

Events

[restSearch] Get a filtered and paginated list of events:

POST

<https://misp.local/events/restSearch>

Request:

```
{
  "page": 1,
  "limit": 0,
  "value": "127.0.0.1",
  "type": "md5",
  "category": "Internal reference",
  "org": "12345",
  "tags": [
    "tlp:amber"
  ],
  "event_tags": [
    "tlp:amber"
  ],
  "searchall": "malware",
  "from": "string",
  "to": "string",
  "last": 0,
  "eventid": "12345",
  "withAttachments": false,
  "sharinggroup": [
    "1"
  ],
  "metadata": true,
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "publish_timestamp": "1617875568",
```

```
"timestamp": "1617875568",
"published": false,
"enforceWarninglist": true,
"sgReferenceOnly": true,
"requested_attributes": [
  "id"
],
"includeContext": true,
"headerless": true,
"includeWarninglistHits": true,
"attackGalaxy": "mitre-attack",
"to_ids": true,
"deleted": false,
"excludeLocalTags": true,
"date": "string",
"includeSightingdb": true,
"tag": "tlp:white",
"object_relation": "filepath",
"threat_level_id": "1",
"returnFormat": "json"
}
```

Resquest:

200:

```
{
  "response": [
    {
      "Event": {
        "id": "12345",
        "org_id": "12345",
        "distribution": "0",
        "info": "logged source ip",
        "orgc_id": "12345",
        "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
        "date": "1991-01-15",
        "published": false,
        "analysis": "0",
        "attribute_count": "321",
```

```
"timestamp": "1617875568",
"sharing_group_id": "1",
"proposal_email_lock": true,
"locked": true,
"threat_level_id": "1",
"publish_timestamp": "1617875568",
"sighting_timestamp": "1617875568",
"disable_correlation": false,
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"event_creator_email": "user@example.com",
"Feed": {
  "id": "3",
  "name": "CIRCL OSINT Feed",
  "provider": "CIRCL",
  "url": "https://www.circl.lu/doc/misp/feed-osint",
  "rules": "{\n  \"tags\": {\n    \"OR\": [],\n    \"NOT\": [],\n  },\n  \"orgs\": {\n    \"OR\": [],\n    \"NOT\": [],\n  },\n  \"url_params\": {\n    \"\": \"\"\n  },\n  \"enabled\": true,\n  \"distribution\": \"0\",\n  \"sharing_group_id\": \"1\",\n  \"tag_id\": \"12345\",\n  \"default\": true,\n  \"source_format\": \"1\",\n  \"fixed_event\": true,\n  \"delta_merge\": true,\n  \"event_id\": \"12345\",\n  \"publish\": false,\n  \"override_ids\": true,\n  \"settings\":\n    \"{\n      \"csv\": {\n        \"value\": \"\",\n        \"delimiter\": \"\\\"\\\"\",\n        \"common\": {\n          \"excluderegex\": \"\\\"\\\"\",\n          \"disable_correlation\": \"1\\\"\"\n        },\n        \"input_source\": \"local\",\n        \"delete_local_file\": true,\n        \"lookup_visible\": true,\n        \"headers\": \"X-Custom-Header-A: Foo\\nX-Custom-Header-B: Bar\\n\",\n        \"caching_enabled\": true,\n        \"force_to_ids\": true,\n        \"orgc_id\": \"12345\",\n        \"cache_timestamp\": \"1617875568\"\n      }\n    }\",\n  },
  "Org": {
    "id": "12345",
```

```
"name": "ORGNAME",
"uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
},
"Orgc": {
  "id": "12345",
  "name": "ORGNAME",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
},
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"ShadowAttribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
```

```
"timestamp": "1617875568",
"distribution": "0",
"sharing_group_id": "1",
"comment": "logged source ip",
"deleted": false,
"disable_correlation": false,
"first_seen": "1581984000000000",
"last_seen": "1581984000000000"
}
],
"RelatedEvent": [
  {}
],
"Galaxy": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "name": "Ransomware",
    "type": "ransomware",
    "description": "Ransomware galaxy based on ...",
    "version": "1",
    "icon": "globe",
    "namespace": "misp",
    "kill_chain_order": {
      "fraud-tactics": [
        "Initiation",
        "Target Compromise",
        "Perform Fraud",
        "Obtain Fraudulent Assets",
        "Assets Transfer",
        "Monetisation"
      ]
    }
  }
],
"Object": [
  {
    "id": "12345",
    "name": "ail-leak",
    "meta-category": "string",
```

```
"description": "string",
"template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"template_version": "1",
"event_id": "12345",
"uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"timestamp": "1617875568",
"distribution": "0",
"sharing_group_id": "1",
"comment": "string",
"deleted": true,
"first_seen": "1581984000000000",
"last_seen": "1581984000000000",
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
},
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
```

```

    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
],
"Tag": [
  {
    "id": "12345",
    "name": "tlp:white",
    "colour": "#ffffff",
    "exportable": true,
    "org_id": "12345",
    "user_id": "12345",
    "hide_tag": false,
    "numerical_value": "12345",
    "is_galaxy": true,
    "is_custom_galaxy": true,
    "inherited": 1
  }
],
"Event": {
  "id": "12345",
  "timestamp": "1617875568",
  "sighting_timestamp": "1617875568",
  "published": false,
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "orgc_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
}
}
]
}

