestAudits/{id}

#### Computers

- post /v2/Computers/Authorise
- post /v2/Computers/Certificate/Renew
- post /v2/Computers/Deactivate
- delete /v2/Computers
- post /v2/Computers/Details/Request
- get /v2/Computers
- get /v2/Computers/{id}/CommandLog
- get /v2/Computers/{id}
- get /v2/Computers/{id}/Logs
- get /v2/Computers/Logs/{id}/Content
- post /v2/Computers/Logs/Request
- post /v2/Computers/Reject



#### **Events**

• get /v2/Events/FromStartDate

#### **File**

• get /v2/File/download/GetYamlApiDefinitionFile

#### **Groups**

- post /v2/Groups/AutoAssignPolicyRevision
- get /v2/Groups
- post /v2/Groups/{id}/AssignComputersByCsv
- post /v2/Groups/{id}/AssignComputers
- post /v2/Groups/{id}/AssignPolicyRevision
- patch /v2/Groups/{id}/ClearPolicy
- delete /v2/Groups/{id}
- get /v2/Groups/{id}
- patch /v2/Groups/{id}/MarkAsDefault
- post /v2/Groups
- put /v2/Groups
- post /v2/Groups/UnassignComputers

#### **Policies**

- get /v2/Policies
- get /v2/Policies/{id}/AssignedGroups
- get /v2/Policies/{id}/Content
- delete /v2/Policies/{id}
- patch /v2/Policies/{id}/DiscardDraft
- get /v2/Policies/{id}
- put /v2/Policies/{id}
- get /v2/Policies/{id}/Revisions
- post /v2/Policies/{id}/Upload
- get /v2/Policies/PolicyRevision/{policyRevisionId}/Content
- post /v2/Policies

#### Roles

- · get /v2/Roles
- get /v2/Roles/{id}



## **ScimResourceTypes**

- get /scim/v2/ResourceTypes
- get /scim/v2/ResourceTypes/User

#### **ScimSchemas**

get /scim/v2/Schemas

#### ScimServiceProviderConfig

get /scim/v2/ServiceProviderConfig

#### **ScimUsers**

- get /scim/v2/Users
- post /scim/v2/Users
- get /scim/v2/Users/{userID}
- patch /scim/v2/Users/{userID}
- put /scim/v2/Users/{userID}

#### **Tasks**

get /v2/Tasks/{id}

#### **Users**

- get /v2/Users
- post /v2/Users/{id}/AssignRoles
- patch /v2/Users/{id}/Disable
- patch /v2/Users/{id}/Enable
- get /v2/Users/{id}
- put /v2/Users/{id}/ModifyUserPreferences
- put /v2/Users/{id}
- patch /v2/Users/{id}/ResendInvite
- post /v2/Users

# **AcceptedDomains**





## get /v2/AcceptedDomains

Retrieves list of Accepted Domains (v2AcceptedDomainsGet)

## Return type

array[ AcceptedDomainListItemModel]

# **Example data**

Content-Type: application/json

```
"created": "2000-01-23T04:56:07.000+00:00",
        "domain": "domain",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true
    },
        "created": "2000-01-23T04:56:07.000+00:00",
        "domain": "domain",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true
]
```

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json



## Responses

#### 200

Success

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 500

Server Error



# delete /v2/AcceptedDomains/{id}

Deletes Accepted Domain (v2AcceptedDomainsIdDelete)

# Path parameters

# id (required)

Path Parameter — format: uuid

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

#### 204

No Content

#### 404

Not Found ProblemDetails



#### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails



# get /v2/AcceptedDomains/{id}

Retrieves Record of Accepted Domain (v2AcceptedDomainsIdGet)

# **Path parameters**

## id (required)

Path Parameter — format: uuid

# Return type

AcceptedDomainDetailModel

# **Example data**

Content-Type: application/json

```
{
   "created" : "2000-01-23T04:56:07.000+00:00",
   "domain" : "domain",
   "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
}
```

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json



## Responses

#### 200

Success AcceptedDomainDetailModel

#### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails



# put /v2/AcceptedDomains/{id}

Modifies Accepted Domain (v2AcceptedDomainsIdPut)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

#### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ModifyAcceptedDomainRequest (optional)

**Body Parameter** —

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json



## Responses

#### 204

No Content

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails



# post /v2/AcceptedDomains

Creates Accepted Domain (v2AcceptedDomainsPost)

#### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body CreateAcceptedDomainRequest (optional)

Body Parameter —

# Return type

UUID



## **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

201

Created **UUID** 

409

Conflict ProblemDetails

# **ActivityAudits**



# get /v2/ActivityAudits/Details

Retrieves list of Details of Activity Audits with pagination (sorting and filtering) (v2ActivityAuditsDetailsGet)

# **Query parameters**

# **Sorts (optional)**

Query Parameter —

# Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32



## **Pagination.PageNumber (optional)**

Query Parameter — The page number to retrieve from results, for example 1 format: int32

## Filter.User (optional)

Query Parameter — Initiated User email or API Client identifier

## Filter.Details (optional)

Query Parameter — Details of activity

## Filter.Created.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

## Filter.Created.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

# Filter.Entity (optional)

Query Parameter — Name of Activity Audit entity

# Filter.AuditType (optional)

Query Parameter — Audit Type Name

# Filter.ChangedBy (optional)

Query Parameter — Audit ChangedBy

# **Return type**

ActivityAuditDetailModelPagedResponse



## **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "computerDataAuditing": {
            "deactivatedAgents": {
                "key": "deactivatedAgents"
            "newDeletedAgents": [
                "newDeletedAgents",
                "newDeletedAgents"
            "updatedPoliciesOn": {
                "key": "updatedPoliciesOn"
        "groupDataAuditing": {
            "oldDescription": "oldDescription",
            "addPolicyRevisions": {
                "key": "addPolicyRevisions"
            "newName": "newName",
            "removePolicyRevisions": {
                "key": "removePolicyRevisions"
            "oldName": "oldName",
            "newAgents": {
                "key": "newAgents"
            "oldIsDefault": true,
            "newDescription": "newDescription",
            "newIsDefault": true,
            "removeAgents": {
                "key": "removeAgents"
        "created": "2000-01-23T04:56:07.000+00:00",
        "policyDataAuditing": {
            "oldDescription": "oldDescription",
            "newName": "newName",
            "oldName": "oldName",
            "newDescription": "newDescription"
        "policyRevisionDataAuditing": {
            "newGroups": {
                "key": "newGroups"
        },
```



```
"auditType": "auditType",
"userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"settingsDataAuditing": {
    "modifyDomainOldValue": "modifyDomainOldValue",
    "modifyDomainNewValue": "modifyDomainNewValue",
    "removeDomain": "removeDomain",
    "addDomain": "addDomain"
"apiClientDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
    "deleted": true,
    "secretUpdated": true,
    "oldName": "oldName",
    "newDescription": "newDescription"
"installationKeyDataAuditing": {
    "newDisabled": true,
    "oldDisabled": true,
    "deleted": true,
    "newLabel": "newLabel",
    "oldLabel": "oldLabel"
"userDataAuditing": {
    "oldDisabled": true,
    "newUserType": "newUserType",
    "oldEmailAddress": "oldEmailAddress",
    "roles": [
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
                },
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
            "oldRoles": [
                null,
                null
            "resourceName": "resourceName",
            "resourceType": "resourceType"
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
```



```
},
                    {
                        "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                        "roleName": "roleName"
                ],
                "oldRoles": [
                   null,
                    null
                ],
                "resourceName": "resourceName",
                "resourceType": "resourceType"
        ],
        "newPreferredLanguage": "newPreferredLanguage",
        "oldDateTimeDisplayFormat": "oldDateTimeDisplayFormat",
        "newDisabled": true,
        "newDateTimeDisplayFormat": "newDateTimeDisplayFormat",
        "oldOlsonTimeZoneId": "oldOlsonTimeZoneId",
        "oldUserType": "oldUserType",
        "oldPreferredLanguage": "oldPreferredLanguage",
        "newOlsonTimeZoneId": "newOlsonTimeZoneId",
        "newEmailAddress": "newEmailAddress"
    "changedBy": "API",
    "details": "details",
    "id": 5,
    "user": "user",
    "entity": "entity"
},
    "computerDataAuditing": {
        "deactivatedAgents": {
            "key": "deactivatedAgents"
        "newDeletedAgents": [
            "newDeletedAgents",
            "newDeletedAgents"
        "updatedPoliciesOn": {
            "key": "updatedPoliciesOn"
    "groupDataAuditing": {
        "oldDescription": "oldDescription",
        "addPolicyRevisions": {
            "key": "addPolicyRevisions"
        "newName": "newName",
        "removePolicyRevisions": {
            "key": "removePolicyRevisions"
        "oldName": "oldName",
```



```
"newAgents": {
        "key": "newAgents"
    "oldIsDefault": true,
    "newDescription": "newDescription",
    "newIsDefault": true,
    "removeAgents": {
        "key": "removeAgents"
},
"created": "2000-01-23T04:56:07.000+00:00",
"policyDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
    "oldName": "oldName",
    "newDescription": "newDescription"
"policyRevisionDataAuditing": {
    "newGroups": {
        "key": "newGroups"
},
"auditType": "auditType",
"userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"settingsDataAuditing": {
    "modifyDomainOldValue": "modifyDomainOldValue",
    "modifyDomainNewValue": "modifyDomainNewValue",
    "removeDomain": "removeDomain",
    "addDomain": "addDomain"
"apiClientDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
"deleted": true,
    "secretUpdated": true,
    "oldName": "oldName",
    "newDescription": "newDescription"
"installationKeyDataAuditing": {
    "newDisabled": true,
    "oldDisabled": true,
    "deleted": true,
    "newLabel": "newLabel",
    "oldLabel": "oldLabel"
"userDataAuditing": {
    "oldDisabled": true,
    "newUserType": "newUserType",
    "oldEmailAddress": "oldEmailAddress",
    "roles": [
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
```



```
"roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                        },
                         {
                             "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                    ],
                    "oldRoles": [
                        null,
                        null
                    "resourceName": "resourceName",
                    "resourceType": "resourceType"
                },
                    "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "newRoles": [
                        {
                             "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                        },
                             "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                    ],
                    "oldRoles": [
                        null,
                        null
                    "resourceName": "resourceName",
                    "resourceType": "resourceType"
            ],
            "newPreferredLanguage": "newPreferredLanguage",
            "oldDateTimeDisplayFormat": "oldDateTimeDisplayFormat",
            "newDisabled": true,
            "newDateTimeDisplayFormat": "newDateTimeDisplayFormat",
            "oldOlsonTimeZoneId": "oldOlsonTimeZoneId",
            "oldUserType": "oldUserType",
            "oldPreferredLanguage": "oldPreferredLanguage",
            "newOlsonTimeZoneId": "newOlsonTimeZoneId",
            "newEmailAddress": "newEmailAddress"
        "changedBy": "API",
        "details": "details",
        "id": 5,
        "user": "user",
        "entity": "entity"
],
```



```
"pageSize": 6,
  "totalRecordCount": 1
}
```

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

#### 200

Success ActivityAuditDetailModelPagedResponse

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 500

Server Error



# get /v2/ActivityAudits

Retrieves list of Activity Audits with pagination (sorting and filtering) (v2ActivityAuditsGet)

# **Query parameters**

# Sorts (optional)

Query Parameter —

# Pagination.PageSize (optional)



Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32

## **Pagination.PageNumber (optional)**

Query Parameter — The page number to retrieve from results, for example 1 format: int32

## Filter.User (optional)

Query Parameter — Initiated User email or API Client identifier

## Filter.Details (optional)

Query Parameter — Details of activity

## Filter.Created.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.Created.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

# Filter.Entity (optional)

Query Parameter — Name of Activity Audit entity

# Filter.AuditType (optional)

Query Parameter — Audit Type Name

# Filter.ChangedBy (optional)

Query Parameter — Audit ChangedBy

# Return type

ActivityAuditListItemModelPagedResponse



## **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "created": "2000-01-23T04:56:07.000+00:00",
        "changedBy": "API",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "details": "details",
        "id": 5,
        "auditType": "auditType",
        "locked": true,
        "user": "user",
        "entity": "entity"
        "created": "2000-01-23T04:56:07.000+00:00",
        "changedBy": "API",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "details": "details",
        "id": 5,
        "auditType": "auditType",
        "locked": true,
        "user": "user",
        "entity": "entity"
],
"pageSize": 6,
"totalRecordCount": 1
```

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.



- · text/plain
- · application/json
- text/json

## Responses

#### 200

Success ActivityAuditListItemModelPagedResponse

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 500

Server Error



## get /v2/ActivityAudits/{id}

Retrieves Record of Activity Audit (v2ActivityAuditsIdGet)

# Path parameters

# id (required)

Path Parameter — format: int64

# Return type

 $\underline{Activity} \underline{AuditDetailModelPagedResponse}$ 

# **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
```



```
"data": [
   {
        "computerDataAuditing": {
            "deactivatedAgents": {
                "key": "deactivatedAgents"
            "newDeletedAgents": [
                "newDeletedAgents",
                "newDeletedAgents"
            "updatedPoliciesOn": {
                "key": "updatedPoliciesOn"
        },
        "groupDataAuditing": {
            "oldDescription": "oldDescription",
            "addPolicyRevisions": {
                "key": "addPolicyRevisions"
            },
            "newName": "newName",
            "removePolicyRevisions": {
                "key": "removePolicyRevisions"
            },
            "oldName": "oldName",
            "newAgents": {
                "key": "newAgents"
            },
            "oldIsDefault": true,
            "newDescription": "newDescription",
            "newIsDefault": true,
            "removeAgents": {
                "key": "removeAgents"
        "created": "2000-01-23T04:56:07.000+00:00",
        "policyDataAuditing": {
            "oldDescription": "oldDescription",
            "newName": "newName",
            "oldName": "oldName",
            "newDescription": "newDescription"
        "policyRevisionDataAuditing": {
            "newGroups": {
                "key": "newGroups"
        "auditType": "auditType",
        "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "settingsDataAuditing": {
            "modifyDomainOldValue": "modifyDomainOldValue",
            "modifyDomainNewValue": "modifyDomainNewValue",
            "removeDomain": "removeDomain",
            "addDomain": "addDomain"
```



```
"apiClientDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
    "deleted": true,
    "secretUpdated": true,
    "oldName": "oldName",
    "newDescription": "newDescription"
"installationKeyDataAuditing": {
    "newDisabled": true,
    "oldDisabled": true,
    "deleted": true,
    "newLabel": "newLabel",
    "oldLabel": "oldLabel"
"userDataAuditing": {
    "oldDisabled": true,
    "newUserType": "newUserType",
    "oldEmailAddress": "oldEmailAddress",
    "roles": [
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
                {
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
                },
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
                }
            "oldRoles": [
                null,
                null
            "resourceName": "resourceName",
            "resourceType": "resourceType"
        },
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
                },
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
            ],
            "oldRoles": [
```



```
null,
                    null
                "resourceName": "resourceName",
                "resourceType": "resourceType"
        ],
        "newPreferredLanguage": "newPreferredLanguage",
        "oldDateTimeDisplayFormat": "oldDateTimeDisplayFormat",
        "newDisabled": true,
        "newDateTimeDisplayFormat": "newDateTimeDisplayFormat",
        "oldOlsonTimeZoneId": "oldOlsonTimeZoneId",
        "oldUserType": "oldUserType",
        "oldPreferredLanguage": "oldPreferredLanguage",
        "newOlsonTimeZoneId": "newOlsonTimeZoneId",
        "newEmailAddress": "newEmailAddress"
    "changedBy": "API",
    "details": "details",
    "id": 5,
    "user": "user",
    "entity": "entity"
},
    "computerDataAuditing": {
        "deactivatedAgents": {
            "key": "deactivatedAgents"
        },
        "newDeletedAgents": [
            "newDeletedAgents",
            "newDeletedAgents"
        "updatedPoliciesOn": {
            "key": "updatedPoliciesOn"
    "groupDataAuditing": {
        "oldDescription": "oldDescription",
        "addPolicyRevisions": {
            "key": "addPolicyRevisions"
        "newName": "newName",
        "removePolicyRevisions": {
            "key": "removePolicyRevisions"
        "oldName": "oldName",
        "newAgents": {
            "key": "newAgents"
        "oldIsDefault": true,
        "newDescription": "newDescription",
        "newIsDefault": true,
        "removeAgents": {
```



```
"key": "removeAgents"
"created": "2000-01-23T04:56:07.000+00:00",
"policyDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
    "oldName": "oldName",
    "newDescription": "newDescription"
"policyRevisionDataAuditing": {
    "newGroups": {
        "key": "newGroups"
"auditType": "auditType",
"userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"settingsDataAuditing": {
    "modifyDomainOldValue": "modifyDomainOldValue",
    "modifyDomainNewValue": "modifyDomainNewValue",
    "removeDomain": "removeDomain",
    "addDomain": "addDomain"
"apiClientDataAuditing": {
    "oldDescription": "oldDescription",
    "newName": "newName",
    "deleted": true,
    "secretUpdated": true,
    "oldName": "oldName",
    "newDescription": "newDescription"
"installationKeyDataAuditing": {
    "newDisabled": true,
    "oldDisabled": true,
    "deleted": true,
    "newLabel": "newLabel",
    "oldLabel": "oldLabel"
"userDataAuditing": {
    "oldDisabled": true,
    "newUserType": "newUserType",
    "oldEmailAddress": "oldEmailAddress",
    "roles": [
            "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
            "newRoles": [
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
                },
                    "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "roleName": "roleName"
```



```
],
                    "oldRoles": [
                       null,
                        null
                    ],
                    "resourceName": "resourceName",
                    "resourceType": "resourceType"
                },
                    "resourceId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                    "newRoles": [
                        {
                             "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                        },
                         {
                             "roleId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                             "roleName": "roleName"
                    ],
                    "oldRoles": [
                        null,
                        null
                    "resourceName": "resourceName",
                    "resourceType": "resourceType"
            ],
            "newPreferredLanguage": "newPreferredLanguage",
            "oldDateTimeDisplayFormat": "oldDateTimeDisplayFormat",
            "newDisabled": true,
            "newDateTimeDisplayFormat": "newDateTimeDisplayFormat",
            "oldOlsonTimeZoneId": "oldOlsonTimeZoneId",
            "oldUserType": "oldUserType",
            "oldPreferredLanguage": "oldPreferredLanguage",
            "newOlsonTimeZoneId": "newOlsonTimeZoneId",
            "newEmailAddress": "newEmailAddress"
        "changedBy": "API",
        "details": "details",
        "id": 5,
        "user": "user",
        "entity": "entity"
],
"pageSize": 6,
"totalRecordCount": 1
```

#### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.



- text/plain
- · application/json
- · text/json

### Responses

#### 200

Success ActivityAuditDetailModelPagedResponse

### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

# **AuthorizationRequestAudits**



### get /v2/AuthorizationRequestAudits

Retrieves the list of Authorization Request Audit with pagination (sorting and filtering) (v2AuthorizationRequestAuditsGet)

# **Query parameters**

# **Sorts (optional)**

Query Parameter —

# Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32

# Pagination.PageNumber (optional)

Query Parameter — The page number to retrieve from results, for example 1 format: int32

# Filter.TicketId (optional)



Query Parameter — Filter.User (optional) Query Parameter — Filter.ComputerName (optional) Query Parameter — Filter.ProductName (optional) Query Parameter — Filter.Reason (optional) Query Parameter — Filter.DecisionPerformedByUser (optional) Query Parameter — **Filter.Decision (optional)** Query Parameter — Filter.TimeOfRequest.Dates (optional) Query Parameter — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time Filter.TimeOfRequest.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

Filter.DecisionTime.Dates (optional)



**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.DecisionTime.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

## Filter.StartTime.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

### Filter.StartTime.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

### **Filter.Duration (optional)**

Query Parameter —

# **Return type**

 $\underline{Authorization Request Audit List Item Model Paged Response}$ 

# **Example data**

Content-Type: application/json



```
"ticketId": "ticketId",
        "productName": "productName",
        "decisionPerformedByUser": "decisionPerformedByUser"
        "duration": "duration",
        "reason": "reason",
        "decision": "decision",
        "computerName": "computerName",
        "decisionTime": "2000-01-23T04:56:07.000+00:00",
        "timeOfRequest": "2000-01-23T04:56:07.000+00:00",
        "startTime": "2000-01-23T04:56:07.000+00:00",
        "id": 5,
        "user": "user",
        "ticketId": "ticketId",
        "productName": "productName",
        "decisionPerformedByUser": "decisionPerformedByUser"
],
"pageSize": 6,
"totalRecordCount": 1
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json

### Responses

#### 200

 $Success\ \textbf{Authorization} \textbf{RequestAuditListItemModelPagedResponse}$ 

### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 403

Forbidden ProblemDetails





### get /v2/AuthorizationRequestAudits/{id}

Retrieves Record of Authorization Request Audit (v2AuthorizationRequestAuditsIdGet)

### **Path parameters**

### id (required)

Path Parameter — format: int64

### Return type

 $\underline{Authorization Request Audit Detail Model Paged Response}$ 

## **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "duration": "duration",
        "reason": "reason",
        "decision": "decision",
        "computerName": "computerName",
        "decisionTime": "2000-01-23T04:56:07.000+00:00",
        "timeOfRequest": "2000-01-23T04:56:07.000+00:00",
        "startTime": "2000-01-23T04:56:07.000+00:00",
        "id": 5,
        "user": "user",
        "ticketId": "ticketId",
        "productName": "productName",
        "decisionPerformedByUser": "decisionPerformedByUser"
        "duration": "duration",
        "reason": "reason",
        "decision": "decision",
        "computerName": "computerName",
        "decisionTime": "2000-01-23T04:56:07.000+00:00",
        "timeOfRequest": "2000-01-23T04:56:07.000+00:00",
        "startTime": "2000-01-23T04:56:07.000+00:00",
        "id": 5,
        "user": "user",
```



### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

### 200

 $Success\, \textbf{Authorization} \textbf{RequestAuditDetailModelPagedResponse}$ 

#### 401

Unauthorized ProblemDetails

### 403

Forbidden ProblemDetails

#### 404

Not Found ProblemDetails

# Computers



## post /v2/Computers/Authorise

Authorises Computers (v2ComputersAuthorisePost)

### Consumes

This API call consumes the following media types via the Content-Type request header:



- · application/json
- · text/json
- application/\*+json

# **Request body**

body ComputersAuthoriseRequest (optional)

Body Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

### 200

Success

### 201

Created **UUID** 

#### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 404

Not Found **ProblemDetails** 

### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails





# post /v2/Computers/Certificate/Renew

Request to Renew Computer Certificate (v2ComputersCertificateRenewPost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- text/json
- · application/\*+json

### **Request body**

body ComputerRenewCertificateRequest (optional)

Body Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

# Responses

#### 202

Accepted

### 400

Bad Request ProblemDetails

#### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails



post /v2/Computers/Deactivate



Deactivates Computers (v2ComputersDeactivatePost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ComputersDeactivateRequest (optional)

Body Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

#### 200

Success

### 201

Created **UUID** 

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails



Client Error ProblemDetails



# delete /v2/Computers

Deletes Computers (v2ComputersDelete)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

### Request body

body ComputersRemoveRequest (optional)

Body Parameter — Request containing data to filter Computers to be removed

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

#### 200

Success

### 201

Created **UUID** 

#### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails



Client Error ProblemDetails



# post /v2/Computers/Details/Request

Retrieves Computer Status Info (v2ComputersDetailsRequestPost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

### **Request body**

body ComputerRetrieveStatusInfoRequest (optional)

Body Parameter —

## Return type

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

#### 201

Created **UUID** 



Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails



get /v2/Computers

Retrieves the list of Computers with pagination (sorting and filtering) (v2ComputersGet)

### **Query parameters**

# **Sorts (optional)**

Query Parameter —

# Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32

# Pagination.PageNumber (optional)

Query Parameter — The page number to retrieve from results, for example 1 format: int32

# Filter.ComputerId (optional)

Query Parameter — The Id of the Computer(Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid



## Filter.Host (optional)

Query Parameter — The host name of the Computer, for example - Computer1

### Filter.HostType (optional)

Query Parameter — The host type of the Computer, for example - MicrosoftWindows, Linux

### Filter.AgentVersion (optional)

Query Parameter — The agent version of the Computer, example - 5.6.126.0

### Filter.AdapterVersion (optional)

Query Parameter — The adapter version of the Computer, example - 20.5.195.0

### Filter.AuthorisationState (optional)

Query Parameter — The state of the Computer, example - Authorised, Pending

# Filter.LastConnected.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.LastConnected.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

# Filter.PolicyRevisionStatus (optional)

Query Parameter — Policy Revision Status, example - AwaitingLatestPolicy

# Filter.Policyld (optional)

Query Parameter — Policy Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid



## Filter.PolicyName (optional)

Query Parameter — Policy Name, example - Policy1

### Filter.GroupId (optional)

Query Parameter — Group Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

### Filter.GroupName (optional)

Query Parameter — Group Name, example - Group1

### Filter.OS (optional)

Query Parameter — OS Name, example - Windows

## Filter.Domain (optional)

Query Parameter — Domain Name, example - BeyondTrust

### Filter.Created.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.Created.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

# Filter.DuplicateCount.Min (optional)

Query Parameter — Min Value of CountRange, example - 1,2,3 format: int32

# Filter.DuplicateCount.Max (optional)

Query Parameter — Max Value of CountRange, example - 1,2,3 format: int32



### Return type

ComputerListItemModelPagedResponse

# **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "rejected": true,
        "deactivatedOn": "2000-01-23T04:56:07.000+00:00",
        "groupId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "deactivated": true,
        "authorisationState": "authorisationState",
        "lastConnected": "2000-01-23T04:56:07.000+00:00",
        "hostType": "Undefined",
        "host": "host",
        "adapterVersion": "adapterVersion",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true,
        "os": "os",
        "policyName": "policyName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "pendingDeactivation": true,
        "duplicate": true,
        "policyRevisionId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "credentialType": "credentialType",
        "groupName": "groupName",
        "policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "duplicateCount": 5,
        "domain": "domain",
        "agentVersion": "agentVersion",
        "policyRevisionStatus": "policyRevisionStatus",
        "policyUpdateTimeStamp": "2000-01-23T04:56:07.000+00:00"
        "rejected": true,
        "deactivatedOn": "2000-01-23T04:56:07.000+00:00",
        "groupId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "errorInfo": {
```



```
"userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "deactivated": true,
        "authorisationState": "authorisationState",
        "lastConnected": "2000-01-23T04:56:07.000+00:00",
        "hostType": "Undefined",
        "host": "host",
        "adapterVersion": "adapterVersion",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true,
        "os": "os",
        "policyName": "policyName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "pendingDeactivation": true,
        "duplicate": true,
        "policyRevisionId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "credentialType": "credentialType",
        "groupName": "groupName",
        "policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "duplicateCount": 5,
        "domain": "domain",
        "agentVersion": "agentVersion",
        "policyRevisionStatus": "policyRevisionStatus",
        "policyUpdateTimeStamp": "2000-01-23T04:56:07.000+00:00"
],
"pageSize": 6,
"totalRecordCount": 1
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

### Responses

#### 200

Success ComputerListItemModelPagedResponse

#### 400

Bad Request ProblemDetails



Unauthorized ProblemDetails



# get /v2/Computers/{id}/CommandLog

Gets Computer Command Logs List (v2ComputersIdCommandLogGet)

### **Path parameters**

## id (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

### Responses

### 200

Success

### 404

Not Found ProblemDetails



# get /v2/Computers/{id}

Retrieves a detail of the Computer (v2ComputersIdGet)

# **Path parameters**

# id (required)



Path Parameter — format: uuid

### Return type

ComputerDetailModel

### **Example data**

Content-Type: application/json

