5.3 Integrations

Bright Pattern Documentation

Generated: 12/09/2021 12:50 am

Table of Contents

1. REDIRECT 5.3:Contact-center-administrator-guide/CallCenterConfiguration/IntegrationAccounts

Integration Accounts Overview

Integration accounts enable your contact center to work with third-party systems, such as customer relationship management (CRM) and workforce management (WFM) applications. The following is a list of articles containing integration account types:

- Amazon AWS
- Bot / Chat suggestions engine
- Co-browsing
- External Knowledge Base
- Loxysoft WFM
- Messenger
- Microsoft Dynamics 365
- Natural Language Understanding
- Next Caller
- NICE
- Remote Assistance
- RightNow
- Salesforce.com
- SCIM
- ServiceNow
- Single Sign-On
- Speech To Text
- Statistics Data Receiver
- Teleopti WFM
- Text To Speech
- The Data Group (TDG)
- WFM
- Zapier
- Zendesk

Call Center Configuration > Integration Accounts

Managing Integration Accounts

How to Add a New Integration Account

1. In Contact Center Administrator, go to *Call Center Configuration* > *Integration Accounts*.
2. At the bottom of the screen, click the **add** (**+**) button. The Types dialog will open.
3. Select the type of integration account to add (see links to various types above).

How to Edit an Existing Integration Account

1. In Contact Center Administrator, go to *Call Center Configuration* > *Integration Accounts*.
2. From the listed accounts shown, select the integration account you want to edit.
3. In the Properties pane that opens, edit properties as desired.
4. Click **Apply** to save your changes.

How to Delete an Integration Account

1. In Contact Center Administrator, go to *Call Center Configuration* > *Integration Accounts*.
2. From the listed accounts shown, select the integration account you want to remove.
3. At the bottom of the screen, click the **delete** (**X**) button.

4. Confirm the deletion and click **Apply** to save your changes.

Notes

Version 1.1 and later of the Transport Layer Security (TLS) encryption protocol is used to ensure the security of the data passed between Bright Pattern and CRM applications.

The reports required for workforce scheduling are configured for automatic generation and delivery via the Scheduled Reports screen of the Contact Center Administrator application.

LogMeIn Integration Quick Start

This article will help administrators enable and configure integration with LogMeIn Rescue for their contact center. After completing the following steps, agents who are also LogMeIn Rescue technicians will be able to support customers with remote assistance during call and chat interactions.

Procedure

1. Make sure that...
    1. You have access to a valid LogMeIn Remote Support On-Demand account and the Rescue Technician Console application.
    2. You know the credentials that the master administrator of LogMeIn Rescue uses to log in to the Rescue Technician Console application.
    3. The master administrator of LogMeIn Rescue is **not** also a technician.
2. Confirm with your service provider that the LogMeIn Rescue Integration feature is enabled for your contact center.
3. In the Contact Center Administrator application, add a Remote Assistance integration account of type LogMeIn. See the *Contact Center Administrator Guide*, section *Integration Accounts* > *Remote Assistance*.
4. In Agent Desktop, an agent can accept a voice call and start a remote assistance session. The agent must be a LogMeIn Rescue technician, have the LogMeIn Rescue Technician Console application installed on their computer, and be logged in to that application.
5. In Agent Desktop, an agent can accept a chat and start a remote assistance session. The agent must be a LogMeIn Rescue technician, have the LogMeIn Rescue Technician Console application installed on their computer, and be logged in to that application.

Learn More

- Overview: Remote Assistance in Chats

- How to Start Remote Assistance During a Chat/SMS/Messaging Session
- How to Transfer a Remote Assistance Session to a Different Agent During a Chat Session
- Overview: Using Remote Assistance During Calls
- How to Start Remote Assistance During a Phone Call
- How to Transfer a Call with an Active Remote Assistance Session

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.

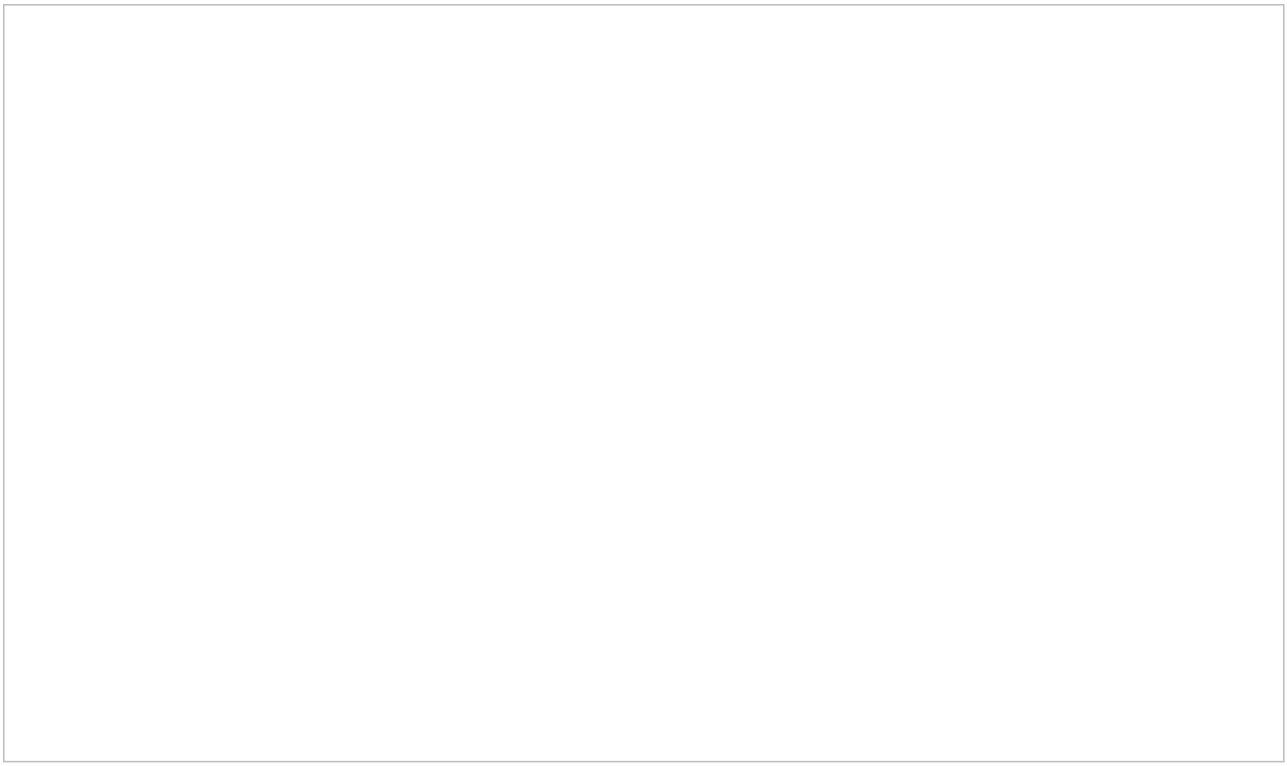
- Microsoft Azure account/subscription (free trial OK). Without this, you will have no directory and will not be able to access any data in Azure AD.
- Bright Pattern Contact Center version 5.3 or later

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.

