Integration Pack for Authentication Solutions 1.2 Administration Guide

About Shibboleth

Shibboleth is an open-source single sign-on (SSO) solution that enables users to log in to a system only once to access secure resources inside and outside of their organization.

Users can select their Identity Provider (IdP) from a list of trusted IdPs (if more than one exists). The IdP asks the user to authenticate using their username and password. Once the user's credentials are validated, the user gains access to Learning Environment, as well as to external secure resources, without the need to sign in again.

Note System administrators can configure their Service Providers (SPs) to only display a list of trusted IdPs that their users can authenticate with.

Back to top

Overview

Purpose of this document

This guide is for system administrators who configure their organization's Integration Pack for Authentication Solutions (IPAS). This SSO solution for Shibboleth can either replace the standard Learning Environment authentication method, or live side-by-side.

This integration pack currently works only with the Shibboleth authentication solution. There are no other authentication solutions that are available with this integration pack at this time.

> **Note** This document assumes that the reader is familiar with Shibboleth. For more information refer to the Shibboleth web site.

Back to top

System requirements

- Correctly installed and configured Shibboleth SP, with corresponding working trust network consisting of other SPs and IdPs.

  > **Note** Tested against the Shibboleth Service Provider 2.5.2. This is the recommended minimum version.

Back to top

Shibboleth

Shibboleth has three main components:

1. A Service Provider (SP), which protects specific resources and allows access to those resources only if the user has been authenticated and authorized.
2. Identity Providers (IdPs), which authenticate users and conveys their attributes to requesting resources. This is also known as the home organization of the user.
3. A Where Are You From (WAYF) page, which enables an SP to support multiple IdPs. This is an optional component if the organization already has its own WAYF page.

Back to top

Shibboleth Service Provider

The information in this section assumes that your system is using the reference implementation of the Shibboleth SP version 2.3.1 (or similar), found at the Shibboleth web site.

> **Note** This section is not exhaustive. It provides a minimal amount of information to help you handle simple configuration issues. Your configuration may be different depending upon how you have configured your system.

Installation and Configuration requirements

The following are a list of pre-requisites for using this Integration Pack for Authentication Solutions:

- The Shibboleth SP has already been installed on each Application Server.
- A functioning web of trust already exists between the SP and its IdPs.
- The IdPs have already been configured correctly.

Configuration file

This section contains configuration information found in the main configuration file (shibboleth2.xml). This file should be located in opt\shibboleth-sp\etc\shibboleth\ somewhere on your local file system.

Site Id configuration

This section of the configuration file determines which site Id in IIS Shibboleth is configured to be used with, as well as the host name.

Note It must match the values associated with the Org.

```
<Inprocess logger="native.logger">
        <ISAPI normalizeRequest="true" safeHeaderNames="true">
        <!-- Maps IIS Instance ID values to the host name. -->
                <Site id="1" name="lms.myorganization.org"/>
        </ISAPI>
</Inprocess>
```

Sample 1 - Site Id Configuration

- This site Id is different for each application server.
- safeHeaderNames should be set to "true" unless there is a compelling reason not to do so. This decreases the likelihood of spoofing attacks being successfully carried out, and also removes all underscores from header names configured in Shibboleth.
- Scheme and port must also be set if using https within the <Site> tag (scheme="https" port="443").

Path protections

This section of the configuration file determines the path that Shibboleth "protects". The "path" must be "d2l/shibbolethSSO", with "requireSession" set to "false". The "name" under "Host" must match the name above (in Sample 1) as it does here.

```
<RequestMapper type="Native">
        <RequestMap applicationId="default">
                <Host name="lms.myorganization.org">
                        <Path name="d2l/shibbolethSSO"
                         authType="shibboleth"
                         requireSession="false"/>
                </Host>
        </RequestMap>
</RequestMapper>
```

Sample 2 - Path Protection

Note It is assumed that only the first Path element actually protects the resources on the server. If you have a configuration in place that protects multiple paths, or you would like to request one, then take caution to ensure it is configured correctly.

