



Chime for Teams Azure and Office 365 Prerequisites for Hosted Environments

April 2020

Copyright and Disclaimer

This document, as well as the software described in it, is furnished under license of the Instant Technologies Software Evaluation Agreement and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Instant Technologies. Instant Technologies assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. All information in this document is confidential and proprietary.

Except as permitted by the Software Evaluation Agreement, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Instant Technologies .

Copyright © 2005 - 2020 Instant Technologies, All rights reserved.

Trademarks

All other trademarks are the property of their respective owners.

Contact Information

See our website for Customer Support information.

<http://www.instant-tech.com/>



ISV/Software Solutions

CONTENTS

Overview	4
Important Roles:	4
Configuring Azure AD Authentication for Chime For Teams	5
Prerequisites.....	5
Configure Active Directory Authentication	6
Retrieve your Azure Tenant ID	6
Create Application	6
Register the Chime Application	7
Configure the Application	7
Configure Application Permissions	8
Add Redirect URIs.....	11
Creating Bots for Chime Dispatchers.....	12
Creating a Bot Registration in Azure	13

OVERVIEW

This document is intended to provide both a high level, as well as technical requirements required to install and configure an Instant Chime for Microsoft Teams application server.

This document covers a scenario where Chime will be installed and managed by a third-party hosting provider (possibly Instant) and items such as configuring Azure AD, AD Authentication, and Application permissions will be important. These areas are also relevant to self-hosted modes.

For more information on installation and architecture visit our [Install and Getting Started](#) page.

At a high level, Chime for Teams will need to be configured to securely communicate with several external services as well as access the following resources:

- Microsoft Azure AD
- Microsoft Office 365 Graph APIs
- Microsoft Bot Framework

IMPORTANT ROLES:

As part of this installation and configuration process, a tenant administrator for the Microsoft Office 365 tenant may need to perform several actions in order to provide the necessary authorization for the Chime server.

Certificate requestor (if your organization is self-hosting)

Administrator for O365 domain

CONFIGURING AZURE AD AUTHENTICATION FOR CHIME FOR TEAMS

Chime for Microsoft Teams requires the configuration of an Azure Active Directory application in order to allow Chime to leverage Office 365 for user authentication, and to communicate with your Microsoft Teams users. This document will outline how to configure these two applications.

PREREQUISITES

- A. You must have an Office365 tenant for your organization.
- B. You must be an administrator of your Office 365 domain.
- C. An Azure account linked with your Office 365 Identity. If this is not done, see <https://technet.microsoft.com/en-us/library/dn832618.aspx>.

All configuration steps in this guide take place in the Azure Active Directory component of the Azure portal.

1. Sign into the Azure AD portal (<https://portal.azure.com>).
2. Select the **Azure Active Directory** in the left-hand navigation pane.

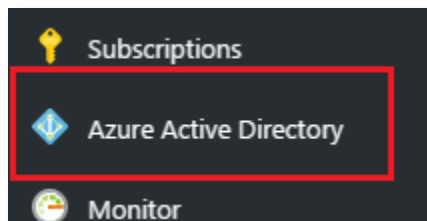


Figure 1: Begin Setting up Active Directory

3. If the **Azure Active Directory** is not available on the left-hand navigation pane, it is available in **All services** then the section labeled **Identity**