```
"deactivatedOn": "2000-01-23T04:56:07.000+00:00",
"groupId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"hostPolicyName": "hostPolicyName",
"policyRevision": 0,
"autoDeactivated": true,
"agentLogs": [
        "created": "2000-01-23T04:56:07.000+00:00",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "returned": "2000-01-23T04:56:07.000+00:00"
    },
        "created": "2000-01-23T04:56:07.000+00:00",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "returned": "2000-01-23T04:56:07.000+00:00"
"deactivated": true,
"authorisationState": "authorisationState",
"certificateInformation": {
    "lastIssued": "2000-01-23T04:56:07.000+00:00",
    "validFrom": "2000-01-23T04:56:07.000+00:00",
    "validTo": "2000-01-23T04:56:07.000+00:00"
},
"lastConnected": "2000-01-23T04:56:07.000+00:00",
"hostType": "hostType",
"authorised": "2000-01-23T04:56:07.000+00:00",
"adapterVersion": "adapterVersion",
"hostLastUpdated": "2000-01-23T04:56:07.000+00:00",
"id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"policyName": "policyName",
"created": "2000-01-23T04:56:07.000+00:00",
"pendingDeactivation": true,
"endpointInformation": {
    "systemModel": "systemModel",
    "systemPrimaryOwnerName": "systemPrimaryOwnerName",
    "osArchitecture": "osArchitecture",
    "systemSystemType": "systemSystemType",
    "systemDomain": "systemDomain",
    "processorManufacturer": "processorManufacturer",
```



```
"osVersion": "osVersion",
    "systemName": "systemName",
    "osVersionString": "osVersionString",
    "osCaption": "osCaption",
    "systemManufacturer": "systemManufacturer",
    "processorName": "processorName",
    "osCodeSet": "osCodeSet",
    "osSystemDrive": "osSystemDrive",
    "osOrganization": "osOrganization",
    "processorDescription": "processorDescription",
    "osCountryCode": "osCountryCode",
    "osInstallDate": "2000-01-23T04:56:07.000+00:00",
    "osSystemDirectory": "osSystemDirectory",
    "osComputerDescription": "osComputerDescription",
    "osSerialNumber": "osSerialNumber",
    "macAddress": "macAddress",
    "processorCaption": "processorCaption",
    "systemDnsHostName": "systemDnsHostName",
    "osManufacturer": "osManufacturer",
    "systemWorkgroup": "systemWorkgroup"
},
"connected": true,
"credentialType": "credentialType",
"groupName": "groupName",
"policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"duplicateCount": 1,
"agentVersion": "agentVersion",
"hostPolicyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"policyRevisionStatus": "policyRevisionStatus",
"hostPolicyRevision": 6,
"policyUpdateTimeStamp": "2000-01-23T04:56:07.000+00:00"
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json

### Responses

#### 200

Success ComputerDetailModel

### 400

Bad Request ProblemDetails



Unauthorized ProblemDetails



# get /v2/Computers/{id}/Logs

Gets Computer Logs (v2ComputersIdLogsGet)

### **Path parameters**

# id (required)

Path Parameter — format: uuid

# Return type

array[ ComputerLogModel]

# **Example data**

Content-Type: application/json

```
[
{
          "created": "2000-01-23T04:56:07.000+00:00",
          "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
          "returned": "2000-01-23T04:56:07.000+00:00"
},
{
          "created": "2000-01-23T04:56:07.000+00:00",
          "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
          "returned": "2000-01-23T04:56:07.000+00:00"
}
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json



### Responses

200

Success

400

Bad Request ProblemDetails

401

Unauthorized ProblemDetails



# get /v2/Computers/Logs/{id}/Content

Downloads Computer Log (v2ComputersLogsIdContentGet)

### **Path parameters**

# id (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

# Responses

404

Not Found ProblemDetails

409

Conflict ProblemDetails





# post /v2/Computers/Logs/Request

Retrieves Computer Logs (v2ComputersLogsRequestPost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- text/json
- · application/\*+json

### **Request body**

body ComputerRetrieveLogsRequest (optional)

Body Parameter —

### Return type

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json

# Responses

### 201

Created **UUID** 

### 400

Bad Request ProblemDetails



Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails



## post /v2/Computers/Reject

Rejects Computers (v2ComputersRejectPost)

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ComputersRejectRequest (optional)

Body Parameter — Request containing data to filter Computers to be rejected

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json

# Responses

#### 200

Success



Created **UUID** 

404

Not Found ProblemDetails

409

Conflict ProblemDetails

423

Client Error ProblemDetails

### **Events**



get /v2/Events/FromStartDate

Gets the list of events by start date ( v2EventsFromStartDateGet)

### **Query parameters**

# StartDate (required)

**Query Parameter** — Start Date(UTC) to search events from (Elastic Ingestion Timestamp in UTC). Example: 2022-08-12T17:34:28.694Z

# RecordSize (optional)

Query Parameter — Maximum records that can be returned. Min size: 1, Max size: 1000, Example: 100 default: 1000 format: int32

# Return type

**EpmEcsEventResponseModel** 

# **Example data**

Content-Type: application/json



```
"totalRecordsReturned": 0,
"events": [
   {
        "container": {
            "image": {
                "name": "name",
                "tag": [
                    "tag",
                     "tag"
                ],
                "hash": {
                     "all": [
                        "all",
                         "all"
            },
            "disk": {
                "read": {
                    "bytes": 4
                },
                "write": {
                     "bytes": 5
            },
            "memory": {
                "usage": 9.965781217890562
            },
            "name": "name",
            "cpu": {
                "usage": 1.1730742509559433
            "runtime": "runtime",
            "id": "id",
            "labels": "labels",
            "network": {
                "ingress": {
                    "bytes": 9
                "egress": {
                    "bytes": 6
            }
        "server": {
            "nat": {
                "port": 7,
                "ip": "ip"
            "address": "address",
            "top_level_domain": "top_level_domain",
            "ip": "ip",
```



```
"mac": "mac",
    "packets": 0,
    "registered_domain": "registered_domain",
    "port": 4,
    "bytes": 0,
    "domain": "domain",
    "subdomain": "subdomain"
"agent": {
    "build": {
        "original": "original"
    "name": "name",
    "id": "id",
    "type": "type",
    "ephemeral_id": "ephemeral_id",
    "version": "version"
},
"faas": {
    "execution": "execution",
    "coldstart": true,
    "name": "name",
    "id": "id",
    "trigger": {
        "type": "type",
        "request id": "request id"
    "version": "version"
},
"log": {
    "file": {
        "path": "path"
    "level": "level",
    "logger": "logger",
    "origin": {
        "file": {
            "line": 7,
            "name": "name"
        "function": "function"
    "syslog": "syslog"
"destination": {
    "nat": {
        "port": 3,
        "ip": "ip"
    "address": "address",
    "top_level_domain": "top_level_domain",
    "ip": "ip",
    "mac": "mac",
```



```
"packets": 6,
    "registered domain": "registered domain",
    "port": 8,
    "bytes": 9,
    "domain": "domain",
    "subdomain": "subdomain"
},
"rule": {
    "reference": "reference",
    "license": "license",
    "author": [
        "author",
        "author"
    ],
    "name": "name",
    "ruleset": "ruleset",
    "description": "description",
    "id": "id",
    "category": "category",
    "uuid": "uuid",
    "version": "version"
"error": {
    "code": "code",
    "id": "id",
    "stack trace": "stack trace",
    "message": "message",
    "type": "type"
"network": {
    "transport": "transport",
    "type": "type",
    "inner": "inner",
    "packets": 0,
    "protocol": "protocol",
    "forwarded ip": "forwarded_ip",
    "community id": "community id",
    "application": "application",
    "vlan": {
        "name": "name",
        "id": "id"
    "bytes": 9,
    "name": "name",
    "iana number": "iana_number",
    "direction": "direction"
"cloud": {
    "availability_zone": "availability_zone",
    "instance": {
        "name": "name",
        "id": "id"
    },
```



```
"provider": "provider",
    "machine": {
        "type": "type"
    "service": {
        "name": "name"
    },
    "origin": {
        "availability_zone": "availability_zone",
        "provider": "provider",
        "region": "region"
    },
    "project": {
        "name": "name",
        "id": "id"
    },
    "region": "region",
    "account": {
        "name": "name",
        "id": "id"
    },
    "target": {
        "availability_zone": "availability_zone",
        "provider": "provider",
        "region": "region"
"observer": {
    "product": "product",
    "ip": [
        "ip",
        "ip"
    "serial number": "serial number",
    "type": "type",
    "version": "version",
    "mac": [
        "mac",
        "mac"
    "egress": "egress",
    "ingress": "ingress",
"hostname": "hostname",
    "vendor": "vendor",
    "name": "name"
"trace": {
    "id": "id"
"file": {
    "extension": "extension",
    "SourceUrl": "SourceUrl",
    "Owner": {
```





```
"Identifier": "Identifier",
    "DomainName": "DomainName",
    "DomainNetBIOSName": "DomainNetBIOSName",
    "Name": "Name",
    "DomainIdentifier": "DomainIdentifier"
},
"gid": "gid",
"Description": "Description",
"drive letter": "drive letter",
"ProductVersion": "ProductVersion",
"type": "type",
"mtime": "2000-01-23T04:56:07.000+00:00",
"accessed": "2000-01-23T04:56:07.000+00:00",
"directory": "directory",
"inode": "inode",
"mode": "mode",
"path": "path",
"uid": "uid",
"Version": "Version",
"ctime": "2000-01-23T04:56:07.000+00:00",
"fork name": "fork name",
"elf": {
    "imports": {
        "key": "imports"
    "shared libraries": [
        "shared_libraries",
        "shared libraries"
    1,
    "byte order": "byte order",
    "exports": {
       "key": "exports"
    "cpu type": "cpu type",
    "header": {
       "object_version": "object_version",
        "data": "data",
        "os abi": "os abi",
        "entrypoint": 7,
        "abi version": "abi version",
        "type": "type",
        "class": "class",
        "version": "version"
    "creation date": "2000-01-23T04:56:07.000+00:00",
    "sections": [
            "chi2": 4,
            "virtual address": 7,
            "entropy": 0,
            "physical offset": "physical offset",
            "flags": "flags",
            "name": "name",
```



```
"physical size": 0,
            "type": "type",
            "virtual_size": 6
            "chi2": 4,
            "virtual address": 7,
            "entropy": 0,
            "physical offset": "physical offset",
            "flags": "flags",
            "name": "name",
            "physical size": 0,
            "type": "type",
            "virtual size": 6
    ],
    "telfhash": "telfhash",
    "architecture": "architecture",
    "segments": [
        {
            "type": "type",
            "sections": "sections"
        },
            "type": "type",
            "sections": "sections"
    ]
},
"group": "group",
"owner": "owner",
"created": "2000-01-23T04:56:07.000+00:00",
"Bundle": {
   "Type": "Type",
    "DownloadSource": "DownloadSource",
    "Version": "Version",
    "InfoDescription": "InfoDescription",
    "Creator": "Creator",
    "Uri": "Uri",
    "Name": "Name"
"target_path": "target_path",
"DriveType": "DriveType",
"x509": {
    "not after": "2000-01-23T04:56:07.000+00:00",
    "public_key_exponent": 3,
    "not before": "2000-01-23T04:56:07.000+00:00",
    "subject": {
        "state_or_province": [
            "state_or_province",
            "state_or_province"
        "country": [
```



```
"country",
        "country"
    ],
    "organization": [
        "organization",
        "organization"
    "distinguished name": "distinguished name",
    "locality": [
        "locality",
        "locality"
    ],
    "common name": [
        "common_name",
        "common_name"
    "organizational_unit": [
        "organizational_unit",
        "organizational unit"
},
"public_key_algorithm": "public_key_algorithm",
"public_key_curve": "public_key_curve",
"signature_algorithm": "signature_algorithm",
"version_number": "version_number",
"serial_number": "serial_number",
"public_key_size": 3,
"alternative names": [
    "alternative names",
    "alternative names"
],
"issuer": {
    "state or province": [
        "state or province",
        "state or province"
    "country": [
        "country",
        "country"
    "organization": [
        "organization",
        "organization"
    "distinguished_name": "distinguished_name",
    "locality": [
        "locality",
        "locality"
    "common_name": [
        "common_name",
        "common_name"
    ],
```



```
"organizational unit": [
                "organizational unit",
                "organizational_unit"
    },
    "size": 6,
    "mime_type": "mime_type",
    "ZoneTag": "ZoneTag",
    "name": "name",
    "attributes": [
        "attributes",
        "attributes"
    "device": "device"
},
"ecs": {
    "version": "version"
},
"related": {
    "hosts": [
        "hosts",
        "hosts"
    ],
    "ip": [
        "ip",
        "ip"
    ],
    "user": [
        "user",
        "user"
    ],
    "hash": [
        "hash",
        "hash"
    ]
"host": {
    "DefaultUILanguage": "DefaultUILanguage",
    "os": {
        "kernel": "kernel",
        "name": "name",
        "ProductType": "ProductType",
        "type": "type",
        "family": "family",
        "version": "version",
        "platform": "platform",
        "full": "full"
    "DomainNetBIOSName": "DomainNetBIOSName",
    "ip": [
        "ip",
        "ip"
```



```
"cpu": {
        "usage": 7.740351818741173
    "pid_ns_ino": "pid_ns_ino",
    "type": "type",
    "mac": [
        "mac",
        "mac"
    ],
    "uptime": 8,
    "network": {
        "ingress": {
            "bytes": 7,
            "packets": 5
        "egress": {
            "bytes": 3,
            "packets": 4
    },
    "DefaultLocale": "DefaultLocale",
    "hostname": "hostname",
    "disk": {
        "read": {
            "bytes": 3
        },
        "write": {
            "bytes": 3
    },
    "domain": "domain",
    "NetBIOSName": "NetBIOSName",
    "name": "name",
    "id": "id",
    "ChassisType": "ChassisType",
    "boot": {
        "id": "id"
    "architecture": "architecture",
    "DomainIdentifier": "DomainIdentifier"
"client": {
    "nat": {
        "port": 5,
        "ip": "ip"
    "address": "address",
    "top_level_domain": "top_level_domain",
    "ip": "ip",
    "mac": "mac",
    "packets": 5,
    "Name": "Name",
```



```
"geo": {
   "continent name": "continent name",
   "region iso code": "region iso code",
   "city name": "city_name",
   "country_iso_code": "country_iso_code",
   "timezone": "timezone",
   "country name": "country name",
   "name": "name",
   "continent code": "continent code",
    "location": {
       "lon": 7.061401241503109,
       "lat": 9.301444243932576
   "region name": "region name",
   "postal_code": "postal code",
   "TimezoneOffset": 3
"registered domain": "registered domain",
"as": {
   "number": 2,
   "organization": {
       "name": "name"
},
"port": 6,
"bytes": 1,
"domain": "domain",
"subdomain": "subdomain",
"user": {
   "DefaultUILanguage": "DefaultUILanguage",
   "DomainNetBIOSName": "DomainNetBIOSName",
   "roles": [
        "roles",
        "roles"
    "changes": {
        "DefaultUILanguage": "DefaultUILanguage",
        "DomainNetBIOSName": "DomainNetBIOSName",
        "roles": [
            "roles",
            "roles"
        "LocalIdentifier": 7,
        "DefaultTimezoneOffset": 6,
        "DefaultLocale": "DefaultLocale",
        "full name": "full name",
        "domain": "domain",
        "name": "name",
        "id": "id",
        "email": "email",
        "hash": "hash",
        "DomainIdentifier": "DomainIdentifier"
   },
```



```
"LocalIdentifier": 4,
        "target": {
            "DefaultUILanguage": "DefaultUILanguage",
            "DomainNetBIOSName": "DomainNetBIOSName",
            "roles": [
                "roles",
                "roles"
            ],
            "LocalIdentifier": 1,
            "DefaultTimezoneOffset": 7,
            "DefaultLocale": "DefaultLocale",
            "full name": "full name",
            "domain": "domain",
            "name": "name",
            "id": "id",
            "email": "email",
            "hash": "hash",
            "DomainIdentifier": "DomainIdentifier"
        "DefaultTimezoneOffset": 2,
        "DefaultLocale": "DefaultLocale",
        "effective": {
            "DefaultUILanguage": "DefaultUILanguage",
            "DomainNetBIOSName": "DomainNetBIOSName",
            "roles": [
                "roles",
                "roles"
            1,
            "LocalIdentifier": 1,
            "DefaultTimezoneOffset": 1,
            "DefaultLocale": "DefaultLocale",
            "full name": "full name",
            "domain": "domain",
            "name": "name",
            "id": "id",
            "email": "email",
            "hash": "hash",
            "DomainIdentifier": "DomainIdentifier"
        "full name": "full name",
        "domain": "domain",
        "name": "name",
        "id": "id",
        "email": "email",
        "hash": "hash",
        "DomainIdentifier": "DomainIdentifier",
        "group": {
            "domain": "domain",
            "name": "name",
            "id": "id"
    }
},
```



```
"event": {
    "reason": "reason",
    "code": "code",
    "timezone": "timezone",
    "type": [
        "type",
        "type"
    ],
    "duration": 2,
    "reference": "reference",
    "agent id status": "agent id status",
    "ingested": "2000-01-23T04:56:07.000+00:00",
    "provider": "provider",
    "action": "action",
    "end": "2000-01-23T04:56:07.000+00:00",
    "id": "id",
    "outcome": "outcome",
    "severity": 1,
    "original": "original",
    "risk score": 6.878052220127876,
    "kind": "kind",
    "created": "2000-01-23T04:56:07.000+00:00",
    "module": "module",
    "start": "2000-01-23T04:56:07.000+00:00",
    "url": "url",
    "sequence": 6,
    "risk score norm": 5.944895607614016,
    "category": [
        "category",
        "category"
    ],
    "dataset": "dataset",
    "hash": "hash"
"email": {
    "cc": {
        "address": [
            "address",
            "address"
    "origination_timestamp": "2000-01-23T04:56:07.000+00:00",
    "attachments": [
            "file": {
                "extension": "extension",
                "size": 6,
                "mime_type": "mime_type",
                "name": "name"
        },
            "file": {
```



```
"extension": "extension",
                "size": 6,
                "mime type": "mime type",
                "name": "name"
    ],
    "bcc": {
        "address": [
            "address",
            "address"
    },
    "local_id": "local_id",
    "subject": "subject",
    "message_id": "message id",
    "x_mailer": "x_mailer",
    "content_type": "content_type",
    "reply to": {
        "address": [
            "address",
            "address"
    },
    "sender": {
        "address": "address"
    },
    "delivery timestamp": "2000-01-23T04:56:07.000+00:00",
    "from": {
        "address": [
            "address",
            "address"
    },
    "to": {
        "address": [
            "address",
            "address"
    "direction": "direction"
"user_agent": {
    "original": "original",
    "name": "name",
    "version": "version",
    "device": {
        "name": "name"
"registry": {
    "hive": "hive",
    "path": "path",
```



```
"data": {
        "strings": [
            "strings",
            "strings"
        "bytes": "bytes",
        "type": "type"
    },
    "value": "value",
    "key": "key"
},
"process": {
    "parent": {
        "ElevationRequired": true,
        "interactive": true,
        "pid": 1,
        "working_directory": "working directory",
        "title": "title",
        "end": "2000-01-23T04:56:07.000+00:00",
        "same as process": true,
        "group_leader": {
            "ElevationRequired": true,
            "interactive": true,
            "pid": 9,
            "working_directory": "working_directory",
            "title": "title",
            "end": "2000-01-23T04:56:07.000+00:00",
            "same as process": true,
            "pgid": 1,
            "start": "2000-01-23T04:56:07.000+00:00",
            "entity id": "entity id",
            "executable": "executable",
            "uptime": 9,
            "env vars": "env vars",
            "args": [
                "args",
                "args"
            ],
            "name": "name",
            "exit_code": 8,
            "tty": "tty",
            "args count": 3,
            "command line": "command line"
        "pgid": 8,
        "start": "2000-01-23T04:56:07.000+00:00",
        "entity id": "entity id",
        "executable": "executable",
        "uptime": 4,
        "env vars": "env vars",
        "args": [
            "args",
            "args"
```



```
"name": "name",
    "exit_code": 8,
    "tty": "tty",
    "args_count": 6,
    "command line": "command line"
"ElevationRequired": true,
"interactive": true,
"pid": 0,
"working_directory": "working_directory",
"title": "title",
"end": "2000-01-23T04:56:07.000+00:00",
"same as process": true,
"previous": {
    "ElevationRequired": true,
    "interactive": true,
    "pid": 0,
    "working_directory": "working directory",
    "title": "title",
    "end": "2000-01-23T04:56:07.000+00:00",
    "same as process": true,
    "pgid": 3,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity id": "entity id",
    "executable": "executable",
    "uptime": 3,
    "env vars": "env vars",
    "args": [
        "args",
        "args"
    ],
    "name": "name",
    "exit code": 8,
    "tty": "tty",
    "args_count": 2,
    "command line": "command line"
"pgid": 7,
"start": "2000-01-23T04:56:07.000+00:00",
"entry_meta": {
    "source": {
        "nat": {
            "port": 2,
            "ip": "ip"
        "address": "address",
        "top_level_domain": "top_level_domain",
        "ip": "ip",
        "mac": "mac",
        "packets": 0,
        "registered_domain": "registered_domain",
        "port": 4,
```



```
"bytes": 3,
        "domain": "domain",
        "subdomain": "subdomain"
    },
    "type": "type"
},
"thread": {
    "name": "name",
    "id": 4
},
"entity id": "entity id",
"executable": "executable",
"uptime": 6,
"env_vars": "env vars",
"args": [
    "args",
    "args"
],
"session leader": {
    "ElevationRequired": true,
    "interactive": true,
    "pid": 3,
    "working_directory": "working_directory",
    "title": "title",
    "end": "2000-01-23T04:56:07.000+00:00",
    "same as process": true,
    "pgid": 3,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity id": "entity id",
    "executable": "executable",
    "uptime": 5,
    "env vars": "env vars",
    "args": [
        "args",
        "args"
    ],
    "name": "name",
    "exit_code": 7,
    "tty": "tty",
    "args_count": 9,
    "command line": "command line"
"entry_leader": {
    "ElevationRequired": true,
    "interactive": true,
    "pid": 0,
    "working directory": "working directory",
    "title": "title",
    "end": "2000-01-23T04:56:07.000+00:00",
    "same_as_process": true,
    "pgid": 5,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity id": "entity id",
```



```
"executable": "executable",
        "uptime": 8,
        "env vars": "env vars",
        "args": [
            "args",
            "args"
        "name": "name",
        "exit_code": 7,
        "tty": "tty",
        "args count": 5,
        "command line": "command line"
    },
    "name": "name",
    "exit_code": 8,
    "tty": "tty",
    "args count": 5,
    "command_line": "command line"
"package": {
    "installed": "2000-01-23T04:56:07.000+00:00",
    "build version": "build version",
    "description": "description",
    "type": "type",
    "version": "version",
    "reference": "reference",
    "path": "path",
    "license": "license",
    "install scope": "install scope",
    "size": 9,
    "name": "name",
    "checksum": "checksum",
    "architecture": "architecture"
"dll": {
    "path": "path",
    "code signature": {
        "valid": true,
        "digest algorithm": "digest_algorithm",
        "signing id": "signing id",
        "trusted": true,
        "subject_name": "subject_name",
        "exists": true,
        "team_id": "team_id",
        "status": "status",
        "timestamp": "2000-01-23T04:56:07.000+00:00"
    },
    "pe": {
        "file version": "file version",
        "product": "product",
        "imphash": "imphash",
        "description": "description",
        "original file name": "original file name",
```



