

## Web Single Sign-On with SAML 2.0

*This tutorial demonstrates the usage of SAML 2.0 in different Web SSO Scenarios. We will use Oracle Weblogic Server 12.1.3 as the technical platform.*

### 1 Contents

Web Single Sign-On with SAML 2.0 .....	1
1 Contents.....	1
2 Introduction .....	2
3 The Web SSO Tutorial.....	2
3.1 Tutorial Files.....	2
3.2 Documentation Links .....	3
3.3 Installation of Java.....	4
3.4 Installation of Weblogic Server 12.1.3.....	6
3.5 Example Overview .....	8
3.6 Creating Domains and Deploying Applications.....	13
3.7 Configuring SAML.....	14
3.7.1 create SAML 2.0 Credential Mapper Provider .....	15
3.7.2 configure SAML 2.0 General Settings.....	16
3.7.3 configure SAML 2.0 Identity Provider .....	18
3.7.4 export adminA_metadata.xml .....	19
3.7.5 create SAML 2.0 Identity Assertion Provider.....	20
3.7.6 configure SAML 2.0 General Settings.....	21
3.7.7 configure SAML 2.0 Service Provider.....	22
3.7.8 export adminB_metadata.xml .....	23
3.7.9 create Partner-Idp-adminA .....	24
3.7.10 import adminA_metadata.xml.....	25
3.7.11 configure Partner-IdP-adminB .....	26
3.7.12 create Partner-SP-adminB .....	27
3.7.13 Import adminB_metadata.xml.....	28
3.7.14 configure Partner-SP-adminB .....	29
3.8 Testing the example.....	30
3.8.1 Testing via URL to IdP .....	31
3.8.2 Testing via URL to SP .....	32
3.9 Setting Debug Flags for the Example.....	33
3.10 Configuring IdP initiated flow with POST Binding. ....	33
3.10.1 Configure an additional end user URL.....	34
3.10.2 Configure the POST Binding POST Form.....	34

Web Single Sign-On with SAML 2.0

3.11	Configuring Virtual User: .....	37
3.12	Setting the Binding Sequence .....	38
3.13	SAML 2.0 Examples in Blog Posts. ....	39
3.14	Conclusion .....	39

## 2 Introduction

While SAML is already widely used in the industry, the configuration within Weblogic Server is complex and in most companies not part of the regular routine. We want to have look at a simple SAML example that was published in an article by Vikrant Sawant in 2007. <http://www.oracle.com/au/products/database/sso-with-saml-099684.html> This former example demonstrates a Web SSO scenario using SAML 1.1 in Weblogic Server 9.2. We want to upgrade this example, using SAML 2.0 in Weblogic Server 12.1.3.

This is a tutorial in which we will walk through all the necessary steps to setup and run the SAML 2.0 example. This includes the installation and configuration of weblogic server, creation of two weblogic server domains, installation of the test applications and configuration of the identity provider and service provider domains. To provide a comprehensive overview, the separate tutorial steps are summarized in mind map diagrams. The tutorial comprises a Service Provider initiated flow and an Identity Provider initiated flow, which both will be demonstrated during the testing steps. As an addition, the tutorial demonstrates the usage of the weblogic feature “virtual user”.

The tutorial was developed and tested on a windows 7 machine. A zip package containing all necessary files is provided at the tutorial website. This also includes a text file with a set of windows commands to help setting up the domains and user configurations. We expect the tutorial to run also on Linux or any other platform supported by weblogic server, although this was not tested.

## 3 The Web SSO Tutorial

### 3.1 Tutorial Files

The following files are located at the website [www.andreaswittmann.de](http://www.andreaswittmann.de):

[www.andreaswittmann.de/weblogic-corner/saml2\\_sso/SAML2\\_Web\\_SSO\\_Tutorial.pdf](http://www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML2_Web_SSO_Tutorial.pdf)  
[www.andreaswittmann.de/weblogic-corner/saml2\\_sso/SAML\\_SSO.zip](http://www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML_SSO.zip)

The zip archive contains the following files:

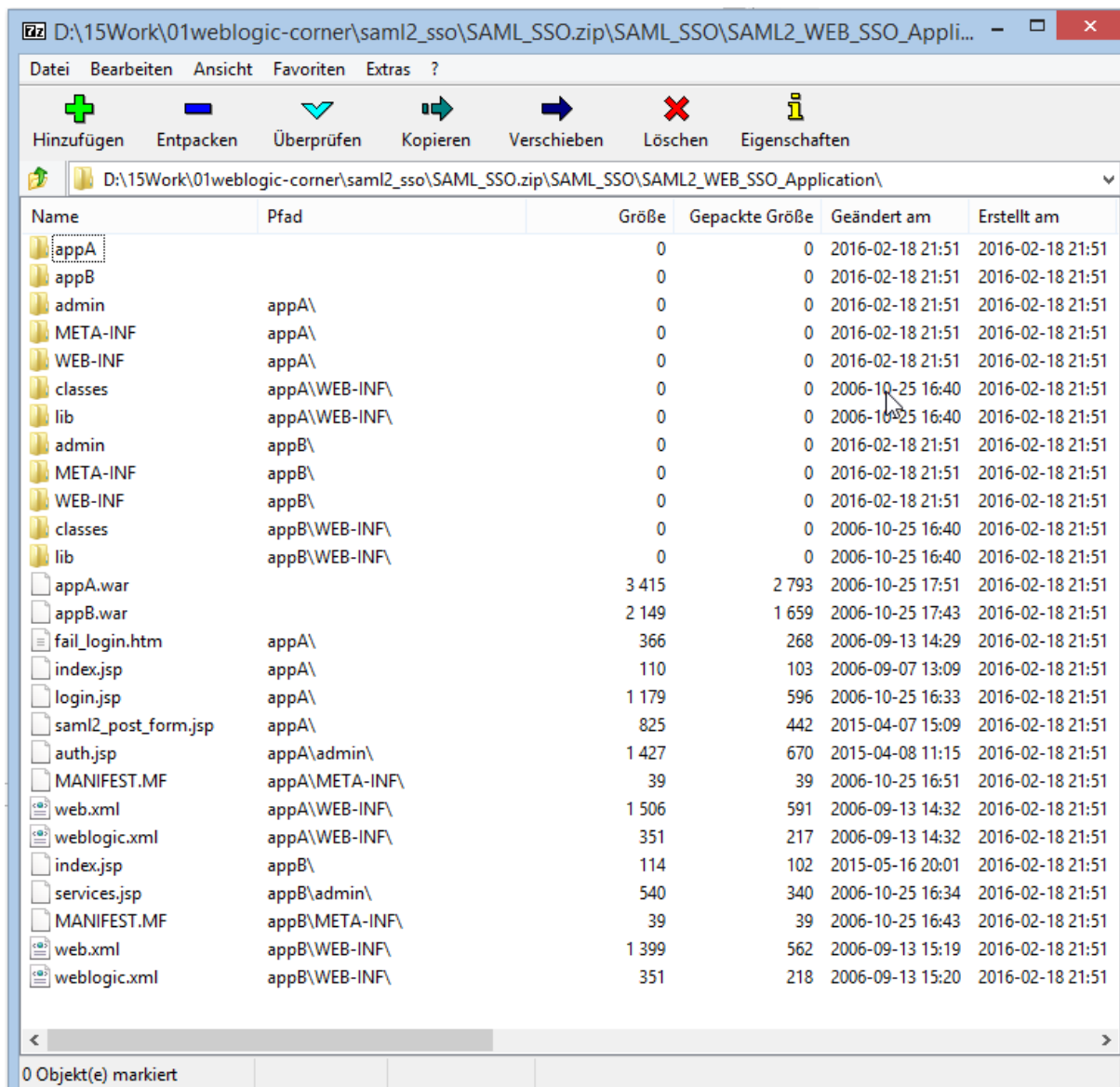


Figure 1. Contents of the archive SAML\_SSO.zip

### 3.2 Documentation Links

We summarize some documentations links in the following table.

OASIS SAML Home Page	<a href="https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security">https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security</a>
OASIS SAML Executive Overview (PDF)	<a href="http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf">http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf</a>
OASIS SAML Technical Overview (PDF)	<a href="http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf">http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf</a>
SAML 2.0,ein Tutorium – Teil 1:	kain_keller_JS_05_0_Annotated.pdf (Article in

Theorie aus XML Spectrum ( <a href="http://www.javaspectrum.de">www.javaspectrum.de</a> )	German)
Configuring SAML 2.0 Services in Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server	<a href="http://docs.oracle.com/middleware/1213/wls/SECMG/saml20.htm#SECMG318">http://docs.oracle.com/middleware/1213/wls/SECMG/saml20.htm#SECMG318</a>

### 3.3 Installation of Java

We install the latest Java 7 JDK from the download link

<http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>

**Java SE Development Kit 7u76**  
You must accept the [Oracle Binary Code License Agreement for Java SE](#) to download this software.  
Thank you for accepting the [Oracle Binary Code License Agreement for Java SE](#); you may now download this software.

Product / File Description	File Size	Download
Linux x86	119.46 MB	<a href="#">jdk-7u76-linux-i586.rpm</a>
Linux x86	136.8 MB	<a href="#">jdk-7u76-linux-i586.tar.gz</a>
Linux x64	120.84 MB	<a href="#">jdk-7u76-linux-x64.rpm</a>
Linux x64	135.66 MB	<a href="#">jdk-7u76-linux-x64.tar.gz</a>
Mac OS X x64	185.91 MB	<a href="#">jdk-7u76-macosx-x64.dmg</a>
Solaris x86 (SVR4 package)	139.47 MB	<a href="#">jdk-7u76-solaris-i586.tar.Z</a>
Solaris x86	95.55 MB	<a href="#">jdk-7u76-solaris-i586.tar.gz</a>
Solaris x64 (SVR4 package)	24.69 MB	<a href="#">jdk-7u76-solaris-x64.tar.Z</a>
Solaris x64	16.37 MB	<a href="#">jdk-7u76-solaris-x64.tar.gz</a>
Solaris SPARC (SVR4 package)	138.74 MB	<a href="#">jdk-7u76-solaris-sparc.tar.Z</a>
Solaris SPARC	98.64 MB	<a href="#">jdk-7u76-solaris-sparc.tar.gz</a>
Solaris SPARC 64-bit (SVR4 package)	23.94 MB	<a href="#">jdk-7u76-solaris-sparcv9.tar.Z</a>
Solaris SPARC 64-bit	18.36 MB	<a href="#">jdk-7u76-solaris-sparcv9.tar.gz</a>
Windows x86	127.81 MB	<a href="#">jdk-7u76-windows-i586.exe</a>
Windows x64	129.55 MB	<a href="#">jdk-7u76-windows-x64.exe</a>

**Java SE Development Kit 7u76 Demos and Samples Downloads**  
You must accept the [Oracle BSD License](#) to download this software.  
Thank you for accepting the [Oracle BSD License](#); you may now download this software.

Product / File Description	File Size	Download
Linux x86	19.91 MB	<a href="#">jdk-7u76-linux-i586-demos.rpm</a>
Linux x86	19.87 MB	<a href="#">jdk-7u76-linux-i586-demos.tar.gz</a>
Linux x64	19.95 MB	<a href="#">jdk-7u76-linux-x64-demos.rpm</a>
Linux x64	19.92 MB	<a href="#">jdk-7u76-linux-x64-demos.tar.gz</a>
Mac OS X	18.5 MB	<a href="#">jdk-7u76-macosx-x86_64-demos.tar.gz</a>
Solaris x86	23 MB	<a href="#">jdk-7u76-solaris-i586-demos.tar.Z</a>
Solaris x86	16.08 MB	<a href="#">jdk-7u76-solaris-i586-demos.tar.gz</a>
Solaris SPARC	23.04 MB	<a href="#">jdk-7u76-solaris-sparc-demos.tar.Z</a>
Solaris SPARC	16.1 MB	<a href="#">jdk-7u76-solaris-sparc-demos.tar.gz</a>
Solaris SPARC 64-bit	1.24 MB	<a href="#">jdk-7u76-solaris-sparcv9-demos.tar.Z</a>
Solaris SPARC 64-bit	0.86 MB	<a href="#">jdk-7u76-solaris-sparcv9-demos.tar.gz</a>
Solaris x64	1.23 MB	<a href="#">jdk-7u76-solaris-x64-demos.tar.Z</a>
Solaris x64	0.83 MB	<a href="#">jdk-7u76-solaris-x64-demos.tar.gz</a>
Windows x86	20.7 MB	<a href="#">jdk-7u76-windows-i586-demos.zip</a>
Windows x64	20.8 MB	<a href="#">jdk-7u76-windows-x64-demos.zip</a>

**JavaFX 2.2.76 Demos and Samples Downloads**  
You must accept the [Oracle BSD License](#) to download this software.  
Thank you for accepting the [Oracle BSD License](#); you may now download this software.

Product / File Description	File Size	Download
Linux	20.24 MB	<a href="#">javafx_samples-2_2_76-linux.zip</a>
Mac OS X	20.24 MB	<a href="#">javafx_samples-2_2_76-macosx-universal.zip</a>
Windows	20.23 MB	<a href="#">javafx_samples-2_2_76-windows.zip</a>

Figure 2. Java 7 Downloads with Demos and Samples.

We run the installer.

Datei: jdk-7u76-windows-x64.exe  
 CRC-32: a549a6a7  
 MD4: b2fbc1a78ca30c96a6e14554488f6b20  
 MD5: 02365745a4a68a44d6b6f5130a4ad4da  
 SHA-1: fa316d3c290172632a0a19afdf70e0361410ff54

The installation needs administration privileges.  
 We install to D:\10Oracle\02Java\jdk1.7.0\_76  
 The documentation can be found <http://docs.oracle.com/javase/7/docs/> here.

### 3.4 Installation of Weblogic Server 12.1.3

Reviewing the certification matrix in Excel from this link:  
<http://www.oracle.com/technetwork/middleware/fusion-middleware/documentation/fmw-1213certmatrix-2226694.xls>

Oracle Fusion Middleware 12c (12.1.3.0.0) Certification Matrix											
Oracle Fusion Middleware 12c (12.1.3.0.0) Products: 1. Oracle WebLogic Server 2. Oracle Coherence 3. Oracle HTTP Server 4. Oracle Application Development Framework 5. Oracle Fusion Middleware Infrastructure which includes: a. Oracle WebLogic and Oracle Fusion Middleware security infrastructure 6. Oracle TopLink 7. Oracle MapViewer 8. Oracle Data Integrator 9. Oracle Enterprise Data Quality 10. Oracle GoldenGate Veridata (Server, C Agent, Java Agent) 11. Oracle Golden Gate Monitor (Server, Java Agent) 12. Oracle Business Process Management 13. SOA Product Line - Oracle Service Bus, Oracle BPEL Process Manager, Oracle Event Processing, Oracle Enterprise Repository, Oracle SOA Suite (Oracle BPEL Process Manager, Oracle Service Bus, Oracle Business Activity Monitoring, Oracle B2B, Oracle Enterprise Scheduler, Oracle Event Processing, Oracle Application Integration Architecture Foundation Pack, Oracle Business Rules, Oracle Mediator, Oracle Human Workflow), Oracle Managed File Transfer and Oracle API Manager.											
ALL includes the following products: Fusion Middleware 12c Products, with the Exception of: Oracle Data Integrator (Agent, Studio, Console), Oracle Data Service Integrator (Server, IDE, Console) Oracle GoldenGate Veridata (Server, C Agent, Java Agent), Oracle Golden Gate Monitor (Server, Java Agent).											
<a href="http://www.oracle.com/technetwork/middleware/fmw/121300/downloads/fusion-certification-100350.html">For complete Fusion Middleware, OBI EE, and EPM product certifications, refer to http://www.oracle.com/technetwork/middleware/fmw/121300/downloads/fusion-certification-100350.html.</a> <a href="http://www.oracle.com/technetwork/middleware/fmw/121300/downloads/oracleas-supported-virtualization-089265.html">For information on supported Virtualization and Partitioning Technologies, refer to http://www.oracle.com/technetwork/middleware/fmw/121300/downloads/oracleas-supported-virtualization-089265.html.</a> <a href="http://www.oracle.com/pls/topic/lookup?ctx=fmw121300&amp;id=INTOP310">For Interoperability and Compatibility Information, refer to http://www.oracle.com/pls/topic/lookup?ctx=fmw121300&amp;id=INTOP310</a> <a href="http://www.oracle.com/technetwork/developer-tools/dev/documentation/121300-cert-2164864.html">For information on Oracle JDeveloper supported configurations, refer to http://www.oracle.com/technetwork/developer-tools/dev/documentation/121300-cert-2164864.html</a> <a href="http://www.oracle.com/technetwork/middleware/adapters/overview/adapters-12c-certmatrix-2328619.xls">For information on Adapter certifications, refer to http://www.oracle.com/technetwork/middleware/adapters/overview/adapters-12c-certmatrix-2328619.xls</a>											
Product Offering	RELEASE	PROCESSOR	OSVERSION	OS Update Type	OS Update Level	OS 32bit	ORA CLEA PPR	JDKVENDOR	JDKVERSION	JDK32bit	EXCEPTIONSADDITIONALINFO
Oracle WebLogic Server Oracle Data Integrator Agent Oracle GoldenGate Veridata Java Agent Oracle GoldenGate Monitor Java Agent	FMW 12.1.3.0.0	Microsoft Windows x64 (64-bit)	7	Service Pack	1	64	64	Oracle JDK	1.7.0_51+	64	This 64 bit operating system is supported for single user only in a development environment.
*OS Update Level		The version listed specifies the minimum update level / service pack / technology level certified. For example, 6 means that 6 and higher is certified.									
*JDKVERSION		A plus sign (+) after the fourth digit in the version number indicates that this and all higher versions of the JRE/JINT/JDK extensions are certified. For example, 1.7.0_55+ means that 1.7.0_55 and any higher 1.7.0_xx versions are certified.									

