

# 5.3 Single Sign-On Integration

## Bright Pattern Documentation

Generated: 12/09/2021 4:28 am

Content is available under license unless otherwise noted.

# Table of Contents

Table of Contents	2
Privileges	4
Interaction Handling group	4
Access full-screen Agent Desktop	4
Delete contacts	4
Edit contacts	4
Force pop-out phone window	4
Handle automatically distributed interactions	4
Handle email	5
Handle service chats	5
Initiate SMS conversation	5
Listen to call recordings and view chat transcripts on assigned services	5
Listening to own call recordings and view own chat transcripts	5
Login to Agent Desktop	5
Make external calls	5
Mask original email content	6
Modify own identification data	6
See other agents/teams in directory	6
See other agents' cases	6
Send internal chats	6
Start recording of interactions	6
Stop recording of interactions	6
Transfer calls	6
Use Calendar	6
Use Favorites tab	6
Use Recent Calls tab	7
Use RightNow	7
Use ServiceNow	7
Use Zendesk	7
Quality Management	7
Accept/dispute evaluations of their interactions by others	7
Assign evaluations and calibrations	7
Confirm evaluations of supervised agents	7
Delete evals completed by anyone	7
Delete evals completed by themselves	7
Edit evaluation forms	8
Edit public interaction searches	8
Evaluate agent interactions	8
Evaluate own interactions	8
Manage evaluations across teams	8
See evals of self	8
Security Administration group	8
Can edit and erase interaction records	8
Grant all privileges	8
Manage roles and security settings	8
Service and Campaign Administration group	9
Configure reporting settings	9
Configure system-wide settings	9
Control campaign operations	9
Edit knowledge base	9
Manage all services and campaigns	9
Manage assigned services and campaigns	9
Manage lists	10
Manage scenarios	10
Manage skills	10
Use SMS/MMS API	10
Supervision group	10
Access Real-time Stats API	10
All assigned teams combined view	10
Can see contents of email push queues	11
Can update final dispositions	11
Can use agent seat maps	11
Change alert configuration	12
Change real-time metric views	12
Customize Wallboards	12
Define/View subteams of selected agents	12

Delete cases	12
Download recordings and transcripts	12
Force agent states	12
Listen to recordings linked to external CRM records	12
Listening to all call recordings and view all chat transcripts	13
Manage canned chat responses system-wide	13
Monitor agent screen	13
Monitor interactions	13
Pull screen pop	13
Push/Pull Global Wallboards	13
Set alerts for real-time metrics system-wide	13
Set real-time metric views system wide	13
View historical reports	14
View interaction records	14
View real-time agent metrics	14
View real-time service metrics	14
Watch agent screen recordings	14
<b>System Administration group</b>	<b>14</b>
Allow recording export API access	14
Bulk Export/Import Contacts	14
Bypass Single Sign-On	14
Configure Contact Forms and fields	15
Configure directory	15
Manage BPO Clients	15
Manage all teams	15
Manage phones	15
Manage users	15
Privileged Access IP Range	15
Publish help	16
View audit log	16
View usage data	16
<b>BPO Client group</b>	<b>16</b>
Listening to call recordings and view chat transcripts on services in reviewer role	16
<b>Integrations</b>	<b>16</b>
<b>Tutorials</b>	<b>16</b>
Integration Account Configuration	16
Remote Assistance	16
Single Sign-On (SSO) Integration Accounts	16

# Privileges

Registered users of your Bright Pattern Contact Center solution are assigned *privileges* that can be used to control access to various contact center functions. Privileges are arranged in the same way as they appear on the [Roles](#) page of the Contact Center Administrator application. For general information about privileges and roles, see section [Roles](#).

Privileges are organized into seven categories (i.e., groups):

- Interaction Handling
- Quality Management
- Security and Administration
- Service and Campaign Administration
- Supervision
- System Administration
- BPO Client

**Note:** Some service configuration changes that affect agent behavior are not picked up dynamically by Agent Desktop. Thus, after making a change to privileges, we recommend that all affected agents re-login to Agent Desktop.

## Interaction Handling group

### Access full-screen Agent Desktop

The *Access full-screen Agent Desktop* privilege allows the user to enable full-screen Agent Desktop view within CRM applications.

Because CRM systems typically have their own email and case management capabilities, the full-screen mode normally would be used by supervisors only.