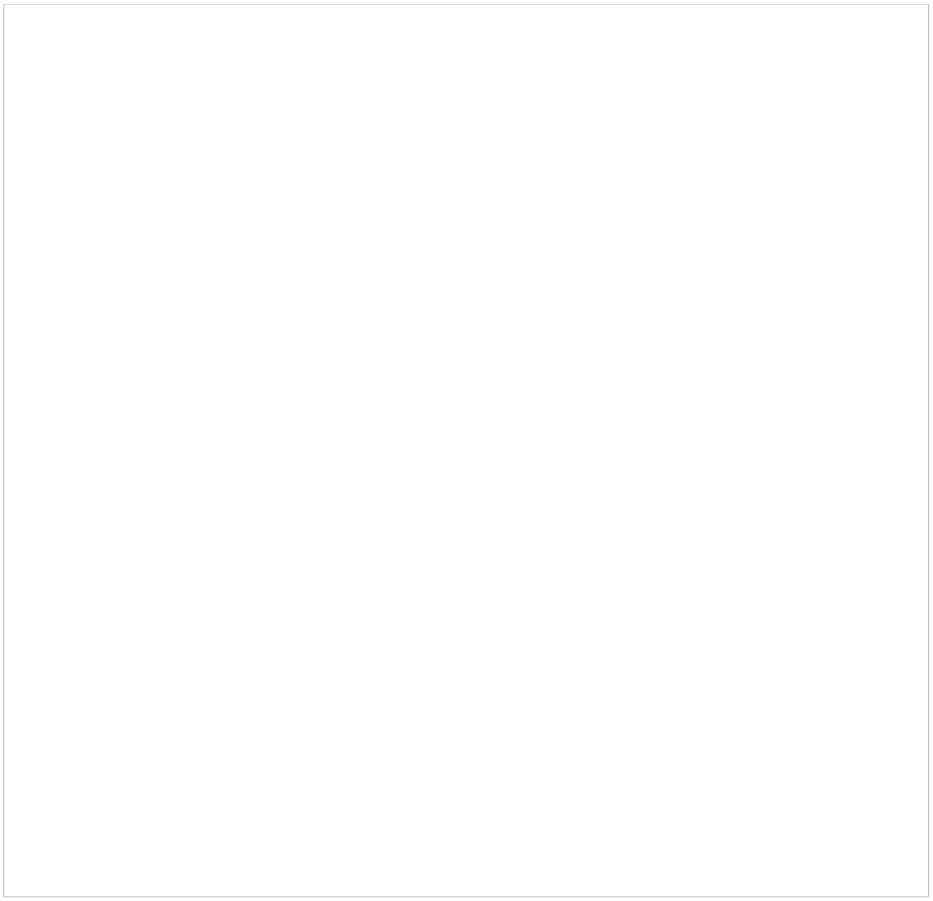
Step 1: Add the Bright Pattern application from the Gallery

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.



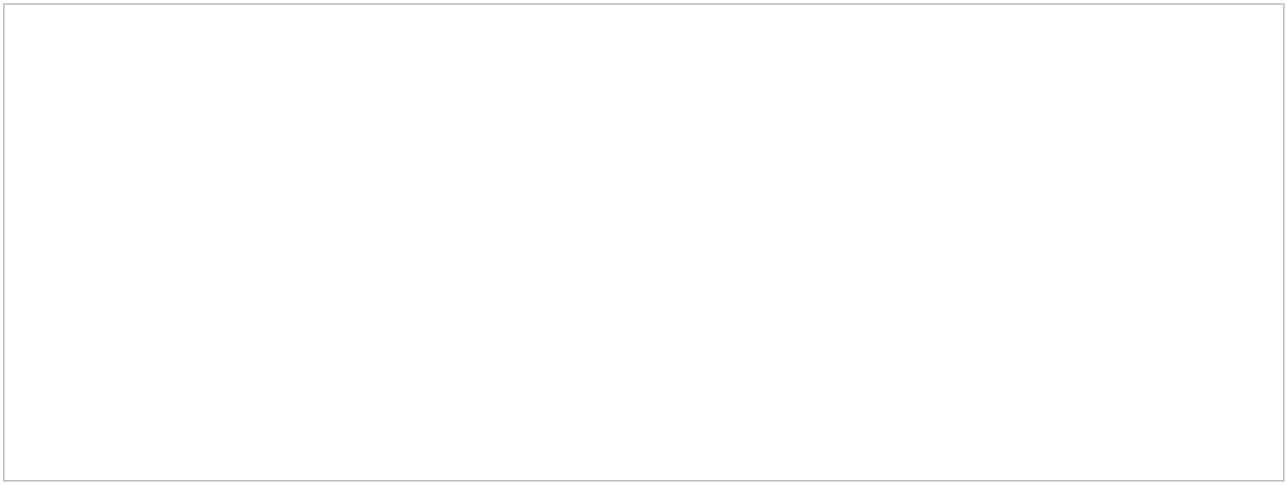
Application properties

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.

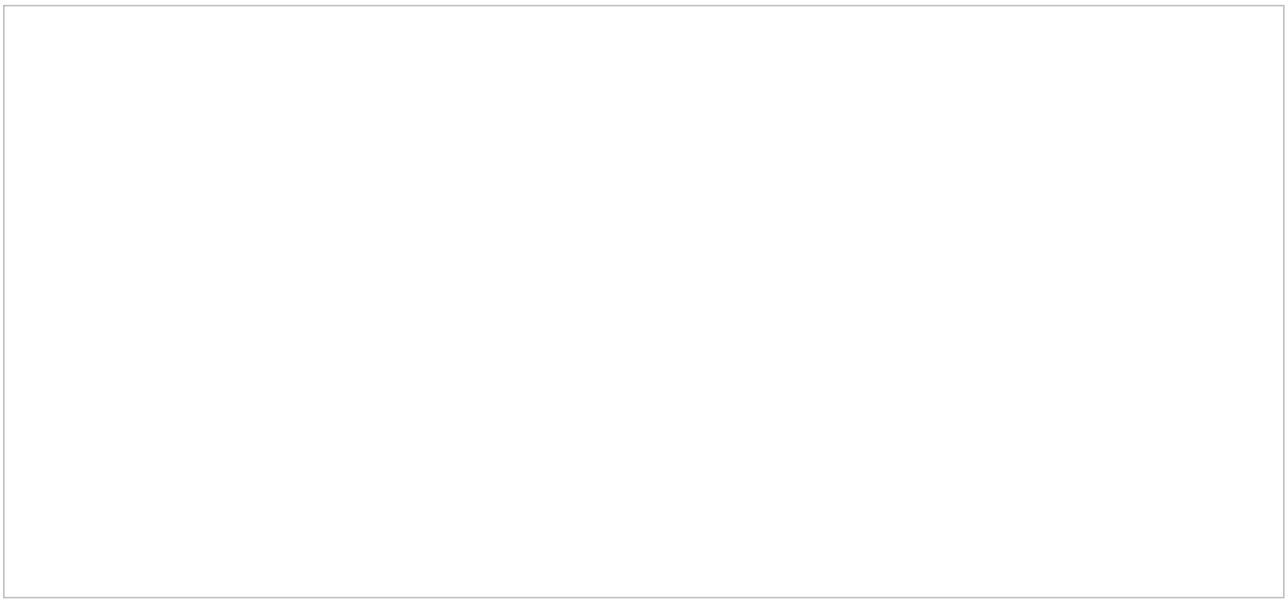
1. On the overview page for the application, go to *Manage* > *Owners* and then click **add**.



