



Chime for Teams Installation Azure and Office 365 Prerequisites and Overview

March 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
Setup Before Chime Install	5
Hostname and Firewalls	5
SSL Certificate	5
Configuring Azure AD Authentication for Chime For Teams	6
Prerequisites	6
Configure Active Directory Authentication	7
Retrieve your Azure Tenant ID	7
Create Application	7
Register the Chime Application	8
Configure the Application	8
Configure Application Permissions	9
Configuring Certificates and Secrets	12
Add Redirect URIs	17
Azure Active Directory Accounts List	18
Setup After Chime Install	19
Install Wizard	19
Creating Bots for Chime Dispatchers	20
Creating a Bot Registration in Azure	21

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 2 general scenarios:

In the first scenario, your organization intends to install Chime in 'self-hosted', or 'on-premise' mode and your organization will install, configure, and manage your Chime server. In this scenario, prior to installing the Chime server, you should pay close attention to the sections in this document related to Hostname, Firewalls, and creating the necessary SSL certificate on the Chime server. After reviewing the core areas related to the machine hosting, public IP, and certificate resourcing you should review the areas related to Azure AD, O365 permissions, and Bot Framework configurations.

In the second scenario, 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

SETUP BEFORE CHIME INSTALL

HOSTNAME AND FIREWALLS

The Chime server will need to have a publicly addressable DNS hostname and public IP address in order for Microsoft Bot Framework to be able to deliver Teams chat messages to the Chime server.

Additionally, it will be necessary to allow incoming traffic on port 443 (HTTPS).

It is not currently possible to provide specific IP address ranges that would need to be whitelisted for incoming requests for Bot Framework requests, as Microsoft does not make that information available and it may change at any time.

More information on Microsoft Bot Framework is available across various Microsoft sites related to Microsoft Bot Framework.

SSL CERTIFICATE

To set up a Chime for Teams deployment, you will need to acquire a SSL certificate. This certificate will be installed on the same server that the Chime instance will be deployed on.

Without this certificate installed, no users will be able to authenticate into the web app. Self-signed certificates won't work, Certificates should be from a valid SSL issuing authority like: GoDaddy, Thawte, Symantec etc...

The certificate must have a **Subject** and **Subject Alternate Name** which matches the public hostname of the Chime application server, as will be configured for the Reply URL in the Azure AD Application Registration in Azure.

It is recommended that a **Signature algorithm** of at least **sha256RSA**.

The certificate should have an **Enhanced Key Usage** property of **Server Authentication (1.3.6.1.5.5.7.3.1)**

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.