```
"company": "company",
        "pehash": "pehash",
        "architecture": "architecture"
    },
    "name": "name",
    "hash": {
        "sha1": "sha1",
        "sha384": "sha384",
        "sha256": "sha256",
        "sha512": "sha512",
        "tlsh": "tlsh",
        "ssdeep": "ssdeep",
        "md5": "md5"
"dns": {
    "op code": "op code",
    "response_code": "response_code",
    "resolved_ip": [
        "resolved ip",
        "resolved ip"
    ],
    "question": {
        "registered domain": "registered domain",
        "top level domain": "top level domain",
        "name": "name",
        "subdomain": "subdomain",
        "type": "type",
        "class": "class"
    },
    "answers": "answers",
    "id": "id",
    "header flags": [
        "header flags",
        "header flags"
    "type": "type"
"vulnerability": {
    "reference": "reference",
    "severity": "severity",
    "score": {
        "environmental": 4.8789878742268815,
        "version": "version",
        "temporal": 6.173804034172511,
        "base": 2.535258963197524
    "report id": "report id",
    "scanner": {
        "vendor": "vendor"
    "description": "description",
    "id": "id",
```



```
"classification": "classification",
    "enumeration": "enumeration",
    "category": [
        "category",
        "category"
"message": "message",
"tags": [
    "tags",
    "tags"
"labels": "labels",
"orchestrator": {
    "cluster": {
        "name": "name",
        "id": "id",
        "version": "version",
        "url": "url"
    },
    "resource": {
        "parent": {
            "type": "type"
        "ip": [
            "ip",
            "ip"
        1,
        "name": "name",
        "id": "id",
        "type": "type"
    },
    "organization": "organization",
    "namespace": "namespace",
    "type": "type",
    "api version": "api version"
"@timestamp": "2000-01-23T04:56:07.000+00:00",
"EPMWinMac": {
    "COM": {
        "AppID": "AppID",
        "CLSID": "CLSID",
        "DisplayName": "DisplayName"
    "AuthorizingUser": {
        "Identifier": "Identifier",
        "DomainNetBIOSName": "DomainNetBIOSName",
        "DomainName": "DomainName",
        "Name": "Name",
        "DomainIdentifier": "DomainIdentifier",
        "CredentialSource": "CredentialSource"
    "PrivilegedGroup": {
```



```
"Access": "Access",
   "RID": "RID",
   "Name": "Name"
},
"AuthorizationRequest": {
   "AuthRequestURI": "AuthRequestURI",
   "ControlAuthorization": true
},
"SchemaVersion": "SchemaVersion",
"Configuration": {
   "Path": "Path",
   "Message": {
        "Authorization": {
            "ResponseStatus": "ResponseStatus",
            "ChallengeCode": "ChallengeCode"
        "AuthMethods": [
            "AuthMethods",
            "AuthMethods"
        ],
        "Type": "Type",
        "Description": "Description",
        "Identifier": "Identifier",
        "Authentication": {
            "User": "User"
        },
        "UserReason": "UserReason",
        "Name": "Name"
    },
    "GPO": {
        "Version": "Version",
        "DisplayName": "DisplayName",
        "LinkInformation": "LinkInformation",
        "ActiveDirectoryPath": "ActiveDirectoryPath"
    "LoadAuditMode": [
        "LoadAuditMode",
        "LoadAuditMode"
    "Token": {
        "Description": "Description",
        "Identifier": "Identifier",
        "Name": "Name"
    "ContentGroup": {
        "Description": "Description",
        "Identifier": "Identifier",
        "Name": "Name"
    "RuleScript": {
        "Outcome": {
            "Version": "Version",
            "Output": "Output",
```



```
"RuleAffected": true,
             "Name": "Name",
             "Result": "Result"
        },
        "FileName": "FileName",
        "Publisher": "Publisher"
    },
    "RevisionNumber": "RevisionNumber",
    "Workstyle": {
        "Description": "Description",
        "Identifier": "Identifier",
        "Name": "Name"
    },
    "Source": "Source",
    "Name": "Name",
    "ApplicationGroup": {
        "Description": "Description",
        "Identifier": "Identifier",
        "Name": "Name"
    },
    "Identifier": "Identifier",
    "Content": {
        "Type": "Type",
        "Description": "Description",
"Identifier": "Identifier"
    },
    "SigningEnforcement": "SigningEnforcement",
    "Rule": {
        "Action": "Action",
        "Identifier": "Identifier",
        "OnDemand": true
    "Application": {
        "Type": "Type",
"Description": "Description",
        "Identifier": "Identifier"
"Installer": {
    "Action": "Action",
    "ProductCode": "ProductCode",
    "UpgradeCode": "UpgradeCode"
"ActiveX": {
    "Version": "Version",
    "CLSID": "CLSID",
    "Codebase": "Codebase"
"GroupId": "GroupId",
"TenantId": "TenantId",
"StoreApp": {
    "Version": "Version",
    "Publisher": "Publisher",
```



```
"Name": "Name"
    "ServiceControl": {
        "Service": {
            "Action": "Action",
            "DisplayName": "DisplayName",
            "Name": "Name"
    },
    "TrustedApplication": {
        "Version": "Version",
        "Name": "Name"
    },
    "Event": {
        "Type": "Type",
        "Action": "Action"
    },
    "RemotePowerShell": {
        "Command": "Command"
    },
    "AdapterVersion": "AdapterVersion",
    "Session": {
        "Locale": "Locale",
        "PowerUser": true,
        "WindowsSessionId": "WindowsSessionId",
        "Administrator": true,
        "Identifier": "Identifier",
        "UILanguage": "UILanguage"
},
"data stream": {
    "namespace": "namespace",
    "type": "type",
    "dataset": "dataset"
"service": {
    "node": {
       "role": "role",
        "name": "name"
    "environment": "environment",
    "address": "address",
    "origin": {
        "environment": "environment",
        "address": "address",
        "name": "name",
        "id": "id",
        "state": "state",
        "type": "type",
        "ephemeral id": "ephemeral id",
        "version": "version"
    },
    "name": "name",
```



```
"id": "id",
    "state": "state",
    "type": "type",
    "ephemeral_id": "ephemeral id",
    "version": "version",
    "target": {
        "environment": "environment",
        "address": "address",
        "name": "name",
        "id": "id",
        "state": "state",
        "type": "type",
        "ephemeral_id": "ephemeral_id",
        "version": "version"
    }
},
"organization": {
    "name": "name",
    "id": "id"
"http": {
    "request": {
        "referrer": "referrer",
        "method": "method",
        "mime type": "mime type",
        "bytes": 6,
        "id": "id",
        "body": {
            "bytes": 0,
            "content": "content"
    },
    "response": {
        "status code": 4,
        "mime type": "mime_type",
        "bytes": 4,
        "body": {
            "bytes": 1,
            "content": "content"
    "version": "version"
"tls": {
    "cipher": "cipher",
    "established": true,
    "server": {
        "not after": "2000-01-23T04:56:07.000+00:00",
        "ja3s": "ja3s",
        "subject": "subject",
        "not before": "2000-01-23T04:56:07.000+00:00",
        "certificate": "certificate",
        "issuer": "issuer",
```



```
"certificate chain": [
            "certificate chain",
            "certificate_chain"
        "hash": {
            "sha1": "sha1",
            "sha256": "sha256",
            "md5": "md5"
    },
    "curve": "curve",
    "next protocol": "next protocol",
    "client": {
        "not after": "2000-01-23T04:56:07.000+00:00",
        "server_name": "server_name",
        "supported_ciphers": [
            "supported_ciphers",
            "supported ciphers"
        ],
        "subject": "subject",
        "not before": "2000-01-23T04:56:07.000+00:00",
        "certificate": "certificate",
        "ja3": "ja3",
        "issuer": "issuer",
        "certificate chain": [
            "certificate chain",
            "certificate chain"
        ],
        "hash": {
            "sha1": "sha1",
            "sha256": "sha256",
            "md5": "md5"
    },
    "resumed": true,
    "version": "version",
    "version protocol": "version protocol"
"threat": {
    "indicator": {
        "first seen": "2000-01-23T04:56:07.000+00:00",
        "last seen": "2000-01-23T04:56:07.000+00:00",
        "confidence": "confidence",
        "ip": "ip",
        "sightings": 4,
        "description": "description",
        "type": "type",
        "url": {
            "extension": "extension",
            "original": "original",
            "scheme": "scheme",
            "top level domain": "top level domain",
            "query": "query",
```



```
"path": "path",
        "registered domain": "registered domain",
        "fragment": "fragment",
        "password": "password",
        "port": 0,
        "domain": "domain",
        "subdomain": "subdomain",
        "full": "full",
        "username": "username"
    },
    "scanner stats": 2,
    "reference": "reference",
    "marking": {
       "tlp": "tlp"
    },
    "port": 9,
    "provider": "provider",
    "modified at": "2000-01-23T04:56:07.000+00:00",
    "email": {
        "address": "address"
},
"feed": {
    "reference": "reference",
    "name": "name",
    "description": "description",
    "dashboard id": "dashboard id"
},
"framework": "framework",
"software": {
    "reference": "reference",
    "name": "name",
    "alias": [
       "alias",
        "alias"
    "id": "id",
    "type": "type",
    "platforms": [
       "platforms",
        "platforms"
"technique": {
    "reference": [
        "reference",
       "reference"
    ],
    "name": [
        "name",
        "name"
    "subtechnique": {
```



```
"reference": [
            "reference",
            "reference"
        ],
        "name": [
            "name",
            "name"
        "id": [
            "id",
            "id"
    "id": [
        "id",
        "id"
},
"enrichments": [
        "indicator": "indicator",
        "matched": {
            "field": "field",
            "occurred": "2000-01-23T04:56:07.000+00:00",
            "atomic": "atomic",
            "index": "index",
            "id": "id",
            "type": "type"
    },
        "indicator": "indicator",
        "matched": {
            "field": "field",
            "occurred": "2000-01-23T04:56:07.000+00:00",
            "atomic": "atomic",
            "index": "index",
            "id": "id",
            "type": "type"
    }
"group": {
    "reference": "reference",
    "name": "name",
    "alias": [
        "alias",
        "alias"
    "id": "id"
"tactic": {
    "reference": [
```



```
"reference",
                 "reference"
            ],
             "name": [
                 "name",
                 "name"
            ],
            "id": [
                 "id",
                 "id"
            ]
        }
    "transaction": {
        "id": "id"
    "span": {
        "id": "id"
},
    "container": {
        "image": {
            "name": "name",
            "tag": [
                "tag",
                 "tag"
            ],
            "hash": {
                 "all": [
                     "all",
                     "all"
        "disk": {
            "read": {
                "bytes": 4
            "write": {
                 "bytes": 5
        },
        "memory": {
            "usage": 9.965781217890562
        "name": "name",
        "cpu": {
            "usage": 1.1730742509559433
        "runtime": "runtime",
        "id": "id",
        "labels": "labels",
```



```
"network": {
        "ingress": {
            "bytes": 9
        "egress": {
            "bytes": 6
    }
},
"server": {
    "nat": {
        "port": 7,
        "ip": "ip"
    "address": "address",
    "top_level_domain": "top_level_domain",
    "ip": "ip",
    "mac": "mac",
    "packets": 0,
    "registered domain": "registered domain",
    "port": 4,
    "bytes": 0,
    "domain": "domain",
    "subdomain": "subdomain"
},
"agent": {
    "build": {
        "original": "original"
    },
    "name": "name",
    "id": "id",
    "type": "type",
    "ephemeral_id": "ephemeral_id",
"version": "version"
"faas": {
    "execution": "execution",
    "coldstart": true,
    "name": "name",
    "id": "id",
    "trigger": {
        "type": "type",
        "request id": "request id"
    "version": "version"
"log": {
    "file": {
        "path": "path"
    "level": "level",
    "logger": "logger",
    "origin": {
```



```
"file": {
            "line": 7,
            "name": "name"
        "function": "function"
    },
    "syslog": "syslog"
"destination": {
    "nat": {
        "port": 3,
        "ip": "ip"
    "address": "address",
    "top_level_domain": "top_level_domain",
    "ip": "ip",
    "mac": "mac",
    "packets": 6,
    "registered domain": "registered domain",
    "port": 8,
    "bytes": 9,
    "domain": "domain",
    "subdomain": "subdomain"
"rule": {
    "reference": "reference",
    "license": "license",
    "author": [
        "author",
        "author"
    ],
    "name": "name",
    "ruleset": "ruleset",
    "description": "description",
    "id": "id",
    "category": "category",
    "uuid": "uuid",
    "version": "version"
"error": {
    "code": "code",
    "id": "id",
    "stack_trace": "stack_trace",
    "message": "message",
    "type": "type"
"network": {
    "transport": "transport",
    "type": "type",
    "inner": "inner",
    "packets": 0,
    "protocol": "protocol",
    "forwarded ip": "forwarded ip",
```



```
"community_id": "community id",
    "application": "application",
    "vlan": {
        "name": "name",
        "id": "id"
    "bytes": 9,
    "name": "name",
    "iana number": "iana number",
    "direction": "direction"
"cloud": {
    "availability zone": "availability zone",
    "instance": {
        "name": "name",
        "id": "id"
    },
    "provider": "provider",
    "machine": {
        "type": "type"
    },
    "service": {
        "name": "name"
    },
    "origin": {
        "availability_zone": "availability_zone",
        "provider": "provider",
        "region": "region"
    },
    "project": {
        "name": "name",
        "id": "id"
    },
    "region": "region",
    "account": {
        "name": "name",
        "id": "id"
    "target": {
        "availability zone": "availability zone",
        "provider": "provider",
"region": "region"
"observer": {
    "product": "product",
    "ip": [
        "ip",
        "ip"
    "serial_number": "serial_number",
    "type": "type",
    "version": "version",
```



```
"mac": [
       "mac",
        "mac"
    "egress": "egress",
    "ingress": "ingress",
    "hostname": "hostname",
    "vendor": "vendor",
    "name": "name"
"trace": {
    "id": "id"
"file": {
    "extension": "extension",
    "SourceUrl": "SourceUrl",
    "Owner": {
        "Identifier": "Identifier",
        "DomainName": "DomainName",
        "DomainNetBIOSName": "DomainNetBIOSName",
        "Name": "Name",
        "DomainIdentifier": "DomainIdentifier"
    },
    "gid": "gid",
    "Description": "Description",
    "drive_letter": "drive_letter",
    "ProductVersion": "ProductVersion",
    "type": "type",
    "mtime": "2000-01-23T04:56:07.000+00:00",
    "accessed": "2000-01-23T04:56:07.000+00:00",
    "directory": "directory",
    "inode": "inode",
    "mode": "mode",
    "path": "path",
    "uid": "uid",
    "Version": "Version",
    "ctime": "2000-01-23T04:56:07.000+00:00",
    "fork name": "fork_name",
    "elf": {
        "imports": {
            "key": "imports"
        "shared libraries": [
            "shared libraries",
            "shared libraries"
        "byte_order": "byte_order",
        "exports": {
            "key": "exports"
        "cpu type": "cpu type",
        "header": {
            "object version": "object version",
```



```
"data": "data",
        "os_abi": "os_abi",
        "entrypoint": 7,
        "abi version": "abi version",
        "type": "type",
        "class": "class",
        "version": "version"
    },
    "creation date": "2000-01-23T04:56:07.000+00:00",
    "sections": [
            "chi2": 4,
            "virtual address": 7,
            "entropy": 0,
            "physical offset": "physical offset",
            "flags": "flags",
            "name": "name",
            "physical_size": 0,
            "type": "type",
            "virtual size": 6
        },
            "chi2": 4,
            "virtual address": 7,
            "entropy": 0,
            "physical offset": "physical offset",
            "flags": "flags",
"name": "name",
            "physical size": 0,
            "type": "type",
            "virtual size": 6
    ],
    "telfhash": "telfhash",
    "architecture": "architecture",
    "segments": [
            "type": "type",
            "sections": "sections"
        },
            "type": "type",
            "sections": "sections"
    ]
"group": "group",
"owner": "owner",
"created": "2000-01-23T04:56:07.000+00:00",
"Bundle": {
    "Type": "Type",
    "DownloadSource": "DownloadSource",
    "Version": "Version",
```



```
"InfoDescription": "InfoDescription",
    "Creator": "Creator",
    "Uri": "Uri",
    "Name": "Name"
"target_path": "target_path",
"DriveType": "DriveType",
"x509": {
    "not after": "2000-01-23T04:56:07.000+00:00",
    "public_key_exponent": 3,
    "not before": "2000-01-23T04:56:07.000+00:00",
    "subject": {
        "state or province": [
            "state_or_province",
            "state_or_province"
        "country": [
            "country",
            "country"
        "organization": [
            "organization",
            "organization"
        "distinguished name": "distinguished name",
        "locality": [
            "locality",
            "locality"
        ],
        "common name": [
            "common name",
             "common name"
        "organizational_unit": [
            "organizational unit",
             "organizational unit"
    "public_key_algorithm": "public_key_algorithm",
    "public_key_curve": "public_key_curve",
    "signature algorithm": "signature algorithm",
    "version_number": "version_number",
"serial_number": "serial_number",
    "public_key_size": 3,
    "alternative_names": [
        "alternative_names",
        "alternative_names"
    "issuer": {
        "state_or_province": [
            "state_or_province",
            "state_or_province"
        ],
```



```
"country": [
                "country",
                "country"
            "organization": [
                "organization",
                "organization"
            "distinguished_name": "distinguished_name",
            "locality": [
                "locality",
                "locality"
            ],
            "common_name": [
                "common_name",
                "common_name"
            ],
            "organizational_unit": [
                "organizational_unit",
                 "organizational unit"
    },
    "size": 6,
    "mime type": "mime_type",
    "ZoneTag": "ZoneTag",
    "name": "name",
    "attributes": [
        "attributes",
        "attributes"
    "device": "device"
"ecs": {
    "version": "version"
"related": {
    "hosts": [
        "hosts",
        "hosts"
    "ip": [
        "ip",
        "ip"
    "user": [
        "user",
        "user"
    "hash": [
        "hash",
        "hash"
    ]
```



```
"host": {
    "DefaultUILanguage": "DefaultUILanguage",
    "os": {
        "kernel": "kernel",
        "name": "name",
        "ProductType": "ProductType",
        "type": "type",
        "family": "family",
        "version": "version",
        "platform": "platform",
        "full": "full"
    },
    "DomainNetBIOSName": "DomainNetBIOSName",
    "ip": [
        "ip",
        "ip"
    ],
    "cpu": {
        "usage": 7.740351818741173
    "pid_ns_ino": "pid_ns_ino",
    "type": "type",
    "mac": [
        "mac",
        "mac"
    ],
    "uptime": 8,
    "network": {
        "ingress": {
            "bytes": 7,
            "packets": 5
        },
        "egress": {
            "bytes": 3,
            "packets": 4
    },
    "DefaultLocale": "DefaultLocale",
    "hostname": "hostname",
    "disk": {
        "read": {
            "bytes": 3
        "write": {
            "bytes": 3
    "domain": "domain",
    "NetBIOSName": "NetBIOSName",
    "name": "name",
    "id": "id",
    "ChassisType": "ChassisType",
```



```
"boot": {
       "id": "id"
    "architecture": "architecture",
    "DomainIdentifier": "DomainIdentifier"
"client": {
    "nat": {
        "port": 5,
        "ip": "ip"
    "address": "address",
    "top level domain": "top level domain",
    "ip": "ip",
    "mac": "mac",
    "packets": 5,
    "Name": "Name",
    "geo": {
        "continent_name": "continent_name",
        "region_iso_code": "region_iso_code",
        "city_name": "city_name",
        "country iso code": "country iso code",
        "timezone": "timezone",
        "country name": "country name",
        "name": "name",
        "continent code": "continent code",
        "location": {
            "lon": 7.061401241503109,
            "lat": 9.301444243932576
        },
        "region name": "region name",
        "postal_code": "postal_code",
        "TimezoneOffset": 3
    },
    "registered domain": "registered_domain",
    "as": {
        "number": 2,
        "organization": {
            "name": "name"
    },
    "port": 6,
    "bytes": 1,
    "domain": "domain",
    "subdomain": "subdomain",
    "user": {
        "DefaultUILanguage": "DefaultUILanguage",
        "DomainNetBIOSName": "DomainNetBIOSName",
        "roles": [
            "roles",
            "roles"
        "changes": {
```



```
"DefaultUILanguage": "DefaultUILanguage",
    "DomainNetBIOSName": "DomainNetBIOSName",
    "roles": [
        "roles",
        "roles"
    "LocalIdentifier": 7,
    "DefaultTimezoneOffset": 6,
    "DefaultLocale": "DefaultLocale",
    "full name": "full name",
    "domain": "domain",
    "name": "name",
    "id": "id",
    "email": "email",
    "hash": "hash",
    "DomainIdentifier": "DomainIdentifier"
},
"LocalIdentifier": 4,
"target": {
    "DefaultUILanguage": "DefaultUILanguage",
    "DomainNetBIOSName": "DomainNetBIOSName",
    "roles": [
        "roles",
        "roles"
    ],
    "LocalIdentifier": 1,
    "DefaultTimezoneOffset": 7,
    "DefaultLocale": "DefaultLocale",
    "full name": "full name",
    "domain": "domain",
    "name": "name",
    "id": "id",
    "email": "email",
    "hash": "hash",
    "DomainIdentifier": "DomainIdentifier"
"DefaultTimezoneOffset": 2,
"DefaultLocale": "DefaultLocale",
"effective": {
    "DefaultUILanguage": "DefaultUILanguage",
    "DomainNetBIOSName": "DomainNetBIOSName",
    "roles": [
        "roles",
        "roles"
    "LocalIdentifier": 1,
    "DefaultTimezoneOffset": 1,
    "DefaultLocale": "DefaultLocale",
    "full name": "full name",
    "domain": "domain",
    "name": "name",
    "id": "id",
    "email": "email",
```



```
"hash": "hash",
            "DomainIdentifier": "DomainIdentifier"
        "full name": "full name",
        "domain": "domain",
        "name": "name",
        "id": "id",
        "email": "email",
        "hash": "hash",
        "DomainIdentifier": "DomainIdentifier",
        "group": {
            "domain": "domain",
            "name": "name",
            "id": "id"
    }
"event": {
    "reason": "reason",
    "code": "code",
    "timezone": "timezone",
    "type": [
        "type",
        "type"
    ],
    "duration": 2,
    "reference": "reference",
    "agent_id_status": "agent_id_status",
    "ingested": "2000-01-23T04:56:07.000+00:00",
    "provider": "provider",
    "action": "action",
    "end": "2000-01-23T04:56:07.000+00:00",
    "id": "id",
    "outcome": "outcome",
    "severity": 1,
    "original": "original",
    "risk score": 6.878052220127876,
    "kind": "kind",
    "created": "2000-01-23T04:56:07.000+00:00",
    "module": "module",
    "start": "2000-01-23T04:56:07.000+00:00",
    "url": "url",
    "sequence": 6,
    "risk_score_norm": 5.944895607614016,
    "category": [
        "category",
        "category"
    "dataset": "dataset",
    "hash": "hash"
"email": {
    "cc": {
```



```
"address": [
        "address",
        "address"
"origination timestamp": "2000-01-23T04:56:07.000+00:00",
"attachments": [
    {
        "file": {
             "extension": "extension",
             "size": 6,
             "mime_type": "mime_type",
             "name": "name"
    },
        "file": {
             "extension": "extension",
             "size": 6,
             "mime_type": "mime_type",
             "name": "name"
],
"bcc": {
    "address": [
        "address",
        "address"
},
"local_id": "local_id",
"subject": "subject",
"message id": "message id",
"x mailer": "x mailer",
"content type": "content type",
"reply to": {
    "address": [
        "address",
        "address"
"sender": {
    "address": "address"
"delivery timestamp": "2000-01-23T04:56:07.000+00:00",
"from": {
    "address": [
        "address",
        "address"
"to": {
    "address": [
```



```
"address",
            "address"
    },
    "direction": "direction"
},
"user agent": {
    "original": "original",
    "name": "name",
    "version": "version",
    "device": {
        "name": "name"
},
"registry": {
    "hive": "hive",
    "path": "path",
    "data": {
        "strings": [
            "strings",
            "strings"
        ],
        "bytes": "bytes",
        "type": "type"
    },
    "value": "value",
    "key": "key"
"process": {
    "parent": {
        "ElevationRequired": true,
        "interactive": true,
        "pid": 1,
        "working_directory": "working_directory",
        "title": "title",
        "end": "2000-01-23T04:56:07.000+00:00",
        "same as process": true,
        "group leader": {
            "ElevationRequired": true,
            "interactive": true,
            "pid": 9,
            "working_directory": "working_directory",
            "title": "title",
            "end": "2000-01-23T04:56:07.000+00:00",
            "same_as_process": true,
            "pgid": 1,
            "start": "2000-01-23T04:56:07.000+00:00",
            "entity_id": "entity_id",
            "executable": "executable",
            "uptime": 9,
            "env vars": "env vars",
            "args": [
                "args",
```



```
"args"
        ],
        "name": "name",
        "exit_code": 8,
        "tty": "tty",
        "args count": 3,
        "command line": "command line"
    },
    "pgid": 8,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity id": "entity id",
    "executable": "executable",
    "uptime": 4,
    "env vars": "env vars",
    "args": [
        "args",
        "args"
    ],
    "name": "name",
    "exit_code": 8,
    "tty": "tty",
    "args_count": 6,
    "command line": "command line"
},
"ElevationRequired": true,
"interactive": true,
"pid": 0,
"working_directory": "working_directory",
"title": "title",
"end": "2000-01-23T04:56:07.000+00:00",
"same as process": true,
"previous": {
    "ElevationRequired": true,
    "interactive": true,
    "pid": 0,
    "working directory": "working_directory",
    "title": "title",
    "end": "2000-01-23T04:56:07.000+00:00",
    "same as process": true,
    "pgid": 3,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity_id": "entity_id",
    "executable": "executable",
    "uptime": 3,
    "env vars": "env vars",
    "args": [
        "args",
        "args"
    "name": "name",
    "exit code": 8,
    "tty": "tty",
    "args count": 2,
```



