5.8 Application Notes

Bright Pattern Documentation

Generated: 1/26/2022 11:25 pm

Table of Contents

Agent Desktop Helper Application Audio-Handling Options

If your contact center requires the use of theAgent Desktop Helper Application, note that you have the capability to control the audio-handling options via the **librtc.ini** file.

After installing and first launching the Agent Desktop Helper Application, this file is automatically created when making the first phone call from the Agent Desktop application; the file is accessible from the following locations:

- For Linux: **/home/<<username>>/.librtc**
- For macOS: **/Users/<<username>>/.librtc**
- For Windows: **/Users/<<username>>**

The following table contains the configurable options from this file.

Option Name	Default Value	Description
automatic_gain_control	0	If set to 1, this option helps the microphone maintain a suitable signal amplitude. Turning this on might amplify echo, so if echo cancellation is not sufficient, keep this off.
echo_control	1	If set to 1, this option removes echo (i.e., sounds from speakers that are reflected back into the microphone). Note that turning this setting off does not necessarily introduce echo, as most USB headsets have echo-cancelling hardware. Additionally, turning this setting off might be beneficial for voice quality.
highpass_filter	0	If set to 1, this option removes low-frequency noises (e.g., the rumble of an air conditioner, wind noise, etc.).
noise_suppression	0	If set to 1, this option removes background noises.

WebRTC Considerations

WebRTC is an open-source project that allows secure (i.e., encrypted) real-time communications in web browsers. Starting from version 5.5.0, Bright Pattern Contact Center software includes the Secure phone via browser audio (Web RTC) phone device option.

If you will be using this option in your contact center, please note the following.

All Browsers

- Your computer's speaker device may not be reliably reported by your web browser. Because of this, Bright Pattern Contact Center software uses your computer's microphone to indicate which audio device is being used.

- If WebRTC is the only phone device option allowed in your contact center, the following functionalities are not supported **unless** the BPClient plugin is installed:
  - Screen monitoring (i.e., a user can monitor others, but they cannot be monitored)
  - Screen recording
  - The GUI popup for inbound interactions (i.e., outside of the web browser window)
  - Client-side diagnostic logging (i.e., BPClient.log)
  - Audio notifications through all audio devices (e.g., ringing on all devices)
  - The Simplified Desktop .NET API
  - Business user presence detection (i.e., system input activity tracking)
  - The G.729 codec
  - For Salesforce.com integrations, the CTI phone in Salesforce Classic
- **Note**: In order to use screen monitoring, both users (i.e., the host of the monitoring and monitored user) should have the BPClient plugin installed.
- Starting from Bright Pattern Contact Center version 5.5.0, the following codecs are supported:
  - For browsers that support WebRTC:
    - G.711 mu-law, a-law, G.722
  - If the Agent Desktop Helper Application plugin is used (i.e., both secure and regular mode):
    - Above + G.729

Firefox

- The Firefox web browser cannot use a microphone if it was plugged in **after** the browser was started; however, it works if there is another microphone registered in the system. In other words, adding a second or third microphone is supported, but adding the first one is not. The only workaround is to restart the entire browser.
- Events about audio device changes may be delayed if a frame with Agent Desktop is out of focus. Bringing it into focus enables the events.

Safari

- The *Allow All Auto-Play* option must be enabled for your contact center's website; this setting is required to play ring tones as well as WebRTC audio. To enable this setting, take the following steps:
  - When you are at your contact center's website, from the *Safari* menu, select *Settings for This Website*.
  - In the pop-up window, locate the *Auto-Play* option.
  - From the pop-up window, select the **Allow All Auto-Play** option.
- Note that audio may not start if a frame with Agent Desktop is out of focus. Bringing it into focus starts the audio.

Internet Explorer

- The Internet Explorer (IE) web browser does not support WebRTC.

Updating IBM Cloud URL Endpoints

On May 26, 2021, IBM Cloud will be retiring the *watsonplatform.net* URL endpoint and moving to *watson.cloud.ibm.com*. This change affects all contact centers with integration accounts configured with the deprecated *watsonplatform.net* URL, including Watson Assistant, Watson Assistant (Legacy), Natural Language Understanding (NLU), Speech to Text (STT), and Text to Speech (TTS).

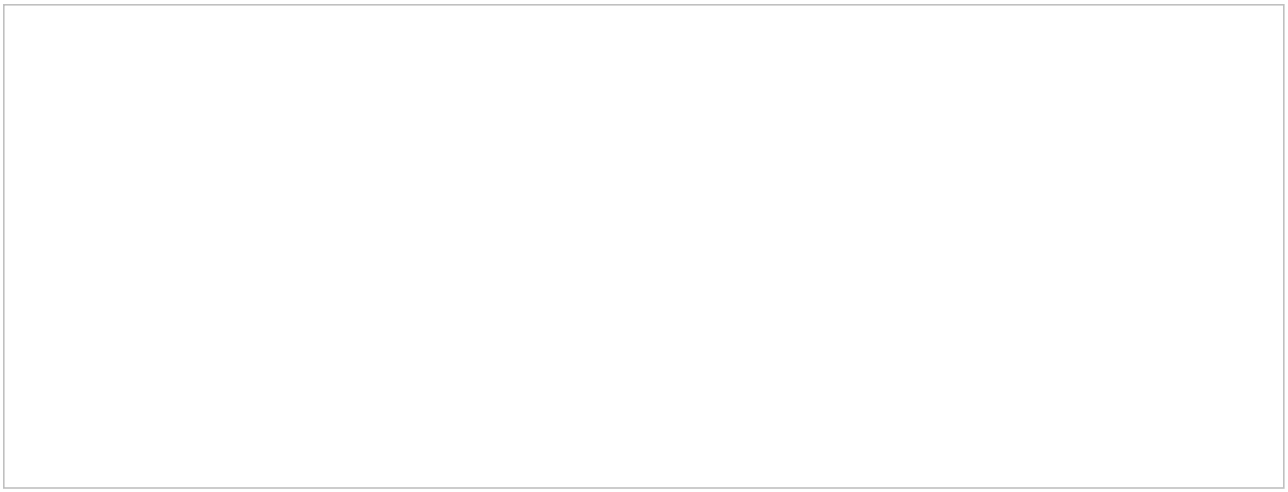
In order to continue using configured Watson Assistant integrations, you must update the URL in the properties for all IBM Watson integration accounts.

Depending on when your IBM Watson service was created, the URL might already include the new *watson.cloud.ibm.com* URL endpoint. Thus, it is important to check the service credentials for all Watson Assistant services that are in use, and update them if necessary.

Procedure

To update the URLs, follow these steps:

1. Log in to your IBM Cloud account, and go to your Resource list.
2. Click into the name of each service in the Resource list to access that service's credentials.
3. Create a new credential for each Watson service that is used in your contact center integration accounts.

   Create a new credential from the Service credentials tab

4. After the new credential has been generated, click the **Manage** tab and copy the new URL (e.g., "https://api.us-south.assistant.watson.cloud.ibm.com/instances/12c34291-0a02-4137-8269-13a1a123456c").
5. In the Contact Center Administrator application, section *Call Center Configuration* > *Integration Accounts*, select the corresponding integration account (e.g., Watson Assistant bot/chat suggestion integration account) from the list to display its properties.
6. In the URL property, if the existing URL shows the old*watsonplatform.net*, edit the URL accordingly so that it takes the form **api.{location}.{offering}.watson.cloud.ibm.com**:
   1. For Watson Assistant integration accounts:

      http[s]://{new service credential}/assistant/v1/workspaces/{skill id}/message

Example: https://api.us-south.assistant.watson.cloud.ibm.com/instances/12c34291-0a02-4137-8269-13a1a123456c/v1/workspaces/12c3a41e-ad2e-341c-12d3-412341ffdffd/message

2. For Watson Assistant (Legacy) integration accounts:

   http[s]://{new service credential}/assistant/v1/workspaces/{skill id}/message

   Example: https://api.us-south.assistant.watson.cloud.ibm.com/instances/12c34291-0a02-4137-8269-13a1a123456c/v1/workspaces/12c3a41e-ad2e-341c-12d3-412341ffdffd/message

3. For Natural Language Understanding integration accounts:

   http[s]://api.{location}.natural-language-understanding.watson.cloud.ibm.com

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

4. For Speech to Text integration accounts of type Watson:

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

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

5. For Text to Speech integration accounts of type Watson:

   http[s]://api.{location}.text-to-speech.watson.cloud.ibm.com/instances/{instance id}

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

7. In the API key property, replace the existing key with the API key copied from your new Watson service credentials.

8. Click **Apply** to save your changes, and repeat these steps for all affected integration accounts. Remember, all URLs must take the form **api.{location}.{offering}.watson.cloud.ibm.com**.

For more information about the change to the URL endpoint, see IBM Cloud documentation.

Microsoft Teams Integration Configuration Overview

Microsoft Teams integration enables contact center users to access Teams communication channels information for internal calls and chats with Teams users (i.e., experts) while working in Bright Pattern Contact Center's Agent Desktop application.

This integration allows the following types of users to interact via Teams and Bright Pattern Contact Center:

- **Agents** - The contact center agents logged in to Bright Pattern
- **Experts** - The knowledge workers logged in to Teams

- **Administrators** - The users who configure the integration (i.e., you)

Tutorials

The Microsoft Teams Integration Configuration Guide provides the following tutorials to help you to configure Teams integration:

- Microsoft Teams Integration Configuration Quick Start
- Azure Application Configuration to Enable Directory and Chat Integration
- Microsoft Teams Direct Routing
- How to Add a Microsoft Teams Integration Account

For information about how to use Teams integration in the Agent Desktop application, after configuration is complete, see the *Agent Guide*, section *Tutorials > Microsoft Teams*.

Features and Limitations

Teams integration provides Bright Pattern Contact Center users with access to some, but not all, features and functions of the Microsoft Teams application from within the Bright Pattern Agent Desktop application.

This section describes the features and functionalities that are currently supported and not supported for agents using Teams integration in Agent Desktop.

What Is Supported

The following features or functionalities are supported by Teams integration:

- Agents who have enabled Microsoft Teams in their User Profile may view and open the Teams Chats folder and Teams Channels folder in the Agent Desktop Directory.
- Agents can have one conversation per Teams channel at any time.
- Agents must close and reopen the Directory's Teams Chats folder in order to receive notifications of chat replies from Teams users or to have incoming messages from Teams users popped to the agent's screen.
- Agents can mark chats and Teams channels as a Favorite.
- In chat conversations, agents can view only the file names of attachments sent by Teams users.
- Agents and web chat customers can see the content type of Teams-rich content elements—including streams, extensions (e.g., Zoom meetings, stocks, and weather), files, and code snippets. They will not see the actual content.

What Is Not Supported

The following features or functionalities are not supported by Teams integration:

- Group chats with multiple Teams users are not supported. This means that agents can only chat with one Teams user at a time, and the Agent Desktop Directory's Teams Chats folder will not display group chats.
- The ability to invite Teams users to join internal group chat conversations is not supported.
- Chat message reactions (e.g., Like, Heart, Laugh, etc.) are not supported, so reactions by Teams users will not

be shown in Agent Desktop.

- The ability for agents and customers to download attachments sent by Teams users during external chats is not supported. Agents and customers can only view the file names of attachments
- Agents cannot mark individual Teams chat messages as a Favorite. They can only mark Teams Channels as a Favorite.
- The display of Teams-rich content elements—including streams, extensions (e.g., Zoom meetings, stocks, and weather), files, and code snippets—during Teams conversations is not supported.
- Hold time by Teams users is not reflected in the Call Detail report, in the same way that hold time by non-agent parties is not reflected in the Call Detail report.
- Rich content (e.g., chat transcripts) in Interaction Records is not supported.
- When a Teams user is invited to the voice conference and the call is placed on hold, the remaining participants will hear the hold music.

