

# XSEDE Capability Delivery Plan

## CB-8: Use XSEDE SSO with campus login servers

### Last revised Mon Jan 23 2017

## Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure “CI” resources and services. A Capability Delivery Plan “CDP” is an executive summary of use case support gaps, of plans to fill those gaps with new or enhanced capabilities, and of existing operational components that already support aspects of a use case.

## Use Case Summary

A campus IT administrator allows XSEDE-registered researchers to log in to campus login servers (remote command shell) using their XSEDE usernames/passwords.

Use case document(s): <http://hdl.handle.net/2142/94821>

## CDP Summary

The functionality described in this use case is 80% supported by the operational components listed below.

Gap(s) that we currently plan to address:

- L3 Resource Login Allocations (suggested priority: high)

Gap(s) that will not be addressed at this time:

- None

Time and effort summary:

- 6 total person weeks to implement L3 Resource Login Allocations
  - 2 person weeks for setting up the L3 Resource Login Allocation process
  - 2 person weeks for SSO Hub enhancements and MyProxy configuration/testing
  - 1 person week for documentation
  - 2 person weeks for end-to-end testing

## Functionality Gaps

1. **XCI-36: L3 Resource Login Allocations** (suggested priority: high)

CB-8 specifies that the "solution should not require the campus services to participate in XSEDE

allocation processes." However, XSEDE SSO depends heavily on artifacts of the XSEDE allocation process, namely, users associated with active allocations in XCDB with AMIE packets notifying SPs of account/allocation mappings. To close this gap, we implement a new allocation type, called an L3 Resource Login Allocation, that can be easily created and managed by the campus IT administrator, without needing to follow the usual XSEDE allocation processes.

**Plans:**

- Document a process whereby interested L3 SPs create the resource in RDR for which they want to support SSO via the XSEDE SSO Hub.
- Establish a process for campus IT administrators to register their campus login server(s) using IPF.
- Establish a process for creating, via XRAS, an XSEDE Project, with the PI / Allocation Managers being the appropriate campus IT administrators and an allocation on the single campus login server resource.
- Enhance the SSO Hub to:
  - recognize researchers on L3 Resource Login Allocations as "allocated users" so it automatically creates their SSO Hub accounts
  - display and facilitate login to a dynamically configured set of login servers based on SP self registration via IPF
- Confirm that XSEDE MyProxy recognizes researchers on L3 Resource Login Allocations as "allocated users" so it issues certificates for them.
- Provide documentation for campus IT administrators on:
  - Registering an L3 Login Resource with XSEDE using IPF
  - Setting up AMIE and GSISSH on an L3 Login Resource
  - Inviting researchers to create XSEDE portal accounts and adding them to the L3 Resource Login Allocation

**System Components That Support This Use Case**

The following XSEDE operational components currently support this use case:

Component	Supported Functionality
<a href="#">AMIE</a>	The Accounting and Account Management (AMIE) system provides mappings between the user's campus identity and XSEDE identity, enabling remote login via GSISSH to the campus login server from the XSEDE SSO Hub. The campus IT administrator will need to install AMIE software on the campus login server(s) to handle AMIE packets and then the campus IT administrator will need to process the packets to create the needed account mappings (i.e., populate the local grid-mapfile used by GSISSH to map XSEDE certificate identities to local campus accounts).
<a href="#">CA Certificate Installer</a>	The campus IT administrator will need to install the bundle of XSEDE trusted CAs to enable GSISSH access.

<a href="#">GSISSH</a>	GSISSH is a Secure Shell (SSH) implementation that supports certificate-based authentication. Researchers use GSISSH to log in to campus login servers from the XSEDE SSO Hub. GSISSH requires a grid-mapfile on the campus login server that maps XSEDE certificate identities to local campus accounts.
<a href="#">IPF</a>	The campus IT administrator will register the campus login server(s) as supporting the login.remoteshell.gsi via the Resource Information Publishing Framework (IPF) so these login resources can be automatically supported by the SSO Hub.
<a href="#">MyProxy</a>	MyProxy issues certificates to XSEDE users on active allocations to enable single sign-on (SSO). To enable SSO access by campus researchers, the campus IT administrator must add those researchers to an L3 Resource Login Allocation, so they can obtain certificates from MyProxy.
<a href="#">RDR</a>	The campus HPC/HTC/storage/Viz resource must be registered as a resource in the Resource Description Repository (RDR) to enable AMIE processing.
<a href="#">SSO Hub</a>	The SSO Hub automatically creates accounts for XSEDE users on active allocations. When users log in to the SSO Hub, it loads a certificate into the user session, so they can use GSISSH to log in to XSEDE SPs and campus login servers.
<a href="#">XCDB</a>	The campus IT administrator 1) registers his/her campus login service(s) in the XSEDE Central Database (XCDB) as a resource eligible for L3 Resource Login Allocations, 2) establishes an allocation associated with that resource in the XCDB, and 3) adds researchers to that allocation. XCDB generates AMIE packets linking the researchers' campus and XSEDE identities.
<a href="#">XRAS</a>	The XSEDE Resource Allocation Service (XRAS) provides the mechanism for creating a project allocation for the campus login server.
<a href="#">XUP</a>	The XSEDE User Portal (XUP) provides the interfaces for managing accounts and allocations.