



BeyondTrust

Privilege Management Cloud 23.7 API Guide - Version 2

Table of Contents

Privilege Management Cloud API - Version 2	12
Authenticate to the PM Cloud API	12
Methods	14
About	18
AcceptedDomains	20
ActivityAudits	25
ApiAccounts	49
AuthenticationProvider	51
AuthorizationRequestAudits	52
Computers	57
Events	79
File	173
Groups	174
Policies	190
Roles	205
ScimResourceTypes	207
ScimSchemas	210
ScimServiceProviderConfig	214
ScimUsers	215
Tasks	223
Users	224
Models	237
AboutModel	244
AcceptedDomainDetailModel	244
AcceptedDomainListItemModel	245
Activex	246
ActivityAuditDetailModel	246
ActivityAuditDetailModelPagedResponse	250
ActivityAuditListItemModel	250
ActivityAuditListItemModelPagedResponse	251
ActivityAuditRoleNameModel	252

ActivityAuditRoleResourceModel	252
Agent	253
AgentBuild	254
AgentDataAuditingDetailModel	254
AgentHostType	256
ApiAccountListItemModel	256
ApiClientDataAuditingDetailModel	258
Application	258
Applicationgroup	259
As	259
AsOrganization	260
AssignComputersToGroupRequest	260
AssignPolicyRevisionToGroupRequest	260
AssignUserToRolesRequest	261
Attribute	261
Authentication	262
Authorization	262
AuthorizationRequestAuditDetailModel	263
AuthorizationRequestAuditDetailModelPagedResponse	264
AuthorizationRequestAuditListItemModel	265
AuthorizationRequestAuditListItemModelPagedResponse	266
AuthorizationRequestDataAuditingDetailModel	267
Authorizationrequest	269
Authorizinguser	269
AutoAssignPolicyRevisionToGroupRequest	270
AzureADIntegrationDataAuditingDetailModel	270
Bundle	272
CertificateInformationModel	273
ChangedBy	273
Client	274
ClientNat	275
Cloud	276
CloudAccount	277

CloudInstance	277
CloudMachine	278
CloudOrigin	278
CloudProject	279
CloudService	279
CloudTarget	279
CodeSignature	280
Com	282
ComputerDataAuditingDetailModel	282
ComputerDetailModel	283
ComputerFilterModel	287
ComputerListItemModel	289
ComputerListItemModelPagedResponse	293
ComputerLogModel	293
ComputerPolicyDataAuditingDetailModel	294
ComputerRenewCertificateRequest	295
ComputerRetrieveLogsRequest	295
ComputerRetrieveStatusInfoRequest	295
ComputersArchiveRequest	295
ComputersAuthoriseRequest	296
ComputersDeactivateRequest	296
ComputersRejectRequest	297
ComputersRemoveRequest	297
ComputersUnarchiveRequest	298
Configuration	298
Container	300
ContainerCpu	302
ContainerDisk	302
ContainerDiskRead	302
ContainerDiskWrite	302
ContainerImage	303
ContainerImageHash	303
ContainerMemory	303

ContainerNetwork	304
ContainerNetworkEgress	304
ContainerNetworkIngress	304
Content	304
Contentgroup	305
CountRange	305
CreateAcceptedDomainRequest	306
CreateGroupRequest	306
DataStream	306
DateFilterModel	307
DateSelectionMode	307
Destination	308
DestinationNat	309
Dll	310
Dns	310
DnsQuestion	311
Ecs	312
Elf	312
ElfHeader	314
ElfSections	315
ElfSegments	316
Email	316
EmailAttachments	318
EmailAttachmentsFile	318
EmailBcc	319
EmailCc	319
EmailFrom	319
EmailReplyTo	319
EmailSender	320
EmailTo	320
EndpointInformationModel	320
EpmEcsEvent	323
EpmEcsEventResponseModel	328

EpmEcsEventSpan	329
EpmEcsEventTrace	329
EpmEcsEventTransaction	329
Epmwinmac	329
Error	331
Event	332
Faas	332
FaasTrigger	333
File	333
Geo	337
GeoPoint	339
Gpo	339
Group	340
GroupDataAuditingDetailModel	340
GroupListItemModel	341
GroupListItemModelPagedResponse	343
Hash	344
Host	345
HostBoot	347
HostCpu	348
HostDisk	348
HostDiskRead	348
HostDiskWrite	348
HostNetwork	349
HostNetworkEgress	349
HostNetworkIngress	349
Http	350
HttpRequest	350
HttpRequestBody	351
HttpResponse	351
HttpResponseBody	352
InstallationKeyDataAuditingDetailModel	352
Installer	353

ListItemErrorInfoModel	353
Log	354
LogFile	355
LogOrigin	355
LogOriginFile	355
MMCRemoteClientDataAuditingDetailModel	355
ManagementRuleDataAuditingDetailModel	356
Message	356
ModifyAcceptedDomainRequest	357
ModifyGroupRequest	358
ModifyPolicyRequest	358
ModifyUserPreferencesRequest	359
ModifyUserRequest	359
Network	360
OS	361
Observer	361
OpenIdConfigDataAuditingDetailModel	363
OperationValue	364
Operator	365
Orchestrator	365
OrchestratorCluster	366
OrchestratorResource	367
OrchestratorResourceParent	367
Organization	368
Os	368
Owner	369
Package	370
Pe	371
PolicyDataAuditingDetailModel	372
PolicyGroupsListItemModel	373
PolicyListItemModel	374
PolicyListItemModelPagedResponse	376
PolicyRevisionDataAuditingDetailModel	377

PolicyRevisionModel	377
PolicyRevisionState	378
Privilegedgroup	378
ProblemDetails	379
Process	379
ProcessEntryLeader	384
ProcessEntryMeta	388
ProcessGroupLeader	388
ProcessParent	392
ProcessPrevious	396
ProcessSessionLeader	399
ProcessThread	403
Registry	404
RegistryData	404
Related	405
Remotepowershell	405
ReputationSettingsDataAuditingDetailModel	406
RoleElement	406
RoleItemModel	407
RoleListItemModel	407
RoleModel	408
RolePermissionModel	408
RoleResourceModel	409
Rule	409
Rulescript	410
RulescriptOutcome	410
SCIMEmail	411
SCIMUserName	411
ScimAuthenticationSchemes	412
ScimBulk	412
ScimOperation	413
ScimResourceMeta	413
ScimResourceResponse	414

ScimResourceResponseScimListResponse	414
ScimSchemaResponse	415
ScimSchemaResponseScimListResponse	416
ScimServiceProviderConfigResponse	417
ScimSupported	418
ScimUserMetaModel	418
ScimUserModel	418
ScimUserModelScimListResponse	420
ScimUserPatchRequest	421
SecuritySettingsDataAuditingDetailModel	421
Server	422
ServerNat	423
Service	424
ServiceNode	425
ServiceOrigin	425
ServiceTarget	426
Servicecontrol	427
ServicecontrolService	428
Session	428
SettingDataAuditingDetailModel	429
SiemIntegrationBaseDetailModel	429
SiemIntegrationQradarAuditingDetailModel	430
SiemIntegrationS3AuditingDetailModel	431
SiemIntegrationSentinelAuditingDetailModel	432
SiemIntegrationSplunkAuditingDetailModel	432
SortDirection	433
SortModel	433
Source	434
SourceNat	435
Storeapp	436
SubAttribute	436
TaskDetailModel	437
Threat	439

ThreatEnrichments	440
ThreatEnrichmentsMatched	440
ThreatFeed	441
ThreatGroup	441
ThreatIndicator	442
ThreatIndicatorEmail	444
ThreatIndicatorMarking	445
ThreatSoftware	445
ThreatTactic	446
ThreatTechnique	446
ThreatTechniqueSubtechnique	447
Tls	447
TlsClient	448
TlsClientHash	450
TlsServer	450
TlsServerHash	451
Token	452
Trustedapplication	452
UnassignComputersToGroupRequest	452
Url	453
User	455
UserAgent	457
UserAgentDevice	457
UserChanges	458
UserDataAuditing	459
UserDetailModel	461
UserEffective	462
UserListItemModel	464
UserListItemModelPagedResponse	465
UserRoleResourceItemModel	466
UserTarget	467
V2CreateUserRequest	469
Vlan	470

Vulnerability	470
VulnerabilityScanner	472
VulnerabilityScore	472
Workstyle	472
X509	473
X509Issuer	474
X509Subject	475
_event	476
_rule	479
id_AssignComputersByCsv_body	480
id_Upload_body	481
v2_Policies_body	481

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.

i For more information about creating an API account, please see [Configure Access to the Management API](#) 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. Replace *example* with the name of your PM Cloud instance in the following URL to access the docs: (<https://<example-services.epm.btrusteng.com/management-api>/swagger>).

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](https://swagger.io/tools/swagger-ui/) at <https://swagger.io/tools/swagger-ui/>.

Methods

[[Jump to Models](#)]

Table of Contents

About

- [get /v2/About](#)

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}](#)

ApiAccounts

- [get /v2/ApiAccounts](#)

AuthenticationProvider

- [get /v2/AuthenticationProvider](#)

AuthorizationRequestAudits

- [get /v2/AuthorizationRequestAudits](#)
- [get /v2/AuthorizationRequestAudits/{id}](#)

Computers

- [post /v2/Computers/archive](#)
- [post /v2/Computers/Authorise](#)

- [post /v2/Computers/Certificate/Renew](#)
- [post /v2/Computers/{computerId}/archive](#)
- [post /v2/Computers/{computerId}/Unarchive](#)
- [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](#)
- [post /v2/Computers/Unarchive](#)

Events

- [get /v2/Events/FromStartDate](#)
- [get /v2/Events/search](#)

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](#)

About

`get /v2/About`

Retrieve version (v2AboutGet)

Return type

array[[AboutModel](#)]

Example data

Content-Type: application/json

```
[ {
  "consoleVersion" : "consoleVersion",
  "policyEditorVersion" : "policyEditorVersion",
  "reportingDatabaseVersion" : "reportingDatabaseVersion"
}, {
  "consoleVersion" : "consoleVersion",
  "policyEditorVersion" : "policyEditorVersion",
  "reportingDatabaseVersion" : "reportingDatabaseVersion"
} ]
```

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

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**

409Conflict **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 — Allow for sorting on multiple properties using "by" and "order". "Sorts[x].by" specifies the property on which to sort e.g. name. "Sorts[x].order" specifies the order in which to sort e.g. asc or desc. The index "x" specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example Sorts[0].by, Sorts[0].order, Sorts[1].by, Sorts[1].order.

