



Canada Health Infoway

Projectathon Tooling

IUA Client & Server Simulators

What are the IUA Client & Server Simulators?



- ❖ **IUA Authorization Client Simulator:** A user interface that executes IUA transactions to simulate an IUA conformant authorization client
- ❖ **IUA Authorization Server Simulator:** A server-side simulator, based on the Open Source Keycloak Identity and Access Management (IAM) solution, used to simulate an IUA conformant authorization server
- ❖ **IUA Resource Server Simulator:** A server-side simulator, that interacts with IUA Authorization Clients and IUA Authorization Servers to utilize and introspect access tokens in exchange workflows

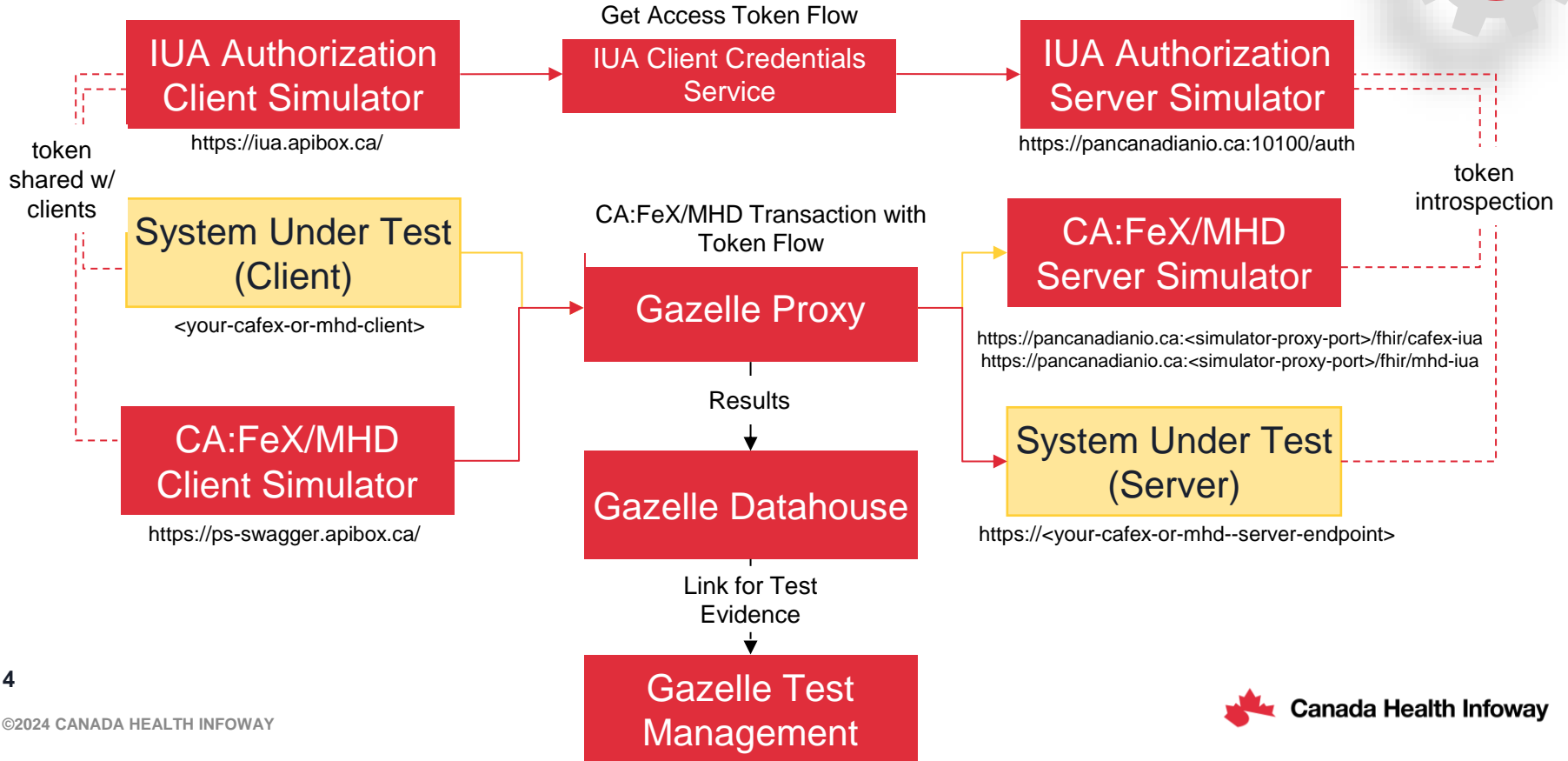
Training Objectives



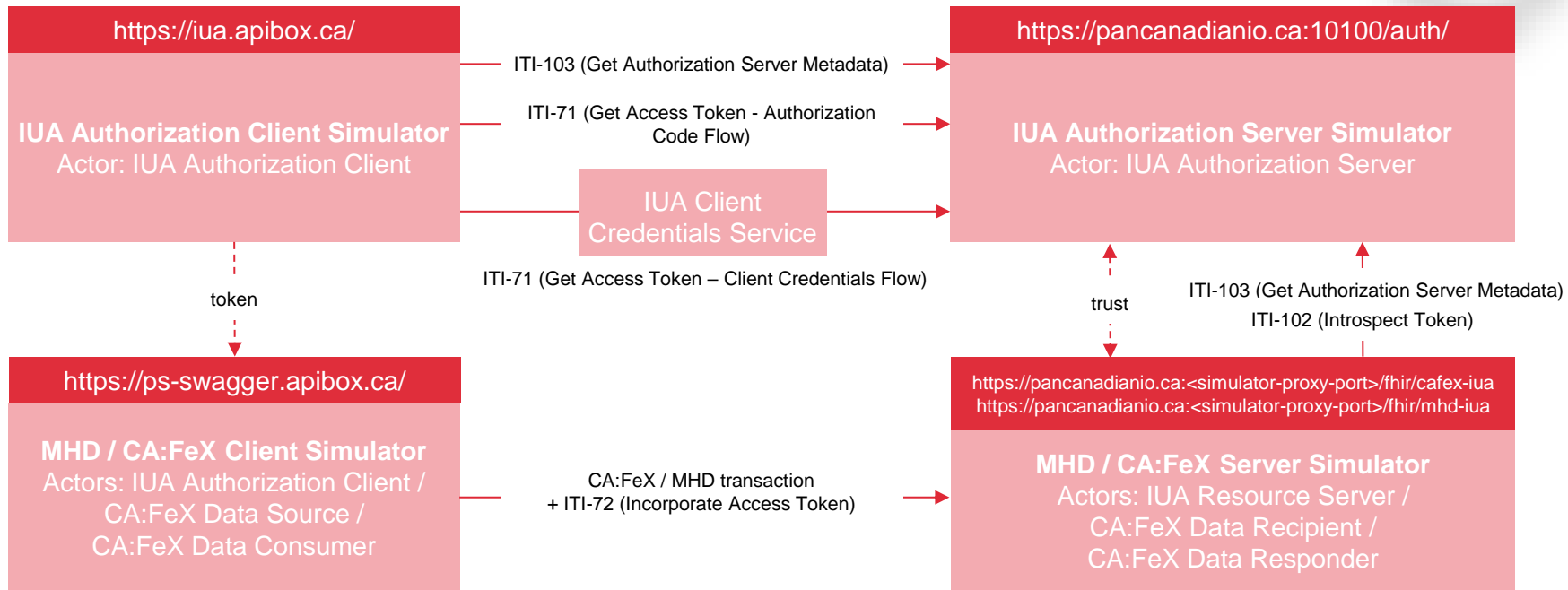
This training aims to meet the following objectives:

- ✓ Provide an understanding of the **IUA Authorization Client Simulator**, when to use it, **how** to use it, and **where** to access it
- ✓ Provide an understanding of the **IUA Authorization Server Simulator**, when to use it, **how** to use it, and **where** to access it
- ✓ Provide an understanding of the **IUA Resource Server Simulator**, when to use it, **how** to use it, and **where** to access it

IUA Simulators Architectural Overview



IUA Transaction Flows





What are the IUA Simulators' Capabilities?