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:

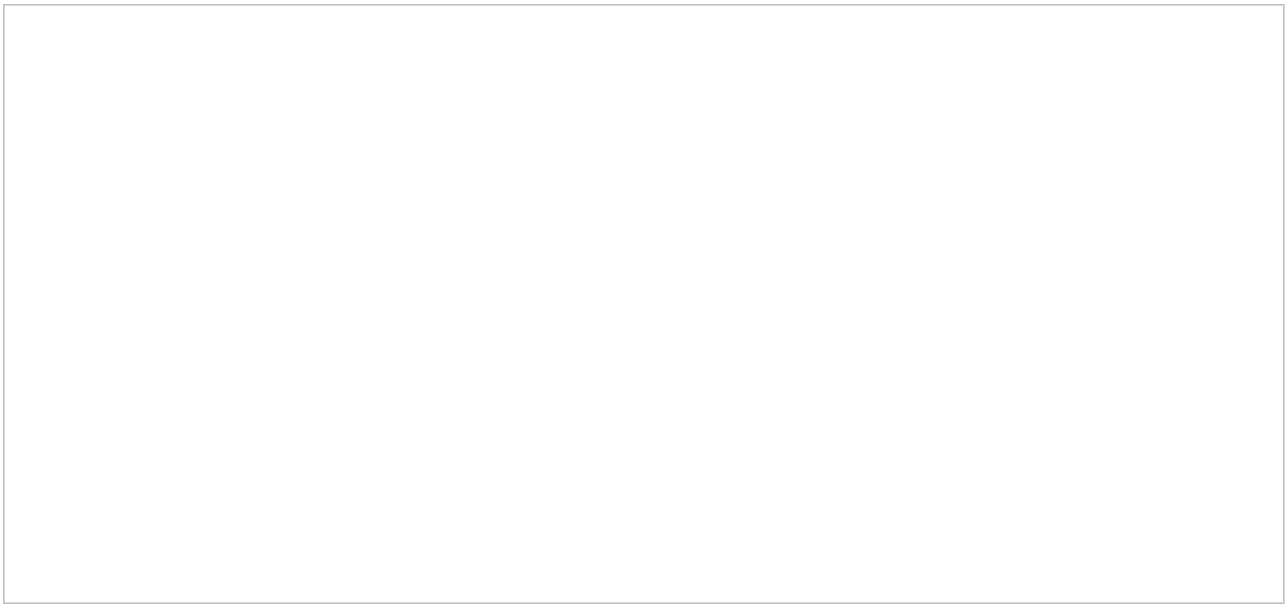
1. In the **Sign-on URL** text box, set a URL using the following pattern: **https://<subdomain>.brightpattern.com/**

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

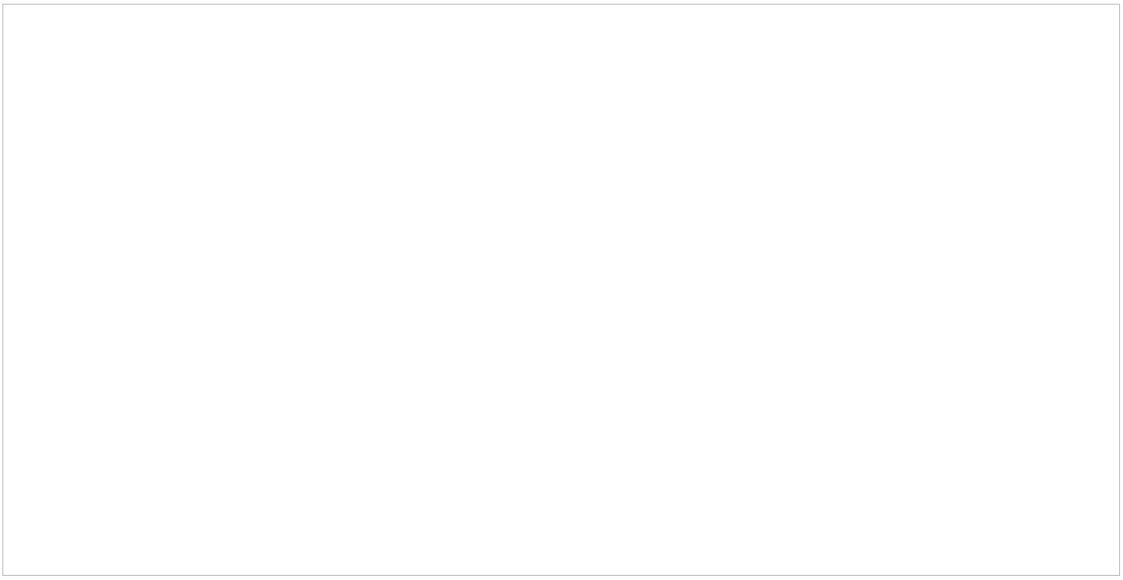
    2. **user.givenname** - Click **Edit** and change *Name* to *FirstName*

    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:



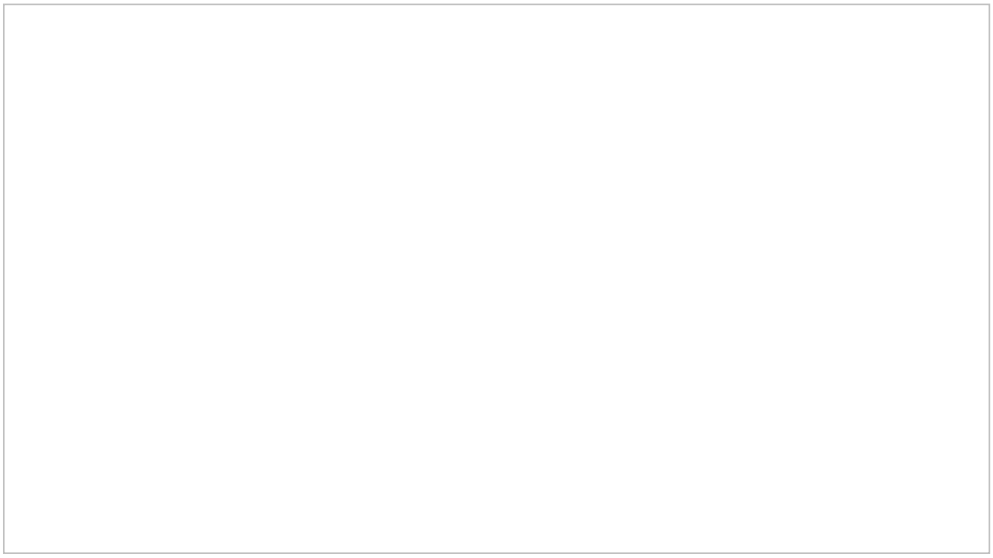
Edited attributes

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

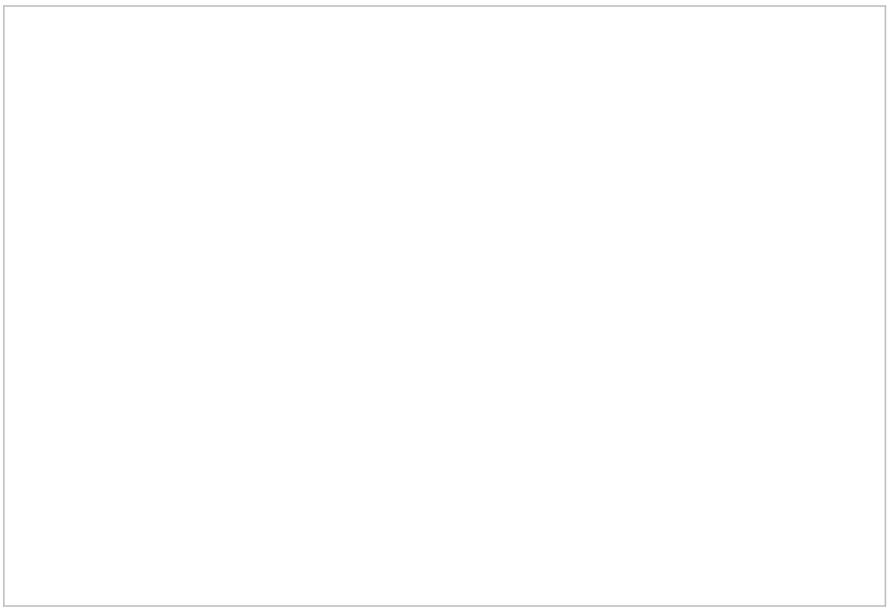
In the *SAML Signing Certificate* section, you will create and download a SAML certificate, which Azure AD uses to sign the SAML tokens that it sends to the application.

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.

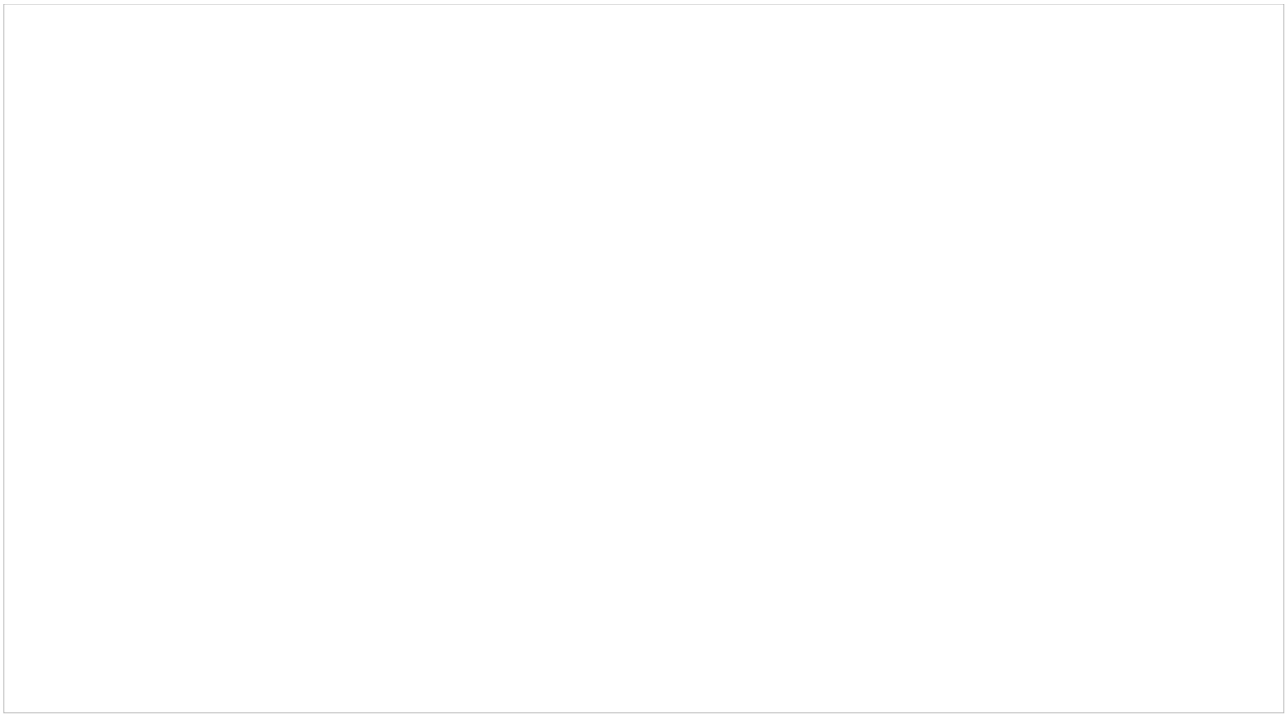
Copy the **Log in URL** value and paste it into a separate text doc. When configuring your SSO integration account in later steps, you will paste this into the *Identity Provider Single Sign-On URL* property in your Bright Pattern SSO integration account.

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.

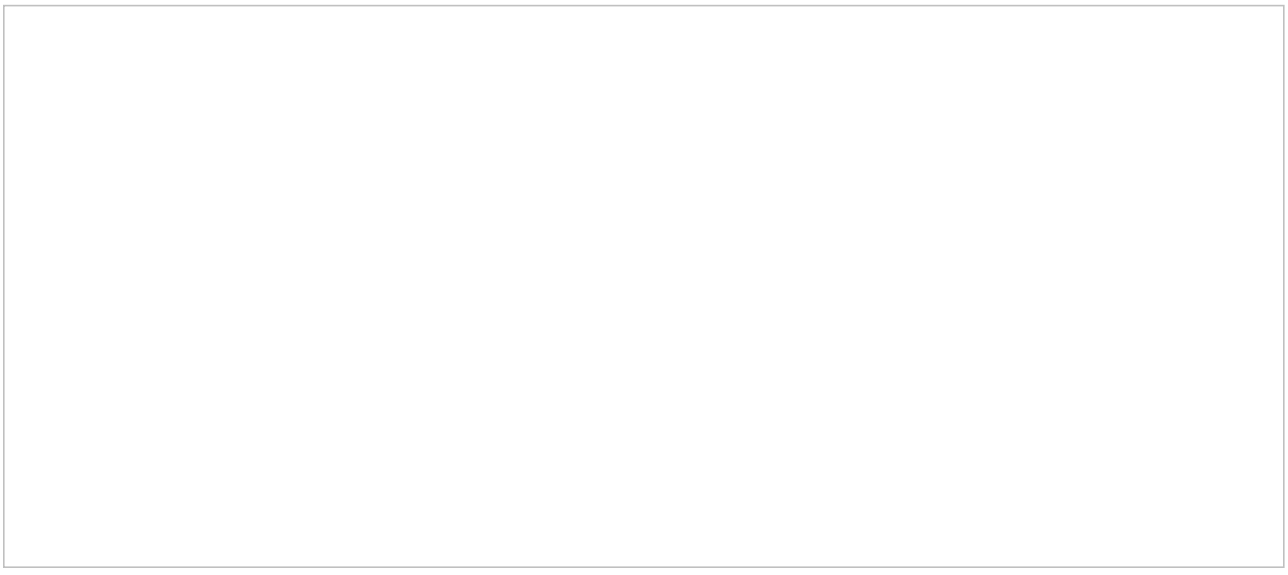
1. Click **Test**.

