

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-successfactors-tutorial>  
Configuring and testing Azure AD single sign-on

# Tutorial: Azure Active Directory integration with SuccessFactors

1

2017-2-22 7 min to read Contributors 

The objective of this tutorial is to show you how to integrate SuccessFactors with Azure Active Directory (Azure AD).

Integrating SuccessFactors with Azure AD provides you with the following benefits:

- 1 You can control in Azure AD who has access to SuccessFactors
- 2 You can enable your users to automatically get signed-on to SuccessFactors (Single Sign-On) with their Azure AD accounts
- 3 You can manage your accounts in one central location - the Azure classic portal

4

If you want to know more details about SaaS app integration with

Azure AD, see [What is application access and single sign-on with Azure Active Directory](#).

## Prerequisites

To configure Azure AD integration with SuccessFactors, you need the following items:

- 1 A valid Azure subscription
- 2 A tenant in SuccessFactors
- 3

### Note

To test the steps in this tutorial, we do not recommend using a production environment.

To test the steps in this tutorial, you should follow these recommendations:

- 1 You should not use your production environment, unless this is necessary.
- 2 If you don't have an Azure AD trial environment, you can get a one-month trial [here](#).
- 3

## Scenario description

The objective of this tutorial is to enable you to test Azure AD single sign-on in a test environment.

The scenario outlined in this tutorial consists of two main building blocks:

- Adding SuccessFactors from the gallery
- Configuring and testing Azure AD single sign-on
-

# Adding SuccessFactors from the gallery

To configure the integration of SuccessFactors into Azure AD, you need to add SuccessFactors from the gallery to your list of managed SaaS apps.

**To add SuccessFactors from the gallery, perform the following steps:**

1 In the Azure classic portal, on the left navigation panel, click



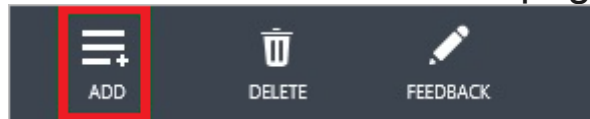
**Active Directory.**

2 From the **Directory** list, select the directory for which you want to enable directory integration.

3 To open the applications view, in the directory view, click **Applications** in the top menu.



4 Click **Add** at the bottom of the page.



5 On the **What do you want to do** dialog, click **Add an application from the gallery.**



6 In the **search box**, type **SuccessFactors**.

Add an application for my organization to use

7 In the results panel, select **SuccessFactors**, and then click



**Complete** to add the application.

8

## Configuring and testing Azure AD single sign-on

The objective of this section is to show you how to configure and test Azure AD single sign-on with SuccessFactors based on a test user called "Britta Simon".

For single sign-on to work, Azure AD needs to know what the counterpart user in SuccessFactors to an user in Azure AD is. In other words, a link relationship between an Azure AD user and the related user in SuccessFactors needs to be established.

This link relationship is established by assigning the value of the **user name** in Azure AD as the value of the **Username** in SuccessFactors.

To configure and test Azure AD single sign-on with SuccessFactors, you need to complete the following building blocks:

- 1 **Configuring Azure AD Single Sign-On** - to enable your users to use this feature.
- 2 **Creating an Azure AD test user** - to test Azure AD single sign-on with Britta Simon.
- 3 **Creating a SuccessFactors test user** - to have a counterpart

of Britta Simon in SuccessFactors that is linked to the Azure AD representation of her.

4 **Assigning the Azure AD test user** - to enable Britta Simon to use Azure AD single sign-on.

5 **Testing Single Sign-On** - to verify whether the configuration works.

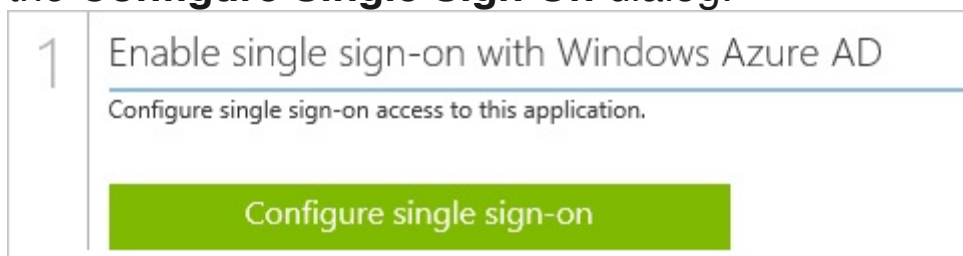
6

## Configuring Azure AD single sign-on

In this section, you enable Azure AD single sign-on in the classic portal and configure single sign-on in your SuccessFactors application.

