

IBM® Security Access Manager
for Versions 6.1.1, 7.0, 8.0 and 9.0

IBM WebSphere Liberty TAI Integration Guide



Contents

PREFACE	4
Access to publications and terminology	4
Publication Library	4
IBM Terminology website	5
Accessibility	5
Technical Training	5
Support information.....	5
Statement of Good Security Practices.....	5
Product name updates	6
INTRODUCING THE INTEGRATION	7
Introduction	7
Integration Architecture	7
Integration Product Version Information.....	8
Integration Product Contents	8
Before you start.....	9
IBM SECURITY ACCESS MANAGER CONFIGURATION	10
Web Gateway Appliance Configuration	10
Authentication Mechanism	10
Importing the Liberty SSL Certificate	10
Junction Management	11
Session Management.....	12
Obtaining PD.jar.....	13
IBM WEBSHERE LIBERTY CONFIGURATION	14
Liberty Configuration.....	14
Group to Java role Synchronization	14
Installing the TAI	14
Configuring the TAI	15
Configuring the Interceptor	15
Deploying the protected application	16
RUNNING THE SAMPLE APPLICATION	17

Before you start.....	17
Security Access Manager for Web configuration	17
User Account Creation	17
WebSphere Liberty Configuration.....	18
Deploying the sample application.....	18
Deploying to BlueMix (optional)	18
Validating Single Sign On	19
TROUBLESHOOTING.....	21
Enabling TAI Trace.....	21
Verifying the TAI without IBM Security Access Manager.....	21
Collecting Support Data	22
Collecting Data for ISAM: Web Gateway Appliance	22
Creating a support file from the Web Gateway Appliance	22
Security Access Manager for Web trace	22
NOTICES	24
TRADEMARKS.....	26

Preface

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM® Tivoli® Access Manager Base Installation Guide*

Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.

- *IBM Security Access Manager Base Administrator's Guide*

Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the pdadmin command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*

Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.

- *IBM Security Access Manager WebSEAL Administrator's Guide*

Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

Provides information about configuring and maintaining a Security Access Manager environment.

- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*

Provides configuration procedures and technical reference information for the Web Gateway Appliance.

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*

Provides a complete stanza reference for the Web Gateway Appliance Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager for Mobile Administration Guide*

Describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

- *IBM Security Access Manager for Mobile Configuration Guide*

Explains how to complete the initial configuration of IBM Security Access Manager for Mobile.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at

<http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical Training

For technical training information, see the following IBM Education website at

<http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at

<http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Introducing the Integration

Introduction

This guide describes the integration steps that are required to achieve Single Sign On (SSO) between IBM Security Access Manager and IBM WebSphere Liberty.

The integration uses Security Access Manager for Web as a reverse-proxy with a junction created and connected to the Liberty server. The user authenticated to Security Access Manager for Web is included as a HTTP request header on the junction and the identity is established within Liberty using a custom Trust Association Interceptor (TAI). The TAI is a Java module that is inserted into the authentication processing pipeline to handle delegated authentication for the Liberty server.

The TAI is an alternative to using LTPA and is a lightweight replacement to traditional-WAS (tWAS) solutions such as eTAI, but is not as full-featured, and due to differences between traditional-WAS and Liberty WAS such features are not possible. It allows identity to be consumed as a JAAS Subject in Liberty and group membership can be provided for group->role mapping for use in J2EE security constraints and Liberty API's can be called to obtain attribute information.

The TAI does not verify that the user ID in the HTTP request header is a Liberty user and does not rely upon the Liberty user registry, however groups which are mapped to Java roles must exist in the registry.

The TAI's configuration parameters include methods for ensuring that only requests authenticated by Security Access Manager for Web are processed by the TAI.

Optionally, when IBM Security Access Manager for Mobile is enabled, fine grained authorization using Context Based Access (CBA) and Risk Based Access (RBA) provides policy driven access control and multi factor authentication capabilities including One-time Password to the Liberty application.