### Delete contacts

The *Delete contacts* privilege allows the deletion of contacts. If enabled, users can delete individual contacts via the Agent Desktop. When a contact is deleted, its activity history is deleted too. Cases are not deleted automatically.

### Edit contacts

The *Edit contacts* privilege provides write access to contacts. If enabled, users can create new contacts, and users can modify any fields in existing contacts (but not activity history).

### Force pop-out phone window

The *Force pop-out phone window* privilege allows the user to open Agent Desktop in a pop-out window. For more information, see section [Understanding Screen-Pop](#) of the *Agent Guide*.

Enabling this privilege is generally not recommended if you plan to deliver [activity forms](#) and/or other web content to agents via [screen pop](#).

Note that if the user has any privileges in the *Supervision* group (see below), the user will not be able to open Agent Desktop in a pop-out window even if the user has this privilege.

### Handle automatically distributed interactions

The *Handle automatically distributed interactions* allows the user to receive calls from a service queue and preview records. This is the basic privilege that allows the user to perform typical call center agent work (i.e., provide services over the phone and participate in outbound campaigns).

The ability to handle customer chat or email interactions is controlled via separate privileges (see *Handle email* and *Handle service chat*).

## Handle email

When enabled, the *Handle email* privilege allows users to:

- Edit cases
- Create new cases manually
- Open cases from search results (even if they are already open by other agent)
- Mark cases as spam

## Handle service chats

With the *Handle service chats* privilege, the user may [handle chat interactions with customers](#). This includes chat interactions started by customers via SMS.

Note that the ability to initiate a chat with a customer via SMS is controlled by a separate privilege (see *Initiate SMS conversation*). Likewise, the ability to use internal chat is controlled by a separate privilege (see *Send internal chats*).

## Initiate SMS conversation

The *Initiate SMS conversation* privilege allows the user to [initiate chats with customers via SMS](#).

## Listen to call recordings and view chat transcripts on assigned services

With this privilege granted, the user may review [call recordings](#) and [chat transcripts](#) of the services that the user is qualified to handle (i.e., has corresponding [service skills](#)).

## Listening to own call recordings and view own chat transcripts

This privilege provides Agent Desktop users the capability, via activity history, to access recordings where the agent participated (at least partially). This privilege applies to Agent Desktop only.

## Login to Agent Desktop

*Login to Agent Desktop* allows the user to log in to Agent Desktop application and perform basic back-office telephony functions. Any user who needs access to Agent Desktop must have this privilege. Note that this privilege alone is not sufficient for performing typical contact center agent work.

Note that any user who logs into Agent Desktop will be counted as a concurrent user for the duration of the login session. Your service provider may impose a limit on how many of your users may be logged on concurrently.

## Make external calls

A user with the *Make external calls* privilege may make external calls and blind transfers to external destinations from the Agent Desktop application. If the user does not have this privilege, an attempt to make an external call or blind transfer will result in a text error message displayed on Agent Desktop.

Note that the absence of this privilege does not prevent users from making external calls using the dial pad of their hardphones.

## Mask original email content

The *Mask original email content* privilege allows the user to mask fragments of original customer email text. For more information, see section [How to Mask Sensitive Data](#) of the *Agent Guide*.

## Modify own identification data

The *Modify own identification data* privilege allows the user to be able to modify specific fields of the user profile. If the privilege is not present, the following fields are locked:

- First Name
- Last Name
- Chat Nickname

## See other agents/teams in directory

This privilege lets the user see all configured teams and team members in the Agent Desktop directory and view their current availability (presence). For more information, see section [How to Use the Directory](#) of the *Agent Guide*.

## See other agents' cases

*See other agents' cases* allows the user to see cases handled by other agents. If the user does not have this privilege, the user will be able to see only cases that with which the user has worked. This privilege affects [case search](#) only. Absence of this privilege does not affect the user's ability to receive emails related to existing cases that the user has not worked on.

## Send internal chats

The *Send internal chats* privilege allows the user to [initiate internal chat conversations](#).

## Start recording of interactions

With this privilege, the user may [start call recording](#).

## Stop recording of interactions

*Stop recording of interactions* allows the user to [stop call recording](#).

## Transfer calls

The *Transfer calls* privilege allows the user to [transfer customer interactions to consultation parties](#) and [host conferences](#) (both via-consultation and single-step).