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*).

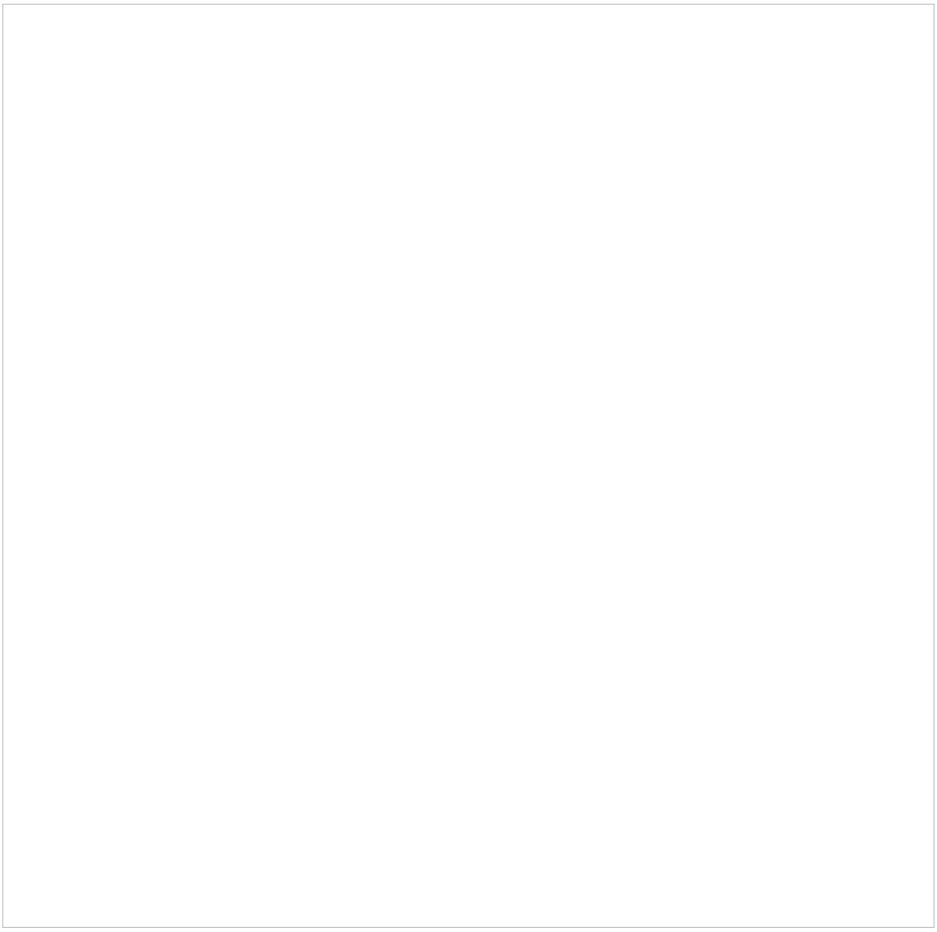


Agent Desktop login

Errors and How to Fix Them

Application with identifier was not found

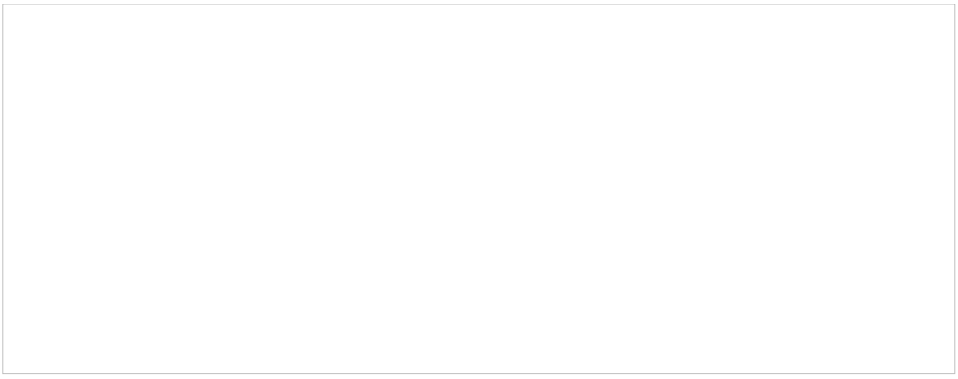
This error means that you are unable to sign in because the application for which SSO is being configured cannot be identified; that is, the Identifier (Entity ID) that you set in Basic SAML configuration is incorrect. Go back to Step 3 of this procedure and make sure that your Identifier is set in the 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**



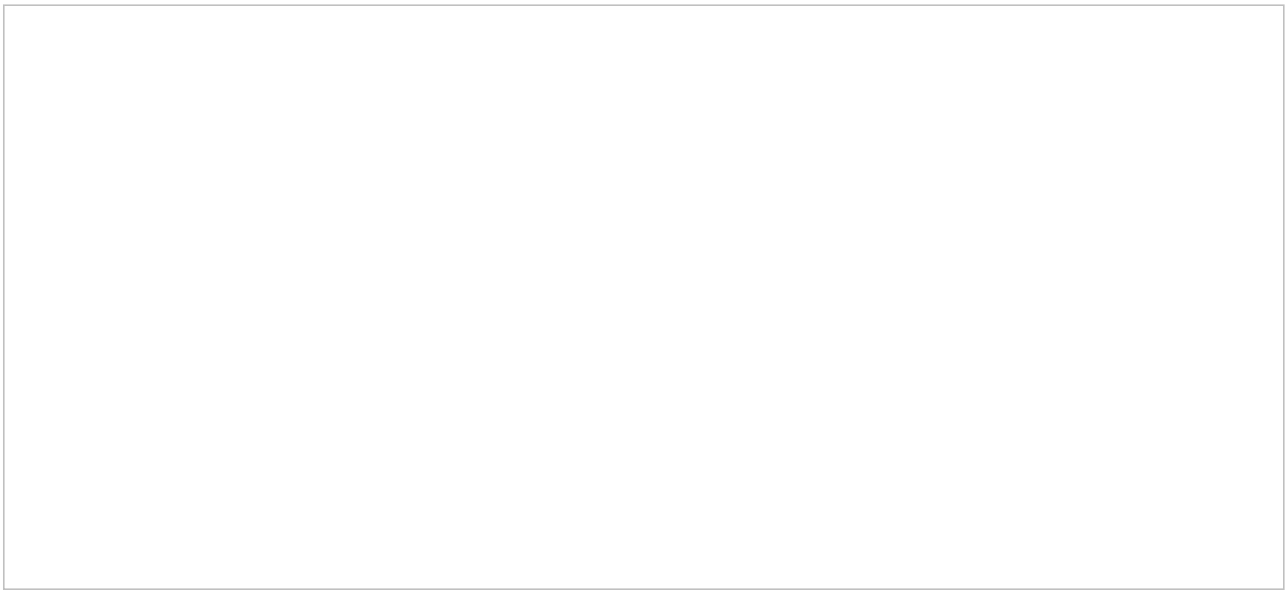
404, Page Not Found

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.