**To configure Azure AD single sign-on with SuccessFactors, perform the following steps:**

1 In the Azure classic portal, on the **SuccessFactors** application integration page, click **Configure single sign-on** to open the **Configure Single Sign On** dialog.



2 On the **How would you like users to sign on to SuccessFactors** page, select **Microsoft Azure AD Single Sign-On**, and then click **Next**.

## CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to SuccessFactors

☒ **Microsoft Azure AD Single Sign-On**

Establish federation between Microsoft Azure AD and SuccessFactors

[Learn more](#)

☐ **Password Single Sign-On**

Microsoft Azure AD stores account credentials for users to sign on to SuccessFactors

[Learn more](#)

☐ **Existing Single Sign-On**

Configures Microsoft Azure AD to support single sign-on to SuccessFactors using Active Directory Federation Services or another third-party single sign-on provider.

[Learn more](#)

3 On the **Configure App URL** page, perform the following steps, and then click **Next**.

CONFIGURE SINGLE SIGN-ON

## Configure App Settings

Enter the settings of SuccessFactors application below. [Learn more](#)

**SIGN ON URL** ?

**https://Contoso.successfactors.com/sf/home?com**

Example: https://EXAMPLE.successfactors.com/EXAMPLE,  
https://EXAMPLE.sapsf.com/EXAMPLE,  
https://EXAMPLE.successfactors.eu/EXAMPLE,  
https://EXAMPLE.sapsf.eu

**REPLY URL** ?

**https://Contoso.successfactors.com/saml2/SAMLA**

Example: https://EXAMPLE.successfactors.com/EXAMPLE,  
https://EXAMPLE.sapsf.com/EXAMPLE,  
https://EXAMPLE.successfactors.eu/EXAMPLE,  
https://EXAMPLE.sapsf.eu,https://EXAMPLE.sapsf.eu/EXAMPLE

☐ Show advanced settings (optional).

☐ Configure the certificate used for federated single sign-on (optional).

a. In the **Sign**

**On URL** textbox, type a URL using one of the following patterns:

4

5 https://<company name>.successfactors.com/<company name>

6 https://<company name>.sapsf.com/<company name>

7 https://<company name>.successfactors.eu/<company name>

8 https://<company name>.sapsf.eu

9 b. In the **Reply URL** textbox, type a URL using one of the following patterns:

10

11 https://<company name>.successfactors.com/<company name>

12 https://<company name>.sapsf.com/<company name>

13 https://<company name>.successfactors.eu/<company name>

14 https://<company name>.sapsf.eu

15 https://<company name>.sapsf.eu/<company name>

- 16 c. Click **Next**. **Note** Please note that these are not the real values. You have to update these values with the actual Sign On URL and Reply URL. To get these values, contact [SuccessFactors support team](#).
- 17 On the **Configure single sign-on at SuccessFactors** page, click **Download certificate**, and then save the certificate file locally on your computer.

## CONFIGURE SINGLE SIGN-ON

# Configure single sign-on at SuccessFactors

SuccessFactors requires configuration to enable federated single sign-on. Follow the steps below to perform this configuration.

- The following certificate will be used for federated single sign-on:  
Thumbprint: B080C...  
Expiry: ...  
[Download certificate](#)
- Configure the certificate and values in SuccessFactors, following the instructions linked below.  
[View SuccessFactors configuration instructions](#)

ISSUER URL

REMOTE LOGIN URL

REMOTE LOGOUT URL

☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate for this application.

Companies

Company Details

New Company

Clone Company

Reports

Operations/Maintenance

SMB

Manage Provisioners

SuccessStore

Upgrade Center Media Content

up to Company Listing

AZQuartzTest

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Others show all...