Integration Architecture

Figure 1 shows the integration architecture with the following process:

1. A browser request to the Liberty server is submitted through Security Access Manager for Web.
2. Security Access Manager for Web intercepts the request, authenticates and authorizes the user as required.
3. Security Access Manager for Web forwards the request to Liberty along with the authenticated data in HTTP headers as well as other required validation configuration items.
4. The TAI is called and passed the request data.
5. The TAI establishes trust with the Security Access Manager for Web server.
6. The TAI parses the authentication data HTTP headers and generates a Subject for the user contained in the header and optional role assignment from the group data.
Note: Group to Java role mapping requires the groups to be created in the Liberty user registry.

7. The Liberty application is executed using the authenticated Principal generated by the TAI.
8. The requested content is returned to Security Access Manager for Web which performs filtering as appropriate for the junction method.
9. The filtered content is returned to the browser.

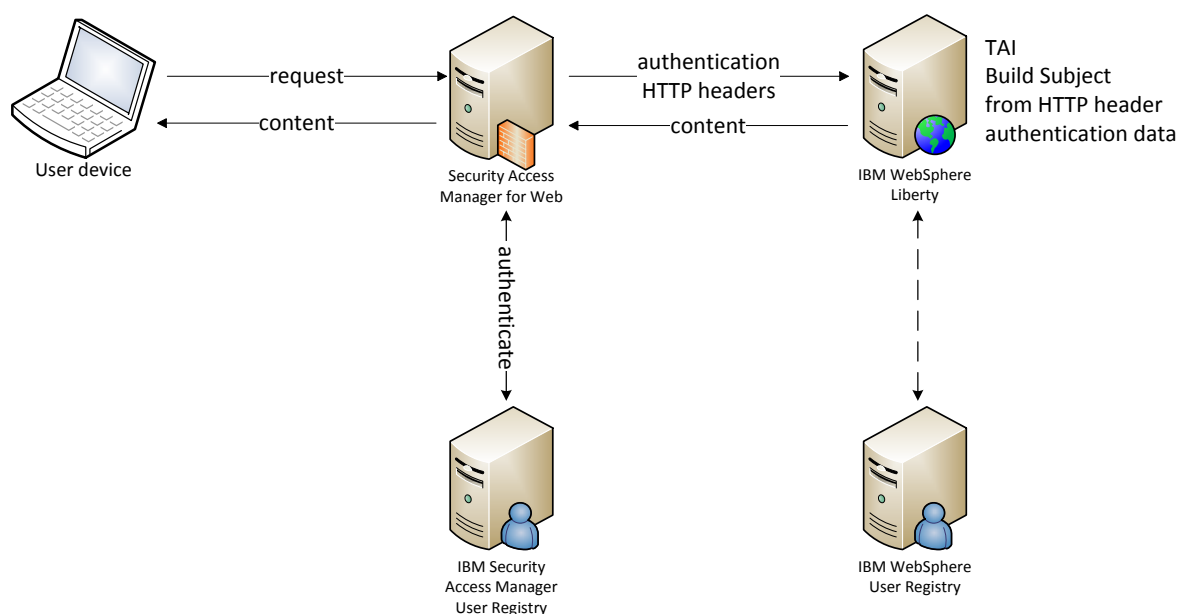


Figure 1: Security Access Manager Integration with IBM WebSphere process flow

Integration Product Version Information

See the Release Notes for supported versions.

Integration Product Contents

The integration solution is packaged as a compressed file. The package contains the following files:

File Name	Description
isam_liberty_tai_sso_int_guide.pdf	This integration guide.
X.X-ISAM-LIBERTY.README	Readme file containing supported versions, enhancements and update history.
ISAMLibertySSOTAI.jar	TAI for providing SSO to IBM WebSphere Liberty protected by Security Access Manager for Web.
server.xml	Sample Liberty server configuration file for TAI.
SubjectDumperEAR.ear	Sample Liberty server application for validating the TAI.

Table 1: Integration Package contents

Before you start

This integration guide details the steps that are required to achieve this integration at a high level in your environment.

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

- IBM Security Access Manager
 - IBM Security Access Manager for Web or WebSEAL
 - IBM Security Access Manager for Mobile (optional)

- IBM WebSphere Liberty
 - Java application requiring authentication and optional authorization is deployed

- User Repository Synchronization
 - Java role to group mapping is defined in the `ibm-application-bnd.xml` file in the `META-INF` directory of the application Enterprise Archive (.ear). Group names created in the Liberty user registry must exactly match Security Access Manager group names.