Figure 3. Certification Matrix showing the certified release for Windows 7, 64 bits.

From the OTN we download the zip distribution and the supplement zip from this download link: <http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html>

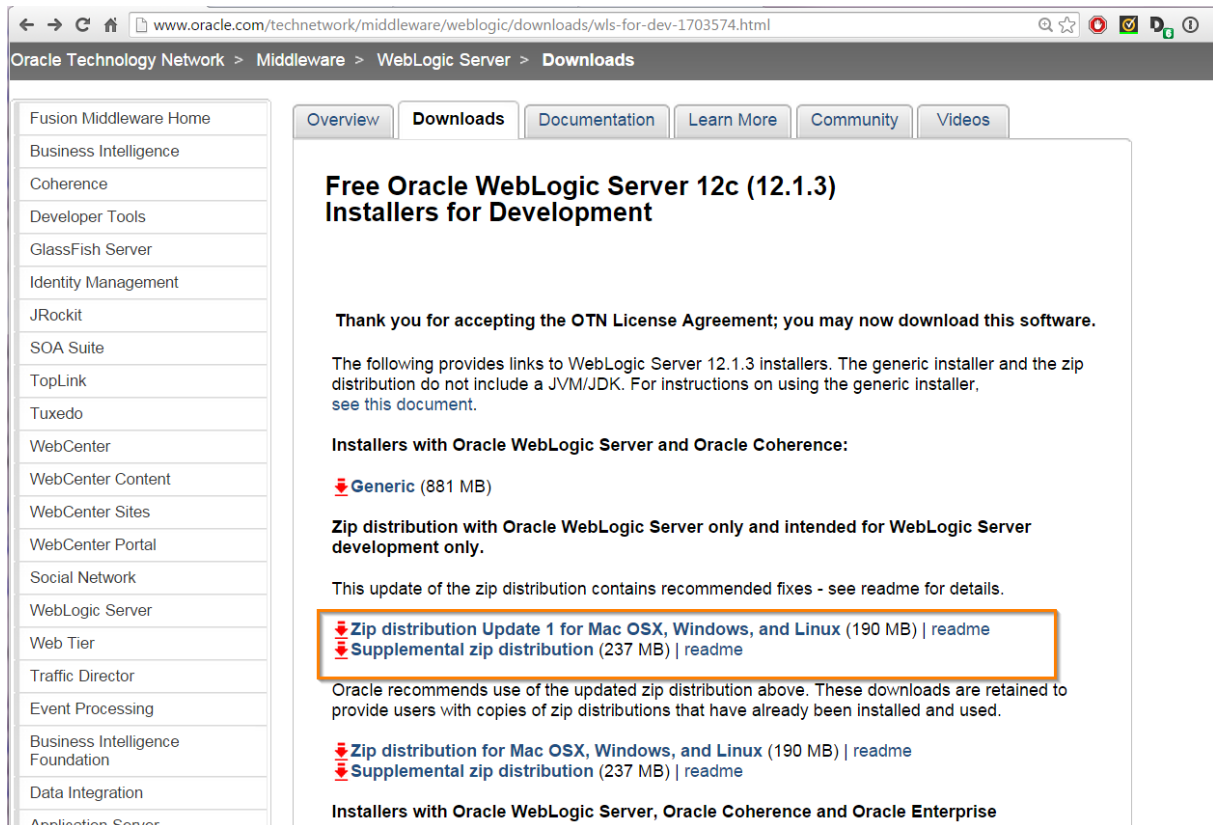


Figure 4. OTN Download Page for Weblogic Server.

We follow the instruction of the Readme.

Frist we unzip the distribution to a location which will become the new middleware home for this installation.

The windows file explorer fails to unzip 2 files from the package because filenames are too long.

We use the jar tool to unzip instead and it works fine.

Running the installation:

```
D:\>cd D:\10Oracle\06WLS12\wls12130
D:\10Oracle\06WLS12\wls12130>set MW_HOME=D:\10Oracle\06WLS12\wls12130
D:\10Oracle\06WLS12\wls12130>set JAVA_HOME=D:\10Oracle\02Java\jdk1.7.0_76
D:\10Oracle\06WLS12\wls12130>configure.cmd

## Creating a new Domain:

D:\10Oracle\06WLS12\domains\mydomain>%JAVA_HOME%\bin\java.exe %JAVA_OPTIONS% -Xmx1024m -XX:MaxPermSize=256m weblogic.Server
## User=weblogic
## Password=welcome1

## Starting new domain (in new shell)
D:
cd D:\10Oracle\06WLS12\domains\mydomain
set MW_HOME=D:\10Oracle\06WLS12\wls12130
set JAVA_HOME=D:\10Oracle\02Java\jdk1.7.0_76
startWebLogic.cmd
```

The newly created domain can be found at <http://localhost:7001/console>

Running the installation of the supplement package:

```
D:\10Oracle\06WLS1213>set JAVA_HOME=D:\10Oracle\02Java\jdk1.7.0_76
D:\10Oracle\06WLS1213>%JAVA_HOME%\bin\jar -xvf wls1213_devzip_supplemental_update1.zip
```

Error Message:

```
D:\10Oracle\06WLS12\wls12130>run_samples.cmd
"Setting up proper ACLs for D:\10Oracle\06WLS12\wls12130 ... (operation takes awhile)"
Zuordnungen von Kontennamen und Sicherheitskennungen wurden nicht durchgefuehrt.
Username:weblogic
```



```
password: Die Version von D:\10Oracle\06WLS12\wls12130\mask.com ist nicht mit der ausgeführten Windows-Version kompatibel.  
Öffnen Sie die Systeminformationen des Computers, um zu überprüfen, ob eine x86-(32 Bit)- oder eine x64-(64 Bit)-Version des Programms erforderlich ist, und wenden Sie sich anschließend an den  
Herausgeber der Software.  
Re-enter password:Die Version von D:\10Oracle\06WLS12\wls12130\mask.com ist nicht mit der ausgeführten Windows-Version  
kompatibel. Öffnen Sie die Systeminformationen des Computers, um zu überprüfen, ob eine x86-(32 Bit)- oder eine x64-(64 Bit)-Version des Programms erforderlich ist, und wenden Sie sich  
anschließend an den Herausgeber der Software.  
"pwdset" kann syntaktisch an dieser Stelle nicht verarbeitet werden.
```

There are conflicts with Windows 64 bit versions.

Solutions: We supply username and password on the command line, thus mask.com is not called.

We ignore the ACL Settings, instead we start a command shell as administrator.

```
D:\10Oracle\06WLS12\wls12130>run_samples.cmd weblogic welcome1
```

To start the example server:

```
D:  
cd D:\10Oracle\06WLS12\wls12130\wlserver\samples\domains\wl_server  
set MW_HOME=D:\10Oracle\06WLS12\wls12130  
set JAVA_HOME=D:\10Oracle\02Java\jdk1.7.0_76  
startWebLogic.cmd
```

It will be available at <http://192.168.56.1:7001/index.jsp>

Ok.

### 3.5 Example Overview

In this tutorial we want to demonstrate two message flows which stem directly from the “OASIS SAML Technical Overview” document. The first case is the “SP-Initiated SSO with Redirect and POST Binding”. We copy the relevant image from the document and overlay it with the servers and components which will form this example.



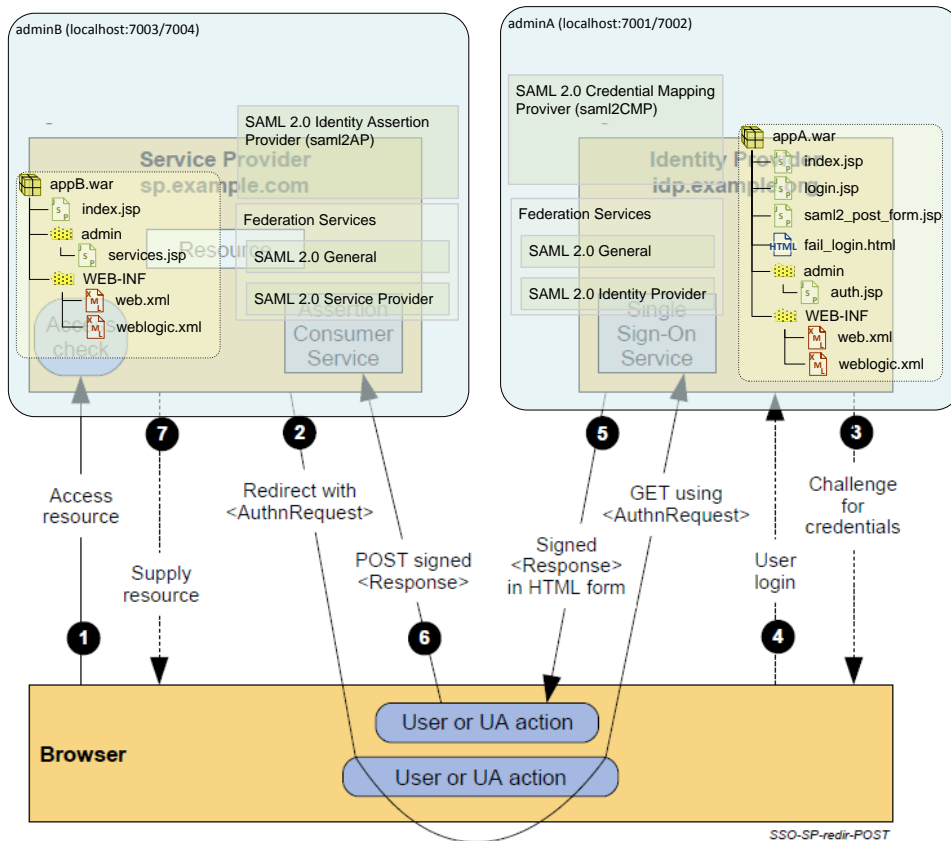


Figure 12: SP-Initiated SSO with Redirect and POST Bindings

Figure 5. OASIS Message Flow picture with overlaid tutorial components.

The Service Provider will be realized by the WLS server adminB, the saml2AP Identity Assertion Provider together with the Federation Services provide the Assertion Consumer Service. The resource, which is accessed, is provided by the services.jsp. The Identity Provider will be configured as adminA. Here we use a SAML 2.0 Credential Mapping Provider together with the Federation Services to provide the Single Sign-On Service. The Login module will be provided by the login.jsp.

With a very similar picture, we present the IdP-Initiated SSO case.

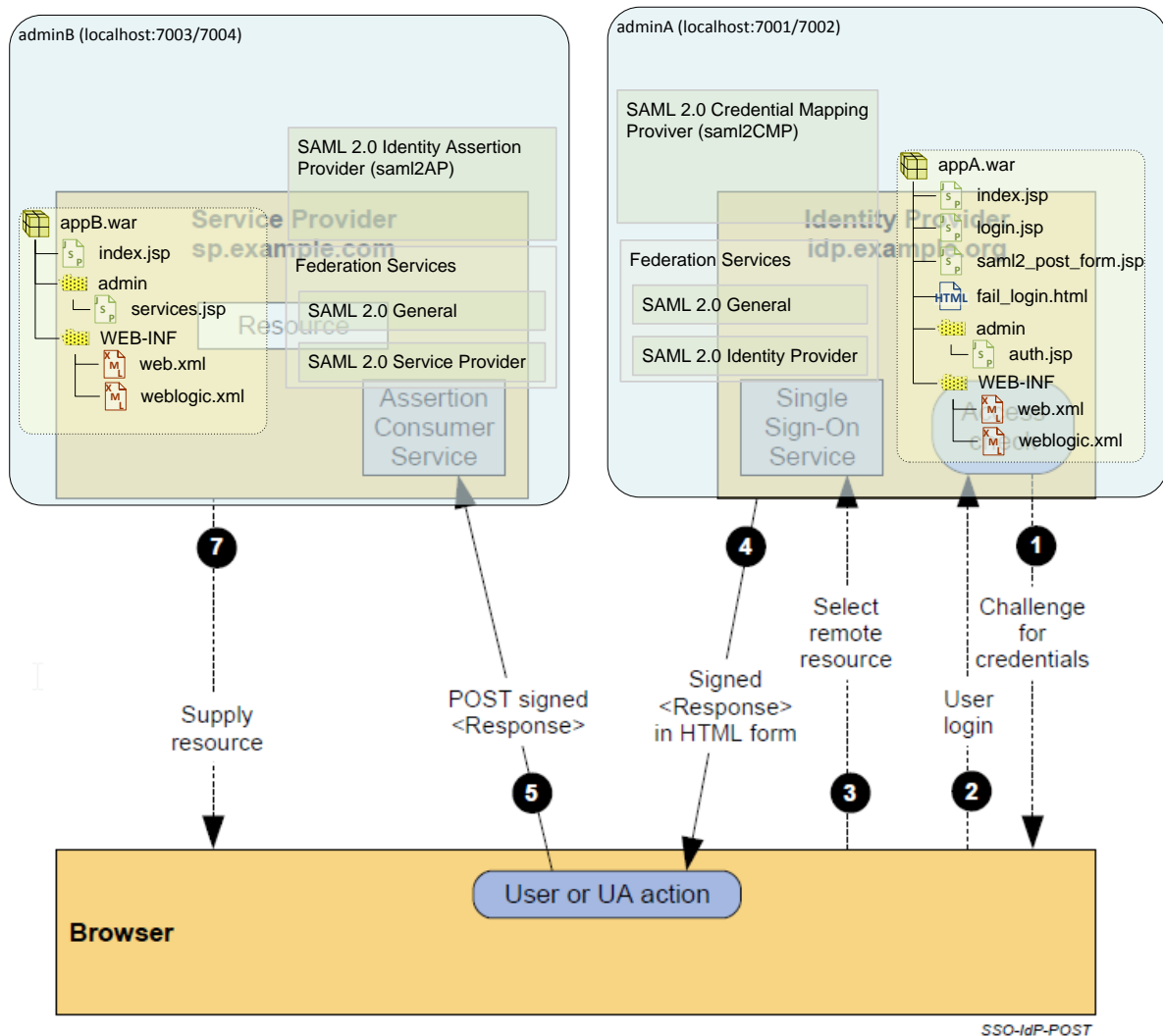
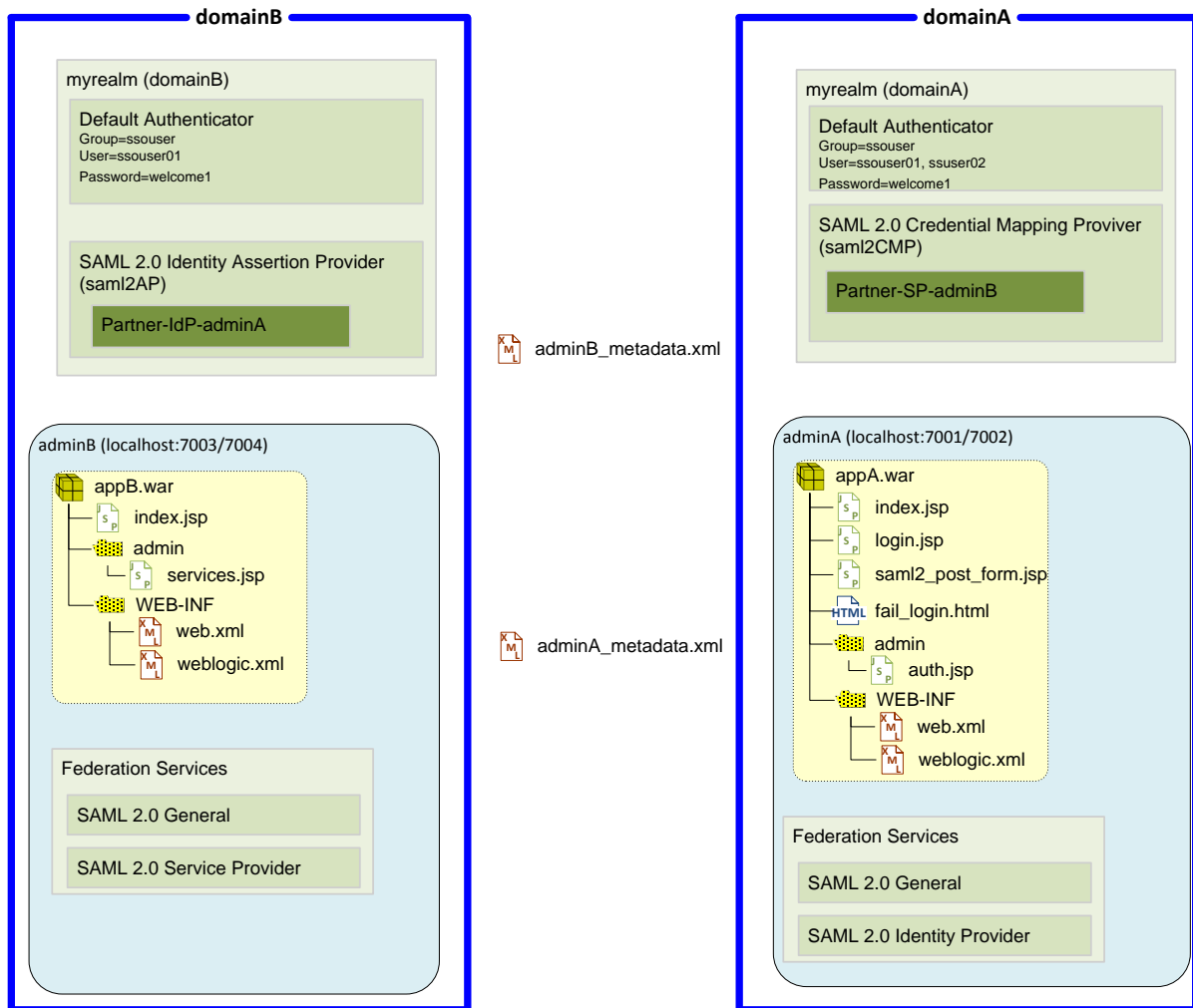


Figure 14: IdP-Initiated SSO with POST Binding

Figure 6. OASIS Message Flow picture with overlaid tutorial components for IdP-Initiated Message Flow.

