



5.8 Integrations

Bright Pattern Documentation

Generated: 8/09/2022 4:12 pm

Content is available under license unless otherwise noted.

Table of Contents

Table of Contents	2
Integrations Overview	3
Tutorials	3
AWS S3 Recordings Storage	3
Integration Account Configuration	3
Single Sign-On (SSO) Integration	3
Microsoft Azure Active Directory SSO Configuration	3
Prerequisites	4
Configuration in Azure Portal	4
Step 1: Add the Bright Pattern application from the Gallery	4
Step 2: Add owner and users	5
Step 3: Configure Azure AD SSO	6
Basic SAML Configuration	7
User Attributes & Claims	9
SAML Signing Certificate	10
Set up	11
Validate single sign-on	11
Errors and How to Fix Them	12
Application with identifier was not found	12
HTTP Error 404	13
Redirects to Microsoftonline with HTTP Error 404	14
Configuration in Bright Pattern	14
Step 1: In Bright Pattern, add SSO integration account	15
Step 2: Edit properties with your Azure AD app credentials	15
Properties	16

Integrations Overview

The tutorials in this section offer step-by-step instructions on how to configure integration accounts for your contact center. For more on integrations, see the *Contact Center Administrator Guide*, section [Integration Accounts](#).

Tutorials

AWS S3 Recordings Storage

- [How to Create and Configure an AWS S3 Bucket](#)
- [How to Add Amazon AWS Integration Account in Bright Pattern](#)
- [Setting up AWS S3 Storage for Call Recordings](#)
- [Setting up AWS S3 Storage for Screen Recordings](#)
- [Setting up AWS S3 Storage for Chat Transcripts](#)

Integration Account Configuration

- [How to Add an Integration Account](#)
- [LogMeIn Integration Quick Start](#)

Single Sign-On (SSO) Integration

- [How to Configure Microsoft Azure Active Directory SSO](#)

1. REDIRECT [5.3:Contact-center-administrator-guide/CallCenterConfiguration/IntegrationAccounts](#)

Microsoft Azure Active Directory SSO Configuration

Microsoft Azure Active Directory (AD) single sign-on (SSO) enables users to sign in just one time to applications in the Microsoft Azure AD in order to access integrated applications.

With Azure AD SSO, users can sign in with one account to launch applications from the Office 365 portal, Dynamics 365, or the Azure AD MyApps access panel. Moreover, administrators can control user account management, and automatically add or remove user access to applications based on group membership. Without SSO, users have to remember passwords and sign in to each application separately.

Bright Pattern supports Azure AD SSO using the SAML (Security Assertion Markup Language) SSO method, which works for applications that authenticate using a SAML protocol like SAML 2.0 or WS-Federation.

With SAML SSO, Azure AD authenticates to the application by using the user's Azure AD account. Azure AD communicates the credentials to the application through a connection protocol. With SAML-based SSO, you can map users to specific application roles based on rules defined in your SAML claims.

This article will show you how to configure Azure AD SSO for your organization.

You will learn how to:

- Create an enterprise application
- Assign owner, users, and user groups to the application

- Configure the application for SAML-based SSO
- Configure application-specific domain and URLs
- Configure user attributes
- Get a SAML signing certificate
- Validate settings
- Add an SSO integration account in Bright Pattern
- Use Azure AD credentials in integration account properties

Prerequisites

Before configuring Azure AD SSO, you will need the following:

- [Microsoft Office 365 account](#). If you are unable to log into Microsoft directly, please contact your Microsoft system administrator to review permission and access level settings.
- [Microsoft Azure account/subscription](#) (free trial OK). Without this, you will have no directory and will not be able to access any data in Azure AD.
- Bright Pattern Contact Center version 5.3 or later

Configuration in Azure Portal

This procedure generally follows Microsoft's tutorial, [Configure SAML-based single sign-on for an application with Azure Active Directory](#). For more information on SSO, see [Microsoft Azure documentation](#).