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"
      }
    },
    "azureADIntegrationDataAuditing" : {
      "oldAzureAdClientSecret" : "oldAzureAdClientSecret",
      "azureAdTenantId" : "azureAdTenantId",
      "azureAdIntegrationEnabled" : true,
      "azureAdConfigChanged" : true,
      "oldAzureAdIntegrationEnabled" : true,
      "azureAdClientSecret" : "azureAdClientSecret",
      "oldAzureAdUseCertificateAuth" : true,
      "azureAdClientId" : "azureAdClientId",
      "oldAzureAdClientId" : "oldAzureAdClientId",
      "oldAzureAdTenantId" : "oldAzureAdTenantId",
      "azureAdUseCertificateAuth" : true
    },
    "disableSiemIntegrationDataAuditing" : {
      "siemIntegrationEnabled" : true,
      "siemFormat" : "siemFormat",
      "siemIntegrationType" : "siemIntegrationType"
    },
    "siemIntegrationS3Auditing" : {
      "siemRegionName" : "siemRegionName",
      "siemIntegrationEnabled" : true,
      "siemAccessKeyId" : "siemAccessKeyId",
      "siemFormat" : "siemFormat",
      "siemBucketName" : "siemBucketName",

```

```
    "siemCodec" : "siemCodec",
    "siemSseEnabled" : true,
    "siemIntegrationType" : "siemIntegrationType"
  },
  "agentDataAuditing" : {
    "oldTimestamp" : "2000-01-23T04:56:07.000+00:00",
    "newOsName" : "newOsName",
    "oldComputerGroupName" : "oldComputerGroupName",
    "oldAdapterVersion" : "oldAdapterVersion",
    "oldOsName" : "oldOsName",
    "newAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "newAdapterVersion" : "newAdapterVersion",
    "newTimestamp" : "2000-01-23T04:56:07.000+00:00",
    "oldHostType" : "oldHostType",
    "newComputerGroupName" : "newComputerGroupName",
    "newHostType" : "newHostType",
    "newComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "oldAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "oldComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
  },
  "policyDataAuditing" : {
    "oldDescription" : "oldDescription",
    "newName" : "newName",
    "oldName" : "oldName",
    "newDescription" : "newDescription"
  },
  "auditType" : "auditType",
  "authorizationRequestDataAuditing" : {
    "oldAuthRequestApiClientSecret" : "oldAuthRequestApiClientSecret",
    "authRequestPassword" : "authRequestPassword",
    "oldAuthRequestHostName" : "oldAuthRequestHostName",
    "oldAuthRequestClientId" : "oldAuthRequestClientId",
    "authRequestUserName" : "authRequestUserName",
    "oldAuthRequestPassword" : "oldAuthRequestPassword",
    "oldAuthRequestApiClientId" : "oldAuthRequestApiClientId",
    "authRequestApiClientSecret" : "authRequestApiClientSecret",
    "authRequestApiClientId" : "authRequestApiClientId",
    "oldAuthRequestUserName" : "oldAuthRequestUserName",
    "authRequestClientId" : "authRequestClientId",
    "authRequestConfigChanged" : true,
    "oldAuthRequestIntegrationEnabled" : true,
    "authRequestIntegrationEnabled" : true,
    "authRequestHostName" : "authRequestHostName",
    "oldAuthRequestClientSecret" : "oldAuthRequestClientSecret",
    "authRequestClientSecret" : "authRequestClientSecret"
  },
  "installationKeyDataAuditing" : {
    "newDisabled" : true,
    "oldDisabled" : true,
    "deleted" : true,
    "newLabel" : "newLabel",
    "oldLabel" : "oldLabel"
  }
},
```

```
"changedBy" : "API",
"siemIntegrationQradarAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,
  "port" : "port",
  "siemFormat" : "siemFormat",
  "cert" : "cert",
  "siemIntegrationType" : "siemIntegrationType"
},
"details" : "details",
"id" : 5,
"siemIntegrationSentinelAuditing" : {
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "siemIntegrationType" : "siemIntegrationType",
  "tableName" : "tableName",
  "workspaceId" : "workspaceId"
},
"managementRuleDataAuditing" : {
  "newPriority" : 7,
  "oldPriority" : 1
},
"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",
"policyRevisionDataAuditing" : {
  "newGroups" : {
    "key" : "newGroups"
  },
  "newAnnotationNote" : "newAnnotationNote"
},
"userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"siemIntegrationSplunkAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,
```

```
    "siemFormat" : "siemFormat",
    "index" : "index",
    "siemIntegrationType" : "siemIntegrationType"
  },
  "securitySettingsDataAuditing" : {
    "tokenTimeout" : 2,
    "oldTokenTimeout" : 4
  },
  "computerPolicyDataAuditing" : {
    "deactivatedAgentDeletionDays" : 3,
    "oldEnableDeactivatedAgentDeletion" : true,
    "oldDeactivatedAgentDeletionDays" : 7,
    "inactivityAgentDeactivationDays" : 9,
    "oldInactivityAgentDeactivationDays" : 2,
    "enableDeactivatedAgentDeletion" : true
  },
  "reputationSettingsDataAuditing" : {
    "reputationConfigChanged" : true,
    "oldReputationIntegrationApiKey" : "oldReputationIntegrationApiKey",
    "oldReputationIntegrationEnabled" : true,
    "reputationIntegrationApiKey" : "reputationIntegrationApiKey",
    "reputationIntegrationEnabled" : true
  },
  "settingsDataAuditing" : {
    "modifyDomainOldValue" : "modifyDomainOldValue",
    "modifyDomainNewValue" : "modifyDomainNewValue",
    "removeDomain" : "removeDomain",
    "addDomain" : "addDomain"
  },
  "apiClientDataAuditing" : {
    "oldDescription" : "oldDescription",
    "newName" : "newName",
    "deleted" : true,
    "secretUpdated" : true,
    "oldName" : "oldName",
    "newDescription" : "newDescription"
  },
  "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"
  },
  "openIdConfigDataAuditing" : {
    "secretUpdated" : true,
    "oldOpenIDConnectProvider" : "oldOpenIDConnectProvider",
    "newAuthenticationType" : "newAuthenticationType",
    "newDomain" : "newDomain",
    "oldDomain" : "oldDomain",
    "newClientId" : "newClientId",
    "newOpenIDConnectProvider" : "newOpenIDConnectProvider",
    "oldAuthenticationType" : "oldAuthenticationType",
    "oldClientId" : "oldClientId"
  },
  "mmcRemoteClientDataAuditing" : {
    "clientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "oldClientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "enabled" : true,
    "oldEnabled" : true
  },
  "user" : "user",
  "entity" : "entity"
}, {
  "computerDataAuditing" : {
    "deactivatedAgents" : {
      "key" : "deactivatedAgents"
    },
    "newDeletedAgents" : [ "newDeletedAgents", "newDeletedAgents" ],
    "updatedPoliciesOn" : {
      "key" : "updatedPoliciesOn"
    }
  }
},
"azureADIntegrationDataAuditing" : {
```

```
"oldAzureAdClientSecret" : "oldAzureAdClientSecret",
"azureAdTenantId" : "azureAdTenantId",
"azureAdIntegrationEnabled" : true,
"azureAdConfigChanged" : true,
"oldAzureAdIntegrationEnabled" : true,
"azureAdClientSecret" : "azureAdClientSecret",
"oldAzureAdUseCertificateAuth" : true,
"azureAdClientId" : "azureAdClientId",
"oldAzureAdClientId" : "oldAzureAdClientId",
"oldAzureAdTenantId" : "oldAzureAdTenantId",
"azureAdUseCertificateAuth" : true
},
"disableSiemIntegrationDataAuditing" : {
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "siemIntegrationType" : "siemIntegrationType"
},
"siemIntegrationS3Auditing" : {
  "siemRegionName" : "siemRegionName",
  "siemIntegrationEnabled" : true,
  "siemAccessKeyId" : "siemAccessKeyId",
  "siemFormat" : "siemFormat",
  "siemBucketName" : "siemBucketName",
  "siemCodec" : "siemCodec",
  "siemSseEnabled" : true,
  "siemIntegrationType" : "siemIntegrationType"
},
"agentDataAuditing" : {
  "oldTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "newOsName" : "newOsName",
  "oldComputerGroupName" : "oldComputerGroupName",
  "oldAdapterVersion" : "oldAdapterVersion",
  "oldOsName" : "oldOsName",
  "newAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "newAdapterVersion" : "newAdapterVersion",
  "newTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "oldHostType" : "oldHostType",
  "newComputerGroupName" : "newComputerGroupName",
  "newHostType" : "newHostType",
  "newComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
},
"policyDataAuditing" : {
  "oldDescription" : "oldDescription",
  "newName" : "newName",
  "oldName" : "oldName",
  "newDescription" : "newDescription"
},
"auditType" : "auditType",
"authorizationRequestDataAuditing" : {
  "oldAuthRequestApiClientSecret" : "oldAuthRequestApiClientSecret",
  "authRequestPassword" : "authRequestPassword",
```



