

Shibboleth - EZproxy HOW-TO

[DRAFT] [DRAFT] [DRAFT] [DRAFT]

Is this document for ME?

It is if you are a staff member at an academic institution (that uses EZProxy) who wishes to begin implementing Shibboleth access to library resources, but are unsure about what is required and what is involved.

Why this document?

By laying out the necessary pre-requisites as well as the steps involved, the hope is that this document will enable the reader to decide IF moving to Shibboleth access to library resources is feasible at his/her institution, and if it is, will provide a "cookbook" for the process.

What are the pre-requisites for integrating Shibboleth and EZproxy?

- An institution-wide (enterprise) directory service that contains information about the users for whom you wish to authorize access to electronic resources.
- An Identity management environment (policies and business practices) that governs the management of identity information for the users in the enterprise directory. This is necessary to build and maintain the trust necessary to participate in a federation such as InCommon.
- A Shibboleth IdP from which service providers (EZproxy itself, JSTOR, OCLC, Elsevier, etc) can obtain sufficient identity information about each user of their services who requests access.
- An EZproxy installation that provides authenticated remote access to library resources.
- Institutional membership in a federation such as InCommon

What are the steps?

Step 1: Configure Identity Provider (IdP) to release standard entitlement attributes (eduPersonEntitlement)

The Best Practice document, <https://spaces.at.internet2.edu/display/inclibrary/Best+Practices>, for the InCommon Federation details the standard entitlement attribute that has been agreed upon in the InCommon Federation to enable authorization for common library licensed resource contracts. In brief, the standard entitlement attribute is eduPersonEntitlement, and the standard entitlement for representing the terms of common library contracts is 'urn:mace:dir:entitlement:common-lib-terms'. More details as to the reason for this particular attribute are available in the Best Practices.

In order for resource providers to make authorization decisions based on this entitlement attribute using the Shibboleth technology and according to the Best Practices, the institution's Shibboleth identity provider must be configured to release this attribute. This step must be performed by the administrator of the institution's identity provider. The identity provider is typically not administered by the library, rather, it is usually maintained by the central IT office for the institution.

The Shibboleth identity provider can be configured with policies to release user attributes to different resource providers. These policies are referred to as attribute release policies (ARPs). The attribute release policy is the mechanism by which the IdP administrator will release the eduPersonEntitlement attribute with the common-lib-terms value. In order for the IdP administrator to configure the attribute release policy to release this attribute properly, they must know two pieces of information: 1) what users should this attribute be released for, and 2) what resource providers should this attribute be released to.

1) What users should this attribute be released for - The common-lib-terms entitlement value was established to represent the members of an institution that are included in the terms of typical library contract with a library resource provider. The interpretation may vary slightly at each institution, but this typically includes students, faculty, staff and people physically present in the library. The common-lib-terms value is registered with MACE and documented here: <http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html>.

The administrator of the identity provider will need to use some logic based on available user attributes from the enterprise directory, to determine what users are covered under the common-lib-terms entitlement. The library and the identity provider administrator will need to work together to interpret common-lib-terms entitlement and the logic that is needed to implement it.

2) What resource providers should this attribute be released to - As this is an attribute that is agreed to as a Best Practice for the InCommon community, this entitlement attribute *can* be released to all resource providers in the InCommon Federation. IdP administrators may choose though to release this selectively to resource providers. If the latter is the case, the entitlement attribute will need to be released to each resource provider that the institution enables Shibboleth access to, as well as the library's EZproxy installation (to be discussed in next step).

Step 2: Shibboleth-enable the EZproxy installation

The next step in integrating Shibboleth and EZproxy is to configure EZproxy to be a Shibboleth Service Provider. This is also referred to as Shibboleth-enabling the EZproxy.

OCLC, in their EZproxy support documentation, provides instruction on how to configure EZproxy as a Shibboleth Service Provider: <http://www.oclc.org/support/documentation/ezproxy/usr/shibboleth.htm>. This document does a good job of introducing the concepts and configuration options, as well as includes a 'quick configuration' section. The shibuser.txt section can be ignored for initial setup, but will be used in step 3.

Once EZproxy is configured as a Shibboleth service provider, the identity provider's attribute release policy should be configured to release the eduPersonEntitlement attribute to EZproxy.

Step 3: EZproxy - authorization based on user attributes

Once EZproxy is configured as a Shibboleth service provider, EZproxy and Shibboleth can be used together to provide authorization based on user attributes. This basically means that EZproxy can be configured to make decisions as to what databases a user can gain access based on who the user is. This is made possible because EZproxy can be configured to proxy access to resources selectively based on user attributes made available to EZproxy through Shibboleth.

This allows for EZproxy and Shibboleth to enforce policies, such as "Deny all alumni users to all databases" or "Allow only nursing students access to journal x". The most basic and widely used policy though may be to allow access to users that have the common-lib-terms entitlement.

