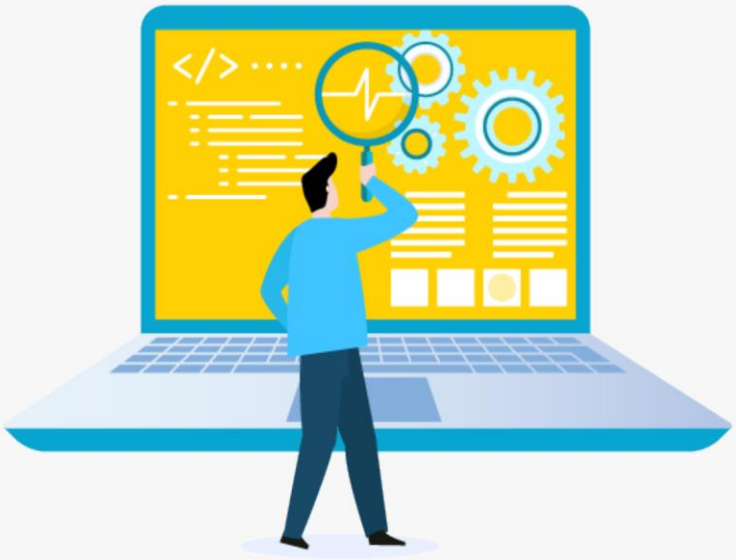
How to Test Firely Server on Inferno

A Step-by-Step Guide to Demonstrate 100% Compliance with the 21st Century Cures Act Final Rule



server@fire.ly www.fire.ly @FirelyTeam

How to Test Firely Server on Inferno

***The following guide, reference servers, and testing data are currently implemented for US Core 3.1.1 USCDI V1 and SMART 1.0 only.**

Are you considering using Firely Server to power your healthcare portal, app, or database? Or maybe you already do?

Either way, with the 'Final Rule' deadline fast approaching, it is good to know that Firely Server is 100% compliant with the § 170.315(g)(10) criterion.

This Step-by-Step Guide shows you how to test that compliance using Inferno **7.2.3**. It should take about 30 minutes to complete.

Contents

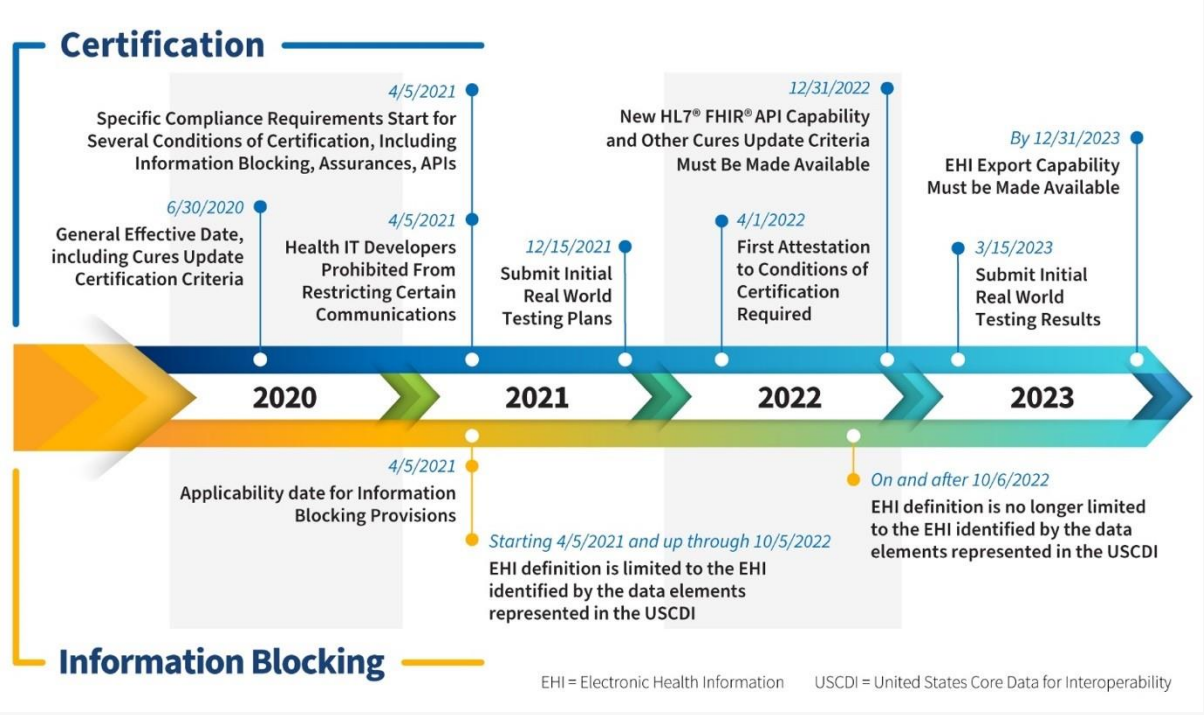
1 The 21st Century Cures Act Final Rule

ONC has adopted a new secure, standards-based API certification criterion in § 170.315(g)(10) to implement the 21st Century Cures Act's requirement that certified health IT APIs can be used "without special effort."

This new criterion requires standardized API access for single patient and population services and is limited to API-enabled "read" services using the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard. The FHIR standard, in addition to a set of adopted implementation specifications, provides known and consistent technical requirements for software developers.

2 Timelines

The timelines for the Final Rule are shown below. The deadline for compliant FHIR APIs to be in place was 31 December 2022[1]. And the regulation for EHI export capabilities - 170.315(b)(10) - is mandatory starting from December 31, 2023



Additional required updates can be found here.

3 Introduction to Inferno

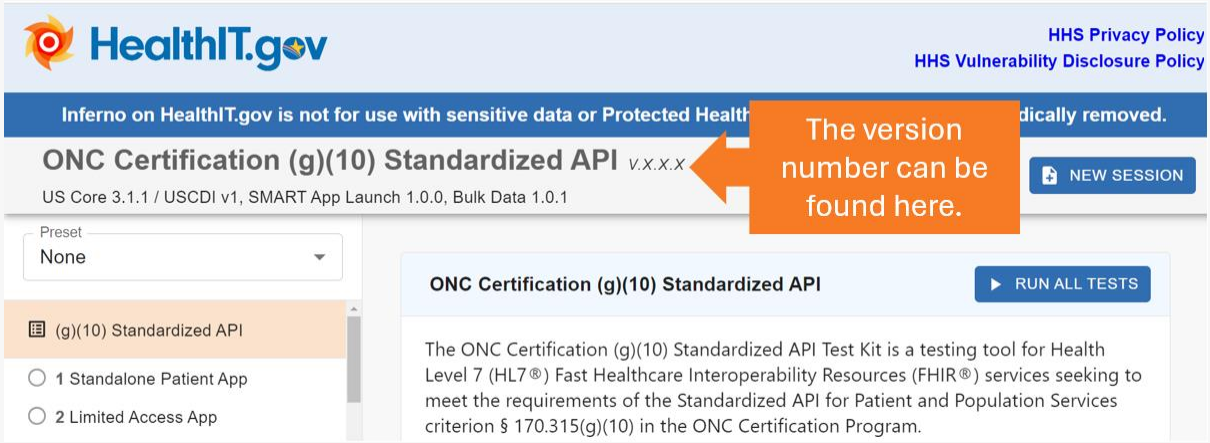
Inferno (https://inferno.healthit.gov/onc-certification-g10-test-kit) is an open-source tool to test if a FHIR server is compliant with the above-mentioned criteria as defined in § 170.315(g)(10. It tests for conformance to authentication, authorization, and FHIR content standards including:

- FHIR Release 4.0.1
- FHIR US Core Implementation Guide (IG) STU 3.1.1
- SMART Application Launch Framework Implementation Guide Release 1.0.0

- HL7 FHIR Bulk Data Access (“Flat FHIR”) (v1.0.1: STU 1)

Firely Server (≥ v4.0) is fully compliant with all these requirements. To demonstrate this, we have documented all the steps you should take to test Firely Server using Inferno.
There are six groups of tests with implicit dependencies between them, and we recommend you run them in the order we have used here. For each test we have described all the information you need to enter manually and provided screenshots with orange rectangles showing where it should be typed in. We also explain and show the overall flow of the test and the end result.

These instructions are based on Inferno version **7.2.3**. The Inferno version number can be found here:



If you’re using an older version of Inferno you should update to version **7.2.3** before using this guide.

Authentication and authorization are a key element of these tests. The tokens you get after logging in are valid for one hour which should be plenty of time to run all the tests. If a test fails because a token has expired you will need to start the process from the beginning.

The public Inferno server can be a bit slow, which can also result in a failing test. If all the data is entered correctly the test should succeed on the second attempt.

All tests should be green when complete. If you do encounter an unexplained failing test, feel free to reach out to server@fire.ly.

4 Now let’s start testing!

1. Navigate to https://inferno.healthit.gov/suites/g10_certification
2. Keep the default radio selections as US Core 3.1.1 / USCDI v1, SMART App Launch 1.0.0 and Bulk Data 1.0.1:

ONC Certification (g)(10) Standardized API Test Kit

Last Updated: *June 10, 2025* ***Test Kit Version:*** *7.2.3* ***Maturity:*** *High*

SMART App Launch US Core Bulk Data

The ONC Certification (g)(10) Standardized API Test Kit is a testing tool for Health IT systems seeking to meet the requirements of the Standardized API for Patient and Population Services criterion § 170.315(g)(10) in the ONC Certification Program. It is an approved test method for the § 170.315(g)(10) test procedure.

Systems may adopt later versions of standards than those named in the rule as approved by the ONC Standards Version Advancement Process (SVAP). Please note that US Core Implementation Guide v.7.0.0 should only be used with SMART App Launch Guide v2.0.0 or above due to granular scope support requirements within this version of US Core.

Please select which approved version of each standard to use, and click 'Create Test Session' to begin testing.

This test kit includes a simulated conformant FHIR API that can be used to demonstrate success for all tests. This simulated API is open source and is available on GitHub. Visit the walkthrough for a demonstration of using these tests against the provided simulated FHIR API.

Status

The ONC Certification (g)(10) Standardized API is actively developed and updates are released monthly.

The test kit currently tests all requirements for the Standardized API for Patient and Population Services criterion § 170.315(g)(10), including updates from the HTI-1 Final Rule. This includes:

- SMART App Standalone Launch with full system access
- SMART App Standalone Launch with limited system access
- SMART App Standalone Launch with OpenID Connect
- SMART App EHR Launch with user scopes
- SMART App EHR Launch with patient scopes
- SMART App Launch Invalid AUD Parameter
- SMART App Launch Invalid Access Token Request
- SMART App Launch Token Introspection
- SMART App Launch v1 and v2 scopes
- SMART App Launch finer-grained scope access
- Support for Capability Statement
- Support for all US Core Profiles
- Searches required for each resource
- Support for Must Support Elements
- Profile Validation
- Reference Validation
- Export of multiple patients using the FHIR Bulk Data Access IG

See the test descriptions within the test kit for detail on the specific validations performed as part of testing these requirements.

Repository and Resources

The ONC Certification (g)(10) Standardized API Test Kit can be downloaded from its GitHub repository, where additional resources and documentation are also available to help users get started with the testing process. The repository Wiki provides a FAQ for testers, and the Releases page provides information about each new release.

Providing Feedback and Reporting Issues

We welcome feedback on the tests, including but not limited to the following areas:

- Validation logic, such as potential bugs, lax checks, and unexpected failures.
- Requirements coverage, such as requirements that have been missed, tests that necessitate features that the IG does not require, or other issues with the interpretation of the IG's requirements.
- User experience, such as confusing or missing information in the test UI.

Please report any issues with this set of tests in the issues section of the repository.

Start Testing

US Core Version

- (●) US Core 3.1.1 / USCDI v1
- ( ) US Core 4.0.0 / USCDI v1
- ( ) US Core 6.1.0 / USCDI v3
- ( ) US Core 7.0.0 / USCDI v4

SMART App Launch Version

- (●) SMART App Launch 1.0.0
- ( ) SMART App Launch 2.0.0
- ( ) SMART App Launch 2.2.0

Bulk Data Version

- (●) Bulk Data 1.0.1
- ( ) Bulk Data 2.0.0

⊕ Create Test Session

Your Recent Sessions

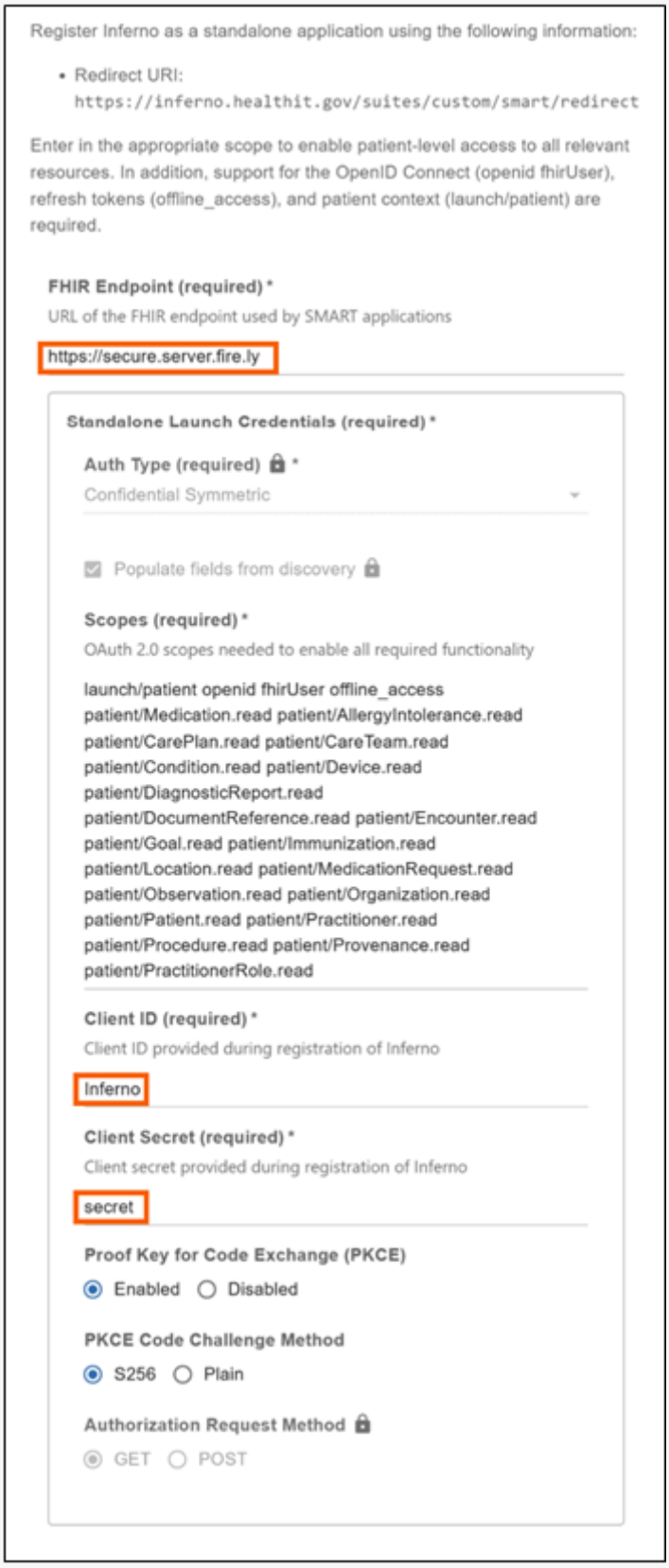
- (g)(10) Standardized API — 5/23/2025, 11:38:44 AM
- (g)(10) Standardized API — 5/9/2025, 8:41:37 PM
- (g)(10) Standardized API — 5/9/2025, 4:03:03 PM
- (g)(10) Standardized API — 4/28/2025, 3:04:26 PM
- (g)(10) Standardized API — 7/5/2024, 12:06:26 PM

