5.3 Integration Accounts

Bright Pattern Documentation

Generated: 6/14/2021 6:09 am

Table of Contents

Table of Contents 2
Integration Accounts Overview 6
Managing Integration Accounts 7
How to Add a New Integration Account 7
How to Edit an Existing Integration Account 7
How to Delete an Integration Account 7
Notes 8
Amazon AWS Integration 8
Amazon AWS S3 Properties 8
Type 9
Name 9
Use private S3 storage 9
Url 9
Region 9
Access Key ID 9
Secret Key 10
S3 bucket 10
Test Connection 10
Amazon AWS Lambda Properties 10
Type 11
Name 11
Region 11
Access Key ID 11
Secret Key 11
Test Connection 12
Bot / Chat Suggestions Engine Integration 12
AWS Lex Properties 12
Name 12
Type 12
User ID 13
Bot name 13
Bot alias 13
Access key 13
Secret key 13
Region 13
Max API calls per day 13
Watson Assistant Properties 13
Name 14
Type 14
Url 14
Skill ID 14
API Key 14
Max API calls per day 15
Maximum suggestions 15
Test Connection 15
Watson Assistant (Legacy) Properties 15
Name 16
Type 16
Url 16
Skill ID 16
Username 17
Password 17
Max API calls per day 17
Maximum suggestions 17
Test Connection 17
Recommended Reading 17
Co-browsing Integration 17
Properties 18
Name 18
Provider 18
Widget key 18
Test widget key 18
External Knowledge Base Integration 18

Properties 18
Url 19
Consumer Key 19
Application Key 19
Use as exclusive KB 19
Test Connection 19
Loxysoft WFM 19
Properties 20
Name 20
Periodic update interval 20
URL 20
Token 20
Test connection 20
Skills Mapping 21
Messenger Integration 21
Facebook Messenger Properties 21
Page Username 22
Type 22
Page ID 22
Token 22
Webhook Verify Token 22
Generate random token 22
Test Connection 22
LINE Properties 22
Name 23
Type 23
Token 23
Test Connection 23
Nexmo Properties 23
Name 23
Type 24
Key 24
Secret 24
Telegram Properties 24
Bot Username 24
Type 24
Token 24
Set Webhook 24
Test Connection 25
Viber Properties 25
Bot Username 25
Type 25
Token 25
Set Webhook 25
Webhook url (host and port) 25
Test Connection 25
Microsoft Dynamics 365 Integration 26
Natural Language Understanding Integration 26
Properties 26
Name 27
Type 27
Url 27
Authentication method 27
API key 27
Username 27
Password 28
Limit 28
Next Caller Integration 28
Properties 28
Name 28
Sandbox Mode 28
Username 29
Password 29
Test Connection 29
Field Mapping 29
How to Add an Internal Field 29

NICE 29
Properties 30
Name 30
Keep alive update interval 30
Username 30
Password 30
Agent ID prefix 30
Extension prefix 30
URL 31
Remote Assistance Integration 31
How to Add a New Remote Assistance Integration Account 31
Properties 32
Name 32
Default account 32
authorize 32
Username 33
Password 33
Learn More 33
RightNow (Oracle Service Cloud) Integration 34
Salesforce.com Integration 34
SCIM 34
Properties 34
Type 35
Name 35
Default team 35
ServiceNow Integration 35
Single Sign-On Integration 35
Properties 35
Name 36
Enable Single Sign-On 36
Use SSO for administrator portal login 36
Identity Provider Single Sign-On URL 36
Identity Provider Issuer 36
Identity Provider Certificate 36
Enable Just-in-time user provisioning 36
Use Template 37
Speech To Text Integration (STT) 37
Google Properties 38
Name 38
Type 38
URL 38
API key 38
GoVivace Properties 38
Name 39
URL 39
API Key 39
Default account 39
Watson Properties 39
Name 40
Type 40
URL 40
API key 40
Default account 40
Test Connection 40
Statistics Data Receiver Integration 41
Properties 41
Name 41
Protocol 41
Host name 41
Port 41
Teleopti WFM Integration 41
Teleopti WFM Integration Account Properties 42
Name 42
Periodic Update Interval 42

URL 42
Source ID 43
Auth Key 43
Text To Speech Integration (TTS) 43
Watson Properties 43
URL 43
Authentication method 44
API key 44
Load Voices 44
Test Connection 44
Google Cloud Properties 44
Name 44
URL 44
API Key 44
Load Voices 45
Test Connection 45
The Data Group (TDG) Integration 45
Properties 45
Name 45
Username 45
Password 45
API Key 46
Field Mapping 46
How to Add an Internal Field 46
WFM Integration 46
WFM Integration Account Properties 47
Name 47
Periodic update interval 47
Protocol 47
TCP (Aspect WFM) 47
HTTP POST 48
Zapier Integration 49
Properties 49
Name 50
Username 50
Password 50
Zendesk Integration 50

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
- Microsoft Teams
- 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.

Amazon AWS Integration

Amazon Web Services (AWS) integration accounts let you configure your contact center with S3, for storing audio and screen recordings, or with Lambda, for creating and executing custom and/or existing functions.

These integration options must be enabled for your contact center by the service provider. To support BPO operations, multiple integration accounts are possible.

Amazon AWS S3 Properties

Amazon AWS S3 integration account properties

Amazon Web Services (AWS) S3 can be used for storing audio and screen recordings, where files are uploaded to or downloaded from an Amazon S3 account for storage or playback. S3 access credentials are stored in integration accounts in order to enable Interaction Records Search playback for recordings stored in S3.

To support BPO operations, multiple integration accounts are possible.