```
"oldAuthRequestHostName" : "oldAuthRequestHostName",
"oldAuthRequestClientId" : "oldAuthRequestClientId",
"authRequestUserName" : "authRequestUserName",
"oldAuthRequestPassword" : "oldAuthRequestPassword",
"oldAuthRequestApiClientId" : "oldAuthRequestApiClientId",
"authRequestApiClientSecret" : "authRequestApiClientSecret",
"authRequestApiClientId" : "authRequestApiClientId",
"oldAuthRequestUserName" : "oldAuthRequestUserName",
"authRequestClientId" : "authRequestClientId",
"authRequestConfigChanged" : true,
"oldAuthRequestIntegrationEnabled" : true,
"authRequestIntegrationEnabled" : true,
"authRequestHostName" : "authRequestHostName",
"oldAuthRequestClientSecret" : "oldAuthRequestClientSecret",
"authRequestClientSecret" : "authRequestClientSecret"
},
"installationKeyDataAuditing" : {
  "newDisabled" : true,
  "oldDisabled" : true,
  "deleted" : true,
  "newLabel" : "newLabel",
  "oldLabel" : "oldLabel"
},
"changedBy" : "API",
"siemIntegrationQradarAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,
  "port" : "port",
  "siemFormat" : "siemFormat",
  "cert" : "cert",
  "siemIntegrationType" : "siemIntegrationType"
},
"details" : "details",
"id" : 5,
"siemIntegrationSentinelAuditing" : {
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "siemIntegrationType" : "siemIntegrationType",
  "tableName" : "tableName",
  "workspaceId" : "workspaceId"
},
"managementRuleDataAuditing" : {
  "newPriority" : 7,
  "oldPriority" : 1
},
"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",
  "policyRevisionDataAuditing" : {
    "newGroups" : {
      "key" : "newGroups"
    },
    "newAnnotationNote" : "newAnnotationNote"
  },
  "userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "siemIntegrationSplunkAuditing" : {
    "hostName" : "hostName",
    "siemIntegrationEnabled" : true,
    "siemFormat" : "siemFormat",
    "index" : "index",
    "siemIntegrationType" : "siemIntegrationType"
  },
  "securitySettingsDataAuditing" : {
    "tokenTimeout" : 2,
    "oldTokenTimeout" : 4
  },
  "computerPolicyDataAuditing" : {
    "deactivatedAgentDeletionDays" : 3,
    "oldEnableDeactivatedAgentDeletion" : true,
    "oldDeactivatedAgentDeletionDays" : 7,
    "inactivityAgentDeactivationDays" : 9,
    "oldInactivityAgentDeactivationDays" : 2,
    "enableDeactivatedAgentDeletion" : true
  },
  "reputationSettingsDataAuditing" : {
    "reputationConfigChanged" : true,
    "oldReputationIntegrationApiKey" : "oldReputationIntegrationApiKey",
    "oldReputationIntegrationEnabled" : true,
    "reputationIntegrationApiKey" : "reputationIntegrationApiKey",
    "reputationIntegrationEnabled" : true
  },
  "settingsDataAuditing" : {
    "modifyDomainOldValue" : "modifyDomainOldValue",
    "modifyDomainNewValue" : "modifyDomainNewValue",
    "removeDomain" : "removeDomain",
    "addDomain" : "addDomain"
  },
  "apiClientDataAuditing" : {
```

```
"oldDescription" : "oldDescription",
"newName" : "newName",
"deleted" : true,
"secretUpdated" : true,
"oldName" : "oldName",
"newDescription" : "newDescription"
},
"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"
},
"openIdConfigDataAuditing" : {
  "secretUpdated" : true,
  "oldOpenIDConnectProvider" : "oldOpenIDConnectProvider",
  "newAuthenticationType" : "newAuthenticationType",
  "newDomain" : "newDomain",
  "oldDomain" : "oldDomain",
  "newClientId" : "newClientId",
```

```
    "newOpenIDConnectProvider" : "newOpenIDConnectProvider",
    "oldAuthenticationType" : "oldAuthenticationType",
    "oldClientId" : "oldClientId"
  },
  "mmcRemoteClientDataAuditing" : {
    "clientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "oldClientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "enabled" : true,
    "oldEnabled" : 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 **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 — Allow for sorting on multiple properties using `"by"` and `"order"`. `"Sorts[x].by"` specifies the property on which to sort e.g. `name`. `"Sorts[x].order"` specifies the order in which to sort e.g. `asc` or `desc`. The index `"x"` specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example `Sorts[0].by`, `Sorts[0].order`, `Sorts[1].by`, `Sorts[1].order`.

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

[ActivityAuditDetailModelPagedResponse](#)

Example data

Content-Type: application/json

```
{
  "pageCount" : 5,
  "pageNumber" : 0,
  "data" : [ {
    "computerDataAuditing" : {
      "deactivatedAgents" : {
        "key" : "deactivatedAgents"
      },
      "newDeletedAgents" : [ "newDeletedAgents", "newDeletedAgents" ],
      "updatedPoliciesOn" : {
        "key" : "updatedPoliciesOn"
      }
    },
    "azureADIntegrationDataAuditing" : {
      "oldAzureAdClientSecret" : "oldAzureAdClientSecret",
      "azureAdTenantId" : "azureAdTenantId",
      "azureAdIntegrationEnabled" : true,
      "azureAdConfigChanged" : true,
      "oldAzureAdIntegrationEnabled" : true,
      "azureAdClientSecret" : "azureAdClientSecret",
      "oldAzureAdUseCertificateAuth" : true,
      "azureAdClientId" : "azureAdClientId",
      "oldAzureAdClientId" : "oldAzureAdClientId",
      "oldAzureAdTenantId" : "oldAzureAdTenantId",
      "azureAdUseCertificateAuth" : true
    },
    "disableSiemIntegrationDataAuditing" : {
      "siemIntegrationEnabled" : true,
      "siemFormat" : "siemFormat",
      "siemIntegrationType" : "siemIntegrationType"
    },
    "siemIntegrationS3Auditing" : {
      "siemRegionName" : "siemRegionName",
      "siemIntegrationEnabled" : true,
      "siemAccessKeyId" : "siemAccessKeyId",
      "siemFormat" : "siemFormat",
      "siemBucketName" : "siemBucketName",
      "siemCodec" : "siemCodec",
      "siemSseEnabled" : true,
      "siemIntegrationType" : "siemIntegrationType"
    }
  },
  ],
}
```



```
"agentDataAuditing" : {
  "oldTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "newOsName" : "newOsName",
  "oldComputerGroupName" : "oldComputerGroupName",
  "oldAdapterVersion" : "oldAdapterVersion",
  "oldOsName" : "oldOsName",
  "newAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "newAdapterVersion" : "newAdapterVersion",
  "newTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "oldHostType" : "oldHostType",
  "newComputerGroupName" : "newComputerGroupName",
  "newHostType" : "newHostType",
  "newComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
},
"policyDataAuditing" : {
  "oldDescription" : "oldDescription",
  "newName" : "newName",
  "oldName" : "oldName",
  "newDescription" : "newDescription"
},
"auditType" : "auditType",
"authorizationRequestDataAuditing" : {
  "oldAuthRequestApiClientSecret" : "oldAuthRequestApiClientSecret",
  "authRequestPassword" : "authRequestPassword",
  "oldAuthRequestHostName" : "oldAuthRequestHostName",
  "oldAuthRequestClientId" : "oldAuthRequestClientId",
  "authRequestUserName" : "authRequestUserName",
  "oldAuthRequestPassword" : "oldAuthRequestPassword",
  "oldAuthRequestApiClientId" : "oldAuthRequestApiClientId",
  "authRequestApiClientSecret" : "authRequestApiClientSecret",
  "authRequestApiClientId" : "authRequestApiClientId",
  "oldAuthRequestUserName" : "oldAuthRequestUserName",
  "authRequestClientId" : "authRequestClientId",
  "authRequestConfigChanged" : true,
  "oldAuthRequestIntegrationEnabled" : true,
  "authRequestIntegrationEnabled" : true,
  "authRequestHostName" : "authRequestHostName",
  "oldAuthRequestClientSecret" : "oldAuthRequestClientSecret",
  "authRequestClientSecret" : "authRequestClientSecret"
},
"installationKeyDataAuditing" : {
  "newDisabled" : true,
  "oldDisabled" : true,
  "deleted" : true,
  "newLabel" : "newLabel",
  "oldLabel" : "oldLabel"
},
"changedBy" : "API",
"siemIntegrationQradarAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,

