Office of the Director of National Intelligence

ICDC Platform User SOP

Office: Open-Source Intelligence Executive (OSIE)

Date: 05/19/2026

About this document. This SOP describes the standard end-to-end workflows for using the platform, including discovering data sources, requesting access, consuming data through three different access mediums (data sources, virtual platform sessions, and APIs), and managing organization membership. It covers two personas: the Analyst (user) and the Organization Administrator.

About the screenshots. Screenshots in this document were captured from a pilot environment and may show example data source names, vendor names, organization names, and URLs. These are illustrative only your environment will display your own catalog entries and your own organization. The procedures themselves are vendor- and agency-agnostic and apply regardless of the specific resource being requested

1. Purpose and Scope

This Standard Operating Procedure (SOP) provides step-by-step guidance for using the ORRIX platform to discover, request, and consume data sources, partner platform workspaces, and APIs through the catalog. It is written for analysts who need a practical, repeatable reference for completing common platform tasks. This will focus on the analysts (users) who need access to data sources, partner platforms, or APIs to perform their work.

Procedures are presented in the order a typical user encounters them: initial login and orientation, selecting the correct access workflow, requesting and consuming resources, using the home-screen chat, and completing Organization Administrator tasks.

1.1 Quick Start: Where to Go

If you need to…	Go to
Understand which access workflow applies	Section 3.5: Workflow Decision Guide
Log in for the first time	Section 4: User Account Creation and Initial Login
Find resources in the catalog	Section 5: Home Screen Orientation
Request access to a dataset or feed	Section 6: Data Source Access
Launch an external partner platform workspace	Section 7: Workspace Session Access
Generate an API access key or bearer token	Section 8: API Access and Key Generation
Download bulk data files	Section 9: Bulk Data Download
Ask questions using the ICDC Chat Interface	Section 10: Platform Chat Queries
Invite users or approve requests	Section 11: Organization Administrator Workflows
Troubleshoot common problems	Section 12: Troubleshooting and Common Edge Cases

1.2 Terminology Note

Platform screens may use product-specific labels such as **Request Purchase**, **Destroy Workspace**, or **Manage Keys**. To improve clarity, this SOP uses plain-language workflow terms to describe each action and references the exact on-screen label when a user must select a specific control.

2. Roles and Responsibilities

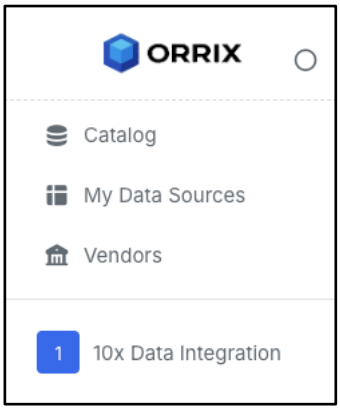
Role	Responsibility
Platform Administrator	Onboards new organizations and designates the initial Org Admin for each. External to user workflow; referenced for context only.
Organization Administrator (Org Admin)	Invites users to their organization, assigns roles (Admin or Member), and approves or rejects access requests submitted by users within the organization.
Analyst (User)	Browses the catalog, submits access requests with justification, and consumes resources through the appropriate access medium (data source, platform session, or API).

3. Access Model Overview

The platform supports three distinct access mediums. Users should identify which medium applies before requesting access because each workflow grants a different type of entitlement and has a different consumption method.

The standard pattern is: Discover Data -> Request Access -> Org Admin Approval -> Users Access Data. Some resources may already be entitled to the user or organization; in those cases, the user can move directly from discovery to consumption.

3.1 Data Source Access



Analysts can browse all available platform data sources by selecting the Catalog link in the left navigation bar. Some datasets in the Catalog may not yet be purchased and will require completion of the Data Purchase Request process before a Data Access Request can be submitted.

Analysts can also access the My Data Sources section from the left navigation bar. Datasets listed in My Data Sources have already been purchased and only require an approved Data Access Request from the analyst's Org Admin before access is granted.

3.2 Platform (Workspace) Access

Access to an external partner platform through a virtual, checked-out workspace session. The session opens in a new browser tab with credentials pre-configured. Sessions are time-bounded and must be returned when finished so the seat is freed for others, similar to checking out a library book.

3.3 API Access

Programmatic access via an API endpoint and/or MCP server URL, authenticated with a user-generated bearer token. The MCP server URL is used by MCP-compatible tools or agents to connect to approved APIs through a standardized tool interface. After approval, the user creates a named, expiration-dated access key, which is displayed once and must be copied immediately.

3.4 Bulk Data Access

Bulk Data Access is used when an approved data source provides downloadable files, such as Parquet files, instead of or in addition to interactive chat, API, or workspace access. After the bulk data source is available, the analyst creates bulk-data credentials, securely saves the Access Key ID, Secret Access Key, and Endpoint URL, browses the Files tab, requests the specific file for download, and downloads the file after the request is approved.

3.5 Workflow Decision Guide

Resource or task	Use this workflow	What the user receives
Dataset, feed, or searchable data source	Workflow A Data Source Access	Access to query or consume the approved data source from My Data Sources and Platform Chat.
External vendor platform, application, or virtual workspace	Workflow B Requesting Vendor Portal Workspace Session Access	A checked-out browser-based workspace session with credentials pre-configured.
API endpoint, MCP server URL, or bearer-token workflow	Workflow C API Access and Key Generation	A user-generated access key and endpoint details for programmatic access.
Bulk data files or data lake downloads	Workflow D Bulk Data Download	Bulk-data credentials and approved file-level download access for selected files, such as Parquet outputs.
User invite, role assignment, or approval queue	Organization Administrator Workflow	Admin ability to create users, assign roles, and approve or reject access requests.

Note. The consent screen appears on first login and may reappear periodically per platform policy. The platform agreement is linked from the consent page; users should review it before accepting.

4. User Account Creation and Initial Login

This section explains how users request an account, receive credentials, and complete the initial login process for the ICDC/ORRIX portal. Account creation is coordinated through the agency-designated Point of Contact (POC) and 10X support before the user logs into the platform.

4.1 Request an Account

Step 1. To request an account for the ICDC/ORRIX portal, contact your agency designated POC and provide the following information. *If there is no designated POC, email your details directly to the email address mentioned in* **Step 2**.

1. Name or First Name and Last Name Initial (John D.) or Penname Aliases

2. Unclassified (Low-side) email address

3. Agency you are affiliated with

4. Role (member/analyst, admin, or procurement officer)

Step 2. The agency POC emails the requested account list from Step 1 to ICDCHelp@10xnatsec.com for user account creation.

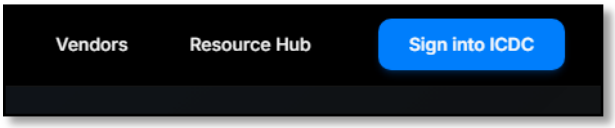
Step 3. 10X manually creates usernames and passwords and emails them to the individual users at their provided low side email addresses.

4.2 Log Into the Portal

Step 4. Once you receive your username and password, go to the ICDC portal: https://10xicdc.com/.

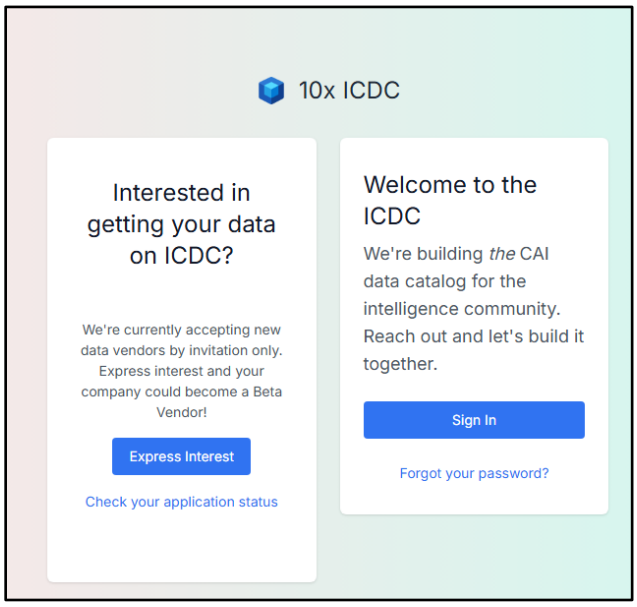
Step 5. Click "Sign into ICDC" from the menu at the top of the ICDC portal. See Pic1.

Pic1



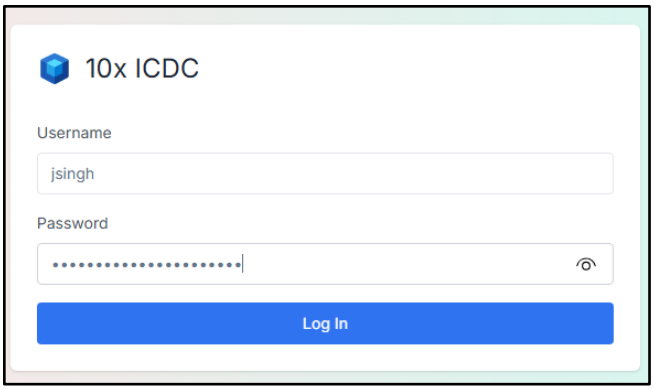
Step 6. Click the "Sign In" link option for the Intelligence Community. See Pic2.

Pic2



Step 7. Enter the username and password received from the 10X team and click "Log In" to access the ICDC/ORRIX portal. See Pic3.

Pic3

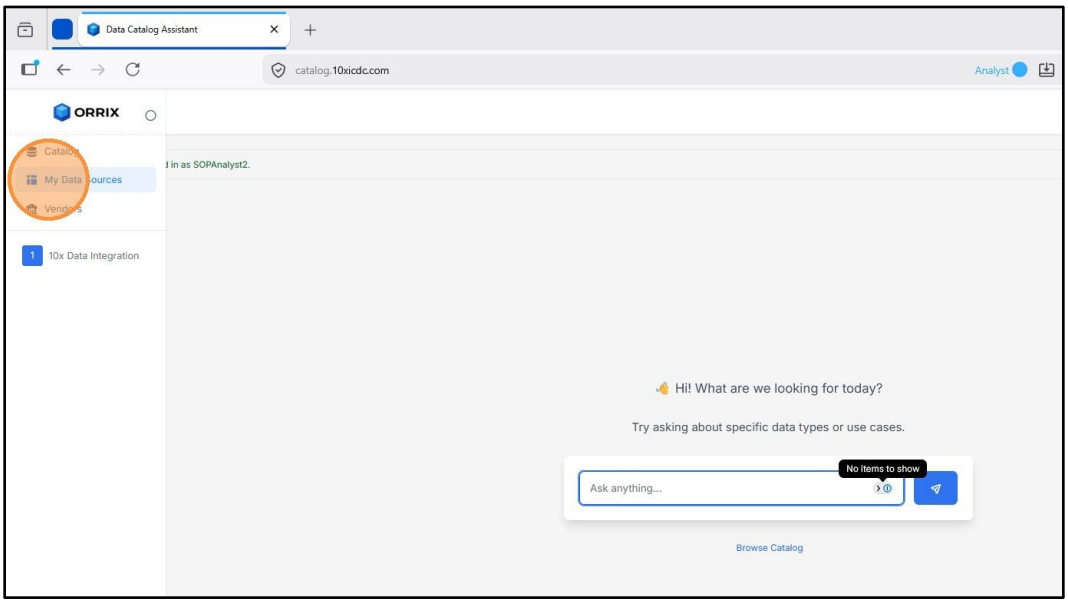


Step 8. Once logged in, continue with Section 5 Home Screen Orientation and the applicable workflows in this SOP.

Note. The consent / terms-of-use screen may appear on first login and may reappear periodically per platform policy. Users should review the platform agreement before accepting.

5. Home Screen Orientation

After login, the user lands on the platform home screen. The screen contains the following primary elements:



Platform Chat (center)

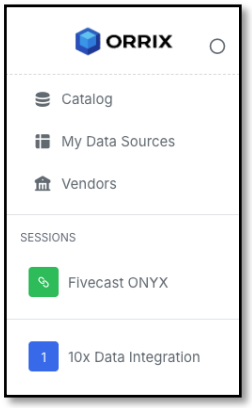
The AI Chat interface provides a natural-language experience for querying data sources and APIs the user has already been granted access to. Users can ask questions in plain language, such as, “What user data feeds do I currently have access to?” or “Which datasets contain information related to China?”

Once access has been approved for one or more data sources the AI Chat interface becomes the primary method for discovering, querying, and interacting with available data. As the ORRIX Platform continues to evolve, the capabilities of the AI Chat interface will expand and mature to support more advanced search, analysis, and data interaction workflows.

Browse Catalog (link / tile)

Entry point to the full catalog of available data sources, platforms, and APIs offered by vendors within ORRIX.

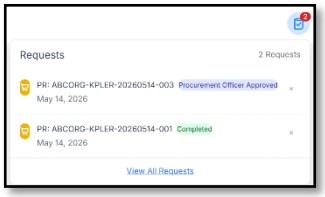
Left-hand navigation



The sidebar provides quick access to:

- Catalog the full catalog of resources available on the platform.
- My Data Sources resources the user's organization currently has access to.
- Vendors list of all vendors represented in the platform.
- Org Profile visible to Org Admins; used for organization management.
- Sessions any currently checked-out workspace sessions appear here as persistent links, allowing the user to return to an in-progress session at any time.

Top-right notifications indicator



A clipboard / notifications icon that surfaces the status of submitted requests (draft, in-flight, approved, rejected) for users, and incoming approval requests for Org Admins.

6. Workflow A Requesting Data Source Access

Use this workflow when the user needs direct access to a published dataset, feed, or searchable data source.

Datasets accessed through the Catalog may require completion of the Data Purchase Request process if the data has not yet been purchased by the organization. Once a dataset has been purchased and is available in My Data Sources, analysts only need to submit a Data Access Request, which must be approved by their Org Admin before access is granted.

6.1 Discover a Data Source

Step 1. From the home screen, click "Browse Catalog" or "Catalog" in the left-hand navigation.

Step 2. Review the list of available data sources.

Step 3. Click into the data source of interest to open its detail page.

6.2 Review Eligibility

On the data source detail page, the user should determine the current access status before submitting a request:

Status	Meaning	User action
Already entitled / pre-approved	The user or organization already has access.	Open the resource from My Data Sources and access the available data.
Published but not entitled	The resource exists in the catalog, but access has not been granted.	Submit a Data Access Request using the on-screen request option.
Unavailable or not published	The resource is not currently available for this user or organization.	The user must submit a Request Purchase request and wait for the dataset to complete the

		purchasing and procurement process before access can be requested.

6.3 Submit a Data Access Request

Step 1. Click "Request Access" on the data source detail page. This is the current screen label for submitting a Data Access Request.

Step 2. The Org Admin will need to approve your request before you can access the data. If your organization has not yet purchased the requested data, the purchase will need be made before Access to the data can be granted

6.4 Track the Request

Step 1. Confirm that the draft data access request has been generated.

Step 2. Click the clipboard / notifications icon in the top right to view request status.

Step 3. Each request displays the request number, submitter, description, and associated metadata.

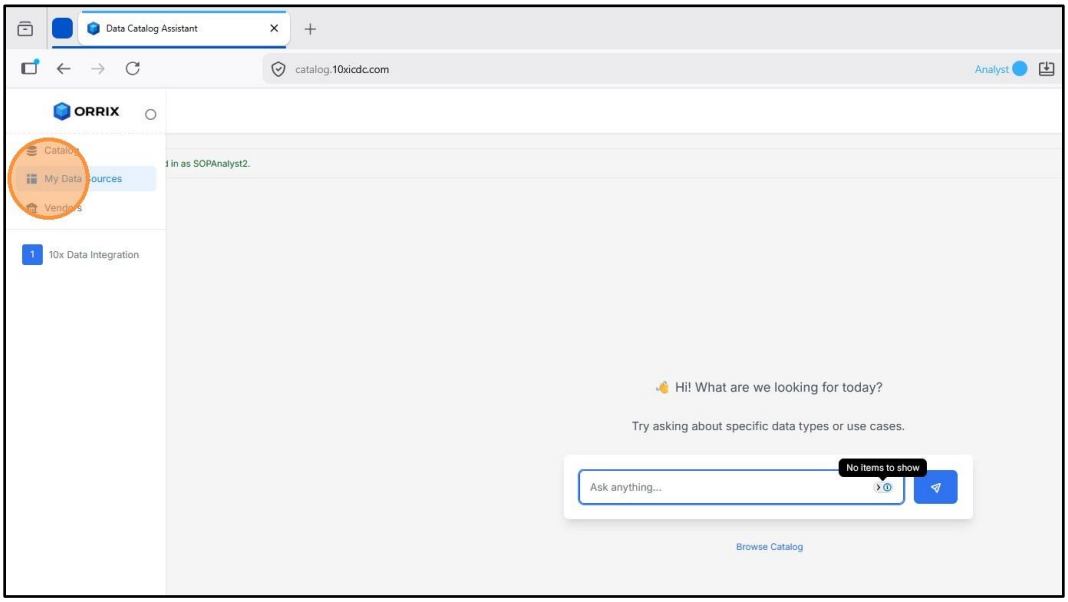
The request remains "in motion" until the Org Admin reviews and acts on it (see Section 11.3). When approved, the data source becomes available under "My Data Sources" and can be queried through the home-screen Platform Chat where supported (see Section 10).

7. Workflow B Requesting Vendor Portal Workspace Session Access

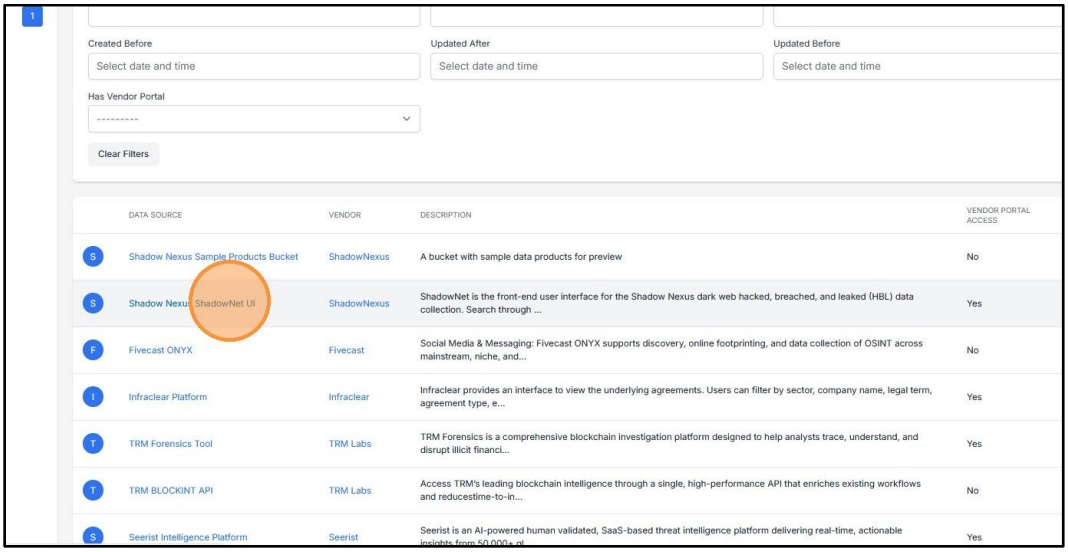
Some catalog entries are external partner platforms accessed through a virtual workspace session rather than direct data delivery. The user requests access once, then checks out a session each time they need to use the platform, and returns the session when finished.