Absence of this privilege does not affect user's ability to

- make blind transfers of customer interactions
- transfer or conference internal calls

## Use Calendar

The *Use Calendar* privilege enables users to use the Agent Desktop [calendar](#) for scheduling.

## Use Favorites tab

*Use Favorites tab* is an agent-level privilege that controls whether the user can see and set favorites from the Agent Desktop application. This privilege is an agent behavior control to prevent users from dialing destinations that they should not based on FCC/TCPA and organizational rules.

## **Use Recent Calls tab**

The *Use Recent Calls tab* privilege lets the user restrict access to recent calls. This privilege uses TCPA manual dialing to limit which agents can access recent calls.

## **Use RightNow**

*Use RightNow* allows the user to use Agent Desktop embedded into the Oracle Service Cloud application (formerly called RightNow). This privilege enables access to the Agent Desktop widget within Oracle Service Cloud.

For more information, see the [Oracle Service Cloud Integration Guide](#).

## **Use ServiceNow**

*Use ServiceNow* allows the user to use Agent Desktop embedded into the ServiceNow application. This privilege enables access to the Agent Desktop widget within ServiceNow.

For more information, see the [ServiceNow Integration Guide](#).

## **Use Zendesk**

With the *Use Zendesk* privilege, the user may use Agent Desktop embedded into the Zendesk application. This privilege enables access to the Agent Desktop widget within Zendesk. To enable full-screen Agent Desktop view within Zendesk application, the user must also have the *Access full Agent Desktop* privilege.

For more information, see the [Zendesk Integration Guide](#).

# **Quality Management**

## **Accept/dispute evaluations of their interactions by others**

*Accept/dispute evaluations of their interactions by others* allows the user to accept or dispute a quality management evaluation of herself.

## **Assign evaluations and calibrations**

*Assign evaluations and calibrations* allows the user to assign quality management evaluations and calibrations to other users.

## **Confirm evaluations of supervised agents**

*Confirm evaluations of supervised agents* allows the user to accept or dispute quality management evaluations of users with the Supervisor role.

## **Delete evals completed by anyone**

*Delete evals completed by anyone* allows the user to delete evaluations of agents in the user's assigned team unless the privilege [Manage evaluations across teams](#) is enabled for the same user.

## **Delete evals completed by themselves**

*Delete evals completed by themselves* allows the user to delete quality management evaluations completed by himself.

## **Edit evaluation forms**

*Edit evaluation forms* allows the user to edit quality management evaluation forms in the [Evaluation Form Editor](#) application. Note that if a form is assigned to a service or campaign, to edit it, one needs either the [Manage all services and campaigns](#) privilege or the [Manage assigned services and campaigns](#) privilege to edit that service.

## **Edit public interaction searches**

*Edit public interaction searches* allows the user to edit the public searches seen in the Agent Desktop application, section Quality Management > Eval Home.

## **Evaluate agent interactions**

*Evaluate agent interactions* allows the user to evaluate agent interactions in the Agent Desktop application, section Quality Management.

## **Evaluate own interactions**

*Evaluate own interactions* allows users to evaluate their own interactions and is assigned to agents by default; supervisors or evaluators are meant to confirm these evaluations. Note that these evaluations can be confirmed by a user's supervisor or a supervisor assigned to a user's team only.

## **Manage evaluations across teams**

*Manage evaluations across teams* removes the restriction of only applying actions and accessing the quality management evaluations of the agents in the teams assigned to the user.

## **See evals of self**

*See evals of self* allows the user to see quality management evaluations of herself as completed by other users.

# **Security Administration group**

## **Can edit and erase interaction records**

This privilege provides access to the manual erasure functions in accordance with PCI DSS 3.2 and GDPR requirements. With this privilege enabled, users will be able to edit and erase interaction records securely and manually in the event that another user has mistakenly included a customer's sensitive data in interaction content (e.g., call recording, chat, etc.).

This privilege is added to predefined Security Administrator and System Administrator roles.

## **Grant all privileges**

*Grant all privileges* allows the user to grant any privilege, regardless of the user's *May grant or revoke* settings with respect to specific privileges. This is helpful during product upgrades where new privileges may be introduced.

