



Chime for Teams Azure and Office 365 Prerequisites for Hosted Environments

May 2022

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 - 2022 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
Adding a Dispatcher	13
Creating a Dispatcher Resource.....	13
Adding the Dispatcher into Chime.....	18

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.

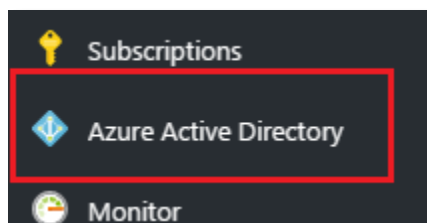


Figure 1: Begin Setting up Active Directory

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**

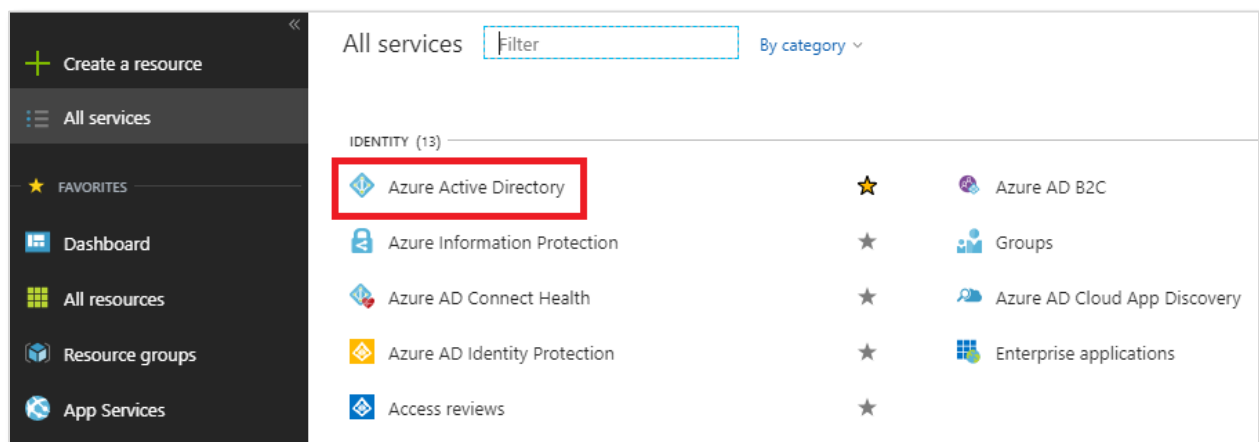

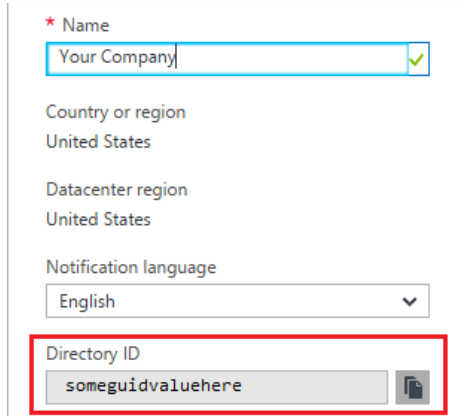


Figure 2: Secondary Option to Active Directory Setup

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.

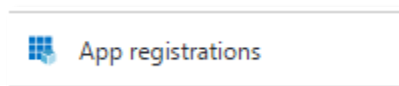


The screenshot shows the 'Properties' blade for an Azure Active Directory tenant. The 'Name' field contains 'Your Company'. The 'Country or region' and 'Datacenter region' are both set to 'United States'. The 'Notification language' is set to 'English'. The 'Directory ID' field, located at the bottom, 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.