7.1 Locate the Platform and Submit Access Request

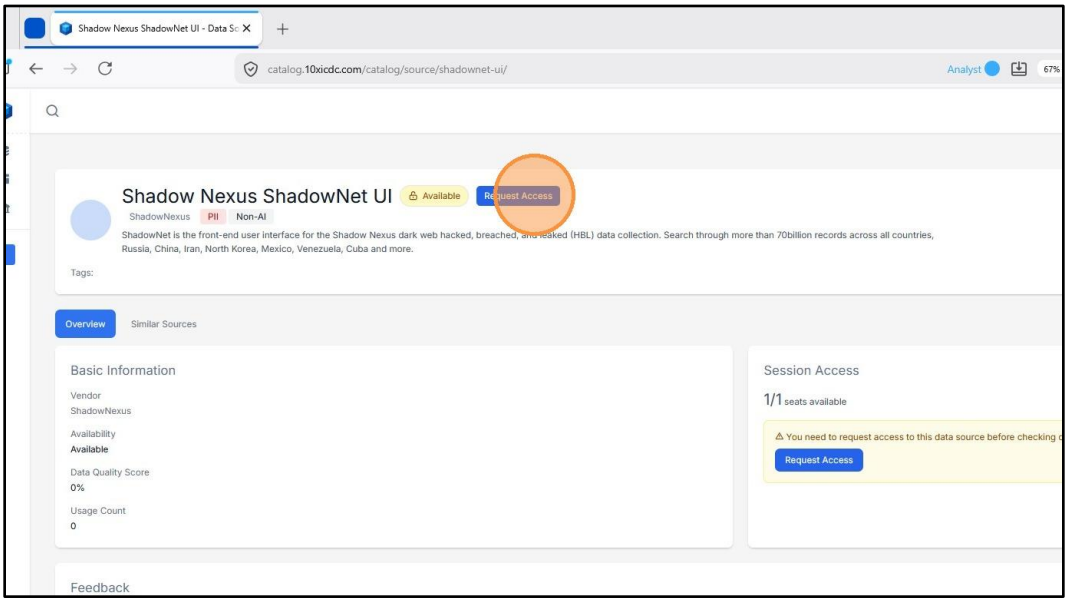
Step 1. From the left-hand navigation, select "My Data Sources" (or "Catalog" to browse all available resources).



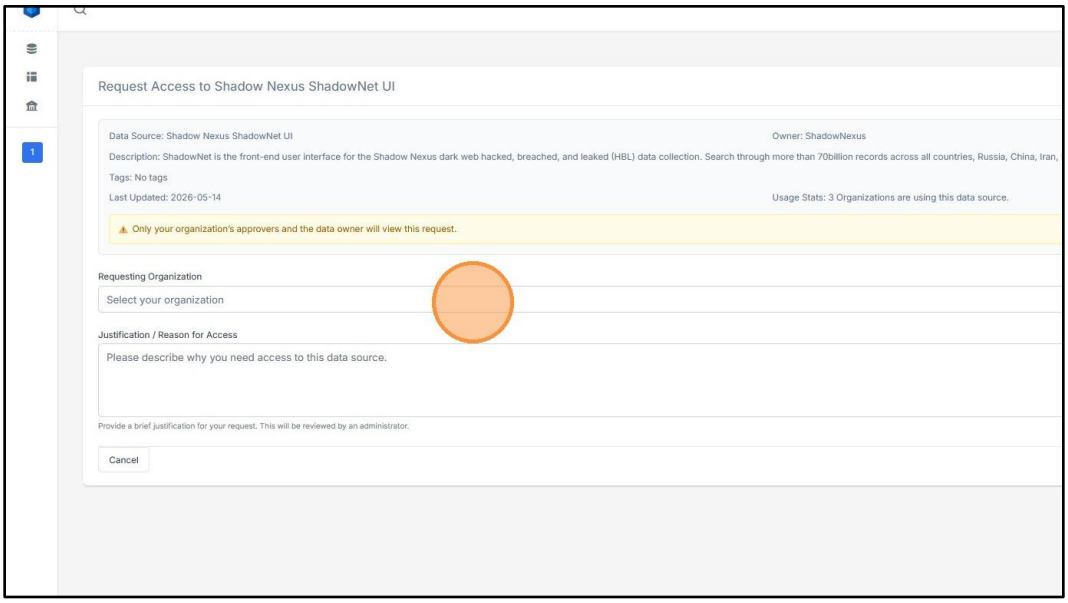
Step 2. From the list of data sources, click the platform you want to access.

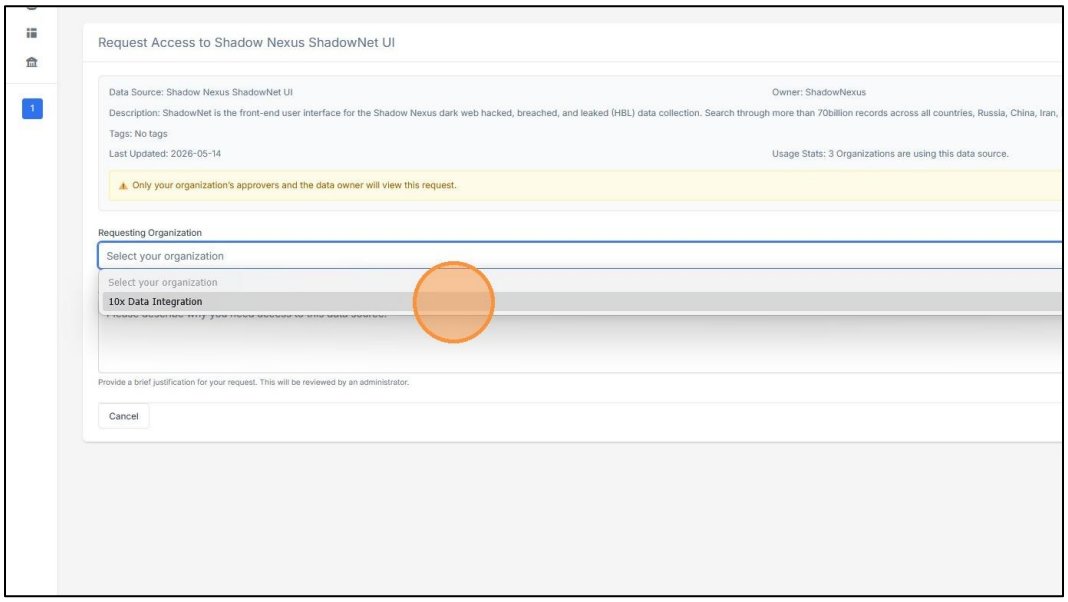


Step 3. On the platform detail page, confirm availability (indicated by an unlocked icon) or click "Request Access" if you do not already have access.

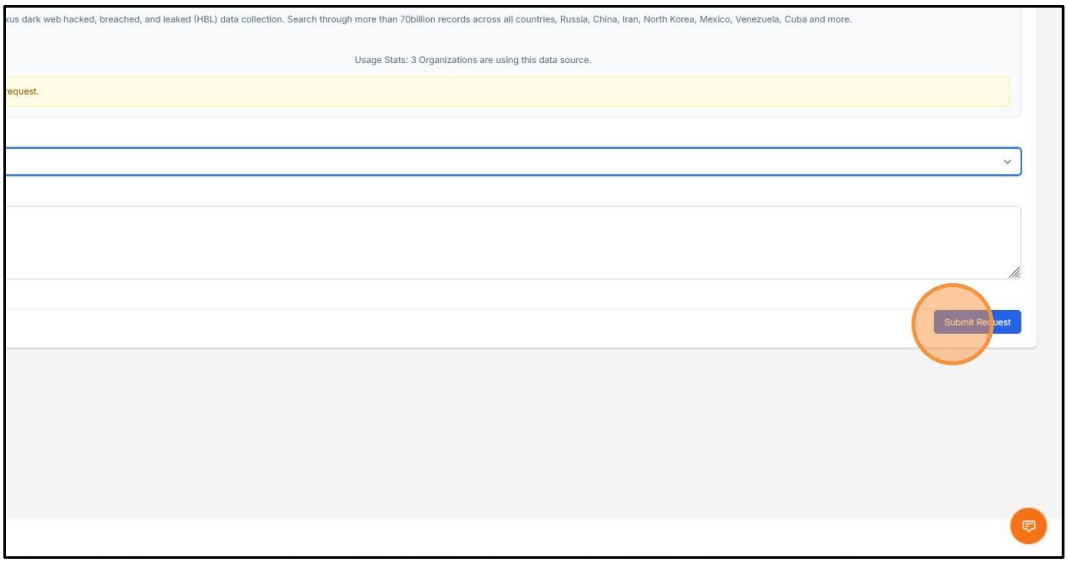


Step 4. On the Request Access form, click the "Requesting Organization" field to open the dropdown, then select your organization.





Step 5. Enter a justification in the "Justification / Reason for Access" field, then click "Submit Request".

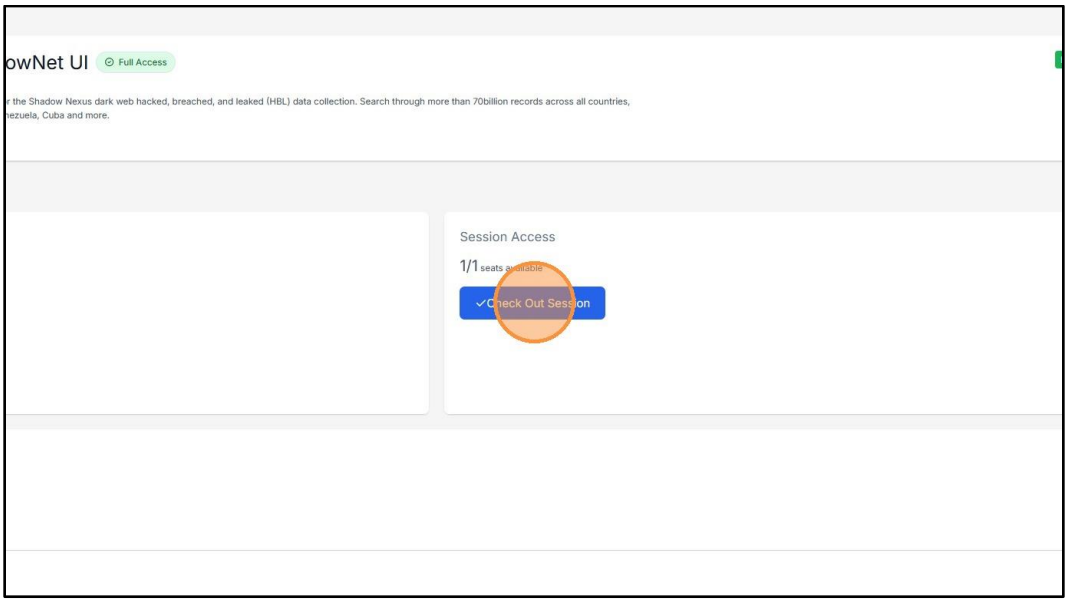


Pilot vs. production note. In a pilot environment, access requests may be approved automatically and access may be granted immediately. In production, an Org Admin must approve the request before the user can proceed to the next step. The user will see the request pending until that approval occurs.

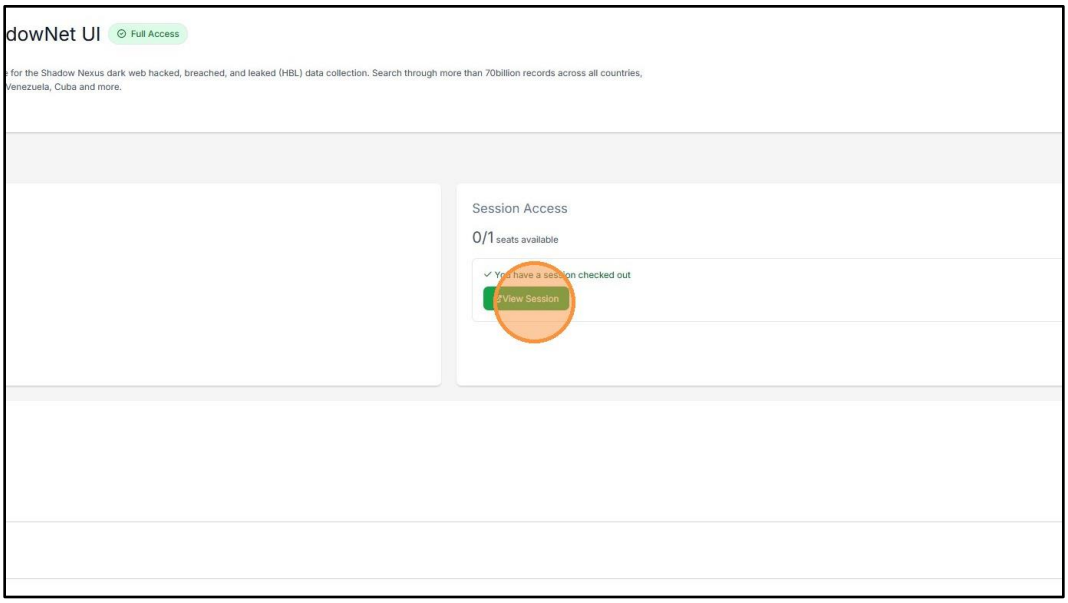
7.2 Check Out a Workspace Session

Once access has been granted (or auto-granted in a pilot):

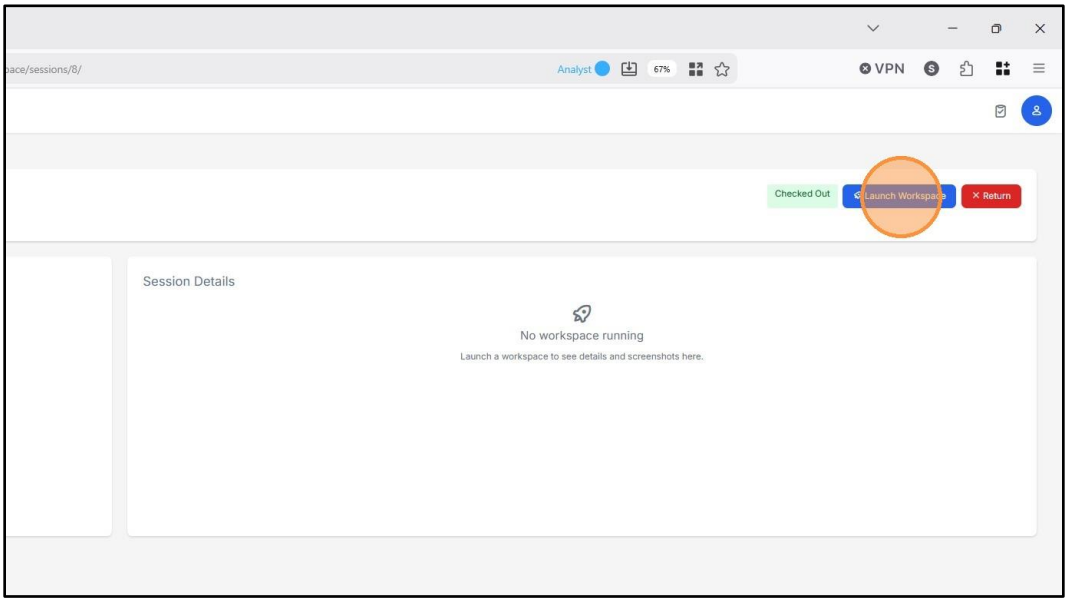
Step 1. On the platform detail page, locate the "Session Access" panel. Click "Check Out Session" to reserve a seat.



Step 2. Once the session is checked out, the panel updates to show "You have a session checked out." Click "View Session" to open the session details.

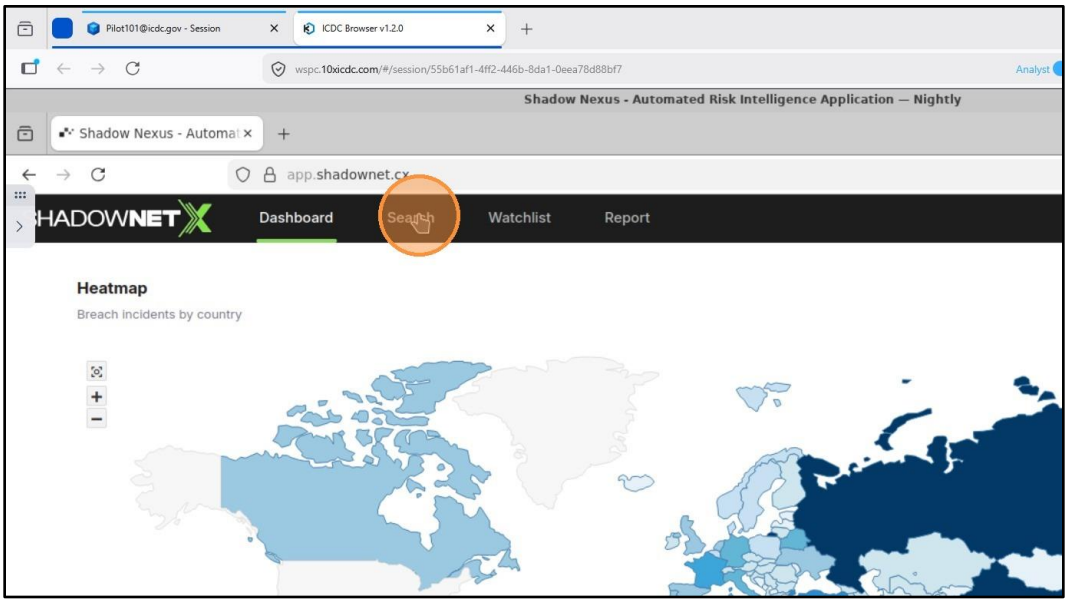


Step 3. On the session details page, click "Launch Workspace" in the top right. The platform will initialize a virtual desktop with credentials pre-configured.



7.3 Use the Workspace

Step 1. The workspace opens in a new browser tab and provides a virtual desktop with the partner platform already loaded. Perform work as needed within the partner platform.



Vendor-specific functionality. For documentation on how to use the specific features of each partner platform, consult the vendor's own user documentation. This SOP covers only the platform-level access workflow, not in-platform feature usage.

7.4 Resuming an In-Progress Session

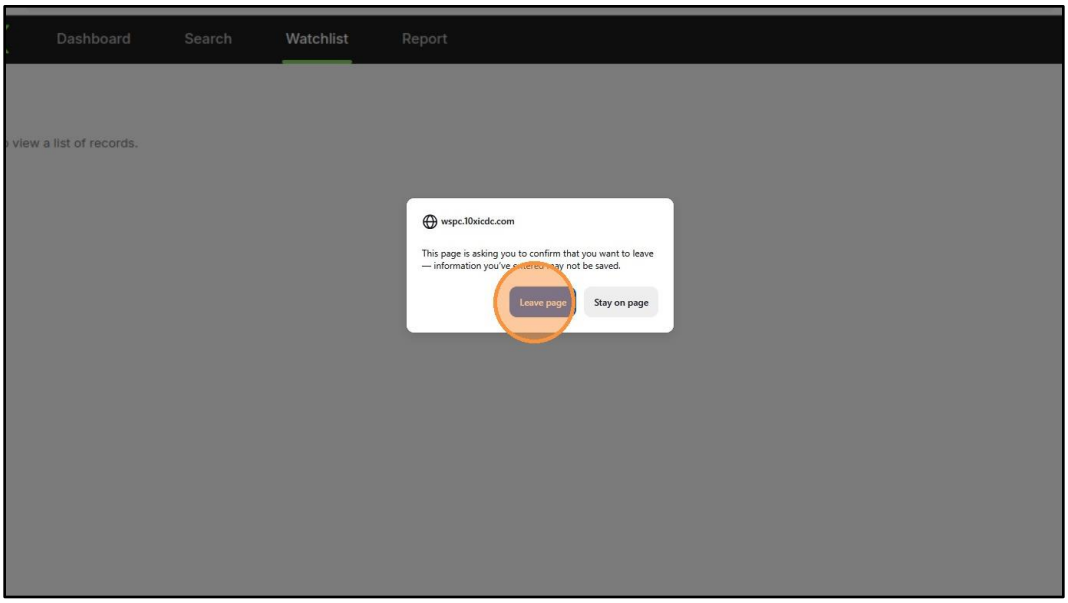
A checked-out session persists until it is explicitly returned. The user can navigate away (close the workspace tab, leave the platform, etc.) and return later to resume.