Single Sign On Features

Token-based login is Off.

Reset Token :

☐ Show Token

Token is required for all SSO

**Note** This value is just used as the on/off switch. If any value is saved, the SAML SSO is ON. If a blank value is saved the SAML SSO is OFF.

- 21 Native to below screenshot and perform the following actions.



**Generated/SP/RP).g. Select Browser/Post Profile as SAML Profile.h. Select No as Enforce Certificate Valid Period.i. Copy the content of the downloaded certificate file, and then paste it into the SAML Verifying Certificate textbox.**  
**Note** The certificate content must have begin certificate and end certificate tags.

22 Navigate to SAML V2, and then perform the following steps:

<b>SAML v2 : SP-initiated logout</b>	
Support SP-initiated Global Logout	Yes ▾
SP sign LogoutRequest	No ▾
SP validate LogoutResponse	No ▾
Global Logout Service URL (LogoutRequest destination)	https://login.windows.net/b7sw34308-bf33-414f-9971-6egj7
<b>SAML V2 : IDP-initiated Global Logout</b>	
SP validate LogoutRequest signature	No ▾
SP sign LogoutResponse	No ▾
Global Logout Service URL (LogoutResponse destination)	
<b>SAML v2: Login Response with Http artifact binding</b>	
Artifact Resolution Service Location (supplied by idp):	
Require ArtifactResolve Signature (sp to idp)	No ▾
Require ArtifactResponse Signature (idp to sp)	No ▾
<b>SAML v2: NameID Setting</b>	
Require sp must encrypt all NameID elements	No ▾
NameID Format	unspecified ▾
<b>SAML v2 : SP-initiated login</b>	
Enable sp initiated login (AuthnRequest)	Yes ▾
Default issuer	<input checked="" type="checkbox"/>
single sign on redirect service location (to be provided by idp)	https://login.windows.net/b7sw34308-bf33-414f-9971-4
Send request as Company-Wide issuer	Yes ▾

a. Select **Yes** as **Support SP-initiated Global Logout**.b. In the **Global Logout Service URL (LogoutRequest destination)** textbox put the value of **Remote Logout URL** from Azure AD application configuration wizard.c. Select **No**

as **Require sp must encrypt all NameID element**.d. Select **unspecified** as **NameID Format**.e. Select **Yes** as **Enable sp initiated login (AuthnRequest)**.f. In the **Send request as Company-Wide issuer** textbox put the value of **Remote Login URL** from Azure AD application configuration wizard.

- 23 Perform these steps if you want to make the login usernames Case Insensitive, .a. Visit **Company Settings**(near the bottom).b. select checkbox near **Enable Non-Case-Sensitive Username**.c.Click **Save**.

Enable Non-Case-Sensitive Username ☐

**Note**If you try to enable this, the system checks if it will create a duplicate SAML login name. For example if the customer has usernames User1 and user1. Taking away case sensitivity makes these duplicates. The system will give you an error message and will not enable the feature. The customer will need to change one of the usernames so it's actually spelled different.

- 24 On the Azure classic portal, select the single sign-on configuration confirmation, and then click **Complete** to close the **Configure Single Sign On** dialog.



Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate for this application.

- 25 On the **Single sign-on confirmation** page, click **Complete**.

CONFIGURE SINGLE SIGN-ON

## Single sign-on confirmation

Congratulations! You have successfully configured federated single sign-on.

NOTIFICATION E-MAIL ?

admin@contoso.com

## Creating an Azure AD test user

The objective of this section is to create a test user in the classic portal called Britta Simon.

DASHBOARD   USERS   ATTRIBUTES   CONFIGURE			
DISPLAY NAME	USER NAME	...	ACCESS
Admin	admin@		No
Britta Simon	BrittaSimon@		No

**To create a test user in Azure AD, perform the following steps:**

1 In the **Azure classic Portal**, on the left navigation pane, click



**Active Directory.**

2 From the **Directory** list, select the directory for which you want to enable directory integration.

3 To display the list of users, in the menu on the top, click **Users**.



4 To open the **Add User** dialog, in the toolbar on the bottom, click



**Add User.**

5 On the **Tell us about this user** dialog page, perform the following steps:

ADD USER

Tell us about this user

TYPE OF USER

New user in your organization ▼

USER NAME ?