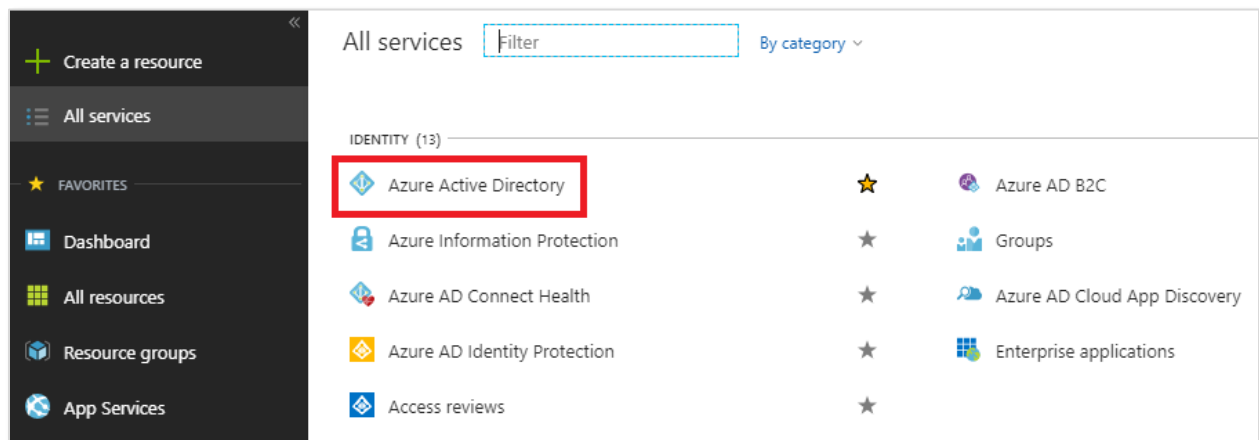

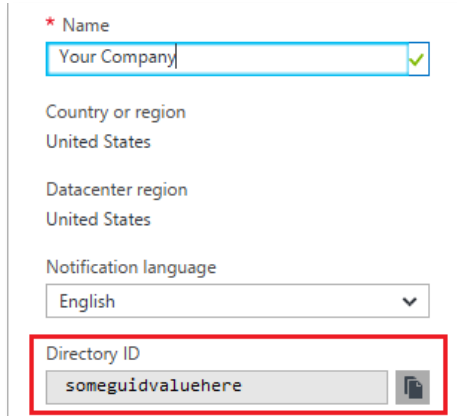


Figure 2: Secondary Option to Active Directory Setup

CONFIGURE ACTIVE DIRECTORY AUTHENTICATION

RETRIEVE YOUR AZURE TENANT ID

1. Select  **Properties** in the navigation pane in the **Azure Active Directory** blade.
2. Copy the **Directory ID** from the field, and save it somewhere convenient. You will need this value when configuring Chime. **Note:** The Directory ID is often referred to as the “Tenant ID” in Microsoft documentation, both terms are referring to this ID.



* Name
Your Company ✓

Country or region
United States

Datacenter region
United States

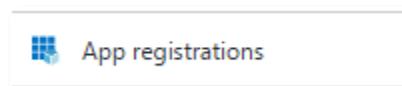
Notification language
English ▼

Directory ID
someguidvaluehere

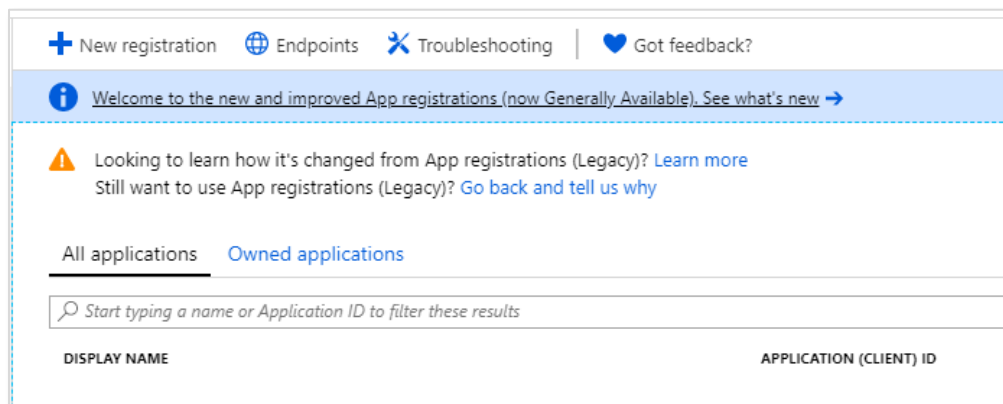
Figure 3: Copy Directory ID

CREATE APPLICATION

1. Select **App Registrations** in the new navigation pane within the **Azure Active Directory** blade.



2. Click the **New application registration** option in the **Azure Active Directory** blade.



+ New registration | Endpoints | Troubleshooting | Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
Still want to use App registrations (Legacy)? [Go back and tell us why](#)

All applications | Owned applications

Start typing a name or Application ID to filter these results

DISPLAY NAME	APPLICATION (CLIENT) ID
--------------	-------------------------

Figure 4: Create New Application Registration

REGISTER THE CHIME APPLICATION

1. Create a name for this application (Chime is a suitable name)
2. Select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)** as the Supported account types to allow for us to host.
3. Enter the URL for the server that Chime will be hosted on, with the */Chime* route in the URL (ex: <https://yourserver.domain.com/Chime>)

NOTE: Be sure that the /Chime is included in the URL, this will automatically configure the Reply URL to correctly work with the Chime application

Dashboard > instant technologies - App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Chime ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (instant technologies)

☐ Accounts in any organizational directory


☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

Figure 5: Create the Chime Web App / API

4. Click the  button in the bottom of the Register an Application blade.

CONFIGURE THE APPLICATION

1. Click on the newly created application in the **App Registrations** blade. If you have many applications, you may need to search for it.
2. In the Overview window, you will be able to record the **Application ID**. This value will be used when configuring Chime. This page also will allow you to record the Directory (tenant) ID if you were unable to in the previously.

CONFIGURE APPLICATION PERMISSIONS

Chime requires the following Microsoft Graph API permissions to be granted for full functionality:

Permission	Type	Usage
User.Read	Delegated	Signing in users to the Chime web portal
User.Read.All	Application	Retrieve metadata information about users contacting a queue.
Directory.Read.All	Application	Perform user and group searches when adding users to Chime and for alert recipients
Group.Read.All	Application	Allows Chime to search for Microsoft Teams Teams and retrieve information about their properties and user membership
Group.ReadWrite.All	Application	OPTIONAL - Allows Chime to add or remove users from Teams Team rosters to match the queue membership in Chime
Presence.Read.All	Delegated	Allows Chime to retrieve presence information for users assigned to a queue. REQUIRED for hunt-style chat routing
AppCatalog.ReadWrite.All	Delegated	OPTIONAL - Allows Chime to programmatically upload generated Teams App packages for a queue to the tenant App Catalog. <i>Without this permission, it is necessary for an administrator to manually upload Teams App packages for the queues.</i>
TeamsApp.ReadWrite.All	Delegated	OPTIONAL - Allows Chime to programmatically assign generated Teams App packages to the Team associated with a queue <i>Without this permission, it is necessary for an administrator to manually add the Team App for a queue's bot dispatcher to the Team associated with the queue</i>