```

403:

```

{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the

```

```
Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Add event:

POST

<https://misp.local/events/add>

Request:

```
{
  "org_id": "12345",
  "distribution": "0",
  "info": "logged source ip",
  "orgc_id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "date": "1991-01-15",
  "published": false,
  "analysis": "0",
  "attribute_count": "321",
  "timestamp": "1617875568",
  "sharing_group_id": "1",
  "proposal_email_lock": true,
  "locked": true,
  "threat_level_id": "1",
  "publish_timestamp": "1617875568",
  "sighting_timestamp": "1617875568",
}
```

```
"disable_correlation": false,
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"event_creator_email": "user@example.com"
}
```

Response:

200:

```
{
  "Event": {
    "id": "12345",
    "org_id": "12345",
    "distribution": "0",
    "info": "logged source ip",
    "orgc_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "date": "1991-01-15",
    "published": false,
    "analysis": "0",
    "attribute_count": "321",
    "timestamp": "1617875568",
    "sharing_group_id": "1",
    "proposal_email_lock": true,
    "locked": true,
    "threat_level_id": "1",
    "publish_timestamp": "1617875568",
    "sighting_timestamp": "1617875568",
    "disable_correlation": false,
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_creator_email": "user@example.com",
    "Feed": {
      "id": "3",
      "name": "CIRCL OSINT Feed",
      "provider": "CIRCL",
      "url": "https://www.circl.lu/doc/misp/feed-osint",
      "rules": "{\\\"tags\\\":{\\\"OR\\\":[],\\\"NOT\\\":[]},\\\"orgs\\\":{\\\"OR\\\":[],\\\"NOT\\\":[]},\\\"url_params\\\":\\\"\\\"}",
      "enabled": true,
      "distribution": "0",
      "sharing_group_id": "1",
```

```
"tag_id": "12345",
"default": true,
"source_format": "1",
"fixed_event": true,
"delta_merge": true,
"event_id": "12345",
"publish": false,
"override_ids": true,
"settings":
{"csv":{"value":"","delimiter":"","common":{"excluderegex":"","disable_correlation":"","1"},"
  "input_source": "local",
  "delete_local_file": true,
  "lookup_visible": true,
  "headers": "X-Custom-Header-A: Foo\nX-Custom-Header-B: Bar\n",
  "caching_enabled": true,
  "force_to_ids": true,
  "orgc_id": "12345",
  "cache_timestamp": "1617875568"
},
"Org": {
  "id": "12345",
  "name": "ORGNAME",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
},
"Orgc": {
  "id": "12345",
  "name": "ORGNAME",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
},
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
```

```
"timestamp": "1617875568",
"distribution": "0",
"sharing_group_id": "1",
"comment": "logged source ip",
"deleted": false,
"disable_correlation": false,
"first_seen": "1581984000000000",
"last_seen": "1581984000000000"
}
],
"ShadowAttribute": [
{
  "id": "12345",
  "event_id": "12345",
  "object_id": "12345",
  "object_relation": "sensor",
  "category": "Internal reference",
  "type": "md5",
  "value": "127.0.0.1",
  "to_ids": true,
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "timestamp": "1617875568",
  "distribution": "0",
  "sharing_group_id": "1",
  "comment": "logged source ip",
  "deleted": false,
  "disable_correlation": false,
  "first_seen": "1581984000000000",
  "last_seen": "1581984000000000"
}
],
"RelatedEvent": [
{}
],
"Galaxy": [
{
  "id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "name": "Ransomware",
  "type": "ransomware",
```

