5.8 Scenario Entries

Bright Pattern Documentation

Generated: 1/29/2022 6:55 am

Table of Contents

Scenario Entries Overview

The logic of automated interaction processing is defined in [scenarios](). Execution of a scenario with respect to a specific interaction is triggered by an interaction arrival at a specific *access point* (e.g., a phone number in the case of inbound calls, or a web page in the case of web chats). The logical entities that associate specific scenarios with access points are called *scenario entries*.

Sections

The following sections are found in the Contact Center Administrator application, section Scenario Entries.

- [Dial-in]()
- [Messaging/Chat]()
- [Web Callback]()
- [Email]()
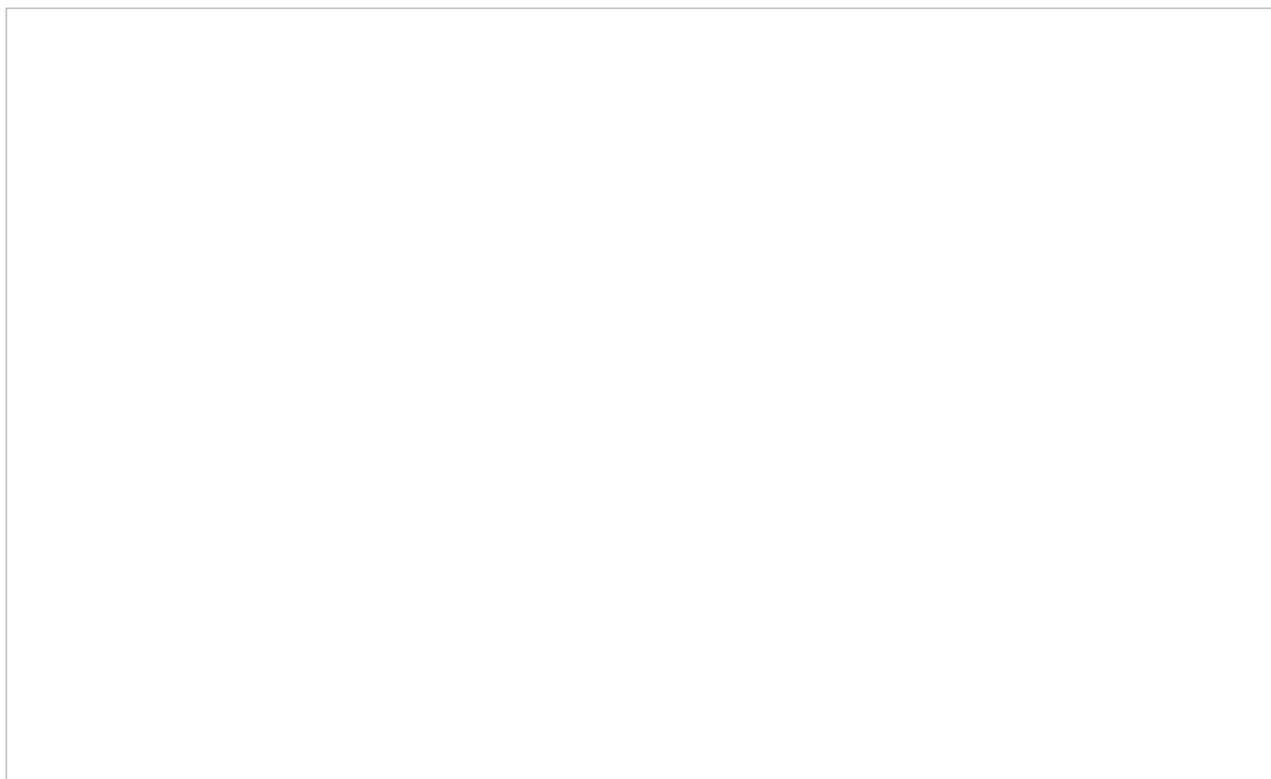
Scenario Entries overview

Dial-in

The logic of processing a phone call is initially determined by the phone number to which this call is delivered. Call arrival activates a [scenario](#) associated with that number. The scenario controls all further steps of call qualification and distribution until the moment when the call is answered by an agent (or sometimes self-serviced). The logical entity that describes the association between a phone number and a call-processing scenario is called a *dial-in scenario entry*.

To set up and manage such associations, select the **Dial-in** option from the *Scenario Entries* menu.

Scenario Entries > Dial-in

Dial-in Scenario Entries Screen Properties

The *Dial-in Scenario Entries* screen properties are described as follows.

Name

Name is the name of the dial-in scenario entry. This field is mandatory and must be unique within the contact center.

Scenario

Scenario is the [Voice scenario](#) that will process calls arriving at the phone numbers defined in this dial-in scenario entry (see below).

Service

Service refers to the service associated with the dial-in scenario entry. Such direct association between telephone number and a service can be used when your access numbers directly identify your services.

Even if you use one access number for many different services (i.e., use an interactive voice script within the associated scenario for service selection), you may still assign a default service directly to the access number in order to account for the calls abandoned before service selection and for the calls that bypass the service selection stage (e.g., someone is unable to use the keypad to enter service selection choice, or someone is confused about which option to choose).

Hours of Operation

Hours of operation (HOP) is a schedule that defines service hours for each day of the year.

- Choose **from service** to use [HOPs of the services](#) associated with interactions processed by the given scenario.
- Choose **select** to select one of the [preconfigured HOPs](#).
- Choose **specify** to define a new HOP specifically for this scenario entry.

Unless you create an entry point for a 24/7 operation, the scenario that you have specified in the *Scenario* property above must define processing of interaction arriving at this entry outside as well as within the specified hours of operation. That is, the scenario should normally begin with an [If](#) block that has the condition *The current date and time is* (or *is not*) *in hours of operation.* For more information, see the [example](#) provided in the *Scenario Builder Reference Guide*.

HOPs can also be [specified at the service level](#).

Note the following:

- If you use options *select* or *specify* to define HOP for this scenario entry, all possible HOP checks within this scenario will use the HOP defined for this entry. Any HOPs specified for any services within this scenario will be disregarded.

- If you use option *from service*, the HOP check will use the HOP of the service that is associated with the interaction at the time when the check is performed. By default, this is the *Service* configured for this scenario entry (see above). However, if the service is redefined within the scenario, a subsequent HOP check will use the HOP of that new service.

- If you (1) use option *from service*, (2) do not have any *Service* configured for this scenario entry, and (3) use an HOP check before any explicit service assignment within the scenario, all incoming interactions will be treated as if they arrived outside of the service hours.

- This HOP setting only specifies when the services provided via this scenario entry are open/closed. In order to complete the HOP configuration, you need to define the following additional elements in the assigned scenario:
    - Checking whether interactions arrive within or outside the HOP. Use the [If](#) scenario block for this purpose with the following condition: *"The current date and time" "is not" "scenario default hours of operation"*.
    - Specifying the action to be applied to interactions if the above condition is met (e.g., [play an announcement](#) and [exit](#) or offer [voicemail](#)).

Internal numbers

Internal numbers are the numbers associated with this scenario. Although service calls normally arrive at [external access numbers](#), you can also set up an internal number to enable agents to transfer calls to this scenario entry. Once assigned, a number cannot be associated with any other scenarios.

Specification of an internal number for a dial-in scenario entry is optional. Note, however, that if you specify an entry without an internal number, it will not be displayed in the *Dial-in Scenario Entries* list. You will be able to see such an entry point in the list of [external access numbers](#) only.

External numbers

These are the [external access numbers](#) associated with the scenario. Select the desired number from the drop-down list. If the number is already assigned to another scenario or to an extension number, the drop down list will provide this information. Once assigned, a number cannot be associated with any other scenarios.

Note that the system allows you to define more than one access number within the same scenario entry point. This may be useful, for example, if you intend to provide your customers with a choice of numbers depending on where they call from, while otherwise applying exactly the same processing logic to all such calls.

Requested skills

Requested skills are the [auxiliary skills](#) and [language skills](#) that the agents must possess in order to handle calls arriving via this scenario entry. By defining such skills externally, you can use the same scenario in multiple scenario entries that differ only in auxiliary or language skills. For example, for your technical support service, you can have separate numbers for Product A support and Product B support, where Product A and B are defined as two different auxiliary skills defined for two different scenario entries associated with the same scenario.

