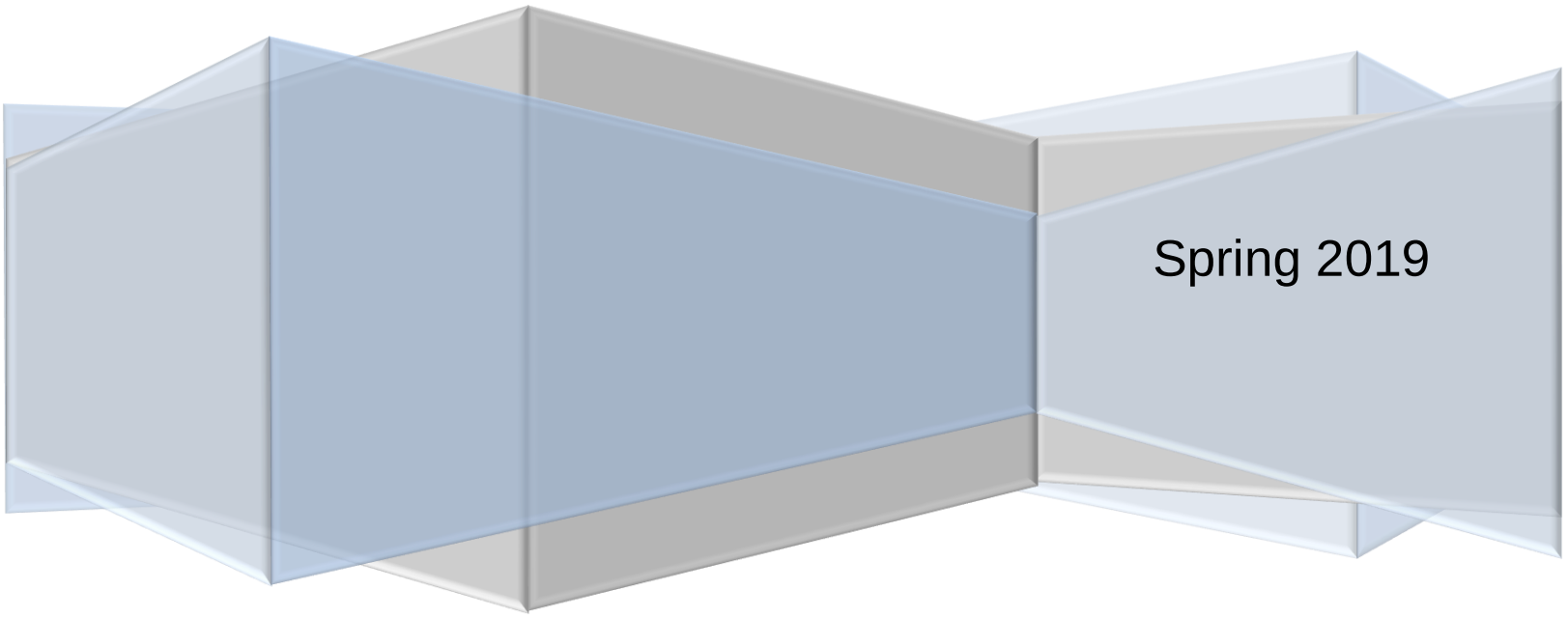
instant

CHIME

PREREQUISITES GUIDE



Spring 2019

Copyright and Disclaimer

Trademarks

Contact Information

See our Web site for Customer Support information.

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

Microsoft CERTIFIED Partner | ISV/Software Solutions

CONTENTS

CHIME PREREQUISITES GUIDE

CONFIGURING AZURE ACTIVE DIRECTORY AUTHENTICATION FOR CHIME

Chime 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:

1. You must have an Office365 tenant for your organization.
2. You must be an administrator of your Office 365 domain.
3. 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.

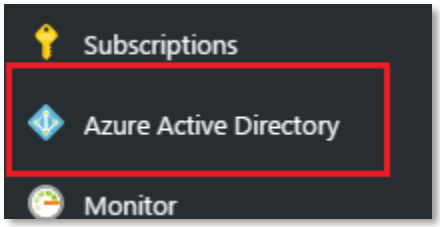


Figure 1: Azure Active Directory Sidebar

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

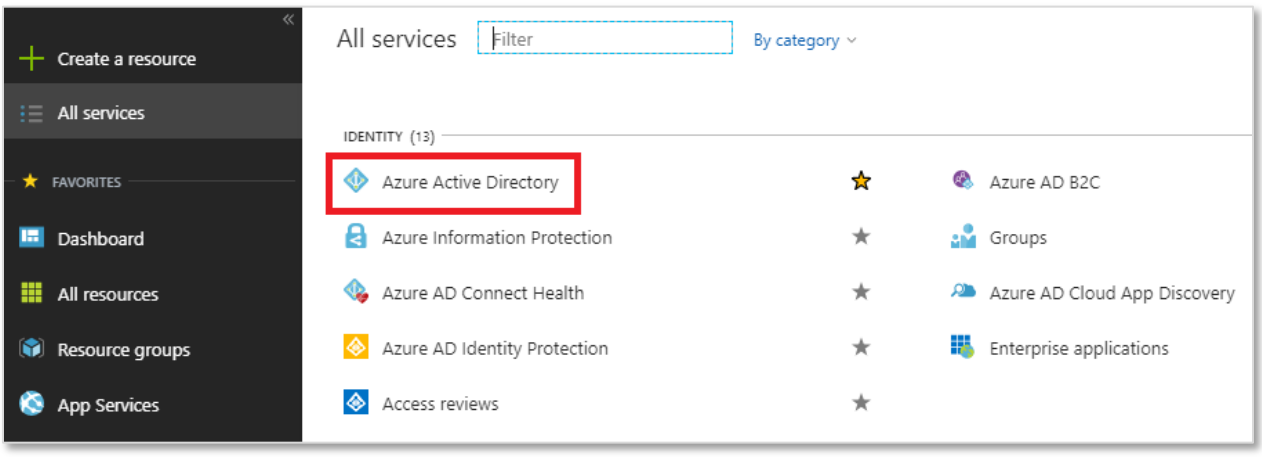
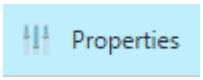


Figure 2: Azure Active Directory Search

CONFIGURE ACTIVE DIRECTORY AUTHENTICATION

RETRIEVE YOUR AZURE TENANT ID

1. Select 

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.

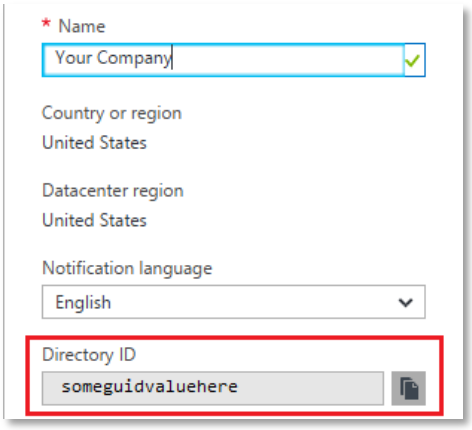
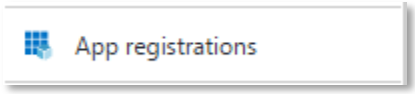


Figure 3: Copy Directory ID

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.

