



Chime for Teams Azure Prerequisites

May 2019

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 - 2019 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

Configuring Azure AD Authentication for Chime For Teams	4
Prerequisites:.....	4
Configure Active Directory Authentication	5
Retrieve your Azure Tenant ID	5
Create Application	5
Register the Chime Application	6
Configure the Application	6
Configure Application Permissions	7
Create a New API Key.....	9
Add Reply URLs	10
Setup Before Chime Install	11
SSL Certificate.....	11
Azure Active Directory Accounts List	11
Setup After Chime Install	12
Install Wizard	12
Creating Bots for Chime Dispatchers.....	13
Creating a Bot Registration in Azure	13

CONFIGURING AZURE AD AUTHENTICATION FOR CHIME FOR TEAMS

Chime for Skype for 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 Skype for Business 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.

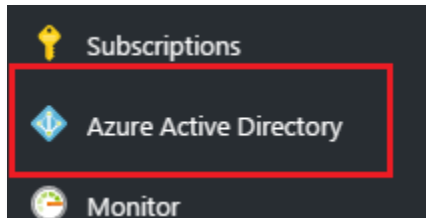


Figure 1: Begin Setting up Active Directory

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**

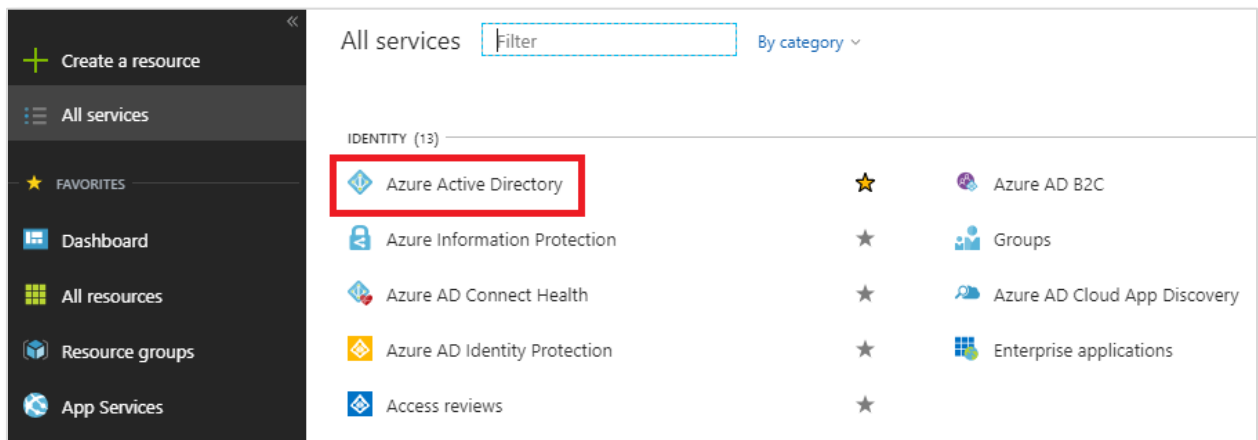

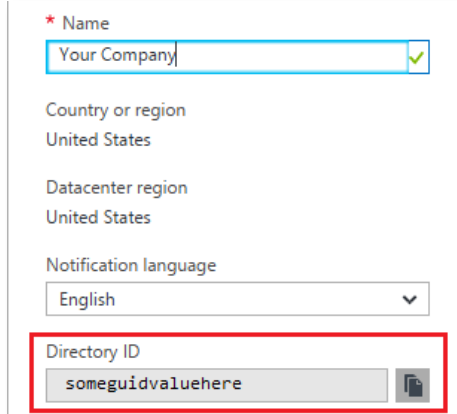


Figure 2: Secondary Option to Active Directory Setup

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.

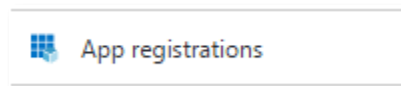


The screenshot shows the 'Properties' blade in the Azure Active Directory portal. The 'Name' field contains 'Your Company'. Below it, 'Country or region' and 'Datacenter region' are both set to 'United States'. The 'Notification language' is set to 'English'. At the bottom, the 'Directory ID' field contains the value 'someguidvaluehere' and is highlighted with a red rectangular box. A copy icon is visible to the right of the Directory ID field.

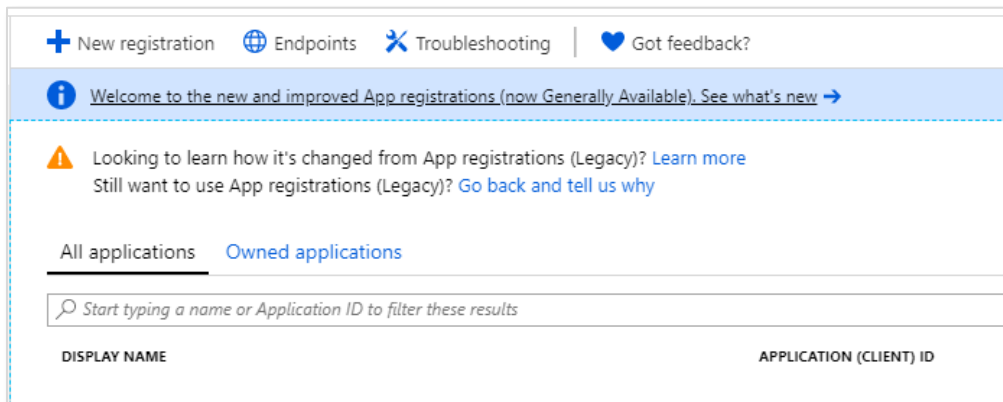
Figure 3: Copy Directory ID

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.



