Reference Guide
SAP SuccessFactors HCM Suite
Document Version: Q3 2015 – September 11

CUSTOMER

SuccessFactors SAML2 Single Sign-On

SuccessFactors Implementation of SAML2 Standard

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	2015-09-11	Initial version

Contents

1 What Is Single Sign-On?

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in to each of them.

SuccessFactors offers a number of SSO options to allow users to access the application without entering their SuccessFactors username and password. This document describes the SAML2 option.

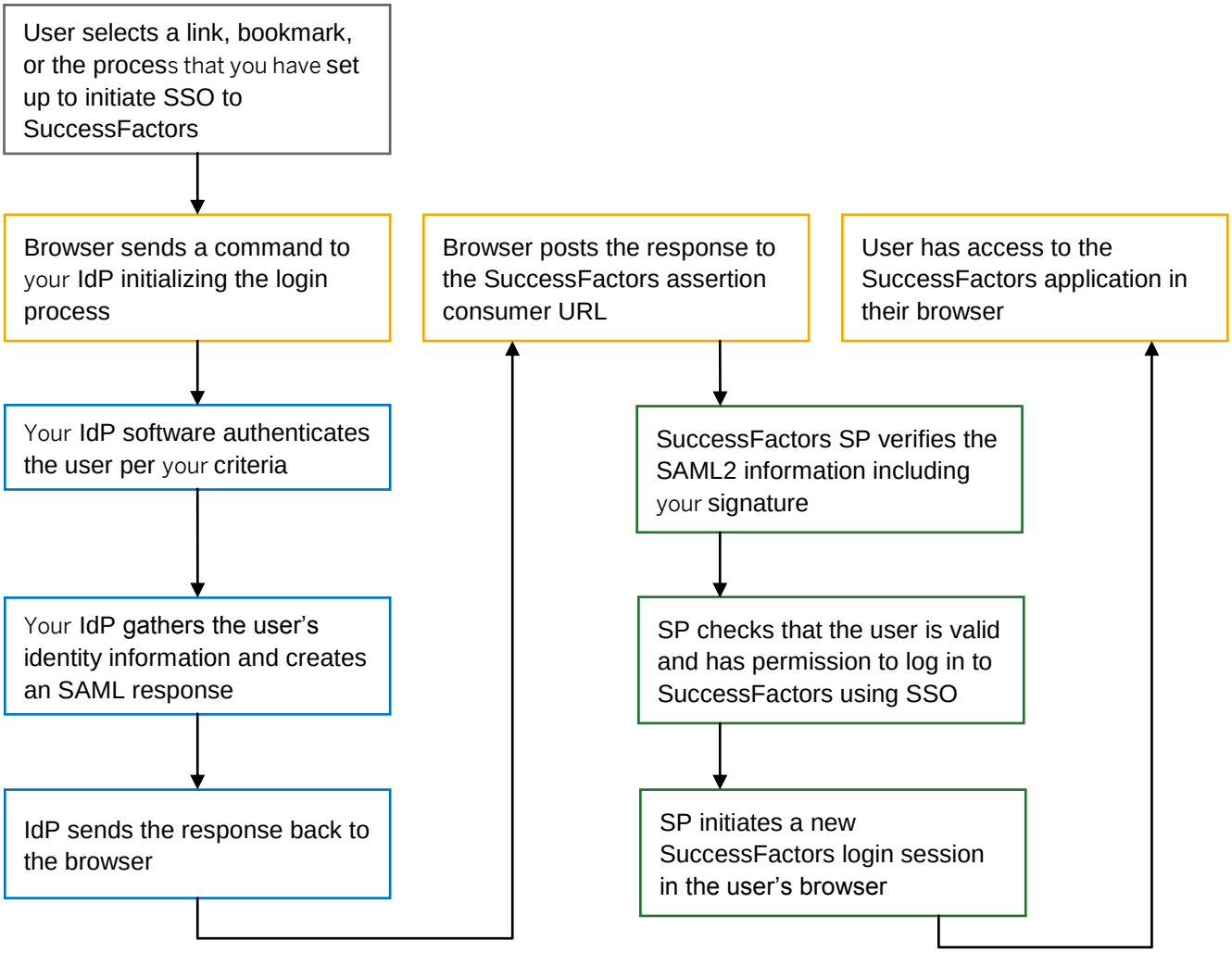
2 How Does SAML2 Work?