IBM Security Access Manager Configuration

Complete the following configuration steps on Web Gateway Appliance or WebSEAL for integration with IBM WebSphere Liberty.

The **pdadmin** command-line utility can be used on the Web Gateway Appliance in addition to the graphical user interface of the Local Management Interface (LMI) for some of the integration steps.

The instructions in this guide are only provided for Security Access Manager for Web. Perform the equivalent configuration steps manually if you are using WebSEAL.

Web Gateway Appliance Configuration

Complete the configuration steps on the IBM Security Access Manager for Web appliance to enable Single Sign On to the Liberty server.

Authentication Mechanism

It is recommended that Forms authentication is used so that single sign-out can be achieved with IBM WebSphere Liberty. To disable Basic Authentication and enable Forms Authentication:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings → Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Edit**.
5. Select the **Authentication** tab.
6. Under **Basic Authentication → Transport**, select **None**.
7. Under **Forms → Forms Authentication**, select **Both**.
8. Click **Save**.
9. Deploy the pending changes.
10. Restart the reverse proxy instance.

If Forms Authentication is not used the browser window must be closed to terminate the IBM Security Access Manager session.

Importing the Liberty SSL Certificate

The Liberty SSL certificate chain must be imported to the Security Access Manager key database.

Note: If you are deploying to a BlueMix host, ensure you import those certificates and not the local Liberty instance used for staging and packaging.

1. In a browser, navigate to the Liberty server. For example `https://liberty.ibm.com`
2. Export the certificate. Using Mozilla Firefox:
 - a. Left-click on the padlock icon to the left of the URL in the address bar
 - b. Click **More Information**.
 - c. In the **Security** panel, click **View Certificate**.
 - d. In the **Details** tab, click **Export...**

- e. Ensure the certificate is saved with the **.crt** file extension and click **Save**.
3. Open the Web Gateway Appliance Web console.
4. Select **Manage System Settings** → **Secure Settings** → **SSL Certificates**.
5. Select the **pdsrv** Certificate Database
6. Click **Manage** → **Edit SSL Certificate Database**.
7. Select the **Signer Certificates** tab.
8. Click **Manage** → **Import** → **Browse** and then select the **.crt** certificate file exported from Liberty.
9. Click **Open**.
10. Type a name for the certificate in the **Certificate Label** for example *Liberty*.
11. Click **Import**.
12. Deploy the pending changes.

Junction Management

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Junctions](#) page for details of each junction type.

The following example uses a Standard junction.

Create a standard junction to the **IBM WebSphere Liberty** server.

Using the Local Management Interface

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Junction Management**.
5. Select **New** → **Standard Junction**.
6. On the Junction tab
 - a. Add the junction name. For example: `/libertytai`
 - b. Click **Create Transparent Path Junction**.
 - c. For Junction Type, select **SSL**.
7. On the Servers tab
 - a. Click **New** to add a target backend server.
 - b. Specify the connection details of the **IBM WebSphere Liberty** server:
 - Hostname: `<ip_or_liberty-fqdn>`. For example: `liberty.ibm.com`
 - TCP or SSL Port: 443
 - c. Click **Save**.
8. On the Basic Authentication tab
 - a. Select **Enable Basic Authentication**
 - b. Provide a **Username**. For example: `tauser`

- c. Provide a **Password**. For example: `taipassw0rd`
9. On the Identity tab
 - a. Select **HTTP Header Identity Information: IV-USER**
 - b. Select **HTTP Header Identity Information: IV-CREDS**
10. Click **Save**.

Using the pdadmin command line

1. Login to pdadmin.

```
pdadmin> login -a sec_master
Enter Password:
pdadmin sec_master>
```
2. Determine the WebSEAL instance name

```
pdadmin sec_master> server list
<instance_name>-webseald-<hostname>
```
3. Create the standard SSL junction passing the iv-user and iv-creds headers and basic username and password

```
pdadmin sec_master> server task <instance_name>-webseald-<hostname> create -
t ssl -h <liberty_hostname> -p <liberty_ssl_port> -c "iv_user,iv_creds" -B -
U <trusted_user> -W <trusted_password> /<junction_name>
```

For example:

```
pdadmin sec_master> server task default-webseald-localhost create -t ssl -h
liberty.ibm.com -p 443 -c "iv_user,iv_creds" -B -U taiuser -W taipassw0rd
/libertytai
```

Session Management

It is recommended that you use the Web Reverse Proxy to manage the cookies generated by Liberty so that when a user is logged out of Security Access Manager or the ISAM credential changes due to step-up authentication they are automatically reset.