1. Click the **API Permissions** button.

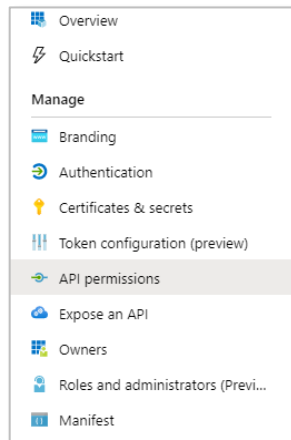


Figure 6: Access Required API Permissions

2. Click the **Add a Permission** button in the API Permissions window.

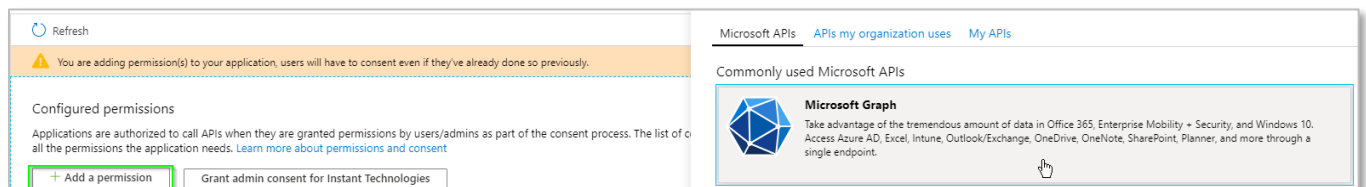


Figure 7: Manage Required Permissions

3. Select **Microsoft Graph** from the list of Microsoft API's listed.

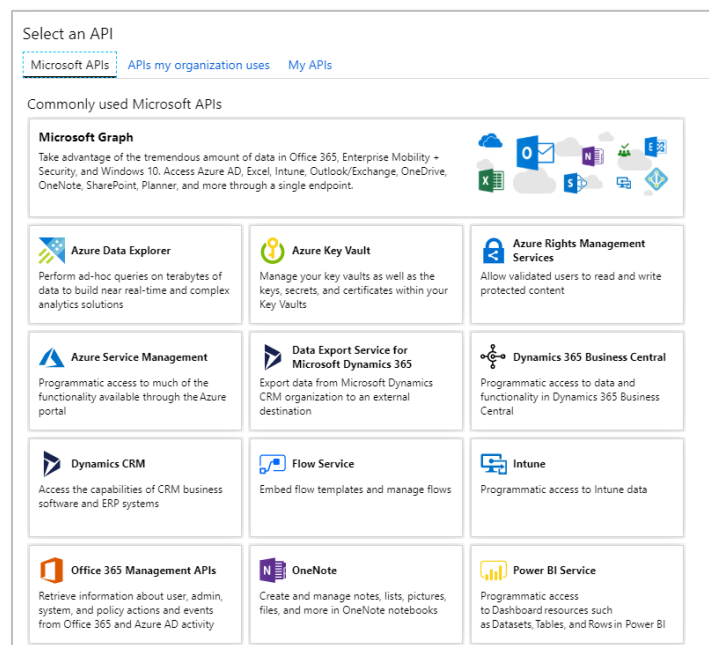


Figure 8: Configure Required Permissions

4. Select **Application permissions**.
5. Use the search bar to find and add the following required permissions
 - a. Directory.Read.All
 - b. Group.Read.All
 - c. Group.ReadWrite.All
 - d. User.Read.All
6. Once all of the above permissions are selected, click the **Add Permissions** button.

▼ Directory (1)		
<input checked="" type="checkbox"/>	Directory.Read.All Read directory data ⓘ	Yes
<input type="checkbox"/>	Directory.ReadWrite.All Read and write directory data ⓘ	Yes
▶ Domain		
▶ EduAdministration		
▶ EduAssignments		
▶ EduRoster		
▶ Files		
▼ Group (1)		
<input type="checkbox"/>	Group.Read.All Read all groups ⓘ	Yes
<input checked="" type="checkbox"/>	Group.ReadWrite.All Read and write all groups ⓘ	Yes

Figure 9: Select Permissions for Graph Api

7. Click the Add a Permission button again.
8. Select **Azure Active Directory Graph**. This might be at the bottom of the list.
9. Select **Delegated permissions**.
10. Use the search bar to find and add the following required permissions:
 - a. User.Read
 - b. Presence.Read.All
 - c. AppCatalog.ReadWrite.All
 - d. TeamsApp.ReadWrite.All

▼ User (1)		
<input checked="" type="checkbox"/>	User.Read Sign in and read user profile ⓘ	-
<input type="checkbox"/>	User.Read.All Read all users' full profiles ⓘ	Yes
<input type="checkbox"/>	User.ReadBasic.All Read all users' basic profiles ⓘ	-

