Automated Indicator Sharing (AIS) Trusted Automated Exchange of Intelligence Information (TAXII™) Server Connection Guide

V2.0

Publication: December 2021
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 Purpose

The purpose of this guide is to document the formal requirements needed to successfully connect to the Cybersecurity and Infrastructure Security Agency (CISA) Automated Indicator Sharing (AIS) Trusted Automated Exchange of Intelligence Information (TAXII™) Server. Common questions and best practices are provided to help support AIS participants successfully connect to the AIS TAXII Server and enable querying of AIS Structured Threat Information Expression (STIX) objects.

2 Customer Access

The CISA AIS TAXII Server operates in a server/client relationship with end-users. To connect to the CISA AIS TAXII Server, AIS participants must either acquire a TAXII-compliant client, identify a Data Aggregator Commercial Service, or hold certain memberships.

Additional requirements vary by access type. For example, a client certificate issued by an Approved Federal Bridge Certification Authority (FBCA) is required for access via a TAXII-compliant client. Requirements based on access method are noted below, with further details on the individual requirements provided in Section 3.

2.1 Standalone TAXII-Compliant Client

AIS participants may implement a TAXII-compliant client within their internal infrastructure. To pull AIS feed content, the client must send valid TAXII queries to the AIS TAXII Server. The client must be able to authenticate the TAXII Server connection using a Collection Name and an SSL/TLS client public certificate provided by the customer. (AIS 1.0 uses Subscription ID while AIS 2.0 uses Collection Name)

See Appendix B for a list of compatible TAXII clients. A TAXII Version 1.1-compliant client is required for AIS 1.0, and a TAXII Version 2.1-compliant client is required for AIS 2.0.

NOTE: AIS participants using any of the Compatible TAXII Clients must obtain a client certificate and must provide CISA with the static IP addresses they will be using to connect to the TAXII Server. A Terms of Use (TOU) and an Interconnection Agreement are also required.

2.2 Data Aggregator Commercial Service

Alternatively, AIS participants can subscribe to a Data Aggregator Commercial Service to access the AIS feed. CISA provides guidance to service providers so that the content available to each entity via their respective service provider is based on the community membership granted to that customer. For example, only federal entities can access the Federal feed and only CISCP members can access the CISCP feed.

See Appendix C for a list of Data Aggregator Commercial Threat Intelligence Platforms that currently support access to the CISA AIS 2.0 TAXII 2.1 Server.

NOTE: AIS participants using a Data Aggregator Commercial Service to access AIS content do not need to obtain a certificate nor provide CISA with static IP addresses (these are provided by the commercial service infrastructure). However, AIS participants must still complete a TOU and an Interconnection Agreement.

2.3 Data Aggregator Commercial Service + Associated Direct Client

AIS participants can subscribe to a Data Aggregator Commercial Service that allows the customer to directly access the AIS TAXII Server through the Data Aggregator Commercial Service infrastructure.

See Appendix C for a list of Data Aggregator Commercial Services, with associated direct client, that currently support access to the CISA AIS TAXII Server.

NOTE: AIS participants using a Data Aggregator Commercial Service, with associated direct client, to access the AIS TAXII Server will need to obtain a certificate and complete the TOU and Interconnection Agreement. However, they do not need to provide CISA with the static IP addresses used to connect to the TAXII Server.

2.4 Other Access

AIS participants may be able to get access to AIS data via memberships or use of other services.

2.4.1 Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations

Many sector-based Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) provide AIS data to their members. Some ISACs and ISAOs provide both AIS Public and CISCP feed data in their cyber threat indicator feeds. Entities who are members of one of the ISACs or ISAOs, can inquire as to whether access to the feeds is available and confirm they are also receiving AIS data. For a current list of ISAC and ISAO providers please refer to the AIS website: https://www.cisa.gov/ais.

NOTE: AIS participants receiving AIS data through these membership-based feeds do not need to provide any information to CISA.