The shibuser.txt configuration file is where EZproxy can be configured to make authorization decisions based on a user's attributes. There are two types of configurations that are useful to understand. The first is the ability to deny access to all databases based on a user's attributes. The second is to selectively allow users to access certain databases based on specific user attributes (e.g., nursing student's access to journal x).

The ability to deny access to all databases based on a user's attributes will be explained by way of example. EZproxy can be configured to deny access to all users that do not have the common-lib-terms entitlement. And these users can be directed to a particular error page if desired. Below is the configuration command that can be added to shibuser.txt in order to enforce this policy:

```
If !(auth:urn:mace:dir:attribute-def:eduPersonEntitlement eq "urn:mace:dir:entitlement:common-lib-terms");
    Deny unaffiliated.html
```

The ability to allow selective access to databases based on user's attributes is done using EZproxy's Group directives. This works by mapping users to groups based on their attributes and defining databases as assigned to groups as well. When a user attempts to access a database through EZproxy, they must be a member of the group that the database is assigned to.

Again, explanation by way of example. Let's say that there exists a journal, Nursing Weekly, and the institution has contracted for access to this journal for its nursing department only. And let's also say that departments are represented at this institution by the user attribute, eduPersonOrgUnitDN, and the Nursing department value for that attribute is 'Nursing'. In order to enforce the policy, EZproxy is configured such that users from the nursing department are assigned to group, Nursing, and the Nursing Weekly database is assigned to the Nursing group as well. Here are snippets from the shibuser.txt and config.txt.

shibuser.txt:

```
If auth:urn:mace:dir:attribute-def:eduPersonOrgUnitDN eq "Nursing";
    Group +Nursing
```

config.txt:

```
Group Nursing

Title Nursing Weekly
URL ...
```

The concepts here can be extended to create more fine-grained policies if desired, but this should be enough example to have a sense for how this might be accomplished.

Step 4: EZproxy to enable Shibboleth access to resource providers

The last step in the integration of Shibboleth and EZproxy is to configure EZproxy to be aware of resources that are Shib-enabled. For these Shib-enabled resources, EZproxy can be configured to hand off to Shibboleth for authentication and authorization, rather than proxy the user's entire session. One of the main benefits to this approach is to lower the amount of traffic that is proxied through ezproxy, which usually results in better performance and end user experience. Another main benefit is that it allows, through Shibboleth, for resource providers to create personalized services for users in their interfaces, while maintaining the user's privacy and seamless experience. [Note, however, that to integrate that level of personalization, the IdP will need to be configured to release a personally identifiable attribute instead of the generic eduPersonEntitlement. Refer to [Best Practice #1](#) for more information.]

This step must be performed for each resource for which you wish to enable Shibboleth access. The Registry of Resources (<https://spaces.at.internet2.edu/display/inclibrary/RegistryOfResources>) has been created to help facilitate this step. In order to set up Shibboleth access to a resource through EZproxy, the resource provider should adhere to the Best Practices. The Registry of Resources provides all of the details for each resource in terms of which resources adhere to the Best Practices, where to go for help, and sample configurations. The text below explains how to use the Registry to enable Shibboleth access through EZproxy.

Resource providers generally have to manage a handful of mechanisms for providing access control to their content, including username/password, IP address validation, Referring URL, Athens and Shibboleth. The resource providers have to configure, for each of their customers, what mechanism(s) that customer is using. Some resource providers have full-blown administrative interfaces for their customers' to configure this themselves, others have support via chat, and others you will need to call your account rep. So, there is going to be a different process for each resource provider to configure Shibboleth as one of the mechanisms for providing access control for your institutions' account. The Registry provides, where we can, contact information for each resource, and also relevant documentation for setting up your account for Shibboleth.

If the administrator for your identity provider has chosen (in Step 1) to selectively release the eduPersonEntitlement attribute to resource providers, the IdP will need to be configured to release the eduPersonEntitlement attribute for each resource provider that is Shib-enabled.

Once Shibboleth is enabled for your institution's account, the resource provider needs to be configured in EZproxy. The configuration for Shibboleth-enabled resources is done with SPU (Starting Point URL) commands in EZproxy. These are SPUEdit and SPUEditVar. These commands are documented in the EZproxy documentation, <http://www.oclc.org/support/documentation/ezproxy/cfg/spuedit/>. The Registry also provides sample EZproxy configurations for each resource provider. The intent of these sample configurations is for you to replace the appropriate institution-specific variables with local variables.

Note that SPUEdit commands for a particular resource need to REPLACE any existing EZproxy configurations for a resource.

Once EZproxy is configured with SPUEdit commands for a Shib-enabled resource, existing software that routes URLs through EZproxy should not need to be modified. This includes OpenURL resolvers, federated search engines, course home pages, etc.