TAXII™ 2.0 Specification

Version 2.0-draft-3

Technical Committee

OASIS Cyber Threat Intelligence (CTI) TC

​Chair

Richard Struse (Richard.Struse@hq.dhs.gov), DHS Office of Cybersecurity and Communications (CS&C)

​Editors

Bret Jordan (bret.jordan@bluecoat.com), Blue Coat Systems, Inc.

Mark Davidson (mdavidson@soltra.com), Soltra

Document Table of Contents

[​1.​ Introduction](#_p93xzd8olzi2)

[​1.1.​ Terminology](#_zcasp8dvxi0s)

[​1.2.​ Overview](#_g6vzg6qixpic)

[​1.2.1.​ Channels Overview](#_pvch43p5vc0z)

[​1.2.2.​ Collections Overview](#_802in1vgfpd)

[​1.3.​ Document Conventions](#_ag2gxbmaqwjw)

[​1.3.1.​ Naming Conventions](#_kv0cuh34vz98)

[​1.3.2.​ Font Colors and Style](#_oh4kptyswepb)

[​2.​ HTTPS Requirements](#_p6ecyqmxyc28)

[​3.​ DNS SRV Records](#_u96rtngphsyd)

[​3.1.​ Requirements](#_a53mif7bp6u8)

[​3.2.​ Example](#_3tfp5dw5jix2)

[​4.​ Discovery API](#_siot3t264oqc)

[​4.1.​ Requirements](#_nmxe82szeuim)

[​4.2.​ Examples](#_3bi0ydmdni7f)

[​5.​ API Root](#_v0ej2u2q3xsd)

[​5.1.​ Requirements](#_a5dhqu6o459w)

[​5.2.​ Examples](#_p2jdsjfawjov)

[​6.​ Content Negotiation](#_vwl52ujjvbnw)

[​6.1.​ TAXII Media Type](#_j42p2xcnwfj0)

[​6.1.1.​ Requirements](#_7hr210mq3phv)

[​6.2.​ STIX Media Type](#_mp0mg6dhwpg2)

[​6.2.1.​ Requirements](#_d9gfdglkgj8o)

[​7.​ Primitive Types](#_1fev7l7zi12l)

[​8.​ TAXII API](#_dwru50atx72x)

[​8.1.​ URL Endpoint Summary](#_elkweoitcg95)

[​8.2.​ URL Parameters](#_w16tj2673s8q)

[​8.3.​ Global Requirements](#_q0a03pfr5x7n)

[​8.3.1.​ Property and String Requirements](#_d9ck4mk7uz34)

[​8.3.2.​ Server Requirements](#_vsjiqzz0xi0c)

[​8.3.3.​ Client Requirements](#_j42im6jb6cop)

[​8.4.​ HTTP Status Codes](#_stvpbojnarvw)

[​8.5.​ GET <discovery>](#_rqkm7tkh8t9g)

[​8.5.1.​ Requirements](#_gwp8881s74nw)

[​8.5.2.​ Examples](#_rdwsl0x8vzgi)

[​8.6.​ GET <api-root>](#_subu0a1w5bvt)

[​8.6.1.​ Requirements](#_o5w53j5ujrf3)

[​8.6.2.​ Examples](#_w13xtrxniipa)

[​8.7.​ GET /collections](#_g5nhvit9iwpo)

[​8.7.1.​ Requirements](#_pc8xid62pihu)

[​8.7.2.​ Examples](#_slh9qy7irtbs)

[​8.8.​ GET /collections/<name>](#_8akkdelgbkrg)

[​8.8.1.​ Requirements](#_7gv0zwr5d6w2)

[​8.8.2.​ Examples](#_29z35kort578)

[​8.9.​ GET /collections/<name>/manifest](#_4jiwyx7i0uyw)

[​8.9.1.​ Requirements](#_p4b92bhu0t34)

[​8.9.2.​ Examples](#_ilpyypj1oxcn)

[​8.10.​ GET /collections/<name>/objects](#_xlss9yvcfjov)

[​8.10.1.​ Requirements](#_5la3bxa91pil)

[​8.10.2.​ Examples](#_qc26j74jmr4m)

[​8.11.​ POST /collections/<name>/objects](#_4miz6vh6cpf5)

[​8.11.1.​ Requirements](#_gqml9e7wxzhp)

[​8.11.2.​ Examples](#_ct7u7f9jo87m)

[​8.12.​ GET /collections/<name>/objects/<object-id>](#_9y37u2nt5euw)

[​8.12.1.​ Requirements](#_3lxnc6obj31j)

[​8.12.2.​ Examples](#_p8xy89pw8463)

[​8.13.​ GET /object-search](#_j7iynwo77sal)

[​8.13.1.​ Requirements](#_cqvlfse0u84o)

[​8.13.2.​ Examples](#_oi3pb45wosrb)

[​8.14.​ GET /status/<status-id>](#_qhki2dow699u)

[​8.14.1.​ Requirements](#_oskl9x63r9bj)

[​8.14.2.​ Examples](#_zebb4as1lofe)

[​9.​ TAXII Resources](#_yeo5yj6uksa9)

[​9.1.​ API Root Resource](#_3n5r3cjoheja)

[​9.2.​ Discovery Resource](#_cnwttwtm2b4k)

[​9.3.​ Collection Resource](#_868250i2vzaz)

[​9.4.​ Error Resource](#_x3qvuund7mi1)

[​9.4.1.​ Example](#_b9atqvcnppmp)

[​9.5.​ Manifest Resource](#_wnjjf6o4mwjt)

[​9.6.​ Object Resource](#_mzunvkrv37rh)

[​9.7.​ Status Resource](#_21tzry6u9dbz)

[​10.​ Customizing TAXII Resources](#_5p0etrr85v8y)

[​10.1.​ Custom Properties](#_cuhggiw0s7fa)

[​10.1.1.​ Requirements](#_3a2x3jdr23tq)

[​11.​ Conformance](#_a0iri07jww47)

[​11.1.​ TAXII Servers](#_2c6m6fwix6p8)

[​11.2.​ Mandatory Features](#_afah9h2pxi28)

[​11.2.1.​ TODO](#_gygtg7mt1jza)

[​11.3.​ Optional Features](#_vdnporb6fgle)

[​11.3.1.​ TODO](#_ymvi1pwwcv6h)

[​12.​ Appendix A. Acknowledgments](#_qwt9kyfe5esq)

[​13.​ Appendix B. Changes from TAXII 1.1](#_kvom18a55dqz)

[​14.​ Appendix C - End to End Workflow](#_36r8f5dnhpyt)

[​15.​ Appendix D - Security Considerations](#_ldhi1g1rg5ug)

# ​1.​ Introduction​1.​ Introduction

TAXII is an open application layer protocol for the communication of cyber threat information. Focusing on simplicity and scalability, TAXII enables authenticated and secure communication of cyber threat information across products and organizations.