2.4.2 Malware Information Sharing Project (AIS 1.0 Only)

Malware Information Sharing Project (MISP) platform users can analyze AIS 1.0 cyber threat indicators within a MISP database using an additional conversion tool. MISP doesn't have a built-in TAXII client, so an intermediary is used to poll the TAXII Server and convert from AIS 1.0 (STIX 1.1 format) into the MISP Data event format.

CISA has built an open-source tool called FLARE MISP Service to retrieve AIS 1.0 data (in STIX 1.1.1 format) from AIS and load the content into a MISP Server. Details are available at the CISA GitHub repository: https://github.com/cisagov/flare-misp-service.

NOTE: AIS 1.0 participants can configure the FLARE MISP client per instructions on GitHub. CISA can offer additional troubleshooting support with the FLARE-MISP service initial setup, as needed.

3 Customer Requirements

The information and signed agreements that CISA requires for connection to the AIS TAXII Server depends on the connection method. Current AIS 1.0 participants looking to convert to AIS 2.0 should consult with CISA via cyberservices@cisa.dhs.gov to determine if any of the following requirements need to be re-accomplished or updated. Table 1 provides a summary. Details are provided in the sub-sections that follow.

Table 1: CISA Connection Requirements

	Standalone TAXII Client	Data Aggregator Commercial Service	Commercial Service w/Direct Client
IP Addresses	X	-	-
Client Certificate	X	-	X
CA Certificates	X	-	X
TOU Agreement	X	X	X

	Standalone TAXII Client	Data Aggregator Commercial Service	Commercial Service w/Direct Client
Interconnection Agreement	X	X	X

3.1 Customer IP Address(es) for TAXII Server Connection

CISA requires the explicit IP address(es) from within the AIS participant's TAXII client network that will be used to connect to the AIS TAXII Server. Each organization can connect to AIS via a maximum of eight IP addresses. Please do not provide IP CIDR ranges (e.g., /16, /24); explicit IP addresses are required.

3.2 Customer SSL/TLS Client Public Certificate

CISA requires an SSL/TLS Client Public Certificate to establish a successful secure connection with the AIS TAXII Server.

To authenticate to the CISA AIS TAXII Server, users must obtain a "Medium Device Assurance Level" client certificate from a CISA-approved FBCA[1]. At a high level, the process is as follows:

1. Select an approved FBCA
2. Generate a Certificate Signing Request (CSR)
3. Complete the online request
4. Provide the FBCA proof of your identity
5. Download the issued certificate

It can take between 7 and 14 days for an SSL/TLS certificate to be issued after paperwork is notarized and submitted to the FBCA. After receiving the certificate, the user should confirm that the certificate is valid for use as a digital signature (see Figure 1).

[1] A list of CISA-approved vendors is available at https://www.cisa.gov/dhs-approved-vendors-offer-ais-taxii-client-compatible-certificates.