Mute IVR toward agent when conferenced

Select this checkbox if you do not wish the agent to hear IVR prompts when on a conference call with a customer and an IVR. This setting can be used if a conferenced IVR contains prompts confirming sensitive data (e.g., credit card information) received from the customer.

Mute DTMF toward agent when conferenced

Select this checkbox if you do not wish the agent to hear the dual tone multi frequency (DTMF) touchtones when the agent is on a conference call. This setting can be used if a conferenced IVR expects the customer to enter sensitive data (e.g., credit card information) using the DTMF keys of their phones.

Queuing priority

Queuing priority refers to the queuing priority of interactions arriving through the scenario entry. Priority determines how fast these interactions will move through the queue relative to interactions arriving through other scenario entries when they compete for the same agents.

The possible value range for priority is from 0.01 to 100. The recommend value range is from 0.1 to 10. Decimals are permitted.

Note that the maximum recommended priority value is 10. If priority is set too high, then the system can wait for the next available agent and will not offer callback if the [Virtual Queue](#) option is enabled.

Note that queuing priority set by the [Set Priority scenario block](#) overrides the priority that may be preconfigured at the scenario entry level.

Consider the following examples:

- Your platinum-level customers are served by the same agents as all other customers, but you may give them a different number to call the same service. In this case, you may define two different entries for the same scenario with a higher queuing priority for the platinum customers.
- You want to make sure that customer calls internally transferred via queue are answered as soon as possible. In this case, you may define a separate entry for internally transferred calls with a higher priority.

For more information and examples of how priority works, see section Set Priority of the *Scenario Builder Reference Guide*.

Visible to agents

Visible to agents provides indication of whether this scenario entry shall appear in the Agent Desktop directory. Select the checkbox if you want your agents to be able to make blind transfers to service queues via this scenario entry.

Directory folder

Directory folder is the folder of the Agent Desktop directory where this scenario entry will appear if enabled by the previous option. You can select an existing folder or define a new one.

Scenario parameters

Bright Pattern Contact Center scenario language has a number of variables that can be set to different values depending on the scenario entry where this scenario is used. If such variables are present in the scenario selected for this entry, they will appear under this option and can be set to the values specific to the given scenario entry. Use of such externally defined variables enables you to have fewer scenarios because they can be re-used for various scenario entries. For more information, see the description of variable *$(app.custom.XXX)* and voice segment type *Voice, from parameter* in the *Scenario Builder Reference Guide*.

Messaging/Chat Scenario Entries

Messaging/Chat scenario entries are used to associate scenarios with contacts requested via mobile and web applications.

To set up and manage such associations, select the **Messaging/Chat** option from the *Scenario Entries* menu.

Scenario Entries > Messaging/Chat

Messaging/Chat Scenario Entries Screen Properties

The *Messaging/Chat Scenario Entries* screen properties are described as follows.

Name

Name is the name of this messaging/chat scenario entry. This field is mandatory and must be unique within the contact center.

Unique identifier

The *Unique identifier* is generated by the system for this scenario entry. This identifier must be used as *Application ID* in the mobile and/or web applications that will connect to your contact center via this scenario entry. For more information, see section [General Information](#) of the Bright Pattern *Mobile/Web API Specification*.

Scenario

Scenario is the [Chat scenario](#) that will process chat requests arriving via this entry point.

Service

This is the *service* associated with this scenario entry. Entering a service is optional. See the corresponding description for the [Dial-in](#) scenario entries for more information.

Default service for voice callback

Select the voice service to be used when a customer requests a voice callback during a mobile or web chat interaction. The *Default service for voice callback* drop-down menu displays the voice services that have been added to [Services & Campaigns](#).

Send read-by-agent notifications

This option allows the Agent Desktop application to send chat message delivery receipts and/or chat message read receipts to customers.

Delivery receipts are sent immediately when chat messages are delivered to the Agent Desktop application (i.e., even if it is in the background or minimized).

Read receipts are sent when:

- The Agent Desktop application is in the foreground
- The chat session is active (i.e., assuming there is more than one active session)
- The UI control displaying the message is visible to the logged-in user

Hours of Operation

Hours of Operation (HOP) refers to the schedule for this scenario entry point. This field is optional. See the corresponding description for the [Dial-in](#) scenario entries for more information.

Web HTML snippet

Web HTML snippet provides access to the web elements of the chat application that customers will use to access your contact center via the given scenario entry.

You can either use an out-of-the-box chat application hosted by your service provider, or you can create your own application.

To use the out-of-the-box application, click the **HTML snippet** button, **copy** the HTML snippet code, and embed it into your web page(s). Normally, it is not necessary to change the default **client web server hostname**. You will do so only if instructed by your service provider.

To create your own application with the full chat code, click the **Client application** button. A zip file with the code of the out-of-the-box application (see above) will be downloaded to your computer. You can modify this code to match the look and feel of your company website, and implement additional application functionality using the Mobile/Web API.

Requested skills

Requested skills are the auxiliary skills and language skills that the agents must possess in order to handle chats arriving through this scenario entry. This field is optional. See the corresponding description for the Dial-in scenario entries for more information.

Parameter expected

A *parameter expected* is the parameter that may be expected by the scenario in session requests coming from the mobile applications (e.g., customer's name). Such parameters are optional. They may be used, for example, to look for the most qualified agents to handle the requested chat sessions and/or to display user information for the agents. For more information, see section Expected parameters of the *Mobile/Web API Specification*.

To define a new parameter, click **add**, select the parameter type, and specify its name. To edit or remove existing parameters, hover over their names.

SMS/MMS access numbers

Bright Pattern Contact Center enables customers to request and carry on chat conversations via SMS or multimedia messaging service (MMS). Such chat requests are initially made to a dedicated access number. Subsequent treatment of such requests, including routing, Agent Desktop, and reporting, is no different from the processing of regular chat sessions.

Use this setting to specify the number that the customers will use to initiate such SMS/MMS chat conversations. Note that this must be an enabled access number assigned to you by the service provider and dedicated to SMS/MMS communications (i.e., an access number that appears in the *[number]/SMS/MMS* format in the Access Numbers list view).

You can assign more than one access number to one scenario entry, but the same number cannot be assigned to multiple entries.

Messenger Accounts

Agents can participate in live chats initiated from a customer's messenger account (e.g., Facebook Messenger, LINE, Telegram, Viber, etc.). Messenger integration accounts that are configured for your call center can be selected from the *Messenger accounts* drop-down menu. To add a messenger account to your Messaging/Chat scenario entry, click **add** and select the desired account.

Bot / Chat suggestions engine

Our system integrates with chat bots to provide meaningful suggestions to an agent during chat session, as well as bot functionality for customers to complete self-service tasks without the assistance of a live agent. From the *Bot / Chat suggestions engine* drop-down menu, you can select one *bot / chat suggestion engine* integration account as a suggestion engine per service. One such integration account can be selected as chat bot on the chat service launch point. The default engine is *None*.

Note that selecting a suggestions engine here will override suggestions engine selections made in the scenario associated with this scenario entry. For more information, see the *Scenario Builder Reference Guide*, section Chat Bot Select Account.

Enable co-browsing

When enabled, this option allows an agent and a customer to navigate the same web resource at the same time during a chat session.

Co-browsing account

When co-browsing is enabled, you may choose the method by which agents will co-browse with customers during chat sessions. You may choose from the list of available integration accounts (e.g., Surfly) or the built-in Bright Pattern Contact Center version, TogetherJS.

Connect agent by phone automatically

Any mobile application contact is initially presented to the agent as a chat request. However, if the mobile application transmits the customer's mobile phone number, this number will be displayed at the Agent Desktop, and the agent can call the number to establish a voice call with the customer. Select the *Connect agent by phone automatically* checkbox if you wish for such voice calls to be initiated automatically whenever the phone number is available.

Connect after delay of

If you selected the *Connect agent by phone automatically* checkbox, you can define how quickly the automated call to the customer mobile number will be initiated. A slight delay may be desirable if, for example, the agent needs some time to review information that comes with the original request.