Step 1: Add the Bright Pattern application from the Gallery

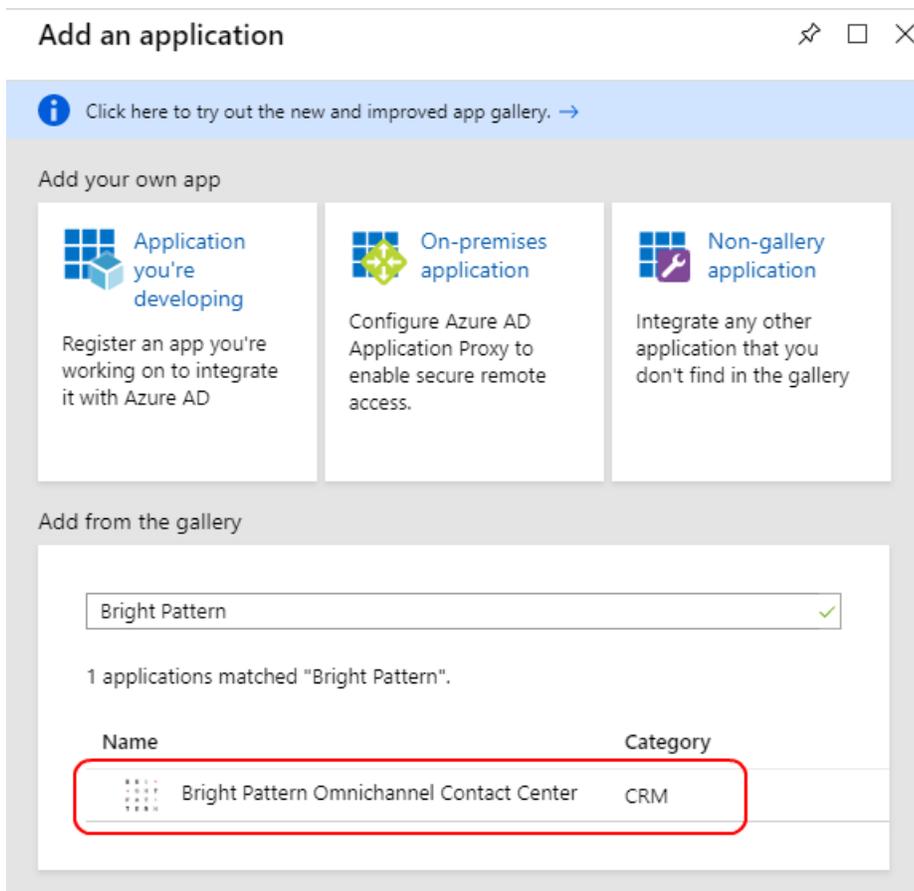
1. Sign in to the Microsoft Azure portal.
2. Go to *Azure Active Directory > Enterprise applications* and click **+ New application**.

The screenshot shows the Azure Portal interface for 'Enterprise applications - All applications'. At the top, there is a search bar and a breadcrumb trail: 'Home > Default Directory > Enterprise applications - All applications'. Below this, the page title is 'Enterprise applications - All applications' with a subtitle 'Default Directory - Azure Active Directory'. On the left, there is a navigation pane with sections: 'Overview' (containing 'Overview'), 'Manage' (containing 'All applications', 'Application proxy', 'User settings'), 'Security' (containing 'Conditional Access'), and 'Activity' (containing 'Sign-ins', 'Usage & insights'). The main content area has a '+ New application' button highlighted with a red box, and a 'Columns' button. Below these are three filters: 'Application Type' (set to 'Enterprise Applications'), 'Applications status' (set to 'Any'), and 'Application visibility' (set to 'Any'). A search box contains the text 'First 50 shown, to search all of your applications, enter a display name or the application ID.' Below the search box is a table with two columns: 'NAME' and 'HOMEPAGE URL'. The table lists several applications:

NAME	HOMEPAGE URL
Office 365 Exchange Online	http://office.microsoft.com/outlook/
Office 365 Management APIs	
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/
Outlook Groups	
SCCC	
Skype for Business Online	

Create new enterprise application

3. In the *Add from the gallery* section, type "Bright Pattern" in the search box.
4. Select **Bright Pattern Omnichannel Contact Center** from the results panel and then add the app.