```

```
    "port" : "port",
    "siemFormat" : "siemFormat",
    "cert" : "cert",
    "siemIntegrationType" : "siemIntegrationType"
  },
  "details" : "details",
  "id" : 5,
  "siemIntegrationSentinelAuditing" : {
    "siemIntegrationEnabled" : true,
    "siemFormat" : "siemFormat",
    "siemIntegrationType" : "siemIntegrationType",
    "tableName" : "tableName",
    "workspaceId" : "workspaceId"
  },
  "managementRuleDataAuditing" : {
    "newPriority" : 7,
    "oldPriority" : 1
  },
  "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",
  "policyRevisionDataAuditing" : {
    "newGroups" : {
      "key" : "newGroups"
    },
    "newAnnotationNote" : "newAnnotationNote"
  },
  "userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "siemIntegrationSplunkAuditing" : {
    "hostName" : "hostName",
    "siemIntegrationEnabled" : true,
    "siemFormat" : "siemFormat",
    "index" : "index",
    "siemIntegrationType" : "siemIntegrationType"
  },
}
```

```
"securitySettingsDataAuditing" : {
  "tokenTimeout" : 2,
  "oldTokenTimeout" : 4
},
"computerPolicyDataAuditing" : {
  "deactivatedAgentDeletionDays" : 3,
  "oldEnableDeactivatedAgentDeletion" : true,
  "oldDeactivatedAgentDeletionDays" : 7,
  "inactivityAgentDeactivationDays" : 9,
  "oldInactivityAgentDeactivationDays" : 2,
  "enableDeactivatedAgentDeletion" : true
},
"reputationSettingsDataAuditing" : {
  "reputationConfigChanged" : true,
  "oldReputationIntegrationApiKey" : "oldReputationIntegrationApiKey",
  "oldReputationIntegrationEnabled" : true,
  "reputationIntegrationApiKey" : "reputationIntegrationApiKey",
  "reputationIntegrationEnabled" : true
},
"settingsDataAuditing" : {
  "modifyDomainOldValue" : "modifyDomainOldValue",
  "modifyDomainNewValue" : "modifyDomainNewValue",
  "removeDomain" : "removeDomain",
  "addDomain" : "addDomain"
},
"apiClientDataAuditing" : {
  "oldDescription" : "oldDescription",
  "newName" : "newName",
  "deleted" : true,
  "secretUpdated" : true,
  "oldName" : "oldName",
  "newDescription" : "newDescription"
},
"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"
},
"openIdConfigDataAuditing" : {
  "secretUpdated" : true,
  "oldOpenIDConnectProvider" : "oldOpenIDConnectProvider",
  "newAuthenticationType" : "newAuthenticationType",
  "newDomain" : "newDomain",
  "oldDomain" : "oldDomain",
  "newClientId" : "newClientId",
  "newOpenIDConnectProvider" : "newOpenIDConnectProvider",
  "oldAuthenticationType" : "oldAuthenticationType",
  "oldClientId" : "oldClientId"
},
"mmcRemoteClientDataAuditing" : {
  "clientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldClientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "enabled" : true,
  "oldEnabled" : true
},
"user" : "user",
"entity" : "entity"
}, {
  "computerDataAuditing" : {
    "deactivatedAgents" : {
      "key" : "deactivatedAgents"
    },
    "newDeletedAgents" : [ "newDeletedAgents", "newDeletedAgents" ],
    "updatedPoliciesOn" : {
      "key" : "updatedPoliciesOn"
    }
  },
  "azureADIntegrationDataAuditing" : {
    "oldAzureAdClientSecret" : "oldAzureAdClientSecret",
    "azureAdTenantId" : "azureAdTenantId",
    "azureAdIntegrationEnabled" : true,
    "azureAdConfigChanged" : true,
```

```
"oldAzureAdIntegrationEnabled" : true,
"azureAdClientSecret" : "azureAdClientSecret",
"oldAzureAdUseCertificateAuth" : true,
"azureAdClientId" : "azureAdClientId",
"oldAzureAdClientId" : "oldAzureAdClientId",
"oldAzureAdTenantId" : "oldAzureAdTenantId",
"azureAdUseCertificateAuth" : true
},
"disableSiemIntegrationDataAuditing" : {
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "siemIntegrationType" : "siemIntegrationType"
},
"siemIntegrationS3Auditing" : {
  "siemRegionName" : "siemRegionName",
  "siemIntegrationEnabled" : true,
  "siemAccessKeyId" : "siemAccessKeyId",
  "siemFormat" : "siemFormat",
  "siemBucketName" : "siemBucketName",
  "siemCodec" : "siemCodec",
  "siemSseEnabled" : true,
  "siemIntegrationType" : "siemIntegrationType"
},
"agentDataAuditing" : {
  "oldTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "newOsName" : "newOsName",
  "oldComputerGroupName" : "oldComputerGroupName",
  "oldAdapterVersion" : "oldAdapterVersion",
  "oldOsName" : "oldOsName",
  "newAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "newAdapterVersion" : "newAdapterVersion",
  "newTimestamp" : "2000-01-23T04:56:07.000+00:00",
  "oldHostType" : "oldHostType",
  "newComputerGroupName" : "newComputerGroupName",
  "newHostType" : "newHostType",
  "newComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldAgentId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "oldComputerGroupId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
},
"policyDataAuditing" : {
  "oldDescription" : "oldDescription",
  "newName" : "newName",
  "oldName" : "oldName",
  "newDescription" : "newDescription"
},
"auditType" : "auditType",
"authorizationRequestDataAuditing" : {
  "oldAuthRequestApiClientSecret" : "oldAuthRequestApiClientSecret",
  "authRequestPassword" : "authRequestPassword",
  "oldAuthRequestHostName" : "oldAuthRequestHostName",
  "oldAuthRequestClientId" : "oldAuthRequestClientId",
  "authRequestUserName" : "authRequestUserName",
  "oldAuthRequestPassword" : "oldAuthRequestPassword",
```

```
"oldAuthRequestApiClientId" : "oldAuthRequestApiClientId",
"authRequestApiClientSecret" : "authRequestApiClientSecret",
"authRequestApiClientId" : "authRequestApiClientId",
"oldAuthRequestUserName" : "oldAuthRequestUserName",
"authRequestClientId" : "authRequestClientId",
"authRequestConfigChanged" : true,
"oldAuthRequestIntegrationEnabled" : true,
"authRequestIntegrationEnabled" : true,
"authRequestHostName" : "authRequestHostName",
"oldAuthRequestClientSecret" : "oldAuthRequestClientSecret",
"authRequestClientSecret" : "authRequestClientSecret"
},
"installationKeyDataAuditing" : {
  "newDisabled" : true,
  "oldDisabled" : true,
  "deleted" : true,
  "newLabel" : "newLabel",
  "oldLabel" : "oldLabel"
},
"changedBy" : "API",
"siemIntegrationQradarAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,
  "port" : "port",
  "siemFormat" : "siemFormat",
  "cert" : "cert",
  "siemIntegrationType" : "siemIntegrationType"
},
"details" : "details",
"id" : 5,
"siemIntegrationSentinelAuditing" : {
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "siemIntegrationType" : "siemIntegrationType",
  "tableName" : "tableName",
  "workspaceId" : "workspaceId"
},
"managementRuleDataAuditing" : {
  "newPriority" : 7,
  "oldPriority" : 1
},
"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",
  "policyRevisionDataAuditing" : {
    "newGroups" : {
      "key" : "newGroups"
    }
  },
  "newAnnotationNote" : "newAnnotationNote"
},
"userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"siemIntegrationSplunkAuditing" : {
  "hostName" : "hostName",
  "siemIntegrationEnabled" : true,
  "siemFormat" : "siemFormat",
  "index" : "index",
  "siemIntegrationType" : "siemIntegrationType"
},
"securitySettingsDataAuditing" : {
  "tokenTimeout" : 2,
  "oldTokenTimeout" : 4
},
"computerPolicyDataAuditing" : {
  "deactivatedAgentDeletionDays" : 3,
  "oldEnableDeactivatedAgentDeletion" : true,
  "oldDeactivatedAgentDeletionDays" : 7,
  "inactivityAgentDeactivationDays" : 9,
  "oldInactivityAgentDeactivationDays" : 2,
  "enableDeactivatedAgentDeletion" : true
},
"reputationSettingsDataAuditing" : {
  "reputationConfigChanged" : true,
  "oldReputationIntegrationApiKey" : "oldReputationIntegrationApiKey",
  "oldReputationIntegrationEnabled" : true,
  "reputationIntegrationApiKey" : "reputationIntegrationApiKey",
  "reputationIntegrationEnabled" : true
},
"settingsDataAuditing" : {
  "modifyDomainOldValue" : "modifyDomainOldValue",
  "modifyDomainNewValue" : "modifyDomainNewValue",
  "removeDomain" : "removeDomain",
  "addDomain" : "addDomain"
},
"apiClientDataAuditing" : {
  "oldDescription" : "oldDescription",
  "newName" : "newName",
  "deleted" : true,
  "secretUpdated" : true,
```

```
    "oldName" : "oldName",
    "newDescription" : "newDescription"
  },
  "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"
  },
  "openIdConfigDataAuditing" : {
    "secretUpdated" : true,
    "oldOpenIDConnectProvider" : "oldOpenIDConnectProvider",
    "newAuthenticationType" : "newAuthenticationType",
    "newDomain" : "newDomain",
    "oldDomain" : "oldDomain",
    "newClientId" : "newClientId",
    "newOpenIDConnectProvider" : "newOpenIDConnectProvider",
    "oldAuthenticationType" : "oldAuthenticationType",
    "oldClientId" : "oldClientId"
  }
},
```



```
"mmcRemoteClientDataAuditing" : {  
  "clientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",  
  "oldClientId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",  
  "enabled" : true,  
  "oldEnabled" : 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 **ActivityAuditDetailModelPagedResponse**

401

Unauthorized **ProblemDetails**

404

Not Found **ProblemDetails**

ApiAccounts



`get /v2/ApiAccounts`

Retrieves list of Api Accounts (v2ApiAccountsGet)

Return type

array[[ApiAccountListItemModel](#)]

Example data

Content-Type: application/json

```
[ {
  "auditAccess" : 1,
  "clientId" : "clientId",
  "createdDate" : "2000-01-23T04:56:07.000+00:00",
  "name" : "name",
  "errorInfo" : {
    "userAccountName" : "userAccountName",
    "parentTaskName" : "parentTaskName",
    "initiated" : "2000-01-23T04:56:07.000+00:00",
    "errorCode" : 0,
    "userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
  },
  "description" : "description",
  "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "locked" : true,
  "scimAccess" : 0,
  "reportingAccess" : 6,
  "managementAccess" : 5
}, {
  "auditAccess" : 1,
  "clientId" : "clientId",
  "createdDate" : "2000-01-23T04:56:07.000+00:00",
  "name" : "name",
  "errorInfo" : {
    "userAccountName" : "userAccountName",
    "parentTaskName" : "parentTaskName",
    "initiated" : "2000-01-23T04:56:07.000+00:00",
    "errorCode" : 0,
    "userId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91"
  },
  "description" : "description",
  "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "locked" : true,
  "scimAccess" : 0,
  "reportingAccess" : 6,
  "managementAccess" : 5
} ]
```

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

AuthenticationProvider



```
get /v2/AuthenticationProvider
```

Retrieves a detail of the configured authentication provider (v2AuthenticationProviderGet)

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**

AuthorizationRequestAudits

 `get /v2/AuthorizationRequestAudits`

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

Query parameters

Sorts (optional)

Query Parameter — Allow for sorting on multiple properties using `"by"` and `"order"`. `"Sorts[x].by"` specifies the property on which to sort e.g. name. `"Sorts[x].order"` specifies the order in which to sort e.g. asc or desc. The index `"x"` specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example `Sorts[0].by`, `Sorts[0].order`, `Sorts[1].by`, `Sorts[1].order`.

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

[AuthorizationRequestAuditListItemModelPagedResponse](#)

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",
    "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 **AuthorizationRequestAuditListItemModelPagedResponse**

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

[AuthorizationRequestAuditDetailModelPagedResponse](#)

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",
    "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 **AuthorizationRequestAuditDetailModelPagedResponse**

401Unauthorized **ProblemDetails****403**Forbidden **ProblemDetails****404**Not Found **ProblemDetails**

Computers

 `post /v2/Computers/archive`

Archive Computers (v2ComputersArchivePost)

Consumes

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

- `application/json`
- `text/json`
- `application/*+json`

Request body

body [ComputersArchiveRequest](#) (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

201Created **UUID****400**Bad Request **ProblemDetails****404**Not Found **ProblemDetails****409**Conflict **ProblemDetails****423**Client Error **ProblemDetails****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 bodybody [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/{computerId}/archive
```

Archive Computer (v2ComputersComputerIdArchivePost)

Path parameters

computerId (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

201

Created **UUID**

400

Bad Request **ProblemDetails**

404

Not Found **ProblemDetails**

409

Conflict **ProblemDetails**

423

Client Error **ProblemDetails**



```
post /v2/Computers/{computerId}/Unarchive
```

Unarchive Computer (v2ComputersComputerIdUnarchivePost)

Path parameters

computerId (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

201

Created **UUID**

400

Bad Request **ProblemDetails**

404

Not Found **ProblemDetails**

409

Conflict **ProblemDetails**

423

Client Error **ProblemDetails**



post /v2/Computers/Deactivate

Deactivate Computer functionality no longer exists To mimic the functionality as closely as possible, this will now archive and delete the computer. (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**

423

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**

423

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**

400

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). Sort by Created Date, Ascending to avoid returning duplicate entries. (v2ComputersGet)

Query parameters

Sorts (optional)

Query Parameter — Allow for sorting on multiple properties using `"by"` and `"order"`. `"Sorts[x].by"` specifies the property on which to sort e.g. name. `"Sorts[x].order"` specifies the order in which to sort e.g. asc or desc. The index `"x"` specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example `Sorts[0].by`, `Sorts[0].order`, `Sorts[1].by`, `Sorts[1].order`.