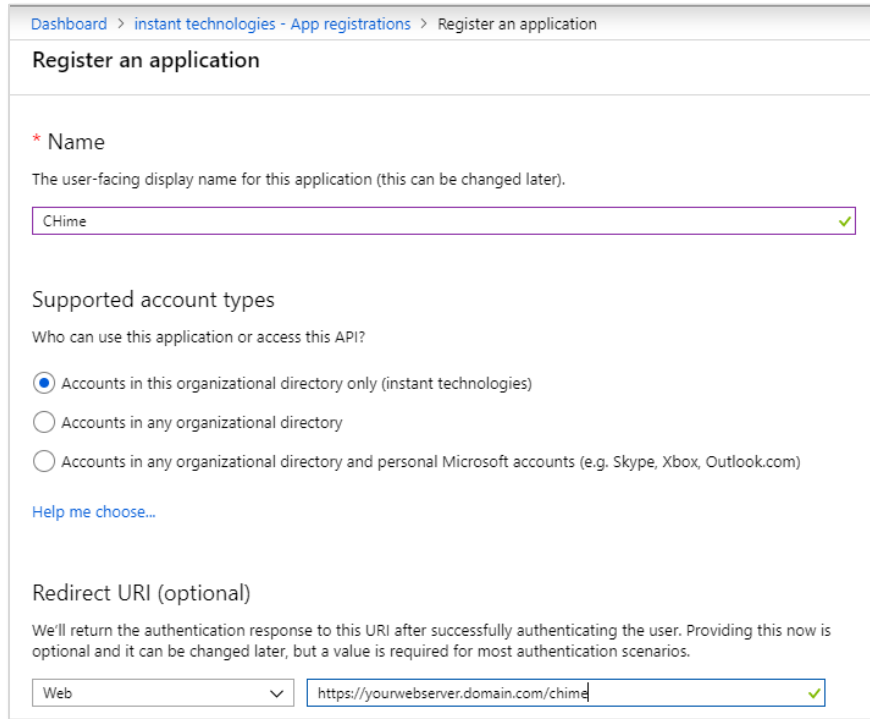
The screenshot shows the 'App Registrations' blade in the Azure Active Directory portal. At the top, there are navigation links: '+ New registration', 'Endpoints', 'Troubleshooting', and 'Got feedback?'. Below these is a blue banner with an information icon and the text: 'Welcome to the new and improved App registrations (now Generally Available). See what's new →'. Underneath is a warning icon and text: 'Looking to learn how it's changed from App registrations (Legacy)? Learn more' and 'Still want to use App registrations (Legacy)? Go back and tell us why'. There are two tabs: 'All applications' and 'Owned applications'. Below the tabs is a search bar with the placeholder text: 'Start typing a name or Application ID to filter these results'. At the bottom, there are two columns: 'DISPLAY NAME' and '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 this organizational directory only** as the Supported account types
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

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

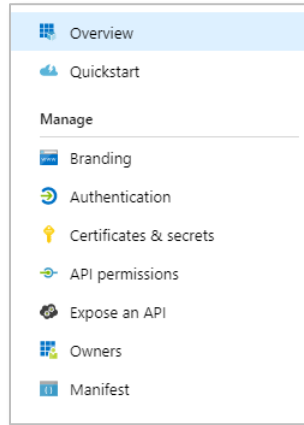


Figure 6: Access Required API Permissions

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

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Azure Active Directory Graph (2)			
Directory.Read.All	Application	Read directory data	Yes <input checked="" type="checkbox"/> Granted for Instant Te...
User.Read	Delegated	Sign in and read user profile	- <input checked="" type="checkbox"/> Granted for Instant Te...
▼ Microsoft Graph (3)			
Directory.Read.All	Application	Read directory data	Yes <input checked="" type="checkbox"/> Granted for Instant Te...
Group.ReadWrite.All	Application	Read and write all groups	Yes <input checked="" type="checkbox"/> Granted for Instant Te...
User.Read.All	Application	Read all users' full profiles	Yes <input checked="" type="checkbox"/> Granted for Instant Te...

Figure 7: Manage Required Permissions

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

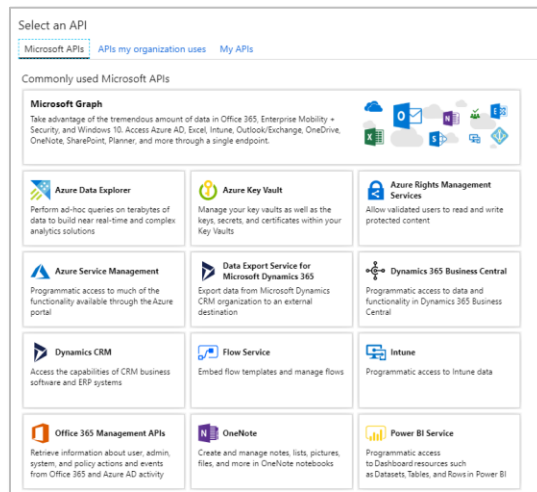


Figure 8: Configure Required Permissions

4. Select **Application permissions**.
5. Use the search bar to find and add the following required permissions
 - a. Directory.Read.All
 - b. Group.ReadWrite.All
 - c. 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. Search for User.Read and Select it.