The components are the same as in the previous picture; however the message flow is different. The page that offers the remote resource in step 3 is provided by admin/auth.jsp. The POST form for step 4 and 5 is provided by saml2\_post\_form.jsp.

We will build up two WLS domains, each consisting only of a single Admin Server. We will configure the Federation Services between these domains as depicted in the following overview.



**Figure 7. Domain configuration for this example with Federation Services.**

We use adminB and adminA in domainB and domainA respectively. adminB will host appB which represents the service provided by the SAML Service Provider. adminA will host appA, which contains a login page and a service selection page. The security realms are also shown, together with the relevant users, groups and security providers.

The following diagram proposes a configuration sequence and depicts configuration details.

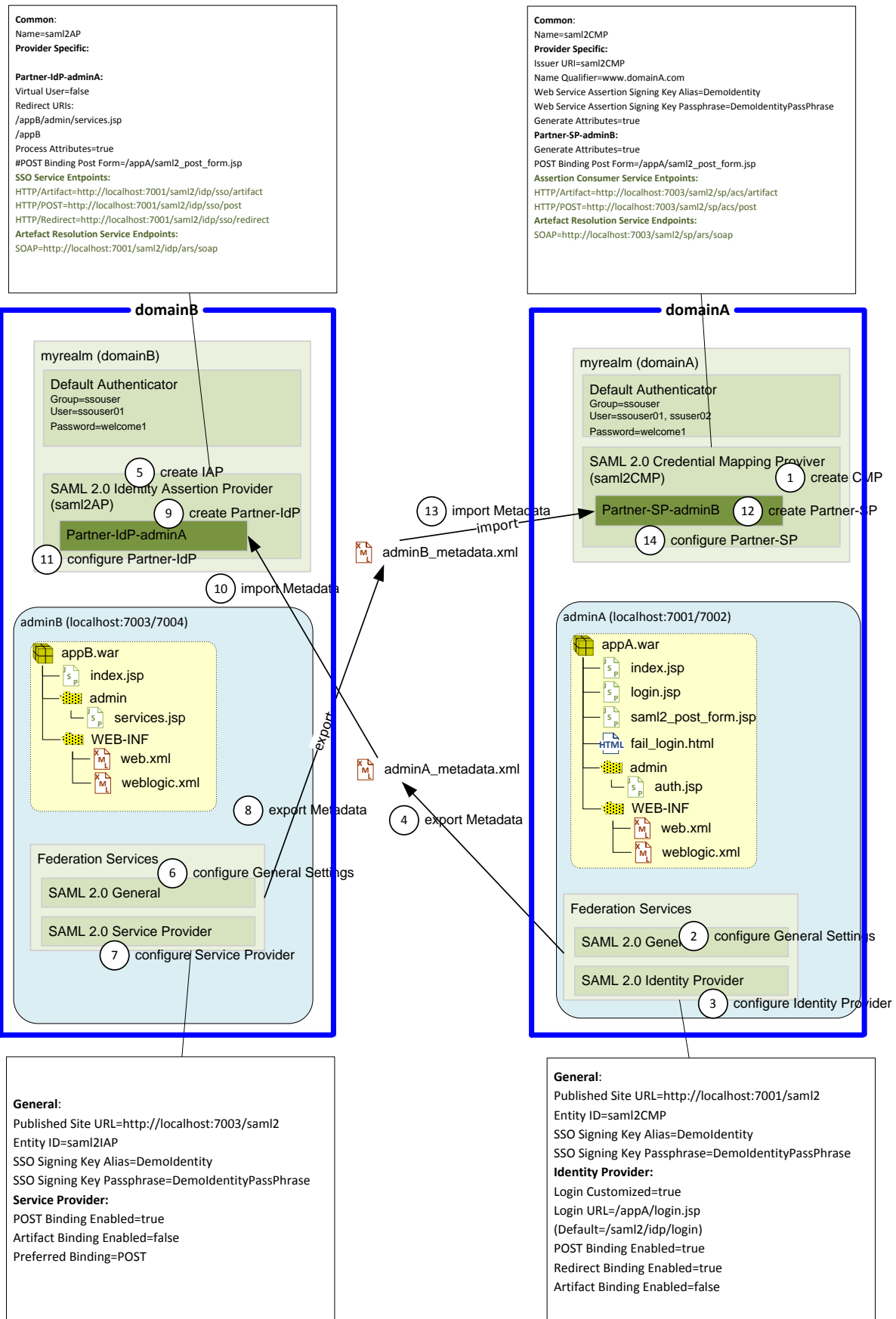


Figure 8. Proposed configuration sequence for the example.

The numbers in the circles propose a configuration sequence which is not mandatory but recommended to complete this task efficiently. The configuration steps are explained on more detail in the Chapter 3.6 and the section numbers map to this sequence.

The activities of the whole tutorial are split into four parts. We depict a summary in the following mind map.

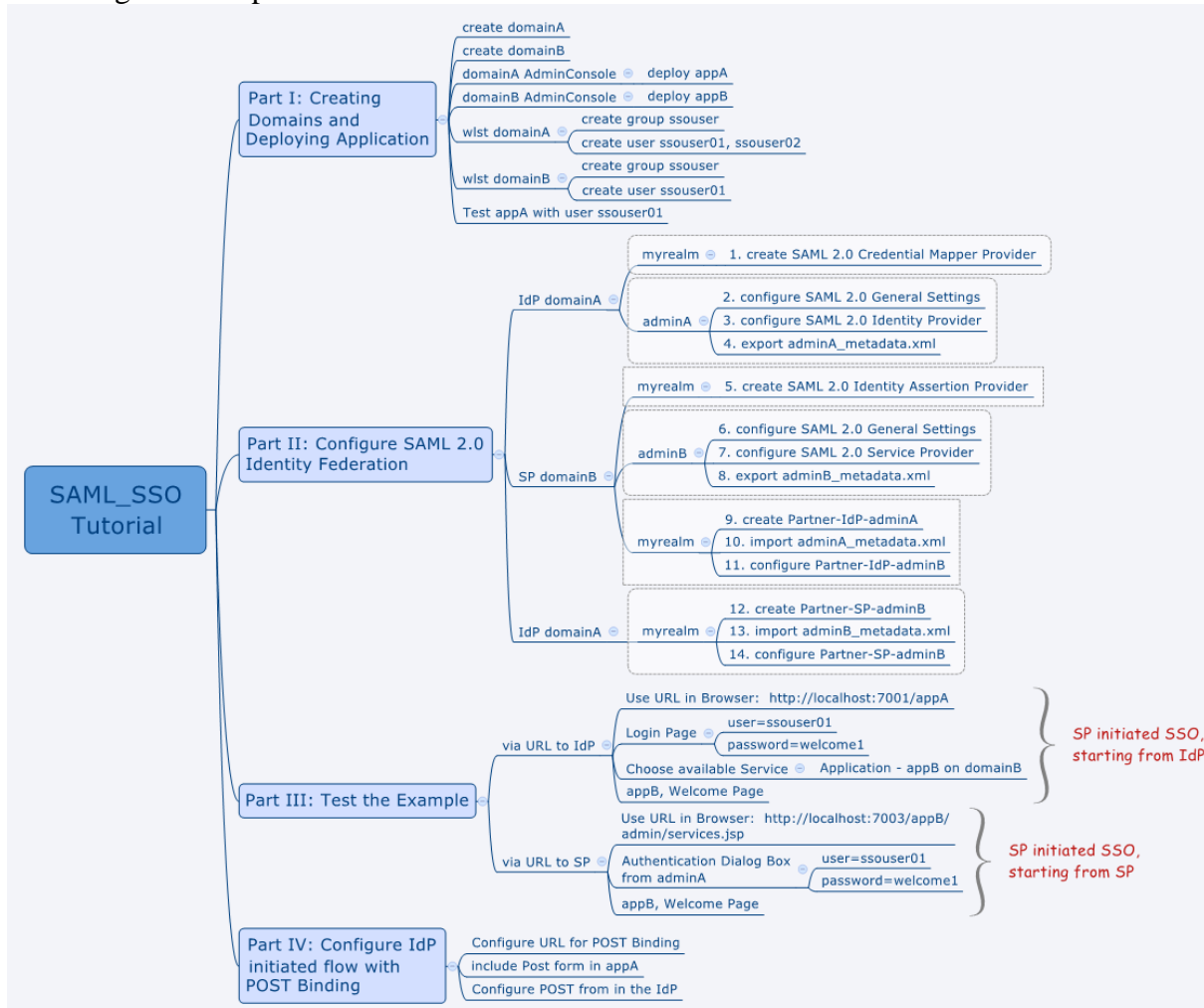


Figure 9. Mind map summarizing the parts of this tutorial.

### 3.6 Creating Domains and Deploying Applications

In this step we configure two domains and deploy the sample application. The commands to setup the domains are contained in the file `${EXAMPLE_HOME}\SAML_SSO\SAML_SSO.TXT`. We provide an overview mind map of the configuration steps.

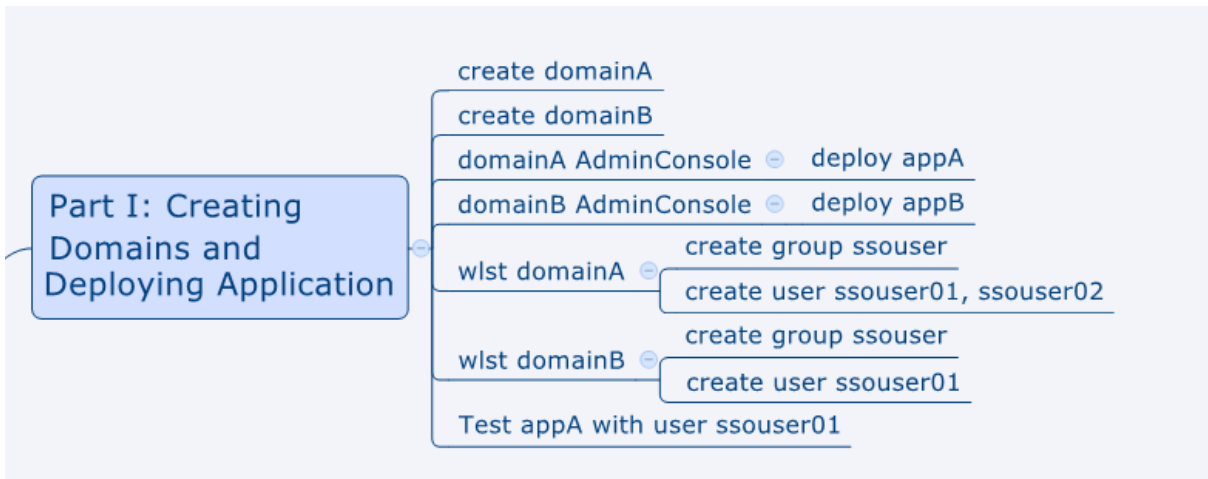


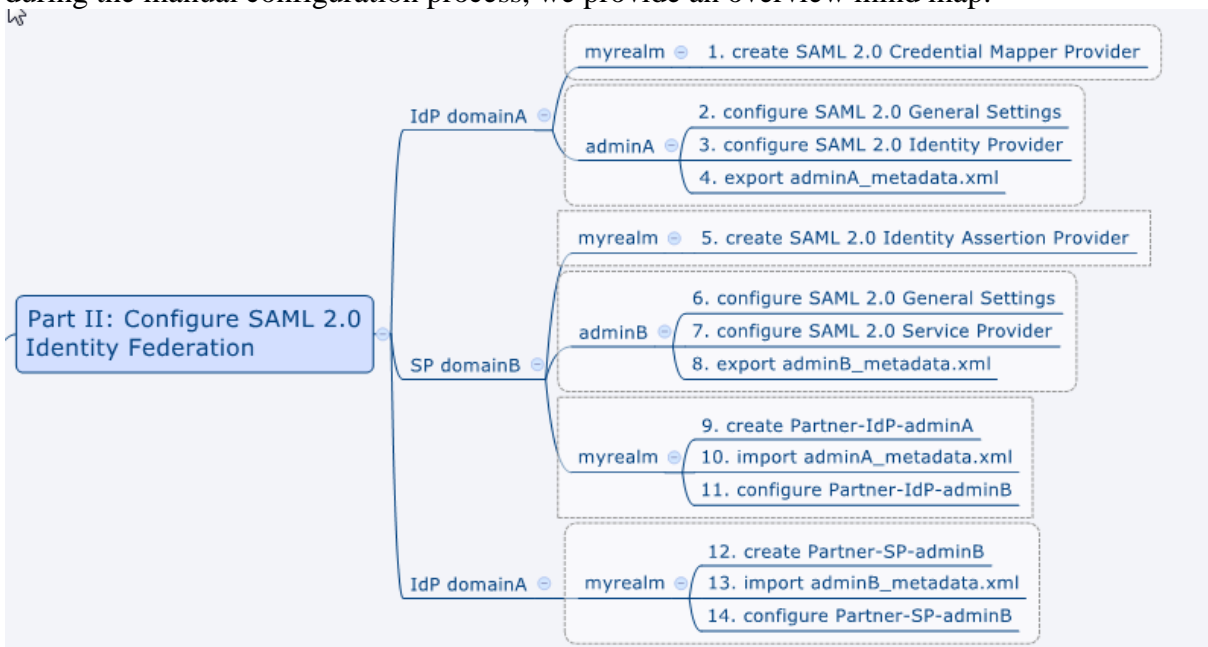
Figure 10. Overview Mind Map for setting up the example domains.

We deploy appA and appB using the admin console. We create the users and groups using the wlst commands in the file SAML\_SSO.TXT.

Application Folder	\${EXAMPLE_HOME}\SAML_SSO\SAML_SSO.TXT.
domainA	<a href="http://localhost:7001/console">http://localhost:7001/console</a>
appA	<a href="http://localhost:7001/appA">http://localhost:7001/appA</a>
User/password	ssouser/welcome1
domainB	<a href="http://localhost:7003/console">http://localhost:7003/console</a>
appB	<a href="http://localhost:7003/appB">http://localhost:7003/appB</a>
appB	<a href="http://localhost:7003/appB/admin/services.jsp">http://localhost:7003/appB/admin/services.jsp</a>

### 3.7 Configuring SAML

In following steps we want to configure this SAML example. Since it is easy to get lost during the manual configuration process, we provide an overview mind map.



**Figure 11. Mind Map Overview of the SAML Configuration Process.**

The configuration begins in domainA, which will be configured as Identity Provider. We need to configure a Credential Mapping Provider in the security realm. In the server settings of adminA we need to configure the “Federation Services”. In order to conclude the configuration of domainA we need to import the metadata file of the Service Provider which will be produced during the SAML configuration in domainB. Therefore we continue with the configuration of domainB. After that, we change back to domainA and complete the configuration here.

The individual steps from the mind map are explained in detail in the following sub sections.

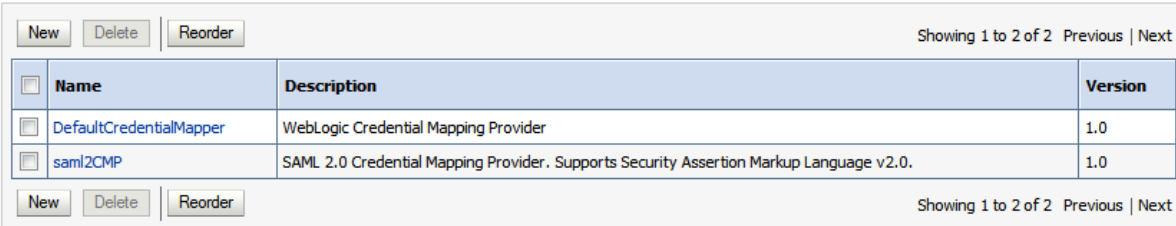
**3.7.1 create SAML 2.0 Credential Mapper Provider**

We start with the IdP in domain.

We enable the SSL Port. We use the Demo Certificates

Configure a new credential mapping provider.

(Security Realms->myrealm->Providers->new->SAML 2.0 Credential Mapping Provider)



The screenshot shows the 'Credential Mapping Providers' management console. At the top, there are buttons for 'New', 'Delete', and 'Reorder'. Below these is a table with the following data:

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultCredentialMapper	WebLogic Credential Mapping Provider	1.0
<input type="checkbox"/>	saml2CMP	SAML 2.0 Credential Mapping Provider. Supports Security Assertion Markup Language v2.0.	1.0

At the bottom of the table, there are again buttons for 'New', 'Delete', and 'Reorder'. The text 'Showing 1 to 2 of 2 Previous | Next' appears on both the top right and bottom right of the table area.