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.PackageManagerVersion (optional)

Query Parameter — The Package Manager version on 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.PolicyId (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

Filter.ConnectionStatus (optional)

Query Parameter — ConnectionStatus

Filter.DaysDisconnected (optional)

Query Parameter — DaysDisconnected format: int32

Filter.DaysSinceArchived (optional)

Query Parameter — DaysSinceArchived format: int32

Return type

[ComputerListItemModelPagedResponse](#)

Example data

Content-Type: application/json

```
{
  "pageCount" : 5,
  "pageNumber" : 0,
  "data" : [ {
    "packageManagerVersion" : "packageManagerVersion",
    "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,
    "authorisedOn" : "2000-01-23T04:56:07.000+00:00",
    "archived" : 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,
    "daysSinceArchived" : 7,
    "os" : "os",
    "policyName" : "policyName",
    "archivedOn" : "2000-01-23T04:56:07.000+00:00",
    "created" : "2000-01-23T04:56:07.000+00:00",
    "pendingDeactivation" : true,
    "duplicate" : true,
    "policyRevisionId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
    "credentialType" : "credentialType",
    "daysDisconnected" : 2,
    "groupName" : "groupName",
    "policyId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
```

```
"duplicateCount" : 5,
"domain" : "domain",
"connectionStatus" : "connectionStatus",
"agentVersion" : "agentVersion",
"policyRevisionStatus" : "policyRevisionStatus",
"policyUpdateTimeStamp" : "2000-01-23T04:56:07.000+00:00"
}, {
  "packageManagerVersion" : "packageManagerVersion",
  "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,
  "authorisedOn" : "2000-01-23T04:56:07.000+00:00",
  "archived" : 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,
  "daysSinceArchived" : 7,
  "os" : "os",
  "policyName" : "policyName",
  "archivedOn" : "2000-01-23T04:56:07.000+00:00",
  "created" : "2000-01-23T04:56:07.000+00:00",
  "pendingDeactivation" : true,
  "duplicate" : true,
  "policyRevisionId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "credentialType" : "credentialType",
  "daysDisconnected" : 2,
  "groupName" : "groupName",
  "policyId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "duplicateCount" : 5,
  "domain" : "domain",
  "connectionStatus" : "connectionStatus",
  "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**

401

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

```
{
  "packageManagerVersion" : "packageManagerVersion",
  "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,
  "authorisedOn" : "2000-01-23T04:56:07.000+00:00",
  "archived" : 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",
  "archivedOn" : "2000-01-23T04:56:07.000+00:00",
  "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",
  "daysDisconnected" : 5,
  "groupName" : "groupName",
  "policyId" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "duplicateCount" : 1,
  "connectionStatus" : "connectionStatus",
  "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**

401

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**

401

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

201

Created **UUID**

404

Not Found **ProblemDetails**

409

Conflict **ProblemDetails**

423

Client Error **ProblemDetails**



`post /v2/Computers/Unarchive`

Unarchive Computers (v2ComputersUnarchivePost)

Consumes

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

- application/json
- text/json
- application/*+json

Request body

body [ComputersUnarchiveRequest](#) (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**

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" ],
      "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"
}
}, {
  "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



```
get /v2/Events/search
```

Gets the list of events by Filters (v2EventsSearchGet)

Query parameters

TimePeriod.StartDate (optional)

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

TimePeriod.EndDate (optional)

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

ComputerGroups (optional)

Query Parameter — The Id of the group(Guid format) format: uuid

OperatingSystem (optional)

Query Parameter — Os name

Events.EventAction (optional)

Query Parameter — The action of the event

Events.EventCode (optional)

Query Parameter — The code of the event

Events.EventType (optional)

Query Parameter — The type of the event

Application.ApplicationType (optional)

Query Parameter — The type of the application

Computers.HostName (optional)

Query Parameter — The host name of the computer

Computers.HostDomain (optional)

Query Parameter — The host domain of the computer

Users.UserName (optional)

Query Parameter — The name of the user

Users.UserDomain (optional)

Query Parameter — The domain of the user

Policies.WorkstyleName (optional)

Query Parameter — The workstyle of the policy

Policies.ApplicationGroupName (optional)

Query Parameter — The application group name of the policy

Policies.OnDemandRule (optional)

Query Parameter — Is on demand rule?

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

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" ],
  "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"
}
}, {
  "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`

```
""
```

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 — Allow for sorting on multiple properties using `"by"` and `"order"`. `"Sorts[x].by"` specifies the property on which to sort e.g. name. `"Sorts[x].order"` specifies the order in which to sort e.g. asc or desc. The index `"x"` specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example `Sorts[0].by`, `Sorts[0].order`, `Sorts[1].by`, `Sorts[1].order`.

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

Filter.Default (optional)

Query Parameter —

Return type

[GroupListItemModelPagedResponse](#)

Example data

Content-Type: application/json

```
{
  "pageCount" : 5,
  "pageNumber" : 0,
  "data" : [ {
    "policyAssigned" : "2000-01-23T04:56:07.000+00:00",
    "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"
}, {
  "policyAssigned" : "2000-01-23T04:56:07.000+00:00",
  "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 —

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**

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

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**



`delete /v2/Groups/{id}`

Deletes group (v2GroupsIdDelete)

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**

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**

404Not 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**

423Client 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 —

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**

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 — Allow for sorting on multiple properties using "by" and "order". "Sorts[x].by" specifies the property on which to sort e.g. name. "Sorts[x].order" specifies the order in which to sort e.g. asc or desc. The index "x" specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example Sorts[0].by, Sorts[0].order, Sorts[1].by, Sorts[1].order.

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"
}, {
  "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**

404Not 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

404Not Found **ProblemDetails****409**Conflict **ProblemDetails**

423Client 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

401Unauthorized **ProblemDetails****404**Not Found **ProblemDetails** `put /v2/Policies/{id}`

Request to update policy properties (v2PoliciesIdPut)

Path parameters

id (required)

Path Parameter — PolicyId 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**

415Client Error **ProblemDetails**

Roles

**get /v2/Roles**

Retrieve list of Roles (v2RolesGet)

Return type

array[[RoleListItemModel](#)]

Example data

Content-Type: application/json

```
[ {
  "name" : "name",
  "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "allowPermissions" : [ {
    "resource" : "resource",
    "action" : "action"
  }, {
    "resource" : "resource",
    "action" : "action"
  } ],
  "denyPermissions" : [ null, null ]
}, {
  "name" : "name",
  "id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
  "allowPermissions" : [ {
    "resource" : "resource",
    "action" : "action"
  }, {
    "resource" : "resource",
    "action" : "action"
  } ],
  "denyPermissions" : [ null, null ]
} ]
```

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



```
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

```
{  
  "name" : "name",  
}
```

```
"id" : "046b6c7f-0b8a-43b9-b35d-6489e6daee91",
"allowPermissions" : [ {
  "resource" : "resource",
  "action" : "action"
}, {
  "resource" : "resource",
  "action" : "action"
} ],
"denyPermissions" : [ null, null ]
}
```

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 **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

Content-Type: application/json

```
{
  "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"
} ]
}
```

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.

- **application/scim+json**

Responses

200Success **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

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

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.

- `application/scim+json`

Responses

200Success **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

Content-Type: application/json

```
{
  "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",
    "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",
    "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"
} ]
}
```

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.

- `application/scim+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

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.

- application/scim+json

Responses

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

Content-Type: application/json

```
{
  "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" : [ "", "" ],
    "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" : [ "", "" ],
    "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"
} ]
}
    
```

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.

- `application/scim+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.

- `application/scim+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

Content-Type: application/json

```
{
  "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"
}
```

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.

- `application/scim+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.

- application/scim+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

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.

- application/scim+json

Responses

200

Success

404


Not Found **ProblemDetails**

409

Conflict **ProblemDetails**

423Client Error **ProblemDetails**

Tasks

 `get /v2/Tasks/{id}`

Retrieves a detail of the Task (v2TaskIdGet)

Path parameters

id (required)

Path Parameter — format: uuid

Return type

[TaskDetailModel](#)

Example data

Content-Type: application/json

```
{
  "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"
}
```

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 **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 — Allow for sorting on multiple properties using `"by"` and `"order"`. `"Sorts[x].by"` specifies the property on which to sort e.g. `name`. `"Sorts[x].order"` specifies the order in which to sort e.g. `asc` or `desc`. The index `"x"` specifies the order the sorts are applied. The index must start at 0 and each index must be consecutive e.g. 0, 1, 2. For example `Sorts[0].by`, `Sorts[0].order`, `Sorts[1].by`, `Sorts[1].order`.

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.RoleId (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

Content-Type: application/json

```
{
  "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
}
```

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 **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

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**

 `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

Content-Type: application/json

```
{
  "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"
}
```

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 **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

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**



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

Resends invitation email to User (v2UsersIdResendInvitePatch)

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**



`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

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**

Models

[[Jump to Methods](#)]

Table of Contents

1. [AboutModel](#)
2. [AcceptedDomainDetailModel](#)
3. [AcceptedDomainListItemModel](#)
4. [Activex](#)
5. [ActivityAuditDetailModel](#)
6. [ActivityAuditDetailModelPagedResponse](#)
7. [ActivityAuditListItemModel](#)
8. [ActivityAuditListItemModelPagedResponse](#)
9. [ActivityAuditRoleNameModel](#)
10. [ActivityAuditRoleResourceModel](#)
11. [Agent](#)
12. [AgentBuild](#)
13. [AgentDataAuditingDetailModel](#)
14. [AgentHostType](#)
15. [ApiAccountListItemModel](#)
16. [ApiClientDataAuditingDetailModel](#)
17. [Application](#)
18. [Applicationgroup](#)
19. [As](#)
20. [AsOrganization](#)
21. [AssignComputersToGroupRequest](#)
22. [AssignPolicyRevisionToGroupRequest](#)
23. [AssignUserToRolesRequest](#)
24. [Attribute](#)
25. [Authentication](#)
26. [Authorization](#)
27. [AuthorizationRequestAuditDetailModel](#)
28. [AuthorizationRequestAuditDetailModelPagedResponse](#)
29. [AuthorizationRequestAuditListItemModel](#)
30. [AuthorizationRequestAuditListItemModelPagedResponse](#)
31. [AuthorizationRequestDataAuditingDetailModel](#)
32. [Authorizationrequest](#)
33. [Authorizinguser](#)
34. [AutoAssignPolicyRevisionToGroupRequest](#)