Figure 10: Select Permissions for Delegated Permissions

11. Finally, it is necessary to grant administrator consent for these permissions. Click the Grant admin consent button

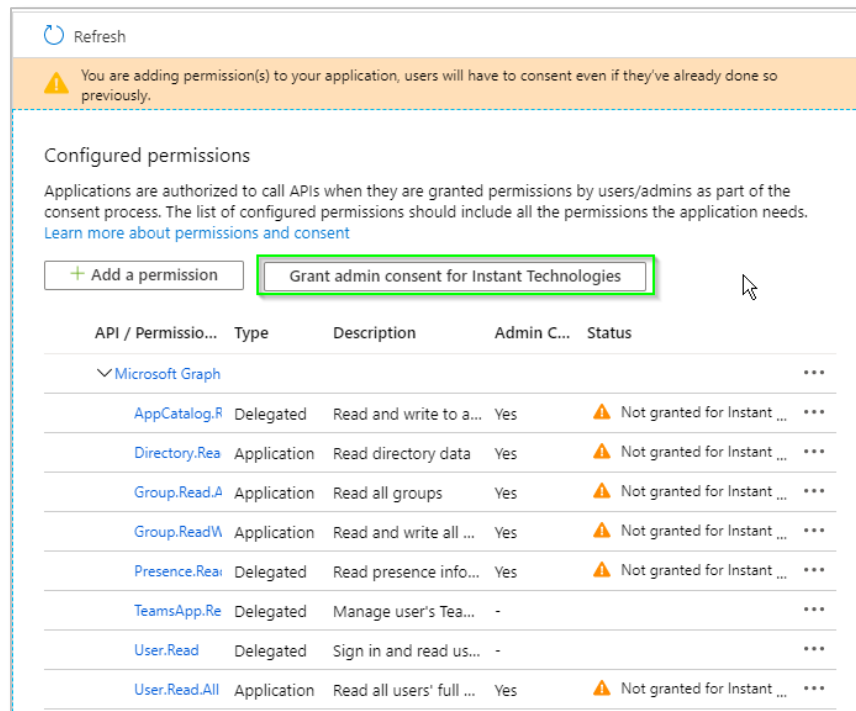


Figure 11: Grant Admin Consent

ADD REDIRECT URIS

1. To add Redirect URLs click the **Authentication** button.

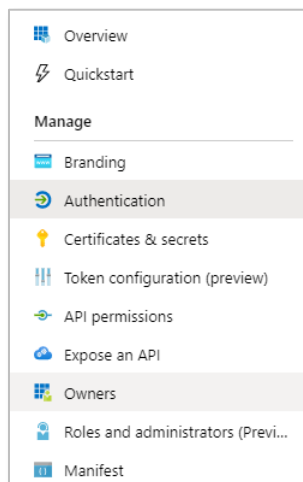


Figure 12: Configure Reply URLs

- Under the Web section there is an area to add in Redirect URIs. There should be 1 Redirect URI saved in there already, it will look something like this: [https://\[yourwebserver\].domain.com/chime](https://[yourwebserver].domain.com/chime) (If there is not a URI there with this format, one should be added before proceeding to the next step)

Figure 13: Configure Reply URLs

- In the text box below, add in a URI with this format: [https://\[yourwebserver\].domain.com/chime/?a](https://[yourwebserver].domain.com/chime/?a)
- Further down, under the Implicit grant section, select **ID tokens**. If you do not select this users will not be able to authenticate into Chime.
- Click the **Save** button.

CREATING BOTS FOR CHIME DISPATCHERS

This must be done after completing the Chime installation.

Each Chime queue will need at least one dispatcher bot endpoint created for users to access seeking help, and to route those requests to an agent. Each bot that is supplied for a queue will allow agents to handle one concurrent chat – i.e. for agents to be able to handle two chats from users at the same time, two bots must be created for the queue.

You must be an administrator for your Microsoft Azure subscription to complete these steps.

CREATING A BOT REGISTRATION IN AZURE

Note: Steps and screenshots displayed here are accurate as of April 2019. The Azure Portal changes rapidly, and the UI and flow may change slightly in the future.

1. Navigate to the Azure Portal, at <https://portal.azure.com>
2. Click the “Create Resource” button in the side bar. Enter “Bot Channels Registration” in the search bar and select the matching option from the list.