The **IUA Authorization Client Simulator** and **IUA Authorization Server Simulator** are configured to support all the IUA options recommended in the pan-Canadian Reference Architecture guidance:

- ❖ OAuth2 / OIDC (Authorization Code and Client Credential grant types)
- ❖ JSON Web Tokens (JWT)
- ❖ Extended Security Features: Proof Key for Code Exchange (PKCE), State and Nonce

The **IUA Resource Server Simulator** is also configured to support all the IUA options

When to use the IUA Authorization Client Simulator



The **IUA Authorization Client Simulator** is used in Pre-Projectathon and No Peer testing when a participant wants to test that their Authorization Server (System Under Test) can supply and validate access tokens as part of the exchange workflow

- ❖ The Authorization Client Simulator UI is organized into pages by IUA Transaction (Authorization Code Flow, Client Credentials Flow, Authorization Server Metadata)
- ❖ The user designates the Authorization Server endpoint that the Authorization Client Simulator will interact with, typically entering the proxied endpoint that allows traffic to be logged for test evidence
- ❖ Responses to the transactions (e.g., Authorization tokens) are viewable in the UI and stored in the Gazelle Datahouse-Proxy to use for test evidence

When to use the IUA Authorization Server Simulator



The **IUA Authorization Server Simulator** is used in Pre-Projectathon and No Peer testing when a participant wants to test that their a) System Under Test can retrieve Authorization Server metadata and access tokens, or b) that their IUA Resource Server can retrieve, accept, and introspect access tokens and protect resources as part of the exchange workflow

- ❖ The Authorization Server Simulator has no UI but is configured to support the required all transactions under IUA Canadian Guidance (ITI-71, ITI-72, ITI-102, ITI-103). Participants can test some or all of the IUA transactions using this tool
- ❖ Responses to the transactions are returned to the System Under Test and stored in the Gazelle Datahouse-Proxy to use for test evidence

When to use the IUA Resource Server Simulator



The **IUA Resource Server Simulator** is used in Pre-Projectathon and No Peer testing when a participant wants to test that their a) Client can incorporate access tokens in the exchange workflow, or b) that their Authorization Server can respond to metadata and token introspection requests

- ❖ The Resource Server Simulator has no UI but is configured to support the required all relevant IUA transactions (ITI-72, ITI-102, ITI-103). Participants can test some or all of the IUA transactions using this tool
- ❖ Responses to the transactions are returned to the System Under Test and stored in the Gazelle Datahouse-Proxy to use for test evidence

Tool Demonstration – Authorization Client Simulator UI



If Executing ITI-103:

- 1 Navigate to the page of the transaction you would like to simulate
- 2 Enter your authorization server's (SUT) proxied endpoint information

See instructions for setting up proxy: <https://pancanadianio.ca/gazelle-documentation/Proxy/user.html>
- 3 Click "Send Request"
- 4 Authorization server's metadata (i.e., Endpoints, JWKS) is returned

