XSEDE Web SSO for Application Developers

Version 1.0

The Web SSO service

The XSEDE Web SSO service offers XSEDE users **a uniform and consistent process to sign on to applications**. It is intended to be used by the XSEDE User Portal, science gateways, training websites, the Community Software Repository, XSEDE staff applications, and any application that is part of the XSEDE user experience.

When a user wishes to sign on to an application, the following happens.

1. The application directs the user to the Web SSO service.
2. The Web SSO service allows the user to securely authenticate using an identity provider of the user's choice (this may or may not be XSEDE).
3. The Web SSO service returns an XSEDE identity to the calling application.
4. The application can then use the XSEDE identity to provide a personalized user experience, including access control (authorization) decisions.
5. 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.

Beyond the sequence above, the Web SSO service provides the following significant features.

- Users are able to use their XSEDE username and password to sign on with applications.
- Users are able to use their identities from InCommon and eduGAIN member institutions and other academic/research organizations to sign on with applications.
- Applications always receive XSEDE identity data regardless of the IdP used for authentication. Users who haven't already registered with XSEDE or linked an XSEDE identity are directed to do so as they sign on.
- If a user has recently signed on to a Web SSO-enabled application and hasn't signed off, the user may sign on with other Web SSO applications without re-authenticating.
- Users can link their own identities from multiple institutions, enabling applications 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 to applications that use the Web SSO service.

Figure 1 shows two different people using an application that uses the XSEDE Web SSO service. One person uses the University of Washington to authenticate, while the other uses ORCID. Because both users previously linked their XSEDE identities in the Web SSO service, the application receives their XSEDE identities. (The application can access data from the user's other identity providers with the user's permission.)

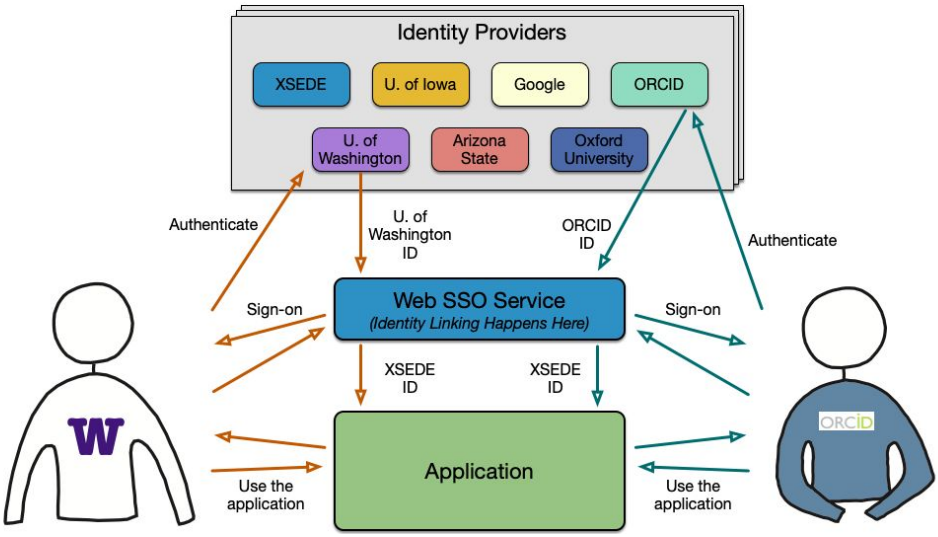

Figure 1. Overview of XSEDE's Web SSO service showing two users and one application.

The XSEDE Web SSO service relies heavily on an existing Web SSO system, Globus Auth. Globus Auth is a service of the University of Chicago. Because XSEDE has selected Globus Auth to be its Web SSO service provider, applications that use the XSEDE Web SSO service, in effect, use Globus Auth. However, XSEDE adds several elements and procedures that customize the Globus Auth experience for application developers and for users.

Globus is responsible for managing the user experience for XSEDE's Web SSO service for both application developers and application users. As described in the section, "How to get help," Globus participates closely in XSEDE's operations and user support activities and provides user and developer support for the Web SSO service.

The "Login with XSEDE" interface element

If your application uses the XSEDE Web SSO service, XSEDE strongly recommends that you use the "Login with XSEDE" or the "Login to XSEDE" button shown in Figure 2 as the interface to initiate sign-on. The button uses the XSEDE 'X' icon and the XSEDE white-on-navy color scheme. You may scale the button to fit your application's interface.