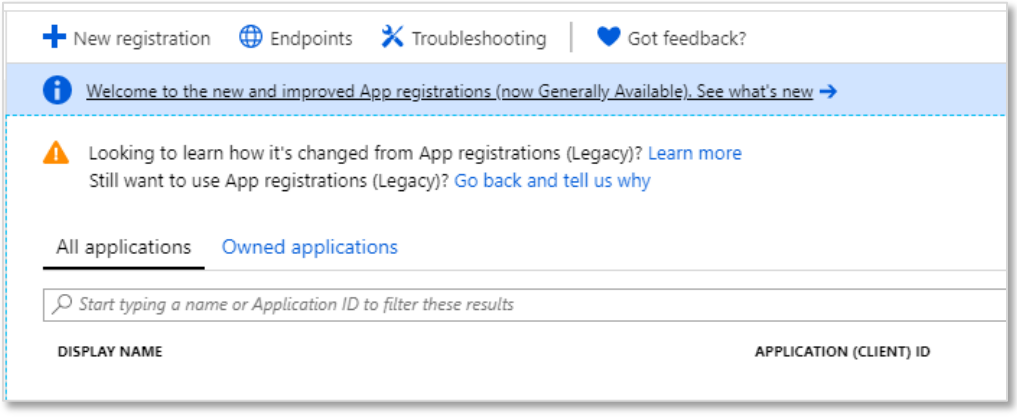


Figure 4: Create New Application Registration

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

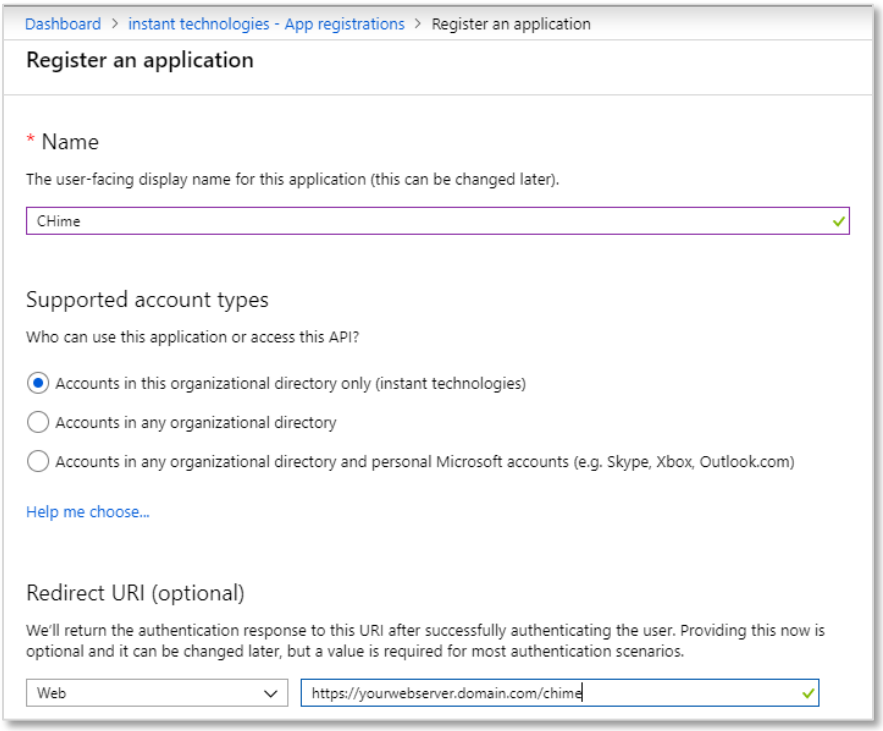


Figure 5: Create the Chime Web App / API

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.

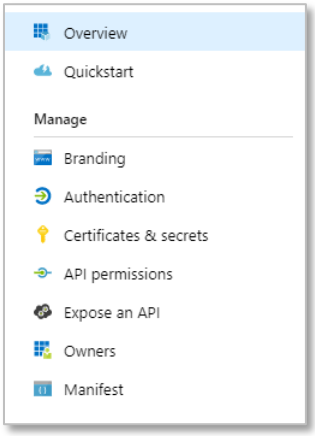
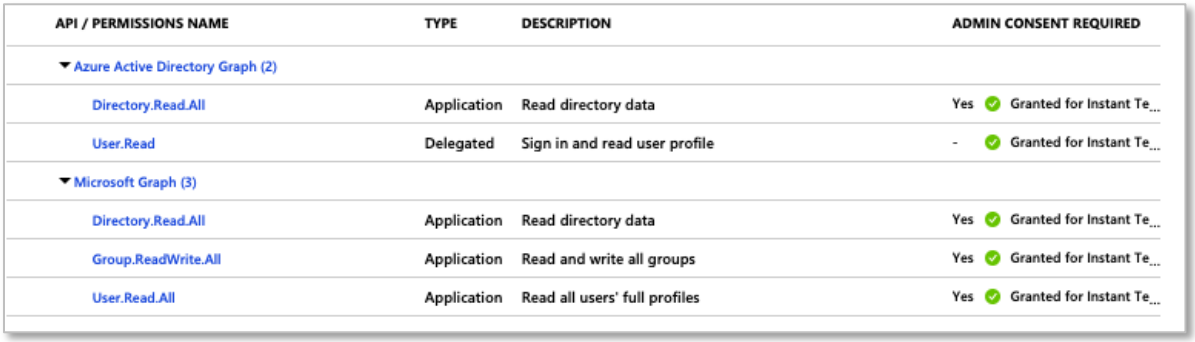


Figure 6: Access Required API Permissions

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 Granted for Instant Te...
User.Read	Delegated	Sign in and read user profile	- Granted for Instant Te...
Microsoft Graph (3)			
Directory.Read.All	Application	Read directory data	Yes Granted for Instant Te...
Group.ReadWrite.All	Application	Read and write all groups	Yes Granted for Instant Te...
User.Read.All	Application	Read all users' full profiles	Yes Granted for Instant Te...

Figure 7: Manage Required Permissions

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

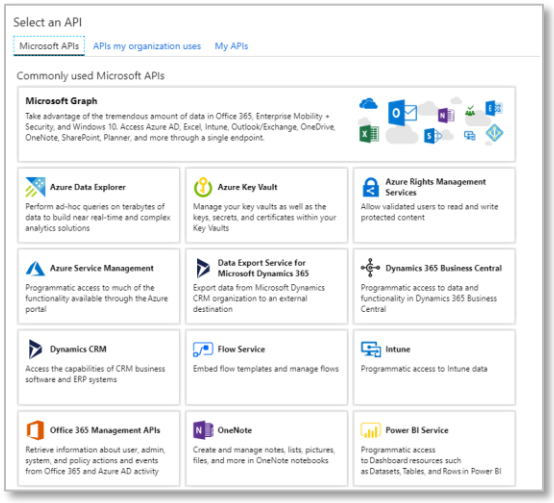


Figure 8: Configure Required Permissions

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.

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.