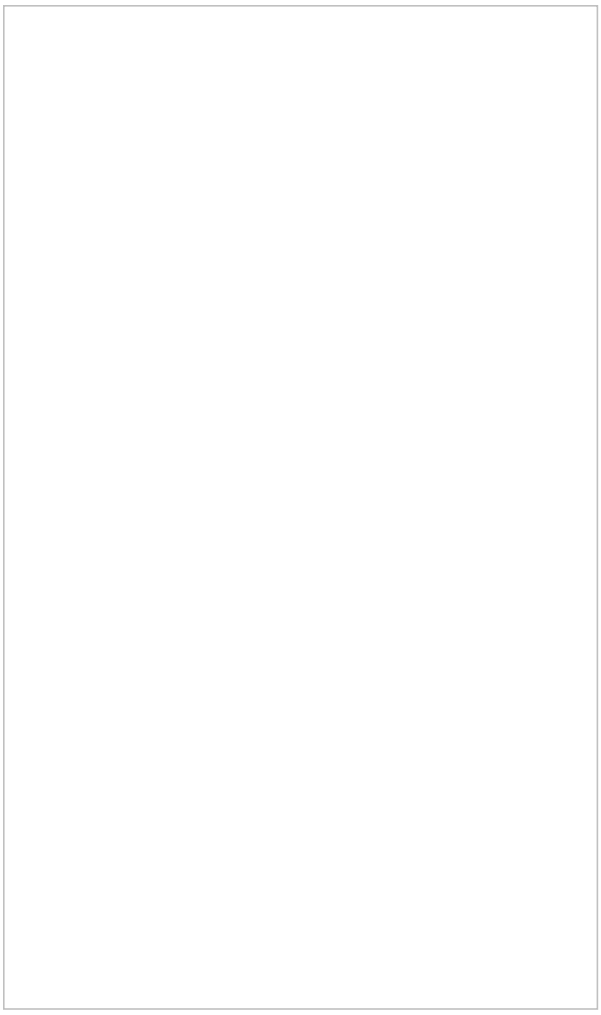
404, Page Not Found

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

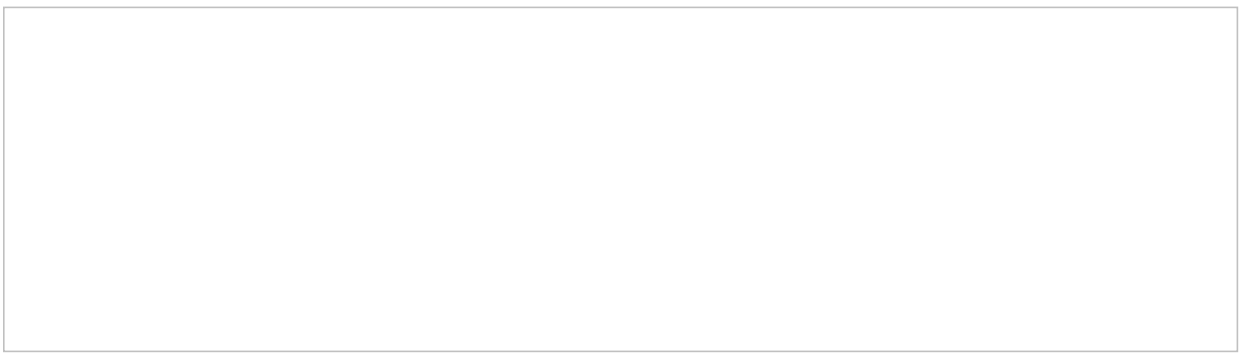
In *Properties*, name the account (any name). The account properties are split into two sections: Agent Desktop SSO and Admin SSO.

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

Add SSO integration account

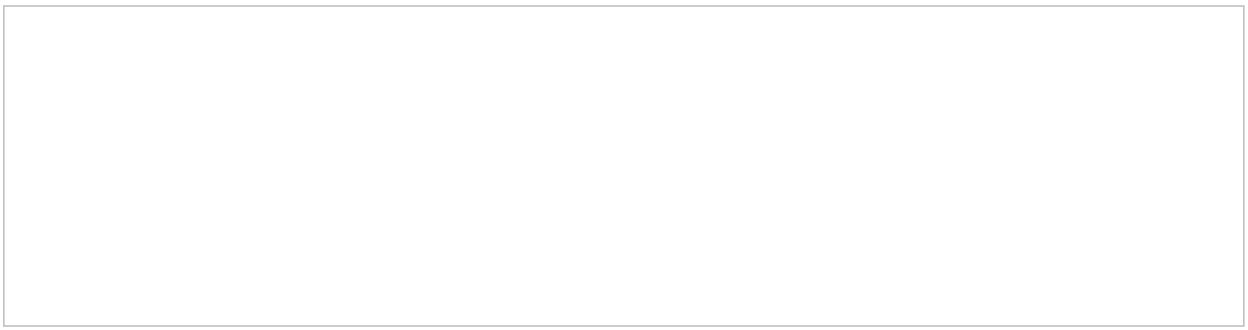
Properties

- **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")



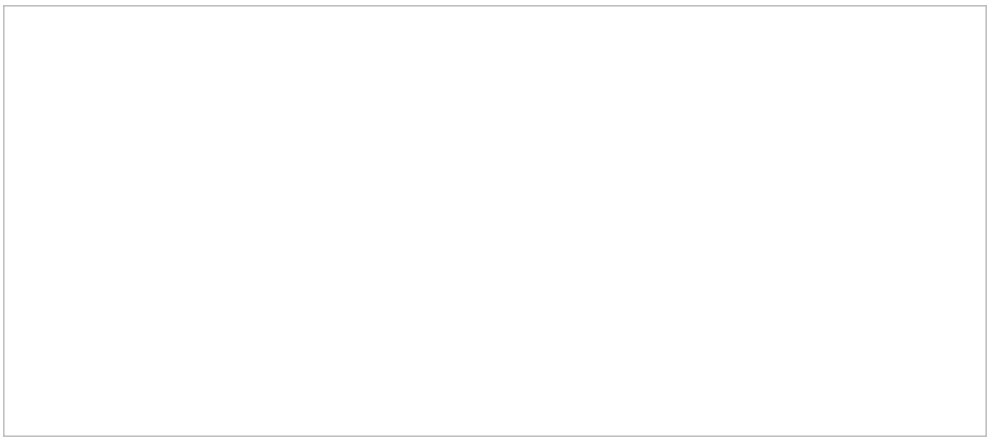
Where to find Login URL

- **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.



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.

Okta SAML 2.0 SSO Integration Configuration

Bright Pattern Contact Center integrates with Security Assertion Markup Language (SAML) 2.0 identity providers like Okta, allowing you to configure single sign-on (SSO) functionality for Bright Pattern's Agent Desktop and Contact Center Administrator applications.

The Okta SAML 2.0 SSO integration supports the following features: SP-initiated SSO and IdP-initiated SSO.

This tutorial provides instructions for how to configure Okta applications to work in an integrated manner with Bright Pattern Contact Center.

You will learn how to:

- Add the Bright Pattern application to your Okta account on the Okta Administrator Dashboard
- Assign users of your organization to the application
- Enable and configure the SAML 2.0 method of SSO for the application
- Use your Okta application credentials to create and configure an SSO integration account in Bright Pattern, as well as enable Just-in-time (JIT) user provisioning

After configuration is complete, users of your contact center will be able to log in to Bright Pattern Contact Center applications without providing Bright Pattern credentials.