3. Click button **Create Test Session**

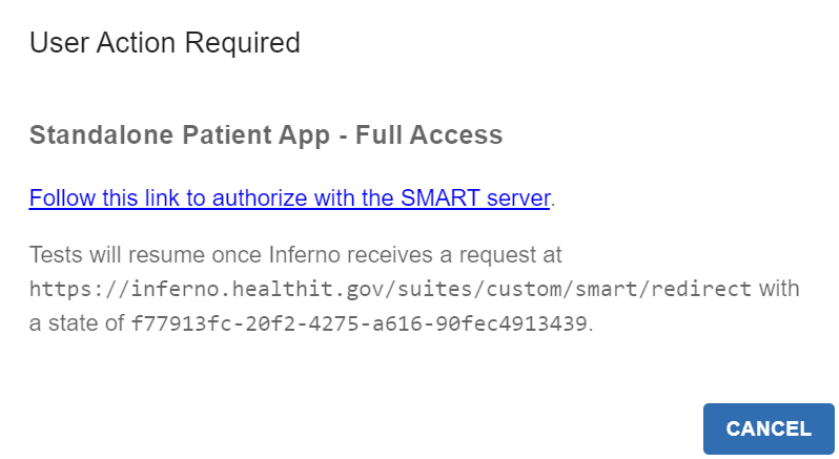
5 Standalone Patient App – Full Patient Access

1. Click **1 Standalone Patient App** on the testing menu on the left of the screen and click **RUN TESTS**
2. Fill in these values:

Field	Value
FHIR Endpoint	https://secure.server.fire.ly
Standalone Client ID	Inferno
Standalone Client Secret	secret



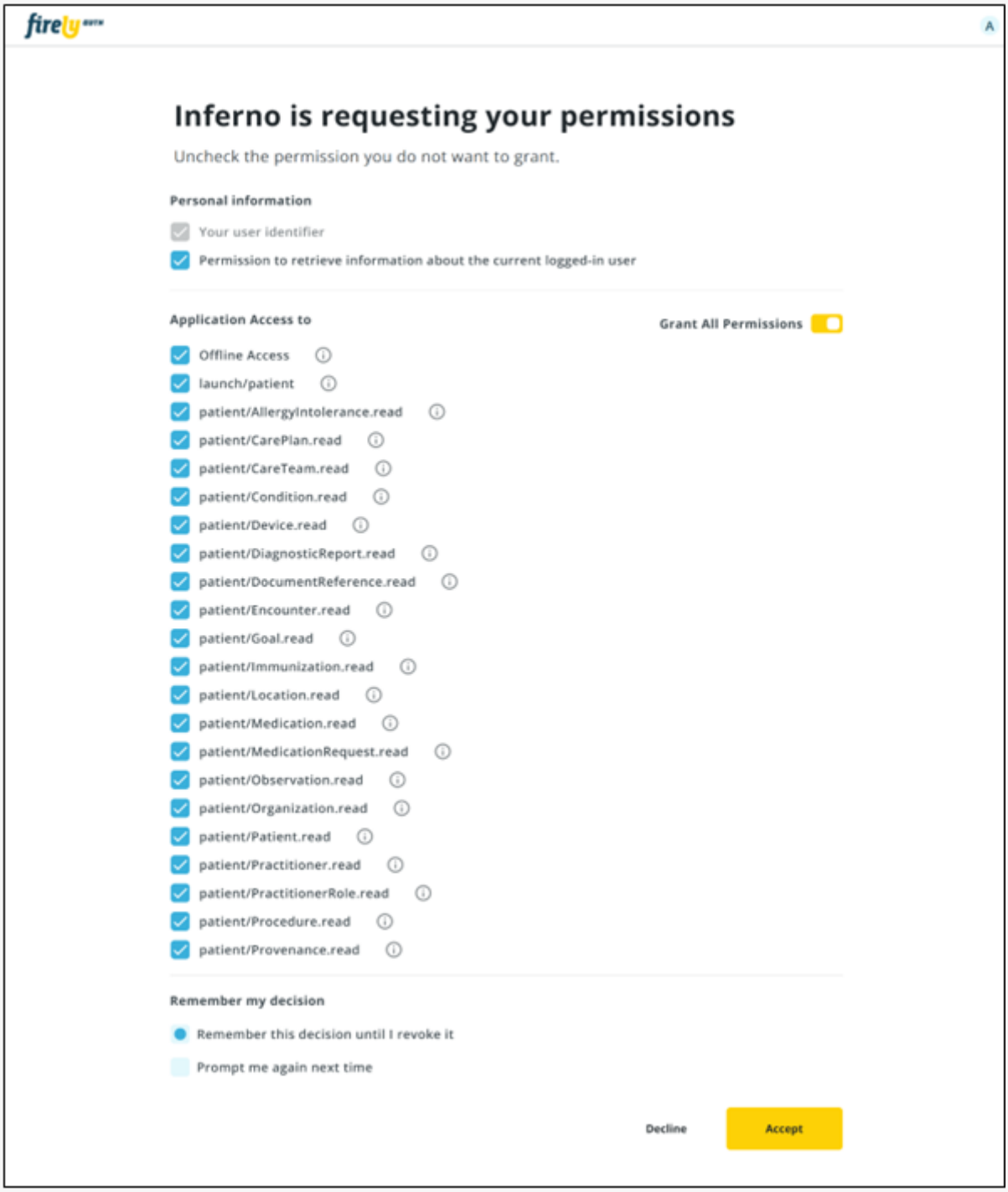
3. Click **SUBMIT**
4. A **User Action Required** dialog opens:



5. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
6. Log in to Firely Identity Server using these credentials:

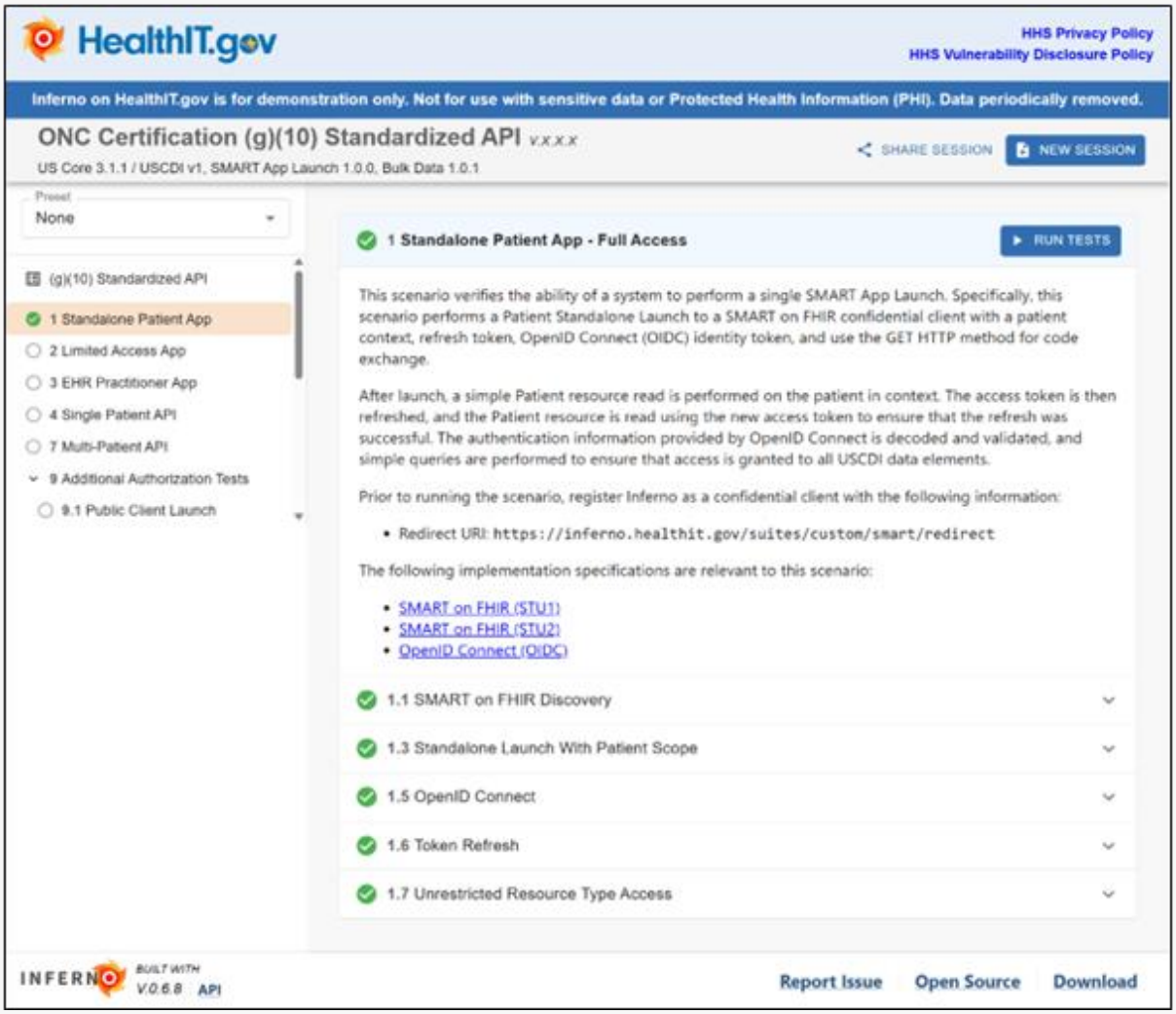
Field	Value
Username	fa_alice@fire.ly
Password	AlicePassword1!

7. Press **Login**
8. A dialog **Inferno is requesting your permission** opens
9. Make sure all the boxes are checked:



10. Click **Accept**
11. When you return to Inferno, a progress bar shows in the bottom right corner

12. When this progress bar finishes and closes, all tests should be green:



6 Standalone Patient App – Limited Access

1. Click **2 Limited Access App** on the testing menu on the left of the screen and click **RUN TESTS**
2. A dialog opens. All the required information should be prefilled:

The purpose of this test is to verify that patient app users can restrict access granted to apps to a limited number of resources. This test can only be run after the Standalone Patient App test, and all other inputs are locked to ensure the same launch configuration in both tests.

Enter which resources the user will grant access to below, and during the launch process only grant access to those resources. Inferno will verify that access granted matches these expectations.

Expected Resource Grant for Limited Access Launch (required) *

the user will only grant access to the following resources during authorization.

patient, condition, observation

Standalone FHIR Endpoint (required) *

URL of the FHIR endpoint used by standalone applications

https://secure.server.fire.ly

Standalone Launch Credentials (required) *

Auth Type (required) *

Confidential Symmetric

Populate fields from discovery

Scopes (required) *

OAuth 2.0 scopes needed to enable all required functionality

launch/patient openid fhirUser offline_access patient/Medication.read patient/AllergyIntolerance.read patient/CarePlan.read patient/CareTeam.read patient/Condition.read patient/Device.read patient/DiagnosticReport.read patient/DocumentReference.read patient/Encounter.read patient/Goal.read patient/Immunization.read patient/Location.read patient/MedicationRequest.read patient/Observation.read patient/Organization.read patient/Patient.read patient/Practitioner.read patient/Procedure.read patient/Provenance.read patient/PractitionerRole.read

Client ID (required) *

Client ID provided during registration of Inferno

Inferno

Client Secret (required) *

Client secret provided during registration of Inferno

secret

Proof Key for Code Exchange (PKCE)