Microsoft Teams Integration Configuration Quick Start

Bright Pattern Contact Center's Microsoft Teams integration enables contact center agents to access Teams communication channels information for internal calls and chats with logged-in Teams users (i.e., experts), while handling customer interactions in the Agent Desktop application. The integration supports internal chat and call capabilities with Teams experts, directory access to Teams users and channels, and user-presence visibility in the directory.

Integration configuration involves several key steps: enabling the integration on the service provider level, creating an application in the Microsoft Azure Active Directory with Microsoft Graph delegated permissions and application permissions, creating a Microsoft Teams integration account on the contact center level, and enabling the agent's Microsoft Teams account to be used on the agent level.

This quick start tutorial will guide you through the integration configuration process.

Procedure

Step 1: Check that Integration with Microsoft Teams is enabled

Microsoft Teams integration is enabled by service providers.

To check that integration is enabled, log in to the Contact Center Administrator application and try adding a Microsoft Teams integration account. If the integration is enabled, you will see Microsoft Teams as an available integration account type. If the integration is disabled, you will not see Microsoft Teams at all.

For assistance with enabling the integration, please contact your service provider.

Step 2: Register a new application in the Azure Active Directory

The integration uses an Azure Active Directory registered application to represent the Enterprise Messenger Integration (EMI) Server. The EMI Server uses Microsoft Graph API subscriptions to receive events from Teams, such as chat creation, chat changes, new chat messages, and so forth. The EMI Server exposes the webhook to the Internet so that Microsoft servers may call it to send event notifications.

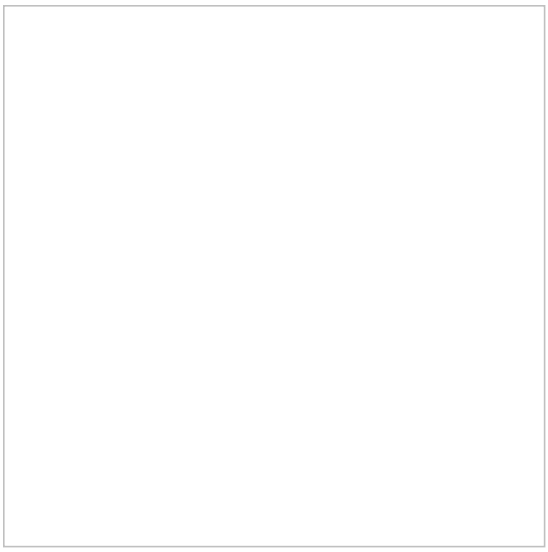
1. In the Azure Active Directory, register a new application to represent the Enterprise Messenger Integration

(EMI) Server. Please see Configuring the Microsoft Graph API as an Authentication Mechanism for Secure Microsoft Teams Content for detailed instructions.

2. To check that the application is configured correctly, log in to the Contact Center Administrator application, add a Microsoft Teams integration account, set the properties for the account, and click the **Test connection** button. Testing the connection will provide you with either a success message or an error message.

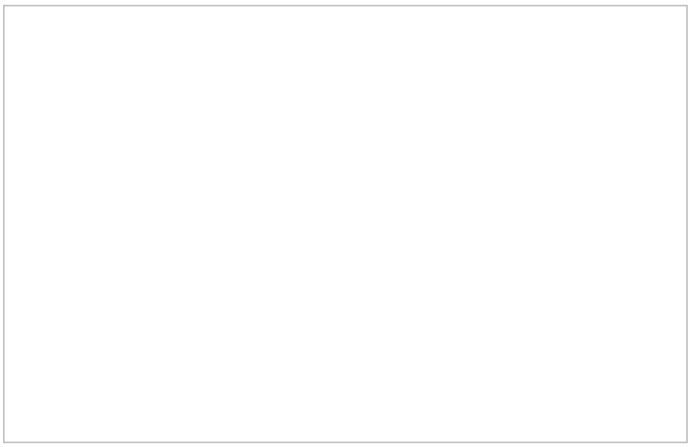
Step 3: Add a Microsoft Teams integration account

1. In the Contact Center Administrator application, section *Call Center Configuration* > *Integration Accounts*, click **+** to add a new integration account, and select **Microsoft Teams**.



Select the Microsoft Teams integration account type

Please note that your contact center is allowed only one instance of a Microsoft Teams integration account. If you wish to create a different Microsoft Teams integration account, you must delete the existing instance. Deleting an existing Microsoft Teams integration account will disable access for all users in the account. Upon creating a new Microsoft Teams integration account, all users in the account will need to re-enable Teams integration in their Agent Desktop user profiles.



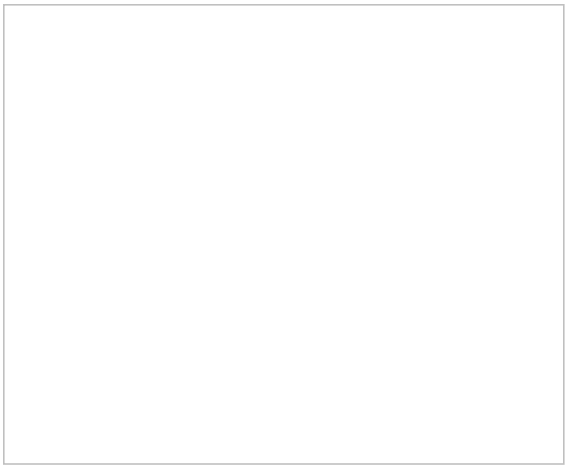
System message reminding you what happens when you disable Teams integration

2. Fill in all the properties for the integration account and click **Apply** to save your changes.

3. To test the connection between Bright Pattern and Teams, log in to the Agent Desktop application as an agent, go to *Settings* > *User Profile*, click the **Enterprise Messaging Accounts** tab, and click **Enable**. Follow the prompts to sign in to your Microsoft account.

   Signing in to Microsoft allows you to access Teams Channels and Teams Chats in the Agent Desktop directory. If the integration account is configured correctly, you should see Microsoft Teams Channels and Microsoft Teams Chats folders in the directory.

   The Microsoft Teams Chats folder will display chats if one or more Teams users have already established a 1:1 chat with the logged-in agent. The Microsoft Teams Channels folder will display a list of channels from all the teams with which the logged-in agent has participated.

   Microsoft Teams Channels and Microsoft Teams Chats folders in the directory

---

The Microsoft Teams integration configuration process is now complete.

Configuring the Microsoft Graph API as an Authentication Mechanism for Secure Microsoft Teams Content

Microsoft Teams integration uses an Azure Active Directory registered application to represent the Enterprise Messenger Integration (EMI) Server.

The EMI Server uses Microsoft Graph API subscriptions to receive events from Microsoft Teams, such as chat creation, chat changes, new chat messages, and so forth. Additionally, some content from the Microsoft Teams application, such as photos and GPS locations, requires authentication, which is processed by Microsoft Graph API requests via the EMI Server. The EMI Server exposes the webhook to the Internet so that Microsoft servers may call it to send event notifications.

The Graph API limits the specific client application to have only one subscription on each resource, which means that only one instance of the EMI Server may subscribe to notifications from specific Azure Active Directory tenants, and only one EMI Server/Azure application may be used per Azure Active Directory tenant. Please note that all users of the same Azure Active Directory tenant will be served by a single instance of the EMI Server.

This article describes how to do the following:

- Register a new application in the Azure Active Directory to represent the Enterprise Messenger Integration (EMI) Server.
- Set a webhook (i.e., redirect URI).
- Set permissions for the application to use the Microsoft Graph API.
- Set a client secret (i.e., token).

Prerequisites

- Be the Microsoft Teams administrator for your contact center.
- Have administrator privileges and permissions in the Microsoft Azure portal.

Procedure

1. Register an application in the Azure Active Directory

1. Log in to the Azure portal. From the Azure Dashboard, navigate to*Azure Active Directory* > *App registrations*.

2. Click **+ New registration** to register a new application. This application will represent the EMI Server and provide API credentials (tokens) so that the EMI Server may authenticate with the Microsoft Graph API.

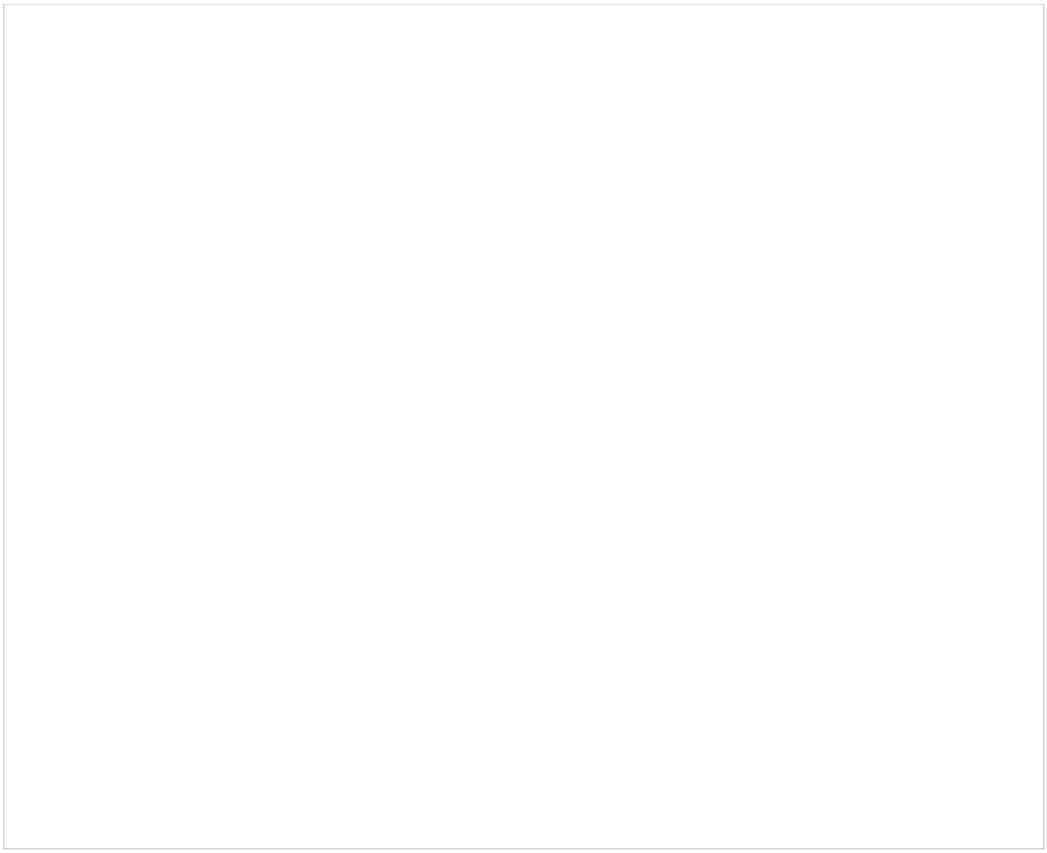
   Azure Active Directory > App registrations > + New registration

3. In *Register an application*, set the following properties:

   1. **Name** - Type a name for the registered application.

   2. **Supported account types** - Select “Accounts in this organizational directory only (<your company’s Azure AD directory name> - Single tenant”).

   3. **Redirect URI** - Select “Web” and set “https://<tenant_url>/agentdesktop/msteamscallback.html” (e.g., https://yourcompany.brightpattern.com>/agentdesktop/msteamscallback.html).