This specification defines the TAXII RESTful API and its resources along with the requirements for TAXII Client and Server implementations.

## ​1.1.​ Terminology​1.1.​ Terminology

The keywords “**MUST**”, “**MUST NOT**”, “**REQUIRED**”, “**SHALL**”, “**SHALL NOT**”, “**SHOULD**”, “**SHOULD NOT**”, “**RECOMMENDED**”, “**MAY**”, and “**OPTIONAL**” in this document are to be interpreted as described in RFC2119 (REF:RFC2119).

**API Root** - An instance of the TAXII API that is often used to align to trust groups.

**API Root URL** - Is the “root” URL for any particular instance of the TAXII API.

**Channel** - A publish-subscribe communications method where messages are exchanged.

**CTI** - Cyber Threat Intelligence

**Collection** - Is a logical group of CTI objects.

**Consumer** - Any entity that receives content via TAXII.

**Discovery Resource** - Contains information about a TAXII Server, including the various API Roots that it knows about.

**Message** - A resource transmitted over a Channel from producer to consumer.

**MTI** - Mandatory to Implement

**Object Resource** - CTI that is often represented in STIX.

**Producer** - Any entity that sends content via TAXII.

**Status Resource** - Contains information about an action that was processed asynchronously.

**STIX** - Structured Threat Information Expression

**STIX Content** - STIX documents, including STIX Objects, grouped as STIX Bundles.

**STIX Object** - A STIX Domain Object (SDO) or STIX Relationship Object (SRO)

**TAXII** - Trusted Automated Exchange of Indicator Information

**TAXII API** -

**TAXII Client** -

**TAXII Server** - A system that supports the exchange of CTI between TAXII Clients known as producers and consumers.

## ​1.2.​ Overview​1.2.​ Overview

This specification defines two communication methods - Channels and Collections - for transmitting CTI. TAXII is designed around a RESTful architecture and requires HTTPS-only communications (i.e., HTTP communications are not conformant with this specification).

Figure 1.1



### ​1.2.1.​ Channels Overview​1.2.1.​ Channels Overview

A Channel enables producers and consumers to exchange information in an asynchronous, event-based manner where both producers and consumers are TAXII clients of a TAXII server and the Channel is maintained by the TAXII server. A TAXII Server may contain multiple Channels per API Root and Channels are used to exchange information in a publish–subscribe manner.

Figure 1 below illustrates how Channel communications are used when a single producer sends a message to the TAXII Server, and that TAXII Server then distributes the message to all authorized consumers that have previously registered with the TAXII server. Normative requirements for Channels are defined later in this document.

### ​1.2.2.​ Collections Overview​1.2.2.​ Collections Overview

A Collection is used by TAXII clients to send information to the TAXII server or request information from the TAXII server. A TAXII Server may support multiple Collections per API Root, and Collections are used to exchange information in a request–response manner.

Figure 2 below illustrates how Collection based communications are used when a single TAXII Client makes a request to a TAXII Server and the TAXII Server fulfills that request with information available to the TAXII Server (nominally from a database). Normative requirements for Collections are defined later in this document.

|  |  |
| --- | --- |
| Figure 1.2 | Figure 1.3 |
|  |

## ​1.3.​ Document Conventions​1.3.​ Document Conventions

### ​1.3.1.​ Naming Conventions​1.3.1.​ Naming Conventions

All type names, property names and literals are in lowercase. Words in property names are separated with an underscore (\_), while words in type names and string enumerations are separated with a dash (-). All type names, property names, object names, and vocabulary terms are between three and 250 characters long.

### ​1.3.2.​ Font Colors and Style​1.3.2.​ Font Colors and Style

The following color, font and font style conventions are used in this document:

* The Consolas font is used for all type names, property names and literals.
	+ resource and type names are in red with a light red background – collection
	+ property names are in bold style – **description**
	+ literals (values) are in green with a green background – complete
* All examples in this document are expressed in Consolas 9 pt font, with straight quotes and have a two space indentation. Parts of the example may be omitted for conciseness and clarity. These omitted parts are denoted with the ellipses (...).

​

# ​2.​ HTTPS Requirements​2.​ HTTPS Requirements

The TAXII Protocol defined in this specification requires HTTPS as the transport for all communications.

* TAXII Servers and Clients **MUST** implement HTTPS [RFC7230].
* TAXII Servers and Clients **MUST** implement TLS version 1.2 [RFC5246], and **MAY** implement later versions.
* The default strategy for authenticating certificates **MUST** be PKIX as defined in RFC 5280, RFC 6818, RFC 6125 et al.
* TAXII Servers and Clients **MAY** support other certification verification policies such as:
	+ Certificate Pinning: A single or limited set of either hard-coded or physically distributed pinned certificate authorities or end-entity certificates.
	+ DANE: DNS-based Authentication of Named Entities [RFC 7671]
	+ Note that Self-Signed Certificates (like other certificates which cannot be verified by PKIX) **MAY** be supported via Certificate Pinning and/or DANE as noted above.

# ​3.​ DNS SRV Records​3.​ DNS SRV Records

This specification defines a DNS SRV record [RFC 2782] that can be used to allow clients to auto-discover the server that the TAXII server is running on.

## ​3.1.​ Requirements​3.1.​ Requirements

* Organizations **MAY** implement a DNS SRV record in their DNS server to advertise the location of their TAXII Server.
* The service name for this version of TAXII **MUST** be “taxii”.
	+ Future versions of TAXII **MAY** define alternate service names.
* TAXII Clients **MUST** support looking up and using the TAXII SRV record from DNS.

## ​3.2.​ Example​3.2.​ Example

The following example is for a DNS SRV record advertising a TAXII server for the domain “example.com” located at taxii-hub-1.example.com:443:

\_taxii.\_tcp.example.com. 86400 IN SRV 0 5 443 taxii-hub-1.example.com

# ​4.​ Discovery API​4.​ Discovery API

This specification defines a Discovery API that clients can use to discover the capabilities that the TAXII Server offers as well as meta-information about the TAXII Server (e.g., contact information). This specification uses the notation **<discovery>** to refer to the Discovery API URL.

## ​4.1.​ Requirements​4.1.​ Requirements

* TAXII Servers **SHOULD** implement the Discovery API
* The URL of the Discovery API **MUST** be /taxii and **MUST** be located at the root of the server, e.g., https://someserver.com/taxii
* A TAXII Server **MAY** advertise TAXII services that are not running on this server.