**Figure 12. Creating a new SAML 2.0 Credential Mapping Provider for domain.**

We configure the newly created provider.

For signing we use the DemoIdentity/DemoIdentityPassPhrase.



Settings for saml2CMP

Configuration Management Migration

Common Provider Specific

Save

Use this page to configure provider-specific information for this SAML 2.0 Credential Mapping provider.

**Issuer URI:**  The Issuer URI, or name, of this SAML 2.0 Credential Mapping provider. The value that you specify for Issuer URI should match the Entity ID specified in the SAML 2.0 General page that configures the per server SAML 2.0 properties. [More Info...](#)

**Name Qualifier:**  The Name Qualifier value used by the Name Mapper. [More Info...](#)

**Default Time To Live:**  The time in seconds that, by default, an assertion should remain valid. The default value is 120 seconds (2 minutes). [More Info...](#)

**Default Time To Live Offset:**  The time factor you can use to allow the Credential Mapping provider to compensate for clock differences between the Identity Provider and Service Provider sites. [More Info...](#)

**Web Service Assertion Signing Key Alias:**  The alias used to retrieve from the keystore the key that is used to sign assertions. This attribute is used for Web Services support of SAML Token Profile only. [More Info...](#)

**Web Service Assertion Signing Key Pass Phrase:**  The credential, or password, used to retrieve from the keystore the keys used to sign assertions. This attribute is used for Web Services support of SAML Token Profile only. [More Info...](#)

**???password.confirmation.label???:**

**Name Mapper Class Name:**

**Generate Attributes** Specifies whether information, in addition to the username, will be generated in the SAML 2.0 assertion. For example, group information. Note that the Service Provider partner needs to have a SAML Authentication provider configured to be able to extract and use the attribute information contained in the assertion. [More Info...](#)

Save

Figure 13. Provider specific configuration of the SAML Credential Mapper.

We need to restart the Admin Server.

### 3.7.2 configure SAML 2.0 General Settings

Now we create the SAML Metadata or the server specific SAML 2 profile.

Settings for adminA

**Configuration** Protocols Logging Debug Monitoring Control Deployments Services Security Notes


General Cluster Services Keystores SSL **Federation Services** Deployment Migration Tuning Overload Health Monitoring Server Start Web Services Coherence

SAML 1.1 Source Site SAML 1.1 Destination Site **SAML 2.0 General** SAML 2.0 Identity Provider SAML 2.0 Service Provider

Save Publish Meta Data

This page configures the general SAML 2.0 per server properties

— General —

 **Replicated Cache Enabled** Specifies whether the persistent cache (LDAP or RDBMS) is used for storing SAML 2.0 artifacts and authentication requests. [More Info...](#)

— Site Info —

<b>Contact Person Given Name:</b>	<input type="text" value="Duck"/>	The contact person given (first) name. <a href="#">More Info...</a>
<b>Contact Person Surname:</b>	<input type="text" value="Donald"/>	The contact person surname (last name). <a href="#">More Info...</a>
<b>Contact Person Type:</b>	<input type="text" value="technical"/> ▼	The contact person type. <a href="#">More Info...</a>
<b>Contact Person Company:</b>	<input type="text" value="Disney"/>	The contact person's company name. <a href="#">More Info...</a>
<b>Contact Person Telephone Number:</b>	<input type="text"/>	The contact person's telephone number. <a href="#">More Info...</a>
<b>Contact Person Email Address:</b>	<input type="text"/>	The contact person's e-mail address. <a href="#">More Info...</a>
<b>Organization Name:</b>	<input type="text"/>	The organization name. <a href="#">More Info...</a>
<b>Organization URL:</b>	<input type="text" value="http://www.domainA.com"/>	The organization URL. <a href="#">More Info...</a>
<b>Published Site URL:</b>	<input type="text" value="http://localhost:7001/saml2"/>	The published site URL. <a href="#">More Info...</a>
<b>Entity ID:</b>	<input type="text" value="saml2CMP"/>	The string that uniquely identifies the local site. <a href="#">More Info...</a>

Figure 14. SAML 2.0 configuration of general per server settings.

— Bindings —		
<input checked="" type="checkbox"/> Recipient Check Enabled		Specifies whether the recipient/destination check is enabled. When true, the recipient of the SAML Request/Response must match the URL in the HTTP Request. <a href="#">More Info...</a>
<input type="checkbox"/> Transport Layer Client Authentication Enabled		Specifies whether TLS/SSL client authentication is required. <a href="#">More Info...</a>
Transport Layer Security Key Alias:	<input type="text"/>	The string alias used to store and retrieve the server's private key, which is used to establish outgoing TLS/SSL connections. <a href="#">More Info...</a>
Transport Layer Security Key Passphrase:	<input type="text"/>	The passphrase used to retrieve the server's private key from the keystore. <a href="#">More Info...</a>
Confirm Transport Layer Security Key Passphrase:	<input type="text"/>	
<input type="checkbox"/> Basic Client Authentication Enabled		Specifies whether Basic Authentication client authentication is required. <a href="#">More Info...</a>
Basic Authentication User Name:	<input type="text"/>	The username that is used to assign Basic authentication credentials to outgoing HTTPS connections. <a href="#">More Info...</a>
Basic Authentication Password:	<input type="text"/>	The password used to assign Basic Authentication credentials to outgoing HTTPS connections. <a href="#">More Info...</a>
Confirm Basic Authentication Password:	<input type="text"/>	
— Artifact Resolution Service —		
Only Accept Signed Artifact Requests:	false	Specifies whether incoming artifact requests must be signed. <a href="#">More Info...</a>
Artifact Cache Size:	10000	The maximum size of the artifact cache. <a href="#">More Info...</a>
Artifact Cache Timeout:	300	The maximum timeout (in seconds) of artifacts stored in the local cache. <a href="#">More Info...</a>
— Single Sign-on —		
Single Sign-on Signing Key Alias:	<input type="text" value="Demolentity"/>	The keystore alias for the key to be used when signing documents. <a href="#">More Info...</a>
Single Sign-on Signing Key Pass Phrase:	<input type="password" value="....."/>	The passphrase used to retrieve the local site's SSO signing key from the keystore. <a href="#">More Info...</a>
Confirm Single Sign-on Signing Key Pass Phrase:	<input type="password" value="....."/>	
<input type="button" value="Save"/> <input type="button" value="Publish Meta Data"/>		

Figure 15. SAML 2.0 configuration of general per server settings. (Part 2)

### 3.7.3 configure SAML 2.0 Identity Provider

Now we change to the “SAML 2.0 Identity Provider” tab and configure the IdP. Settings of this tab will also go into the xml file containing the metadata.

We need to choose the preferred binding “Redirect”. Otherwise the Artifact Binding will be chosen from WLS.

The preferred binding will be used by the SP in domainB when sending the authentication request to the IdP (Step 2 of the SP-Initiated Flow). This information is transferred to domainB, when the metadata file is exchanged, i.e. when the metadata\_adminA.xml is imported to the “Partner-IdP-adminA”.

Home > Summary of Servers > adminA

Settings for adminA

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start

Web Services Coherence

SAML 1.1 Source Site SAML 1.1 Destination Site SAML 2.0 General SAML 2.0 Identity Provider SAML 2.0 Service Provider

Save

This page configures the SAML 2.0 per server identity provider properties

<input checked="" type="checkbox"/> Enabled	Specifies whether the local site is enabled for the Identity Provider role. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Only Accept Signed Authentication Requests	Specifies whether incoming authentication requests must be signed. If set, authentication requests that are not signed are not accepted. <a href="#">More Info...</a>
<input type="checkbox"/> Login Customized	Specifies whether a customized login web application is used. If you use a customized login web application, you must specify a login URL. If you do not customize the login, the login URL and login return query parameter are cleared when you save the changes. <a href="#">More Info...</a>
Login URL:	<input type="text" value="/saml2/idp/login"/> The URL of the login form web application to which unauthenticated requests are directed. <a href="#">More Info...</a>
Login Return Query Parameter:	<input type="text"/> The name of the query parameter to be used for conveying the login-return URL to the login form web application. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> POST Binding Enabled	Specifies whether the POST binding is enabled for the Identity Provider. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Redirect Binding Enabled	Specifies whether the Redirect binding is enabled for the Identity Provider. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Artifact Binding Enabled	Specifies whether the Artifact binding is enabled for the Identity Provider. <a href="#">More Info...</a>
Preferred Binding:	<input type="text" value="Redirect"/> Specifies the preferred binding type for endpoints of the Identity Provider services. Must be set to None,HTTP/POST, HTTP/Artifact, orHTTP/Redirect. <a href="#">More Info...</a>

Save

Figure 16. IdP configuration.

### 3.7.4 export adminA\_metadata.xml

We change back to the “SAML 2.0 General” tab and publish the Metadata to the XML file:  
D:\10Oracle\06WLS12\domains\domainA\admin\_metadata.xml

Home > Summary of Servers > adminA

Settings for adminA

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start

Web Services Coherence

SAML 1.1 Source Site SAML 1.1 Destination Site SAML 2.0 General SAML 2.0 Identity Provider SAML 2.0 Service Provider

Save Publish Meta Data

This page configures the general SAML 2.0 per server properties

— General —

Replicated Cache Enabled Specifies whether the persistent cache (LDAP or RDBMS) is used for storing SAML 2.0 artifacts and authentication requests. [More Info...](#)

— Site Info —

Contact Person Given Name: Duck The contact person given (first) name. [More Info...](#)

Contact Person Surname: Donald The contact person surname (last name). [More Info...](#)

Contact Person Type: technical The contact person type. [More Info...](#)

Contact Person Company: Disney The contact person's company name. [More Info...](#)

Contact Person Telephone Number: The contact person's telephone number. [More Info...](#)

Contact Person Email Address: The contact person's e-mail address. [More Info...](#)

Organization Name: The organization name. [More Info...](#)

Organization URL: http://www.domainB.com The organization URL. [More Info...](#)

Published Site URL: http://localhost:7001/saml2 The published site URL. [More Info...](#)

Entity ID: saml2CMP The string that uniquely identifies the local site. [More Info...](#)

Figure 17. Publishing the Metadata File of the IdP.

### 3.7.5 create SAML 2.0 Identity Assertion Provider

We create a new SAML2 Authentication Provider in the security realm “myrealm”.

The screenshot shows the 'Messages' section with a green checkmark: 'All changes have been activated. However 1 items must be restarted for the changes to take effect.' Below is the 'Settings for myrealm' page, with the 'Providers' tab selected. The 'Authentication' sub-tab is active, showing a list of authentication providers. The 'saml2AP' provider is highlighted with an orange border. The table below shows the details of the providers:

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
saml2AP	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0

Figure 18. Creating a SAML 2.0 Authentication Provider in domainB.

We restart the server.

### 3.7.6 configure SAML 2.0 General Settings

We configure the server specific SAML2.0 General settings.

The screenshot shows the 'Messages' section with two green checkmarks: 'All changes have been activated. No restarts are necessary.' and 'Settings updated successfully.' Below is the 'Settings for adminB' page, with the 'Federation Services' tab selected. The 'SAML 2.0 General' sub-tab is active. The 'Save' button is visible. The page content is as follows:

This page configures the general SAML 2.0 per server properties

**General**

**Replicated Cache Enabled** Specifies whether the persistent cache (LDAP or RDBMS) is used for storing SAML 2.0 artifacts and authentication requests. [More Info...](#)

**Site Info**

**Contact Person Given Name:**  The contact person given (first) name. [More Info...](#)

**Contact Person Surname:**  The contact person surname (last name). [More Info...](#)

**Contact Person Type:**  The contact person type. [More Info...](#)

**Contact Person Company:**  The contact person's company name. [More Info...](#)

**Contact Person Telephone Number:**  The contact person's telephone number. [More Info...](#)

**Contact Person Email Address:**  The contact person's e-mail address. [More Info...](#)

**Organization Name:**  The organization name. [More Info...](#)

**Organization URL:**  The organization URL. [More Info...](#)

**Published Site URL:**  The published site URL. [More Info...](#)

**Entity ID:**  The string that uniquely identifies the local site. [More Info...](#)

— Bindings —		
<input checked="" type="checkbox"/> Recipient Check Enabled		Specifies whether the recipient/destination check is enabled. When true, the recipient of the SAML Request/Response must match the URL in the HTTP Request. <a href="#">More Info...</a>
<input type="checkbox"/> Transport Layer Client Authentication Enabled		Specifies whether TLS/SSL client authentication is required. <a href="#">More Info...</a>
Transport Layer Security Key Alias:	<input type="text"/>	The string alias used to store and retrieve the server's private key, which is used to establish outgoing TLS/SSL connections. <a href="#">More Info...</a>
Transport Layer Security Key Passphrase:	<input type="text"/>	The passphrase used to retrieve the server's private key from the keystore. <a href="#">More Info...</a>
Confirm Transport Layer Security Key Passphrase:	<input type="text"/>	
<input type="checkbox"/> Basic Client Authentication Enabled		Specifies whether Basic Authentication client authentication is required. <a href="#">More Info...</a>
Basic Authentication User Name:	<input type="text"/>	The username that is used to assign Basic authentication credentials to outgoing HTTPS connections. <a href="#">More Info...</a>
Basic Authentication Password:	<input type="text"/>	The password used to assign Basic Authentication credentials to outgoing HTTPS connections. <a href="#">More Info...</a>
Confirm Basic Authentication Password:	<input type="text"/>	
— Artifact Resolution Service —		
Only Accept Signed Artifact Requests:	false	Specifies whether incoming artifact requests must be signed. <a href="#">More Info...</a>
Artifact Cache Size:	10000	The maximum size of the artifact cache. <a href="#">More Info...</a>
Artifact Cache Timeout:	300	The maximum timeout (in seconds) of artifacts stored in the local cache. <a href="#">More Info...</a>
— Single Sign-on —		
Single Sign-on Signing Key Alias:	<input type="text" value="Demolentity"/>	The keystore alias for the key to be used when signing documents. <a href="#">More Info...</a>
Single Sign-on Signing Key Pass Phrase:	<input type="password" value="....."/>	The passphrase used to retrieve the local site's SSO signing key from the keystore. <a href="#">More Info...</a>
Confirm Single Sign-on Signing Key Pass Phrase:	<input type="password" value="....."/>	
<input type="button" value="Save"/> <input type="button" value="Publish Meta Data"/>		

Figure 19. Configuration of the SAML2 General Settings in server adminB.

For signing we use the DemoIdentity/DemoIdentityPassPhrase.

### 3.7.7 configure SAML 2.0 Service Provider

We change the „SAML 2.0 Service Provider“ Page of adminB. We choose “POST” as preferred Binding. This will influence how the SingleSignOn Service in domainA, or more specific the “Partner-SP-adminB” in the “SAML 2.0 Credential Mapping Provider”, communicates the SAML Assertion to the Service Provider.

There are two options. If we choose POST, the Assertion will be place into an HTML Form and send via POST to the Assertion Consumer Service (samlAP) of domainB.

If we don't choose anything or choose “Artifact” the IdP will sent a signed artifact via HTTP redirect.

These values will be communicated to the domainA during import of the “adminB\_metadata.xml” file.



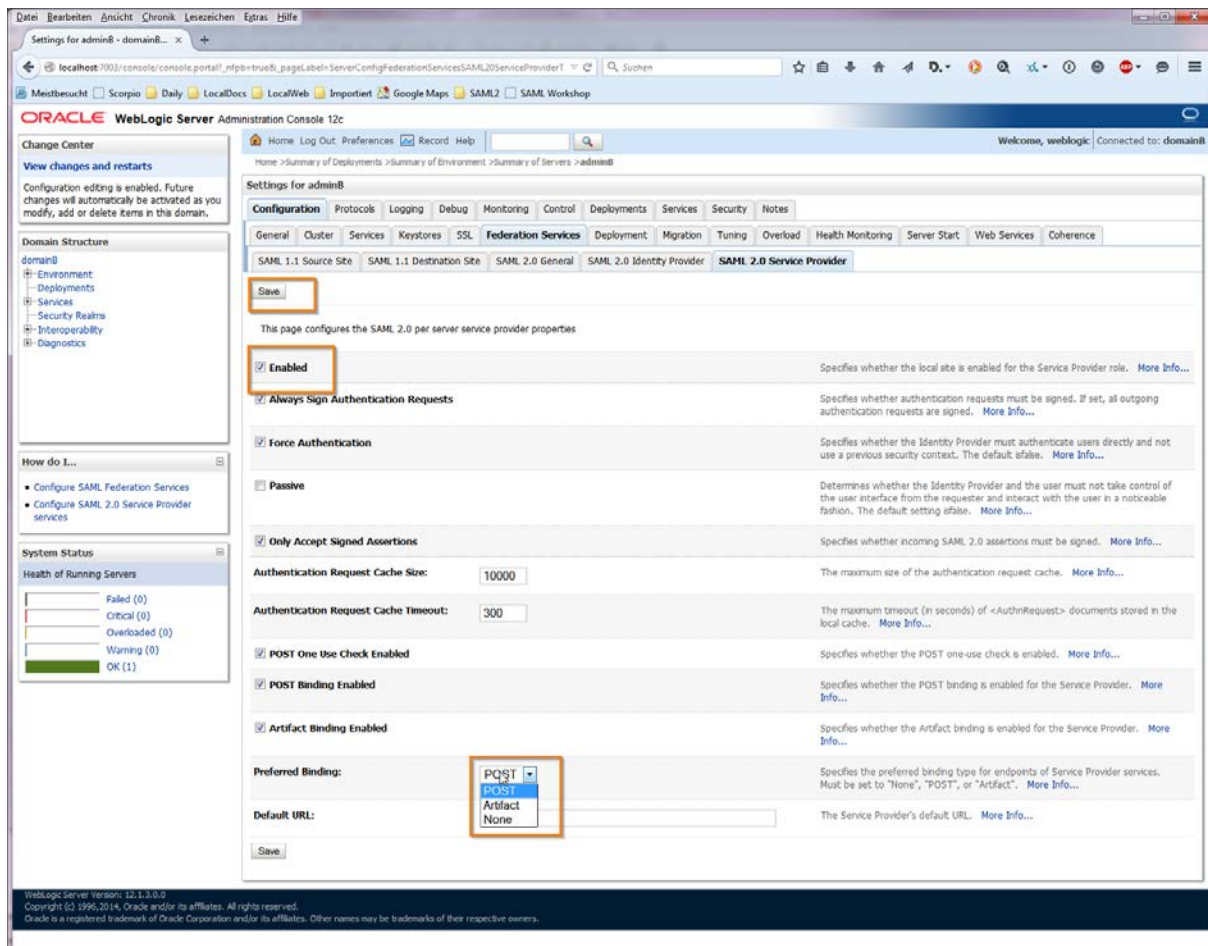


Figure 20. Configuration of the SAML 2.0 Service Provider Settings in adminB.