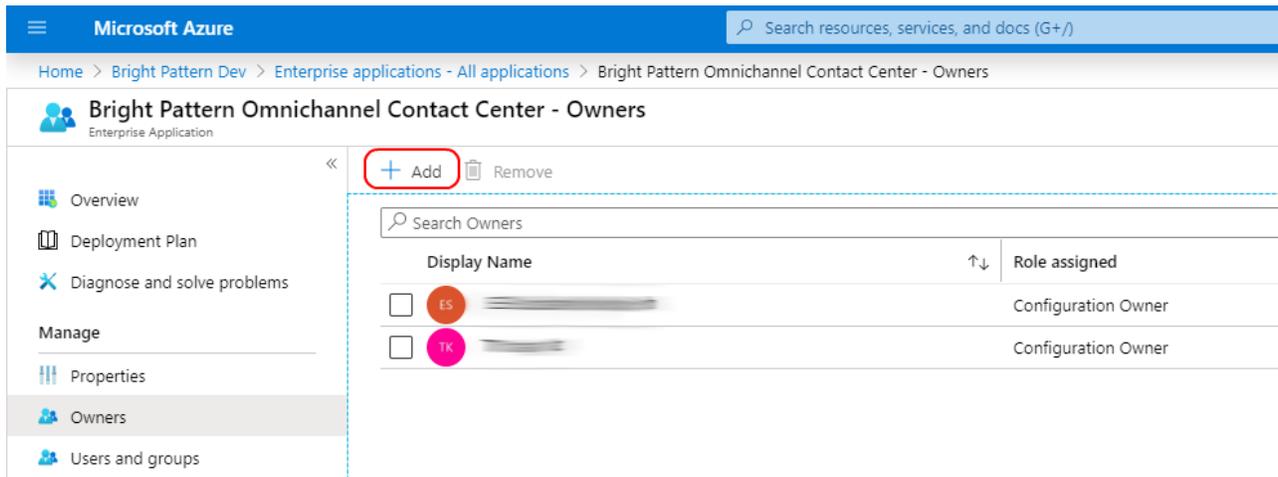
Application properties

Then you will see the overview page for the application.

Step 2: Add owner and users

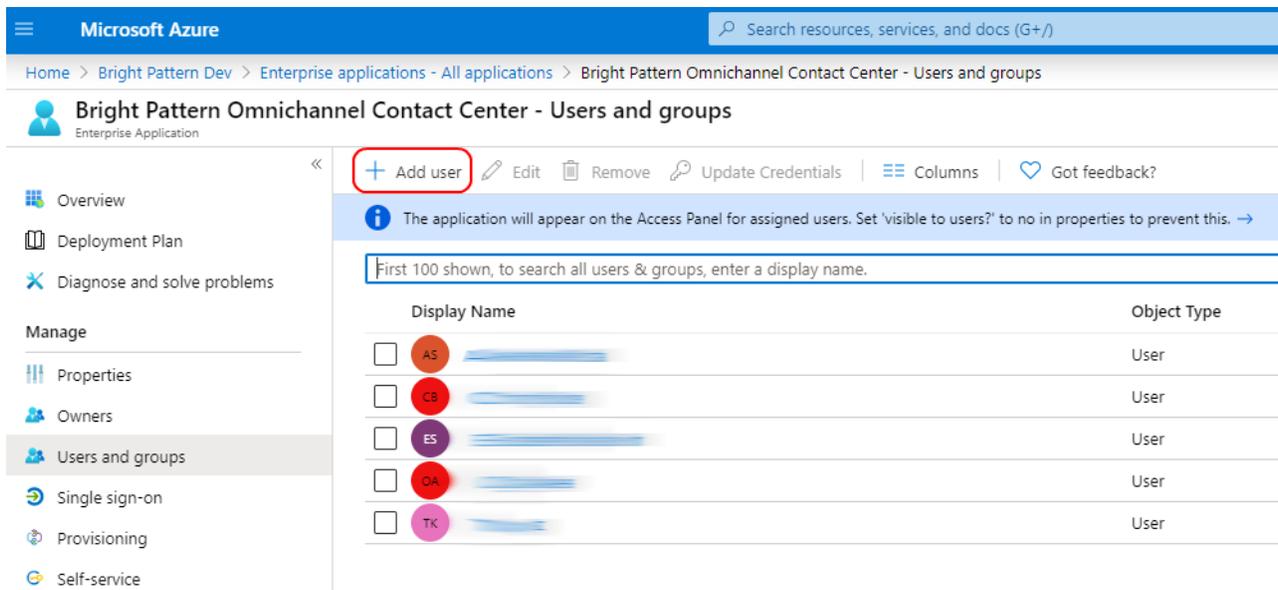
Adding yourself, the admin, as a user allows you to configure and test the Bright Pattern Omnichannel Contact Center application. Adding other users allows others to use it as well.

