Single Sign-On between SAP Portal and SuccessFactors

Dimitar Mihaylov
7/1/2012
## Contents

1. Overview .................................................................................................................................................. 3  
2. Trust between SAP Portal 7.3 and SuccessFactors .................................................................................. 5  
   2.1. Initial configuration in SAP Portal 7.3 ............................................................................................. 5  
   2.2. Add SuccessFactors system as trusted SAML 2.0 service provider .............................................. 10  
   2.3. Add Portal 7.3 as a trusted identity provider in SuccessFactors .................................................... 17  
   2.4. Create in SAP Portal an URL iView to SuccessFactors ................................................................. 21  
3. Additional configuration required for SAP Portal 7.0x ......................................................................... 25  
   3.1. Establish trust between the AS Java 7.3 system (IDP) and the SAP Portal 7.0x .............................. 26  
   3.2. Enable authentication with SAP Logon Tickets in the IDP .......................................................... 29  
4. User Mapping ......................................................................................................................................... 31  
5. Troubleshooting ..................................................................................................................................... 32  
   5.1. Security Troubleshooting Wizard on AS Java 7.2/7.3 .................................................................. 32  
   5.2. Web Diagnostic Tool on SAP Portal 7.0x ....................................................................................... 32  
   5.3. SuccessFactors .............................................................................................................................. 32  

Copyright...................................................................................................................................................... 34
1. Overview

This document describes how to enable single sign-on from a customer’s on-premise SAP Portal to SuccessFactors. Single sign-on is based on standard SAML 2.0 mechanisms and the Identity Provider of SAP Netweaver Single Sign-On is used.

For simplicity, the example setup assumes that the user IDs in SAP Portal and SuccessFactors are the same. However, you can set up the same scenario when the user IDs in the two systems are different, as briefly described in section 4 of this document.

You can configure a direct trust relationship between the systems if you are using SAP Portal 7.3. In this case, the SAP Portal can act directly as SAML 2.0 identity provider (IDP), and the SuccessFactors system can act as SAML 2.0 service provider (SP).
If you are using SAML Portal 7.0x, an additional NetWeaver Application Server Java 7.2 or 7.3 is required.

Note: In order for an SAP NetWeaver Application Server 7.2 or 7.3 to act as a SAML 2.0 identity provider, you need to install the IDMFEDERATION software component (SCA), which is included in both SAP NetWeaver Single Sign-On or SAP NetWeaver Identity Management.
2. Trust between SAP Portal 7.3 and SuccessFactors

2.1. Initial configuration in SAP Portal 7.3


Select the “SAML 2.0” tab and click the “Enable SAML 2.0 Support” button.
Enter the name of the local provider and select operational mode “Identity Provider”.

Click the “Browse” button for the signing key-pair. A signing key-pair should be generated for the local provider. It will be used as an encryption key-pair as well.
Here are the next steps:

Step 1

Step 2
Continue with the initial wizard.

Use the default settings (might differ from the screenshot) and click “Finish”.
2.2. Add SuccessFactors system as trusted SAML 2.0 service provider

Click on link “Trusted Providers”

Click “Add” and select “Manually”.

Click “Add” and select “Manually”.
Enter the name of the service provider. Check the information provided by SuccessFactors for the correct name - in most of the cases this is https://www.successfactors.com. After entering the name, click “Next” to continue.

Click “Browse” to select the signing and encryption certificates.
Click “Import Entry” to upload the certificate provided by SuccessFactors.

Select type “X.509 Certificate”, find the file, and click “Import”.
Select the newly imported certificate and click “OK”.

Select the same certificate as an encryption certificate and click “Next”.

Add an Assertion Consumer Service. Note: Check the documentation provided by SuccessFactors for the correct URL.

Optionally you may also add a Single Logout Service.
Do not enter other endpoints. Click “Next” to the end, then click “Finish”.

Click “Edit”, then click “Add” under “Supported Name ID Formats”. Select format “Unspecified” and source “Logon ID”.
Afterwards click “OK”, “Save”, and “Enable”.
2.3. Add Portal 7.3 as a trusted identity provider in SuccessFactors

In order to perform the next steps, you need to have a provisioning account in SuccessFactors. If you do not have this yet, the SuccessFactors administrators have to establish the trust relationship.

As a first step, you need to export the signing certificate of the Portal 7.3 identity provider. Open NetWeaver Administrator and go to Configuration ➔ Certificates and Keys.
Select the view “SAML2” and the entry “portal73-cert”. Then click “Export Entry”.