### 3.7.8 export adminB\_metadata.xml

We change back to the “SAML 2.0 General” Tab and publish the metadata to the file:  
D:\10Oracle\06WLS12\domains\domainB\adminB\_metadata.xml.

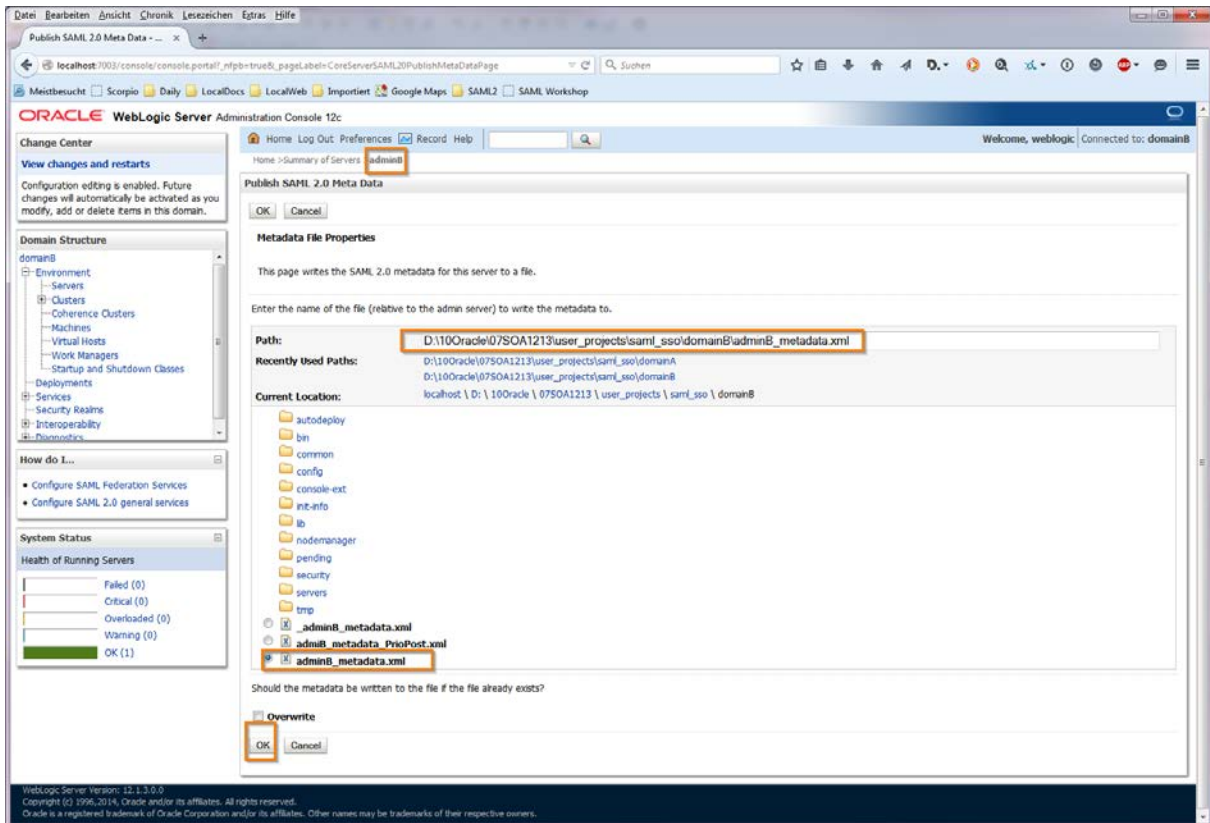


Figure 21. Publishing Metadata for SAML 2.0 Federation Services of adminB

### 3.7.9 create Partner-Idp-adminA

Now we create a new SSO Identity Provider Partner in the security realm of domainB.

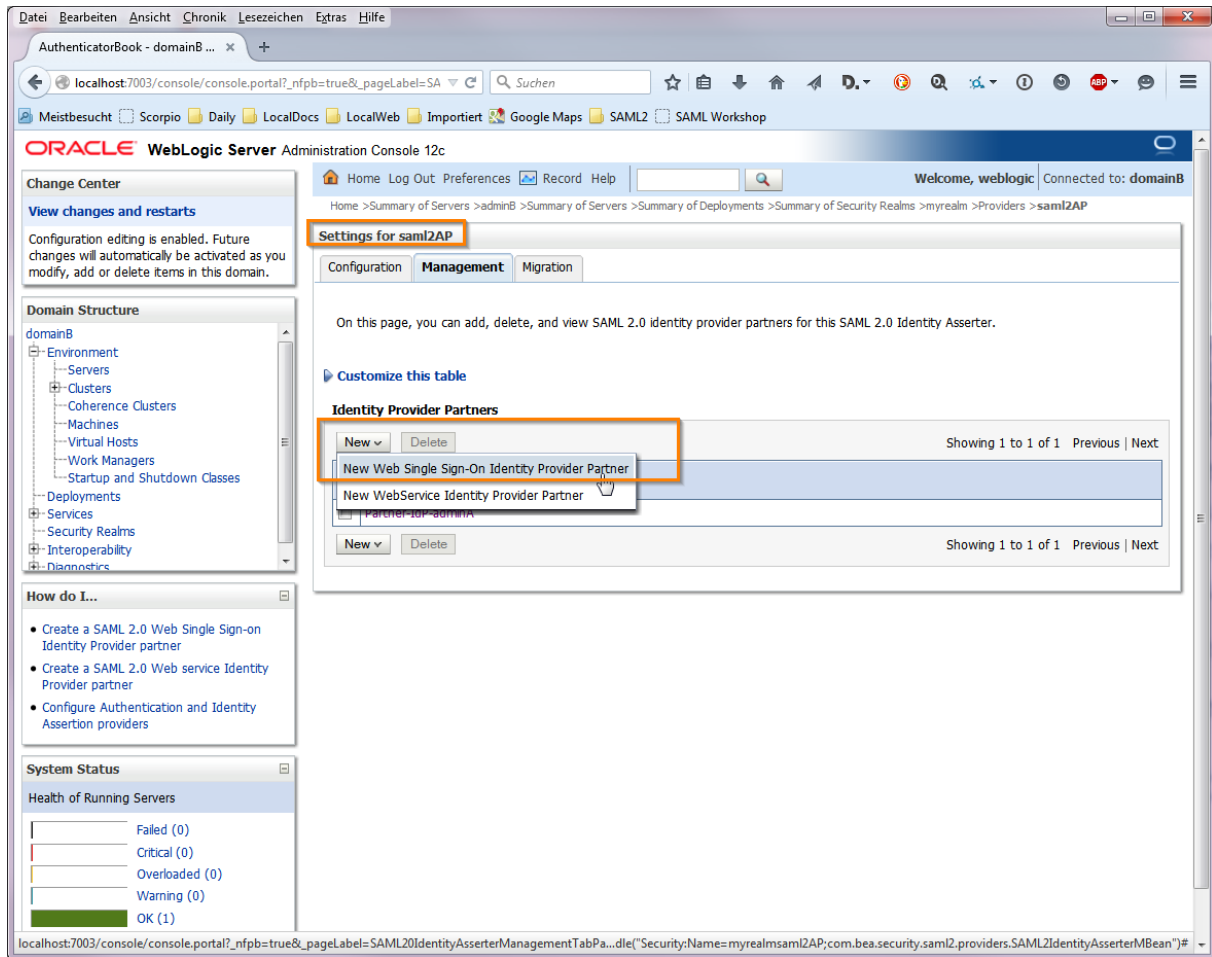


Figure 22. Creating a new SSO IdP Partner Configuration at the “SAML 2.0 Authentication Provider” in domainB

This

### 3.7.10 import adminA\_metadata.xml

We import the metadata file from domainA, which is the IdP Partner.

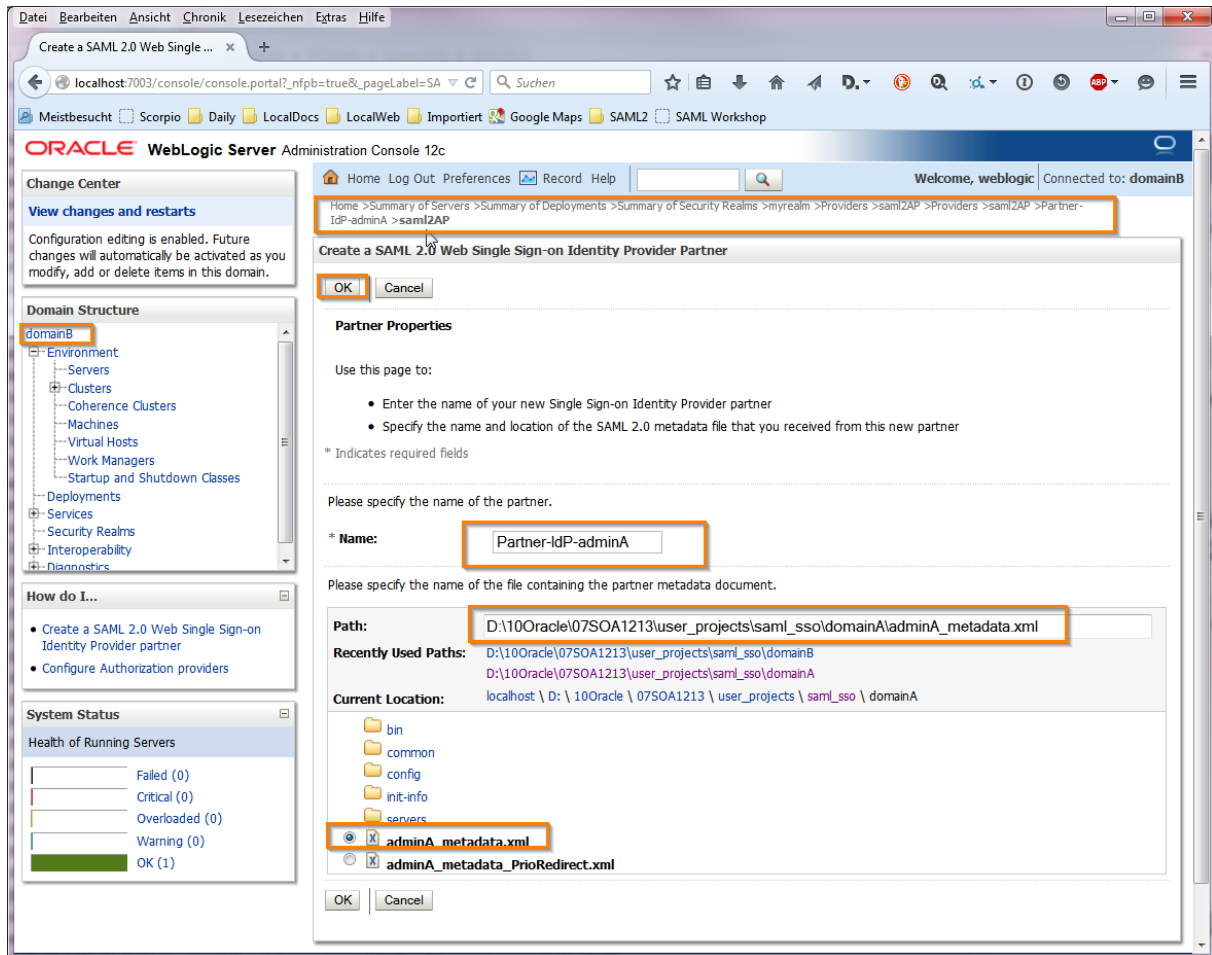


Figure 23. Creating the IdP Partner for the Service Provider domainB.

### 3.7.11 configure Partner-IdP-adminB

And we enable the newly created Partner site and add redirect URIs for Service Provider initiated SSO.

Redirect URIs:

/appB/admin/services.jsp

/appB

Home > Summary of Deployments > Summary of Security Realms > myrealm > Providers > saml2AP > Providers > saml2AP > Partner-IdP-adminA > saml2AP > Partner-IdP-adminA

Settings for saml2AP

General Site Info Single Sign-On Signing Certificate Transport Layer Client Certificate Single Sign-On Service Endpoints Artifact Resolution Service Endpoints

Save

Configures a SAML 2.0 Web Single Sign-on Identity Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.

Overview

Name: Partner-IdP-adminA The name of this Identity Provider partner. [More Info...](#)

Enabled Specifies whether interactions with this Identity Provider partner are enabled on this server. [More Info...](#)

Description: A short description of this Identity Provider partner. [More Info...](#)

Authentication Requests

Identity Provider Name Mapper Class Name: The Java class that overrides the default username mapper class with which the SAML 2.0 Identity Asserter provider is configured in this security realm. [More Info...](#)

Issuer URI: saml2CMP The Issuer URI of this Identity Provider partner. [More Info...](#)

Virtual User Specifies whether user information contained in assertions received from this Identity Provider partner are mapped to virtual users in this security realm. [More Info...](#)

Redirect URIs: An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. [More Info...](#)

/appB/admin/services.jsp  
/appB

Process Attributes Specifies whether the SAML 2.0 Identity Asserter provider consumes attribute statements contained in assertions received from this Identity Provider partner. [More Info...](#)

Signing

Only Accept Signed Authentication Requests: true Specifies whether authentication requests sent to this Identity Provider partner must be signed. [More Info...](#)

Only Accept Signed Artifact Requests Specifies whether SAML artifact requests received from this Identity Provider partner must be signed. [More Info...](#)

Transport

Send Artifact via POST Specifies whether SAML artifacts are delivered to this Identity Provider partner via the HTTP POST method. [More Info...](#)

Artifact Binding POST Form: The URL of the custom web application that generates the POST form for carrying the SAML response for Artifact bindings to this Identity Provider partner. Details about the required fields in this custom application are available in the OASIS SAML 2.0 specifications. [More Info...](#)

POST Binding POST Form: The URL of the custom web application that generates the POST form for carrying the SAML response for POST bindings to this Identity Provider partner. [More Info...](#)

Client User Name: The user name that must be specified in the basic authentication header that is expected from this Identity Provider partner when the partner connects to the local site's SOAP/HTTPS binding. [More Info...](#)

Client Password: The password of the client user name. [More Info...](#)

Confirm Client Password:

Save

Figure 24. Configuration of the IdP Partner site in domainB.

This concludes the configuration in domainB.

### 3.7.12 create Partner-SP-adminB

We change to the Admin Server of domain to the “SAML 2.0 Credential Mapping Provider”. We want to create a Service Provider partner.