SSO generally takes place between two parties. The Identity Provider (IdP) has information to authenticate the users and generate SSO logins. The Service Provider (SP) offers a service that is accessible using your SSO. The SP must be able to accept customer-generated SSO logins and identify the user who you want to log in. This document covers the SAML2 SSO standard. In general, any SAML2 SSO software should work with the SuccessFactors application. We support the following SAML2 protocols:

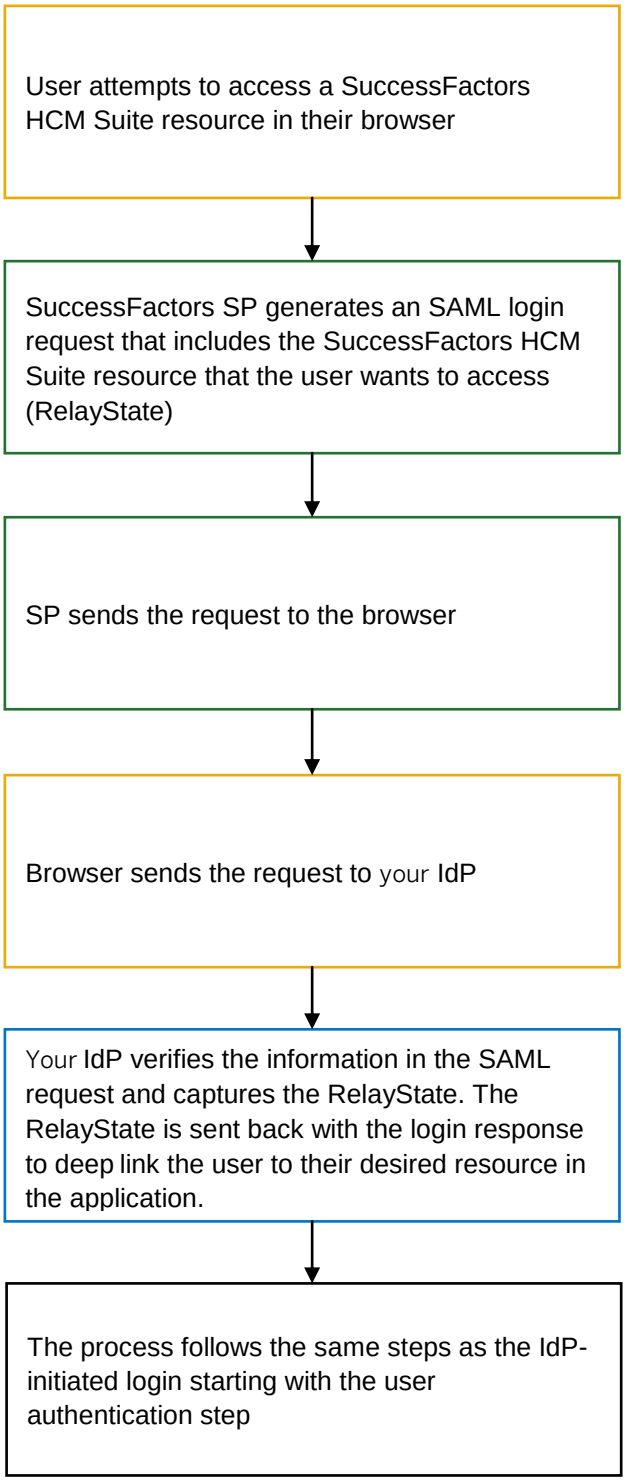
- IdP-initiated where a user starts the process internally
- SP-initiated where a user starts the process by attempting to connect to SuccessFactors

The processes look like this:

Identity Provider (IdP) Initiated SAML Single Sign-On



Service Provider (SP) Initiated SAML Single Sign-On



3 SuccessFactors Implementation of SAML2

The SAML2 specification provides a general framework to ensure SAML identity providers (IdP) and service providers (SP) work together properly. Within that framework, service providers offer features that best support their application and their customers. SuccessFactors offers the following:

IdP and SP Logins

You can connect using either or both. The default setup is for IdP-initiated and this must be completed for all SSO customers. Additional settings need to be configured to allow the optional SP-initiated logins.

Dynamic Deep Linking

The SP-initiated login option is designed to allow users to deep link to someplace other than the default landing page after an SSO login. For example, SuccessFactors typically sends users to our home page. With deep linking, they can land on their performance review or a course in SuccessFactors Learning or countless other locations within the application. When a user is not logged in and tries to access SuccessFactors, we send an SAML request to your identity provider URL. The response contains the login information and landing page details in an additional value called RelayState.

If you do not support SP-initiated SAML2, we offer a generic deep link feature. This accomplishes the same result (deep linking) as SP logins, but uses cookies. When a user is not logged in and tries to access SuccessFactors, we send their browser to the IdP-initializing URL that you provided. This is typically the same URL that users use to log in directly from their internal systems. The user goes through the IDP-initiated login process. After they are logged in, we read a cookie that was stored with their initial destination, and place them there instead of on the home page.

If you have both deep linking and SP-initiated logins enabled from a single IdP, we use SP-initiated rather than deep linking.