1. On the overview page for the application, go to *Manage > Owners* and then click **add**.



Add owners

- In *Select Owners*, add yourself as the owner of the application so that you can modify the application. Then click **Select**.
- Then go to *Manage > Users and groups* and click **Add user**.



Add users

- Click **Users and groups**, select the users with rights to use this application, and click **Assign**. Assigning allows the user to use Azure AD SSO.
- After you add the users, you can repeat these steps to add the group, if desired.

Step 3: Configure Azure AD SSO

- On the *Bright Pattern Omnichannel Contact Center* application integration page, go to *Manage > Single sign-on* and select **SAML** as the single sign-on method.
- The *Set up SSO with SAML Preview* page will open with the following boxes.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Bright Pattern Dev > Enterprise applications - All applications > Bright Pattern Omnichannel Contact Center - Single sign-on > SAML-based Sign-on

Bright Pattern Omnichannel Contact Center - SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on**
- Provisioning
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Provisioning logs (Preview)
- Access reviews

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Bright Pattern Omnichannel Contact Center.

- ### Basic SAML Configuration

Identifier (Entity ID)	bpexample.brightpattern.com_sso
Reply URL (Assertion Consumer Service URL)	https://bpexample.brightpattern.com/agentdesktop/sso/redirect
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- ### User Attributes & Claims

firstName	user.givenname
lastName	user.surname
email	user.mail
Unique User Identifier	user.userprincipalname
- ### SAML Signing Certificate

Status	Active
Thumbprint	EEDA692365B961E557FF4C48A3578703AE7A6A65
Expiration	7/1/2022, 1:05:22 PM
Notification Email	...@microsoft.com
App Federation Metadata Url	https://login.microsoftonline.com/7f3b7d01-a0...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
- ### Set up Bright Pattern Omnichannel Contact Center

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/7f3b7d01-a0...
Azure AD Identifier	https://sts.windows.net/7f3b7d01-a049-4dfd-9...
Logout URL	https://login.microsoftonline.com/common/wsf...

[View step-by-step instructions](#)
- ### Test single sign-on with Bright Pattern Omnichannel Contact Center

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

SSO configuration page

Basic SAML Configuration

In *Basic SAML Configuration*, you will name the application being configured for SSO and specify the source of the SAML token.

Basic SAML Configuration



Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

bpexample.brightpattern.com_sso ✓



Patterns: *.brightpattern_sso, http://adapplicationregistry.onmicrosoft.com/brightpattern

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://bpexample.brightpattern.com/agentdesktop/sso/redirect ✓



Patterns: https://*.bugfocus.com/agentdesktop/sso/redirect, https://*.brightpattern.com/agentdesktop/sso/redirect

Sign on URL ⓘ

Enter a sign on URL

Relay State ⓘ

Enter a relay state

Logout Url ⓘ

Enter a logout url

Basic SAML Configuration

In this section, if you wish to configure the application in IDP initiated mode, enter the values for the following fields:

1. **Identifier (Entity ID)** - Identifies the application for which SSO is being configured. This is also known as the Entity ID. Set the Identifier in the following pattern: **<subdomain>_sso** (e.g., "mycompany.brightpattern.com_sso").
2. **Reply URL** - Specifies where the application expects to receive the SAML token. Set **https://<subdomain>.brightpattern.com/agentdesktop/sso/redirect** and be sure to replace "<subdomain>" with your contact center name.

For example:

<https://mycompany.brightpattern.com/agentdesktop/sso/redirect>

3. Click **Save**.

Click **Set additional URLs** and perform the following step if you wish to configure the application in SP initiated mode:

1. In the **Sign-on URL** text box, set a URL using the following pattern: **https://<subdomain>.brightpattern.com/**
2. Click **Save**.

User Attributes & Claims

In *User Attributes & Claims*, you will specify what information (e.g., user's name, email, etc.) Azure AD sends to the application in the SAML token when a user signs in.

1. Click **Edit** to set attributes for the identity provider to identify your system. You will see the following list of claims and values.

