



SourceID Liberty 2.0 Beta

User's Guide

© 2004 Ping Identity Corporation. All rights reserved

Part Number 3004-014
Version 1.00
07/19/2004

Ping Identity Corporation
1400 16th St. Suite 220
Denver, CO 80202
U.S.A.
Phone: 303.468.2900
<http://www.pingidentity.com>

Contents

	About This Guide	1
	SourceID Overview	1
	Intended Audience	1
	Support	1
	Text Conventions	2
	Special Notices	3
	Introduction	5
	System Requirements	6
Chapter 1	Installation Instructions	7
	Installing SourceID Liberty 2.0 Beta and the Demo Application	7
Chapter 2	Using the Demo Application	9
	Federating Accounts	9
	Performing Single Sign On	10
	Additional Liberty Profiles	10
	Deploying IDP and SP on Separate Servers	11
	Runtime Configuration	11
	Identity Provider Introduction (IPI)	12
Chapter 3	SourceID Liberty 2.0 Beta System Architecture	13
Chapter 4	The SourceID Liberty 2.0 Beta Framework	15
	Building and Packaging the Toolkit	15

About This Guide

SourceID Overview

SourceID is an open source project for enabling identity federation and cross-boundary security. SourceID focuses on ease-of-integration and deployment within existing web applications, products, or services. In addition, SourceID provides a high-level of developer functionality and customization and is designed to shield the integrator and enterprise from needing to understand the complexities of federation, or the rapidly evolving federation standards.

Intended Audience

This guide is written for individuals who have basic knowledge of Ant, JBoss, Java, and Liberty Alliance specifications. More information for Liberty Alliance is located at www.projectliberty.org.

Support

User and developer support documentation and mailing lists are located on the SourceID Website at www.sourceid.org.

Text Conventions

Text emphasis techniques help make following procedures much easier. This document uses the text conventions identified below.

Table 1 Text Convention Definitions

Convention	Description
Bold	Indicates first time use of product specific terminology defined in the glossary and identifies the beginning of procedures, examples, and menu selections.
Fixed With	Indicates you must type text exactly as shown in the instructions. Also used to represent computer code, file names, and directory paths.
Fixed With Bold	Used to identify event handlers, function calls, and API objects.
Cross References	Blue colored text is used in online documents to indicate hyperlinks you can click to direct you to the referred material.
<i>Emphasis</i>	Italics are used to emphasize a point and identify titles of documents.
Parameter	Teal colored text is used to identify parameters and attributes in online documents.
Screen Text	Identifies GUI text as shown on a screen. View the Print Document dialog for print settings.
GUI Selections	Identifies menu items or buttons operators click with the mouse. Example: Click Start > Programs > Photoshop

Special Notices

This User's Guide contains procedures for installing operating system functions and software, which, if not properly followed, may result in a system failure. The special notices listed below identify precautions and helpful information used in this User's Guide.



Note: Indicates additional or helpful information.



Important: Indicates material to which you should pay close attention.

Introduction

There are two components included in this distribution: the SourceID Liberty 2.0 Beta framework and a demonstration application. The demonstration application shows how to integrate the SourceID Liberty 2.0 Beta framework into an existing application.

This release of SourceID Liberty 2.0 Beta supports the core profiles necessary for conformance, including:

- Single Sign On (SSO) (Artifact & POST)
- Single Logout
- Register Name Identifier
- Federation Termination Notification
- Identity Provider Introduction



Note: Profiles not included in the list above are not implemented or supported at this time.

This version of SourceID Liberty 2.0 Beta was certified for conformance to the IDP and SP Basic profiles by the Liberty conformance process. This certification was achieved during the Liberty conformance event that occurred during the week of June 14, 2004.

System Requirements

The following is required to install SourceID Liberty 2.0 Beta:

- Windows XP or Linux (kernel 2.4.2+)
- Sun Java JDK 1.4.2
- JBoss 3.2.4
- Ant 1.5.1 (or higher)

Installation Instructions

Installing SourceID Liberty 2.0 Beta and the Demo Application

Go to the SourceID Website (<http://www.sourceid.org/download.do>) and download the SourceID Liberty 2.0 Beta zip file.

- 1 Unzip the source archive into a work directory.
- 2 Open the CastlePeak directory.
- 3 Edit the `build.local.properties` file and set the `jboss.dir` property to point to the directory where JBoss is installed.
- 4 After editing `build.local.properties` file, copy it to the Infrastructure directory and the Demo directory.
- 5 Run `ant deploy` from the Demo directory.
- 6 Enable SSL in JBoss.