If you do not use the Web Reverse Proxy to manage the Liberty cookies another mechanism must be enabled to ensure that the `JSESSIONID` and `LTPAToken2` cookies issued by Liberty and sent to the browser are expired or invalidated when a Security Access logout or session timeout occurs.

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage** → **Configuration** → **Edit Configuration File**.
5. Locate the **[junction]** stanza.
 Alternatively to enable for just the example `/libertytai` junction locate the **[junction:/libertytai]** stanza.
6. Add the `JSESSIONID` and `Ltpa` cookies to the list.
 For example:

```
managed-cookies-list = JSESS*,Ltpa*
reset-cookies-list = JSESS*,Ltpa*
```

7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Obtaining PD.jar

The `PD.jar` file is required to interpret the `iv-cred` HTTP request header passed to the TAI.

It is downloaded from the Security Access Manager appliance.

1. Open the Web Gateway Appliance Web console.
2. Select **Manage System Settings → File Downloads**.
3. Expand the **isam** folder.
4. Download `pdjrte-<version>.zip`
5. Extract `PD.jar` from the `pdjrte/java/export/pdjrte` directory of the zip.
6. Copy `PD.jar` to a location accessible from the Liberty server.

IBM WebSphere Liberty Configuration

Complete the following configuration steps on the IBM WebSphere Liberty server.

Liberty Configuration

Complete the configuration steps on the Liberty server appliance to enable Single Sign On from Security Access Manager.

You must have a local machine installation of the Liberty server for deployment of the TAI and your application, even if you plan to run your application on Bluemix. These instructions will assume creation of a new Liberty server called **tailiberty**.

Group to Java role Synchronization

To enable group to Java role mapping for use in J2EE security constraints ensure:

1. Role definitions are created in the `web.xml` of the protected application.
2. Roles are mapped to corresponding groups which are defined in the `ibm-application-bnd.xml` file in the `META-INF` directory of the application Enterprise Archive (.ear).

For example:

```
<security-role name="RoleA">
  <group name="groupa" />
</security-role>
<security-role name="RoleB">
  <group name="groupb" />
</security-role>
```

3. Groups with corresponding names are created in the Liberty user repository.
4. Groups with corresponding names are created in the IBM Security Access Manager User Directory and are assigned to users as required.

Users do not need to be created in the Liberty user repository. In the configuration sample below a basic user registry with no users and with two groups is defined.

Installing the TAI

Upload the `ISAMLibertySSOTAI.jar` file and the IBM Security Access Manager `PD.jar` file to the Liberty server.

1. Create a directory for the TAI in the root directory of the Liberty server. For example:

```
proxytai
# cd <liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/<servername>
# mkdir proxytai
```
2. Copy the `ISAMLibertySSOTAI.jar` file to the `proxytai` directory.
For example:

```
<liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/tailiberty/proxytai
```
3. Copy the `PD.jar` file to the `proxytai` directory. Refer to *Obtaining PD.jar* on page 13 to access this file.
For example:

```
<liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/tailiberty/proxytai
```

Configuring the TAI

The `server.xml` of the Liberty server must be updated to enable the features required for the TAI to execute. A sample `server.xml` is provided with the integration package.