## ​4.2.​ Examples​4.2.​ Examples

https://taxii.example.com:443/taxii

https://someserver.foo.com/taxii

# ​5.​ API Root​5.​ API Root

An API Root is the "root" URL of a particular instance of the TAXII API. Hosting multiple API Roots allows an implementer to mimic trust groups or groups of interest on a single TAXII Server.

## ​5.1.​ Requirements​5.1.​ Requirements

* A TAXII Server **MUST** host at least one API Root.
* A TAXII Server **MAY** host more than one API Root.
* Each API Root **MUST** have a unique URL within the scope of the TAXII Server.
* Each API Root **MAY** have different authentication requirements.

## ​5.2.​ Examples​5.2.​ Examples

https://subdomain.example.com:12345/api-root-1

https://subdomain.example.com:12345/api-root-2

# ​6.​ Content Negotiation​6.​ Content Negotiation

TAXII 2 uses HTTP content negotiation as defined below.

## ​6.1.​ TAXII Media Type​6.1.​ TAXII Media Type

This specification defines the media type for TAXII.

### ​6.1.1.​ Requirements​6.1.1.​ Requirements

* The TAXII media type representing any version of TAXII is: application/vnd.oasis.taxii+json
* The TAXII media type representing TAXII 2.0 is: application/vnd.oasis.taxii+json; version=2.0
* TAXII Clients **SHOULD** include the version token wherever a TAXII media type is used.
	+ If the version token is omitted from a TAXII media type, implementations **SHOULD** respond with the highest version of TAXII that the server supports.
* TAXII Servers **MUST** honor the version token during content negotiation. If the server does not support the version, it should return a HTTP 406 (Not Acceptable) error.

## ​6.2.​ STIX Media Type ​6.2.​ STIX Media Type

This specification makes use of the STIX media type for representing Object and Message resources.

### ​6.2.1.​ Requirements​6.2.1.​ Requirements

* The STIX media type representing any version of STIX is: application/vnd.oasis.stix+json
* The STIX media type representing STIX 2.0 is:
 application/vnd.oasis.stix+json; version=2.0
* TAXII Clients **SHOULD** include the version token wherever a STIX media type is used.
	+ If the version token is omitted from a STIX media type, implementations **SHOULD** respond with the highest version of STIX that the server supports.
* TAXII Servers **MUST** honor the version token during content negotiation. If the server does not support the version, it should return a HTTP 406 (Not Acceptable) error.

# ​7.​ Primitive Types​7.​ Primitive Types

This section defines the primitive types used throughout TAXII. These types will be referenced by the “Type” column in other sections. This section defines the names and permitted values of common types that are used in TAXII; it does not, however, define the meaning of any fields using these types. These types may be further restricted elsewhere in the document.

|  |  |
| --- | --- |
| **Type** | **Description** |
| boolean | A boolean is a value of either true or false. Properties with this type **MUST** have a literal (unquoted) value of true or false. |
| integer | The integer data type represents a whole number. Unless otherwise specified, all integers **MUST** be capable of being represented as a signed 64-bit value. Additional restrictions **MAY** be placed on the type as described where it is used. |
| list | The list type defines an ordered sequence of one or more values. The phrasing “list of type <type>” is used to indicate that all values within the list must conform to a specific type. For instance, list of type string means that all values of the list must be of the string type. This definition does not specify the maximum or minimum number of allowed values in a list, however specific TAXII resource properties may define more restrictive upper and/or lower bounds for the length of the list.If a list property is required but no data is available, then an empty list **MUST** be returned.  |
| string | The string data type represents a finite-length string of valid characters from the Unicode coded character set [REF:ISO.10646] that are encoded in UTF-8. Unicode incorporates ASCII [REF: RFC20] and the characters of many other international character sets.  |
| timestamp | The timestamp type defines how timestamps are represented in TAXII and is represented in serialization as a string. * The timestamp field **MUST** be a valid RFC 3339-formatted timestamp [TODO add reference] using the format YYYY-MM-DDTHH:mm:ss[.s+]Z where the “s+” represents 1 or more sub-second values. The brackets denote that sub-second precision is optional, and that if no digits are provided, the decimal place **MUST NOT** be present.
* The timestamp **MUST** be represented in the UTC timezone and **MUST** use the “Z” designation to indicate this.
 |

​

# ​8.​ TAXII API​8.​ TAXII API

This section defines the TAXII API and all of the URL endpoints that are part of this specification.

## ​8.1.​ URL Endpoint Summary​8.1.​ URL Endpoint Summary

|  |  |  |
| --- | --- | --- |
| **Resource URL** | **Methods** | **Resource Type** |
| **<discovery>** | GET | discovery |
| **<api-root>** | GET | api |
| **Collections** |  |  |
| **<api-root>**/status/<status-id> | GET | status |
| **<api-root>**/collections | GET | list of type collection |
| **<api-root>**/collections/<name> | GET | collection |
| **<api-root>**/collections/<name>/manifest | GET | list of type manifest |
| **<api-root>**/collections/<name>/objects | GET, POST | object\* |
| **<api-root>**/collections/<name>/objects/<object-id> | GET | object\* |
| **<api-root>**/object-search | GET | object\* |
| **Channels** |  |  |
| <TBD in a future RC> |  |  |

*\* The actual format of objects is dependent on HTTP Content negotiation, as discussed in Section [TODO REF]*

​

## ​8.2.​ URL Parameters​8.2.​ URL Parameters

This section defines URL parameters and their meaning. The URL parameters defined in this section are used in the query portion of a URL. Each URL section defines which URL parameters are used.

|  |  |
| --- | --- |
| **URL Parameter** | **Description** |
| id | The identifier of the object that you are requesting. This is often a STIX ID. One or more identifiers **MAY** be specified in a single URL ID Parameter, comma separated.Example?id=1234,123,12334 |
| type | The object type that you want to filter on. TAXII Servers **MUST** support the following values:* campaign
* course-of-action
* indicator
* malware
* relationship
* report
* sighting
* threat-actor

TAXII Servers **MAY** support other values.Implementers are strongly recommended to support all SDO and SRO types from all STIX versions that they support. |
| version | The version of the STIX object that you are wanting. * latest tells the server to give you the latest one it knows about,
* first tell the server to give you the first one it knows about.
* all tells the server to give you all versions it knows about.
* An actual version number aka "2" tells the server to give you version 2.
* If the version parameter is not present in the request, it defaults to latest.
 |
| added\_after | Filters the result set to only include items added to the Channel or Collection after the specified datetime. The value of this is a timestamp |

## ​8.3.​ Global Requirements​8.3.​ Global Requirements

This section defines the behavior and requirements that apply globally to all URLs listed in this section.

### ​8.3.1.​ Property and String Requirements​8.3.1.​ Property and String Requirements

* All property names and string literals **MUST** be exactly the same, including case, as the names listed in the property tables in this specification.
	+ For example, the discovery resource has a property called **api\_roots** and it must result in the JSON key name "api\_roots".
* Properties marked required in the property tables **MUST** be present in the JSON serialization.