Queuing priority

Queuing priority is the priority of interactions arriving through this scenario entry. This field is optional. See the corresponding description for the Dial-in scenario entries for more information.

Chat nick for system messages

Chat nick for system messages is the name that will be displayed to the customers when they get automated chat responses through this scenario entry (e.g., during an initial data collection stage). By default, this is the name of your contact center (tenant name) that is defined at the service provider level.

Override agent name if nickname is not set

When this setting is checked, the name defined in the setting's edit field will be displayed to customers using the chat widget (i.e., if the agent's *chat nickname* was *not* defined). Leaving this setting unchecked allows the chat widget to display either the agent's *chat nickname* or first and last names (i.e., if the *chat nickname* is not defined). This setting is checked for any new messaging/chat scenario entries; it is unchecked by default for existing entries.

How long an agent could wait for reply before chat times out

This is the amount of time (in minutes) that an agent could wait for a reply before the chat interaction expires. It can be redefined for each Messaging/Chat scenario entry separately.

This setting overrides the Customer Inactivity Timeout setting.

How long a client browser may stay unresponsive before chat times out

This is the amount of time (in minutes) that the client's browser may stay unresponsive before the chat interaction expires.

Visible to agents

Visible to agents indicates whether this scenario entry shall appear in the Agent Desktop directory. See the corresponding description for the [Dial-in](#) scenario entries for more information.

Checking this box enables agents to transfer chats to another chat directory. In order to be able to transfer chats to another chat scenario, the Messaging/Chat scenario entry must be updated to be visible to agents and have a directory that is named for the transfer. For more information on how agents transfer chats, see the *Agent Guide*, section [How to Transfer Your Chat Session](#).
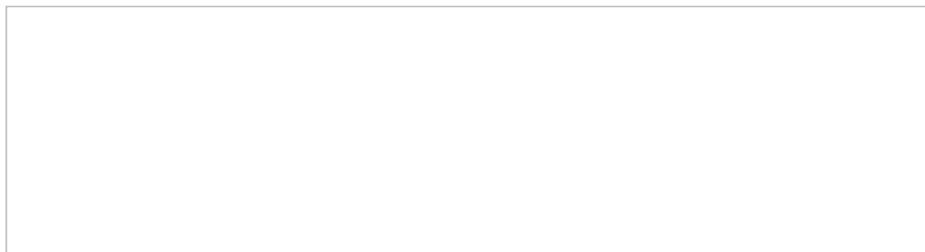
Check "Visible to agents" and add directory to enable agent chat transfer

Directory folder

Directory folder is the folder of the Agent Desktop directory where this scenario entry will appear if enabled by the previous option. See the corresponding description for the [Dial-in](#) scenario entries for more information.

Scenario parameters

Scenario parameters are optional. See the corresponding description for the [Dial-in](#) scenario entries for more information.

Chat session icon

The *chat session icon* appears in the customer-facing chat window during active chat sessions. You have the option of uploading an icon (e.g., logo, photo, etc.), which will be seen in chat windows for all customers interacting with agents in your tenant. If uploaded, this icon overrides photos that agents have uploaded to their [User Profile](#) in the Agent Desktop application, which are normally seen by customers in their active chat windows.

Leaving this field empty or removing a chat session icon allows chat windows to display the photo that an agent has uploaded to his or her *User Profile* (if available).

For example, agent Christy Borden has uploaded a photo to her *User Profile*, as shown. The agent's uploaded photo appears in the customer's active chat window.
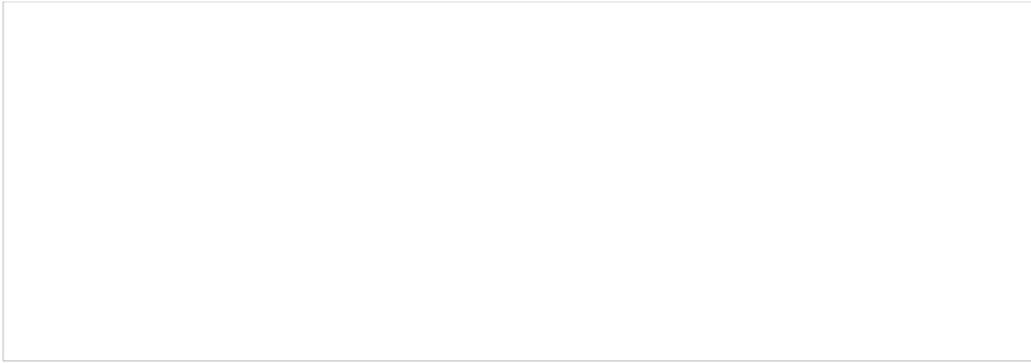
Agents can upload photos or icons to their User Profiles in Agent Desktop

Uploading a chat session icon causes the agent's photo in the chat window to be replaced by the icon that you uploaded. Note that you must click **Apply** to save your changes. Also note that the chat session icon that you upload does not override agents' *User Profile* photos--only the display photos shown in active chat windows.
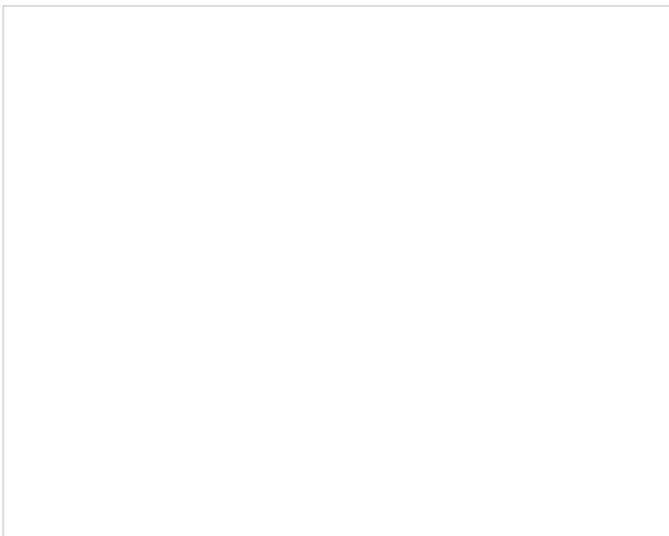
To upload a chat session icon, click Upload and then
click Apply

In all new chat interactions, the customer's chat window will display the chat session icon that you have uploaded. In addition, web notifications that pop on agent replies when the visitor's browser window with chat is minimized, or overlapped by other windows, will also contain the chat session icon for all agents.

Co-browsing

During a web chat, co-browsing functionality allows the agent to view the customer's screen and follow the customer's scrolling movements. Co-browsing is initiated during the chat when the customer--not the agent--clicks the co-browsing ☐ icon. Screen sharing ends when either the customer clicks the icon ☐ or when the chat is terminated. For more information, see the *Agent Guide*, section [Co-browsing](#).

Mobile

If your contact center utilizes a mobile/chat application that was developed from a Bright Pattern Contact Center SDK (iOS or Android), the *Mobile* tab is where settings for sending push notifications to the chat customers are defined.

Mobile tab properties

How long a mobile application may be inactive or locked before chat times out

This setting allows you to define an application timeout (in minutes) for inactive or locked device screens; the default is 30 minutes.

Apple iOS push notifications

In order to make push notifications appear on a user's Apple iPhone, a specific Bright Pattern Contact Center (BPCC) server passes requests to either an Apple Push Notification service (APNs) server or a Firebase Cloud Messaging (FCM) server.

APNs Certificate

The *APNs Certificate* is an option for allowing push notifications to be passed from Bright Pattern to a user's Apple iPhone; this is accomplished via a certificate-based connection. The APNs certificate must be uploaded here for a connection to be established. **Note**: If you wish to use a sandbox environment, ensure you generate an APNs certificate **for sandbox use only**.

Use sandbox environment

If the *Use sandbox environment* checkbox is selected, the Bright Pattern Contact Center (BPCC) server will use the **api.sandbox.push.apple.com** servers; if the setting is unchecked, the BPCC server will use **api.push.apple.com**.

