Outbound SSO to 3rd-Party Guide

PArtner and support

Here you will find the information that you need to set up 3rd-Party SAML2 with SF Platform/BizX as the IDP.

# Overview of the process:

|  |  |  |
| --- | --- | --- |
| Action: | | To be performed by: |
| Service Provider Initiated SAML2 | | |
|  | Step 1 – To provide SF SAML Metadata | Partner or Support |
|  | Step 2 – To provide the Assertion Consumer Service URL | Partner or Customer |
|  | Step 3 – To provide a DeepLink URL into the 3rd-Party application | Partner or Customer |
|  | Step 4 – To create a link within SF application | Partner or Support |
|  | Step 5 – To setup a Trusted Service Provider URL | Partner or Support |
|  | Step 6 – To configure the 3rd-Party vendor to accept SAML2 logins from SF | Customer or 3rd-Party vendor |
|  | Step 7 – To sync users between SF and the 3rd-Party vendor system | Everyone |
|  | Step 8 – To test the login | Customer |
| Identity Provider Initiated SAML2 | | |
|  | Step 1 – To provide the SP Initiated URL | Partner or Support |
|  | Step 2 – Create the IDP URL | Partner or Support |
|  | Step 3 – To place the link within SF application | Partner or Support |

# Service Provider Initiated SAML2

## Step 1 – To provide SF SAML Metadata

SuccessFactors consultant provides Customer/3rd Party Vendor the SAML Metadata for the SuccessFactors Instance.

Here is the generic URL to grab the metadata:

https://[SFSF data center servername]/idp/samlmetadata?company=[sf\_company\_instance]

E.g.: <https://performancemanager5.successfactors.eu/idp/samlmetadata?company=test_customer>

## Step 2 – To provide the Assertion Consumer Service URL

The customer or their vendor provides SuccessFactors consultant the ACS (Assertion Consumer Service) URL for their application. This is the location where SF will send the SAML Login Responses. It will also be included in the SAML Login Requests that the vendor sends to SF.

## Step 3 – To provide a DeepLink URL into the 3rd-Party application

The customer or their vendor provides SuccessFactors consultant a deep link URL into the 3rd-Party application. This URL will start a Service Provider Initiated login process at the vendor and cause them to send a SAML Request to SuccessFactors.

For IDP Initiated Login see additional instructions on Identity Provider Initiated SAML2.

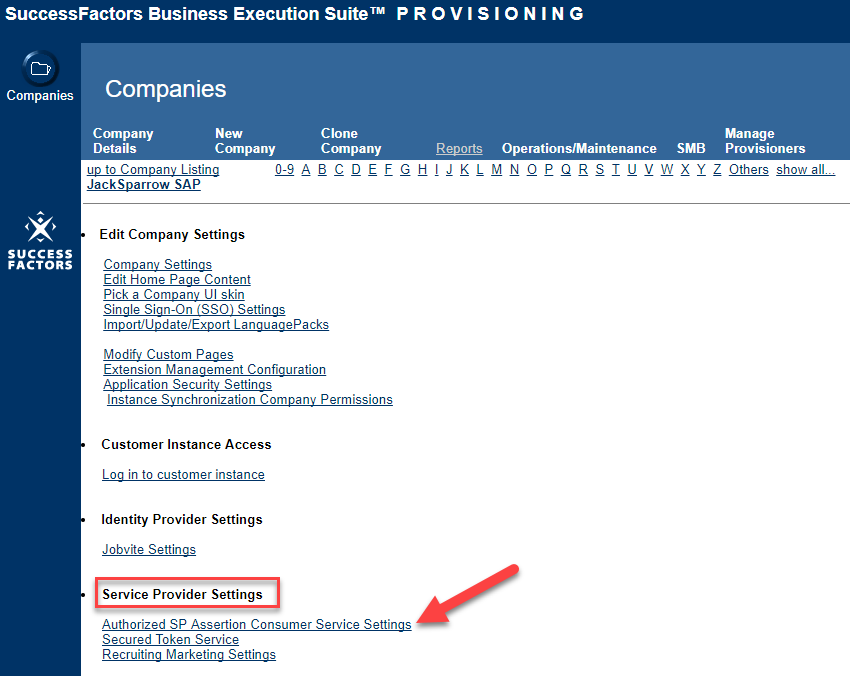
## Step 4 – To create a link within SF application

The SuccessFactors Consultant will create a link within SF application with the URL from Step 3. The consultant will work with the customer to determine the location in the app and other details for creating the link.