▼ 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. Select **Application permissions**.
12. Search for Directory.Read.All and Select it.

▼ 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

Figure 11: Select Permissions for Application Permissions

13. Click the **Add Permissions** button.

CREATE A NEW API KEY

1. Click the **Certificates & secrets** button.

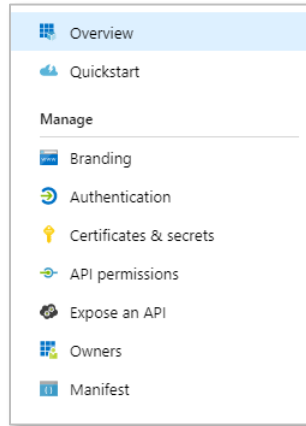


Figure 12: Access Certificates & Secrets

2. Click the **New client secret** button.
3. Enter a description for your client secret.
4. Select a duration for this API key. We suggest creating a key which never expires.
5. Click **Add** to create a new API key.
6. Copy the newly created API key somewhere you can retrieve it. You will need this API key when configuring the Chime application

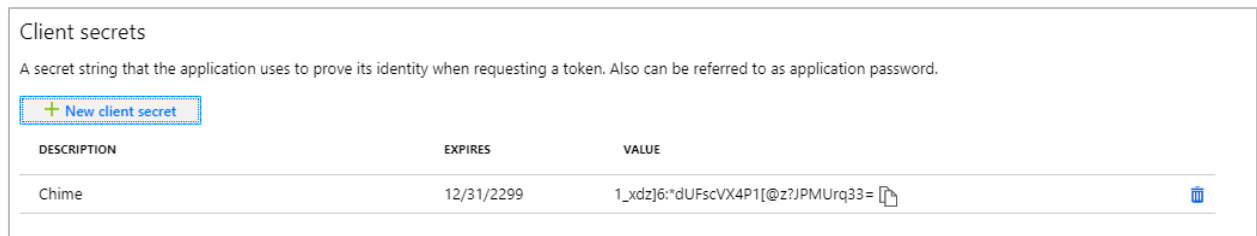


Figure 13: Setup API Key

ADD REPLY URLS

1. To add Reply URLs we will need to navigate to legacy version of the App Registrations blade.
2. Navigate back to the dashboard of your Azure Active Directory.
3. Click the **App registrations (Legacy)** button.
4. Select the app registration that you created earlier.
5. Click the **Settings** button on the blade that opens.
6. In the **Settings** blade, click the **Reply URLs** button.

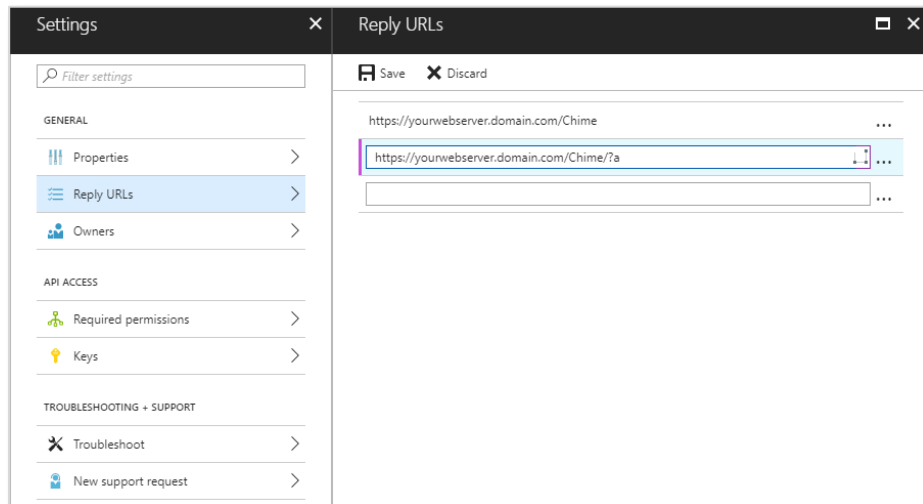


Figure 14: Configure Reply URLs

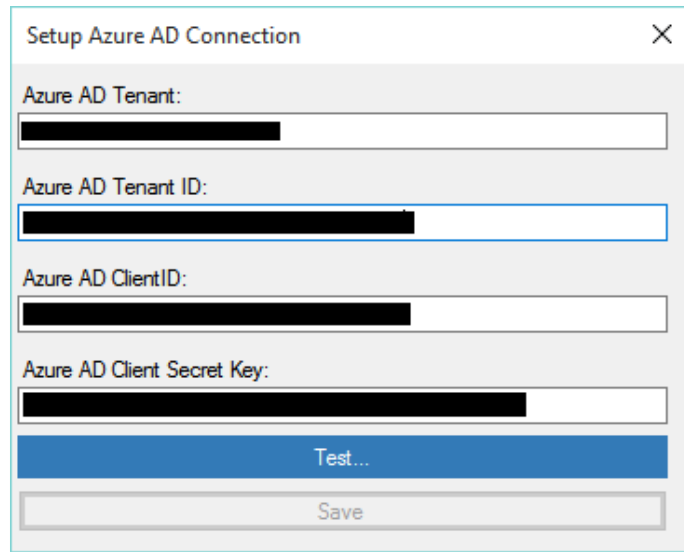
7. There should be 1 reply URL saved in there already, it will look something like this: [https://\[yourwebservice\].domain.com/chime](https://[yourwebservice].domain.com/chime) (If there is not a URL there with this format, one should be added before proceeding to the next step)
8. In the text box below, add in a reply URL with this format: [https://\[yourwebservice\].domain.com/chime/?a](https://[yourwebservice].domain.com/chime/?a)
9. Click the **Save** button.
10. Close the Reply URLs blade.