Note the following:

- This integration option must be enabled for your contact center by the service provider.
- In order to use this integration, you must have an existing AWS account and S3 bucket in which to store recordings. AWS is separate from Bright Pattern.
- Export of recordings is configured for specific services. For more information see Periodic Recording Export Jobs.
- Recordings exported to Amazon AWS will be accessible via Bright Pattern on demand for the detailed records storage time agreed upon with your service provider.
- Instead of using AWS, you can use this integration account to set up an S3-compatible local storage.

For more information about using this type of integration, see the following tutorials:

- 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

Type

The type of integration account: Amazon AWS

Name

The unique name of this integration account. It is helpful to have a descriptive name if your contact center uses multiple integration accounts of the same type.

Use private S3 storage

You can use this option to set up an S3-compatible private storage. For more information see Appendix: Setting up Private S3 Storage.

If you are setting up AWS S3 storage, do not check this box.

Url

This is the URL path to private S3 storage. The URL must be specified if **Use private S3 storage** is enabled.

If you are setting up AWS S3 storage, leave this empty. The URL field is available only if using private S3 storage.

Region

The geographic region in which your S3 bucket exists. You may choose a region from the drop-down menu or type one in. It must be set in the format shown in the drop-down menu (i.e., “us-west-2” and not “US West (Oregon)”).

Access Key ID

The Access Key ID (e.g., AKIAIOSFODNN7EXAMPLE) of the user who has administrator access to AWS services (i.e., in the user's permissions, the user should be added to the Admin group that has the attached policy called "AdministratorAccess").

You can find the access key ID in the*IAM Dashboard > Access Management > Users > Security Credentials tab of the user*.

AWS access keys always consist of an access key ID and a secret access key. The Access Key ID is part of your AWS access key, a security credential created with Amazon Identity and Access Management (IAM) that allows you to sign programmatic requests that you make to AWS if you use the AWS SDKs, REST, or Query API operations. The AWS SDKs use your access keys to sign requests for you.

Secret Key

The Secret Key (e.g., wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) of the user who has administrator access to AWS services (i.e., in the user's permissions, the user should be added to the Admin group that has the attached policy called "AdministratorAccess").

Secret keys are only shown when the user is created. If you do not have the secret key, you should generate a new one in the *IAM Dashboard > Access Management > Users > Security Credentials tab of the user.*

The Secret Key is the other part of your AWS access key. Referred to as a secret access key, the Secret ID is a security credential created with Amazon Identity and Access Management (IAM) that allows you to sign programmatic requests that you make to AWS if you use the AWS SDKs, REST, or Query API operations. The AWS SDKs use your access keys to sign requests for you.

S3 bucket

The exact name of the S3 bucket that stores your data (e.g., photos, videos, documents, etc.) on the cloud. In order to upload or download audio and screen recordings to S3, you must specify the S3 bucket that will be used to hold your data.

Test Connection

Click this button to test the credentials and confirm that the connection is valid.

Possible messages include:

- **Access Forbidden** - This means Bright Pattern cannot access the S3 bucket. Check the S3 bucket's policy in AWS and make sure you have granted permission to an admin user to access it.
- **Credentials are invalid** - This means that the URL, region, access keys, or bucket name are wrong. Check all and try testing the connection again.
- **The credentials appear to be valid** - The connection is OK.

Amazon AWS Lambda Properties

Amazon AWS Lambda integration properties

Amazon AWS Lambda is used for creating and executing custom and/or existing functions (i.e., programs).

In order to use this integration, you must have an existing AWS account and configured Lambda functions. Additionally, this integration option must be enabled for your contact center by the service provider. AWS is separate from Bright Pattern.

For more information about using this type of integration, see the*Amazon AWS Lambda Integration Guide*.

Type

Type is the type of integration account.

Name

Name is the unique name of this integration account. It is helpful to have a descriptive name if your tenant uses multiple integration accounts of the same type.

Region

The geographic region in which your Amazon AWS account exists. You may choose a region from the drop-down menu or type one in.

Access Key ID

The *Access Key ID* (e.g., AKIAIOSFODNN7EXAMPLE) is part of your AWS access key, a security credential created with Amazon Identity and Access Management (IAM) that allows you to sign programmatic requests that you make to AWS if you use the AWS SDKs, REST, or Query API operations. The AWS SDKs use your access keys to sign requests for you.

AWS access keys always consist of an access key ID and a secret access key.

Secret Key

The *Secret Key* (e.g., wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) is the other part of your AWS access key. Referred to as a secret access key, the *Secret ID* is a security credential created with Amazon Identity and Access Management (IAM) that allows you to sign programmatic requests that you make to AWS if you use the AWS SDKs, REST, or Query API operations. The AWS SDKs use your access keys to sign requests for you.

AWS access keys always consist of an access key ID and a secret access key.

Test Connection

This button tests the credentials and confirms whether the connection is valid.

Bot / Chat Suggestions Engine Integration

Bot/chat suggestions engine integration accounts allow you to use third-party bots to automate chat conversations, provide self-service options, intelligently route customers to agents, and provide meaningful suggestions to an agent during active chat sessions.

This version of Bright Pattern Contact Center supports the following types of bot/chat integration: AWS Lex and Watson Assistant.

See [How to Add a Bot/Chat Suggestions Engine Integration Account].

AWS Lex Properties

After you add an AWS Lex account, the Properties dialog will appear. In Properties, you enter the credentials of your Lex bot instance. This allows Bright Pattern to access your bot and use it in chat interactions.

For more information, see *Tutorials for Admins*, section [Set up an AWS Lex Integration Account].

AWS Lex bot/chat suggestions engine integration account properties

Name

The unique name of this integration account (any). Because you can have multiple integration accounts of the same type, it is helpful to have a descriptive, memorable name.