```
"command line": "command line"
},
"pgid": 7,
"start": "2000-01-23T04:56:07.000+00:00",
"entry_meta": {
    "source": {
        "nat": {
            "port": 2,
            "ip": "ip"
        "address": "address",
        "top_level_domain": "top_level_domain",
        "ip": "ip",
        "mac": "mac",
        "packets": 0,
        "registered_domain": "registered_domain",
        "port": 4,
        "bytes": 3,
        "domain": "domain",
        "subdomain": "subdomain"
    },
    "type": "type"
},
"thread": {
    "name": "name",
    "id": 4
},
"entity id": "entity id",
"executable": "executable",
"uptime": 6,
"env vars": "env vars",
"args": [
    "args",
    "args"
],
"session_leader": {
    "ElevationRequired": true,
    "interactive": true,
    "pid": 3,
    "working_directory": "working_directory",
    "title": "title",
    "end": "2000-01-23T04:56:07.000+00:00",
    "same_as_process": true,
    "pgid": 3,
    "start": "2000-01-23T04:56:07.000+00:00",
    "entity id": "entity_id",
    "executable": "executable",
    "uptime": 5,
    "env vars": "env_vars",
    "args": [
        "args",
        "args"
    ],
```



```
"name": "name",
        "exit_code": 7,
        "tty": "tty",
        "args count": 9,
        "command line": "command line"
    },
    "entry_leader": {
        "ElevationRequired": true,
        "interactive": true,
        "pid": 0,
        "working_directory": "working_directory",
        "title": "title",
        "end": "2000-01-23T04:56:07.000+00:00",
        "same as process": true,
        "pgid": 5,
        "start": "2000-01-23T04:56:07.000+00:00",
        "entity id": "entity id",
        "executable": "executable",
        "uptime": 8,
        "env vars": "env vars",
        "args": [
            "args",
            "args"
        ],
        "name": "name",
        "exit_code": 7,
        "tty": "tty",
        "args_count": 5,
        "command line": "command line"
    },
    "name": "name",
    "exit code": 8,
    "tty": "tty",
    "args count": 5,
    "command line": "command line"
"package": {
    "installed": "2000-01-23T04:56:07.000+00:00",
    "build version": "build version",
    "description": "description",
    "type": "type",
    "version": "version",
    "reference": "reference",
    "path": "path",
    "license": "license",
    "install scope": "install scope",
    "size": 9,
    "name": "name",
    "checksum": "checksum",
    "architecture": "architecture"
"dll": {
    "path": "path",
```



```
"code signature": {
        "valid": true,
        "digest algorithm": "digest algorithm",
        "signing id": "signing id",
        "trusted": true,
        "subject_name": "subject_name",
        "exists": true,
        "team id": "team id",
        "status": "status",
        "timestamp": "2000-01-23T04:56:07.000+00:00"
    },
    "pe": {
        "file version": "file version",
        "product": "product",
        "imphash": "imphash",
        "description": "description",
        "original_file_name": "original_file_name",
        "company": "company",
        "pehash": "pehash",
        "architecture": "architecture"
    },
    "name": "name",
    "hash": {
        "sha1": "sha1",
        "sha384": "sha384",
        "sha256": "sha256",
        "sha512": "sha512",
        "tlsh": "tlsh",
        "ssdeep": "ssdeep",
        "md5": "md5"
"dns": {
    "op code": "op code",
    "response code": "response code",
    "resolved ip": [
        "resolved ip",
        "resolved_ip"
    ],
    "question": {
        "registered domain": "registered domain",
        "top level domain": "top level domain",
        "name": "name",
        "subdomain": "subdomain",
        "type": "type",
        "class": "class"
    "answers": "answers",
    "id": "id",
    "header_flags": [
        "header_flags",
        "header flags"
    ],
```



```
"type": "type"
"vulnerability": {
    "reference": "reference",
    "severity": "severity",
    "score": {
        "environmental": 4.8789878742268815,
        "version": "version",
        "temporal": 6.173804034172511,
        "base": 2.535258963197524
    },
    "report id": "report id",
    "scanner": {
        "vendor": "vendor"
    "description": "description",
    "id": "id",
    "classification": "classification",
    "enumeration": "enumeration",
    "category": [
        "category",
        "category"
},
"message": "message",
"tags": [
    "tags",
    "tags"
"labels": "labels",
"orchestrator": {
    "cluster": {
        "name": "name",
        "id": "id",
        "version": "version",
        "url": "url"
    },
    "resource": {
        "parent": {
            "type": "type"
        "ip": [
            "ip",
            "ip"
        "name": "name",
        "id": "id",
        "type": "type"
    "organization": "organization",
    "namespace": "namespace",
    "type": "type",
    "api version": "api version"
```





```
"@timestamp": "2000-01-23T04:56:07.000+00:00",
"EPMWinMac": {
    "COM": {
        "AppID": "AppID",
        "CLSID": "CLSID",
        "DisplayName": "DisplayName"
    "AuthorizingUser": {
        "Identifier": "Identifier",
        "DomainNetBIOSName": "DomainNetBIOSName",
        "DomainName": "DomainName",
        "Name": "Name",
        "DomainIdentifier": "DomainIdentifier",
        "CredentialSource": "CredentialSource"
    },
    "PrivilegedGroup": {
        "Access": "Access",
        "RID": "RID",
        "Name": "Name"
    },
    "AuthorizationRequest": {
        "AuthRequestURI": "AuthRequestURI",
        "ControlAuthorization": true
    },
    "SchemaVersion": "SchemaVersion",
    "Configuration": {
        "Path": "Path",
        "Message": {
            "Authorization": {
                "ResponseStatus": "ResponseStatus",
                "ChallengeCode": "ChallengeCode"
            "AuthMethods": [
                "AuthMethods",
                "AuthMethods"
            "Type": "Type",
            "Description": "Description",
            "Identifier": "Identifier",
            "Authentication": {
                "User": "User"
            "UserReason": "UserReason",
            "Name": "Name"
        "GPO": {
            "Version": "Version",
            "DisplayName": "DisplayName",
            "LinkInformation": "LinkInformation",
            "ActiveDirectoryPath": "ActiveDirectoryPath"
        "LoadAuditMode": [
```



```
"LoadAuditMode",
    "LoadAuditMode"
],
"Token": {
    "Description": "Description",
    "Identifier": "Identifier",
    "Name": "Name"
},
"ContentGroup": {
    "Description": "Description",
    "Identifier": "Identifier",
    "Name": "Name"
},
"RuleScript": {
    "Outcome": {
        "Version": "Version",
        "Output": "Output",
        "RuleAffected": true,
        "Name": "Name",
        "Result": "Result"
    "FileName": "FileName",
    "Publisher": "Publisher"
},
"RevisionNumber": "RevisionNumber",
"Workstyle": {
    "Description": "Description",
    "Identifier": "Identifier",
    "Name": "Name"
},
"Source": "Source",
"Name": "Name",
"ApplicationGroup": {
    "Description": "Description",
    "Identifier": "Identifier",
    "Name": "Name"
"Identifier": "Identifier",
"Content": {
   "Type": "Type",
"Description": "Description",
    "Identifier": "Identifier"
"SigningEnforcement": "SigningEnforcement",
"Rule": {
    "Action": "Action",
    "Identifier": "Identifier",
    "OnDemand": true
"Application": {
    "Type": "Type",
"Description": "Description",
    "Identifier": "Identifier"
```



```
},
    "Installer": {
        "Action": "Action",
        "ProductCode": "ProductCode",
        "UpgradeCode": "UpgradeCode"
    },
    "ActiveX": {
        "Version": "Version",
        "CLSID": "CLSID",
        "Codebase": "Codebase"
    },
    "GroupId": "GroupId",
    "TenantId": "TenantId",
    "StoreApp": {
        "Version": "Version",
        "Publisher": "Publisher",
        "Name": "Name"
    },
    "ServiceControl": {
        "Service": {
            "Action": "Action",
            "DisplayName": "DisplayName",
            "Name": "Name"
    },
    "TrustedApplication": {
        "Version": "Version",
        "Name": "Name"
    },
    "Event": {
        "Type": "Type",
        "Action": "Action"
    "RemotePowerShell": {
        "Command": "Command"
    "AdapterVersion": "AdapterVersion",
    "Session": {
        "Locale": "Locale",
        "PowerUser": true,
        "WindowsSessionId": "WindowsSessionId",
        "Administrator": true,
        "Identifier": "Identifier",
        "UILanguage": "UILanguage"
"data stream": {
    "namespace": "namespace",
    "type": "type",
    "dataset": "dataset"
"service": {
```



```
"node": {
        "role": "role",
        "name": "name"
    "environment": "environment",
    "address": "address",
    "origin": {
        "environment": "environment",
        "address": "address",
        "name": "name",
        "id": "id",
        "state": "state",
        "type": "type",
        "ephemeral_id": "ephemeral_id",
        "version": "version"
    },
    "name": "name",
    "id": "id",
    "state": "state",
    "type": "type",
    "ephemeral_id": "ephemeral_id",
    "version": "version",
    "target": {
        "environment": "environment",
        "address": "address",
        "name": "name",
        "id": "id",
        "state": "state",
        "type": "type",
        "ephemeral_id": "ephemeral_id",
        "version": "version"
"organization": {
    "name": "name",
    "id": "id"
"http": {
    "request": {
        "referrer": "referrer",
        "method": "method",
        "mime type": "mime type",
        "bytes": 6,
        "id": "id",
        "body": {
            "bytes": 0,
            "content": "content"
    "response": {
        "status code": 4,
        "mime type": "mime type",
        "bytes": 4,
```



```
"body": {
            "bytes": 1,
            "content": "content"
    "version": "version"
},
"tls": {
    "cipher": "cipher",
    "established": true,
    "server": {
        "not_after": "2000-01-23T04:56:07.000+00:00",
        "ja3s": "ja3s",
        "subject": "subject",
        "not before": "2000-01-23T04:56:07.000+00:00",
        "certificate": "certificate",
        "issuer": "issuer",
        "certificate chain":
            "certificate chain",
            "certificate chain"
        ],
        "hash": {
            "sha1": "sha1",
            "sha256": "sha256",
            "md5": "md5"
    },
    "curve": "curve",
    "next protocol": "next protocol",
    "client": {
        "not after": "2000-01-23T04:56:07.000+00:00",
        "server name": "server name",
        "supported ciphers": [
            "supported ciphers",
            "supported_ciphers"
        "subject": "subject",
        "not before": "2000-01-23T04:56:07.000+00:00",
        "certificate": "certificate",
        "ja3": "ja3",
        "issuer": "issuer",
        "certificate_chain": [
            "certificate chain",
            "certificate_chain"
        "hash": {
            "sha1": "sha1",
            "sha256": "sha256",
            "md5": "md5"
    "resumed": true,
    "version": "version",
```



```
"version protocol": "version protocol"
"threat": {
    "indicator": {
        "first_seen": "2000-01-23T04:56:07.000+00:00",
        "last seen": "2000-01-23T04:56:07.000+00:00",
        "confidence": "confidence",
        "ip": "ip",
        "sightings": 4,
        "description": "description",
        "type": "type",
        "url": {
            "extension": "extension",
            "original": "original",
            "scheme": "scheme",
            "top level domain": "top level domain",
            "query": "query",
            "path": "path",
            "registered_domain": "registered_domain",
            "fragment": "fragment",
            "password": "password",
            "port": 0,
            "domain": "domain",
            "subdomain": "subdomain",
            "full": "full",
            "username": "username"
        },
        "scanner stats": 2,
        "reference": "reference",
        "marking": {
            "tlp": "tlp"
        },
        "port": 9,
        "provider": "provider",
        "modified at": "2000-01-23T04:56:07.000+00:00",
        "email": {
            "address": "address"
    "feed": {
        "reference": "reference",
        "name": "name",
        "description": "description",
        "dashboard id": "dashboard id"
    "framework": "framework",
    "software": {
        "reference": "reference",
        "name": "name",
        "alias": [
            "alias",
            "alias"
        ],
```



```
"id": "id",
    "type": "type",
    "platforms": [
        "platforms",
        "platforms"
},
"technique": {
    "reference": [
        "reference",
        "reference"
    ],
    "name": [
        "name",
        "name"
    ],
    "subtechnique": {
        "reference": [
            "reference",
            "reference"
        ],
        "name": [
            "name",
            "name"
        ],
        "id": [
            "id",
            "id"
    "id": [
        "id",
        "id"
"enrichments": [
        "indicator": "indicator",
        "matched": {
            "field": "field",
            "occurred": "2000-01-23T04:56:07.000+00:00",
            "atomic": "atomic",
            "index": "index",
            "id": "id",
            "type": "type"
        "indicator": "indicator",
        "matched": {
            "field": "field",
            "occurred": "2000-01-23T04:56:07.000+00:00",
            "atomic": "atomic",
```



```
"index": "index",
                     "id": "id",
                     "type": "type"
        ],
         "group": {
            "reference": "reference",
             "name": "name",
             "alias": [
                 "alias",
                 "alias"
             ],
             "id": "id"
         },
         "tactic": {
             "reference": [
                "reference",
                 "reference"
             ],
             "name": [
                 "name",
                 "name"
             ],
             "id": [
                 "id",
                 "id"
    "transaction": {
        "id": "id"
    "span": {
        "id": "id"
}
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json



## Responses

### 200

Success EpmEcsEventResponseModel

### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails

### 500

Server Error

## **File**



# get /v2/File/download/GetYamlApiDefinitionFile

Get the API definition file in YAML format (v2FileDownloadGetYamlApiDefinitionFileGet)

# **Return type**

String

# **Example data**

Content-Type: application/json

11.1

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json



· text/json

## Responses

200

Success String

401

Unauthorized ProblemDetails

404

Not Found ProblemDetails

# **Groups**



## post /v2/Groups/AutoAssignPolicyRevision

Auto assign policy revision to the group (v2GroupsAutoAssignPolicyRevisionPost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body AutoAssignPolicyRevisionToGroupRequest (optional)

Body Parameter —

# **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"



### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

## Responses

### 200

Success **UUID** 

### 400

Bad Request ProblemDetails

### 404

Not Found ProblemDetails

### 423

Client Error ProblemDetails



# get /v2/Groups

Retrieves the list of Groups with pagination (sorting and filtering) (v2GroupsGet)

# **Query parameters**

# **Sorts (optional)**

Query Parameter —

# Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32

# Pagination.PageNumber (optional)



Query Parameter — The page number to retrieve from results, for example 1 format: int32

## Filter.Id (optional)

Query Parameter — The Id of the group(Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

### Filter.Name (optional)

Query Parameter — The name of the group

## **Filter.Description (optional)**

Query Parameter — The description of the group

## Filter.PolicyName (optional)

Query Parameter — The policy name of the group

## Filter.PolicyRevisionStatus (optional)

Query Parameter — The policy revision status of the group

# Filter.ComputerCount (optional)

Query Parameter — Number of computers in a group format: int32

# Filter.ActiveComputers.Value (optional)

**Query Parameter** — Integer value for the filter, e.g. 100 format: int32

# Filter.ActiveComputers.Operator (optional)

Query Parameter —

# Filter.Created.Dates (optional)



**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.Created.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

## Return type

GroupListItemModelPagedResponse

## **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "policyName": "policyName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "description": "description",
        "policyRevisionId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "revision": 7,
        "computerCount": 5,
        "activeComputers": 2,
        "default": true,
        "policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "name": "name",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true,
        "policyRevisionStatus": "OnLatestPolicy"
        "policyName": "policyName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
```



```
"userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
},
    "description": "description",
    "policyRevisionId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "revision": 7,
    "computerCount": 5,
    "activeComputers": 2,
    "default": true,
    "policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "name": "name",
    "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "locked": true,
    "policyRevisionStatus": "OnLatestPolicy"
}
],
    "pageSize": 6,
    "totalRecordCount": 1
}
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

### Responses

### 200

Success GroupListItemModelPagedResponse

#### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 500

Server Error



# post /v2/Groups/{id}/AssignComputersByCsv

assigns computers to the group by input of csv file (v2GroupsIdAssignComputersByCsvPost)



## Path parameters

## id (required)

Path Parameter — format: uuid

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

· multipart/form-data

# Form parameters

## csvFile (optional)

Form Parameter — format: binary

## **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

# Responses

### 201

Created **UUID** 



### 404

Not Found ProblemDetails

### 423

Client Error ProblemDetails



### post /v2/Groups/{id}/AssignComputers

assigns computers to the group (v2GroupsIdAssignComputersPost)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- application/\*+json

# **Request body**

body AssignComputersToGroupRequest (optional)

**Body Parameter** —

# Return type

**UUID** 

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the



Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

201

Created **UUID** 

404

Not Found ProblemDetails

423

Client Error ProblemDetails



# post /v2/Groups/{id}/AssignPolicyRevision

Assigns policy revision to the group (v2GroupsIdAssignPolicyRevisionPost)

# **Path parameters**

# id (required)

Path Parameter — format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body AssignPolicyRevisionToGroupRequest (optional)

Body Parameter —



UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

### 200

Success **UUID** 

### 404

Not Found ProblemDetails

### 423

Client Error ProblemDetails



# patch /v2/Groups/{id}/ClearPolicy

Clears policy from group (v2GroupsIdClearPolicyPatch)

# Path parameters

# id (required)

Path Parameter — format: uuid



UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

204

No Content **UUID** 

404

Not Found ProblemDetails

423

Client Error ProblemDetails



delete /v2/Groups/{id}

Deletes group (v2GroupsIdDelete)

# Path parameters

# id (required)

Path Parameter — format: uuid



UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

### 204

No Content **UUID** 

### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



# get /v2/Groups/{id}

Retrieves a detail of the group (v2GroupsIdGet)

# Path parameters

# id (required)



Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

### Responses

### 200

Success

### 401

Unauthorized ProblemDetails

### 404

Not Found **ProblemDetails** 



# patch /v2/Groups/{id}/MarkAsDefault

Marks group as default (v2GroupsIdMarkAsDefaultPatch)

# **Path parameters**

# id (required)

Path Parameter — format: uuid

# **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"



### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

#### 204

No Content **UUID** 

### 404

Not Found ProblemDetails

### 423

Client Error ProblemDetails



post /v2/Groups

Creates Group (v2GroupsPost)

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- text/json
- · application/\*+json

# Request body

body CreateGroupRequest (optional)

Body Parameter —

# **Return type**

UUID



## **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

### 201

Created **UUID** 

### 409

Conflict ProblemDetails



put /v2/Groups

Modifies Group (v2GroupsPut)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ModifyGroupRequest (optional)

Body Parameter —



UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

### 204

No Content **UUID** 

### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



# post /v2/Groups/UnassignComputers

Unassigns computers from the groups (v2GroupsUnassignComputersPost)

### Consumes

This API call consumes the following media types via the Content-Type request header:

- application/json
- text/json



· application/\*+json

## **Request body**

body UnassignComputersToGroupRequest (optional)

Body Parameter —

## Return type

array[UUID]

# **Example data**

Content-Type: application/json

[ "046b6c7f-0b8a-43b9-b35d-6489e6daee91", "046b6c7f-0b8a-43b9-b35d-6489e6daee91" ]

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

202

Accepted

204

No Content

404

Not Found ProblemDetails

423

Client Error ProblemDetails



## **Policies**



get /v2/Policies

Retrieve list of Policies with pagination (sorting and filtering) (v2PoliciesGet)

### **Query parameters**

## **Sorts (optional)**

Query Parameter —

## Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200, format: int32

## Pagination.PageNumber (optional)

Query Parameter — The page number to retrieve from results, for example 1 format: int32

# Filter.Name (optional)

Query Parameter — The Name of the Policy, e.g. - Policy1

# Filter.Size (optional)

Query Parameter — The Size of the Policy in Kb, e.g. 225 format: int32

# Filter.Revision (optional)

Query Parameter — The number of revisions for the Policy, e.g. 5 format: int32

# Filter.TotalAssignedRevisions (optional)

Query Parameter — The total number of Groups with the Policy assigned (any Revision), e.g. 10 format: int32



### Filter.Created.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.Created.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

## Filter.DraftUser (optional)

**Query Parameter** — The 'Locked By' user, i.e. the user that created the last draft which has locked the Policy, e.g. jbloggs@email.com

## Return type

PolicyListItemModelPagedResponse

# **Example data**

Content-Type: application/json

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "latestAssignedRevisions": 3,
        "created": "2000-01-23T04:56:07.000+00:00",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "description": "description",
        "hasOpenDraft": true,
        "periodLocked": "periodLocked",
        "revision": 2,
        "totalAssignedRevisions": 9,
        "totalRevisions": 7,
        "openDraftId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "checkedOutDate": "2000-01-23T04:56:07.000+00:00",
        "isAssignedToGroup": true,
```



```
"size": 5,
        "draftUserId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "name": "name",
        "lastModifiedUserId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "lastModifiedUser": "lastModifiedUser",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "lastModified": "2000-01-23T04:56:07.000+00:00",
        "draftUser": "draftUser",
        "locked": true,
        "lastPolicyToGroupAssignment": "2000-01-23T04:56:07.000+00:00"
    },
        "latestAssignedRevisions": 3,
        "created": "2000-01-23T04:56:07.000+00:00",
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "description": "description",
        "hasOpenDraft": true,
        "periodLocked": "periodLocked",
        "revision": 2,
        "totalAssignedRevisions": 9,
        "totalRevisions": 7,
        "openDraftId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "checkedOutDate": "2000-01-23T04:56:07.000+00:00",
        "isAssignedToGroup": true,
        "size": 5,
        "draftUserId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "name": "name",
        "lastModifiedUserId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "lastModifiedUser": "lastModifiedUser",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "lastModified": "2000-01-23T04:56:07.000+00:00",
        "draftUser": "draftUser",
        "locked": true,
        "lastPolicyToGroupAssignment": "2000-01-23T04:56:07.000+00:00"
],
"pageSize": 6,
"totalRecordCount": 1
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json



### Responses

### 200

Success PolicyListItemModelPagedResponse

### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 500

Server Error



## get /v2/Policies/{id}/AssignedGroups

Retrieves list of Groups that are assigned to Policy (v2PoliciesIdAssignedGroupsGet)

## **Path parameters**

# id (required)

Path Parameter — format: uuid

# **Return type**

array[ PolicyGroupsListItemModel]

# **Example data**

Content-Type: application/json



```
},
{
    "isDefault": true,
    "policyId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "name": "name",
    "description": "description",
    "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "policyRevisionId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
}
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

### Responses

#### 200

Success

### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails



# get /v2/Policies/{id}/Content

Downloads Latest Policy Revision (v2PoliciesIdContentGet)

# **Path parameters**

# id (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the



Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

404

Not Found ProblemDetails



## delete /v2/Policies/{id}

Deletes policy (v2PoliciesIdDelete)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

# **Query parameters**

# forceDelete (optional)

Query Parameter —

# **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the



Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

### 201

Created **UUID** 

### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



# patch /v2/Policies/{id}/DiscardDraft

Reverts and discards policy changes (v2PoliciesIdDiscardDraftPatch)

# **Path parameters**

# id (required)

Path Parameter — Policy identifier format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- text/json



## Responses

204

No Content

404

Not Found ProblemDetails

409

Conflict ProblemDetails

423

Client Error ProblemDetails



get /v2/Policies/{id}

Retrieves a detail of the policy (v2PoliciesIdGet)

# **Path parameters**

# id (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

200

Success

401

Unauthorized ProblemDetails



### 404

Not Found ProblemDetails



## put /v2/Policies/{id}

Request to update policy properties (v2PoliciesIdPut)

## **Path parameters**

## id (required)

Path Parameter — Policyld format: uuid

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ModifyPolicyRequest (optional)

Body Parameter — policy properties

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

### 204

No Content

### 404

Not Found ProblemDetails



### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



## get /v2/Policies/{id}/Revisions

Retrieves list of policy revisions (v2PoliciesIdRevisionsGet)

# **Path parameters**

## id (required)

Path Parameter — format: uuid

# Return type

array[ PolicyRevisionModel]

# **Example data**

Content-Type: application/json

```
[
    "size": 6,
    "created": "2000-01-23T04:56:07.000+00:00",
    "isAssignedGroup": true,
    "comment": "comment",
    "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "user": "user",
    "revision": 0
},
{
    "size": 6,
    "created": "2000-01-23T04:56:07.000+00:00",
    "isAssignedGroup": true,
    "comment": "comment",
    "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "user": "user",
```



```
"revision": 0
}
```

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

### 200

Success

### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails



# post /v2/Policies/{id}/Upload

Upload New Policy Revision (v2PoliciesIdUploadPost)

# **Path parameters**

# id (required)

Path Parameter — Policy Id format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

· multipart/form-data



## Form parameters

# PolicyFile (optional)

Form Parameter — format: binary

# **AutoAssignToGroup (optional)**

Form Parameter —

## **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

# Responses

### 201

Created UUID

### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails



### 409

Conflict ProblemDetails

### 415

Client Error ProblemDetails

### 423

Client Error ProblemDetails



# get /v2/Policies/PolicyRevision/{policyRevisionId}/Content

Downloads Policy Revision (v2PoliciesPolicyRevisionPolicyRevisionIdContentGet)

## Path parameters

## policyRevisionId (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

## Responses

#### 404

Not Found ProblemDetails



post /v2/Policies

Creates new policy with provided file (v2PoliciesPost)

### Consumes

This API call consumes the following media types via the Content-Type request header:



· multipart/form-data

## Form parameters

# Name (optional)

Form Parameter —

# **Description (optional)**

Form Parameter —

# PolicyFile (optional)

Form Parameter — format: binary

# Return type

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

201

Created **UUID** 



### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

### 409

Conflict ProblemDetails

### 415

Client Error ProblemDetails

## **Roles**



## get /v2/Roles

Retrieve list of Roles (v2RolesGet)

## **Return type**

array[ RoleListItemModel]

# **Example data**



This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

## Responses

### 200

Success

#### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### **500**

Server Error





# get /v2/Roles/{id}

Retrieve role details (v2RolesIdGet)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

## **Return type**

RoleModel

## **Example data**

Content-Type: application/json

### **Produces**

- text/plain
- · application/json
- · text/json



#### 200

Success RoleModel

#### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

#### 500

Server Error

# **ScimResourceTypes**



get /scim/v2/ResourceTypes

gets types of resources available ( scimV2ResourceTypesGet)

# **Query parameters**

# api-version (required)

Query Parameter —

# Return type

ScimResourceResponseScimListResponse

# **Example data**