User Attributes & Claims □ ×

[+ Add new claim](#)

Name identifier value: **user.userprincipalname [nameid-format:emailAddress]** 

Groups returned in claim: **None** 

CLAIM NAME	VALUE	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

User Attributes & Claims

2. Edit the following attributes for Just-in-time (JIT) user provisioning:
 1. **user.mail** - Delete this from the list because it is unnecessary
 2. **user.givenname** - Click **Edit** and change *Name* to *FirstName*
 3. **user.userprincipalname** - (Note there are two--choose the one with claim name that ends with *"/nameidentifier"*.) Leave this attribute as-is. This attribute is the username of the user in Bright Pattern Contact Center.
 4. **User.userprincipalname** - (Note there are two--choose the one with claim name that ends with *"/name"*.) Click **Edit** and change *Name* to *Email*
 5. **User.surname** - Click **Edit** and change *Name* to *LastName*

When done, your list should look like this:

User Attributes & Claims	
+ Add new claim	
Name identifier value:	user.userprincipalname [nameid-format:emailAddress]
Groups returned in claim:	None
CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Email	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/FirstName	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Edited attributes

Note: Bright Pattern does not map claims to email; Bright Pattern maps claims to the same user account name only. This means that existing users logging in with their username will be logged in only if their username matches an existing user account in Bright Pattern Contact Center. If JIT is enabled, if a user logs in, and if their username does not match an existing account name, a new user account will be created.

SAML Signing Certificate

In the *SAML Signing Certificate* section, you will create and download a SAML certificate, which Azure AD uses to sign the SAML tokens that it sends to the application.

1. Click **Edit** and select **New Certificate**.

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

[Save](#) [+ New Certificate](#) [↑ Import Certificate](#)

STATUS	EXPIRATION DATE	THUMBPRINT
Active	5/3/2022, 4:51:43 PM	721669AC4F4F87567439D692FD056510

Signing Option:

Signing Algorithm:

NOTIFICATION EMAIL ADDRESSES

Create new certificate

2. In the new certificate row that appears, set the desired Signing Option and Signing Algorithm, and then click **Save**. In this example, we selected “Sign SAML response and assertion” and “SHA-256”.

SAML Signing Certificate
Manage the certificate used by Azure AD to sign SAML tokens issued to your app

 Save  New Certificate  Import Certificate

STATUS	EXPIRATION DATE	THUMBPRINT
Active	5/3/2022, 4:51:43 PM	721669AC4F4F87567439D69
n/a	5/3/2022, 4:58:18 PM	Will be displayed on save

Signing Option

Signing Algorithm

NOTIFICATION EMAIL ADDRESSES

Signing Option and Signing Algorithm

3. Click **download** for the Certificate (Base64). The contents of this certificate will be pasted into our configuration in later steps.
4. After it downloads, open it and **Install Certificate**.

Set up

Next you will set up the application to use Azure AD as a SAML identity provider. This is needed for your app to connect to Azure AD.

Copy the **Log in URL** value and paste it into a separate text doc. When configuring your SSO integration account in later steps, you will paste this into the *Identity Provider Single Sign-On URL* property in your Bright Pattern SSO integration account.

Validate single sign-on

After configuration is done on the Azure portal, you should validate the settings to make sure that sign-in works correctly.

1. Click **Test**.
2. Click **Sign in as current user**. This lets you see if SSO works for you.

Bright Pattern Omnichannel Contact Center - SAML-based Sign-on

Test single sign-on with Bright Pattern Omnichannel Contact Center

Please make sure you have configured Bright Pattern Omnichannel Contact Center before testing.

Sign in as current user

Sign in as someone else

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please retry.

What does the error look like? [?](#)

