

Integrations

StixTaxii For Director Console API

V6.0.0

CONTENTS

1	StixTaxii Application	1
2	Installation	2
2.1	Prerequisites	2
2.2	Uploading the StixTaxii Application to the Fabric Storage	2
2.3	Listing the StixTaxii Application in the Fabric Storage	4
2.4	Installing the StixTaxii Application in LogPoint	4
3	Configuration	6
3.1	Uploading a SSL Certificate File in the Fabric Storage	6
3.2	Listing the SSL Certificate File in the Fabric Storage	8
3.3	Configuring the STIX/TAXII Enrichment Source for STIX v1.0	10
3.4	Configuring the STIX/TAXII Enrichment Source for STIX v2.0	14
3.5	General Information	18
3.6	Listing all the StixTaxii Enrichment Source Configurations	18
3.7	Editing the STIX/TAXII Enrichment Source Configuration	19
3.8	Deleting the STIX/TAXII Enrichment Source Configuration	23
3.9	Deleting the SSL Certificate File in the Fabric Storage	23
4	Uninstallation	26
4.1	Uninstalling the StixTaxii Application in LogPoint	26
5	StixTaxii - RefreshList	27
5.1	Refreshing the list for StixTaxii Collections	27
6	StixTaxii - Trash	28
6.1	Deleting the StixTaxii Application from the Fabric Storage	28

STIXTAXII APPLICATION

The StixTaxii application adds a threat intelligence source in LogPoint's Threat Intelligence application to enrich logs with cyber threat intelligence (CTI). The CTI is written in *STIX* format and is shared via a *TAXII* server. The application supports *STIX* version 1.0 and 2.0.

INSTALLATION

2.1 Prerequisites

- Director Fabric v1.4.0 or later
- Director Console v1.6.0 or later
- LogPoint v6.12.2 or later
- Threat Intelligence v5.0.0 or later

2.2 Uploading the StixTaxii Application to the Fabric Storage

2.2.1 Private Storage

You can upload the StixTaxii application to a *private storage* in the Fabric Storage using the **Upload - Upload** API.

Endpoint URL:

`https://api-server-host-name/configapi/Uploads/{pool_UUID}/`

Method:

`POST`

Header:

FIELD	DESCRIPTION
file_name	Name of the StixTaxii pak file.
Content-Type	Content type of the StixTaxii pak file. It must be (<i>application/octet-stream</i>).

Parameters:

FIELD	TYPE	DESCRIPTION	REQUIRED
file	[Object]	The StixTaxii pak file to be uploaded.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "StixTaxii_6.0.0.pak successfully uploaded in the private storage. "
}
```

2.2.2 Public Storage

You can upload the StixTaxii application to a *public storage* in the Fabric Storage using the **Upload - UploadPublic files** API.

Endpoint URL:

```
https://api-server-host-name/configapi/Uploads/PublicUpload
```

Method:

```
POST
```

Header:

FIELD	DESCRIPTION
file_name	Name of the StixTaxii pak file.
Content-Type	Content type of the StixTaxii pak file. It must be (application/octet-stream).

Parameters:

FIELD	TYPE	DESCRIPTION	REQUIRED
file	[Object]	The StixTaxii pak file to be uploaded.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "StixTaxii_6.0.0.pak successfully uploaded in the public storage. "
}
```

2.3 Listing the StixTaxii Application in the Fabric Storage

2.3.1 Private Storage

You can list the StixTaxii application file uploaded in the private storage using the **Upload - List** API.

Endpoint URL:

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/list
```

Method:

```
GET
```

Success Response:

```
[  
  "StixTaxii_6.0.0.pak"  
]
```

2.3.2 Public Storage

You can list the StixTaxii application file uploaded in the public storage using the **Upload - ListPublic** API.

Endpoint URL:

```
https://api-server-host-name/configapi/Uploads/list
```

Method:

```
GET
```

Success Response:

```
[  
  "StixTaxii_6.0.0.pak"  
]
```

2.4 Installing the StixTaxii Application in LogPoint

You can install the StixTaxii application in LogPoint using the **Upload - Install** API. You must upload the application package to the Fabric Storage before the installation.

Endpoint URL:

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/{logpoint_identifier}/install
```