Figure 10: Select Permissions for Delegated Permissions

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

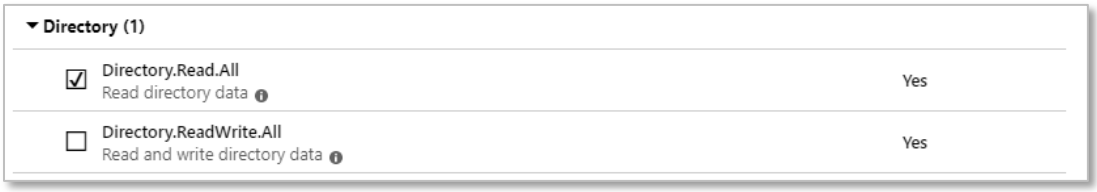


Figure 11: Select Permissions for Application Permissions

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

CREATE A NEW API KEY

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

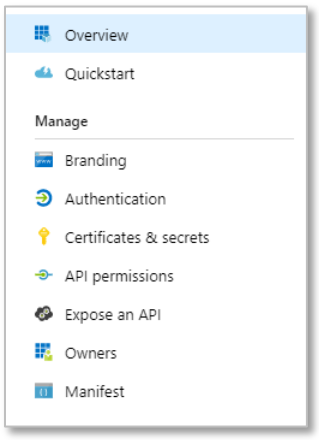


Figure 12: Access Certificates & Secrets

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.

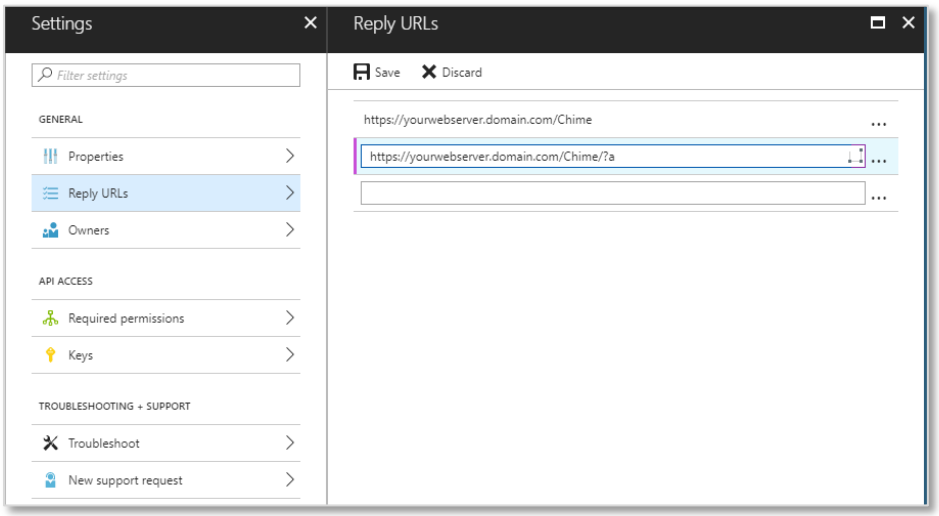


Figure 14: Configure Reply URLs

7. There should be 1 reply URL saved in there already, it will look something like this: https://[yourwebserver].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://[yourwebserver].domain.com/chime/?a
9. Click the **Save** button.
10. Close the Reply URLs blade.

GET SSL CERTIFICATE FOR APACHE TOMCAT (JAVA) SERVER

To set up Chime, you will need to acquire SSL certificate for Apache Tomcat (Java) server. This certificate will be installed in Apache Tomcat (Java) server running Chime application. Without this certificate installed, no users will be able to authenticate into the web app using Azure OAuth and Microsoft Teams won't be able to connect with Chime.

ENABLE MICROSOFT OFFICE 365 TO ACCESS CHIME OVER PORT 443

Chime instance should be accessible to Microsoft Azure services. Microsoft Azure requires access to send across IM events and messages in real time to Chime instance.

CREATING BOTS FOR CHIME QUEUE 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 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

