

# Centrally-Hosted Bamboo Services - Development-Deployment-Invocation

Bamboo's centrally-hosted services include an IAM (Identity and Access Management) suite, Collection Interoperability Hub, and proxy services to remotely-hosted tools for scholarship. This set of services runs on [FUSE ESB](#), an enterprise distribution of Apache's open-source [ServiceMix](#) (acquired in 2012 by RedHat). A number of additional, open-source technologies are required to support these services, including Apache Web Server ([httpd](#)), and [Grouper](#).

Information on the centrally-hosted services' architectural overview; a service developer "workbench" environment in which to extend or develop services; sys admin documentation for deployment of additional technologies in support of services; and the services' API are organized in this section of the Bamboo documentation, as follows:

- **Overview:** [Architectural Overview of the Bamboo Services Platform](#)
- **Service Developer Workbench:** [Developer Workbench Environment for BSP Service Developers](#)
- **Additional technology installation instructions:** see table, below
- **Service APIs:** [Service APIs - Centrally-Hosted Bamboo Services](#)
- **Other service APIs:** [Service APIs - Other Services](#)

## Installing and Configuring technology components

Technology Component (s)	Documentation Link (s)	Notes
Developer toolkit	<a href="#">Developer Workbench Environment for BSP Service Developers</a>	Java, Maven, Eclipse and IDE plugins, required filesystem directories, required environment variables
FUSE ESB	<a href="#">Developer Workbench Environment for BSP Service Developers</a>	Core element of Bamboo Services Platform (BSP, the deployment container for centrally-hosted services whose APIs are linked from <a href="#">Service APIs - Centrally-Hosted Bamboo Services</a> )
PostgreSQL database	<a href="#">Developer Workbench Environment for BSP Service Developers</a>	Relational database providing persistence for BSP-deployed services
Core BSP-deployed services	<a href="#">Developer Workbench Environment for BSP Service Developers</a>	Core services, including those that support IAM
Apache Web Server (httpd)	<a href="#">Configure Apache Web Server for Client Auth</a>	httpd supports client auth (authenticating trusted client applications), as well as proxy-forwarding over AJP of BSP services
Grouper	<a href="#">Grouper Install - Configure - Populate</a>	Grouper provides persistence for the "Application Catalog" (known/trusted client applications in the Bamboo Trust Federation); as well as for user-created and -managed groups
Application Catalog data	<a href="#">Maintaining Application Catalog Data for Trusted Clients</a>	For an application to be trusted (a key element of gaining permission to invoke services protected by policies that restrict access), Application Catalog data must be maintained.
Trust Federation metadata	<a href="#">Maintaining SAML Metadata that establishes a Trust Federation</a>	Identity providers and service providers trusted within the Bamboo Trust Federation must be identified with SAML metadata.
Social/SAML Gateway	<a href="#">Social/SAML Gateway to enable social media identity provision</a>	A Social/SAML gateway must be a part of the Authentication 'machinery' if social media Identity Providers (e.g., Google) are to be used for user logins.

Clients	<ul style="list-style-type: none"><li>• <a href="#">Shibboleth SP Installation and Configuration for Bamboo Trust Federation Clients</a></li><li>• <a href="#">Configure Apache Web Server for Client Auth</a> (<i>Certificate Exchange</i> section)</li></ul>	<p>When policies in effect restrict access to anonymous users or anonymous applications, only "Trusted Applications" can succeed in invoking the affected services. Only "Trusted Applications" can assert the identity of a user to BSP-deployed services (anonymous client apps imply anonymous users).</p> <ul style="list-style-type: none"><li>• Clients acting as a "Trusted Application" generally do so by functioning with an authentication context backed by Shibboleth SP (<a href="#">Shibboleth Service Provider</a>). Note install and configure document linked from column at left.</li><li>• In addition, exchange of certificates and metadata are necessary for a client application to act as a "Trusted Application" in the Bamboo Trust Federation (this includes simple web service clients such as Firefox <a href="#">Poster</a> or <a href="#">curl</a>). Note Client Auth document linked from column at left, particularly the <i>Certificate Exchange</i> section of that page..</li><li>• In addition to the installation and configuration documentation linked from the column at left, see the <i>Client responsibilities for implementing the conventions</i> section of the page <a href="#">Conventions for representing Identity Providers in the Bamboo Trust Federation</a>.</li></ul>
---------	--	--