Type

By default, the type is “AWS Lex” because you selected this type when adding the account.

User ID

Your AWS Account ID. Find it in AWS by going to *My Account* > *Account Settings*

Bot name

The bot name (e.g., “TripBooker”); note this may be different than an alias name. Find it in *Amazon Lex* > *Bots (select the name of your bot)* > *Settings*

Bot alias

The alias name (if any); you can add an alias now if you haven’t already

Access key

The access key ID (e.g., AKIAIOSFODNN7EXAMPLE).

You need to set up access key for AWS Identity and Access Management (IAM) service to get this. See Managing Access Keys for IAM Users and AWS Management Console.

Secret key

The secret access key (e.g., wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)

Region

The region for your bot instance (e.g., “US West (Oregon)”)

Max API calls per day

The maximum number of calls that can be done each day. This limit is here to keep your account from being charged for additional calls beyond what is included in a free account.

Watson Assistant Properties

After you add a Watson Assistant account, the Properties dialog will appear. In Properties, you enter the credentials of your Watson Assistant bot instance. This allows Bright Pattern to access your bot and use it in chat interactions.

For more information, see *Tutorials for Admins*, section Set up a Watson Assistant Integration Account.

Watson Assistant bot/chat suggestions engine integration account properties

Name

The name of this integration account.

Type

By default, the type is “Watson Assistant” because you selected this type when adding the account.

Url

The API endpoint of your Watson Assistant Skill (note that in IBM Watson Assistant Skill Details, this URL is called “Legacy v1 workspace URL” or the "Assistant URL").

For example:

https://gateway.watsonplatform.net/assistant/api/v1/workspaces/12c3a41e-ad2e-341c-12d3-412341ffdffd/message

You can find the URL by going to *Skills* > *your skill* > *Options*. Click **View API Details** and then you will see the skill details and service credentials, and you can copy the URL.

Skill ID

The identifying number (string) of your Watson Assistant Skill (i.e., instance). Note that in IBM Watson, skills used to be called workspaces.

To find this ID, go to *Skills* > *your skill* > *Options* and click **View API Details**.

API Key

The API Key (string) used to authenticate the service (e.g., “EEE-MTX13ZS1Ta4pD8qO4rmGP_SXR7HPB8IAAnPgTwKV”).

You can find the API Key by going to *Skills* > *your skill* > *Options* and clicking **View API Details**. The API key is either auto-generated for you or created manually in IBM Cloud, in *Access (IAM)* > *IBM Cloud API keys*.

Max API calls per day

The maximum number of calls that can be done each day. This limit is here to keep your account from being charged for additional calls beyond the first 1,000 that are included in a free account.

Maximum suggestions

The maximum number of suggestions (e.g., 3) that can be delivered to the Agent Desktop during active chat interactions. Suggestions are the bot-generated replies that agents can select and use during chats.

Test Connection

Click to be sure Bright Pattern Contact Center can connect to your Watson Assistant.

If the credentials are invalid, go back to the Url property and make sure you’ve entered it exactly as explained. Test until you see the success dialog: "Account credentials appear to be valid."

Lastly, be sure to click **Apply** at the bottom of the screen to save your account properties.

Watson Assistant (Legacy) Properties

Watson Assistant (Legacy) is the legacy version of IBM Watson Assistant that uses IBM's V1 runtime API and username/password authentication.

Previously, Watson Assistant was called Watson Conversation, and credentials for Watson Conversation included username and password. IBM has since renamed it Watson Assistant and changed its credentials from username/password to API key.

To integrate a legacy Watson Conversation bot, add a Watson Assistant (Legacy) account and edit the Properties of your bot instance as follows. This allows Bright Pattern to access your bot and use it in chat interactions.

For more information, see *Tutorials for Admins*, section Set up a Watson Assistant Integration Account.

Watson Assistant (Conversation) bot/chat suggestions engine integration account properties

Name

The name of this integration account.

Type

By default, the type is “Watson Assistant (Legacy)” because you selected this type when adding the account.

Url

The Legacy v1 Workspace URL of your Watson Assistant Skill.

For example:

https://api.us-south.assistant.watson.cloud.ibm.com/instances/c1f234f5-1d23-4e51-23af-4cef51b2b345/v1/workspaces/012b31f4-51c2-345d-1aad-23e45d123f4d/message

To find this ID, go to *IBM Watson Assistant* > *Skills*, and click **View API details**.

Please note that earlier versions of Bright Pattern Contact Center (earlier than version 5.3.21) required the URL to be in the format “<Legacy v1 Workspace URL>?version=2017-05-26”. Now, “version=2017-05-26” is added by default (so you do not have to append the version to the URL manually). You have the option to use another version from the list recommended by IBM.

Skill ID

The identifying number (string) of your Watson Assistant (Conversation) Skill (i.e., instance). Note that in IBM Watson, skills used to be called workspaces.

To find this ID, go to *IBM Watson Assistant* > *Skills*, and click **View API details**.

Username

The *username* (string) that is used to authenticate the Watson Assistant API. The username is provided in the service credentials for the service instance that you want to use.

If you do not know your username, you can set **apikey** as the username.

Password

The *password* (string) used to authenticate the Watson Assistant API. The password is provided in the service credentials for the service instance that you want to use.

If you do not know your password, you can set your skill's API key.

Max API calls per day

The maximum number of calls that can be done each day. This limit is here to keep your account from being charged for additional calls beyond the first 1,000 that are included in a free account.

Maximum suggestions

The maximum number of suggestions (e.g., 3) that can be delivered to the Agent Desktop during active chat interactions. Suggestions are the bot-generated replies that agents can select and use during chats.

Test Connection

Click to be sure Bright Pattern Contact Center can connect to your Watson Assistant (Legacy).