SETUP BEFORE CHIME INSTALL

SSL CERTIFICATE

To set up a Chime deployment with Office 365, you will need to acquire a SSL certificate. This certificate will be installed on the server on the same server that the Chime instance will be on. Without this certificate installed, no users will be able to authenticate into the web app.

AZURE ACTIVE DIRECTORY ACCOUNTS LIST



The screenshot shows a dialog box titled "Setup Azure AD Connection" with a close button (X) in the top right corner. It contains four text input fields, each with a blacked-out value: "Azure AD Tenant:", "Azure AD Tenant ID:", "Azure AD Client ID:", and "Azure AD Client Secret Key:". Below the fields are two buttons: a blue "Test..." button and a grey "Save" button.

Figure 15: Setup Azure AD Connection

Azure AD Tenant: _____

This is usually the domain associated with your Office 365 email address, e.g. example.com

Azure AD Tenant ID: _____

This value is from Page 5 (Directory ID)

Azure AD Client ID _____

This value is from Page 6 (Application ID)

Azure AD Client Secret Key _____

This value is from Page 9

SETUP AFTER CHIME INSTALL

INSTALL WIZARD

Once Chime has been installed, there will be a configuration wizard that opens. The configuration wizard provides a tool to register a SSL certificate with the Chime application.

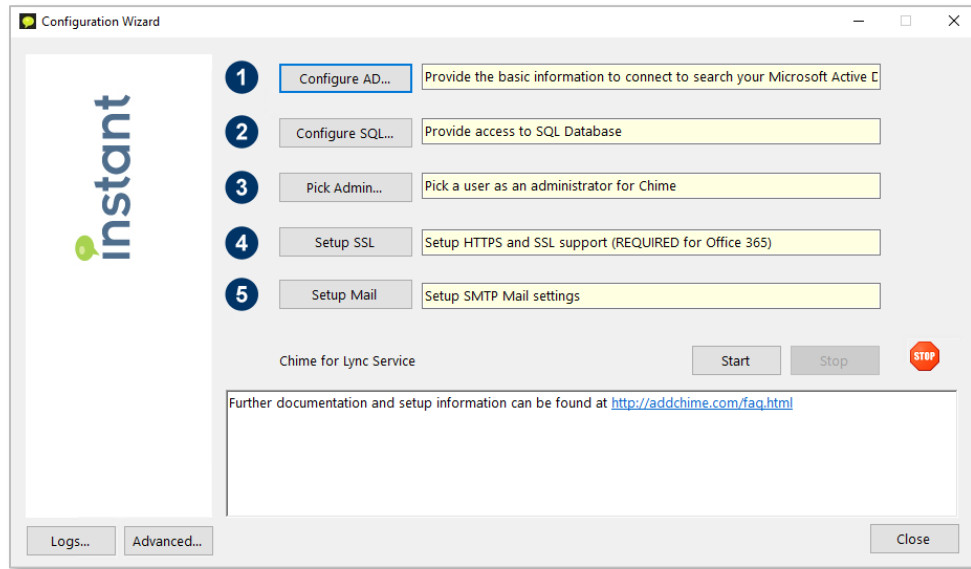


Figure 16: Configuration Wizard

Once the certificate has been installed on the server, you can follow these steps.

1. Click the **Setup SSL** button.
2. Under SSL Binding, click **Add**.

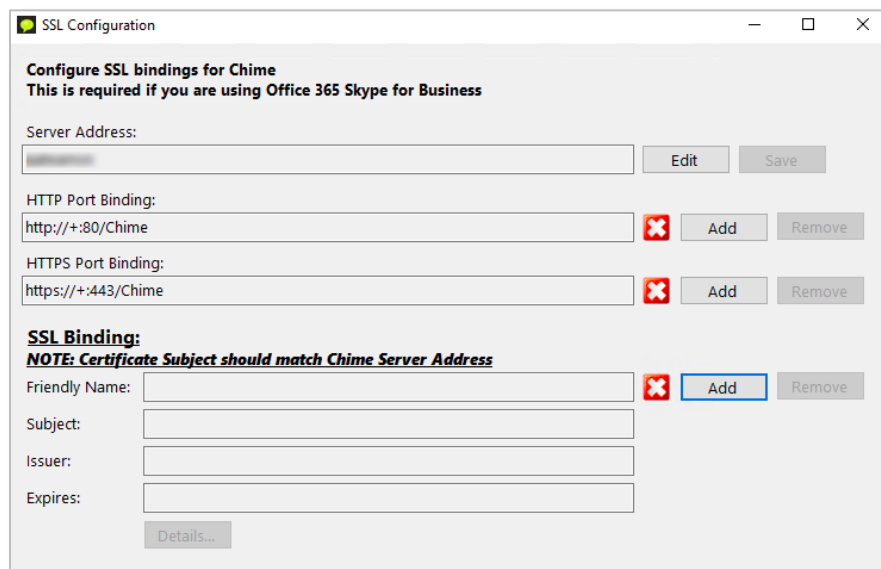


Figure 17: Setup SQL Connection

3. When the Select SSL Certificate window opens, select the *.imchime.com certificate.

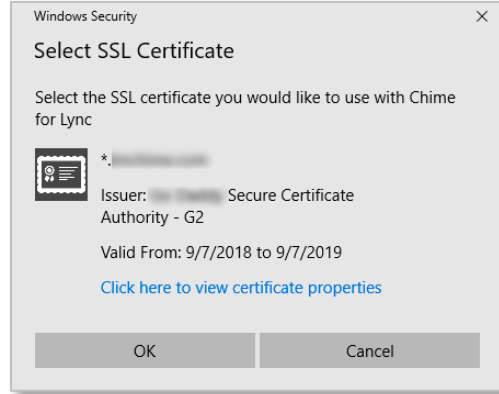


Figure 18: Select SSL Certificate

4. Close the SSL Configuration modal

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.

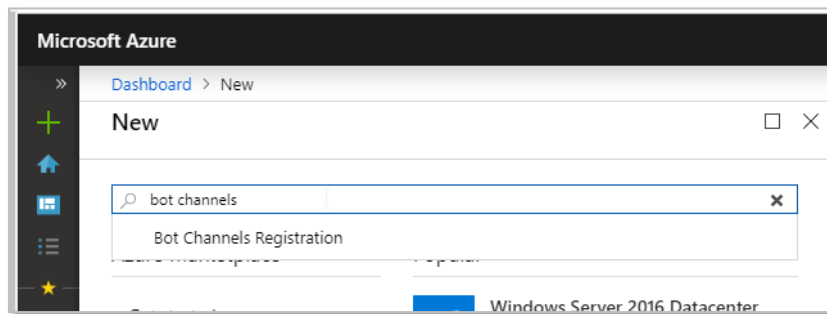


Figure 19: Search for Bot Channels Registration

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

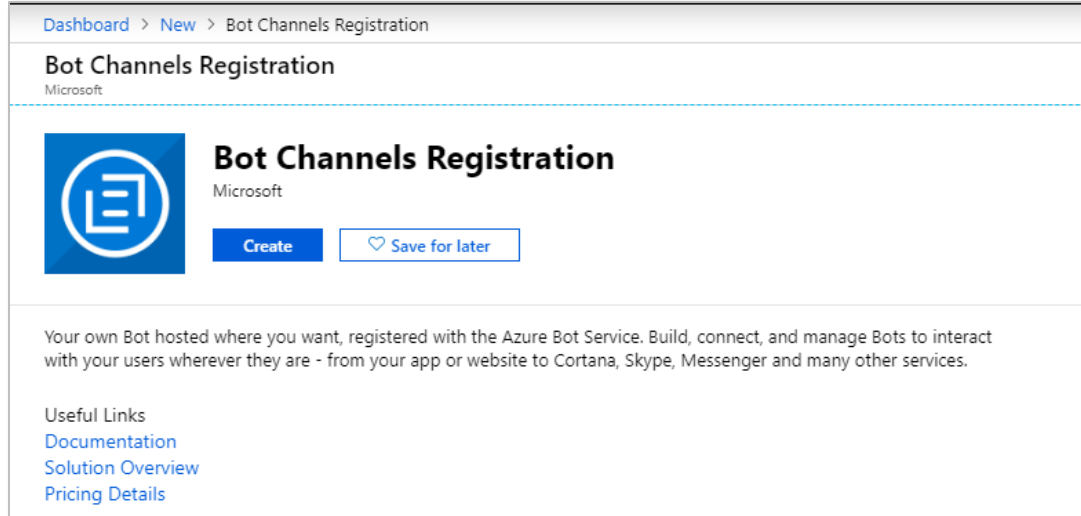


Figure 20: Create Bot Channels Registration

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 ⓘ
 ✓

* Subscription

* Resource group

[Create new](#)

* Location

Pricing tier ([View full pricing details](#))

Messaging endpoint

Application Insights ⓘ

Microsoft App ID and password ⓘ
 >

[Automation options](#)

