Running Web Clients inside an IFrame

By default, a Web Client runs in the main browser window, but it is possible to run the Web Client inside a Frame/IFrame embedded in another webpage.

Embed HMTL code

To embed a Web Client solution into an IFrame, use the following HTML fragment inside the webpage where the Web Client solution is to be embedded:

```
<iframe name="{someName}" src="{serverUrl}/servoy-webclient/ss/s/{mySolutionName}"></iframe>
```

Note: Make sure to provide a unique name for each IFrame within the webpage: the Servoy Web Client internals use the name to control page reloads when those occur. Failure to uniquely identify a specific IFrame may result in unexpected behavior.

Cross domain embedding

When a Web Client solution is run inside an Frame or IFrame (here onwards just called frame) and the domain of the page into which the frame is embedded (for example: http://www.mycompany.com/pagewithframes.html) does not equal the domain from which the Web Client is hosted (for example http://mycompany.hostingcompany.com), there is a possible issue with the ability of storing HTTP Cookies.
Based on the settings of the browser, these so-called Third Party Cookies are blocked from storage. Internet Explorer does this by default, most other browsers allow it by default, but this can be turned off by the user.

The Web Client uses HTTP Cookies to save the position and location of dialogs and the functions application.setUserProperty(...) and application.getUserProperty(...) also utilize Cookies for string the User Property value. If the cookies cannot be stored, the Web client will continue to operate, but the position and sized of the dialogs and the value of User Properties will not be remembered.

The only remedy to the issue is configuring the browser to accept Third Party Cookies and this needs to be done by the user. As Internet Explorer does not allow Third Party Cookies by default, this browser is usually the one that causes Problems. Luckily, for Internet Explorer there is something that can be done by the developer of the webpage that is being displayed in the frame.

Adding a "Compact Privacy Policy" header to the Web Client pages
A Compact Privicy policy header is a specific header in the HTTP Response of a Web Client page, with a compact description of a Platform for Privacy Preferences (P3P) policy.

P3P is a standard for websites to provide the users of the website with information about the usage and possible storage of privacy related data. See http://www.w3.org/P3P/ for more information. Although the standard never really took off and isn't widely supported, it will come in handy in this scenario as Internet Explorer does implement it.

A P3P policy can be created online using http://p3pedit.com/ or with a downloadable tool provided by IBM here. When generated, it will also produce the Compact Privacy Policy string required for the configuration below.

Having said all of the above, many sites skip the generation of a full P3P policy and just take a appropriate value from the many websites that discuss the use of third party cookies in Internet Explorer and move on. The description of the required configuration below uses such a value, but we encourage developers/admins to set it up properly.

The P3P Compact Privacy Policy header can be added to all Web Client pages served by the Application Server, by adding and configuring a Filter in the webserver used by the Servoy Application Server.

The Filter is a small Java library and can be downloaded here: FilterP3P.jar. Place the downloaded jar file in <serverUrl>/application_server/server/webapps/ROOT/WEB-INF/lib (create the lib directory iif it doesn't yet exist).

Secondly, open <serverUrl>/application_server/server/webapps/ROOT/WEB-INF/web.xml and add the filter configuration shown below between the "</servlet-mapping>" and "</web-app>" tags.

Replace the value of the param-value with the generated Compact Privacy Policy string.

web.xml

```
...
  <filter>
          <filter-name>P3PHeaderFilter</filter-name>
          <filter-class>com.servoy.extensions.server.filter.P3PHeaderFilter</filter-class>
          <init-param>
                  <param-name>P3P-value</param-name>
                  <param-value>CP="CAO PSA OUR"</param-value>
          </init-param>
  </filter>
  <filter-mapping>
          <filter-name>P3PHeaderFilter</filter-name>
          <url-pattern>/*</url-pattern>
  </filter-mapping>
...
```


The other option: Altering the Security level in Internet Explorer on every client machine

By default the privacy level setting of Internet Explorer is set to Medium. This setting can be found under Tools > Internet Options > Privacy tab.

When the level is set to Medium, third party cookies without a Compact Privicy Policy will be blocked. By altering the privacy level to the lowest level "Accept All Cookies" the third party cookies will get accepted. Although this works, it means that in order to be able to use the Solution properly the setting needs to be altered in the browser of all individual users. It can be that corporate IT departments restrict the user from altering this setting.

Cookies without Compact Privicy Policy: These are cookies from pages that do not include a so-called P3P header in the HTTP Response