Prerequisites

- Have an active Okta account through your organization
- Have access to Bright Pattern Contact Center Administrator and Agent Desktop

Procedure

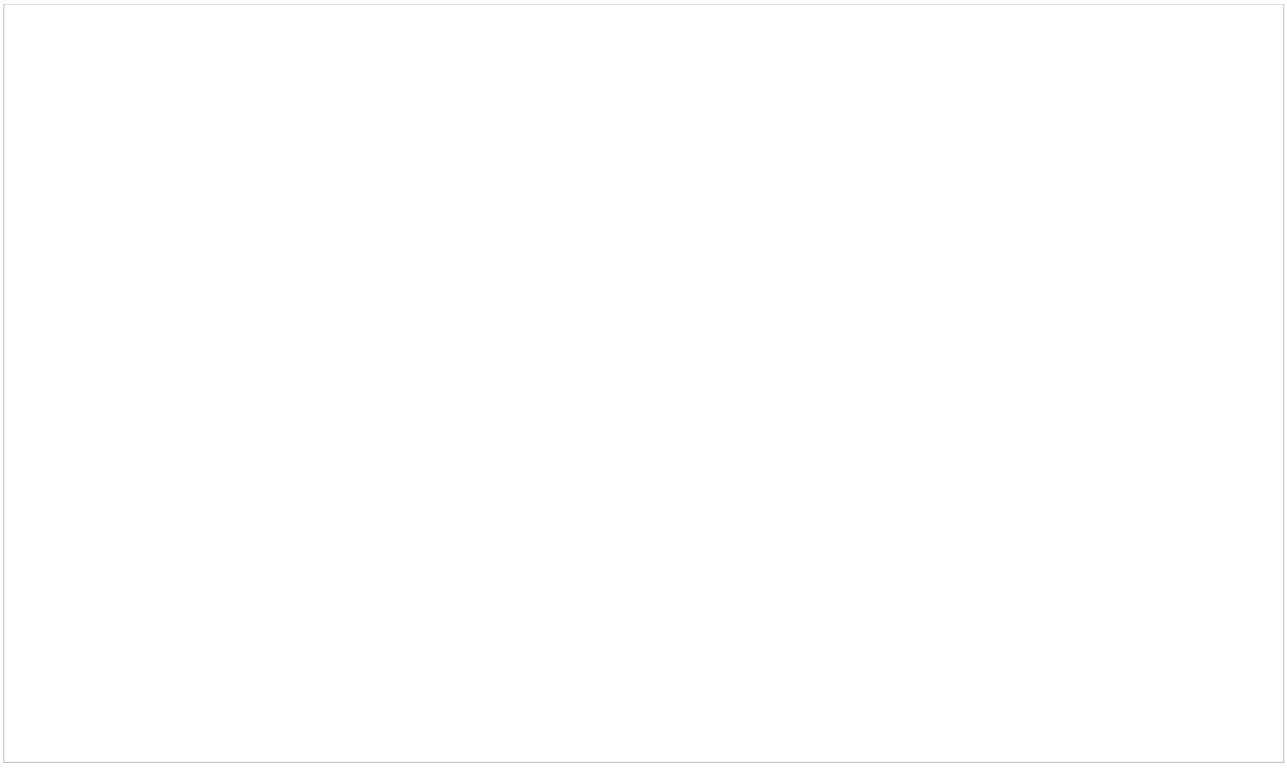
Step 1: Add the Bright Pattern application to your organization's Okta account

1. On the Okta Administrator Dashboard, go to *Applications* and click **Add Application**.
2. In the Search bar, type **Bright Pattern** and select the Bright Pattern app from the list of available apps.
3. Then click **Add**. This adds the application to your Okta account.

Step 2: Set your contact center's domain for the app

On the application's *General Settings* page that opens, set the following options, and then click **Done**:

1. **Application label**- String (any)
2. **Domain** - Your Bright Pattern Contact Center domain name (e.g., "corporation.brightpattern.com")
3. **Application Visibility** - Optional



Application General Settings

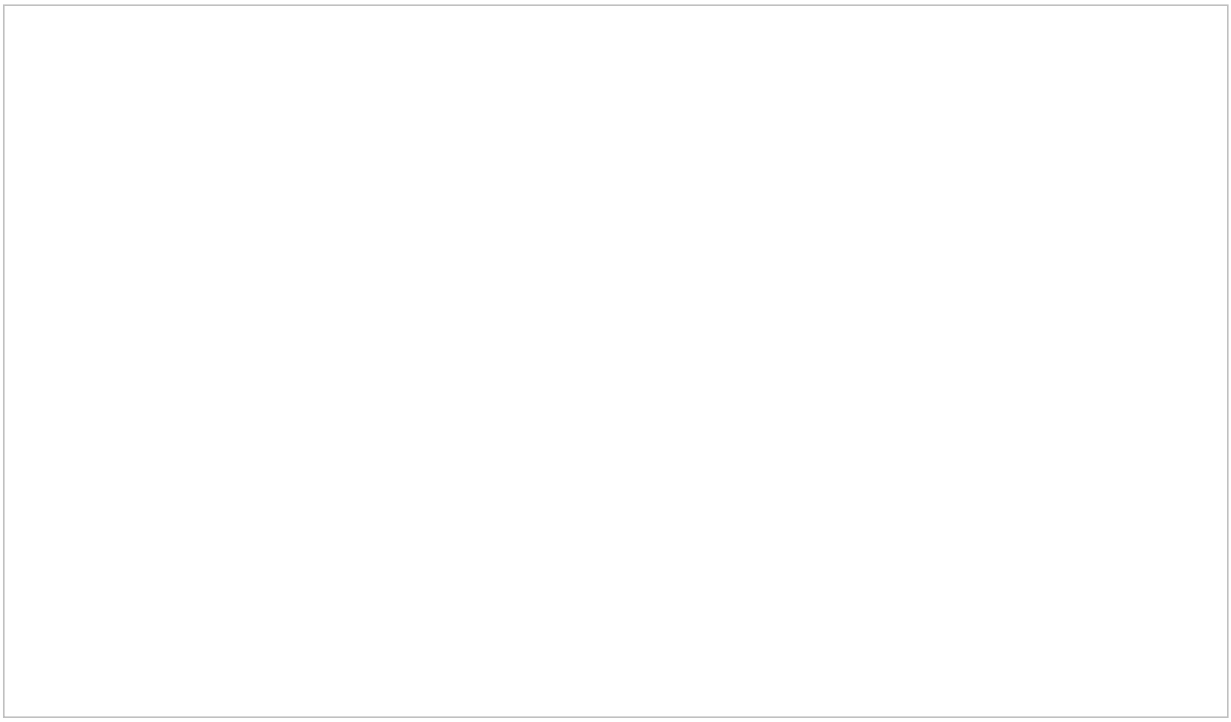
Step 3: Assign users to the app so they can use it

1. Go to the application's *Assignments* tab.

2. Click **Assign** to assign the Bright Pattern application to **People** and/or **Groups**. Note: To do this part of setup, you must first have some users added to your Okta account.

