

Troubleshooting CILogon Authentication for the ATAP BinderHub

Alex Ip, AARNet Pty Ltd – November 20, 2023

The BinderHub for the LDaCA (Language Data Commons of Australia) ATAP (Australian Text Analytics Platform) at <https://binderhub.atap-binder.cloud.edu.au/> uses CILogon for authentication because of its support for non-Australian institutions. CILogon (<https://www.cilogon.org/>) is an Integrated Identity and Access Management Platform for Science, providing federated identity management for institutions around the world. We need to authenticate users to mitigate the risk of malicious users abusing the resource and to ensure that the service remains sustainable.

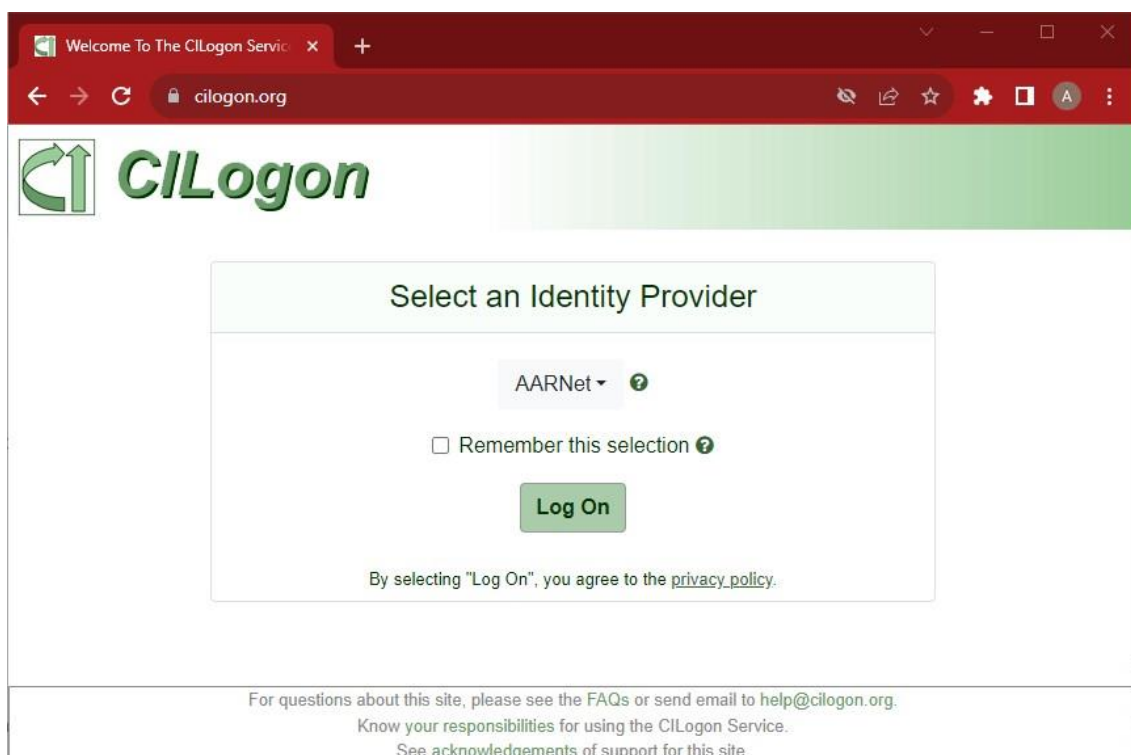
If you have any issues authenticating with the LDaCA ATAP BinderHub it is most likely an issue between your institutional IDP (Identity provider) and CILogon. In most cases, it is because the institutional IDP does not provide all of the necessary information, and action will be required by the institution's IT department. In other cases, notably within China, access to the CILogon endpoint in the US may be blocked for the user's location.

Testing CILogon

CILogon has provided a test page to help diagnose issues with specific institutional logins. Please follow the instructions below if you experience any issues authenticating with the LDaCA ATAP BinderHub.

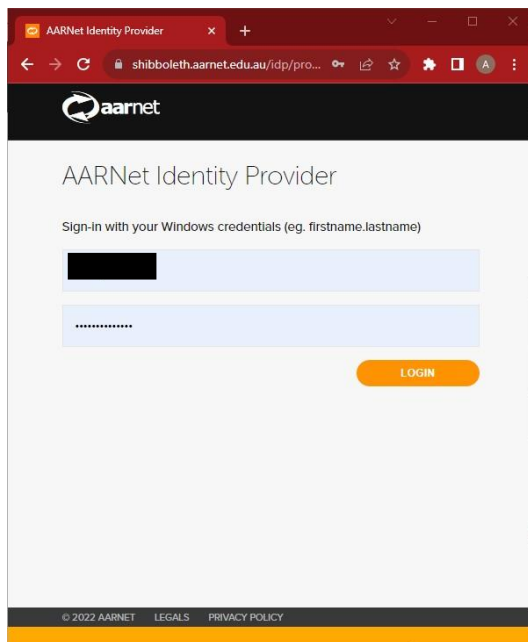
To test CILogon authentication and obtain diagnostic information, you will need to visit the CILogon test page at <https://cilogon.org/> and log in using your institutional credentials. If you are unable to access the test page, then the issue is almost definitely because access to CILogon is blocked from your location, and we are unable to assist. In such cases, you may need to raise the matter directly with your institution.

Step 1: Visit the CILogon test page at <https://cilogon.org/> and choose your institutional identity provider from the drop-down menu (AARNet is the selected IDP in the example below)

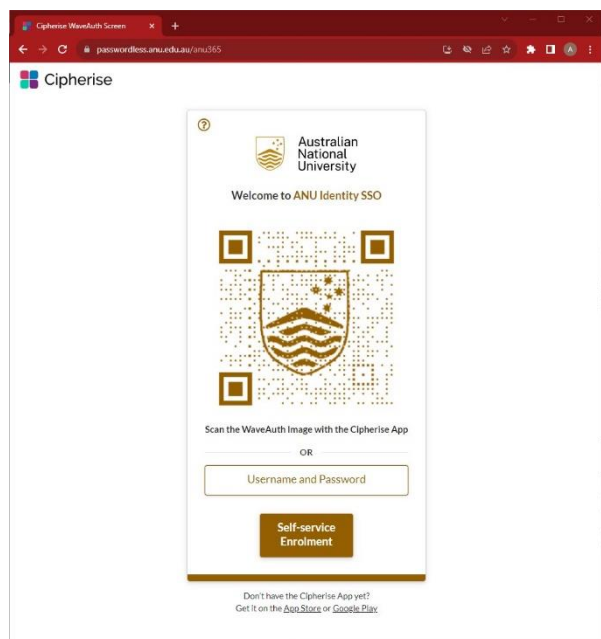


The screenshot shows a web browser window with the address bar displaying 'cilogon.org'. The page features the CILogon logo at the top left. Below the logo is a green header bar. The main content area is titled 'Select an Identity Provider'. It contains a dropdown menu with 'AARNet' selected, a checkbox for 'Remember this selection', and a green 'Log On' button. Below the button, a line of text states: 'By selecting "Log On", you agree to the [privacy policy](#).' At the bottom of the page, there is a footer with the following text: 'For questions about this site, please see the FAQs or send email to help@cilogon.org. Know your responsibilities for using the CILogon Service. See acknowledgements of support for this site.'

Step 2: Enter your institutional credentials, noting that the screens and procedures will vary according to your institution's implementation. There may also be a requirement for 2FA (Two-Factor Authentication). Below are two examples of institutional login screens.

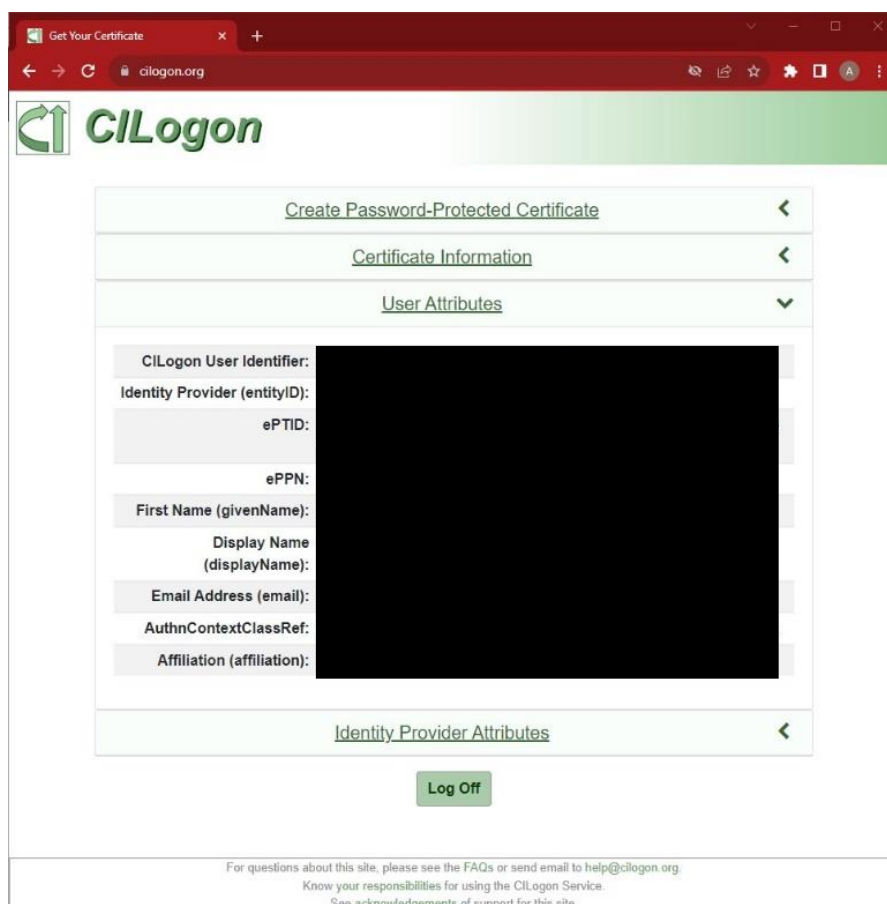


The screenshot shows the AARNet Identity Provider login page. The browser address bar displays 'shibboleth.aarnet.edu.au/idp/pro...'. The page features the AARNet logo and the text 'AARNet Identity Provider'. Below this, it says 'Sign-in with your Windows credentials (eg. firstname.lastname)'. There are two input fields: one for the username (containing a redacted name) and one for the password (containing a redacted password). A yellow 'LOGIN' button is positioned below the password field. At the bottom of the page, there is a footer with '© 2022 AARNET', 'LEGALS', and 'PRIVACY POLICY'.



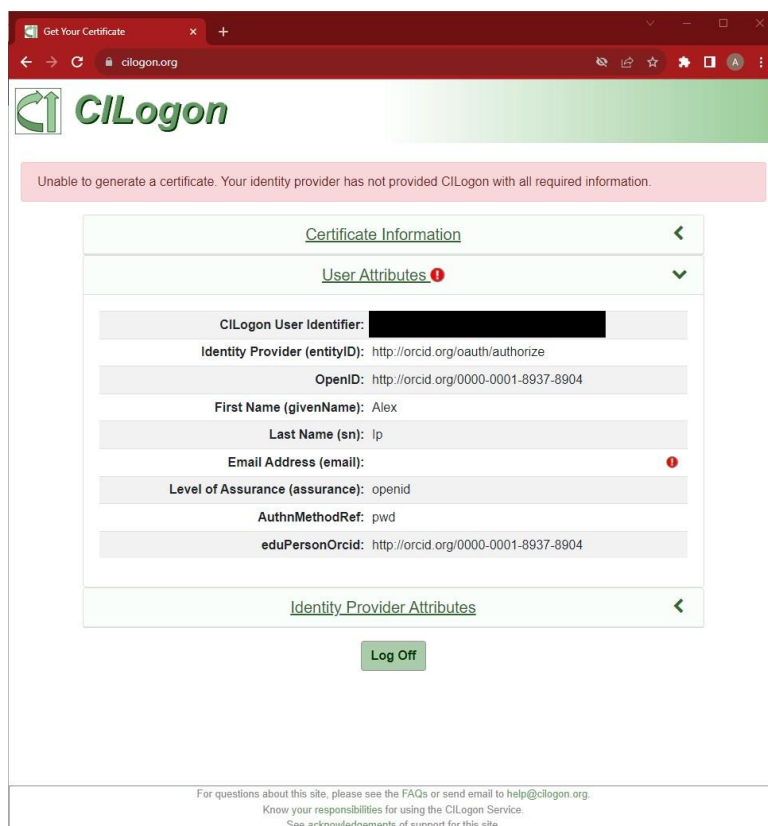
The screenshot shows the CIPHERISE WaveAuth screen for the Australian National University (ANU). The browser address bar displays 'passwordless.anu.edu.au/anu365'. The page features the ANU logo and the text 'Welcome to ANU Identity SSO'. It displays a large QR code (WaveAuth Image) and a prompt to 'Scan the WaveAuth Image with the Cipherise App'. Below the QR code, there is an 'OR' option and a 'Username and Password' input field. A yellow 'Self-service Enrolment' button is located at the bottom. At the very bottom, there is a note: 'Don't have the Cipherise App yet? Get it on the [App Store](#) or [Google Play](#)'.