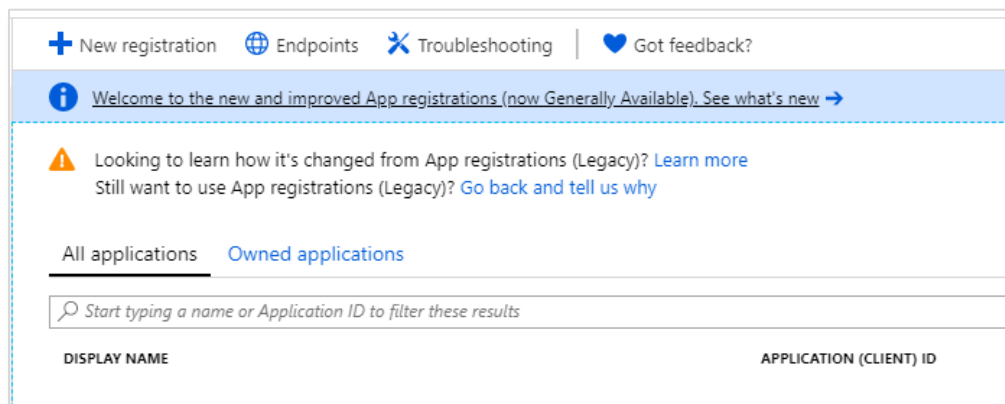
Figure 3: Copy Directory ID

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 interface. At the top, there are links for 'New registration', 'Endpoints', 'Troubleshooting', and 'Got feedback?'. Below these is a welcome message: 'Welcome to the new and improved App registrations (now Generally Available). See what's new →'. A warning message follows: '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'. Below the messages are two tabs: 'All applications' and 'Owned applications'. A search bar is present with the placeholder text 'Start typing a name or Application ID to filter these results'. At the bottom, there is a table with 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 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.