Enabled Disabled

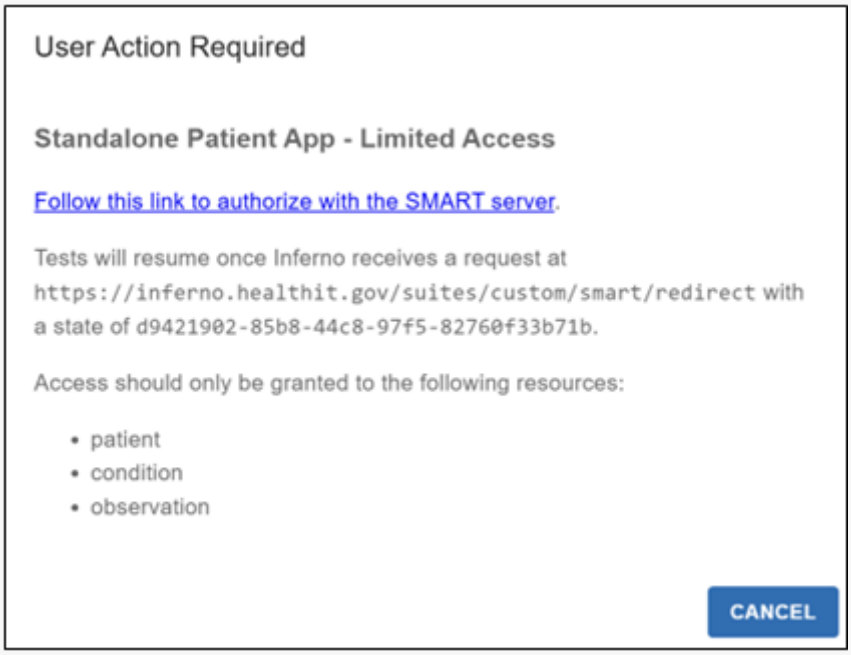
PKCE Code Challenge Method

S256 Plain

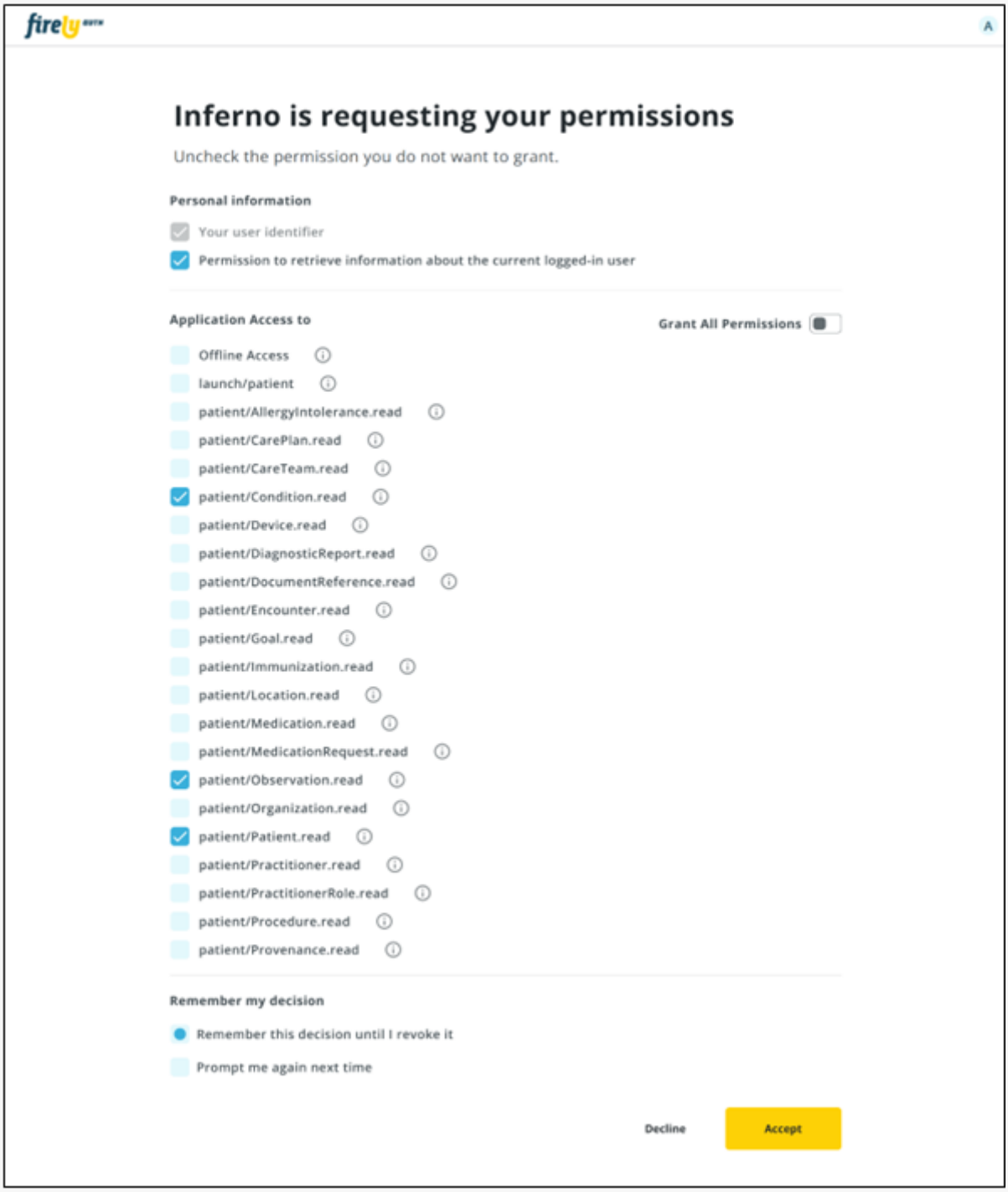
Authorization Request Method

GET POST

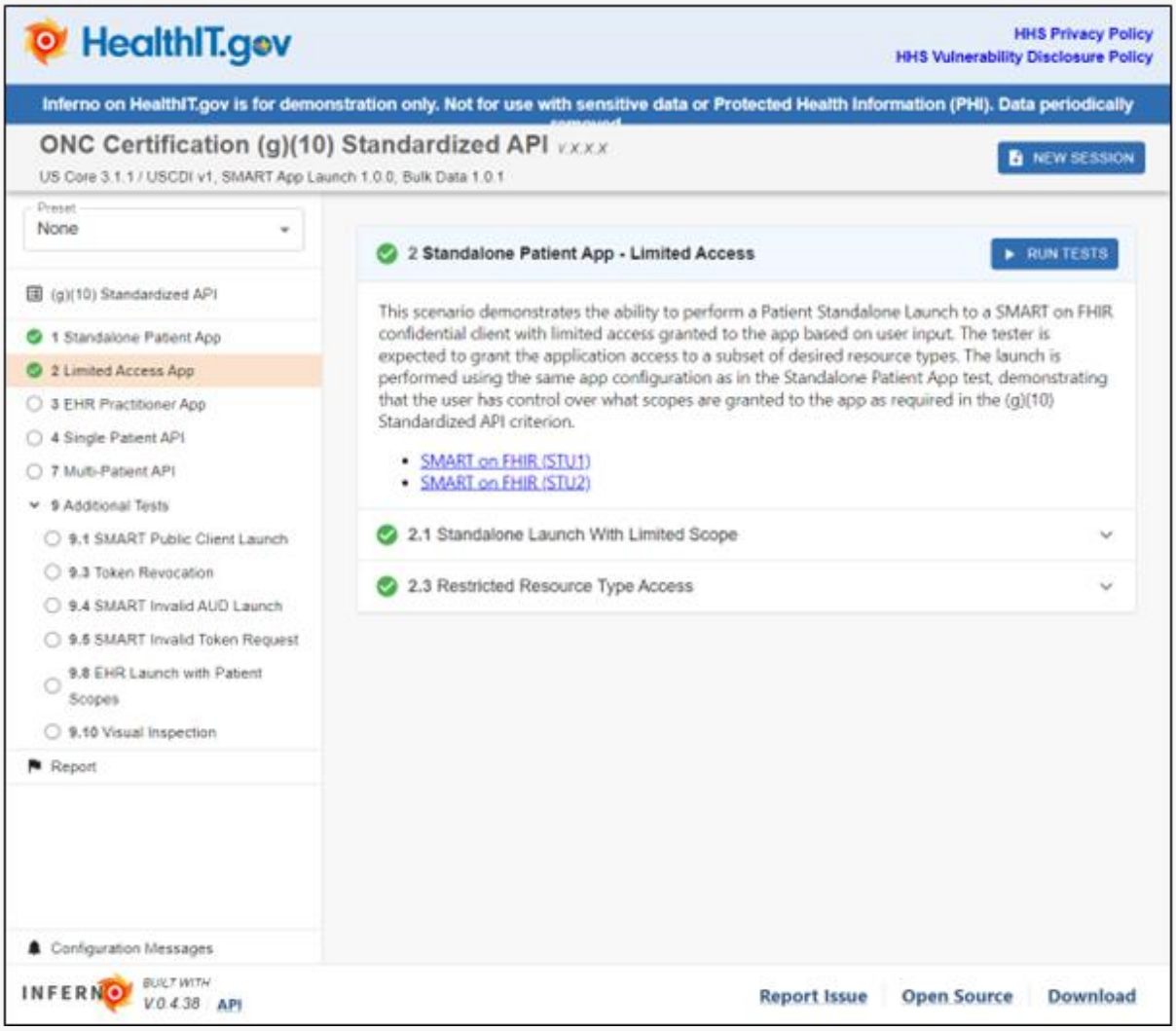
3. Click **SUBMIT**
4. A **User Action Required** dialog opens:



5. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
6. A dialog **Inferno is requesting your permission** opens
7. Make sure to uncheck all *patient* scopes except **patient/Patient.read**, **patient/Condition.read** and **patient/Observation.read:**



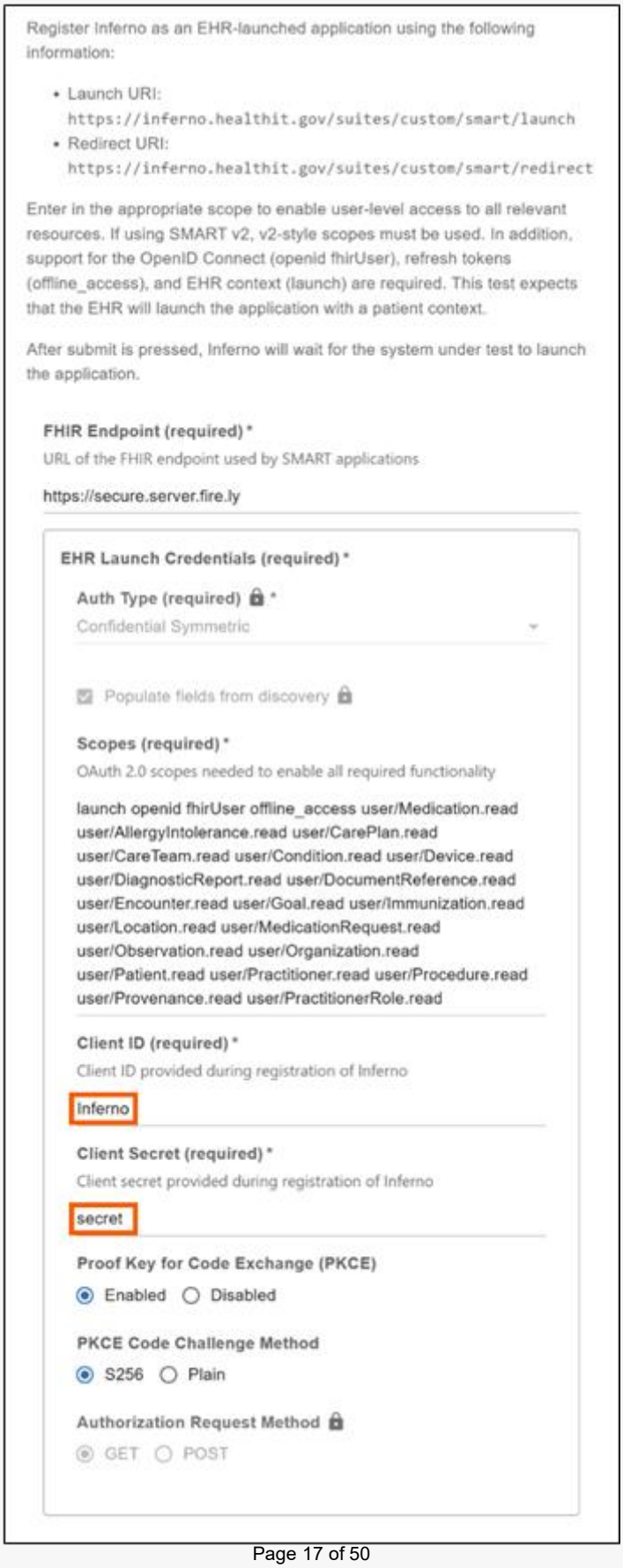
8. Click **Accept**
9. When you return to Inferno, a progress bar shows in the bottom right corner
10. When this progress bar finishes and closes, all tests should be green:



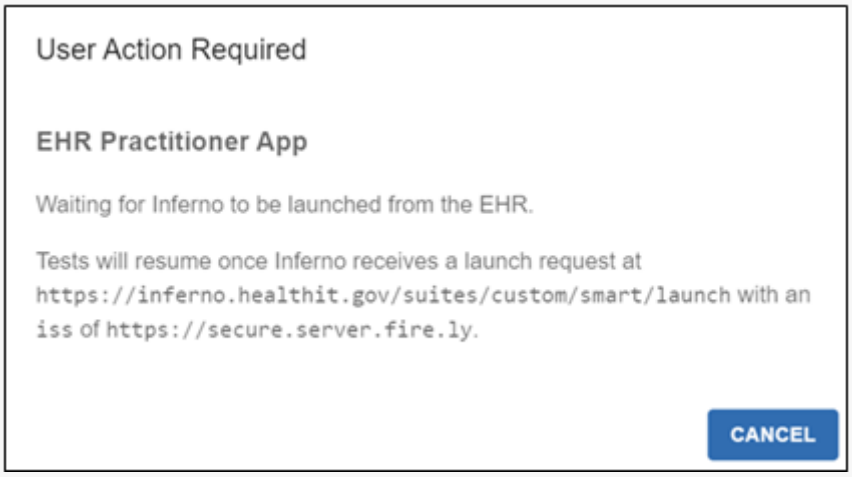
7 EHR Practitioner App

1. Click **3 EHR Practitioner App** on the testing menu on the left of the screen and click **RUN TESTS**
2. Besides prefilled values, fill in these values:

Field	Value
EHR Launch Client ID	Inferno
EHR Launch Client Secret	secret

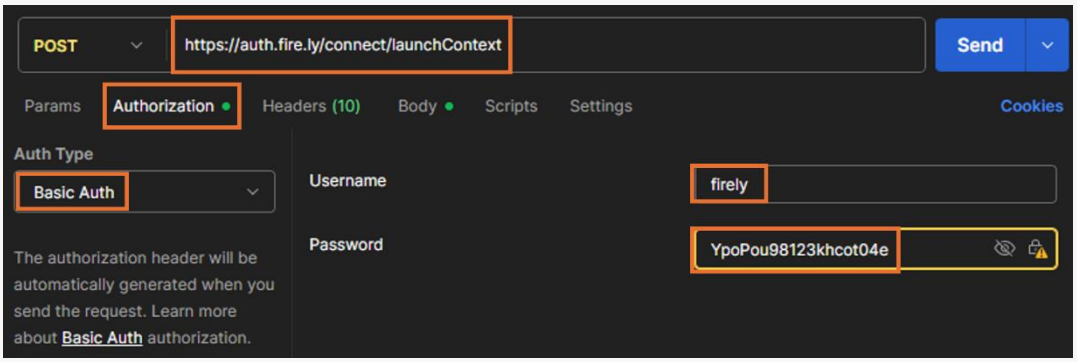


3. Click **SUBMIT**
4. A **User Action Required** dialog opens:



5. Now open Postman and open a new tab for making a request
6. Select the **Authorization** tab
7. Fill in/select the following values:

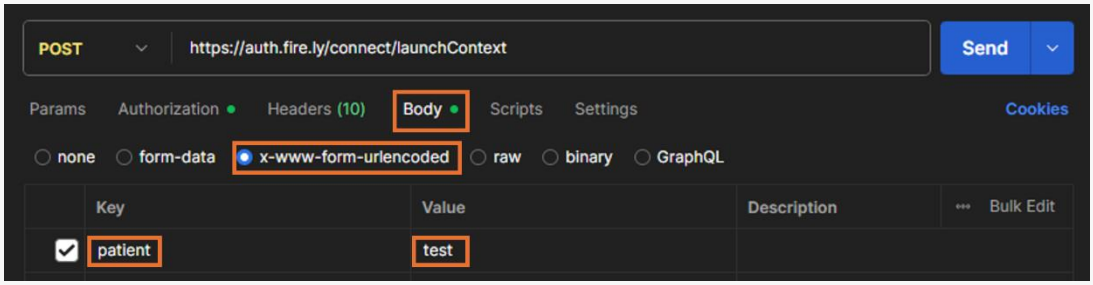
Field	Value
HTTP verb	POST
Request URL	https://auth.fire.ly/connect/launchContext
Type	Basic Auth
Username	firely
Password	YpoPou98123khcot04e



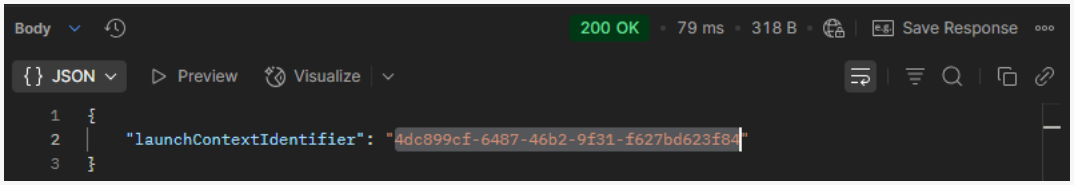
8. Select the **Body** tab
9. Select **x-www-form-urlencoded**

10. Fill in/select the following values:

KEY	VALUE
patient	test



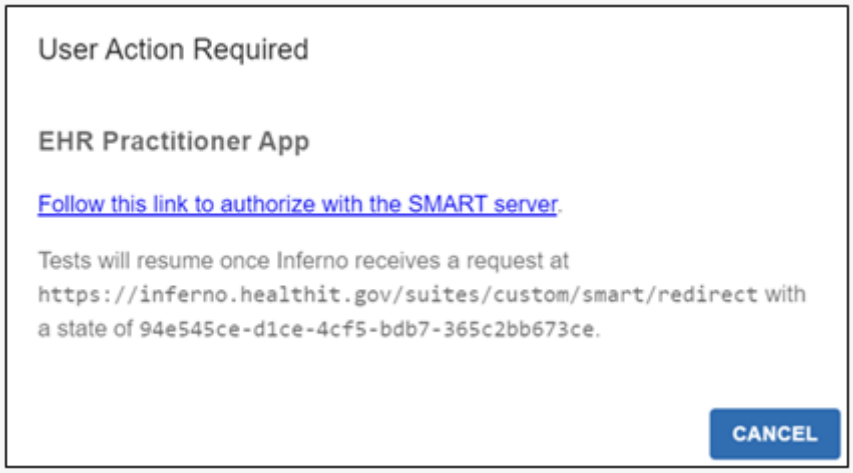
11. Click **Send**
12. The response should be a **200 OK**