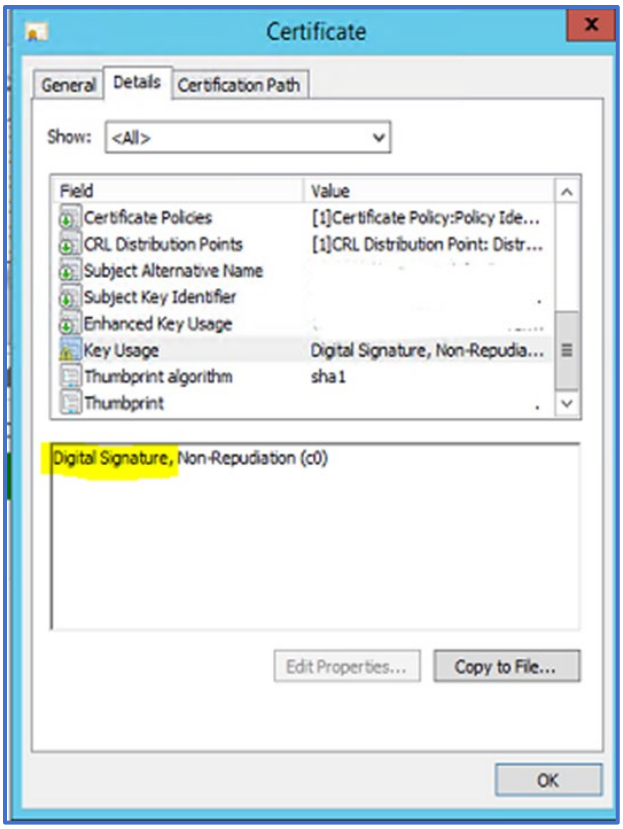

Figure 1: Client Certificate – Digital Signature Enabled

The file should be provided to CISA in a ".PEM" or ".txt" format and should only include the certificate itself (see Figure 2).

```
-----BEGIN CERTIFICATE-----
MI[redacted]nyevpZAM5lMA0GCSqGSIb3DQEBDAUAMHAxFzAVBgNVBAMTDmRpbWUu
bWl0cmUub3JnMR4wHAYDVQQKExVUaGUgTUlUUkUgQ29ycG9yYXRpb24xEDAOBgNVBAcTB0JlZGZv
cmQxFjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxCzAJBgNVBAYTAlV[redacted]TExNTYxOFoX
DTE5MDEyODExNTYxOFowcDEXMBUGA1UEAxM0ZGltZS5taXRyZS5vcmcxHjAcBgNVBAoTFVRoZSBN
SVRSRSBDb3Jwb3JhdGlvbjEQMA4GA1UEBxMHQmVkZm9yZDEWMBQGA1UECBMNTWFzc2FjaHVzZXR0
czELMAkGA1U[redacted]EiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCSHS0z/abdGcXY
33kvKxecOgxRlGFezsl+Ss1fXGHl4BGNdHYbTJMac8+lV6v29Xb6lC1AcHSN5USHaSsZV9KJeKwy
uAGZLSTpLkt8LzPsEWcObTWvK5QbRanoa3swtWGRiHqziGBrEkgAc+8VROvHhyHMU6OeixotIcky
E1uufRLzs+WE/jZd9ErZObEEmYkreMtedQ1FY/KpKJpfomvXXaKdId3egM0a19/RzdLartrkVZvZ
VRUluv+GQS2wgohNI/WFMs0ARs7r573ciP6TR/iQBpiXTyXffWA9E7u3w3vqE71nbObVP+RNuM3h
f1rH8HM3k/v0u/Nt01P2oqwpAgMBAAGjQjBAMB0GA1UdDgQWBBRu3DnFiw1NodGIaO3Cu7JlJmum
EjAfBgNVHSMEGDAWgBRu3DnFjw1NodGIaO3Cu7JlJmumE[redacted]AOCAQEAWOBk
hKsTYpBvm6cuUGj/Cl5BQ99/9BIKHsZeHDikFXu9liSOhaAK/50iRS1kB9TGqGqUmpt2uSo0xl/E
xkaa02RFAQ99Re2//Ei6xhddQPFBsd0yXi3tIULZSy2u0dRe5OflFs/Q/8fI3sKgvJvhfVz2CGFg
g9[redacted]KzexfBhWCW8KqU3CZLZJGRCkU0hqI6nTZKbbvc06XJDSHWBxj
QANoFx46dxjt5n6eTqF0wwnwt/e/x2Qt217RXqhnDRCl8hVOBOgp41f2H3jhBlRqJgvdM1+NUlt5
LPa7JD3U0b59JqRKSgDn6OQyx2Xodooc2Q==
-----END CERTIFICATE-----
```

Figure 2: SSL/TLS Client Public Certificate PEM Format Example

3.3 Certificate Authority Certificate and any Intermediate Certificates

To successfully connect with the AIS TAXII Server, CISA requires the Certificate Authority (CA) certificate and any intermediate certificates associated with your SSL/TLS Client Public Certificate (see Figure 3). There may be one or more intermediate certificates associated with the certificate supplied by your selected FBCA CA vendor. The file should be in a ".PEM" or ".txt" format.