1. Enable **appSecurity-2.0** and **ssl-1.0**

```
<featureManager>
...
<feature>appSecurity-2.0</feature>
<feature>ssl-1.0</feature>
...
</featureManager>
```

2. Only **httpsPort** is defined in **httpEndpoint**

```
<httpEndpoint id="defaultHttpEndpoint" httpsPort="9443" host="*" />
```

3. Configure **LTPA**

```
<ltpa keysFileName="ltpa.keys" keysPassword="Passw0rd" expiration="120" />
```

4. Enable **trustAssociation** for the `com.ibm.security.isam.liberty.proxytai.ProxyTAI` interceptor

```
<trustAssociation id="myTrustAssociation"
invokeForUnprotectedURI="false" failOverToAppAuthType="false">
...
<interceptors id="PROXYTAI" enabled="true"
className="com.ibm.security.isam.liberty.proxytai.ProxyTAI"
invokeBeforeSSO="false" invokeAfterSSO="true" libraryRef="PROXYTAI">
<properties realm="defaultRealm"
proxyVerificationMethod="BASICAUTH" proxyBasicAuthVerificationValue="Basic
dGFpdXNlcjpw0YWlwYXNzdzByZA==" />
</interceptors>
...
</trustAssociation>
```

5. Configure the **library** for the `com.ibm.security.isam.liberty.proxytai.ProxyTAI` interceptor

```
<library id="PROXYTAI">
<fileset dir="${server.config.dir}/proxytai" includes="*.jar"/>
<fileset dir="${server.config.dir}/../../../../lib" includes="*.jar"/>
</library>
```

6. Configure a user registry. For example, a basic registry with two groups representing J2EE roles:

```
<basicRegistry id="basic" realm="defaultRealm">
<group name="groupa" />
<group name="groupb" />
</basicRegistry>
```

7. Optional: Configure trace logging

```
<logging
traceSpecification="*=info:com.ibm.security.isam.liberty.proxytai.*=all"/>
```

Configuring the Interceptor

In the `interceptors` stanza it is highly recommended you leave the `invokeBeforeSSO='false'` and `invokeAfterSSO='true'` for performance of the Liberty server and the TAI.

In the `properties` stanza the `proxyVerificationMethod` and `proxyBasicAuthVerificationValue` parameters of the interceptor enables the TAI to verify the request originated from a trusted WebSEAL server.

When the value of the `proxyVerificationMethod` is configured to `BASICAUTH` the value of `proxyBasicAuthVerificationValue` must be `"Basic XXXX"`, where `XXXX` is the value of `base64(username+':'+password)`.

The example `server.xml` contains the configuration sample:

```
proxyBasicAuthVerificationValue="Basic dGFpdXNlcjp0YWlwYXNzdzByZA=="
```

The value of `base64decode('dGFpdXNlcjp0YWlwYXNzdzByZA==')` is `taiuser:taipassw0rd` which corresponds to the sample username and password entered on the Basic Authentication tab in *Junction Management* on page 11.

When updating the value in the `server.xml` to a complex username and password, ensure the junction configuration is updated with the corresponding values. The `realm` parameter can be modified as required.

Deploying the protected application

Ensure an application is deployed to the `dropins/` directory in the root directory of the Liberty server. For the TAI to execute, the application must not enable unauthenticated access.

Running the Sample Application

Use the example scenario to validate SSO from Security Access Manager to the Liberty server. The sample environment uses the embedded directory server of Security Access Manager for Web and a basic user registry configured in the Liberty server.

Before you start

This section does not cover the configuration of the entire environment. It focuses on running the test scenarios and performing the configuration with sample values.

References are made to the configuration steps provided in

- *IBM Security Access Manager Configuration* on page 10
- *IBM WebSphere Liberty Configuration* on page 14

Security Access Manager for Web configuration

Install and configure a Security Access Manager for Web appliance:

1. When configuring the Runtime Component, use the **Embedded LDAP**.
2. Create a **Web Reverse Proxy instance**.
3. Configure **Forms Authentication** for the *Authentication Mechanism* on page 10.
4. Complete *Importing the Liberty SSL Certificate* on page 10.
5. Create the SSL junction to the Liberty server described in *Junction Management* on page 11.
6. Complete the configuration steps in *Session Management* on page 12.
7. Download the IBM Security Access Manager Java SDK by following the steps in *Obtaining PD.jar* on page 13.