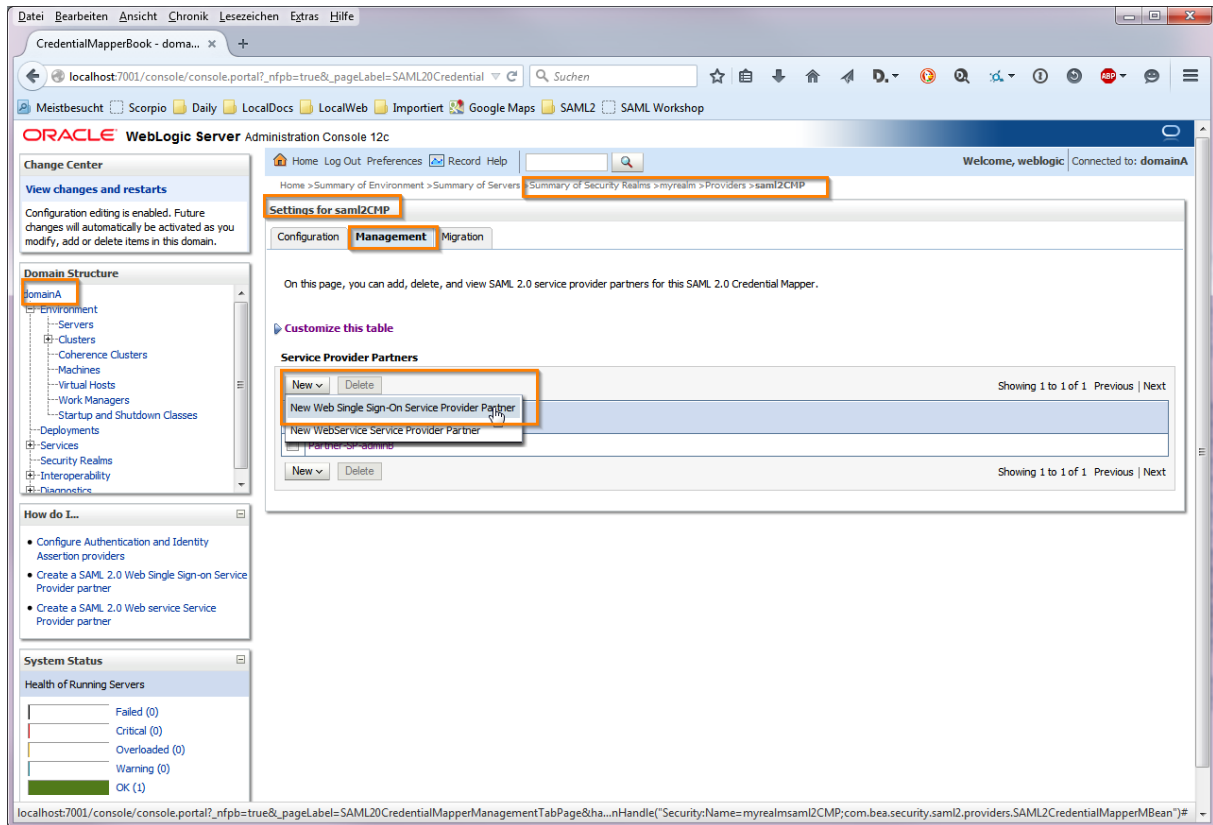


Figure 25. Creating a new Service Provider Partner in domainA.

### 3.7.13 Import adminB\_metadata.xml

We import the metadata file from domainB.

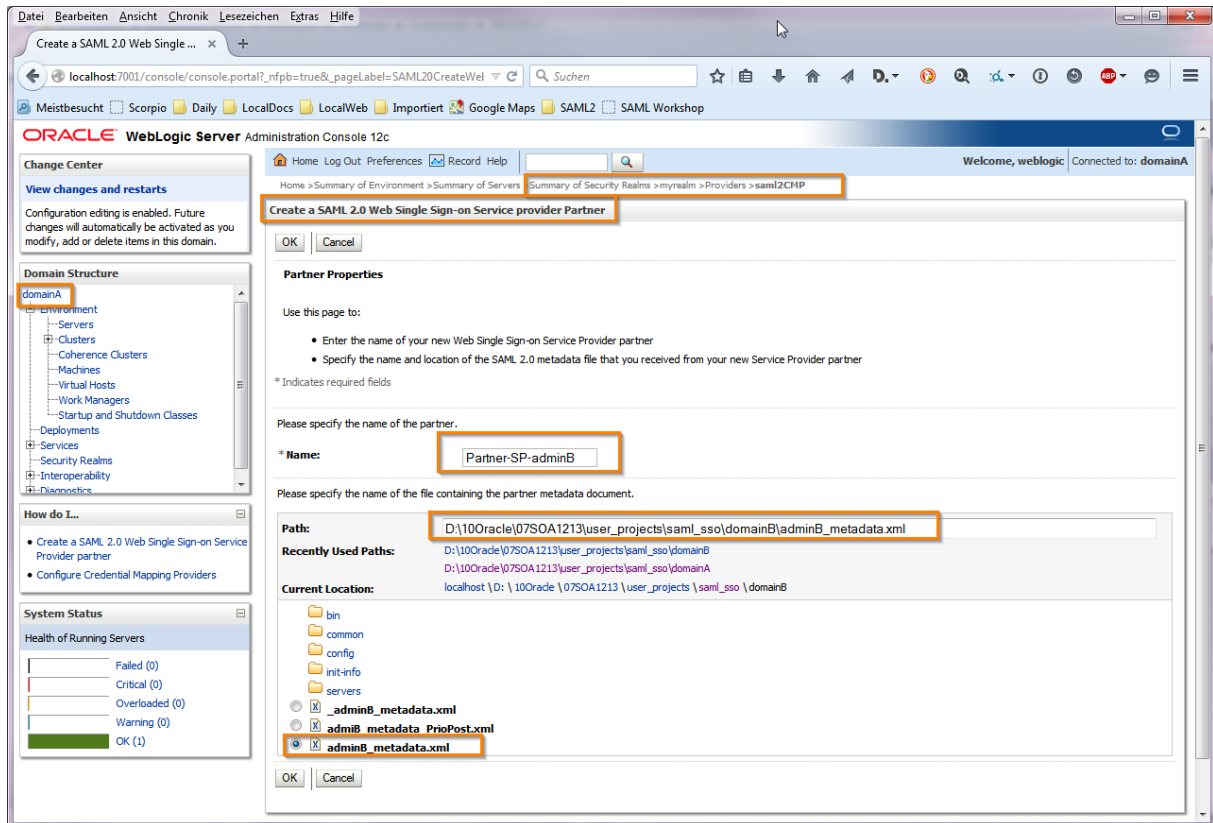


Figure 26. Importing the metadata from domainB.

### 3.7.14 configure Partner-SP-adminB

And we enable domainB as SAML partner service provider.



Home > Summary of Servers > adminA > Summary of Security Realms > myrealm > Providers > saml2CMP > domainB

**Settings for saml2CMP**

General | Site Info | Single Sign-On Signing Certificate | Transport Layer Client Certificate | Assertion Consumer Service Endpoints | Artifact Resolution Service Endpoints

Save

Configures a SAML 2.0 Web Single Sign-on Service Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.

Overview

**Name:** domainB The name of this Service Provider partner. [More Info...](#)

**Enabled** Specifies whether interactions with this Service Provider partner are enabled on this server. [More Info...](#)

**Description:**  A short description of this Service Provider partner. [More Info...](#)

Assertions

**Service Provider Name Mapper Class Name:**  The Java class that overrides the default username mapper class with which the SAML 2.0 Credential Mapping provider is configured in this security realm. [More Info...](#)

**Time To Live:**  The time to live value, in seconds, for assertions generated for this Service Provider partner. [More Info...](#)

**Time To Live Offset:**  The time to live offset value, in seconds, for assertions generated for this Service Provider partner. [More Info...](#)

**Generate Attributes** Specifies whether this server's SAML 2.0 Credential Mapping provider creates attribute statements in the assertions generated for this Service Provider partner. [More Info...](#)

**Include One Time Use Condition** Specifies whether the assertions sent to this Service Provider partner are disposed of immediately after use and are not available for reuse. [More Info...](#)

**Key Info Included** Specifies whether this server's signing certificate is included in assertions generated for this Service Provider partner. [More Info...](#)

Signing

**Only Accept Signed Assertions:** true Specifies whether the Service Provider partner is configured to receive only assertions that have been signed. [More Info...](#)

**Only Accept Signed Authentication Requests:** true Specifies whether the local Identity Provider services are configured to accept only signed authentication requests. [More Info...](#)

**Only Accept Signed Artifact Requests** Specifies whether inbound SAML artifact requests from this Service Provider partner must be signed. [More Info...](#)

Transport

**Send Artifact via POST** Specifies whether SAML artifacts are delivered to this Service Provider partner via the HTTP POST binding. [More Info...](#)

**Artifact Binding POST Form:**  The URI of the custom web application that generates the HTTP POST form for sending the SAML artifact. [More Info...](#)

**POST Binding POST Form:**  The URI of the custom web application that generates the HTTP POST form for sending the message via the POST binding. [More Info...](#)

**Client User Name:**  The username that is expected from this Service Provider partner when connecting to the partner site's SOAP/HTTPS binding using Basic authentication. [More Info...](#)

**Client Password:**  The password for the client username. [More Info...](#)

**Confirm Client Password:**

Save

Figure 27. Enable the Service Provider Partner Configuration from the Metadata import.

That's all for the basic configuration of this SAML example.

### 3.8 Testing the example

We want to test the example via two URLs as indicated in the following mind map.



Figure 28. Testing SP initiated SSO

### 3.8.1 Testing via URL to IdP

First we go to appA and get redirected to the login page. We provide the credentials.

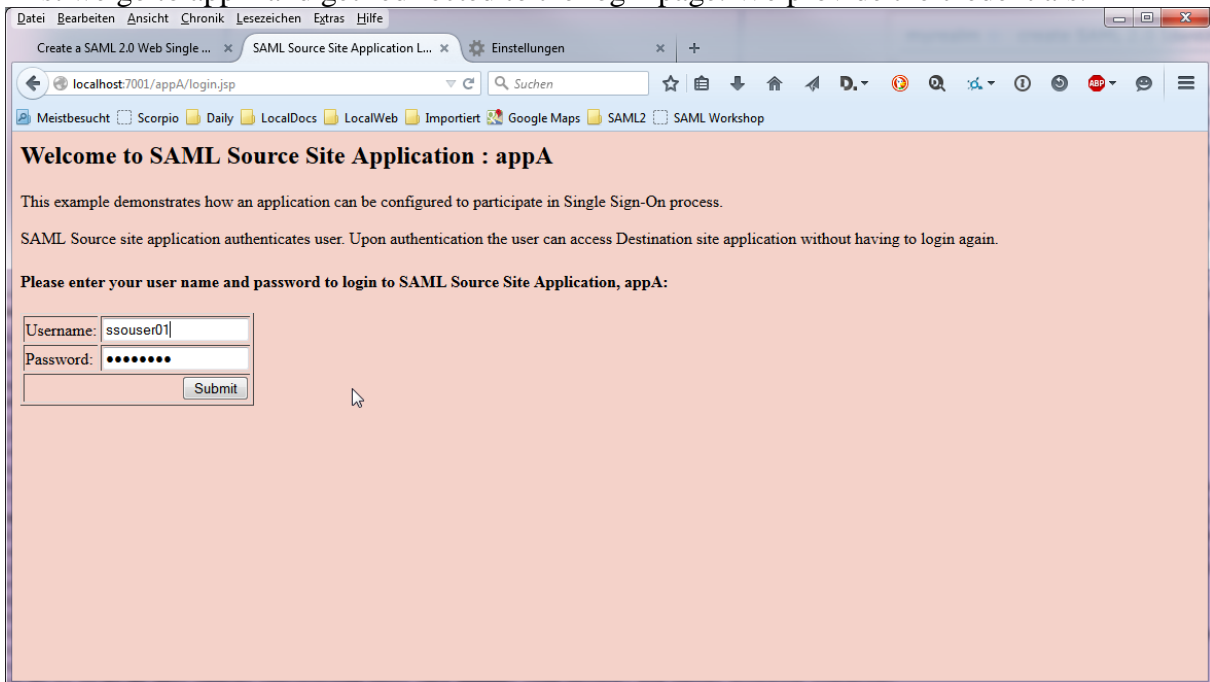


Figure 29. Logging in to appA.

We are logged in. Next we choose a service on appB.

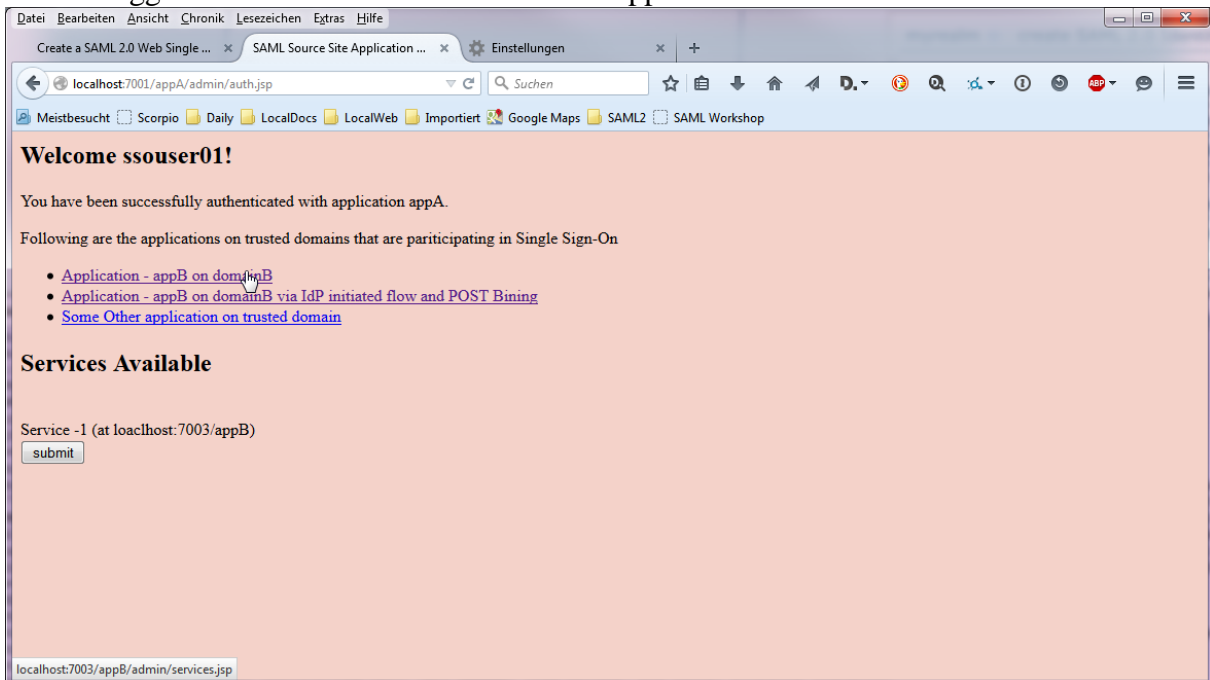


Figure 30. Service Selection Page from the IdP.

We get redirected to appB and are already logged in.

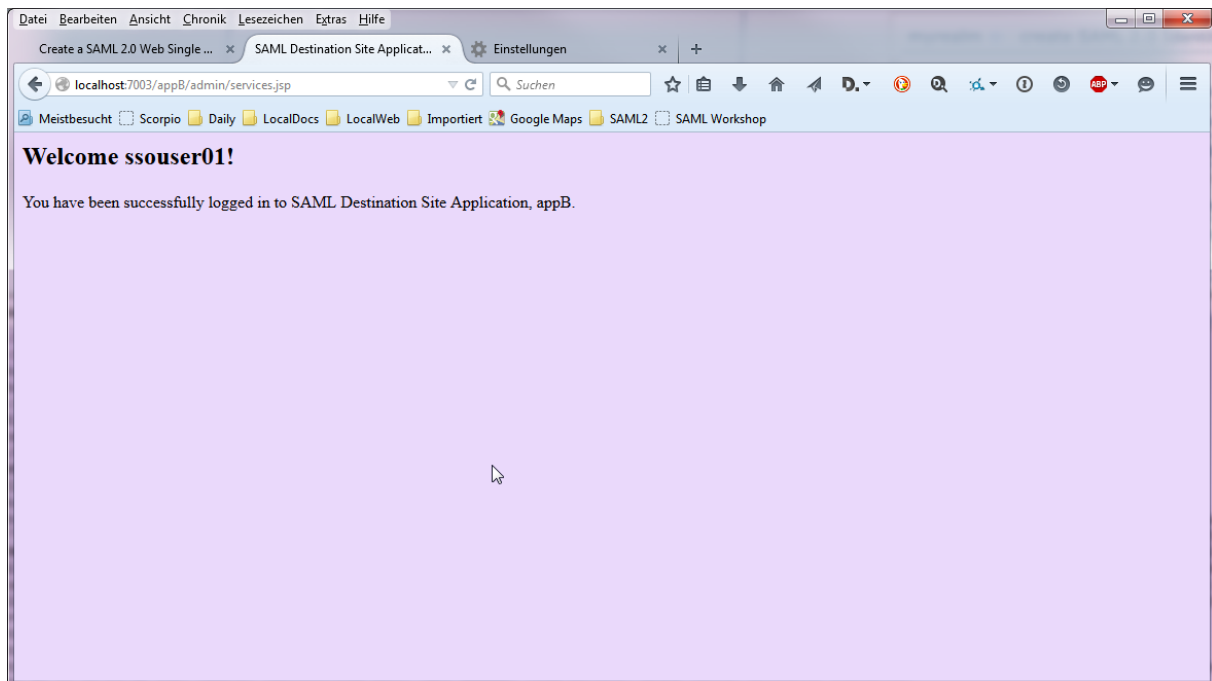


Figure 31. Service Page of appB.

While this looks like an IdP initiated flow, it is actually a SP initiated flow, however starting on the IdP. If we analyze the log files, we will discover that there is no SAML Assertion attached to the HTTP Request for appB. Instead the Assertion Consumer Service from domainB intercepts the call, builds a SAML AuthnRequest, sends it to domainA and receives the SAML Assertion in turn. It verifies the SAML Assertion and forwards to the appB Service page.

### 3.8.2 Testing via URL to SP

Now we want to go to the appB directly with an unauthenticated request. In Firefox we delete the history and all cookies first.

