INTERNAL PARTNERS AND CUSTOMERS

SAP SuccessFactors Suite: Identity and Access Management
An overview of Single Sign-On in SuccessFactors for addressing the needs of two main user groups:

1) Employees and White-Collar workers
2) Contractors, Externals and Blue-Collar Workers

SuccessFactors Customers: IT and HR professionals;
SuccessFactors Implementation Partners: Consultants, solution architects and project managers

The recommendations in this document are based on the functionality available up to SuccessFactors release mentioned above. Future functionality can impact recommendations provided by this document. We strive to keep these recommendations up-to-date, however, in case you find that recent new functionality have not yet been considered in the latest version of this document, please reach out to your Customer Success Manager / Partner Delivery Manager or send an email to: SAPSuccessFactorsIDPDoc@sap.com.

Implementation Design Principles (IDPs) are delivered by SAP for helping customers and implementation partners on how to choose the most appropriate strategy and solution architecture for SuccessFactors implementations. IDPs are compiled taking into consideration experience of past implementation projects and addressing frequent business requirements as well as real-life implementation challenges. They are intended to be in line with today's and tomorrow's product capabilities considering scalability and operational requirements and are continuously reviewed and updated as product functionality evolves.
# TABLE OF CONTENTS

1. TERMINOLOGY .................................................................................................................. 4
2. ABSTRACT............................................................................................................................... 5
3. INTRODUCTION AND PROBLEM STATEMENT .................................................................. 5
4. SOLUTION DESIGN APPROACH .......................................................................................... 5
   4.1 Overview of Authentication and Authorization Tools .................................................... 5
   4.2 Overview of Single Sign-On Setup .............................................................................. 6
   4.3 SuccessFactors Using SAP Identity Authentication Service as IdP ............................ 6
   4.4 Support for Multiple IdPs ......................................................................................... 6
   4.5 SuccessFactors as IdP ............................................................................................... 7
   4.6 Single Sign-on for Mashups ..................................................................................... 7
   4.7 Single Sign-on for Custom Navigation Links ........................................................... 8
5. DETAILED SOLUTION ......................................................................................................... 8
   5.1 SuccessFactors with a Single Identity Provider ........................................................... 8
   5.3 Identity Authentication Service (IAS) ........................................................................ 8
      5.3.1 Centralized place to manage user accounts ......................................................... 8
      5.3.2 Proxy IdP and conditional authentication to support multiple IdPs ................. 9
      5.3.3 Self-registration features for user accounts ...................................................... 10
      5.3.4 Usage of Identity Provisioning Service with SuccessFactors .......................... 11
   5.5 SCP Identity Authentication Service as default IdP for SuccessFactors .................... 11
   5.6 Limitations of IAS ...................................................................................................... 12
   5.7 Impact on Existing Customers .................................................................................. 12
6. REFERENCES ......................................................................................................................... 14
1. TERMINOLOGY

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>Employee Central</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>SAML 2.0</td>
<td>Common protocol for SuccessFactors SSO cases</td>
</tr>
<tr>
<td>IAS</td>
<td>Identity Authentication Service</td>
</tr>
<tr>
<td>IPS</td>
<td>Identity Provisioning Service</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>IDP</td>
<td>Implementation Design Principle</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SCP</td>
<td>SAP Cloud Platform</td>
</tr>
<tr>
<td>MSAD</td>
<td>Microsoft Active Directory</td>
</tr>
</tbody>
</table>

www.sap.com/contactsap
2. ABSTRACT
This document describes enablement of secure user access using single sign-on for customers with a landscape consisting of SuccessFactors in the cloud, on-premise consisting of SAP applications, SCP extensions, as well as other third-party applications. It also explains some of the single sign on scenarios involving internal employees as well as externals/contractors, besides explaining the upcoming features and updates regarding IAS on SuccessFactors.