Dynamic deep linking should work with all links sent out by the application itself. These include things sent in system emails, course links generated by SuccessFactors Learning administrators, exported JAM links, and so on. We do **not** recommend copying the URLs directly from the browser and using them for bookmarks. There is no guarantee that a URL in the browser will create a valid link, or that a link will be valid in the future.

Static Deep Linking

If you use IdP-initiated logins, you can provide us with a RelayState value to send users somewhere other than the home page. We provide a list of supported RelayState values if you plan to use this option.

SP-Initiated Single Logout

You may want to perform some action in your home system when a user logs out of SuccessFactors. If you provide us with the destination URL, we can send a logout request when a user ends a SuccessFactors session.

Multiple Asserting Parties

If you have multiple identity providers, we can set up asserting parties for each one. This includes separate values for SAML issuer, signing certificate, and other settings. If one or more of the asserting parties is set to use SP-initiated logins, one of them can be set to be the default asserting party.

If you have multiple asserting parties and use deep linking, we need to identify to which IdP to send users for login information. If you have a default asserting party, we send them to that IdP. If not, we display a list of the available asserting parties and ask the user to select the appropriate one. Your administrator can configure the text identifying each available asserting party. After a user has logged on using a specific asserting party, we store a cookie in their browser. As long as they use the same browser and don't clear their cookies, they don't need to select the asserting party again.

SSO Redirects

By default, the SuccessFactors application shows users the login page when they log out, time out, or when they get a login error. You can host your own pages for these use cases. If you provide us with the URL or each page, we configure our SSO system to send the users there instead of the home page. We can redirect for the following use cases:

Use Case	Description
Logout	When the user logs out, we send them to the customer-hosted page.
Timeout	After a 30-minute inactivity timeout, we send the user to this page.
Invalid login	If the SSO login fails, we send the user to this page.
Invalid manager	The SuccessFactors HCM Suite application requires a valid manager hierarchy. If it is broken, we send the user to this page.
Missing credentials	If SuccessFactors receives an SSO login with no user information, we send the user to this page.
Deep link	Your IdP login link goes here if you plan to deep link, but are not using SP-initiated SAML.

Partial Organization SSO

You can allow some users to use SSO while others log in with passwords. No single user can have access to both methods at the same time. We can provide a document detailing the steps to set up partial SSO.

SAML SSO users do not have access to the password management system and are never forced to change their passwords. Passwords are not used as part of the SAML login process.

Users logging in with passwords are subject to all the password management rules and features that you have enabled.

4 SuccessFactors SAML2 Technical Details

The SuccessFactors service provider is configured to accept a wide variety of SAML responses and assertions. However, your IdP must adhere to the following rules:

Supported Attributes in SAML Response

SuccessFactors supports the following attributes in a SAML response:

- SSO_ID
- companyid
- companyuuid
- locale
- Loggedinuserid

HTTPS Encryption and POST

All communication with the SuccessFactors application must use HTTPS in the browser. SAML responses sent to SuccessFactors must use POST. URLs sent to deep link into the application and SAML requests do not need to be POSTed.

User Identifier

SuccessFactors accepts two values to identify the user logging in using SAML2. The most common is NameID. SuccessFactors also supports the UserName attribute. Whichever method is used, the value is compared with the UserName in the SuccessFactors application. If that user does not exist or does not have permission to log in, the user is unable to access the application.

The system checks for the UserName attribute first. In the assertion, SuccessFactors expects something similar to the following:

```
<saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string"> lhadley</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

If the UserName attribute is not found, SuccessFactors looks for the NameID value. In the assertion, SuccessFactors expects something like the following:

```
<Subject><NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">lhadley</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
InResponseTo="_f6e21384-e33b-4a5f-a532-e58ce3f0a5e2" NotOnOrAfter="2014-10-
21T16:30:56.599Z"
```