Firebase Server Key

Firebase Cloud Messaging (FCM) is another option for allowing push notifications to be passed from Bright Pattern to a user's Apple iPhone; the requests are authenticated with an FCM Server Key, which is obtained from an FCM console. The key must be entered here for a connection to be established.

Android push notifications

Firebase Server Key

Firebase Cloud Messaging (FCM) is the only option for allowing push notifications to be passed from Bright Pattern to a user's Android phone device; the requests are authenticated with an FCM Server Key, which is obtained from an FCM console. The key must be entered here for a connection to be established.

Chat widget

The *chat widget* provides access to the web elements of the chat application that customers will use to access your contact center via the given scenario entry. The chat widget may be customized for color, size, fonts, font size, display elements, and more.

To edit the chat widget, click **customize** and the Chat Widget Configuration window will open. For step-by-step instructions explaining how to configure your chat widget, including [chat widget auto-start](#), see section [Web Chat Configuration](#)

For additional information, see the [Chat Widget Configuration Guide](#).

Chat transcript template

The *chat transcript template* allows you to configure an email template for the purpose of sending chat/messaging transcripts. Note that this chat transcript template is specific to the given Messaging/Chat Scenario Entry; if the template is not defined, the [template defined at the system level](#) will be used.

Example chat transcript template

When configuring the settings in this section, you will need the following:

- **A sender display name**

- **A sender email address**

- **The chat transcript variable** - When configuring the template message, you must include the variable *$(CHAT_TRANSCRIPT)*. This variable inserts the transcript into the message.

Please note that in order for transcripts to be emailed, you will also need the following:

- **A configured SMTP server** - In order for the system to automatically send emails, you will need complete [SMTP Configuration](#).

- **A configured [pre-chat form](#) with an email field** - Transcripts are emailed to the address(es) specified in fields containing the variable [$(item.email)](#) when the session ends.

- **A chat scenario containing $(item.sendTranscript)** - In the corresponding chat scenario, you must include a [Set Variable](#) scenario block with the variable [$(item.sendTranscript)](#); the value must be set to **1** in order for the transcript to send.
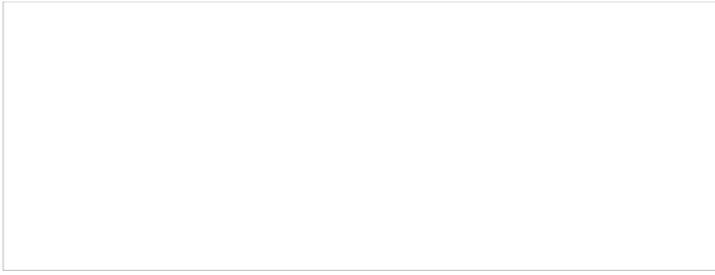
Set Variable block with the variable $(item.sendTranscript)

Web Callback

Web Callback scenario entries are used to associate [scenarios](#) with services used to provide callbacks requested by customers via mobile and web applications.

To set up and manage such associations, select the **Web Callback** option from the *Scenario Entries* menu.

Scenario Entries > Web Callback

Web Callback Scenario Entries Screen Properties

The *Web Callback Scenario Entries* screen properties are described as follows.

Name

Name is the name of the web callback scenario entry. This field is mandatory and must be unique within the contact center.

Unique identifier

The *Unique identifier* is generated by the system for this scenario entry. This identifier must be used as *Application ID* in the mobile and/or web applications that will connect to your contact center via this scenario entry. For more information, see section [General Information](#) of the Bright Pattern *Mobile/Web API Specification*.

Scenario

Scenario is the [Chat scenario](#) that will process chat interactions in which the customer requests a web callback.

Service

Service refers to the service associated with the dial-in scenario entry. Such direct association between telephone number and a service can be used when your access numbers directly identify your services.

Even if you use one access number for many different services (i.e., use an interactive voice script within the associated scenario for service selection), you may still assign a default service directly to the access number in order to account for the calls abandoned before service selection and for the calls that bypass the service selection stage (e.g., someone is unable to use the keypad to enter service selection choice, or someone is confused about which option to choose).

Default service for voice callback

The *default service for voice callback* is the [voice service](#) to be used to provide a callback to the customer.

Show chat window

It is possible to view the chat interaction while a web callback is taking place. Select this checkbox to show the chat window during web callbacks.

Hours of Operation

Hours of operation (HOP) is a schedule that defines service hours for each day of the year.

- Choose **from service** to use [HOPs of the services](#) associated with interactions processed by the given scenario.
- Choose **select** to select one of the [preconfigured HOPs](#).
- Choose **specify** to define a new HOP specifically for this scenario entry.

Unless you create an entry point for a 24/7 operation, the scenario that you have specified in the *Scenario* property above must define processing of interaction arriving at this entry outside as well as within the specified hours of operation. That is, the scenario should normally begin with an [If](#) block that has the condition *The current date and time is* (or *is not*) *in hours of operation.* For more information, see the [example](#) provided in the *Scenario Builder Reference Guide*.

HOPs can also be [specified at the service level](#).

Note the following:

- If you use options *select* or *specify* to define HOP for this scenario entry, all possible HOP checks within this scenario will use the HOP defined for this entry. Any HOPs specified for any services within this scenario will be disregarded.
- If you use option *from service*, the HOP check will use the HOP of the service that is associated with the interaction at the time when the check is performed. By default, this is the *Service* configured for this scenario entry (see above). However, if the service is redefined within the scenario, a subsequent HOP check will use the HOP of that new service.
- If you (1) use option *from service*, (2) do not have any *Service* configured for this scenario entry, and (3) use an HOP check before any explicit service assignment within the scenario, all incoming interactions will be treated as if they arrived outside of the service hours.

Form fields

Customers who request a web callback will provide information (e.g., name, phone number, email, etc.) to the agent by typing into *form fields*. To add a new form field and/or change the field's label, click**add.** You will be prompted to select the *type* of form field and to enter*label text* for the form field.

Web HTML snippet

The *Web HTML snippet* provides access to the web elements of the chat application that customers will use to access your contact center via the given scenario entry.

To use the out-of-the-box application, click the**HTML snippet** button, **copy** the HTML snippet code, and embed it into your web page(s). Normally, it is not necessary to change the default **client web server hostname**. You will do so only if instructed by your service provider.

Email

The logic of processing of an inbound email interaction is initially determined by the email address that was used by the email sender. In the simplest case, such email addresses can correspond to your email services (e.g., your *sales@company-name.com* and *support@company-name.com* may be associated with your *Sales* and *Support* services, respectively). In a more complex configuration, you may want to apply some keyword-based analysis of email texts to associated emails with appropriate services (e.g., an email coming to *support@company-name.com* can be further categorized into *Smartphone Support* and *Tablet Support* services based on the presence of the words*phone* and *tablet* in the text of email messages).

The logical entity that describes the association between email addresses and keywords on the one hand and email services, on the other hand, is called *email scenario entry.* Unlike the other types of scenario entries, the email entries do not currently refer to any actual scenarios. All information required for the association of incoming emails with services in the current release is contained in the configuration settings of the email entries themselves.

Note that before you configure an email scenario entry, you should set up a corresponding[email service](). If you plan any keyword-based categorization, it may also be easier to define upfront all of the known services to which the emails arriving via this entry may be attributed. Once the email entry is set up according to your initial needs, you can add more services and update the categorization rules at any time.

Notes

- Bright Pattern Contact Center stores all processed emails for activity history, reporting, and quality management purposes. These storage practices may not coincide with the general email retention policies of your organization. For compliance with such general retention policies, we recommend that you always store copies of all emails received to and sent from the email addresses used for email scenario entries.

    Email scenario entries are managed in the Contact Center Administrator application. To set up and manage email scenario entries, navigate to *Configuration > Scenario Entries > Email*.

- This option is visible and available to you only if the email management capability is enabled for your contact center at the service provider level.

    If you have no email scenario entries set up, create them by clicking the "+" button. Once you have added an email scenario entry, screen properties will be visible on the right-hand pane of the screen.

- Email attachment limits are set by the service provider. By default, these limits are:
    - Single email attachment size: 10 MB
    - Single email with attachments size: 25 MB

Screen Properties

The screen properties for email scenario entries are organized into three tabs:*Account*, *Services*, and *Case Fields*. The settings for each tab are described as follows.

Account tab

Protocol type

Protocol type defines what protocols are used to send and retrieve email messages. The following protocols are supported:

- POP3/SMTP
- Microsoft Exchange Web Services (EWS)
- Microsoft Graph API

The drop-down menu provides three options: POP3/SMTP, Microsoft EWS, and Microsoft Graph. The email settings that follow are dependent on the protocol type that you select.

Note: For customers using EWS for email (e.g., Outlook.com, Hotmail.com, Office 365, etc.), on Oct. 13, 2020, Microsoft stopped Basic Authentication for new email accounts of this type. Moving forward, all new email accounts will use the Microsoft Graph API for OAuth authentication.

As such, Bright Pattern Contact Center software now allows service providers to enable the Microsoft Graph API on a cluster-wide basis. This means that any contact centers with email scenario entries of the *Microsoft EWS* protocol **must** be transitioned to the new *Microsoft Graph* protocol. Note that existing accounts will not be immediately affected; however, all accounts should be transitioned **before** mid-2021.
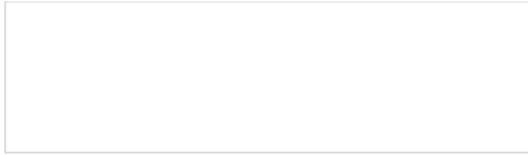
Supported email protocols

POP3 Properties

Selecting protocol type POP3/SMTP will bring up the following properties for Incoming Mail and Outgoing Mail.

Account

Email address

Email address is the address that customers will use to send emails to a specific service or a range of services. This address will also appear in the *From:* field of corresponding email replies as well as any outbound emails related to services associated with this scenario entry. This parameter is mandatory.

Display name

Display name is the name that will be shown for the email address that customers will use to send emails to a specific service or a range of services (e.g., "Bright Pattern Support" is a display name for "support@brightpattern.com"). This parameter is mandatory.

Incoming Mail
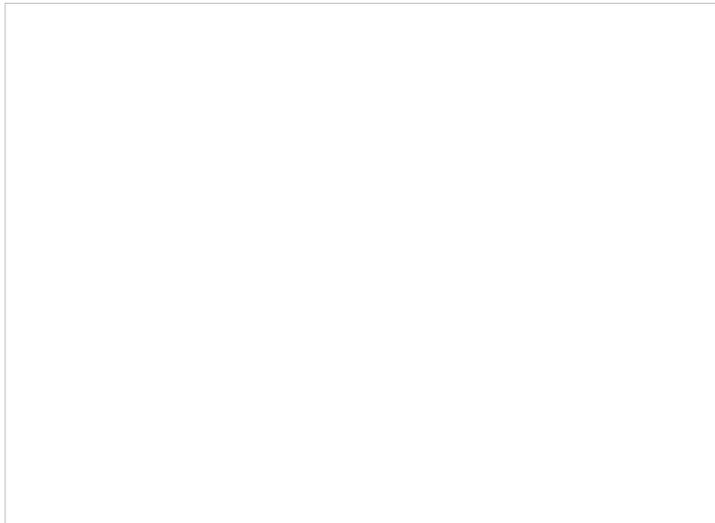
POP3 Incoming Mail properties

Server

Server is the type of server used for the transmission of email messages to the email address. It is read-only. The POP3 protocol is supported.

Host

Host is the name of the host where the server is run. This parameter is mandatory.

Connection security

Connection security provides indication of whether a cryptographic protocol (TLS or SSL) will be used to secure this connection.

- For a nonsecure connection, select **none**.
- To negotiate encryption in a plain connection, select **negotiate encryption in a plain connection (STARTTLS)**.
- For an immediate secure connection, select **use an encrypted connection (TLS/SSL v3)**.

Port

Port is the port assigned to the server on the host. This parameter is mandatory.

Username

Username is the username for email client authentication. This parameter is mandatory.

Password

Password is the password for email client authentication. This parameter is mandatory.

Test

The *Test* button is used to verify the correctness of your connection settings.

Error reported

In case the account has been disabled automatically (see above), this parameter displays the error message that caused the system to disable the account. This parameter is read-only; the parameter's label is hidden while the testing attempt is successful.

Retrieval interval

Retrieval interval is the mail retrieval period. By default, the account is checked for the presence of new mail every 15 seconds. Some POP3 mail servers may be configured to lock out accounts that access mailboxes at this rate due to excessive activity. If this is the case, use this *Incoming Mail, Retrieval interval* parameter to increase the retrieval period to any value between 15 and 86400 seconds.

Enabled

Enabled indicates whether the account is currently enabled. Accounts can be disabled manually or automatically, as described. Accounts can only be enabled manually.

After incoming emails have been retrieved for processing, Bright Pattern Contact Center normally deletes those emails from the mailbox. However, if the POP3 server is configured for read-only access, the emails will stay in the mailbox and will be retrieved repeatedly until the system runs out of disk space. To prevent this from happening, the system will automatically disable the email account if an attempt to delete incoming mail returns an error from the POP3 server.

If an account is disabled, you should check the *Last error* message. If the message indicates that the account has been disabled for the aforementioned reason, reconfigure your POP3 server for full access, and enable the account manually.

Bulk delete received email

This button allows you to delete emails received by the system in bulk. Specifically, when the button is selected a window pops, which allows you to configure emails to be deleted that were received between a range of dates and hours for a selected time zone. Note that you must select the **Delete** button in the window in order to confirm the bulk deletion.

Note: This button is available to users with credentials for the Service Provider application*only*. That is, you must log in to the Contact Center Administrator application with your system credentials (e.g., *sys:user_name*).
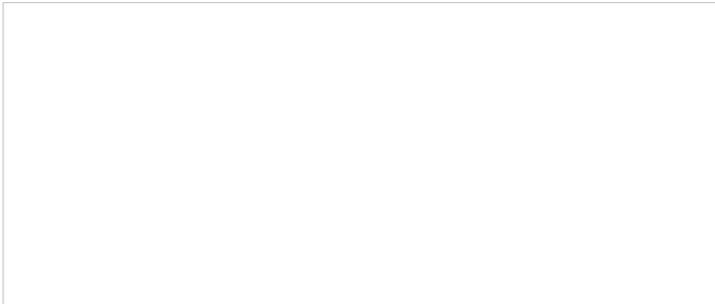
Deletion of emails in bulk is reserved for service providers only

Outgoing Mail
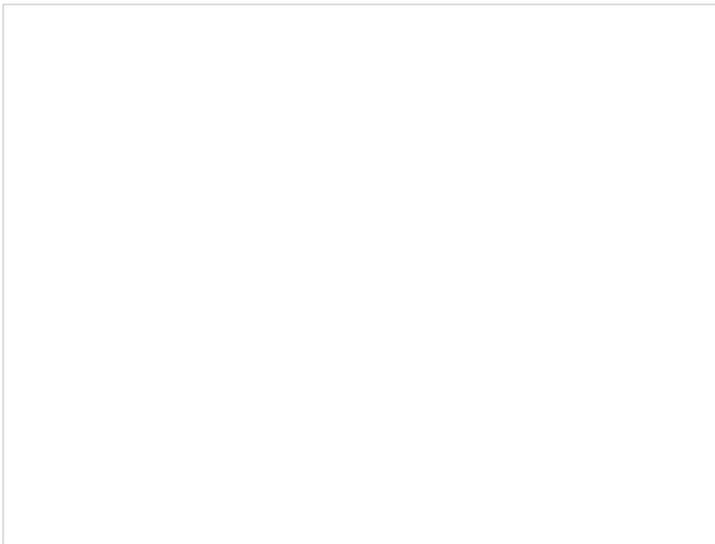
SMTP Outgoing Mail settings

Server

Server defines what protocol is used to send and retrieve email messages. It is read-only. The SMTP protocol is supported.

Host

Host is the name of the host where the server is run. This parameter is mandatory.

Connection security

Connection security provides indication of whether a cryptographic protocol (TLS or SSL) will be used to secure this connection.