”Register an application” properties

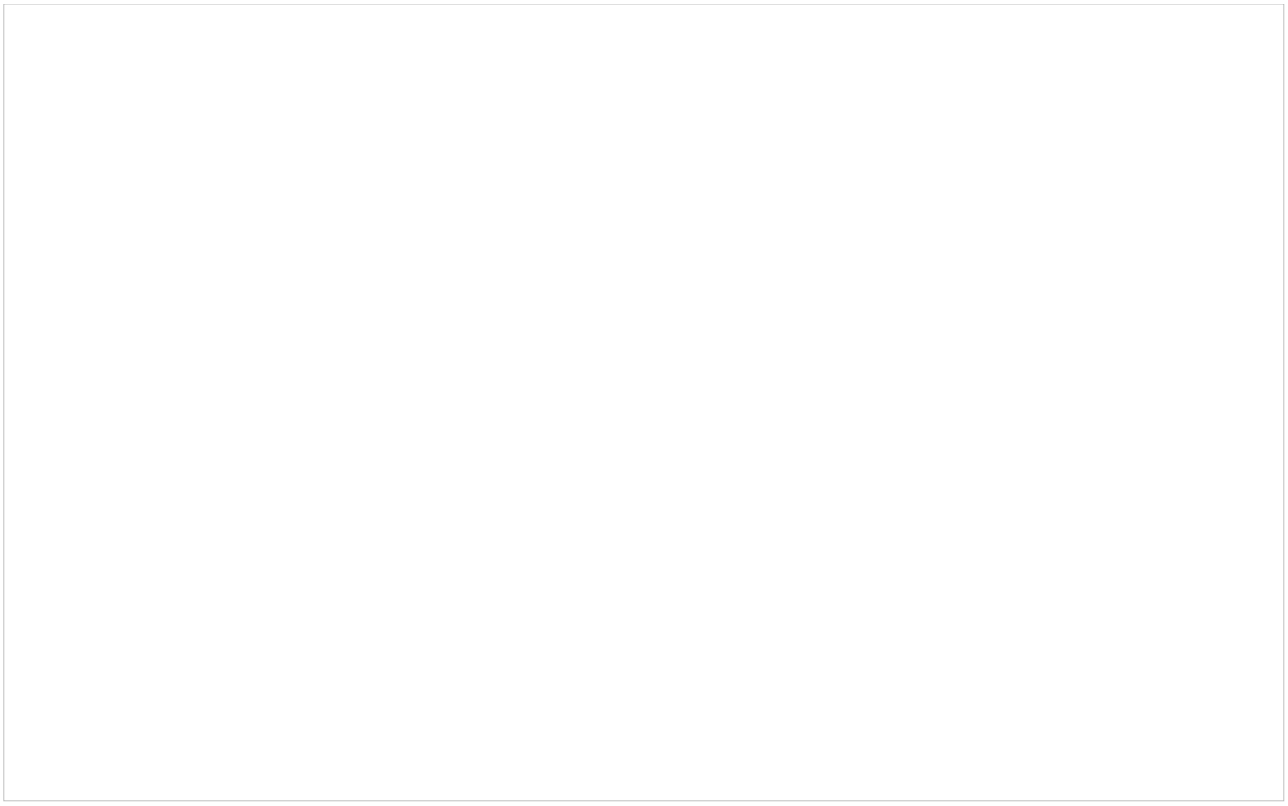
4. Click **Register**. After registration, your new app’s dashboard will display.

2. Add a new client secret for the application

1. From the app’s dashboard, go to *Manage* > *Certificates & secrets*.

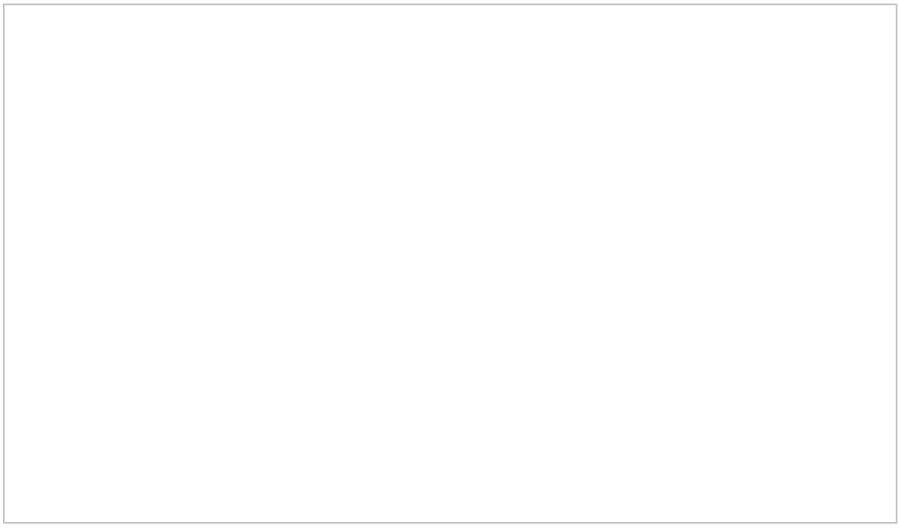
From the app dashboard, “Certificates & secrets” in the side menu

2. On *Certificates & secrets*, scroll down to the *Client secrets* section and click **+ New client secret**. (Note that adding a certificate is optional.)



In Certificates & secrets, go to the Client secrets section to generate a new client secret

3. In *Add a client secret*, set the description of what the secret is for, set the expiration to longest option possible or as your contact center's own security policy requires, and then click **Add**. Note that the *Custom* option currently allows 10+ years.



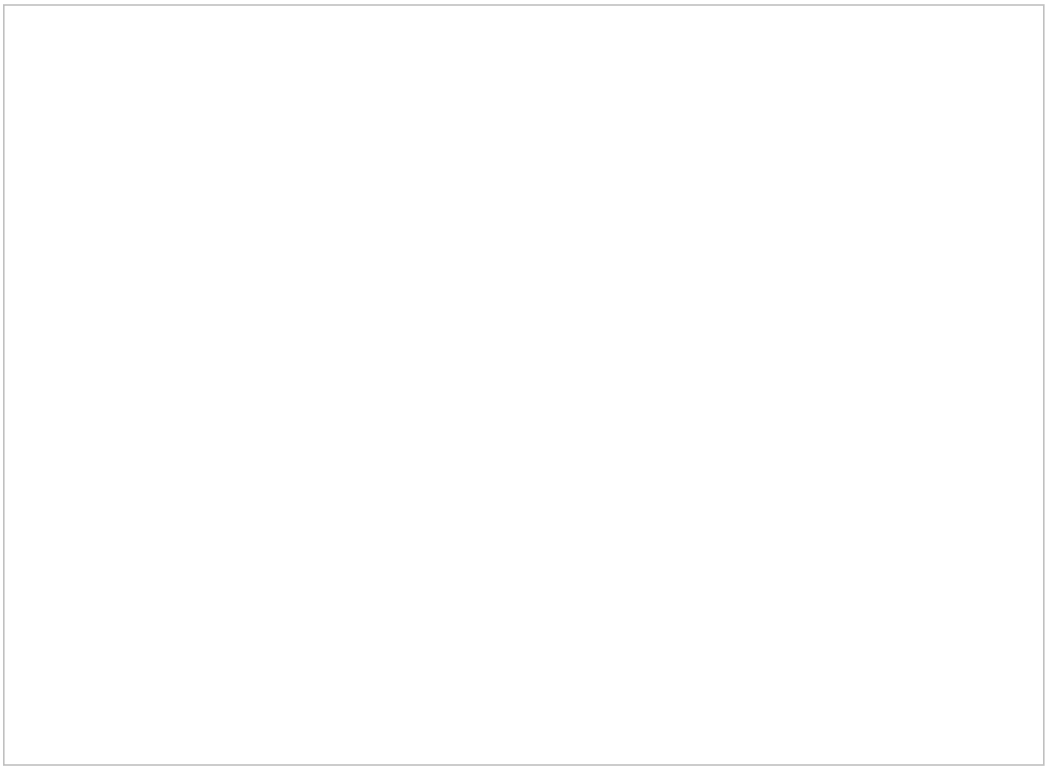
In “Add a client secret,” name it and set the expiration

4. Copy the **client secret value** and save it somewhere safe now because it is only shown once. Make sure you copy the **value** (not the ID).

Copy the client secret value

3. Set required API permissions

1. Microsoft Teams integration requires certain delegated permissions and application permissions for the Graph API. Set permissions by going to the app's *API permissions* section and clicking **+ Add a permission**.

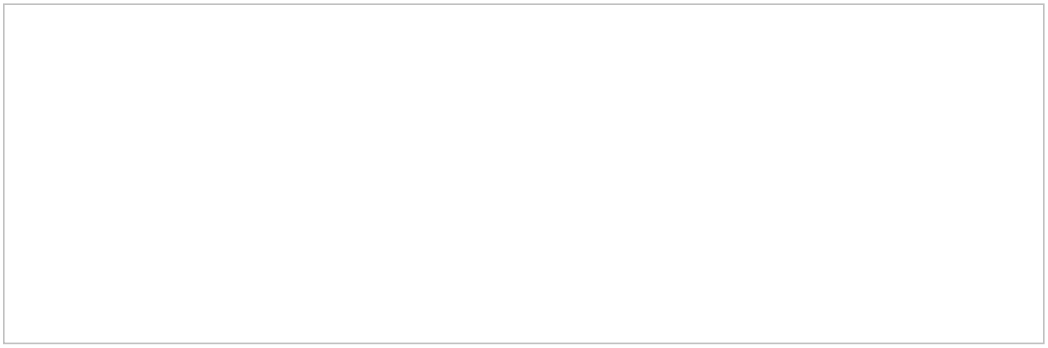


In API permissions, click "+ Add a permission"

2. From *Request API permissions*, click the "Microsoft APIs" tab and select **Microsoft Graph**.

Select Microsoft Graph

3. Select **Delegated permissions**.



For Microsoft Graph, select “Delegated permissions”

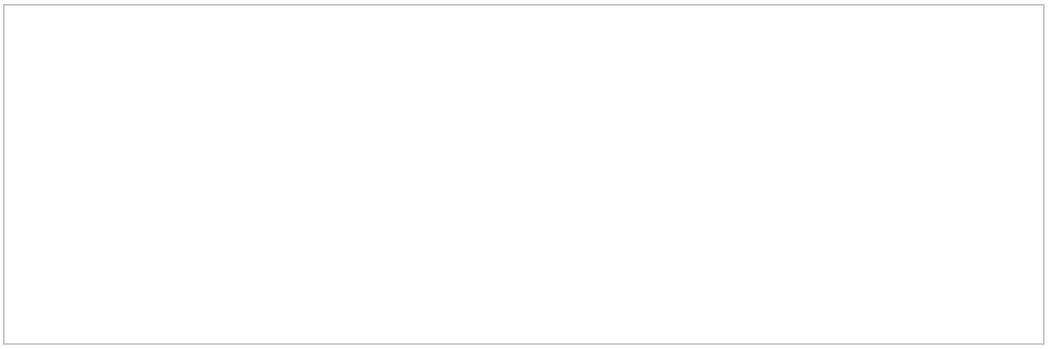
4. Copy and paste each of the following permission names into the Search field, expand the permission’s options, select the checkbox for it, and click **Add permission**. Note that most of these permissions require admin consent, and you should add each of them separately.

   Add the following delegated permissions:

   1. Chat.ReadWrite
   2. ChatMessage.Send
   3. ChannelMessage.Send
   4. Directory.Read.All
   5. Group.Read.All
   6. Presence.Read.All

7. Subscription.Read.All
8. User.Read.All

5. Go back to *Request API permissions* > *Microsoft Graph API*, and this time, select **Application permissions**.



For Microsoft Graph, select “Application permissions”

6. Copy and paste each of the following permission names into the *Search* field, expand the permission’s options, select the checkbox for it, and click **Add permission**. Note that most of these permissions require admin consent, and you should add each of them separately.