In `${jboss.server.dir}\deploy\jbossweb-tomcat50.sar\server.xml` remove the SSL connector comment and add/change the keystore and truststore parameters as follows:

```
<Connector port="8443"
address="${jboss.bind.address}"
maxThreads="100"
minSpareThreads="5"
maxSpareThreads="15"
scheme="https"
secure="true"
```

```
clientAuth="false"  
keystoreFile="${jboss.server.home.dir}/conf/  
sourceid.keystore"  
keystorePass="changeit"  
truststoreFile="${jboss.server.home.dir}/conf/  
sourceid.keystore"  
truststorePass="changeit"  
sslProtocol="TLS"/>
```

An option exists to disable the verbose logging of the embedded workflow engine by adding the following to the `${jboss.server.dir}/conf/log4j.xml` file above the configuration for the root logger:

```
<category name="org.obe">  
  <priority value="WARN"/>  
</category>
```

7 Start JBoss.

8 At this point, the Demo application using the SourceID Liberty 2.0 Beta toolkit should be deployed and ready to use. You can access the Demo application by going to:

`https://localhost:8443/demo/sp/` (SP side)

`https://localhost:8443/demo/idp/` (IDP side)

On the SP login, use the following username/password:

joe / test

On the IDP login, use the following username/password:

joe123 / test

Please note that default deployment of the SourceID Liberty 2.0 Beta server acts as both SP and IDP.

Using the Demo Application

Federating Accounts

Before single sign on can be achieved, the accounts must be federated.

- 1 Login at the at the SP Login page <https://localhost:8443/demo/sp/> by entering the User Name [joe] and Password [test].
- 2 Click **Login**.
- 3 In the SP Application, click **Post** or **Artifact**.
- 4 Login at the at the IDP Login page and enter the User Name [joe123] and Password [test].
- 5 You will be redirected to the SP and the message You are federated with the following IDPs: will appear at the bottom of the page.

You have now federated the accounts between the SP and IDP. Continue to the single sign on procedure.

Performing Single Sign On

After federating the accounts, you can perform single sign on.

- 1 Select Click **here** to logout of all single sign-on sessions option.
Logging out directs you to the SP Login Page.
- 2 Click either **Post** or **Artifact**.



Important: Do not login on this page.

- 3 Log in at the at the IDP Login Page and enter the User Name [joe123] and Password [test].
- 4 Click **Login**.

You have performed single sign on and are now logged in at the SP Application page.

Additional Liberty Profiles

To explore additional profiles, explore the links provided on the demo application SP and IDP page.

Deploying IDP and SP on Separate Servers

In order to deploy this demonstration application across multiple machines (such as having one machine configured as the IDP, and one as the SP), you will need to update some configuration files and ensure that they are in the `${jboss.server.home.dir}/conf` directory before starting each server.

Some sample configuration files have been provided to help in getting started with deploying to multiple machines. In `//Demo/example-2server-config` there are two subdirectories, one contains a sample configuration for an IDP and the other contains sample configuration for an SP. Each directory contains all the files that need to be copied to each server's `jboss conf` directory, however, only `sourceid-core-config.xml`, `sourceid-soap-auth.xml`, `sourceid-provider-directory.xml` differ between the two deployments. In both of the `sourceid-provider-directory.xml` files you will need to change `https://IDP_DOMAIN:8443` and `https://SP_DOMAIN:8443` to point to the name or IP address of the machines that you have the IDP and SP deployed on.

Runtime Configuration

Some application functionality can be configured at runtime via the JBoss JMX Management Console (at `https://localhost:8443/jmx-console/` if you are running the server on your local machine). Go to the bottom of the page and under the `sourceid.demo.idp` heading click the `service=Config` link. This will take you to a page where you can dynamically reload the `sourceid-provider-directory.xml` and `sourceid-core-config.xml` files from disk.

In addition, an MBean exists (`service=metadata`) for managing the import of Liberty metadata. However, further discussion of this MBean is beyond the scope of this document.

You can also toggle two flags that tell the IDP how to behave in certain situations. You can tell the IDP if it should initiate Register Name Identifier during SSO. Also you can tell the IDP if it should attempt to set the common domain cookie (for Identity Provider Introduction) after authenticating a user.

Identity Provider Introduction (IPI)

Identity Provider Introduction (IPI) works by redirecting the user to a common domain to set and read the common domain cookie. This functionality is implemented in the demo application and various options are configured in the `sourceid-core-config.xml` file.

By default the common domain is configured to `common-domain.com` to make this functionality work on your local machine you will need to create a mapping of that domain to your local machine in your local `hosts` file. You will also need to configure the IDP to set the cookie (this can be done via the JBoss JMX Management Console as described above).

SourceID Liberty 2.0 Beta System Architecture

SourceID Liberty 2.0 Beta is a Java application which was developed on the JBoss application server. From a developer and deployment standpoint, SourceID Liberty 2.0 Beta's adapter tier is a critical aspect of the architecture.

The adapter tier is a set of Java interfaces that allow developers to customize how data is stored and how interactions with the web application occur. Developers implement these interfaces in order to integrate SourceID with their application environment. To select the implementation to use for a given adaptor, see the `sourceid-core-config.xml` file.

