

Galaxy Cluster

Add galaxy cluster:

GET

<https://misp.local/galaxies>

Request:

```
{
  "id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "type": "mitre-enterprise-attack-attack-pattern",
  "value": "Brute Force - T1110",
  "tag_name": "tlp:white",
  "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained...",
  "galaxy_id": "12345",
  "source": "https://github.com/mitre/cti",
  "authors": [
    "MITRE"
  ],
  "version": "1",
  "distribution": "0",
  "sharing_group_id": "1",
  "org_id": "12345",
  "orgc_id": "12345",
  "default": true,
  "locked": true,
  "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "extends_version": "1",
  "published": false,
  "deleted": false,
```

```
"GalaxyElement": [  
  {  
    "id": "12345",  
    "galaxy_cluster_id": "12345",  
    "key": "categories",  
    "value": "Military"  
  }  
]  
}
```

Response:

200:

```
{  
  "GalaxyCluster": {  
    "id": "12345",  
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "type": "mitre-enterprise-attack-attack-pattern",  
    "value": "Brute Force - T1110",  
    "tag_name": "tlp:white",  
    "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords  
are unknown or when password hashes are obtained...",  
    "galaxy_id": "12345",  
    "source": "https://github.com/mitre/cti",  
    "authors": [  
      "MITRE"  
    ],  
    "version": "1",  
    "distribution": "0",  
    "sharing_group_id": "1",  
    "org_id": "12345",  
    "orgc_id": "12345",  
    "default": true,  
    "locked": true,  
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
    "extends_version": "1",  
    "published": false,  
    "deleted": false,
```

```
"GalaxyElement": [  
  {  
    "id": "12345",  
    "galaxy_cluster_id": "12345",  
    "key": "categories",  
    "value": "Military"  
  }  
]  
}  
}
```

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"  
}
```

404:

```
{  
  "name": "Invalid attribute",  
  "message": "Invalid attribute",  
  "url": "/attributes/1234"  
}
```

Default:

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

Edit galaxy cluster

POST

https://misp.local/galaxy_clusters/add/{galaxyId}

Request:

```
{
  "id": "12345",
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "type": "mitre-enterprise-attack-attack-pattern",
  "value": "Brute Force - T1110",
  "tag_name": "tlp:white",
  "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained...",
  "galaxy_id": "12345",
  "source": "https://github.com/mitre/cti",
  "authors": [
    "MITRE"
  ],
  "version": "1",
  "distribution": "0",
  "sharing_group_id": "1",
  "org_id": "12345",
  "orgc_id": "12345",
  "default": true,
  "locked": true,
  "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  "extends_version": "1",
  "published": false,
  "deleted": false,
  "GalaxyElement": [
    {
      "id": "12345",
      "galaxy_cluster_id": "12345",
      "key": "categories",
      "value": "Military"
    }
  ]
}
```

```
}
```

Response:

200:

```
{
  "GalaxyCluster": {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "type": "mitre-enterprise-attack-attack-pattern",
    "value": "Brute Force - T1110",
    "tag_name": "tlp:white",
    "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords
are unknown or when password hashes are obtained...",
    "galaxy_id": "12345",
    "source": "https://github.com/mitre/cti",
    "authors": [
      "MITRE"
    ],
    "version": "1",
    "distribution": "0",
    "sharing_group_id": "1",
    "org_id": "12345",
    "orgc_id": "12345",
    "default": true,
    "locked": true,
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "extends_version": "1",
    "published": false,
    "deleted": false,
    "GalaxyElement": [
      {
        "id": "12345",
        "galaxy_cluster_id": "12345",
        "key": "categories",
        "value": "Military"
      }
    ]
  }
}
```

```
}  
}
```

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"  
}
```

404:

```
{  
  "name": "Invalid attribute",  
  "message": "Invalid attribute",  
  "url": "/attributes/1234"  
}
```

Default:

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

Get galaxy clusters:

GET

https://misp.local/galaxy_clusters/add/{galaxyId}

Response:

200:

```
[
  {
    "GalaxyCluster": {
      "id": "12345",
      "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "type": "mitre-enterprise-attack-attack-pattern",
      "value": "Brute Force - T1110",
      "tag_name": "tlp:white",
      "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords
are unknown or when password hashes are obtained...",
      "galaxy_id": "12345",
      "source": "https://github.com/mitre/cti",
      "authors": [
        "MITRE"
      ],
      "version": "1",
      "distribution": "0",
      "sharing_group_id": "1",
      "org_id": "12345",
      "orgc_id": "12345",
      "default": true,
      "locked": true,
      "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "extends_version": "1",
      "published": false,
      "deleted": false,
      "GalaxyElement": [
        {
          "id": "12345",
          "galaxy_cluster_id": "12345",
          "key": "categories",
          "value": "Military"
        }
      ]
    }
  }
]
```

```
{
  "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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Search galaxy clusters:

POST

https://misp.local/galaxy_clusters/add/{galaxyId}

Request:

```
{
  "context": "all",
  "searchall": "botnet"
}
```

Response:

200:


```
[
  {
    "GalaxyCluster": {
      "id": "12345",
      "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "type": "mitre-enterprise-attack-attack-pattern",
      "value": "Brute Force - T1110",
      "tag_name": "tlp:white",
      "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords
are unknown or when password hashes are obtained...",
      "galaxy_id": "12345",
      "source": "https://github.com/mitre/cti",
      "authors": [
        "MITRE"
      ],
      "version": "1",
      "distribution": "0",
      "sharing_group_id": "1",
      "org_id": "12345",
      "orgc_id": "12345",
      "default": true,
      "locked": true,
      "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
      "extends_version": "1",
      "published": false,
      "deleted": false,
      "GalaxyElement": [
        {
          "id": "12345",
          "galaxy_cluster_id": "12345",
          "key": "categories",
          "value": "Military"
        }
      ]
    }
  }
]
```

```
{
  "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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Get galaxy cluster by ID:

Get

https://misp.local/galaxy_clusters/view/{galaxyClusterId}

Response:

200:

```
{
  "GalaxyCluster": {
    "id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "collection_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
  }
}
```

```
"type": "mitre-enterprise-attack-attack-pattern",
"value": "Brute Force - T1110",
>tag_name": "tlp:white",
"description": "Adversaries may use brute force techniques to attempt access to accounts when passwords
are unknown or when password hashes are obtained...",
"galaxy_id": "12345",
"source": "https://github.com/mitre/cti",
"authors": [
  "MITRE"
],
"version": "1",
"distribution": "0",
"sharing_group_id": "1",
"org_id": "12345",
"orgc_id": "12345",
"default": true,
"locked": true,
"extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
"extends_version": "1",
"published": false,
"deleted": false,
"GalaxyElement": [
  {
    "id": "12345",
    "galaxy_cluster_id": "12345",
    "key": "categories",
    "value": "Military"
  }
],
"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"
  ]
}
},
"GalaxyClusterRelation": [
  {
    "id": "12345",
    "galaxy_cluster_id": "12345",
    "key": "categories",
    "value": "Military"
  }
],
"Org": {
  "id": "12345",
  "name": "ORGNAME",
  "date_created": "2021-06-14 14:29:19",
  "date_modified": "2021-06-14 14:29:19",
  "description": "string",
  "type": "ADMIN",
  "nationality": "string",
  "sector": "string",
  "created_by": "12345",
  "uuid": "string",
  "contacts": "string",
  "local": true,
  "restricted_to_domain": [
    "example.com"
  ],
  "landingpage": "string",
  "user_count": "3",
  "created_by_email": "string"
},
"Orgc": {
  "id": "12345",
  "name": "ORGNAME",
```

```
"date_created": "2021-06-14 14:29:19",
"date_modified": "2021-06-14 14:29:19",
"description": "string",
"type": "ADMIN",
"nationality": "string",
"sector": "string",
"created_by": "12345",
"uuid": "string",
"contacts": "string",
"local": true,
"restricted_to_domain": [
  "example.com"
],
"landingpage": "string",
"user_count": "3",
"created_by_email": "string"
},
"tag_count": 0,
"tag_id": "12345"
}
}
```

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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Publish galaxy cluster:

POST

https://misp.local/galaxy_clusters/publish/{galaxyClusterId}

Response:

200:

```
{
  "message": "Publish job queued. Job ID: 4e9d26c275a7b190fcab10029df8c6b6"
}
```

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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Unpublish galaxy cluster:

POST

https://misp.local/galaxy_clusters/unpublish/{galaxyClusterId}

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "GalaxyCluster unpublished",
  "message": "GalaxyCluster unpublished",
  "url": "/galaxy_clusters/publish/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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
}
```

```
"url": "/attributes/1234"
}
```

Default:

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

Delete galaxy cluster:

POST

https://misp.local/galaxy_clusters/unpublish/{galaxyClusterId}

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "Galaxy cluster successfully soft deleted.",
  "message": "Galaxy cluster successfully soft deleted.",
  "url": "/galaxy_clusters/delete/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"
}
```

404:


```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Restore galaxy cluster:

POST

https://misp.local/galaxy_clusters/unpublish/{galaxyClusterId}

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "GalaxyCluster restored",
  "message": "GalaxyCluster restored",
  "url": "/galaxy_clusters/restore/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"
}
```

404:

```
{
  "name": "Invalid attribute",
  "message": "Invalid attribute",
  "url": "/attributes/1234"
}
```

Default:

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

Revision #3

Created 13 April 2024 15:30:22 by İlayda Durlanık

Updated 13 April 2024 16:04:43 by İlayda Durlanık