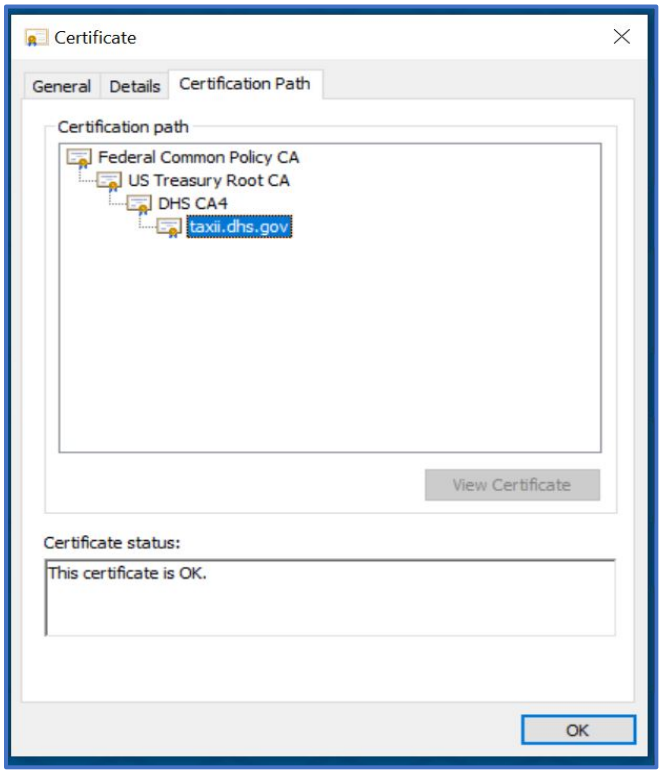

Figure 3: Certificate Authority and Intermediate Certificates Example

3.4 Terms of Use

The CISA AIS Terms of Use (TOU)[2] defines the rules for using the AIS TAXII Server. A completed and signed AIS TOU document is required to be on file with CISA prior to interfacing with CISA's TAXII server. For entities that do not already have an AIS TOU on file with CISA, send a signed TOU to cyberservices@cisa.dhs.gov.

3.5 Interconnection Agreement

To ensure you and CISA have the proper security Points of Contacts (POCs), a completed and signed Interconnection Agreement[3] is required. It must be sent to cyberservices@cisa.dhs.gov.

[2] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[3] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

4 CISA-provided Information

CISA provides the following items so a customer can successfully authenticate and connect to the AIS TAXII Server.

4.1 TAXII Server SSL/TLS Certificates

CISA will provide the AIS TAXII Server public SSL/TLS certificate (taxii.dhs.gov) and associated CA certificates.

4.2 TAXII Server Data Feed Subscription Identification/Customer Feed Name

After receiving the customer information specified in Section 3, CISA will provide the AIS TAXII Server Subscription Identification (ID) associated with the appropriate AIS data feed(s). The subscription ID must be present in all TAXII Server queries.

An example AIS 1.0 TAXII Server poll request (with subscription_id attribute), is shown in Figure 4.

```
<? Xml version="1.0" encoding="UTF-8" ?>
<taxii:Poll_Request
xmlns:taxii="http://taxii.dhs.gov/messages/taxii_xml_binding-
1"message_id="111111111" feed_name="feedName" subscription_id="01234567-
89ab-cdef-0123-456789abcdef">
</taxii:Poll_Request>
```

Figure 4: AIS 1.0 TAXII Server query (poll request)

