Configuring ClearQuest for LTPA SSO

Lightweight Third-Party Authentication (LTPA) is a method for web application to share identity information using a cookie on the browser. The cookie is encrypted using shared keys that are shared between the WebSphere profiles that are running the applications that need the identity information.

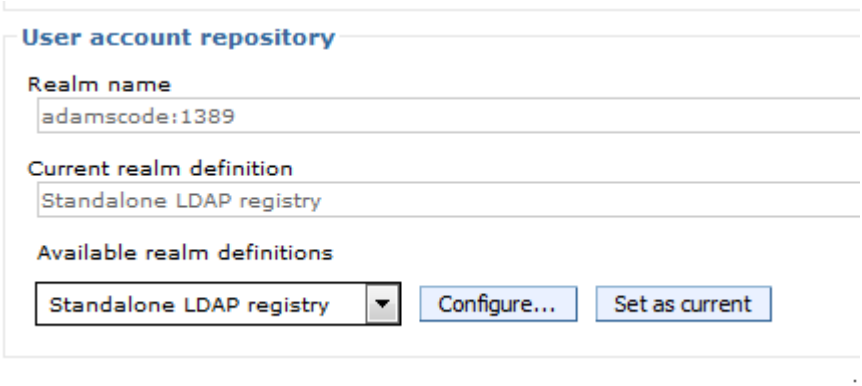
ClearQuest® can be configured to use the identity information provided by LTPA cookies, and IBM® WebSphere® can be configured to perform authentication of the user based on a configured federated or non-federated user repository (for example, an LDAP directory).

Configuring ClearQuest to use LTPA for single sign-on (SSO) is a two-step process. The first step is to configure the WebSphere profiles to share LTPA between them. The second step is to tell the ClearQuest database and web server that it should use LTPA for SSO.

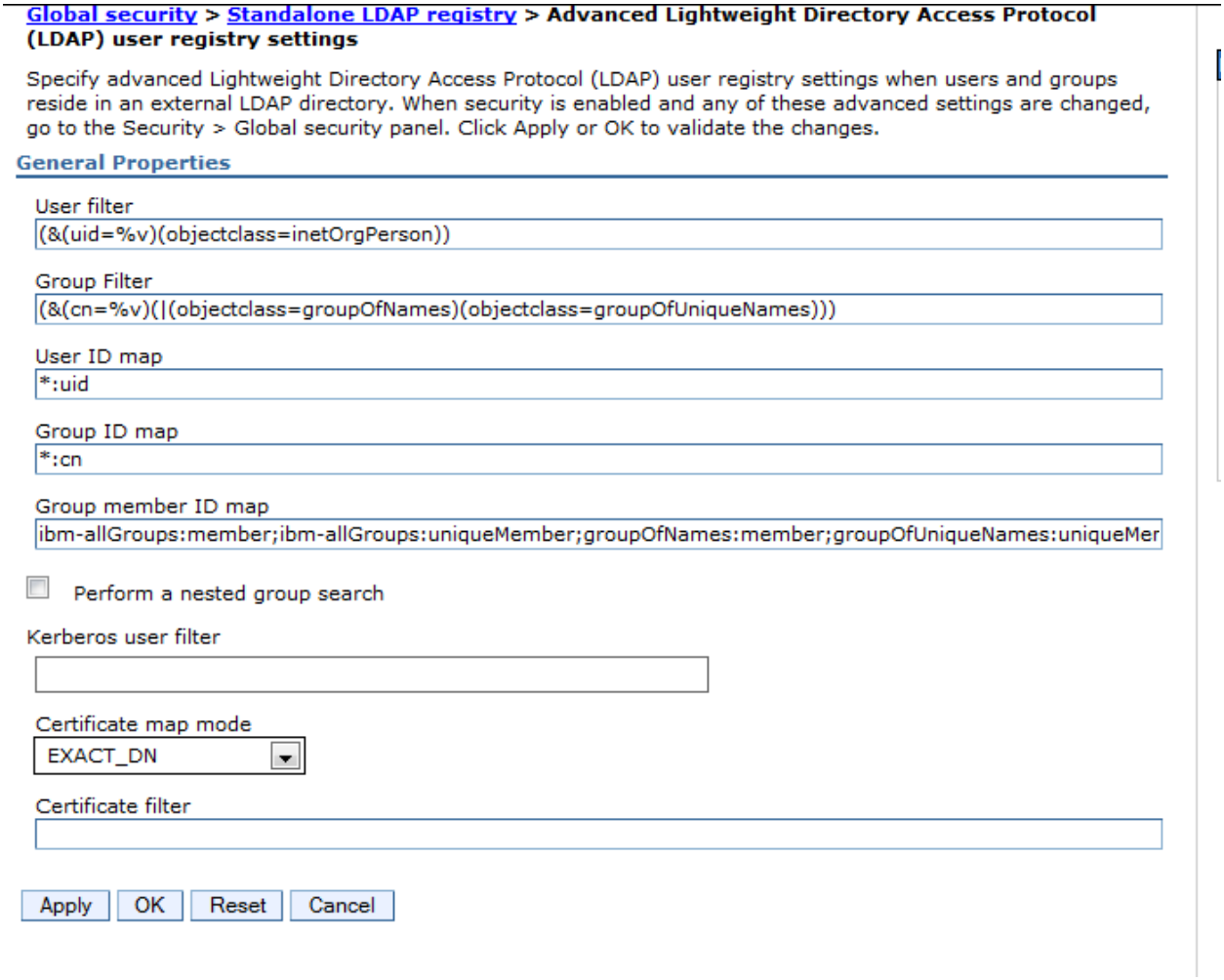
Setting up LTPA Between WebSphere Servers