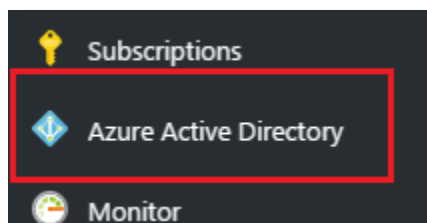


Figure 1: Begin Setting up Active Directory

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**

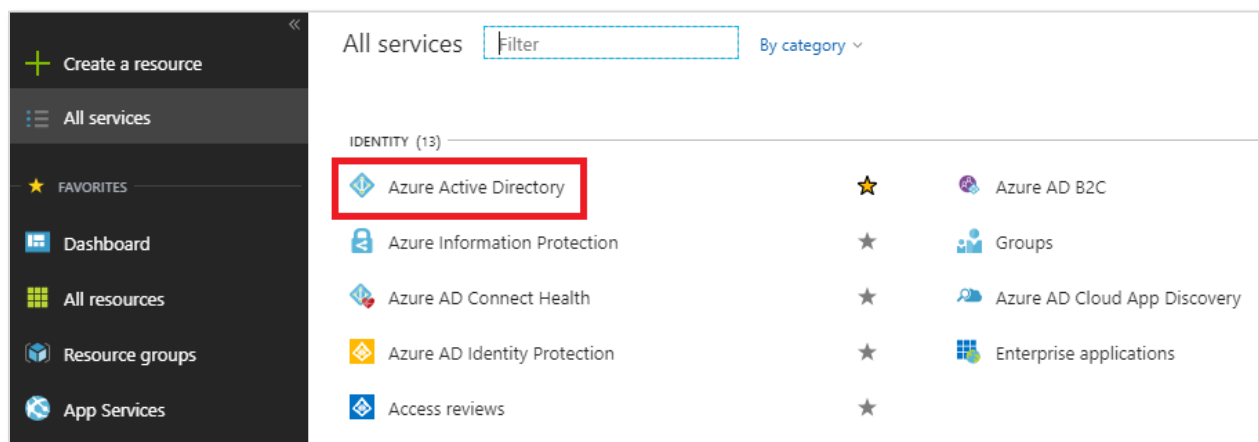

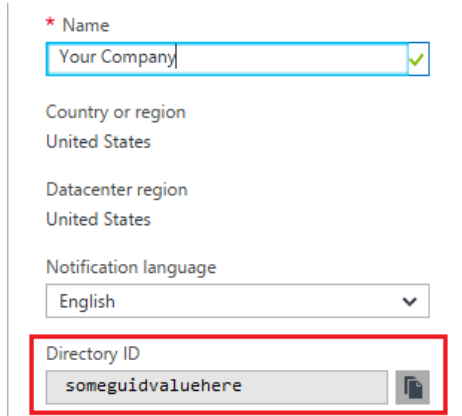


Figure 2: Secondary Option to Active Directory Setup

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

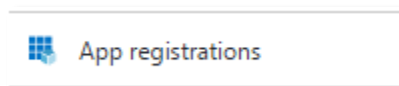
Notification language
English ▼

Directory ID
someguidvaluehere

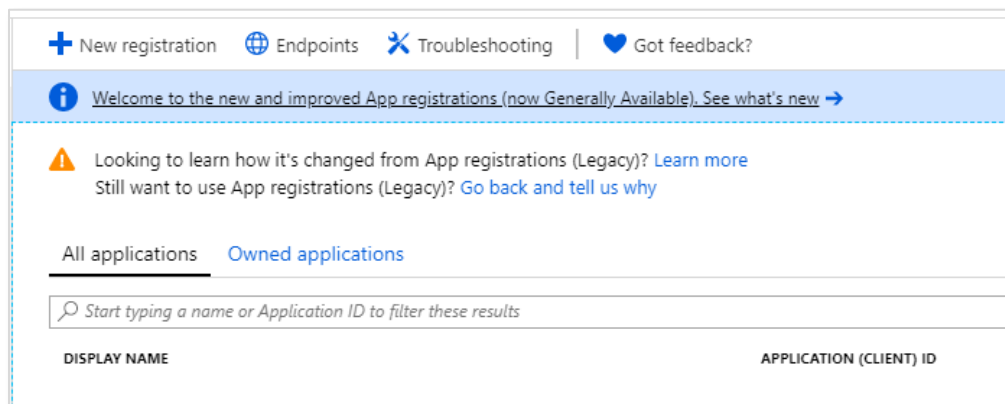
Figure 3: Copy Directory ID

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 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

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.

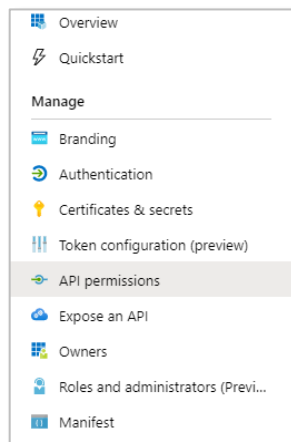


Figure 6: Access Required API Permissions

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

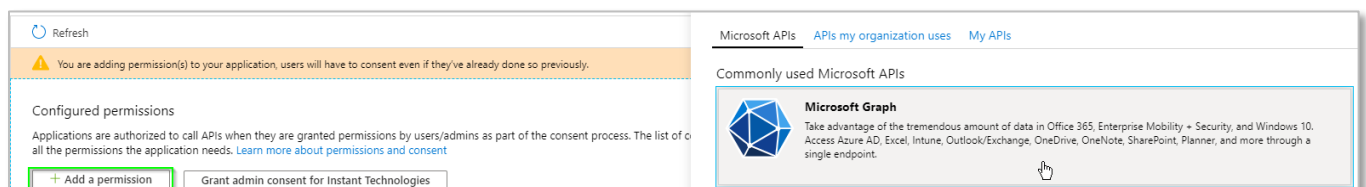


Figure 7: Manage Required Permissions

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

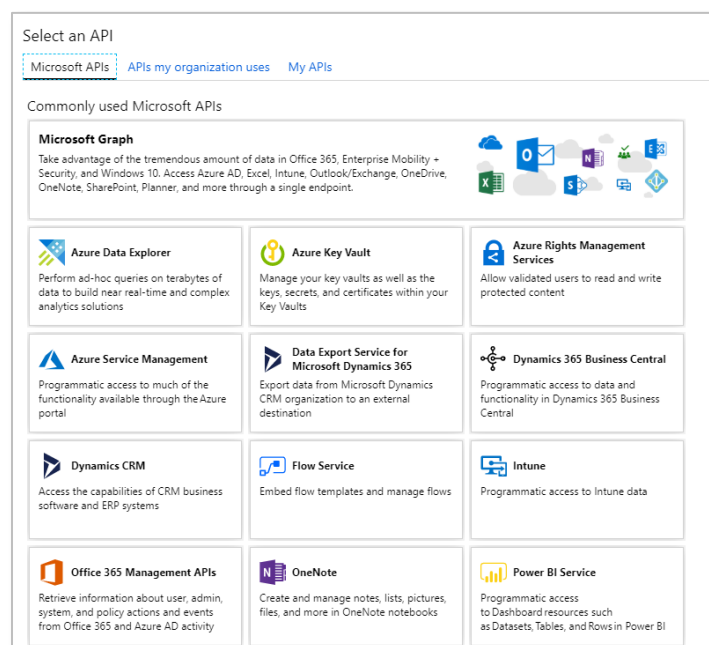


Figure 8: Configure Required Permissions

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.