```
Recipient="https://performancemanager4.successfactors.com/saml2/SAMLAssertionConsumer?
company=TestCompany"/></SubjectConfirmation></Subject>
```

Notice that in addition to NameID, there is nameid-format:unspecified. SuccessFactors expects a nameid-format. Typically, you send the value unspecified. SuccessFactors accepts other common values like persistent or transient. However, there is no support for these other options. Irrespective of the nameid-format sent, SuccessFactors simply compares the NameID from the login to the username in the application. The only exception is the UserName attribute that is sent. In that case, the NameID is ignored entirely.

Certificates and Signatures

SuccessFactors expects the SAML logins to be signed by your certificate. The signature can be on the response, assertion, or both. To verify the signature, you need to provide SuccessFactors with your X509 signing certificate. SuccessFactors accepts both CA and self-signed certificates.

SuccessFactors provides an X.509 certificate for you to encrypt assertion elements if desired. The same certificate is used to sign SP-initiated logout requests.

If you use SP-initiated logins, SuccessFactors provides the X.509 certificate used to sign the SAML login requests.

IP Address Restrictions

SuccessFactors allows you to restrict logins to specific IP addresses or ranges. This feature does not require SSO. However, it applies to SSO logins if SSO is enabled.

Information Exchanged to Set Up SAML2

SuccessFactors supplies you with a setup sheet containing the values that you need and requesting the values that SuccessFactors needs. SuccessFactors can also provide and receive metadata files. SuccessFactors does not provide an automated exchange of metadata files.

SuccessFactors provides:

- X.509 certificate that you can use to encrypt assertion values
- SuccessFactors entity ID values

  The SuccessFactors entity ID is unique for each SuccessFactors customer instance.
- Assertion consumer service URL

  This URL is unique for each SuccessFactors customer instance.
- Global logout response handler URL

  This URL is unique for each SuccessFactors customer instance.

You provide:

- X.509 certificate used to sign the response or assertion
- SAML issuer or IdP entity ID
- If you are using IdP-initiated logout, SuccessFactors needs your global logout service URL
- If you are enabling IP address restrictions, SuccessFactors needs the list of IPs
- If you are using the SuccessFactors redirect pages (highly recommended), SuccessFactors needs the URL for each

Timestamps and Server Synchronization

SAML2 requires you to send and SuccessFactors to respect NotBefore and NotAfter values that define when a login is valid. These values are always sent in GMT/UTC. SuccessFactors syncs server time to public time servers

on a regular basis. You are expected to do the same. However, there still may be slight variances in the clocks. SuccessFactors asks you to allow a small window of NotBefore time to prevent login failures if server time gets slightly out of sync.

RelayState

If you use IdP-initiated logins, you can specify a RelayState value to deep link your users to a specific page in the application. RelayState is optional. SuccessFactors can provide a list of valid RelayState values. If the deep link value has been populated with your URL, and a user tries to deep link into the application, they go to the destination they expect rather than the RelayState. If SP-initiated logins are enabled, you send SuccessFactors a dynamic value in the RelayState. This takes precedence over the non SP deep link process.

4.1 Example of Typical Login Response (Decoded)

SuccessFactors accepts a wide variety of formats and values in the SAML2 response. The following is a typical example. Your provided responses may differ.

```
<samlp:Response ID="gf8b65pFRW3JOvrV9z8_fjCJJtO"
       IssueInstant="2009-02-09T11:52:09.484Z" Version="2.0"
       xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
       <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
idp1.test.org</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="#gf8b65pFRW3JOvrV9z8_fjCJJtO">
                            <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#">
                                          <ec:InclusiveNamespaces PrefixList="ds saml
samlp xs xsi"

       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" />
```

```
                        <ds:DigestValue>8crrNj4pAptpLQKlAzbsS37tfOI=
                        </ds:DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>

      bdmIryj5+K9tGsK7sO89j0UwBNQDRee8XpF/aDY61ERrazaIC1NFwfXN6ETdz61gU5EKY5tJkaHR

      YjYTTr8NG1JwSj8JCGePoabuh3KbjgNuE21nQ8JY0TcttPZGMysD4NOzkLIGOTKARp2BUVx7COJC
                  egN9yX+SNphxlWD2vMQ=</ds:SignatureValue>
      </ds:Signature>
      <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" />
      </samlp:Status>
      <saml:Assertion ID="xv5BP-.Sl_aNbpsNwMX259HTgxL"
            IssueInstant="2009-02-09T11:52:09.500Z" Version="2.0"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">idp1.test.org
            </saml:Issuer>
            <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified"
                        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
lhadley</saml:NameID>
                  <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
                        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <saml:SubjectConfirmationData
                              InResponseTo="_F499B815F2BA7AB15F1207741929643"
NotOnOrAfter="2010-04-09T11:57:09.515Z"
                              Recipient="
https://performancemanager.successfactors.com /saml2/SAMLAssertionConsumer" />
                  </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2009-02-09T11:47:09.500Z"
                  NotOnOrAfter="2009-12-09T11:57:09.500Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:AudienceRestriction
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <saml:Audience>https://www.successfactors.com
```

```
                        </saml:Audience>
                    </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant="2009-02-09T11:52:09.500Z"
                    SessionIndex="xv5BP-.Sl_aNbpsNwMX259HTgxL"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                    <saml:AuthnContext
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <saml:AuthnContextClassRef>
                            urn:oasis:names:tc:SAML:2.0:ac:classes:Password
                        </saml:AuthnContextClassRef>
                    </saml:AuthnContext>
                </saml:AuthnStatement>
                <saml:AttributeStatement
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema">
                    <saml:Attribute Name="password"
                        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"
                        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <saml:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                            xsi:type="xs:string"> lhadley</saml:AttributeValue>
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
</samlp:Response>
```

www.sap.com/contactsap

Material Number: