XSEDE Web SSO Service Overview

This document provides an overview of the information and resources available for XSEDE's Web Single Sign-On (Web SSO) service. Links are provided for each resource.

Table of contents

Intended uses

XSEDE's Web Single Sign-On (Web SSO) service is described in the Web SSO design document (Section C: System overview). *The remaining text in this section is an excerpt from the design document.*

XSEDE's Web Single Sign-On (Web SSO) service offers XSEDE users **a uniform and consistent process to sign-on to multiple applications**. These applications include: the XSEDE User Portal, the Community Software Repository, science gateways, training websites, and potentially more as time passes and the community grows.

When a user wishes to sign on to an application, the application directs the user to the Web SSO service. The Web SSO service allows the user to securely authenticate--using an identity provider of the user's choice--and returns an XSEDE identity to the calling application. The application can then use the identity to provide a personalized user experience, including access control (authorization) decisions. Meanwhile, the Web SSO service maintains a sign-on session for the user that is used when the user signs on to other Web SSO applications, until the user explicitly signs off.

XSEDE's Web SSO service provides a number of significant features described in use case CAN-06 and its related use cases, which include: IDM-02, IDM-04, IDM-05, IDM-06, IDM-07, CB-01, and SGW-01.

- Users can sign on to applications either using their XSEDE username and password or using the authentication services from InCommon and eduGAIN members (academic institutions), ORCID, Google (provider of G Suite, used by many academic institutions), and national/international research facilities.
- If a user has recently signed on to a Web SSO-enabled application and hasn't signed off, other Web SSO applications can allow the user to sign on without re-authenticating.
- Users can link their own identities from multiple institutions, enabling applications using the Web SSO service to make authorization decisions based on a user's full set of identities.
- Users' private credentials (passwords, one-time tokens, etc.) are never exposed to the Web SSO service or applications that use the Web SSO service.
- Applications can require users to register with XSEDE (obtain an XSEDE identity) before they are able to sign on, allowing the application to always receive XSEDE identity data regardless of the IdP used for authentication.

Figure 1 shows two different people using an application that uses the Web SSO service. One person uses the University of Washington to authenticate, while the other uses ORCID. The application is configured to require an XSEDE identity. (This is the recommended configuration for XSEDE applications.) Because both users previously linked their XSEDE identities in the Web SSO service, the service is able to give the application their XSEDE identities, simplifying the application's user management.

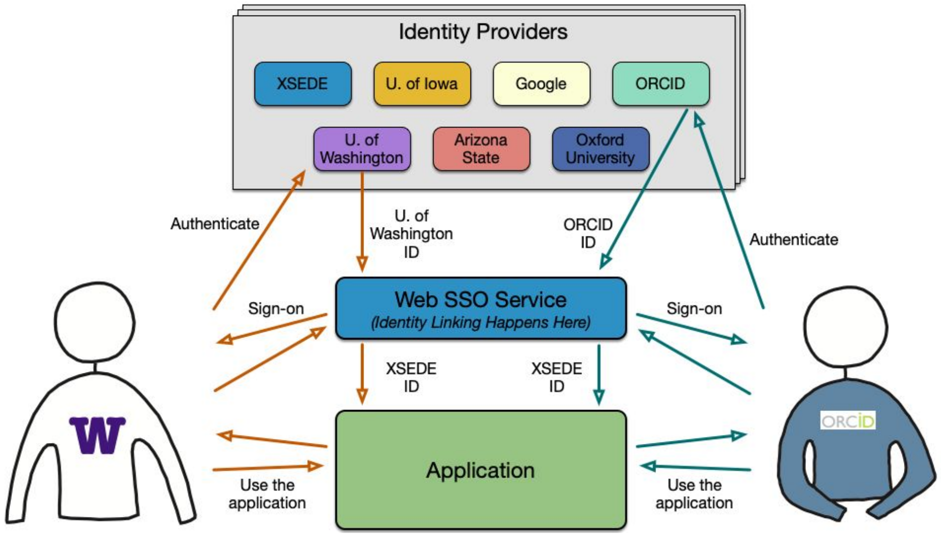

Figure 1. Overview of XSEDE's Web SSO service showing two users and one application.

Details of the application developer's experience and the application user's experience are described in the design document for the Web SSO service.

Service design

XSEDE's Web SSO design document provides a comprehensive design for the service. It provides the following design elements.

- Purpose and intended features, including:
  - intended interactions with applications
  - intended user sign-on experience
  - important security requirements and other constraints
- Implementation, including:
  - identity data returned by the service
  - relationship between the service and IdPs
  - supporting elements (e.g., documentation, technical support) included with the service

User and developer documentation

XSEDE's documentation for application developers covers the following topics.

- Description of the Web SSO service (key features, behaviors)
- The "Login with XSEDE" interface element
- Application registration (how-to, important settings)

- Guidelines for using XSEDE identity claims
- Notifying XSEDE support staff about new applications
- How to get technical support for the Web SSO service
- References to Globus Auth Developer's Guide and API Reference
- Reference to Globus Auth Python SDK
- Reference to Globus Auth developer tutorial materials

XSEDE's documentation for **application users** (not yet available) will appear on the XSEDE User Portal in a form suitable for reference in application documentation. It will cover the following topics.