- In the left-hand navigation, an active session appears as a green "Sessions" link.
- Click that link to return to the session details page, then click "Open Workspace" to relaunch the virtual desktop.

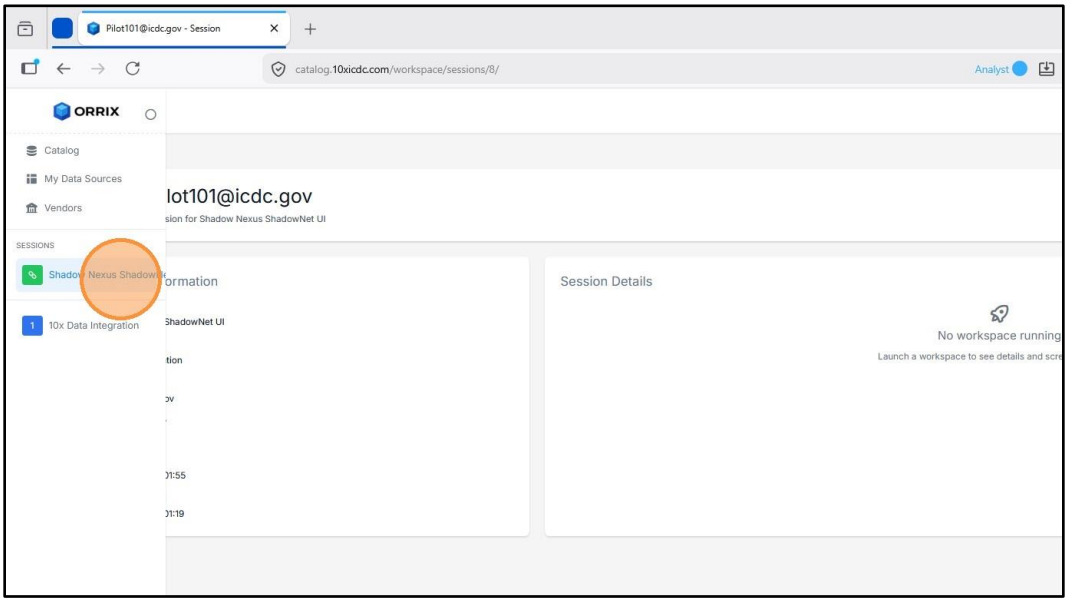
7.5 Ending and Returning the Session

Important. Session access works on a checkout model like checking out a library book. Sessions must be returned when the user is finished so the seat is freed for others. Leaving the workspace tab open or simply closing the browser does not return the session.

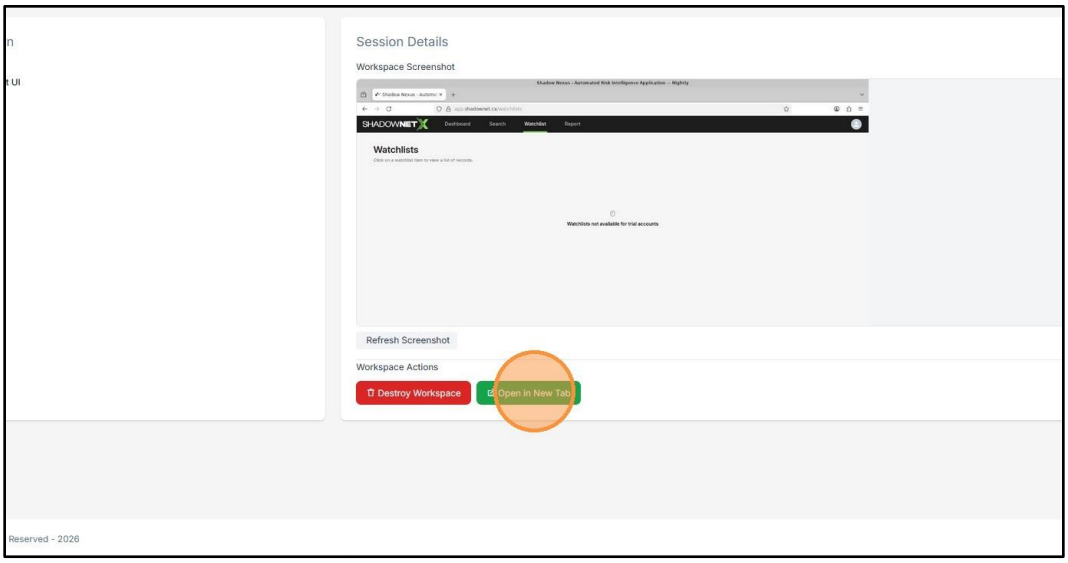
Step 1. Close the workspace browser tab. Confirm the browser prompt by clicking "Leave page".



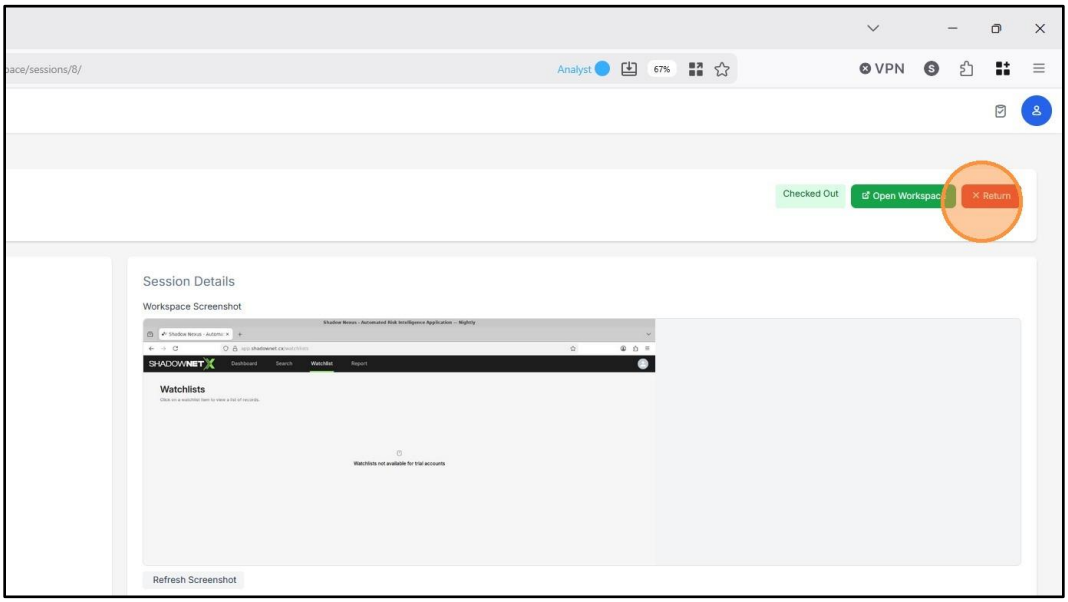
Step 2. The user is returned to the session details page on the platform. The session is still checked out under the user's name.



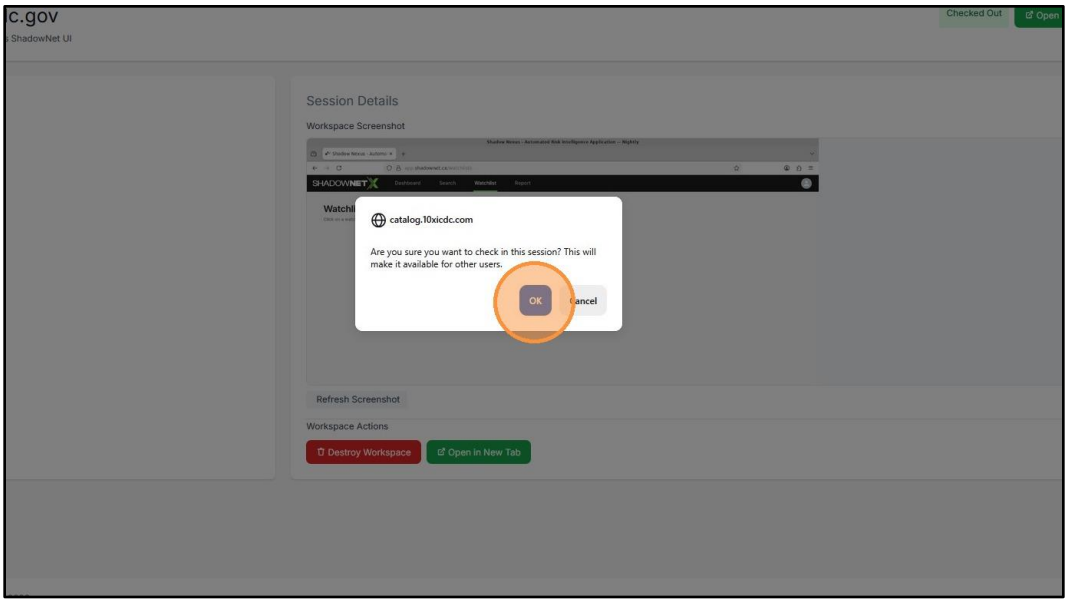
Step 3. On the session details page, click "Destroy Workspace" under Workspace Actions. This screen label terminates the virtual desktop; it does not by itself return the checked-out seat.



Step 4. Click "Return" in the top right of the session details page to release the checked-out session back to the available pool.

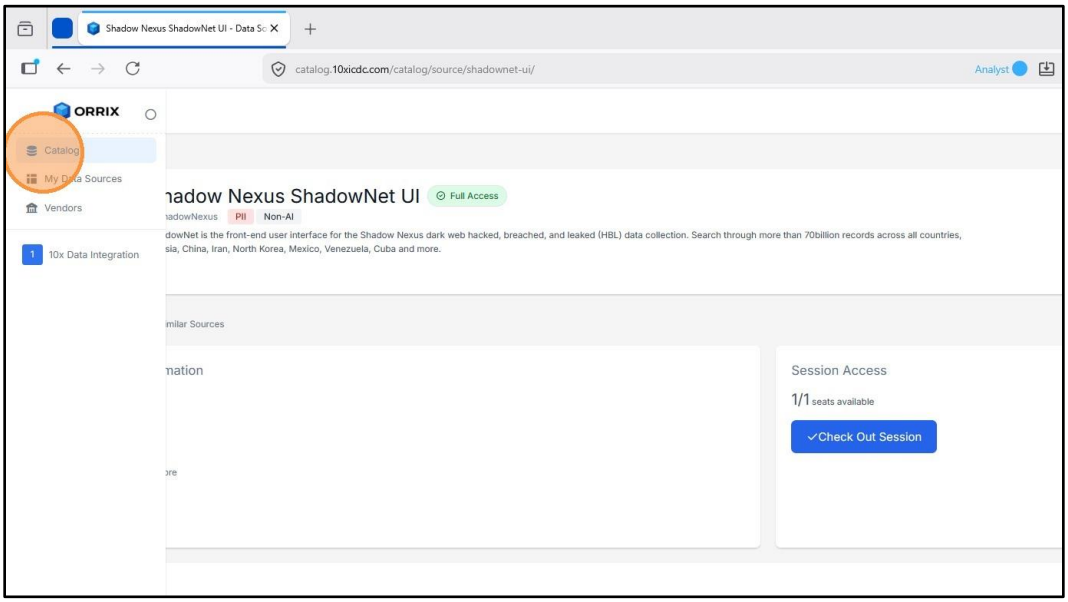


Step 5. In the confirmation dialog ("Are you sure you want to check in this session? This will make it available for other users."), click "OK".

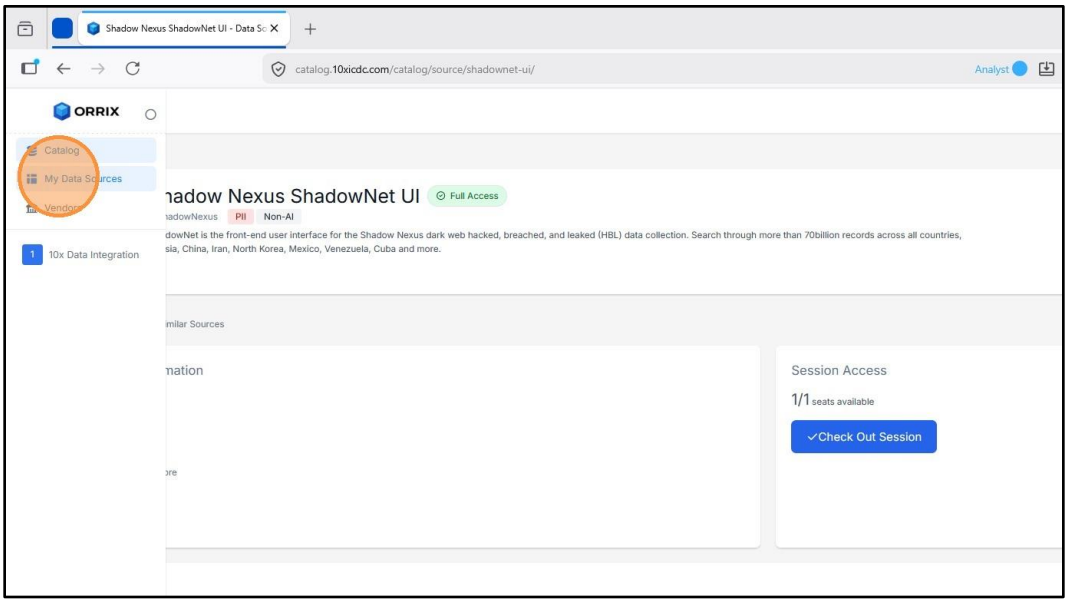


The session is now returned. The seat count returns to its available state (for example, 1 of 1) for the next user.

Step 6. To continue browsing or to access a different resource, click "Catalog" in the left-hand navigation...



Step 7. ...or click "My Data Sources" to view all resources currently available to your organization.

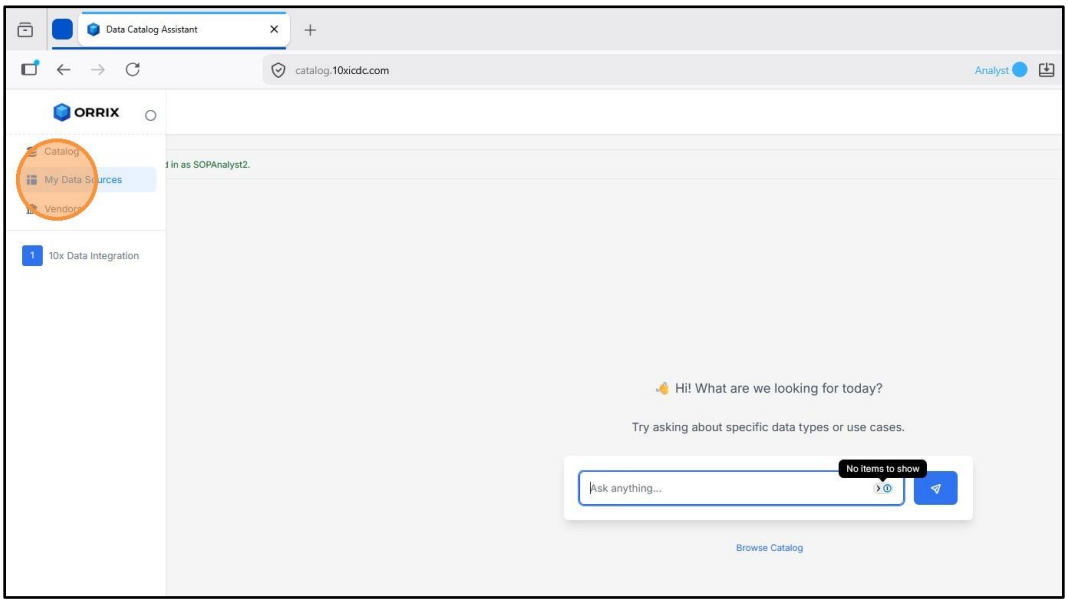


8. Workflow C Requesting API Access and Generating Keys

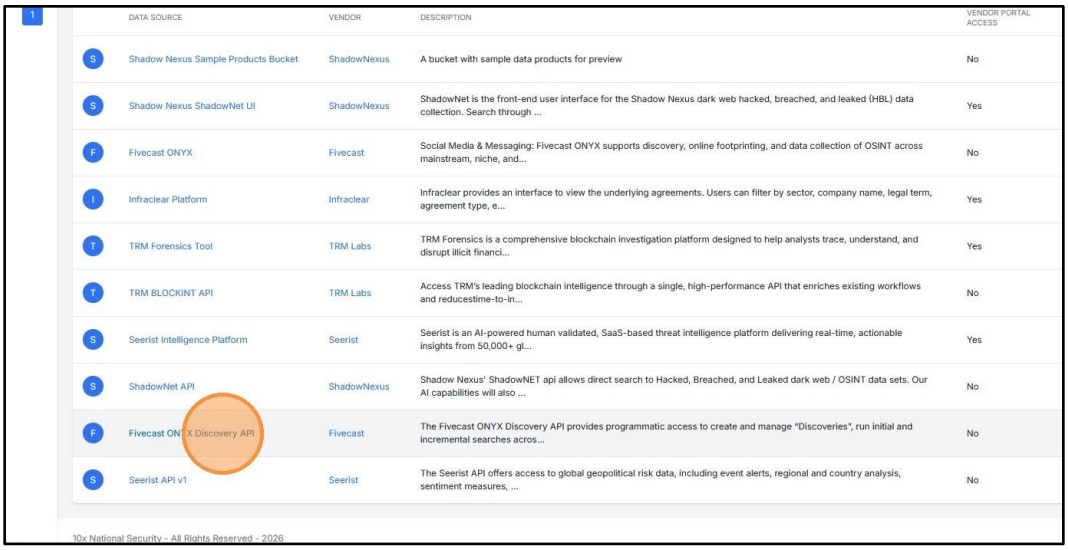
Use this workflow when the user needs programmatic access to a data source through an API endpoint or MCP server endpoint. After approval, the user generates a personal access key, typically used as a bearer token. The key is displayed only once and must be stored securely immediately.

8.1 Submit the API Access Request

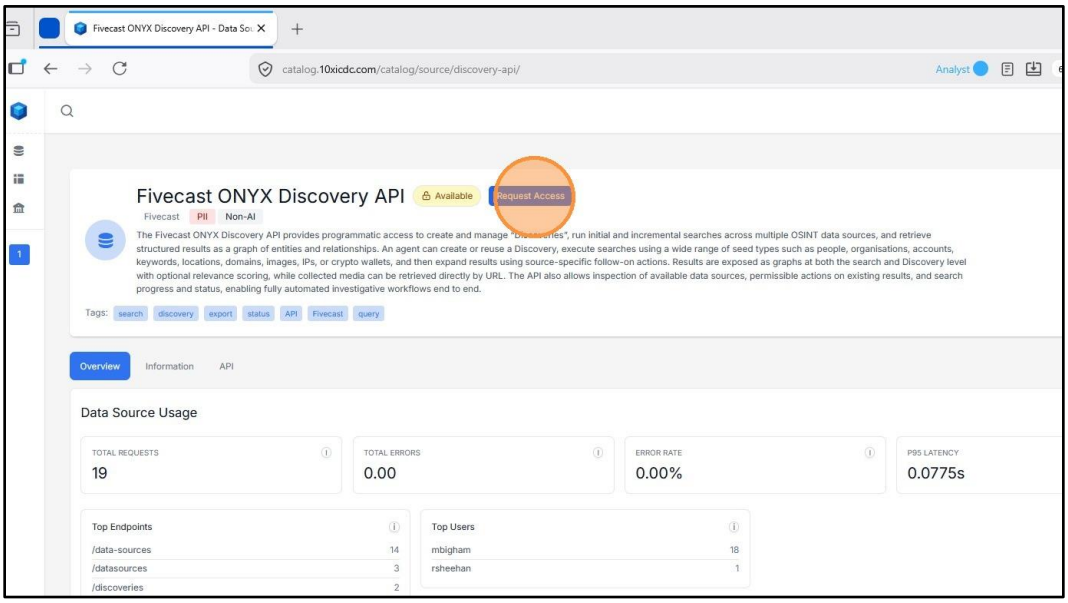
Step 1. From the left-hand navigation, select "My Data Sources".



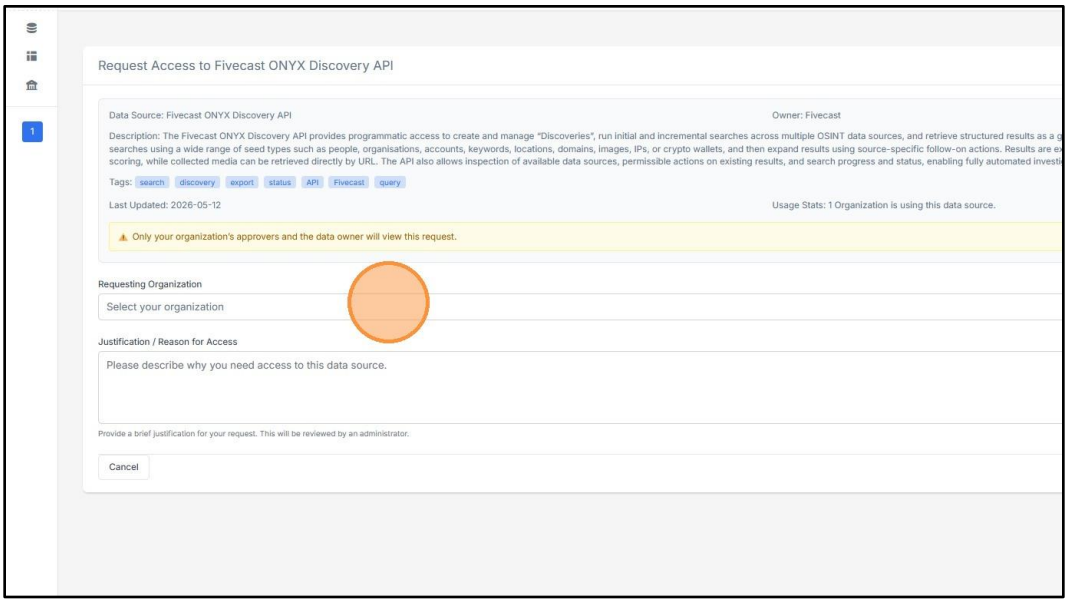
Step 2. From the data source list, click the desired API.



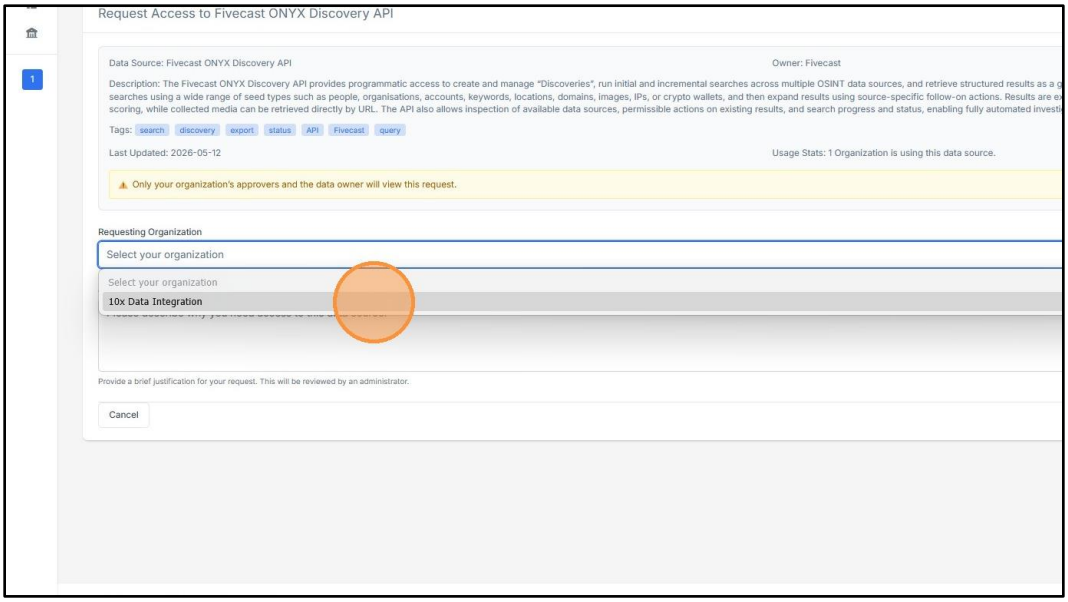
Step 3. On the API detail page, click "Request Access".



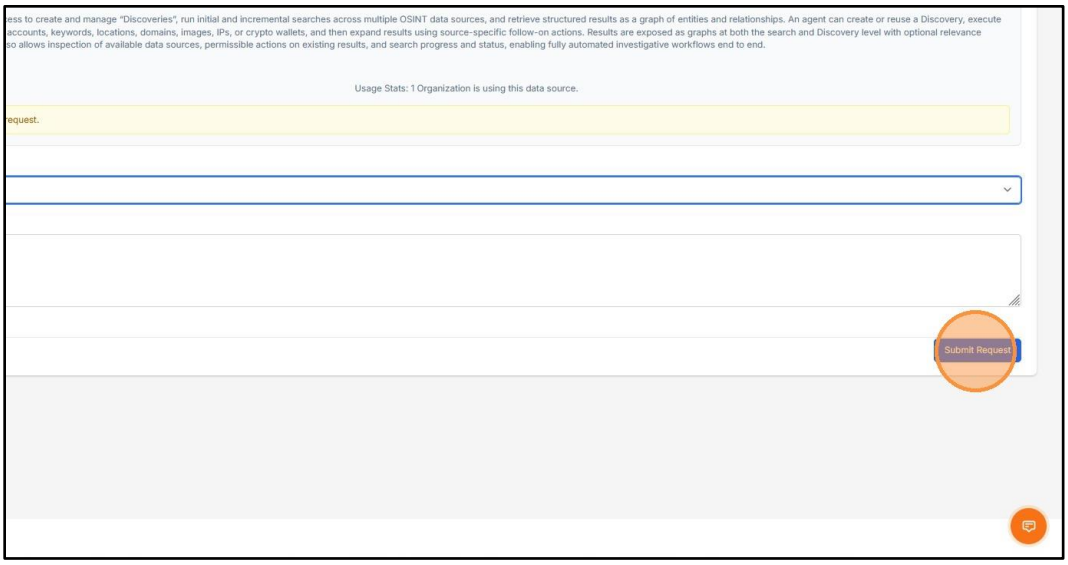
Step 4. On the Request Access form, click the "Requesting Organization" field.



Step 5. Select your organization from the dropdown.

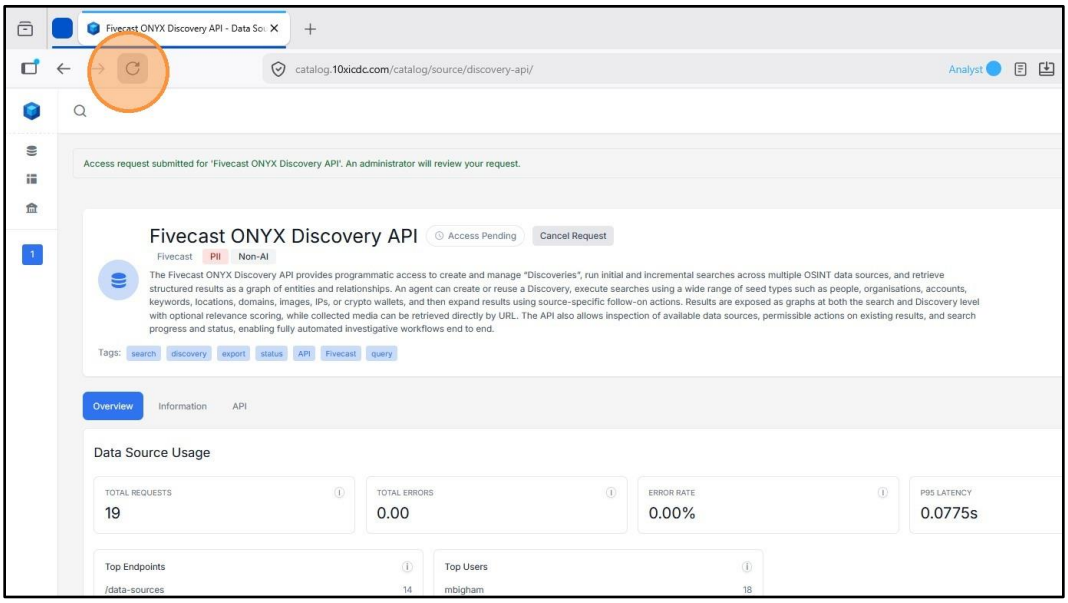


Step 6. Enter a justification in the "Justification / Reason for Access" field, then click "Submit Request".



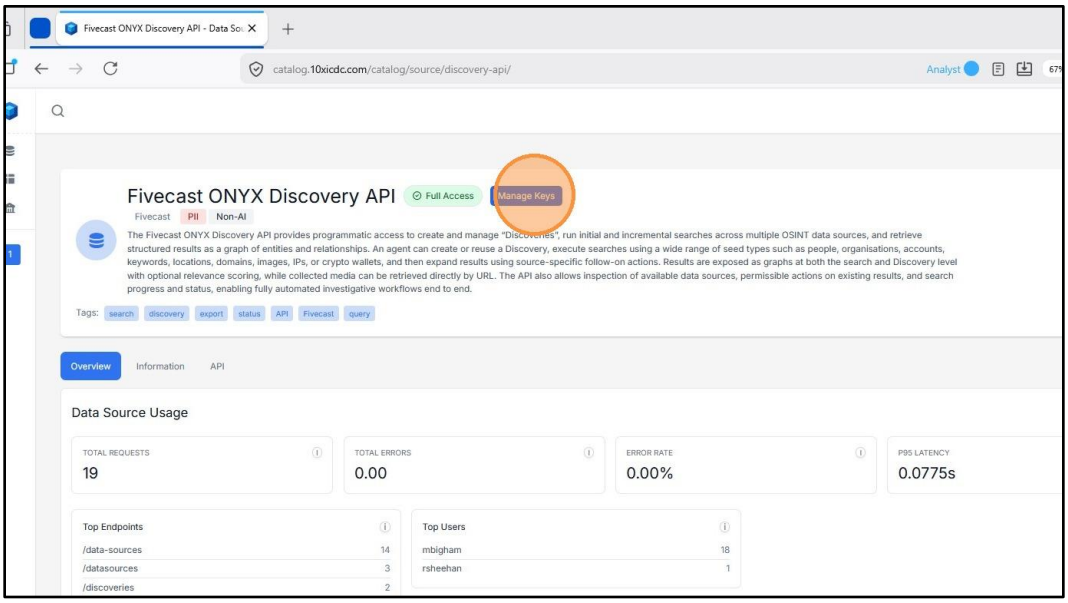
8.2 Confirm Approval

Step 1. After the Org Admin has approved the request, click the browser refresh icon (or use the in-app reload control) to refresh the API detail page. The "Access Pending" badge will change to "Full Access".

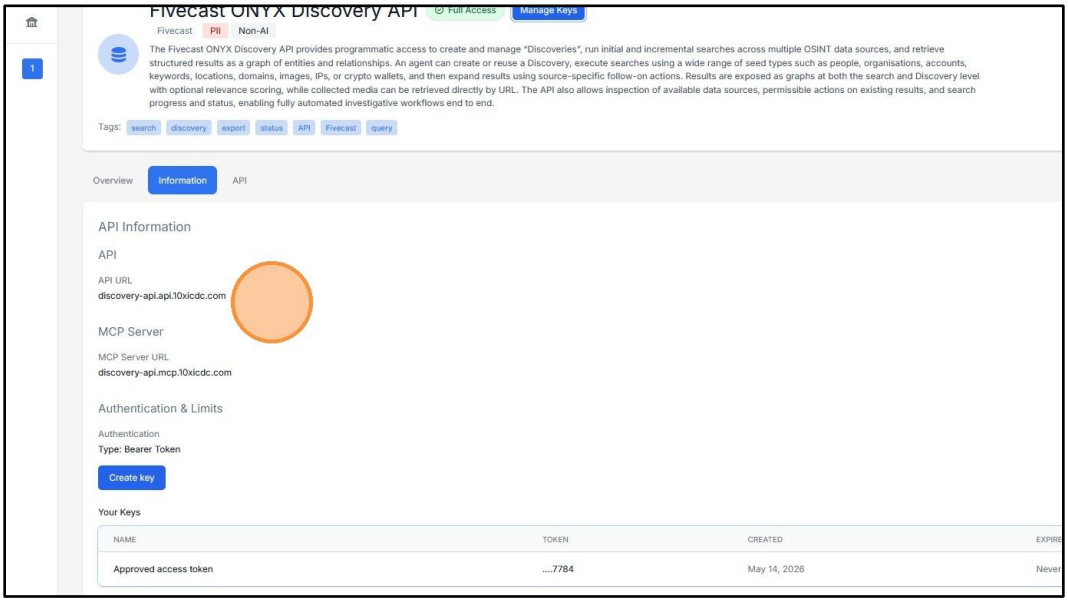


8.3 Generate an Access Key

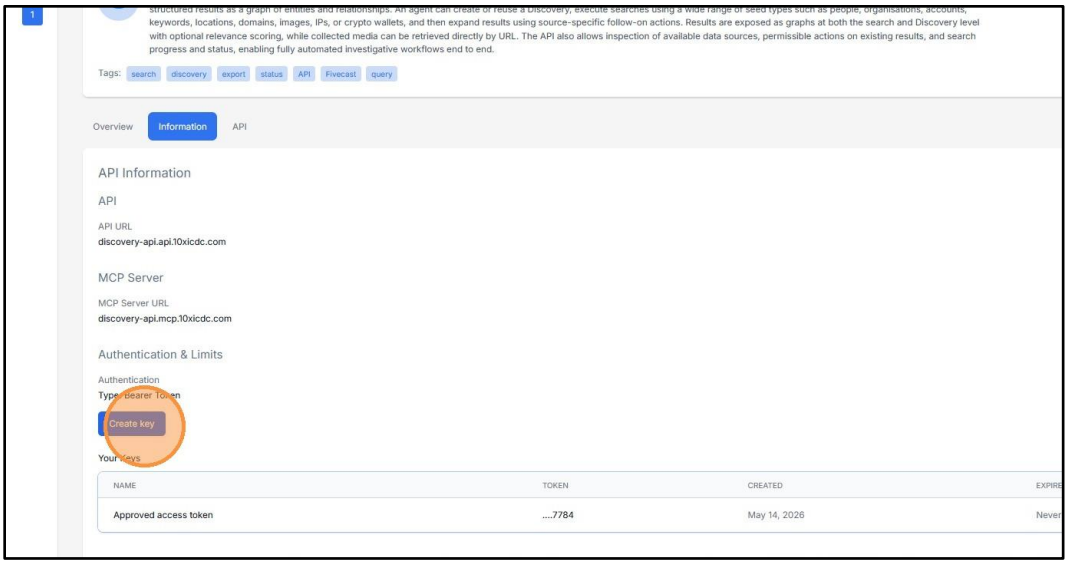
Step 1. On the API detail page, click "Manage Keys" in the top right.



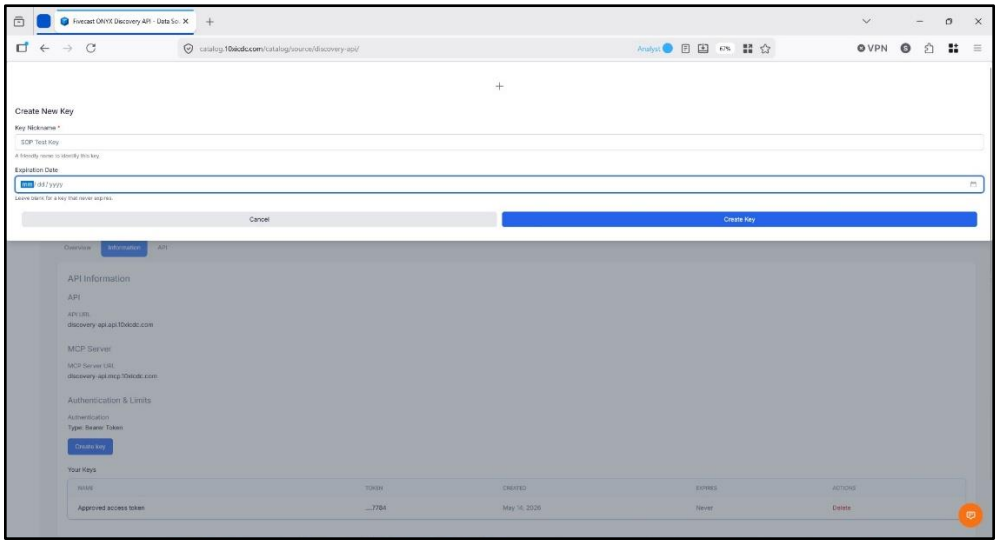
Step 2. Select the "Information" tab to view API connection details. The page displays the API URL, MCP Server URL, and the authentication type (typically Bearer Token), along with any existing keys.



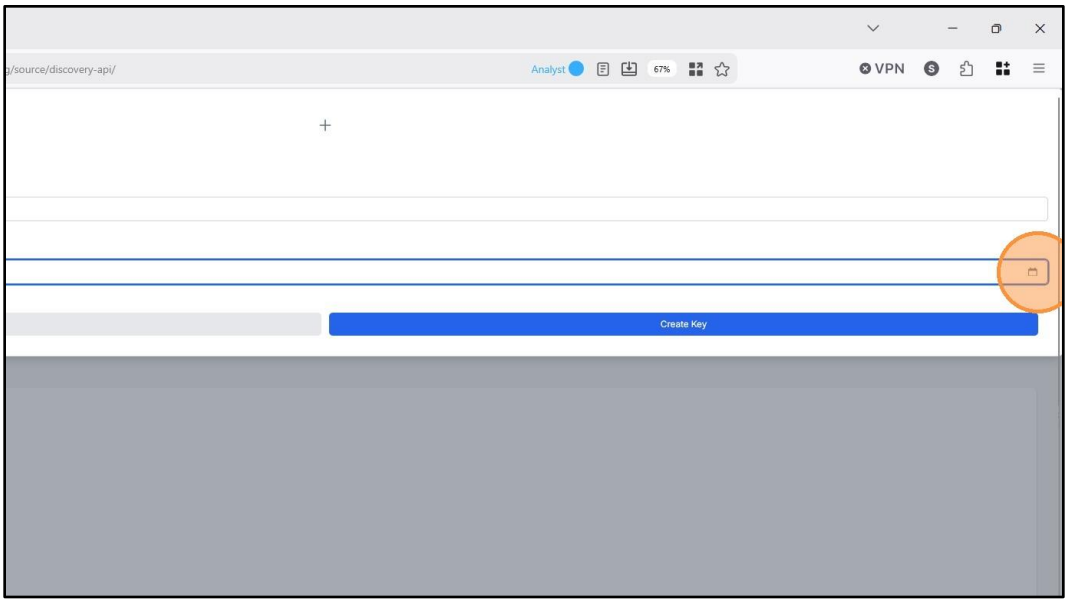
Step 3. Click "Create key" to begin generating a new API token.



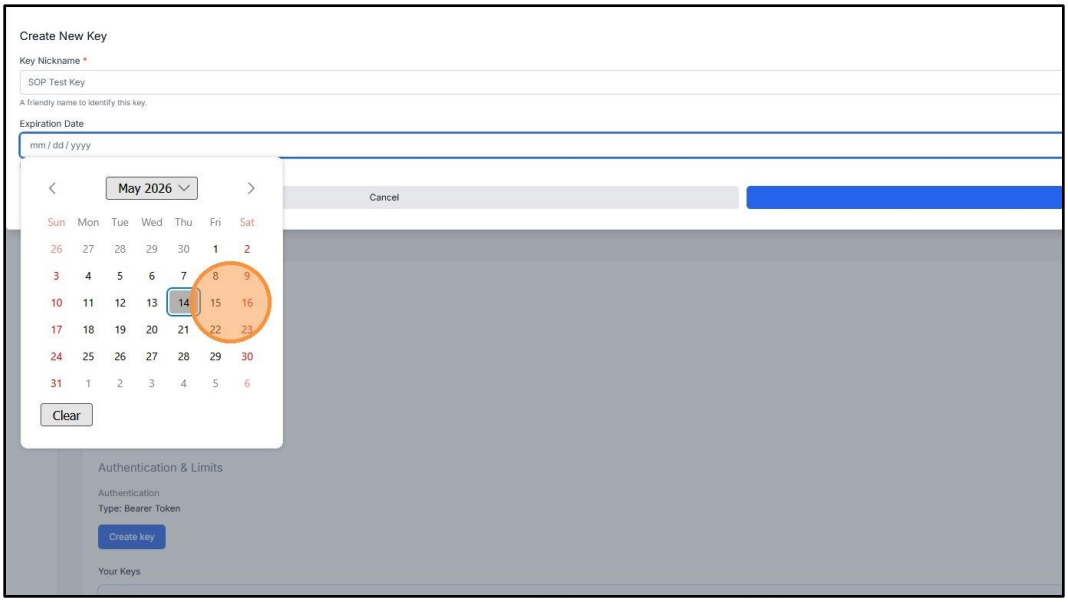
Step 4. On the Create New Key form, enter a friendly Key Nickname, then click the "Expiration Date" field.



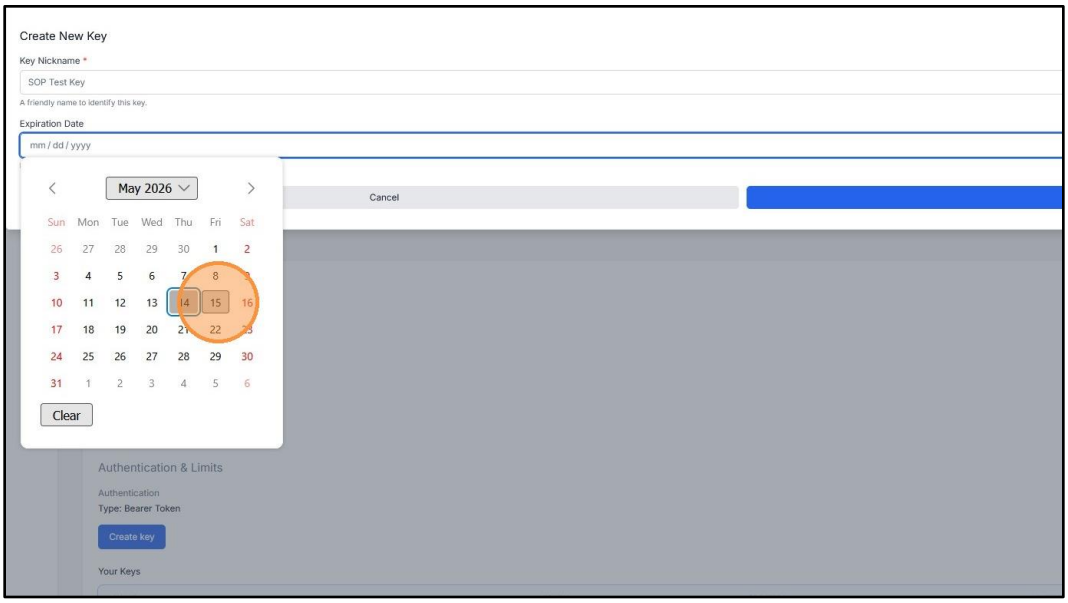
Step 5. Click the calendar icon to open the date picker.



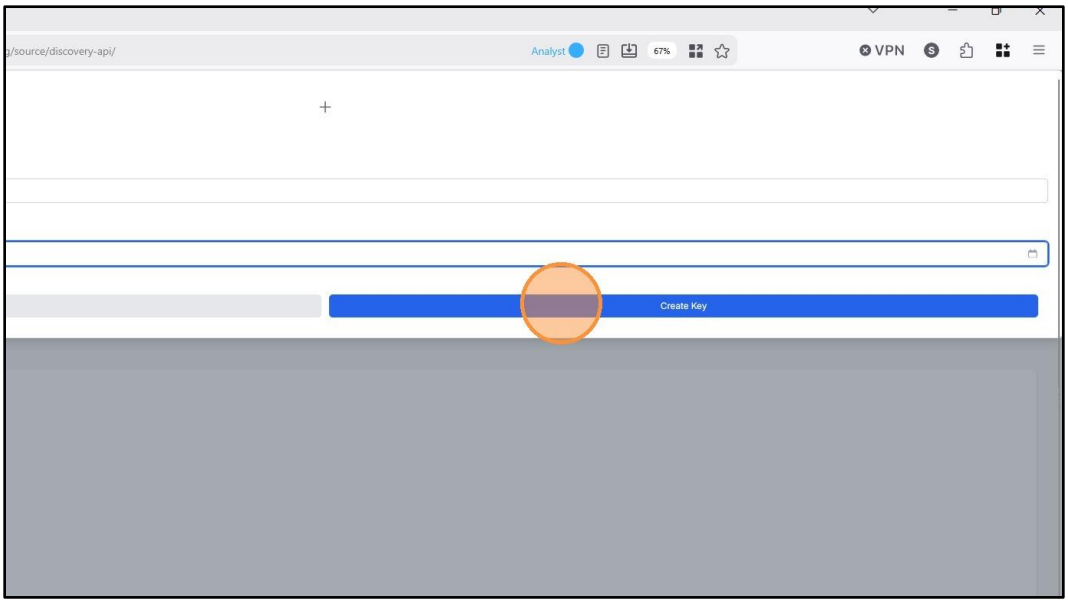
Step 6. Select an expiration date from the calendar.



Step 7. Confirm the selected date is shown in the Expiration Date field.



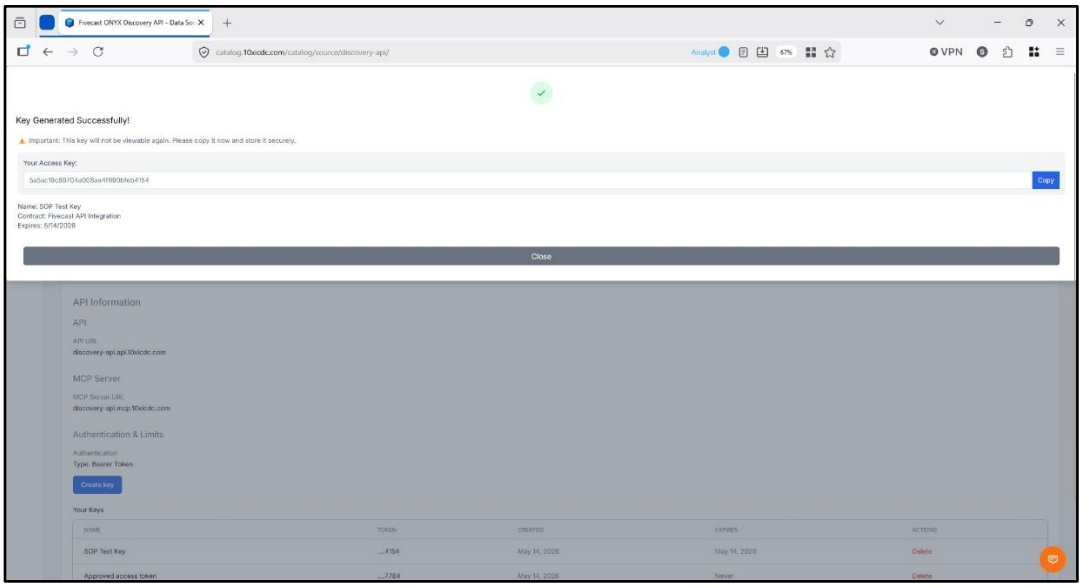
Step 8. Click "Create Key" to finalize the generation.



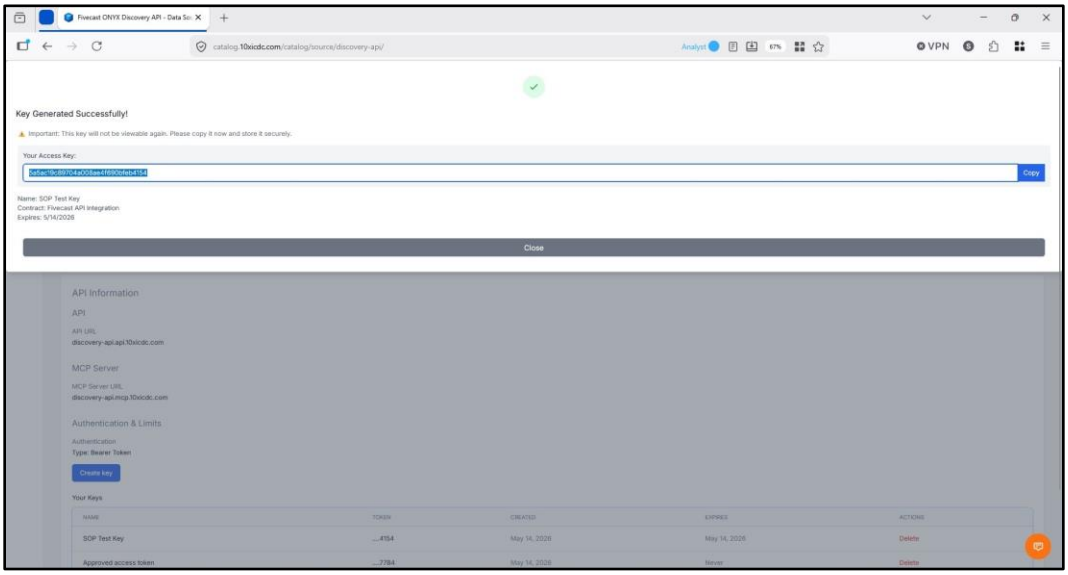
8.4 Copy and Store the Access Key

> **Critical.** The access key is displayed only once at the moment of creation. Copy it immediately and store it securely in a password manager or secrets vault. The key cannot be retrieved from the platform afterward if lost, a new key must be generated.

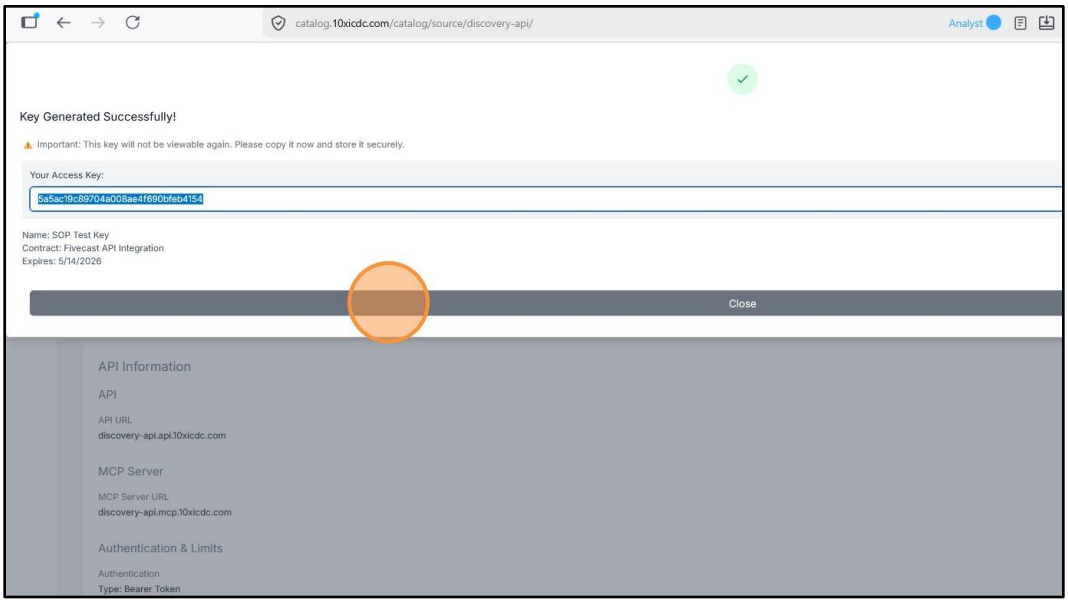
Step 1. On the "Key Generated Successfully!" screen, review the new key details (name, contract, expiration date).



Step 2. Click the "Copy" button (or press Ctrl + C) to copy the generated access key, then paste it into your secure storage location.

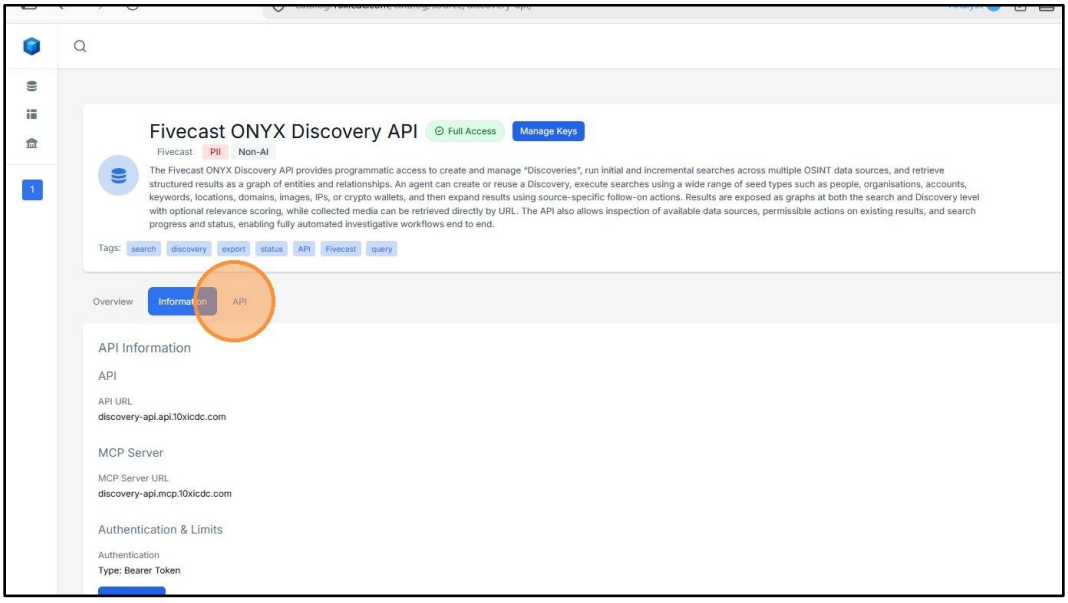


Step 3. Once the key has been safely copied, click "Close" to dismiss the key display.

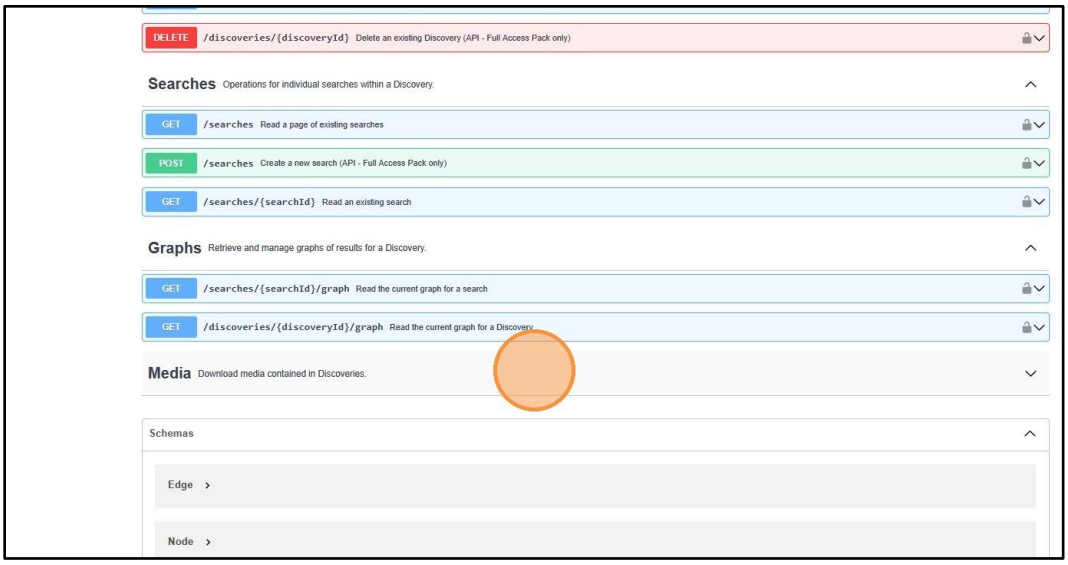


8.5 Locate API Documentation and Endpoints

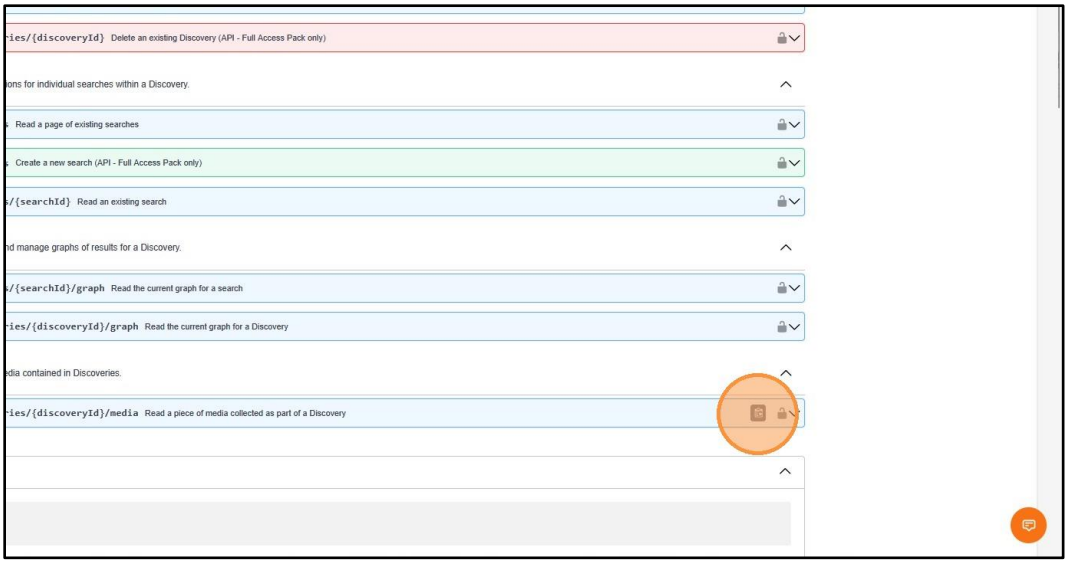
Step 1. On the API detail page, switch to the "API" tab to view interactive API documentation.



Step 2. Expand any API endpoint (organized by category such as Searches, Graphs, Media, etc.) to view documentation details including parameters, request format, and response schema.



Step 3. Use the copy icon next to an endpoint to copy its path for use in your client code or API testing tool.



8.6 Using the Access Key

With the access key, the API URL, and the relevant endpoint path, the user can make authenticated calls from an HTTP client, script, MCP-compatible tool, or approved integration. The authentication method is typically Bearer Token. Include the key as an Authorization header on each request, for example: Authorization: Bearer <access_key>.

8.7 Protecting, Rotating, and Revoking API Keys

API keys and bearer tokens should be handled like passwords because they grant access under the user or service account identity.

- Do not paste API keys into email, chat, tickets, screenshots, shared documents, or unsecured spreadsheets.
- Store keys only in an approved password manager, secrets vault, or approved credential store.
- Use expiration dates that match the mission need; avoid long-lived keys unless the workflow requires them and leadership approves.
- Generate a new key if the original is lost. Because generated keys are displayed only once, the platform cannot retrieve a lost key.

- Rotate or revoke a key immediately if it may have been exposed, copied into an unsafe location, or used on an unapproved system.
- Use service-account or organization-managed keys for shared or scheduled workflows whenever platform policy supports them.

9. Workflow D Bulk Data Download

Use this workflow when an approved bulk data source provides downloadable files rather than only interactive chat, API, or workspace access. In this workflow, the analyst creates bulk-data credentials, saves the Access Key ID, Secret Access Key, and Endpoint URL, browses the file structure, requests a specific file for download, and downloads the file after Org Admin approval.

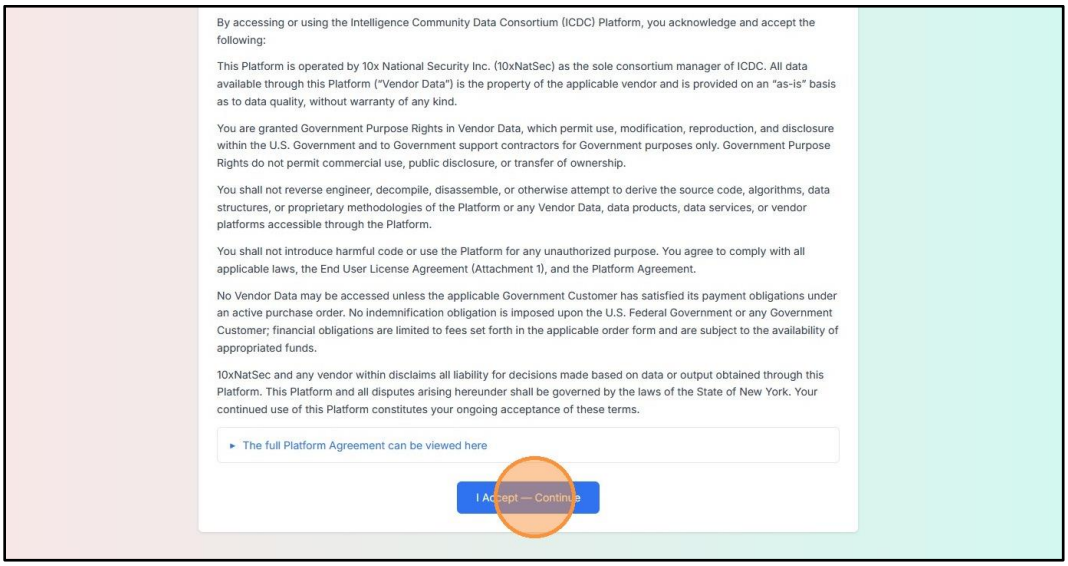
9.1 Before You Begin

Before starting a bulk data download, confirm the following:

- The analyst can log in to the ICDC/ORRIX portal.
- The bulk data source is available under My Data Sources, or access has been requested and approved.
- The analyst has an approved secure location to store the Access Key ID, Secret Access Key, and Endpoint URL.
- The analyst understands which folder, date range, or file type is needed for the analysis.
- The analyst is authorized to download, store, and analyze the requested bulk data file.

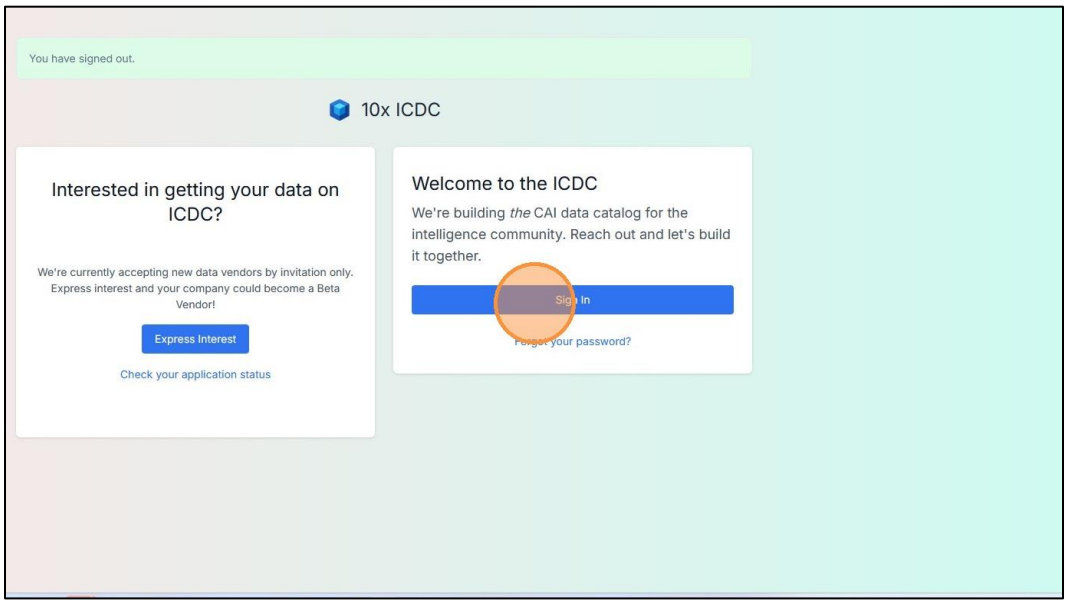
9.2 Locate the Bulk Data Source

Step 1. Log in to the ICDC/ORRIX portal using the account workflow described in Section 4. If the consent screen appears, review the terms and click the acceptance option to continue.

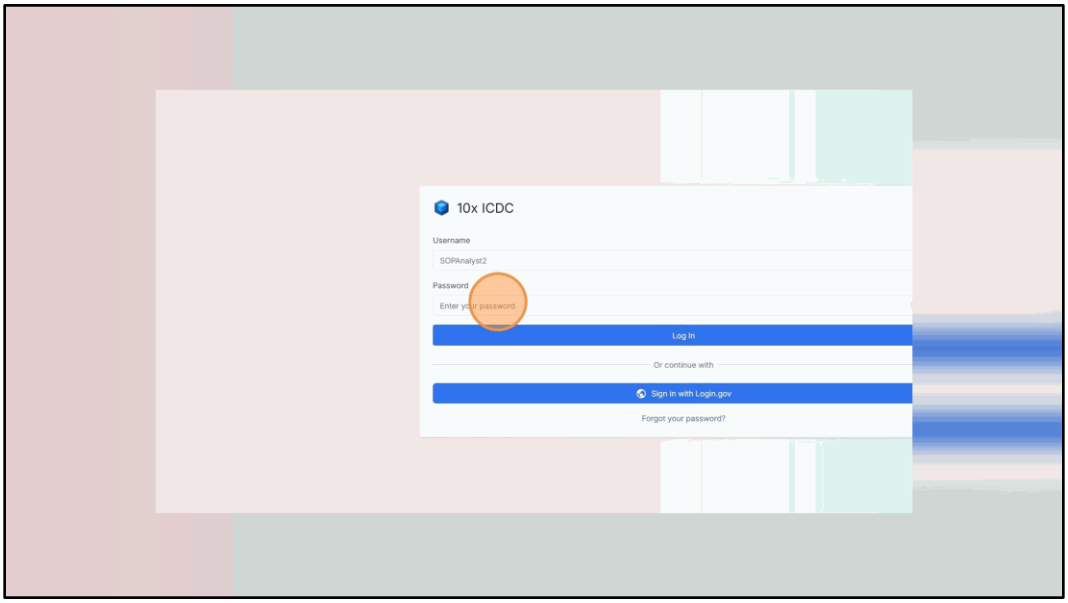


Bulk Data Screenshot 1 - Accept the system use consent, if prompted.

Step 2. Click "Sign In" and enter the analyst username and password previously provided through the account creation process.

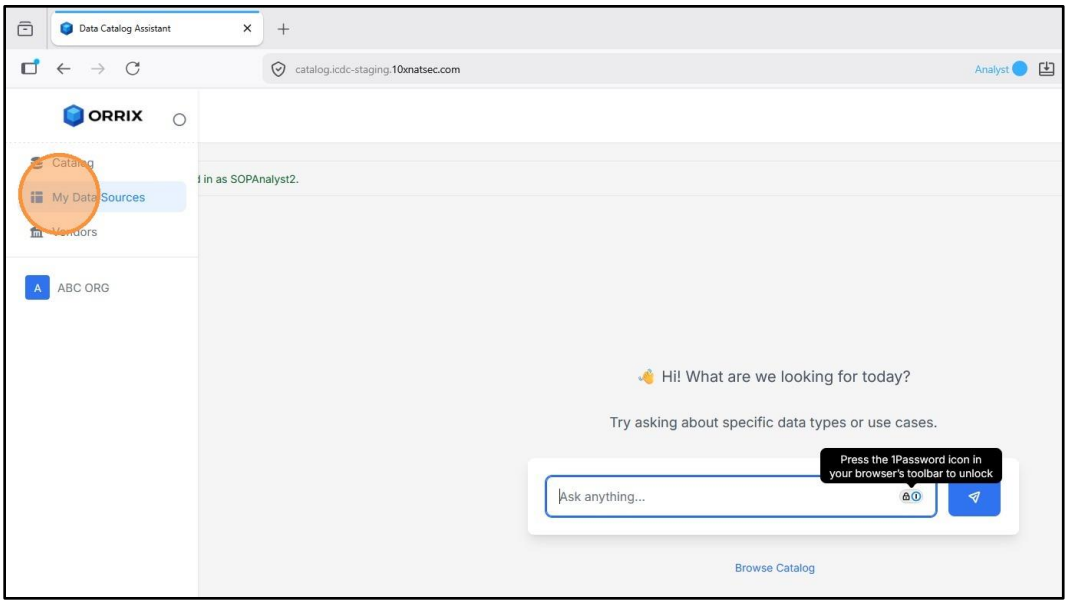


Bulk Data Screenshot 2 - Sign in to the portal.

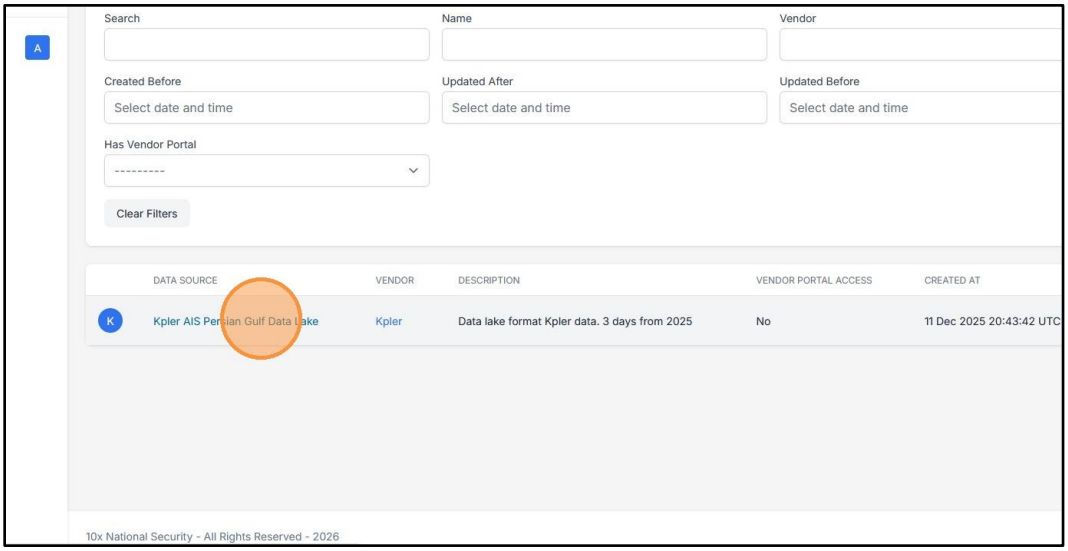


Bulk Data Screenshot 3 - Enter username and password.

Step 3. From the platform home screen, navigate to My Data Sources or use the catalog/search capability to locate the bulk data source. In the screenshots, the pilot example is "Kpler AIS Persian Gulf Data Lake"; your environment may show a different source name.



Bulk Data Screenshot 4 - Search for or locate the bulk data source.

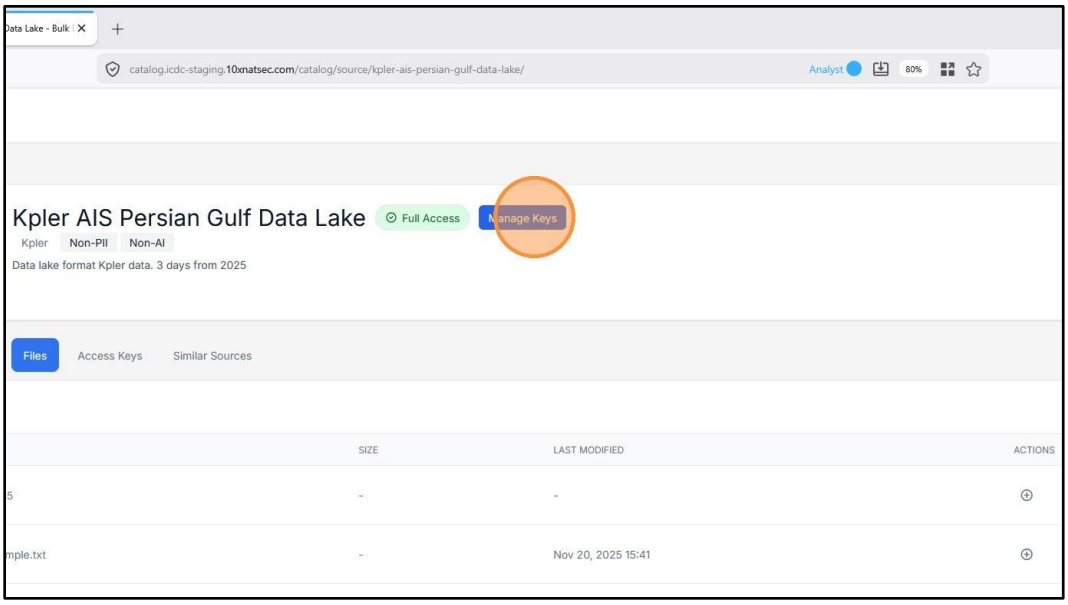


Bulk Data Screenshot 5 - Open the bulk data source detail page.

9.3 Generate and Save Bulk Data Credentials

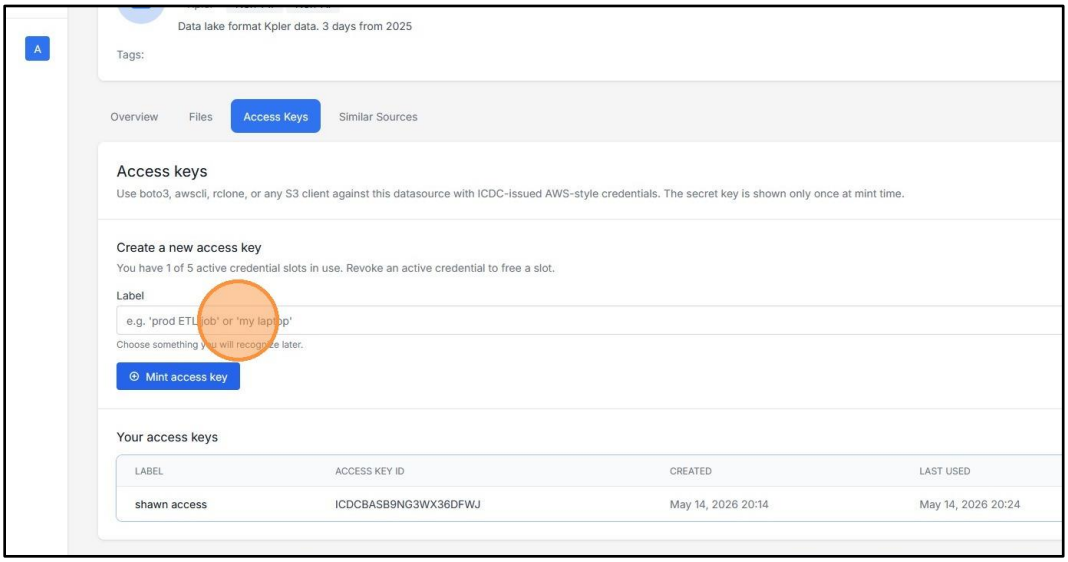
Bulk data downloads require credentials that are separate from the normal portal login. These values are displayed during credential creation and must be copied to an approved secure storage location.

Step 1. On the bulk data source detail page, click "Manage Keys."

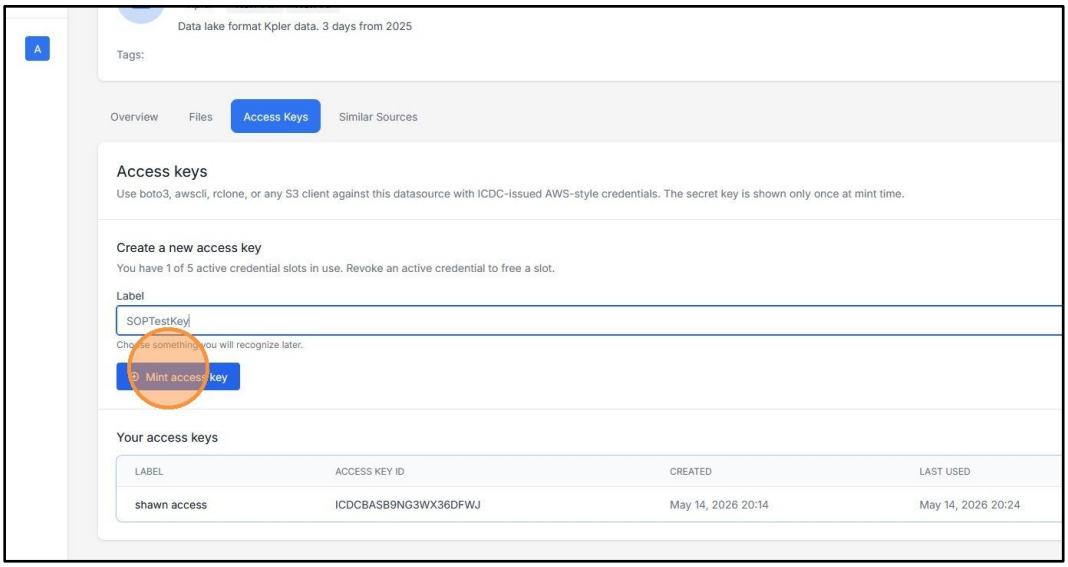


Bulk Data Screenshot 6 - Manage Keys on the bulk data source detail page.

Step 2. Enter a friendly label for the credential, such as a mission name, project name, or date-specific label that helps identify why the credential was created.

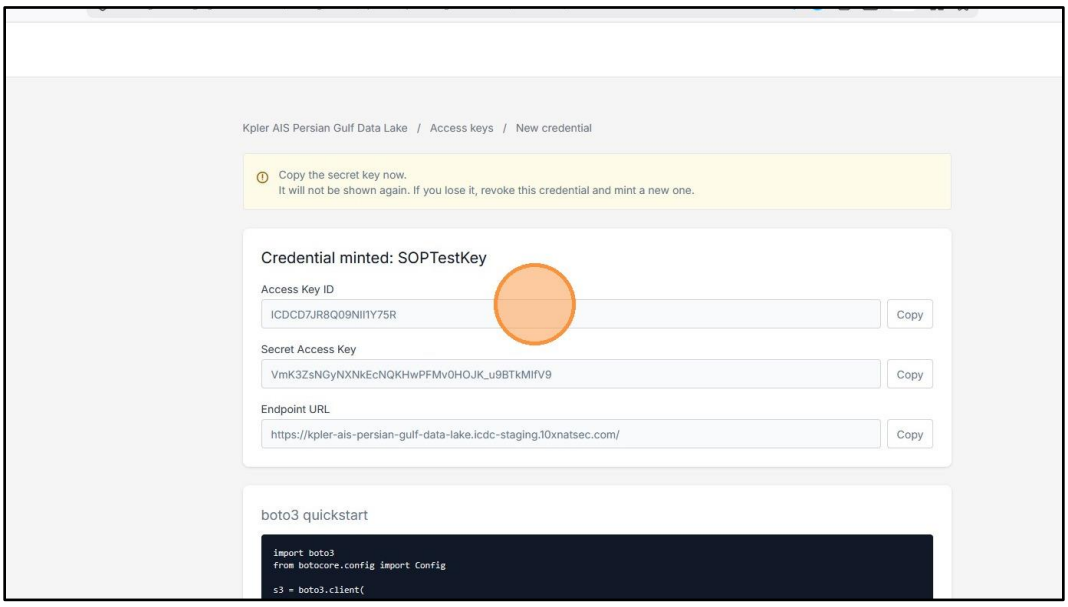


Bulk Data Screenshot 7 - Enter a credential label.



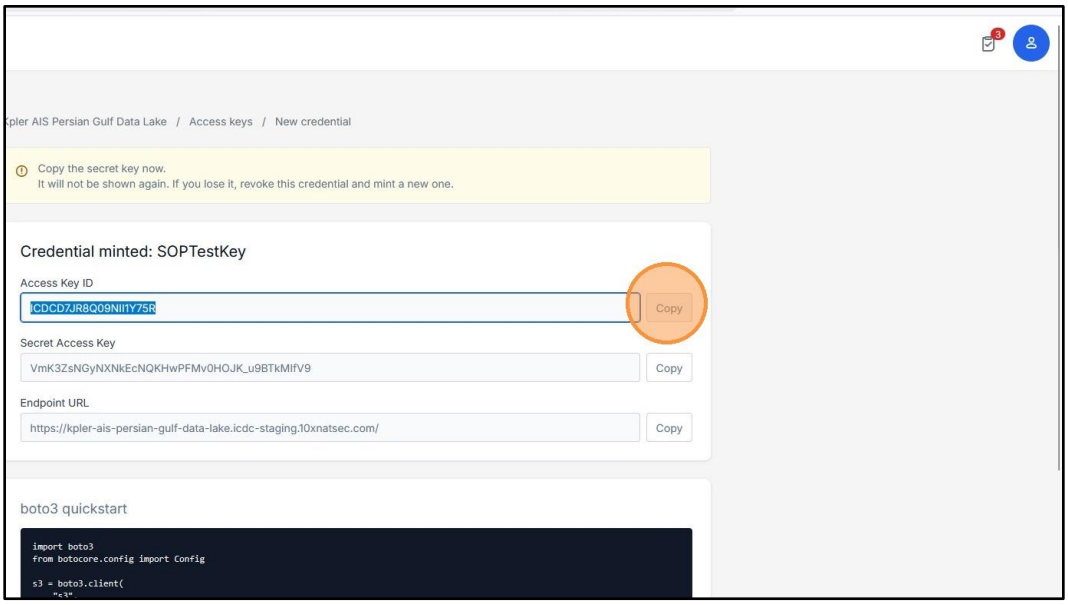
Bulk Data Screenshot 8 - Confirm or complete the credential label before minting the access key.

Step 3. Click "Mint access key" to generate the credential set.

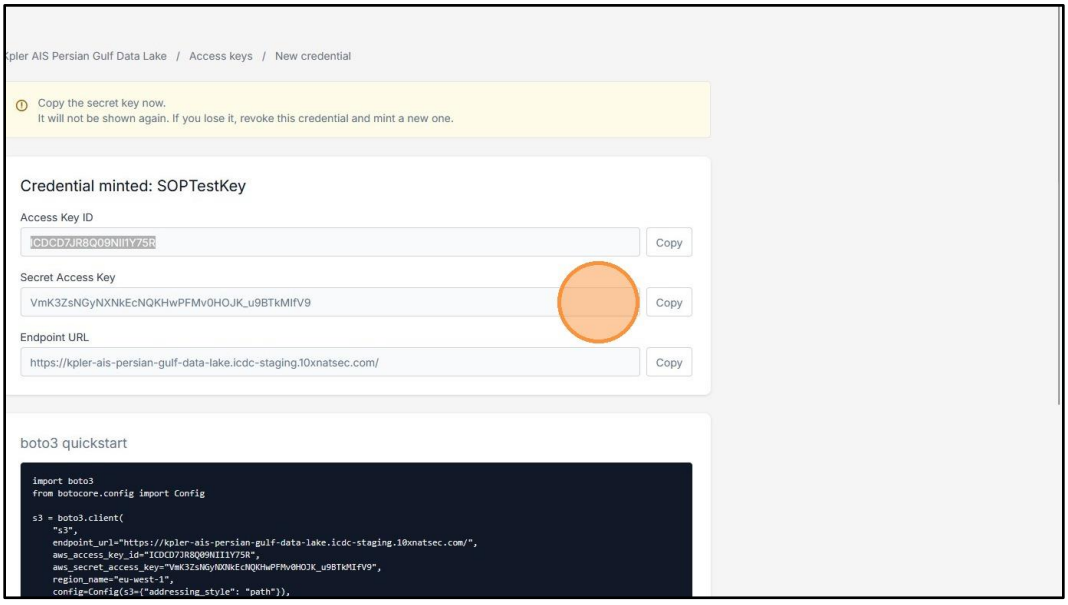


Bulk Data Screenshot 9 - Mint the access key.

Step 4. Copy the Access Key ID and save it in the approved secure location.

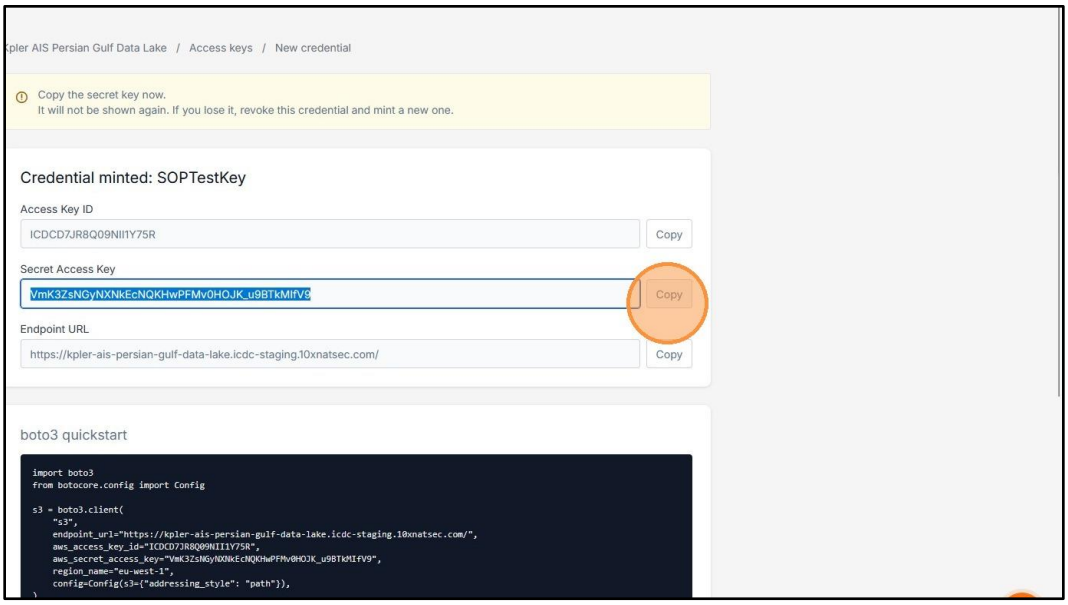


Bulk Data Screenshot 10 - Copy the Access Key ID.

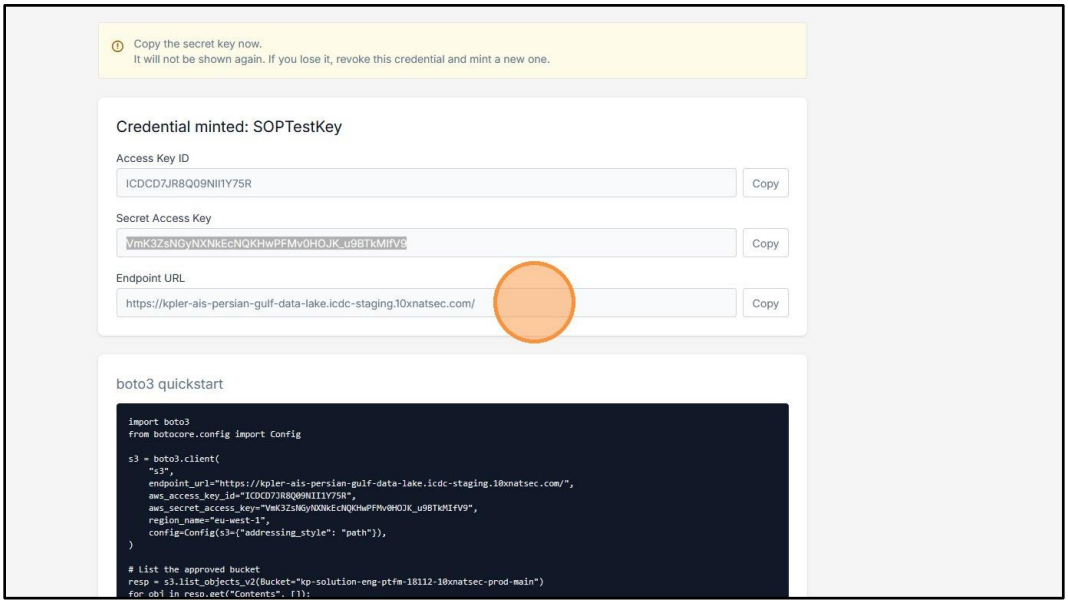


Bulk Data Screenshot 11 - Access Key ID copy confirmation.

Step 5. Copy the Secret Access Key and save it in the approved secure location. Treat this value as sensitive; it should not be pasted into email, chat, screenshots, shared documents, or unsecured spreadsheets.

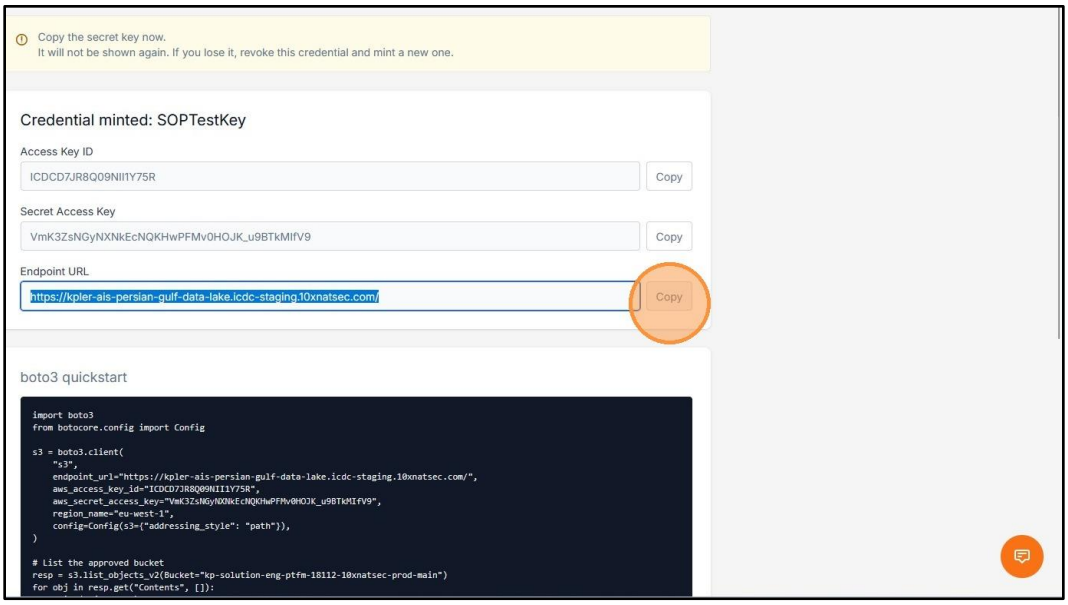


Bulk Data Screenshot 12 - Copy the Secret Access Key.



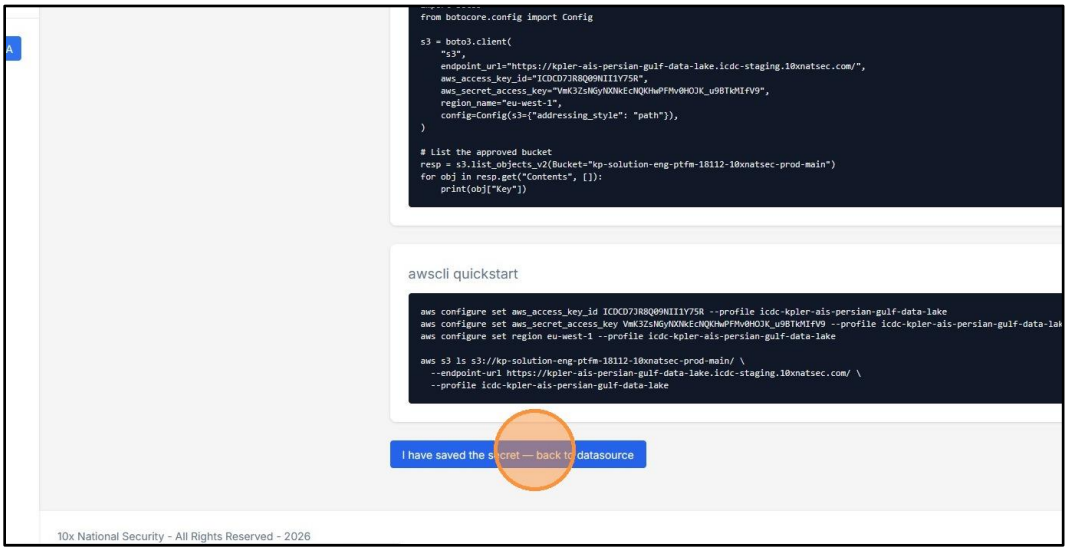
Bulk Data Screenshot 13 - Secret Access Key copy confirmation.

Step 6. Copy the Endpoint URL and save it with the credential set. The endpoint is required when connecting to the bulk data store or when using quick-start scripts.



Bulk Data Screenshot 14 - Copy the Endpoint URL.

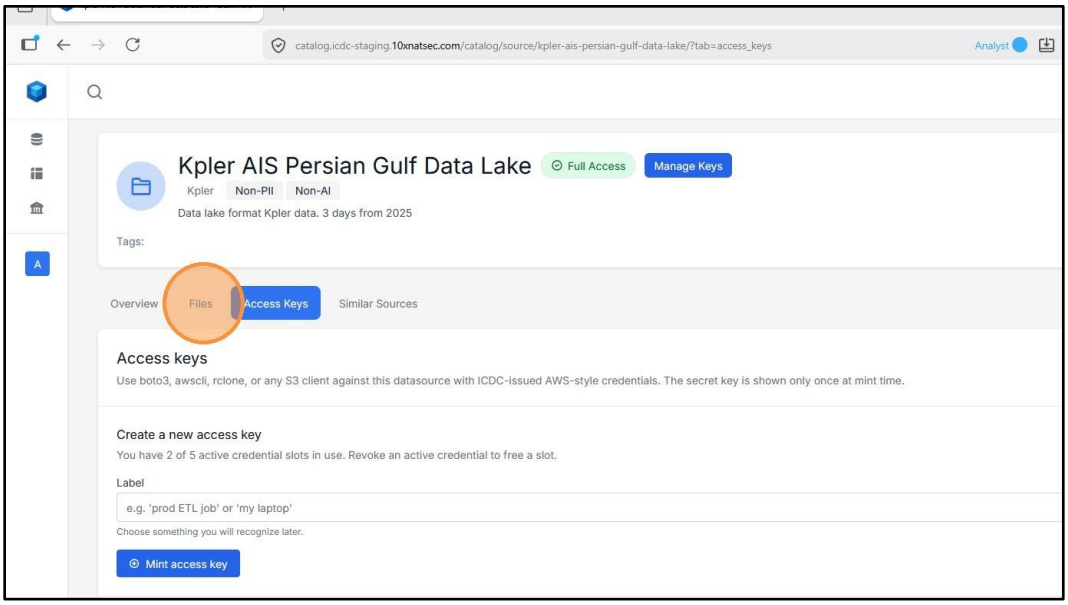
Step 7. After the Access Key ID, Secret Access Key, and Endpoint URL have been securely saved, click the confirmation option indicating that the secret has been saved and return to the data source.



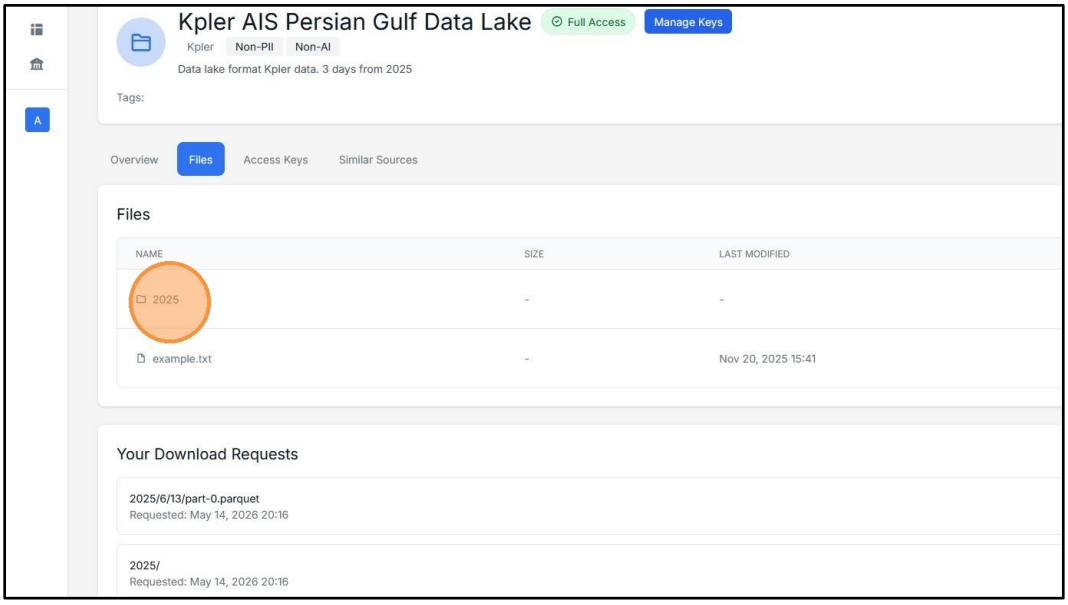
Bulk Data Screenshot 15 - Confirm the secret has been saved and return to the data source.