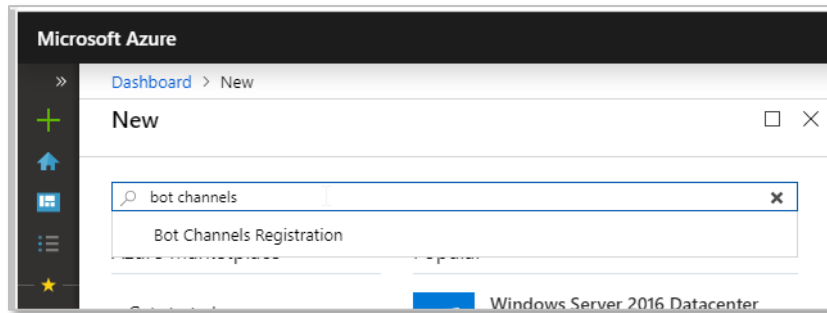


Figure 14: Search for Bot Channels Registration

3. Click “Create” to start creating the resource.

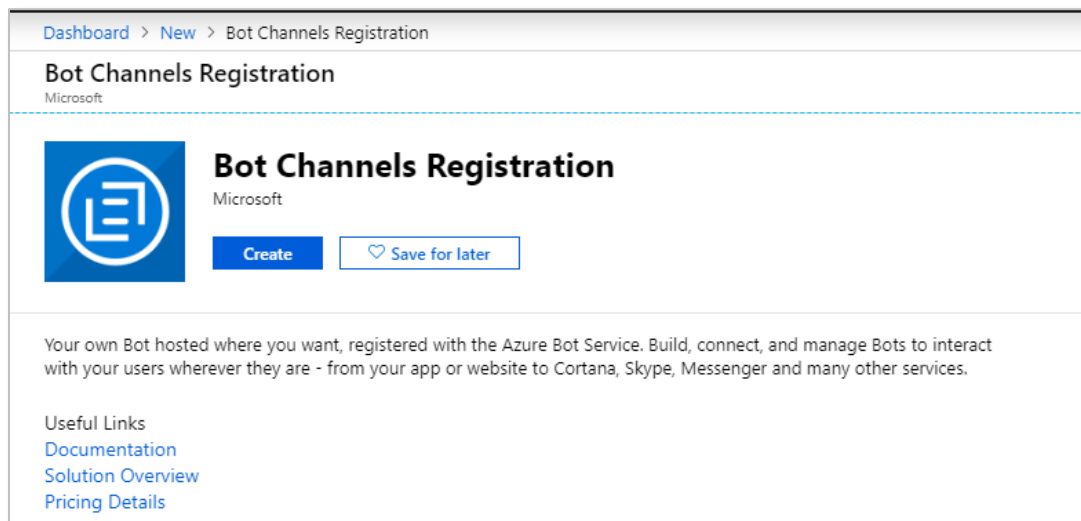


Figure 15: Create Bot Channels Registration

4. You should see a configuration page to create the Bot Channel Registration. Fill out the following fields:
 - a. **BotName:** Select an appropriate name for the bot – we would suggest matching the name of the queue in Chime that this bot will be used with
 - b. **Subscription:** Select an Azure subscription to tie this bot registration to.
 - c. **Resource Group:** Select an existing Azure Resource Group to contain this registration, or create a new resource group. We would suggest creating a group and using it for all Chime bot registrations.

- d. **Location:** Select the most appropriate Azure datacenter location for your users.
- e. **Pricing Tier:**
 - i. If users will be primarily contacting Chime through the Teams client, then the F0 tier may be the most cost-effective and appropriate level
 - ii. If users will be primarily using the web client to contact Chime, then select the S1 tier.
- f. **Messaging endpoint:** For now, leave this blank. It will be necessary to update this later, once the bot has been assigned to a Chime queue.
- g. **Application Insights:** Off
- h. **Microsoft App ID and password:** Leave this as “Auto create App ID and password”

Dashboard > New > Bot Channels Registration

Bot Channels Registration Bot Service

* Bot name *ChimeBot* ✓

* Subscription *[selected]*

* Resource group *[selected]*

[Create new](#)

* Location *East US*

Pricing tier ([View full pricing details](#)) *S1 (1K Premium Msgs/Unit)*

Messaging endpoint *https URL*

Application Insights *Off*

Microsoft App ID and password *Auto create App ID and password*

Create [Automation options](#)

Figure 16: Create the Bot Channel Registration

5. When this is completed, click “Create” and the bot registration will be created. After some time, this provisioning will complete, and you can navigate to the settings for the bot registration.
6. Next, navigate to the Channels tab for the bot registration

