

Hannon Hill Corporation

800.407.3540 | www.hannonhill.com | info@hannonhill.com

Makers of the Award-Winning Cascade Server content management software

Integrating Cascade with Single Sign-On

By

Monday, April 23rd, 2007 at 3:00pm

As you may already know, [Cascade Server](#) offers several different methods of authenticating users, including LDAP and native user authentication. However, with the usage of single sign-on (SSO) software such as [CAS](#) and [Kerberos](#) on the rise, prospective clients are increasingly interested in Cascade Server's ability to integrate with various third-party authentication frameworks. In fact, Cascade does have the capability to integrate with these types of solutions using what is known as a "custom authentication plug-in." This plug-in is a Java class, or set of classes, that handles the CMS's end of the custom authentication lifecycle.

Typically, the custom authentication lifecycle for Cascade Server goes something like this:

1. The user accesses the CMS at a particular URL.
2. The CMS redirects the user's browser to an external login page, appending some extra information used to forward the user back to the CMS's custom authentication service URL.
3. The user logs in to said external service. If authentication fails, the user remains at the external login until successful.
4. Once authentication succeeds, the external service sends the user back to the CMS's custom authentication URL, appending a "ticket."
5. The CMS contacts the external authentication service, using the ticket to verify that authentication was successful.
6. The external service returns a response notifying the CMS which user logged in.
7. Cascade logs the user in and establishes a session for the authenticated user.

In addition to the custom login procedure, the plug-in can also redirect the user to a particular page upon logout.

Thus, the plug-in class simply handles browser redirection based upon the authentication phase (login/logout) and the authentication of the user against the third-party service. The plug-in class and any supporting classes are packaged in a separate JAR archive that is deployed to a client CMS's classpath (along with Cascade's authentication API JAR and any other necessary libraries). Finally, an authentication configuration file is placed in the client's Cascade Server installation directory. This file specifies the plug-in class to be used when authenticating users into the CMS.

You can find detailed instructions for developing your own custom authentication plug-ins on our [knowledge base](#).

Hannon Hill's [Professional Services](#) team also develops plug-ins for clients on a regular basis. So, even if you don't currently have the resources to implement custom authentication for your particular framework, you're still in luck. Please feel free to [contact us](#) for more information.

Category

- Resources

© 2001-2008 Hannon Hill Corporation. All rights reserved.