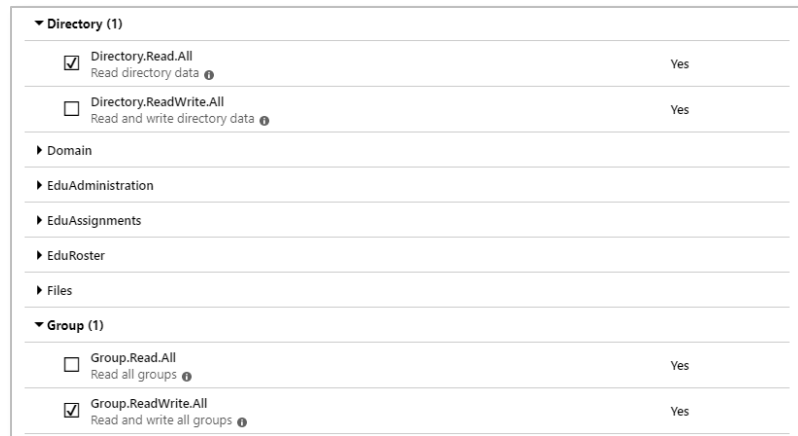


Figure 9: Select Permissions for Graph Api

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



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

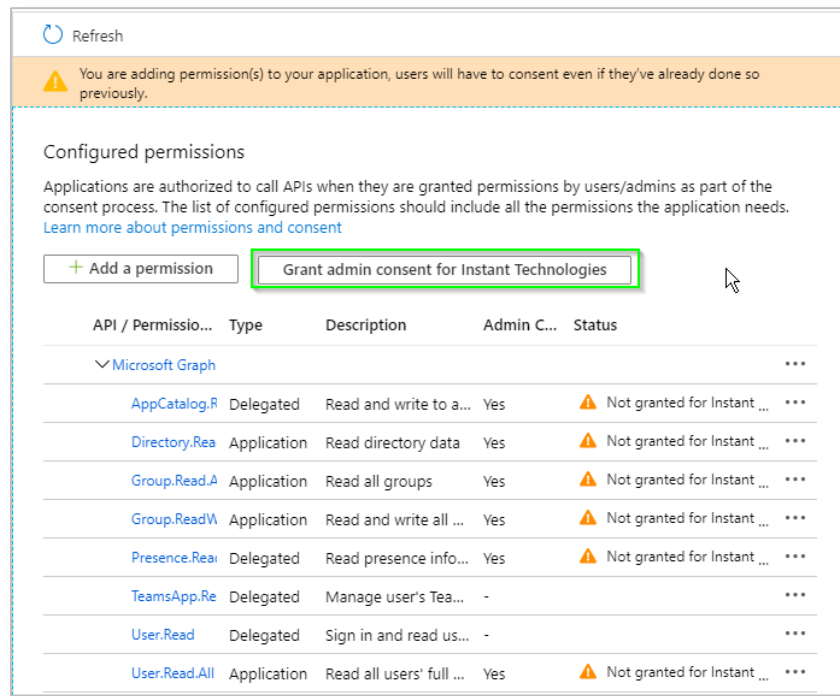


Figure 11: Grant Admin Consent

CONFIGURING CERTIFICATES AND SECRETS

Chime for Teams can either use a client secret password or a client certificate to access Azure AD and Graph API resources.

CREATING A CLIENT SECRET

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

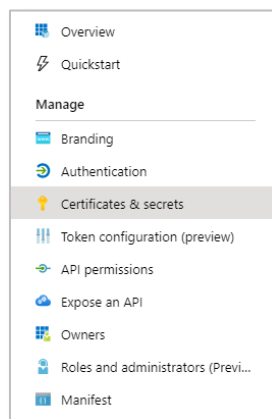


Figure 12: Access Certificates & Secrets

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

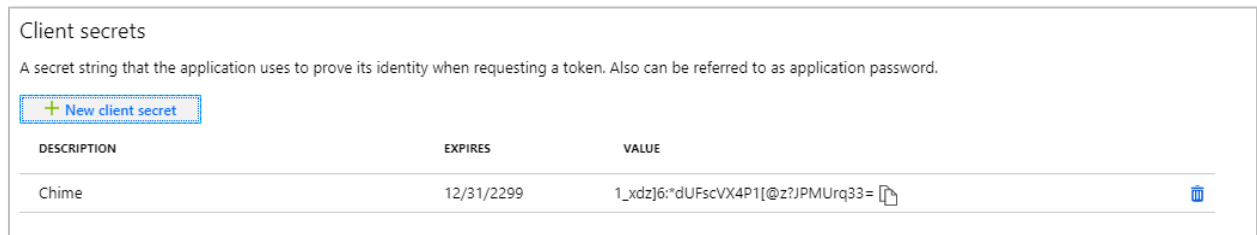


Figure 13: Setup API Key

CREATING A CLIENT CERTIFICATE

To use certificate-based authentication with Azure AD for Chime for Lync or Graph API for Chime for Teams, follow these steps:

A certificate will need to be created to authenticate the connection from the Chime server to Azure AD/Graph API.

- This must be a Client Authentication certificate.
- This certificate must be installed to the **Local Machine\Personal** certificate store on the Chime server.
- The Chime service account (which is the service account which the Chime Windows Service runs as) must have access to the Private Key of the certificate.
- There is no particular requirement for the Subject of the certificate, but it is recommended to use the public hostname of the Chime server.
- The KeySpec of the certificate should be KeyExchange.

