Automated Indicator Sharing (AIS) 2.0 Public Facing Test Environment (PFTE)

V1.0

Publication: November 2021
Cybersecurity and Infrastructure Security Agency

Table of Contents

WHAT IS THE AIS PUBLIC FACING TEST ENVIRONMENT (PFTE)?

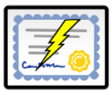
The PFTE is a pre-production instance of the Automated Indicator Sharing (AIS) 2.0 Trusted Automated Exchange of Intelligence Information (TAXII) server that hosts sample content and allows testing of many AIS 2.0 TAXII server capabilities before they are rolled out to production.[1]

WHAT CAN I DO WITH THE PFTE?

The PFTE can be used to test publishing test content, retrieving sample content, and checking test submission statuses. The PFTE provides access to static sample data that can be used for testing purposes –this test data should not be used in production environments and real cyber threat indicators (CTIs) and defensive measures (DMs) should not be used in the PFTE. Testing on the PFTE will help make your experience on the production AIS system smooth, and minimize problems of user access, data compatibility, and object retrieval. CISA therefore recommends that AIS participants use the PFTE to test AIS 2.0 connectivity and test data publishing prior to connecting to and using the production environment.

The PFTE capabilities will expand over time. New features will be added to the PFTE for testing by AIS participants prior to being added to the AIS production environment. With participant feedback, CISA will assess updates to the PFTE that will make AIS as useful and relevant to the community as possible. Please send any feedback to cyberservices@cisa.dhs.gov.

KEY FEATURES



Test Connectivity and Certificates: AIS requires certificates for participants to connect. The PFTE enables participants to test the certificates and that their TAXII client can connect to the AIS environment. Once setup is complete, participants should experience a seamless transition from the PFTE to the AIS production environment.

Access to Sample STIX Content: The PFTE provides access to thousands of samples that exercise different Structured Threat Information Expression (STIX) objects, relationships, data markings, and enrichments (such as Opinion objects from CISA with simulated scores).[2] Samples demonstrate what participants could see on the AIS feeds.

Enhanced TAXII Filtering STIX Content: The PFTE supports enhanced TAXII Filtering for TAXII Clients to test tailored access to thousands of sample STIX objects from the TAXII server. More information on TAXII filters can be found in *Filtering AIS Content Based on Specified Criteria*.[3]

Submit STIX Content: Participants can test that their TAXII client can connect to the AIS environment and send test STIX objects to the TAXII server. Sample STIX objects can be submitted to the TAXII server to see if it is valid content and includes everything that is needed (i.e., follows the *AIS Profile* and *AIS Submission Guide*[4]) as well as to see what the TAXII server provides as a response to input. In addition, to help provide awareness of new features in AIS 2.0, test data submitted within the PFTE will be enriched randomly with

[1] https://oasis-open.github.io/cti-documentation/
[2] https://oasis-open.github.io/cti-documentation/
[3] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[4] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

simulated CISA Opinion scores. If automated checks find potential personally identifiable information (PII) in test submissions, the system will simulate the AIS Human Review process, providing a random determination for testing purposes only. Test data submitted into the PFTE, if it clears automated validation and process, will also be available to other PFTE participants as sample content, though user-submitted test data may be replaced or overwritten periodically.

Check Status of Submissions: Participants can leverage the PFTE AIS Status Service to determine if their sample test submission is pending simulated human review (for PII), whether it passed validation, and if the submission went to the correct test feeds. If the submission failed validation or went to the wrong test test feed, the participant can make modifications to their submission and resubmit it to the PFTE. This allows participants to get comfortable with the service for when they interact with the AIS production environment.

Test Tool Updates: As updates are pushed to TAXII clients, participants can test them against the PFTE to confirm everything works as expected before deploying the updates to production and against the AIS production environment.

HOW DO I ACCESS THE PFTE?

To gain access to the PFTE, the AIS on-boarding procedure must be followed. This includes:

1. Providing the name of the TAXII 2.1 client
2. Providing the client certificate/key pair from an approved FedBridge provider
3. Providing the IP address that will be used to access the TAXII server
4. Completing the *AIS Interconnection Agreement* and on-boarding documentation[5]

When the above four items have been provided to CISA, you will be sent an email containing your log on instructions for the PFTE.

For more information about the PFTE, please contact cyberservices@cisa.dhs.gov.

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

APPENDIX A - ACRONYMS

Table 1: Acronyms

AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
PFTE	Public Facing Test Environment
PII	Personally Identifiable Information
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information