3. INTRODUCTION AND PROBLEM STATEMENT
Single-sign on enables users to access multiple independent applications including SuccessFactors and other applications with one set of login credentials. Single sign-on must be thoughtfully planned out with consideration to the two main user groups. The first user group consists of employees and white-collar workers which makes up the general single-sign on scenario for logging in users into SuccessFactors. This user group receive their authenticated access with the credentials stored in a company’s corporate identity provider. The second user group includes contractors, externals and blue-collar workers who may not be suited to the general single-sign on scenario because of various reasons. For instance, company policy might dictate that employees need to access SuccessFactors but are not allowed to have their data stored in the company’s corporate IdP. It could also be that blue-collar workers might require a special approach because they do not have e-mail address and work in remote off-site areas with little or no internet connection. Identity & Access Management that IAS can provide is independent of the scenario above, therefore, it can provide SSO even for customer who does not has any existing (corporate) IdP

In addition to this, there are several cases where customers require multiple IdPs authenticating users from the same SuccessFactors instance. Examples include having employees on a separate IdP than contractors OR having acquired companies which still use the existing IdPs. This document explains how to setup for such a scenario.

4. SOLUTION DESIGN APPROACH
The solution outlined here explains single sign-on in SuccessFactors to raise awareness about the various possible approaches. One of the key and prominent architectural change from SSO perspective is the introduction of IAS as the default IdP for SuccessFactors. Refer the below sections for more details.

4.1 Overview of Authentication and Authorization Tools
The authentication and authorization of the Service Provider (SP) and Identity Provider (IdP) as part of single sign-on is an integral piece in any HRIS project. During single sign-on, user information is exchanged between the identity provider and service provider. The information is used to authenticate users to the different applications that they are authorized to access.

The following table describes the authentication and authorization tools that can be used with SuccessFactors:

<table>
<thead>
<tr>
<th>Name of Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuccessFactors Single Sign on</td>
<td>Single sign-on setup can be done in provisioning to enable SSO with an external IdP to access SuccessFactors. SuccessFactors can also act as an IdP to authenticate users to access certain applications.</td>
</tr>
<tr>
<td>SAP Cloud Platform Identity Authentication Service (IAS)</td>
<td>Cloud solution for identity lifecycle management that provides features for authentication, single sign-on and on-premise integration as well as self-services such as registration or password reset for employees, customers, partners, and consumers.</td>
</tr>
<tr>
<td>SAP Cloud Platform Identity Provisioning Service (IPS)</td>
<td>SAP’s solution for identity lifecycle management in the cloud to automatically set up user accounts and authorizations by re-using existing on-premise and cloud user stores.</td>
</tr>
</tbody>
</table>
SAP Netweaver Single Sign-On | An on-premise single sign-on tool that can also support SAP and non-SAP landscapes for cloud and on-premise applications.
---|---
SAP Identity Management | An on-premise tool for administering user identities and their authorizations to provision users to SAP and non-SAP systems. SAP Identity Management can use information from SAP HCM systems and even SuccessFactors for provisioning to applications in the landscape.

4.2 Overview of Single Sign-On Setup
SuccessFactors SSO can be configured for IdP initiated and SP-initiated SSO. For details on a scenario with multiple identity providers please refer to section 4.4. In addition, the recommended method is to use SAML 2.0 when setting up SSO with an IdP.
SuccessFactors SSO can be setup with an identity provider such as Active Directory, Google Platform, Okta, and Centrify, to authenticate users accessing SuccessFactors. This can be done with SuccessFactors provisioning access, which can only be performed by certified SuccessFactors implementation partners or SAP support. The SSO setup of the connection between an IdP and SuccessFactors requires an exchange of metadata between the two systems. SuccessFactors inputs the certificate from the IdP into provisioning by adding the IdP as an asserting party. For more details on the setup of SSO, refer to the SAP guide, “SuccessFactors SAML2 Single Sign-On” as referenced in section 6.

Both the IdP-initiated and SP-initiated SSO are supported by SuccessFactors. The IdP-initiated SSO is when access starts from the user selecting a predefined IdP link to initiate the SSO process. On the other hand, the SP-initiated SSO refers to when access starts from an attempt by the user to log in to the service provider, in this case SuccessFactors.

Once SSO with an IdP is configured, customers can then proceed to additional steps such as full or partial SSO, as well as considering mobile SSO. If a partial SSO is enabled in provisioning, then employees should have their login method specified usually through the Employee Import process whether they should login through SSO or username/password. Once SSO with an IdP is configured and the site of the IdP is exposed to the general internet, mobile SSO can also be used for accessing the SuccessFactors mobile application.