Method:

```
POST
```

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
application_type	–	String	Type of the application. Must be <i>Application</i> .	Mandatory
file_name	File	String	Name of the application file.	Mandatory
file_location	–	String	Location of the application file. Can be either <i>private</i> or <i>public</i> .	Mandatory

Request Example:

```
{
  "data": {
    "application_type": "Application",
    "file_name": "stixtaxii_6.0.0.pak",
    "file_location": "private"
  }
}
```

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CONFIGURATION

3.1 Uploading a SSL Certificate File in the Fabric Storage

3.1.1 Private Storage

You can upload a SSL certificate file to a private storage in the Fabric storage using the **PluginConfiguration-Upload** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/  
→StixTaxiiEnrichmentSource/upload
```

Method:

```
POST
```

Header:

FIELD	LABEL IN UI	DESCRIPTION
Content-Type	–	Content type of the certificate file. It must be <i>Multipart/Form-data</i> .

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
file_name	–	Object	File to be uploaded.	Mandatory

Success Response:

```
{  
  "status": "Success",  
}
```

(continues on next page)

(continued from previous page)

```
"message": "certificate.crt successfully uploaded in private storage."
}
```

3.1.2 Public Storage

You can upload a SSL certificate file to a public storage in the Fabric storage using the **PluginConfiguration-UploadPublic** API.

Endpoint URL:

```
https://api-server-host-name/configapi/PluginConfiguration/StixTaxiiEnrichmentSource/
↪publicupload
```

Method:

```
POST
```

Header:

FIELD	LABEL IN UI	DESCRIPTION
Content-Type	–	Content type of the certificate file. It must be <i>Multipart/Form-data</i> .

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
file_name	–	Object	File to be uploaded.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "certificate.crt successfully uploaded in public storage."
}
```

3.2 Listing the SSL Certificate File in the Fabric Storage

3.2.1 List Private Uploads

You can list the uploaded files to a private storage in the Fabric storage using the **PluginConfiguration-ListPrivateUploads** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/
↪StixTaxiiEnrichmentSource/list
```

Method:

```
GET
```

Success Response:

```
[  
  "certificate.crt",  
  "privateKey.key"  
]
```

3.2.2 List Public Uploads

You can list the uploaded files to a public storage in the Fabric storage using the **PluginConfiguration-ListPublicUploads** API.

Endpoint URL:

```
https://api-server-host-name/configapi/PluginConfiguration/StixTaxiiEnrichmentSource/list
```

Method:

```
GET
```

Success Response:

```
[
  "certificate.crt",
  "privateKey.key"
]
```

3.3 Configuring the STIX/TAXII Enrichment Source for STIX v1.0

You can configure the StixTaxii Enrichment Source in a Fabric-enabled LogPoint using the **PluginConfiguration - Create** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪ StixTaxiiEnrichmentSource
```

Method:

```
POST
```

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
st_enable_source	Enable Source	boolean	Parameter to enable or disable fetching of STIX data from a TAXII server.	Mandatory

Continued on next page

Table 1 – continued from previous page

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
discovery_url	Base URL	String	Location of the discovery service in the <i>TAXII</i> server.	Mandatory
begin	Fetch From	int	Parameter to fetch data from the last selected month, hour, or day.	Mandatory
begin_unit	Fetch From	String	Unit of the begin.	Mandatory
fetch_interval	Fetch Interval	int	An interval between the adjacent fetches.	Mandatory
fetch_interval_unit	Fetch Interval	String	Unit of the fetch interval.	Mandatory
stix_version	Version	String	STIX Version.	Mandatory
basic_auth_mode	Basic Authentication	JSON	Basic Authentication: basic_auth_status: Parameter to enable or disable the basic authentication. username: Username of the <i>TAXII</i> server. password: Password of the <i>TAXII</i> server.	Mandatory