Any certificate that meets these parameters should be acceptable, whether obtained from a Certificate Authority or created as a self-signed certificate.

1. Create or obtain the certificate
2. We provide a PowerShell script to create such a script, CreateAzureADCert.ps1, which is reproduced below:

```
# Script to create a self-signed certificate to use as a client certificate when
# accessing Azure AD/Graph API
#
# Should support Server 2012+ Powershell
# Run this script as an administrator
param (
    [string]$dnsName = $(Read-Host "Enter the DnsName of the machine"),
    [string]$password = $(Read-Host "Enter a password for the private key"),
    [string]$folderPath = $(Read-Host "Enter the folder path where the certificates
should be exported"),
    [string]$fileName = $(Read-Host "Enter a filename (without extension) for the
generated certificates")
)

$certStoreLocation = "cert:\LocalMachine\My" # Chime will require this certificate to
be in the LocalMachine/Personal store

$certificate = New-SelfSignedCertificate -DnsName "$dnsName" -CertStoreLocation
"$certStoreLocation" -KeySpec KeyExchange

$certificatePath = $certStoreLocation + '\ ' + $certificate.Thumbprint
$filePath = $folderPath + '\ ' + $fileName
$securePassword = ConvertTo-SecureString -String $password -Force -AsPlainText
Export-Certificate -Cert $certificatePath -FilePath ($filePath + '.cer')
Export-PfxCertificate -Cert $certificatePath -FilePath ($filePath + '.pfx') -Password
$securePassword
```

This script will ask for the required parameters, and generate a .pfx/.cer public/private key pair for the certificate. The certificate will be installed in the **LocalMachine\Personal** certificate store of the machine that the script is run on.

Figure 14: Create Azure Cert

3. Next ensure that the Chime service account has access to the certificate.
 - a. The MMC Certificates snap-in for the Local Machine store can be opened by running **certlm.msc**
 - b. Expand the Personal\Certificates store in the left pane and find the certificate that has been generated for the client certificate

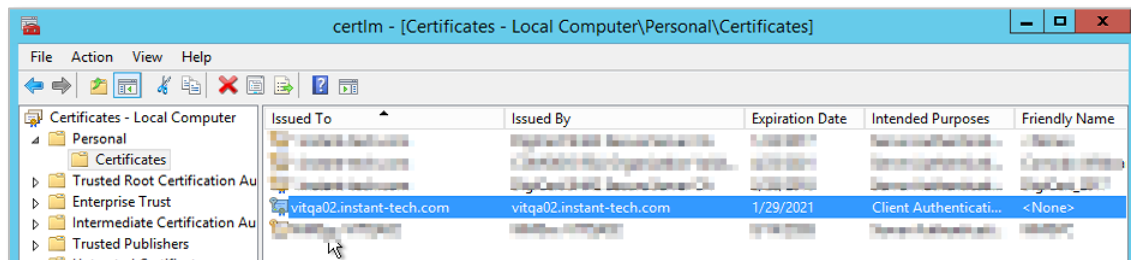


Figure 15: Chime Service Account

- c. Right-click the certificate to open the context menu, and select All Tasks -> Manage Private Keys

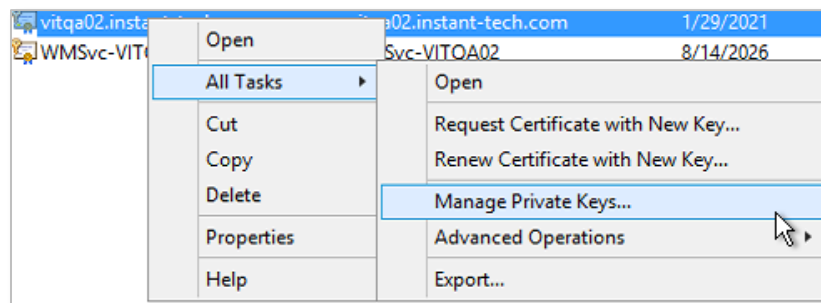


Figure 16: Manage Private Keys

- d. If the Chime service account is not shown as having access permissions, add that account.

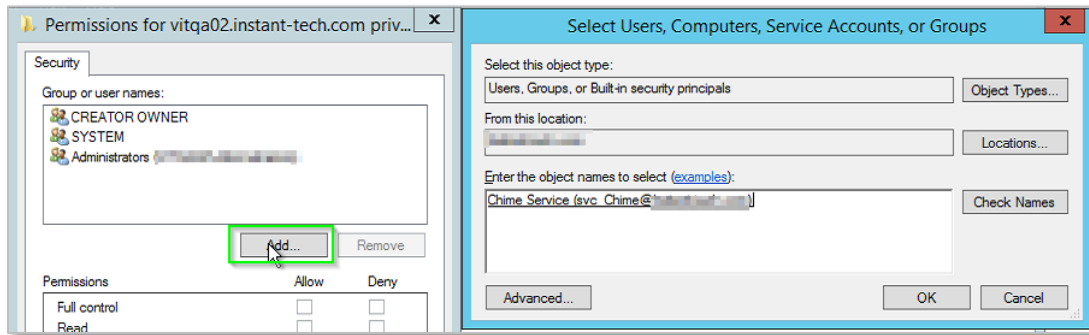


Figure 17: Add Account to Permissions

4. Next, it is necessary to upload the client certificate that has been created or installed on the Chime server to Azure AD as an access certificate.
- a. Go to the Azure portal at <https://portal.azure.com>, and then find the Azure AD App Registration that was previously created.