4.3 SuccessFactors Using SAP Identity Authentication Service as IdP
As mentioned earlier, Identity Authentication Service is a SAP cloud solution for identity lifecycle management that provides features for authentication, single sign-on and on-premise integration, as well as self-services such as registration or password reset for employees, customer partners, and consumers. It uses identity federation based on the SAML2.0 protocol for single sign-on with risk-based authentication, as well as authentication with social media credentials.

There are several ways you can connect IAS within the existing corporate SSO environment, such as delegated or proxy identity provider, integration with corporate user store or Kerberos based authentication. Refer SAP Help for more detailed information.

There are two ways SAP IAS can be setup as an IdP for SuccessFactors:
1. One way is to set up IAS as any other SAML asserting party from SuccessFactors provisioning.
2. Recommended way is to setup IAS as the default asserting party. Once the setup is complete, then the rest of the settings are made from SuccessFactors Admin Center. Refer the section below for more details.

4.4 Support for Multiple IdPs
With SAP IAS, it is possible to support multiple corporate IdPs for SuccessFactors, allowing SP initiated SSO. With conditional authentication feature in IAS can be used to direct login request to appropriate IdP.
SAP highly recommends to setup SAP IAS for SuccessFactors, for any customer who wants to use SP initiated SSO with multiple corporate IdPs. In the interim while customers implement IAS, the excerpt below explains a workaround for customers who cannot wait until the implementation is completed.

Workaround: SP initiated SSO for multiple IdPs
SuccessFactors Single Sign On supports multiple identity providers by adding each of them as asserting parties. It was always a challenge to manage multiple asserting parties for SuccessFactors because multiple asserting parties is supported only with IdP initiated SSO and not SP initiated SSO.

SP-initiated SSO with multiple asserting parties is not supported. Though by using deep linking feature provided under SuccessFactors provisioning, user experience similar to that the SP-initiated SSO can be offered, though this is always a workaround. This deep linking is set up with the “Deeplink IdP Login redirect URL” option in SuccessFactors provisioning as shown in the image below:

When users attempt to access a SuccessFactors instance configured to be authenticated with multiple asserting parties, then they will be redirected to a page to select the appropriate IdP. An example landing page to select an appropriate IdP with two separate IdPs against a single instance of SuccessFactors is shown below:

![SSO Redirect Landing Page](image)

Once the user has successfully logged in with the chosen asserting party, the decision is stored as a browser cookie so that the user does not have to go through the selection of the asserting party again. The base URL of a SuccessFactors instance varies depending on the data center and whether the instance is a production or test environment. After the base URL, add a deeplink to the initial URL such as those listed in the “SuccessFactors Deep links” guide.

4.5 SuccessFactors as IdP
SuccessFactors itself can act as an identity provider. Various use cases are applicable for having SuccessFactors itself act as an IdP:

- Accessing SAP Cloud Platform extension applications. This scenario is applicable as well to enable users to access a third-party provider such as a document management system, analytics solution, benefit provider, etc.
- Mashups within SuccessFactors can also use it as an IdP. Please refer section 4.6.

Customers currently use SuccessFactors provisioning to perform these settings. When IAS is bundled with SuccessFactors as default IdP, then it is recommended to use IAS as the the IdP for the scenarios mentioned above.

4.6 Single Sign-on for Mashups
As part of a hybrid landscape, some functions may continue to operate in the SAP on-premise solution alongside SuccessFactors. A mashup can use data from SAP on-premise and embed a page directly on the SuccessFactors screen. For example: SuccessFactors can also act as the identity provider to display the mashups such as pay statement and infotype screens from on-premise SAP payroll system, within SuccessFactors Employee Central. Please note that SuccessFactors should be used as identity provider only
for relevant applications and not all for all applications in SAP ERP. For example: users may be re-directed to SuccessFactors authentication only for mashups or pay slips but not for any non-HR transactions such as purchase orders or sales orders.