Continued on next page

Table 1 – continued from previous page

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
ssl_mode	SSL Authentication	JSON	SSL Authentication: ssl_status: Parameter to enable or disable the SSL authentication. key_pass: Password used to decrypt the SSL key.	Mandatory
file_location	–	String	Location of the file.	Mandatory
files	Files	JSON	SSL configuration of the <i>TAXII</i> server: cert_file: SSL certificate. cert_key: SSL key.	Mandatory
st_proxy	Proxy Configuration	JSON	Proxy configuration of the <i>TAXII</i> server: status: Parameter to enable or disable the proxy server. ip: IP of the proxy server. port: Port of the proxy server. protocol: <i>HTTP</i> or <i>HTTPS</i> protocol used by the proxy server.	Mandatory

Request Example:

```
{
  "data":{
    "st_enable_source": true,
    "discovery_url": "https://open.taxiistand.com/services/discovery",
    "fetch_interval": 2,
    "fetch_interval_unit": "Days",
    "begin": 20,
    "begin_unit": "Days",
    "st_proxy": {
      "status": false,
      "ip": "127.0.0.1",
      "protocol": "http",
      "port": 22
    },
    "ssl_mode":{
      "ssl_status": false,
      "key_pass": "12345"
    },
    "file_location": "public",
    "files": {
      "cert_file": "client.crt",
      "cert_key": "client.key"
    },
    "stix_version": "1",
    "basic_auth_mode": {
      "username": "guest",
      "basic_auth_status": false,
      "password": "guest"
    }
  }
}
```

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

3.4 Configuring the STIX/TAXII Enrichment Source for STIX v2.0

You can configure the StixTaxii Enrichment Source in a Fabric-enabled LogPoint using the **PluginConfiguration - Create API**.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/  
↪ StixTaxiiEnrichmentSource
```

Method:

POST

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
st_enable_source	Enable Source	boolean	Parameter to enable or disable fetching of STIX data from a TAXII server.	Mandatory
discovery_url	Base URL	String	Location of the discovery service in the TAXII server.	Mandatory
begin	Fetch From	int	Parameter to fetch data from the last selected month, hour, or day.	Mandatory
begin_unit	Fetch From	String	Unit of the begin.	Mandatory
fetch_interval	Fetch Interval	int	An interval between the adjacent fetches.	Mandatory
fetch_interval_unit	Fetch Interval	String	Unit of the fetch interval.	Mandatory
stix_version	Version	String	STIX Version.	Mandatory

Continued on next page

Table 2 – continued from previous page

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
basic_auth_mode	Basic Authentication	JSON	Basic Authentication: basic_auth_status: Parameter to enable or disable the basic authentication. username: Username of the <i>TAXII</i> server. password: Password of the <i>TAXII</i> server.	Mandatory
ssl_mode	SSL Authentication	JSON	SSL Authentication: ssl_status: Parameter to enable or disable the SSL authentication. key_pass: Password used to decrypt the SSL key.	Mandatory
file_location	–	String	Location of the file.	Mandatory
files	Files	JSON	SSL configuration of the <i>TAXII</i> server: cert_file: SSL certificate. cert_key: SSL key.	Mandatory

Continued on next page

Table 2 – continued from previous page

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
st_proxy	Proxy Configuration	JSON	Proxy configuration of the <i>TAXII</i> server: status: Parameter to enable or disable the proxy server. ip: IP of the proxy server. port: Port of the proxy server. protocol: <i>HTTP</i> or <i>HTTPS</i> protocol used by the proxy server.	Mandatory

Request Example:

```
{
  "data":{
    "st_enable_source": true,
    "discovery_url": "https://open.taxiistand.com/services/discovery",
    "fetch_interval": 2,
    "fetch_interval_unit": "Days",
    "begin": 20,
    "begin_unit": "Days",
    "st_proxy": {
      "status": false,
      "ip": "127.0.0.1",
      "protocol": "http",
      "port": 22
    },
    "ssl_mode":{
      "ssl_status": false,
      "key_pass": "12345"
    },
    "file_location": "public",
    "files": {
      "cert_file": "client.crt",
      "cert_key": "client.key"
    },
    "stix_version": "2",
    "basic_auth_mode": {
      "username": "guest",
      "basic_auth_status": false,
      "password": "guest"
    }
  }
}
```

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

3.5 General Information

You can get an overview of the fetched information from STIX/TAXII using the **PluginConfiguration-List** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪ Ti_general
```