```
"description": "Ransomware galaxy based on ...",
"version": "1",
"icon": "globe",
"namespace": "misp",
"kill_chain_order": {
  "fraud-tactics": [
    "Initiation",
    "Target Compromise",
    "Perform Fraud",
    "Obtain Fraudulent Assets",
    "Assets Transfer",
    "Monetisation"
  ]
}
],
"Object": [
  {
    "id": "12345",
    "name": "ail-leak",
    "meta-category": "string",
    "description": "string",
    "template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "template_version": "1",
    "event_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "string",
    "deleted": true,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000",
    "Attribute": [
      {
        "id": "12345",
        "event_id": "12345",
        "object_id": "12345",
        "object_relation": "sensor",
        "category": "Internal reference",
```

```
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
},
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
],
"Tag": [
  {
    "id": "12345",
    "name": "tlp:white",
    "colour": "#ffffff",
    "exportable": true,
    "org_id": "12345",
    "user_id": "12345",
    "hide_tag": false,
    "numerical_value": "12345",
    "is_galaxy": true,
```

```
"is_custom_galaxy": true,  
"inherited": 1  
}  
]  
}  
}
```

403:

```
{  
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "url": "/attributes"  
}
```

Default:

```
{  
  "name": "string",  
  "message": "string",  
  "url": "/attributes"  
}
```

Edit event:

PUT

<https://misp.local/events/edit/{eventId}>

Request:

```
{  
  "org_id": "12345",  
  "distribution": "0",  
  "info": "logged source ip",  
  "orgc_id": "12345",  
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
```

```
"date": "1991-01-15",
"published": false,
"analysis": "0",
"attribute_count": "321",
"timestamp": "1617875568",
"sharing_group_id": "1",
"proposal_email_lock": true,
"locked": true,
"threat_level_id": "1",
"publish_timestamp": "1617875568",
"sighting_timestamp": "1617875568",
"disable_correlation": false,
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"event_creator_email": "user@example.com"
}
```

Response:

200:

```
{
  "Event": {
    "id": "12345",
    "org_id": "12345",
    "distribution": "0",
    "info": "logged source ip",
    "orgc_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "date": "1991-01-15",
    "published": false,
    "analysis": "0",
    "attribute_count": "321",
    "timestamp": "1617875568",
    "sharing_group_id": "1",
    "proposal_email_lock": true,
    "locked": true,
    "threat_level_id": "1",
    "publish_timestamp": "1617875568",
    "sighting_timestamp": "1617875568",
    "disable_correlation": false,
```

```
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"event_creator_email": "user@example.com",
"Feed": {
  "id": "3",
  "name": "CIRCL OSINT Feed",
  "provider": "CIRCL",
  "url": "https://www.circl.lu/doc/misp/feed-osint",
  "rules": "{ \"tags\": { \"OR\": [], \"NOT\": [] }, \"orgs\": { \"OR\": [], \"NOT\": [] }, \"url_params\": \"\" }",
  "enabled": true,
  "distribution": "0",
  "sharing_group_id": "1",
  "tag_id": "12345",
  "default": true,
  "source_format": "1",
  "fixed_event": true,
  "delta_merge": true,
  "event_id": "12345",
  "publish": false,
  "override_ids": true,
  "settings":
  "{ \"csv\": { \"value\": \"\", \"delimiter\": \"\" }, \"common\": { \"excluderegex\": \"\", \"disable_correlation\": \"1\" },
    \"input_source\": \"local\",
    \"delete_local_file\": true,
    \"lookup_visible\": true,
    \"headers\": \"X-Custom-Header-A: Foo\\nX-Custom-Header-B: Bar\\n\",
    \"caching_enabled\": true,
    \"force_to_ids\": true,
    \"orgc_id\": \"12345\",
    \"cache_timestamp\": \"1617875568\"
  },
  "Org": {
    "id": "12345",
    "name": "ORGNAME",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
  },
  "Orgc": {
    "id": "12345",
    "name": "ORGNAME",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
  },
}
```

```
"Attribute": [  
  {  
    "id": "12345",  
    "event_id": "12345",  
    "object_id": "12345",  
    "object_relation": "sensor",  
    "category": "Internal reference",  
    "type": "md5",  
    "value": "127.0.0.1",  
    "to_ids": true,  
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "timestamp": "1617875568",  
    "distribution": "0",  
    "sharing_group_id": "1",  
    "comment": "logged source ip",  
    "deleted": false,  
    "disable_correlation": false,  
    "first_seen": "1581984000000000",  
    "last_seen": "1581984000000000"  
  }  
],
```