35. [AzureADIntegrationDataAuditingDetailModel](#)
36. [Bundle](#)
37. [CertificateInformationModel](#)
38. [ChangedBy](#)
39. [Client](#)
40. [ClientNat](#)
41. [Cloud](#)
42. [CloudAccount](#)
43. [CloudInstance](#)
44. [CloudMachine](#)
45. [CloudOrigin](#)
46. [CloudProject](#)
47. [CloudService](#)
48. [CloudTarget](#)
49. [CodeSignature](#)
50. [Com](#)
51. [ComputerDataAuditingDetailModel](#)
52. [ComputerDetailModel](#)
53. [ComputerFilterModel](#)
54. [ComputerListItemModel](#)
55. [ComputerListItemModelPagedResponse](#)
56. [ComputerLogModel](#)
57. [ComputerPolicyDataAuditingDetailModel](#)
58. [ComputerRenewCertificateRequest](#)
59. [ComputerRetrieveLogsRequest](#)
60. [ComputerRetrieveStatusInfoRequest](#)
61. [ComputersArchiveRequest](#)
62. [ComputersAuthoriseRequest](#)
63. [ComputersDeactivateRequest](#)
64. [ComputersRejectRequest](#)
65. [ComputersRemoveRequest](#)
66. [ComputersUnarchiveRequest](#)
67. [Configuration](#)
68. [Container](#)
69. [ContainerCpu](#)
70. [ContainerDisk](#)
71. [ContainerDiskRead](#)
72. [ContainerDiskWrite](#)
73. [ContainerImage](#)
74. [ContainerImageHash](#)

75. [ContainerMemory](#)
76. [ContainerNetwork](#)
77. [ContainerNetworkEgress](#)
78. [ContainerNetworkIngress](#)
79. [Content](#)
80. [Contentgroup](#)
81. [CountRange](#)
82. [CreateAcceptedDomainRequest](#)
83. [CreateGroupRequest](#)
84. [DataStream](#)
85. [DateFilterModel](#)
86. [DateSelectionMode](#)
87. [Destination](#)
88. [DestinationNat](#)
89. [DII](#)
90. [Dns](#)
91. [DnsQuestion](#)
92. [Ecs](#)
93. [Elf](#)
94. [ElfHeader](#)
95. [ElfSections](#)
96. [ElfSegments](#)
97. [Email](#)
98. [EmailAttachments](#)
99. [EmailAttachmentsFile](#)
100. [EmailBcc](#)
101. [EmailCc](#)
102. [EmailFrom](#)
103. [EmailReplyTo](#)
104. [EmailSender](#)
105. [EmailTo](#)
106. [EndpointInformationModel](#)
107. [EpmEcsEvent](#)
108. [EpmEcsEventResponseModel](#)
109. [EpmEcsEventSpan](#)
110. [EpmEcsEventTrace](#)
111. [EpmEcsEventTransaction](#)
112. [Epmwinmac](#)
113. [Error](#)
114. [Event](#)

- 115. [Faas](#)
- 116. [FaasTrigger](#)
- 117. [File](#)
- 118. [Geo](#)
- 119. [GeoPoint](#)
- 120. [Gpo](#)
- 121. [Group](#)
- 122. [GroupDataAuditingDetailModel](#)
- 123. [GroupListItemModel](#)
- 124. [GroupListItemModelPagedResponse](#)
- 125. [Hash](#)
- 126. [Host](#)
- 127. [HostBoot](#)
- 128. [HostCpu](#)
- 129. [HostDisk](#)
- 130. [HostDiskRead](#)
- 131. [HostDiskWrite](#)
- 132. [HostNetwork](#)
- 133. [HostNetworkEgress](#)
- 134. [HostNetworkIngress](#)
- 135. [Http](#)
- 136. [HttpRequest](#)
- 137. [HttpRequestBody](#)
- 138. [HttpResponse](#)
- 139. [HttpResponseBody](#)
- 140. [InstallationKeyDataAuditingDetailModel](#)
- 141. [Installer](#)
- 142. [ListItemErrorInfoModel](#)
- 143. [Log](#)
- 144. [LogFile](#)
- 145. [LogOrigin](#)
- 146. [LogOriginFile](#)
- 147. [MMCRemoteClientDataAuditingDetailModel](#)
- 148. [ManagementRuleDataAuditingDetailModel](#)
- 149. [Message](#)
- 150. [ModifyAcceptedDomainRequest](#)
- 151. [ModifyGroupRequest](#)
- 152. [ModifyPolicyRequest](#)
- 153. [ModifyUserPreferencesRequest](#)
- 154. [ModifyUserRequest](#)

- 155. [Network](#)
- 156. [OS](#)
- 157. [Observer](#)
- 158. [OpenIdConfigDataAuditingDetailModel](#)
- 159. [OperationValue](#)
- 160. [Operator](#)
- 161. [Orchestrator](#)
- 162. [OrchestratorCluster](#)
- 163. [OrchestratorResource](#)
- 164. [OrchestratorResourceParent](#)
- 165. [Organization](#)
- 166. [Os](#)
- 167. [Owner](#)
- 168. [Package](#)
- 169. [Pe](#)
- 170. [PolicyDataAudtingDetailModel](#)
- 171. [PolicyGroupsListItemModel](#)
- 172. [PolicyListItemModel](#)
- 173. [PolicyListItemModelPagedResponse](#)
- 174. [PolicyRevisionDataAuditingDetailModel](#)
- 175. [PolicyRevisionModel](#)
- 176. [PolicyRevisionState](#)
- 177. [Privilegedgroup](#)
- 178. [ProblemDetails](#)
- 179. [Process](#)
- 180. [ProcessEntryLeader](#)
- 181. [ProcessEntryMeta](#)
- 182. [ProcessGroupLeader](#)
- 183. [ProcessParent](#)
- 184. [ProcessPrevious](#)
- 185. [ProcessSessionLeader](#)
- 186. [ProcessThread](#)
- 187. [Registry](#)
- 188. [RegistryData](#)
- 189. [Related](#)
- 190. [Remotepowershell](#)
- 191. [ReputationSettingsDataAuditingDetailModel](#)
- 192. [RoleElement](#)
- 193. [RoleItemModel](#)
- 194. [RoleListItemModel](#)

- 195. [RoleModel](#)
- 196. [RolePermissionModel](#)
- 197. [RoleResourceModel](#)
- 198. [Rule](#)
- 199. [Rulescript](#)
- 200. [RulescriptOutcome](#)
- 201. [SCIMEmail](#)
- 202. [SCIMUserName](#)
- 203. [ScimAuthenticationSchemes](#)
- 204. [ScimBulk](#)
- 205. [ScimOperation](#)
- 206. [ScimResourceMeta](#)
- 207. [ScimResourceResponse](#)
- 208. [ScimResourceResponseScimListResponse](#)
- 209. [ScimSchemaResponse](#)
- 210. [ScimSchemaResponseScimListResponse](#)
- 211. [ScimServiceProviderConfigResponse](#)
- 212. [ScimSupported](#)
- 213. [ScimUserMetaModel](#)
- 214. [ScimUserModel](#)
- 215. [ScimUserModelScimListResponse](#)
- 216. [ScimUserPatchRequest](#)
- 217. [SecuritySettingsDataAuditingDetailModel](#)
- 218. [Server](#)
- 219. [ServerNat](#)
- 220. [Service](#)
- 221. [ServiceNode](#)
- 222. [ServiceOrigin](#)
- 223. [ServiceTarget](#)
- 224. [Servicecontrol](#)
- 225. [ServicecontrolService](#)
- 226. [Session](#)
- 227. [SettingDataAuditingDetailModel](#)
- 228. [SiemIntegrationBaseDetailModel](#)
- 229. [SiemIntegrationQradarAuditingDetailModel](#)
- 230. [SiemIntegrationS3AuditingDetailModel](#)
- 231. [SiemIntegrationSentinelAuditingDetailModel](#)
- 232. [SiemIntegrationSplunkAuditingDetailModel](#)
- 233. [SortDirection](#)
- 234. [SortModel](#)

- 235. [Source](#)
- 236. [SourceNat](#)
- 237. [Storeapp](#)
- 238. [SubAttribute](#)
- 239. [TaskDetailModel](#)
- 240. [Threat](#)
- 241. [ThreatEnrichments](#)
- 242. [ThreatEnrichmentsMatched](#)
- 243. [ThreatFeed](#)
- 244. [ThreatGroup](#)
- 245. [ThreatIndicator](#)
- 246. [ThreatIndicatorEmail](#)
- 247. [ThreatIndicatorMarking](#)
- 248. [ThreatSoftware](#)
- 249. [ThreatTactic](#)
- 250. [ThreatTechnique](#)
- 251. [ThreatTechniqueSubtechnique](#)
- 252. [Tls](#)
- 253. [TlsClient](#)
- 254. [TlsClientHash](#)
- 255. [TlsServer](#)
- 256. [TlsServerHash](#)
- 257. [Token](#)
- 258. [Trustedapplication](#)
- 259. [UnassignComputersToGroupRequest](#)
- 260. [Url](#)
- 261. [User](#)
- 262. [UserAgent](#)
- 263. [UserAgentDevice](#)
- 264. [UserChanges](#)
- 265. [UserDataAuditing](#)
- 266. [UserDetailModel](#)
- 267. [UserEffective](#)
- 268. [UserListItemModel](#)
- 269. [UserListItemModelPagedResponse](#)
- 270. [UserRoleResourceItemModel](#)
- 271. [UserTarget](#)
- 272. [V2CreateUserRequest](#)
- 273. [Vlan](#)
- 274. [Vulnerability](#)

- 275. [VulnerabilityScanner](#)
- 276. [VulnerabilityScore](#)
- 277. [Workstyle](#)
- 278. [X509](#)
- 279. [X509Issuer](#)
- 280. [X509Subject](#)
- 281. [_event](#)
- 282. [_rule](#)
- 283. [id_AssignComputersByCsv_body](#)
- 284. [id_Upload_body](#)
- 285. [v2_Policies_body](#)

AboutModel

AboutModel

consoleVersion (optional)

String ConsoleVersion

reportingDatabaseVersion (optional)

String ReportingDatabaseVersion

policyEditorVersion (optional)

String PolicyEditorVersion

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 (optional)

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)