An example AIS 2.0 TAXII Server Polling Sample via curl request (with COLLECTION ID = a6313101-fa6c-4276-bb96-7e826f0b248a and Specific Object ID: a1578c4f-d14f-4df8-bcc7-29723af96d18) is shown in Figure 5.

```
curl --insecure --cert /home/user/certs/client.crt --key /home/user/certs/client.key --header
"Accept: application/taxii+json; version=2.1"        --request GET
https://ais2.cisa.dhs.gov/public/collections/a6313101-fa6c-4276-bb96-
7e826f0b248a/objects/url--a1578c4f-d14f-4df8-bcc7-29723af96d18/ --silent | jq '.'
```

Figure 5: AIS 2.0 TAXII Server Polling Sample

4.3 Estimated Timelines

CISA tasks have the following estimated timelines for implementation:

- **Install Customer Client SSL/TLS Certificates**: CISA needs at least two (2) business days to install customer Client SSL/TLS certificates in order to generate and provide TAXII login credentials (Collection Name) to the customer.
- **Add IP Addresses to ALLOW Lists**: CISA needs up to two (2) weeks to integrate customer infrastructure IP addresses into ALLOW lists. Therefore, infrastructure specific IP addresses should be provided as soon as possible. The listing of customer infrastructure IP addresses is done by the CISA Trusted Internet Connection (TIC) team and in accordance with TIC requirements.

5 TAXII Production Feeds

The AIS TAXII Server has three AIS data feeds in production:

1. **AIS 2.0: Public/AIS 1.0: AIS** – The AIS Public feed contains data from federal and non-federal participants to include State, Local, Tribal and Territorial (SLTT), international, and industry to the broader private sector community.
2. **AIS 2.0: Federal / AIS 1.0: FEDGOV**– The FEDGOV feed is bi-directional and contains all data.
3. **AIS 2.0 and AIS 1.0: CISCP** – The CISCP member community feed contains more enriched data for non-federal entities. Access is authorized by signed CISCP Agreement.

The AIS 2.0 TAXII Server has a single production submission feed:

- **AIS INGEST** – Use the AIS INGEST feed to submit data to the AIS environment.

5.1 Feed Addresses

To access the CISA AIS data feeds, please use the following production feed addresses.

- **TAXII 1.1**
    - Feed polling: https://taxii.dhs.gov:8443/flare/taxii11/poll
        - Requires use of Subscription ID.
    - Feed discovery: https://taxii.dhs.gov:8443/flare/taxii11/discovery
        - No Subscription ID required
    - IMPORTANT: Port 8443 must be open inbound and outbound. Bi-directional traffic is required for a SSL/TLS secured connection.
- **TAXII 2.1**
    - Collection discovery: https://ais2.cisa.dhs.gov/taxii2/
    - Feed polling example:

```
curl --insecure --cert /home/user/certs/client.crt --key /home/user/certs/client.key --header "Accept: application/taxii+json; version=2.1" --request GET https://ais2.cisa.dhs.gov/public/collections/a6313101-fa6c-4276-bb96-7e826f0b248a/objects/url--a1578c4f-d14f-4df8-bcc7-29723af96d18/ --silent | jq '.'
```

    - IMPORTANT: Port 443 must be open inbound and outbound. Bi-directional traffic is required for a SSL/TLS secured connection.

5.2 Recommended Query Timeframes

Recommended timeframes for queries are below.

- **AIS 2.0: PUBLIC/AIS 1.0: AIS and AIS 2.0: FEDERAL/AIS 1.0: FEDGOV Feeds**

  Queries for current date and archive data for the AIS Public (AIS) and Federal (FEDGOV) feeds must be limited to 4-hour time periods because responses with excessive content will be dropped due to HTTPS timeouts.

- **CISCP Feed**

  Queries for the CISCP feed are limited to a 90-day time period. The timeframe is larger than for the other feeds due to a lesser amount of data, making searches that result in HTTPS timeouts less common.

6 Frequently Asked Questions

Frequently asked questions (FAQs) are answered below.