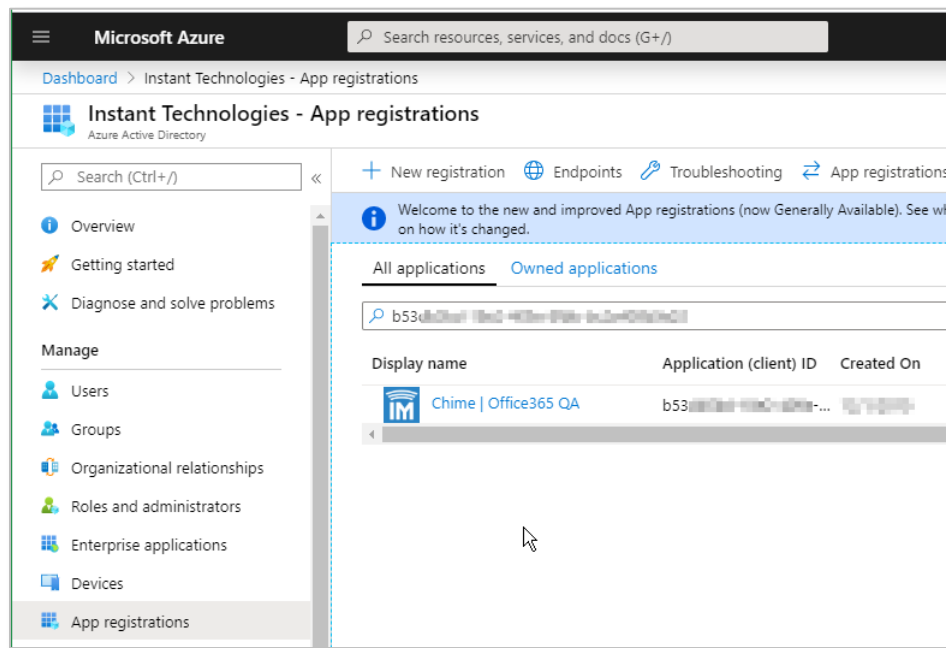


Figure 18: Navigate to App Registration

- b. Go to the Certificates and Secrets tab on the left. You should see a button to upload a client certificate.

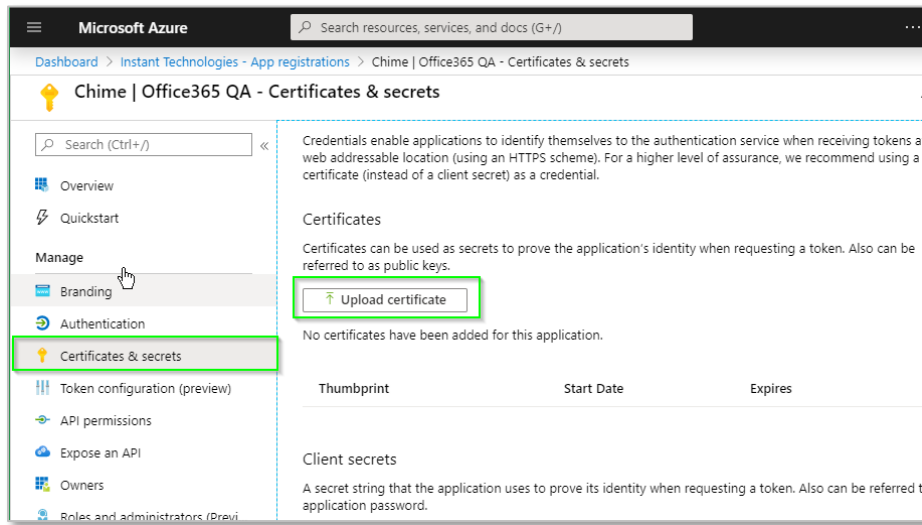


Figure 19: Upload Certificate

- c. Click the add certificate button, and then select the .cer file matching the certificate that was installed on the Chime server.
- d. After the certificate is added, verify that the Thumbprint shown in the Azure Portal UI matched the Thumbprint of the certificate installed on the Chime server.