```
"ShadowAttribute": [  
  {  
    "id": "12345",  
    "event_id": "12345",  
    "object_id": "12345",  
    "object_relation": "sensor",  
    "category": "Internal reference",  
    "type": "md5",  
    "value": "127.0.0.1",  
    "to_ids": true,  
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "timestamp": "1617875568",  
    "distribution": "0",  
    "sharing_group_id": "1",  
    "comment": "logged source ip",  
    "deleted": false,  
    "disable_correlation": false,  
    "first_seen": "1581984000000000",  
    "last_seen": "1581984000000000"  
  }  
]
```

```
}
],
"RelatedEvent": [
  {}
],
"Galaxy": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "name": "Ransomware",
    "type": "ransomware",
    "description": "Ransomware galaxy based on ...",
    "version": "1",
    "icon": "globe",
    "namespace": "misp",
    "kill_chain_order": {
      "fraud-tactics": [
        "Initiation",
        "Target Compromise",
        "Perform Fraud",
        "Obtain Fraudulent Assets",
        "Assets Transfer",
        "Monetisation"
      ]
    }
  }
]
},
],
"Object": [
  {
    "id": "12345",
    "name": "ail-leak",
    "meta-category": "string",
    "description": "string",
    "template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "template_version": "1",
    "event_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
```

```
"comment": "string",
"deleted": true,
"first_seen": "1581984000000000",
"last_seen": "1581984000000000",
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
],
```

```
"Tag": [  
  {  
    "id": "12345",  
    "name": "tlp:white",  
    "colour": "#ffffff",  
    "exportable": true,  
    "org_id": "12345",  
    "user_id": "12345",  
    "hide_tag": false,  
    "numerical_value": "12345",  
    "is_galaxy": true,  
    "is_custom_galaxy": true,  
    "inherited": 1  
  }  
]  
}  
}
```

403:

```
{  
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "url": "/attributes"  
}
```

Default:

```
{  
  "name": "string",  
  "message": "string",  
  "url": "/attributes"  
}
```

Delete event:

DELETE

https://misp.local/events/delete/{eventId}

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "Event deleted.",
  "message": "Could not delete Event",
  "url": "/events/delete/1",
  "errors": "Event was not deleted."
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Get a list of events:

GET

https://misp.local/events

Response:

```
[
  {
    "id": "12345",
    "org_id": "12345",
    "distribution": "0",
    "info": "logged source ip",
    "orgc_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "date": "1991-01-15",
    "published": false,
    "analysis": "0",
    "attribute_count": "321",
    "timestamp": "1617875568",
    "sharing_group_id": "1",
    "proposal_email_lock": true,
    "locked": true,
    "threat_level_id": "1",
    "publish_timestamp": "1617875568",
    "sighting_timestamp": "1617875568",
    "disable_correlation": false,
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_creator_email": "user@example.com",
    "Feed": {
      "id": "3",
      "name": "CIRCL OSINT Feed",
      "provider": "CIRCL",
      "url": "https://www.circl.lu/doc/misp/feed-osint",
      "rules": "{\\\"tags\\\":{\\\"OR\\\":[],\\\"NOT\\\":[]},\\\"orgs\\\":{\\\"OR\\\":[],\\\"NOT\\\":[]},\\\"url_params\\\":\\\"\\\"}",
      "enabled": true,
      "distribution": "0",
      "sharing_group_id": "1",
      "tag_id": "12345",
      "default": true,
      "source_format": "1",
      "fixed_event": true,
      "delta_merge": true,
      "event_id": "12345",
      "publish": false,
```