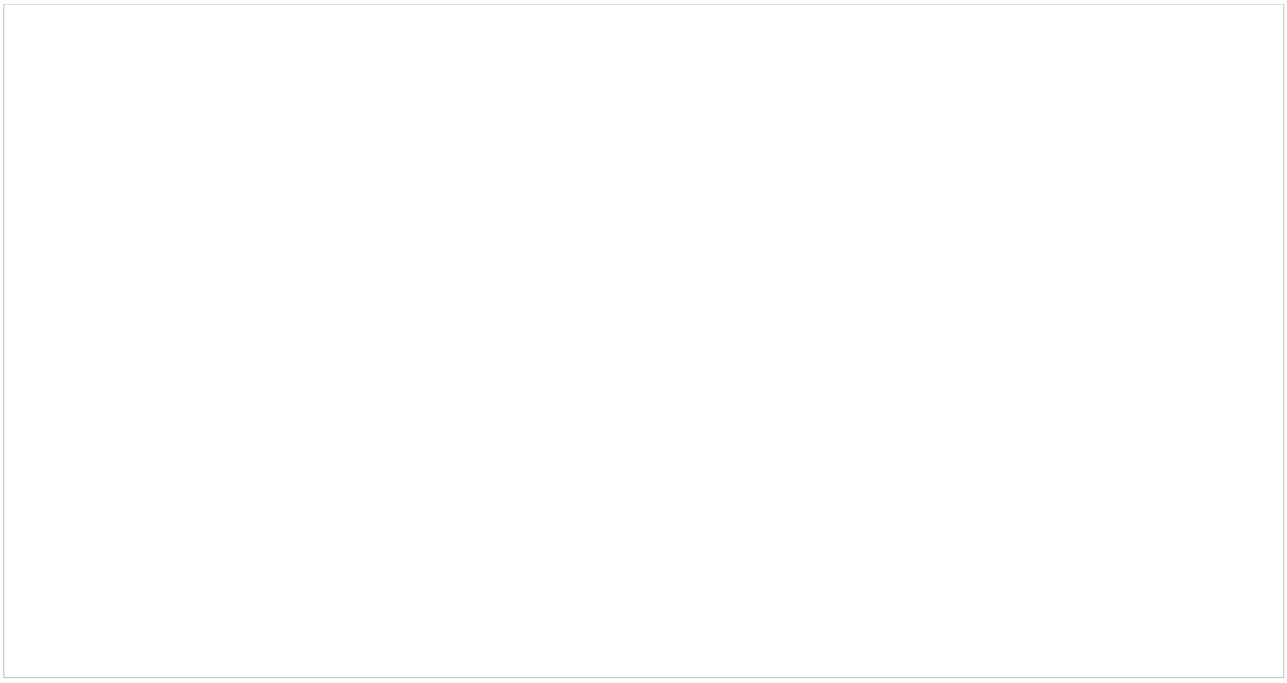
   Add the following application permissions:

   1. Chat.ReadWrite.All
   2. ChannelMessage.Read.All
   3. User.Read.All

7. After all the permissions are added, click the **Grant admin consent for <your organization>** button to authorize the Graph API to be used.

Remember to click “Grant admin consent for <your organization>”

If you are successful, the status for each permission should be “Granted.”

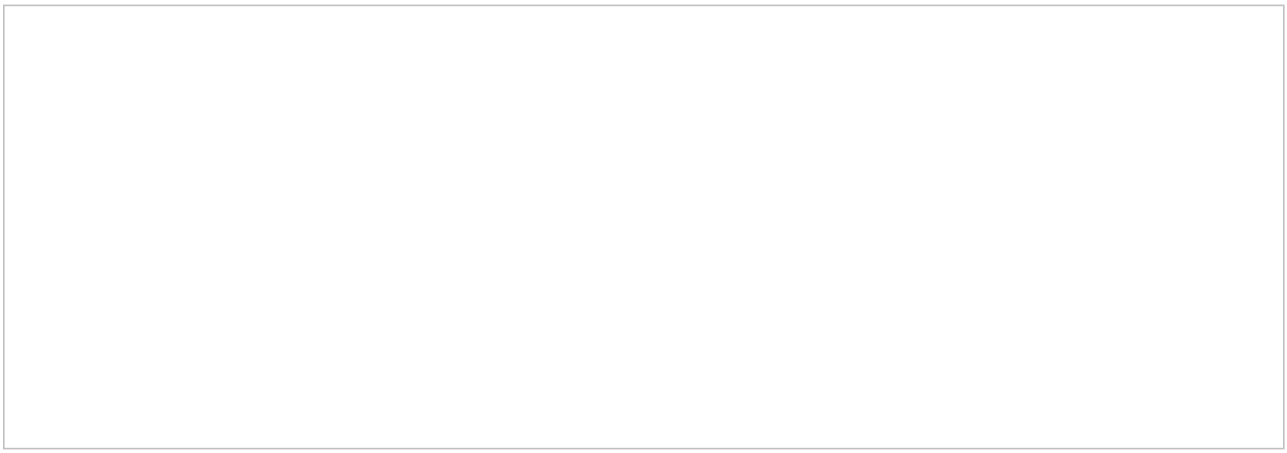


Example list of Microsoft Graph permissions granted

4. Copy your credentials

In order to configure a Microsoft Teams integration account in Bright Pattern Contact Center (see section Microsoft Teams Integration Account) you will need to copy the following items from your Azure Active Directory account and registered app:

- **Tenant ID**, which is found in *Azure Active Directory* > *Dashboard* > *Your registered app* > *Overview*.

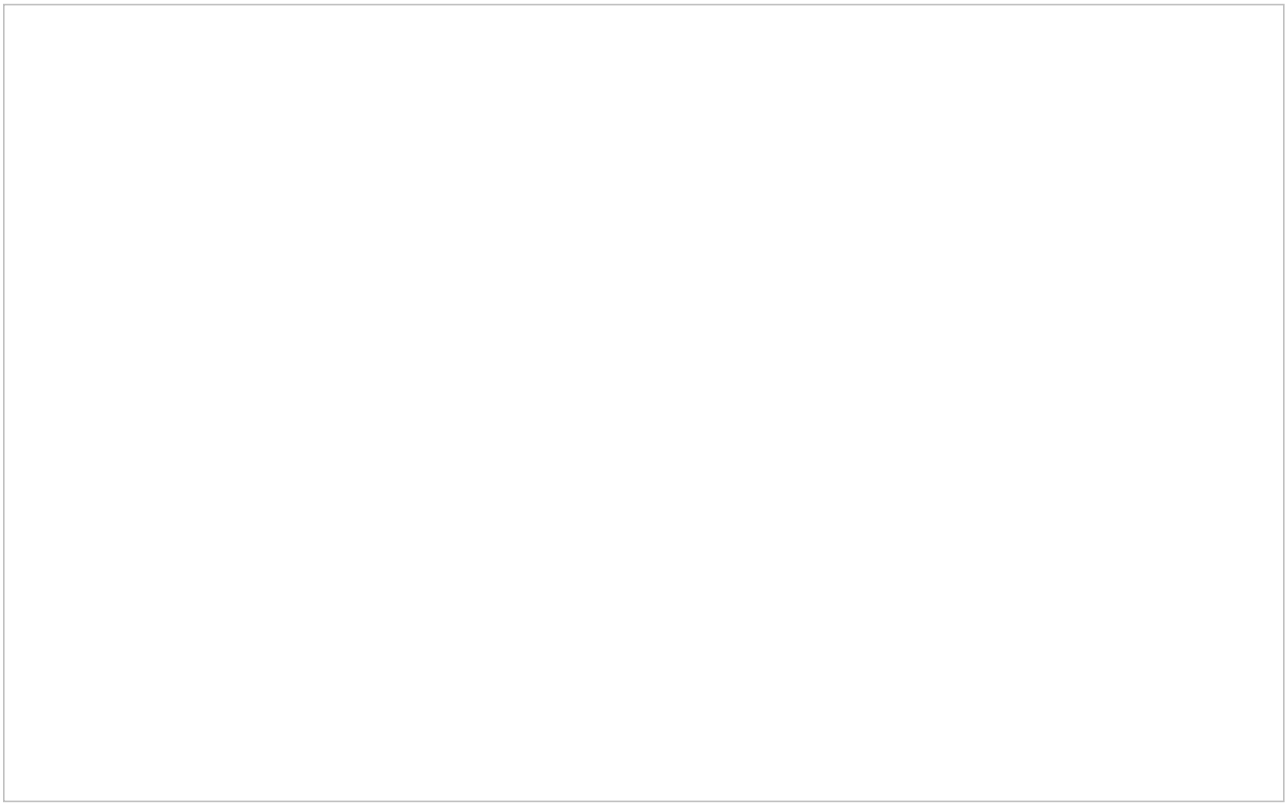


Azure Active Directory > Dashboard > Your registered app > Overview page

- **Application (client) ID**, which is found in *Azure Active Directory* > *Dashboard* > *Your registered app* > *Overview*.

Azure Active Directory > Dashboard > Your registered app > Overview page

- **Client Secret**, which you added to your registered app in Step 2 of this procedure. If you forgot to copy the client secret, you must add a new client secret and copy it now.



The app's Certificates & secrets section

Azure app configuration is now complete.

Next Step

In Bright Pattern Contact Center's Contact Center Administrator application, add a Microsoft Teams Integration Account.

Configuration for Microsoft Teams Direct Routing

Direct voice routing allows your Bright Pattern Contact Center (BPCC) to connect to your Microsoft Teams environment via a single-tenant PBX trunk. Configuring direct voice routing allows the following:

- Users of either system (Teams/BPCC) may call each other directly without incurring a PSTN carrier charge.
- Microsoft Teams users may make outgoing calls to a PSTN via BPCC and receive incoming calls from a PSTN via BPCC.

As your contact center's Microsoft Teams admin, you will do the following in order to allow direct routing:

1. Add an alias domain to your Microsoft Office 365 instance
2. Configure the session border controller (SBC) and routing in Microsoft Teams
3. Configure a Teams user for calling
4. Configuring reachability of all Teams users from BPCC via an Attendant

Procedure

1. Add an Alias Domain to Your Office 365 Instance

This step is required so that Microsoft Teams will trust the domain when you add the session border controller (SBC) in the following step.

1. In the Microsoft 365 admin center, navigate to *Settings* > *Domains* > *Add domain (proxy TLS domain)* and add the alias domain. When you do this, a text string will be generated that will be used by your service provider to validate your domain. Note that you must provide this string to your service provider.

2. Next, navigate to *Users* > *Active Users* > *Add a user*. Here you will add a user (e.g. "proxy") for the previously created domain. After you have registered a domain name, you must activate it by creating at least one E1, E3, or E5 licensed user on that domain. Note that the license can be revoked after the domain activation (i.e., it can take up to 24 hours).

2. Configure the Session Border Controller (SBC) and Routing in Microsoft Teams

1. In the Microsoft Teams admin center, navigate to *Voice* > *Voice Routing Policies* > *Edit Global* OR *create new*. This is what you will assign to users; however, note that Global is already assigned. They consist of PSTN usage records that, in turn, are linked to voice routed below. Add PSTN usage "To BPCC" (i.e., it's just a text label).

2. Next, navigate to *Voice* > *Direct Routing* > *SBCs* > *Add* and add the proxy TLS domain that was added as an alias. Set the port to 5064 and disable the *send Options*.

3. Next, navigate to *Voice* > *Direct Routing* > *Voice Routes* > *Add* and add the route that the number should match to be sent to BPCC. Add "1100" (it is a special invalid US area code), and then link it to "To BPCC" usage.

4. Note that depending on your country, Microsoft will insist on all phone numbers to either start with a leading

+ sign or start with your country code. You can affect the process of short number translation to long ones in the following section: *Voice* > *Dial plans* > <*dial plan*> > *Localization rules*.

3. Configure Teams Users for Calling

In order for all Microsoft Teams users to take advantage of Bright Pattern Contact Center (BPCC) direct-routing capabilities, users must have at a minimum an E1/E3 + Office 365 Phone System license or an E5 license; however, the license has to be from the enterprise-family level.

For a user to be reachable from BPCC software, they must have a business/enterprise phone number defined. The number can be set only by the Skype for Business command-line interface, via the Windows Powershell, or via the Azure Cloud Shell.

Note: This applies to users who will get their phone numbers from BPCC. For users who will have a phone number via a Microsoft Calling Plan, see 3a. Configuring Microsoft 365 Calling Plan Users.