BrittaSimon @ [Domain] ▼

a.

- As Type Of User, select New user in your organization.  
 b. In the User Name **textbox**, type **BrittaSimon**.  
 c. Click **Next**.
- 6 On the **User Profile** dialog page, perform the following steps:

ADD USER

user profile

FIRST NAME LAST NAME

Britta Simon

DISPLAY NAME

Britta Simon

ROLE ?

User ▼

MULTI-FACTOR AUTHENTICATION ?

☐ Enable Multi-Factor Authentication

a.

- In the **First Name** textbox, type **Britta**. b. In the **Last Name** textbox, type, **Simon**.  
 c. In the **Display Name** textbox, type **Britta Simon**.  
 d. In the **Role** list, select **User**.  
 e. Click **Next**.
- 7 On the **Get temporary password** dialog page, click **create**.

ADD USER

## Get temporary password

The new user 'BrittaSimon@[REDACTED]' will be assigned a temporary password that must be changed on first sign in. To display the temporary password and to create the account, click Create.

**create**


8 On the **Get temporary password** dialog page, perform the following steps:

ADD USER

## Get temporary password

Successfully created user 'BrittaSimon@[REDACTED]' with the following new password

NEW PASSWORD

Coya7332 

SEND PASSWORD IN EMAIL

The password will be sent in clear text

Maximum of five email addresses separated by semi-colons.

a.

Write down the value of the **New Password**.b. Click **Complete**.

9

## Creating a SuccessFactors test user

In order to enable Azure AD users to log into SuccessFactors, they must be provisioned into SuccessFactors.

In the case of SuccessFactors, provisioning is a manual task.

To get users created in SuccessFactors, you need to contact the [SuccessFactors support team](#).

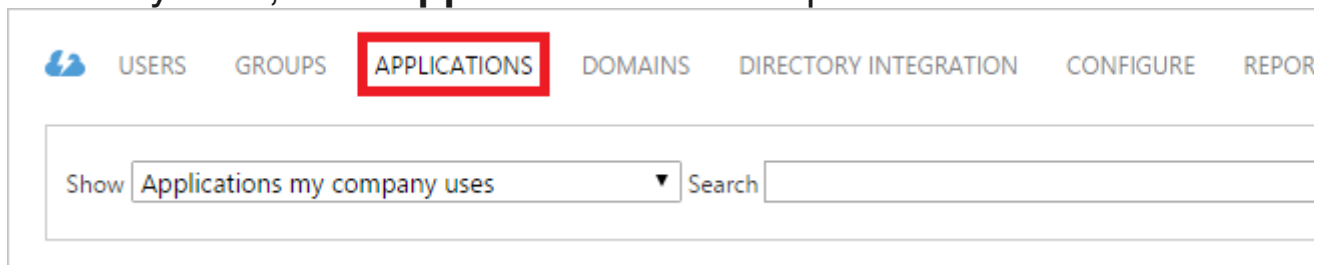
## Assigning the Azure AD test user

The objective of this section is to enabling Britta Simon to use Azure single sign-on by granting her access to SuccessFactors.

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT
Britta Simon	BrittaSimon@successfactors.com		

**To assign Britta Simon to SuccessFactors, perform the following steps:**

- 1 On the classic portal, to open the applications view, in the directory view, click **Applications** in the top menu.



- 2 In the applications list, select **SuccessFactors**.

NAME	PUBLISHER	TYPE
SuccessFactors	SuccessFactors, Inc. A SAP Company	Web application

- 3 In the menu on the top, click **Users**.



- 4 In the Users list, select **Britta Simon**.

- 5 In the toolbar on the bottom, click **Assign**.



6

## Testing single sign-on

The objective of this section is to test your Azure AD single sign-on configuration using the Access Panel.

When you click the SuccessFactors tile in the Access Panel, you should get automatically signed-on to your SuccessFactors application.

## Additional resources

- [List of Tutorials on How to Integrate SaaS Apps with Azure Active Directory](#)

[What is application access and single sign-on with Azure Active Directory?](#)