6.1 General Questions

- **Why do I need to provide my client SSL/TLS certificate?**

  A client certificate is required because access is via a two-way SSL/TLS encrypted communication.

- **How often should I poll/query?**

  Polling frequency is up to each customer. Because AIS STIX objects are published throughout the day, AIS participants using a TAXII client may want to poll several times a day. Given the volume of the AIS Public and Federal feeds, best practice is to poll at least every four hours and start and end dates should be specified.

- **Are usernames and passwords associated with TAXII?**

  No. TAXII authenticates via PKI certificates using machine-to-machine communications without the need for usernames or passwords.

- **Why is my query hanging?**

  If your query is hanging, it may be timing out due to data volume. Using start and end dates should help AIS participants pull data successfully.

6.2 AIS 2.0 Questions

The following questions are specific to AIS 2.0, pertaining to the Server Discovery, Get Collection, Get Objects, Get Status, and Add Objects Endpoints.

- **Why am I getting the following TAXII 2.1 error codes?**

  400 – The server did not understand the request

  Your request is not a valid TAXII 2.1 message. Check the body of your POST Request to ensure that it complies with TAXII 2.1 specifications. You must properly specify certain HTTP Headers, in addition to having a valid TAXII 2.1 payload.

  401 – The client needs to authenticate

  You are not being recognized as a fully registered user on the CISA AIS system. This is likely an issue requiring additional support to resolve. Please contact taxiiadmins@us-cert.gov to determine if you and your client SSL/TLS certificates have been properly registered on the system.

  403 – The client does not have access to this resource

  You have been authenticated to the system, but your access is limited. This is likely an issue requiring additional support to resolve. Please contact taxiiadmins@us-cert.gov.

  404 – The *<URL Parameter(s)>* is not found, or the client does not have access to the resource

  Check the URL parameters (e.g., api-root, id, object-id) to identify any errors. If the query parameters are correct, please contact taxiiadmins@us-cert.gov to address access issues.

  406 – The media type provided in the Accept header is invalid

  The Accept header is malformed or otherwise unacceptable. For compatibility with the AIS TAXII

Server, the value must be "application/taxi+json; version=2.1."

- **When using the Add Objects Endpoint, why am I getting the following TAXII 2.1 error codes?**

  413 – The POSTed payload exceeds the max_content_length of the API Root

  The payload is too large. Content length cannot exceed 100 MB.

  415 – The client attempted to POST a payload with a content type the server does not support

  Your request is not a valid TAXII 2.1 message. Check the body of your POST Request to ensure that it complies with TAXII specifications. You must properly specify certain HTTP Headers, in addition to having a valid TAXII 2.1 payload.

  422 – The object type or version is not supported or could not be processed

  The body is malformed or contains content that the AIS TAXII Server cannot process.

6.3 AIS 1.0 Questions

The following questions are specific to AIS 1.0.

- **Will my AIS 1.0 submissions be available to AIS 2.0 participants?**

  Legacy AIS 1.0 capabilities will run in parallel to AIS 2.0 advanced features for a limited time. Current AIS 1.0 users that continue to submit in the legacy STIX 1.1 will automatically have their shared data translated and disseminated where possible within the STIX 2.1 threat feeds to enable all AIS 2.0 participants to receive the same set of cyber threat indicators, to the extent possible, regardless of which STIX standard was used for the submission. CISA will not be translating the latest STIX 2.1 standard back down to the older STIX 1.1 standard, so CISA encourages all participants to utilize the latest AIS 2.0 feed when possible.