The screenshot shows the 'IUA OAuth2/OIDC Client Simulator' interface. At the top, there are three tabs: 'Authorization Code Flow [ITI-71]', 'Client Credentials Flow [ITI-71]', and 'Authorization Server Metadata [ITI-103]'. The 'Authorization Server Metadata' tab is selected. Below the tabs, the title is 'Authorization Server Metadata (IUA ITI-103 Get Authorization Server Metadata)'. A form field for 'Well Known URI (required)' contains the URL 'https://pancanadianio.ca:10100/auth/realms/ps-ca/.well-known/openid-configuration'. A 'SEND REQUEST' button is visible. Below the form, a code block displays the JSON response for 'Authorization Server Metadata', with a red box highlighting the 'authorization_endpoint' and 'jwks_uri' fields.

```
Authorization Server Metadata
```

```
{  
  "issuer": "https://pancanadianio.ca:10100/auth/realms/ps-ca",  
  "authorization_endpoint": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/auth",  
  "token_endpoint": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/token",  
  "introspection_endpoint": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/token/introspection",  
  "userinfo_endpoint": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/userinfo",  
  "end_session_endpoint": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/logout",  
  "jwks_uri": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/certs",  
  "check_session_iframe": "https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/login-status-iframe",  
  "grant_types_supported": [  
    "authorization_code",  
    "implicit",  
    "refresh_token",  
    "password",  
    "client_credentials"  
  ],  
  "response_types_supported": [  
    "code",  
    "none",  
    "id_token",  
    "token"  
  ]  
}
```

Tool Demonstration – Gazelle Datahouse



After Executing Any Transaction:

5 After successfully executing the request against your proxied authorization server, navigate to the Gazelle Datahouse to select the "Access detail" you would like to use for evidence

6 Copy the permanent link for pasting into Gazelle Test Instance

Standard	Timestamp	Sender	Proxy	Receiver	Message type	Action
HTTP [L5]	02:42:46:848 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:42:46:865 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	GET	Access details
HTTP [L5]	02:42:46:547 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:42:46:546 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	OPTIONS	Access details
HTTP [L5]	02:43:07:025 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:43:06:942 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L5]	02:43:06:836 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:43:06:793 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L5]	02:43:06:596 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:43:06:535 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L5]	02:43:06:401 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L5]	02:43:06:338 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details

Connection detail

Type: HTTP [TLS]
Connection id: 675f13c322814b4ad4726b5
Permanent link: [copy URL](#) 6
Proxy port: 10100
Certificate subject: CN=pancanadiani.ca

Initiator

Hostname: pool-99-229-166-143.cpe.net.cable.rogers.com
IP address: 99.229.166.143
Port: 55133
TLS version: TLSv1.3
Cipher suite: TLS_AES_256_GCM_SHA384

Responder

Hostname: keycloak.apibox.ca
IP address: 3.96.81.134
Port: 443
TLS version: TLSv1.3
Cipher suite: TLS_AES_128_GCM_SHA256
Certificate subject: CN=*.apibox.ca, CN=Amazon RSA 2048 M02, O=Amazon, C=US, CN=Amazon Root CA 1, O=Amazon, C=US, CN=Starfield Services Root Certificate Authority - G2, O=Starfield Technologies, Inc., L=Scottsdale, ST=Arizona, C=US

Http Response < 4 of 10 >

Validation
[Validate]

Overview | Content | Validation

Tool Demonstration – Authorization Client Simulator UI



If Executing ITI-71 or ITI-72:

IUA actors who participate in No-Peer and Peer-to-Peer testing have mandatory prerequisites.

See the IUA Authorization Registration Form for details on how to register systems acting as an:

- IUA Authorization Client
- IUA Authorization Server
- IUA Resource Server

Link to Form: https://infoscribe.infoway-inforoute.ca/display/PCI/Actions+for+Participants%3A+Projectathon+2025?preview=/266960954/266960946/IUA_Registration_Form_Prjectathon_Testing_v1.docx

IUA No-Peer and Peer-to-Peer Testing: Registration
Instructions: <ul style="list-style-type: none">- If your system is registered as an IUA Authorization Client, please see Section A- If your system is registered as an IUA Authorization Server, please see Section B- If your system is registered as an IUA Resource Server, please see Section C
Section A (for IUA Authorization Clients):
This information is required if you want to: <ul style="list-style-type: none"><input type="checkbox"/> Act as an IUA Authorization Client to perform testing (No-Peer and/or Peer-to-Peer) against the IUA Authorization Server Simulator or an IUA Authorization Server test partner<input type="checkbox"/> Act as an IUA Authorization Client to perform testing (No-Peer and/or Peer-to-Peer) against CA:FeX or MHD Resource Server with IUA authorization (as this requires access token issued by the IUA Authorization Server), including testing against test partners or simulators.
1. Fill in the following information:
Your Organization Name:
Your Contact Email:
IUA Flow: (Tip: The IUA flow depends on the kind of client your application is: user-facing or backend/system) <ul style="list-style-type: none"><input type="checkbox"/> Authorization Code Flow<input type="checkbox"/> Client Credentials Flow
If you selected Authorization Code Flow, please provide this additional information:
Type of Client (Tip: Confidential Clients can store a secret safely) <ul style="list-style-type: none"><input type="checkbox"/> Confidential Client<input type="checkbox"/> Public Client
Redirect URI:

Tool Demonstration – Authorization Client Simulator UI



ITI-71 – Authorization Code Flow:

- 1 Navigate to the page of the transaction you would like to simulate
- 2 Populate your authorization server (SUT) url to pre-populate authorize and token endpoints, or enter them manually
- 3 Enter the Client ID (Confidential Client is recommended) and Redirect URI as registered with the authorization server
- 4 Indicate the Scopes to be included in the access token
 - 4.1 *Recommended:* Populate additional details if using additional security features (e.g., PKCE, State, Nonce)

Canada Health Infoway
Inforoute Santé du Canada

IUA OAuth2/OIDC Client Simulator

1 Authorization Code Flow [ITI-71] Client Credentials Flow [ITI-71] Authorization Server Metadata [ITI-103]

2 Populate Authorize and Token endpoints from server metadata

Well Known URI (required)
https://pancanadianio.ca:10100/auth/realms/ps-ca/.well-known/openid-confi

Populate

Authorization Code Flow (IUA ITI-71 Get Access Token)

2 Authorize URI (required)
https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/

Token URI (required)
https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/

3 Redirect URI (required)
https://iua.apibox.ca/authorize

Client ID (required)
ps-ca-standard-PKCE-client

Client Type
 Confidential Client

Client Secret (required)
.....

4 Scopes

CAFEX CAFEX-1 CAFEX-2 CAFEX-3

MHD ITI-65 ITI-66 ITI-67 ITI-68

Other

4.1 PKCE
 Use PKCE

State
8pTfxiODamIRjhu4S1pu5wjxjx0W

Nonce
9u4wDT7kvhTvPTiCkK6xZdGIWHSqD

Tool Demonstration – Authorization Client Simulator UI



ITI-71 – Authorization Code Flow:

- 5 Review the HTTP request with provided parameters
- 6 Click “Send Request”
- 7 You will be redirected to the authorization server to enter your user credentials, Click “Log in”
- 8 Click “Yes” to provide consent to the requested scopes

```
https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/auth
?client_id=ps-ca-standard-PKCE-client
&redirect_uri=https://iua.apibox.ca/authorize
&scope=CAFEX-1 CAFEX-2
&response_type=code
&state=8pTfxiODamLRjhu4S1puf5wjqjxu0W
&nonce=9u4wDT7kvhTVPTiCKK6xZdIG1WHSqD
```

PS-CA

Log In

Username or email
pscauser1

Password

SEND REQUEST

Log In

PS-CA

Grant Access to ps-ca-standard-PKCE-client

Do you grant these access privileges?

Email address

User profile

Consent to CAiFeX transaction CAFEX-2?

Consent to CAiFeX transaction CAFEX-1?

User roles

No Yes

Tool Demonstration – Gazelle Datahouse



After Executing Any Transaction:

13

After successfully executing the request against your proxied authorization server, navigate to the Gazelle Datahouse to select the "Access detail" you would like to use for evidence

Gazelle Datahouse - Proxy

Standard Sender hostname Sender ip address Proxy port Receiver hostname Receiver ip address Message type Secured message