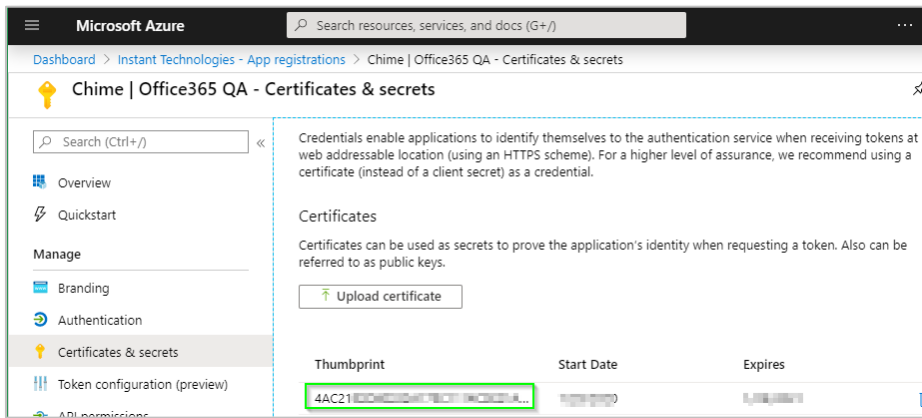


Figure 20: Verify Thumbprint

ADD REDIRECT URIS

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

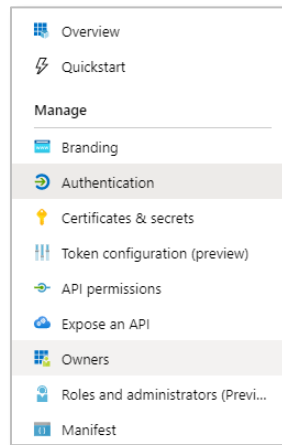


Figure 21: Configure Reply URLs

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)

A screenshot of a web configuration page titled 'Redirect URIs'. It contains a description of the field, a list of two existing URIs with delete icons, an 'Add URI' link, a 'Logout URL' section with a description and a text input field, and an 'Implicit grant' section with a description and two radio button options: 'Access tokens' and 'ID tokens' (which is selected).

Figure 22: 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.

AZURE ACTIVE DIRECTORY ACCOUNTS LIST

Figure 23: 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.

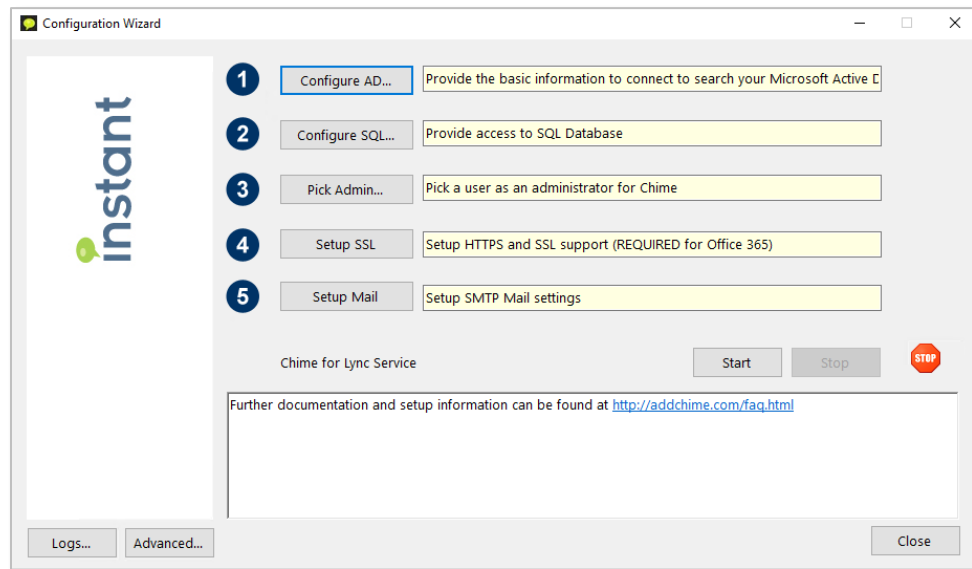


Figure 24: Configuration Wizard

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**.

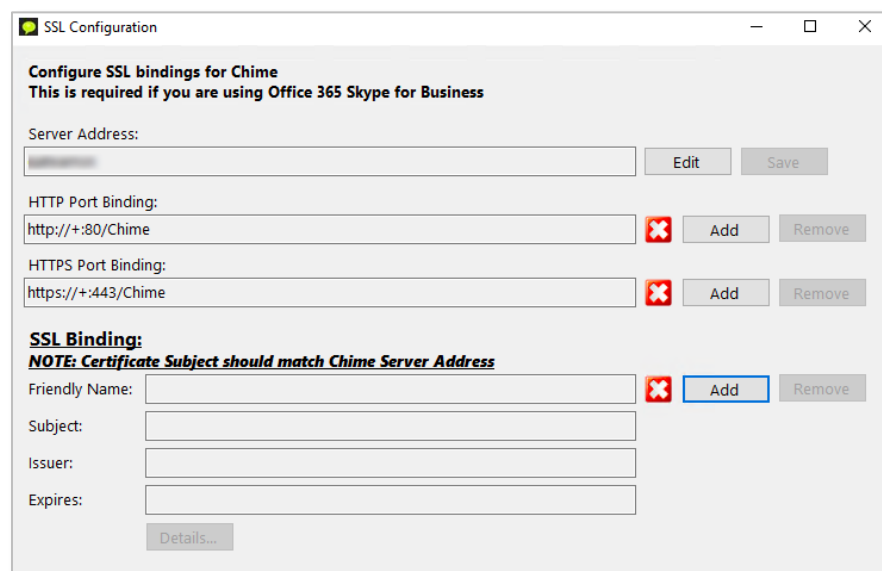


Figure 25: Setup SQL Connection

3. When the Select SSL Certificate window opens, select the certificate you set up earlier.

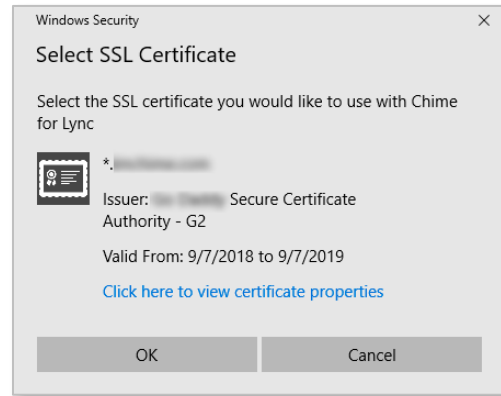


Figure 26: Select SSL Certificate

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.

