Security

Security is implemented in Repertoire Server at various levels. Here is a list of security features at each level.

Data Source Level

Read-Only: When selected and saved, the next time a user opens this datasource, the user will not be able to edit any details of the datasource like name, description and column names.

Hide Details: When this option is selected and saved, the next time this datasource is opened, the user will only be able to see the name and description of the datasource.

Encrypted: This option is to be used with either the Read-Only option or the Hide Details option or both. Enabling this option, prompts the user to enter a password, then re-enter to confirm the password (Both passwords must be the same).

After this is done, if another user would like to edit any selections, he/she will need to enter the password.

Report Ouput Level

PDF Output: When this check box is selected, the PDF fle is encrypted with user and owner passwords. Encryption allows owners to control certain functions such as printing the file, and copying and pasting from the file. When this check box is selected, you can set the fag values. If the owner password is left blank, the system generates a random password, effectively preventing anyone from changing the access options.

The encryption strength of either 40 bits or 128 bits is selected from the combo box. The 40-bit strength is the standard one. You can increase a document's cryptographic strength by using 128-bit security.

Embedded Scripting Level: JavaScript, which can be executed within the report template or datasource file is protected via the JavaScript Security Manager.

See http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch05s05.html

Communication Protocol Level

Elixir Repertoire Server supports secure encrypted connection (HTTPS). When HTTPS is turned on, all data packets are sent between the client and server are encrypted.

See http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch04s04.html#SecureMode

Elixir Repertoire Server also supports connections using:

- Proxy Server - http://sites.google.com/a/elixirtech.com/wiki/repertoireserver/deployment/proxyserver
- SSH Tunneling - http://sites.google.com/a/elixirtech.com/wiki/repertoireserver/deployment/ssh

Authenication Level

All resources within the Repertoire Server are protected and authentications are required.

Default Authenication is via database - See http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch06s05.html#d0e1153

For LDAP Authentication - http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch04s04.html#d0e700

Authorization/Access Control Level

All resource authorization can be individually configured via the DBFS filesystems. This allows resources to be well managed.

See http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch05s04.html

Session Level

All users who log in to the Repertoire Server have a validity of 100 minutes (by default). The timeout value can be configured using configuration files to cater to Single-Sign-On needs.

Deployment Level

Elixir Repertoire Server can allow or refuse connections based on IP addresses. The Accept value is a regular expression that will be tested against the dotted-byte IP string of the client. Only those clients with accepted IP addresses will be allowed to connect. By default, this parameter is disabled, so that all clients can connect.

See http://www.elixirtech.com/release/Rep7.5.0/Repertoire-Server/ch04s04.html

API Level

You can secure the channels for generating report outputs or data from the Repertoire Server via API, using HTTPS.

See http://sites.google.com/a/elixirtech.com/wiki/repertoireserver/serverapi/rest/rest-api-for-java/rendering-a-report-with-rest/post-a-rendered-report-to-a-target

Web Security Level

Repertoire Server 7.5.0 has also been validated by IBM Rational AppScan 7.7 to achieve Security Risks level results of:

0 High , 2 medium, 2 Low and 1 informal Security Risks

This ensures that Repertoire Server is at low risk of web attacks.