Figure 2. The "Login with XSEDE" and the "Login to XSEDE" buttons

The “Login with XSEDE” button is appropriate for applications that work with, but are not part of, the XSEDE system, even if there’s a strong relationship to XSEDE. We specifically recommend the “Login with XSEDE” button for Service Provider (SP) web interfaces, for science gateways, for campus services that use XSEDE, and for any other application “powered by XSEDE.”

The “Login to XSEDE” button is appropriate for XSEDE system applications, like the XSEDE User Portal (XUP).

Using the “Login with/to XSEDE” button is important for two reasons.

1. It offers a uniform user experience across applications that use the service.
2. When users see the same design element in multiple applications, it signals that these applications are using a common sign-on mechanism, so signing on (or off) with one application may affect the sign-on status in other applications that display the same element.

The second point is important: when your users sign on to your application (or sign off!), it will affect the behavior of other applications that use the Web SSO service. Giving the user a hint via a common user interface element that a common service is being used will help avoid confusion.

The two examples below show how this button can be used in the XSEDE user portal and other XSEDE applications.

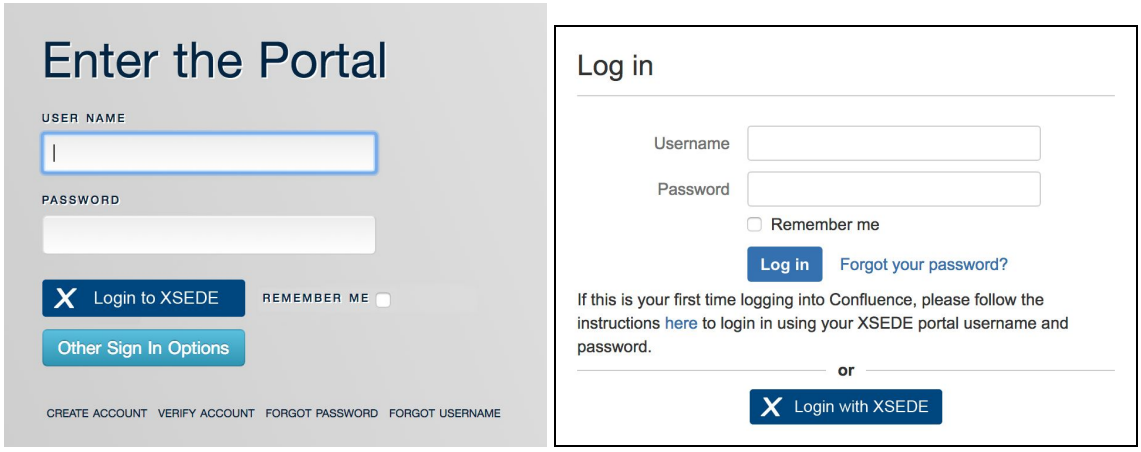

Figure 3. Two examples of the “Login to/with XSEDE” button

If possible, your application should also indicate the user’s signed-on status by displaying the username, especially if your application uses the XSEDE username as described below in “Elements of an XSEDE identity.” This will also help users understand that their sign on session is related to XSEDE.

How it works

To adapt an application to use the Web SSO service, you'll follow these high-level steps.

1. Choose an OIDC plugin, adapter, module, or SDK.
2. Register your application.
3. Configure your OIDC plugin, adapter, module, or SDK to use the XSEDE Web SSO service.
4. If you're using an SDK, write code to obtain and use the user's XSEDE identity.
5. If you're using a plugin, adapter, or module, configure it to use XSEDE identities.

Choosing an OIDC plugin, adapter, module, or SDK

If you're developing a Web application in a development framework like Django or Flask, or if you're deploying a Web application like WordPress, Drupal, or Liferay, there's most likely a plugin or module that you can install to use the XSEDE Web SSO service. If you can't find it in the product documentation, try a Google search for "*productname* OIDC plugin". Then follow the instructions in the rest of this section to register your application and configure your plugin.

If you're writing your application from scratch, you should look for an OIDC SDK for the programming language you're using. Try a Google search for "*language* OIDC SDK" or "*language* OIDC client". Follow the instructions below to register your application, configure the SDK to use the Web SSO service, and write the code necessary to call the SDK and use the XSEDE identity data it returns.

Registering your application

Like all OIDC services, XSEDE's Web SSO service requires applications to be registered. You'll be registering your application with Globus. To register a new application, visit developers.globus.org, click "Register your app with Globus," and sign in. Next, either create a project (if this is your first Web SSO application) or select an existing one. The project allows you to organize your application registrations. You can also add other project administrators who will be able to access and manage your application registrations. (See "Continuity service for application registrations" later in this document.) Finally, click the "Add..." menu in your project and select "Add new app."