User Account Creation

Use **Policy Administration** or the `pdadmin` command-line utility to create user accounts for accessing the sample application. For example:

```
pdadmin sec_master> user create testuser1 uid=testuser1,dc=iswga Test
User1 password1
pdadmin sec_master> user modify testuser1 account-valid yes
pdadmin sec_master> group create groupa cn=groupa,dc=iswga "RoleA"
pdadmin sec_master> group modify groupa add testuser1
pdadmin sec_master> user create testuser2 uid=testuser2,dc=iswga Test
User2 password2
pdadmin sec_master> user modify testuser2 account-valid yes
pdadmin sec_master> group create groupb cn=groupb,dc=iswga "RoleB"
pdadmin sec_master> group modify groupb add testuser2
pdadmin sec_master> user create testuser3 uid=testuser3,dc=iswga Test
User3 password3
pdadmin sec_master> user modify testuser3 account-valid yes
pdadmin sec_master> group modify groupa add testuser3
```

```
pdadmin sec_master> group modify groupb add testuser3
```

WebSphere Liberty Configuration

Install and configure a Liberty server:

1. Complete *Group to Java* role Synchronization on page 14, including the configuration of the user registry for Liberty.
2. Complete *Installing the TAI* on page 14.
3. Complete *Configuring the TAI* on page 15.
4. Complete *Configuring the Interceptor* on page 15. Ensure the trust validation parameters are updated with the values corresponding to the junction settings.
5. Deploy a sample application which requires authentication and optional authorization. Refer to *Deploying the sample application* below for the sample **SubjectDumperEAR.ear**.
6. Optional. Package and deploy the Liberty server to BlueMix. See *Deploying to BlueMix (optional)* below.

Deploying the sample application

A sample application for validating the TAI and Subject assertion is included with the integration package.

You can deploy the **SubjectDumperEAR.ear** sample to verify the installation and configuration of the TAI.

1. Copy the `SubjectDumperEAR.ear` file to the `dropins` directory in the root directory of the Liberty server.
For example:

```
# cp SubjectDumperEAR.ear <liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/tailiberty/dropins
```
2. If already started, the Liberty server will detect the new application and deploy it, otherwise start the Liberty server instance.

Deploying to BlueMix (optional)

The TAI can be run on local Liberty installations and alternatively, if you have a BlueMix account, the TAI can be configured and uploaded to a BlueMix instance.

For BlueMix deployment the Liberty server must be packaged before it can be uploaded.

Ensure you have configured the TAI, user directory and included the sample application.

1. Package the Liberty server using the `package` utility.
For example:

```
<liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/bin/server package tailiberty --include=usr
```

2. Use the Cloud Foundry tools to push the zip file of the server package created in the root directory of your server instance.
Specify the **appname** to create on BlueMix and the zip file corresponding to the packaged Liberty server name.

```
cf push <appname> -p tailiberty.zip
```

For example:

```
cf push mybluemixtaiapp -p tailiberty.zip
```

3. Monitor the progress and verify the success of the upload using the cf logs command.

```
cf logs <appname>
```

For example:

```
cf logs mybluemixtaiapp
```

Once the packaged server has been deployed to BlueMix, ensure the BlueMix certificates are imported into the IBM Security Access Manager appliance and the junction is updated to reference the BlueMix host.

Validating Single Sign On

Use the sample accounts created, verify that all users can access the `dump.jsp` indicating successful authentication.

To verify the group to role mapping, ensure

- testuser1 is only granted access to resources protected by RoleA
- testuser2 is only granted access to resources protected by RoleB
- testuser3 is granted access to resources protected by RoleA or RoleB

1. Open the sample Liberty application via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/dump.jsp`
2. Enter the credentials for testuser1.
 - a. Username: **testuser1**
 - b. Password: **password1**
3. Validate access is granted which will display the output of the user authentication.
4. Open the page protected by RoleA via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/rolea/whoami.jsp`
5. Validate access is granted which will display the output of the user authentication.
6. Open the page protected by RoleB via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/roleb/whoami.jsp`
7. Verify access is denied.
8. Log out of Security Access Manager for Web. For example:
`https://isam.ibm.com/pkmslogout`

9. Open the page protected by RoleA via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/rolea/whoami.jsp`
10. Enter the credentials for testuser2.
 - a. Username: **testuser2**
 - b. Password: **password2**
11. Verify access is denied.
12. Open the page protected by RoleB via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/roleb/whoami.jsp`
13. Validate access is granted which will display the output of the user authentication.
14. Log out of Security Access Manager for Web. For example:
`https://isam.ibm.com/pkmslogout`
15. Open the page protected by RoleA via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/rolea/whoami.jsp`
16. Enter the credentials for testuser3.
 - a. Username: **testuser3**
 - b. Password: **password3**
17. Validate access is granted which will display the output of the user authentication.
18. Open the page protected by RoleB via the Web Reverse proxy. For example:
`https://isam.ibm.com/libertytai/roleb/whoami.jsp`
19. Validate access is granted which will display the output of the user authentication.