```
{
  "totalResults": 0,
  "startIndex": 6,
  "itemsPerPage": 1,
```



```
"schemas": [
   "schemas",
   "schemas"
"Resources": [
   {
        "schema": "schema",
        "endpoint": "endpoint",
        "meta": {
            "resourceType": "resourceType"
        "schemas": [
            "schemas",
            "schemas"
        "name": "name",
        "description": "description"
        "schema": "schema",
        "endpoint": "endpoint",
        "meta": {
            "resourceType": "resourceType"
        "schemas": [
            "schemas",
            "schemas"
        "name": "name",
        "description": "description"
```

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

#### 200

Success ScimResourceResponseScimListResponse





## get /scim/v2/ResourceTypes/User

gets types of resources available ( scimV2ResourceTypesUserGet)

## **Query parameters**

## api-version (required)

Query Parameter —

## Return type

ScimResourceResponse

## **Example data**

Content-Type: application/json

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- · application/json
- · text/json

## Responses

#### 200

Success ScimResourceResponse



## **ScimSchemas**



## get /scim/v2/Schemas

Get the Schema supported by the SCIM Api (scimV2SchemasGet)

## **Query parameters**

# api-version (required)

Query Parameter —

## Return type

ScimSchemaResponseScimListResponse

# **Example data**

```
"totalResults": 0,
"startIndex": 6,
"itemsPerPage": 1,
"schemas": [
    "schemas",
    "schemas"
],
"Resources": [
        "meta": {
            "resourceType": "resourceType"
        "schemas": [
            "schemas",
            "schemas"
        "name": "name",
        "description": "description",
        "attributes": [
                "uniqueness": "uniqueness",
                "name": "name",
```



```
"description": "description",
    "mutability": "mutability",
    "type": "type",
    "caseExact": true,
    "multiValued": true,
    "returned": "returned",
   "required": true,
    "subAttributes": [
            "uniqueness": "uniqueness",
            "name": "name",
            "description": "description",
            "canonicalValues": [
                "canonicalValues",
                "canonicalValues"
            ],
            "mutability": "mutability",
            "type": "type",
            "caseExact": true,
            "multiValued": true,
            "returned": "returned",
            "required": true
        },
            "uniqueness": "uniqueness",
            "name": "name",
            "description": "description",
            "canonicalValues": [
                "canonicalValues",
                "canonicalValues"
            "mutability": "mutability",
            "type": "type",
            "caseExact": true,
            "multiValued": true,
            "returned": "returned",
            "required": true
   ]
},
   "uniqueness": "uniqueness",
   "name": "name",
   "description": "description",
   "mutability": "mutability",
   "type": "type",
   "caseExact": true,
   "multiValued": true,
   "returned": "returned",
   "required": true,
   "subAttributes": [
            "uniqueness": "uniqueness",
```

23.1 API GUIDE - VERSION 2



```
"name": "name",
                     "description": "description",
                     "canonicalValues": [
                         "canonicalValues",
                         "canonicalValues"
                     ],
                     "mutability": "mutability",
                     "type": "type",
                     "caseExact": true,
                     "multiValued": true,
                     "returned": "returned",
                     "required": true
                },
                     "uniqueness": "uniqueness",
                     "name": "name",
                     "description": "description",
                     "canonicalValues": [
                         "canonicalValues",
                         "canonicalValues"
                    ],
                     "mutability": "mutability",
                     "type": "type",
                     "caseExact": true,
                     "multiValued": true,
                     "returned": "returned",
                     "required": true
            ]
        }
    "id": "id"
},
    "meta": {
        "resourceType": "resourceType"
    "schemas": [
        "schemas",
        "schemas"
    "name": "name",
    "description": "description",
    "attributes": [
            "uniqueness": "uniqueness",
            "name": "name",
            "description": "description",
            "mutability": "mutability",
            "type": "type",
            "caseExact": true,
            "multiValued": true,
            "returned": "returned",
```

23.1 API GUIDE - VERSION 2



```
"required": true,
    "subAttributes": [
            "uniqueness": "uniqueness",
            "name": "name",
            "description": "description",
            "canonicalValues": [
                "canonicalValues",
                "canonicalValues"
            ],
            "mutability": "mutability",
            "type": "type",
            "caseExact": true,
            "multiValued": true,
            "returned": "returned",
            "required": true
        },
            "uniqueness": "uniqueness",
            "name": "name",
            "description": "description",
            "canonicalValues": [
                "canonicalValues",
                "canonicalValues"
            ],
            "mutability": "mutability",
            "type": "type",
            "caseExact": true,
            "multiValued": true,
            "returned": "returned",
            "required": true
    ]
},
    "uniqueness": "uniqueness",
    "name": "name",
    "description": "description",
    "mutability": "mutability",
    "type": "type",
    "caseExact": true,
    "multiValued": true,
    "returned": "returned",
    "required": true,
    "subAttributes": [
            "uniqueness": "uniqueness",
            "name": "name",
"description": "description",
            "canonicalValues": [
                "canonicalValues",
                "canonicalValues"
            ],
```



```
"mutability": "mutability",
                         "type": "type",
                         "caseExact": true,
                         "multiValued": true,
                         "returned": "returned",
                         "required": true
                         "uniqueness": "uniqueness",
                         "name": "name",
                         "description": "description",
                         "canonicalValues": [
                             "canonicalValues",
                             "canonicalValues"
                         "mutability": "mutability",
                         "type": "type",
                         "caseExact": true,
                         "multiValued": true,
                         "returned": "returned",
                         "required": true
                ]
            }
        "id": "id"
]
```

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

### 200

Success ScimSchemaResponseScimListResponse

# ScimServiceProviderConfig





# get /scim/v2/ServiceProviderConfig

gets the Json structure available (scimV2ServiceProviderConfigGet)

## **Query parameters**

## api-version (required)

Query Parameter —

## Return type

ScimServiceProviderConfigResponse

## **Example data**

Content-Type: application/json

```
"patch": {
   "supported": true
"authenticationSchemes": {
    "name": "name",
    "description": "description",
    "type": "type",
    "primary": true
},
"meta": {
    "resourceType": "resourceType"
},
"schemas": [
    "schemas",
    "schemas"
],
"bulk": {
    "maxPayloadSize": 6,
    "maxOperations": 0,
    "supported": true
```

### **Produces**



- · text/plain
- · application/json
- text/json

200

Success ScimServiceProviderConfigResponse

## **ScimUsers**



get /scim/v2/Users

(scimV2UsersGet)

# **Query parameters**

# filter (optional)

Query Parameter —

# startIndex (optional)

Query Parameter — format: int32

## count (optional)

Query Parameter — format: int32

# api-version (required)

Query Parameter —

# **Return type**

ScimUserModelScimListResponse



# **Example data**

```
"totalResults": 0,
"startIndex": 6,
"itemsPerPage": 1,
"schemas": [
    "schemas",
    "schemas"
"Resources": [
    {
        "entitlements": [
           null,
            null
        "displayName": "displayName",
        "timezone": "timezone",
        "roles": [
                "value": "value",
                "primary": true
                "value": "value",
                "primary": true
        "externalId": "externalId",
        "groups": [
            "",
            11 11
        "active": true,
        "userName": "userName",
        "locale": "locale",
        "emails": [
                "type": "type",
                "value": "value",
                "primary": true
            },
                "type": "type",
                "value": "value",
                "primary": true
        "password": "password",
        "dateTimeFormat": "dateTimeFormat",
        "meta": {
```



```
"created": "2000-01-23T04:56:07.000+00:00",
        "resourceType": "resourceType"
    },
    "schemas": [
        "schemas",
        "schemas"
    ],
    "name": {
        "givenName": "givenName",
        "familyName": "familyName",
        "middleName": "middleName"
    "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
},
    "entitlements": [
       null,
        null
    "displayName": "displayName",
    "timezone": "timezone",
    "roles": [
        {
            "value": "value",
            "primary": true
        },
            "value": "value",
            "primary": true
    "externalId": "externalId",
    "groups": [
       "",
        11 11
    "active": true,
    "userName": "userName",
    "locale": "locale",
    "emails": [
            "type": "type",
            "value": "value",
            "primary": true
        },
            "type": "type",
            "value": "value",
            "primary": true
    "password": "password",
    "dateTimeFormat": "dateTimeFormat",
```



This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

#### 200

Success ScimUserModelScimListResponse



## post /scim/v2/Users

(scimV2UsersPost)

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- text/json
- · application/\*+json



## Request body

body ScimUserModel (optional)

Body Parameter —

## **Query parameters**

## api-version (required)

Query Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

## Responses

#### 201

Created

#### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails



# get /scim/v2/Users/{userID}

(scimV2UsersUserIDGet)

# Path parameters

# userID (required)



Path Parameter — format: uuid

## **Query parameters**

## api-version (required)

Query Parameter —

## Return type

ScimUserModel

## **Example data**

```
"entitlements": [
   null,
    null
"displayName": "displayName",
"timezone": "timezone",
"roles": [
        "value": "value",
        "primary": true
        "value": "value",
        "primary": true
"externalId": "externalId",
"groups": [
    "",
"active": true,
"userName": "userName",
"locale": "locale",
"emails": [
        "type": "type",
        "value": "value",
        "primary": true
```



```
"type": "type",
        "value": "value",
        "primary": true
"password": "password",
"dateTimeFormat": "dateTimeFormat",
"meta": {
   "created": "2000-01-23T04:56:07.000+00:00",
   "resourceType": "resourceType"
},
"schemas": [
   "schemas",
   "schemas"
],
"name": {
   "givenName": "givenName",
   "familyName": "familyName",
   "middleName": "middleName"
"id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
```

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

#### 200

Success ScimUserModel

### 404

Not Found ProblemDetails



# patch /scim/v2/Users/{userID}

Patch operation (scimV2UsersUserIDPatch)



## Path parameters

## userID (required)

Path Parameter — format: uuid

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body ScimUserPatchRequest (optional)

Body Parameter —

## **Query parameters**

## api-version (required)

Query Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

#### 200

Success

#### 404

Not Found ProblemDetails



### 423

Client Error ProblemDetails



## put /scim/v2/Users/{userID}

Modify a user (scimV2UsersUserIDPut)

## **Path parameters**

## userID (required)

Path Parameter — format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

## **Request body**

body ScimUserModel (optional)

Body Parameter —

# **Query parameters**

## api-version (required)

Query Parameter —

### **Produces**

- · text/plain
- · application/json
- · text/json



200

Success

404

Not Found ProblemDetails

409

Conflict ProblemDetails

423

Client Error ProblemDetails

## **Tasks**



get /v2/Tasks/{id}

Retrieves a detail of the Task (v2TasksldGet)

# **Path parameters**

# id (required)

Path Parameter — format: uuid

# **Return type**

TaskDetailModel

# **Example data**

```
{
   "initiated": "2000-01-23T04:56:07.000+00:00",
   "messageParameters": [
      {
```



```
"key": "messageParameters"
},
{
        "key": "messageParameters"
}
],
"stateName": "stateName",
"tenantId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"name": "name",
"id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"state": 0,
"completed": "2000-01-23T04:56:07.000+00:00",
"completedWithErrors": true,
"userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"user": "user"
}
```

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- · text/json

# Responses

### 200

Success TaskDetailModel

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

## **Users**



get /v2/Users



Retrieves the list of Users with pagination (sorting and filtering) (v2UsersGet)

## **Query parameters**

## **Sorts (optional)**

Query Parameter —

## Pagination.PageSize (optional)

Query Parameter — The number of records per page, for example 1. Shouldn't exceed 200. format: int32

# Pagination.PageNumber (optional)

Query Parameter — The page number to retrieve from results, for example 1 format: int32

## Filter.EmailAddress (optional)

**Query Parameter** — Email

# Filter.Roleld (optional)

Query Parameter — Role identifier format: uuid

# Filter.LastSignedIn.Dates (optional)

**Query Parameter** — Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# Filter.LastSignedIn.SelectionMode (optional)

Query Parameter — The selection mode of date criteria e.g single, multiple, range

# Filter.Disabled (optional)

Query Parameter — Is user disabled



## Filter.Language (optional)

Query Parameter — Language

## Return type

UserListItemModelPagedResponse

# **Example data**

```
"pageCount": 5,
"pageNumber": 0,
"data": [
        "accountName": "accountName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "roles": [
                "resourceId": "resourceId",
                "name": "name",
                "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                "resourceType": "resourceType"
                "resourceId": "resourceId",
                "name": "name",
                "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                "resourceType": "resourceType"
        ],
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "language": "language",
        "emailAddress": "emailAddress",
        "olsonTimeZoneId": "olsonTimeZoneId",
        "roleName": "roleName",
        "disabled": true,
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true,
        "dateTimeDisplayFormat": "dateTimeDisplayFormat",
        "lastSignedIn": "2000-01-23T04:56:07.000+00:00"
```



```
},
        "accountName": "accountName",
        "created": "2000-01-23T04:56:07.000+00:00",
        "roles": [
                "resourceId": "resourceId",
                "name": "name",
                "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                "resourceType": "resourceType"
            },
                "resourceId": "resourceId",
                "name": "name",
                "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
                "resourceType": "resourceType"
        ],
        "errorInfo": {
            "userAccountName": "userAccountName",
            "parentTaskName": "parentTaskName",
            "initiated": "2000-01-23T04:56:07.000+00:00",
            "errorCode": 0,
            "userId": "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
        "language": "language",
        "emailAddress": "emailAddress",
        "olsonTimeZoneId": "olsonTimeZoneId",
        "roleName": "roleName",
        "disabled": true,
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "locked": true,
        "dateTimeDisplayFormat": "dateTimeDisplayFormat",
        "lastSignedIn": "2000-01-23T04:56:07.000+00:00"
],
"pageSize": 6,
"totalRecordCount": 1
```

- · text/plain
- · application/json
- text/json



#### 200

Success UserListItemModelPagedResponse

#### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

#### 500

Server Error



## post /v2/Users/{id}/AssignRoles

Assign Roles to User (v2UsersIdAssignRolesPost)

## Path parameters

# id (required)

Path Parameter — UserId format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

## **Request body**

body AssignUserToRolesRequest (optional)

**Body Parameter** — Role assignment request containing Role identifier

### **Produces**



- · text/plain
- · application/json
- text/json

#### 204

No Content

### 404

Not Found ProblemDetails

#### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



## patch /v2/Users/{id}/Disable

Disables User (v2UsersIdDisablePatch)

# Path parameters

## id (required)

Path Parameter — UserId format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

#### 204

No Content



### 404

Not Found ProblemDetails

#### 423

Client Error ProblemDetails



### patch /v2/Users/{id}/Enable

Enables User (v2UsersIdEnablePatch)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- text/plain
- application/json
- · text/json

## Responses

### 204

No Content

#### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails

#### 423

Client Error ProblemDetails





# get /v2/Users/{id}

Retrieves a detail of the User (v2UsersIdGet)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

## Return type

UserDetailModel

## **Example data**

```
"emailAddress": "emailAddress",
"accountName": "accountName",
"created": "2000-01-23T04:56:07.000+00:00",
"olsonTimeZoneId": "olsonTimeZoneId",
"roles": [
        "resourceId": "resourceId",
        "name": "name",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "allowPermissions": [
                "resource": "resource",
                "action": "action"
            },
                "resource": "resource",
                "action": "action"
        "denyPermissions": [
            null,
            null
        "resourceType": "resourceType"
        "resourceId": "resourceId",
```



