5.8 Integrations

Bright Pattern Documentation

Generated: 8/09/2022 4:12 pm

Table of Contents

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:

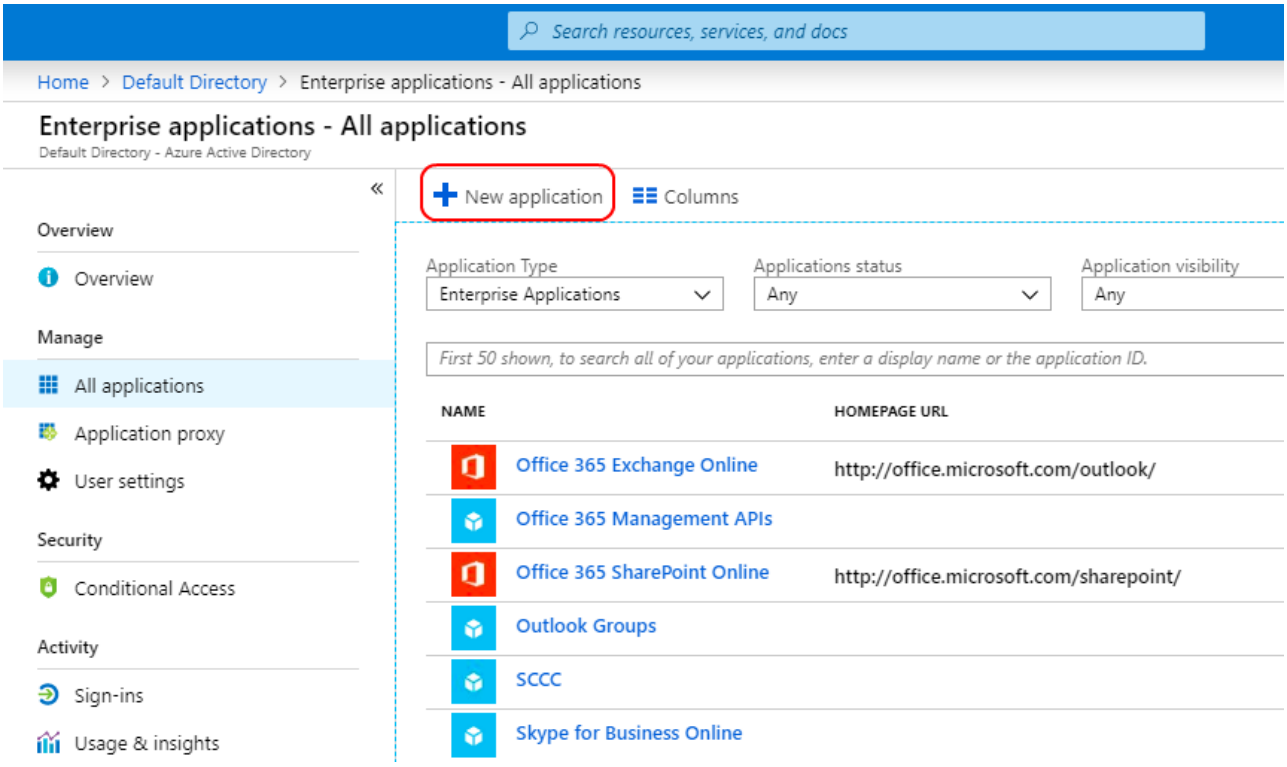
- Microsoft Office 365 account. If you are unable to log into Microsoft directly, please contact your Microsoft system administrator to review permission and access level settings.
- Microsoft Azure account/subscription (free trial OK). Without this, you will have no directory and will not be able to 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

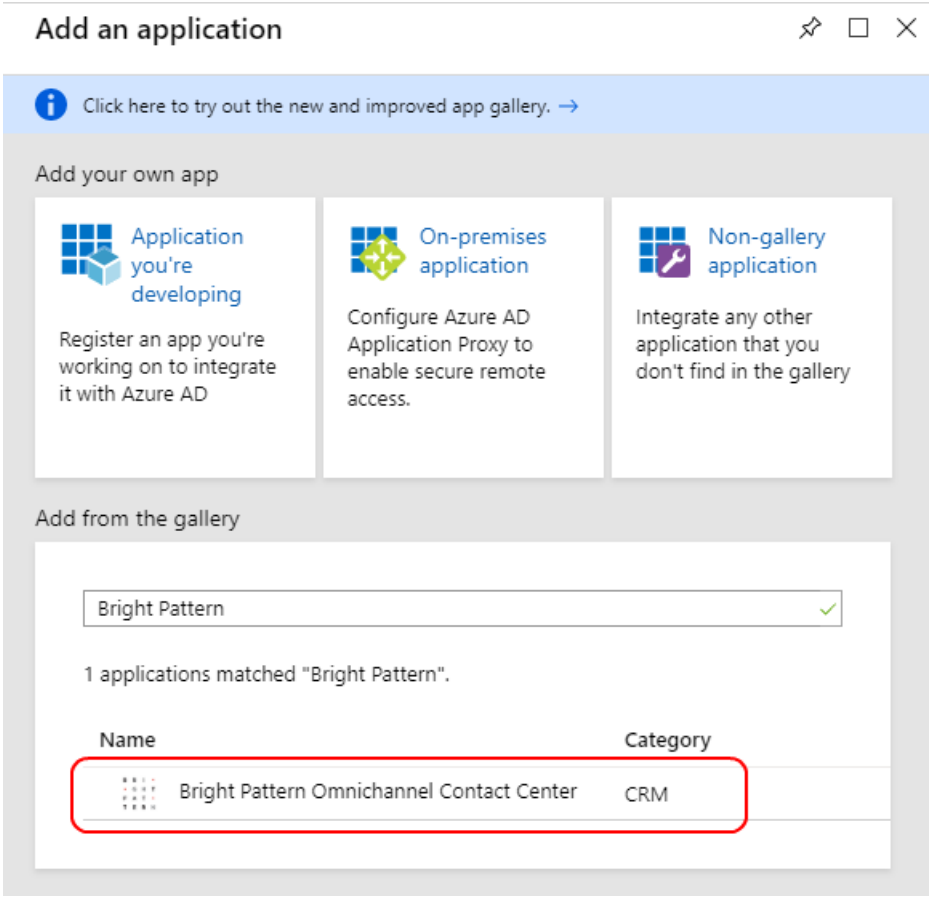
1. Sign in to the Microsoft Azure portal.
2. Go to *Azure Active Directory* > *Enterprise applications* and click **+ New application**.



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.



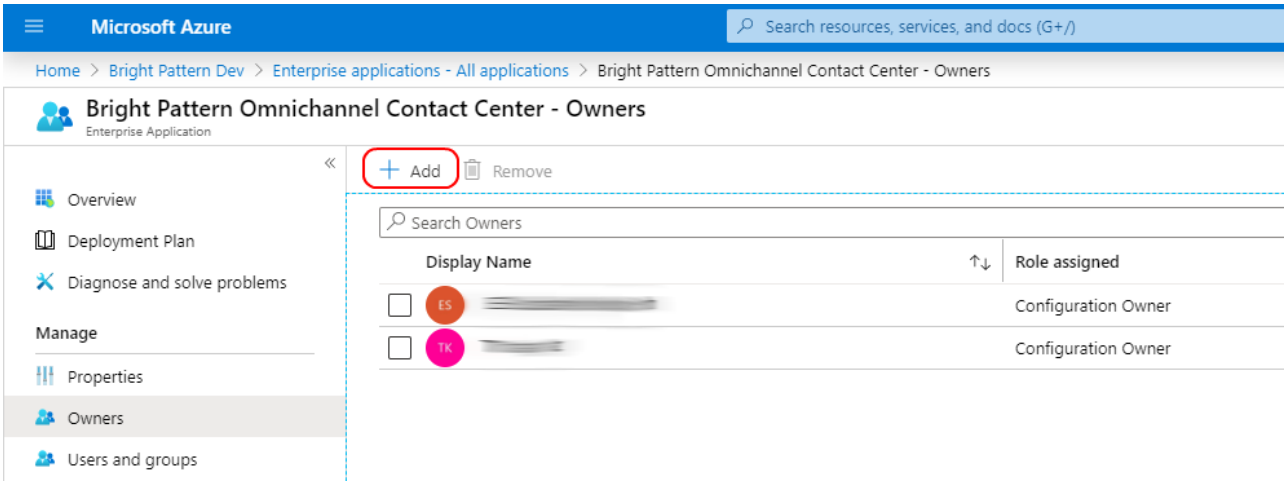
Application properties

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.

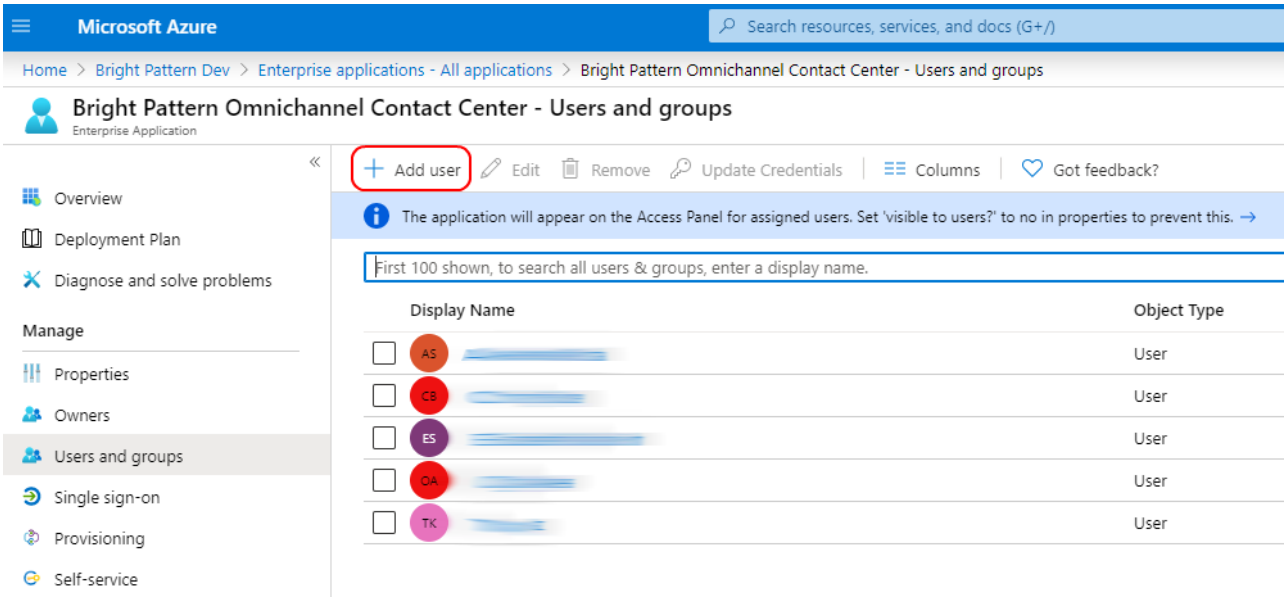
1. On the overview page for the application, go to *Manage* > *Owners* and then click **add**.



Add owners

2. In *Select Owners*, add yourself as the owner of the application so that you can modify the application. Then click **Select**.

3. Then go to *Manage* > *Users* and groups and click **Add user**.



Add users

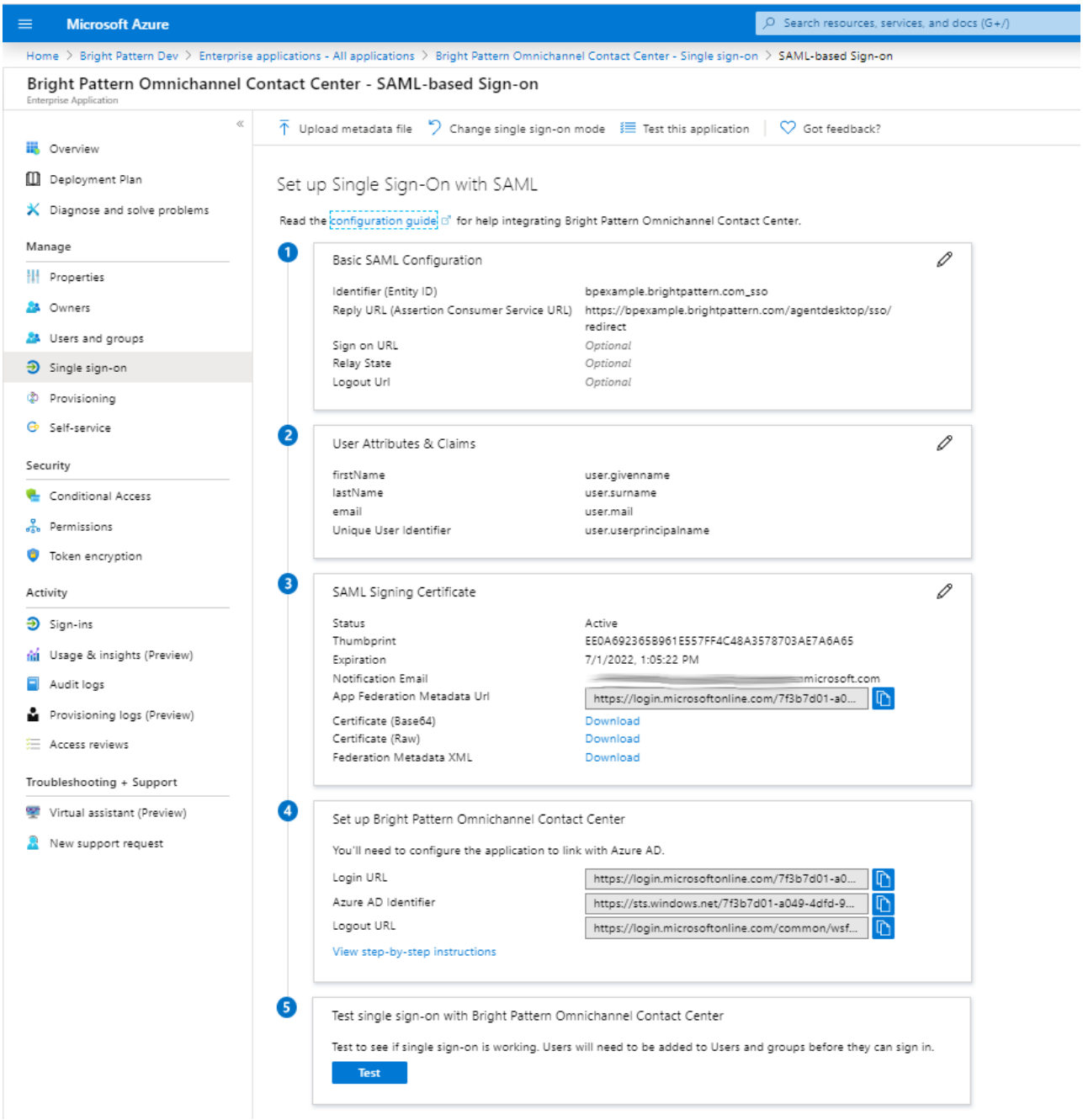
4. Click **Users and groups**, select the users with rights to use this application, and click**Assign**. Assigning allows the user to use Azure AD SSO.

5. After you add the users, you can repeat these steps to add the group, if desired.

Step 3: Configure Azure AD SSO

1. 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.

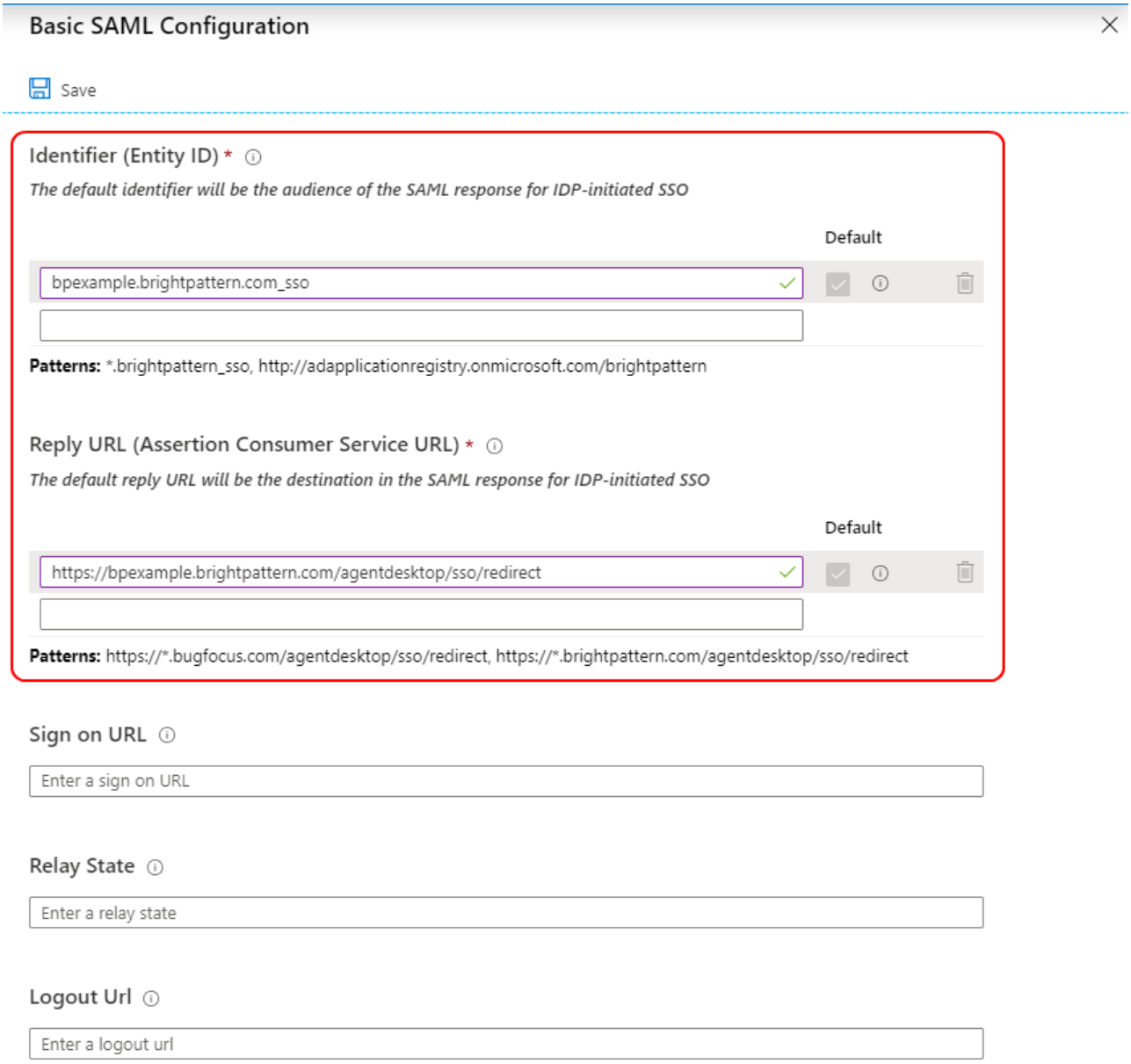
2. The *Set up SSO with SAML Preview* page will open with the following boxes.



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

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:

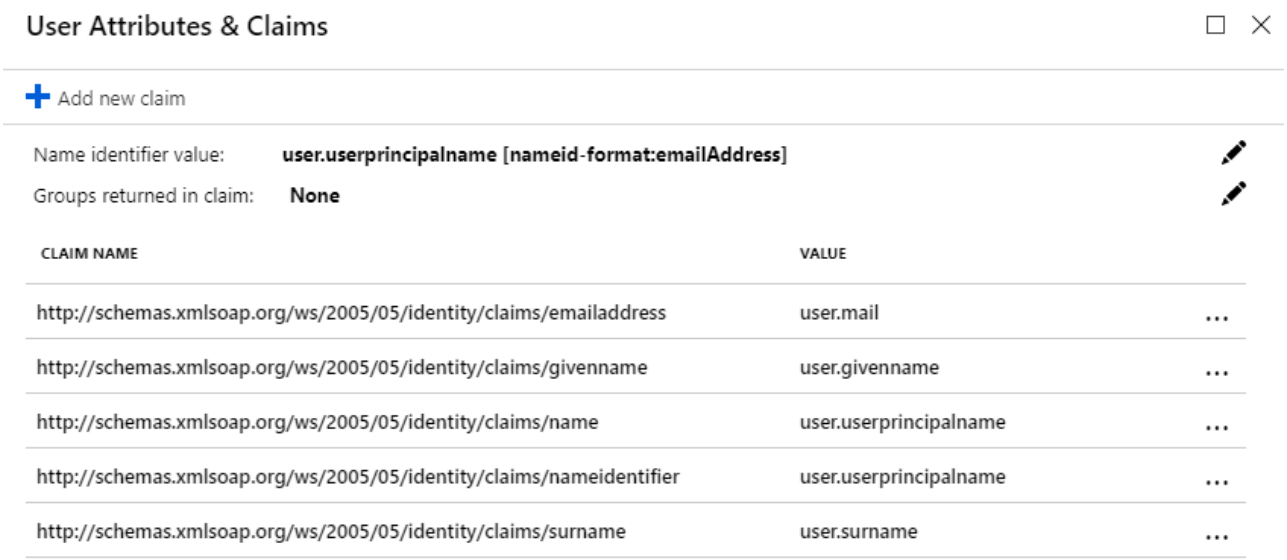
1. In the **Sign-on URL** text box, set a URL using the following pattern: **https://<subdomain>.brightpattern.com/**

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

2. Edit the following attributes for Just-in-time (JIT) user provisioning:

    1. **user.mail** - Delete this from the list because it is unnecessary

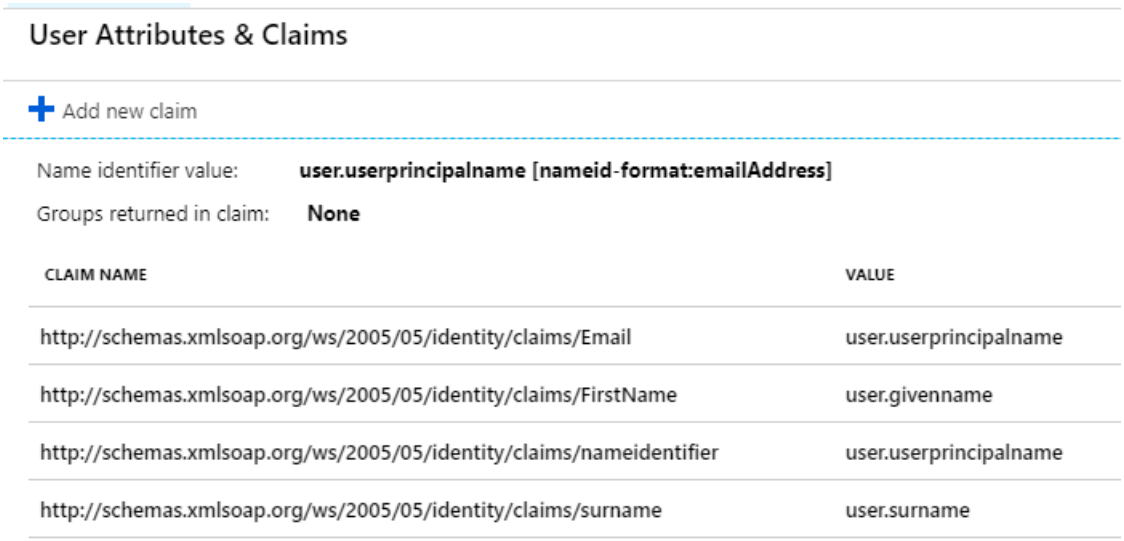
    2. **user.givenname** - Click **Edit** and change *Name* to *FirstName*

    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:



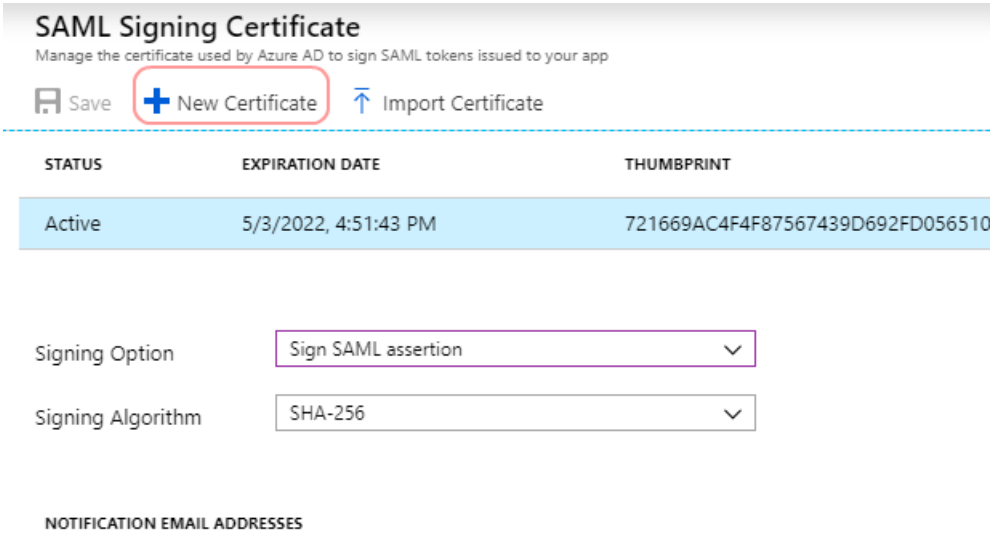
Edited attributes

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

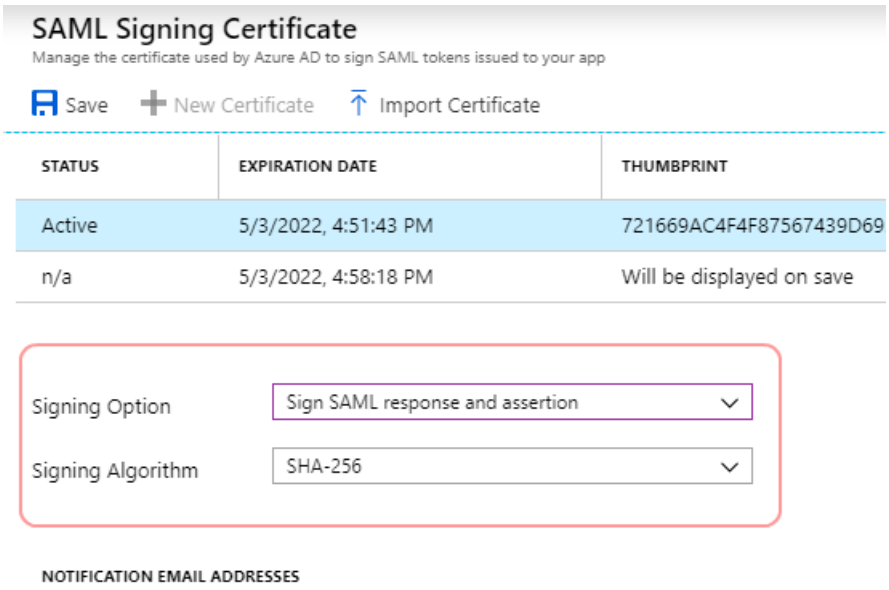
In the *SAML Signing Certificate* section, you will create and download a SAML certificate, which Azure AD uses to sign the SAML tokens that it sends to the application.

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



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”.



Signing Option and Signing Algorithm

3. Click **download** for the Certificate (Base64). The contents of this certificate will 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.

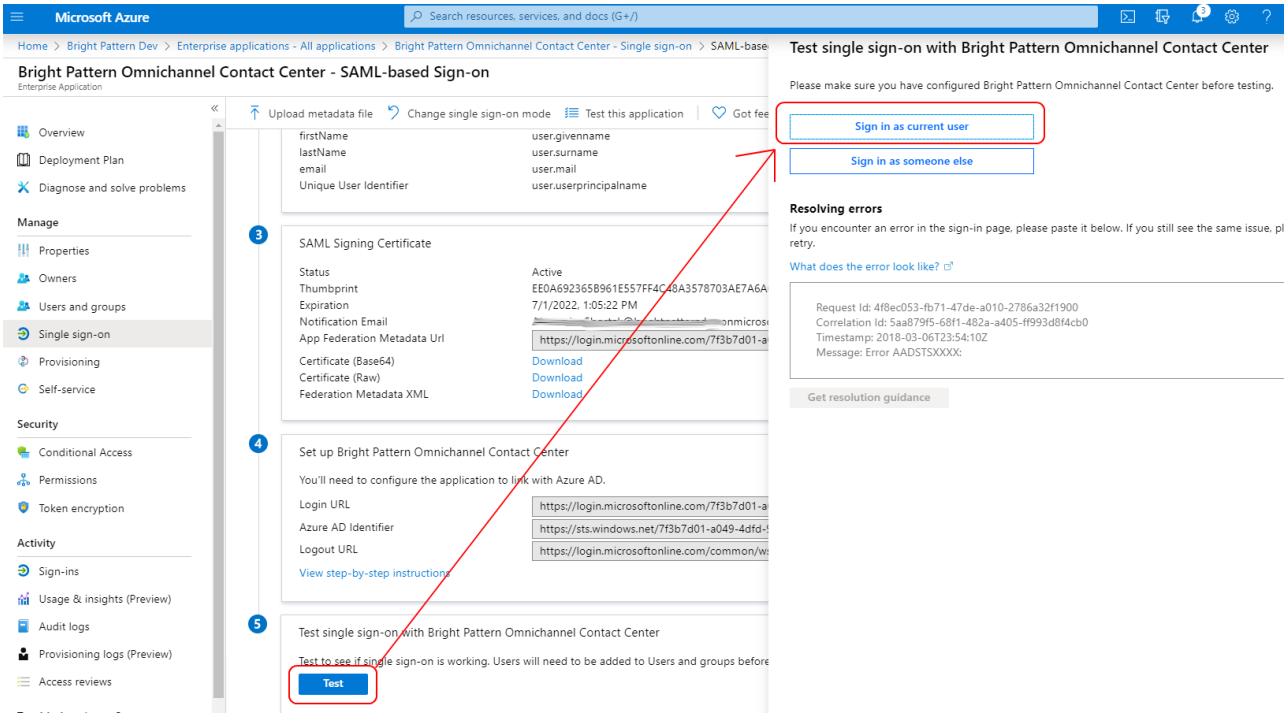
Copy the **Log in URL** value and paste it into a separate text doc. When configuring your SSO integration account in later steps, you will paste this into the *Identity Provider Single Sign-On URL* property in your Bright Pattern SSO integration account.

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.

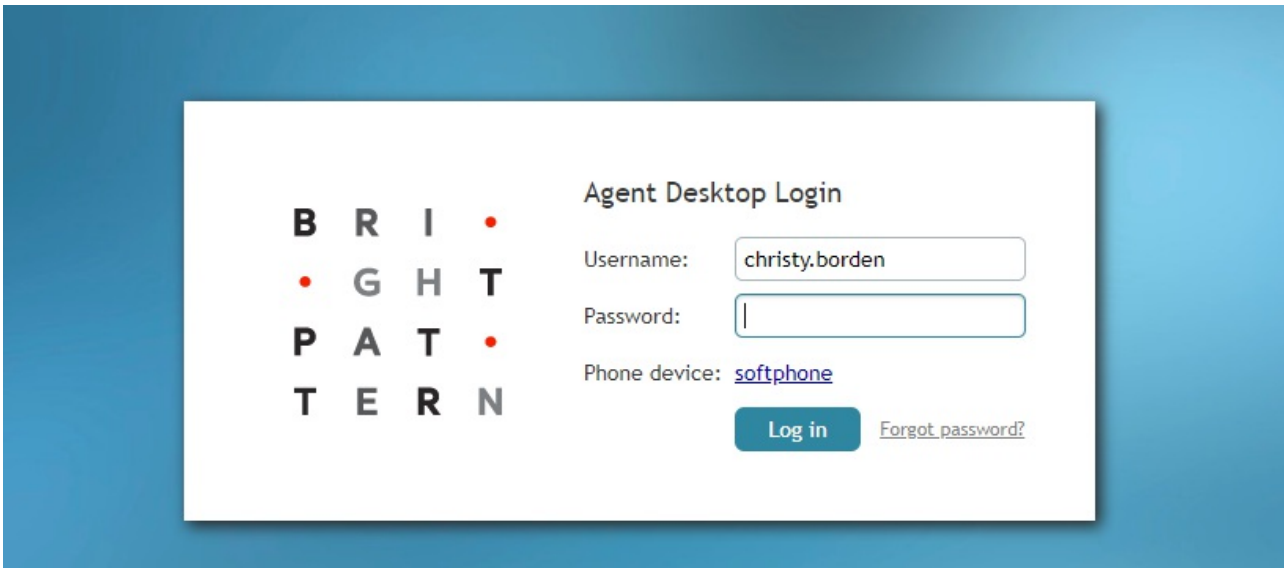
1. Click **Test**.

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



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*).

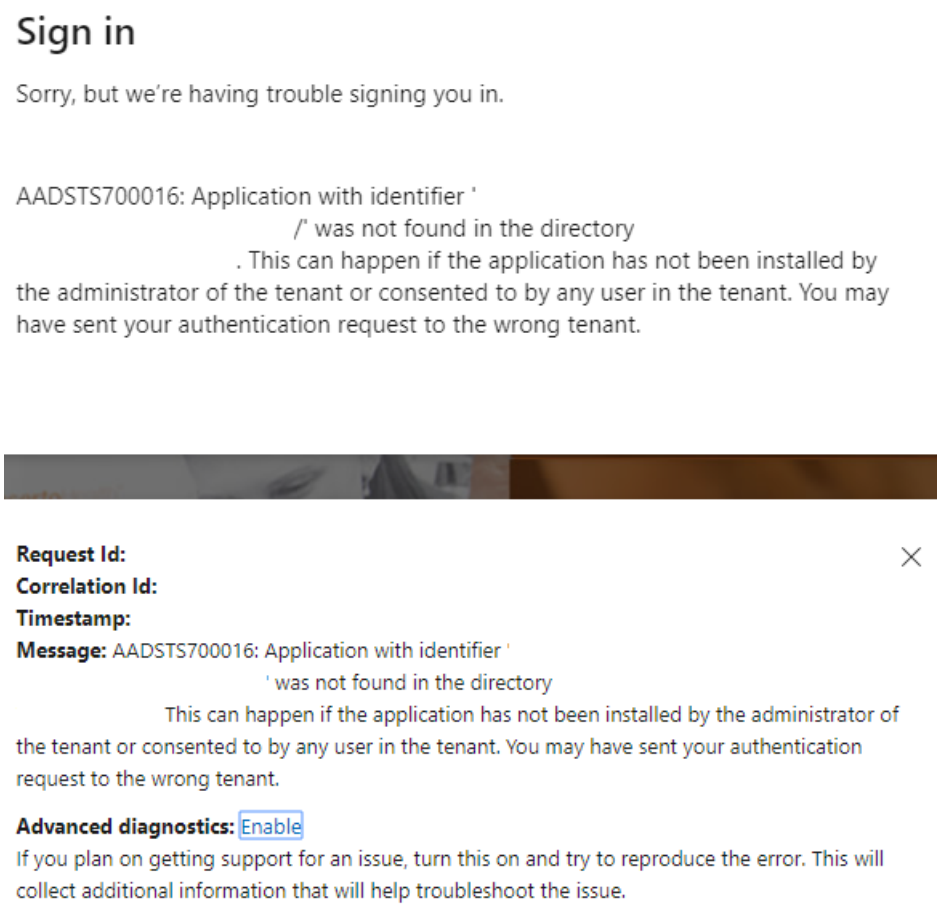


Agent Desktop login

Errors and How to Fix Them

Application with identifier was not found

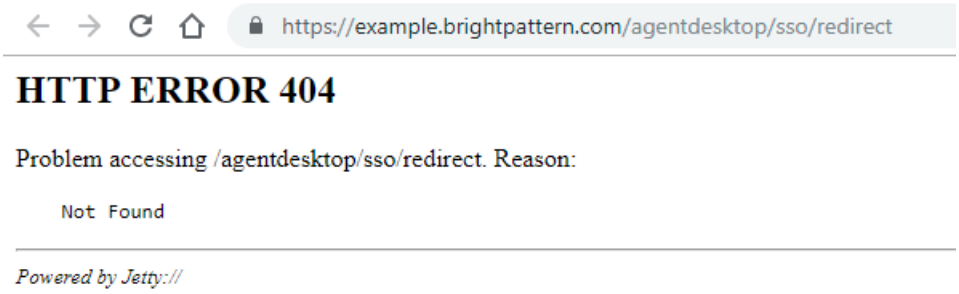
This error means that you are unable to sign in because the application for which SSO is being configured cannot be identified; that is, the Identifier (Entity ID) that you set in Basic SAML configuration is incorrect. Go back to Step 3 of this procedure and make sure that your Identifier is set in the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