Recommended Reading

For more information on bot integrations, see:

- How to Create a Watson Assistant
- How to Integrate Bots with Chat
- Set up a Watson Assistant Integration Account

Co-browsing Integration

Co-browsing integration provides co-browsing capabilities during chat sessions to users in the Agent Desktop application (i.e., the ability for an agent and a customer to navigate the same web resource at the same time) via the Surfly co-browsing solution. In order to configure this integration option, this feature must be enabled for your contact center by your service provider first. Additionally, a Surfly account must be configured for your website. For more information, see the *Surfly Integration Guide*.

Co-browsing integration properties

Properties

The properties of the Co-browsing integration account are described as follows.

Name

The name of the integration account (any name).

Provider

The provider of the co-browsing service; the only current option is Surfly.

Widget key

The key (i.e., string) to the provider’s co-browsing widget; in Surfly, the Widget Key is located in section *Settings* > *Integration*.

Test widget key

This button allows you to test the configured Surfly widget key; if the key works, a validation message will pop.

External Knowledge Base Integration

Integration an external knowledge base (KB) enables your Agent Desktop application to use and search a third-party KB. You can search external KB topics, submit new topics, and so forth. The external KB can be enabled as the exclusive KB for Agent Desktop or as a supplementary provider only.

At this time, Bright Pattern integrates with Synthetix. When you add an integration account of type External Knowledge Base, the Synthetix Url will be filled in automatically (see Properties below), and you will add the other credentials for your Synthetix account.

Note that integration accounts of this type are only available to your contact center if they are enabled for your contact center by your system administrator. If *External Knowledge Base* is not listed as an integration account type, the feature is not enabled for your contact center.

Properties

The properties of the External Knowledge Base type of integration account are described as follows.

External Knowledge Base integration account properties

Url

The default value for *Url* is https://api.syn-finity.com/1.1/

Consumer Key

The *Consumer Key* is the consumer key for Synthetix.

Application Key

The *Application Key* is the application key for Synthetix.

Use as exclusive KB

Select the checkbox for *Use as exclusive KB* if you wish the corresponding API to search KB topics, submit new topics, and so forth. If *Use as exclusive KB* is not checked, the external KB will be used as a supplementary provider only (i.e., Agent Desktop will try to use the native KB first and search the external KB if nothing is found in the native KB).

Test Connection

When the *Test Connection* button is clicked, the Test Connection Portal executes GET <URL>/external/views as described at https://www.synthetix.com/api/documentation.

Loxysoft WFM

Integration with the Loxysoft WFM application provides a number of automatically generated reports for workforce scheduling and real-time monitoring of agents' adherence to work schedules. Setup of the WFM integration account is only necessary if you plan to use WFM for real-time adherence monitoring.

Note that you can only have one WFM integration account in your contact center.

Loxysoft WFM integration account properties

Properties

The properties of Loxysoft type integration are as follows.

Name

Name is the name of the integration account.

Periodic update interval

Periodic update interval is the period (in seconds) with which real-time metrics will be updated; the default interval is 10 seconds.

URL

The *URL* field is the unique URL field of your Loxysoft account and the place where the call flow data is submitted to.

Token

This is the authorization token for your Loxysoft account.

Test connection

This button tests the credentials and confirms whether the connection is valid.

Skills Mapping

This box allows you to map service names to corresponding Loxysoft codes.

Messenger Integration

When Bright Pattern Contact Center is integrated with messengers (e.g., Facebook Messenger, LINE, Telegram, Viber, etc.), your Bright Pattern Agent Desktop environment is equipped to handle customer-initiated interactions from the Messenger application or the application on a customer’s mobile phone, tablet, or computer. Incoming chat interactions are routed to the integrated Agent Desktop environment, where agents also have direct access to the phone, live chat, email, SMS text, various other mobile messenger apps, customer and agent records, interaction details, and more. Integration configuration involves linking your organization's messenger account to your Bright Pattern Contact Center tenant.

To add a messenger integration account, click the **add** "+" button and select the desired type of messenger.

Selecting the type of Messenger integration account

The properties of each type of messenger integration account are described as follows. For more information about each type, see the corresponding integration guide.

Facebook Messenger Properties

The properties of the Facebook Messenger type of integration account are described as follows. For complete integration instructions and configuration, see the Facebook Messenger Integration Guide.

Facebook Messenger integration account properties

Page Username

The exact username of your Facebook Page

Type

Select Facebook as the *type* of messenger integration account.

Page ID

The exact page ID for your Facebook Page

Token

The Page Access Token for your Facebook Page

Webhook Verify Token

The token used to confirm that Facebook is the real server, which is needed for Facebook to send you a message from the customer. If you do not have a token, click the Generate random token below.

Generate random token

Creates a random webhook token that you can copy and paste into your Facebook App management page in *Webhooks* > *Edit Page Subscription* > *Verify Token*

Test Connection

Tests the credentials and confirms whether the connection is valid

LINE Properties

The properties of the LINE type of integration account are described as follows. For complete integration instructions and configuration, see the LINE Integration Guide.

LINE integration account properties

Name

The name of your integration account (this does not need to be your LINE@ account name)

Type

For this integration account, select LINE as the *type* of integration.

Token

The access token for your LINE@ account

Test Connection

Tests the credentials and confirms whether the connection is valid

Nexmo Properties

The properties of the Nexmo type of integration account are described as follows.

Nexmo integration account properties

Name

The name of your integration account (can be any name of your choosing)

Type

"Nexmo" by default because you already selected this type of messenger integration account

Key

The API key that was created when you created a Nexmo account. You can find the API key and secret in your Nexmo Dashboard account settings.

