User authentication service for XSEDE science gateways

Version 1.1
May 10, 2017

This is an introduction to the user authentication service that XSEDE offers for science gateway developers and operators. This service provides a user "login" function so that gateway developers don't need to write their own login code or maintain user password databases.

Contents

Purpose

Science gateways that use XSEDE services are required to report on the number of researchers who use them, and--in certain situations, notably, security incidents--to be able to provide information about specific users and their activities within the gateway. Gateway developers and operators may use any method they like to do this, but XSEDE provides services intended to make this task easier.

XSEDE's authentication service is an option available to gateway developers and operators. It provides a "login" user interface that the gateway can present to its users. It provides the gateway with a specific, authenticated user identity that the gateway can then use for tracking use and authorizing access to specific gateway features. This service offer several benefits to gateway developers, gateway operators, and gateway users.

- It relieves the gateway developer and operator from managing a user database.
- It simplifies the code required for user authentication in the gateway.
- It helps XSEDE and gateway developers jointly maintain a consistent level of quality in our security interfaces.
- It enables researchers to use existing identities (their campus credentials, for example) to login to the gateway instead of setting up brand-new identities.
- Existing identities (e.g., campus credentials) are generally more reliable than identities established solely for use with a gateway, so encouraging their use improves our overall security.
- When researchers use existing identities to authenticate to a gateway, it helps us (and our sponsors) understand the relationship between people who use the gateway and people who use other services (other gateways, XSEDE services, campus services).

This document describes XSEDE's authentication service and provides references for getting started using it. *This is not the "how to" documentation!* Please use the references provided to learn how to use XSEDE's authentication service in a science gateway.

XSEDE's authentication service

In 2016, XSEDE began offering a public authentication service based on the popular OAuth 2.0 (OAuth2) [1] and OpenID Connect 1.0 (OIDC) [2] interfaces. This service allows other services (including science gateways) to register and authenticate users without maintaining a local user database or writing significant code. It supports the InCommon federation to which many academic and research organizations belong, and it also supports identities issued by other major research service providers, including NERSC/DOE, NIH, Google, and ORCID. Client SDKs and APIs are public, open source, and used and supported by a wide community of developers. XSEDE itself uses this service for the XSEDE User Portal (XUP).

XSEDE's authentication service is provided by Globus Auth [3], one of several services offered by Globus at the University of Chicago. In combination with a few supporting services, Globus Auth and XSEDE are able to offer user authentication services to science gateways, campuses, XSEDE and other service providers.

Globus Auth and XSEDE

Globus Auth is the primary authentication interface offered by XSEDE for use by external services. Globus Auth provides the ability to authenticate individual identities and to register new identities. A familiar way to think of this is as a "Login with X" service (e.g., "Login with Google" or "Login with Facebook"), where "X" can be any of several hundred academic and research organizations and public services. An important "X" is, of course, XSEDE itself, which has a registered user community of more than 20,000 individuals who have used XSEDE services (and their predecessors) directly. Another 30-40,000 individuals use Globus via other organizations, which means that more than 50,000 individuals can already authenticate with Globus Auth without re-registering. New registrations are very easy for researchers, and usually involve linking to an existing campus user identity. XSEDE requests additional information--particularly for individuals who are not at participating institutions--but science gateways are not required to collect this information.

Science gateways can use Globus Auth at no cost. Science gateways must register with Globus Auth to use the authentication service. Most gateways will be able to use Globus Auth's free services for as long as the gateway needs them and will not need to directly use any of the additional supporting services offered by XSEDE. For gateways with specialized needs, both XSEDE and Globus offer further services.

Documentation on how to use Globus Auth is available online at **https://docs.globus.org/api/auth/**. [4] The service is operated and supported by the University of Chicago. University of Chicago is an XSEDE partner and an XSEDE service provider. Funding for Globus is provided by subscriptions from colleges, universities, and major research service providers, and in part by federal grant funding. Globus's services are not dependent on XSEDE for ongoing support.

Other supporting services

Globus Auth supports applications and gateways that are able to use an OAuth2 or an OIDC mechanism. Most development frameworks, and even many public applications, have OAuth2 or OIDC "plugins," modules, or libraries that can be easily imported to support Globus Auth. For applications with more specialized needs, XSEDE provides several supporting services. All of these are available for use by research applications and gateways at no cost.

- Applications and gateways that already work with InCommon's SAML-based mechanism [5] can use idp.xsede.org [6] to authenticate individuals who have registered with XSEDE. The idp.xsede.org service is an InCommon identity provider for XSEDE, supporting the SAML authentication interface used in the InCommon federation.
- Applications and science gateways that need access to XSEDE-issued X.509 certificates (presumably because they use other services that only support X.509) can use OAuth for MyProxy (OA4MP) [7], which offers X.509 certificates for researchers who have registered with XSEDE.
- Finally, both XSEDE and Globus Auth use the CILogon service [8], provided by the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign, to allow Globus Auth to work with the InCommon federation. Applications and gateways do not need to use CILogon directly because it is already integrated with Globus Auth, but users at InCommon organizations will see CILogon when they authenticate with Globus Auth.

Globus Auth itself also offers specialized services via a subscription model. Most science gateways will not need these services as they are intended for research institutions or large research service providers.

- Applications that must provide a seamless user interface--with their own "look and feel" and Internet domain throughout the entire login process--can be supported via a subscription.
- Applications that need to support an existing user database that isn't already accessible via InCommon, OAuth2, or OIDC can be supported with a subscription.

Further technical details regarding XSEDE's public authentication services are available [9], but these are intended solely for the purpose of informing future design and development work.

Get started

To get started using XSEDE's authentication service in a science gateway or other application, you will first need to identify the specific development or portal framework you are using in your Gateway, or possibly the development language it uses. Then, search the documentation for your framework (or search the Web) to find an existing OIDC or OAuth2 plugin, module, or library that you can use. If you do not find a way to support OIDC or OAuth2 in your web application, look for one for the programming language you are developing in.

In many cases, you won't need to write any code yourself and will merely need to add OIDC or OAuth2 support to your web application, register it with Globus Auth to obtain client credentials, and configure it to use Globus Auth and the credentials you received. These steps are described and documented in the Globus Auth documentation. [4]

If neither OIDC nor OAuth2 are supported by your gateway but InCommon/SAML/Shibboleth or X.509 are, see the section above on supporting services to identify the service offering that interface. Instructions for using these services are available on their websites.

Finally, if you have questions or need help with the instructions provided in these references, contact us at help@xsede.org.

References

[1] https://en.wikipedia.org/wiki/OAuth

[2] https://openid.net/connect/

[3] S. Tuecke *et al.*, "Globus auth: A research identity and access management platform," *2016 IEEE 12th International Conference on e-Science (e-Science)*, Baltimore, MD, 2016, pp. 203-212. DOI=10.1109/eScience.2016.7870901. (https://www.globus.org/sites/default/files/GlobusAuth.pdf)

[4] https://docs.globus.org/api/auth/

[5] https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[6] https://www.xsede.org/security/incommon

[7] https://oa4mp.xsede.org/oauth2/

[8] http://www.cilogon.org/

[9] "Technical overview of XSEDE public authentication services." Technical report, version 1.1, June 29, 2017. (http://hdl.handle.net/2142/97880)