- For a nonsecure connection, select **none**.
- To negotiate encryption in a plain connection, select **negotiate encryption in a plain connection (STARTTLS)**.
- For an immediate secure connection, select **use an encrypted connection (TLS/SSL v3)**.

Port

Port is the port assigned to the server on the host. This parameter is mandatory.

Server requires authentication

Selecting the *Server requires authentication* checkbox forces the user to enter a username and password for email client authentication. If you do not select the checkbox, a username and password will not be necessary.

Username

Username is the username for email client authentication. This parameter is mandatory.

Password

Password is the password for email client authentication. This parameter is mandatory.

Test

The *Test* button is used to verify the correctness of your connection settings.

Error reported

In case the account has been disabled automatically (see above), this parameter displays the error message that caused the system to disable the account. This parameter is read-only; the parameter's label is hidden while the testing attempt is successful.

Current error

The label *Current error* is displayed if the account type is enabled by your service provider and the last retrieval or send attempt was not successful; the label is hidden if both the last retrieval and last send did not have an error. If the account type is not enabled by your service provider , the label *Current error* is not shown. The content of this field is reset when the account is changed from *disabled* to *enabled*.

Microsoft Exchange Web Services Properties

Selecting the protocol type **Microsoft EWS** will bring up the following properties for Incoming Mail and Outgoing Mail.

Microsoft Exchange Web Services (EWS) consumes extra memory when processing email attachments. It will consume approximately 4 times the size of a single email attachment sent in a message. For example, if the single attachment is 15 MB, you will need an extra 60 MB allocated to the email service.

Note: For customers using Exchange Web Services (EWS) for email (e.g., Outlook.com, Hotmail.com, Office 365, etc.), on Oct. 13, 2020, Microsoft [stopped Basic Authentication](#) for new email accounts of this type. Moving forward, all new email accounts will use the Microsoft Graph API for OAuth authentication.

As such, Bright Pattern Contact Center software now allows service providers to enable the Microsoft Graph API on a cluster-wide basis. This means that any contact centers with email scenario entries of the *Microsoft EWS* protocol **must** be transitioned to the new *Microsoft Graph* protocol. Note that existing accounts will not be immediately affected; however, all accounts should be transitioned **before** mid-2021.
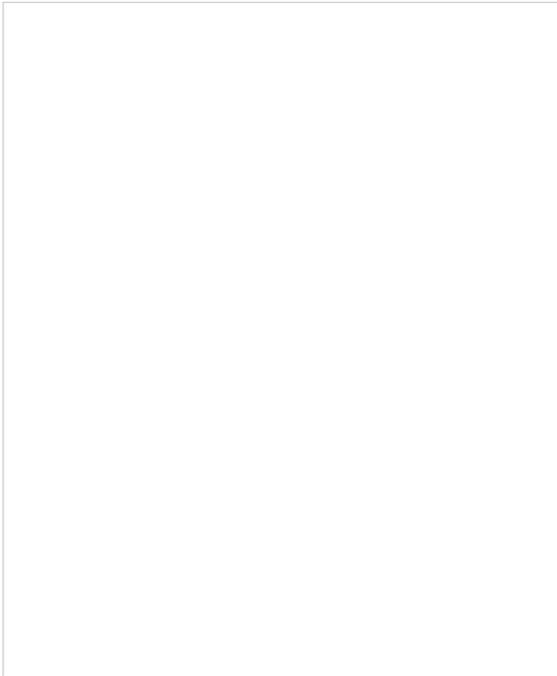
Microsoft EWS settings

Account

Email address

Email address is the address that customers will use to send emails to a specific service or a range of services. This address will also appear in the *From:* field of corresponding email replies as well as any outbound emails related to services associated with this scenario entry. This parameter is mandatory.

Display name

Display name is the name that will be shown for the email address that customers will use to send emails to a specific service or a range of services (e.g., "Bright Pattern Support" is a display name for "support@brightpattern.com"). This parameter is mandatory.

Microsoft Exchange Web Service

EWS URL

EWS URL is the Exchange Web Services URL from which the email will be retrieved.

Username

Username is the username for email client authentication. This parameter is mandatory.

Password

Password is the password for email client authentication. This parameter is mandatory.

Test

The *Test* button is used to verify the correctness of your connection settings.

Error reported

In case the account has been disabled automatically (see above), this parameter displays the error message that caused the system to disable the account. This parameter is read-only; the parameter's label is hidden while the testing attempt is successful.

Incoming Mail

Retrieval interval

Retrieval interval is the mail retrieval period. By default, the account is checked for the presence of new mail every 15 seconds. Some mail servers may be configured to lock out accounts that access mailboxes at this rate due to excessive activity. If this is the case, use this Incoming Mail, Retrieval interval parameter to increase the retrieval period to any value between 15 and 86400 seconds.

Enabled

Enabled indicates whether the account is currently enabled. Accounts can be disabled manually or automatically, as described. Accounts can only be enabled manually.

After incoming emails have been retrieved for processing, the emails will stay in the mailbox, will be marked as read, and will be retrieved repeatedly. The system will detect that the emails already exist in the database and will not create multiple copies in the database/disk. It is possible to delete emails from EWS by setting up retention rules directly on the exchange server. Note that deleting them from the system does not impact the emails on EWS, as they are marked as read and are still kept on EWS.

If an account is disabled, you should check the Last error message. If the message indicates that the account has been disabled, reconfigure your Microsoft Exchange Web Services server for full access, and enable the account manually.
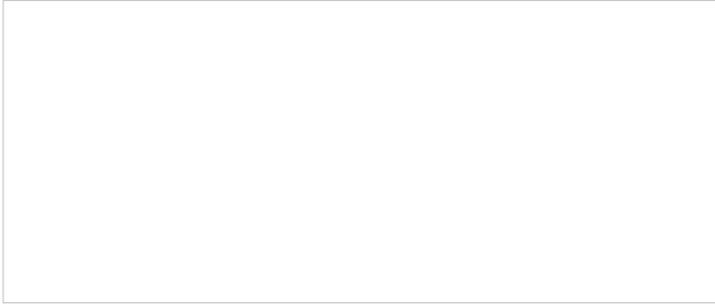
Current error

The label *Current error* is displayed if the account type is enabled by your service provider and the last retrieval or send attempt was not successful; the label is hidden if both the last retrieval and last send did not have an error. If the account type is not enabled by your service provider, the label *Current error* is not shown. The content of this field is reset when the account is changed from *disabled* to *enabled*.

Bulk delete received email

This button allows you to delete emails received by the system in bulk. Specifically, when the button is selected a window pops, which allows you to configure emails to be deleted that were received between a range of dates and hours for a selected time zone. Note that you must select the **Delete** button in the window in order to confirm the bulk deletion.

Note: This button is available to users with credentials for the Service Provider application*only*. That is, you must log in to the Contact Center Administrator application with your system credentials (e.g., *sys:user_name*).

Deletion of emails in bulk is reserved for service providers only

Microsoft Graph

Selecting protocol type Microsoft Graph will bring up the following properties for Incoming Mail and Outgoing Mail. Note that this option must be enabled by your service provider.
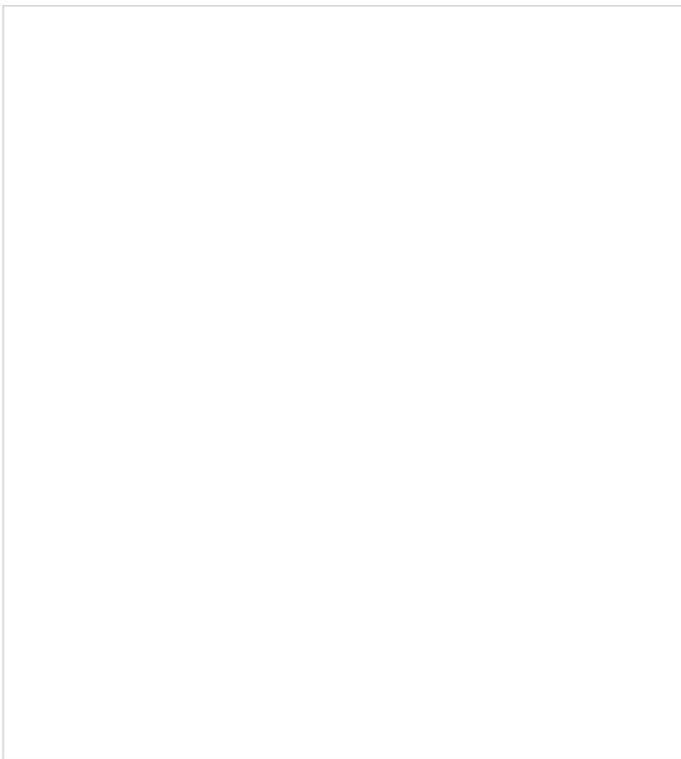
Microsoft Graph settings

Connect account

When selecting the *Connect account* button, a separate window will pop and you will be prompted to log into your Microsoft account and authorize access. The application can request grant permissions, so you will need to give the required permissions to the application. **Note:** If you are already signed into a Microsoft email account, a session cookie will be detected and credentials will not need to be entered.