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**



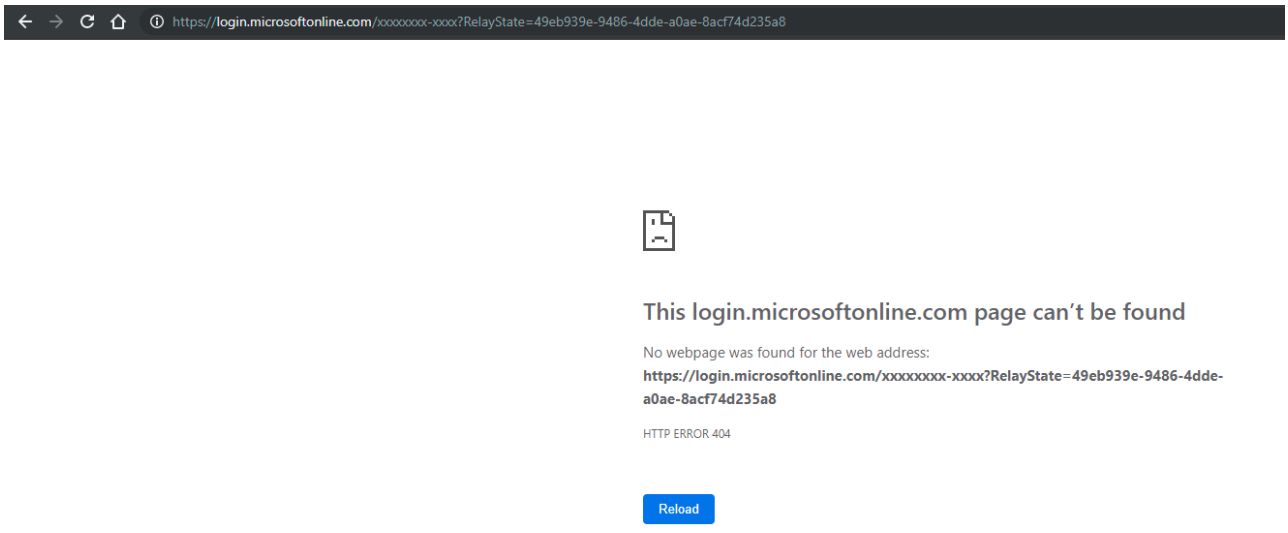
404, Page Not Found

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.



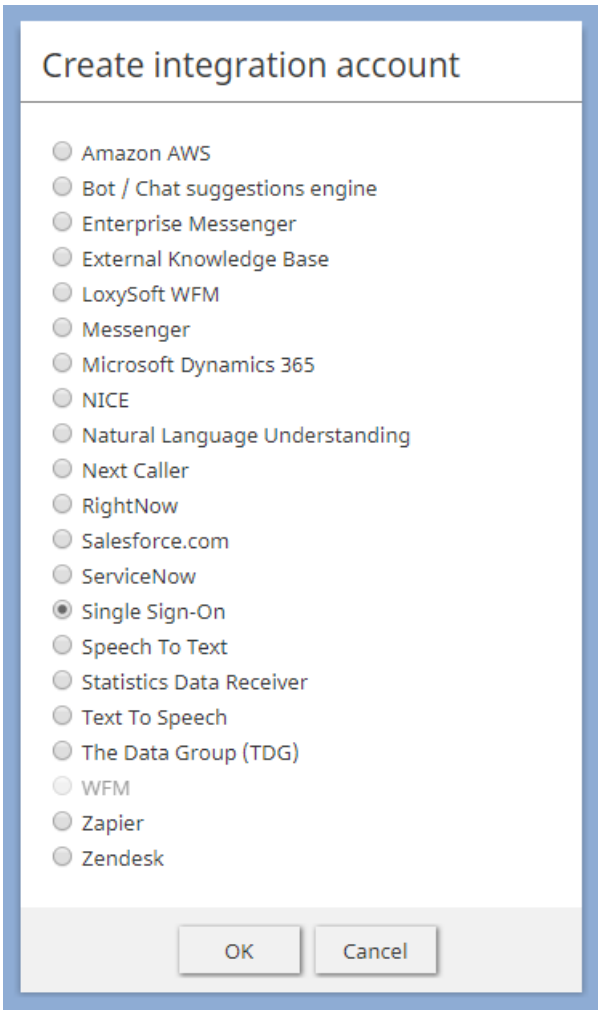
404, Page Not Found

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.

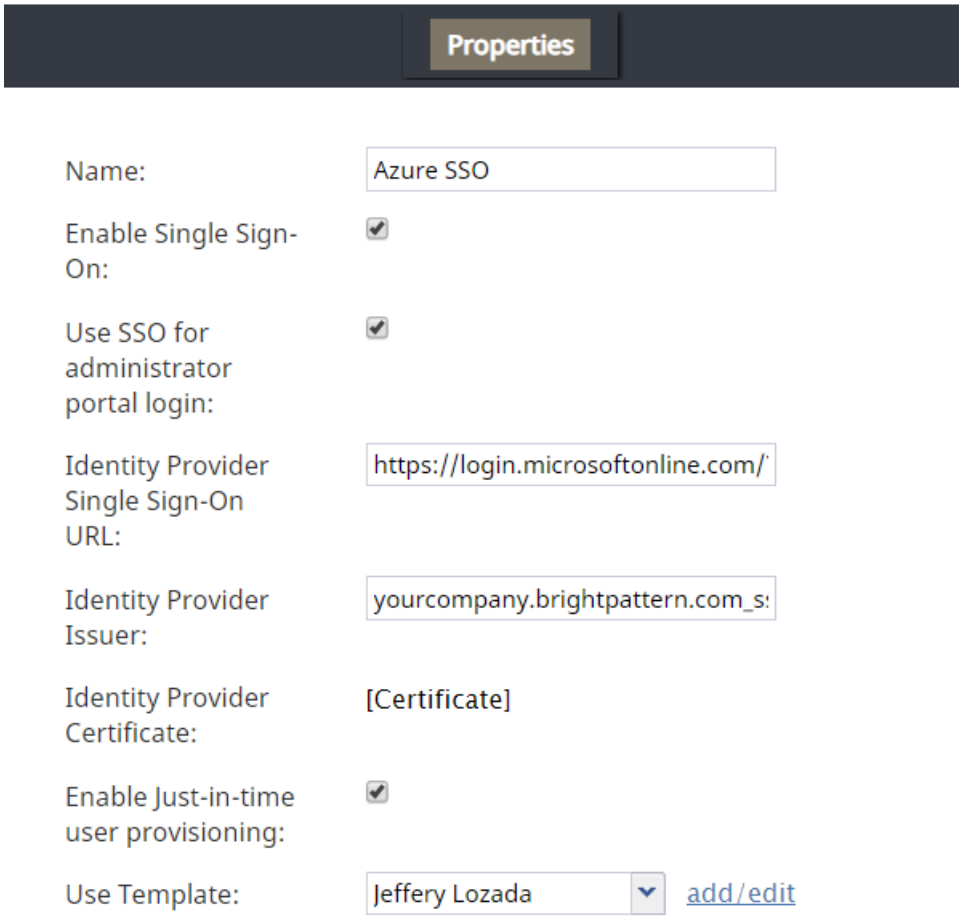


Add SSO integration account

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.