Secret

The API secret that was created when you created a Nexmo account. You can find the API key and secret in your Nexmo Dashboard account settings.

Telegram Properties

The properties of the Facebook Messenger type of integration account are described as follows. For complete integration instructions and configuration, see the Telegram Integration Guide.

Telegram messenger integration account properties

Bot Username

The exact username of your Telegram bot

Type

For this integration account, select Telegram as the *type* of integration.

Token

The API token for your Telegram bot

Set Webhook

Click the *Set Webhook* button to confirm that Telegram is the real server, which is needed for Telegram to send you a message from the customer. Note that you must get the token/webhook from Telegram; you cannot generate one here.

Test Connection

Tests the credentials and confirms whether the connection is valid

Viber Properties

The properties of the Viber type of integration account are described as follows. For complete integration instructions and configuration, see the Viber Integration Guide.

Viber messenger integration account properties

Bot Username

The exact name of your Viber Public Account username.

Type

For this integration account, select Viber as the *type* of integration.

Token

The password that is given to you after your Public Account application is approved

Set Webhook

Set Webhook is necessary for Viber to send you a message from the customer. Clicking the *Set Webhook* button opens the Set Webhook window, where the Webhook URL is entered.

Webhook url (host and port)

The address of your server and port number (e.g., “office.yourcompany.com:1234”). If you do not know the server URL or port number, ask your system administrator.

Test Connection

Tests the credentials and confirms whether the connection is valid.

Microsoft Dynamics 365 Integration

Microsoft Dynamics 365 is a cloud customer relationship management (CRM) solution running on Microsoft Azure. Dynamics 365 uses a suite of business applications connected through a common Microsoft cloud platform to provide insights into a business's customers, interactions, and operations.

Through integration, you can access and use Dynamics 365 data in your Bright Pattern Contact Center operations, providing comprehensive customer service to your existing contacts. Our integration enables you to embed Bright Pattern's Agent Desktop widget into your Dynamics 365 environment to get full call and chat capability in your CRM operations. In addition, integration allows contact center users, such as supervisors, to use Dynamics 365 data in contact center operations via a separate, pop-out Agent Desktop.

For integration properties, see the *Microsoft Dynamics 365 Integration Guide*, section Reference: How to Add an Integration Account.

Microsoft Dynamics 365 integration account properties

Natural Language Understanding Integration

Bright Pattern offers IBM Watson Natural Language Understanding integration to provide sentiment analysis for services. Natural Language Understanding is enabled for voice and chat per service and for email in the scenario entry point.

Properties

The properties of the Natural Language Understanding type of integration account are described as follows.

Natural Language Understanding integration account properties

Name

The name of the integration account.

Type

Watson Natural Language Understanding is the type of integration.

Url

Your URL copied from the Natural Language Understanding service credentials.

For example:

https://api.us-south.natural-language-understanding.watson.cloud.ibm.com/instances/1234ede1-23b4-1fb2-ad34-b123afbb4123

Authentication method

Select either **API key** or **username/password (legacy)** to set the appropriate credentials for your Natural Language Understanding service.

API key

The API key from your Natural Language Understanding service credentials.

Username

The username used to authenticate the Watson Natural Language Understanding API with Basic Authentication. The username is provided when you sign up for IBM Bluemix and create an account.

Password

The password used to authenticate the Watson Natural Language Understanding API with Basic Authentication. The password is provided when you sign up for IBM Bluemix and create an account.

Limit

The maximum number of API calls per day. A limit (e.g., “100”) can help keep the number of API calls within the boundaries of free subscriptions. The default is no limit.

Next Caller Integration

Bright Pattern integrates with Next Caller to identify unknown callers from incoming chats, as well as to augment contact data with new information available on the cloud.

Properties

The properties of the Next Caller type of integration account are described as follows.

Next Caller integration account properties

Name

Name is the name of the integration account.

Sandbox Mode

Select the *Sandbox Mode* checkbox if this account is to be used in Sandbox mode.

Username

The *username* (string) is the username used to authenticate the Next Caller API with via Basic Access authentication. The username is provided when you create an account.

Password

The *password* (string) is the username used to authenticate the Next Caller API. The password is provided when you create an account.

Test Connection

The *Test Connection* button tests the credentials and confirms whether the connection is valid.

Field Mapping

Use the Field Mapping tab to add internal fields or external fields to contact data forms. Next Caller will populate these fields with suggested data found on the cloud.

Field mapping

How to Add an Internal Field

1. Click **add**.
2. Click **<none>** to review the *Select Mapping* drop-down selector.
3. Open the Contact folder, and select the desired type of field to add.

Note that only one field can be added at a time. You can select fields from categories (addresses, phone by type, phones by order, social links by order, emails by type, emails by order) or by basic type (Title, First name, Last name, Position, Segment, Summary, Date of birth, Messengers, Status, my_custom_field).

NICE

Bright Pattern offers NICE recording integration to provide quality management (QM) of your call center by allowing reporting on call state and agent messages.

Note that this integration option must be enabled for your contact center by the service provider.

NICE account integration properties

Properties

The properties of the NICE type of integration account are described as follows.

Name

Name is the name of the integration account.

Keep alive update interval

Keep alive update interval sends periodic messages back to NICE servers to ensure the pathway stays open; the default interval is 60 seconds.

Username

The *username* (string) is the username used to authenticate the NICE account. The username is provided when you sign up for NICE and create an account.

Password

The *password* (string) is the password used to authenticate the NICE account. The password is provided when you sign up for NICE and create an account.

Agent ID prefix

The *agent ID prefix* field is where you may specify a prefix for agent ID data. The default values are empty, but if you specify them, Bright Pattern's Real-Time Data Provider server component will add corresponding these prefixes to user IDs whenever it reports them to you.