Select the export format to be Base64 and click “Download”. 
Save the file and open it with a text editor. The content should look like this:

Now that you have the signing certificate, you can start with the configuration in the SuccessFactors system. There, open the “Single Sign-On (SSO) Settings”: 
The minimal set of settings is the following:

The “SAML Issuer” field has to be the same as the name of the identity provider entered in the SAP Portal 7.3 system. The “SAML Asserting Party Name” is just an alias and could have any value. In “SAML Verifying Certificate”, paste the signing certificate you have exported from the identity provider. Finally do not forget to click the button “Add an asserting party”.

To enable the SAML login, you also have to enter a “Reset Token” and save it.

2.4. Create in SAP Portal an URL iView to SuccessFactors
Enter the host name of the SAP Portal 7.3 system and the path “/saml2/idp/sso”.

Edit the newly created iView, then add two parameters: “saml2sp” and “RelayState”. In our case, they have the following values:

saml2sp: https://www.successfactors.com
RelayState: [https://salesdemo4.successfactors.com/xi/ui/home/pages/home.xhtml](https://salesdemo4.successfactors.com/xi/ui/home/pages/home.xhtml)

Please note that you need to consult the SuccessFactors documentation to find the correct values for your configuration.

Save the changes and close the iView.
Now you can test your configuration by logging in with a user that has accounts in both the SAP Portal and SuccessFactors. Then navigate to this URL iView.

You may change the options of the URL iView and open the SuccessFactors application in a new browser window, for example.
3. Additional configuration required for SAP Portal 7.0x

If you have a SAP Portal 7.0x version, the Identity Provider cannot be deployed on this system directly. You need an additional SAP NetWeaver Application Server Java 7.2 or 7.3 for the Identity Provider. Besides that, the scenario is identical to the one previously described.

Thus, the difference is that the user will first authenticate to the SAP Portal 7.0x system, and then navigate to the IDP in order to get an SAML 2.0 assertion to access the SuccessFactors system. To establish single sign-on between the SAP Portal 7.0x and the IDP, we will use the SAP Logon Ticket which the SAP Portal 7.0x issues by default. This cookie is then returned as a domain cookie with the name MYSAPSSO2. Please note that both systems, SAP Portal 7.0x and IDP, have to be in the same domain for the cookie to be sent to the IDP.
3.1. Establish trust between the AS Java 7.3 system (IDP) and the SAP Portal 7.0x

You should configure the IDP system to trust SAP Logon Tickets issued by the SAP Portal 7.0x system. Go to NetWeaver Administrator → Configuration → Trusted Systems.

Connect to the Portal 7.0x system to obtain its signing certificate. First click on “Add Trusted Systems” button and select the option “By Querying Trusted System”. If you have previously exported the certificate, you may use also the other option.
Enter the connection data into the SAP Portal 7.0x system.

Confirm the creation of the trust relationship by clicking “Finish”
Now you will see that the system was added to the list of trusted systems.
3.2. Enable authentication with SAP Logon Tickets in the IDP

By default, the IDP will accept authentication with user name and password. In order to enable authentication with SAP Logon Tickets, open the SAML 2.0 configuration. In “Local Provider”, select the tab “Identity Provider Settings”.

![Authentication and Single Sign-On: SAML 2.0](image)
Click on “Edit” and the table “Supported Authentication Contexts”. Select “SAPLogonTicket”. Select “Default HTTPS Authentication Contexts” from “Copy to”.

Save the changes. The list of “Default HTTP Authentication Contexts” should contain “SAPLogonTicket” as shown in the screenshot.
4. User Mapping

If the user identifiers in the SAP Identity Provider (IDP) and the SuccessFactors system are not identical, you can configure a user mapping at the identity provider side. Please note that the user ID for the SuccessFactors system has to be available as a user attribute in the User Management Engine (UME) of the IDP.

Change the following configuration: In the SAML 2.0 configuration UI, select Trusted Providers → SuccessFactors system → Identity Federation → Select source “User Attribute”, then enter the name of the attribute. In our case, this is “sfuserid”:

![Configuration UI screenshot]

Note: This is the only configuration change you have to perform for user mapping.
5. **Troubleshooting**

5.1. **Security Troubleshooting Wizard on AS Java 7.2/7.3**

5.2. **Web Diagnostic Tool on SAP Portal 7.0x**

5.3. **SuccessFactors**
A link to the SSO Log Viewer is available at the end of the “Single Sign-On (SSO) Settings” page.
You will find information on failed SSO attempts there.