Date from / to mm/dd/yyyy, ---- AM AST - mm/dd/yyyy, ---- AM AST

Standard	Timestamp	Sender	Proxy	Receiver	Message type	Action
HTTP [L3]	02:42:46:848 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:42:46:865 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	GET	Access details
HTTP [L3]	02:42:46:547 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:42:46:546 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	OPTIONS	Access details
HTTP [L3]	02:43:07:925 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:942 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:836 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:793 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:598 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:535 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:401 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:338 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details

14

Copy the permanent link for pasting into Gazelle Test Instance

Gazelle Datahouse - Proxy

Connection detail

Type: HTTP [L3]

Connection id: 675f13c322814b4ad4726b5

Permanent link: [sdpvLUBL](#)

Proxy port: 10100

Certificate subject: CN=pancanadiani.ca

Initiator

Hostname: pool-99-229-166-143.cpe.net.cable.rogers.com

IP address: 99.229.166.143

Port: 55133

TLS version: TLSv1.3

Cipher suite: TLS_AES_256_GCM_SHA384

Responder

Hostname: keycloak.apibox.ca

IP address: 3.96.81.134

Port: 443

TLS version: TLSv1.3

Cipher suite: TLS_AES_128_GCM_SHA256

Certificate subject: CN=*.apibox.ca, CN=Amazon RSA 2048 M02, O=Amazon, C=US, CN=Amazon Root CA 1, O=Amazon, C=US, CN=Starfield Services Root Certificate Authority - G2, O=Starfield Technologies, Inc., L=Scottsdale, ST=Arizona, C=US

Http Response < 4 of 10 >

Validation

Validate

Overview | Content | Validation

Tool Demonstration – Authorization Client Simulator UI



ITI-71 – Client Credentials Flow:

- 1 Navigate to the page of the transaction you would like to simulate
- 2 Populate your authorization server (SUT) url to pre-populate token endpoint, or enter it manually
- 3 Enter the Client ID and Client Secret as registered with the authorization server
- 4 Indicate the Scopes to be included in the access token
- 5 Click “Send Request”
- 6 Copy access token for use in CA:FeX-IUA/MHD-IUA exchange workflows that incorporate IUA Access Token (ITI-72)

Note: This flow does not include any user authentication or consent granting steps

The screenshot displays the 'IUA OAuth2/OIDC Client Simulator' interface. At the top, there are three tabs: 'Authorization Code Flow [ITI-70]', 'Client Credentials Flow [ITI-71]', and 'Authorization Server Metadata [ITI-103]'. The 'Client Credentials Flow [ITI-71]' tab is active.

Step 2: A form section titled 'Populate Token endpoint from server metadata' with a checked checkbox. Below it, the 'Well Known URI (required)' field contains the URL 'https://pancanadianio.ca:10100/auth/realms/ps-ca/.well-known/openid-confi'. A 'Populate' button is located below the field.

Step 3: A section titled 'Client Credentials Flow (IUA ITI-71 Get Access Token)'. It contains a 'Token URI (required)' field with the URL 'https://pancanadianio.ca:10100/auth/realms/ps-ca/protocol/openid-connect/'.

Step 4: A section for 'Client ID (required)' with the value 'ps-ca-rest-client' and 'Client Secret (required)' with a masked value '*****'.

Step 5: A 'Scopes' section with a table of checkboxes:

Scope	CA:FeX	MHD	Other
CAFEX-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CAFEX-2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CAFEX-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITI-65	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITI-66	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITI-67	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITI-68	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 6: A 'SEND REQUEST' button at the bottom of the main form.

Available authorizations dialog (Step 6): A modal window titled 'Available authorizations' showing 'Bearer Authorization (http, Bearer)'. It states: 'This API uses Bearer Authorization that requires a valid access token provided by the authorization server.' The 'Value:' field contains the token 'MzhGCF-GylCzq3fXbsmR3iqDGAM6zRPb97-tfAs9LdKsWqNfutCGcHBSUpAcTf1tIiw'. There are 'Authorize' and 'Close' buttons at the bottom.