7. Click the Teams icon to enable the bot for Microsoft Teams

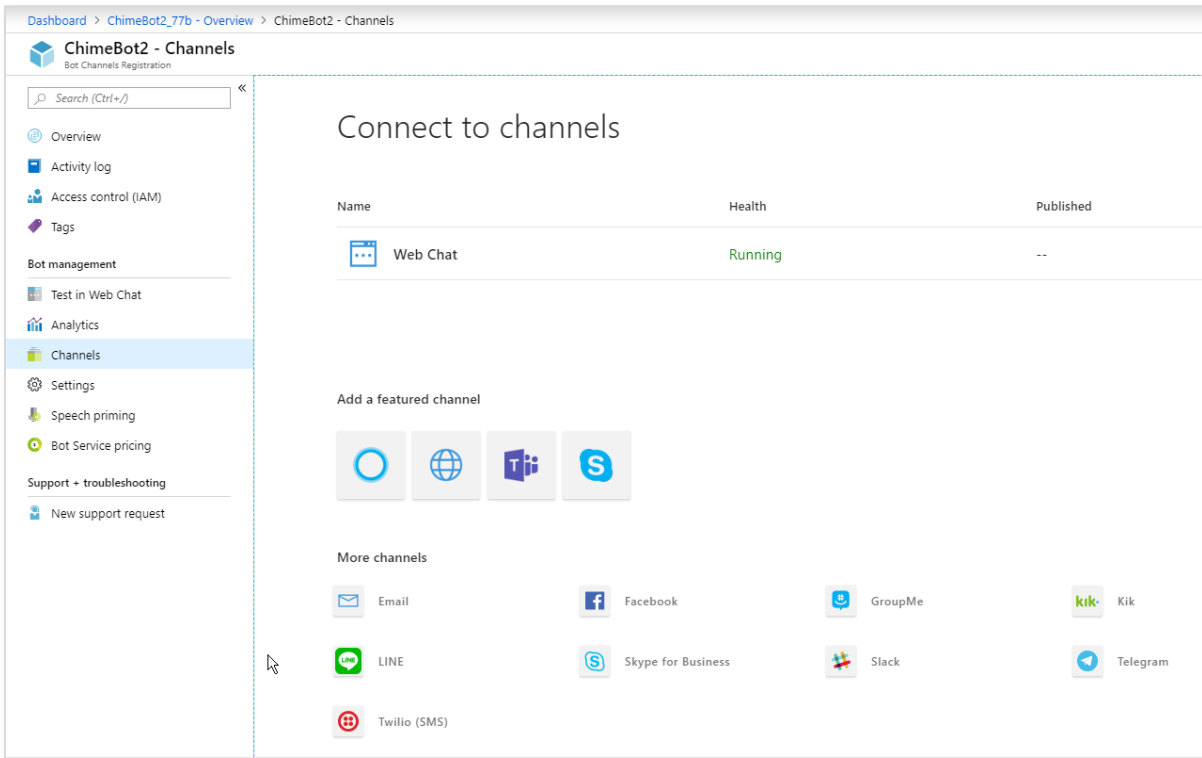


Figure 17: Click the Teams Icon

8. No additional configuration is needed for Chime functionality, so just click Save to enable the Teams channel

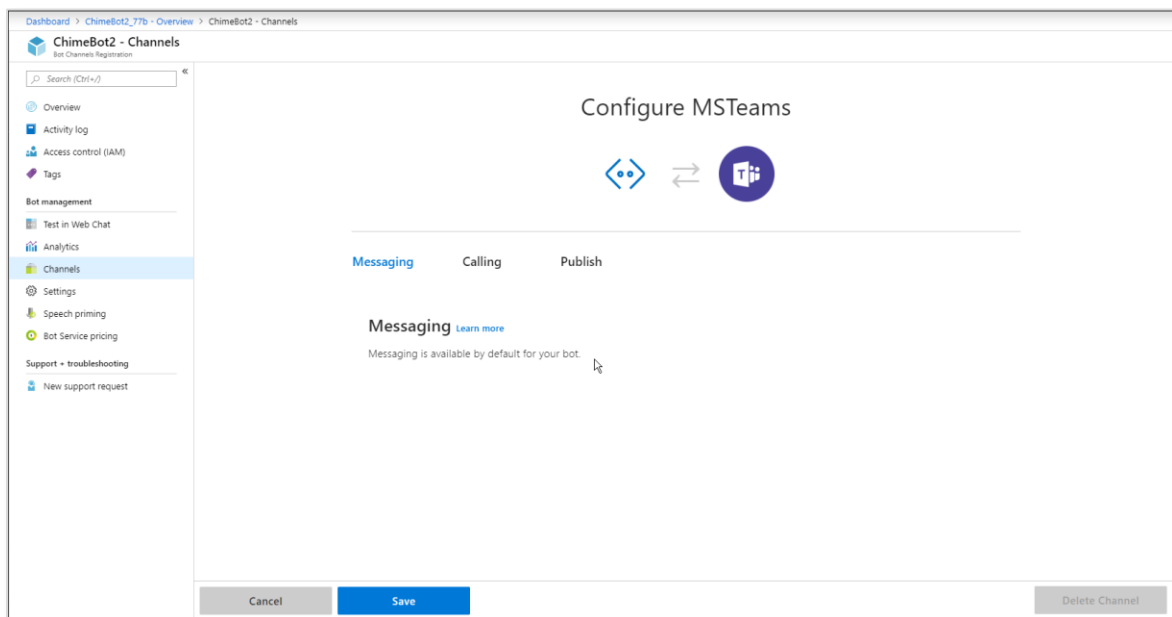


Figure 18: Configure MSTEams

9. If the Chime web client is going to be used to contact the queue, it is also necessary to configure the Direct Line channel