Before you start here are the permissions this Teams bot will have

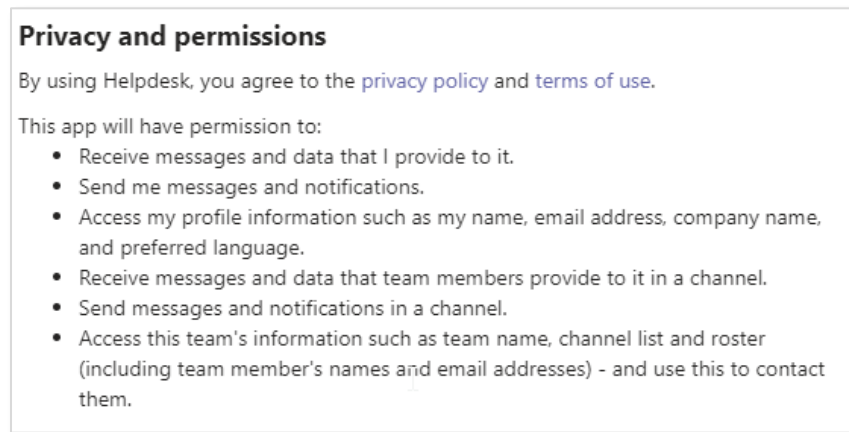


Figure 27: Teams Dispatcher Privacy and Permissions

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.

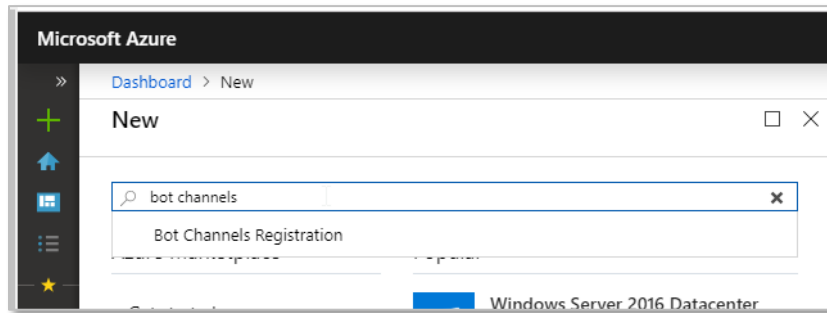


Figure 28: Search for Bot Channels Registration

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

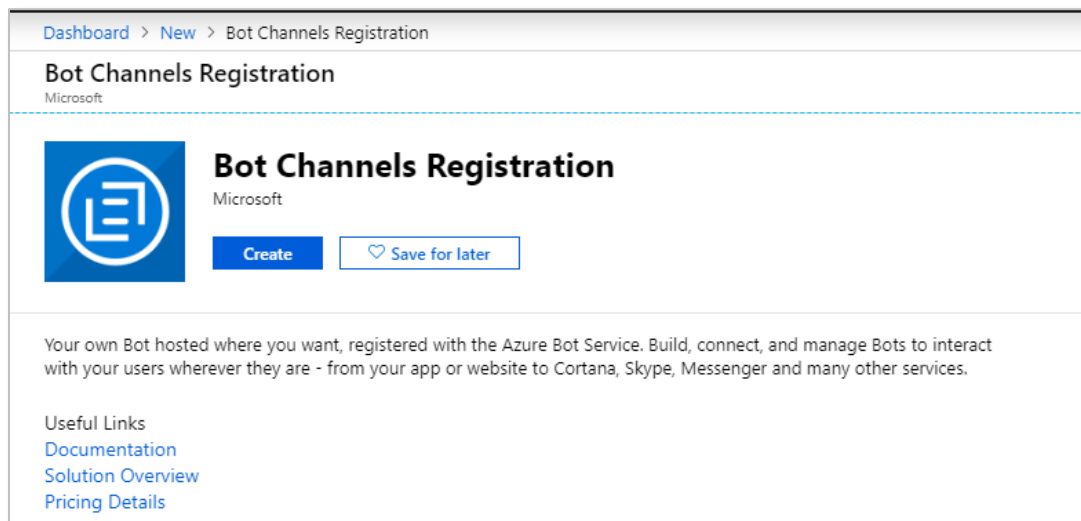


Figure 29: Create Bot Channels Registration

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
[Dropdown]

* Resource group
[Dropdown]
[Create new](#)

* Location
East US [Dropdown]

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

Messaging endpoint
https URL

Application Insights ⓘ
On Off

Microsoft App ID and password ⓘ
Auto create App ID and password >

[Create](#) [Automation options](#)