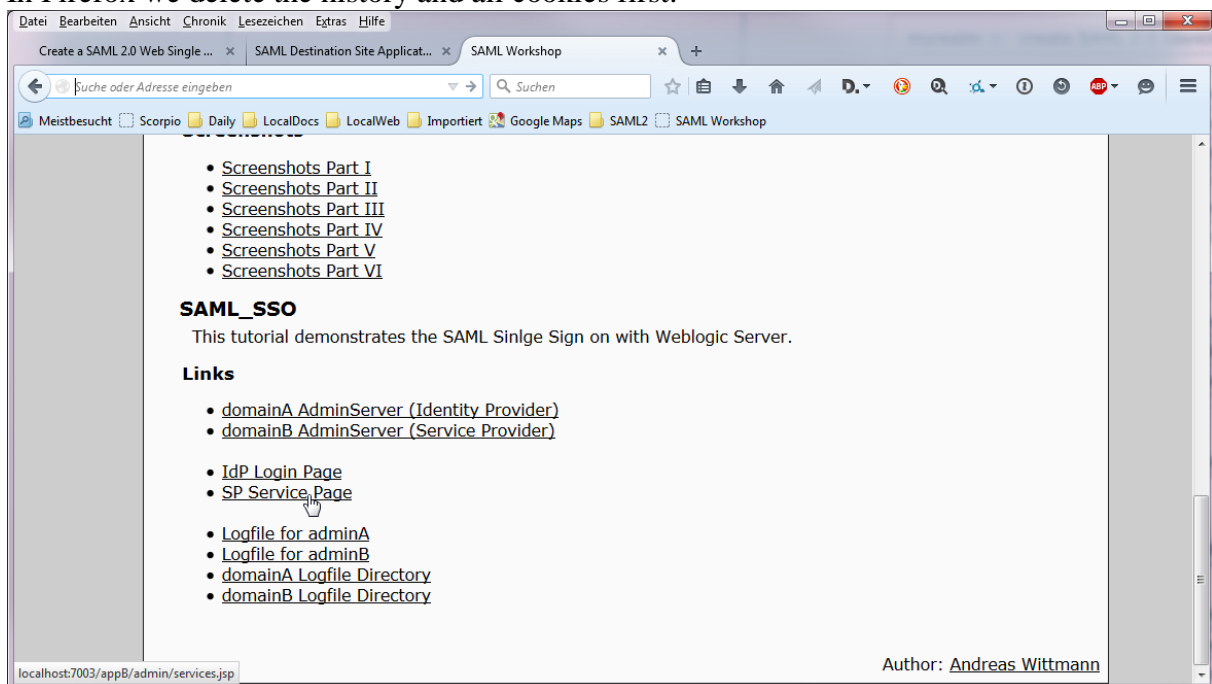
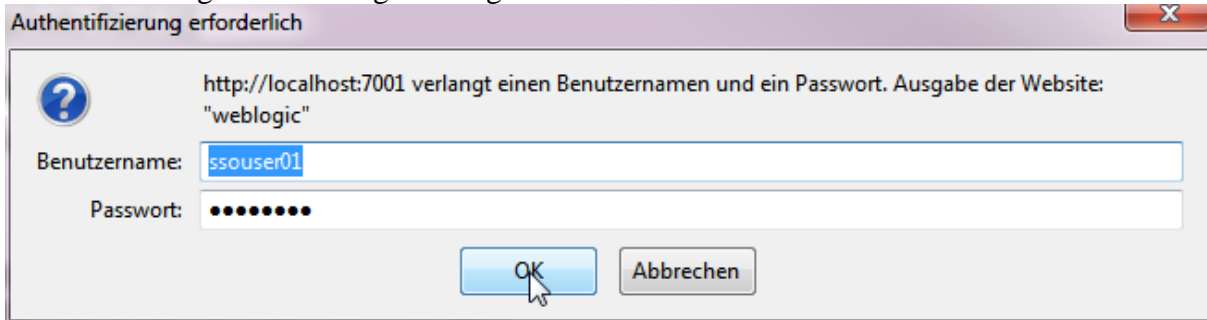


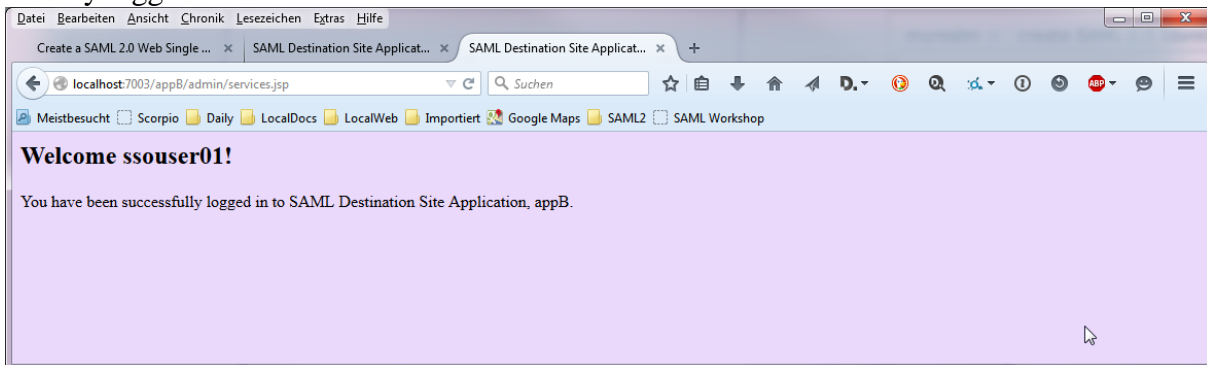
Figure 32. Calling the Service on appB directly.

We are challenged with a Login dialog from adminA.



**Figure 33. Login Dialog from adminA**

After providing user and password we are redirected to the service page of appB and are already logged in.



**Figure 34. Service page of appB in the SP initiated flow.**

Further configuration is needed to specify the login.jsp as login page instead of the standard Authentication Dialog box. We leave this exercise to the interested readers.

### 3.9 Setting Debug Flags for the Example

For debugging we set the these Properties in the files

D:\10Oracle\06WLS12\domains\domainB\bin\setDomainEnv.cmd  
D:\10Oracle\06WLS12\domains\domainA\bin\setDomainEnv.cmd

```
set EXTRA_JAVA_PROPERTIES=-Dweblogic.debug.DebugSecuritySAMLAtn=true -Dweblogic.debug.DebugSecuritySAMLlib=true -  
Dweblogic.debug.DebugSecuritySAML2Service=true -Dweblogic.debug.DebugSecuritySAML2CredMap=true -  
Dweblogic.debug.DebugSecuritySAML2Atn=true
```

We also want to see milliseconds in the logfiles.

We navigate to Domain->Logging->Advanced and set

Date Format Pattern = yyyy-MM-dd' 'HH:mm:ss.S

We do this for both domains and both servers.

### 3.10 Configuring IdP initiated flow with POST Binding.

This Blog explains how to configure the IdP initiated flow.

<http://fusionsecurity.blogspot.de/2012/06/before-i-forget-it-howto-saml-20-idp.html>

Here are the steps to configure this within this example:

### 3.10.1 Configure an additional end user URL.

In appA/admin/auth.jsp we add an additional URL that points to IdP and uses the target Service URL in the parameter.

It is of the form:

<http://<idp-server>:<port>/saml2/idp/sso/initiator?SPName=<SP-Partner-Name>&RequestURL=<target-application-url>>

In our case we use:

<http://localhost:7001/saml2/idp/sso/initiator?SPName=domainB&RequestURL=http://localhost:7003/appB/admin/services.jsp>

### 3.10.2 Configure the POST Binding POST Form

Within appA we need a jsp that contains a POST form, which posts the SAML Assertion to the Service Provider.

We include sam2\_post\_form.jsp in appA and redeploy App.

The post form is contained in the file /appA/saml2\_post\_form.jsp:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page contentType="text/html; charset=windows-1252"%>
<html>
<head>
</head>
<%
String samlResponse = (String) request.getAttribute("com.bea.security.saml2.samlContent");
String relayState = (String) request.getAttribute("com.bea.security.saml2.relayState");
System.out.println("saml2_post_form.jsp: the samlResponse is: " + samlResponse + ".");
System.out.println("saml2_post_form.jsp: the relayState is: " + relayState + ".");
%>
<body onLoad="document.forms[0].submit();" >
<FORM METHOD="POST" ACTION="http://localhost:7003/saml2/sp/acs/post">
<INPUT TYPE="HIDDEN" NAME="RelayState" VALUE="<%=relayState%>" />
<INPUT TYPE="HIDDEN" NAME="SAMLResponse" VALUE="<%=samlResponse%>" />
</FORM>
</body>
</html>
```

In the IdP-Partner configuration we specify the post form. We use the /appA/saml2\_post\_form.jsp

Home > Summary of Servers > Summary of Security Realms > myrealm > Providers > saml2CMP > Partner-SP-adminB

### Settings for saml2CMP

**General** | Site Info | Single Sign-On Signing Certificate | Transport Layer Client Certificate | Assertion Consumer Service Endpoints | Artifact Resolution Service Endpoints

Configures a SAML 2.0 Web Single Sign-on Service Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see [Related Topics](#)

**Overview**

<b>Name:</b>	<input type="text" value="Partner-SP-adminB"/>	The name of this Service Provider partner. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Enabled</b>		Specifies whether interactions with this Service Provider partner are enabled. <a href="#">More Info...</a>
<b>Description:</b>	<input type="text"/>	A short description of this Service Provider partner. <a href="#">More Info...</a>

**Assertions**

<b>Service Provider Name Mapper Class Name:</b>	<input type="text"/>	The Java class that overrides the default username mapper class with Mapping provider is configured in this security realm. <a href="#">More Info...</a>
<b>Time To Live:</b>	<input type="text" value="0"/>	The time to live value, in seconds, for assertions generated for this Service Provider partner. <a href="#">More Info...</a>
<b>Time To Live Offset:</b>	<input type="text" value="0"/>	The time to live offset value, in seconds, for assertions generated for this Service Provider partner. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Generate Attributes</b>		Specifies whether this server's SAML 2.0 Credential Mapping provider generates the assertions for this Service Provider partner. <a href="#">More Info...</a>
<input type="checkbox"/> <b>Include One Time Use Condition</b>		Specifies whether the assertions sent to this Service Provider partner after use and are not available for reuse. <a href="#">More Info...</a>
<input type="checkbox"/> <b>Key Info Included</b>		Specifies whether this server's signing certificate is included in assertions sent to this Service Provider partner. <a href="#">More Info...</a>

**Signing**

<b>Only Accept Signed Assertions:</b>	<input checked="" type="checkbox"/>	Specifies whether the Service Provider partner is configured to receive signed assertions. <a href="#">More Info...</a>
<b>Only Accept Signed Authentication Requests:</b>	<input checked="" type="checkbox"/>	Specifies whether the local Identity Provider services are configured to receive signed authentication requests. <a href="#">More Info...</a>
<input type="checkbox"/> <b>Only Accept Signed Artifact Requests</b>		Specifies whether inbound SAML artifact requests from this Service Provider partner are accepted. <a href="#">More Info...</a>

**Transport**

<input type="checkbox"/> <b>Send Artifact via POST</b>		Specifies whether SAML artifacts are delivered to this Service Provider partner via the POST binding. <a href="#">More Info...</a>
<b>Artifact Binding POST Form:</b>	<input type="text"/>	The URI of the custom web application that generates the HTTP POST artifact. <a href="#">More Info...</a>
<b>POST Binding POST Form:</b>	<input type="text" value="/appA/saml2_post_form.jsp"/>	The URI of the custom web application that generates the HTTP POST artifact via the POST binding. <a href="#">More Info...</a>
<b>Client User Name:</b>	<input type="text"/>	The username that is expected from this Service Provider partner with site's SOAP/HTTPS binding using Basic authentication. <a href="#">More Info...</a>
<b>Client Password:</b>	<input type="text"/>	The password for the client username. <a href="#">More Info...</a>
<b>Confirm Client Password:</b>	<input type="text"/>	

**Figure 35. Setting the POST Form on the IdP site for the POST Binding.**

For testing, we login at appA with souser01 and choose the link for the POST Binding.

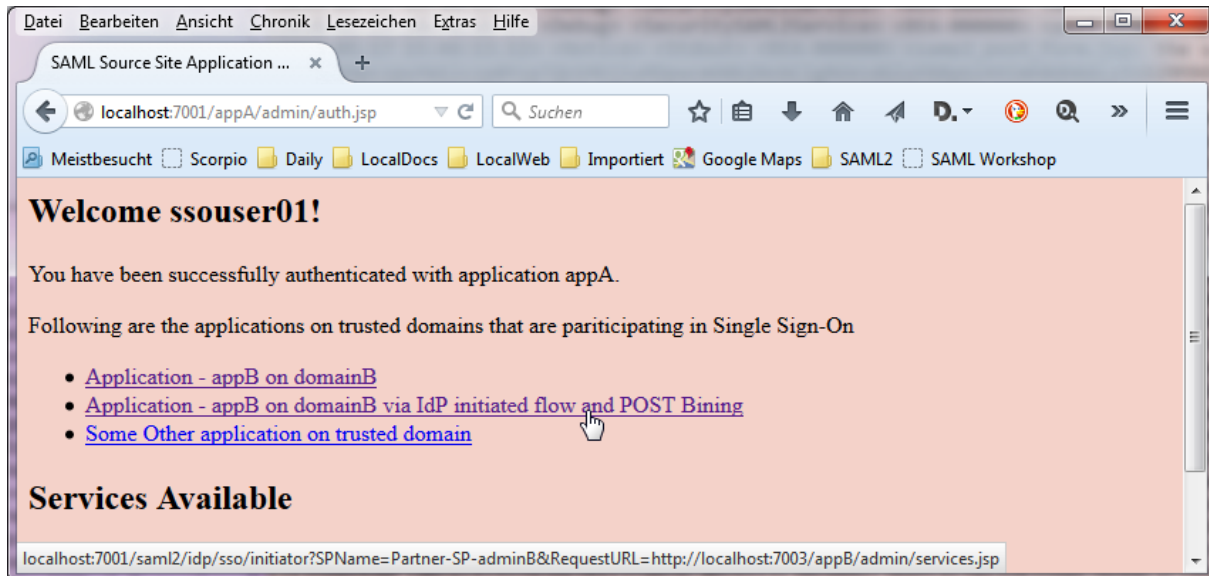


Figure 36. Choosing the IdP initiated flow from appA.

We are directly transferred to the service page of domainB. This time the request is processed by the “Assertion Consumer Service” of domainB. It contains the SAML Assertion, as the following excerpt from the adminB.log demonstrates.

```
<2015-05-17 15:48:39.114> <Debug> <SecuritySAML2Service> <BEA-000000> <SAML2Servlet: Processing request on URI  
'/saml2/sp/acs/post'>  
<2015-05-17 15:48:39.114> <Debug> <SecuritySAML2Service> <BEA-000000> <getServiceTypeFromURI(): request URI is  
'/saml2/sp/acs/post'>  
<2015-05-17 15:48:39.115> <Debug> <SecuritySAML2Service> <BEA-000000> <getServiceTypeFromURI(): service URI is  
'/sp/acs/post'>  
<2015-05-17 15:48:39.115> <Debug> <SecuritySAML2Service> <BEA-000000> <getServiceTypeFromURI(): returning service type 'ACS'>  
<2015-05-17 15:48:39.116> <Debug> <SecuritySAML2Service> <BEA-000000> <Assertion consumer service: processing>  
<2015-05-17 15:48:39.116> <Debug> <SecuritySAML2Service> <BEA-000000> <get SAMLResponse from http  
request: PD94bWwgdmYyc2l2bWVjIiB1bWVZgluZz0iVVRGLTgiPz48c2FtbnA6UmVzcG9uc2UgeGlsbnM6c2Ft  
...  
<2015-05-17 15:48:39.123> <Debug> <SecuritySAML2Service> <BEA-000000> <BASE64 decoded saml message:<?xml version="1.0"  
encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:  
2.0:protocol" Destination="http://localhost:7003/saml2/sp/acs/post" ID="_0xab777ac5ef829a8140572b099b538d07"  
IssueInstant="2015-05-17T13:48:39.030Z" Version="2.0"><saml:Issuer xmlns:saml="ur  
n:oasis:names:tc:SAML:2.0:assertion">saml2CMP</saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
<ds:SignedInfo>  
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>  
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>  
<ds:Reference URI="#_0xab777ac5ef829a8140572b099b538d07">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"><ec:InclusiveNamespaces  
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml samlp xs xsi"/></ds:Transform>  
</ds:Transforms>  
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>  
<ds:DigestValue=SDY0Hn76mvZTuCoQF45+/LB510KumkmBIGZ63F82I/s=</ds:DigestValue>  
</ds:Reference>  
</ds:SignedInfo>  
<ds:SignatureValue>  
VMQpiMFhDI34XJz8C8LVRKY9cWaxyQJdBrzTlPdvSxFhd2q7PITSGIMOshdP2HiB2dsmdYcVcHJ  
F+FOYKTC+81jSABFVbZJfwdZBIMJKU8wvPz3uGWKAz7JeKZ431ZEhwaXxG85BNgkdyMq8T0nmu7R  
U9YQQYGL5tT/QOQZbmRosIjWZJYe+/Kc4BOQdJPxkXfd5EvHiUI7KleZiYALxAQBjxkFOC2oGo5k  
Kj15eJgBIX2qjt9v2Qzakelhq0uR6frcTt3vycTxrxmXSwwhyfetejtXGmKMFTY9ykTsdM3f6SEZP  
ADXNviuA4yQ+QzCW8s7DBp95tyv7H82ZLayQ==  
</ds:SignatureValue>  
</ds:Signature><samlp:Status><samlp:StatusCode  
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion  
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_0x97  
4db452305af2bf491b72eff5bd736a" IssueInstant="2015-05-17T13:48:39.014Z"  
Version="2.0"><saml:Issuer>saml2CMP</saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
<ds:SignedInfo>  
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>  
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>  
<ds:Reference URI="#_0x974db452305af2bf491b72eff5bd736a">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"><ec:InclusiveNamespaces  
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml xs"/></ds:Transfo  
rm>  
</ds:Transforms>  
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>  
<ds:DigestValue=627CMXnG8VWRb+STsiWzuYavZLMLQV4xGBj3H3pQH8=</ds:DigestValue>  
</ds:Reference>  
</ds:SignedInfo>  
<ds:SignatureValue>  
hd7p4jd0UNvMSa4WpPy7XZm57OVTaqURmvEaOrvOkoTLJKPhlAovVollFznpeJXi75FudVJrMLQbl  
5eQtE6QfB20gryzZM82TVjnrA0cTvpU5od861VX3kZuVagE5QphoxToCldwDntZvvpJAm8qVvVdaJ  
6E61L/8Pv10kQFuk3eFn8UvLYP3Nd3nITLH9ID9STrHaRovxwDwFjs2yGIAN/Y7LII8aem96iil  
71jgJpfl1pHysDx0Lw2Ud4Wnc4atXbDdWdWu1GEZJP7Xcix635vSNGV5067Uz7Srt25hv+KCYAv  
yGyKuJiSL0CE3e9p8rt+/5jkVKG/SFTvcac+nQ==  
</ds:SignatureValue>
```