If you experience any problems during integration, examine the following notes for help in identifying problems.

When <logging

- `<liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/<servername>/logs/trace.log`
- `<liberty_install_root>/wlp-javaee7-8.5.5.9/wlp/usr/servers/<servername>/logs/messages.log`

It is recommended that trace is turned off once the TAI deployment has been verified.

Once the TAI is configured and the sample application is deployed it can be tested directly, without accessing via the Web Reverse proxy.

When using the sample `SubjectDumperEAR.ear` the response should be HTML displaying user credential information. The response can be output to a .html file and loaded in a browser to view the result.

Replace `liberty.ibm.com` sample host with your own deployment.

```
# curl -k -u "taiuser:taiPASSw0rd" https://liberty.ibm.com/dump.jsp -H "iv-user:
testuser" -H "iv-creds:
BAKs3DCCBjUMADCCBi8wggyrAgIJATBaMcSwHwIEcDAIRgIDA0veAgIR5QICAJ4CAgD8BAYADClKuYAMCHR
lc3Rlc2VyMCSwKTafAgQNbfICAGMA6+ACAhHlAgIAngICAPwEBgAMKUq5gAwGZ3JvdXBhAgEEMIIFxDCCBC
AwIgwUqVVUSEVOVEldQVRJT05fTEVWRUuwCjAIAgEDEAEExBSAAWmQwXQVPoX0NSRURfQVVUSE5NRUNIX01OR
k8wfFJAUAQEEDA1MREFFtFJlZlZhdHJ5BAAWmwsSQVPOX0NSRURfQVVUSFPoX01EMB0wvIBBAAWUY249dgVz
dHVzZXIsZGM9aXN3ZEEADAQDBRBWk5fq1JFRF9BVVRXOX01FEVhPRDARMA8CAQQQMCHbc3N3b3JkBAAGdAw
VQVPoX0NSRURfQ1JPV1NFU19JTkZPMFswQIBBAxSTW96aWxsYS81LjAgKE1hY21udG9zaDsGSW50ZWwgTW
FjIE9TIFggMTAuMTE7IHJ2OjM4LjApIEDly2tvLzIwMTAwMTAxIEZpcmvmb3gvMzgumAQAMCIMD0Fat19DU
kVEX0dSt1VQUzAPMA0CAQQMBmdyb3VwYyQAAMD0MG0Fat19DUkVEX0dSt1VQX1JFR01TVFJJZX01EUzAbMBkC
AQQMEEmNuPWdyb3VwYsSxkyZlp3dnYyQQAUMEUFEFat19DUkVEX0dSt1VQX1VVSURTMC0wKwIBBAwkMGQ2ZGY
yMDItZSJw1MCOxMWU1LT1lZmMtMDAwYzI5NGFiOTGwBAAWJgWSQPoX0NSRURfSVBfrkfNSUsZMBAWdGIBBA
whQUZFUS5FVAQAMCKMEEFat19DUkVEX01FQ0hfSUQWTATAgEEDAXJVL9MRFFQX1YZfLjAEADZdBxBWk5fQ
1JFRF9ORVRXT1JLX0MERFfJU1nfQklOMBmEQIBBAWKMHhjMGE4MmEwMQQAMDMUEHFat19DUkVEX05FVFdP
UktfQUREUKVTU19TVFIwFTATAgEEDAwXOTIUmtY4LjQyLjEEADAtDB1BWk5fq1JFRF9QUk1OQ01QQUXFRE9
NQULOMBAWdGIBBAWHRGVmYXVsdaQAMCWmf0Fat19DUkVEX1BSSU5DSVBbTF9OQU1FMBEWDwIBBAwidGVzdH
VzZXIEADBIDbDbWk5fq1JFRF9QUk1OQ01QQUXfvVVJRdatMCScaQQMJdcwmZawODQ2LWViZGUtMTFlNS05Z
WZjLTAwMGMyOTRhYjk4MAQAMCOMEUFat19DUkVEX1PFUF9JTkZPMBgwFgIBBAwPU1NLOibUTFNWMTI6IDBB
BAANQwUQVPoX0NSRURfUKVHSVNuu1lfSUQwHTABAgEEDBRbj10ZXN0dXN1cixkYzlp3dnYyQQAAMB8MEKF
at19DUkVEX1VTRVJfsU5GTzAJMACAOOMAACCMEEFat19DUkVEX1ZFU1NJTO4wEZARAQAEEDAowedAwDM
```

```
AwOTAxBAAwMAwMZWlhaWxBZGRyZXNzMCAwHgIBBAwXdGVzdHVzZXJAbWFpbGluYXRvci5jb20EADArDALma
XJzdE5hbWUwHjALAgEEDARUZXXN0BAAwDwIBBAwIdGVzdHVzZXIEADAZDAhsYXN0TmFtZTANMAAsCAQQMBFVz
ZXIEADAtDBh0YWd2YWx1ZV9sb2dpbl91c2VyX25hbWUwETAPAgEEDAh0ZXN0dXNlcgQAMdYmJHRhZ3ZhbHV
lX21heF9jb25jdXJyZW50X3dlY19zZXNzaW9uc2AOMAwCAQQMBXVuc2V0BAAwRwwWdGFndmFsdWVfc2Vzc2
lvbl9pbmRleDatMCsCAQQMJDNkNjc0ZTc4LWVjY2EtMTFlNSliZTRmLTAwMGMyOTRhYjk4MAQAMIGpDBh0Y
Wd2YWx1ZV91c2VyX3Nlc3Npb25faWQwgYwwgYkCAQQMGYFiRzlgWVd4b2IzTjBMV1JsWmlGMWJIUUFfVnVl
Ui9BQUFBQUlBQUFBd0FBQUFBG1JQ21pd2Z3QUFWMnM1WXpOSWVtMW5aVnB4UWxreFYxTTRiRGREUkdSb2J
IZEpha296WWpCNmEzTjJibmhLV0dwTlFXNXFSMnRPOmRlZmFlbHQEAA=="
```