Windows Powershell

To configure phone numbers from BPCC through the Windows Powershell, take the following steps:

1. Install the Skype for Business Powershell module.
2. After installing, start the powershell with administrator privileges.
3. Enter the following commands:

```
Import-Module "C:\\Program Files\\Common Files\\Skype for Business
Online\\Modules\\SkypeOnlineConnector\\SkypeOnlineConnector.psd1"
Import-Module SkypeOnlineConnector
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession
```

4. Note that the *Import-PSSession* command will display the login window. From here, enter your Microsoft Teams admin credentials.
5. Set the phone number for the user with the following command (i.e., using the special invalid US area code 000):

```
Set-CsUser -Identity firstname.lastname@officedomain.com -EnterpriseVoiceEnabled $true -
HostedVoiceMail
$true -OnPremLineURI tel:+10005555555
```

6. Assign to the user the voice routing policy that was defined in this procedure.
7. Once the phone number is added to the user's account in the Microsoft Teams admin center, it must be manually added to the same user's contact card in the Microsoft 365 admin center, section *User*.

Azure Cloud Shell

To configure phone numbers from BPCC through the Azure Cloud Shell, take the following steps:

1. Log into your Azure portal: https://portal.azure.com/
2. Click on the **terminal/console** button in the top bar.
3. Enter the following commands, ensuring you substitute your own domain name:

```
import-module MicrosoftTeams
$sfboSession = New-CsOnlineSession -Credential $credential -OverrideAdminDomain
"domain.onmicrosoft.com"
Import-PSSession $sfboSession
```

4. Set the phone number for the user with the following command (i.e., using the special invalid US area code 000):

```
Set-CsUser -Identity firstname.lastname@officedomain.com -EnterpriseVoiceEnabled $true -
HostedVoiceMail
$true -OnPremLineURI tel:+10005555555
```

3a. (Optional) Configuring Microsoft 365 Calling Plan Users

If a user already has a Microsoft 365 Calling Plan and a Microsoft phone number, adding a voice routing policy is sufficient for making calls to and from BPCC.

Note: These users might require a policy separate from other users, depending on whether you want their calls to the PSTN to go through SBC/BPCC or the Microsoft Calling Plan.

To configure a Microsoft Calling Plan user, do the following:

1. Create a location (i.e., an emergency location).
2. Give the user a Microsoft 365 Domestic Calling Plan license.
3. Order a phone number, and then specify the location created previously.
4. Note that you will search for locations by their city name (i.e., not by the defined location names).
5. From the phone number, assign the user to the license, and then set the emergency location.
6. Edit the user policies and then set the voice routing policy with the BPCC routing entries, if needed.

4. Configuring Reachability of All Teams Users from BPCC

All Teams users can be dialed from BPCC via an attendant. In order to do this, take the following steps:

1. Create a *Resource User* in the Microsoft Teams admin portal (i.e., *Org Wide Settings* > *Resource Accounts*).
2. Give the new user the *Phone Systems Virtual User* add-on license in the Microsoft Office 365 Admin portal.
3. Give the new user a phone number via Windows Powershell or Azure Cloud Shell using the following command:

```
Set-CsOnlineApplicationInstance -Identity resourceuser@domain.onmicrosoft.com -
OnpremPhoneNumber
+10005555555
```

4. Create an attendant that plays a menu prompt and offers dial by name.
5. Associate the attendant with the resource user (i.e., via *Resource User* properties).
6. The calling attendant number via BPCC will reach the attendant. Any user can be reached by dialing their name followed by the pound symbol.
7. A string now can be entered into the Office 365 user contact field (e.g., Office Phone: 1111111,,222222 where 111111 is the attendant number and 222222 is the dial by name string. Note that this tool uses 0 for space.).

Diagnostics Checklists

Testing Microsoft Teams to Bright Pattern Contact Center Calls

- The Teams user has an E1/E3 license + Office 365 Phone System, or an E5 license.
- The Teams user has a calling policy selected that includes usage that selects the matching prefix that points to the repro proxy domain.
- The BPCC tenant has a matching extension or a dial-out entry.

Testing Bright Pattern Contact Center to Microsoft Teams Calls

- The BPCC contact center has a single-tenant PBX trunk.
- The dialed number matches the prefix on the trunk.
- The trunk's number-mangling parameters change from and to numbers to their proper destinations.
- The repro proxy has BPCC SIP processor addresses enabled in the ACL
- The repro proxy has firewall ports open toward BPCC.
- The repro proxy has a matching route that point to Teams.
- The repro proxy has the proper certificate(s).
- There is a Teams user with a tel URL set to the dialed number.

How to Add a Microsoft Teams Integration Account

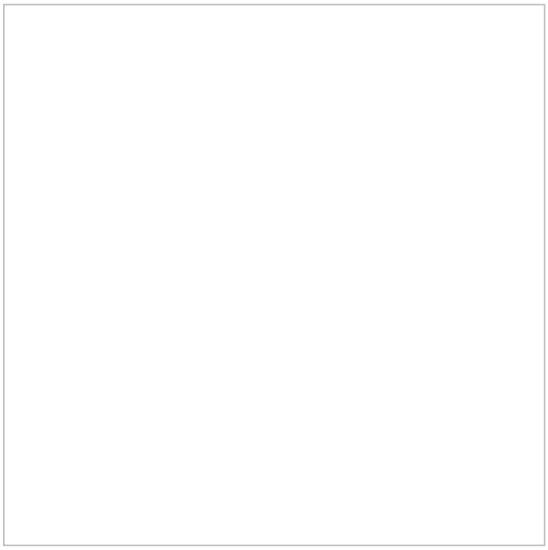
Configuring a Microsoft Teams integration account allows your contact center to use an enterprise-level communications channel that comes with chat and call capabilities, user-presence visibility, and directory access during service interactions with customers.

Please note that your contact center is allowed only one instance of a Microsoft Teams integration account. If you wish to create a different Microsoft Teams integration account, you must delete the existing instance.

Deleting an existing Microsoft Teams integration account will disable access for all users in the account. Upon creating a new Microsoft Teams integration account, all users in the account will need to re-enable Teams integration in their Agent Desktop user profiles.

Procedure

1. In the Contact Center Administrator application, go to section *Configuration* > *Call Center Configuration* > *Integration Accounts* and click **+** to add a new integration account of type **Microsoft Teams**.

   Select the Microsoft Teams integration account type

2. Set the following properties for the account:

   1. **Name** - The name of the integration account (any name)
   2. **Directory (Tenant) ID** - Your Microsoft Azure registered app's Directory (tenant) ID
   3. **Client ID** - Your registered app's Account (client) ID
   4. **Client Secret** - Your registered app's client secret
   5. **Test connection** - Tests the credentials and confirms whether the connection is valid. If the connection is

not OK, you may get one of the following validation connection error messages:

1. **Error: Failed to request refresh token** - This means that the provided Client Secret, Directory (Tenant) ID, or Client ID is invalid and the refresh token could not be requested. Try copying each of those items from the Azure registered app and pasting them into the property fields again.

2. **Error: Account credentials are incomplete** - Make sure that all fields are filled, and click **Apply** at the bottom of the screen to save changes to the integration account properties.

3. In Properties section *System Messages for Conferencing Microsoft Teams Users to a Customer Chat*, you may choose to redefine the automatic system response options and various commands agents will use for chat interactions.

   The default values for these messages are as follows:

   1. **Party joined** - joined the session

   2. **Party left** - left the session

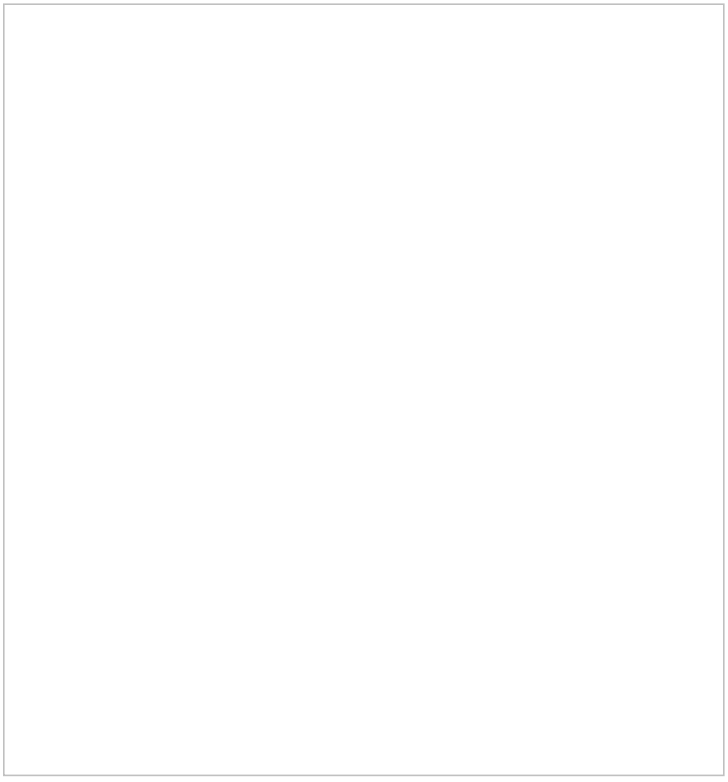
   3. **Invitation to join** - You are invited to customer chat session, would you like to accept (YES/NO)?

   4. **Positive response** - YES

   5. **Negative response** - NO

   6. **Session ended** - Customer chat session ended

   7. **Leave any time command** - BYE

   Microsoft Teams integration account properties

Bria Mobile Softphone Configuration

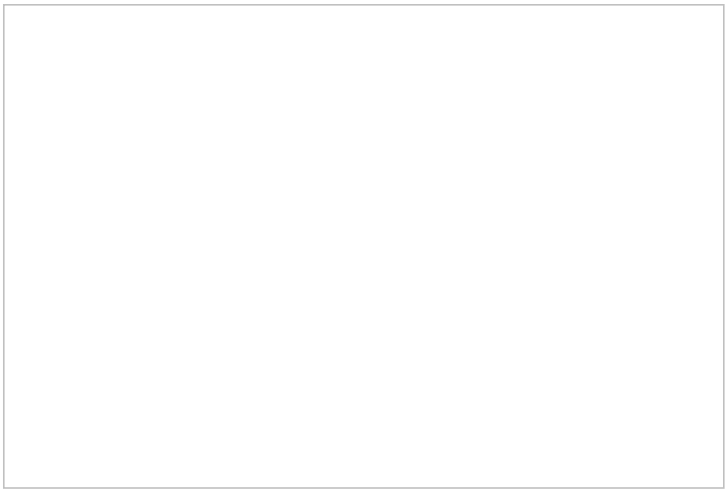
The Bria Mobile softphone app works well for phone calls with Bright Pattern Contact Center software; it minimizes battery drain in standby by using Bria Push Service.

Configuration

In the Contact Center Administrator Application

To configure Bria Mobile with Bright Pattern Contact Center, take the following steps:

1. Add a hardphone account in the Contact Center Administrator application, and edit Properties.



Hardphone Properties

2. In the Authentication tab, make sure the authentication username is the same as the phone's extension.

Hardphone Authentication tab

3. Note your domain (e.g., from the Properties tab, see “Phone registers as <ext>@<domain>”), extension, and password.

In the Bria Mobile Softphone

In the Bria Mobile app, add a new account. This is done by going to **Settings > Accounts > “+” > Select Provider > User-Defined Generic Accounts > SIP**.

Note that the steps that follow are for User-Defined Generic Accounts. You do not have to select a VoIP provider. Also note that you can only edit account options when the account is disabled.

Section SIP Account

To configure the SIP account, take the following steps:

1. Give your account an *Account Name.*
2. Set the desired *Display as* name.
3. Set the *Username* and *Password* to the same username (e.g., "3001") and password from your configured hardphone account.
4. Set the domain to the hardphone account's domain and add **:5080** (Bright Pattern CCaaS service uses the non-standard SIP port 5080). For example: "example.brightpattern.com:5080"
5. Enable the option *Use Push Notifications* and set the option *Registration Mode* to **Single Device Emulation**.
6. Disable the option *NAT Emulation*.
7. Leave the option *Push Advanced Settings* disabled.