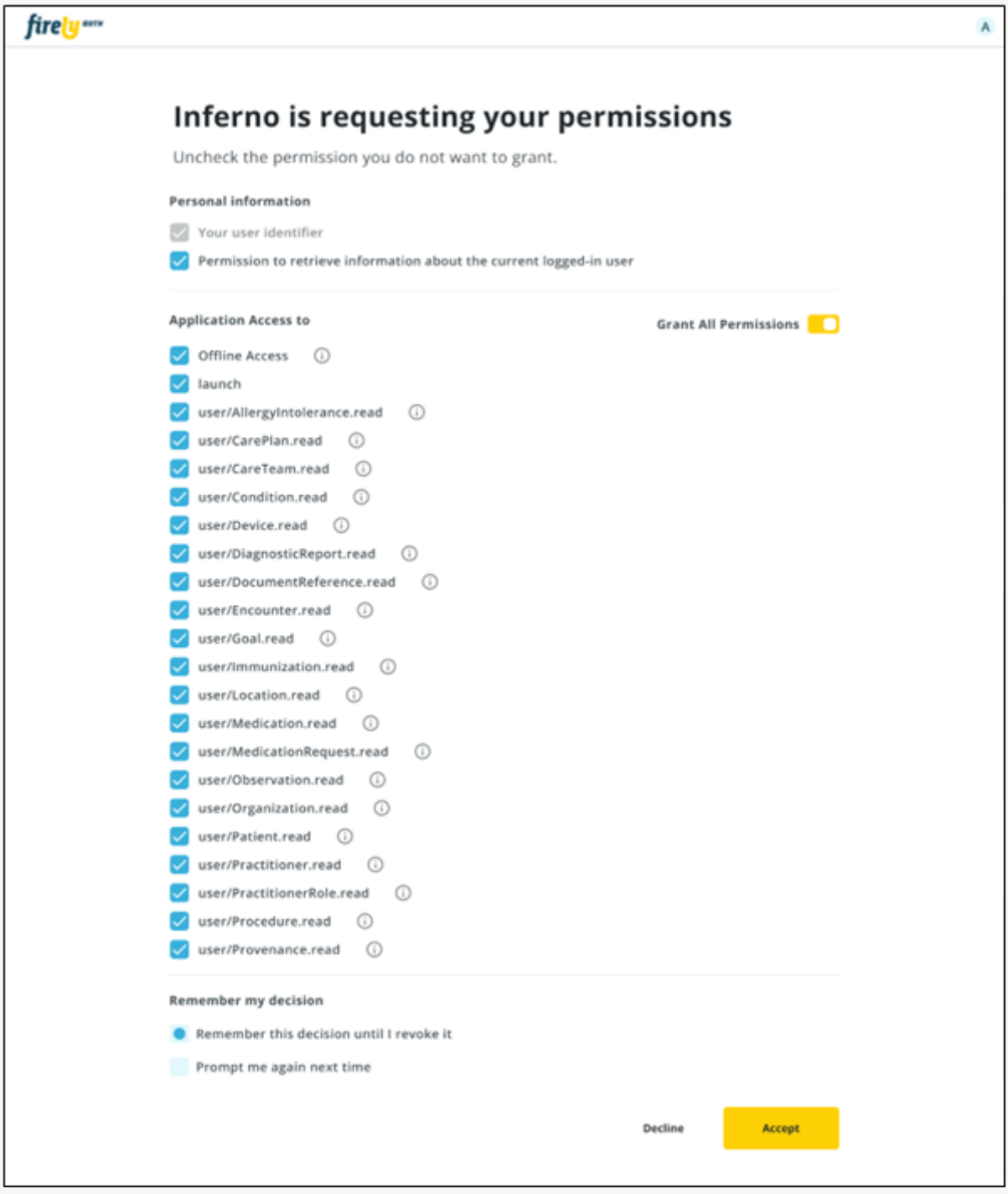
13. Open a new web browser tab and go to the following URL containing using the **launchContextIdentifier** value received (this value will be refreshed with each new request):

https://inferno.healthit.gov/suites/custom/smart/launch?iss=https://secure.server.fire.ly&launch=4dc899cf-6487-46b2-9f31-f627bd623f84

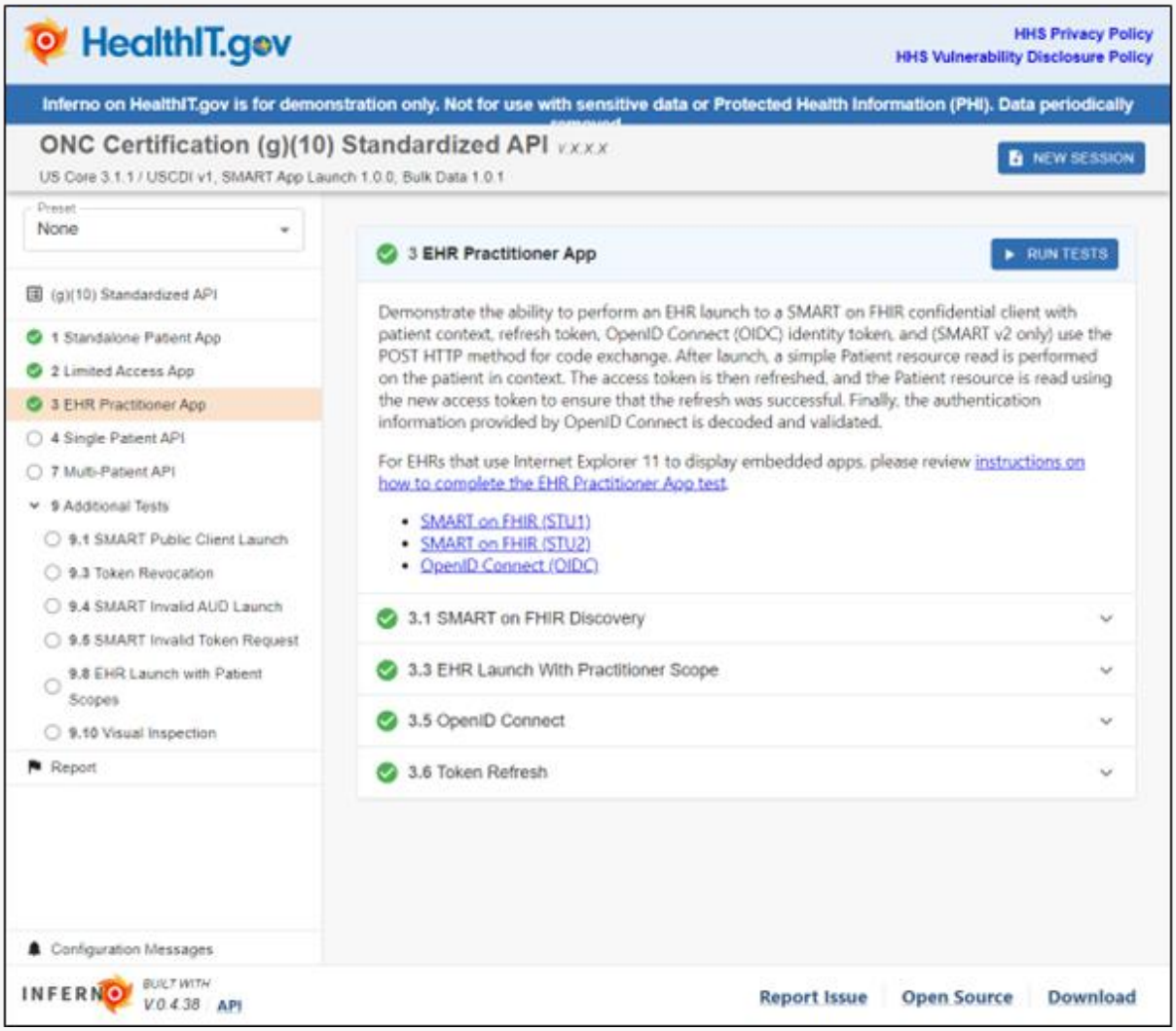
14. Another **User Action Required** dialog opens:



15. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
16. A dialog **Inferno is requesting your permission** opens
17. Make sure all the boxes are checked:

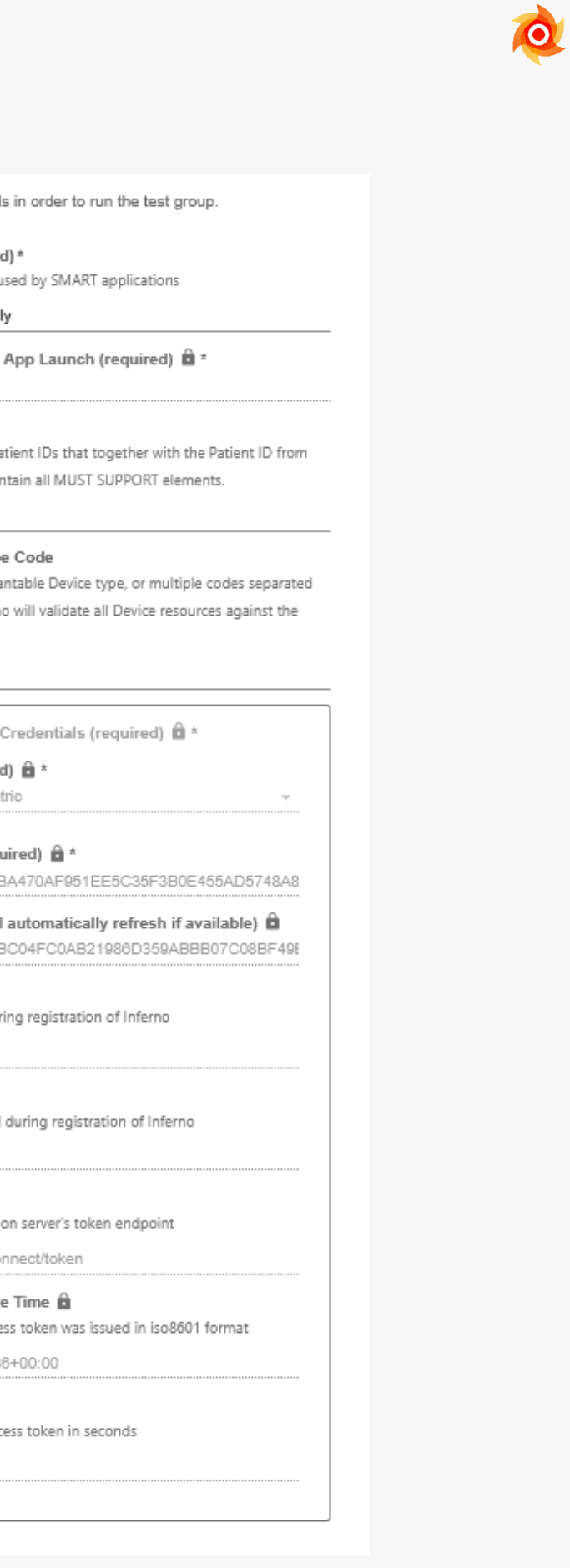


18. Click **Accept**
19. When you return to Inferno, a progress bar shows in the bottom right corner
20. When this progress bar finishes and closes, all tests should be green:

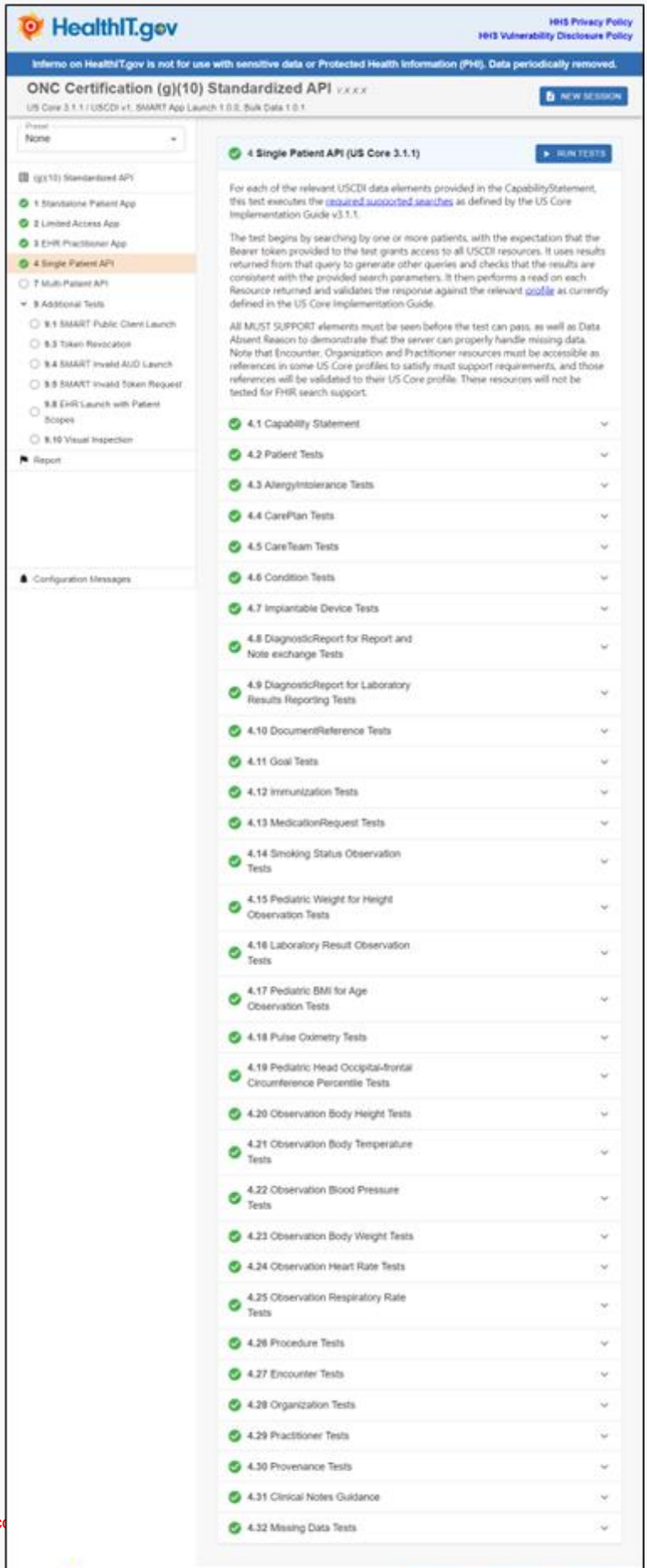


8 Single Patient API

1. Click **4 Single Patient API** on the testing menu on the left of the screen and click **RUN TESTS**
2. All relevant information should be prefilled. (The value in the **Bearer Token** field will differ from our screenshot.)



3. Click **SUBMIT**
4. A progress bar shows in the bottom right corner
5. These tests take about 5 minutes to complete. Once the progress bar finishes and closes, all tests should be green:

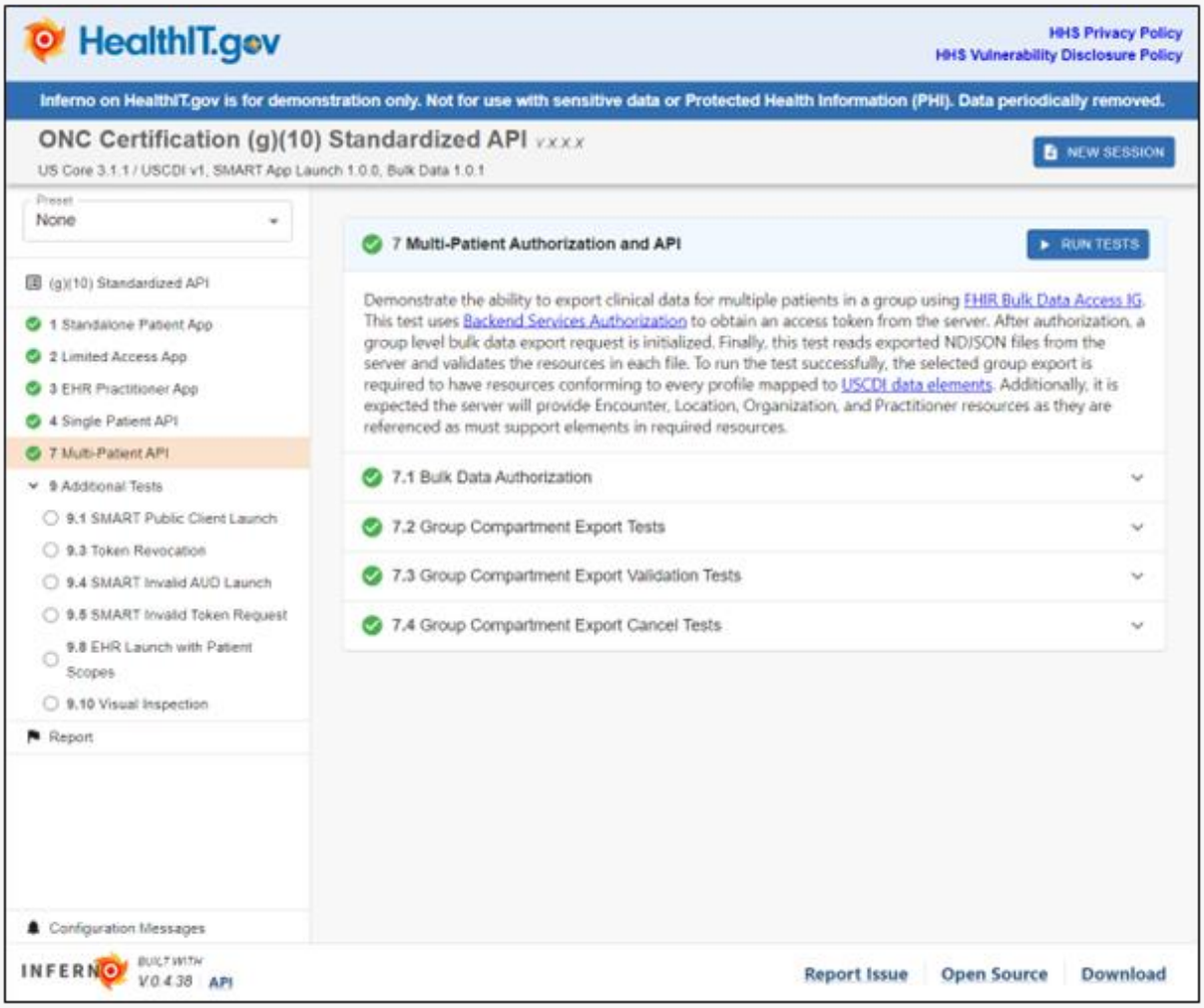


9 Multi Patient API

1. Click **7 Multi-Patient API** on the testing menu on the left of the screen and click **RUN TESTS**
2. Besides the prefilled values, fill in these values:

Field	Value
Bulk Data FHIR URL	https://secure.server.fire.ly
Backend Services Token Endpoint	https://auth.fire.ly/connect/token
Bulk Data Client ID	Inferno-Bulk
Group ID	test
Patient IDs in exported Group	test, test2
Scopes	system/*.read

3. Click **SUBMIT**
4. A progress bar shows in the bottom right corner
5. These tests take about 4 minutes to complete. Once the progress bar finishes and closes, all tests should be green:

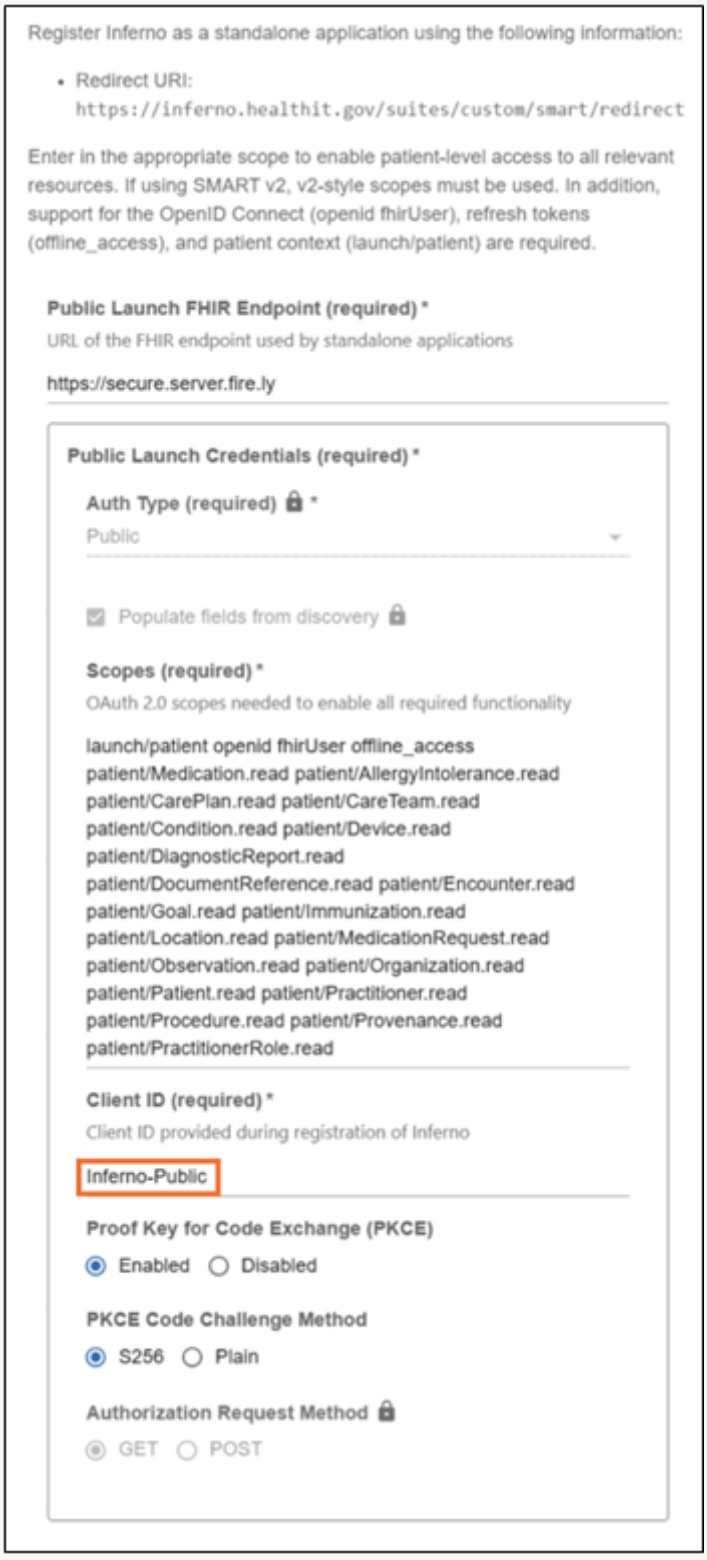


10 Additional Tests

10.1 Public Client Standalone Launch with OpenID Connect

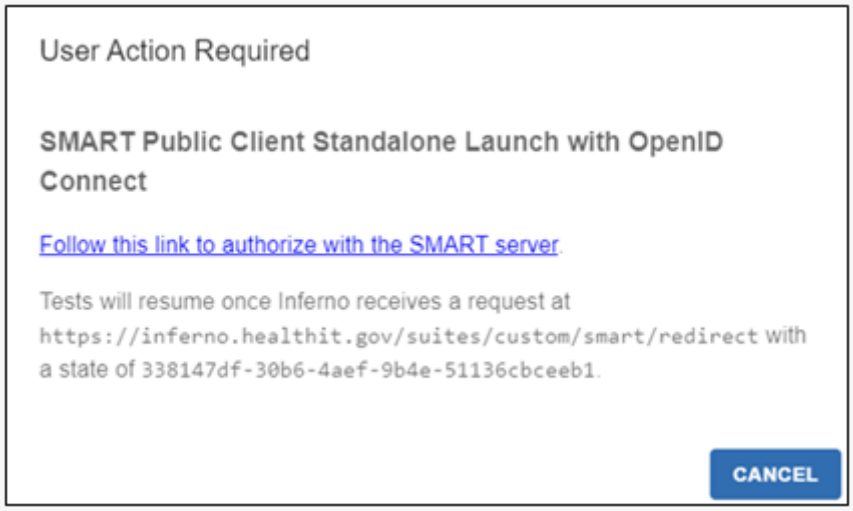
1. Click **9.1 SMART Public Client Launch** on the testing menu on the left of the screen and click **RUN TESTS**
2. Besides the prefilled values, fill in this value:

Field	Value
Public Launch Client ID	Inferno-Public

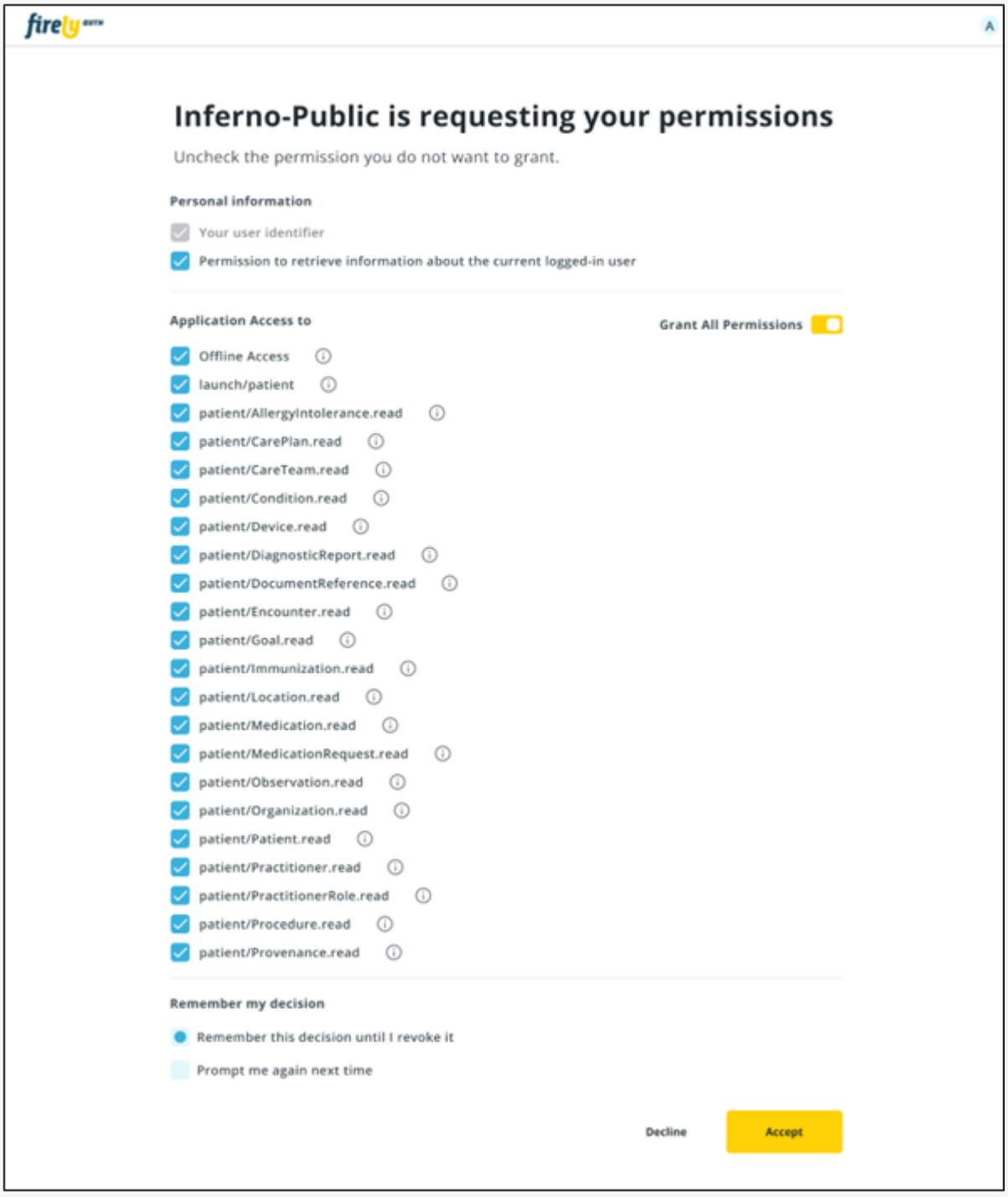


3. Click **SUBMIT**

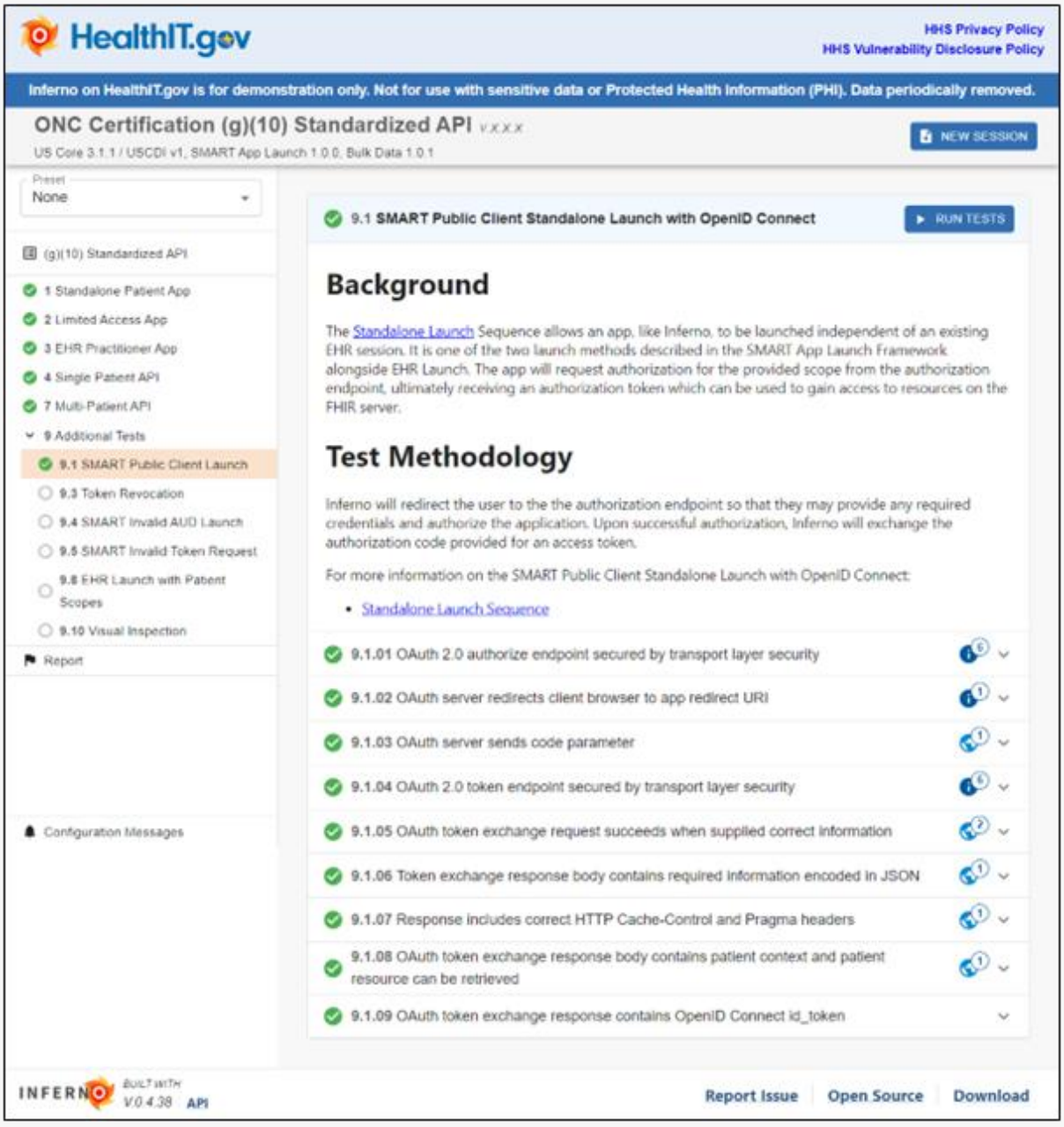
4. A **User Action Required** dialog opens



5. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
6. A dialog **Inferno-Public is requesting your permission** opens
7. Make sure all the boxes are checked:



8. Click **Accept**
9. When you return to Inferno, a progress bar shows in the bottom right corner
10. When this progress bar finishes and closes, all tests should be green:



10.2 Token Revocation

This test requires you to perform two POSTs to revoke both the bearer and refresh token.

The explanation and screenshots here are based on using Postman.

1. Click **9.3 Token Revocation** on the testing menu on the left of the screen and click **RUN TESTS**
2. Select **Yes** for the 'Prior to executing … patient standalone launch' option:

Please fill out required fields in order to run the test group.

The Health IT developer demonstrated a patient's request for revoking the tokens provided during the patient standalone launch within the last hour

(•) Yes ( ) No

Notes, if applicable:

Patient ID (required) *

Patient ID associated with revoked tokens provided as context in the patient standalone launch. This will be used to verify access is no longer granted using the revoked token.

test

FHIR Endpoint (required) *

URL of the FHIR endpoint used by standalone applications

https://secure.server.fire.ly

Revoked Bearer Token (required) *

Prior to the test, please revoke this bearer token from patient standalone launch.

Auth Type (required) *

Prior to the test, please revoke this bearer token from patient standalone launch.