Application settings

This section of the configuration file is used to specify settings for the application. The "entityID" specified here is the Id the Service Provider has in the Shibboleth infrastructure.

```
<ApplicationDefaults id="default" policyId="default"
 REMOTE_USER="eppn"
 entityID="https://lms.myorganization.org/shibboleth-sp"
 homeURL="https://lms.myorganization.org">
```

Sample 3 - Application Settings

SP configuration

Under SessionInitiator, this section of the configuration file contains information on how the SP is configured to be used with one (or more) IdP/WAYF. One <SessionInitiator> tag is required for each IdP/WAYF. Consider the following two examples in Sample 4 and Sample 5:

```
<SessionInitiator type="Chaining"
 Location="/Login" isDefault="true"
 id="Intranet" relayState="cookie"
 entityID="https://idp.logintest.lms.myorganization.org/shibboleth">
</SessionInitiator>
```

Sample 4 - Service Provider Configuration 1

```
<SessionInitiator type="SAML2"
 Location="/TestShib"
 isDefault="true"
 defaultACSIndex="1"
 id="TestShib"
 entityID="https://idp.testshib.org/idp/shibboleth"
 template="bindingTemplate.html"
</SessionInitiator>
```

Sample 5 - Service Provider Configuration 2

- Each SessionInitiator contains an entityID representing the IdP/WAYF for the entry, and a relative path "Location" that can be visited by users to initiate the authentication process using this IdP/WAYF for this SP.
- These values are used to help populate the IDENTITY_PROVIDERS table in the Shibboleth database component.
- homeURL is typically not utilized, but it is the default redirect target after authentication if no other is supplied; however, one is typically supplied.

Service Provider Windows service

This section contains settings for the Service Provider windows service. The address and port attributes specify the IP and port the service should use on that local machine, and the access control list (ACL) attribute specifies which IPs should be allowed to contact the service. All application servers must have their IP listed in the ACL and should share the same configuration, unless you have a different solution implemented for load balancing.

```
<TCPListener address="172.21.16.72" port="12345" acl="127.0.0.1 172.21.16.71
 172.21.16.72 172.21.16.73"/>
```

Sample 6 - Service Provider Windows Service

Service Provider metadata

This section contains settings that control which metadata the SP uses, and which entities it can interact with.

```
<MetadataProvider type="Chaining">
        <MetadataProvider type="XML"
         uri="http://www.testshib.org/metadata/testshib-two-metadata.xml"
         backingFilePath="Testshib-metadata.xml" reloadInterval="180000">
        <SignatureMetadataFilter certificate="Testshib.pem"/>
                <MetadataFilter type="RequireValidUntil"
                 maxValidityInterval="2419200"/>
                <MetadataFilter type="Whitelist">
                        <Include>https://idp.testshib.org/idp/shibboleth
                        </Include>
                        <Include>https://lms.myorganization.org/shibboleth-sp
                        </Include>
                </MetadataFilter>
        </MetadataProvider>
</MetadataProvider>
```

Sample 7 - Service Provider Metadata

- In this case, metadata is provided by http://www.testshib.org/metadata/testshib-two-metadata.xml, with a backing file (cache) named Testshib-metadata.xml. A certificate named Testshib.pem to verify the xml is also provided. All of this is located in the same directory as shibboleth2.xml.
- The metadatafilter type is whitelist, and specifies which entities are configured for use, with all others not allowed.

Shibboleth ISAPI filter

The Shibboleth ISAPI filter must be set up and installed on the website. Check under ISAPI filters in IIS for the website, and verify that opt\shibboleth sp\lib\shibboleth\ isapi_shib.dll is installed as a filter. Under Configuration in the Home Directory, verify that the .sso extension points to opt\shibboleth-sp\lib\shibboleth\isapi_shib.dll for all verbs. In addition:

- Script engine should be checked.
- Verify that file exists is unchecked.