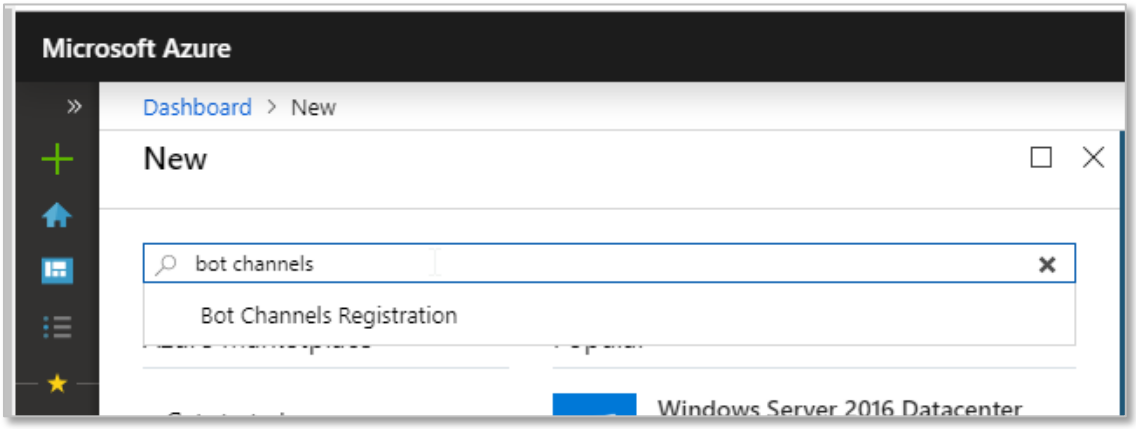


Figure 15: Navigate to Bot Channels Registration

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.
3. Click **Create** to start creating the resource.

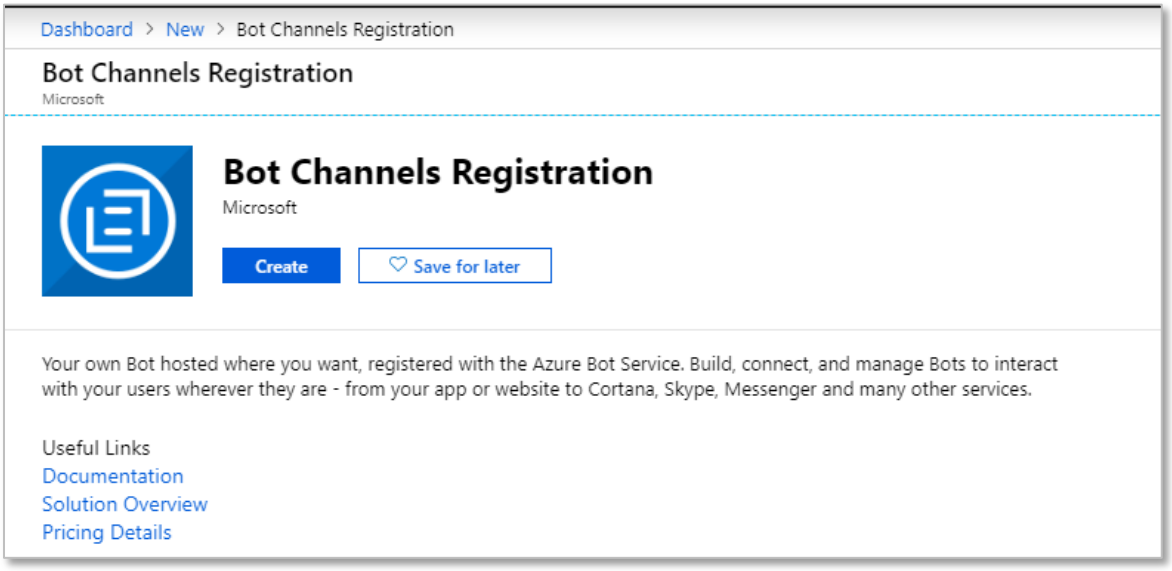


Figure 16: Create Bot Channels Registration

4. You should see a configuration page to create the Bot Channel Registration. Fill out the following fields:

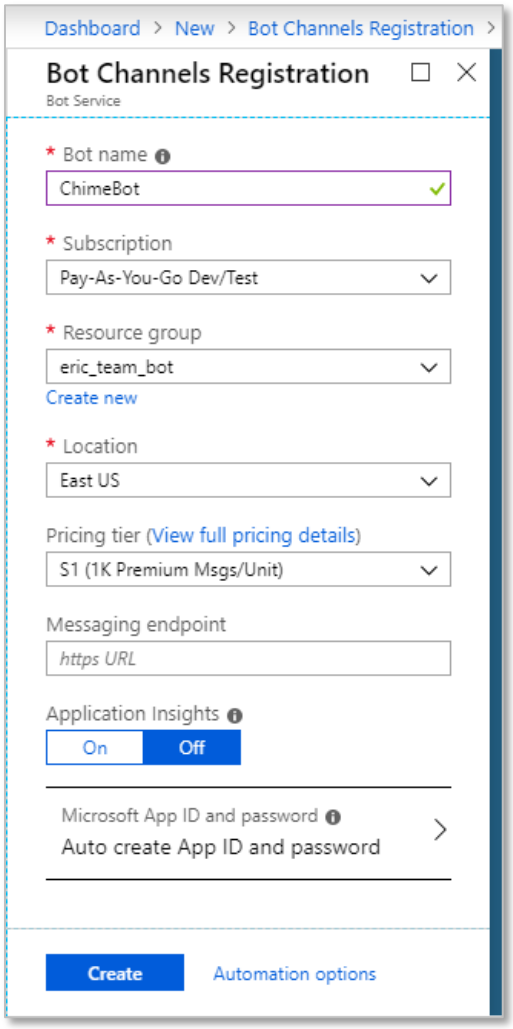


Figure 17: Bot Channels Registration Fields

Bot name: 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
Subscription: Select an Azure subscription to tie this bot registration to.
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.
Location: Select the most appropriate Azure datacenter location for your users.
Pricing Tier:
a. If users will be primarily contacting Chime through the Teams client, then the F0 tier may be the most cost-effective and appropriate level
b. If users will be primarily using the web client to contact Chime, then select the S1 tier.
Messaging endpoint: Enter Chime instance HTTPS URL: https://[yourwebserver].domain.com/ITFramework/api/messages This value will remain same for all Chime Bot Ids
Application Insights: Off
Microsoft App ID and password: Leave this as “Auto create App ID and password”

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
   Click the Teams icon to enable the bot for Microsoft Teams

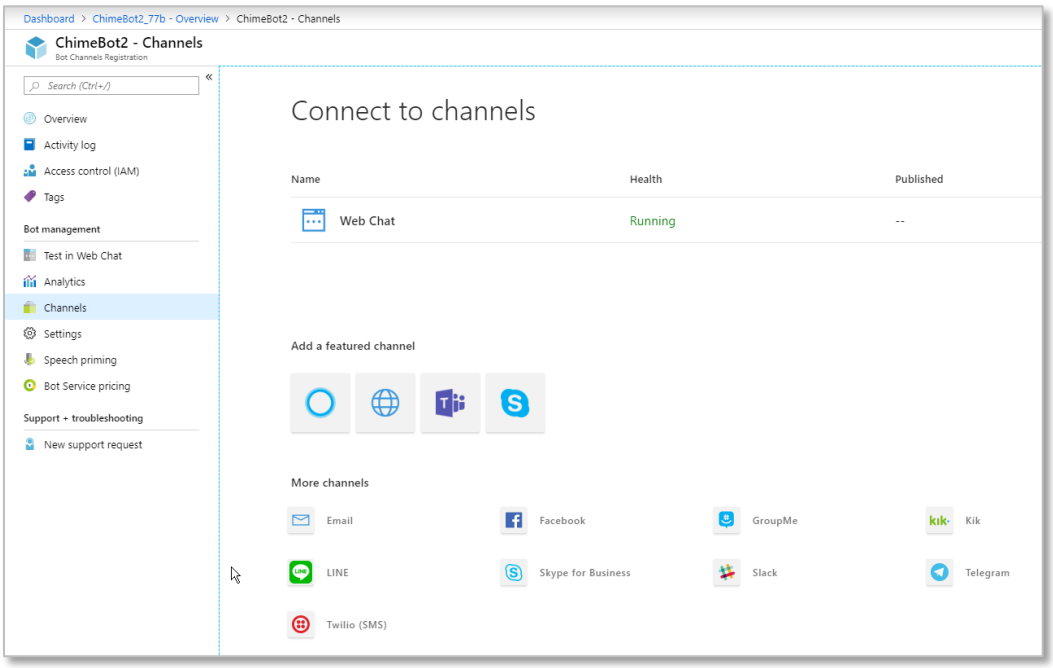


Figure 18: Add Teams to Channels Tab

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

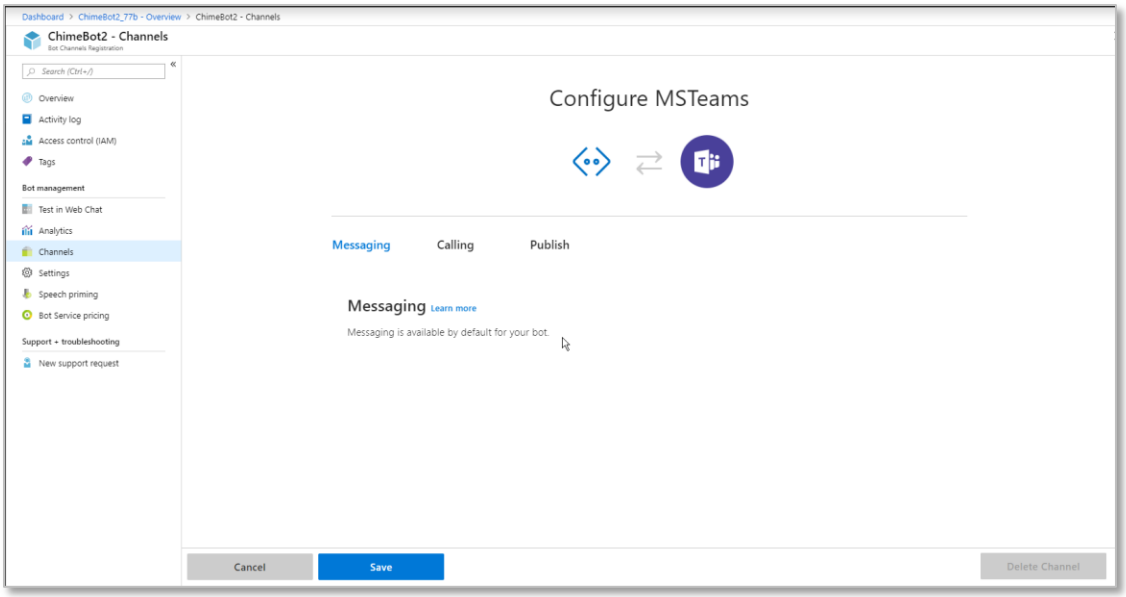


Figure 19: Save Configuration

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

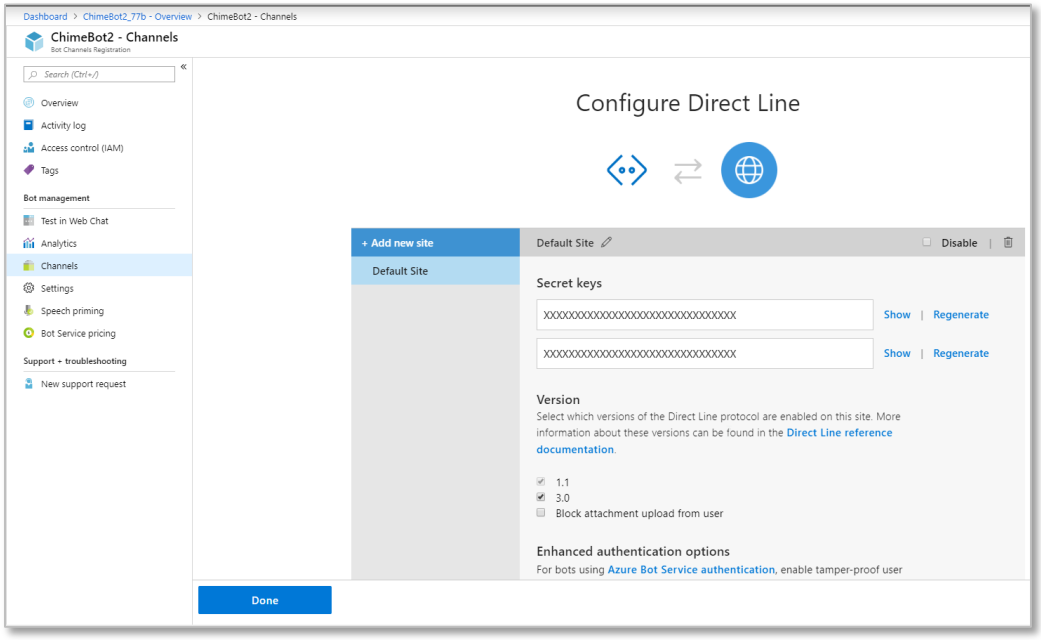


Figure 20: Configure Direct Line

9. 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.
10. Next navigate to the Settings tab on the bot registration.

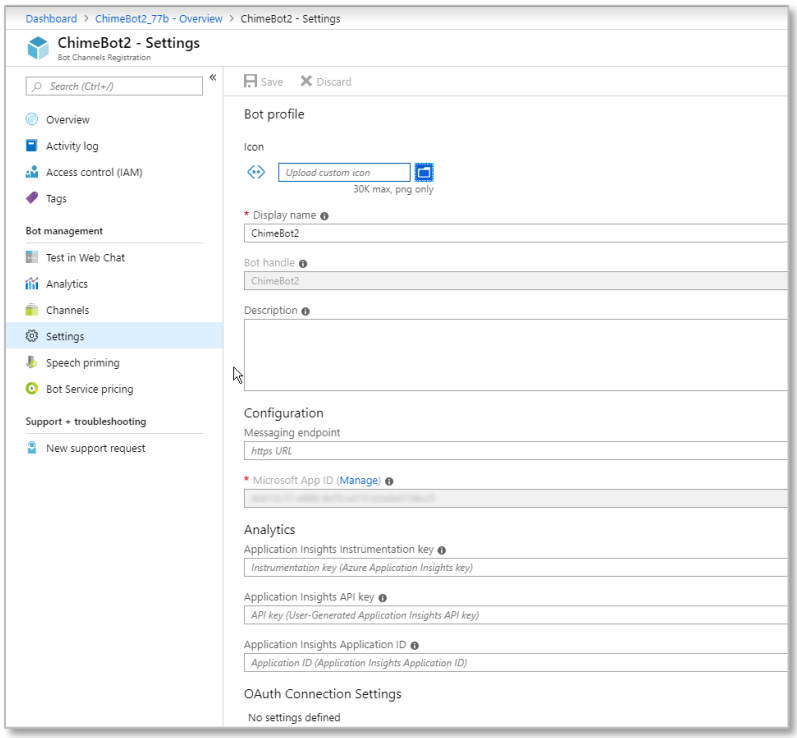


Figure 21: Settings Tab

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.

