Table of Contents

[NextGen SSO Environment Overview 1](#_Toc250840271)

[Reverse Proxying and Enforcement 2](#_Toc250840272)

[Canonical Versus Application Space Enforcement 3](#_Toc250840273)

[User Attribute Injection 3](#_Toc250840274)

[*Protecting Resource Access* 3](#_Toc250840275)

[*Interlinking Applications* 4](#_Toc250840276)

[*Cookies and Site Domains* 4](#_Toc250840277)

[SSO Environment Simulator 4](#_Toc250840278)

[Configuring the SSO Environment Simulator 5](#_Toc250840279)

[Aliases and Macros 6](#_Toc250840280)

[Rewriting Redirects 8](#_Toc250840281)

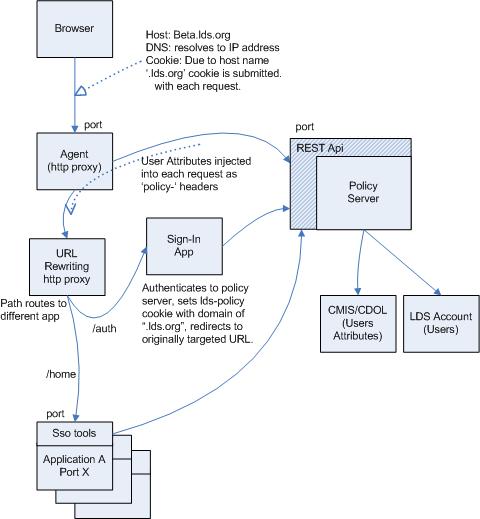
[Rewritting Cookie Paths 9](#_Toc250840282)

[APPENDIX A - DTD 9](#_Toc250840283)

# 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, policy-service-url, 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 require 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.

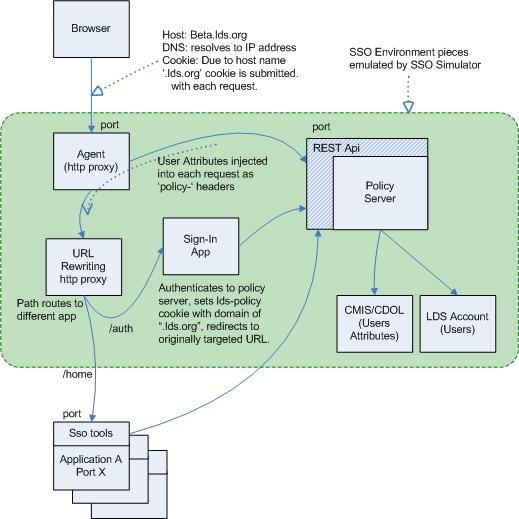
## *Cookies and Site Domains*

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.

# SSO Environment Simulator

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

Figure : Portion of NextGen SSO Environment Simulated



# Configuring the SSO Environment Simulator

As can be seen in Figure 2, the simulator listens on two ports. One is known as the proxy port and is meant to simulate a next gen church site like labs.lds.org or beta.lds.org. Via configuration, traffic intended for applications under development and running on different ports on the local box is proxied to those other ports essentially mapping those applications into and making them appear as one seamless site.

The second port has two purposes: it implements the REST api of the OpenSSO policy server for calls from applications and it provides a number of console pages. An example of the REST api usage is the sign-in application known as ml-auth used for labs and beta.lds.org. That application accepts user credentials, calls the REST api to start a session in the policy server and acquire the session token and SSO cookie name, then sets the SSO session cookie in the browser as it redirects to the originally targeted URL. Using the simulator’s REST implementation allows ml-auth to be developed and tested locally without a full OpenSSO environment. Before we show how such a set up is configured lets start with a more simple example that simply demonstrates the available console pages within the simulator.

## Getting the Simulator

The simulator runtime environment and all dependents are available from the SSO team or from the their ldsteams site. Once unzipped on a local machine it creates a “simulator” directory. Within that directory is a sim.bat are a sim.sh file. These must be modified slightly for your machine to include the path to java’s tools.jar so that the simulator is able to compile its jsp pages.

Once modified, the simulator can be started by calling sim.bat or sim.sh and passing a single parameter which is the configuration file that should be used. This has two formats. It can be a path on the machine like myApp.xml which would be a file assumed to be in the current directory. Alternatively, it can be fully qualified. In addition to file based resources classpath based files can be used by prefixing their path within the classpath with the text “classpath:”. This is how we will be demonstrating the simulator in the following pages.

## Accessing the Console

Included in the simulator’s jar are a number of example configuration files to help demonstrate its functionality. To start the simulator in its most simple configuration to show the console pages that are available to assist with troubleshooting issues run the following command:

./sim.bat classpath:config-samples/console-only.xml

Note that if you specify a path that is not found on the classpath you’ll get an error appearing as follows clearly indicating the problem which was a leading ‘/’ character in this case.

IllegalArgumentException: Unable to find resource '/config-samples/console-only.xml' on classpath.

Assuming that you started it correctly you’ll see console output similar to the following:

Using configuration file classpath:config-samples/console-only.xml  
2010-01-11 21:44:14.781::INFO: Logging to STDERR via org.mortbay.log.StdErrLog  
admin-rest port: 1776  
http proxy port: 80  
2010-01-11 21:44:14.843::INFO: jetty-6.1.7  
2010-01-11 21:44:14.890::INFO: Extract jar:file:/D:/saw/lib/appwrap-4.0.jar!/webapp to  
 C:\DOCUME~1\BOYDMR\LOCALS~1\Temp\Jetty\_0\_0\_0\_0\_1776\_webapp\_\_admin\_\_-usxbqe\webapp  
2010-01-11 21:44:15.359::INFO: Started [SocketConnector@0.0.0.0:1776](mailto:SocketConnector@0.0.0.0:1776)  
Started r-proxy on port 80

The console-only.xml configuration file used to start the simulator in this configuration is shown in Listing 1. The root element of the configuration is the config element. It supports three attributes defined in Table 1.

Table : Config - Attributes

|  |  |
| --- | --- |
| Atribute Name | Description |
| proxy-port | The port on which the simulated site will appear with all back-end applications mapped into its subdirectory space. Must be an integer. |
| console-port | The port on which the simulator’s console is located. Must be an integer. |
| allow-non-sso-traffic | Indicates if the simulator should allow for proxying non-SSO traffic as defined in section ?????. If allowed, then the simulator can be used a full http proxy and used by a browser by configuring the browser to use the simulator’s proxy-port as its http proxy. It defaults to false and caused the simulator to serve a 404 for any traffic that does not match the configured SSO traffic. |

Listing : Simple Config to Show Console Pages

<?xml version="1.0" encoding="UTF-8"?>

<config proxy-port="80" console-port="1776" allow-non-sso-traffic="false">

<console-recording sso="true" rest="true"/>

</config>

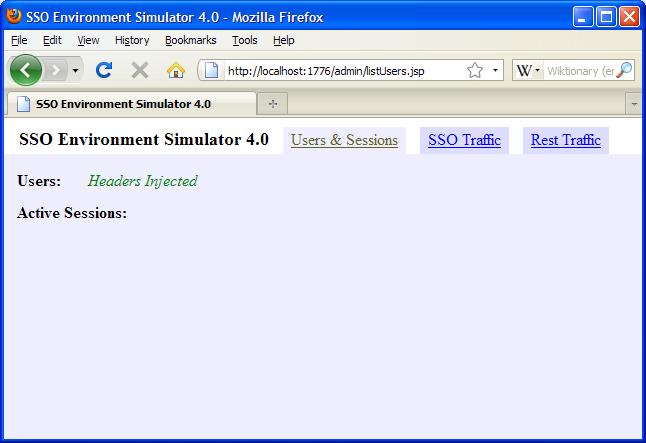
An optional child element of config is console-recording. It has the attributes shown in

Table : console-recording – Attributes

|  |  |
| --- | --- |
| Attribute Name | Description |
| sso | Indicates if the console should record in-memory the traffic that is hitting the http-proxy port and display it on the SSO Traffic tab. Defaults to false. Can be ‘true’ or ‘false’. |
| rest | Indicates if the console should record in-memory the traffic that is hitting the rest API and display it on the Rest Traffic tab. Defaults to false. Can be ‘true’ or ‘false’. |

To see the console pages of the simulator for this configuration point your browser to <http://localhost:1776/> and hit enter. You are presented with the simulator’s console with the User’s & Sessions tab selected as shown in Figure 3. Note that no users are defined in our configuration file nor did we declare any SSO traffic. Therefore, both the User & Sessions tab and SSO Traffic tab will appear empty. However, even with this simple set up we can exercise the rest API.

Figure : Console - Users Tab



## Accessing the Rest API

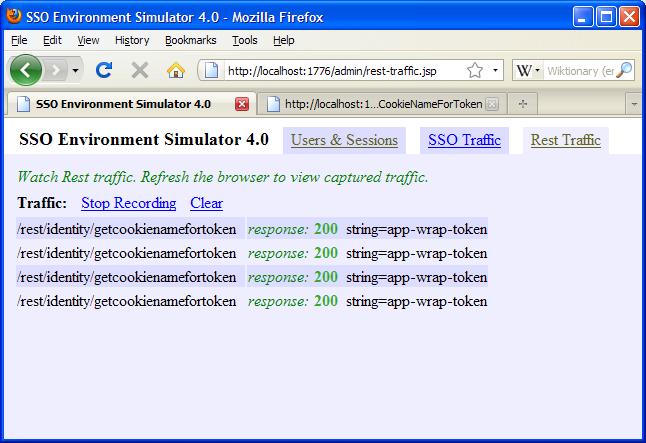
Either open a new browser tab or a new browser window and point it to:

<http://localhost:1776/rest/identity/getCookieNameForToken>

This will result in a single line of text, “string=app-wrap-token”. Congratulations, you just hit the REST API implemented by the simulator. This particular call returns the name of the cookie that should be set to hold the SSO session token value. Now return to your original browser window containing the console and select the Rest Traffic tab as shown in Figure 4. For each time that the API was accessed an entry was recorded and is displayed in the tab. The entries can be cleared with the Clear link or recording can be turned off with the Stop Recording link. If our console-recording element in our configuration file was missing or specified rest=’false’ then recording would have been off upon staring and the Stop Recording link would have been a Start Recording link.

Also note that for each API entry the lines alternate in background color to help identify all of the information for a single response. As will be seen, some responses consist of multiple lines in the console. Each response indicates the REST API that was accessed, the http response code, and the content of the response. We’ll revisit this output again later. Now lets add to our configuration.

Figure : Watching Rest API Traffic



## Setting the SSO Cookie’s Name

UI known Included in the console pages are two versions of 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 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 rest-api={{rest-port}}/identity?>

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

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

The first four instructions use literal text values although the second and third’s values also contain a macro reference to the first alias. Hence, the console-port alias will have the same value as that of the rest-port alias and the rest-api value will be “1776/identity”.

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 as the value for that alias. Additionally, if its contents contain any alias macros they will be resolved. 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

# Rewriting Redirects

Applications should be designed as much as possible to be cognizant of running in an environment where there is a difference between canonical and application URL space and and ensure that any redirects issued by it are canonical. But sometimes that is not possible when using third party libraries. In such cases a rewriting proxy like apache or its IBM variant HIS can be used to fix application space redirects that have no meaning in the canonical space where the browser is running..