```
"name": "name",
        "id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
        "allowPermissions": [
                "resource": "resource",
                "action": "action"
            },
                "resource": "resource",
                "action": "action"
        ],
        "denyPermissions": [
           null,
           null
        "resourceType": "resourceType"
],
"isFirstSignIn": true,
"disabled": true,
"language": "language",
"allowInvites": true,
"id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"dateTimeDisplayFormat": "dateTimeDisplayFormat",
"lastSignedIn": "2000-01-23T04:56:07.000+00:00"
```

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

## Responses

### 200

Success UserDetailModel

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails



### 404

Not Found ProblemDetails



## put /v2/Users/{id}/ModifyUserPreferences

Modifies User Preferences (v2UsersIdModifyUserPreferencesPut)

## **Path parameters**

## id (required)

Path Parameter — format: uuid

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

## **Request body**

body ModifyUserPreferencesRequest (optional)

Body Parameter —

### **Produces**

This API call produces the following media types according to the Accept request header; the media type will be conveyed by the Content-Type response header.

- · text/plain
- · application/json
- text/json

# Responses

### 204

No Content

### 400

Bad Request ProblemDetails



### 401

Unauthorized ProblemDetails

#### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails

#### 423

Client Error ProblemDetails



# put /v2/Users/{id}

Modifies User (v2UsersIdPut)

## **Path parameters**

# id (required)

Path Parameter — format: uuid

### Consumes

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- application/\*+json

# **Request body**

body ModifyUserRequest (optional)

Body Parameter —

### **Produces**

- · text/plain
- · application/json



· text/json

## Responses

### 204

No Content

#### 400

Bad Request ProblemDetails

#### 401

Unauthorized ProblemDetails

### 404

Not Found ProblemDetails

### 409

Conflict ProblemDetails

### 423

Client Error ProblemDetails



# patch /v2/Users/{id}/ResendInvite

Resends invitation email to User (v2UsersIdResendInvitePatch)

## **Path parameters**

# id (required)

Path Parameter — format: uuid

### **Produces**

- · text/plain
- · application/json
- · text/json



204

No Content

401

Unauthorized ProblemDetails

404

Not Found ProblemDetails



post /v2/Users

Creates User (v2UsersPost)

### **Consumes**

This API call consumes the following media types via the Content-Type request header:

- · application/json
- · text/json
- · application/\*+json

# **Request body**

body V2CreateUserRequest (optional)

Body Parameter —

# **Return type**

UUID

# **Example data**

Content-Type: application/json

"046b6c7f-0b8a-43b9-b35d-6489e6daee91"

### **Produces**



- text/plain
- · application/json
- text/json

### 201

Created **UUID** 

### 400

Bad Request ProblemDetails

### 401

Unauthorized ProblemDetails

### 409

Conflict ProblemDetails



### **Models**

[ Jump to Methods ]

#### **Table of Contents**

- 1. AcceptedDomainDetailModel
- 2. AcceptedDomainListItemModel
- 3. Activex
- 4. ActivityAuditDetailModel
- 5. ActivityAuditDetailModelPagedResponse
- 6. ActivityAuditListItemModel
- 7. ActivityAuditListItemModelPagedResponse
- 8. ActivityAuditRoleNameModel
- 9. ActivtyAuditRoleResourceModel
- 10. Agent
- 11. AgentBuild
- 12. AgentHostType
- 13. ApiClientDataAuditingDetailModel
- 14. Application
- 15. Applicationgroup
- 16. **As**
- 17. AsOrganization
- 18. AssignComputersToGroupRequest
- 19. AssignPolicyRevisionToGroupRequest
- 20. AssignUserToRolesRequest
- 21. Attribute
- 22. Authentication
- 23. Authorization
- 24. AuthorizationRequestAuditDetailModel
- $25. \quad \textbf{Authorization} \textbf{RequestAuditDetailModelPagedResponse}$
- 26. AuthorizationRequestAuditListItemModel
- 27. AuthorizationRequestAuditListItemModelPagedResponse
- 28. Authorizationrequest
- 29. Authorizinguser
- 30. AutoAssignPolicyRevisionToGroupRequest
- 31. Bundle
- 32. CertificateInformationModel
- 33. ChangedBy
- 34. Client



- 35. ClientNat
- 36. Cloud
- 37. CloudAccount
- 38. Cloudinstance
- 39. CloudMachine
- 40. CloudOrigin
- 41. CloudProject
- 42. CloudService
- 43. CloudTarget
- 44. CodeSignature
- 45. **Com**
- 46. ComputerDataAuditingDetailModel
- 47. ComputerDetailModel
- 48. ComputerFilterModel
- 49. ComputerListItemModel
- ${\bf 50.} \quad \underline{\textbf{ComputerListItemModelPagedResponse}}$
- 51. ComputerLogModel
- 52. ComputerRenewCertificateRequest
- 53. ComputerRetrieveLogsRequest
- 54. ComputerRetrieveStatusInfoRequest
- 55. ComputersAuthoriseRequest
- 56. ComputersDeactivateRequest
- 57. ComputersRejectRequest
- 58. ComputersRemoveRequest
- 59. Configuration
- 60. Container
- 61. ContainerCpu
- 62. ContainerDisk
- 63. ContainerDiskRead
- 64. ContainerDiskWrite
- 65. ContainerImage
- 66. ContainerImageHash
- 67. ContainerMemory
- 68. ContainerNetwork
- 69. ContainerNetworkEgress
- 70. ContainerNetworkIngress
- 71. Content
- 72. Contentgroup
- 73. CountRange
- 74. CreateAcceptedDomainRequest



- 75. CreateGroupRequest
- 76. DataStream
- 77. DateFilterModel
- 78. DateSelectionMode
- 79. Destination
- 80. DestinationNat
- 81. DII
- 82. **Dns**
- 83. **DnsQuestion**
- 84. Ecs
- 85. Elf
- 86. ElfHeader
- 87. ElfSections
- 88. ElfSegments
- 89. Email
- 90. EmailAttachments
- 91. EmailAttachmentsFile
- 92. EmailBcc
- 93. EmailCc
- 94. EmailFrom
- 95. EmailReplyTo
- 96. EmailSender
- 97. EmailTo
- 98. EndpointInformationModel
- 99. EpmEcsEvent
- 100. EpmEcsEventResponseModel
- 101. EpmEcsEventSpan
- 102. EpmEcsEventTrace
- 103. EpmEcsEventTransaction
- 104. Epmwinmac
- 105. **Error**
- 106. **Event**
- 107. **Faas**
- 108. FaasTrigger
- 109. File
- 110. **Geo**
- 111. GeoPoint
- 112. **Gpo**
- 113. **Group**
- 114. GroupDataAuditingDetailModel



- 115. GroupListItemModel
- 116. GroupListItemModelPagedResponse
- 117. Hash
- 118. Host
- 119. HostBoot
- 120. HostCpu
- 121. HostDisk
- 122. HostDiskRead
- 123. HostDiskWrite
- 124. HostNetwork
- 125. HostNetworkEgress
- 126. HostNetworkIngress
- 127. Http
- 128. HttpRequest
- 129. HttpRequestBody
- 130. HttpResponse
- 131. HttpResponseBody
- 132. InstallationKeyDataAuditingDetailModel
- 133. Installer
- 134. ListItemErrorInfoModel
- 135. Log
- 136. LogFile
- 137. LogOrigin
- 138. LogOriginFile
- 139. Message
- 140. ModifyAcceptedDomainRequest
- 141. ModifyGroupRequest
- 142. ModifyPolicyRequest
- 143. ModifyUserPreferencesRequest
- 144. ModifyUserRequest
- 145. Network
- 146. OS
- 147. Observer
- 148. OperationValue
- 149. Operator
- 150. Orchestrator
- 151. OrchestratorCluster
- 152. OrchestratorResource
- 153. OrchestratorResourceParent
- 154. Organization



- 155. Os
- 156. Owner
- 157. Package
- 158. Po
- 159. PolicyDataAudtingDetailModel
- 160. PolicyGroupsListItemModel
- 161. PolicyListItemModel
- 162. PolicyListItemModelPagedResponse
- 163. PolicyRevisionDataAuditingDetailModel
- 164. PolicyRevisionModel
- 165. PolicyRevisionState
- 166. Privilegedgroup
- 167. ProblemDetails
- 168. Process
- 169. ProcessEntryLeader
- 170. ProcessEntryMeta
- 171. ProcessGroupLeader
- 172. ProcessParent
- 173. ProcessPrevious
- 174. ProcessSessionLeader
- 175. ProcessThread
- 176. Registry
- 177. RegistryData
- 178. Related
- 179. Remotepowershell
- 180. RoleElement
- 181. RoleItemModel
- 182. RoleListItemModel
- 183. RoleModel
- 184. RolePermissionModel
- 185. RoleResourceModel
- 186. Rule
- 187. Rulescript
- 188. RulescriptOutcome
- 189. SCIMEmail
- 190. SCIMUserName
- 191. ScimAuthenticationSchemes
- 192. ScimBulk
- 193. ScimOperation
- 194. ScimResourceMeta



- 195. ScimResourceResponse
- 196. ScimResourceResponseScimListResponse
- 197. ScimSchemaResponse
- 198. ScimSchemaResponseScimListResponse
- 199. ScimServiceProviderConfigResponse
- 200. ScimSupported
- 201. ScimUserMetaModel
- 202. ScimUserModel
- 203. ScimUserModelScimListResponse
- 204. ScimUserPatchRequest
- 205. Server
- 206. ServerNat
- 207. Service
- 208. ServiceNode
- 209. ServiceOrigin
- 210. ServiceTarget
- 211. Servicecontrol
- 212. ServicecontrolService
- 213. Session
- 214. SettingDataAuditingDetailModel
- 215. SortDirection
- 216. SortModel
- 217. Source
- 218. SourceNat
- 219. Storeapp
- 220. SubAttribute
- 221. TaskDetailModel
- 222. Threat
- 223. ThreatEnrichments
- 224. ThreatEnrichmentsMatched
- 225. ThreatFeed
- 226. ThreatGroup
- 227. ThreatIndicator
- 228. ThreatIndicatorEmail
- 229. ThreatIndicatorMarking
- 230. ThreatSoftware
- 231. ThreatTactic
- 232. ThreatTechnique
- 233. ThreatTechniqueSubtechnique
- 234. <u>Tls</u>



- 235. TIsClient
- 236. TIsClientHash
- 237. TIsServer
- 238. TIsServerHash
- 239. **Token**
- 240. Trustedapplication
- 241. UnassignComputersToGroupRequest
- 242. Url
- 243. User
- 244. UserAgent
- 245. UserAgentDevice
- 246. UserChanges
- 247. UserDataAuditing
- 248. UserDetailModel
- 249. UserEffective
- 250. UserListItemModel
- 251. UserListItemModelPagedResponse
- 252. UserRoleResourceItemModel
- 253. UserTarget
- 254. V2CreateUserRequest
- 255. Vlan
- 256. Vulnerability
- 257. VulnerabilityScanner
- 258. VulnerabilityScore
- 259. Workstyle
- 260. **X509**
- 261. X509Issuer
- 262. X509Subject
- 263. \_event
- 264. \_rule
- 265. id\_AssignComputersByCsv\_body
- 266. id\_Upload\_body
- 267. v2 Policies body



### AcceptedDomainDetailModel

### id (optional)



**UUID** Accepted Domain Id format: uuid

#### domain (optional)

String Accepted Domain name

#### created (optional)

Date Created date format: date-time



#### AcceptedDomainListItemModel

Model of Accepted Domain list item

#### id (optional)

UUID The Id (Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

### locked (optional)

**Boolean** 

## errorInfo (optional)

ListItemErrorInfoModel

## domain (optional)

String Accepted Domain name

#### created (optional)

Date Created date format: date-time





Activex

#### **Codebase (optional)**

String

**CLSID** (optional)

**String** 

**Version (optional)** 

String



### ActivityAuditDetailModel

Activity audit detail model

## id (optional)

Long Id format: int64

# details (optional)

String Details

### userId (optional)

**UUID** User id format: uuid

### user (optional)

String user name



entity	(0	ntic	nal)
Cittity	10	Ptit	, iiui

String entity

#### auditType (optional)

String audit type

### created (optional)

Date created format: date-time

#### changedBy (optional)

ChangedBy

#### apiClientDataAuditing (optional)

ApiClientDataAuditingDetailModel

# computerDataAuditing (optional)

ComputerDataAuditingDetailModel

# groupDataAuditing (optional)

GroupDataAuditingDetailModel

## installationKeyDataAuditing (optional)

In stall at ion Key Data Auditing Detail Model

# policyDataAuditing (optional)

PolicyDataAudtingDetailModel



### policyRevisionDataAuditing (optional)

PolicyRevisionDataAuditingDetailModel

#### settingsDataAuditing (optional)

SettingDataAuditingDetailModel

### userDataAuditing (optional)

**UserDataAuditing** 



### ActivityAuditDetailModelPagedResponse

# pageNumber (optional)

Integer format: int32

## pageSize (optional)

Integer format: int32

## totalRecordCount (optional)

Integer format: int32

## pageCount (optional)

Integer format: int32

#### data (optional)

array[ActivityAuditDetailModel]





# ActivityAuditListItemModel

Model of Activity Audit list item

#### id (optional)

Long Activity Audit identifier format: int64

#### locked (optional)

**Boolean** 

#### errorInfo (optional)

ListItemErrorInfoModel

#### details (optional)

String Activity Audit Details

## user (optional)

String Initiated User email or API Client identifier

#### created (optional)

Date Created date format: date-time

#### entity (optional)

String Name of Activity Audit entity

# auditType (optional)

String Audit Type Name



#### changedBy (optional)

ChangedBy



### ActivityAuditListItemModelPagedResponse

#### pageNumber (optional)

Integer format: int32

### pageSize (optional)

Integer format: int32

#### totalRecordCount (optional)

Integer format: int32

## pageCount (optional)

Integer format: int32

### data (optional)

array[ActivityAuditListItemModel]



## ActivityAuditRoleNameModel

activity audit role name mapping model

### roleld (optional)



**UUID** role id format: uuid

#### roleName (optional)

String role name



### ActivtyAuditRoleResourceModel

Role Resource Model for activity audits

# resourceType (optional)

String Type of resource

#### resourceld (optional)

UUID Id of the resource format: uuid

### resourceName (optional)

String Resource name

## newRoles (optional)

array[ActivityAuditRoleNameModel] List of new roles

# oldRoles (optional)

array[ActivityAuditRoleNameModel] List of oldRoles





**String** 

build (optional)

AgentBuild

name (optional)

String

type (optional)

String

id (optional)

String

ephemeral\_id (optional)

String



AgentBuild

original (optional)





# AgentHostType

#### enum

#### String

- Undefined
- MicrosoftWindows
- AppleMacOS
- Linux



# ApiClientDataAuditingDetailModel

newName (optional)

**String** 

oldName (optional)

String

newDescription (optional)

String

oldDescription (optional)

**String** 

secretUpdated (optional)

Boolean



#### deleted (optional)

**Boolean** 



Application

#### **Type (optional)**

String

#### **Description (optional)**

String

### **Identifier (optional)**

String



Applicationgroup

#### Name (optional)

String

### **Description (optional)**

**String** 

# **Identifier (optional)**



String





#### number (optional)

Long format: int64

#### organization (optional)

**AsOrganization** 



**AsOrganization** 

### name (optional)

String



#### AssignComputersToGroupRequest

#### computerIds (optional)

array[UUID] computer ids which will be assigned to the group format: uuid

# excludedComputerIds (optional)

array[UUID] computer ids which will not be assigned to group format: uuid

# filter (optional)



ComputerFilterModel

#### allComputers (optional)

Boolean assigns all computers to the group



### AssignPolicyRevisionToGroupRequest

#### policyRevisionId (optional)

**UUID** format: uuid



#### AssignUserToRolesRequest

Assign user to roles request

# roleResource (optional)

array[RoleResourceModel] list of user role resources



# Attribute

attributes of schemas

# name (optional)

String name of attribute

# description (optional)

String description of attribute



### type (optional)

String type of attribute

#### caseExact (optional)

Boolean Flag for whether or not the attribute's casing should be exact

#### multiValued (optional)

Boolean Flag for whether or not the attribute has multi values

#### mutability (optional)

String Mutability of the attribute

#### required (optional)

Boolean Flag for whether or not the attribute is required

#### returned (optional)

String how the attribute is returned

# uniqueness (optional)

String Is the value unique

### subAttributes (optional)

array[SubAttribute] List of subattributes





Authentication

**User (optional)** 

**String** 



Authorization

**ChallengeCode (optional)** 

**String** 

ResponseStatus (optional)

String



AuthorizationRequestAuditDetailModel

id (optional)

Long format: int64

ticketId (optional)

String

productName (optional)



computerName (optional) String reason (optional) String decisionPerformedByUser (optional) String timeOfRequest (optional) Date format: date-time decisionTime (optional) Date format: date-time decision (optional) String startTime (optional) Date format: date-time	user (optional)
reason (optional) string decisionPerformedByUser (optional) string timeOfRequest (optional) Date format: date-time decisionTime (optional) Date format: date-time decision (optional) String startTime (optional) Date format: date-time	String
reason (optional) String  decisionPerformedByUser (optional) String  timeOfRequest (optional) Date format: date-time  decisionTime (optional) Date format: date-time  decision (optional) String  startTime (optional) Date format: date-time	computerName (optional)
decisionPerformedByUser (optional) String  timeOfRequest (optional) Date format: date-time  decisionTime (optional)  Date format: date-time  decision (optional) String  startTime (optional) Date format: date-time	String
decisionPerformedByUser (optional) String  timeOfRequest (optional) Date format: date-time  decisionTime (optional) Date format: date-time  decision (optional) String  startTime (optional) Date format: date-time	reason (optional)
timeOfRequest (optional)  Date format: date-time  decisionTime (optional)  Date format: date-time  decision (optional)  String  startTime (optional)  Date format: date-time	String
timeOfRequest (optional)  Date format: date-time  decisionTime (optional)  Date format: date-time  decision (optional)  String  startTime (optional)  Date format: date-time	decisionPerformedByUser (optional)
Date format: date-time  decisionTime (optional)  Date format: date-time  decision (optional)  String  startTime (optional)  Date format: date-time	String
decisionTime (optional)  Date format: date-time  decision (optional)  String  startTime (optional)  Date format: date-time	timeOfRequest (optional)
Date format: date-time  decision (optional)  String  startTime (optional)  Date format: date-time	Date format: date-time
decision (optional) String startTime (optional) Date format: date-time	decisionTime (optional)
String  startTime (optional)  Date format: date-time	Date format: date-time
startTime (optional)  Date format: date-time	decision (optional)
Date format: date-time	String
	startTime (optional)
densition (antique)	Date format: date-time
duration (optional)	duration (optional)
String	String





# AuthorizationRequestAuditDetailModelPagedResponse

#### pageNumber (optional)

Integer format: int32

### pageSize (optional)

Integer format: int32

#### totalRecordCount (optional)

Integer format: int32

#### pageCount (optional)

Integer format: int32

#### data (optional)

array[AuthorizationRequestAuditDetailModel]



# AuthorizationRequestAuditListItemModel

## id (optional)

Long format: int64

## ticketId (optional)



productName (optional)
String
user (optional)
String
computerName (optional)
String
reason (optional)
String
decisionPerformedByUser (optional)
String
timeOfRequest (optional)
Date format: date-time
decisionTime (optional)
Date format: date-time
decision (optional)
String
duration (optional)
String



#### startTime (optional)

Date format: date-time



AuthorizationRequestAuditListItemModelPagedResponse

### pageNumber (optional)

Integer format: int32

#### pageSize (optional)

Integer format: int32

#### totalRecordCount (optional)

Integer format: int32

## pageCount (optional)

Integer format: int32

### data (optional)

array[AuthorizationRequestAuditListItemModel]



Authorizationrequest

### **ControlAuthorization (optional)**



**Boolean** 

**AuthRequestURI** (optional)

String



Authorizinguser

**Identifier (optional)** 

String

Name (optional)

String

**DomainIdentifier (optional)** 

String

**DomainNetBIOSName (optional)** 

String

DomainName (optional)

**String** 

**CredentialSource (optional)** 





## AutoAssignPolicyRevisionToGroupRequest

Auto Assign Policy Revision to Group Request Either PolicyRevisionId or PolicyId is required to complete the request

### policyRevisionId (optional)

UUID Identify Latest Policy Revision and Groups based on provided PolicyRevisionId format: uuid

#### policyld (optional)

UUID Identify Latest Policy Revision and Groups based on provided Policyld format: uuid



Bundle

#### Name (optional)

String

#### **Type (optional)**

String

### **Creator (optional)**

String

## **InfoDescription (optional)**

String

# **Version (optional)**



### **DownloadSource (optional)**

String

### **Uri (optional)**

String



# CertificateInformationModel

#### validFrom (optional)

Date format: date-time

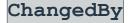
### validTo (optional)

Date format: date-time

## lastIssued (optional)

Date format: date-time

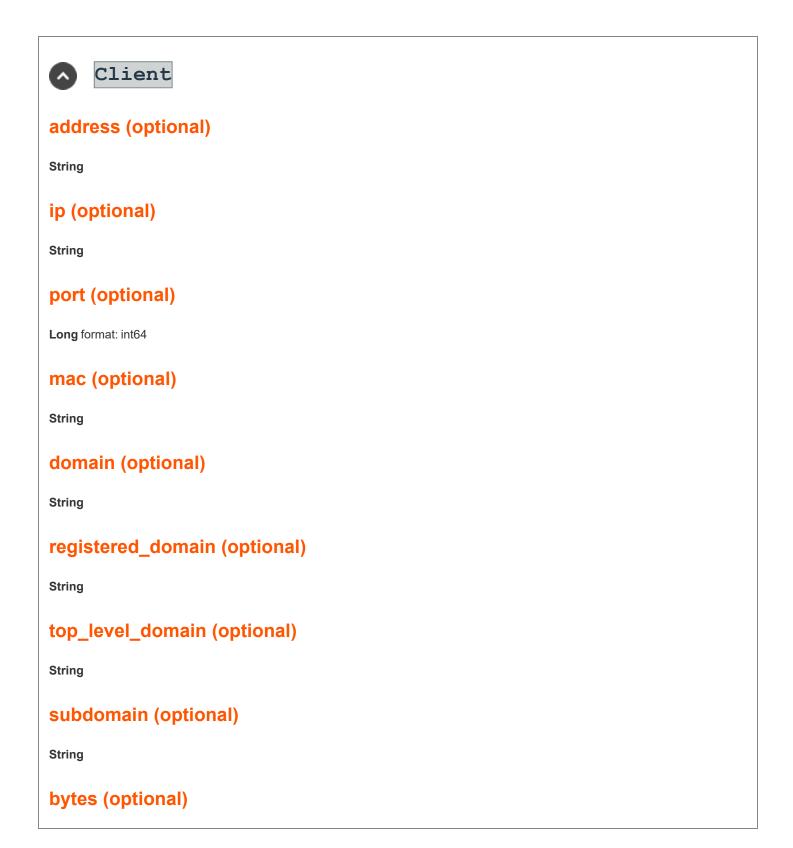




#### enum

- API
- Portal







Long format: int64 packets (optional) Long format: int64 nat (optional) ClientNat Name (optional) String as (optional) As geo (optional) Geo user (optional) User



ClientNat

ip (optional)

String

port (optional)



Long format: int64



Cloud

provider (optional)

**String** 

availability\_zone (optional)

String

region (optional)

**String** 

instance (optional)

CloudInstance

machine (optional)

CloudMachine

account (optional)

CloudAccount

service (optional)

CloudService

project (optional)



CloudProject

origin (optional)

CloudOrigin

target (optional)

CloudTarget



CloudAccount

id (optional)

String

name (optional)

**String** 



CloudInstance

id (optional)

**String** 

name (optional)





CloudMachine

type (optional)

String



CloudOrigin

provider (optional)

**String** 

availability\_zone (optional)

String

region (optional)

**String** 

instance (optional)

CloudInstance

machine (optional)

CloudMachine

account (optional)

CloudAccount



service (optional)

CloudService

project (optional)

CloudProject



CloudProject

id (optional)

**String** 

name (optional)

String



CloudService

name (optional)

String



CloudTarget

provider (optional)



**String** availability\_zone (optional) String region (optional) String instance (optional) CloudInstance machine (optional) CloudMachine account (optional) CloudAccount service (optional) CloudService project (optional) CloudProject



CodeSignature

exists (optional)



Boolean
subject_name (optional)
String
valid (optional)
Boolean
trusted (optional)
Boolean
status (optional)
String
team_id (optional)
String
signing_id (optional)
String
digest_algorithm (optional)
String
timestamp (optional)
Date format: date-time







**AppID** (optional)

String

**CLSID** (optional)

**String** 

**DisplayName (optional)** 

String



ComputerDataAuditingDetailModel

updatedPoliciesOn (optional)

map[String, String]

deactivatedAgents (optional)

map[String, String]

newDeletedAgents (optional)

array[String]





## ComputerDetailModel

#### id (optional)

**UUID** format: uuid

### hostType (optional)

**String** 

#### created (optional)

Date format: date-time

#### adapterVersion (optional)

String

# agentVersion (optional)

String

# authorisationState (optional)

String

# authorised (optional)

Date format: date-time

# connected (optional)

**Boolean** 

## lastConnected (optional)



Date format: date-time deactivated (optional) **Boolean** autoDeactivated (optional) **Boolean** pendingDeactivation (optional) **Boolean** deactivatedOn (optional) Date format: date-time groupld (optional) **UUID** format: uuid groupName (optional) **String** policyld (optional) **UUID** format: uuid policyName (optional) String policyRevision (optional)



Integer format: int32

## policyRevisionStatus (optional)

**String** 

#### endpointInformation (optional)

EndpointInformationModel

### certificateInformation (optional)

CertificateInformationModel

### hostPolicyld (optional)

**UUID** format: uuid

#### hostPolicyName (optional)

String

# hostPolicyRevision (optional)

Integer format: int32

# hostLastUpdated (optional)

Date format: date-time

# agentLogs (optional)

array[ComputerLogModel]

# duplicateCount (optional)



Integer format: int32

### credentialType (optional)

String

#### policyUpdateTimeStamp (optional)

**Date** Describe the instant that a computer receives the policy from the server. This value will be present for computers running PM Windows Adapter V21.8 onwards. Value from Policy Synced At Column from AgentHost Table. format: date-time



### ComputerFilterModel

#### computerId (optional)

UUID The Id of the Computer(Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

### host (optional)

String The host name of the Computer, for example - Computer1

# hostType (optional)

AgentHostType

# agentVersion (optional)

**String** The agent version of the Computer, example - 5.6.126.0

# adapterVersion (optional)

String The adapter version of the Computer, example - 20.5.195.0

### authorisationState (optional)



String The state of the Computer, example - Authorised, Pending

### lastConnected (optional)

**DateFilterModel** 

#### policyRevisionStatus (optional)

String Policy Revision Status, example - AwaitingLatestPolicy

### policyld (optional)

UUID Policy Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

#### policyName (optional)

String Policy Name, example - Policy1

#### groupld (optional)

**UUID** Group Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

# groupName (optional)

String Group Name, example - Group1

# os (optional)

OS

### domain (optional)

String Domain Name, example - BeyondTrust

# created (optional)



**DateFilterModel** 

### duplicateCount (optional)

CountRange



## ComputerListItemModel

#### id (optional)

UUID The Id (Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

## locked (optional)

**Boolean** 

## errorInfo (optional)

ListItemErrorInfoModel

# created (optional)

Date Created Date of the computer, example - 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562 format: date-time

# host (optional)

String The host name of the Computer, for example - Computer1

# hostType (optional)

AgentHostType

## os (optional)



String OS Name, example - Windows

### domain (optional)

String Domain Name, example - BeyondTrust

#### adapterVersion (optional)

String The adapter version of the Computer, example - 20.5.195.0

### agentVersion (optional)

String The agent version of the Computer, example - 5.6.126.0

#### authorisationState (optional)

String The state of the Computer, example - Authorised, Pending

#### lastConnected (optional)

Date Date when computer is last connected, example - 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562 format: date-time

# deactivated (optional)

Boolean if computer is deactivated, example - false

# deactivatedOn (optional)

**Date** Date when computer turned into deactivation state, example - 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562 format: date-time

# pendingDeactivation (optional)

Boolean if computer is in PendingDeactivation state, example - false

# rejected (optional)



Boolean if computer is deactivated, example - false

### duplicate (optional)

Boolean if computer has/is duplicate, example - false

#### duplicateCount (optional)

Integer Computer duplicate count, Min and Max Ranges, example - 1,2,3 format: int32

### policyRevisionId (optional)

**UUID** format: uuid

#### policyld (optional)

UUID Policy Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

#### policyName (optional)

String Policy Name, example - Policy1

# policyRevisionStatus (optional)

String

# groupld (optional)

UUID Group Id, example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

# groupName (optional)

String Group Name, example - Group1

# credentialType (optional)



**String** 

### policyUpdateTimeStamp (optional)

**Date** Describe the instant that a computer receives the policy from the server. This value will be present for computers running PM Windows Adapter V21.8 onwards. Value from Policy Synced At Column from AgentHost Table. format: date-time



## ComputerListItemModelPagedResponse

#### pageNumber (optional)

Integer format: int32

### pageSize (optional)

Integer format: int32

# totalRecordCount (optional)

Integer format: int32

# pageCount (optional)

Integer format: int32

# data (optional)

array[ComputerListItemModel]





ComputerLogModel