Method:

```
GET
```

Success Response:

```
[
  {
    "services": {
      "stix_taxii": {
        "last_successful_fetch": 0,
        "name": "Stix Taxii",
        "error": null,
        "fetch_status": "Completed",
        "no_of_entries": 0,
        "last_fetch_attempt": 1569403863
      },
    },
    "no_of_entries": 0,
    "type": "ti_general",
    "tid": "",
    "id": "5c81f48e10959135395cabea"
  }
]
```

3.6 Listing all the StixTaxii Enrichment Source Configurations

You can list the StixTaxii configurations using the **PluginConfiguration - List** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪ Ti_stixtaxii
```

Method:

GET

Success Response:

```
[
  {
    "st_proxy": {
      "status": true,
      "ip": "127.0.0.1",
      "protocol": "http",
      "port": 22
    },
    "begin": 1,
    "ssl_mode": {
      "key_pass": "pass1",
      "ssl_status": True
    },
    "cert_file": "certificate.crt",
    "cert_key": "privateKey.key",
    "id": "5d8b2a522be2374b84949c82",
    "basic_auth_mode": {
      "username": "user1",
      "basic_auth_status": true,
      "password": "psw1"
    },
    "stix_version": "2",
    "fetch_interval": 1,
    "st_enable_source_confirmed": false,
    "tid": "",
    "discovery_url": "http://taxiiserver.com/taxii-discovery-service",
    "fetch_interval_unit": "Hours",
    "st_enable_source": true
  }
]
```

3.7 Editing the STIX/TAXII Enrichment Source Configuration

You can edit a StixTaxii configuration in a Fabric-enabled LogPoint using the **PluginConfiguration - Edit API**.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪ StixTaxiiEnrichmentSource/{id}
```

Method:

PUT

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
st_enable_source	Enable Source	boolean	Parameter to enable or disable fetching of <i>STIX</i> data from a <i>TAXII</i> server.	Mandatory
discovery_url	Base URL	String	Location of the discovery service in the <i>TAXII</i> server.	Mandatory
begin	Fetch From	int	Parameter to fetch data from the last selected month, hour, or day.	Mandatory
begin_unit	Fetch From	String	Unit of the begin.	Mandatory
fetch_interval	Fetch Interval	int	An interval between the adjacent fetches.	Mandatory
fetch_interval_unit	Fetch Interval	String	Unit of the fetch interval.	Mandatory
stix_version	Version	String	<i>STIX</i> Version.	Mandatory
basic_auth_mode	Basic Authentication	JSON	Basic Authentication: basic_auth_status: Parameter to enable or disable the basic authentication. username: Username of the <i>TAXII</i> server. password: Password of the <i>TAXII</i> server.	Mandatory
ssl_mode	SSL Authentication	JSON	SSL Authentication: ssl_status: Parameter to enable or disable the SSL authentication. key_pass: Password used to decrypt the SSL key.	Mandatory
file_location	–	String	Location of the file.	Mandatory

Continued on next page

Table 3 – continued from previous page

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
files	Files	JSON	SSL configuration of the <i>TAXII</i> server: cert_file : SSL certificate. cert_key : SSL key.	Mandatory
st_proxy	Proxy Configuration	JSON	Proxy configuration of the <i>TAXII</i> server: status : Parameter to enable or disable the proxy server. ip : IP of the proxy server. port : Port of the proxy server. protocol : <i>HTTP</i> or <i>HTTPS</i> used by the proxy server.	Mandatory
id	–	String	Existing StixTaxii Enrichment Source ID . Obtain the value of the ID using the StixTaxiiEnrichmentSource - List API.	Mandatory