```
"override_ids": true,
"settings":
"{\"csv\":{\"value\":\"\",\"delimiter\":\"\"},\"common\":{\"excluderegex\":\"\"},\"disable_correlation\":\"1\"}\",
  \"input_source\": \"local\",
  \"delete_local_file\": true,
  \"lookup_visible\": true,
  \"headers\": \"X-Custom-Header-A: Foo\\nX-Custom-Header-B: Bar\\n\",
  \"caching_enabled\": true,
  \"force_to_ids\": true,
  \"orgc_id\": \"12345\",
  \"cache_timestamp\": \"1617875568\"
},
\"Org\": {
  \"id\": \"12345\",
  \"name\": \"ORGNAME\",
  \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\"
},
\"Orgc\": {
  \"id\": \"12345\",
  \"name\": \"ORGNAME\",
  \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\"
},
\"Attribute\": [
  {
    \"id\": \"12345\",
    \"event_id\": \"12345\",
    \"object_id\": \"12345\",
    \"object_relation\": \"sensor\",
    \"category\": \"Internal reference\",
    \"type\": \"md5\",
    \"value\": \"127.0.0.1\",
    \"to_ids\": true,
    \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\",
    \"timestamp\": \"1617875568\",
    \"distribution\": \"0\",
    \"sharing_group_id\": \"1\",
    \"comment\": \"logged source ip\",
    \"deleted\": false,
    \"disable_correlation\": false,
    \"first_seen\": \"1581984000000000\",
```

```
    "last_seen": "1581984000000000"
  }
],
"ShadowAttribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"RelatedEvent": [
  {}
],
"Galaxy": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "name": "Ransomware",
    "type": "ransomware",
    "description": "Ransomware galaxy based on ...",
    "version": "1",
    "icon": "globe",
    "namespace": "misp",
    "kill_chain_order": {
      "fraud-tactics": [
        "Initiation",
```

```
    "Target Compromise",
    "Perform Fraud",
    "Obtain Fraudulent Assets",
    "Assets Transfer",
    "Monetisation"
  ]
}
}
],
"Object": [
{
  "id": "12345",
  "name": "ail-leak",
  "meta-category": "string",
  "description": "string",
  "template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "template_version": "1",
  "event_id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "timestamp": "1617875568",
  "distribution": "0",
  "sharing_group_id": "1",
  "comment": "string",
  "deleted": true,
  "first_seen": "1581984000000000",
  "last_seen": "1581984000000000",
  "Attribute": [
    {
      "id": "12345",
      "event_id": "12345",
      "object_id": "12345",
      "object_relation": "sensor",
      "category": "Internal reference",
      "type": "md5",
      "value": "127.0.0.1",
      "to_ids": true,
      "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "timestamp": "1617875568",
      "distribution": "0",
      "sharing_group_id": "1",
```

```
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
}
],
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
],
"Tag": [
  {
    "id": "12345",
    "name": "tlp:white",
    "colour": "#ffffff",
    "exportable": true,
    "org_id": "12345",
    "user_id": "12345",
    "hide_tag": false,
    "numerical_value": "12345",
    "is_galaxy": true,
    "is_custom_galaxy": true,
    "inherited": 1
  }
]
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Search events:

POST

<https://misp.local/events/index>

Request:

```
{
  "page": 1,
  "limit": 0,
  "sort": "timestamp",
  "direction": "asc",
  "minimal": false,
  "attribute": "covert channel",
  "eventid": "12345",
  "datefrom": "2021-03-05",
  "dateuntil": "2021-03-05",
  "org": "CIRCL",
  "eventinfo": "Phishing campaing",
  "tag": "tlp:white",
}
```

```
"tags": [  
  "tlp:amber",  
  "cycat:scope=\"exploit\"",  
],  
"distribution": "0",  
"sharinggroup": "1",  
"analysis": "0",  
"threatlevel": "1",  
"email": "admin@admin.test",  
"hasproposal": "1",  
"timestamp": "1",  
"publish_timestamp": "1",  
"searchDatefrom": "2020-01-20",  
"searchDateuntil": "2020-01-20"  
}
```

Response:

200:

```
[  
  {  
    "id": "12345",  
    "org_id": "12345",  
    "distribution": "0",  
    "info": "logged source ip",  
    "orgc_id": "12345",  
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "date": "1991-01-15",  
    "published": false,  
    "analysis": "0",  
    "attribute_count": "321",  
    "timestamp": "1617875568",  
    "sharing_group_id": "1",  
    "proposal_email_lock": true,  
    "locked": true,  
    "threat_level_id": "1",  
    "publish_timestamp": "1617875568",  
    "sighting_timestamp": "1617875568",  
  }  
]
```

```
"disable_correlation": false,
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"event_creator_email": "user@example.com",
"Feed": {
  "id": "3",
  "name": "CIRCL OSINT Feed",
  "provider": "CIRCL",
  "url": "https://www.circl.lu/doc/misp/feed-osint",
  "rules": "{\"tags\":{\"OR\":[],\"NOT\":[]},\"orgs\":{\"OR\":[],\"NOT\":[]},\"url_params\":{\"\"}},",
  "enabled": true,
  "distribution": "0",
  "sharing_group_id": "1",
  "tag_id": "12345",
  "default": true,
  "source_format": "1",
  "fixed_event": true,
  "delta_merge": true,
  "event_id": "12345",
  "publish": false,
  "override_ids": true,
  "settings":
  "{\"csv\":{\"value\":\"\", \"delimiter\":\"\", \"common\":{\"excluderegex\":\"\"}, \"disable_correlation\":\"1\"}},",
    "input_source": "local",
    "delete_local_file": true,
    "lookup_visible": true,
    "headers": "X-Custom-Header-A: Foo\nX-Custom-Header-B: Bar\n",
    "caching_enabled": true,
    "force_to_ids": true,
    "orgc_id": "12345",
    "cache_timestamp": "1617875568"
  },
  "Org": {
    "id": "12345",
    "name": "ORGNAME",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
  },
  "Orgc": {
    "id": "12345",
    "name": "ORGNAME",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
```

```
},
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"ShadowAttribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
```

```
    "last_seen": "1581984000000000"
  }
],
"RelatedEvent": [
  {}
],
"Galaxy": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "name": "Ransomware",
    "type": "ransomware",
    "description": "Ransomware galaxy based on ...",
    "version": "1",
    "icon": "globe",
    "namespace": "misp",
    "kill_chain_order": {
      "fraud-tactics": [
        "Initiation",
        "Target Compromise",
        "Perform Fraud",
        "Obtain Fraudulent Assets",
        "Assets Transfer",
        "Monetisation"
      ]
    }
  }
]
},
"Object": [
  {
    "id": "12345",
    "name": "ail-leak",
    "meta-category": "string",
    "description": "string",
    "template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "template_version": "1",
    "event_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
```

```
"sharing_group_id": "1",
"comment": "string",
"deleted": true,
"first_seen": "1581984000000000",
"last_seen": "1581984000000000",
"Attribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
},
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
]
```

```
],
"Tag": [
  {
    "id": "12345",
    "name": "tlp:white",
    "colour": "#ffffff",
    "exportable": true,
    "org_id": "12345",
    "user_id": "12345",
    "hide_tag": false,
    "numerical_value": "12345",
    "is_galaxy": true,
    "is_custom_galaxy": true,
    "inherited": 1
  }
]
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Get event by ID:

GET

Response:

200:

```
{
  "Event": {
    "id": "12345",
    "org_id": "12345",
    "distribution": "0",
    "info": "logged source ip",
    "orgc_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "date": "1991-01-15",
    "published": false,
    "analysis": "0",
    "attribute_count": "321",
    "timestamp": "1617875568",
    "sharing_group_id": "1",
    "proposal_email_lock": true,
    "locked": true,
    "threat_level_id": "1",
    "publish_timestamp": "1617875568",
    "sighting_timestamp": "1617875568",
    "disable_correlation": false,
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_creator_email": "user@example.com",
    "Feed": {
      "id": "3",
      "name": "CIRCL OSINT Feed",
      "provider": "CIRCL",
      "url": "https://www.circl.lu/doc/misp/feed-osint",
      "rules": "{\"tags\":{\"OR\":[],\"NOT\":[]},\"orgs\":{\"OR\":[],\"NOT\":[]},\"url_params\":{\"\"}}",
      "enabled": true,
      "distribution": "0",
      "sharing_group_id": "1",
      "tag_id": "12345",
      "default": true,
      "source_format": "1",
```