Complete the App Registration form using the instructions from the Globus Auth Developer's Guide. Be sure to follow the special XSEDE Web SSO instructions below, and don't forget to click "Create App" when you've finished filling out the form.

Special XSEDE Web SSO registration instructions:

1. When registering your application with Globus, *you must check the **Required Identity** box and select "XSEDE."* This instructs the Web SSO service to always return the user's XSEDE identity, regardless of which organization the user authenticates with. Users who haven't already registered with XSEDE or linked an XSEDE identity are directed to do so as they sign on. If you

don't enable this function when you register your application, the service won't behave as described in this documentation.

2. Check the **Pre-select Identity Provider** box and select "XSEDE." This instructs the Web SSO service to make XSEDE the default organization on your app's login page.

Configuring OIDC plugins, modules, and SDKs

The Web SSO service provides a standard OIDC interface, so it will work with existing OIDC plugins, modules, and SDKs. You'll need to configure your OIDC interface to use XSEDE's service, however. The settings in Table 1 will allow an OIDC interface to use the XSEDE Web SSO service.

OIDC setting	**Web SSO service**
Authorization endpoint	`https://auth.globus.org/v2/oauth2/authorize`
Token endpoint	`https://auth.globus.org/v2/oauth2/token`
UserInfo endpoint	`https://auth.globus.org/v2/oauth2/userinfo`
OIDC metadata URL	`https://auth.globus.org/.well-known/openid-configuration`
OIDC scopes	`"openid email profile"`
Client ID	`Obtained by registering your application (see above)`
Client Secret	Obtained by registering your application (see above)

Table 1. OpenID Connect (OIDC) configuration settings for the XSEDE Web SSO service

Using XSEDE identities in your application

The Web SSO service returns identity data as a JSON object containing name/value pairs. These pairs are called *claims*. The specific claims included in the response are determined by the Web SSO service, the XSEDE IdP, and the consents granted by the application user. (Users must provide consent for their identity data to be released to an application.) Figure 4 provides an example of this response.

In Figure 4, the claims that contain XSEDE IdP data are: name, email, organization, and preferred_username. The name, email, and organization values come from the user's XSEDE user profile. The value of the preferred_username claim is the user's XSEDE username with the suffix "@xsede.org".

```
{
   'identity_provider_display_name': 'XSEDE',
   'sub': 'b3804ef4-d274-11e5-94fb-1f2e32b95784',
   'preferred_username': 'ysvenkat@xsede.org',
   'identity_provider': '36007761-2cf2-4e74-a068-7473afc1d054',
   'organization': 'University of Illinois at Urbana-Champaign',
   'email': 'vyekkira@illinois.edu',
   'name': 'Venkatesh Yekkirala'
}
```

Figure 4. Identity claims returned by the Web SSO service

If you're using a third-party OIDC plugin, module, or SDK, it might decode the JSON object for you, returning only some of the claims. When you configure the plugin, you'll probably need to choose which of these claims will be used for the username in your application. The following claims will most likely be offered as choices: email, sub, preferred_username, and name.

Whether you're using a third-party plugin or your own code, **the preferred_username value is the best choice for uniquely identifying users in your application.** XSEDE, by policy, does not change or recycle usernames, so a given username will always refer to the same person.

When using the preferred_username claim, you may strip off the "@xsede.org" part or leave it. If you strip it off, you should take care that it actually contains "@xsede.org" and not something else. There are rare error conditions where a different IDP appears in the preferred_username value, and it will be harder to detect and resolve those conditions if you strip off the IdP domain without checking that it is, indeed, "@xsede.org".

We strongly recommend against using the email or name fields to uniquely identify users in your application. Users often change these values in their XSEDE profile and they aren't guaranteed to be unique to a single person. This will confuse your application's user database and result in a poor user experience. You can use the email, name, and organization fields as extra information about each user, as long as they are associated with a unique username.

Like the preferred_username, the sub (short for *subject*) claim is guaranteed to be unique for each user. You might have noticed, however, that the sub claim isn't listed above as coming from XSEDE. It is generated by Globus the first time the user uses Globus to authenticate to XSEDE. Other than its use in the Web SSO service, this value is unknown to XSEDE. If, at any time in the future, XSEDE changes its Web SSO service from Globus to something else, this value would become meaningless and you would need to reassign all of your users to a new identifier. It isn't likely that XSEDE or Globus will provide a migration plan for applications that use the sub claim to identify XSEDE users, so we don't recommend that approach.