Extension prefix

The *extension prefix* field is where you may specify a prefix for phone extension data. The default values are empty, but if you specify them, Bright Pattern's Real-Time Data Provider server component will add corresponding these prefixes to extensions whenever it reports them to you.

URL

The *URL* field is the URL the call flow data is submitted to.

Remote Assistance Integration

Remote Assistance integration adds remote desktop support and mobile device support to Bright Pattern Contact Center voice or chat service interactions.

How to Add a New Remote Assistance Integration Account

1. In the Contact Center Administrator application, go to section *Configuration* > *Call Center Configuration* > *Integration Accounts*.

2. Click **+** to add a **Remote Assistance** integration account.

   Select "Remote Assistance" integration account

3. Select account type **LogMeIn Rescue**.

Select "LogMeIn Rescue"

4. Complete the account properties.

5. Click **Apply** at the bottom of the screen to save your changes.

Properties

The properties of the LogMeIn Rescue type of integration account are described as follows.

LogMeIn Rescue integration account properties

Name

The name of the integration account (any name).

Default account

Select the checkbox to set this integration account as the default Remote Assistance account.

authorize

When you first create the integration account, the properties page will display *The integration is not authorized in LogMeIn Rescue*.

Authorization is required for contact centers that allow agents to provide remote assistance during voice and chat services.

Click **authorize** and you will be prompted to set the credentials that the master administrator of LogMeIn Rescue uses to log in to the Rescue Technician Console application.

Note that for this integration, the **master administrator cannot also be a technician**, as the user's email address is used for establishing remote sessions (see *Username* description below).

LogMeIn Rescue User Credentials

Username

The email address of the user who has administrator-level access to the LogMeIn Rescue Technician Console application. The identity of this user is used for setting up and starting sessions for other users/technicians.

Password

Your password for the Rescue Technician Console.

After setting the credentials, the integration account properties page will show that you are authorized to use the account. You may click **re-authorize** to enter your LogMeIn credentials again, if needed.

LogMeIn Rescue integration account properties

Learn More

For more information on LogMeIn integration configuration and usage, see [LogMeIn Integration Quick Start].

RightNow (Oracle Service Cloud) Integration

Integration with Oracle Service Cloud customer relationship management applications provides the integrated Agent Desktop, access to CRM data from scenarios, screen-pop, and activity history functions. You can configure multiple Oracle Service Cloud integration accounts for access to different Oracle Service Cloud systems.

For detailed integration instructions, including specification of the Oracle Service Cloud integration account properties, see Oracle Service Cloud Integration Guide.

Salesforce.com Integration

Integration with Salesforce.com (SFDC) customer relationship management applications provides the integrated Agent Desktop, single sign-on, access to CRM data from scenarios, screen pop, activity history, and click-to-dial functions.

You can also create calling lists using contact records imported from SFDC and export the corresponding campaign results directly to SFDC. You can define more than one Salesforce.com integration account.

For detailed integration instructions, including specification of the Salesforce.com integration account properties, see Salesforce.com Integration Guide.

SCIM

The SCIM (RFC 7643 / RFC 7644) integration account is required for using the BPCC SCIM-Compliant User Provisioning API. Only one SCIM integration account is allowed for your contact center. If the SCIM integration account is not configured for your contact center, the method Create User will fail to process requests.

For more information, see the BPCC SCIM-compliant User Provisioning API documentation on Postman.

Properties

The properties of the SCIM type of integration account are described as follows.

SCIM integration account properties

Type

SCIM

Name

The name of the integration account (any)

Default team

The team to which the new user should be automatically assigned upon creation.

ServiceNow Integration

Integration with ServiceNow IT service management applications provides the integrated Agent Desktop, softphone and click-to-call, access to CRM data from scenarios, screen-pop, and activity stream functions. You can configure multiple ServiceNow integration accounts for access to different ServiceNow systems.

For detailed integration instructions, including specification of the ServiceNow integration account properties, see the ServiceNow Integration Guide.

Single Sign-On Integration

Bright Pattern integrates with Security Assertion Markup Language (SAML) 2.0 identity providers, allowing you to configure single sign-on (SSO) functionality for the Agent Desktop application or the Contact Center Administrator (Admin) application.

Note that only one instance can be created per contact center.

Note that SSO bypass is allowed by privilege. For more information, see section Privileges.

For specific instructions on configuring SSO with specific providers see *Administration Tutorials*, section Integrations.

Properties

There are two types of properties for Single Sign-On integration accounts: Agent Desktop SSO and Admin SSO. You can enable just Agent Desktop SSO functionality and keep Admin login credentials local or you can enable both Agent Desktop and Admin SSO functionality.

Single Sign-On integration account properties

Name

The name of the integration account (any name).

Enable Single Sign-On

Select the checkbox to enable single sign-on functionality for the Agent Desktop application.

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 of your identity provider.

Identity Provider Issuer

The unique identifier of your identity provider.

Identity Provider Certificate

The contents of the SAML certificate that the identity provider uses to sign the SAML tokens that it sends to the application.

Enable Just-in-time user provisioning

Select this checkbox to enable Just-in-time user provisioning (JIT). JIT user provisioning automatically creates call center users on the first SSO login attempt authorized by the identity provider.

Note that JIT is disabled if SSO is not enabled.

You should enable JIT user provisioning if:

- JIT user provisioning is enabled for the application
- The tenant URL is known (extracted from the domain name, tenantUrl parameter, or SAML additional parameter)
- The user with login Id does not exist in that tenant
- SAML assertion is signed and valid

When creating a new user using JIT user provisioning:

- The newly created user should copy assignments (e.g., roles, teams, skills, etc.) from the selected user template
- User contact information should be copied from SAML assertion. As a minimum, this contact information should include first name, last name, login ID, and email address (others are optional)
- Once the user is created, that user should be logged in immediately

Use Template

Select this checkbox to copy assignments (e.g., roles, teams, skills, etc.) from a specific user, and apply them to new call center users created by JIT user provisioning.

