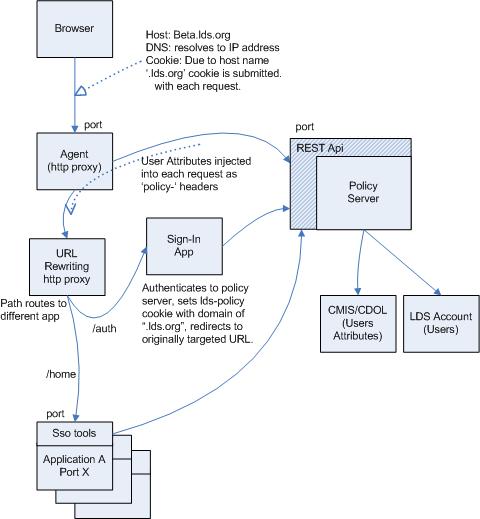
# NextGen SSO Environment Overview

The SSO Environment Simulator (SES) is a standalone tool enabling simulation of the runtime environment seen by applications when running in the NextGen single sign-on environment. That environment leverages the OpenSSO solution with http web agents and reverse proxies to route traffic to back end applications as shown in Figure 1. Inherent in this environment is that all applications appear to be on the same domain server. Some number of top level directory paths are used to uniquely identify a specific application and route traffic to that application after it has passed through the agent.

Figure : Church Single Sign-On Environment



For example, https://labs.lds.org/mls/mbr/… identifies the MLS Web member application and all URLs starting with /mls/mbr would be routed to the server cluster housing that application provided the user is allowed to access that URL resource. This is known as reverse proxying. Forward proxying refers to user agents having to use a proxy to access internet resources.

## Reverse Proxying and Enforcement

As shown in Figure 1, traffic to the site is resolved by DNS to hit a special reverse proxy known in opensso terminology as an agent. An agent looks at each request and checks to see if that URL is in a list of unenforced URLs. If so then the traffic is proxied on to the appropriate application server cluster. If not then it must ensure access by the user is allowed. If the user does not have a currently active session the agent redirects the user agent to a sign-in page. This sign-in page also happens to be an application protected by the agent but its URLs are included in the unenforced list allowing its traffic to pass through the agent. Upon receiving the user’s credentials it then uses an REST api on the policy server to authenticate the user. If successful, the application sets the resultant token in a cookie and redirects the user agent back to the original URL.

Upon receiving the original request with the active cookie the agent now contacts the policy server asking if the URL is allowed to be accessed by the user. The policy server consults all configured policies protecting that URL to see if the user meets any of the conditions for access and accordingly forbids access or allows the traffic onward to be routed to the targeted application.

## Canonical Versus Application Space Enforcement

A result of using a reverse proxy approach is that the agent evaluates URLs in the canonical space, the URLs that show in the user’s browser. The rewriting proxy can and does rewrite URLs to accommodate some requirements of application implementation technologies. The java context is a notable example. The application residing at /mls/mbr… is a java application and more applications will be coming that will be mapped beneath the mls tier. But java contexts must be a single path level and this application’s java context root happens to be /mls-membership. The rewriting reverse proxy infrastructure rewrites the URL before it hits the application server.

This is a subtle but important point. If enforcement of access were implemented within the applications themselves via a filter in java or a rewriting module in xquery for example, then the URLs used to enforce that access would be application space URLs not canonical space URLs. When problems arise with access to a specific resource and user call the help desk, the problematic URL being targeted can not be compared directly against the URLs configured in policies when using application space enforcement. With canonical space enforcement the URLs seen by the users match those in the policies.

## User Attribute Injection

In addition to enforcing access to URLs the agent is configured to inject a number of headers into each request passing onward to the application servers. These headers will be discussed in more detail in section ???????. One such header is an indication of the location of the REST api used by the agent to protect resources. A library of utilities provided by the SSO team then allows applications to call to that REST api and evaluate URL access decisions themselves. This allows an application designer to identify some resources by URIs that are not associated with a protocol for access like http but rather used only to protect some functionality in the application and conditionally allow access if the user is granted access according to policies.

*Protecting Resource Access*

For example, application B wants Bishops and members to see most of the landing page but one teaser section should only be seen by Bishops. That section can conditionally be rendered by protecting that resource by a designated URI like, “app://beta.lds.org/app-B/restricted-teaser-block”, and then granted to users with a condition of having the position of Bishop.

*Implementing Application Roles*

For another example, application C uses the concept of roles to implement workflows. URIs representing each role are crafted like, “app://beta.lds.org/app-C/role/ip-moderator”, and policies are crafted with a condition requiring the user have one of the lds account identifier in a given list. By delegating to the policy server asking if the user can access that URI the application can identify if the user has that role and act accordingly.

In both examples, the greatest benefit of placing the access characteristics in policies external to the application is that the policies can be adjusted without having to redeploy the application or requiring the application to implement its own security database. If we wish to broaden the access to the Bishop’s teaser to his counselors that is easily achieved in the policy. If we need to add an additional user to those having the IP Moderator role specific to application C we add them to the corresponding policy.

Such roles could be assigned by adding attributes into the ldap store for a user but this is an application role and applications come and go over time. Policies are designed to protect resources as in application **B** or aggregate those who should have a given role as in application **C**. As applications change so too will their resources and naturally requiring adjustment to the corresponding policies. Changes to the ldap store should be for longer lived, less changing data.

*Interlinking Applications*

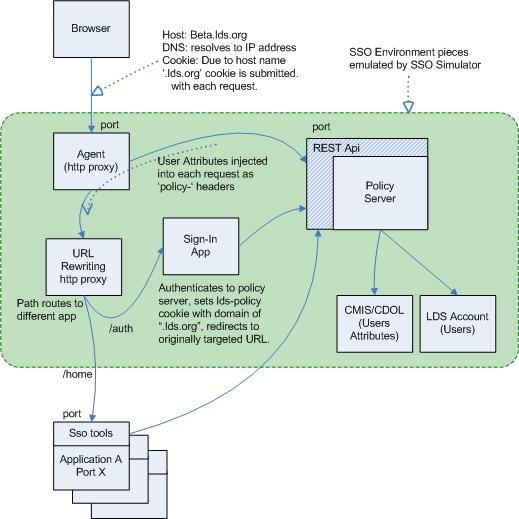
An additional benefit arises when using policies for applications that interlink to each other. If access to an application is restricted by the URL for that application and a link to that application is embedded within another application then that single URL can be used both to prevent access via the agent and by restricting rendering of that link in the other application. As the access for a given user changes based on their being added to the policy both the link will appear in the second application and they will be allowed to access the application when the link is selected.

*Cookies and Site Domains*

One more important characteristic must be highlighted in Figure 1. The cookie being used in the SSO environment matches the domain of the site. For example, the site is beta.lds.org and the domain of the cookies is configured to be “.lds.org”. Therefore, when requests are made to the site the cookie is passed in identifying the user toi the agent and to the application. If the domain of the cookie does not match that of the site then the cookie will not be submitted and result in a ping pong effect with the request hitting the agent, the agent redirecting to the sign-in page since it sees no valid seesion cookie, the sign-in page seeing the valid cookie and redirecting back to the agent, and so on until the browser stops the loop and indicates a problem or spins indefinitely.

We are now ready to discuss the SSO Environment Simulator. The SES appears to applications as shown in Figure 2. Specifically, it provides a proxying agent, policies, implementation of the opensso REST api, a user store, rewriting and routing, injection of headers both general and user specific, and a sign-in page. Lets take a closer look using its configuration as a vehicle for our discussion.

Figure : Portion of NextGen SSO Environment Simulated



# Configuring the SSO Environment Simulator

The simulator is configured via XML. A file containing the XML must be specified when starting the simulator from the command line. Alternatively, the simulator can be started programmatically and the XML can be located in a file or can be passed as a java.lang.String to the simulator at creation. The XML is parsed using a non-validating SAX parser which means that extra elements and attributes beyond those expected by the simulator are ignored.

# Aliases and Macros

The simulator’s parser supports a single XML processing instruction: “alias”. This instruction defines a key and value pair enabling use of references to values to be used in multiple places in the document. This instruction supports two patterns for defining alias values; literal text and classpath file references. In either case macro references can be embedded within the literal text source to inject values of previously defined aliases. The formal definition of the alias is:

[1] alias := “<?alias ” <name> “=” [<classpath-ref> | +[<clean-text> | <macro>]] “?>”  
[2] name := <clean-text>  
[3] clean-text := << any characters except patterns “<?”, “?>”, “{{“, or “}}” >>  
[4] classpath-ref := “classpath:” + << path to file on classpath >>   
[5] macro := “{{“ <name> “}}”

Examples of valid versions of this processing instruction are:

<?alias rest-port=1776?>

<?alias console-port={{rest-port}}?>

<?alias marks-lds-account-id=000111222333?>

<?alias is-ip-moderator=classpath:is-ip-mod.xml?>

The first three instructions use literal text values although the second’s value also happens to be a macro reference to the first alias. Hence, the console-port alias will have the same value as that of the rest-port alias. The fourth instruction uses a classpath file reference. Suppose that the contents of that file contained the following text. What this text means and why it is used will be explained in section ???????.

<HasLdsAccountId>

<LdsAccount id='3431968674741880'/>

<LdsAccount id='{{marks-lds-account-id}}'/>

</HasLdsAccountId>

Upon processing the is-ip-moderator instruction the file will be searched and loaded and any aliases within it resolved before setting the result as the value of the alias. Hence the value of the is-ip-moderator will be:

<HasLdsAccountId>

<LdsAccount id='3431968674741880'/>

<LdsAccount id='000111222333'/>

</HasLdsAccountId>

The DTD for the configuration file is found in APPENDIX A - DTD. :

be the same with an embedded alias Lets look at an example. Suppose that we desire to use the simulator’s built-in sign-in page in our configuration for testing an application. The configuration could appear as follows. Notice how the console-port alias uses the rest-port alias and is then used in the config element to tell the simulator to listen on that port for its console and it is also used in specifying via the sso-sign-in-url element where the simulator’s agent should redirect traffic if a session is required before allowing access to a protected resource.

<?alias rest-port=1776?>

<?alias console-port={{rest-port}}?>

<?alias site-port=80?>

<config proxy-port="{{site-port}}" console-port="{{console-port}}">

<sso-sign-in-url value="http://labs-local.lds.org:{{console-port}}/admin/selectUser.jsp"/>

...

**Listening Ports**

Although the simulator is an http proxy supporting both forward and reverse proxying its main goal is to provide reverse proxying to applications running on the same box allowing developers to simulate the full SSO environment without needing to be connected the latter to simulate our deployment environments at the church where numerous different technologies and server clusters can appear to be on the same site but located at different points of the and it provides a console both for monitoring traffic, users, and sessions and providing an implementation of the opensso policy server rest API. Hence it uses two ports one for http proxying and one for its console and rest service. The ports on which the simulator listens are defined on the XML document’s root element, config, which has two required attributes:

Proxy-port := [ integer | alias-macro ]

.for selecting a user or even an already established session. Alternatively, the The simulator requires two ports to run. The config elementValues for macros can be it to be maintained are ignored. either a file can be speand can be specified as aby starting the simulator on the command line XML file specified when

Scratch pad------

The mapping of incoming traffic for a single site to various backend applications is known as reverse proxying. The simulator supports this feature through configuring what are known as context mappings as is explained in section ????????.

Forward proxying is when a user agent can not go to servers directly but is told it must route all traffic through an http proxy and the proxy will hit the resource for a given URL and spool the response back to the browser. Although disabled by default, the simulator can be configured to allow forward proxying for testing certain SSO simulations which are discussed in section ???????.

# APPENDIX A - DTD

<!ELEMENT config ( sso-cookie, sso-sign-in-url, sso-header\*, sso-traffic, users ) >

<!ATTLIST config allow-non-sso-traffic CDATA #IMPLIED >

<!ATTLIST config console-port CDATA #REQUIRED >

<!ATTLIST config proxy-port CDATA #REQUIRED >

<!ELEMENT sso-cookie EMPTY >

<!ATTLIST sso-cookie domain CDATA #REQUIRED >

<!ATTLIST sso-cookie name CDATA #REQUIRED >

<!ELEMENT sso-sign-in-url EMPTY >

<!ATTLIST sso-sign-in-url value CDATA #REQUIRED >

<!ELEMENT sso-header EMPTY >

<!ATTLIST sso-header name CDATA #REQUIRED >

<!ATTLIST sso-header value CDATA #REQUIRED >

<!ELEMENT sso-traffic (( by-site|by-resource)\*) >

<!ELEMENT by-site ( allow | cctx-mapping | unenforced )\* >

<!ATTLIST by-site host CDATA #REQUIRED >

<!ATTLIST by-site port CDATA #REQUIRED >

<!ATTLIST by-site scheme CDATA #IMPLIED >

<!ELEMENT by-resource EMPTY >

<!-- one of allow or unenforced is required. it is an error to exclude both. -->

<!ATTLIST by-resource allow CDATA #IMPLIED >

<!-- conditions are optional. If not specified then the only requirement for

accessing the cpath is that the user be signed-in -->

<!ATTLIST by-resource condition CDATA #IMPLIED >

<!ATTLIST by-resource unenforced CDATA #IMPLIED >

<!ATTLIST by-resource uri CDATA #REQUIRED >

<!ELEMENT allow EMPTY >

<!ATTLIST allow action CDATA #REQUIRED >

<!-- conditions are optional. If not specified then the only requirement for

accessing the cpath is that the user be signed-in -->

<!ATTLIST allow condition CDATA #IMPLIED >

<!ATTLIST allow cpath CDATA #REQUIRED >

<!ELEMENT cctx-mapping EMPTY >

<!ATTLIST cctx-mapping cctx CDATA #REQUIRED >

<!ATTLIST cctx-mapping thost CDATA #REQUIRED >

<!ATTLIST cctx-mapping tpath CDATA #REQUIRED >

<!ATTLIST cctx-mapping tport CDATA #REQUIRED >

<!ELEMENT unenforced EMPTY >

<!ATTLIST unenforced cpath CDATA #REQUIRED >

<!ELEMENT users ( user+ ) >

<!-- session-timeout-seconds defaults to 300 seconds (five minutes) -->

<!ATTLIST users session-timeout-seconds CDATA #IMPLIED >

<!ELEMENT user ( sso-header+ ) >

<!ATTLIST user name CDATA #REQUIRED >

<!ATTLIST user pwd CDATA #REQUIRED >