

Galaxies

Get galaxies:

GET

<https://misp.local/galaxies>

Response:

200:

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

```
]
```

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 galaxies:

POST

<https://misp.local/galaxies>

Request:

```
{
  "value": "botnet"
}
```

Response:

200:

```
[
  {
```

```
"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"
    ]
  }
}
```

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 galaxy by ID:

POST

<https://misp.local/galaxies>

Response:

200:

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

```

Default:

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

Force update the galaxies with the galaxy json definitions:

POST

<https://misp.local/galaxies/update>

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "Galaxies updated.",
  "message": "Galaxies updated.",
  "url": "/galaxies/update"
}
```

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 a galaxy:

DELETE

<https://misp.local/galaxies/delete/{galaxyId}>

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "Galaxy deleted",
  "message": "Galaxy deleted",
  "url": "/galaxies/delete"
}
```

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"
}
```

Import a galaxy cluster:

POST

<https://misp.local/galaxies/import>

Request:

```
[
  {
    "GalaxyCluster": {
      "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": {
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b"
}
}
```

Response:

200:

```
{
  "saved": true,
  "success": true,
  "name": "'Galaxy clusters imported. 1 imported, 0 ignored, 0 failed.",
  "message": "'Galaxy clusters imported. 1 imported, 0 ignored, 0 failed.",
  "url": "/galaxies/import"
}
```

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"
}
```

Export galaxy clusters

POST

<https://misp.local/galaxies/export/{galaxyId}>

Request:

```
{
  "Galaxy": {
    "default": true,
    "custom": true,
    "distribution": "0",
    "format": "default",
    "download": true
  }
}
```

```
}  
}
```

Response:

200:

GalaxyMispFormat:

```
{  
  "name": "Ransomware",  
  "type": "ransomware",  
  "authors": [  
    "MITRE"  
  ],  
  "version": true,  
  "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
  "source": "https://github.com/mitre/cti",  
  "values": [  
    {  
      "description": "Adversaries may use brute force techniques to attempt access to accounts when passwords  
are unknown or when password hashes are obtained...",  
      "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
      "value": "Brute Force - T1110",  
      "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",  
      "extends_Version": "1",  
      "meta": [  
        {  
          "categories": "botnet"  
        },  
        {  
          "refs": "http://example.com"  
        },  
        {  
          "aliases": [  
            "malware",  
            "win32",  
            "windows"  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```
    },
    {
      "topics": [
        "Windows",
        "Malware"
      ]
    }
  ]
}
```

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"
}
```

Attach the galaxy cluster tag a given entity

POST

https://misp.local/galaxies/attachCluster/{attachTargetId}/{attachTargetType}/local:{local}

Request:

```
{
  "Galaxy": {
    "target_id": 1235
  }
}
```

Response:

200:

```
{
  "saved": true,
  "success": "Cluster attached.",
  "check_publish": true
}
```

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 #2

Created 13 April 2024 14:59:08 by İlayda Durlanık

Updated 13 April 2024 15:28:56 by İlayda Durlanık