9.4 Browse Files and Request a Bulk Data Download

Step 1. From the bulk data source detail page, click the "Files" tab to open the file browser.

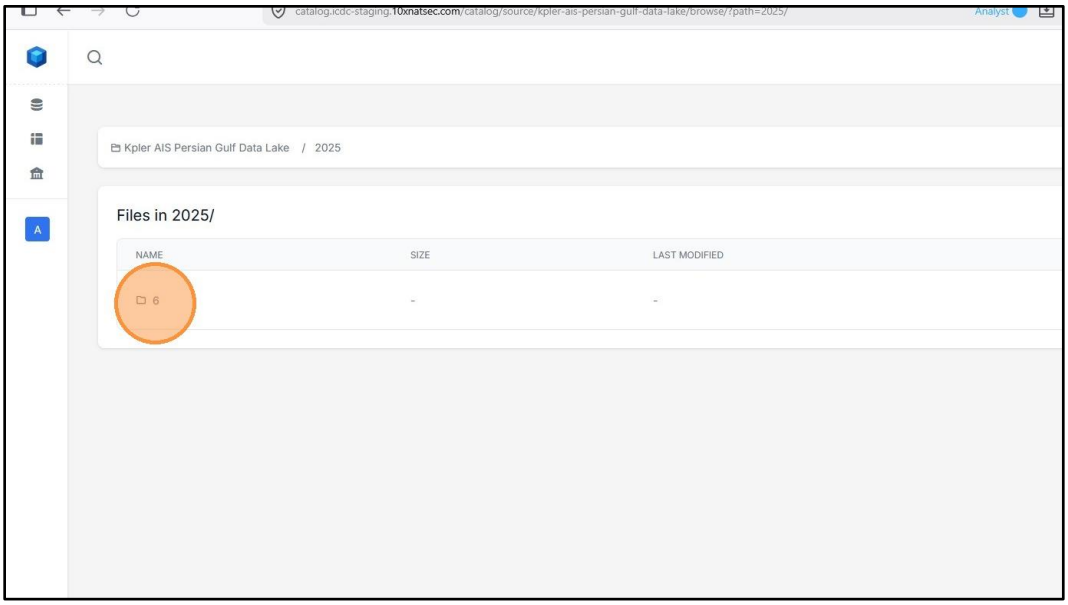


Bulk Data Screenshot 16 - Open the Files tab.



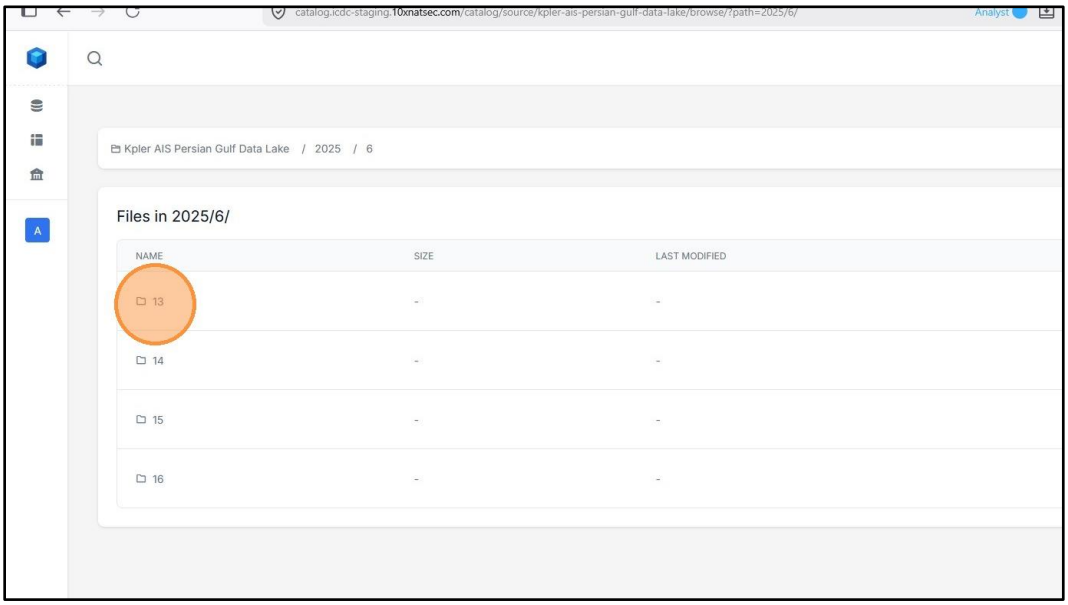
Bulk Data Screenshot 17 - Review the available bulk data files.

Step 2. Navigate through the file structure to the desired folder. Bulk data may be organized by year, month, day, or another vendor-specific folder structure.



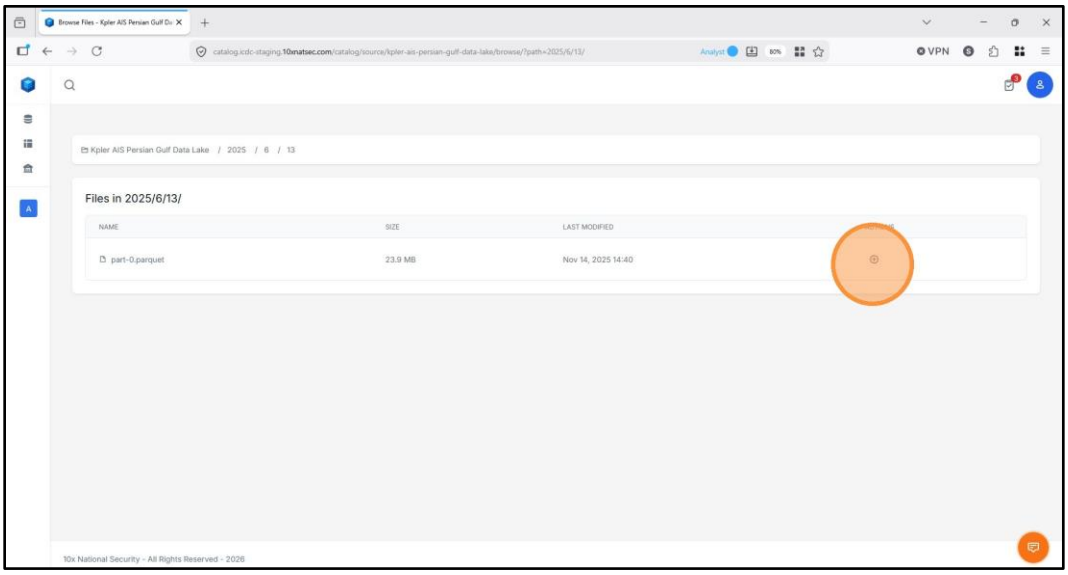
Bulk Data Screenshot 18 - Navigate the folder structure.

Step 3. Continue drilling down until the target file is visible. In the pilot example, the target file is a Parquet file.



Bulk Data Screenshot 19 - Locate the desired file.

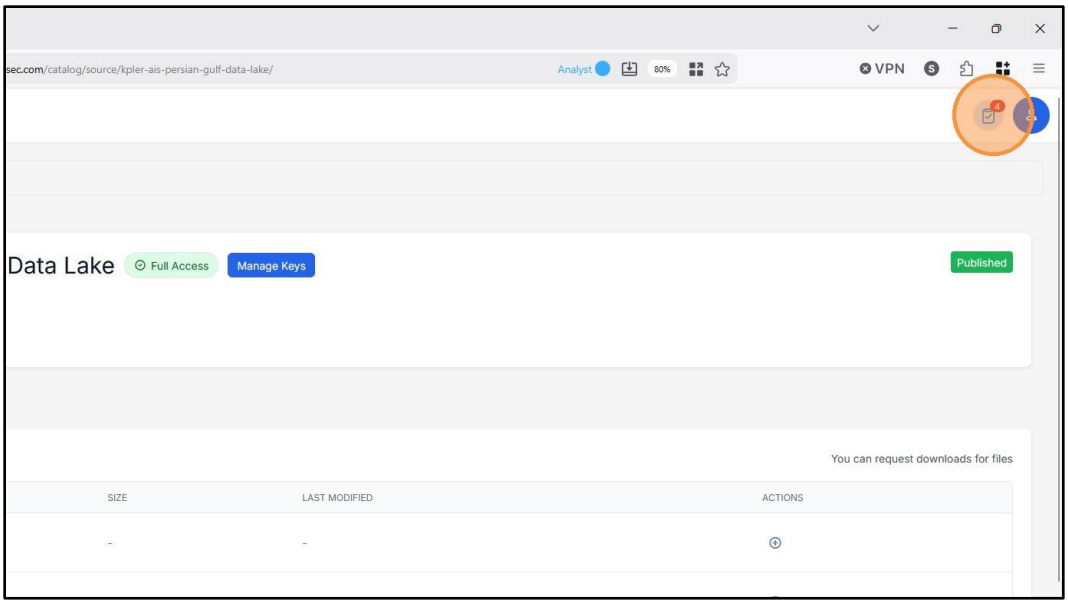
Step 4. Click the action control, such as the plus icon, next to the file to request the download. This creates a download request that is routed for Org Admin approval.



Bulk Data Screenshot 20 - Request download for the selected file.

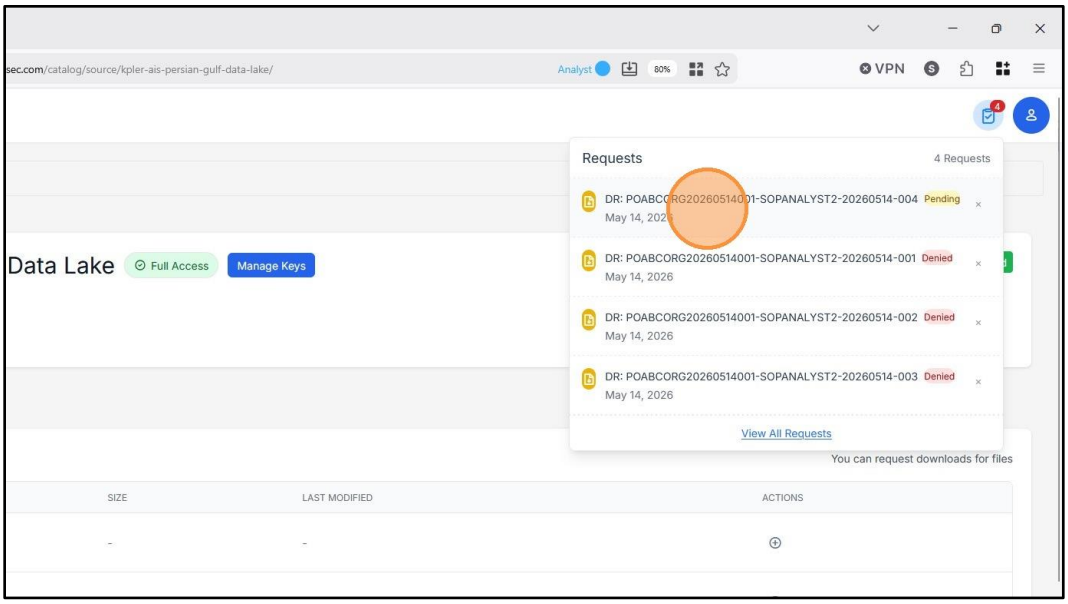
9.5 Track Approval and Download the Approved File

Step 1. Open the notifications menu to view the status of the bulk download request.



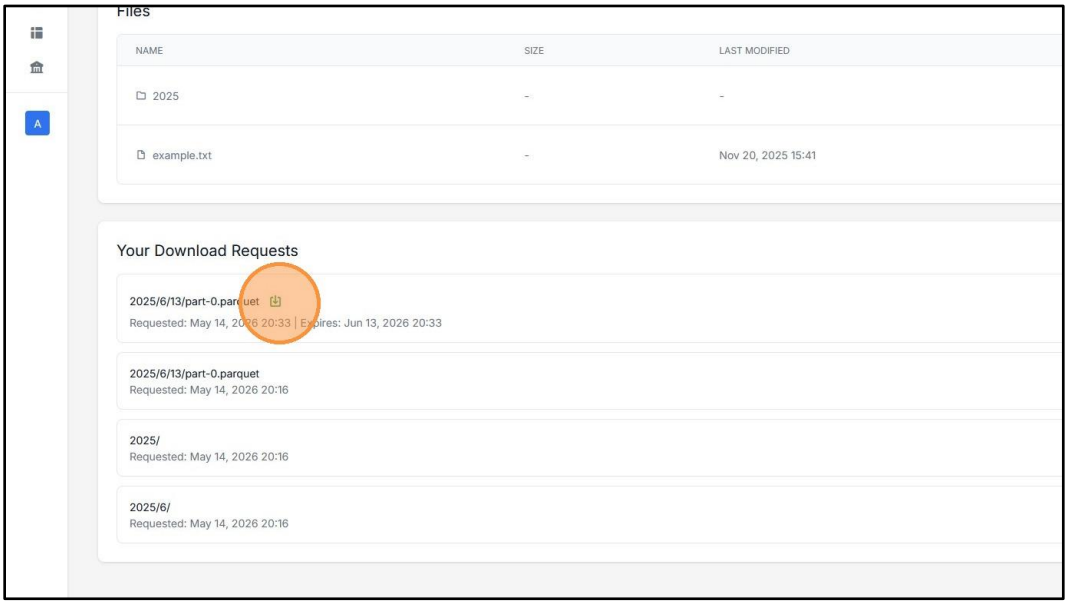
Bulk Data Screenshot 21 - Open the notifications menu.

Step 2. Select "View All Requests" to review submitted requests and their current status.



Bulk Data Screenshot 22 - View all submitted requests.

Step 3. After the Org Admin approves the request, refresh the page if needed. Return to the download request and click the green download button to download the approved file.



Bulk Data Screenshot 23 - Download the approved file.

9.6 Bulk Data Handling Notes

- Bulk data files may be large. Confirm local storage, network bandwidth, and approved storage location before downloading.
- Parquet files typically require tools such as Python, Spark, DuckDB, Power BI, or other data analysis tools capable of reading columnar data.
- Do not share downloaded data outside approved users, organizations, or systems. Follow all classification, licensing, and handling restrictions associated with the data source.

- If a credential is lost or potentially exposed, create a new credential set and revoke or rotate the prior credential according to platform policy.
- If a file download request remains pending, contact the Org Admin with the resource name, requested file path, and request number.

10. Using Platform Chat for Queries

Once the user has been granted access to one or more data sources or APIs, the home-screen Platform Chat (Platform Chat) can be used to ask natural-language questions across granted resources.

10.1 What Platform Chat Can Do

- Answer questions about what data is available to the user (e.g., "What data do I have from this <vendor name>?").
- Query specific data sources by name or topic.
- Identify which of the user's granted APIs or data sources contain the information needed for a given task.

10.2 What Platform Chat Cannot Do

Platform Chat only operates against resources the user has already been granted access to. It will not return results from resources that exist in the catalog but have not yet been requested and approved. To discover and request new resources, use the Catalog (see Sections 6, 7, 8, and 9).

10.3 Asking a Question

Step 1. From the home screen, click in the Platform Chat and type the question.

Step 2. Submit the question. The platform responds with relevant data, source citations, and follow-up suggestions where applicable.

Example question: "I want to know what data I have available from a particular vendor I have access to." The response identifies the matching data sources and summarizes what each provides.

11. Organization Administrator Workflows

This section covers tasks performed by Organization Administrators (Org Admins). Users without admin privileges will not see these options.

11.1 Accessing the Org Profile

Step 1. From the left-hand navigation, click the Org Profile entry (labeled with the organization name).

Step 2. The Org Profile page exposes the following tabs:

- About organization details, including name, description, and contact information.
- Metrics usage and activity statistics for the organization.
- Members list of all current members of the organization.
- Invites list of pending invitations and the entry point for sending new ones.

11.2 Inviting and Creating Users

Step 1. Where enabled by platform policy, from the Org Profile page, open the Members tab (or the Invites tab) and click "Create User". For ODNI/ICDC account provisioning, follow the agency POC process in Section 4 and Appendix A.

Step 2. Complete the user information:

- Full Name the user's display name.
- Username the unique identifier the user will sign in with.
- Email the email address where the invitation will be sent.
- Role either Admin (full org-admin privileges) or Member (standard user).

Step 3. Submit the invitation. The invited user receives instructions to complete account setup at the email address provided.

11.3 Reviewing and Acting on Access Requests

When a user in the organization submits an access request (for a data source, platform, or API), the request is routed to all Org Admins for that organization.

Step 1. Pending requests appear on the clipboard / notifications icon in the top right of any platform page.

Step 2. Click the icon to open the queue of pending requests. Each request displays the requesting user, the resource requested, the access type, and the justification provided.

Step 3. Open the request and choose one of the following:

- Approve grants the requested access to the user.
- Reject declines the request.
- Add a reason optional but recommended, particularly for rejections and conditional approvals. The reason is visible to the requesting user.

Step 4. Submit the decision. The decision is recorded with a timestamp and is visible to both the Org Admin and the requesting user. The user is notified of the decision.

11.4 Decision Criteria

Org Admins should evaluate each request based on:

- Usage need does the user's role require this resource?
- Relevance does the resource align with the organization's mission and current work?
- Capacity does the organization have the seats, quota, or budget to support the request?

12. Troubleshooting and Common Edge Cases

Use this section when the happy-path workflow does not behave as expected. Most issues fall into one of four categories: pending approvals, session capacity, credential handling, or resource entitlement.

12.1 Approval and Entitlement Issues

- Request still pending Check the notifications icon. If the request is mission-critical, contact the Org Admin with the request number and justification.
- Request denied Review the rejection reason. If appropriate, resubmit with a clearer mission need, timeframe, and expected use.
- Resource appears in Catalog but not in My Data Sources The resource may exist in the catalog but not be entitled to the user or organization. Submit the correct access request or ask an Org Admin to confirm entitlement.

- Platform Chat returns no results Confirm the user has access to the relevant resource, then rephrase the question with a specific data source, vendor, topic, or time range.

12.2 Workspace Session Issues

- Workspace will not launch Allow pop-ups for the platform URL, refresh the session page, and try Launch Workspace again. Contact support if initialization fails repeatedly.
- No workspace seats available All sessions may be checked out by other users. Wait for a session to be returned or ask an Org Admin to review seat capacity and active checkouts.
- Workspace closed but seat still unavailable Closing the browser tab does not return the session. Return to the session details page, click Destroy Workspace if needed, then click Return to check the session back in.

12.3 API Key and Access Issues

- API key lost Generate a new key. If the old key may still be active, revoke or rotate it according to platform policy.
- API key expired Generate a new key with an appropriate expiration date and update approved clients or scripts.
- API returns 401 Unauthorized Confirm the Authorization header uses the format Bearer <access_key> and that the key has not expired.
- API returns 403 Forbidden Confirm the request was approved for the correct data source/API and that the endpoint is within scope.

12.4 Escalation Information to Capture

If a problem is not resolved by the actions above, capture the resource name, request number, username, approximate time of the error, browser type, and a screenshot that does not expose API keys or sensitive data. Provide that information to platform support or the designated Org Admin.

13. End-to-End Reference Summary

From a user's perspective, the typical end-to-end journey is:

1. Log in to the platform using credentials provided by the Org Admin.
2. Land on the home screen Platform Chat in the center, catalog tile, sidebar navigation on the left.
3. Browse the catalog to discover available data sources, platforms, and APIs.
4. Request access to the desired resource via the appropriate workflow (data source, workspace session, or API).
5. Wait for Org Admin approval. Track status via the top-right notifications icon.
6. Consume the resource once approved (open the data source, check out a workspace session, generate an API key, or download an approved bulk data file).
7. Use the home-screen Platform Chat to ask natural-language questions across all granted data sources and APIs.
8. Return any checked-out session-based access when finished so the seat is freed for others.