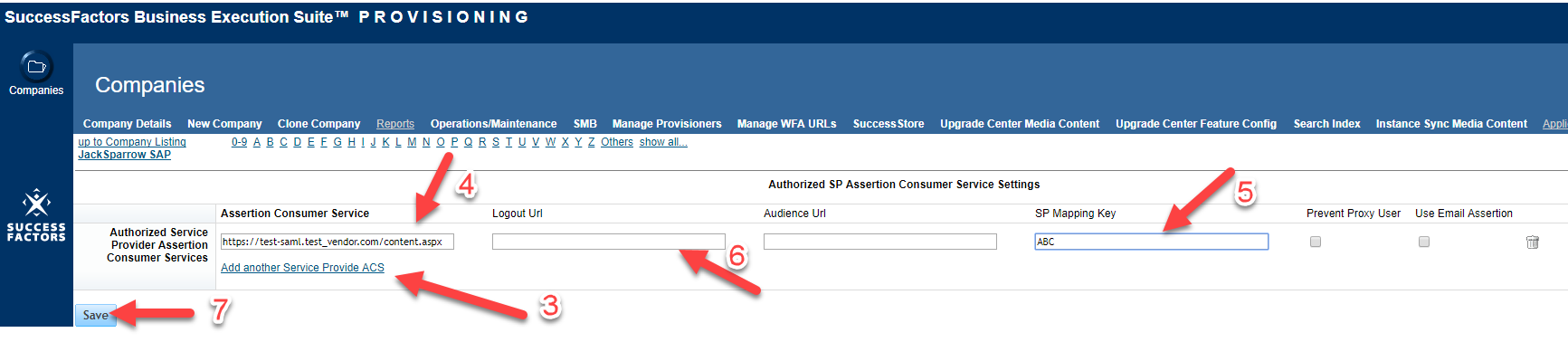
## Step 5 – To setup a Trusted Service Provider URL

The SuccessFactors Consultant sets up a Trusted Service Provider using the URL from Step 2. This is done by logging into the internal SuccessFactors Provisioning system. Accessing the customer specific instance. In Provisioning, access:

1. *Service Provider Settings*
2. *Authorized SP Assertion Consumer Service Settings*



1. *Add another Service Provider ACS*
2. Enter the URL from the customer in the new blank line under *Assertion Consumer Service*
3. Enter a name for the *Mapping Key* (you can set any name/key/abbreviation here).
4. If the customer has provided a SAML Logout URL this will be added in column 2
5. Click on Save



**Note**: By default, Bizx sends the UserID as the NameID parameter in the SAML message. There is a checkbox on the right side of the screen that can be enabled if you wish for the system to send the Email Address as the NameID parameter instead. Email or UserID are the only supported values.

## Step 6 – To configure the 3rd-Party vendor to accept SAML2 logins from SF

The 3rd-Party vendor configures their system to accept SAML2 logins from SuccessFactors.

If their system supports metadata import they can import the file from Step 1. Otherwise, they can pull the values they need manually from the file.

Different vendors may use specific details but they should find anything they need in the metadata file. One of the key items everyone will need is the SuccessFactors ACS where they will send the SAML Requests to.

E.g.:

<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://performancemanager5.successfactors.eu/sf/idp/SAML2/SSO/POST/company/test\_company"/>

## Step 7 – To sync users between SF and the 3rd-Party vendor system

The users need to be synched between SuccessFactors and the 3rd party vendor. For this, there are numerous options to be followed. The SuccessFactors Consultant will work with the customer, the vendor and any other teams required to accomplish this. Typically, the users are exported from SuccessFactors and loaded in the vendors system.

There are two possible values that can be sent in the logins. By default UserID will be sent as NameID. If the customer prefers we can send Email Address as NameID. SuccessFactors will be sending the value out in the NameID field in the SAML Response to the vendor. The vendor will perform whatever additional steps are required to provision the users in their system.

## Step 8 – To test the login

At this point the process should be ready to test. The test flow will be:

1. User logs into SuccessFactors
2. User clicks on link to the 3rd-Party vendor.
3. Vendor checks if user is logged in to their application.
   1. If they are, it will show them their content.
   2. If not, the vendor POSTS (not GET) a SAML Request to SuccessFactors.