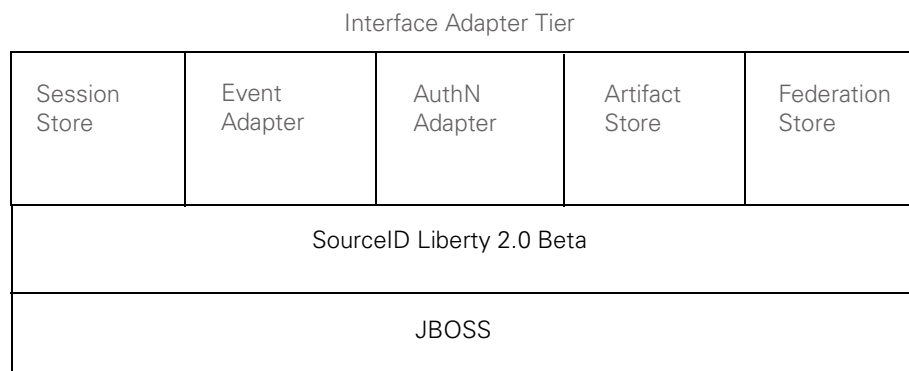


Figure 1 SourceID Liberty 2.0 Beta High Level Architecture

Session Store—The mechanism the SourceID implementation uses to track which users have logged in and logged out. An in-memory implementation is provided in SourceID Liberty 2.0 Beta

(`org.sourceid.idff12.adapters.impl.SimpleSessionStore`).

No additional configuration is required to use this default adapter.

Event Adapter—A notification mechanism that is used to update the local session system when a SSO event occurs. Separate adaptor instances must be created for handling IDP and/or SP side behavior. An implementation of this adaptor must be provided for your specific deployment (no default implementation is provided).

AuthN Adapter—SourceID uses this interface to retrieve the session identifier provided in a previous call to the **onSessionCreated** method on the EventAdapter interface. The session identifier is used by SourceID to track state information about a user's current session so that functionality such as Single Log Out works correctly. Separate adaptor instances must be created for handling IDP and/or SP side behavior. An implementation of this adaptor must be provided for your specific deployment (no default implementation is provided).

Artifact Store—Supports the artifact profile defined in the Liberty specification by keeping track of an associated array of artifacts to assertions. An in-memory implementation is provided with SourceID Liberty 2.0 Beta (`org.sourceid.idff12.adapters.impl.SimpleArtifactStore`). No additional configuration is required to use this default adapter.

Federation Store—Keeps track of information about account linkages. Hides all implementation details of mapping user account identifiers to pseudonyms. An in-memory implementation is provided with SourceID Liberty 2.0 beta (`org.sourceid.idff12.adapters.impl.SimpleFederationStore`). No additional configuration is required to use this default adapter.

The SourceID Liberty 2.0 Beta Framework

Building and Packaging the Toolkit

You must build the SourceID Liberty 2.0 Beta framework and integrate it into an existing application in order to incorporate Liberty functionality into the application. The following procedure will guide you through this process.

- 1 From the `CastlePeak` directory, run the `ant dist` command to build the SourceID Liberty 2.0 Beta framework. This creates the `sourceid-idff.zip` file in the `CastlePeak\dist` directory.
- 2 Extract the `sourceid-idff.zip` file to a *defined location*.
- 3 Copy the contents from the `{defined location}\lib` directory to the `WEB-INF\lib` directory of your application.



Note: If the `WEB-INF\lib` directory does not exist on the application, place the contents in the runtime class path of the application.

- 4 Merge the contents of the `web.xml` file template (located in the `{defined location}\templates` directory) with the `web.xml` file for the application.

You will need to edit the following files to configure CastlePeak. They are located at `{defined location}\template\conf`.

The files that require editing are:

```
sourceid-core-config.xml
sourceid-provider-directory.xml
sourceid-soap-auth.xml
```

Examples of edited versions of these files for the demo application are located at `\Demo\src\config`.

- 5 Copy the `jboss-web.xml` file (located in the *{defined location}*\templates directory) to the `\WEB-INF` directory of the application.
- 6 Copy the contents of the *{defined location}*\conf directory into the `jboss\server\conf` directory of the application.
- 7 Copy the contents of the *{defined location}*\resource directory to the class path `WEB-INF\classes`.

The files that require editing are:

```
sourceid-log-messages.properties (optional)
sourceid-url-resources.properties
```

Examples of edited versions of these files for the demo application are located at `\Demo\src\resource`.

- 8 Copy the contents of the *{defined location}*\templates\web directory to the location where the JSPs and other web content are stored for the application.
- 9 Examples of how to invoke the SourceID Liberty functionality to run your application are available in the following files at:

```
{defined location}\Demo\src\web\sp\
app.jsp
login.jsp
```

```
{defined location}\Demo\src\web\idp\
app.jsp
```

*SourceID*TM

Ping Identity Corporation
1400 16th St. Suite 220
Denver, CO 80202
U.S.A.