Section Account Advanced

To configure section *Account Advanced*, take the following steps:

1. In section *Network Traversal*, option *Custom configuration*, turn all options off.
2. In section *IP Version*, set option *Wi-Fi IP Version* to **IPv4**
3. Also in section *IP Version*, set option *Mobile IP Version* to **IPv4**.
4. In section *DTMF Type*, make sure option *Send DTMF using* is set to **RFC2833**.
5. In section *Transport and Security*, set option *SIP transport* to **UDP**.
6. In section *SIP Registration*, set options *Wi-Fi Refresh Interval* and *Mobile Refresh Interval* to **30** seconds.
7. In section *TLS Cert Management*, disable option *Verify TLS cert*.
8. In section *SIP Miscellaneous*, leave option *Show Miscellaneous* disabled.

Cisco SPA Hardphone Configuration

These instructions will show you how to configure and register a Cisco hardphone manually on the Cisco Configuration Utility web interface. We are using a Cisco SPA508G as an example. Note that this example can be used for any Cisco hardphone in the "SPA" model family.

Prerequisites

You should have Bright Pattern Contact Center version 5.2.x or later.

In order to configure your Cisco phones with Bright Pattern Contact Center software, you will require a special **outbound proxy**; Bright Pattern Operations will create this for you upon request. (See Step 5.1.b. in the following procedure.)

Procedure

1. Locate the IP address of the phone

On your phone, press the **Menu** button, and then select the **Network** option; the IP address should be listed here.

2. Check for software updates on the Cisco phone (important)

Make sure you are running the latest firmware version for your phone. We recommend updating your phone at least once per year. For updates, visit the Cisco Software Download page.

3. Perform a factory reset (important)

On your phone, press the **Menu** button, and then select **Factory Reset**. The phone will restart.

4. Open the phone's configuration utility web interface

1. Enter the IP address of the Cisco phone in the address bar of your web browser.
2. In the top right corner of the page, click **Admin Login** and then click **advanced**.

   Cisco-SPA-1.PNG

   Alternatively, you may navigate directly to the following to get to the same place: **http://<your-phone-IP-address>/admin/advanced**

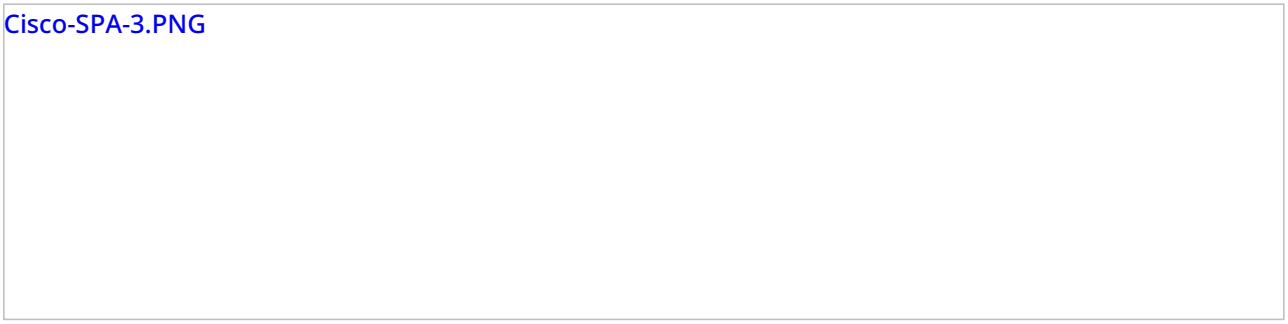
3. Click **Voice** and then select the extension tab you wish to configure. In this example, we are configuring **Ext 2**.

   Cisco-SPA-2.PNG

5. Edit the extension settings

Note: Configuration requires the following settings to be changed. Any settings not specifically mentioned in this step are set by user.

1. In the extension settings, under *Proxy and Registration*, set:
   - **Proxy**: The access domain of your Bright Pattern tenant, which is found in the Bright Pattern Service Provider application, section *Tenants* > *Properties*
   - **Outbound Proxy**: The setting created for you upon request to Bright Pattern Operations (e.g., "yourcorporation-sip.brightpattern.com")
   - **Use Outbound Proxy**: Select "yes" (default is "no")
   - **Register**: Select "yes"
   - **Use DNS SRV**: Select "yes"
   - **DNS SRV Auto Prefix**: Select "yes"

2. Under *Subscriber Information*, set:
   - **User ID**: The phone extension number (e.g., "1000")
   - **Password**: The password of the phone extension, set by user

6. Edit System configuration settings

1. Click the **System** tab to edit system configuration settings.

2. Under *Optional Network Configuration*, set:
   - **NTP Enable**: Select "yes"
   - **Secondary NTP Server**: Set "**0.pool.ntp.org**"

Polycom Hardphone Configuration

These instructions will show you how to configure and register a Polycom hardphone manually on the Polycom Configuration Utility web interface. We are using a Polycom SoundStation IP 6000 as an example.

There are several ways to configure a Polycom phone on the web interface: Simple Setup, Lines settings, and SIP. The following instructions will guide you through Lines settings configuration. **We recommend that you do not use Simple Setup or SIP.**

Prerequisites

In order to configure your Polycom phones with Bright Pattern Contact Center software, you will require a special SIP address; Bright Pattern Operations will create this for you upon request. Note that the address has built-in redundancy (i.e., it contains two servers), so you will only need one SIP address.

Procedure

Step 1: Locate the IP address, SIP extension number, and password of the Polycom phone

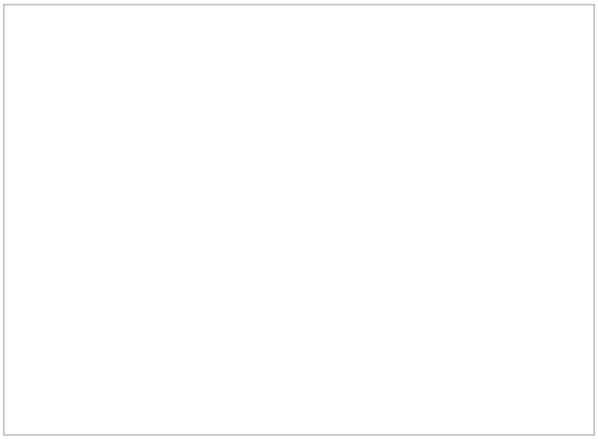
1. On the Polycom phone, hit *Menu* > *Status* > *Network* > *TCP/IP Parameters*, and note the listed IP address.

2. Note the SIP extension number on the display of the Polycom phone.

3. You can locate or set the phone password by logging into*/Admin* > *Setup* > *Manage* > *Modify (pencil button)* > *the SIP extension you wish to register* > *Phone Settings tab* > *Common Settings* > *Phone Password.*

Step 2: Open the phone's configuration utility web interface on a web browser

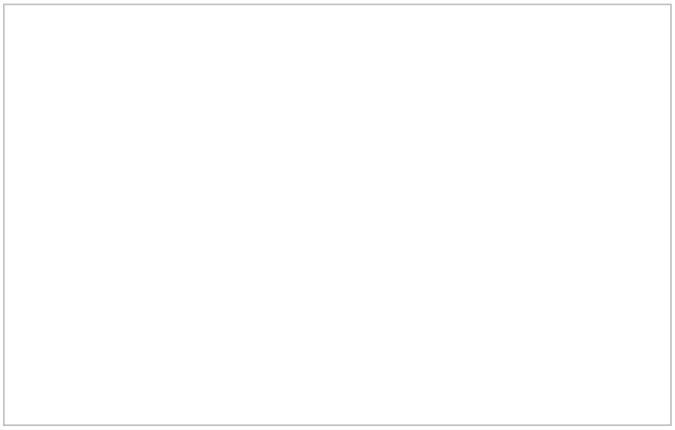
1. Enter the IP address of the Polycom phone in the address bar of your web browser. # When prompted for credentials, select Admin and enter your password. If you don't know the password or you have never changed it, it is likely "456".

   Polycom web interface login screen

2. The phone cannot be in use during configuration. Before proceeding to Step 3, check that the phone is not being used. Note that if the phone is in use, you will not be able to access the configuration utility.

3. We recommend doing a phone backup before proceeding, in case you need to undo what you did. Go to *Utilities* > *Phone Backup & Restore* and click **Phone Backup**.

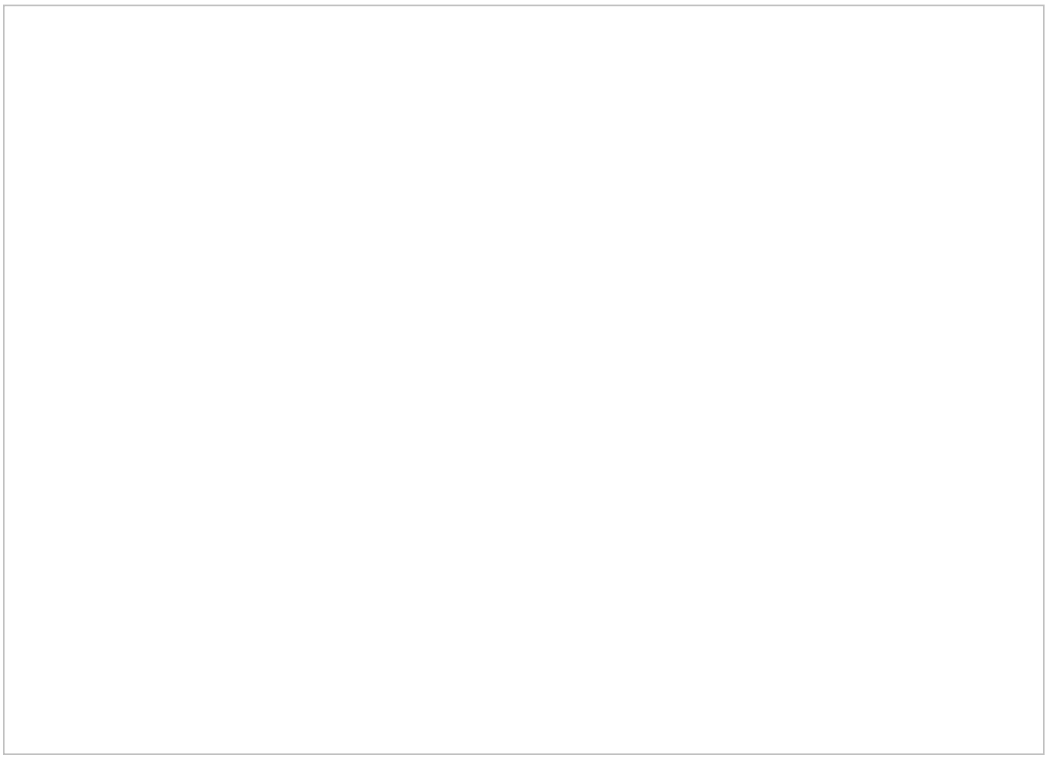


Utilities > Phone Backup & Restore

Step 3: Edit Lines settings

Note that if your phone freezes during any part of configuration, you can unplug/restart it and try again.

1. Go to *Settings* > *Lines*.



Settings > Lines

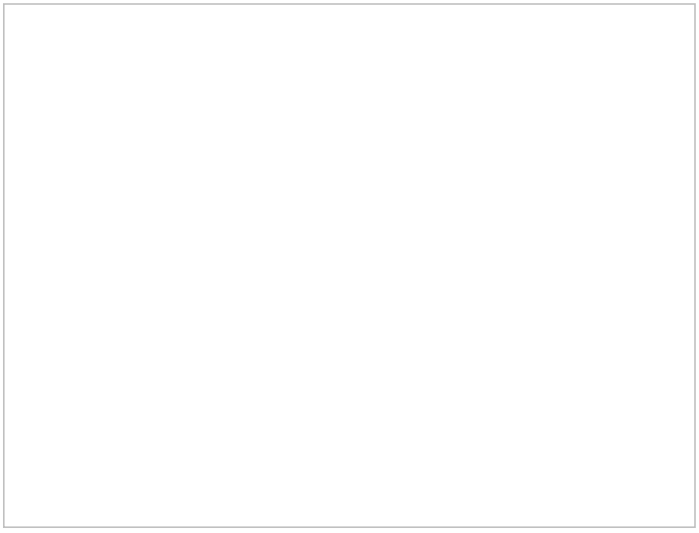
2. Under *Line 1* > *Identification*, set:

Settings > Line 1 > Identification settings

1. **Display name:** Any name

2. **Address:** The path to your Polycom phone in the following format: extension number@<tenant>.brightpattern.com.