Confidential Symmetric

Access Token (required) *

074EDED22FC89E6D869D78E8E0DE3A1575CAB149E65E93

Refresh Token (will automatically refresh if available) (required) *

0E7AA52270F7734BC04FC0AB21986D359ABBB07C08BF49E

Client ID

Client ID provided during registration of Inferno

Inferno

Client Secret

Client secret provided during registration of Inferno

secret

Token URL (required) *

URL of the authorization server's token endpoint

https://auth.fire.ly/connect/token

Access Token Issue Time

The time that the access token was issued in iso8601 format

2025-06-12T12:22:54+00:00

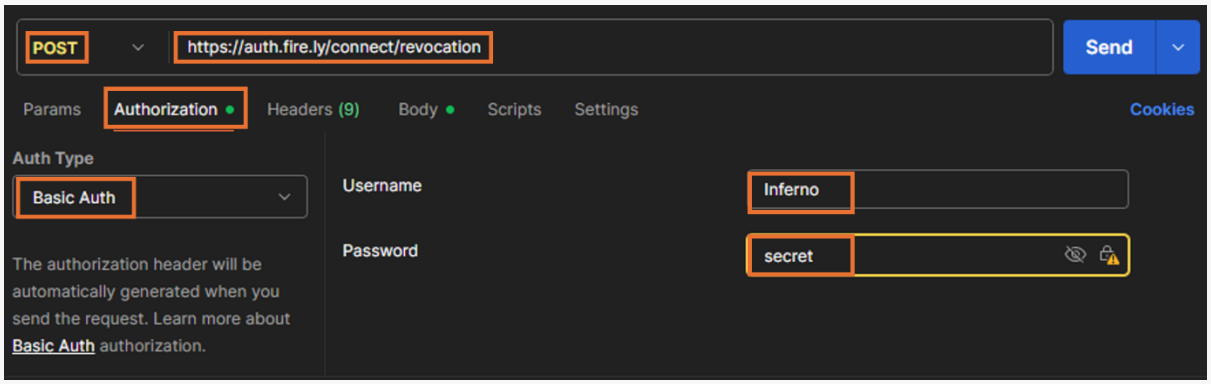
Token Lifetime

The lifetime of the access token in seconds

3600

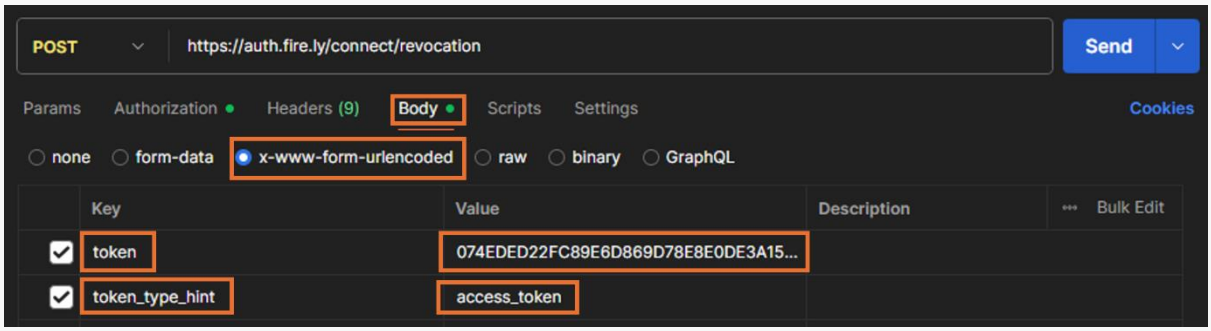
3. Now open Postman and open a new tab for making a request
4. Select the **Authorization** tab
5. Fill in/select the following values:

Field	Value
HTTP verb	POST
Request URL	https://auth.fire.ly/connect/revocation
Type	Basic Auth
Username	Inferno
Password	secret



6. Select the **Body** tab
7. Select **x-www-form-urlencoded**
8. Fill in/select the following values:

KEY	VALUE
token	Copy/paste the value from the **Revoked Bearer Token** field in the Inferno dialog
token_type_hint	access_token

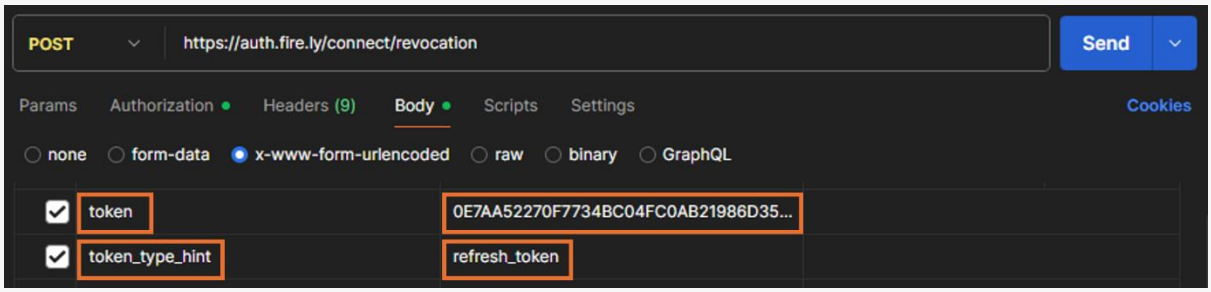


9. Click **Send**

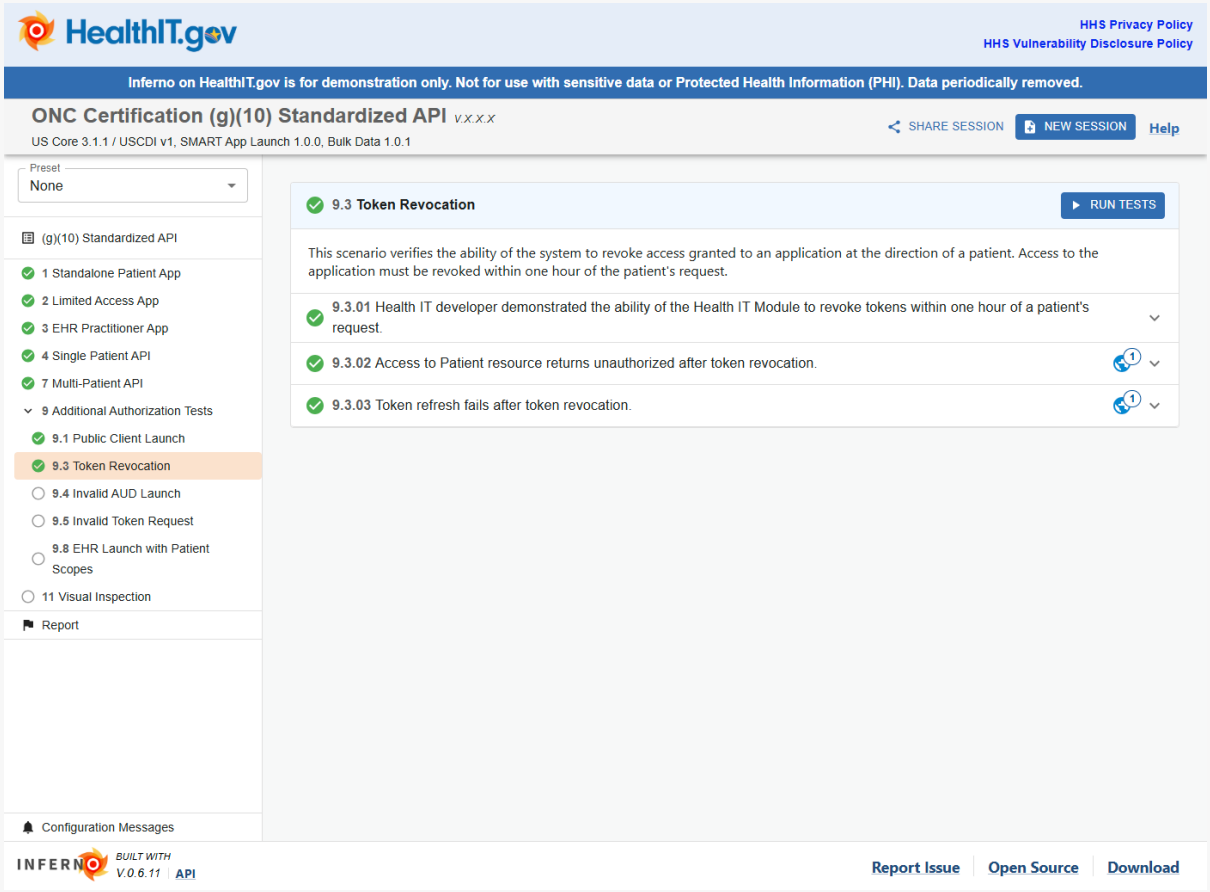
10. The response should be a **200 OK**

11. Change the following values:

KEY	VALUE
token	Copy/paste the value from the **Revoked Refresh Token** field in the Inferno dialog
token_type_hint	refresh_token



12. Click **Send**. The response should again be a **200 OK**
13. Go back to the Inferno dialog and click **SUBMIT**
14. A progress bar shows in the bottom right corner
15. When this progress bar finishes and closes, all tests should be green:

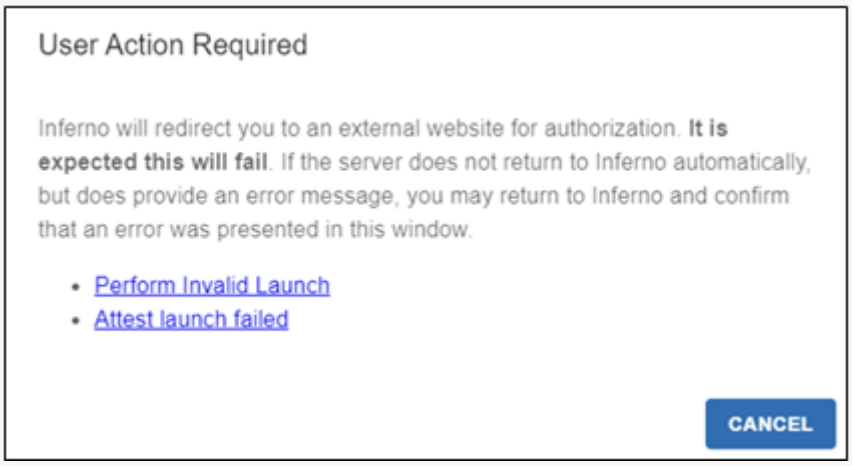


10.3 SMART App Launch Error: Invalid AUD Parameter

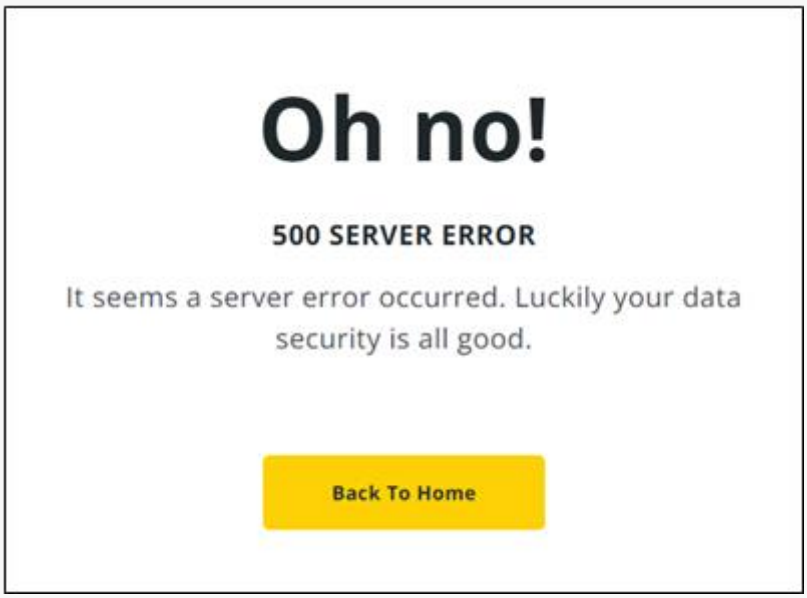
1. Click **9.4 SMART Invalid AUD Launch** on the testing menu on the left of the screen and click **RUN TESTS**
2. A dialog opens with all relevant information prefilled:

3. Click **SUBMIT**

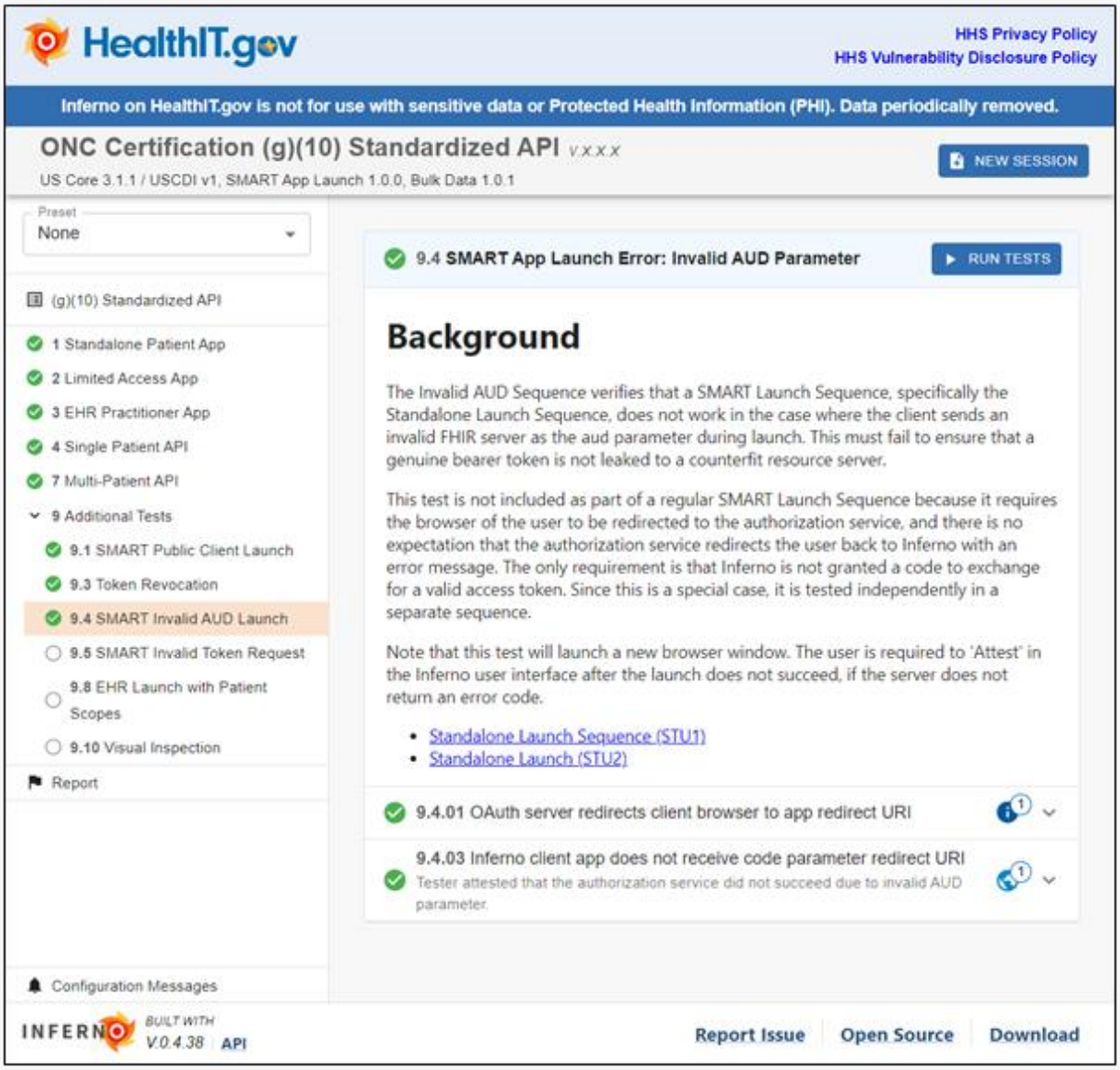
4. A **User Action Required** dialog opens:



5. Right click **Perform Invalid Launch** and select **Open link in new tab**
6. A login attempt to Firely Identity Server will open in a new tab, this should fail:

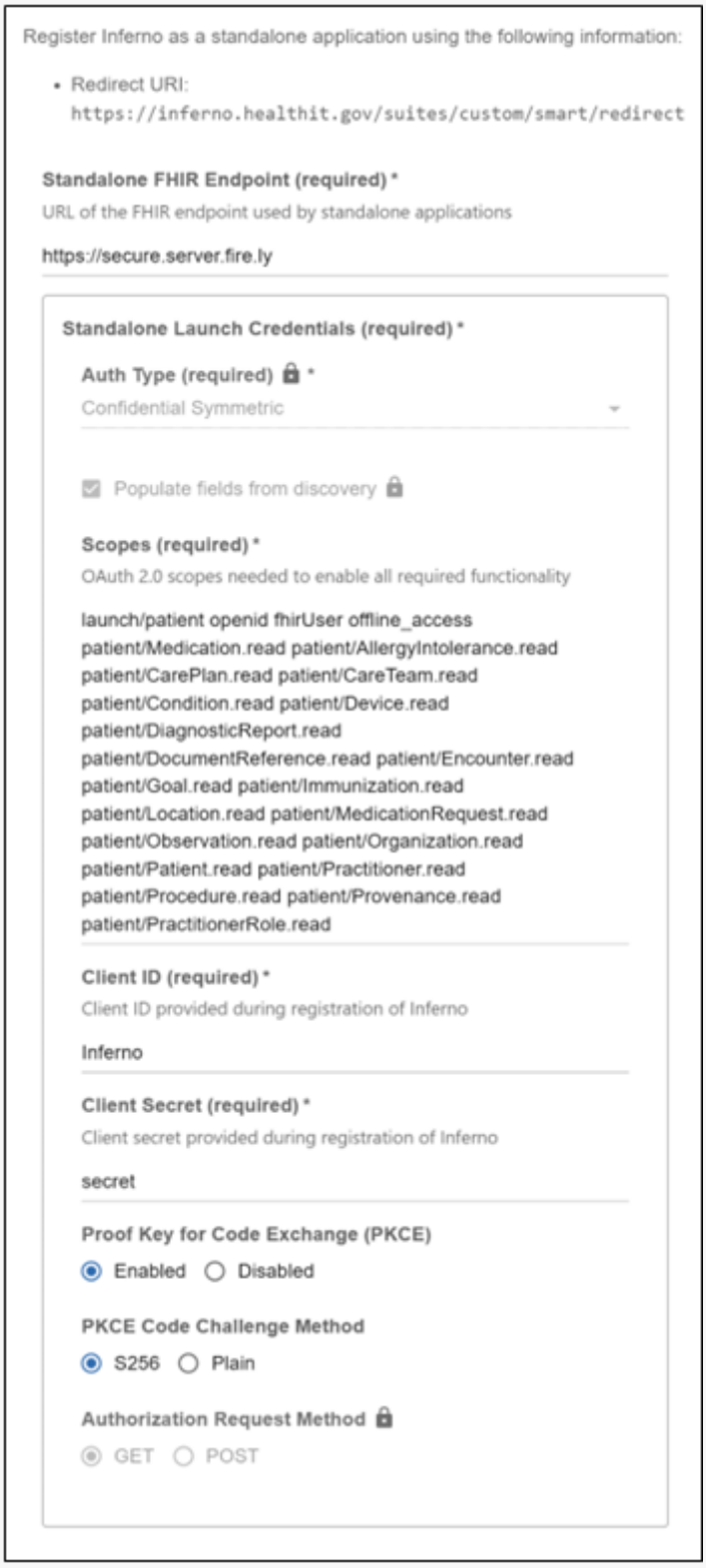


7. Return to the Inferno browser tab from step 4
8. Click **Attest Launch Failed**
9. A progress bar shows in the bottom right corner
10. When this progress bar finishes and closes, all tests should be green:



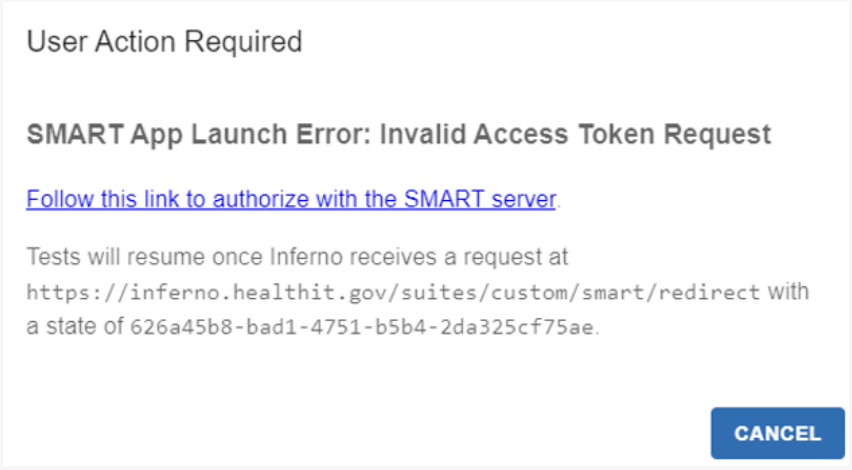
10.4 SMART App Launch Error: Invalid Access Token Request

1. Click **9.5 SMART Invalid Token Request** on the testing menu on the left of the screen and click **RUN TESTS**
2. A dialog opens with all relevant information prefilled:

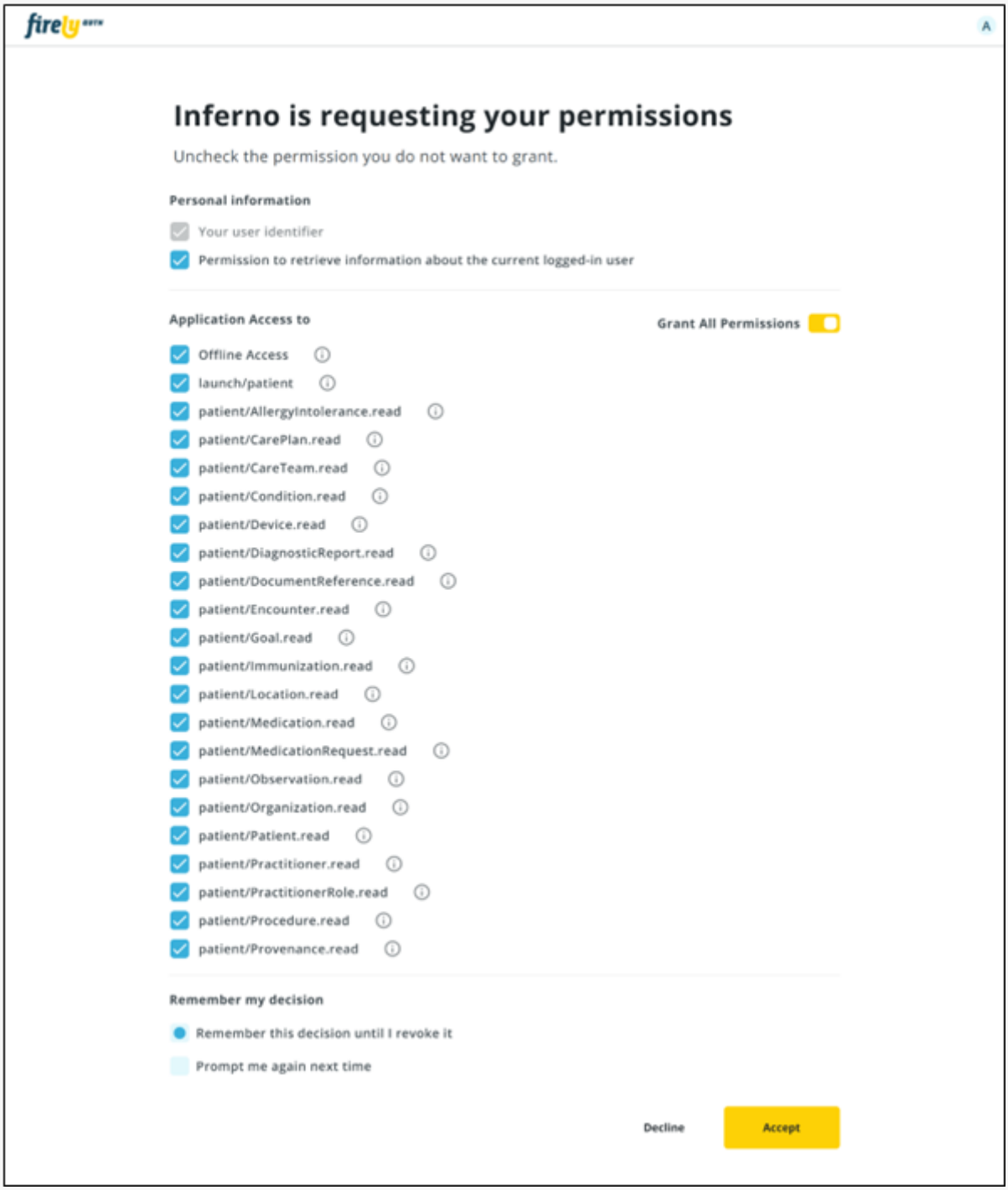


3. Click **SUBMIT**

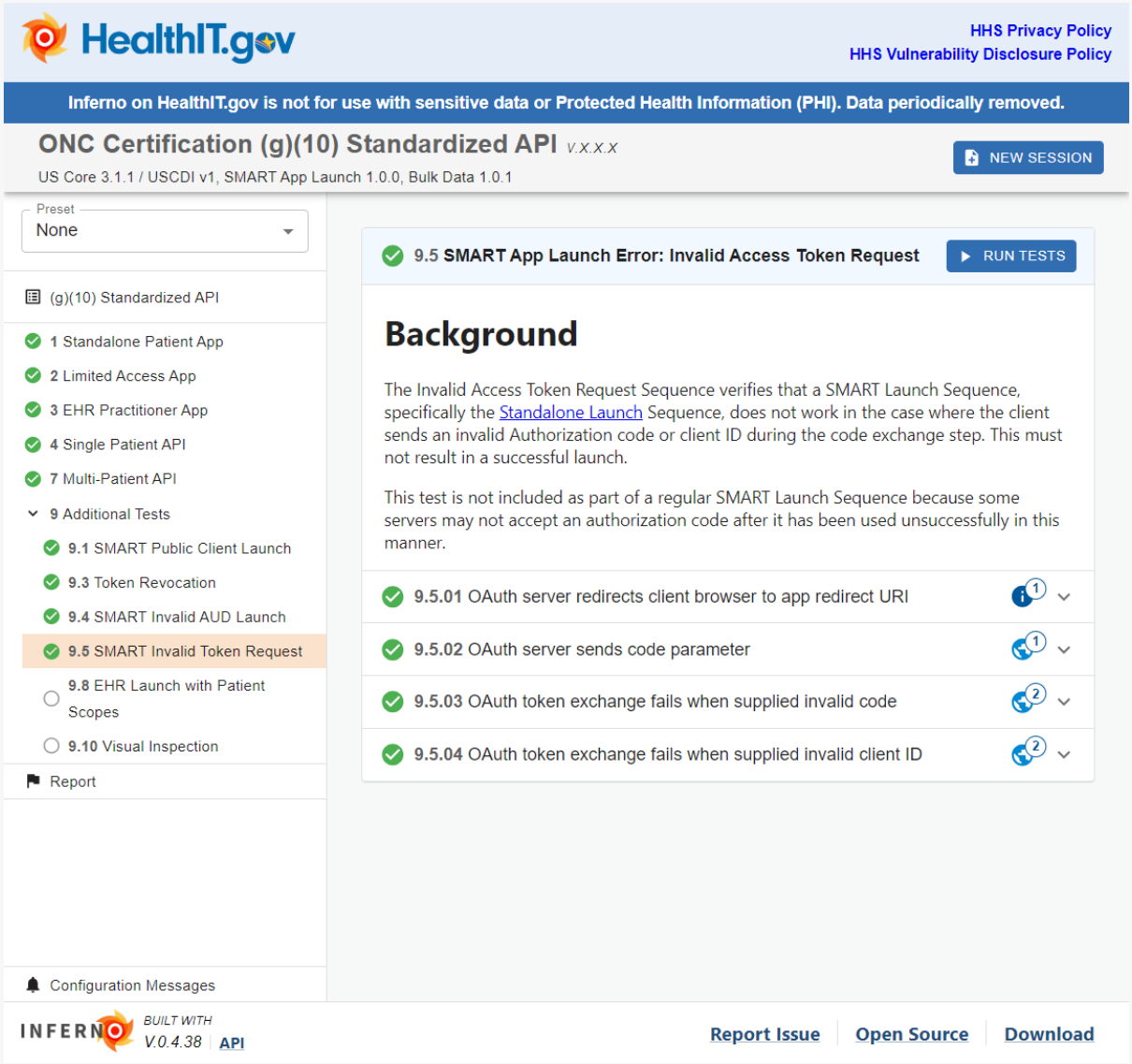
4. A **User Action Required** dialog opens



5. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
6. A dialog **Inferno is requesting your permission** opens
7. Make sure all the boxes are checked:



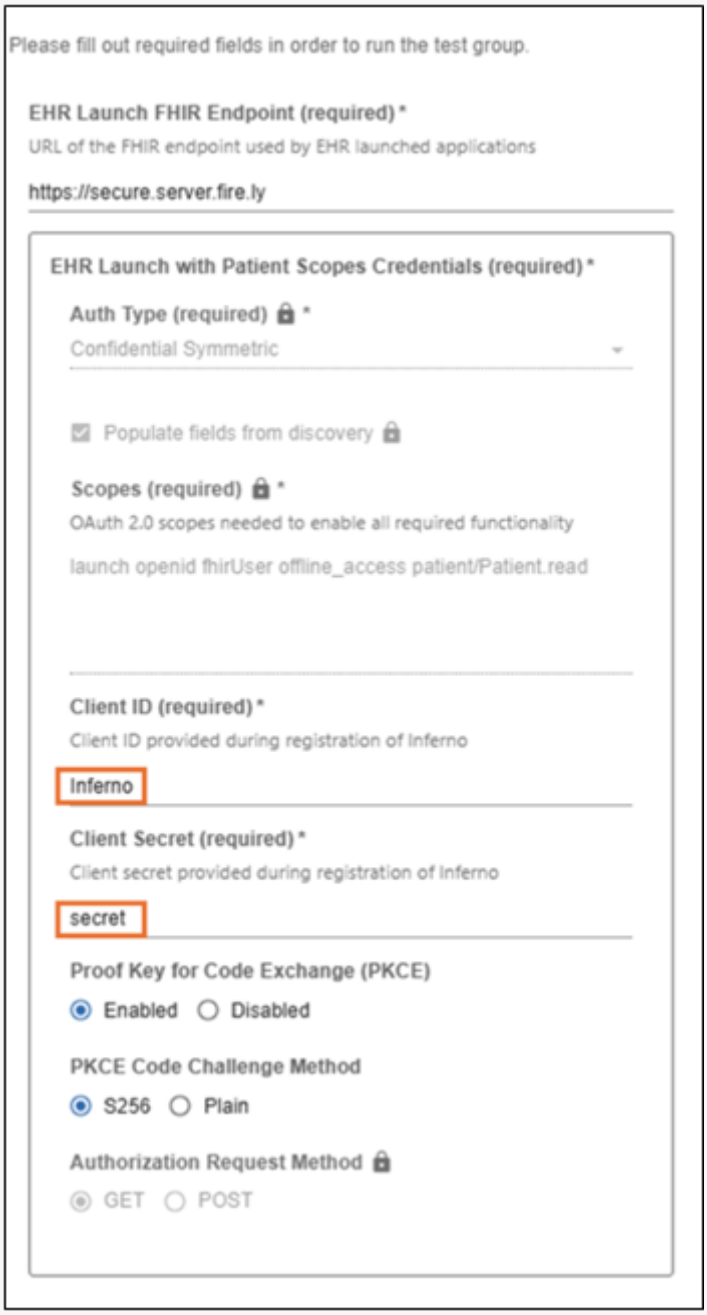
8. Click **Accept**
9. When you return to Inferno, a progress bar shows in the bottom right corner
10. When this progress bar finishes and closes, all tests should be green:



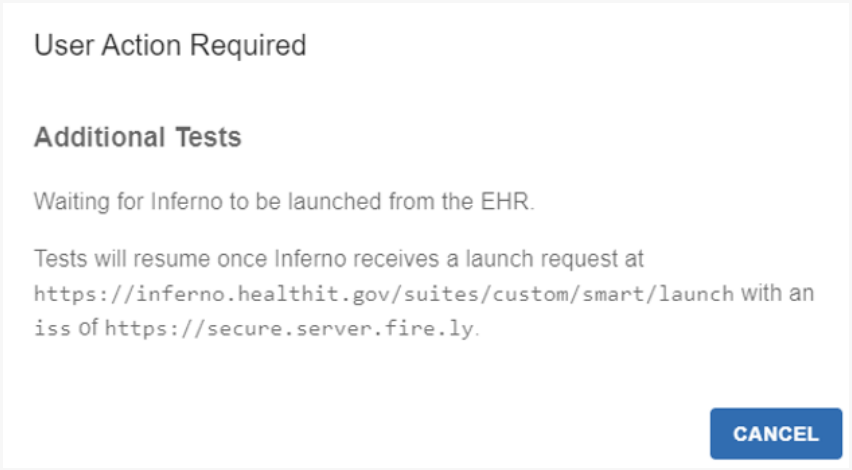
10.5 EHR Launch with Patient Scopes

1. Click **9.8 EHR Launch with Patient Scopes** on the testing menu on the left of the screen and click **RUN TESTS**
2. Besides prefilled values, fill in these values:

Field	Value
EHR Launch Client ID	Inferno
EHR Launch Client Secret	secret

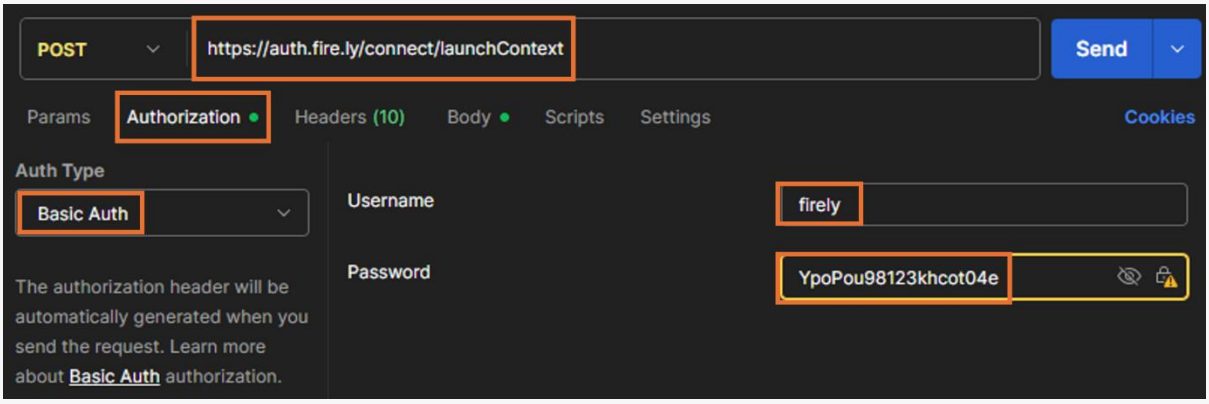


3. Click **SUBMIT**
4. A **User Action Required** dialog opens



5. Now open Postman and open a new tab for making a request
6. Select the **Authorization** tab
7. Fill in/select the following values:

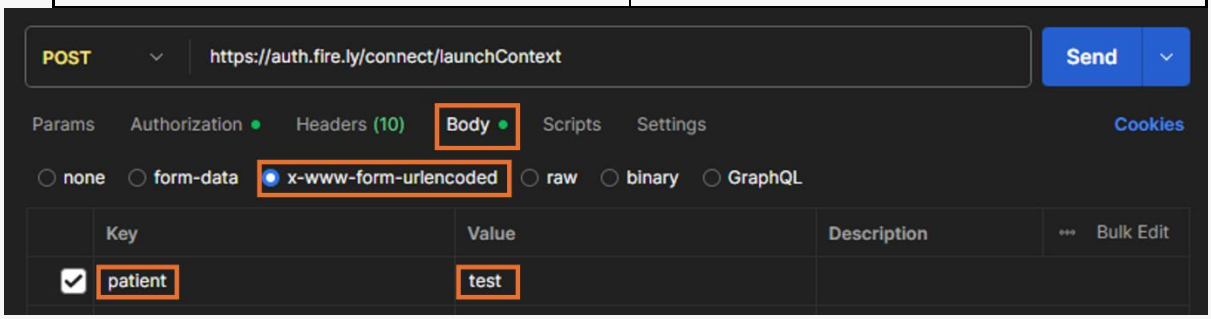
Field	Value
HTTP verb	POST
Request URL	https://auth.fire.ly/connect/launchContext
Type	Basic Auth
Username	firely
Password	YpoPou98123khcot04e



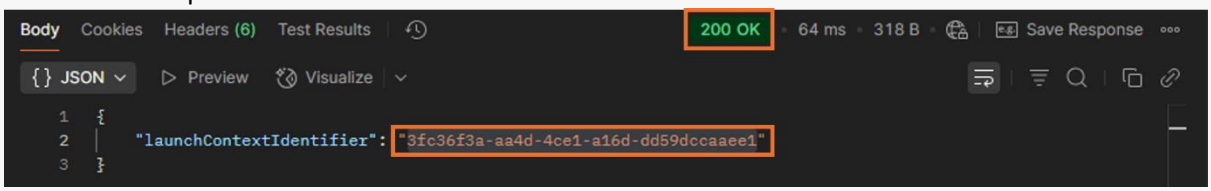
8. Select the **Body** tab
9. Select **x-www-form-urlencoded**
10. Fill in/select the following values:

KEY	VALUE

patient	test



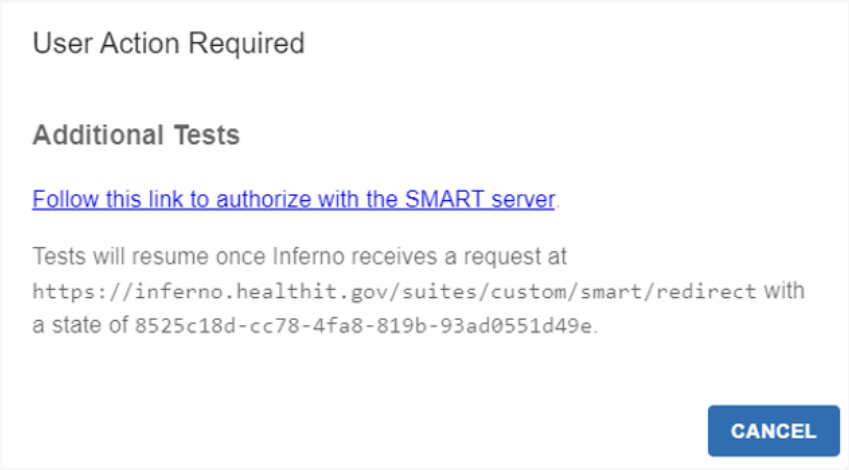
11. Press **Send**
12. The response should be a **200 OK**



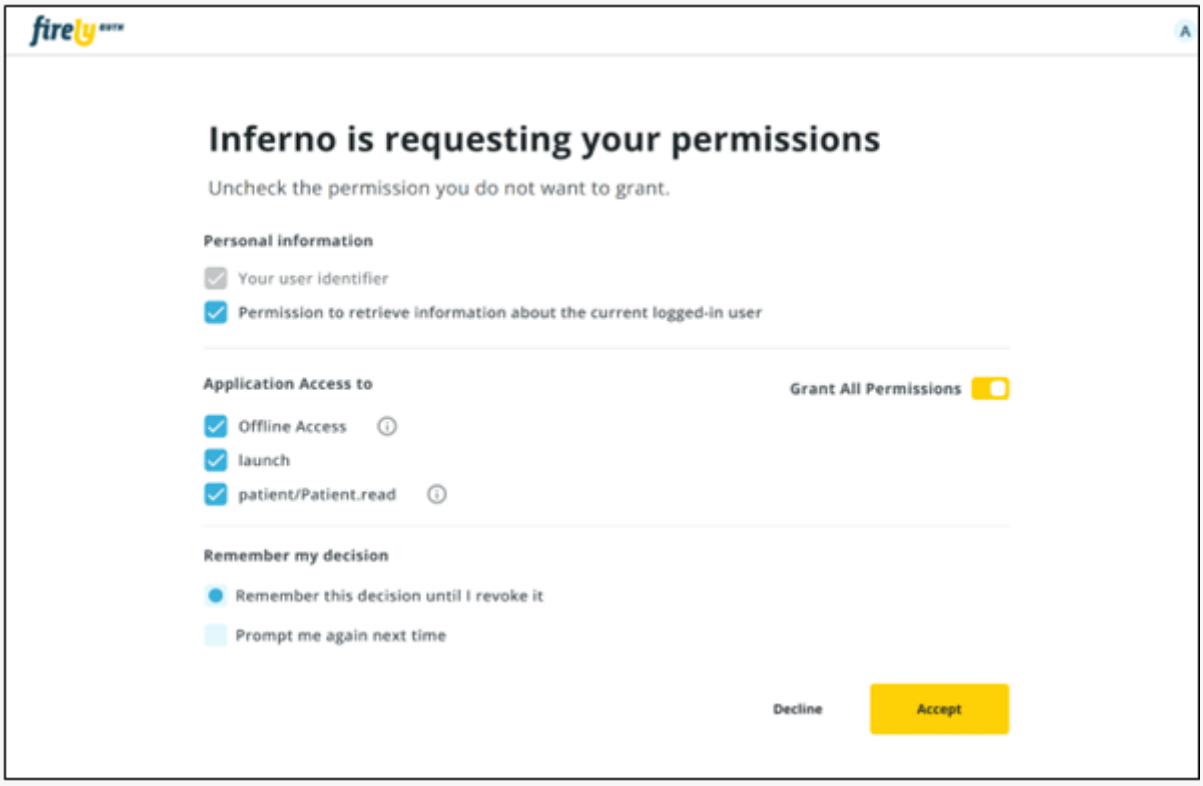
13. Open a new web browser tab and go to the following URL containing using the **launchContextIdentifier** value received (this value is refreshed with each new request):

    https://inferno.healthit.gov/suites/custom/smart/launch?iss=https://secure.server.fire.ly&launch=3fc36f3a-aa4d-4ce1-a16d-dd59dccaaee1

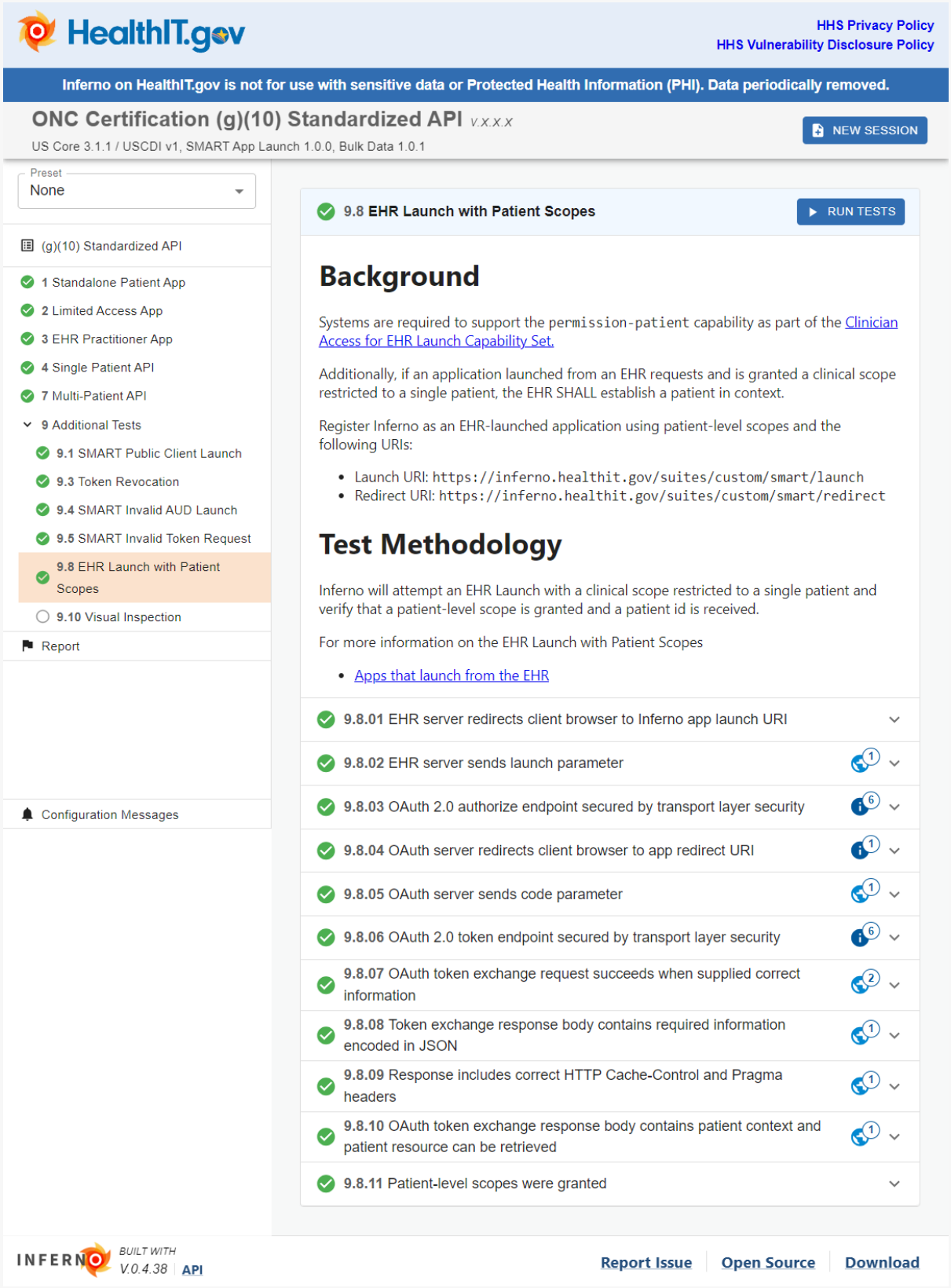
    Another **User Action Required** dialog opens:



14. Click on **Follow this link to authorize with the SMART server**. This will redirect you to Firely Identity Server
15. A dialog **Inferno is requesting your permission** opens
16. Make sure all the boxes are checked:



17. Click **Accept**
18. When you return to Inferno, a progress bar shows in the bottom right corner
19. When this progress bar finishes and closes, all tests should be green:



10.6 Visual Inspection and Attestation

This does not contain automated tests and a number of these tests are not applicable to Firely Server. You can still 'run' these tests yourself based on the results you have so far.

11 Wrapping things up

Congratulations, you ran all the tests! Thanks for taking the time to check that Firely Server is compliant with ONC regulations relevant to FHIR servers. So, what's next?

You could download a trial version of Firely Server and continue testing it with your own set of tools, such as Postman. We have two blog posts to help you get started with that:

- Installing your first FHIR server with Firely Server
- Your first interactions with your FHIR server

Or maybe you've hit a blocker with your own FHIR server, and you're wondering how we created the infrastructure to pass all the Inferno tests? It took Firely Server, an authorization server, some extra configuration, and a lot of hours to make it all work seamlessly together, and we'd love to share that story with you. Let us know by sending an email to server@fire.ly.

12 About Firely

Firely provides all the software, training, and expertise needed to bring FHIR to life.

We're the authors of one of the two main open source FHIR libraries: Firely .NET SDK. Our software powers FHIR APIs and systems around the world, and many governments, hospitals, payers, and MedTech companies rely on our software for their FHIR capabilities.

Firely also provides FHIR training courses and workshops, and is the organizer of FHIR DevDays, the world's leading FHIR event. In 2019, we became a founding member of the FHIR Business Alliance.

You can find out more about Firely solutions, services, and education on our website (https://fire.ly).

13 Contact us

Your feedback is very welcome. Please send us your comments, compliments, and questions – and if you're interested in the commercial side of things, we'd be more than happy to schedule a meeting.

Just send us an email at info@fire.ly and we'll get back to you asap.

Made with TLC in Amsterdam

Firely Amsterdam
Westerdok 442
1013 BH Amsterdam
The Netherlands
+31 20 2461 241
info@fire.ly