### ​8.3.2.​ Server Requirements​8.3.2.​ Server Requirements

* TAXII Servers **MUST** implement all URLs and HTTP methods defined in this section.
	+ TAXII Servers **MAY** implement other URLs and/or methods.
* TAXII Servers **MUST** include the version parameter in the Content-Type header when responding to Accept: headers of application/vnd.oasis.taxii+json and application/vnd.oasis.stix+json; . For example: Content-Type:application/vnd.oasis.taxii+json; version=2.0
* The status resource **MUST** be returned when an HTTP 202 (Accepted) response is given to a POST request.
* A server generating an HTTP error response **SHOULD** also include the error message in the response payload to give additional application specific details about the error.
* Servers **MAY** silently ignore unauthorized requests from clients.
* If a TAXII Client is unauthorized to access one or more objects or resources in a returned list, the server **SHOULD** filter those records from the returned list instead of refusing to fulfill the request.

### ​8.3.3.​ Client Requirements​8.3.3.​ Client Requirements

* Requests **MUST** include an Accept: header.
* Requests that expect a STIX or TAXII response **SHOULD** include an appropriate media range in the accept header.
	+ A media range of application/vnd.oasis.taxii+json in the accept header indicates that any version of TAXII is acceptable in the response.
	+ A media range of application/vnd.oasis.taxii+json; version=2.0 in the accept header indicates that ONLY TAXII 2.0 is acceptable in the response.
	+ A media range of application/vnd.oasis.stix+json in the accept header indicates that any version of STIX is acceptable in the response.
	+ A media range of application/vnd.oasis.stix+json; version=2.0 in the accept header indicates that ONLY STIX 2.0 is acceptable in the response.

## ​8.4.​ HTTP Status Codes​8.4.​ HTTP Status Codes

This section lists commonly used HTTP status codes as a reference for implementers. This specification does not modify the usage or meaning of HTTP status codes, and implementations are not restricted to using HTTP status codes listed in this section.

|  |  |  |
| --- | --- | --- |
| **HTTP Code** | **Text Value** | **Notes (if any)** |
| HTTP 200 | OK |  |
| HTTP 202 | Accepted | The request was accepted but has not yet been processed. This is used when a group of Objects or Messages are POSTed, and the server will process them asynchronously. |
| HTTP 400 | Bad Request |  |
| HTTP 401 | Unauthorized |  |
| HTTP 403 | Forbidden |  |
| HTTP 404 | Not Found |  |
| HTTP 405 | Method Not Allowed | Each section defines requirements for certain HTTP Methods (e.g., GET, POST); each of these methods is said to be a supported method for the URL. HTTP requests that use a supported method MUST NOT result in an HTTP response with a status of 405 (Method Not Allowed). Other methods MAY result in an HTTP response with a status of 405. For example, the <api-root> defines requirements for the GET method, but not other methods. In this case, GET requests cannot result in an HTTP response with a status of 405; but POST requests may. |
| HTTP 406 | Not Acceptable | For HTTP responses that contain a message body, the format of the message body is negotiated using the HTTP Accept header. Formats that are specified in the HTTP Accept header that the server is capable of providing are said to be acceptable. Formats specified in the HTTP Accept header that the server is not capable of providing are said to be unacceptable. If all options listed in the HTTP request’s Accept header are unacceptable, the HTTP response must have a status code of HTTP 406 (Not Acceptable). Each section defines which response formats must be acceptable. |
| HTTP 410 | Gone |  |
| HTTP 415 | Unsupported Media Type | For HTTP requests that contain a message body, the format of the message body is identified using the HTTP Content-Type header. For Content-Types that the server does not support, the HTTP response must have a status code of HTTP 415 (Unsupported Media Type). Each section defines which Content-Types must be supported. Additional Content-Types, beyond those listed, MAY be supported. |
| HTTP 429 | Too Many Requests |  |
| HTTP 500 | Internal Server Error |  |

## ​8.5.​ GET <discovery>​8.5.​ GET <discovery>

This URL allows TAXII Clients to discover information about a TAXII Server and learn the API Roots that this TAXII Server knows about.

The following tables illustrate a conformant request/response pair.

*Figure XX - Discovery Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <discovery> |
| **URL Variable(s)** | n/a |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Discovery Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | discovery |

### ​8.5.1.​ Requirements​8.5.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain a JSON discovery object.

### ​8.5.2.​ Examples​8.5.2.​ Examples

GET Request

|  |
| --- |
| GET /taxii HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "display\_name": "Some TAXII Server", "description": "This TAXII server contains a listing of...", "contact": "string containing contact information", "default": "https://example.com/api2", "api\_roots": [ "https://example.com/api1", "https://example.com/api2", "https://companyfoo.com/trustgroup1" ]} |

## ​8.6.​ GET <api-root>​8.6.​ GET <api-root>

This URL allows TAXII Clients to discover the available channels and collections at this specific API Root.

The following tables illustrate a conformant request/response pair.

*Figure XX - API Root Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root> |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - API Root Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | api-root |

### ​8.6.1.​ Requirements​8.6.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain a JSON api-root object.
* Servers **MAY** elide results from the response. For example, a server might choose to elide an API root if the requestor did not have sufficient permissions to view it.

### ​8.6.2.​ Examples​8.6.2.​ Examples

GET Request

|  |
| --- |
| GET /some-api-base HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "display\_name": "Malware Research Group", "description": "A trust group setup for malware researchers", "versions": ["taxii-2.0"], "channels": [], "collections": [ { "url": "https://example.com/api-1/collections/high-value-indicators", "display\_name": "High Value Indicator Collection", "description": "This data collection is for collecting high value IOCs", "can\_read": true, "can\_write": false, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ], "objects\_count": 923 }, { "url": "https://example.com/tg1/collections/24-hour-indicators", "display\_name": "Indicators from the past 24-hours", "description": "This data collection is for collecting current IOCs", "can\_read": true, "can\_write": false, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ], "objects\_count": 7 } ], "max\_content\_length": 9765625,} |

## ​8.7.​ GET /collections​8.7.​ GET /collections

This URL allows TAXII Clients to get a list of Collection resources that are available within an API Root.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collections Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/collections |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Collections Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | list of type collection |

### ​8.7.1.​ Requirements​8.7.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain a JSON list, where each item in the list is a collection.
	+ If there are zero collection to return, the result is an empty list.
	+ If there is one collection to return, the result is a list with one item.
* Servers **MAY** elide results from the response. For example, a server might choose to elide a collection if the requestor did not have sufficient permissions to view it.