Attribute Mapping

Default behavior for the IPAS requires that the request headers be populated by the SP as follows:

- The header name specified in the config variable **d2l.ShibbolethSSO.SP.IdPHeaderName** (by default SHIBIDENTITYPROVIDER) must be populated with the user attribute specifying the IdP that was used to authenticate the user.
- The header name specified in the config variable **d2l.ShibbolethSSO.SP.UserNameHeaderName** (by default REMOTEUSER) must be populated with the user attribute that should, in turn, be mapped to a username or orgDefinedId for that user.

If you have implemented a different mapping logic that does not populate this item, the logic must be modified.

Whether or not these are being populated is verified using the following asp script (aspinfo.asp) placed in the /d2l/shibbolethSSO virtual directory.

> **Note** This should be deleted prior to any production deployment going live.

```
<%@ Language=VBScript %> <HTML> <BODY> <table border=1> <%For Each s In
 Request.ServerVariables%> <tr><td><%=s%></td><td>
<%=Request.ServerVariables(s)%> </td></tr> <%Next%> </table> </BODY> </HTML>
```

Sample 8 - Attribute Mapping

- This collection pre-pends the HTTP_ prefix. The names of the headers likely do not include this.

Initiate the SP session manually by visiting the following location, and by replacing each constant with your system appropriate values:

```
http(s)://SERVER/SESSION_INITIATOR.sso?entityID=ENTITY_ID&target=http(s):
//SERVER/d2l/shibbolethSSO/aspinfo.asp
```

Sample 9 - Session Initiation Location

- SERVER: address for the org
- SESSION_INITIATOR: name of SessionInitiator you want to use (located in shibboleth2.xml)

Note You should see all server variables listed here after you complete authentication. If you receive errors, there is likely a problem with the configuration.

Configuring SP for multiple orgs

ApplicationOverrides modify the default application settings for the new org.

- Application override information is found at this location:

```
https://spaces.internet2.edu/display/SHIB2/NativeSPApplicationOverride
```

Sample 10 - Application Override Information Location

- New Orgs inherit default settings in the ApplicationDefaults tag; ApplicationOverrides override these settings if required.

Three components must be modified for the New Org in the SP config:

```
<InProcess logger="native.logger">
        <ISAPI normalizeRequest="true">
        <!-- Maps IIS Instance ID values to the host name. -->
                <Site id="1" name="lms.myorganization.org"/>
                        <Site id="2" name="lms-2.myorganization.org"/>
        </ISAPI>
</InProcess>
```

Sample 11 - Configuring SP For Multiple Orgs 1

- lms-2 is the new Org, with a new entry under the ISAPI tag for its site Id.

```
<RequestMapper type="Native">
        <RequestMap applicationId="default">
                <Host name="lms.myorganization.org" applicationId="default">
                        <Path name="d2l/shibbolethSSO" authType="shibboleth"
                         requireSession="false"/>
                </Host>
                <Host name="lms-2.myorganization.org" applicationId="lms-2">
                        <Path name="d2l/shibbolethSSO" authType="shibboleth"
                         requireSession="false"/>
                </Host>
        </RequestMap>
</RequestMapper>
```

Sample 12 - Configuring SP For Multiple Orgs 2

- New Host tag must be added to identify the new applicationId and path name to protect.

```
<ApplicationOverride id="lms-2">
        <Sessions lifetime="28800" timeout="3600" checkAddress="false"
         handlerURL="/Shibboleth.sso" handlerSSL="false">
                <SessionInitiator type="SAML2" Location="/TestShib"
                 isDefault="true" defaultACSIndex="2" id="TestShib"
                 entityID=https://idp.testshib.org/idp/shibboleth
                 template="bindingTemplate.html" />
                <md:AssertionConsumerService Location="/SAML2/POST" index="2"
                 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
                <Handler type="MetadataGenerator" Location="/Metadata"
                 signing="false"/>
                <Handler type="Status" Location="/Status" acl="127.0.0.1"/>
                <Handler type="Session" Location="/Session"/>
        </Sessions>
</ApplicationOverride>
```

Sample 13 - Configuring SP For Multiple Orgs 3

- This might be different depending on what must be configured. It should serve as a good example.
- This tag is placed inside the ApplicationDefaults tag.
- The main differences in the AssertionConsumerService (ACS) are as follows:
    - New index is defined at 2.
    - SessionInitiator is modified to default to this new ACS.