InstallationKeyDataAuditingDetailModel

policyDataAuditing (optional)

PolicyDataAuditingDetailModel

policyRevisionDataAuditing (optional)

PolicyRevisionDataAuditingDetailModel

settingsDataAuditing (optional)

SettingDataAuditingDetailModel

userDataAuditing (optional)

UserDataAuditing

openIdConfigDataAuditing (optional)

OpenIdConfigDataAuditingDetailModel

mmcRemoteClientDataAuditing (optional)

MMCRemoteClientDataAuditingDetailModel

computerPolicyDataAuditing (optional)

ComputerPolicyDataAuditingDetailModel

azureADIntegrationDataAuditing (optional)

AzureADIntegrationDataAuditingDetailModel

authorizationRequestDataAuditing (optional)

AuthorizationRequestDataAuditingDetailModel

reputationSettingsDataAuditing (optional)

ReputationSettingsDataAuditingDetailModel

securitySettingsDataAuditing (optional)

SecuritySettingsDataAuditingDetailModel

disableSiemIntegrationDataAuditing (optional)

SiemIntegrationBaseDetailModel

siemIntegrationQradarAuditing (optional)

SiemIntegrationQradarAuditingDetailModel

siemIntegrationS3Auditing (optional)

SiemIntegrationS3AuditingDetailModel

siemIntegrationSentinelAuditing (optional)

SiemIntegrationSentinelAuditingDetailModel

siemIntegrationSplunkAuditing (optional)

SiemIntegrationSplunkAuditingDetailModel

agentDataAuditing (optional)

AgentDataAuditingDetailModel

managementRuleDataAuditing (optional)

ManagementRuleDataAuditingDetailModel



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

roleId (optional)

UUID role id format: uuid

roleName (optional)

String role name

**ActivityAuditRoleResourceModel**

Role Resource Model for activity audits

resourceType (optional)

String Type of resource

resourceId (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

**Agent****version (optional)**

String

build (optional)

AgentBuild

name (optional)

String

type (optional)

String

id (optional)

String

ephemeral_id (optional)

String

**AgentBuild****original (optional)**

String

**AgentDataAuditingDetailModel**

Class that holds all the information that will be deserialized as result of the Agent(Computer) Data Auditing process.

newAgentId (optional)

UUID Guid to store the new Agent Id assigned to the computer. format: uuid

oldAgentId (optional)

UUID Guid to store the old Agent Id if there is a change in Agent Id. format: uuid

newTimestamp (optional)

Date TimeStamp of the audit event. format: date-time

oldTimestamp (optional)

Date TimeStamp of a previous audit event. format: date-time

newHostType (optional)

String The host type detected for the agent.

oldHostType (optional)

String The present Host type found by the adapter.

newOsName (optional)

String Os Name assigned detected by the adapter

oldOsName (optional)

String The present Os Name detected by the adapter

newAdapterVersion (optional)

String Adapter version installed in the computer.

oldAdapterVersion (optional)

String Present adapter version, in case of updating, this value can reflect the last adapter version used.

newComputerGroupid (optional)

UUID The computer group Id that the agent is going to be assigned to. If the value is Guid.Empty, and if OldComputerGroupid in not Guid.Empty, it represents an unassignment. format: uuid

oldComputerGroupid (optional)

UUID The computer group Id that the agent was assigned to. If the value is Guid.Empty, and if NewComputerGroupId in not Guid.Empty, it represents an assignment. format: uuid

newComputerGroupName (optional)

String The computer group name that the agent is going to be assigned to. If the value is empty, the action represent an unassignment.

oldComputerGroupName (optional)

String The computer group name that the agent was assigned to. If the value is empty, the action represent an assignment.



AgentHostType

enum

String

- Undefined
- MicrosoftWindows
- AppleMacOS
- Linux



ApiAccountListItemModel

Model of Api Accounts

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** Name of Api Account**description (optional)****String** Description of Api Account**clientId (optional)****String** Client Id**createdDate (optional)****Date** Date api account was created format: date-time**scimAccess (optional)****Integer** Scim Access Permissions NoAccess = 0 FullAccess = 2 format: int32**reportingAccess (optional)****Integer** Reporting Access Permissions NoAccess = 0 ReadOnly = 1 format: int32**auditAccess (optional)****Integer** Audit Access Permissions NoAccess = 0 ReadOnly = 1 format: int32**managementAccess (optional)****Integer** Management Api Access Permissions NoAccess = 0 ReadOnly = 1 FullAccess = 2 format: int32



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

**As****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)

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

startTime (optional)

Date format: date-time

duration (optional)

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)

String

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]



AuthorizationRequestDataAuditingDetailModel

Properties for Authorization Request Data Auditing

oldAuthRequestIntegrationEnabled (optional)

Boolean Old Value is Authorization Request Integration Enabled?

oldAuthRequestHostName (optional)

String Old Value Authorization Requests Hostname

oldAuthRequestClientId (optional)

String Old Value Authorization Request ClientId

oldAuthRequestClientSecret (optional)

String Old Value Authorization Request Client Secret

oldAuthRequestPassword (optional)

String Old Value Authorization Request Password

oldAuthRequestUserName (optional)

String Old Value Authorization Request User Name

oldAuthRequestApiClientId (optional)

String Old Value Authorization Request API Client ID

oldAuthRequestApiClientSecret (optional)

String Old Value Authorization Request Client Secret

authRequestIntegrationEnabled (optional)

Boolean Old Value is Authorization Request Integration Enabled?

authRequestHostName (optional)

String Authorization Requests Hostname

authRequestClientId (optional)

String Authorization Request ClientId

authRequestClientSecret (optional)

String Authorization Request Client Secret

authRequestPassword (optional)

String Authorization Request Password

authRequestUserName (optional)

String Authorization Request User Name

authRequestApiClientId (optional)

String Authorization Request API Client ID

authRequestApiClientSecret (optional)

String Authorization Request Client Secret

authRequestConfigChanged (optional)

Boolean Is Authorization Request Config changed?



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)

String



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

policyId (optional)

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



AzureADIntegrationDataAuditingDetailModel

Properties for Azure AD Integration

oldAzureAdTenantId (optional)

String Old Value Azure AD Tenant ID

oldAzureAdClientId (optional)

String Old Value Azure AD Client Id used in the integration

oldAzureAdClientSecret (optional)

String Old Value Azure AD Client Secret

oldAzureAdUseCertificateAuth (optional)

Boolean Old Value Azure AD Use Certified Authorization

oldAzureAdIntegrationEnabled (optional)

Boolean Old Value Is azure AD Integration enabled?

azureAdTenantId (optional)

String Old Value Azure AD Tenant ID

azureAdClientId (optional)

String Azure AD Client Id used in the integration

azureAdClientSecret (optional)

String Azure AD Client Secret

azureAdUseCertificateAuth (optional)

Boolean Azure AD Use Certified Authorization

azureAdIntegrationEnabled (optional)

Boolean Is azure AD Integration enabled?

azureAdConfigChanged (optional)

Boolean Is Azure AD Configuration changed?



Bundle

Name (optional)

String

Type (optional)

String

Creator (optional)

String

InfoDescription (optional)

String

Version (optional)

String

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



ChangedBy

Changed by enum used for activity audits

enum

String

- API
- Portal

 **Client****address (optional)**

String

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)

ClientNat

Name (optional)

String

as (optional)

As

geo (optional)

Geo

user (optional)

User



ClientNat

ip (optional)

String

port (optional)

Long format: int64



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)

String

 **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

**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

packageManagerVersion (optional)

String

agentVersion (optional)

String

authorisationState (optional)

String

authorised (optional)

Date format: date-time

authorisedOn (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

groupId (optional)

UUID format: uuid

groupName (optional)

String

policyId (optional)

UUID format: uuid

policyName (optional)

String

policyRevision (optional)

Integer format: int32

policyRevisionStatus (optional)

String

endpointInformation (optional)

EndpointInformationModel

certificateInformation (optional)

CertificateInformationModel

hostPolicyId (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

daysDisconnected (optional)

Integer DaysDisconnected format: int32

connectionStatus (optional)

String ConnectionStatus

archived (optional)

Boolean Archived

archivedOn (optional)

Date ArchivedOn 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

packageManagerVersion (optional)

String The Package Manager version on 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

policyId (optional)

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

policyName (optional)

String Policy Name, example - Policy1

groupId (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

connectionStatus (optional)

array[String] ConnectionStatus

daysDisconnected (optional)

Integer DaysDisconnected format: int32

daysSinceArchived (optional)

Integer DaysSinceArchived format: int32



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

policyId (optional)

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

policyName (optional)

String Policy Name, example - Policy1

policyRevisionStatus (optional)

String

groupId (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

authorisedOn (optional)

Date format: date-time

daysDisconnected (optional)

Integer DaysDisconnected format: int32

connectionStatus (optional)

String ConnectionStatus

packageManagerVersion (optional)

String Package Manager Version on the computer

archived (optional)

Boolean Archived

archivedOn (optional)

Date ArchivedOn format: date-time

daysSinceArchived (optional)

Integer DaysSinceArchived format: int32



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



ComputerPolicyDataAuditingDetailModel

Properties to audit computer Policy data auditing

oldInactivityAgentDeactivationDays (optional)

Integer Old Value Deactivation Days for inactivity format: int32

oldEnableDeactivatedAgentDeletion (optional)

Boolean Old Value Is enable deactivated Agent Deletion

oldDeactivatedAgentDeletionDays (optional)

Integer Old Value Deactivated Agent Deletion Days format: int32

inactivityAgentDeactivationDays (optional)

Integer Deactivation Days for inactivity format: int32

enableDeactivatedAgentDeletion (optional)

Boolean Is enable deactivated Agent Deletion

deactivatedAgentDeletionDays (optional)

Integer Deactivated Agent Deletion Days format: int32

 **ComputerRenewCertificateRequest****computerId (optional)**

UUID format: uuid

 **ComputerRetrieveLogsRequest****computerId (optional)**

UUID format: uuid

 **ComputerRetrieveStatusInfoRequest****computerId (optional)**

UUID format: uuid

 **ComputersArchiveRequest**

Request to archive Computer(s)

computerIds (optional)

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



ComputersAuthoriseRequest

computerIds (optional)

array[UUID] format: uuid

excludedComputerIds (optional)

array[UUID] format: uuid

filter (optional)

ComputerFilterModel

allComputers (optional)

Boolean

groupId (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



ComputersUnarchiveRequest

Request to unarchive Computer(s)

computerIds (optional)

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



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)