### ​8.7.2.​ Examples​8.7.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/collections HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0[ { "url": "https://example.com/api-1/collections/high-value-indicators", "display\_name": "High Value Indicator Collection", "description": "This data collection is for collecting high value IOCs", "can\_read": true, "can\_write": false, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ], "objects\_count": 923 }, { "url": "https://example.com/tg1/collections/24-hour-indicators", "display\_name": "Indicators from the past 24-hours", "description": "This data collection is for collecting current IOCs", "can\_read": true, "can\_write": false, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ], "objects\_count": 7 }] |

## ​8.8.​ GET /collections/<name>​8.8.​ GET /collections/<name>

This URL allows TAXII Clients to get details about this specific Collection.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collection Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/collections/<name> |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection<name> - the name of the collection being requested |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Collection Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | collection |

*Figure XX - Common Errors*

|  |
| --- |
| **Common Errors** |
| **Status Code** | **Possible Reason** |
| HTTP 404 | The Collection is not found |

### ​8.8.1.​ Requirements​8.8.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain a JSON collection object.
	+ If no collection is returned, the result is an HTTP 404 (Not Found).
* Servers **MAY** elide results from the response. For example, a server might choose to elide a collection if the requestor did not have sufficient permissions to view it.

### ​8.8.2.​ Examples​8.8.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/collections/high-value-indicators HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "url": "https://example.com/api-1/collections/high-value-indicators", "display\_name": "High Value Indicator Collection", "description": "This data collection is for collecting high value IOCs", "can\_read": true, "can\_write": false, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ], "objects\_count": 923} |

## ​8.9.​ GET /collections/<name>/manifest​8.9.​ GET /collections/<name>/manifest

This URL allows TAXII Clients to get a Manifest of Objects in this collection. This URL supports URL parameters to filter the results.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collection Manifest Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/collections/<name>/manifest |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection<name> - the name of the collection being requested |
| **URL Parameters** | idtypeversionadded\_after |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Collection Manifest Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | list of type manifest |

### ​8.9.1.​ Requirements​8.9.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain a JSON list, where each item in the list is a manifest.
	+ If there are zero manifest to return, the result is an empty list.
	+ If there is one manifest to return, the result is a list with one item.
* Servers **MAY** elide results from the response. For example, a server might choose to elide a manifest if the requestor did not have sufficient permissions to view it.
* The id, type, version, and added\_after URL parameters **MUST** be supported at this URL endpoint.

### ​8.9.2.​ Examples​8.9.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/collections/high-value-indicators/manifest HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0[ { "url": "https://example.com/api-1/collections/high-value-indicators/objects/ indicator--c410e480-...-85307c12bcbf", "date\_added": "2016-11-01T03:04:05Z", "last\_modified": "2016-11-03T12:30:59Z", "versions": [1,2,4,6,9], "media\_types": ["application/vnd.oasis.stix+json; version=2.0"] }, { "url": "https://example.com/api-1/collections/high-value-indicators/objects/ indicator--c410e480-...-85307c121112", "date\_added": "2016-11-01T10:29:05Z", "last\_modified": "2016-11-01T10:29:05Z", "versions": [4], "media\_types": ["application/vnd.oasis.stix+json; version=2.0"] }] |

## ​8.10.​ GET /collections/<name>/objects​8.10.​ GET /collections/<name>/objects

This URL allows TAXII Clients to get multiple Objects in this collection. This URL supports URL parameters to filter the results.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collection Objects Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/collections/<name>/objects |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection<name> - the name of the collection being requested |
| **URL Parameters** | idtypeversionadded\_after |
| **Accept Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Collection Objects Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Message Body** | object\* |

*\* The actual format of objects is dependent on HTTP Content negotiation, as discussed in Section [TODO REF]*

### ​8.10.1.​ Requirements​8.10.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.stix+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.stix+json **MUST** contain an object resource.
	+ If there are no object to return, the result is an HTTP 404 (Not Found).
* Servers **MAY** elide results from the response. For example, a server might choose to elide a manifest if the requestor did not have sufficient permissions to view it.
* The id, type, version, and added\_after URL parameters **MUST** be supported at this URL endpoint.

### ​8.10.2.​ Examples​8.10.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/collections/high-value-indicators/objects HTTP/1.1Accept: application/vnd.oasis.stix+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "bundle", ..., "indicators": [ { "type": "indicator", ..., } ]} |

## ​8.11.​ POST /collections/<name>/objects​8.11.​ POST /collections/<name>/objects

This URL allows TAXII Clients to create an Object in this collection.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collection Objects Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | POST <api-root>/collections/<name>/objects |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection<name> - the name of the collection being requested |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Message Body** | object |

*Figure XX - Collection Objects Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 202 Accepted |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | status |

### ​8.11.1.​ Requirements​8.11.1.​ Requirements

* A TAXII Server **MUST** support POST requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* Requests with a Content-Type header that contains application/vnd.oasis.stix+json **MUST NOT** result in an HTTP 415 (Unsupported Media Type) response.
* HTTP 202 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain an status resource.
	+ The client should periodically poll the URL contained in the status **url** property to retrieve the most up-to-date status, until such a time that the **status** property returns a value of complete.
	+ TAXII Servers **SHOULD NOT** delete status messages for at least 24 hours.

### ​8.11.2.​ Examples​8.11.2.​ Examples

​​POST Request

|  |
| --- |
| POST https://example.com/api-1/collections/high-value-indicators/objects HTTP/1.1Accept: application/vnd.oasis.taxii+jsonContent-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "bundle", ..., "indicators": [ { "type": "indicator", "id": "indicator--c410e480-e42b-47d1-9476-85307c12bcbf", ..., } ]} |

​POST Response

|  |
| --- |
| HTTP/1.1 202 AcceptedContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "url": "https://example.com/api-1/status/1234", "status": "pending", "request\_url": "https://example.com/api-1/collections/coll1/objects", "request\_timestamp": "2016-11-02T12:34:34.12345Z", "total\_items": 1, "success\_count": 1, "success\_items": [ {  "id": "indicator--c410e480-e42b-47d1-9476-85307c12bcbf", "url": "https://example.com/api-1/collections/coll1/objects/indicator-- c410e480-e42b-47d1-9476-85307c12bcbf" } ],} |

## ​8.12.​ GET /collections/<name>/objects/<object-id>​8.12.​ GET /collections/<name>/objects/<object-id>

This URL allows TAXII Clients to get a specific Object from this collection. This URL only supports the version URL parameters to filter the results.

The following tables illustrate a conformant request/response pair.