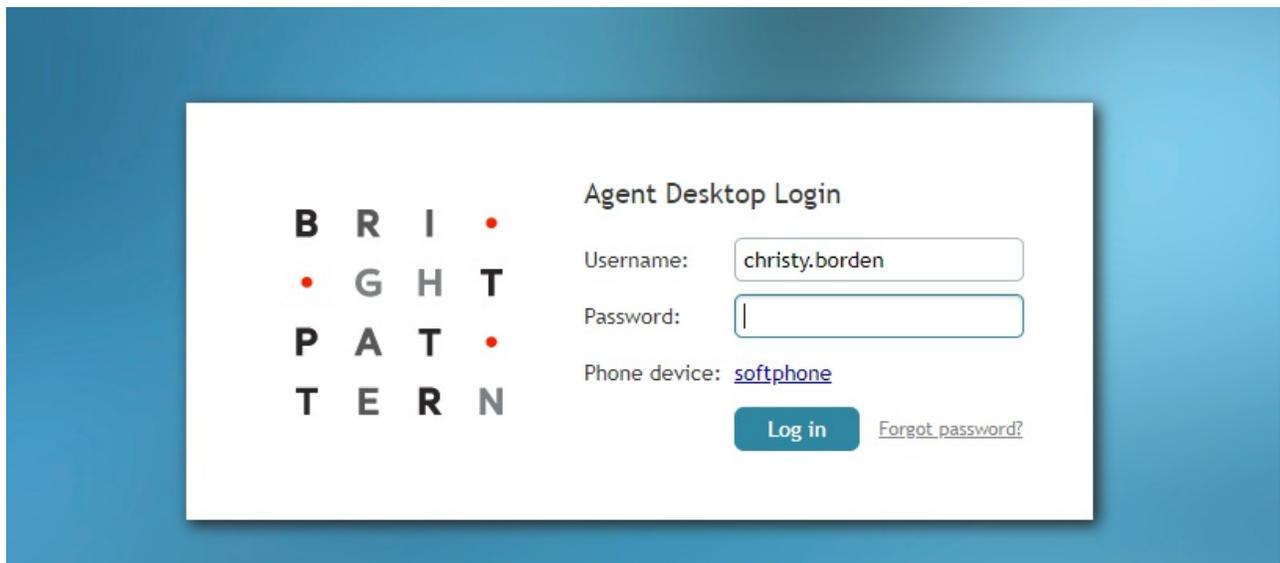
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
 Correlation Id: 5aa879f5-68f1-482a-a405-f993d8f4cb0
 Timestamp: 2018-03-06T23:54:10Z
 Message: Error AADSTSXXXXX

Get resolution guidance

Test

Validate SSO

3. If it works, you should see the Bright Pattern Agent Desktop login page. If it doesn't work, you will see an error message (see next section, *Errors*).



Agent Desktop login

Errors and How to Fix Them

Application with identifier was not found

This error means that you are unable to sign in because the application for which SSO is being configured cannot be identified; that is, the Identifier (Entity ID) that you set in Basic SAML configuration is incorrect. Go back to Step 3 of this procedure and make sure that your Identifier is set in the following pattern: <subdomain>_sso (e.g., "mycompany.brightpattern.com_sso").

Sign in

Sorry, but we're having trouble signing you in.

AADSTS700016: Application with identifier '
' was not found in the directory
. This can happen if the application has not been installed by
the administrator of the tenant or consented to by any user in the tenant. You may
have sent your authentication request to the wrong tenant.



Request Id: ×
Correlation Id:
Timestamp:
Message: AADSTS700016: Application with identifier '
' was not found in the directory
This can happen if the application has not been installed by the administrator of
the tenant or consented to by any user in the tenant. You may have sent your authentication
request to the wrong tenant.

Advanced diagnostics: [Enable](#)
If you plan on getting support for an issue, turn this on and try to reproduce the error. This will
collect additional information that will help troubleshoot the issue.

Application with identifier was not found

HTTP Error 404

This likely means that the Reply URL is incorrect, and your tenant's Agent Desktop cannot be found. Go back to *Basic SAML Configuration* and check that the Reply URL is **https://<subdomain>.brightpattern.com/agentdesktop/sso/redirect**

HTTP ERROR 404

Problem accessing /agentdesktop/sso/redirect. Reason:

Not Found

Powered by Jetty://

404, Page Not Found

Redirects to Microsoftonline with HTTP Error 404

This error could mean one of the following:

1. In *Basic SAML Configuration*, you tried to set a value for Relay State, which is unsupported. Go back and leave all optional URLs blank, and **Save**.
2. More than one Azure AD application has a Reply URL that is pointing to the same tenant. Try checking other registered applications and enterprise applications in your Active Directory. Check their Reply URLs and remove any extraneous app Reply URLs that have a callback to your tenant.