This will go to the ACS URL for the customer’s instance.

1. SuccessFactors processes the Request. Among other things there is a check that the ACS URL within the SAML Request matches the one configured in SuccessFactors in Step 5 (setup a Trusted Service Provider URL).
2. SuccessFactors verifies that the user is currently logged in.
3. SuccessFactors POSTS (not GET) the SAML Response to the vendors ACS URL. It will contain a NameID value that matches the SuccessFactors UserID or NameID.
4. The vendor verifies that the Response is correct, logs in the user and shows the user the expected content.

Here is an example of the process for a test user in the test\_customer instance. The 3rd party vendor is test\_vendor.

Example:

1. The user clicks on the link in the application from within SuccessFactors:

<https://test-saml.test_vendor.com/content.aspx>

1. The vendor sends SuccessFactors a SAML Response to the ACS URL. The examples below contain UserID in the NameID. There is an example of the Email Address as NameID format at the bottom.

<https://performancemanager5.successfactors.eu/sf/idp/SAML2/SSO/POST/company/test_company>

SAMLRequest=

Decoded the request looks like this:

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="\_13a0af95-3dff-428d-b0fa-bd5091999fd5" Version="2.0" IssueInstant="2016-03-08T16:43:35Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="https://test-saml.test\_vendor.com/content.aspx"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">test\_vendor</saml:Issuer><samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" AllowCreate="true"/><samlp:RequestedAuthnContext xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Comparison="exact"><saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef></samlp:RequestedAuthnContext></samlp:AuthnRequest>

SuccessFactors Send a SAML Response back to the vendors SAML ACS URL. This is POSTed to the vendors ACS URL

<https://test-saml.test_vendor.com/content.aspx>

SAMLResponse= 

Decoded the response looks like this:

<?xml version="1.0" encoding="UTF-8"?>

<saml2p:Response Destination="https://test-saml.test\_vendor.com/content.aspx" ID="\_5b493bf1-027f-4889-8f43-0d0cd8bf8ff2" InResponseTo="\_17ece8d8-b1ea-4d7f-9b62-3fd05aa9b1fa" IssueInstant="2016-03-11T20:11:14.092Z" Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://salesdemo5.successfactors.eu/sf/idp/SAML2/company/test\_company</saml2:Issuer><saml2p:Status><saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status><saml2:Assertion ID="SF\_SAML2.0\_1808aa0d-6f64-4edb-a47b-d789c54cb13c" IssueInstant="2016-03-11T20:11:14.091Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><saml2:Issuer>https://salesdemo5.successfactors.eu/sf/idp/SAML2/company/test\_company</saml2:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>

<ds:Reference URI="#SF\_SAML2.0\_1808aa0d-6f64-4edb-a47b-d789c54cb13c" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>

<ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">hOTQzDhQwywRlIwjiKFOFvFHbUU=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

AA/5UEpMEldiS0CcCfk13bWMpPoD9RMYMifKG3mw4Pfp+J72kxA4UNtm3lnCyYqHj4aUM7qIjBy5

V0hoR0qPClhCBFf6WqIVQEpBVi7Utuz8ENsCzMNPjQ3mq/NjB4Q7lv5IJfQvHrV727QPwoT5rPsh

m/rlvKmCP7PCsdJk6CM=

</ds:SignatureValue>

<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICDTCCAXagAwIBAgIETJj9LjANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzEbMBkGA1UE