*Figure XX - Collection Objects ID Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/collections/<name>/objects/<object-id> |
| **URL Variable(s)** | <api-root> - the base URL of the API Root containing the collection<name> - the name of the collection being requested<object-id> - the ID of the object being requested |
| **URL Parameters** | version |
| **Accept Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Collection Objects ID Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Message Body** | object\* |

*\* The actual format of objects is dependent on HTTP Content negotiation, as discussed in Section [TODO REF]*

### ​8.12.1.​ Requirements​8.12.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.stix+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.stix+json **MUST** contain an object resource..
	+ If no object is returned, the result is an HTTP 404 (Not Found).
* Servers **MAY** elide results from the response. For example, a server might choose to elide an object if the requestor did not have sufficient permissions to view it.
* The version URL parameter **MUST** be supported at this URL endpoint.

### ​8.12.2.​ Examples​8.12.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/collections/high-value-indicators/object/indicator--252c7c11- daf2-42bd-843b-be65edca9f61 HTTP/1.1Accept: application/vnd.oasis.stix+json; version=2.0 |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "bundle", ..., "indicators": [ { "type": "indicator", "id": "indicator--252c7c11-daf2-42bd-843b-be65edca9f61", ..., } ]} |

## ​8.13.​ GET /object-search​8.13.​ GET /object-search

This URL allows TAXII Clients to retrieve multiple Objects from any collection in this API Root. This URL supports URL parameters to filter the results.

The following tables illustrate a conformant request/response pair.

*Figure XX - Object Search Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/object-search |
| **URL Variable(s)** | <api-root> - the base URL of the API Root |
| **URL Parameters** | idtypeversionadded\_after |
| **Accept Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Object Search Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.stix+json; version=2.0 |
| **Message Body** | object\* |

*\* The actual format of objects is dependent on HTTP Content negotiation, as discussed in Section [TODO REF]*

### ​8.13.1.​ Requirements​8.13.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.stix+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.stix+json **MUST** contain an object resource..
	+ If no object is returned, the result is an HTTP 404 (Not Found).
* Servers **MAY** elide results from the response. For example, a server might choose to elide an object if the requestor did not have sufficient permissions to view it.
* The id, type, version, and added\_after URL parameters **MUST** be supported at this URL endpoint.

### ​8.13.2.​ Examples​8.13.2.​ Examples

GET Request

|  |
| --- |
| GET https://example.com/api-1/object-search?type=indicator HTTP/1.1Accept: application/vnd.oasis.stix+json; version=2.0 |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "bundle", ..., "indicators": [ { "type": "indicator", ..., } ]} |

## ​8.14.​ GET /status/<status-id>​8.14.​ GET /status/<status-id>

This URL allows TAXII Clients to get a Status of a previous request. This is used to monitor the status of requests that have resulted in an HTTP 202 (Accepted) response.

The following tables illustrate a conformant request/response pair.

*Figure XX - Status Request Properties*

|  |
| --- |
| **Request Properties** |
| **Request Line** | GET <api-root>/status/<status-id> |
| **URL Variable(s)** | <api-root> - the base URL of the API Root<status-id> - the ID of the status message being requested |
| **URL Parameters** | n/a |
| **Accept Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Content-Type Header** | n/a |
| **Message Body** | n/a |

*Figure XX - Status Response Properties*

|  |
| --- |
| **Response Properties** |
| **Status Line** | HTTP/1.1 200 OK |
| **Content-Type Header** | application/vnd.oasis.taxii+json; version=2.0 |
| **Message Body** | status |

*Figure XX - Common Errors*

|  |
| --- |
| **Common Errors** |
| **Status Code** | **Possible Reason** |
| HTTP 404 | The Status ID is not found |

### ​8.14.1.​ Requirements​8.14.1.​ Requirements

* A TAXII Server **MUST** support GET requests at this URL and **MAY** support other request types.
* Requests with an Accept header that contains application/vnd.oasis.taxii+json **MUST NOT** result in an HTTP 406 (Not Acceptable) response.
* HTTP 200 Responses with a Content-Type of application/vnd.oasis.taxii+json **MUST** contain an status resource..
	+ If no status is returned, the result is an HTTP 404 (Not Found).
* Servers **MAY** elide results from the response. For example, a server might choose to elide the status if the requestor did not have sufficient permissions to view it.

### **​8.14.2.​ Examples**​8.14.2.​ Examples

GET Request

|  |
| --- |
| GET /some-api-root/status/123456 HTTP/1.1Accept: application/vnd.oasis.taxii+json |

GET Response

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "url": "https://example.com/api-1/status/1234", "status": "pending", "request\_url": "https://example.com/api-1/collections/coll1/objects", "request\_timestamp": "2016-11-02T12:34:34.12345Z", "total\_items": 4, "success\_count": 1, "success\_items": [ {  "id": "indicator--c410e480-e42b-47d1-9476-85307c12bcbf", "url": "https://example.com/api-1/collections/coll1/objects/indicator-- c410e480-e42b-47d1-9476-85307c12bcbf" } ], "failure\_count": 1, "failure\_items": [ { "id": "malware--664fa29d-bf65-4f28-a667-bdb76f29ec98", "message": "Unable to process object" } ], "pending\_count": 2, "pending\_items": [ "indicator--252c7c11-daf2-42bd-843b-be65edca9f61", "relationship--045585ad-a22f-4333-af33-bfd503a683b5" ]} |

# ​9.​ TAXII Resources​9.​ TAXII Resources

This section defines the TAXII resources and their representations.

## ​9.1.​ API Root Resource​9.1.​ API Root Resource

**Resource Name:** api-root

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **display\_name** (required) | string | A human readable text/plain name used to identify this API instance. This is not the name of this API Root that is found in the URL. |
| **description** (optional) | string | A human readable text/plain description for this API Root. |
| **versions** (required) | list of type string | Lists the versions of TAXII that this API Root is compatible with. taxii-2.0 MUST be included in this list to indicate conformance with this specification. |
| **channels** (required) | list of type channel | <TODO> |
| **collections** (required) | list of type collection | <TODO> |
| **max\_content\_length** (optional) | integer | The maximum value of the request body "Content-Length" in octets (8-bit bytes) that the server can support. This applies to requests and responses and is determined by the server. Requests or responses with total body lengths values smaller than this value **MUST NOT** result in an HTTP 413 (Request Entity Too Large) response. Absence of this value means the server is choosing to not provide this information..This property is needed to help make sure a client does not have to keep guessing at how much data it can send. For example, if a server only supports payloads up to 10MB and a client wants to send 50MB of data, without this, the client would have to keep guessing as to what the server will support. |

## ​9.2.​ Discovery Resource​9.2.​ Discovery Resource

**Resource Name:** discovery

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **display\_name** (require) | string | A human readable text/plain name used to identify this server. |
| **description** (optional) | string | A human readable text/plain description for this server. |
| **contact** (optional) | string | The human readable text/plain contact information for this server and or the administrator of this server.  |
| **default** (optional) | string | The default API Root that a TAXII Client **MAY** use. Absence of this field indicates that there is no default API Root. |
| **api\_roots** (required) | list of type string | A list of URLs that identify API Roots that are hosted on this server or that this server knows about. This list **MAY** be filtered on a per-client basis. |