This login.microsoftonline.com page can't be found

No webpage was found for the web address:

<https://login.microsoftonline.com/xxxxxxxx-xxxx?RelayState=49eb939e-9486-4dde-a0ae-8acf74d235a8>

HTTP ERROR 404

Reload

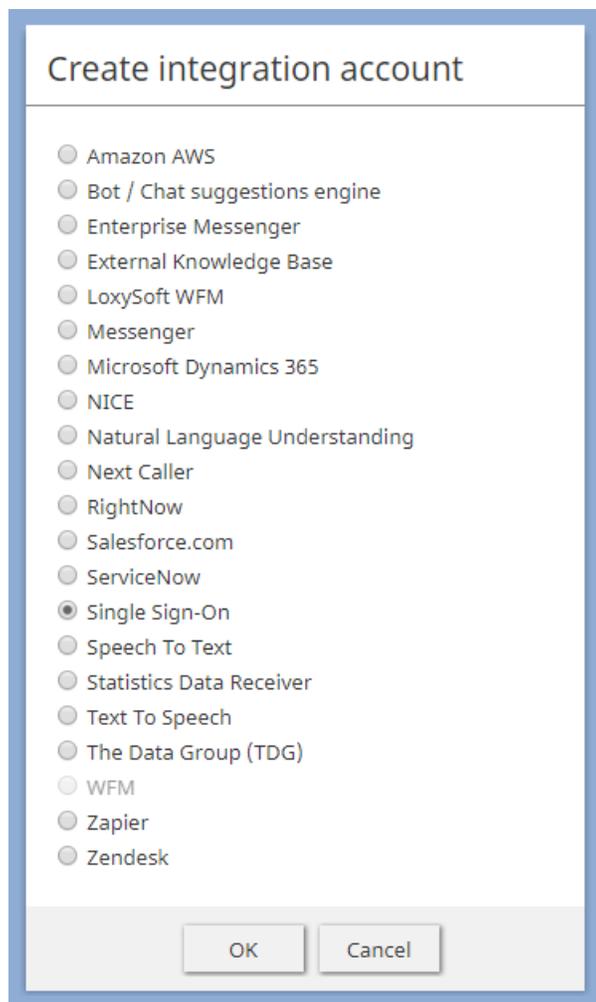
404, Page Not Found

Configuration in Bright Pattern

Next you will set up the integration account that enables your contact center to work with Azure AD.

Step 1: In Bright Pattern, add SSO integration account

In the Bright Pattern Contact Center Administrator application, go to *Call Center Configuration > Integration Accounts* and add a new [Single Sign-On integration account](#). This is a general type of SSO account that Bright Pattern uses for various integrations.



Add SSO integration account

Step 2: Edit properties with your Azure AD app credentials

In *Properties*, name the account (any name). The account properties are split into two sections: Agent Desktop SSO and Admin SSO.

In the Agent Desktop SSO properties, specify the following properties.

Properties

Name:	<input type="text" value="Azure SSO"/>
Enable Single Sign-On:	<input checked="" type="checkbox"/>
Use SSO for administrator portal login:	<input checked="" type="checkbox"/>
Identity Provider Single Sign-On URL:	<input type="text" value="https://login.microsoftonline.com/"/>
Identity Provider Issuer:	<input type="text" value="yourcompany.brightpattern.com_s"/>
Identity Provider Certificate:	[Certificate]
Enable Just-in-time user provisioning:	<input checked="" type="checkbox"/>
Use Template:	<input type="text" value="Jeffery Lozada"/> add/edit

Add SSO integration account

Properties

- **Enable Single Sign-On** - Select the checkbox to enable SSO
- **Use SSO for administrator portal login** - Select the checkbox in order to enable SSO for users of the Contact Center Administrator application (i.e., the "administrator portal") who have the admin role.
- **Identity Provider Single Sign-On URL** - The "Login URL", which is taken from Setup in Azure AD SAML SSO configuration (e.g., "<https://login.microsoftonline.com/1f2b3d04-a056-7dfd-8dbd-d910e111c2a0/saml2>")

4

Set up Bright Pattern Omnichannel Contact Center

You'll need to configure the application to link with Azure AD.

Login URL	<input type="text" value="https://login.microsoftonline.com/7f3b7d01-a0..."/>	
Azure AD Identifier	<input type="text" value="https://sts.windows.net/7f3b7d01-a049-4dfd-9..."/>	
Logout URL	<input type="text" value="https://login.microsoftonline.com/common/wsf..."/>	

[View step-by-step instructions](#)

Where to find Login URL