The OpenID Connect (OIDC) model

XSEDE's Web SSO service provides an OpenID Connect (OIDC) authentication interface. This interface provides three different ways for applications to authenticate users, two of which are documented here. (The third method is not permitted for most applications.) Both methods result in the application gaining access to identity data about the user from XSEDE, and possibly other identity providers as well.

- **Confidential application** - By far the most common method, this is intended for web portals (hosted web applications). The application runs on a web server and the user interacts with it via a browser.
- **Native application** - Less commonly, OIDC can also be used in applications that users download and run on their own systems or access via a command line. These applications lack a browser interface, but the user will use a browser when signing on to the application. (The browser doesn't have to run on the same system as the application.)

When the user wishes to sign on, the following interactions take place. *If you're using a third-party OIDC plugin or module, all of these interactions are handled by the plugin or module and your application only sees the user identity that's returned.*

1. The application directs the user's web browser to the Web SSO service. (Native applications prompt the user to open a browser to a specific link.)
2. The Web SSO service guides the user to authenticate using an identity provider of the user's choice (this may or may not be XSEDE).
3. If the user hasn't already linked an XSEDE identity to the identity the user authenticates with, the Web SSO service guides the user to do so, including registering with XSEDE if necessary.
4. The Web SSO service requests the user's permission to release identity data to the application.
5. The Web SSO service then returns one or more tokens to the application that can be used to access the user's identity data. (For native applications, the Web SSO service gives the user a code to pass on to the application, and the application uses the code to obtain the tokens by which it gains access to the user's identity data.)

If you're using an SDK, you'll add code to your application to call the SDK for steps 1 and 5 above and to extract the resulting identity data. (Steps 2-4 are interactions between the user and the Web SSO service.) Details on the necessary code are provided with your SDK. If you're using Globus's SDK, see "Globus Auth documentation and resources" below.

Globus Auth documentation and resources

If you're using a third-party OIDC plugin or module to access the Web SSO service, you're unlikely to need the following resources. If you're writing your own code using an SDK (including the Globus Python SDK), the following references provide details on how to code applications to use the Web SSO service.

The *Globus Auth Developer's Guide* and *Globus Auth API Reference* offer general and detailed guidance, respectively, on how to develop applications using Globus Auth. Globus Auth provides XSEDE's Web SSO

service. When using these references, bear in mind that you're following the special XSEDE Web SSO instructions described in the previous section, and this affects the service's behavior.

The Globus Python SDK provides a high-level Python interface for the Web SSO service. Using the Python SDK will simplify your application code and make the interaction with the Web SSO service easier to understand and debug. The SDK Tutorial provides several simple examples that use the SDK for authentication, though it's important to notice that the examples use the native application method (for locally installed applications), as opposed to the confidential application method used by web portals.

Globus's *Modern Research Data Portal* is a design pattern used in application developer tutorials that illustrates how to develop a portal using Globus Auth and related services. It includes code, a working portal that you can install on your own server, and a narrative code walk-through explaining how the code works.

The Globus Jupyter Notebooks GitHub repository provides interactive Python examples that use Globus Auth. The examples are meant to be run in Jupyter notebooks, an interactive, web browser-based Python environment that you can install on your own system.

Finally, the GitHub repository for the XSEDE Globus ID Explorer application (see description below) provides simple, but good, example code for a web portal using the Web SSO service.

How to get help

Technical support

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.

Notify XSEDE support staff about new applications

When you get your application working with the Web SSO service, please send a brief email message to the XSEDE Help Desk (help@xsede.org) describing how your application uses the service. It will speed our response to any support questions that come up later. Please tell us the Client ID from your application registration, the OIDC plugin/adapter/module or SDK your application uses, and the specific identity claims used by the application. Please also confirm that you set the Required Identity setting to "XSEDE" as described in "Registering your application." If you mention that this information is for use by the XSEDE XCI team, it will help us record the information in the right place.

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 original 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 a project administrator for your application registrations ensures that XCI staff will be able to recover your application's registration if/when you change jobs without assigning a new project manager.

XSEDE Globus ID Explorer

XSEDE provides the XSEDE Globus ID Explorer application, 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 and identity claims returned by specific interfaces. The source code for this application provides good example code, including examples of accessing linked identities, accessing authentication events, and use of helper pages.

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/.

Globus application 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.

Please provide us feedback

We would like feedback! Please go to the URL below and let us know your experiences using these instructions and/or getting help from our team.

https://software.xsede.org/node/3099/vote