#### id (optional)

**UUID** format: uuid

### created (optional)

Date format: date-time

#### returned (optional)

Date format: date-time



ComputerRenewCertificateRequest

### computerId (optional)

**UUID** format: uuid



ComputerRetrieveLogsRequest

# computerId (optional)

**UUID** format: uuid





### ComputerRetrieveStatusInfoRequest

# computerId (optional)

**UUID** format: uuid



#### ComputersAuthoriseRequest

# computerIds (optional)

array[UUID] format: uuid

### excludedComputerIds (optional)

array[UUID] format: uuid

### filter (optional)

ComputerFilterModel

# allComputers (optional)

**Boolean** 

# groupld (optional)

**UUID** format: uuid





## ComputersDeactivateRequest

#### computerIds (optional)

array[UUID] format: uuid

## excludedComputerIds (optional)

array[UUID] format: uuid

#### filter (optional)

ComputerFilterModel

#### allComputers (optional)

**Boolean** 



# ComputersRejectRequest

Request to reject Computer(s)

### computerIds (optional)

array[UUID] List of Computers identifiers to be rejected format: uuid

## excludedComputerIds (optional)

array[UUID] List of Computers identifiers to be excluded from the rejection list format: uuid

# filter (optional)

ComputerFilterModel



#### allComputers (optional)

**Boolean** Is all Computers matching BT.Common.ManagementApi.Computer.ComputerFilterModel and ExcludedComputerIds should be rejected



#### ComputersRemoveRequest

Request to remove Computer(s)

#### computerIds (optional)

array[UUID] List of Computers identifiers to be removed (optional when allComputers is true, otherwise its required) format: uuid

#### excludedComputerIds (optional)

array[UUID] List of Computers identifiers to be excluded from the deletion list format: uuid

# filter (optional)

ComputerFilterModel

# allComputers (optional)

**Boolean** Is all Computers matching BT.Common.ManagementApi.Computer.ComputerFilterModel and ExcludedComputerIds should be removed



## Configuration

# **Identifier (optional)**

String



RevisionNumber (optional)
String
Source (optional)
String
Name (optional)
String
Path (optional)
String
LoadAuditMode (optional)
array[String]
SigningEnforcement (optional)
String
Application (optional)
Application
ApplicationGroup (optional)
Applicationgroup
Content (optional)
Content



ContentGroup (optional)
Contentgroup
GPO (optional)
Gpo
Message (optional)
Message
Rule (optional)
Rule
RuleScript (optional)
Rulescript
Token (optional)
Token
Workstyle (optional)
Workstyle



Container

cpu (optional)

ContainerCpu



disk (optional)
ContainerDisk
id (optional)
String
image (optional)
ContainerImage
labels (optional)
String
memory (optional)
ContainerMemory
name (optional)
String
network (optional)
ContainerNetwork
runtime (optional)
String





ContainerCpu

#### usage (optional)

Double format: double



ContainerDisk

#### read (optional)

ContainerDiskRead

### write (optional)

ContainerDiskWrite



ContainerDiskRead

# bytes (optional)

Long format: int64



ContainerDiskWrite

# bytes (optional)

Long format: int64





ContainerImage

name (optional)

String

tag (optional)

array[String]

hash (optional)

ContainerlmageHash



ContainerImageHash

all (optional)

array[String]



ContainerMemory

usage (optional)

Double format: double





ContainerNetwork

#### ingress (optional)

ContainerNetworkIngress

### egress (optional)

ContainerNetworkEgress



ContainerNetworkEgress

# bytes (optional)

Long format: int64



ContainerNetworkIngress

# bytes (optional)

Long format: int64



Content

# **Type (optional)**

String



#### **Description (optional)**

**String** 

**Identifier (optional)** 

String



Contentgroup

Name (optional)

**String** 

**Description (optional)** 

**String** 

**Identifier (optional)** 

String



CountRange

min (optional)

Integer Min Value of CountRange, example - 1,2,3 format: int32

max (optional)



Integer Max Value of CountRange, example - 1,2,3 format: int32



#### CreateAcceptedDomainRequest

Create Accepted Domain Model

#### domainName (optional)

String Accepted Domain Name



### CreateGroupRequest

#### name (optional)

String name of the group, for example - Alianse Group

# description (optional)

String description of the group, for example - Alianse Group Description

# isDefault (optional)

Boolean



DataStream

# type (optional)

String



### dataset (optional)

String

#### namespace (optional)

String



#### DateFilterModel

DateFilter to specify Dates to be filtered

### dates (optional)

**array[Date]** Valid date formats for filter - 2020-12-24, 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# selectionMode (optional)

**DateSelectionMode** 

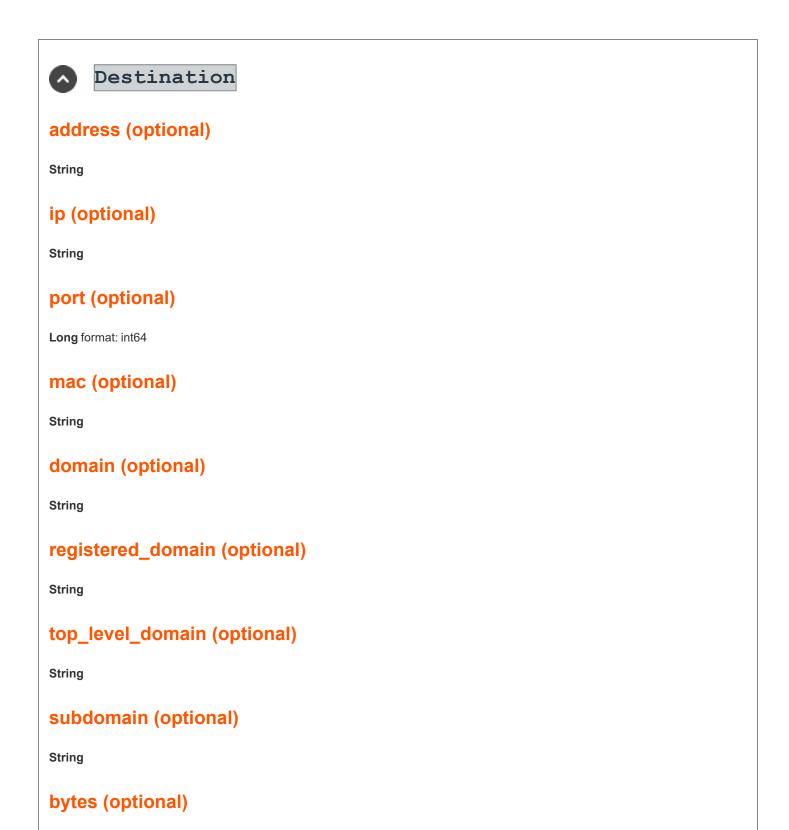


#### DateSelectionMode

Date Selection Mode for filter enum String

- Single
- Multiple
- Range







Long format: int64

packets (optional)

Long format: int64

nat (optional)

DestinationNat

as (optional)

As

geo (optional)

Geo

user (optional)

User



DestinationNat

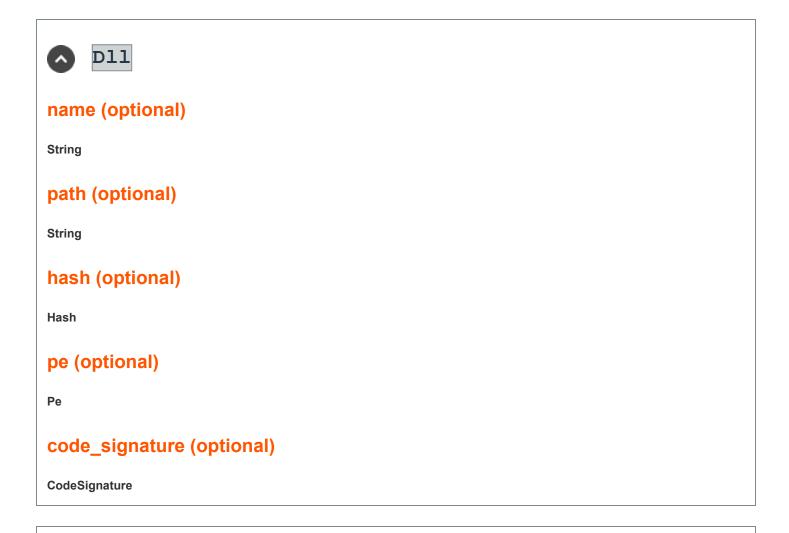
ip (optional)

String

port (optional)

Long format: int64









type (optional)

String

id (optional)

String



op_code (optional)
String
header_flags (optional)
array[String]
response_code (optional)
String
question (optional)
DnsQuestion
answers (optional)
String
resolved_ip (optional)
array[String]



DnsQuestion

name (optional)

String

type (optional)

**String** 



	ant		Í١
class (	opt	iona	I)

**String** 

registered\_domain (optional)

String

top\_level\_domain (optional)

String

subdomain (optional)

String





version (optional)

String





creation\_date (optional)

Date format: date-time

architecture (optional)



**String** byte\_order (optional) String cpu\_type (optional) String header (optional) **ElfHeader** sections (optional) array[ElfSections] exports (optional) map[String, String] imports (optional) map[String, String] shared\_libraries (optional) array[String] telfhash (optional) String segments (optional)



array[ElfSegments]



ElfHeader

class (optional)

**String** 

data (optional)

String

os\_abi (optional)

String

type (optional)

String

version (optional)

String

abi\_version (optional)

String

entrypoint (optional)

Long format: int64

object\_version (optional)



**String** 



ElfSections

flags (optional)

**String** 

name (optional)

String

physical\_offset (optional)

String

type (optional)

String

physical\_size (optional)

Long format: int64

virtual\_address (optional)

Long format: int64

virtual\_size (optional)

Long format: int64

entropy (optional)



Long format: int64

### chi2 (optional)

Long format: int64



ElfSegments

#### type (optional)

String

## sections (optional)

String



Email

### attachments (optional)

array[EmailAttachments]

**bcc** (optional)

**EmailBcc** 

cc (optional)

**EmailCc** 

content\_type (optional)



**String** delivery\_timestamp (optional) Date format: date-time direction (optional) String from (optional) **EmailFrom** local\_id (optional) String message\_id (optional) String origination\_timestamp (optional) Date format: date-time reply\_to (optional) **EmailReplyTo** sender (optional) EmailSender subject (optional)



**String** 

to (optional)

**EmailTo** 

x\_mailer (optional)

String



EmailAttachments

file (optional)

**EmailAttachmentsFile** 



**EmailAttachmentsFile** 

extension (optional)

String

mime\_type (optional)

**String** 

name (optional)

String

size (optional)



Long format: int64

## hash (optional)

Hash



EmailBcc

#### address (optional)

array[String]



EmailCc

# address (optional)

array[String]



**EmailFrom** 

# address (optional)

array[String]



EmailReplyTo

address (optional)



array[String]



EmailSender

address (optional)

String



**EmailTo** 

address (optional)

array[String]



EndpointInformationModel

macAddress (optional)

**String** 

osArchitecture (optional)

String

osCaption (optional)

**String** 

osCodeSet (optional)



String osComputerDescription (optional) String osCountryCode (optional) String osInstallDate (optional) Date format: date-time osManufacturer (optional) String osOrganization (optional) String osSerialNumber (optional) String osSystemDirectory (optional) String osSystemDrive (optional) String osVersion (optional)



String osVersionString (optional) String processorCaption (optional) String processorDescription (optional) **String** processorManufacturer (optional) String processorName (optional) String systemDnsHostName (optional) **String** systemDomain (optional) String systemManufacturer (optional) String systemModel (optional)



systemName (optional)

**String** 

systemPrimaryOwnerName (optional)

String

systemSystemType (optional)

String

systemWorkgroup (optional)

String



**EpmEcsEvent** 

agent (optional)

Agent

**@timestamp (optional)** 

Date format: date-time

tags (optional)

array[String]

labels (optional)



String
message (optional)
String
client (optional)
Client
cloud (optional)
Cloud
container (optional)
Container
data_stream (optional)
DataStream
destination (optional)
Destination
dll (optional)
DII
dns (optional)
Dns
ecs (optional)



Ecs
email (optional)
Email
error (optional)
Error
event (optional)
_event
faas (optional)
-aas
file (optional)
File
group (optional)
Group
host (optional)
Host
http (optional)
Http
og (optional)



Log network (optional) Network observer (optional) Observer orchestrator (optional) **Orchestrator** organization (optional) Organization package (optional) **Package** process (optional) **Process** registry (optional) Registry related (optional) Related rule (optional)



\_rule server (optional) Server service (optional) **Service** source (optional) Source threat (optional) **Threat** tls (optional) TIs trace (optional) **EpmEcsEventTrace** transaction (optional) **EpmEcsEventTransaction** span (optional) **EpmEcsEventSpan** url (optional)



Url

user (optional)

User

user\_agent (optional)

**UserAgent** 

vulnerability (optional)

Vulnerability

**EPMWinMac (optional)** 

**Epmwinmac** 



# EpmEcsEventResponseModel

This class holds Epm Ecs Event response

# totalRecordsReturned (optional)

Long Total records returned by query format: int64

events (optional)

array[EpmEcsEvent] List of events returned by query





**EpmEcsEventSpan** 

id (optional)

String



**EpmEcsEventTrace** 

id (optional)

String



**EpmEcsEventTransaction** 

id (optional)

String



Epmwinmac

**SchemaVersion (optional)** 

**String** 

**GroupId** (optional)

String



Tenantld (optional)
String
AdapterVersion (optional)
String
ActiveX (optional)
Activex
AuthorizationRequest (optional)
Authorizationrequest
AuthorizingUser (optional)
Authorizinguser
COM (optional)
Com
Configuration (optional)
Configuration
Event (optional)
Event
Installer (optional)
Installer



Privilegedgroup

RemotePowerShell (optional)

Remotepowershell

ServiceControl (optional)

Servicecontrol

**Session (optional)** 

Session

StoreApp (optional)

Storeapp

**TrustedApplication (optional)** 

Trustedapplication



Error

id (optional)

String

message (optional)

String



code (optional)

**String** 

type (optional)

**String** 

stack\_trace (optional)

String



Event

**Type (optional)** 

**String** 

**Action (optional)** 

String



Faas

name (optional)

String

id (optional)



version (optional)

String

coldstart (optional)

**Boolean** 

execution (optional)

String

trigger (optional)

**FaasTrigger** 



FaasTrigger

type (optional)

String

request\_id (optional)

String



File

name (optional)



String
attributes (optional)
array[String]
directory (optional)
String
drive_letter (optional)
String
path (optional)
String
target_path (optional)
String
extension (optional)
String
type (optional)
String
device (optional)
String
inode (optional)



String
uid (optional)
String
owner (optional)
String
gid (optional)
String
group (optional)
String
mode (optional)
String
size (optional)
Long format: int64
mtime (optional)
Date format: date-time
ctime (optional)
Date format: date-time
created (optional)



Date format: date-time accessed (optional) Date format: date-time mime\_type (optional) String fork\_name (optional) **String DriveType (optional)** String SourceUrl (optional) String **ZoneTag (optional)** String **ProductVersion (optional)** String **Description (optional)** String **Version (optional)** 



**String** hash (optional) Hash pe (optional) Pe x509 (optional) X509 **Bundle (optional) Bundle Owner (optional)** Owner code\_signature (optional) CodeSignature elf (optional) Elf





location (optional)



**GeoPoint** continent\_code (optional) String continent\_name (optional) String country\_name (optional) String region\_name (optional) String city\_name (optional) String country\_iso\_code (optional) String postal\_code (optional) String region\_iso\_code (optional) String timezone (optional)



name (optional)

String

**TimezoneOffset (optional)** 

Long format: int64



GeoPoint

Ion (optional)

Double format: double

lat (optional)

Double format: double





**Version (optional)** 

**String** 

**DisplayName (optional)** 

**String** 

**ActiveDirectoryPath (optional)** 



**LinkInformation (optional)** 

**String** 



Group

id (optional)

String

name (optional)

String

domain (optional)

String



GroupDataAuditingDetailModel

newName (optional)

**String** 

oldName (optional)

**String** 

newDescription (optional)



oldDescription (optional)

String

newIsDefault (optional)

Boolean

oldIsDefault (optional)

Boolean

addPolicyRevisions (optional)

map[String, String]

removePolicyRevisions (optional)

map[String, String]

newAgents (optional)

map[String, String]

removeAgents (optional)

map[String, String]



GroupListItemModel

locked (optional)



	n	

#### errorInfo (optional)

ListItemErrorInfoModel

#### id (optional)

UUID The ld of the group(Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

# name (optional)

String The name of the group

### description (optional)

String The description of the group

#### computerCount (optional)

Integer The Computer count of the group format: int32

# activeComputers (optional)

Integer Active Computers in the Group format: int32

# created (optional)

**Date** The created date of resource e.g 2020-12-24 19:09:47, 2020-12-24 19:09:47.6816562, 2020-12-24 19:09:47.6816562 +00:00 format: date-time

# policyRevisionId (optional)

**UUID** format: uuid

#### policyld (optional)



**UUID** format: uuid

# policyRevisionStatus (optional)

**PolicyRevisionState** 

#### policyName (optional)

String

#### revision (optional)

Integer format: int32

#### default (optional)

**Boolean** 



#### GroupListItemModelPagedResponse

# pageNumber (optional)

Integer format: int32

# pageSize (optional)

Integer format: int32

# totalRecordCount (optional)

Integer format: int32

# pageCount (optional)



Integer format: int32

# data (optional)

array[GroupListItemModel]





md5 (optional)

String

sha1 (optional)

String

sha256 (optional)

String

sha384 (optional)

String

sha512 (optional)

String

ssdeep (optional)

String

tlsh (optional)







### hostname (optional)

**String** 

#### name (optional)

String

# id (optional)

String

## ip (optional)

array[String]

# mac (optional)

array[String]

# type (optional)

String

# uptime (optional)

Long format: int64

# architecture (optional)



**String** domain (optional) String cpu (optional) **HostCpu** disk (optional) **HostDisk** network (optional) **HostNetwork** boot (optional) **HostBoot** pid\_ns\_ino (optional) String **DomainIdentifier (optional)** String **NetBIOSName (optional)** String **DomainNetBIOSName (optional)** 



ChassisType (optional)
String

DefaultLocale (optional)
String

DefaultUILanguage (optional)
String

geo (optional)
Geo
Os (optional)
Os



HostBoot

id (optional)

String



HostCpu

usage (optional)



Double format: double



HostDisk

#### read (optional)

HostDiskRead

#### write (optional)

**HostDiskWrite** 



HostDiskRead

# bytes (optional)

Long format: int64



HostDiskWrite

# bytes (optional)

Long format: int64



HostNetwork

# ingress (optional)



HostNetworkIngress

#### egress (optional)

HostNetworkEgress



# HostNetworkEgress

#### bytes (optional)

Long format: int64

#### packets (optional)

Long format: int64



# HostNetworkIngress

# bytes (optional)

Long format: int64

# packets (optional)

Long format: int64





# request (optional)



**HttpRequest** 

response (optional)

**HttpResponse** 

version (optional)

String



HttpRequest

id (optional)

String

method (optional)

String

mime\_type (optional)

String

body (optional)

HttpRequestBody

referrer (optional)

String

bytes (optional)



Long format: int64



HttpRequestBody

content (optional)

**String** 

bytes (optional)

Long format: int64



HttpResponse

status\_code (optional)

Long format: int64

mime\_type (optional)

String

body (optional)

HttpResponseBody

bytes (optional)

Long format: int64





# HttpResponseBody

content (optional)

String

bytes (optional)

Long format: int64



# InstallationKeyDataAuditingDetailModel

oldLabel (optional)

String

newLabel (optional)

String

newDisabled (optional)

**Boolean** 

oldDisabled (optional)

**Boolean** 

deleted (optional)

Boolean





Installer

ProductCode (optional)

String

**UpgradeCode** (optional)

String

**Action (optional)** 

String



ListItemErrorInfoModel

parentTaskName (optional)

**String** 

errorCode (optional)

Integer format: int32

userId (optional)

**UUID** format: uuid

userAccountName (optional)

String



ini	itiated (	(optional)
		(

Date format: date-time





#### level (optional)

String

## file (optional)

LogFile

# logger (optional)

**String** 

# origin (optional)

LogOrigin

# syslog (optional)

**String** 



LogFile

# path (optional)





LogOrigin

file (optional)

LogOriginFile

function (optional)

String



LogOriginFile

name (optional)

String

line (optional)

Long format: int64



Message

**Type (optional)** 

**String** 

Name (optional)



**Description (optional)** 

String

**UserReason (optional)** 

**String** 

**Identifier (optional)** 

**String** 

**AuthMethods (optional)** 

array[String]

**Authorization (optional)** 

**Authorization** 

**Authentication (optional)** 

**Authentication** 



# ModifyAcceptedDomainRequest

**Update Accepted Domain Model** 

domain (optional)

String Accepted Domain Name

domainName (optional)



String Accepted Domain Name Either DomainName or Domain required to update Accepted Domain



### ModifyGroupRequest

### id (optional)

UUID id of the group, for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

#### name (optional)

String name of the group, for example - Alianse Group

#### description (optional)

String description of the group, for example - Alianse Group desc



## ModifyPolicyRequest

## name (optional)

String

## description (optional)

String



## ModifyUserPreferencesRequest

## olsonTimeZoneld (optional)



dateTimeDisplayFormat (optional)

String

preferredLanguage (optional)

String



ModifyUserRequest

emailAddress (optional)

String

olsonTimeZoneld (optional)

String

dateTimeDisplayFormat (optional)

String

language (optional)

String



Network

name (optional)



String
type (optional)
String
iana_number (optional)
String
transport (optional)
String
application (optional)
String
protocol (optional)
String
direction (optional)
String
forwarded_ip (optional)
String
community_id (optional)
String
bytes (optional)



Long format: int64

## packets (optional)

Long format: int64

## inner (optional)

**String** 

## vlan (optional)

Vlan



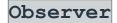


#### enum

#### String

- Windows
- Mac





# mac (optional)

array[String]

## ip (optional)

array[String]



hostname (optional)
String
name (optional)
String
product (optional)
String
vendor (optional)
String
version (optional)
String
serial_number (optional)
String
type (optional)
String
ingress (optional)
String
egress (optional)
String



geo (optional)

Geo

os (optional)

Os



#### OperationValue

Storing the values of the scim operation

### value (optional)

String Generic string value location if no specifc field is specified.

### valueBoolean (optional)

Boolean Generic boolean value if no specific field is specifed.

### active (optional)

**Boolean** Active value of a user

## timezone (optional)

String Timezone value of a user

## locale (optional)

String Locale/language value of a user

### email (optional)



String Email of a user

### role (optional)

String Role of a user



## Operator

enum String

- Equal To
- LessThan
- GreaterThan
- LessThanOrEqualTo
- GreaterThanOrEqualTo



## Orchestrator

## cluster (optional)

**OrchestratorCluster** 

type (optional)

**String** 

organization (optional)

String

namespace (optional)

String



## resource (optional)

**OrchestratorResource** 

api\_version (optional)

String



#### OrchestratorCluster

name (optional)

String

id (optional)

**String** 

url (optional)

**String** 

version (optional)

**String** 



OrchestratorResource

name (optional)



type (optional)

String

parent (optional)

**OrchestratorResourceParent** 

ip (optional)

array[String]

id (optional)

String



OrchestratorResourceParent

type (optional)

String



Organization

name (optional)

String

id (optional)







## type (optional)

String

#### platform (optional)

String

## name (optional)

**String** 

# full (optional)

String

## family (optional)

**String** 

## version (optional)

String

## kernel (optional)

String

## ProductType (optional)





Owner

**Identifier (optional)** 

**String** 

Name (optional)

String

**DomainIdentifier (optional)** 

String

**DomainName (optional)** 

String

**DomainNetBIOSName (optional)** 

String



Package

name (optional)

String

version (optional)



String
build_version (optional)
String
description (optional)
String
size (optional)
Long format: int64
installed (optional)
Date format: date-time
path (optional)
String
architecture (optional)
String
checksum (optional)
String
install_scope (optional)
String
license (optional)



reference (optional)

**String** 

type (optional)

String





original\_file\_name (optional)

String

file\_version (optional)

String

description (optional)

String

product (optional)

String

company (optional)

String

imphash (optional)



architecture (optional)

**String** 

pehash (optional)

String



PolicyDataAudtingDetailModel

newName (optional)

String

oldName (optional)

String

newDescription (optional)

String

oldDescription (optional)

String



PolicyGroupsListItemModel

id (optional)



**UUID** format: uuid

name (optional)

**String** 

description (optional)

String

policyRevisionId (optional)

**UUID** format: uuid

policyld (optional)

**UUID** format: uuid

isDefault (optional)

Boolean



## PolicyListItemModel

## id (optional)

UUID The Id (Guid format), for example - 59A00329-87AC-49EC-BC2C-9B9E26F05185 format: uuid

locked (optional)

**Boolean** 

errorInfo (optional)



ListItemErrorInfoModel

name (optional)

**String** 

size (optional)

Integer format: int32

revision (optional)

Integer format: int32

totalRevisions (optional)

Integer format: int32

totalAssignedRevisions (optional)

Integer format: int32

latestAssignedRevisions (optional)

Integer format: int32

created (optional)

Date format: date-time

lastModified (optional)

Date format: date-time

lastModifiedUserId (optional)



**UUID** format: uuid

## lastModifiedUser (optional)

String

#### hasOpenDraft (optional)

**Boolean** 

### openDraftId (optional)

**UUID** format: uuid

### isAssignedToGroup (optional)

**Boolean** 

#### draftUserId (optional)

**UUID** format: uuid

## draftUser (optional)

String

## lastPolicyToGroupAssignment (optional)

Date format: date-time

### checkedOutDate (optional)

Date format: date-time

## description (optional)



periodLocked (optional)

String



PolicyListItemModelPagedResponse

pageNumber (optional)

Integer format: int32

pageSize (optional)

Integer format: int32

totalRecordCount (optional)

Integer format: int32

pageCount (optional)

Integer format: int32

data (optional)

array[PolicyListItemModel]



PolicyRevisionDataAuditingDetailModel

newGroups (optional)



map[String, String]



## PolicyRevisionModel

## id (optional)

**UUID** format: uuid

#### created (optional)

Date format: date-time

## revision (optional)

Integer format: int32

## size (optional)

Integer format: int32

## comment (optional)

String

## user (optional)

String

## isAssignedGroup (optional)

**Boolean** 





## PolicyRevisionState

#### enum String

- OnLatestPolicy
- OnAnEarlierPolicy
- NoPolicy
- AwaitingLatestPolicy
- AwaitingAnEarlierPolicy



## Privilegedgroup

## Name (optional)

String

#### **RID** (optional)

**String** 

## **Access (optional)**

String



# ProblemDetails

type

**String** 

title



String

status
integer(\$int32)

detail
String
instance
String



Process

## pid (optional)

Long format: int64

entity\_id (optional)

String

name (optional)

**String** 

pgid (optional)

Long format: int64

command\_line (optional)



String args (optional) array[String] args\_count (optional) Long format: int64 executable (optional) **String** title (optional) String thread (optional) **ProcessThread** start (optional) Date format: date-time uptime (optional) Long format: int64 working\_directory (optional) String exit\_code (optional)



Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional) String entry\_meta (optional) **ProcessEntryMeta** tty (optional) String **ElevationRequired (optional) Boolean** group (optional) Group real\_group (optional)



Group
saved_group (optional)
Group
supplemental_groups (optional)
Group
hash (optional)
Hash
pe (optional)
Pe
code_signature (optional)
CodeSignature
elf (optional)
Elf
HostedFile (optional)
File
user (optional)
User
saved_user (optional)



real\_user (optional)

User

parent (optional)

ProcessParent

entry\_leader (optional)

ProcessEntryLeader

session\_leader (optional)

ProcessSessionLeader

group\_leader (optional)

ProcessGroupLeader

previous (optional)



ProcessEntryLeader

pid (optional)

Long format: int64

**ProcessPrevious** 

entity\_id (optional)



String name (optional) String pgid (optional) Long format: int64 command\_line (optional) **String** args (optional) array[String] args\_count (optional) Long format: int64 executable (optional) String title (optional) String thread (optional) **ProcessThread** start (optional)



Date format: date-time uptime (optional) Long format: int64 working\_directory (optional) String exit\_code (optional) Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional) String entry\_meta (optional) **ProcessEntryMeta** tty (optional)



String **ElevationRequired (optional) Boolean** group (optional) Group real\_group (optional) Group saved\_group (optional) Group supplemental\_groups (optional) Group hash (optional) Hash pe (optional) Pe code\_signature (optional) CodeSignature elf (optional)



HostedFile (optional)
File
user (optional)
User
saved\_user (optional)
User
real\_user (optional)
User
parent (optional)
ProcessParent



ProcessEntryMeta

type (optional)

String

source (optional)

Source





## ProcessGroupLeader

#### pid (optional)

Long format: int64

entity\_id (optional)

**String** 

name (optional)

String

pgid (optional)

Long format: int64

command\_line (optional)

String

args (optional)

array[String]

args\_count (optional)

Long format: int64

executable (optional)

String

title (optional)