4.7 Single Sign-on for Custom Navigation Links

Custom navigation links can be placed within various places in SuccessFactors for accessing various third-party applications as well as the SAP on-premise solution. A user can navigate to these third-party tools or within SuccessFactors itself through adding custom links to various locations in the SuccessFactors suite. It is possible to add URL tokens to the custom link with the properties of the user such as the user ID, person ID, locale, etc and thereby bringing the properties of the user when navigating to the custom link.

5. DETAILED SOLUTION

Section 4 described the various use cases for single sign-on that provides background as to how these aforementioned approaches can be applied to address the needs of the end users in the system landscape. This section covers the possible solutions in more detail to authenticate and authorize users to access SuccessFactors for end users.

5.1 SuccessFactors with a Single Identity Provider

In the general use case for employees and white-collar workers, the minimum setup involves those that use single corporate identity provider as the authenticating authority. This can be done with the basic configuration outlined in section 4.2. Refer SAP Help for detailed implementation steps.

Externals, contractors, and blue-collar workers may reside in the same identity provider as employees and white-collar workers. However, additional authentication rules may be in place for these externals, contracts and blue-collar workers such as two-factor authentication.

5.3 Identity Authentication Service (IAS)

This section intends to describe the advantages and capabilities of IAS.

IAS can be used as the main IdP for employees and white-collar workers, but it is also a solution worthwhile to consider for contractors, external and blue-collar workers. These types of workers may not be suited to the general single-sign on scenario that was mentioned earlier for employees and white-collar workers.

IAS can be considered as a solution in the following cases:

- **Contractors**
  - Company policy might not allow data of contractors to be stored in the main identity provider and they are not allowed to access SuccessFactors. IAS can be a solution to store the user profiles of contractors. IAS tenant admins can view the data of all user accounts stored in IAS.

- **Externals**
  - Externals may include candidates that need to access a career portal that is not SuccessFactors. To provision externals users quickly to access the applications they need, IAS can provide self-service capabilities for users to register for their own access credentials.

- **Blue-collar workers**
  - Blue-collar workers do not have e-mail accounts and have no regular access to a desktop. In addition, they work in off-site work areas. IAS provides the ability for risk-based authentication allowing those not using corporate devices to access securely.

The following sections outline some of the main features of IAS.

5.3.1 Centralized place to manage user accounts

A useful feature of the identity authentication service is the ability to manage user accounts from multiple source and target systems such as SuccessFactors in one consolidated place. The ability to view data of all user accounts in a one-stop-shop solution is a useful feature in the case of heterogeneous landscapes with
various identity providers whereby user account data is stored in various places. A tenant administrator can use a CSV file to import new users, update existing ones, as well as export a CSV file with data of all users on IAS. **Addtionally IPS can also be used to provision users from SuccessFactors to IAS.** Users who are imported into IAS have user profiles without passwords but can receive an email on how to activate their accounts, or a default password can be set for these users. Depending on the authentication rules that have been setup for each of the applications, users can log in to the applications that are connected to the IAS tenant.

### 5.3.2 Proxy IdP and conditional authentication to support multiple IdPs

Multiple IdPs are also supported using SAP Cloud Platform Identity Authentication Service with its ability to act as a proxy IdP. Initially IAS is set as the default local identity provider, but if another identity provider is specified as the default, then IAS acts as a proxy IdP. Here, the “Conditional Authentication” feature can be used to select a default identity provider for an application. With conditional authentication, it is possible to require users trying to access a certain application to authenticate via a selected authentication identity provider. In the image below, any user trying to access SuccessFactors will be authenticated via IAS. The IdP can be selected for each of the applications connected to the IAS tenant.

Another advantage of the conditional authentication feature is the ability to set risk-based authentication rules for users that meet a certain. In the example below, IAS is the default authentication IdP for any user in the user trying to authenticate to SuccessFactors. The example below also shows that a risk-based authentication rule has been applied to users in the “BlueCollarWorkers” group who have actually been assigned automatically through the Identity Provisioning Service (IPS) as described in more detail in section 5.3.4. User groups can also be assigned through the CSV file or manually on the IAS administration console. A risk-based authentication rule is applied for any user in the “BlueCollarWorkers” group below that have the domain name “noemail.com” and falls under the category of any type of user. In the example of the risk-based authentication rule below, it requires two-factor authentication access using the SAP Authenticator application for users that meet these criteria.