- Recognizing the "Login with XSEDE" button
- Choosing an IdP
- How signing on (or off) affects other Web SSO applications
- How and why to link identities
- How to view your identity data and application permissions

The following Globus documents describe the Globus Auth service in detail.

- Globus Auth API documents (index page)
- Globus Auth API Reference
- Globus Auth Specification
- Globus Auth Developer Guide

Developer tools

The Web SSO service provides a standard OpenID Connect 1.0 (OIDC) interface. OIDC builds on OAuth 2.0, so the Web SSO service also provides a standard OAuth 2.0 interface. This means that all existing open source and commercial OIDC clients, plug-ins, modules, and software development kits (SDKs)–and many OAuth 2.0 ones as well–should work with the Web SSO service with appropriate configuration settings. However, neither XSEDE nor Globus can verify the quality or guarantee the usability of software from other providers.

Globus provides the following downloadable software for use with Globus Auth. Support for each of these is available via the XSEDE Help Desk (support@xsede.org), provided by Globus team members who participate in the help desk activity.

- A Python SDK for Globus Auth that serves as an excellent starting point for application developers using Python.
- A collection of Jupyter notebooks--used frequently in tutorials--that demonstrate use of Globus Auth.
- A Python command-line interface (CLI) that includes basic Globus Auth features.

XSEDE provides the XSEDE Globus ID Explorer application (see description below), which allows application developers and application users to view and manage their identity data and application permissions in the Web SSO service. Application developers can see the JSON data structures returned by specific interfaces. The source code for this application provides good example code.

Support resources

In addition to the documentation and developer tools mentioned above, the following additional resources and services are available to support the Web SSO service.

XSEDE Help Desk

The Web SSO service is supported by Globus team members who participate in the XSEDE Help Desk (support@xsede.org). Application developers and application users who need help with the Web SSO service should send email to support@xsede.org. Help Desk personnel should assign Web SSO tickets to the Globus members of the Help Desk team.

Integration tracking

XSEDE's XCI team maintains a set of application integration notes that describes how individual applications use the Web SSO service. These notes include the client interface used, configuration settings, and any identity mapping details. The purpose of these notes is to help Globus team members on the Help Desk debug Web SSO service issues with specific applications.

XSEDE Globus ID Explorer

XSEDE provides the XSEDE Globus ID Explorer application, which allows XSEDE users to view and manage their identity data and application permissions in the Web SSO service.

Preview environment

Globus provides a preview environment in which the next version of the Auth service is available for application testing. Application developers can register and test their applications in the preview environment the same as they do in the primary environment. The Globus Preview environment and instructions for its use are described at https://docs.globus.org/how-to/preview/.

Developer email list

Globus provides an email list for application developers: developer-discuss@globus.org. Significant changes to the Globus Auth service are announced ahead of time on this list. The list is also available for Q&A with the Globus team. The list's archive and instructions for joining the list are available at https://www.globus.org/mailing-lists.

Continuity service for application registrations

Applications that use the Web SSO service must be registered. This registration is part of the ongoing maintenance for the application. The registration interface allows multiple administrators of registrations, so if the original developer leaves the application in someone else’s care, the new person can continue using the application’s registration.

XSEDE’s XCI team provides a Globus identity, **xsede@globusid.org**, that can be added as an administrator for application registrations. Adding this identity as an administrator for an application ensures that XCI staff will be able to recover the application’s registration if/when the original developer changes jobs without assigning new project managers.

Service usage data (work in progress)

Globus and XSEDE are preparing to collect usage data for XSEDE’s Web SSO service. Specifically, Globus is preparing to deliver Globus Auth usage data to XSEDE for XSEDE’s registered applications.

Q: Why is XSEDE collecting usage data for Globus Auth?
A: XSEDE has been asked by NSF to collect usage data for *all XSEDE services* in order to better understand the ROI (return on investment) for each service. In a nutshell, NSF and its peer review panels want to be assured that each XSEDE service is worth the funds and effort spent on it. Globus Auth is one of these services, so NSF is interested in its use.

Q: What data is collected?
A: For Globus Auth, XSEDE obtains usage records from Globus. Each record contains a timestamp, an identifier for the application being logged into, and the XSEDE username that logged into the application. No other details are included.

Q: Isn't this private data? It includes Personally Identifiable Information (PII).
A: Yes, the data contains XSEDE usernames, which are PII. The XSEDE Acceptable Use Policy (AUP)–which all XSEDE users must acknowledge at least once a year–states that user identities and usage data will be shared among XSEDE partners for the purpose of operating the system. XSEDE and its predecessors have been collecting this data for decades from allocated XSEDE resources (computation & data services). XSEDE manages this data very carefully to avoid disclosure. Now, at NSF's request, we're extending usage data collection to cover other parts of the XSEDE system.