## ​9.3.​ Collection Resource​9.3.​ Collection Resource

**Resource Name:** collection

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **url** (optional) | string | The full URL of this collection. This property **MUST** be present in GET responses. |
| **display\_name** (required) | string | A human readable text/plain name used to identify this Collection. |
| **description** (optional) | string | A human readable text/plain description for this Collection. |
| **can\_read** (optional) | boolean | Indicates if the requester can read (i.e., GET) objects from this Collection. Absence of this field is equivalent to a value of false. |
| **can\_write** (optional) | boolean | Indicates if the the requester can write (i.e., POST) objects to this Collection. Absence of this field is equivalent to a value of false. |
| **media\_types** (optional) | list of type string | A list of supported media types for Objects in this collection. Absence of this field is equivalent to a value of application/vnd.oasis.stix+json. |
| **objects\_count** (required) | integer | The current number of objects contained in this Collection. |

## ​9.4.​ Error Resource​9.4.​ Error Resource

**Resource Name:** error

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **error\_id** (optional) | string | An identifier for this particular error. A TAXII Server might choose to assign each error occurrence it's own identifier in order to facilitate debugging. |
| **display\_name** (required) | string | A human readable text/plain name describing this error. |
| **description** (optional) | string | A human readable text/plain description that gives details about the error or problem that was encountered by the application. |
| **error\_code** (optional) | string | The error code for this error. A TAXII Server might choose to assign a common error code to all errors of the same type. |
| **http\_status** (optional) | string | The HTTP status code applicable to this error. |
| **external\_details** (optional) | string | A URL that points to additional details. Absence of this field indicates that there are not additional details. |
| **details** (optional) | object | The details objects provide a location for additional application specific details. |

### ​9.4.1.​ Example​9.4.1.​ Example

{

 "error\_id": "1234",

 "display\_name": "Error condition XYZ",

 "description": "This error is caused when the application tries to access data...",

 "error\_code": "581234",

 "http\_status": "409",

 "external\_details": "http://someserver.com/ticketnumber1/errorid-1234",

 "details": {

 "somekey1": "somevalue",

 "somekey2": "some other value"

 }

}

## ​9.5.​ Manifest Resource​9.5.​ Manifest Resource

**Resource Name:** manifest

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **url** (required) | string | The full URL of this object |
| **date\_added** (optional) | timestamp | The date this object was add to the server. |
| **last\_modified** (optional) | timestamp | The date this object was last updated or the last modified date of the most current version. For example, if version 2 was added after version 3, this date would contain the last modified date from version 3 not version 2 as version 3 is the most current version. |
| **versions** (optional) | list of type string | A list of available STIX versions. This field is only meaningful for objects that are available in a STIX format. |
| **media\_types** (optional) | list of type string | The media types that this object can be requested in. |

## ​9.6.​ Object Resource​9.6.​ Object Resource

**Resource Name:** object

This resource type is negotiated by the media type. If the media type in the Accept or Content-Type header contains application/vnd.oasis.stix+json; version=2.0 then this resource type is a STIX Bundle version 2.0 as defined in the STIX specification located here [TODO add reference].

## ​9.7.​ Status Resource​9.7.​ Status Resource

**Resource Name:** status

This resource is returned when an HTTP 202 (Accepted) response is given to a POST request. This resource conveys the status of a bulk creation.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **url** (required) | string | The full URL of the this Status resource. Absence of this field means that there is no URL to get this status again. |
| **status** (required) | string | The overall status of a previous POST request where an HTTP 202 (Accept) was returned. The value of this property MUST be one of complete or pending. A value of complete indicates that this resource will not be updated further and **MAY** be removed in the future. A status of pending indicates that this resource **MAY** update in the future. |
| **request\_url** (optional) | string | The URL of the request that this status resource is monitoring. |
| **request\_timestamp** (optional) | timestamp | The datetime of the request that this status resource is monitoring. |
| **total\_items** (required) | integer | The total number of items that were in the request. For a STIX Bundle this would be the number of objects in the Bundle. |
| **success\_count** (optional) | integer | The number of items that were successfully created. Absence of this field is equivalent to a value of “0” (zero). |
| **success\_items** (optional) | list of type success-items | A list of items that were successfully processed.  |
| **failure\_count** (optional) | integer | The number of items that failed to be created. Absence of this field is equivalent to a value of “0” (zero). |
| **failure\_items** (optional) | list of type failure-items | A list of items that were not successfully processed. |
| **pending\_count** (optional) | integer | The number of items that have yet to be processed. |
| **pending\_items** (optional) | list of type string | A list of identifiers for items that have yet to be processed. |

**Type Name:** success-items

This type contains a list of success items by ID and location.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **id** (required) | string | The identifier of the item that was created. For types that have an identifier, that identifier should be used here. |
| **url** (required) | string | The URL location of the created item. |

**Type Name:** failure-items

This type contains a list of success items by ID and location.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **id** (required) | string | The identifier of the item that was created. For types that have an identifier, that identifier should be used here.  |
| **message** (optional) | string | A message indicating why the item failed to be created. |

# ​10.​ Customizing TAXII Resources​10.​ Customizing TAXII Resources

[TODO add section description]

## ​10.1.​ Custom Properties​10.1.​ Custom Properties

It is understood that there will be cases where certain information exchanges can be improved by adding properties that are not specified nor reserved in this document; these properties are called **Custom Properties**. This section provides guidance and requirements for how TAXII Servers can use Custom Properties and how TAXII Clients should interpret them in order to extend TAXII in an interoperable manner.

### ​10.1.1.​ Requirements​10.1.1.​ Requirements

* A TAXII resource **MAY** have any number of Custom Properties.
* Custom Property names **MUST** be in ASCII and are limited to characters a-z (lowercase ASCII) and underscore (\_).
* Custom Property names **SHOULD** start with “x\_” followed by a source unique identifier (like a domain name), an underscore and then the name. For example: **x\_examplecom\_customfield**.
* Custom Property names **SHOULD** be no longer than 30 ASCII characters in length.
* Custom Property names **MUST** have a minimum length of 3 ASCII characters.
* Custom Property names **MUST** be no longer than 256 ASCII characters in length.
* Custom Property names that are not prefixed with “x\_” may be used in a future version of the specification for a different meaning. If compatibility with future versions of this specification is required, the “x\_” prefix **MUST** be used.
* Custom Property names **SHOULD** be unique when produced by the same source and **SHOULD** use a consistent namespace prefix (e.g., a domain name).
* Custom Properties **SHOULD** only be used when there is no existing properties defined by the TAXII specification that fulfills that need.