![Conditional Authentication Example](image-url)
Once a user accesses his/her user profile for the first time, it is possible now to activate the SAP Authenticator Mobile Application for two-factor authentication. The SAP Authenticator application must be installed in the mobile device and can be downloaded from the mobile device's application store. On the user profile, a QR code as shown in the image below can be scanned by the application.

With two-factor authentication, users who meet the risk-based authentication rule's criteria can be redirected to the IAS user profile login page when attempting to access SuccessFactors. As a second factor authentication, the user is prompted for their passcode from the SAP Authenticator application. A new passcode is also generated by the application every 60 seconds. The Mobile SSO capabilities are also supported with the SAP Authentication application to enable users to stay logged in on mobile devices by selecting the “Remember Me” checkbox.

![QR Code Scanning](image1.png)

5.3.3 Self-registration features for user accounts

Another feature worth mentioning is the self-registration capabilities of IAS. If self-registration is enabled, a user can sign up for an account when trying to attempt to log in to a particular application. The user types available for the risk-based authentication rule is consumer, partner, or employee. These self-registration features may be more applicable in the case of consumers and partners wherein such users are allowed to register to access only certain applications. A specific group can be created with a risk-based authentication rule assigned that contains these external users.

![Self-Registration Features](image2.png)
5.3.4 Usage of Identity Provisioning Service with SuccessFactors

The SAP Identity Provisioning Service (IPS) is SAP’s solution is a lifecycle management cloud solution that provisions users to access various applications across the enterprise landscape. This section discusses how IPS can be used in the particular case of blue-collar workers, but the items mentioned here could also be helpful in the cases of covering other generic use cases such as employees and white-collar workers. For this use case, SuccessFactors and IAS were set up as the source and target system respectively. SuccessFactors as a source system manages the user identities, whereas, IAS as the target systems receives the user information to provide the necessary authorizations.

The process of provisioning the blue-collar worker starts when the user is hired in SuccessFactors, in which then the provisioning job in IPS runs to obtain the data from SuccessFactors. Once users have their profiles created in IAS, they can access their IAS user profile to activate the SAP Authenticator mobile application. Here, IAS must be set as the master of passwords in the JSON transformation so that blue-collar workers can access their user profiles with their IAS password. For the initial activation of access to IAS, internet connection is required, so the customer would need to setup mobile kiosks by the work location, or the blue-collar worker would need to go to an internet café when they are off duty.

Customers can use IPS with IAS as a way for blue-collar workers need to be able to access the SuccessFactors without an email using non-managed devices. Customers may not want to create usernames and emails for their blue-collar workers on the IdP because it would not be financially worthwhile to do so given that these workers do not have access to internet in their remote locations.

While IPS can cover use cases other than blue-collar workers, this specific use case is discussed to explain the benefits of using IPS. When the tenant admin then runs a provisioning job on demand or schedules an automated job, user data between the source system, SuccessFactors, and target system, IAS is synced. The main setup of IPS involved JSON transformations that maps the target and source system where IPS access the SuccessFactors User entity. The JSON transformation codes were setup to do the following:

- Create a dummy email for each blue-collar worker with no email in SuccessFactors since email is a required attribute by IAS. The final result of the dummy email was 10001234no_email@noemail.com wherein “10001234” is the user ID while “no_email” is a value obtained from the email field which is a default value for users with no email.
- Map organizational information such as cost centre, department, and company using data from SF to IAS
- Provision users automatically to a group already available in IAS, called “BlueCollarWorkers” group when users do not have an email

Enable automatic activation and deactivation capabilities based on hire, promotion, and termination of user in SuccessFactors

5.5 SCP Identity Authentication Service as default IdP for SuccessFactors

Starting 1902, SAP started offering IAS as a default IdP for SuccessFactors as an opt-in feature. This is part of the overall goal is to connect all SAP applications to IAS and IAS to act as an identity hub and either authenticate users locally or federate to a corporate IdP. This was a remarkable improvement which provided several advantages which are provided in the standard help guide. Few additional key benefits are listed below:

- Customers always had to resort to work-around for SP initiated SSO whenever there were multiple asserting parties assigned to a single SuccessFactors instance. Refer section 4.4. With IAS as IdP, no such workaround is required anymore.
- Additional data model changes and steps were required to manage partial SSO and even the URL required to logon were different for such users. None of these are required when IAS is used as a default IdP. Customers were dependent on partners and consultants, as SSO setting were handled via SuccessFactors provisioning and with IAS as default IdP, all the SAML settings are now available from Admin Center.
5.6 Limitations of IAS

As of December 2019, SAP Cloud Platform Identity Authentication Service does not support Global Assignment and Concurrent Employment (GA/CE). Hence SAP Employee Central customers currently using these feature must not upgrade or use it. SAP Cloud Platform Identity Authentication Service still remains the strategic product direction hence we are currently looking into lifting this limitation. Please check out SAP Help Document Setting Up SuccessFactors with SAP Cloud Platform Identity Authentication Service for the latest status.

5.7 Impact on Existing Customers

There are no license costs for customers who opt to bundle IAS with SuccessFactors and this is one of the key cost benefit for customers who currently need to pay per login requests to SuccessFactors from IAS. Refer SAP Help for all the technical benefits of using SAP IAS as IDP.

Consider the scenario shown below, where a customer is using Microsoft Active Directory as IdP for SuccessFactors used to authenticate all the employees.

Existing SuccessFactors Setup without IAS

When SuccessFactors is bundled with IAS as default IdP, in that case, all the user records needs to be stored in IAS. Though with conditional authentication feature of IAS, it is always possible to setup IAS as a proxy which can forward the requests to MSAD to authenticate users. Revised architecture in such a case will look like as shown below:
Revised SuccessFactors Setup with IAS

The scenarios mentioned above is the most common scenario with customers. The existing architecture can be more complex, therefore the implementation time and effort can also increase marginally.

Some of the scenarios are explained below:

<table>
<thead>
<tr>
<th>Scenario for existing customer</th>
<th>Impact</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer is already using IAS as Corporate (authenticating) IdP</td>
<td>Minimum to Nil</td>
<td>In this case, there will not be any major effort. The existing IAS will be bundled with SuccessFactors as default IdP.</td>
</tr>
<tr>
<td>Customer is already using IAS as Corporate IdP but as a proxy (non-authenticating) IdP without any users</td>
<td>Minimum to Nil</td>
<td>In this case, there will not be any major effort. The existing IAS will be bundled with SuccessFactors as default IdP. In the conditional authentication, the IAS needs to be configured as a proxy IdP.</td>
</tr>
</tbody>
</table>
| Customer is already using IAS but only to authenticate subset of employees (for eg: externals are authenticated using IAS and internal employees are authenticated using MSAD) | Medium | This scenario is very similar to section 4.4 where existing customer is using multiple IdPs to authenticate different set of employees. In this case, after IAS is setup as default IdP, IAS conditional authentication configuration needs to be updated as follows:
  - Setup IAS as authenticating IdP for employees who needs to be authenticated using IAS.
  - Setup IAS as proxy IdP for employees who needs to be authenticated by other IdPs. |
| Customer is not using IAS today | Medium to High | This scenario is similar to example shown in the figure above. In this case customer needs to setup IAS as default IdP. The existing IdP needs to be re-configured to receive SAML requests from IAS than from SuccessFactors directly. Additionally IAS needs to be configured to authenticate users. |
It needs to be noted that in future customers will be able to setup IAS as default IdP using SuccessFactors upgrade center. Any additional costs for the implementation of IAS is not covered as part of the default setup.

6. REFERENCES

SAP KBA

2370144 - SSO: Multiple Asserting party for SAML IdP and SP-Initiated login methods

2253359 - How to enable Pay Statement service to view payslip in EmployeeCentral System?
https://launchpad.support.sap.com/#/notes/0002253359

2493928 – SuccessFactors Deep links guide

SAP Guides

SAP Cloud Platform Identity Authentication Service Q4 2018
SAP Cloud Platform Identity Platform Service Q4 2018
SuccessFactors SAML2 Single Sign-On Q4 2018