Section 14.30 of RFC 2616 defines the “Location” response header used to convey a redirect instruction to the browser. It states that, “The field value consists of a single absolute URI.” Accordingly, the servlet specification dictates that servlet containers must convert relative URIs passed to the sendRedirect method of HttpServletResponse to absolute values. As noted in the 1.4 version of this method’s javadoc, “If the location is relative without a leading '/' the container interprets it as relative to the current request URI.” This means that it will prefix its path as needed including using the java context root. If the canonical space is different from the application space this can be a problem.

Lets look at an example. Suppose we have some bishop application written in java and having a java context of nextgen-bishop. We have taken care to ensure that we always issue absolute redirects that are cognizant of canonical space. But suppose further that it uses a third party ajax library that has embedded relative redirects over which we have no control. These will result in Location headers like so:

Location: http://labs-local.lds.org/nextgen-bishop/some/resource.html

But suppose that our application has been deployed at a canonical space of /bishop since we do not wish to have the “nextgen” identifier showing up in the browser. This will require that our Location header be modified to appear as follows:

Location: http://labs-local.lds.org/bishop/some/resource.html

The mechanism for achieving this in apache and HIS is the proxyPassReverse directive. The simulator supports this feature with its rewrite-redirect directive. There is no limit tn the number of such directives. They must be declared as a child of the sso-traffic element and have the following structure:

<rewrite-redirect from='from-value' to='to-value' />

Although it performs the same functionality as apache’s proxyPassRevers it varies in its declaration syntax by requiring fully qualified prefixes including the scheme, host, and port of the URI. Specifically, the Location header value will only be rewritten if it starts with the from-value. Further, only the the from-value portion of the Location header value will be replaced with the to-value portion. For example, to fix the improper redirect above to the correct value also shown above the following directive would be declared as a child element of the sso-traffic elements:

<rewrite-redirect from='http://labs-local.lds.org/nextgen-bishop/'   
 to='http://labs-local.lds.org/bishop/' />

# Rewritting Cookie Paths

Related to redirects are path based cookies. The java servlet specification dictates that the name of the session tracking cookie be “JSESSIONID”. Let suppose that we have two distinct java applications implementing different portions of our site at labs.lds.org. One will reside at /bishop in the canonical space with a java context root in the application space of /nextgen-bishop and traffic routed with suitable URL rewriting of requests as shown in ???? and Location header rewriting on redirect responses as shown in **Rewriting Redirects**. The other application will reside at /mls/mbr in the canonical space with a java context of /mls-membership in the application space with similar rewrites for requests and responses.

Now consider that both make use of java’s HttpSession functionality. When /bishop is accessed a JSESSIONID cookie is set in the browser to track the user’s session. If the user then accesses /mls/mbr the JSESSIONID cookie is submitted for the domain but does not match a session in that application. Accordingly, the application sets a new JSESSIONID cookie in the browser and any information in the /bishop application is now orphaned. Upon returning to /bishop the application sees a JSESSIONID that does not match any of its sessions and hence starts a new session and sets the JSESSIONID cookie accordingly in the browser orphaning the session from /mls/mbr.

To resolve such a problem typically the container specific functionality must be relied upon to set a path for the cookie which usually is the servlet context of the application. That means that for the /bishop application the JSESSIONID path will be /nextgen-bishop and that for the /mls/mbr application will be /mls-membership. Since the applications will be accessed from the browser using their canonical paths the cookie will never be submitted for either application.

Apache and IHS support directives for rewriting such cookie paths. The simulator provides a similar mechanism through its rewrite-cookie directive. It is similar in form to rewrite-redirect and must also be declared as a child of the sso-traffic element. It has the structure as shown in the example below which would handle the cookie path rewrites needed for our two applications:

<rewrite-cookie from-path='/nextgen-bishop' to-path='/bishop' />

<rewrite-cookie from-path='mls-membership' to-path='/mls/mbr' />

It is important to note that these again are prefix values. If a container supported setting a multi-level path like /mls-membership/app-1 then the rewriting only rewrites the matching portion and leaves the unmatched portion unchanged. For such a case the resulting cookie path of “/mls/mbr/app-1” would result.

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 >