A TAXII Client that receives a TAXII message with one or more Custom Properties it does not understand **MAY** refuse to process the message further, or silently ignore non-understood properties and continue processing the message.

The reporting and logging of errors originating from the processing of Custom Properties depends heavily on the TAXII Server and Client implementations and is therefore not covered in this specification.

*Non-Normative:* TAXII Servers that produce messages that contain Custom Properties should be aware of the variability of TAXII Client behavior depending on whether or not the TAXII Client understands the Custom Properties present in a TAXII message. Rules for processing Custom Properties should be well defined and accessible to any TAXII Client that would be reasonably expected to parse them.

​

Examples

{

 ...,

 "x\_acmeinc\_scoring": {

 "impact": "high",

 "probability": "low"

 },

 ...

}

# ​11.​ Conformance​11.​ Conformance

## ​11.1.​ 8.1 TAXII Servers​11.1.​ TAXII Servers

A "TAXII 2.0 Server" is any software that creates publishes CTI content and conforms to the following normative requirements:

1. It **MUST** communicate over HTTPS using at least TLS version 1.2.
2. It **MUST** be able to create content encoded as JSON.
3. All required properties **MUST** be present in the created content.
4. All properties **MUST** conform to the data type and normative requirements for that property.
5. It **MUST** support at least Collections or Channels.
6. It **MUST** support all features listed in Section 11.2, Mandatory Features.
7. It **MAY** support any features listed in Section 11.3, Optional Features. Software supporting an optional feature **MUST** comply with the normative requirements of that feature.

A "TAXII 2.0 Client" is any software that consumes CTI content and conforms to the following normative requirements:

1. It **MUST** communicate over HTTPS using at least TLS version 1.2.
2. It **MUST** support parsing all required properties for the content that it consumes.
3. It **MUST** support all features listed in Section 8.2, Mandatory Features.
4. It **MAY** support any features listed in Section 8.3, Optional Features. Software supporting an optional feature **MUST** comply with the normative requirements of that feature.

## ​11.2.​ 8.2 Mandatory Features​11.2.​ Mandatory Features

### ​11.2.1.​ TODO​11.2.1.​

A TAXII 2.0 Server or TAXII 2.0 Client **MUST** support X by following the normative requirements listed in Section X.

## ​11.3.​ Optional Features

### ​11.3.1.​ TODO

A TAXII 2.0 Server or TAXII 2.0 Client **MAY** support X. Software claiming to support X **MUST** follow the normative requirements listed in Section X and X.

​11.3.2.​ Granular Data Markings

# ​12.​ Appendix A. Acknowledgments

**TAXII Subcommittee Chairs:**

Bret Jordan (bret.jordan@bluecoat.com), Blue Coat Systems, Inc.

Mark Davidson (mdavidson@soltra.com), Soltra

**Special Thanks:**

The following individuals made substantial contributions to this specification in the form of normative text and proofing and their contributions are gratefully acknowledged:

* Bret Jordan, Blue Coat Systems, Inc.
* Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)
* Eric Burger, Georgetown University
* Jason Keirstead, IBM
* Mark Davidson, Soltra
* Allan Thomson, LookingGlass Cyber
* John Wunder, MITRE Corporation
* John-Mark Gurney, New Context Services, Inc.

**Contributors:**

The following individuals were members of the OASIS CTI Technical Committee during the creation of this specification and their contributions are gratefully acknowledged:

<todo, make sure this is up to date>

# ​13.​ Appendix B. Changes from TAXII 1.1

For the TAXII 2.x series of releases, TAXII is no longer an acronym; TAXII is now just “TAXII”. TAXII previously expanded to “The Trusted Automated eXchange of Indicator Information”. TAXII’s use has proven to be broader than indicators, and therefore the original name became artificially limiting.

Network level discovery is added through the definition of a DNS SRV record. Prior versions of TAXII did not have network level discovery.

HTTP Long Polling is explicitly defined in an attempt to reduce time-delay in server-push scenarios (with the understanding that HTTP is not well-suited to server pushes of information). TAXII 1.x was silent on HTTP Timeouts.

Authentication requirements are specified in an attempt to improve interoperability. Previous versions of TAXII were silent on authentication requirements.

The protocol and format are explicitly defined in one document (this document). Previous versions of TAXII used one document per protocol/format definition, resulting in multiple documents per TAXII release. This change is the result of removing a requirement that TAXII be implementable across *any* protocol and format combination.

TAXII is now explicitly JSON over HTTPS. Previous versions of TAXII were flexible regarding protocol and format.

While TAXII 2 maintains all the capabilities of previous releases, many capabilities have been transformed into their RESTful equivalents. Those changes are:

* TAXII Services have been removed as a concept. In their place are RESTful interactions (e.g., HTTP GET, HTTP POST).
* TAXII Data Sets have been formalized as containers of content. This specification calls them TAXII Collections.
* TAXII Data Feeds have been formalized as a Publish/Subscribe messaging pattern. This specification calls them TAXII Channels.

# ​14.​ Appendix C - End to End Workflow

When this Discovery API is used with a DNS SRV record, clients auto-discover TAXII services as follows:

*Step 1:* Client uses DNS to retrieve a TAXII DNS Service Record, example:

\_taxii.\_tcp.example.com. 86400 IN SRV 0 5 443 taxii.example.com

If no SRV record is present for the domain, the client assumes the TAXII service is available at the domain itself, and the default HTTPS port of 443.

*Step 2:* Client uses the TAXII information provided in the DNS Service Record to construct the Discovery API URL. Using the port (443) and the hostname (taxii.example.com) from the DNS SRV Record, the TAXII Discovery URL is constructed as follows:

https:// + hostname + : + port + /taxii/

*Step 3:* Client issues a request to the fully constructed TAXII Discovery URL:

https://taxii.example.com:443/taxii/

1. Discuss DNS discovery
2. Get Discovery
3. Follow default to API Root
4. List collections
5. Pick collection to interact with
6. List objects
7. Get an object
8. Create an object

# ​15.​ Appendix D - Security Considerations

This appendix should talk about security issues with DNS SRV Records. For TAXII Server the reference identifier expected in certificates SHALL be the original name, as per RFC 6125. The concern has to do with a DNS query to example.com and then getting back a result of taxii-hub-1.example.com and the client then making a followon request. Dave Cridland can give more details here. ​The problem we are trying to address is that if you do a DNS lookup for the domain example.com and it returns a SRV record for taxii.example.com, there is no way to verify that record without DNSSEC. 1) remove 2) just call out that you SHOULD use DNSSEC 3) talk about the end server needing a cert for all of the names aka example.com + foo.example.com