- **What do the following TAXII 1.1 responses mean?**

  status_type= "UNSUPPORTED_PROTOCOL"

  Either you are not using HTTPS (TLS/SSL) or you aren't presenting a valid CA certificate. Check the URL you are hitting and confirm the request is using your client certificate. Also, ensure you are using the TAXII Server Public certificate provided to you from CISA.

  status_type= "UNAUTHORIZED"

  You have successfully made it past the 2-way SSL/TLS handshake with the AIS TAXII Server, but you are not being recognized as a fully registered user on the CISA AIS system. This is likely an issue requiring additional support to resolve. Please contact taxiiadmins@us-cert.gov to determine if you and your client SSL/TLS certificates have been properly registered on the system.

  status_type= "BAD_MESSAGE"

  You have been authenticated and authorized on the AIS TAXII Server. However, your request is not a valid TAXII 1.1 message. Check the body of your POST request to ensure that it complies with TAXII specifications. You need to properly specify certain HTTP Headers, in addition to having a valid TAXII 1.1 payload.

  status_type= "FAILURE"

You were authenticated and authorized on the AIS TAXII Server and your message was validated against the TAXII 1.1 specification. However, some other generic failure has occurred. Please contact taxiiadmins@us-cert.gov for assistance.

- **Why am I not able to connect to the TAXII Server and why did I receive a "Validation Schema Error" during a Polling request?**

  Ensure that the certificate is valid for use as a digital signature (see Section 3.2).

7 Notes & Best Practices

Notes are listed below:

- STIX Objects may be updated over time with new information, so understanding STIX sightings and versioning is important[4].
- It is possible to request STIX Objects shared within AIS to be redacted by contacting taxiiadmins@us-cert.gov with details of the target indicator (Package ID, Indicator ID, and/or Indicator Content (e.g. IP Address or Domain Name)). After a redact request is verified and approved, future Poll Requests for that data will not include the redacted content in responses.
- All AIS participants must keep their SSL/TLS certificate current. If your SSL/TLS certificate expires, you will not be able to authenticate to the CISA AIS TAXII Server.

For assistance, please reach out to the TAXII Admin team at taxiiadmins@us-cert.gov.

CISA recommends that AIS participants follow these best practices:

- The connection to the CISA AIS TAXII Server should be documented according to your organization's security requirements.
- AIS participants should configure their clients to query/poll using Coordinated Universal Time (UTC) instead of local time.

[4] Please refer to the STIX specification for details: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html.

8 Appendix A – Acronyms

Acronyms are provided below.

Acronym	Definition
AIS	Automated Indicator Sharing
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CISA	Cybersecurity and Infrastructure Security Agency
CISCA	Cyber Information Sharing and Collaboration Agreement
CISCP	Cyber Information Sharing and Collaboration Program
CTI	Cyber Threat Indicator
CTIS	Cyber Threat Information Sharing
DM	Defensive Measure
FAQ	Frequently Asked Questions
FBCA	Federal Bridge Certification Authority
ID	Identification
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
MISP	Malware Information Sharing Project
POC	Point of Contact
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TIC	Trusted Internet Connection
TOU	Terms of Use
UTC	Coordinated Universal Time

9 Appendix B - Compatible TAXII Clients

The TAXII implementations below are interoperable with the CISA TAXII 2.1 Server. Additional clients are available that may work with the CISA server, but they have not been tested.

- **CISA TAXII Client** (called "FLAREClient" internally, available free of charge)
  - https://github.com/cisagov/FLAREclient-Java
  - This is the preferred client to use for complex/problematic troubleshooting when difficult-to-solve polling or publishing issues occur.
- **OASIS cti-taxii-client** (open-souce)
  - https://github.com/oasis-open/cti-taxii-client

NOTE: AIS participants using any of these clients will still need to obtain a PKI-medium certification and provide CISA with static IP addresses that they will be using to connect to the TAXII Server.

10 Appendix C - Data Aggregator Commercial Threat Intelligence Platforms

If interested in a commercial Data Aggregator Threat Intelligence Platform that provides AIS data to existing subscribers at no extra cost, please refer to the AIS website: https://www.cisa.gov/ais.

AIS participants must still complete the AIS Terms of Use (TOU) document and return it to cyberservices@cisa.dhs.gov.