- The metadata for SP must also be changed in the following ways:

```
<md:AssertionConsumerService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://
 lms.myorganization.org/Shibboleth.sso/SAML2/POST" index="1"/>
```

Sample 14 - Configuring SP For Multiple Orgs 4

```
<md:AssertionConsumerService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://
 lms-2.myorganization.org/Shibboleth.sso/SAML2/POST" index="2"/>
```

Sample 15 - Configuring SP For Multiple Orgs 5

- Each Org must have at least one ACS pointing to its domain with a unique index, as shown in Sample 15.
- This must be modified within the federation, the process of which varies.

Note Ensure that the ISAPI filter and extension handler are installed as previously documented for each application server, that the ShibbolethSSO tool for the org is enabled, and that the IDENTITY_PROVIDERS table as previously documented is properly setup.

Back to top

Identity Providers

Provide your list of IdPs to your Deployment Services Consultant. The Deployment Services Consultant will populate the database with this information so that the IdPs will appear in the drop-down list on the WAYF page.

Back to top

WAYF Page

The WAYF page allows users to select which IdP to log in with. Once the IdPs are updated in the database by the Deployment Services Consultant, the list is populated with those values. Depending on how your federation/institution is set up, you may already have a WAYF page and you will not need to reference this one.

Back to top

Configuration Variables

This section describes configuration variables in Learning Environment:

- **d2l.ShibbolethSSO.Auth.InvalidRedirectLocation** Information about the number of retries and the reason for login failure will be forwarded to the page configured at this value so that it can display a user friendly message to the end user. The Default value is "/d2l/shibbolethSSO/errorPage.d2l".
- **d2l.ShibbolethSSO.Logout.LEAuthRedirect** This variable should be set to wherever users should be directed if they used plain Learning Environment authentication to enter the system.
- **d2l.ShibbolethSSO.Logout.ShibAuthRedirect** This variable should be set to wherever users should be directed to if they used Shibboleth authentication to enter the system.
- **d2l.ShibbolethSSO.Plugin.PluginName** This variable can be used to modify the logic that is used for each org to match Shibboleth users to Learning Environment users. The default value is the only current valid value and should not be changed. The current default value **D2L.ShibbolethSSO.LPUserNameShibMapperPlugin.LPUserNameShibMapperPlugin** specifies a strategy that attempts to map Shibboleth users based first on username, and then on orgDefinedId. The specific configuration for this strategy is described below.
- **d2l.ShibbolethSSO.LPUserNameShibMapper.IsDirectMap** This variable should be set to true if the username values coming across from the SP will match 100% the username or orgDefinedId in the Learning Environment system without modification (and false otherwise).
- **d2l.ShibbolethSSO.LPUserNameShibMapper.Delimiter** This variable should be set to either the empty string, or the value that is used in the username/orgDefinedId to separate the Shibboleth username from the domain of the IdP. For example, if users have usernames like "john!idp.org", the ! symbol would be appropriate. However, if the users lack domain information in the names (for example "john"), then the empty string is appropriate. This value has no effect if **d2l.ShibbolethSSO.LPUserNameShibMapper.IsDirectMap** is set to true.
- **d2l.ShibbolethSSO.SP.IdPHeaderName** This variable should be set to the name of the http header that contains the entityID of the IdP. It should usually not include any leading HTTP_. For example, if the variable is documented as HTTP_SHIBIDENTITYPROVIDER, then SHIBIDENTITYPROVIDER is likely the correct value.
- **d2l.ShibbolethSSO.SP.UserNameHeaderName** This variable specifies the name of the http header that contains the username that will be mapped to the username/orgDefinedId in Learning Environment. This should also likely exclude HTTP_.