If the user's Subject details are not successfully output in the HTML

- Examine cURL command output for any error messages
- Complete the steps in *Enabling TAI Trace* on page 21
- Verify all steps in *Liberty Configuration* on page 14 were completed

Collecting Support Data

To assist with resolution of a support issue, ensure you have collected and reviewed the trace for the components configured in this integration.

Collecting Data for ISAM: Web Gateway Appliance

In most cases, submitting the support file to IBM Support is the first step in successfully assisting IBM in troubleshooting your support issue.

Please follow these instructions to create then upload file to IBM support:

<http://www-01.ibm.com/support/docview.wss?uid=swg27041789>.

Creating a support file from the Web Gateway Appliance

To create and upload the support file to IBM support from the IBM Security Web Gateway Appliance, refer to <http://www-01.ibm.com/support/docview.wss?uid=swg21663426>.

Security Access Manager for Web trace

For additional trace options, refer to <http://www-01.ibm.com/support/docview.wss?uid=swg21663410>.

pdweb.debug

The `pdweb.debug` trace will assist in identifying errors related to SSO from Security Access Manager.

To enable tracing:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Edit**.

7. In the Edit Trace Component window:
 - a. Level: **2**
 - b. Flush Interval (seconds): **5**
 - c. Rollover Size (bytes): <default>
 - d. Click **Save**.

To disable trace, set the Level to 0.

To review the trace file generated:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the **pdweb.debug** row.
6. Click **Files**.
7. In the Manage Trace Files – pdweb.debug window
 - a. Select **pdweb.debug.log**
 - b. Click **View**
 - c. Number of lines to view: **1000** (depending on the number of requests)
 - d. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation
224A/101
11400 Burnet Road*

Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2016. Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp 2016, 2016. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.