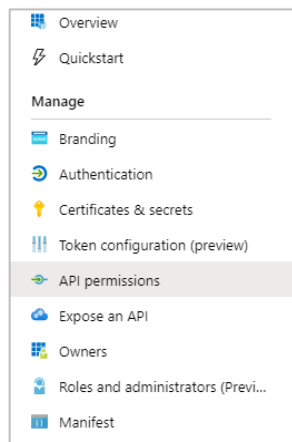


Figure 6: Access Required API Permissions

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

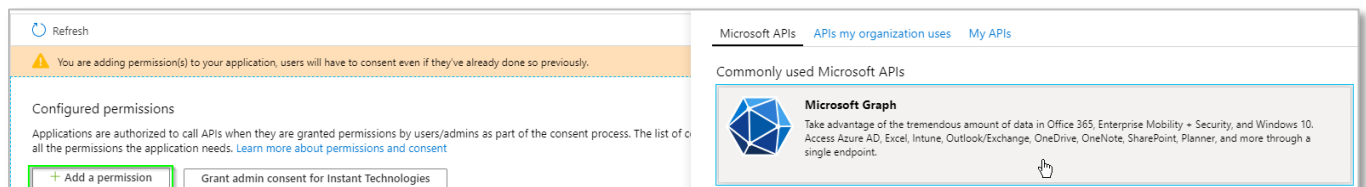


Figure 7: Manage Required Permissions

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

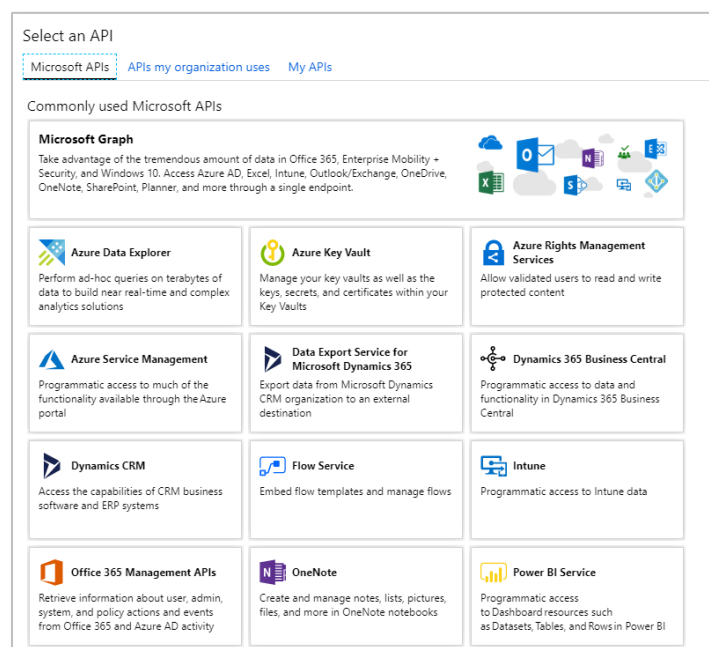


Figure 8: Configure Required Permissions

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

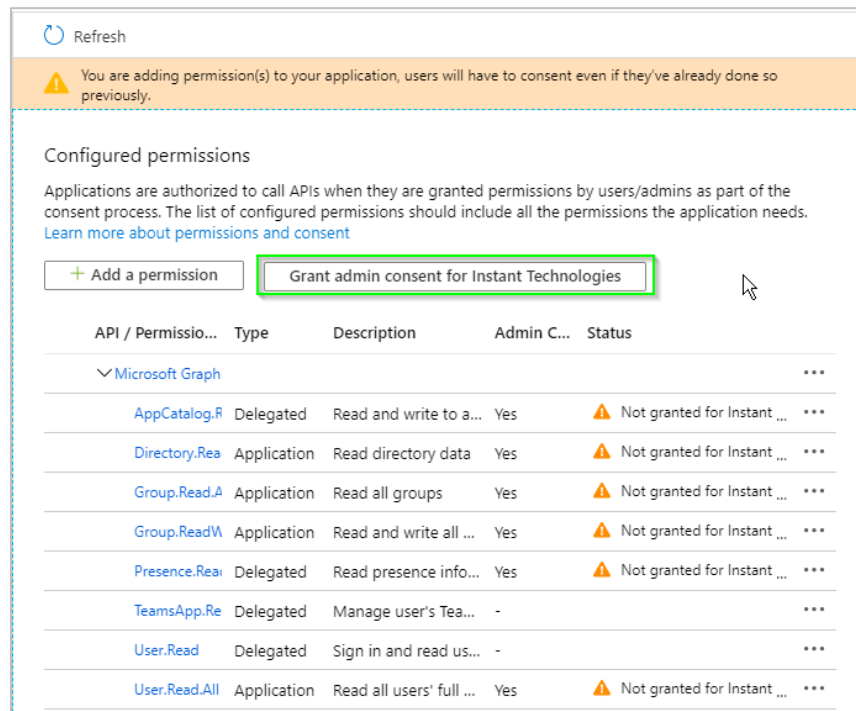


Figure 11: Grant Admin Consent

ADD REDIRECT URIS

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

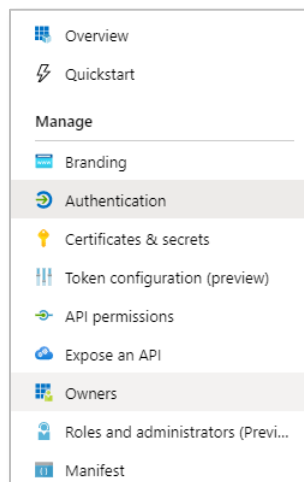


Figure 12: Configure Reply URLs

2. 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)

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred as reply URIs. [Learn more about redirect URIs and the restrictions](#)

[https://\[yourwebserver\].domain.com/chime/?a](https://[yourwebserver].domain.com/chime/?a)

[https://\[yourwebserver\].domain.com/chime](https://[yourwebserver].domain.com/chime)

[Add URI](#)

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://myapp.com/logout>

Implicit grant

Allows an application to request a token directly from the authorization endpoint. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens

☒ ID tokens

Figure 13: Configure Reply URLs

3. In the text box below, add in a URI with this format: [https://\[yourwebserver\].domain.com/chime/?a](https://[yourwebserver].domain.com/chime/?a)
4. 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.
5. 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.

ADDING A DISPATCHER

In order to create queues, route chats to agents, and send out alerts; Chime needs Azure Bot Resource created in Microsoft Azure that will be able to broker chats to agents and guests. Each queue you create needs a dispatcher and the Azure Bot will act as the dispatcher.

CREATING A DISPATCHER RESOURCE

To create a Dispatcher for Chime you will need permissions to create resources in your organization's Microsoft Azure Subscription.

1. Navigate to the Azure Portal, at <https://portal.azure.com>

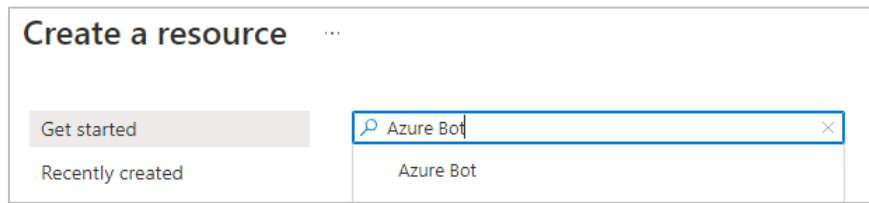


Figure 14: Searching for Azure Bot

2. Click the "Create Resource" button in the side bar. Enter "Azure Bot" in the search bar and select the matching option from the list.
3. Click **Create** to start creating the resource.

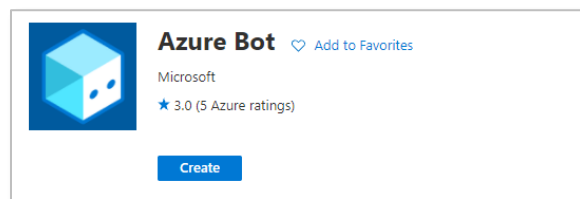


Figure 15: Create Azure Bot Resource

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

Create an Azure Bot ...

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Bot handle * ⓘ Support-Dispatcher ✓

Subscription * ⓘ Pay-As-You-Go Dev/Test ✓

Resource group * ⓘ (New) Chime-Test-RG ✓
[Create new](#)

New resource group location ⓘ East US ✓

Pricing

Select a pricing tier for your Azure Bot resource. You can change your selection later in the Azure portal's resource management. Learn more about available options, or request a pricing quote, by visiting the [Azure Bot Services pricing](#)

Pricing tier * Free
[Change plan](#)

Microsoft App ID

A Microsoft AppID is required to create an Azure Bot resource. An App ID can be automatically created below, or you can manually create your own, then return here to input your new App ID and password.
[Manually create App ID](#)

The app secret will be stored in Azure Key Vault in the same resource group as your Azure bot. [Learn more](#)

Microsoft App ID ☒ Create new Microsoft App ID
☐ Use existing app registration

Figure 16: Create Azure Bot - Basics

- Bot handle:** 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:**
- If users will be primarily contacting Chime through the Teams client, then the F0 tier may be the most cost-effective and appropriate level
 - If users will be primarily using the web client to contact Chime, then select the S1 tier.
- Microsoft App ID:** “Create new Microsoft App ID”
5. When this is completed, click “Review + create” then 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

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.
12. 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.