When an account is successfully connected, the email address will appear in the *Email address* field and the *Display name* field below.

Account

Email address

When your Microsoft account has been successfully authorized and connected to your contact center, the email address will appear in this field.

Display name

When your Microsoft account has been successfully authorized and connected to your contact center, the email's display name will appear in this field.

Test

The *Test* button is used to verify the correctness of your connection settings.

Error reported

In case the account has been disabled automatically (see above), this parameter displays the error message that caused the system to disable the account. This parameter is read-only; the parameter's label is hidden if the testing attempt is successful.

Incoming Mail

Retrieval interval

This setting allows you to define the mail retrieval period. By default, the account is checked for the presence of new mail every 15 seconds.

Enabled

Enabled indicates whether the account is currently enabled. Accounts can be disabled manually or automatically, as described. Accounts can only be enabled manually.
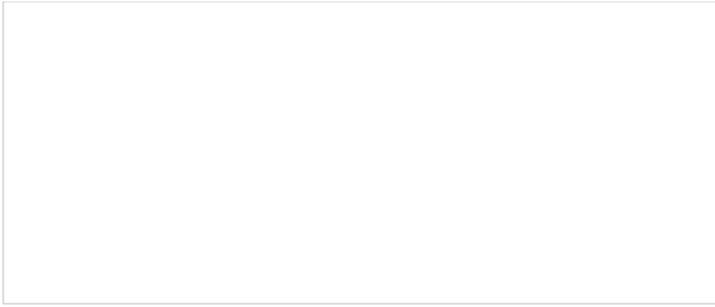
Current error

The label *Current error* is displayed if the account type is enabled by your service provider and the last retrieval or send attempt was not successful; the label is hidden if both the last retrieval and last send did not have an error. If the account type is not enabled by your service provider, the label *Current error* is not shown. The content of this field is reset when the account is changed from *disabled* to *enabled*.

Bulk delete received email

This button allows you to delete emails received by the system in bulk. Specifically, when the button is selected a window pops, which allows you to configure emails to be deleted that were received between a range of dates and hours for a selected time zone. Note that you must select the **Delete** button in the window in order to confirm the bulk deletion.

Note: This button is available to users with credentials for the Service Provider application *only*. That is, you must log in to the Contact Center Administrator application with your system credentials (e.g., *sys:user_name*).

Deletion of emails in bulk is reserved for service providers only

Services tab

The Services tab presents settings related to email services.

Email > Services properties

Default service

Default service is the email service that will be associated with emails arriving via this entry if categorization rules are not set or do not provide any keyword matches. This parameter is mandatory.

Note: If you intend to delete an email service you must reassign this setting to another email service in order to move all existing emails to that new service.

It is recommended to not allow the deletion of the last remaining email service if there are any emails in the service's [push queue or pull queue](#); however, it is OK to delete the last email service if there are emails in a[case's activity history](#) or in an agent's list of [pinned cases](#).

Queueing priority

Queueing priority is the priority that will be given to emails received by this email scenario entry. Priority determines the position of the email interaction requesting the default service in the queue (i.e., *Team Queue* and *Personal Queue*), relative to email interactions associated with other services that are competing for the same agents. Priority is set by the email sender in the form of an X-Priority header.

Note: The Bright Pattern Contact Center (BPCC) importance value range is from 1 (the lowest and the default value) to 5. Unlike other media types, the priority of email is absolute (i.e., an email with a higher priority always will be distributed to a qualified resource before emails with lower priority regardless of the time any of those emails spent in the queue).

For more information regarding configuring queueing priority, see *Tutorials for Admins*, section *[Configuring High-Importance Email Routing](#)*.

When importance (X-Priority header) is

There are four options (i.e., columns) for importance. They are as follows:

- **Default** - This column allows you to define the queue placement for emails without X-Priority headers
- **3 (normal)** - This column allows you to define the queue placement for emails received with an X-Priority header value of **3**.
- **1 (high)** - This column allows you to define the queue placement for emails received with an X-Priority header value of **5**.
- **5 (low)** - This column allows you to define the queue placement for emails received with an X-Priority header value of **1**.

Notes:

- You may define priority for each column per the following*First email* and *Subsequent email* rows.
- X-Priority headers set to either 2 or 4 correspond to the BPCC values of 5 and 1, respectively.

First email

This row allows you to define the queueing priority for all new incoming emails (i.e., not replies); you may set priority for all four *When importance (X-Priority header) is* column options.

Subsequent email

Subsequent email priority is the queuing priority of customer emails related to existing email threads.

The system automatically checks whether an incoming email may be part of an existing email thread (e.g., after receiving a reply to an original email request, the customer may have additional questions). Such emails bypass the keyword-based analysis. Instead, they are automatically attributed to the same service as the original request. This parameter allows you to distribute such emails with a higher (or lower) priority than any new email requests.

Ignore Reply-To Header

The *Ignore Reply-To Header* checkbox, when selected, allows the system to ignore the header in the reply-to field of an email. When this setting is checked, the behavior is as follows:

- The *From* field is used for identification.
- The *From* field is used for agent replies.
- The *Return-Path* header is used for auto-replies.

If this setting is unchecked, the behavior is as follows:

- If a reply-to header is present, it is used for identification, agent replies, and auto-replies.
- If a reply-to header is missing, the behavior is the same as if the **Ignore Reply-To Header** box is checked.

Set Language Skill Based on Detected Language

The *Set Language Skill Based on Detected Language* checkbox, when selected, allows the following:

- Emails with undetected languages will be sent to the default email service regardless of keyword matches.
- If the detected language of an email is not in the call center's list of configured languages, the email will be sent to the default email service, regardless of keyword matches.

Insert thread id in email subject

When disabled, the *Insert thread id in email subject* checkbox excludes the email case's [thread ID](#) from the email's subject line. Note that this setting is automatically enabled for existing email entries; if you are creating a new scenario entry for email, this setting is not enabled.

Note that if you disable this option, the thread ID will instead be inserted in one of the hidden fields in the email body. In this case, possible auto-replies (e.g., "out of the office" messages) may not always be processed correctly as part of the case. Therefore, if processing of auto-replies is important for your case workflow, you should keep this the thread ID in the email subject.

Optional Filters

Optional Filters is where you add the list of filters that will be used to assign emails arriving at the given email scenario entry to different services using keyword-based analysis of the email subjects and body text.

To add a filter, click **add**.

Filters are checked for possible keyword matches in the order in which they appear on the list. As soon as a match is found, the corresponding service and priority are assigned to the email interaction. Note that this order may be affected by the language setting of the filter. See the description of the [Language](#) setting for more details.

Newly created filters will appear at the end of the list. To change the position of a filter in the list, drag it to the desired location.

To edit or remove an existing filter, hover over it and select the desired function.

Language

The *Language* setting is where you select the language in which the keywords of the given filter will be written. This setting only matters if the filter's keywords may have different meanings in different languages. Otherwise, leave this parameter set to the default value **<Any>**. The list of languages here is limited to the configured [Language Skills](#) that are auto-detectable.