Figure 21: 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

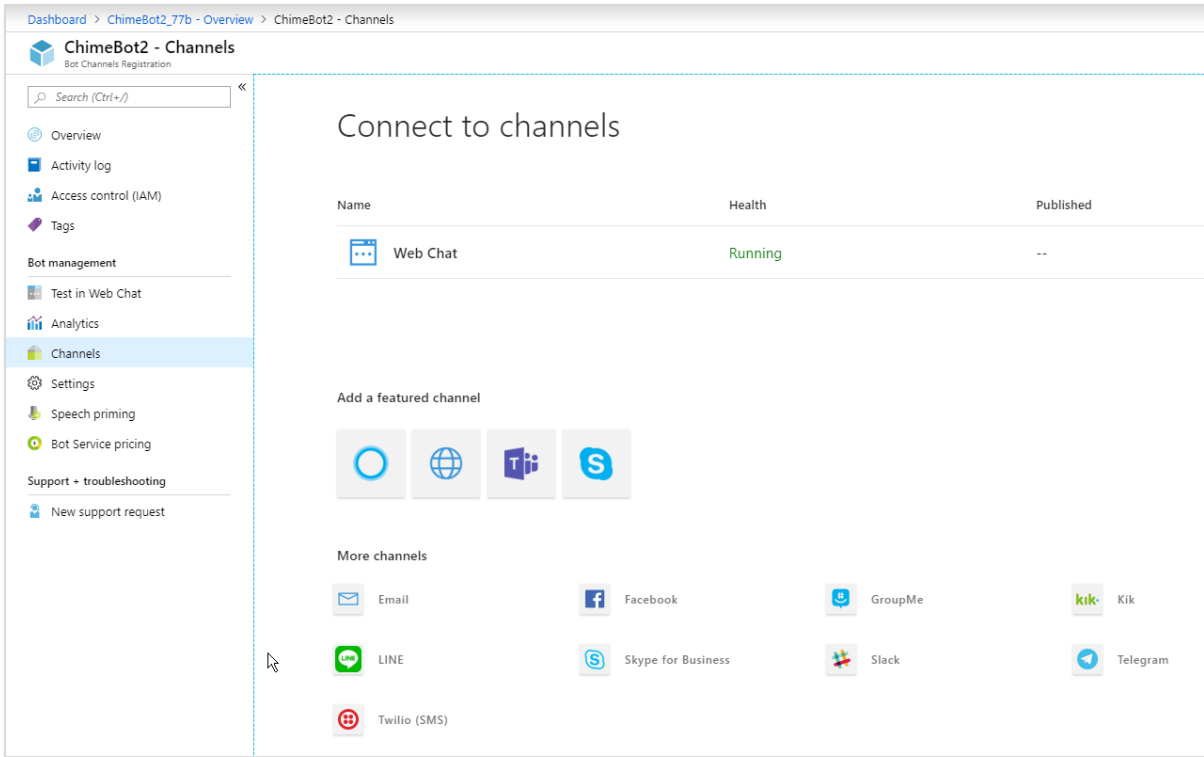


Figure 22: Click the Teams Icon

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

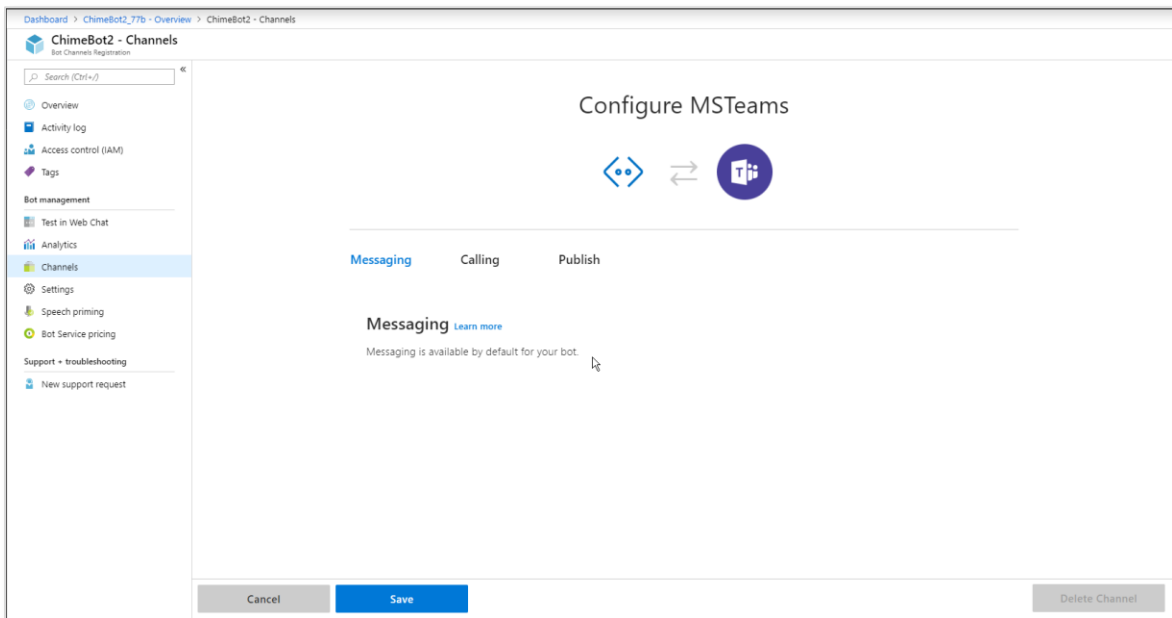


Figure 23: Configure MStTeams

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

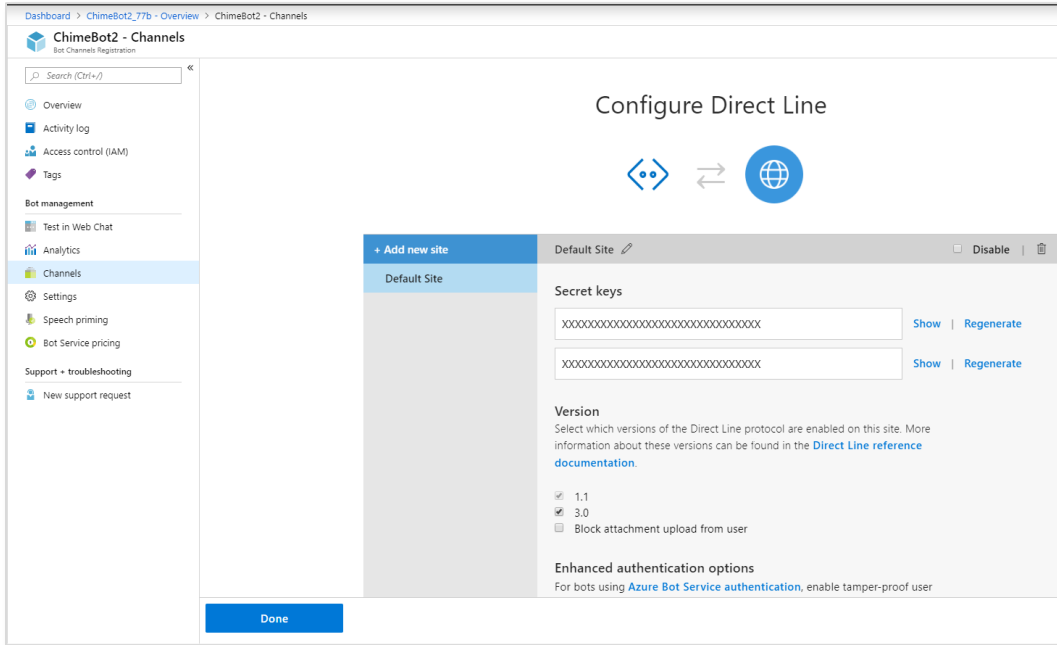


Figure 24: Configure Direct Line

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.

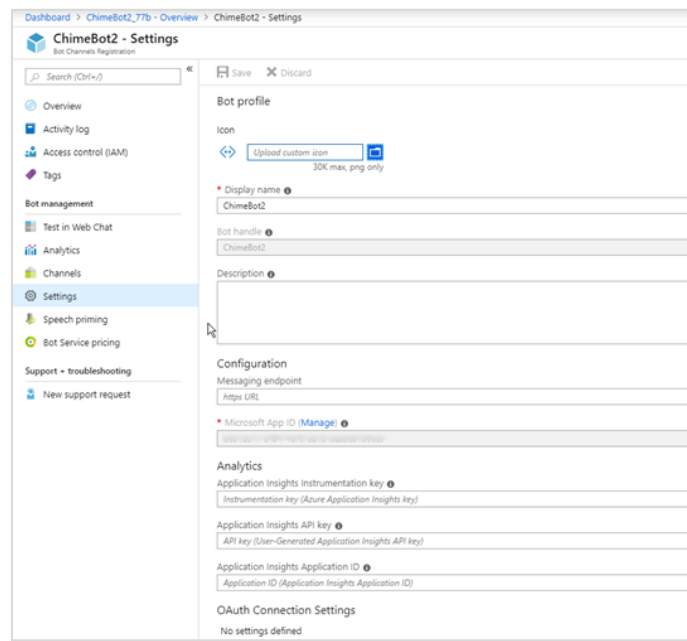


Figure 25: Bot Settings

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.

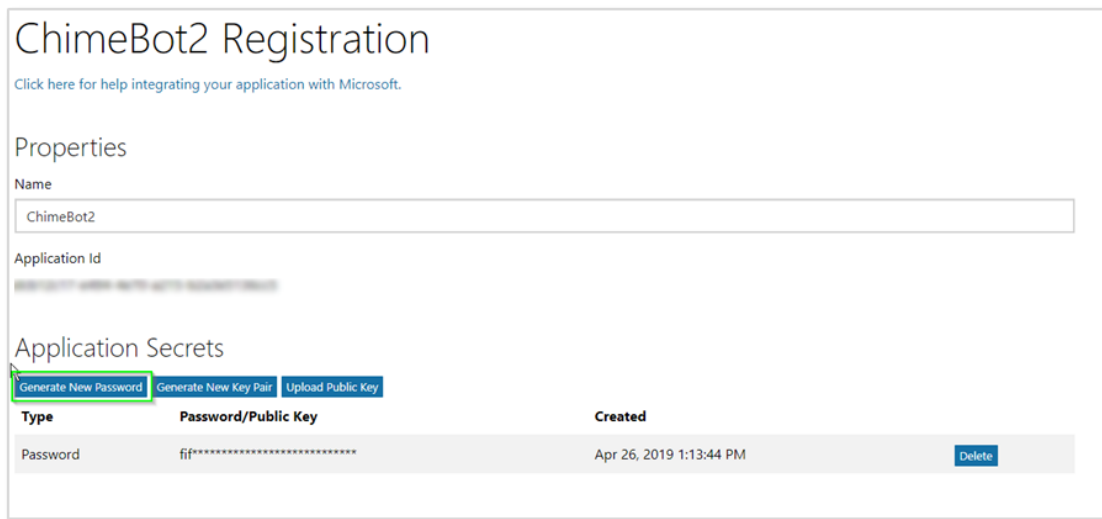


Figure 26: Bot Registration App Secret

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.

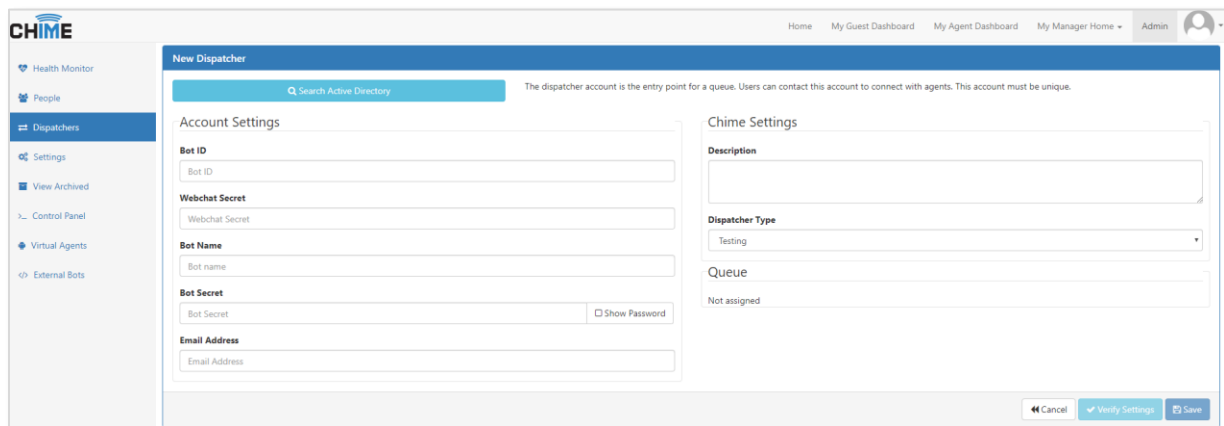


Figure 27: Add New Dispatcher in Chime

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
 - e.
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:

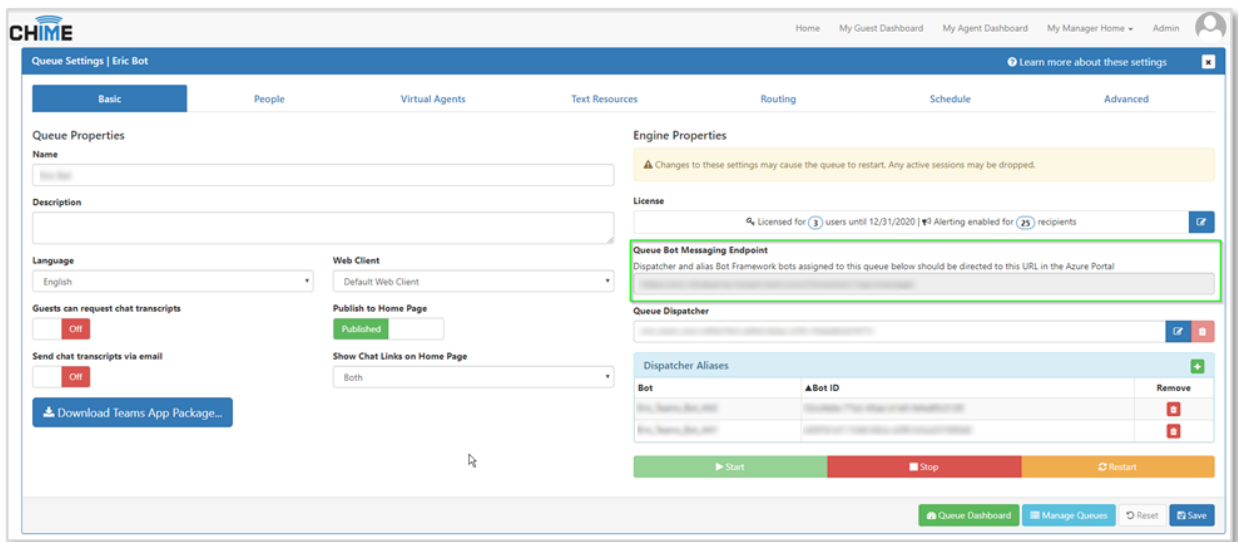


Figure 28: Chime Queue Settings

18. Take this URL, and go back to the Bot Channel Registration in the Azure portal, then navigate to the Settings tab.
Paste this URL into the Messaging endpoint field for the bot and save the changes.

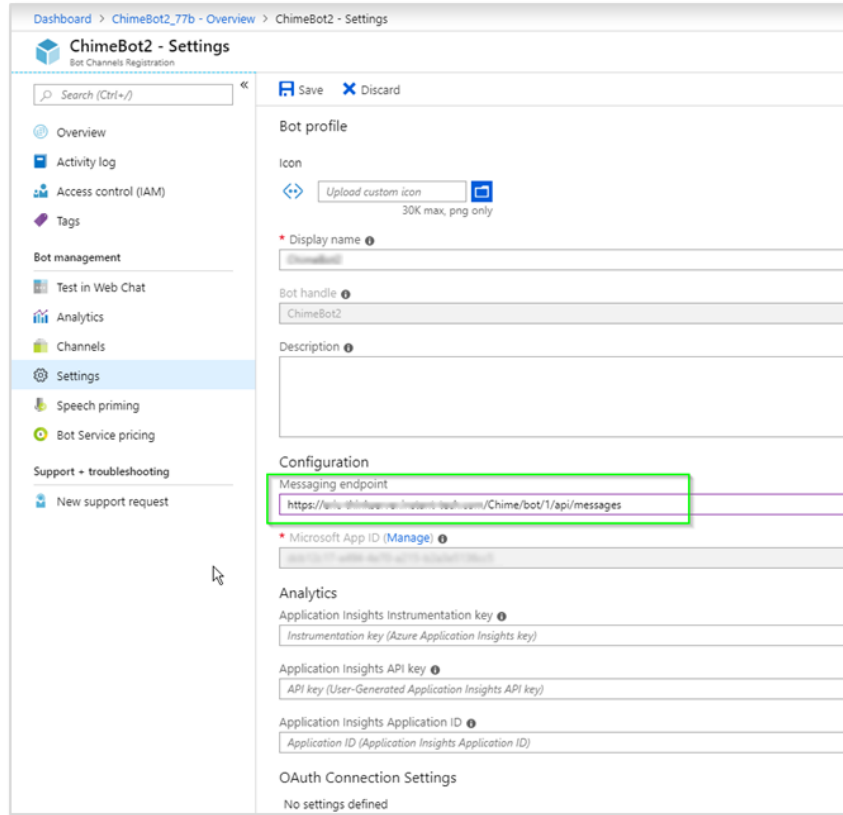


Figure 29: Settings - Configuration