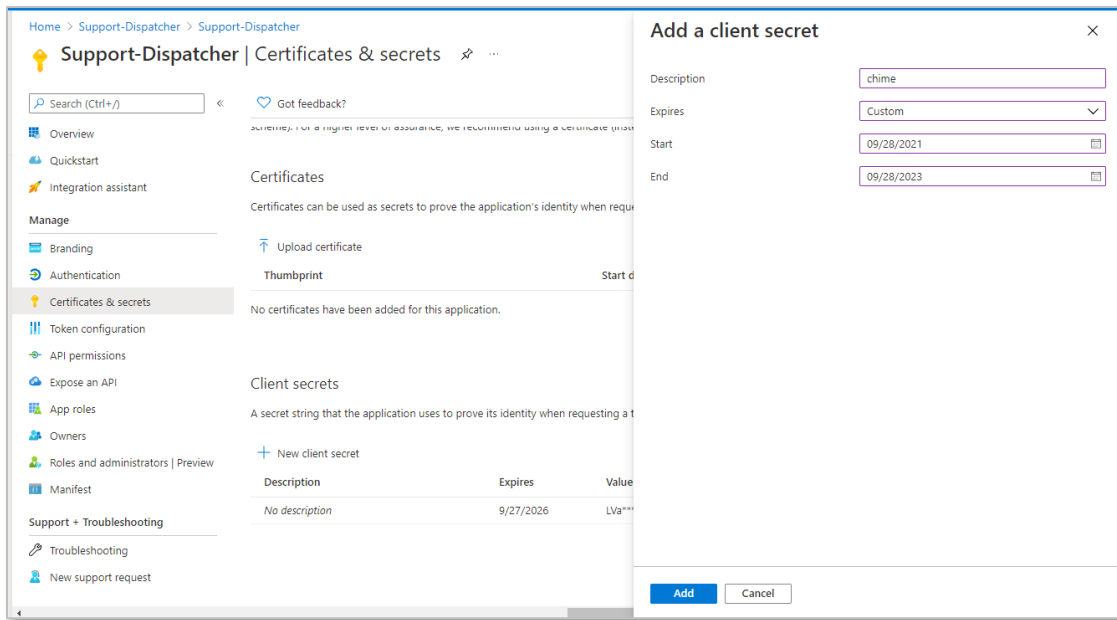


Figure 21: Add Client Secret

13. Click the “New client secret” button.
14. Add a description (*example*: “chime”) and set 2 years expiration date (max).
15. Record the Client Secret value that is generated – it will be necessary to configure the bot in Chime.
16. With the **Bot Handle**, **Microsoft App ID**, **Client Secret**, and **Direct Line secret**, it is possible to setup the bot as a dispatcher in Chime.

Note: often time’s users will want to have multiple bots added to a Queue so that each Agent can take multiple chats at the same time. If you would like to do this, repeat the “Creating A Dispatcher Resource” steps for however many concurrent chats you want Agents to be able to take at once.

ADDING THE DISPATCHER INTO CHIME

Once you have created the dispatcher, you will want to add it into your Chime instance. Follow these next steps to add the Dispatcher in Chime and how to configure the messaging endpoint in the bot.

1. 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.

The screenshot shows the 'New Dispatcher' form in the Chime interface. The form is titled 'New Dispatcher' and has a search bar for 'Search Active Directory'. Below the title, there is a note: 'The dispatcher account is the entry point for a queue. Users can contact this account to connect with agents. This account must be unique.' The form is divided into two main sections: 'Account Settings' and 'Chime Settings'. The 'Account Settings' section includes fields for 'Bot ID', 'Webchat Secret', 'Bot Name', 'Bot Secret' (with a 'Show Password' checkbox), and 'Email Address'. The 'Chime Settings' section includes a 'Description' field, a 'Dispatcher Type' dropdown menu (set to 'Testing'), and a 'Queue' dropdown menu (set to 'Not assigned'). At the bottom right, there are buttons for 'Cancel', 'Verify Settings', and 'Save'.

Figure 22: Add New Dispatcher in Chime

3. 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
4. Once this is completed, you should be able to verify and then save the new dispatcher.
5. 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:

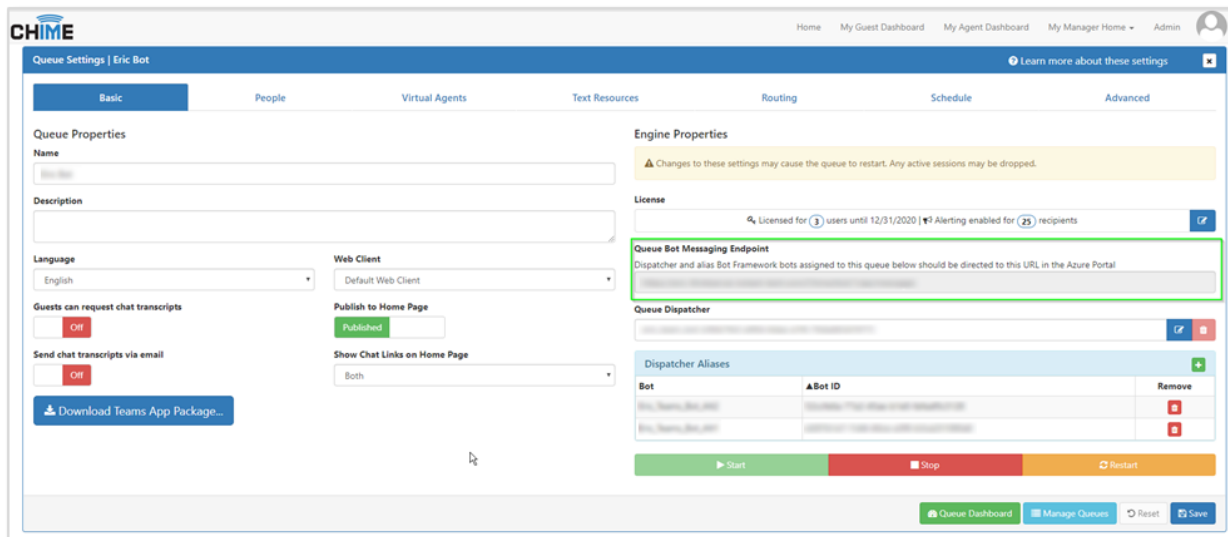


Figure 23: Chime Queue Settings

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

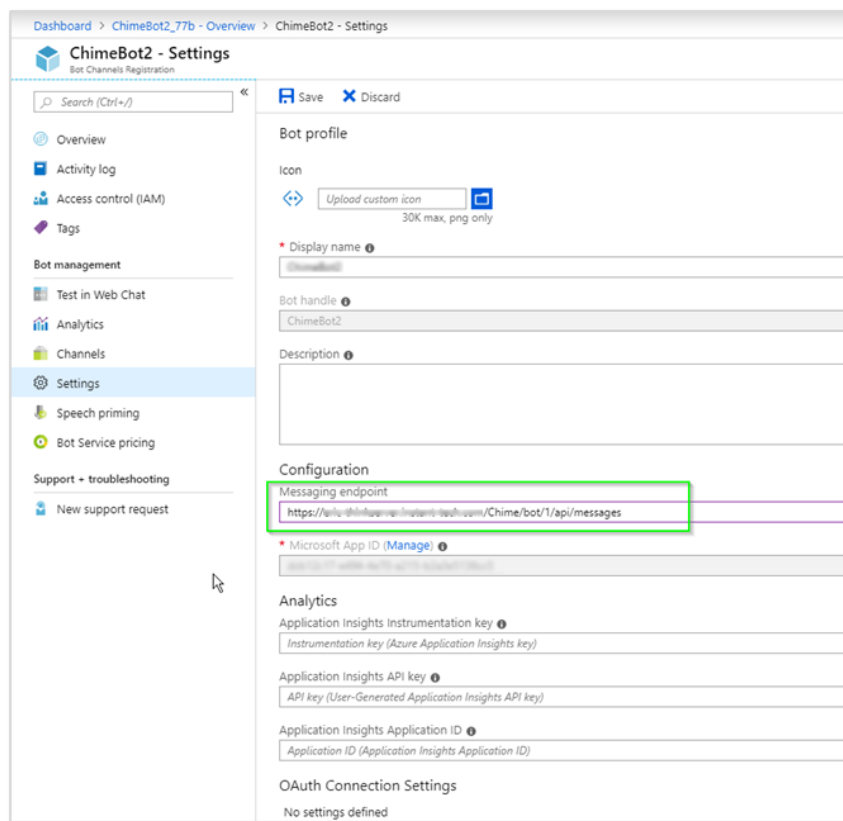


Figure 24: Settings - Configuration