Application Assignment tab

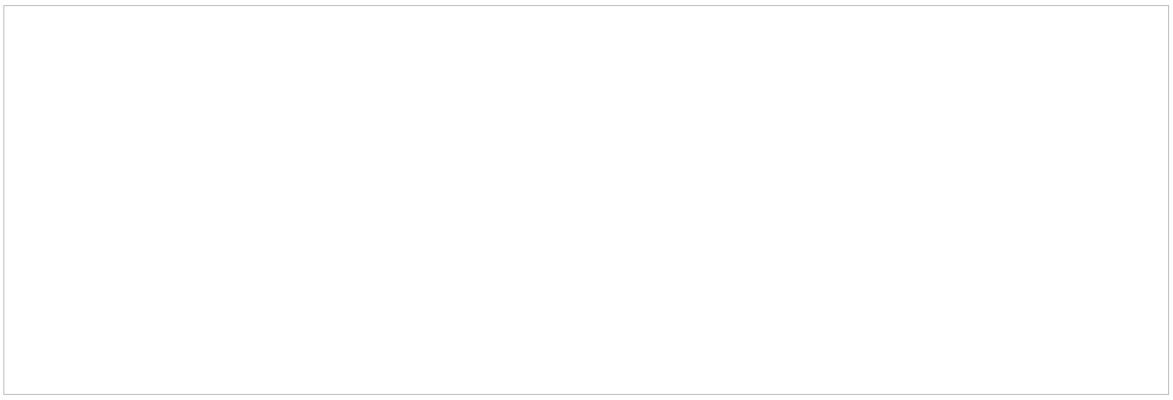
3. Select **Assign to People** or **Assign to Groups**.



Select "Assign to People" or "Assign to Groups"

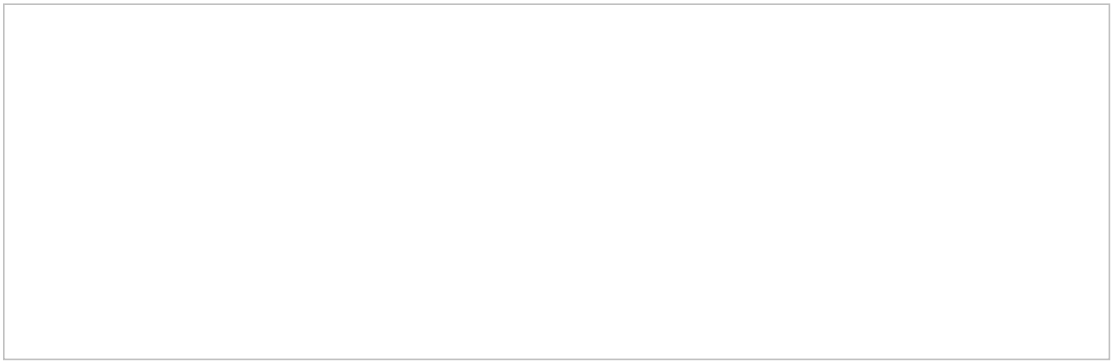
4. If you **Assign to People**, then you also need to click the pencil icon to edit their **User Name**. By default, the

User Name is the person’s email address.



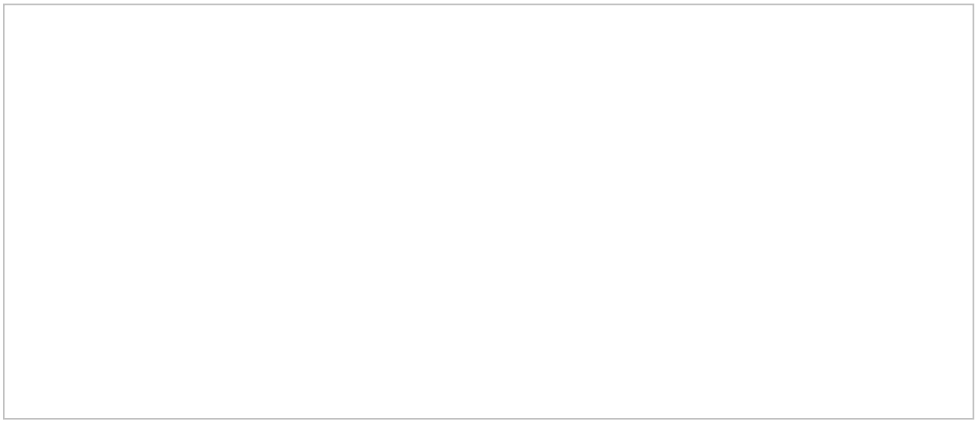
The User Name should be changed

1. In *Edit User Assignment*, change it to match the person’s username as set in Bright Pattern Contact Center.



Change the name to match the person's username format

5. If you **Assign to Groups**, you can easily assign the app to **Everyone** in your organization.



Select "Assign to People" or "Assign to Groups"

Step 4: Configure SSO

1. Go to the app’s *Sign On* tab.

2. In the *Settings* box, in the *SAML 2.0* section, click **View Setup Instructions**.

Click "View Setup Instructions" to set up SAML 2.0

3. This will open a new browser page offering instructions on how to configure SAML 2.0 for your app. This page makes configuration easy because it automatically populates the fields that you need to fill in your SSO integration account properties (in the next step of this procedure), allowing you to copy and paste **Identity Provider Single Sign-On URL**, **Identity Provider Issuer**, and **Identity Provider Certificate**.

4. Now, in a new browser tab, sign in to your Contact Center Administrator application.

5. Go to *Configuration* > *Call Center Configuration* > *Integration Accounts*, and click the **Add account** ("**+**") button.

6. Select **Single Sign-On** as the account type. You will then see the integration account properties.

Single Sign-On integration account properties

7. In Properties, set the following for both *Agent Desktop SSO* and *Admin SSO* sections:
    1. **Name** - Any name for the integration account
    2. **Enable Single Sign On** - Select checkbox
    3. **Identity Provider Single Sign-On URL** - This is generated for you when you click **View Setup Instructions** in *Okta* > *Settings* > *Sign On Methods*.

Where to find the URL for your app on Okta.com

The URL will take the following pattern:
https://<your-organization-name>.okta.com/app/<your-app-name>/<your-app-entity-id>/sso/saml

For example:
https://corporation.okta.com/app/brightpatternapp/exk27skzeeqnKvIy04x6/sso/saml

4. **Identity Provider Issuer** - The ID of Okta, the identity provider. This is also generated for you when you click **View Setup Instructions** in *Okta* > *Settings* > *Sign On Methods*.

   The Identity Provider Issuer will take the following pattern:
   http://www.okta.com/<your-app-entity-id>

   For example:
   http://www.okta.com/exk27skzeeqnKvIy04x6

5. **Identity Provider Certificate** - The certificate contents.

   This is also generated for you when you click**View Setup Instructions** in *Okta* > *Settings* > *Sign On Methods*. Copy the full certificate and paste it into the**Certificate** box.

6. **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).

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

   For *Agent Desktop SSO*, be sure to select a user who is an agent or supervisor.

   For *Admin SSO*, be sure to select a user who is an administrator.

8. Click **Apply** to save your changes.

Step 5: Try logging in to Agent Desktop

Open the Agent Desktop application. You should be able to log in to Agent Desktop without providing Bright Pattern credentials.

Okta SSO integration configuration is now complete.