ContainerImageHash

 **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



Destination

address (optional)

String

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)

DestinationNat

as (optional)

As

geo (optional)

Geo

user (optional)

User



DestinationNat

ip (optional)

String

port (optional)

Long format: int64

**name (optional)**

String

path (optional)

String

hash (optional)

Hash

pe (optional)

Pe

code_signature (optional)

CodeSignature

**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

class (optional)

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)

String

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)

Dll

dns (optional)

Dns

ecs (optional)

Ecs

email (optional)

Email

error (optional)

Error

event (optional)

`_event`

faas (optional)

Faas

file (optional)

File

group (optional)

Group

host (optional)

Host

http (optional)

Http

log (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)

Tls

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

TenantId (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 (optional)

Privilegedgroup

RemotePowerShell (optional)

Remotepowershell

ServiceControl (optional)

Servicecontrol

Session (optional)

Session

StoreApp (optional)

Storeapp

TrustedApplication (optional)

Trustedapplication



id (optional)

String

message (optional)

String

code (optional)

String

type (optional)

String

stack_trace (optional)

String

**Type (optional)**

String

Action (optional)

String

**name (optional)**

String

id (optional)

String

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)

String

name (optional)

String

TimezoneOffset (optional)

Long format: int64



GeoPoint

lon (optional)

Double format: double

lat (optional)

Double format: double



Gpo

Version (optional)

String

DisplayName (optional)

String

ActiveDirectoryPath (optional)

String

LinkInformation (optional)

String

Group

id (optional)

String

name (optional)

String

domain (optional)

String

GroupDataAuditingDetailModel

newName (optional)

String

oldName (optional)

String

newDescription (optional)

String

oldDescription (optional)

String

newsDefault (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)

Boolean

errorInfo (optional)

ListItemErrorInfoModel

id (optional)

UUID The Id 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

policyId (optional)

UUID format: uuid

policyRevisionStatus (optional)

PolicyRevisionState

policyName (optional)

String

policyAssigned (optional)

Date Date when a policy is assigned to a group format: date-time

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)

String



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)

String

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

 **Http****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

initiated (optional)

Date format: date-time



level (optional)

String

file (optional)

LogFile

logger (optional)

String

origin (optional)

LogOrigin

syslog (optional)

String

 **LogFile**

path (optional)

String


 **LogOrigin**

file (optional)

LogOriginFile

function (optional)

String

 **LogOriginFile**

name (optional)

String

line (optional)

Long format: int64

 **MMCRemoteClientDataAuditingDetailModel**

MMCRemote Client properties for enabling Remote Access

enabled (optional)

Boolean Is Remote Client enabled?

oldEnabled (optional)

Boolean Old Value Is Remote Client enabled?

clientId (optional)

UUID ClientId selected format: uuid

oldClientId (optional)

UUID Old Value ClientId selected format: uuid



ManagementRuleDataAuditingDetailModel

Management Rule detail auditing model

newPriority (optional)

Integer New Priority Value for rule format: int32

oldPriority (optional)

Integer Old priority value for rule format: int32



Message

Type (optional)

String

Name (optional)

String

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)**

String

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

**OpenIdConfigDataAuditingDetailModel**

Properties audited when OpenIdConfig is modified in PMC

oldAuthenticationType (optional)

String Old Authentication Type

newAuthenticationType (optional)

String New Authentication Type

oldDomain (optional)

String Old domain

newDomain (optional)

String New Domain

oldClientId (optional)

String Old client ID

newClientId (optional)

String New ClientId

secretUpdated (optional)

Boolean Is Secret Updated?

oldOpenIDConnectProvider (optional)

String Old OpenId Provider

newOpenIDConnectProvider (optional)

String New OpenIdProvider



OperationValue

Storing the values of the scim operation

value (optional)

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

valueBoolean (optional)

Boolean Generic boolean value if no specific field is specified.

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

username (optional)

String username 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)

String

type (optional)

String

parent (optional)

OrchestratorResourceParent

ip (optional)

array[String]

id (optional)

String



OrchestratorResourceParent

type (optional)

String



Organization

name (optional)

String

id (optional)

String



Os

type (optional)

String

platform (optional)

String

name (optional)

String

full (optional)

String

family (optional)

String

version (optional)

String

kernel (optional)

String

ProductType (optional)

String



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)

String

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)

String

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

policyId (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)

String

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]

newAnnotationNote (optional)

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)

User

real_user (optional)

User

parent (optional)

ProcessParent

entry_leader (optional)

ProcessEntryLeader

session_leader (optional)

ProcessSessionLeader

group_leader (optional)

ProcessGroupLeader

previous (optional)

ProcessPrevious



ProcessEntryLeader

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



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)

Elf

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)

String

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



ReputationSettingsDataAuditingDetailModel

Reputation properties for enabling Integration

oldReputationIntegrationEnabled (optional)

Boolean Old Value Is reputation integration enabled?

oldReputationIntegrationApiKey (optional)

String Old Value Reputation Integration Key

reputationIntegrationEnabled (optional)

Boolean Is reputation integration enabled?

reputationIntegrationApiKey (optional)

String Reputation Integration Key

reputationConfigChanged (optional)

Boolean Reputation Configuration changed



RoleElement

role object

primary (optional)

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

value (optional)

String User role value



RoleItemModel

Model of role list item

id (optional)

UUID Identifier format: uuid

name (optional)

String Name

resourceId (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

resourceType (optional)

String Type of resource

resourceId (optional)

UUID Id of the resource format: uuid

roleId (optional)

UUID Role Id format: uuid



Rule

Identifier (optional)

String

OnDemand (optional)

Boolean

Action (optional)

String

 **Rulescript****FileName (optional)**


String

Publisher (optional)

String

Outcome (optional)

RulescriptOutcome

 **RulescriptOutcome****Version (optional)**

String

Name (optional)

String

RuleAffected (optional)

Boolean

Result (optional)

String

Output (optional)

String



SCIMEmail

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 authentication

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, replace, remove

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`

bulk (optional)

`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

externalId (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



SecuritySettingsDataAuditingDetailModel

Properties for Security settings

tokenTimeout (optional)

Integer Token Timeout format: int32

oldTokenTimeout (optional)

Integer Old Value Token Timeout format: int32

 **Server****address (optional)**

String

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)

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)

String

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)

String



ServiceOrigin

environment (optional)

String

id (optional)

String

name (optional)

String

node (optional)

ServiceNode

type (optional)

String

state (optional)

String

version (optional)

String

ephemeral_id (optional)

String

address (optional)

String



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)

String

address (optional)

String



Servicecontrol

Service (optional)

ServicecontrolService

⬆ `ServicecontrolService`

DisplayName (optional)

String

Name (optional)

String

Action (optional)

String

⬆ `Session`

Administrator (optional)

Boolean

Locale (optional)

String

Identifier (optional)

String

PowerUser (optional)

Boolean

WindowsSessionId (optional)

String

UILanguage (optional)

String



SettingDataAuditingDetailModel

addDomain (optional)

String

removeDomain (optional)

String

modifyDomainOldValue (optional)

String

modifyDomainNewValue (optional)

String



SiemIntegrationBaseDetailModel

Common properties for the different siem integrations to Audit

siemIntegrationEnabled (optional)

Boolean Is siem integration enabled?

siemIntegrationType (optional)

String Type of integration selected

siemFormat (optional)

String Data format selected



SiemIntegrationQradarAuditingDetailModel

QRadar integration properties to audit

siemIntegrationEnabled (optional)

Boolean Is siem integration enabled?

siemIntegrationType (optional)

String Type of integration selected

siemFormat (optional)

String Data format selected

hostName (optional)

String Hostname

port (optional)

String Port

cert (optional)

String Cert



SiemIntegrationS3AuditingDetailModel

S3 integration properties to Audit

siemIntegrationEnabled (optional)

Boolean Is siem integration enabled?

siemIntegrationType (optional)

String Type of integration selected

siemFormat (optional)

String Data format selected

siemAccessKeyId (optional)

String AccessKeyId

siemBucketName (optional)

String AWS Bucket name

siemCodec (optional)

String Codec

siemRegionName (optional)

String Region

siemSseEnabled (optional)

Boolean Is SSE enabled



SiemIntegrationSentinelAuditingDetailModel

Sentinel integration properties to audit

siemIntegrationEnabled (optional)

Boolean Is siem integration enabled?

siemIntegrationType (optional)

String Type of integration selected

siemFormat (optional)

String Data format selected

tableName (optional)

String TableName

workspaceId (optional)

String WorkspaceId



SiemIntegrationSplunkAuditingDetailModel

Splunk integration properties to audit

siemIntegrationEnabled (optional)

Boolean Is siem integration enabled?

siemIntegrationType (optional)

String Type of integration selected

siemFormat (optional)

String Data format selected

hostName (optional)

String Hostname

index (optional)

String Index



SortDirection

enum

String

- Asc
- Desc



SortModel

by (optional)

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

order (optional)

SortDirection

**Source****address (optional)**

String

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)

String

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]]



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)

String

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

file (optional)

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]

 Tls**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)

TlsClient

server (optional)

TlsServer

**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)

TlsClientHash

x509 (optional)

X509

 **TlsClientHash****md5 (optional)**

String

sha1 (optional)

String

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)

String

hash (optional)

TlsServerHash

x509 (optional)

X509



TlsServerHash

md5 (optional)

String

sha1 (optional)

String

sha256 (optional)

String

 **Token****Name (optional)**

String

Description (optional)

String

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

**original (optional)**

String

full (optional)

String

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

**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

target (optional)

UserTarget

effective (optional)

UserEffective

changes (optional)

UserChanges

 **UserAgent****original (optional)**

String

name (optional)

String

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)

String

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[ActivityAuditRoleResourceModel] 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]

olsonTimeZoneId (optional)

String

dateTimeDisplayFormat (optional)

String

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

olsonTimeZonedId (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

resourceId (optional)

String

resourceType (optional)

String



UserTarget

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



V2CreateUserRequest

V2CreateUserRequest

emailAddress (optional)

String EmailAddress

olsonTimeZonedId (optional)

String OlsonTimeZonedId

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



id (optional)

String

name (optional)

String



classification (optional)

String

enumeration (optional)

String

reference (optional)

String

score (optional)

VulnerabilityScore

category (optional)

array[String]

description (optional)

String

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

**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)

String

`_rule`**id (optional)**

String

uuid (optional)

String

version (optional)

String

name (optional)

String

description (optional)

String

category (optional)

String

ruleset (optional)

String

reference (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