```
</ds:Signature><saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="www.domainA.com">ssouser01</saml:NameID><saml:SubjectConfirmation Meth
od="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData NotOnOrAfter="2015-05-17T13:50:34.014Z"
Recipient="http://localhost:7003/saml2/sp/acs/post"/></saml:SubjectConfirmati
on></saml:Subject><saml:Conditions NotBefore="2015-05-17T13:48:34.014Z" NotOnOrAfter="2015-05-
17T13:50:34.014Z"><saml:AudienceRestriction><saml:Audience>saml2AP</saml:Audience></saml:Audience
Restriction></saml:Conditions><saml:AuthnStatement AuthnInstant="2015-05-
17T13:48:39.014Z"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</
saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement><saml:AttributeStatement><saml:Attribute Name="Groups"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><sam
l:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">ssouser</saml:AttributeValue></saml:Attribute></saml:A
ttributeStatement></saml:Assertion></samlp:Response>>
<2015-05-17 15:48:39.153> <Debug> <SecuritySAML2Service> <BEA-000000> <<samlp:Response> is signed.>
```

The user is contained in the NameID element and the group is contained in the AttributeStatement element.  
This concludes the IdP initiated POST Binding example.

### 3.11 Configuring Virtual User:

This is explained in the blog post from Biemond: <http://biemond.blogspot.de/2011/09/virtual-users-with-saml-in-weblogic.html>

We can use virtual users at the SP side, if we need users that are authenticated at the IdP but do not exist in the security realm of domainB. These foreign users are created as virtual users by an extra SAML Authenticator, i.e. this Authenticator populates the subject with principals from the SAML assertion (user and groups).

We need to configure an extra SAML Authenticator in domainA.

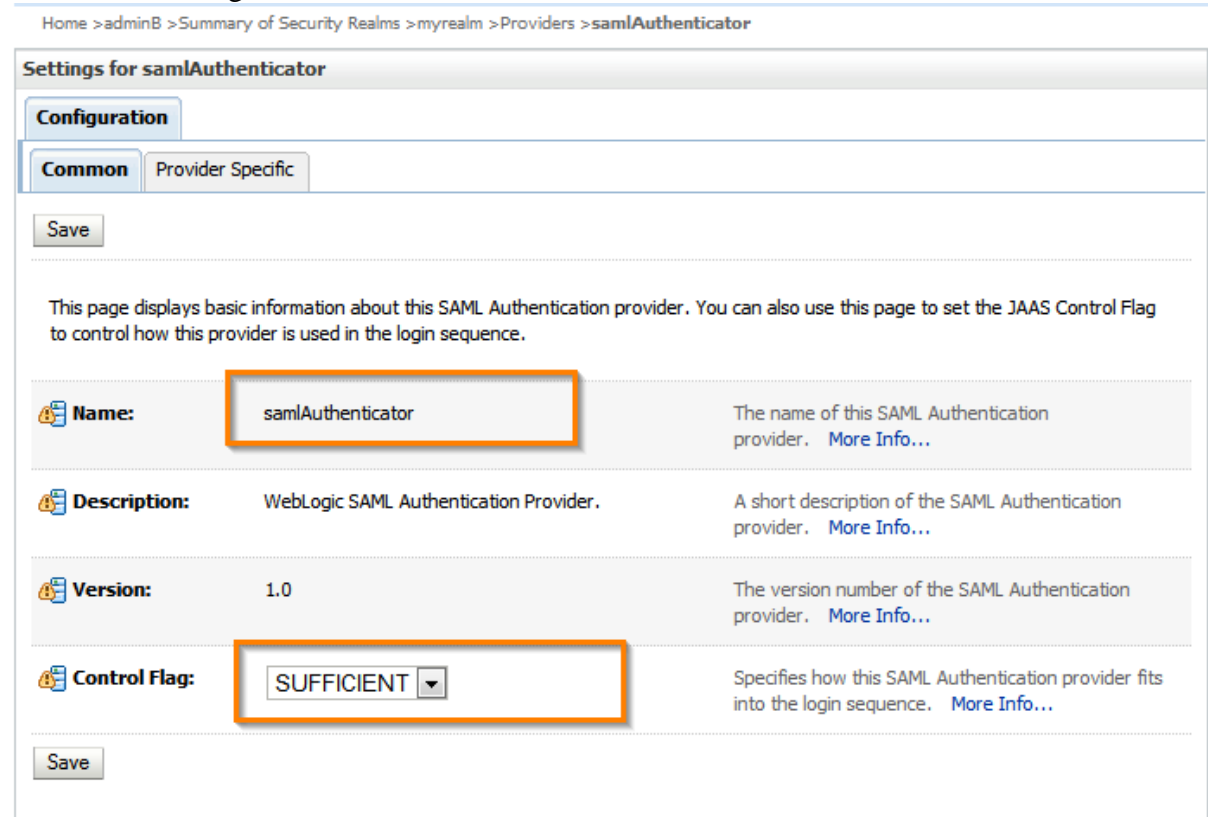


Figure 37. Configuring a SAMLAuthenticator to use virtual users.

We can test this with the user ssouser02 which is present in domainA but not in domainB.

### 3.12 Setting the Binding Sequence

The SAML Bindings which is chosen by the Federation Services is determined by the sequence as the Bindings appear in the Metadata file. We configure this in step 3. configure SAML 2.0 Identity Provider explained in Chapter 3.6.3 and in step 7. configure SAML 2.0 Service Provider as explained in Chapter 3.6.7. just before exporting the metadata files. In the Admin Server Console we can prefer a binding and set a default. This is visible in the resulting metadata files as shown below.

adminA\_metadata.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="saml2CMP">
<md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIEYzCCA0ugAwIBAgIJMqBVFVTXfCMA0GCSqGSIb3DQEBCwUAMHgxGzAUBG9NBVBAITAlVTMRAw
DgYDVQQLIDAdNeVNOYXRlMQ8wDQYDVQQHDAZNeVrVd24xZmFzAVB9NVBAOmdk15T3JnYW5pemF0aW9u
MRkwFwYDVQQLDBBBGT1IgwEVVTVElORyBPTkxZMRlWEAYDVQDDA1DZXJ0R2VUQ0EwHhcNMjUwNTE1
MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAw
MA0GALUEBwwGTXlUb3duMRcwFQYDVQKDA5NeU9yZ2FuaXphdG1vb3JlZmBcGALUECwwQkR9SIFRF
U1RJTkcwT05MWTETQMA4GALUEAwHU2NvcnBpbzCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAlf4SfSNVpV8dK6+pK+W5pq0YgKA9bMeTPfIJMdHnuhLIMWudqDnE+gVGuALKLqoxCo+dleJ
fEfJz9BzmlsesAnt4K8QDNzUFac5X0dpS1liI2SUTB1LYVGRHW9E2EFmWEU74f9P/vLy1llykf7f
VXonWgxZpY2XvetEni7V/j1abIMW46DErJ+04+R3zOMsBRRBLA9/8thp1QJLppq09bzeRt+utuB
EnstGW63h5ndSgZtWwhurg5Hq3lZQNsQwE92kEHhfjyzG2sG27UTKzwrOb18m/3i9e1SbychrgVS
7QtwsPp1MvC43X3PoyQPvW9b9CEQue19uZkpkY+OkCAwEAAaOB8TCB7jAUBGNVHRMEA JAAMA4G
A1UdDwEB/wQEAWID+DadBgNVHQ4EFQQUV03RZqkGbAtLe0ArTD034gbvZAWgBEGALUdIwSBqTCB
poAUNDj9RdiAz8fS6N8d+KE5sBGIAGqhfKR6MHgxCzAUBGNVBAITAlVTMRAwDgYDVQQLIDAdNeVNO
YXRlMQ8wDQYDVQQHDAZNeVrVd24xZmFzAVB9NVBAOmdk15T3JnYW5pemF0aW9uMRkwFwYDVQQLDBBB
GT1IgwEVVTVElORyBPTkxZMRlWEAYDVQDDA1DZXJ0R2VUQ0GCEEAES1bEeQe87ZDqAZkCa/KAWDQYJ
KoZlHvcNAQELBQADggEBAAcGpFZWVtoZ8fnVXe6LxHB3dAo2706t659e412nsj3tYmANIC6N+EP
LhryvBTz3540KngBhuwFEe5B509yZrTJKyUyTSSyxW7Aw5VSHNgQuhdNda9Y0K0Bl3A
M8msNRA2MCjLtey59Enl5OpKtVw1C/1ZzhHF7bgc4W5yOew+yODXvQgtE22bAHmlL0FBekTozaSa
/wyNfTSBmhUZGQuOghuJtX9m/BdomV9+ZvW2da6DZnzqcelLlVbtKWe3t3k8d8TAPnIzY9hzy4Tx
euUdASdif2bxjxiix5yD2V2StiQpr0dnY/JJJurOzkEFG47rMoOmt2e0zCE=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://localhost:7001/saml2/idp/ars/soap" index="0" isDefault="true"/>
<md:SingleSignOnService Bindings="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="http://localhost:7001/saml2/idp/sso/artifact"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://localhost:7001/saml2/idp/sso/post"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://localhost:7001/saml2/idp/sso/redirect"/>
</md:IDPSSODescriptor>
<md:Organization>
<md:OrganizationName xml:lang="de"/>
<md:OrganizationDisplayName xml:lang="de"/>
<md:OrganizationURL xml:lang="de">http://www.domainB.com</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="technical">
<md:Company>Disney</md:Company>
<md:GivenName>Duck</md:GivenName>
<md:SurName>Donald</md:SurName>
<md:EmailAddress/>
<md:TelephoneNumber/>
</md:ContactPerson>
</md:EntityDescriptor>
```

Here the artifact binding will be chose as the preferred binding for the SingleSignOnServices. In adminB\_metadata.xml the format is more explicit, containing an index number and a default flag.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="saml2AP">
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIEYzCCA0ugAwIBAgIJAJWd1sRbDhskMA0GCSqGSIb3DQEBCwUAMHgxGzAUBG9NBVBAITAlVTMRAw
DgYDVQQLIDAdNeVNOYXRlMQ8wDQYDVQQHDAZNeVrVd24xZmFzAVB9NVBAOmdk15T3JnYW5pemF0aW9u
MRkwFwYDVQQLDBBBGT1IgwEVVTVElORyBPTkxZMRlWEAYDVQDDA1DZXJ0R2VUQ0EwHhcNMjUwNTE1
MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAwNTE2MTEzNTUyWhcNMzAw
MA0GALUEBwwGTXlUb3duMRcwFQYDVQKDA5NeU9yZ2FuaXphdG1vb3JlZmBcGALUECwwQkR9SIFRF
U1RJTkcwT05MWTETQMA4GALUEAwHU2NvcnBpbzCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAlf4SfSNVpV8dK6+pK+W5pq0YgKA9bMeTPfIJMdHnuhLIMWudqDnE+gVGuALKLqoxCo+dleJ
fEfJz9BzmlsesAnt4K8QDNzUFac5X0dpS1liI2SUTB1LYVGRHW9E2EFmWEU74f9P/vLy1llykf7f
VXonWgxZpY2XvetEni7V/j1abIMW46DErJ+04+R3zOMsBRRBLA9/8thp1QJLppq09bzeRt+utuB
EnstGW63h5ndSgZtWwhurg5Hq3lZQNsQwE92kEHhfjyzG2sG27UTKzwrOb18m/3i9e1SbychrgVS
7QtwsPp1MvC43X3PoyQPvW9b9CEQue19uZkpkY+OkCAwEAAaOB8TCB7jAUBGNVHRMEA JAAMA4G
A1UdDwEB/wQEAWID+DadBgNVHQ4EFQQUV03RZqkGbAtLe0ArTD034gbvZAWgBEGALUdIwSBqTCB
poAUNDj9RdiAz8fS6N8d+KE5sBGIAGqhfKR6MHgxCzAUBGNVBAITAlVTMRAwDgYDVQQLIDAdNeVNO
YXRlMQ8wDQYDVQQHDAZNeVrVd24xZmFzAVB9NVBAOmdk15T3JnYW5pemF0aW9uMRkwFwYDVQQLDBBB
GT1IgwEVVTVElORyBPTkxZMRlWEAYDVQDDA1DZXJ0R2VUQ0GCEEAES1bEeQe87ZDqAZkCa/KAWDQYJ
KoZlHvcNAQELBQADggEBADd/OJ4vuhG5Ijv0y5Haf44/Y/ajUVowqil/Cx5HwL27K6v03FC7Xxha
```

```
80o2ZwtTYinsVopDsgaKu/34+tkoYMwHpbxscJ6vSuDRi7+3gTsakle/DQgupfUDrm6JFVPLiid
P6wehJteDKQ3gg4jtbm23qzvsIYNP0D4eVdCfcXNg9WwKkOeY9RvKST/7Us0SkelffJZRvtHrmi
qp6sz7KyUjLTAmPm3wHke2rQJl5MGyhBXehKPlEpud+VGxAA81tuGylYAdAivrVz+/4OdChblHsx
eYKkoTVl4wygSv26JkilpYFyOk/qyRBIWCmPtNUKP91mMJCQtA+VLthMJE=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://localhost:7003/saml2/sp/ars/soap" index="0" isDefault="true"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://localhost:7003/saml2/sp/acs/post" index="0" isDefault="true"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="http://localhost:7003/saml2/sp/acs/artifact" index="1"/>
</md:SPSSODescriptor>
<md:Organization>
<md:OrganizationName xml:lang="de">www.domainB.com</md:OrganizationName>
<md:OrganizationDisplayName xml:lang="de">www.domainB.com</md:OrganizationDisplayName>
<md:OrganizationURL xml:lang="de">http://www.domainB.com</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="technical">
<md:Company>Disney</md:Company>
<md:GivenName>Daisy</md:GivenName>
<md:SurName>Duck</md:SurName>
<md:EmailAddress/>
<md:TelephoneNumber/>
</md:ContactPerson>
</md:EntityDescriptor>
```

Here the HTTP-POST Binding will be chosen for the AssertionConsumerService. If we want to change this behavior for a Partner-SP or Partner-IdP, we can modify the xml files directly and re-import the modified metadata files. Alternatively we could change the settings in the configurations of the Identity Provider and Service Provider (step 3 and step 7). But then we have to export and import the files again, just changing the settings will have no effect.

### 3.13 SAML 2.0 Examples in Blog Posts.

The following is a list of some blogs that demonstrate different aspects of SAML configuration in WLS.

SAML 2.0 Example from Biemond, based on earlier blog post, using ssl demo certs and saml metadata file.

- <http://biemond.blogspot.de/2009/09/sso-with-weblogic-1031-and-saml2.html>
- <http://biemond.blogspot.de/2009/05/sso-with-weblogic-103-and-saml.html>

Steps to configure SAML 2 on Weblogic Server 10.3.0, using pointbase for the rdbms security realm.

<https://blogbypuneeth.wordpress.com/2011/01/15/steps-to-configure-saml-2-on-weblogic-server-10-3-0/>

Configure WSO2 Identity Server SAML2 IDP with Oracle Weblogic as Service Provider Example of integration between WSO2 and WLS

<http://tanyamadurapperuma.blogspot.de/2013/09/configure-wso2-identity-server-saml2.html>

### 3.14 Conclusion

This tutorial comprises a comprehensive description of a web single-sign-on scenario using SAML 2.0 in weblogic server. It demonstrates all steps necessary to install, configure and run a demo application. The whole tutorial is split into four parts. In the first part we walked through the installation of weblogic server on a windows machine and the creation of two domains. We also installed the sample applications in this part. In part two we looked at the SAML configuration in weblogic server, using the Administration Console. We introduced a recommended configuration sequence which comprises 14 steps and was illustrated by

## Web Single Sign-On with SAML 2.0

diagrams and mind maps. While this sequence is not mandatory, it structures the manual configuration process in an efficient manner and can serve as a template for configuring real world SAML scenarios.

In the third part we demonstrated two test cases for the service provider initiated flow scenario. In the fourth part we extended the example to include an identity provider initiated flow scenario and demonstrated an advanced weblogic feature called virtual user.

The tutorial concludes with some configuration and debugging tips and a brief overview of other blog post covering similar subjects.