## **Manage roles and security settings**

With this privilege enabled, the user has full access to the following settings:



- [Roles](#)
- [Security Policy](#)
- [System Access Restrictions](#)
- [Encryption Key Management](#)

## Service and Campaign Administration group

### Configure reporting settings

With this privilege enabled, the user has full access to the following settings:

- [Report Templates](#)
- [Scheduled Reports](#)
- [Reporting Settings](#)

### Configure system-wide settings

The *Configure system-wide settings* privilege gives the user full access to all pages of the following menus: *Tasks*, *Call Center Configuration*, and *Quality Management*.

For tasks, note that all users who have the *Configure system-wide settings* privilege enabled will receive an email notification each time a scheduled task fails.

### Control campaign operations

*Control campaign operations* enables the user to [view and control assigned campaigns](#) via Agent Desktop.

A user must have this privilege in order to be available for selection as a service/campaign operator via the *Services and Campaigns > Assignments* page. In the Agent Desktop application, access will be limited to campaigns where the user is assigned as an operator.

If this privilege is revoked from a user, the user's name will appear in red color in the list of operators of any services/campaigns that the user may have been previously assigned to operate.

### Edit knowledge base

The *Edit knowledge base* privilege gives the user full access to the [Knowledge Base](#) via the Contact Center Administrator application. It also allows the user to create articles in the *Knowledge Base* via the Agent Desktop application.

Note that access to the *Knowledge Base* via the Agent Desktop application is provided in the context of the services that the user can handle.

### Manage all services and campaigns

The *Manage all services and campaigns* privilege allows the user to configure all existing services campaigns regardless of whether the user is assigned to them as an administrator. Note that in order to [assign teams to campaigns](#), the user must also have the *Manage teams* privilege.

Another privilege exists to enable the user to access only assigned services campaigns (see below). Note that in order to prevent the user from creating new services and campaigns, both these privileges must be disabled.

### Manage assigned services and campaigns

With this privilege, the user has full access to configuration of the services and campaigns that the user is assigned to as an administrator. For more information, see section [Services and Campaigns - Assignments Tab](#).

Note that in order to assign teams to a service/campaign, the user must also have the *Manage teams* privilege.

Another privilege exists to enable the user to access all configured campaigns regardless of assignment (see above). Note that in order to prevent the user from creating new campaigns, both these privileges must be disabled.

## Manage lists

The *Manage lists* privilege gives the user full access to [calling lists](#) and [do-not-call \(DNC\)](#) lists. Absence of this privilege does not affect the user's ability to [associate existing lists with campaigns](#).

## Manage scenarios

The *Manage scenarios* privilege allows the user to create, view, and edit [scenarios](#). Absence of this privilege does not affect the user's ability to [configure scenario entries](#) and associate such entries with existing scenarios.

## Manage skills

With the *Manage skills* privilege, the user may create and edit existing [auxiliary skills](#) and [assign skills to agents](#) with specific levels.

## Use SMS/MMS API

This privilege allows the user to use the [SMS/MMS API](#) to send and receive SMS/MMS messages. Note that in addition to granting this privilege, the contact center administrator also must create a role, a user with the *Use SMS/MMS API* property, and generate an API key.

## Supervision group

### Access Real-time Stats API

The *Access Real-time Stats API* privilege gives the user access to applications that are connected to Bright Pattern Contact Center via the Real-time Stats API; this includes viewing the [wallboard application](#). **Note:** The availability of data on the Agent Desktop Home Screen is not affected by this privilege, with the exception of the wallboard icon.

### All assigned teams combined view

When enabled, this privilege will show, on the supervisor's home screen, the agents from all teams assigned to the logged in supervisor, specifically with the following metrics:

- State
- Time in State
- Not Ready Reason (if not ready for a reason)
- Team (new metric)
- Active interactions

It shows all services that are the teams are assigned to (individual services can be hidden if needed), specifically the following metrics:

- Calls in Queue
- Service Level

- # of Agents in Queue
- # of Ready Agents
- Current Max Wait Time (for calls in Queue)

## Can see contents of email push queues

This privilege allows supervisors of teams with [the push distribution method](#) enabled to view push queues. Push queue items appear in team queues when the “All Services with Push Queues” option is selected; however, it is possible to select only one service and see only its queue.