WebSphere documentation describes how to configure two WebSphere servers to share LTPA. In summary, each WebSphere profile must use the same user registry and LTPA cookie name, and must be in the same domain (for example, *.ibm.com). By default, the LTPA cookie is LtpaToken2, but if you change this you have to change each WebSphere server to use the same cookie name.

Note: If ClearQuest does not work with a federated user registry set up, use a **Standalone LDAP registry**.



Furthermore, ensure that the advanced settings for the LDAP registry can find the users you plan to log in as. The following illustration shows an example of a set of advanced settings. Your configuration might require different settings.



ClearQuest SSO Setup

ClearQuest configuration for SSO follows almost the same directions as in the help topic Configuring strong authentication with smart-cards.

The steps to set up SSO with LTPA are:

1) Configure ClearQuest database for SSO.
2) Configure ClearQuest Web server for SSO.
3) Map LTPA/LDAP users to CQ Web application.

Configure ClearQuest database for SSO

1) You must set an SSO password in the database. See the procedure in help topic Configuring ClearQuest databases for container authentication.
2) Create an sso.properties file using cqrpc/cqrpc.exe and the password you used in step 1. See the procedure in help topic Configuring ClearQuest Web server for container authentication.
3) Configure the sso.properties file for LTPA. See the procedure in help topic Configuring the ClearQuest Web client for container authentication.

Configure ClearQuest Web server for SSO

Reference the help topic Configuring client certificate authentication for ClearQuest Web to modify the web.xml descriptor, but for the security constraint and other clauses in web.xml use this:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>secure</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>ClearQuestUsers</role-name>
    </auth-constraint>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>

<security-constraint>
    <web-resource-collection>
        <web-resource-name>CQBridge</web-resource-name>
        <!-- <url-pattern>/oslc/*</url-pattern> -->
        <url-pattern>/oslc/repo/sso2/discovery</url-pattern>
        <url-pattern>/oauth-request-consumer/*</url-pattern>
        <url-pattern>/oauth-authorize-consumers/*</url-pattern>
        <url-pattern>/oauth-request-token/*</url-pattern>
        <url-pattern>/oauth-authorization/*</url-pattern>
        <url-pattern>/oauth-access-token/*</url-pattern>
        <url-pattern>/scripts/*</url-pattern>
        <url-pattern>/images/*</url-pattern>
        <url-pattern>/stylesheets/*</url-pattern>
        <url-pattern>/gadgets/*</url-pattern>
        <url-pattern>/cqquerywizard.cq</url-pattern>
        <url-pattern>/cqartifactdetails.cq</url-pattern>
        <url-pattern>/cqqueryresults.cq</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
</security-constraint>

<security-role>
    <role-name>ClearQuestUsers</role-name>
</security-role>
```

Map LTPA/LDAP users to ClearQuest Web application

ClearQuest Web must be told which users can access the CQ Web application. You can either tell ClearQuest Web that all authenticated users can access the CQ Web application or choose specific groups or users that can access the application. Just accessing the application does not mean they can actually log in to ClearQuest Web, it only means that they can load the CQ Web resources in their browser. Whether they can actually log in to a ClearQuest database depends on whether the user is already subscribed to the ClearQuest database. For example, if the user “tom” is allowed access to the CQ Web application but does not have any access to a ClearQuest database, they will probably only see the database selection dialog but will not be able to actually connect to the database.

To LTPA/LDAP users to the CQ Web application, use the procedure in help topic Mapping users to LDAP groups.

As an alternative, you can also map ClearQuestUsers to “all authenticated users” or “all authenticated users in trusted realms.”