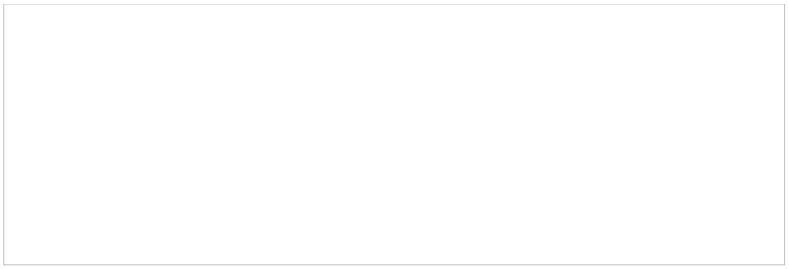
   This corresponds to the field “Phone registers dynamically as” in Bright Pattern’s Contact Center Administrator application, section *Directory* > *Hardphones* > <*Your extension number*> > *Properties*. For example:

   Contact Center Administrator > Hardphones > Properties

3. **Authentication User ID:** The authentication username of your Polycom phone (e.g., “9999”).

   The Authentication User ID and Authentication password correspond to the “Username” and password as set in Bright Pattern’s Contact Center Administrator application, section *Directory* > *Hardphones* > <*Your extension number* > *Authentication*. For example:



Contact Center Administrator > Directory > Hardphones > <Your extension number > Authentication

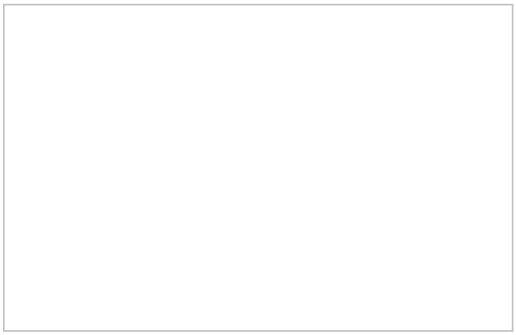
4. **Authentication password:** The password of your Polycom phone
5. **Label:** Any; this will be shown on the phone's screen
6. **Type:** Select "Private" or "Shared"
7. **Third Party Name:** Any; OK to leave blank
8. **Number of Line Keys:** Any (e.g., "1")
9. **Calls Per Line:** Any (e.g., "8")
10. **Ring Type:** Select

3. Under *Line 1* > *Outbound Proxy*, set:

Line 1 > Outbound Proxy settings

1. **Address:** Must be empty (if any value is here, you must remove it)
2. **Port:** Must be "0"
3. **Transport:** Leave as "UDPOnly"

4. Under *Line 1* > *Server 1*:

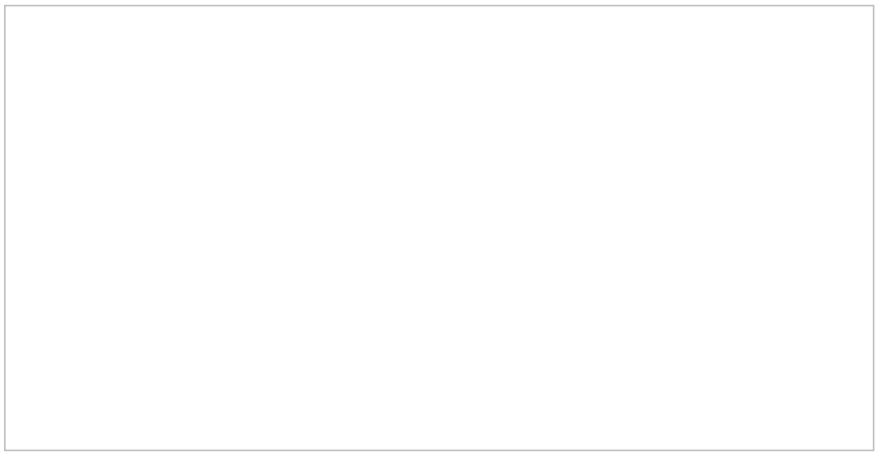


Line 1 > Server 1 settings

1. **Address:** The address in the following format: <tenant>-sip.brightpattern.com (e.g., “example-sip.brightpattern.com). Note that this address is created by Bright Pattern Operations upon request.
2. **Port:** Set “0” (The default is 0. Do not type any other port number here because it comes from the DNS server automatically.)
3. **Transport:** Select “DNSnaptr”. (default).
4. **Expires (s):** The expiration period in seconds - “60” (default is “3600”)
5. **Register:** Select “Yes” (if you select “No,” the phone will not be registered)
6. **Retry Timeout (ms):** The timeout period in milliseconds (e.g., “0”). The default is 100 ms. If you set “0”, the timeout will be set to default.
7. **Retry Maximum Count:** The max number of times to retry (e.g., “3”)
8. **Line Seize Timeout (s):** The line seize timeout in seconds (e.g., “30”)

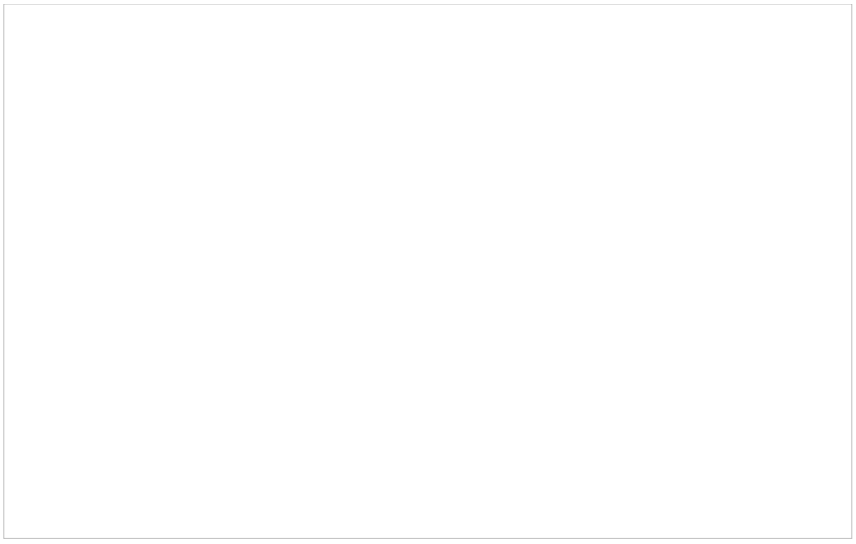
Step 4: Check for software updates on the Polycom phone

1. We recommend updating to the latest software on the Polycom phone at least once per year.
2. Still in Polycom’s web interface, go to *Utilities* > *Software Upgrade*.



Utilities > Software Upgrade

3. In *Phone Details*, you will see your current software version. Leave this as-is.
4. Click **Check for Updates**.



Phone Details

5. Now you will see the Software available at Polycom server drop-down list. Select and run the latest version (e.g., “4.0.14.1388D”).

6. Click **Install**. The phone will restart. The software update takes about 2–5 minutes.

Polycom phone configuration is now complete.

How to Configure Softphone Solo for Remote Desktop

This article describes how to configure Softphone Solo for remote desktop use. Softphone Solo is an application (Windows) that installs the softphone functions of Bright Pattern’s Agent Desktop Helper Application component (i.e., *bpclient.exe*) outside of a user’s main client machine.

When Softphone Solo is set up, contact center users are able to have softphone functionality on Agent Desktop through a remote session—without having to download and install the Agent Desktop Helper Application component.

Procedure

In this procedure, we treat Softphone Solo as a default hardphone, and we assign it to each Agent Desktop user with a specific number.

Step 1: Configure a hardphone for your contact center

1. Log in to the Contact Center Administrator application and go to section *Configuration* > *Directory* > *Hardphones.*

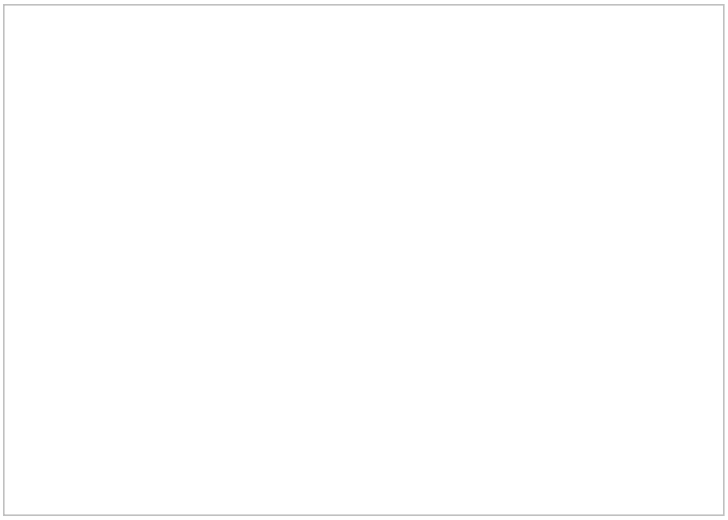
2. Click **Add hardphone** (“**+**”) to add a new hardphone.

3. In the *Properties* tab, set the following:

    1. **Number** - The number (e.g., “5001”) that will be used for users who log in to Agent Desktop with a remote session; choose a number that is different than the number range of users’ extensions

    2. **Caller ID** - Optional; OK to leave empty

    3. **MAC address** - Leave empty

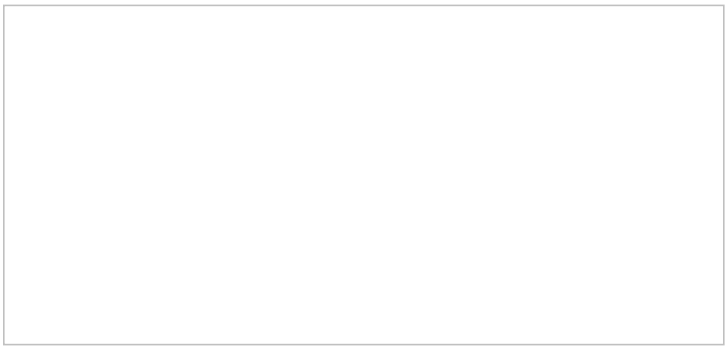
    

    Hardphone Properties

4. In the *Authentication* tab, set:

    1. **Username** - Set the hardphone number (e.g., “5001”)

    2. **Password** - Set any, but follow the rules of your contact center’s password policy

    Hardphone Authentication

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

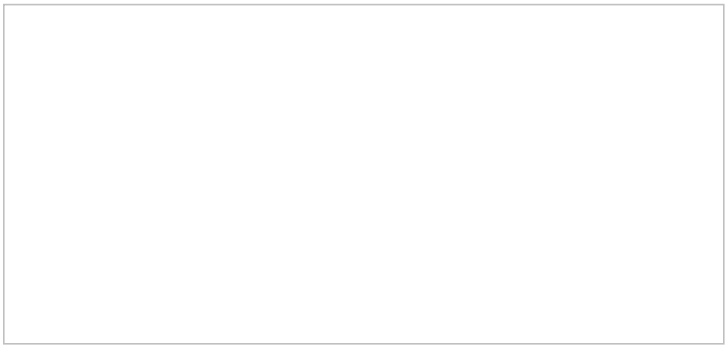
Step 2: Set the agent’s default hardphone number

As a best practice, set the agent's default hardphone number. This is the number that the agent will use for placing calls in Agent Desktop. Note that this step is not required for using Softphone Solo, but it is recommended. The agent can choose a number manually at a later time.

1. Go to section *Configuration* > *Users & Teams* > *Users*.

2. From the *Users* list, select the agent who will be using Softphone Solo.

3. In the agent's *Contacts* tab, set the **Default hardphone number** to the same number you configured for the hardphone in Step 1 of this procedure.