Note that SSO templates are required if JIT user provisioning enabled. SSO templates are disabled if JIT user provisioning is disabled.

Speech To Text Integration (STT)

Speech To Text (STT) integration allows your contact center to use speech-to-text functionality to transcribe voice calls and save the transcriptions to interaction records. Full-text transcripts are searchable and include sentiment attributes (if Natural Language Understanding is enabled).

Bright Pattern integrates with STT providers such as IBM Watson, GoVivace, and Google.

Select the type of STT integration

Google Properties

Google's Cloud Speech API converts audio to text. In the Properties dialog, enter the credentials of your Google synchronous STT instance as follows. This allows Bright Pattern to access your STT resource and use it in interactions.

Please note: Google STT requires a payment method to be attached to the account; without this, the STT service would silently not work, and there would be an error in the Google API dashboard.

Google synchronous STT integration account properties

Name

The unique name of this integration account (any)

Type

By default, “Google synchronous STT” because you selected this type when adding the account.

URL

By default, https://speech.googleapis.com/v1/

API key

The service key ID that is used to authenticate Google's Cloud Speech API. This is generated when you get credentials for your service account.

GoVivace Properties

In the Properties dialog, enter the credentials of your GoVivace STT instance as follows. This allows Bright Pattern to access your STT resource and use it in interactions.

GoVivace integration account properties

Name

The unique name of this integration account (any). Because you can have multiple integration accounts of the same type, it is helpful to have a descriptive, memorable name.

URL

By default, wss://services.govivace.com/telephony

STT integration uses the secure WebSocket protocol (i.e., "wss"), so only the *wss://* prefix is allowed.

API Key

The GoVivace API key

Default account

Select the *Default account* checkbox if this integration account is to be the default STT integration account.

Watson Properties

In the Properties dialog, enter the credentials of your IBM Watson STT instance as follows. This allows Bright Pattern to access your STT resource and use it in interactions.

Watson integration account properties

Name

The name of this integration account.

Type

By default, “Watson” because you selected this type when adding the account.

URL

Websocket prefix + your IBM Speech to Text URL in the following format:

For example:

wss://api.us-south.speech-to-text.watson.cloud.ibm.com/instances/1a23456f-121d-4c52-bc06-62168f5a18de

You can find the URL in your IBM Speech to Text service credentials. Note that STT integration uses the secure WebSocket protocol (i.e., "wss"), so only the wss:// prefix is allowed.

API key

The API key (string) for the service instance in your IBM Speech to Text resource, which is used for making secure, authenticated requests.

You can find your API key on IBM Cloud by going to your Speech to Text service credentials.

Default account

Select the *Default account* checkbox to enable the STT integration account.

Test Connection

Click to be sure Bright Pattern Contact Center can connect to your Watson Speech to Text account.

Statistics Data Receiver Integration

Properties

The properties of Statistics Data Receiver integration accounts are described as follows.

Statistics Data Receiver integration account properties

Name

Name is the name of the integration account.

Protocol

The *protocol* is TCP.

Host name

Host name is the host name.

Port

Port is the port number.

Teleopti WFM Integration

Integration with the Teleopti WFM (workforce management) application makes it possible to send real-time agent state data to Teleopti for schedule adherence monitoring via API.

The Teleopti WFM integration account connects Bright Pattern Contact Center to Teleopti WFM using Teleopti-provided authentication credentials like URL and auth key.

For this integration, note the following:

- The feed will provide full updates of all agents every 15 minutes.
- The feed will provide periodic updates at the configured Periodic update interval of agents who have changed their states.
- Updated agent data will include the user's unique ID and their state at the time of the update.
- The feed includes the following agent states:
  - Ready
  - Busy
  - After Call Work
  - Not Ready (or configured/system Not Ready reason)
  - Logged Out

Teleopti WFM Integration Account Properties

The parameters that must be configured on the Bright Pattern side to enable the real-time data feed are described as follows.

Teleoptic WFM Integration Account Properties

Name

The name of the integration account.

Periodic Update Interval

The period (in seconds) in which real-time metrics will be updated.

URL

The URL for the real-time feed, which is provided by the Teleopti application administrator.

Source ID

Source ID (string, 50 character max.) identifies your contact center and is received from the Teleopti application administrator.

Auth Key

The authentication key (string) that is provided by the Teleopti application administrator.

Text To Speech Integration (TTS)

Bright Pattern integrates with text-to-speech (TTS) providers IBM Watson and Google Cloud for creating voice prompts. When text-to-speech functionality is enabled, call prompts may use a variety of pre-recorded voices, accents, and languages to automate responses.

Watson Properties

After you add this TTS account, the Properties dialog will appear. In Properties, you enter the credentials of your Watson Text-to-Speech service.

Watson TTS integration properties

URL

Your unique IBM Text to Speech service instance URL in the following format:

https://api.{location}.text-to-speech.watson.cloud.ibm.com/instances/{instance id}

For example:

https://api.us-south.text-to-speech.watson.cloud.ibm.com/instances/0123a4c0-5d67-8cec-9c10-a0cdbb1234b5

You can find the URL in your Text to Speech service credentials. You must get the URL from your service credentials on IBM Cloud.

Authentication method

API key

The API key (string) for your IBM Text to Speech service instance, which is used for making secure, authenticated requests to IBM Cloud APIs. You can find the API key in your Text to Speech service credentials.