Request Example:

```
{
  "data":{
    "st_enable_source": true,
    "discovery_url": "https://open.taxiistand.com/services/discovery",
    "fetch_interval": 2,
    "fetch_interval_unit": "Days",
    "begin": 20,
    "begin_unit": "Days",
    "st_proxy": {
      "status": false,
      "ip": "127.0.0.1",
      "protocol": "http",
      "port": 22
    },
    "ssl_mode": {
      "ssl_status": false,
      "key_pass": "12345"
    },
    "file_location": "public",
    "files": {
      "cert_file": "client.crt",
      "cert_key": "client.key"
    },
    "stix_version": "2",
    "basic_auth_mode": {
      "username": "guest",
      "basic_auth_status": false,
      "password": "guest"
    }
  }
}
```

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```


3.8 Deleting the STIX/TAXII Enrichment Source Configuration

You can delete a StixTaxii configuration in a Fabric-enabled LogPoint using the **PluginConfiguration - Trash** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪StixTaxiiEnrichmentSource/{id}
```

Method:

Delete

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
id	–	String	Existing StixTaxiiEnrichmentSource id . Obtain the value of the ID using the StixTaxiiEnrichmentSource - List API	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

3.9 Deleting the SSL Certificate File in the Fabric Storage

3.9.1 Trash Private Uploads

You can delete the uploaded certificate files in a private storage in the Fabric storage using the **PluginConfiguration-TrashPrivateUploads** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/
↪StixTaxiiEnrichmentSource/{file_name}
```

Method:

DELETE

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
file_name	–	String	File to be deleted.	Mandatory

Success Response:

```
{  
  "status": "Success",  
  "message": "certificate.crt successfully deleted."  
}
```

3.9.2 Trash Public Uploads

You can delete the certificate uploaded files in a public storage in the Fabric storage using the **PluginConfiguration-TrashPublicUploads** API.

Endpoint URL:

```
https://api-server-host-name/configapi/PluginConfiguration/StixTaxiiEnrichmentSource/{file_↵name}
```

Method:

```
DELETE
```

Header:

FIELD	LABEL IN UI	DESCRIPTION
Content-Type	–	Content type of the certificate file. It must be <i>Multipart/Form-data</i> .

Parameters:

FIELD	LABEL IN UI	TYPE	DESCRIPTION	REQUIRED
file_name	–	String	File to be deleted.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "certificate.crt successfully deleted."
}
```

UNINSTALLATION

4.1 Uninstalling the StixTaxii Application in LogPoint

You can uninstall the StixTaxii application in a Fabric-enabled LogPoint using the **Plugins - Uninstall** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Plugins/{id}
```

Method:

```
DELETE
```

Parameters:

FIELD	TYPE	DESCRIPTION	REQUIRED
id	String	The ID of the existing StixTaxii application. Obtain the value of the ID using the StixTaxiiEnrichmentSource - List API.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

STIXTAXII - REFRESHLIST

5.1 Refreshing the list for StixTaxii Collections

You can refresh the updated collections of StixTaxii application using the **PluginConfiguration - RefreshList** API.

Endpoint URL:

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/  
↪ StixTaxiiEnrichmentSource/refreshlist
```

Method:

```
POST
```

Request Example:

```
{  
  "data": {  
  }  
}
```

Success Response:

```
{  
  "status": "Success",  
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"  
}
```

STIXTAXII - TRASH

6.1 Deleting the StixTaxii Application from the Fabric Storage

6.1.1 Private Uploads

You can delete the StixTaxii application package from a private storage in the Fabric Storage using the **Upload - TrashPrivate** API.

Endpoint URL:

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/{file_name}
```

Method:

```
DELETE
```

Parameters:

FIELD	TYPE	DESCRIPTION	REQUIRED
id	String	StixTaxii application ID. Obtain the ID of the StixTaxiiEnrichmentSource application using the Plugins - List API.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

6.1.2 Public Uploads

You can delete the StixTaxii application package from a public storage in the Fabric Storage using the **Upload - TrashPrivate** API.

Endpoint URL:

`https://api-server-host-name/configapi/Uploads/{file_name}`

Method:

DELETE

Parameters:

FIELD	TYPE	DESCRIPTION	REQUIRED
id	String	StixTaxii application ID. Obtain the ID of the StixTaxiiEnrichmentSource application using the Plugins - List API.	Mandatory

Success Response:

```
{
  "status": "Success",
  "message": "monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id} "
}
```