2.1 Using OpenClinica Web Services

Installation

To use OpenClinica Web Services, they must first be installed. Follow the instructions in the installation guide in your OpenClinica download, or contact your OpenClinica Enterprise support representative.

The OpenClinica Web Services module is deployed on Apache Tomcat as a separate "war" (web application archive) from the main OpenClinica application. A typical OpenClinica Web Services installation is as follows: the 2 directories ("OpenClinica" for 3.1.x-web and "OpenClinica-ws" for 3.1.x-ws) are present in the tomcat/webapps with the same db connection parameters (db=openclinica and clinica user).

In this configuration, you can access the usual web interface through https://yourDomain.com/OpenClinica, and access the web services by SOAP requests using https://yourDomain.com/OpenClinica-ws. When you verify (as it is explained in the documentation) your -ws installation by loading https://yourDomain.com/OpenClinica-ws in your browser, it is only for confirming the application is deployed and can connect to the database. It will return a login page with an empty rss feed, but you cannot access the web application through this login page.

You can then begin to work on SOAP requests, authenticating with the login and the password of a user with the option "Authorize SOAP web services in this account" ticked.

Dates

All date values in OpenClinica Web Services should use the (ISO 8601) YYYY-MM-DD format.

OpenClinica SOAP Web Services Security

OpenClinica Web services use the same security infrastructure as the OpenClinica web application. A valid username and password are required, and the roles/permissions for that account will apply. Passwords should not be added in plain-text, they must be hashed using SHA-1 before being

To authenticate with OpenClinica SOAP Web services:

- Make sure the user account is authorized to use web services (this authorization is granted in User Account setup).
- Hash the password using the SHA-1 algorithm (google for a 'SHA-1 hash generator' if you don't know what this is).
- Modify the "<soapenv:Header/>" line in the SOAP XML request with the following. Provide the user name in clear text and the hashed password string in the appropriate fields.

```
<soapenv:Header>
<wsse:Security soapenv:mustUnderstand="1"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurit
y-secext-1.0.xsd">
<wsse:UsernameToken wsu:Id="UsernameToken-27777511"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity
```

```
-utility-1.0.xsd">
<wsse:Username>username</wsse:Username>
<wsse:Password
type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
profile-1.0#PasswordText">
SHA1-password</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
```

Spring XwsSecurityInterceptor is used to secure OpenClinica Web Services. For more information on Spring XwsSecurity go to:

http://static.springsource.org/spring-ws/sites/1.5/reference/html/security.html

Approved for publication by Cal Collins. Signed on 2016-05-09 4:55PM

Not valid unless obtained from the OpenClinica document management system on the day of use.