Load Voices

Allows you to choose a voice type from a preconfigured list of IBM voice models. After clicking**Load Voices**, wait a few minutes for confirmation that the voices have loaded. If the field still says "empty", wait a few more minutes and try again.

Test Connection

Tests the connection between Bright Pattern and IBM. When testing the connection, if the account has been configured correctly, you will see the message, "Account credentials appear to be valid."

Google Cloud Properties

After you add this TTS account, the Properties dialog will appear. In Properties, you enter the credentials of your Google Cloud Text-to-Speech service.

Please note: Google TTS requires a payment method to be attached to the account; without this, the TTS service would silently not work, and there would be an error in the Google API dashboard.

Google Cloud TTS integration properties

Name

The unique name of this integration account (any)

URL

https://www.googleapis.com/auth/cloud-platform

API Key

The API key that you created for your Google Cloud APIs and services.

Note that this is not the same as the service key ID.

Load Voices

Load Voices allows you to choose a voice type from a pre-configured list of voices.

Test Connection

Tests the connection between Bright Pattern and Google Cloud. When testing the connection, if the account has been configured correctly, you will see the message, "Account credentials appear to be valid."

The Data Group (TDG) Integration

Bright Pattern integrates with The Data Group (TDG) to identify unknown callers from incoming chats, as well as to augment contact data with new information available on the cloud.

Properties

The properties of the The Data Group type of integration account are described as follows.

TDG integration account properties

Name

Name is the name of the integration account.

Username

The *username* (string) is the username used to authenticate The Data Group REST API. The username is provided when you register for an API key.

Password

The *password* (string) is the username used to authenticate The Data Group REST API. The password is provided when you register for an API key.

API Key

The *API Key* is needed to access The Data Group REST API. The API key is provided after registration.

Field Mapping

Use the Field Mapping tab to add internal fields or external fields to contact data forms. The Data Group will populate these fields with suggested data found on the cloud.

Field mapping

How to Add an Internal Field

1. Click **add**.
2. Click **<none>** to review the *Select Mapping* drop-down selector.
3. Open the Contact folder, and select the desired type of field to add.

Note that only one field can be added at a time. You can select fields from categories (addresses, phone by type, phones by order, social links by order, emails by type, emails by order) or by basic type (Title, First name, Last name, Position, Segment, Summary, Date of birth, Messengers, Status, my_custom_field).

WFM Integration

Integration with the WFM workforce management application provides a number of automatically generated reports for workforce scheduling and real-time monitoring of agents’ adherence to work schedules.

Setup of the WFM integration account is only necessary if you plan to use WFM for real-time adherence monitoring. Typically in this case, the Universal interface of the Aspect Real-Time Adherence server (RTA) must be configured to be ready to receive a data feed. For more information, please refer to the *Aspect Workforce Management 7.5 Installation Guide*, chapter *Configuring ACD Instances*, section *Universal ACD*. Note that the *Unicode* checkbox of the Universal interface must be selected (the ASCII option is not supported).

Note that you can only have one WFM integration account in your contact center.

WFM Integration Account Properties

The parameters that must be configured on the Bright Pattern side to enable the real-time adherence data feed are described as follows.

Name

Name is the name of the integration account.

Periodic update interval

Periodic update interval is the period (in seconds) with which real-time metrics will be updated.

Protocol

Protocol refers to the communication protocol, which is read-only. Two options are available: TCP (Aspect WFM) and HTTP POST.

TCP (Aspect WFM)

If TCP (Aspect WFM) is selected, the following options appear:

- **Host name** - The name or IP address of the host where the Aspect Real-Time Adherence server (RTA) is run
- **Port** - The TCP port assigned to the Aspect RTA server on the above host; it must correspond to the port configured on the RTA side
- **Record field sizes** - The property that specifies the lengths of the data fields communicated to Aspect RTA; the default values correspond to the default settings of the same fields on the RTA side; if values of these fields are changed on the RTA side, they must be changed accordingly in this property
- **Reason codes mapping** (optional) - This box allows you to configure Not Ready reasons as numerical codes for WFM reports. In Bright Pattern Contact Center software, reason codes are defined as text. Aspect WFM only accepts reason codes as numbers. If you need to account for reason codes in your real-time reporting on the WFM side, this box allows you to define a numerical code corresponding to each *Not Ready* reason code, as shown in the picture.

WFM TCP protocol settings

HTTP POST

If HTTP POST is selected, the following options appear:

- **URL** - The unique URL of your WFM account
- **Token** (optional) - The access token for your WFM account
- **Test connection** - This button sends POST with an empty agent and services list
- **Reason codes mapping** (optional) - This box allows you to configure Not Ready reasons as numerical codes for WFM reports.

HTTP POST protocol settings

When enabled, POST is sent to the provided URL. Errors are ignored, and the next request is done after the defined interval.

Zapier Integration

Integration of the BrightPattern workflow engine with Zapier lets Zapier use your contact center's data to automate workflow events called "zaps." Zapier integration configuration involves adding a Zapier integration account and defining how data is retrieved in scenarios.

Properties

The properties of the Zapier type of integration account are described as follows.

Zapier integration account properties

Name

Name is the name of the integration account.

Username

The *username* (string) specifies a username that Zapier will use to access data.

Password

The *password* (string) specifies a password that Zapier will use to access data.

Zendesk Integration

Integration with the Zendesk customer relationship management application provides the integrated Agent Desktop, single sign-on, access to CRM data from scenarios, screen pop, activity history, and click-to-dial functions. You can configure multiple Zendesk integration accounts for access to different Zendesk systems.

For detailed integration instructions, including specification of the Zendesk integration account properties, see Zendesk Integration Guide.