Back to top

Workflow

This section lists the sequence of events that a user experiences during the authentication process:

1. The user's initial point of entry is the D2L WAYF page, or another one supplied by the federation/institution.
2. If a WAYF page exists, the user selects their IdP from the list. If there is only one IdP configured for the system, the user is redirected immediately to that IdP.
3. The user enters their username and password to be verified by the IdP. This may be logged in the IdP, but no log entry is made in Learning Environment.
4. The IdP redirects the user back to the SP with the authentication and authorization related information it has found.
5. If the user has been authenticated, they are then redirected to the login script as part of the IPAS solution.
6. The user is matched to one in Learning Environment and is then logged in. In Learning Environment, an entry will appear with the login date and IP Address for that user in **Admin Tools** under Users. To access this information, select **View User Tracking** from the action menu of the user you wish to track. A log entry is

made within Learning Environment to keep track of users. The log entry can contain the following information:

- Org Defined ID: Organization Id.
- AuthMethodId: Code for type of authentication used. For Shibboleth, this is always a value of 3.
- LoginName: Username supplied from the IdP.
- StatusType: Status of the attempt. It identifies the type of authentication used.
    - UserAuthenticated = 0
    - UserNotFound = 1
    - LockedOut = 2
    - Inactive = 3
    - UserNotAuthenticated = 4
- UserId: The Learning Environment user Id.
- IP: The IP address of the user's machine.
- SessionId: Unique identifier for the session that was created.

7. The user is then redirected to the org unit homepage.

Back to top

Deep Link Login

Note When using deep link login, the sequence of events are the same as listed in the Workflow section, except that the D2L WAYF page is not seen. Whether or not a federation/organization supplied WAYF page is seen depends on how the system is configured.

IPAS supports the use of static deep links into Learning Environment. Only those links that do not require query string parameters or those that require only a single query string parameter are compatible. The links are in the following format:

- https://ORG_URL/Shibboleth.sso/SESSION_INITIATOR.sso?entityID=IDP_ENTITYID&target=https://ORG_URL/d2l/shibbolethSSO/deepLinkLogin.d2l?target=TARGET_ADDRESS.
    - ORG_URL is the site URL for the organization.
    - IDP_ENTITYID is the entityID of the IdP that should be used for authentication.
    - TARGET_ADDRESS is the address in Learning Environment that the user should be sent to. For example: /d2l/lp/homepage/home.d2l?ou=6606.
    - SESSION_INITIATOR is the name of the SessionInitiator that should be used for creating the session.

Back to top

Logs

Logs are stored in the following two areas:

1. Learning Environment Logs
    - The System Error Log contains errors caught or generated by Learning Environment.

2. Shibboleth Logs
   - Logs are located in your Shibboleth SP installation under opt\shibboleth-sp\var\log\shibboleth\. This assumes you are using the reference implementation of the Shibboleth SP version 2.3.1 (or similar) located at the Shibboleth web site.
   - There are three types of logs:
     1. **native.log** This logs information related to the operation of the ISAPI filter in IIS.

        > **Note** This defaults to 10 megabytes. The oldest log files are deleted at that point in First In First Out (FIFO) order.

     2. **shibd.log** This logs information related to the operation of the Shibboleth SP Windows Service, which handles the creation and caching of sessions.

        > **Note** This defaults to 10 megabytes. The oldest log files are deleted at that point in First In First Out (FIFO) order.

     3. **transaction.log** This logs transaction records for users that have been authenticated. This log facilitates cross referencing between other logs.

        > **Note** This defaults to 20 megabytes. The oldest log files are deleted at that point in First In First Out (FIFO) order.

To view the logs, you must have direct access to the application servers. Only self-hosted clients will have this type of access.

Back to top

Integration Pack for Authentication Solutions 1.2 Administration Guide