Tool Demonstration – Gazelle Datahouse



After Executing Any Transaction:

7

After successfully executing the request against your proxied authorization server, navigate to the Gazelle Datahouse to select the "Access detail" you would like to use for evidence

8

Copy the permanent link for pasting into Gazelle Test Instance

The screenshot shows the Gazelle Datahouse interface. The top part displays a table of transactions with columns for Standard, Timestamp, Sender, Proxy, Receiver, Message type, and Action. A red circle with the number 7 highlights the 'Access details' link in the Action column for the first transaction.

Standard	Timestamp	Sender	Proxy	Receiver	Message type	Action
HTTP [L3]	02:42:46:848 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:42:46:865 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	GET	Access details
HTTP [L3]	02:42:46:547 PM - AST Dec 05, 2024	ps-swagger-api.apibox.ca	10001	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:42:46:546 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10001	ps-swagger-api.apibox.ca	OPTIONS	Access details
HTTP [L3]	02:43:07:025 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:942 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:836 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:793 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:596 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:535 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details
HTTP [L3]	02:43:06:401 PM - AST Dec 05, 2024	keycloak.apibox.ca	10100	pool-99-229-166-143.cpe.net.cable.rogers.com	200	Access details
HTTP [L3]	02:43:06:338 PM - AST Dec 05, 2024	pool-99-229-166-143.cpe.net.cable.rogers.com	10100	keycloak.apibox.ca	GET	Access details

The bottom part of the screenshot shows the detailed view of a transaction. It includes sections for Connection detail, Initiator, Responder, and Http Response. A red circle with the number 8 highlights the 'Permanent link' field in the Connection detail section.

Connection detail

- Type: HTTP [TLS]
- Connection id: 675f13c322814b4ad4726b5
- Permanent link: [sdpvLUBL](#)
- Proxy port: 10100
- Certificate subject: CN=pancanadiani.ca

Initiator

- Hostname: pool-99-229-166-143.cpe.net.cable.rogers.com
- IP address: 99.229.166.143
- Port: 55133
- TLS version: TLSv1.3
- Cipher suite: TLS_AES_256_GCM_SHA384

Responder

- Hostname: keycloak.apibox.ca
- IP address: 3.96.81.134
- Port: 443
- TLS version: TLSv1.3
- Cipher suite: TLS_AES_128_GCM_SHA256
- Certificate subject: CN=*.apibox.ca, CN=Amazon RSA 2048 M02, O=Amazon, C=US, CN=Amazon Root CA 1, O=Amazon, C=US, CN=Starfield Services Root Certificate Authority - G2, O=Starfield Technologies, Inc., L=Scottsdale, ST=Arizona, C=US

Http Response 4 of 10

Validation:

Where to Access the IUA Simulators



Simulator	URL
IUA Authorization Client Simulator	https://iua.apibox.ca/
IUA Authorization Server Simulator	https://pancanadianio.ca:10100/auth/realms/ps-ca/
IUA Resource Server (CA:FeX)	https://pancanadianio.ca:10001/fhir/cafex-iua (Option A) https://pancanadianio.ca:10002/fhir/cafex-iua (Option B) https://pancanadianio.ca:10003/fhir/cafex-iua (Option C) https://pancanadianio.ca:10004/fhir/cafex-iua (Option D)
IUA Resource Server (MHD)	https://pancanadianio.ca:10005/fhir/mhd-iua
IUA Client Simulator (grouped with CA:FeX and MHD, for ITI-72)	https://ps-swagger.apibox.ca/index.html



Canada Health Infoway

Thank you!

To learn more about the Projectathon 2025, visit:

<https://infoscribe.infoway-inforoute.ca/display/PCI/Scope%3A+Projectathon+2025>

Contact Information:

interoperability@infoway-inforoute.ca

VISIT OUR WEBSITE
infoway-inforoute.ca

VISIT OUR SURVEY WEBSITE
insights.infoway-inforoute.ca/

LET'S CONNECT ON LINKEDIN
linkedin.com/company/canada-health-infoway/

LET'S CONNECT ON TWITTER
@infoway