11. 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.

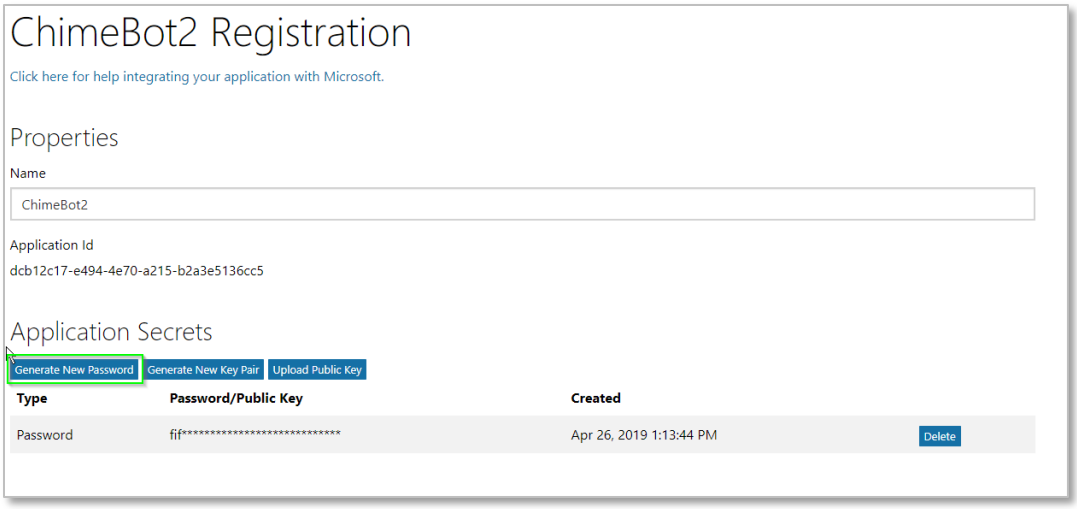


Figure 22: Generate New Password

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 record the password value that is generated – it will be necessary to configure the bot in Chime.

12. 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 -> Bots & Dispatchers**, and click the New Dispatcher button.

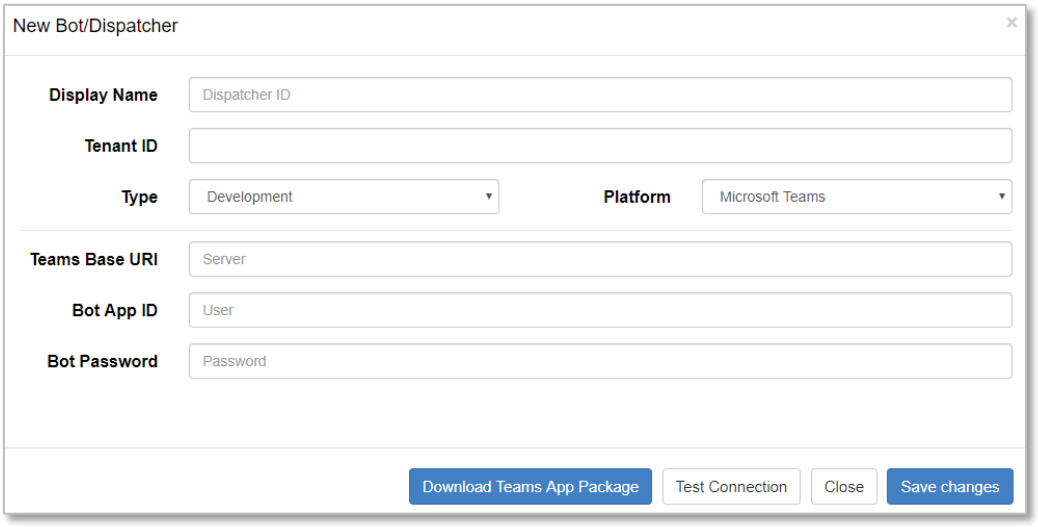


Figure 23: Setup Bot as Dispatcher in Chime

For Teams Base URI enter value as: https://smba.trafficmanager.net/amer/
After specifying values you should be able to verify and then save the new dispatcher.

AZURE ACTIVE DIRECTORY ACCOUNTS LIST

After following the steps in this guide, we should have the following details:

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 4 (Directory ID)

Azure AD Client ID: _____

This value is from Page 5 (Application ID)

Azure AD Client Secret Key: _____

This value is from Page 8