   The Users > Contacts properties for the agent

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

Step 3: Configure Softphone Solo

1. Download and install the Softphone Solo for Windows application (*SoftphoneSolo_5.x.x.xxxxx.msi*). Please contact Customer Success Management for the file.

2. Launch the application after installation is complete, or right-click the **Softphone Solo tray icon** (phone icon) and select **Configure** to launch it.

   Softphone Solo tray icon,
   right-clicked

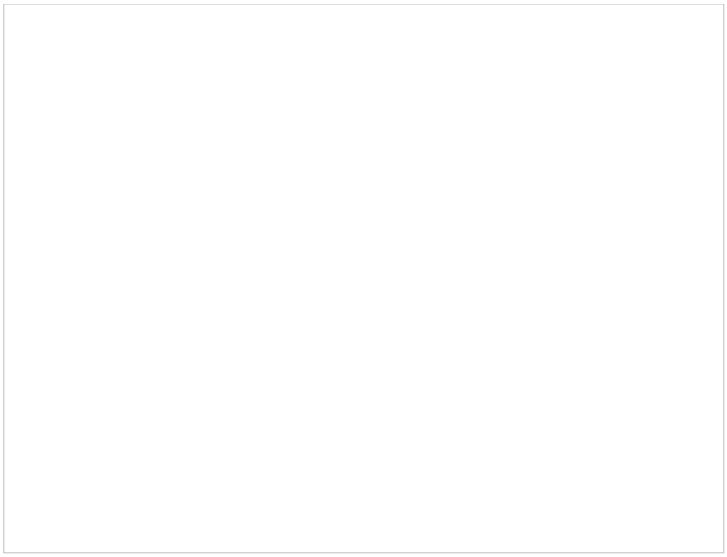
3. The Softphone Solo configuration dialog will open.

Softphone Solo configuration settings

4. Set the following:
    1. **HTTP(s) URL to access the system** - The URL of the contact center (e.g., "http://company.brightpattern.com")
    2. **Tenant name** - The contact center domain (e.g., "company.brightpattern.com")
    3. **Login** - The agent's username (e.g., "christy.borden")
    4. **Password** - The user's password
5. Click **Apply**.
6. If you see an error message, go back and check your configuration, as you may have set the wrong username/password or the wrong URL. The Troubleshooting section describes some common errors you may encounter.

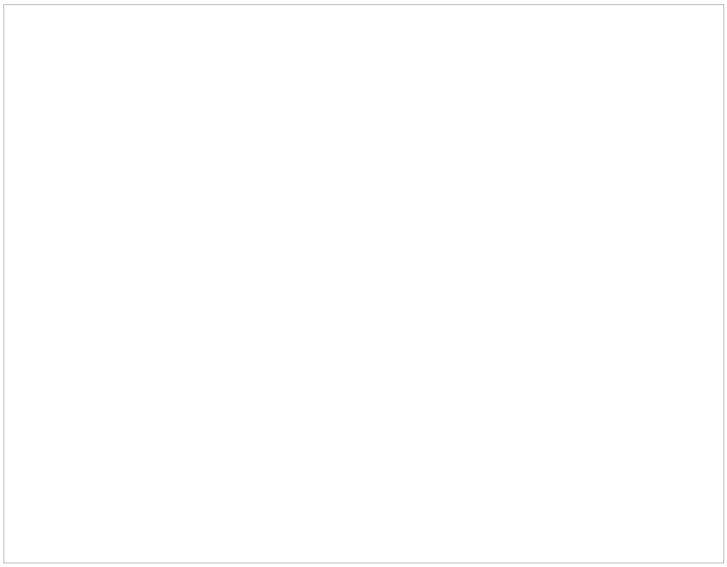
Step 4: Check that the agent can use the phone in Agent Desktop

1. Go to the Agent Desktop application, and log in as the agent, using the same Authentication user name and password as set in the Softphone Solo configuration dialog.
2. Go to *Settings* > *Phone Device* and set **Internal hardphone, my default number**. You will have to log out and log in again for the change to take effect.



Selecting the phone device in Agent Desktop

Note that if the agent (or an administrator) has configured Softphone Solo manually, the agent has the option to use the **Internal hardphone, number** setting, with the number of their choice, as shown.



Selecting the "Internal hardphone, number" setting

3. After logging in again, if you hover your cursor over the agent's **Settings**, you will see that the agent's phone number is the default hardphone number (e.g., "5001").

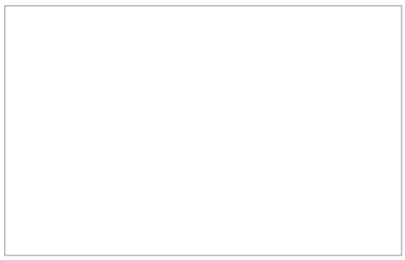
Hover text over agent's profile/Settings shows the agent's phone number

4. Configuration is now complete. Try placing a call.

Troubleshooting

This section describes error messages and what they mean.

Unable to access the system

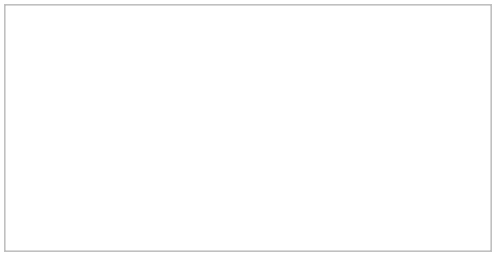


Unable to access the system error message

This error could mean that you may have set the wrong URL in configuration. Make sure that in the field HTTP(s) URL to access the system, that you have set the correct URL of your contact center, including the leading "http://" (e.g., "http://company.brightpattern.com").

You can quickly check the status of both configuration options (automatic and manual) by looking at Softphone Solo's Windows tray icon (phone icon) color at the bottom of your desktop screen: green = OK, gray = fail.

Unable to obtain phone configuration. Error: HTTP error: 401 Unauthorized



HTTP error:401 message

This likely means that you did not set the user's default hardphone number to the correct number, and because of that, the configuration could not be completed.

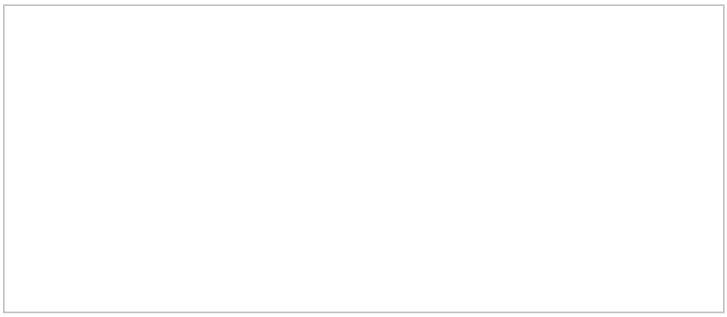
Or, it means that some other values have not been configured. If this is the case:

1. Right-click the Softphone Solo tray icon and select **Configure**.

Configure Softphone Solo

2. Select the checkbox for **Use manual configuration** and click **Configure**.

3. In the *Advanced SIP configuration* dialog that opens, if you see that the Advanced SIP configuration is empty, fill in the blank fields. These settings are normally filled in by the system automatically during manual configuration. However, these settings could be affected if the default number was not set correctly, or some other setting was wrong.



Advanced SIP configuration, empty

    1. **Phone number** - The hardphone number you configured in Step 1 of this procedure (e.g., “5001”); this will be filled in for you once you enter the Authentication user name and password (see below)

    2. **SIP domain** - Your SIP domain; this will be filled in for you once you enter the Authentication user name and password (see below)

    3. **SIP Server address** - Your SIP Server address (e.g., “<tenant_url>.brightpattern.com”); this will be filled in for you once you enter the Authentication user name and password (see below)

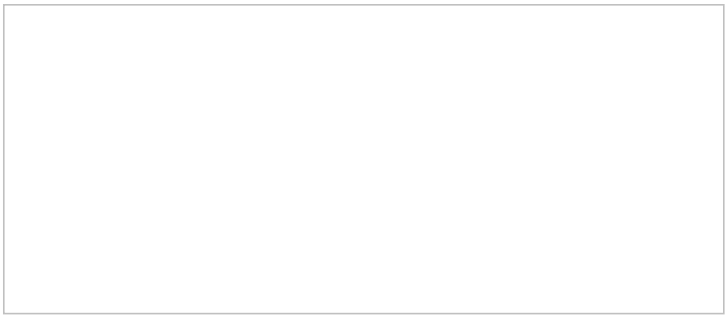
    4. **Port** - 5060 (default)

    5. **Authentication user name** - The username of the agent (e.g., “christy.borden”) who was assigned the hardphone in Step 2 of this procedure

    6. **Password** - The agent’s password

    7. **Registration interval** - 90 seconds (default)

4. When done, the settings should look like this:



Advanced SIP configuration settings completed

5. Click **OK**.

6. Back in the *Softphone Solo configuration* dialog, click **Apply**.

Setting up Private S3 Storage

Bright Pattern Contact Center allows you to export audio recordings and screen recordings to external storage servers, such as Amazon Web Services (AWS) S3 or Minio for storage or playback.

This article explains how to 1) set up Minio as S3-compatible local storage, 2) get the access credentials to integrate Bright Pattern Contact Center with Minio, and 3) use those credentials to configure an Amazon AWS integration account.

You can learn more about integration accounts in section Amazon AWS Integration of this guide.

Procedure

Step 1: Install Minio

You can install Minio on either a Linux- or Windows-based system. After installing the app, you will have the Minio credentials needed for integrating Minio with your contact center as a private S3 storage option.

If Using a Linux-Based System

Docker container:

```
docker run -p 9000:9000 -v /mnt/data:/data -v /mnt/config:/root/.minio minio/minio server /data
```

Linux x86 (CentOS 6 or CentOS 7):

```
wget https://dl.minio.io/server/minio/release/linux-amd64/minio
chmod +x minio
./minio server /mnt/data
```

Get credentials

After the app is installed, the console will show these credentials:

- **Endpoint:** http://<hostname>:9000 (e.g., http://127.0.0.1:9000)
- **AccessKey:** <generated accesskey>
- **SecretKey:** <generated secretkey>

Copy the Endpoint, AccessKey, and SecretKey. You will be using these credentials next to set up your Amazon AWS integration account in Contact Center Administrator.

If Using a Windows-Based System

1. Download the Minio application.
2. Run:

```
minio.exe server F:\Data
```

Get credentials

After the app is installed, the console will show these credentials:

- **Endpoint:** http://<hostname>:9000 (e.g., http://127.0.0.1:9000)
- **AccessKey:** <generated accesskey>
- **SecretKey:** <generated secretkey>

Copy the Endpoint, AccessKey, and SecretKey. You will be using these credentials later to set up your Amazon AWS integration account in Contact Center Administrator.

Step 2: Create a bucket

A bucket is a container for stored objects. Before you can export recordings to your private S3 storage, you first have to create a bucket to store them.

1. Go to the Minio web interface. Note that by default, Minio uses port 9000 for access.
2. Log in to Minio using your AccessKey and SecretKey.
3. Create a new bucket and name it (e.g., "test").

Step 3: Integrate with Minio

After Minio is installed and you have a bucket, you can configure your contact center to work in an integrated manner with Minio. This is done in the Contact Center Administrator application.

Add integration account

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

2. Click the **Add** button (**+**) to add a new integration account of type **Amazon AWS**. (Note that in order to add this account type, the AWS feature must first be enabled for your contact center by your system administrator.)

Add-Amazon-52.PNG

Edit integration account properties

1. Name the integration account (any name).
2. Select the **Use private S3 storage** checkbox.
3. In field **Url**, paste the Minio endpoint that you copied earlier.
4. In field **Access Key ID**, paste the Minio AccessKey.
5. In field **Secret Key**, paste the Minio SecretKey.
6. In field **S3 bucket**, add the name of the bucket you created.
7. Click **Apply** to save your changes.

Minio-Prop-52.PNG

Your S3-compatible private storage option is now set up and ready to be used for storing screen recordings, call recordings, and so forth.

For more information about integration account properties, see the *Contact Center Administrator Guide*, section Amazon AWS Integration.