Initially, the system will try to detect the language of the email text automatically. If the language is not identified, only the filters set to *Any* will be checked for keyword matches. If the language is identified, the system will first check the filters set to *Any* and then check the filters set to the detected language.

Search for keywords in

The *Search for keywords in checkboxes* allow you to specify the part of the email where your filter keywords will apply. You may select *Body text, Subject*, or both of these options; once you have specified the desired option(s), you must enter your keyword expressions in the *Filter keywords* field. Note that both options are checked by default.

Filter keywords

Filter keywords are the keyword expressions that you specify. Each keyword/phrase in the expression must be set in quotation marks. Logical expressions can include logical operators AND, OR, XOR, NOT, and parentheses (e.g., *"connection loss" AND ("router" OR "modem")*).

Search for keywords in sender's address

The *Search for keywords in sender's address* checkbox lets you include or exclude an incoming email's *From* field in a keyword search. When this option is selected, you must define your keywords in the *Email addresses* field. Note that this option is unchecked by default.

Email addresses

The *Email addresses* field allows you to define email addresses that will be used to filter an incoming email by the contents of the *From* field. You may enter complete addresses (e.g. jane.doe@brightpattern.com), domains (e.g., brightpattern.com), or both. A domain can be specified both with and without the "@" character. If you use several addresses and/or domains, they can be separated by space, comma, or semicolon. Quotation marks should not be used when specifying anything in this field.

Service and Priority

The *Service* is the email service that will be associated with email interactions matching this filter.

The *Priority* is the priority that will be assigned to email interactions matching the filter. For more information about email priority, see the description of the *Default priority* setting.
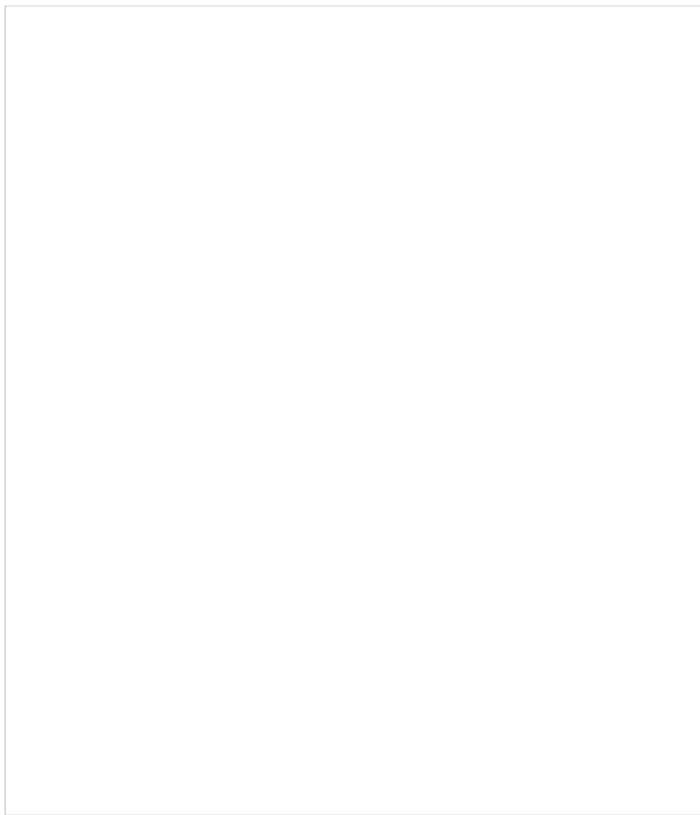
Language, keywords, service, and priority can be configured all at once

Natural Language Understanding

Our contact center solution integrates with IBM Watson to provide Natural Language Understanding (NLU) functionality and sentiment analysis capabilities to your tenant on a per-service basis. To enable NLU for email scenario entries, select the applicable integration account from the *Natural Language Understanding* drop-down menu.

Integration account

The default integration account is < < *None* > >. If no integration accounts are listed, that means no integration accounts of the type "Natural Language Understanding" have been configured for your tenant. To add an integration account, see section [Integration Accounts](#) of the *Contact Center Administrator Guide*.

Salesforce.com synchronization

If your contact center is integrated with [Salesforce.com (SFDC)](#), emails from the Agent Desktop application can be synchronized with SFDC for routing and reporting. Emails from Agent Desktop link to SFDC Person Accounts, Contacts, and Accounts. Note that you may configure [Screenpop URL](#) to make synchronized SFDC cases pop in Agent Desktop.

With this setting enabled, the following happens for all incoming and outgoing email:

- Emails are received and processed by agents in Agent Desktop.
- After emails are processed, the system conducts a search in Salesforce.com using Salesforce Object Query Language (SOQL). The search looks in *Contact* objects for field *Email* (i.e., the customer's email, specifically "from" or "to" fields based on the message direction). The search also looks in *Users* objects for field *Email* (i.e.,

the agent's email, specifically the "from" field based on message direction).
- If multiple matches are found, the search takes the first result.
- If a new Agent Desktop case was created, a new SFDC case is created.
- Whether a match was found or a new case was created, the system creates an*EmailMessage* object for the match, which passes case ID, related case ID, activity ID, and attachment data.
- If an email contains an attachment, the system creates an*Attachment* object.
- Finally, the system creates a *Task* object, which contains user, case, account, and contact data.

If neither a matching contact nor a matching user is found, the case is not created (i.e., only known addresses are synchronized); if the case is not created, neither the first nor subsequent messages are synchronized.

If the Screenpop URL setting is configured with a Salesforce URL, note the following:

- After emails are received and processed in Agent Desktop, cases and emails are synchronized to SFDC as cases and emails in Activity history, and they are linked to an agent (user) and a contact.
- The first email routed in such a way results in a screen pop of the customer/contact record in SFDC.
- Agent Desktop will also display the contact and activity history (if contact feature is used).
- Each subsequent email results in a screen pop of the SFDC case.
- Bright Pattern Contact Center would retain all of the routing control and reporting data. Switching between two screens (Agent Desktop and SFDC) is required.

Note that Bright Pattern and SFDC need to be integrated on both the server and client side. For more information on SFDC integration, see the Salesforce.com Integration Guide.

**Integration account**

The default integration account is < < *None* > >. If no integration accounts are listed, that means no integration accounts of the type "Salesforce.com" have been configured for your tenant. To add an integration account, see the the *Contact Center Administrator Guide*, section Integration Accounts.

Case Fields Tab

You may utilize custom case fields when configuring email to pull data from email subject line and body; these custom case fields then can be used in custom reporting fields.

Parse email Subject into case fields

To create case fields from the text in an email subject line, you will need to first configure a regex expression. Once this has been configured, name the configured expression in the **case field** field.
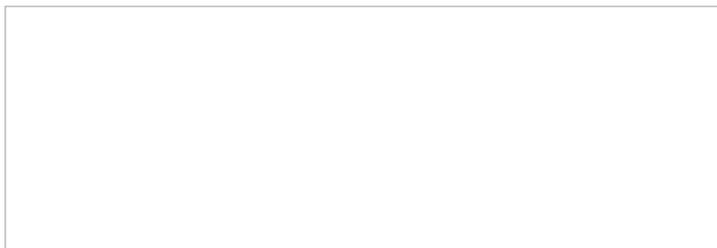
Regex expressions are used to create case fields from an
email's subject line

Parse email Body into case fields

To create case fields from the text in an email body, enter in words or phrases your customers use at the beginning of sentences in the **Line starting with** field. Once configured, name the field in **case field**.
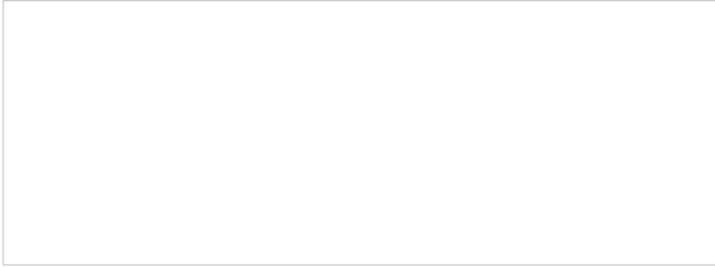
Words or phrases from the beginning of sentences may be used to create case fields