String thread (optional) **ProcessThread** start (optional) Date format: date-time uptime (optional) Long format: int64 working\_directory (optional) String exit\_code (optional) Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional)



String entry\_meta (optional) **ProcessEntryMeta** tty (optional) String **ElevationRequired (optional) Boolean** group (optional) Group real\_group (optional) Group saved\_group (optional) Group supplemental\_groups (optional) Group hash (optional) Hash pe (optional)



Pe code\_signature (optional) CodeSignature elf (optional) Elf **HostedFile (optional)** File user (optional) User saved\_user (optional) User real\_user (optional) User



ProcessParent

pid (optional)

Long format: int64

entity\_id (optional)



String name (optional) String pgid (optional) Long format: int64 command\_line (optional) **String** args (optional) array[String] args\_count (optional) Long format: int64 executable (optional) String title (optional) String thread (optional) **ProcessThread** start (optional)



Date format: date-time uptime (optional) Long format: int64 working\_directory (optional) String exit\_code (optional) Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional) String entry\_meta (optional) **ProcessEntryMeta** tty (optional)



String **ElevationRequired (optional) Boolean** group (optional) Group real\_group (optional) Group saved\_group (optional) Group supplemental\_groups (optional) Group hash (optional) Hash pe (optional) Pe code\_signature (optional) CodeSignature elf (optional)



HostedFile (optional)

File

user (optional)

User

saved\_user (optional)

User

real\_user (optional)

User

group\_leader (optional)

ProcessGroupLeader



ProcessPrevious

pid (optional)

Long format: int64

entity\_id (optional)

String

name (optional)



**String** pgid (optional) Long format: int64 command\_line (optional) String args (optional) array[String] args\_count (optional) Long format: int64 executable (optional) String title (optional) String thread (optional) **ProcessThread** start (optional) Date format: date-time uptime (optional)



Long format: int64 working\_directory (optional) String exit\_code (optional) Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional) String entry\_meta (optional) **ProcessEntryMeta** tty (optional) String **ElevationRequired (optional)** 



Boolean
group (optional)
Group
real_group (optional)
Group
saved_group (optional)
Group
supplemental_groups (optional)
Group
hash (optional)
Hash
pe (optional)
Pe
code_signature (optional)
CodeSignature
elf (optional)
Elf
HostedFile (optional)



File

user (optional)

User

saved\_user (optional)

User

real\_user (optional)

User



#### ProcessSessionLeader

### pid (optional)

Long format: int64

entity\_id (optional)

String

name (optional)

String

pgid (optional)

Long format: int64

command\_line (optional)



**String** args (optional) array[String] args\_count (optional) Long format: int64 executable (optional) **String** title (optional) String thread (optional) **ProcessThread** start (optional) Date format: date-time uptime (optional) Long format: int64 working\_directory (optional) String exit\_code (optional)



Long format: int64 end (optional) Date format: date-time interactive (optional) **Boolean** same\_as\_process (optional) **Boolean** env\_vars (optional) String entry\_meta (optional) **ProcessEntryMeta** tty (optional) String **ElevationRequired (optional) Boolean** group (optional) Group real\_group (optional)



Group
saved_group (optional)
Group
supplemental_groups (optional)
Group
hash (optional)
Hash
pe (optional)
Pe
code_signature (optional)
CodeSignature
elf (optional)
Elf
HostedFile (optional)
File
user (optional)
User
saved_user (optional)



User

real\_user (optional)

User

parent (optional)

**ProcessParent** 



ProcessThread

id (optional)

Long format: int64

name (optional)

String



Registry

hive (optional)

**String** 

key (optional)

String

value (optional)



path (optional)

String

data (optional)

RegistryData



RegistryData

type (optional)

String

strings (optional)

array[String]

bytes (optional)

String



Related

ip (optional)

array[String]

user (optional)



array[String]

hash (optional)

array[String]

hosts (optional)

array[String]



Remotepowershell

**Command (optional)** 

String



RoleElement

role object

primary (optional)

Boolean boolena flag for whether or not this is the primary role

value (optional)

String User role value



RoleItemModel

Model of role list item



<ul> <li></li></ul>	/ _	2.45			×
id (		nti	<b>M</b>	าลเ	١
I'M (	V	PLI	V	IUI	,

**UUID** Identifier format: uuid

# name (optional)

String Name

#### resourceld (optional)

String Resource Id

#### resourceType (optional)

String Resource Type



#### RoleListItemModel

### id (optional)

**UUID** format: uuid

### name (optional)

**String** 

## allowPermissions (optional)

array[RolePermissionModel]

## denyPermissions (optional)

array[RolePermissionModel] deprecated. rbac only support allow permissions





RoleModel

#### id (optional)

**UUID** format: uuid

### name (optional)

String

#### allowPermissions (optional)

array[RolePermissionModel]

#### denyPermissions (optional)

array[RolePermissionModel] deprecated. rbac only support allow permissions



## RolePermissionModel

## resource (optional)

String

## action (optional)

**String** 



### RoleResourceModel

Model for user role resource



resourceTy	vpe (o	ptional)
	, p	ptional

String Type of resource

#### resourceld (optional)

UUID Id of the resource format: uuid

#### roleld (optional)

**UUID** Role Id format: uuid



Rule

### **Identifier (optional)**

**String** 

### **OnDemand (optional)**

**Boolean** 

### **Action (optional)**

**String** 



Rulescript

## FileName (optional)



**Publisher (optional)** 

String

**Outcome (optional)** 

RulescriptOutcome



RulescriptOutcome

**Version (optional)** 

**String** 

Name (optional)

String

**RuleAffected (optional)** 

**Boolean** 

**Result (optional)** 

String

**Output (optional)** 





**SCIME**mail

primary (optional)

**Boolean** 

value (optional)

**String** 

type (optional)

String



SCIMUserName

givenName (optional)

**String** 

familyName (optional)

String

middleName (optional)

String



ScimAuthenticationSchemes

authentication schemes for scim



### name (optional)

String name of authentication

#### description (optional)

String description of authentication

#### type (optional)

String type of authentiation

#### primary (optional)

Boolean flag for whether or not the authentication scheme is the primary



ScimBulk

flag to see if scim bulk operations is supported

### maxOperations (optional)

Integer max operations format: int32

## maxPayloadSize (optional)

Integer max payload size format: int32

## supported (optional)

Boolean flag for bulk operations





### ScimOperation

SCIM Operations going to be performed on a user

#### op (optional)

String Operation to be performed on a user. add or replace

#### path (optional)

String Which field the operation should affect. optional

#### value (optional)

array[OperationValue] Values of the fields going that are going to be changed



#### ScimResourceMeta

resource type meta data

### resourceType (optional)

String resource type meta data



### ScimResourceResponse

Json structure for resource type response

#### schemas (optional)

array[String] schema

# name (optional)



String name of resource type

#### description (optional)

String description of resource type

#### endpoint (optional)

String endpoint

#### schema (optional)

String schema

#### meta (optional)

ScimResourceMeta



### ScimResourceResponseScimListResponse

### schemas (optional)

array[String]

## totalResults (optional)

Integer format: int32

### startIndex (optional)

Integer format: int32

### itemsPerPage (optional)



Integer format: int32

#### **Resources (optional)**

array[ScimResourceResponse]



### ScimSchemaResponse

Structure of the schema response

### schemas (optional)

array[String] schema

#### id (optional)

String id of schema

### name (optional)

String name of schema

### description (optional)

String description of schema

### attributes (optional)

array[Attribute] available attributes

### meta (optional)

ScimResourceMeta





### ScimSchemaResponseScimListResponse

#### schemas (optional)

array[String]

#### totalResults (optional)

Integer format: int32

#### startIndex (optional)

Integer format: int32

#### itemsPerPage (optional)

Integer format: int32

### **Resources (optional)**

array[ScimSchemaResponse]



### ScimServiceProviderConfigResponse

## schemas (optional)

array[String] service provider config schema

### patch (optional)

**ScimSupported** 



1. 11 /	/ 4 * 1	ı٨
niik i	Ontional	n
Duin (	(optional	١,

ScimBulk

#### filter (optional)

**ScimSupported** 

### changePassword (optional)

**ScimSupported** 

#### sort (optional)

**ScimSupported** 

### etag (optional)

**ScimSupported** 

### authenticationSchemes (optional)

**ScimAuthenticationSchemes** 

## meta (optional)

ScimResourceMeta



### ScimSupported

Flag to see if scim feature if supported

### supported (optional)



Boolean flag to see if scim feature is supported



ScimUserMetaModel

resourceType (optional)

**String** 

created (optional)

Date format: date-time



ScimUserModel

schemas (optional)

array[String]

id (optional)

**UUID** format: uuid

userName (optional)

**String** 

name (optional)

**SCIMUserName** 

emails (optional)



array[SCIMEmail] displayName (optional) String locale (optional) String timezone (optional) String externalld (optional) String dateTimeFormat (optional) String groups (optional) array[null] password (optional) String active (optional) Boolean boolean flag of whether or not a user is active roles (optional)



array[RoleElement] A complex role object for scim

#### entitlements (optional)

array[RoleElement] A complex role object for scim

#### meta (optional)

ScimUserMetaModel



#### ScimUserModelScimListResponse

#### schemas (optional)

array[String]

### totalResults (optional)

Integer format: int32

### startIndex (optional)

Integer format: int32

## itemsPerPage (optional)

Integer format: int32

### **Resources (optional)**

array[ScimUserModel]





## ScimUserPatchRequest

Patch request used to update a user through SCIM

#### schemas (optional)

array[String] Schema of the request, should be urn:ietf:params:scim:api:messages:2.0:PatchOp

#### operations (optional)

array[ScimOperation] SCIM Operations going to be performed on a user



Server

#### address (optional)

String

### ip (optional)

String

## port (optional)

Long format: int64

### mac (optional)

String

### domain (optional)



registered_domain (optional)
String
top_level_domain (optional)
String
subdomain (optional)
String
bytes (optional)
Long format: int64
packets (optional)
Long format: int64
nat (optional)
ServerNat
as (optional)
As
geo (optional)
Geo
user (optional)
User





ServerNat

#### ip (optional)

String

#### port (optional)

Long format: int64



Service

#### environment (optional)

String

id (optional)

**String** 

name (optional)

String

node (optional)

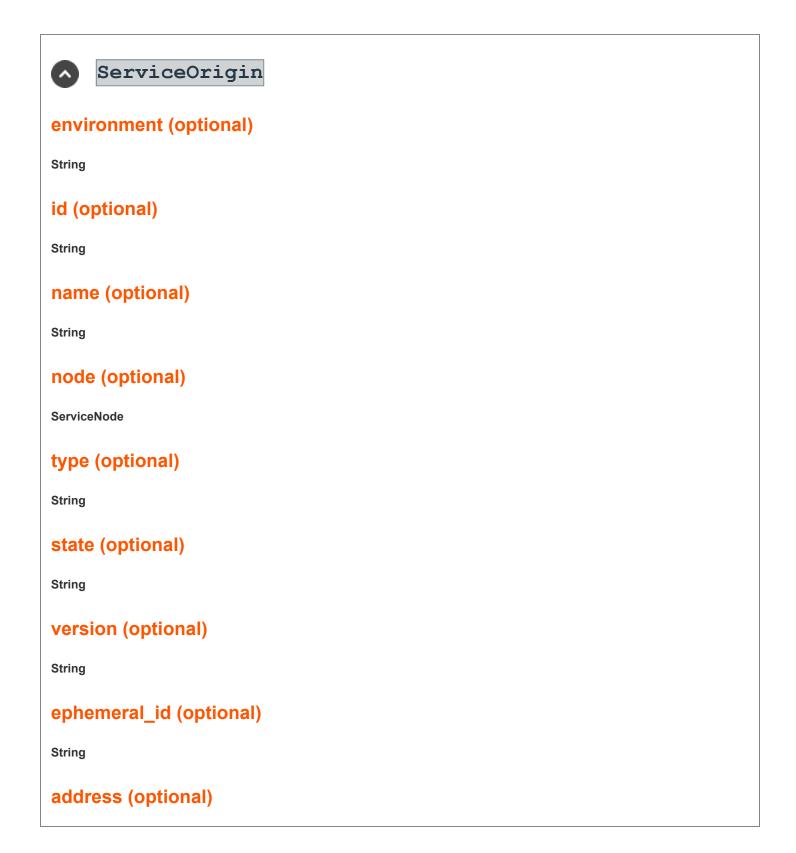
ServiceNode

type (optional)



state (optional)
String
version (optional)
String
ephemeral_id (optional)
String
address (optional)
String
origin (optional)
ServiceOrigin
target (optional)
ServiceTarget
ServiceNode
name (optional)
String
role (optional)









ServiceTarget

environment (optional)

**String** 

id (optional)

String

name (optional)

String

node (optional)

ServiceNode

type (optional)

String

state (optional)

String

version (optional)

String

ephemeral\_id (optional)



address (optional)

String



Servicecontrol

**Service (optional)** 

ServicecontrolService



ServicecontrolService

**DisplayName (optional)** 

**String** 

Name (optional)

String

**Action (optional)** 

String



Session

**Administrator (optional)** 



Locale (optional)
String

Identifier (optional)
String

PowerUser (optional)
Boolean

WindowsSessionId (optional)
String

UlLanguage (optional)
String



SettingDataAuditingDetailModel

addDomain (optional)

String

removeDomain (optional)

String

modifyDomainOldValue (optional)



modifyDomainNewValue (optional)

**String** 



SortDirection

#### enum

#### String

- Asc
- Desc



SortModel

### by (optional)

String The property on which to sort e.g. name

## order (optional)

SortDirection



Source

## address (optional)



ip (optional)
String
port (optional)
Long format: int64
mac (optional)
String
domain (optional)
String
registered_domain (optional)
String
top_level_domain (optional)
String
subdomain (optional)
String
bytes (optional)
Long format: int64
packets (optional)
Long format: int64



nat (optional)		
SourceNat		
as (optional)		
As		
geo (optional)		
Geo		
user (optional)		



User

SourceNat

ip (optional)

**String** 

port (optional)

Long format: int64



Storeapp

Name (optional)



#### **Publisher (optional)**

String

#### **Version (optional)**

String



#### SubAttribute

Schema for subattributes

#### name (optional)

String name of attribute

### description (optional)

String description of attribute

## type (optional)

String type of attribute

### canonicalValues (optional)

array[String] list of canonical values

#### caseExact (optional)

Boolean Flag for whether or not the attribute's casing should be exact

### multiValued (optional)



Boolean Flag for whether or not the attribute has multi values

#### mutability (optional)

String Mutability of the attribute

#### required (optional)

Boolean Flag for whether or not the attribute is required

#### returned (optional)

String how the attribute is returned

#### uniqueness (optional)

String Is the value unique



### TaskDetailModel

## id (optional)

**UUID** format: uuid

## tenantId (optional)

**UUID** format: uuid

## name (optional)

String

### state (optional)



Integer format: int32

#### stateName (optional)

String

#### initiated (optional)

Date format: date-time

#### completed (optional)

Date format: date-time

### userId (optional)

**UUID** format: uuid

#### user (optional)

String

# completedWithErrors (optional)

**Boolean** 

### messageParameters (optional)

array[map[String, String]]



Threat

### enrichments (optional)



array[ThreatEnrichments] feed (optional) **ThreatFeed** framework (optional) String group (optional) **ThreatGroup** indicator (optional) **ThreatIndicator** software (optional) **ThreatSoftware** tactic (optional) **ThreatTactic** technique (optional) **ThreatTechnique** 



ThreatEnrichments

indicator (optional)



### matched (optional)

**ThreatEnrichmentsMatched** 



### ThreatEnrichmentsMatched

#### atomic (optional)

String

field (optional)

String

id (optional)

String

index (optional)

String

occurred (optional)

Date format: date-time

type (optional)

String





### ThreatFeed

dashboard\_id (optional)

String

name (optional)

String

description (optional)

String

reference (optional)

String



# ThreatGroup

alias (optional)

array[String]

id (optional)

String

name (optional)

String



#### reference (optional)

String



#### ThreatIndicator

#### first\_seen (optional)

Date format: date-time

#### last\_seen (optional)

Date format: date-time

#### modified\_at (optional)

Date format: date-time

## sightings (optional)

Long format: int64

### type (optional)

**String** 

# description (optional)

String

### scanner\_stats (optional)

Long format: int64



confidence (optional)
String
ip (optional)
String
port (optional)
Long format: int64
email (optional)
ThreatIndicatorEmail
marking (optional)
ThreatIndicatorMarking
reference (optional)
String
provider (optional)
String
x509 (optional)
X509
as (optional)
As



<b>C</b>	4 =	1
TIIA /	optiona	
1116	UUIIIUIIA	
	0000000	-,

File

geo (optional)

Geo

registry (optional)

Registry

url (optional)

Url



ThreatIndicatorEmail

address (optional)

String



ThreatIndicatorMarking

tlp (optional)

String





## ThreatSoftware

id (optional)

String

name (optional)

String

alias (optional)

array[String]

platforms (optional)

array[String]

reference (optional)

String

type (optional)

**String** 



ThreatTactic

id (optional)

array[String]



#### name (optional)

array[String]

reference (optional)

array[String]



#### ThreatTechnique

#### id (optional)

array[String]

name (optional)

array[String]

reference (optional)

array[String]

subtechnique (optional)

ThreatTechniqueSubtechnique



ThreatTechniqueSubtechnique

id (optional)



array[String]

name (optional)

array[String]

reference (optional)

array[String]





version (optional)

String

version\_protocol (optional)

String

cipher (optional)

String

curve (optional)

String

resumed (optional)

**Boolean** 

established (optional)



**Boolean** 

next\_protocol (optional)

**String** 

client (optional)

**TIsClient** 

server (optional)

**TIsServer** 



TlsClient

ja3 (optional)

String

server\_name (optional)

String

supported\_ciphers (optional)

array[String]

subject (optional)

String

issuer (optional)



**String** not\_before (optional) Date format: date-time not\_after (optional) Date format: date-time certificate\_chain (optional) array[String] certificate (optional) String hash (optional) **TIsClientHash** x509 (optional) X509



TlsClientHash

md5 (optional)

String

sha1 (optional)



sha256 (optional)

String



TlsServer

ja3s (optional)

String

subject (optional)

String

issuer (optional)

String

not\_before (optional)

Date format: date-time

not\_after (optional)

Date format: date-time

certificate\_chain (optional)

array[String]

certificate (optional)



hash (optional)

TIsServerHash

x509 (optional)

X509



TlsServerHash

md5 (optional)

String

sha1 (optional)

String

sha256 (optional)

String



Token

Name (optional)

String

**Description (optional)** 



**Identifier (optional)** 

String



Trustedapplication

Name (optional)

String

**Version (optional)** 

String



UnassignComputersToGroupRequest

allComputers (optional)

Boolean

filter (optional)

ComputerFilterModel

excludedComputerIds (optional)

array[UUID] format: uuid

selectionComputerIds (optional)



array[UUID] selection computers ids will work when "allComputers" : false format: uuid



scheme (optional)

String

domain (optional)

String

registered\_domain (optional)

String

top\_level\_domain (optional)

String

subdomain (optional)

String

port (optional)



Long format: int64 path (optional) String query (optional) **String** extension (optional) **String** fragment (optional) **String** username (optional) String password (optional) String User

id (optional)

String

name (optional)



**String** full\_name (optional) String email (optional) String hash (optional) String domain (optional) String roles (optional) array[String] **DomainIdentifier (optional)** String DomainNetBIOSName (optional) String **DefaultLocale (optional)** String **DefaultTimezoneOffset (optional)** 



Long format: int64

DefaultUlLanguage (optional)

String

LocalIdentifier (optional)

Long format: int64

group (optional)

Group

target (optional)

UserTarget

effective (optional)

UserEffective



**UserChanges** 

UserAgent

original (optional)

changes (optional)

String

name (optional)



version (optional)

String

device (optional)

**UserAgentDevice** 

os (optional)

Os



UserAgentDevice

name (optional)

String



UserChanges

id (optional)

**String** 

name (optional)

String

full\_name (optional)



String
email (optional)
String
hash (optional)
String
domain (optional)
String
roles (optional)
array[String]
DomainIdentifier (optional)
String
DomainNetBIOSName (optional)
String
DefaultLocale (optional)
String
DefaultTimezoneOffset (optional)
Long format: int64
DefaultUILanguage (optional)



#### **Localidentifier (optional)**

Long format: int64

### group (optional)

Group



#### UserDataAuditing

Activity Audit User Data

#### newEmailAddress (optional)

String New Email Address

### oldEmailAddress (optional)

String Old Email Address

### newOlsonTimeZoneld (optional)

String New Timezone

## oldOlsonTimeZoneld (optional)

String Old Timezone

## newDateTimeDisplayFormat (optional)

String New Datetime Display Format

# oldDateTimeDisplayFormat (optional)



String Old Datetime Display Format

#### newPreferredLanguage (optional)

String New Preferred Language

#### oldPreferredLanguage (optional)

String Old Preferred Language

#### newDisabled (optional)

**Boolean** New Disabled

#### oldDisabled (optional)

**Boolean** Old Disabled

#### newUserType (optional)

String new user type

## oldUserType (optional)

String old user type

## roles (optional)

array[ActivtyAuditRoleResourceModel] Role audit data



UserDetailModel

## id (optional)



**UUID** format: uuid accountName (optional) String emailAddress (optional) String created (optional) Date format: date-time isFirstSignIn (optional) **Boolean** lastSignedIn (optional) Date format: date-time disabled (optional) **Boolean** roles (optional) array[UserRoleResourceItemModel] olsonTimeZoneld (optional) String dateTimeDisplayFormat (optional)



language (optional)

**String** 

allowInvites (optional)

**Boolean** 



UserEffective

id (optional)

String

name (optional)

String

full\_name (optional)

String

email (optional)

String

hash (optional)

String

domain (optional)



**String** roles (optional) array[String] **DomainIdentifier (optional)** String **DomainNetBIOSName (optional) String DefaultLocale (optional)** String **DefaultTimezoneOffset (optional)** Long format: int64 **DefaultUILanguage (optional) String Localidentifier (optional)** Long format: int64 group (optional) Group





### UserListItemModel

Model of user list item

### locked (optional)

**Boolean** 

# errorInfo (optional)

ListItemErrorInfoModel

### id (optional)

**UUID** User identifier format: uuid

#### accountName (optional)

String Account name

# emailAddress (optional)

String Email

## created (optional)

Date Creation date format: date-time

## lastSignedIn (optional)

Date Last logged in date format: date-time

# disabled (optional)

Boolean Is user disabled



#### roles (optional)

array[RoleItemModel] List of user roles

#### roleName (optional)

String Role name

#### olsonTimeZoneld (optional)

String Time zone

#### dateTimeDisplayFormat (optional)

String Date and time display format

#### language (optional)

String Preferred language



## UserListItemModelPagedResponse

## pageNumber (optional)

Integer format: int32

## pageSize (optional)

Integer format: int32

## totalRecordCount (optional)

Integer format: int32



### pageCount (optional)

Integer format: int32

#### data (optional)

array[UserListItemModel]



#### UserRoleResourceItemModel

#### id (optional)

**UUID** format: uuid

#### name (optional)

String

### allowPermissions (optional)

array[RolePermissionModel]

## denyPermissions (optional)

array[RolePermissionModel] deprecated. rbac only support allow permissions

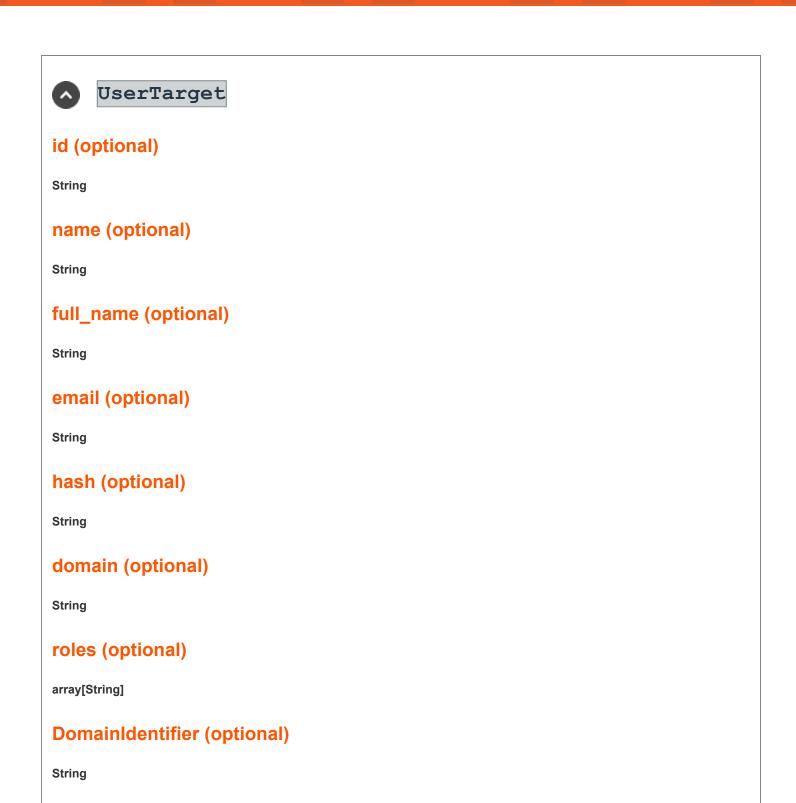
## resourceld (optional)

String

## resourceType (optional)

String





**DomainNetBIOSName (optional)** 



**DefaultLocale (optional)** 

**String** 

**DefaultTimezoneOffset (optional)** 

Long format: int64

**DefaultUILanguage (optional)** 

**String** 

**LocalIdentifier (optional)** 

Long format: int64

group (optional)

Group



V2CreateUserRequest

V2CreateUserRequest

emailAddress (optional)

String EmailAddress

olsonTimeZoneld (optional)

String OlsonTimeZoneId

dateTimeDisplayFormat (optional)



String DateTimeDisplayFormat

#### language (optional)

String Language

#### enabled (optional)

**Boolean** Enabled

#### roleResource (optional)

array[RoleResourceModel] list of user role resources

#### admin (optional)

Boolean admin

#### allGroups (optional)

Boolean full permissions for all groups

# groupRoles (optional)

array[UUID] roles to assign all groups format: uuid

# allPolicies (optional)

Boolean full permissions for all policies

# policyRoles (optional)

array[UUID] role to assign all policies format: uuid





Vlan

id (optional)

String

name (optional)

**String** 



Vulnerability

classification (optional)

**String** 

enumeration (optional)

**String** 

reference (optional)

String

score (optional)

**VulnerabilityScore** 

category (optional)

array[String]



All the second second	4 * 4 * 4	/ 4 " 1	×
aecri	ntion i	(optional	h
<b>ucscii</b>	ptioii (	Optional	•

id (optional)

String

scanner (optional)

VulnerabilityScanner

severity (optional)

String

report\_id (optional)

String



VulnerabilityScanner

vendor (optional)

**String** 



VulnerabilityScore

base (optional)



Double format: double

### temporal (optional)

Double format: double

#### environmental (optional)

Double format: double

#### version (optional)

String



Workstyle

### Name (optional)

String

## **Description (optional)**

String

# **Identifier (optional)**

String



**x**509

### version\_number (optional)



**String** serial\_number (optional) String issuer (optional) X509Issuer signature\_algorithm (optional) String not\_before (optional) Date format: date-time not\_after (optional) Date format: date-time subject (optional) X509Subject public\_key\_algorithm (optional) String public\_key\_size (optional) Long format: int64 public\_key\_exponent (optional)



Long format: int64

public\_key\_curve (optional)

String

alternative\_names (optional)

array[String]



X509Issuer

distinguished\_name (optional)

String

common\_name (optional)

array[String]

organizational\_unit (optional)

array[String]

organization (optional)

array[String]

locality (optional)

array[String]

state\_or\_province (optional)



array[String]

country (optional)

array[String]



X509Subject

distinguished\_name (optional)

**String** 

common\_name (optional)

array[String]

organizational\_unit (optional)

array[String]

organization (optional)

array[String]

locality (optional)

array[String]

state\_or\_province (optional)

array[String]

country (optional)



array[String]



event

id (optional)

**String** 

code (optional)

String

kind (optional)

String

category (optional)

array[String]

action (optional)

String

outcome (optional)

String

type (optional)

array[String]

module (optional)



String
dataset (optional)
String
provider (optional)
String
severity (optional)
Long format: int64
original (optional)
String
hash (optional)
String
duration (optional)
Long format: int64
sequence (optional)
Long format: int64
timezone (optional)
String
created (optional)



Date format: date-time start (optional) Date format: date-time end (optional) Date format: date-time risk\_score (optional) Double format: double risk\_score\_norm (optional) Double format: double ingested (optional) Date format: date-time reference (optional) String url (optional) String reason (optional) String agent\_id\_status (optional)



reference (optional)

String rule id (optional) String uuid (optional) String version (optional) String name (optional) String description (optional) String category (optional) **String** ruleset (optional) String



author (optional)

array[String]

license (optional)

String



id AssignComputersByCsv body

csvFile (optional)

byte[] format: binary



id\_Upload\_body

PolicyFile (optional)

byte[] Policy Content File format: binary

AutoAssignToGroup (optional)

Boolean Auto Assign Policy Revision to Computer Groups



v2 Policies body

Name (optional)



String Policy Name

# **Description (optional)**

**String** Policy Description

### PolicyFile (optional)

byte[] Policy Content File format: binary