Step 3: After a successful institutional authentication, check for any red exclamation mark icons indicating problems. Below is an example of a successful authentication with AARNet (details redacted)



The screenshot shows the CILogon 'Get Your Certificate' page. The browser address bar displays 'cilogon.org'. The page features the CILogon logo and a navigation menu with the following items: 'Create Password-Protected Certificate', 'Certificate Information', 'User Attributes', and 'Identity Provider Attributes'. The 'User Attributes' section is expanded, showing a list of attributes: 'CILogon User Identifier:', 'Identity Provider (entityID):', 'ePTID:', 'ePPN:', 'First Name (givenName):', 'Display Name (displayName):', 'Email Address (email):', 'AuthnContextClassRef:', and 'Affiliation (affiliation):'. All the values for these attributes are redacted with a black box. At the bottom of the page, there is a 'Log Off' button. The footer contains the text: 'For questions about this site, please see the FAQs or send email to help@cilogon.org. Know your responsibilities for using the CILogon Service. See acknowledgements of support for this site.'

If you see any red exclamation mark icons, open the section(s). Below is an example where the ORCID IDP does not provide an email address¹. The red exclamation mark appears on the “User Attributes” section, and, within that, against the “Email Address (email)” field.



The screenshot shows a web browser window with the address bar displaying 'cilogon.org'. The page title is 'Get Your Certificate'. Below the CILogon logo, a pink message box states: 'Unable to generate a certificate. Your identity provider has not provided CILogon with all required information.' The main content area has a green header with 'Certificate Information' and a green arrow pointing left. Below this is a green header with 'User Attributes' and a red exclamation mark icon. The 'User Attributes' section contains a list of fields: 'CILogon User Identifier' (redacted), 'Identity Provider (entityID): http://orcid.org/oauth/authorize', 'OpenID: http://orcid.org/0000-0001-8937-8904', 'First Name (givenName): Alex', 'Last Name (sn): Ip', 'Email Address (email):' (with a red exclamation mark icon), 'Level of Assurance (assurance): openid', 'AuthnMethodRef: pwd', and 'eduPersonOrcid: http://orcid.org/0000-0001-8937-8904'. Below the 'User Attributes' section is a green header with 'Identity Provider Attributes' and a green arrow pointing left. At the bottom of the main content area is a green button labeled 'Log Off'. The footer contains the text: 'For questions about this site, please see the FAQs or send email to help@cilogon.org. Know your responsibilities for using the CILogon Service. See acknowledgements of support for this site.'

If you observe any red exclamation marks, please take complete screenshot(s) of the offending section(s) and forward them to your contact at LDaCA or directly to alex.ip@aarnet.edu.au or steele.cooke@aarnet.edu.au so that we can pass them on to CILogon to raise with your institution.

FAQs

Why does my institution appear in the IDP list, but I am still unable to log in?

Having an institution appear in the list of CILogon IDPs when it doesn't work does raise the reasonable expectation that it can be used to authenticate when in fact it can't. The reason is that the institutions listed are most likely provided via third-party identity federations (such as AAF for Australia), and there is no way for CILogon to test the correctness of individual IDPs without having institutional credentials and testing from every possible user location.

What can I do while I am waiting for my institution to address the issue?

- If you have a Google account, you could try selecting Google as your IDP. Alternatively, you can sign up for a free ORCID and use that. These IDPs have both been tested and are known to work.

¹ Ordinarily, the lack of an email address would result in an authentication failure in the LDaCA ATAP BinderHub, but we have implemented a specific exemption for ORCID to allow its use.

- There is a free BinderHub available at <https://mybinder.org/> - it may not provide the same resources as the LDaCA ATAP BinderHub, but it may be sufficient for your needs.
- In the future, we may be able to provide instructions on how to run the notebooks in a Docker container on your local computer.

I have further questions – whom can I contact?

Please direct queries to alex.ip@aarnet.edu.au or steele.cooke@aarnet.edu.au. Please provide as much detail as possible, including your institution name, your username, and the approximate time of your authentication failure so we can inspect the BinderHub logs.