ChMSU3VjY2Vzc2ZhY3RvcnMuY29tMQwwCgYDVQQLEwNPcHMxETAPBgNVBAMTCFNGIEFkbWluMB4X

DTEwMDkyMTE4NDUwMloXDTI1MDkxOTE4NDUwMlowSzELMAkGA1UEBhMCVVMxGzAZBgNVBAoTElN1

Y2Nlc3NmYWN0b3JzLmNvbTEMMAoGA1UECxMDT3BzMREwDwYDVQQDEwhTRiBBZG1pbjCBnzANBgkq

hkiG9w0BAQEFAAOBjQAwgYkCgYEArA9RLNnL9Pt6xynFfYfa8VXAXFDG9Y8xkgs3lhIOlsjqEYwb

SoghiqJIJvfYM45kx3aB7ZrN96tAR5uUupEsu/GcS6ACxhfruW+BY6uw8v6/w2vXhBdfFjBoO+Ke

Lx4k3llleVgKsmNlf81okOXv1ree8wErfZ3ssnNxkuQgGB0CAwEAATANBgkqhkiG9w0BAQUFAAOB

gQBeBCSMFnY8TB6jtWoSP/lorBudhptgvO7/3r+l/QK0hdk6CVv+VQmSilNPgWVgU9ktZGbNkZhw

IgwnqIQHAi6631ufkYQJB+48YUe1q/pv6EWaeIwGvcGYSXZp/E/aGZPtceTIXFPfqOyHQoFtb0nq

MMFWoDhpXUHmlroyTc9sJg==</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature><saml2:Subject><saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">Admin</saml2:NameID><saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml2:SubjectConfirmationData InResponseTo="\_17ece8d8-b1ea-4d7f-9b62-3fd05aa9b1fa" NotOnOrAfter="2016-03-11T20:21:14.091Z" Recipient="https://test-saml.test\_vendor.com/content.aspx"/></saml2:SubjectConfirmation></saml2:Subject><saml2:Conditions NotBefore="2016-03-11T20:01:14.091Z" NotOnOrAfter="2016-03-11T20:21:14.091Z"><saml2:AudienceRestriction><saml2:Audience>test\_vendor</saml2:Audience></saml2:AudienceRestriction></saml2:Conditions><saml2:AuthnStatement AuthnInstant="2016-03-11T20:11:14.091Z" SessionIndex="vHKWVnxD3T3di2NxVM4KNyUkX1FC7noFTXxgclS2k9KpqKmgPNJ/vjPJ0w3dugpyJMJLsFlWhRXFoRq3gjxPRQ=="><saml2:AuthnContext><saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef></saml2:AuthnContext></saml2:AuthnStatement><saml2:AttributeStatement><saml2:Attribute Name="companyid"><saml2:AttributeValue xsi:type="xs:string">test\_company</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="locale"><saml2:AttributeValue xsi:type="xs:string">en\_US</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="companyuuid"><saml2:AttributeValue xsi:type="xs:string">80c5ed70\_d668\_48b3\_a951\_e57c7deed7ed</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="loggedinuserid"><saml2:AttributeValue xsi:type="xs:string">Admin</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="zonesessionid"><saml2:AttributeValue xsi:type="xs:string">b1424bf1-b03e-46b5-b02b-efdc0e03989a</saml2:AttributeValue></saml2:Attribute></saml2:AttributeStatement></saml2:Assertion></saml2p:Response>

Notice the NameID value of “Admin” that identifies the user attempting to login to the vendor using SSO.

**Note**: If we send Email address in NameID rather than UserID it will look like this.

Subject><saml2:NameID Format=\"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress\">daniel.hayes@sap.com</saml2:NameID><saml2:SubjectConfirmation Method=\"urn:oasis:names:tc:SAML:2.0:cm:bearer\"><saml2:SubjectConfirmationData

# Identity Provider Initiated SAML2

For some 3rd-Parties, we can support IDP Initiated Logins. Follow all the instructions from Service Provider Initiated SAML2 section except Step 3. Instead of getting a deep link to customer, we will be creating a SuccessFactors hosted URL that will initiate a IDP login to the 3rd party.

## Step 1 – To provide the SP Initiated URL

Copy the SP Initiated URL from step 3 above.

Example of URL: <https://test_saml.test_vendor.com/content.aspx>

## Step 2 – Create the IDP URL

Create the IDP URL. The basic format will be:

Example of URL:

<https://performancemanagerX.successfactor.com/sf/idp-init-sso/mappingkey?RelayState=SPInitiatedURL>

Where:

* **Mapping Key test\_vendor**: We create this up while setting the Assertion Consumer Service URL in provisioning.
* **RelayState**: It is defined by the customer. E.g.: <https://test_saml.test_vendor.com/content.aspx>

## Step 3 – To place the link within SF application

Place the link created in the SF application, on a location that the customer will decide. When a user clicks it, we will send the SAML Response directly to the 3rd party.

**Note**: IDP Initiated Login to a 3rd-Party is not a commonly used feature. As of January 2017 it has only been configured/tested with one 3rd party (ADP). Customers should be informed that it may not work with their 3rd-Party vendor. We will need to do the actual setup/test/troubleshooting to find out on a case by case basis.