```
"fixed_event": true,
"delta_merge": true,
"event_id": "12345",
"publish": false,
"override_ids": true,
"settings":
"{\"csv\":{\"value\":\"\",\"delimiter\":\"\"},\"common\":{\"excluderegex\":\"\"},\"disable_correlation\":\"1\"}\",
  \"input_source\": \"local\",
  \"delete_local_file\": true,
  \"lookup_visible\": true,
  \"headers\": \"X-Custom-Header-A: Foo\\nX-Custom-Header-B: Bar\\n\",
  \"caching_enabled\": true,
  \"force_to_ids\": true,
  \"orgc_id\": \"12345\",
  \"cache_timestamp\": \"1617875568\"
},
\"Org\": {
  \"id\": \"12345\",
  \"name\": \"ORGNAME\",
  \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\"
},
\"Orgc\": {
  \"id\": \"12345\",
  \"name\": \"ORGNAME\",
  \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\"
},
\"Attribute\": [
  {
    \"id\": \"12345\",
    \"event_id\": \"12345\",
    \"object_id\": \"12345\",
    \"object_relation\": \"sensor\",
    \"category\": \"Internal reference\",
    \"type\": \"md5\",
    \"value\": \"127.0.0.1\",
    \"to_ids\": true,
    \"uuid\": \"c99506a6-1255-4b71-afa5-7b8ba48c3b1b\",
    \"timestamp\": \"1617875568\",
    \"distribution\": \"0\",
    \"sharing_group_id\": \"1\",
```

```
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"ShadowAttribute": [
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
],
"RelatedEvent": [
  {}
],
"Galaxy": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "name": "Ransomware",
    "type": "ransomware",
    "description": "Ransomware galaxy based on ...",
    "version": "1",
    "icon": "globe",
```

```
"namespace": "misp",
"kill_chain_order": {
  "fraud-tactics": [
    "Initiation",
    "Target Compromise",
    "Perform Fraud",
    "Obtain Fraudulent Assets",
    "Assets Transfer",
    "Monetisation"
  ]
}
},
],
"Object": [
{
  "id": "12345",
  "name": "ail-leak",
  "meta-category": "string",
  "description": "string",
  "template_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "template_version": "1",
  "event_id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "timestamp": "1617875568",
  "distribution": "0",
  "sharing_group_id": "1",
  "comment": "string",
  "deleted": true,
  "first_seen": "1581984000000000",
  "last_seen": "1581984000000000",
  "Attribute": [
    {
      "id": "12345",
      "event_id": "12345",
      "object_id": "12345",
      "object_relation": "sensor",
      "category": "Internal reference",
      "type": "md5",
      "value": "127.0.0.1",
      "to_ids": true,
```

```
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
}
],
"EventReport": [
  {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_id": "12345",
    "name": "Report of the incident",
    "content": "string",
    "distribution": "0",
    "sharing_group_id": "1",
    "timestamp": "1617875568",
    "deleted": false
  }
],
"Tag": [
  {
    "id": "12345",
    "name": "tlp:white",
    "colour": "#ffffff",
    "exportable": true,
    "org_id": "12345",
    "user_id": "12345",
    "hide_tag": false,
    "numerical_value": "12345",
    "is_galaxy": true,
    "is_custom_galaxy": true,
    "inherited": 1
  }
]
```

```
]
}
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Publish an event:

POST

<https://misp.local/events/publish/{eventId}>

Response:

200:

```
{
  "name": "Publish",
  "message": "Job queued",
  "url": "https://misp.local/events/alert/1",
  "id": "string"
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Unpublish an event:

POST

<https://misp.local/events/addTag/{eventId}/{tagId}/local:{local}>

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "Event unpublished.",
  "message": "Event unpublished.",
  "url": "/events/unpublish/1"
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the
Authorization header.",
```

```
"message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
"url": "/attributes"
}
```

Default:

```
{
  "name": "string",
  "message": "string",
  "url": "/attributes"
}
```

Add event tag:

POST

<https://misp.local/events/addTag/{eventId}/{tagId}/local:{local}>

Response:

200:

```
{
  "saved": true,
  "success": "Tag added.",
  "check_publish": true,
  "errors": "Tag could not be added."
}
```

403:

```
{
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the Authorization header.",
  "url": "/attributes"
}
```

Default:

```
{  
  "name": "string",  
  "message": "string",  
  "url": "/attributes"  
}
```

Remove event tag:

POST

<https://misp.local/events/removeTag/{eventId}/{tagId}>

Response:

200:

```
{  
  "saved": true,  
  "success": "Tag removed.",  
  "check_publish": true,  
  "errors": "Tag could not be added."  
}
```

403:

```
{  
  "name": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "message": "Authentication failed. Please make sure you pass the API key of an API enabled user along in the  
Authorization header.",  
  "url": "/attributes"  
}
```

Default:

```
{  
  "name": "string",  
  "message": "string",  
}
```

```
"url": "/attributes"
```

```
}
```

Revision #4

Created 13 April 2024 13:43:39 by İlayda Durlanık

Updated 13 April 2024 14:07:01 by İlayda Durlanık