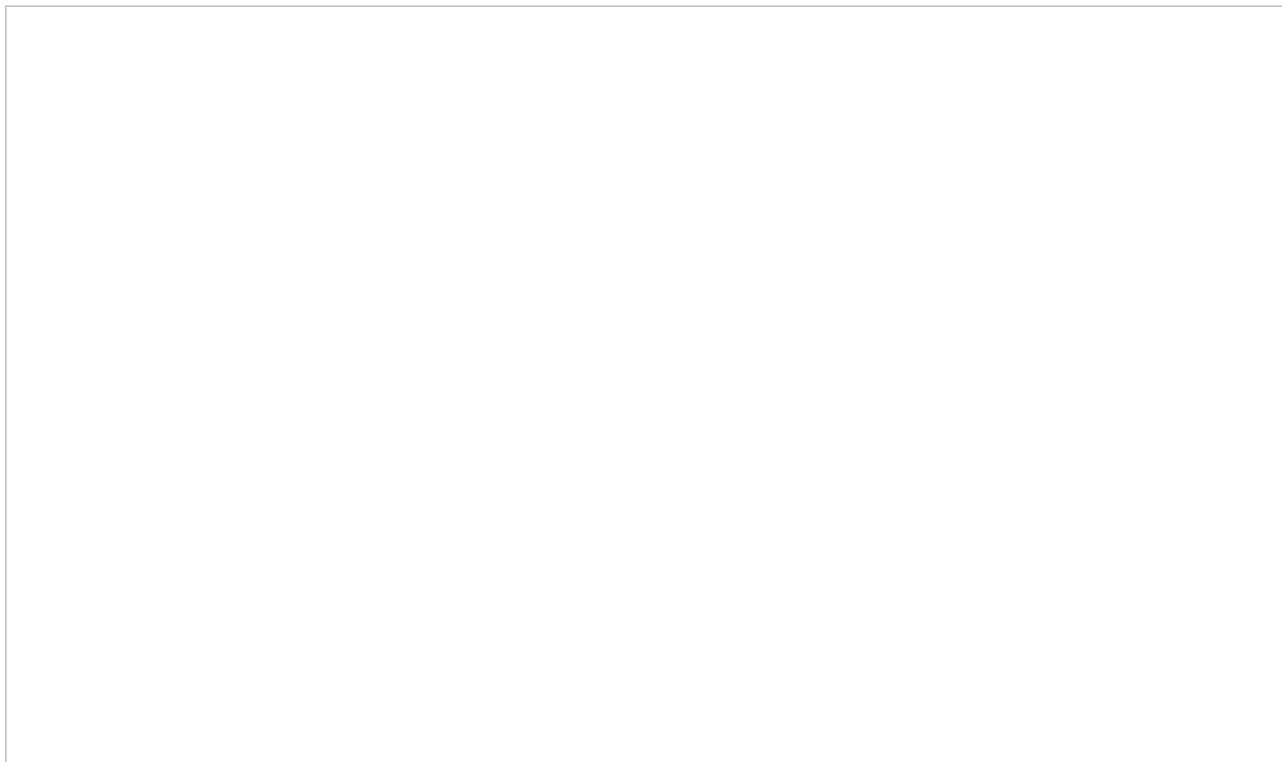
While looking at a push queue, a supervisor can:

- Sort the queue as they like (i.e., using existing pull queue sort controls)
- Assign an item to an agent
- Assign one or more items to another queue and skill requirement
- Open an item to work with
- Delete an item or mark it as spam

Note that this setting is not assigned to any roles by default.

## Can update final dispositions

This privilege enables users to update dispositions when final. A final disposition can be updated in the interaction record by clicking the Change Disposition  button.



Changing final disposition in Interaction Records Search Results record

For more information about interaction records, see section [Interaction Records Search](#) and [Search Results](#).

## Can use agent seat maps

This privilege provides users access to the Agent Seating Map application; it is required for creating and editing agent seating maps. For more information, see the [Agent Seating Map Guide](#).

## Change alert configuration

Users with the *Change alert configuration* privilege may enable/disable [alerts](#) available for some real-time metric displayed via Agent Desktop, change their appearance, and modify threshold values that trigger such alerts.

Note that the ability to set configured alerts as system-wide defaults is controlled via a separate privilege (see *Set alerts for real-time metrics system-wide*).

If the user does not have this privilege, the Alert Configuration dialog of the Agent Desktop will provide read-only information about the current alert configuration.

## Change real-time metric views

The *Change real-time metric views* privilege allows the user to add metrics to, and remove them from, any [real-time metric views](#) of the Agent Desktop application. The user may also change the order in which the metrics appear in the table views.