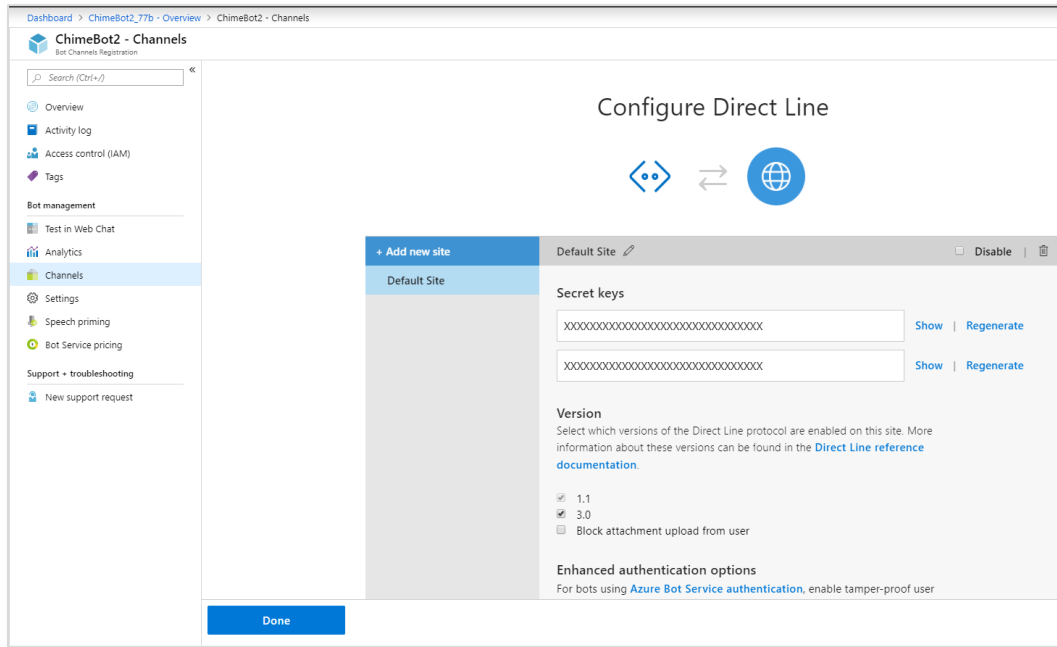


Figure 19: Configure Direct Line

10. Click on the Show button to reveal the **Direct Line secret key**. Save this value, as it will be required later to configure the bot in Chime.
11. Next navigate to the Settings tab on the bot registration.

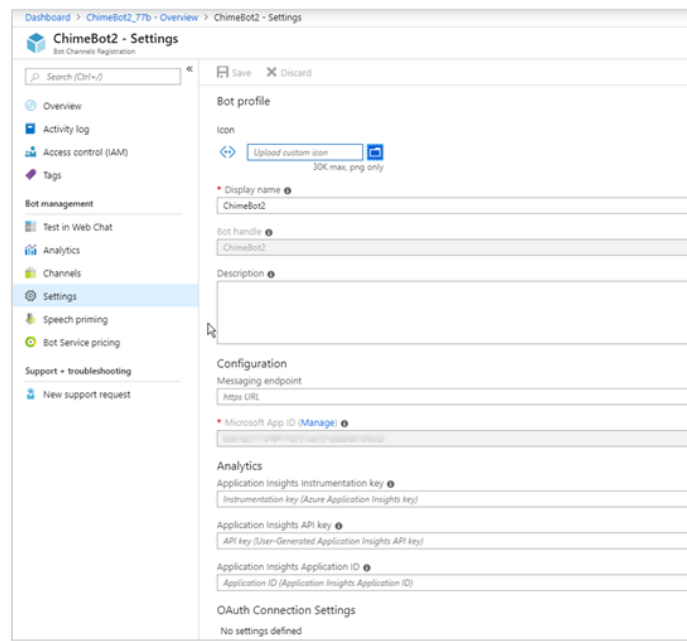
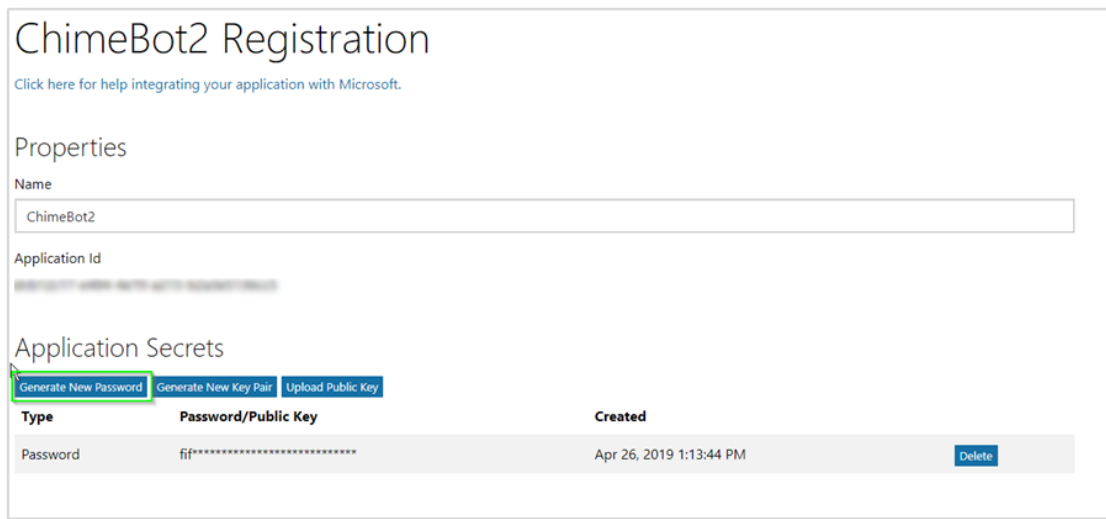


Figure 20: Bot Settings

12. You may upload a custom avatar image and customize the Display Name of the bot if you choose.
Note the **Bot handle** and **Microsoft App ID** fields here, as they will be needed to configure the bot in Chime.
13. At the present time, there is no way to determine the password that is associated with the automatically created App ID for the bot registration, so it is necessary to create a new password. Click the Manage link next to the Microsoft App ID field.
This should bring you to a new page where it is possible to create a new password. Click the “Generate New Password” button and note the password value that is generated – it is not possible to recover this password later after it has been generated and will be necessary to configure the bot in Chime.