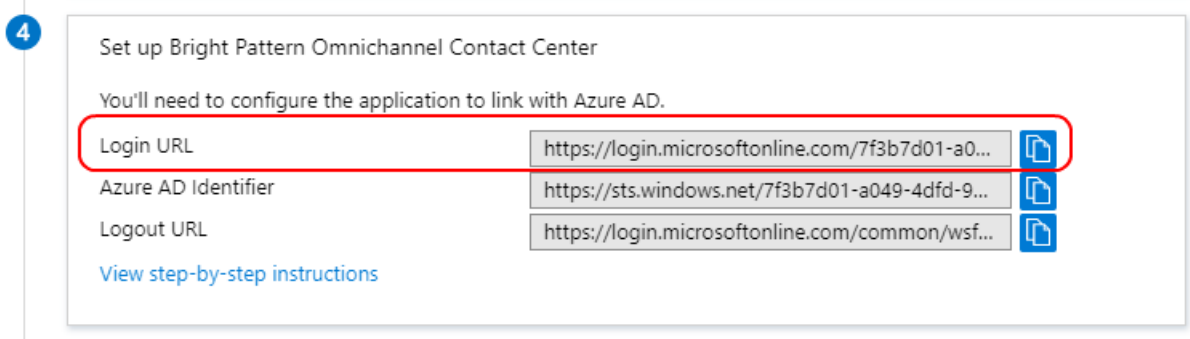
In the Agent Desktop SSO properties, specify the following properties.



Add SSO integration account

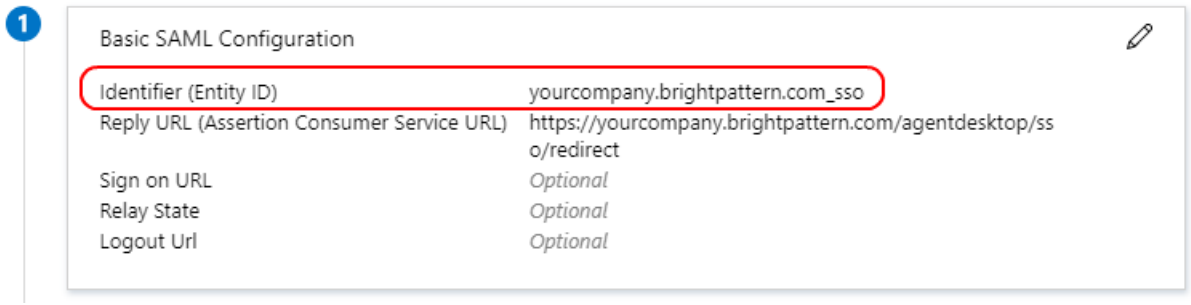
Properties

- **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")



Where to find Login URL

- **Identity Provider Issuer** - The “Identifier (Entity ID)”, as set in the Basic SAML Configuration section of Azure AD SAML SSO configuration (e.g., “<subdomain>_sso”). The Identifier (Entity ID) set in Azure must match the Identity Provider Issuer in the Bright Pattern Configuration.



Where to find the Identifier (Entity ID)

- **Identity Provider Certificate** - The Base 64 certificate that you downloaded from Azure AD. Copy and paste the entire contents, **including** the “BEGIN” and “END” tags.

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQYERvavxSd5dGEr+ZOzykqTANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylNaWNyb3NvZnQgQXplcmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0xOTA3MDEyMDAl
MjJaFw0yMjA3MDEyMDAlMjJaMDQxMjAwBgNVBAMTKUlpY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQg
UlNPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArFQv5BxJEkAc
MAZjXxUlhpzVSeiyz37MpS75c/mOqC+voP4f99at272RC92x+pirZTMavWwQ+HCjlwTsbLAehAD4
RJHiyaSVnuTfHmfP80fe7BNjKpqjVCNZhJ38NVyxB4wpTuxK9GDJg5MlfZ8ORnVCNXzVfc7RZ9f6
uuN/xIxx4Pq6ZZFw5/ISGzneLMBslo/Gz7BRp8sxW0ybcKTXpjWCwsryHjkSteKINykyxi5vwk59
yR4+SDp8veGZx0VbJbRm6scAxhE949noxkqetIilZLgUMJHcR+00gxQhDUXv3YYti7XpgQcDKQ3g
QHkjnebqYJNSFd8cblMlbzmFZwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3ToA/mfDjuloLnVm4
DcccQfAvhgYE3bGt3lQlwIabeVhLUKVpuSSJhESnvwMX5/dMP72N2/emjVZcm3luRy3e8vXg/zT0
SXqp5PQpr5RRC2BNWoqDJc3btY5m6464CWdOplTdzIMWdt7M3M9GaDHcwcS6wCCCwXT93bart9ex
Y6j6BvtcpS+ORbill/JJbGumkAuVAoXFKig0knxIkoB+Ww3BuqGr38qnyvyU8qqXwJu4Ne5q5Obh
Ic5h9xKaA3ciqnovG7/MVyES2Lgj9Mpv4Wf2t+Wt/Y4hzalQc/XXvUY66tTk73VYCl5XGi8Sf6Nx
wg84WPPSM6KQUQxrNwjr
-----END CERTIFICATE-----
```

Copy certificate contents

- **Enable Just-in-time user provisioning** - Select the checkbox to enable just-in-time (JIT) user provisioning. JIT user provisioning automatically creates call center users on the first SSO login attempt authorized by the identity provider. If you enable JIT, you must also use a template (see next property).

- **Use Template** - Select this checkbox to copy assignments (e.g., username format, email, roles, teams, skills, etc.) from a specific user with the agent role, and apply them to new call center users created by JIT user provisioning.

Lastly, click **Apply** to save your changes.

This completes Azure AD SSO configuration.