Absence of this privilege does not affect the user's ability to add services and campaigns to, and remove them from, real-time metric views.

Note that the ability to set created real-time metric views as system-wide defaults is controlled via a separate privilege (see *Set real-time metric views system-wide*).

## Customize Wallboards

The *Customize Wallboards* privilege allows additional elements to appear on the user's wallboard. These elements include title, selector, flip arrows, and menu. Using these elements, users can customize the look and display of their Agent Desktop wallboard. Using the Wallboard Layout Editor, cards and cells can be added, deleted, scaled, and expanded using mouseovers, click-and-drag, and drag-and-drop movements.

## Define/View subteams of selected agents

The privilege *Define/View subteams of selected agents* enables subteam controls to be displayed in Agent Desktop and the Reports portal. In addition, the privilege allows users to switch between them. Subteams are smaller groups of agents that supervisors have selected from full teams.

## Delete cases

The *Delete cases* privilege allows the deletion of cases. If enabled, users can delete individual cases via the Agent Desktop. When a case is deleted, all interactions related to a case are deleted.

## Download recordings and transcripts

With this privilege, the user may download [call/screen recordings](#), [chat transcripts](#), and [email messages](#) from the interaction search and review pages of the Contact Center Administrator application.

## Force agent states

The *Force agent states* privilege allows the user to [change current agent states](#) of members of any team that the user is assigned to supervise.

## Listen to recordings linked to external CRM records

This privilege allows the user to listen to call recordings linked to activity history in the CRM records.

## Listening to all call recordings and view all chat transcripts

With *Listening to all call recordings and view all chat transcripts*, the user may [review voice recordings and chat transcripts](#) via the Contact Center Administrator application.

Absence of this privilege does not affect the user's ability to review screen recordings in the [Agent Timeline](#) or email messages in the [Interaction Search](#).

When removing this privilege from a user, make sure this user also does not have the privilege *Listen to call recordings and view chat transcripts for assigned services* in the *BPO Client* group (see below).

## Manage canned chat responses system-wide

The *Manage canned chat responses system-wide* privilege allows the user to make canned chat responses available to all other agents of the contact center. For more information, see section [How to Create and Edit Canned Chat Responses](#) of the *Agent Guide*.

## Monitor agent screen

When enabled, the *Monitor agent screen* privilege allows the user to view and monitor the screens of a selected agent that the user is assigned to supervise.

## Monitor interactions

The *Monitor interactions* privilege allows the user to connect to calls handled by agents that the user is assigned to supervise in [silent monitoring, coaching, and barge-in modes](#). For more information, see section *Call Monitoring, Coaching and Barge-In* of the *Supervisor Guide*.

## Pull screen pop

*Pull screen pop* allows the user to [get snapshots of the Context Information Area](#) of the desktops of agents that the user is assigned to supervise. Note that in order to be able to get a snapshot, the user must be connected to the agent in one of the call monitoring modes. Thus, the user also must have the privilege *Monitor interactions* (see above).

## Push/Pull Global Wallboards

Users with the privilege *Push/Pull Global Wallboards* can push their personal wallboards to other users and/or teams, as well as pull shared wallboards from a global pool. Note that only global wallboards can be pulled.

## Set alerts for real-time metrics system-wide

This privilege allows the user to [set alerts](#) that the user configures as system-wide defaults. Note that in order to use this privilege, the user must also have privilege *Change alert configuration*.

## Set real-time metric views system wide

*Set real-time metric views system wide* allows the user to set real-time metric views that the user configures as system-wide defaults. Note that in order to use this privilege, the user must also have the privilege *Change real-time metric views*.

For more information, see section [Customization of Metric Views](#) of the *Supervisor Guide*.

## View historical reports

The *View historical reports* privilege allows the user to [generate and view reports](#) via the Contact Center Administrator application. Absence of this privilege does not affect the user's ability to access any of the general reporting settings or be a recipient of emailed scheduled reports.

## View interaction records

With this privilege, the user may [search for and review interaction records](#) via the Contact Center Administrator application.

Absence of this privilege does not affect the user's ability to generate and view the [Call Detail Report](#) or [Email Detail Report](#). To prevent access to these reports, use privilege *View historical reports* (see above).

## View real-time agent metrics

*View real-time agent metrics* allows the user to [view real-time metrics for the agents](#) of the teams that the user is assigned to supervise.