ChimeBot2 Registration

[Click here for help integrating your application with Microsoft.](#)

Properties

Name
ChimeBot2

Application Id
[Redacted]

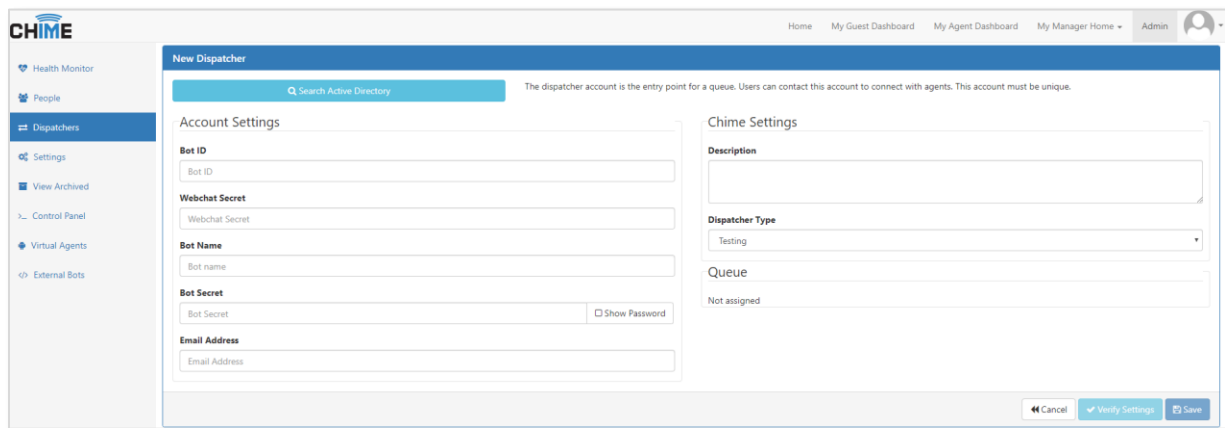
Application Secrets

[Generate New Password](#) [Generate New Key Pair](#) [Upload Public Key](#)

Type	Password/Public Key	Created	
Password	fif*****	Apr 26, 2019 1:13:44 PM	Delete

Figure 21: Bot Registration App Secret

14. With the Bot Handle, App ID, App password, and Direct Line secret, it is possible to setup the bot as a dispatcher in Chime. Navigate to your Chime server, and then to Admin/Dispatchers, and click the New Dispatcher button.



CHIME

Home My Guest Dashboard My Agent Dashboard My Manager Home Admin

Health Monitor People Dispatchers Settings View Archived Control Panel Virtual Agents External Bots

New Dispatcher

Search Active Directory

The dispatcher account is the entry point for a queue. Users can contact this account to connect with agents. This account must be unique.

Account Settings

Bot ID
Bot ID

Webchat Secret
Webchat Secret

Bot Name
Bot name

Bot Secret
Bot Secret ☐ Show Password

Email Address
Email Address

Chime Settings

Description

Dispatcher Type
Testing

Queue
Not assigned

Cancel Verify Settings Save

Figure 22: Add New Dispatcher in Chime

15. Enter the information from the bot registration in the following fields:
 - a. **Bot ID:** the Microsoft App ID of the bot registration
 - b. **Webchat Secret:** The Direct Line secret key
 - c. **Bot Name:** The Bot Handle
 - d. **Bot Secret:** The Microsoft App ID password
16. Once this is completed, you should be able to verify and then save the new dispatcher.
17. Once the dispatcher has been created in Chime, the next step is to create a new queue or add the dispatcher to an existing queue. Once this is done, you should see a block on the queue settings page that displays the URL for the messaging endpoint for the queue when it is running in Chime:

Figure 23: Chime Queue Settings

18. Take this URL, and go back to the Bot Channel Registration in the Azure portal, then navigate to the Settings tab.

19. Paste this URL into the Messaging endpoint field for the bot and save the changes.

Dashboard > ChimeBot2_77b - Overview > ChimeBot2 - Settings

ChimeBot2 - Settings

Bot Channels Registration

Search (Ctrl+/)

Save Discard

Bot profile

Icon
Upload custom icon
30K max, png only

* Display name
ChimeBot2

Bot handle
ChimeBot2

Description

Configuration

Messaging endpoint
<https://api.chimebot2.com/Chime/bot/1/api/messages>

* Microsoft App ID (Manage)
a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6

Analytics

Application Insights Instrumentation key
Instrumentation key (Azure Application Insights key)

Application Insights API key
API key (User-Generated Application Insights API key)

Application Insights Application ID
Application ID (Application Insights Application ID)

OAuth Connection Settings

No settings defined

Figure 24: Settings - Configuration