## View real-time service metrics

With *View real-time service metrics*, the user may [view real-time metrics for all services](#) associated with the teams that the user is assigned to supervise.

Absence of this privilege does not affect the user's ability to [view campaign-specific metrics](#). To prevent access to these metrics, use privilege *Control campaign operations* (see above).

## Watch agent screen recordings

The privilege *Watch agent screen recordings* allows supervisors to search for and view the screen recording sessions of agents on their teams. The screen recordings appear in interaction records in agent timeline searches. If a screen recording is available for the selected agent, and if the privilege is enabled, then the *Watch screen recording* button is shown to the supervisor.

## System Administration group

Privileges associated with system administration are described as follows.

### Allow recording export API access

This privilege allows users to access the [Interaction Content API](#) that retrieves call recordings and metadata based on the call identifier.

### Bulk Export/Import Contacts

When enabled, the privilege *Bulk Export/Import Contacts* allows the export/import icon on the Agent Desktop Contacts screen to be shown.

### Bypass Single Sign-On

Users with this privilege can log in to any Bright Pattern application (e.g., Contact Center Administrator, Agent Desktop, etc.) via a direct authentication method (i.e., with Bright Pattern username and password), even if a corporate-level single sign-on (SSO) is configured for the given contact center.

Users without the privilege should not be able to log in with their Bright Pattern credentials when SSO is enabled; they should, however, be able to log in when it is disabled. By default, this privilege is enabled only for the pre-defined System Administrator role.

If SSO is configured for a contact center, users with this privilege can bypass single sign-on by using special URLs that take the following form:

`https://<tenant.domain.com>/admin/?bypass-sso=1`

`https://<tenant.domain.com>/agentdesktop/?bypass-sso=1`

## Configure Contact Forms and fields

The *Configure Contact Forms and field* privilege allows users to edit contact, activity history, and augmentation and case forms.

## Configure directory

The *Configure directory* privilege allows the user to [create and modify external contacts](#) that appear in the [Directory](#) of the Agent Desktop application.

## Manage BPO Clients

When enabled, the *Manage BPO Clients* privilege allows users to:

- Create, edit, and delete BPO clients in the Contact Center Administrator application
- Assign forms and teams to BPO clients

## Manage all teams

If granted the *Manage all teams* privilege, the user may

- create teams and change configuration of all existing users and teams
- create users and change configuration of existing users, provided that the user also has the *Manage users* privilege (see below)
- assign skills to, and change skill levels of, all existing agents, provided that the user also has the *Manage skills* privilege (see above)

For more information, see sections [Users](#), [Teams](#), and [Skill Levels](#).

Note that if a user is assigned as a supervisor of a particular team, the absence of this privilege does not affect the user's ability to change most of the configuration settings of the given team and its current members.

## Manage phones

The *Manage phones* privilege gives the user full access to configuration of [softphones](#), [hardphones](#), [access numbers](#), and [scenario entries](#). Absence of this privilege does not affect the user's ability to assign phone numbers to users.

## Manage users

The *Manage users* privilege allows the user to create [users](#) and change the configuration of existing users within the team he is part of or that he is a supervisor of.

## Privileged Access IP Range

The *Privileged Access IP Range* privilege allows users (e.g., administrators) to be able to log in to the system from any IP address (e.g., a public place such as a coffee shop). Without this privilege, users can only log in from specific IP addresses.

## **Publish help**

*Publish help* gives the user full access to configuring [help screens](#).

## **View audit log**

With the *View audit log* privilege, the user can view the [audit log](#).

## **View usage data**

The *View usage data* privilege allows the user to access to reports about usage of telecom carriers' resources via *Contact Center Administrator > Reports > Usage*.

## **BPO Client group**

### **Listening to call recordings and view chat transcripts on services in reviewer role**

With this privilege granted, the user may listen to [call recordings](#) and view [chat transcripts](#) of the services to which the user is assigned as a [reviewer](#).

# **Integrations**

The tutorials in this section offer step-by-step instructions on how to configure integration accounts for your contact center.

For more on integrations, see the *Contact Center Administrator Guide*, section [Integration Accounts](#).

## **Tutorials**

### **Integration Account Configuration**

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

### **Remote Assistance**

- [LogMeIn Integration Quick Start](#)

### **Single Sign-On (SSO) Integration Accounts**

- [How to Configure Microsoft Azure AD SSO](#)
- [How to Configure Okta SSO](#)