Figure 30: 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

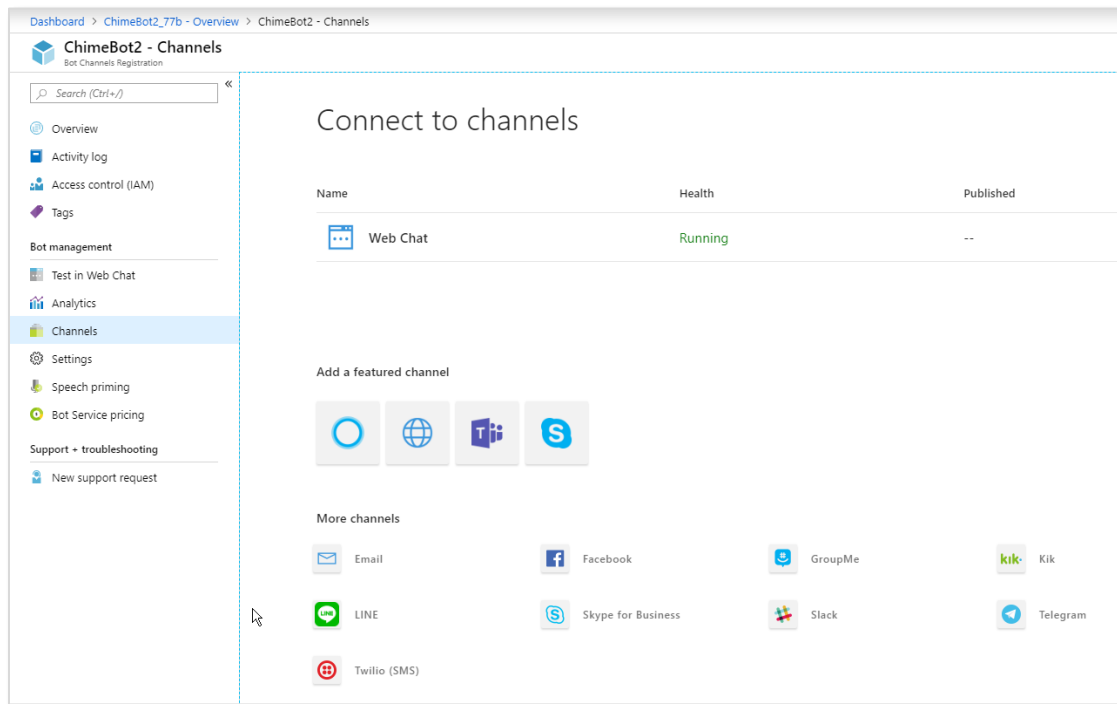


Figure 31: Click the Teams Icon

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

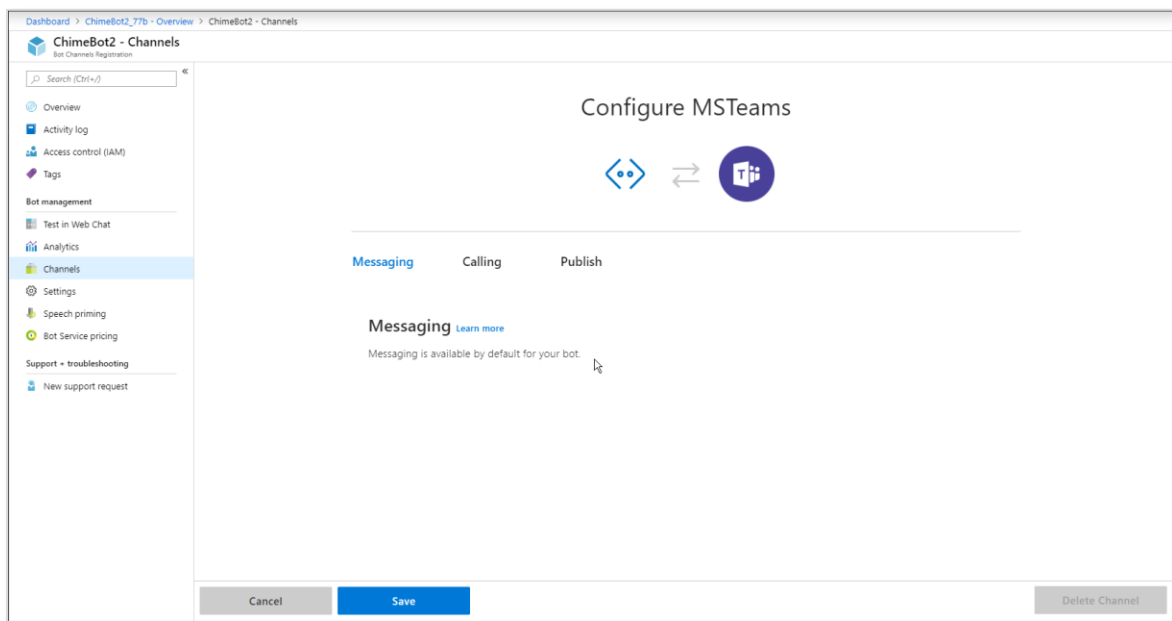


Figure 32: Configure MSTEams

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

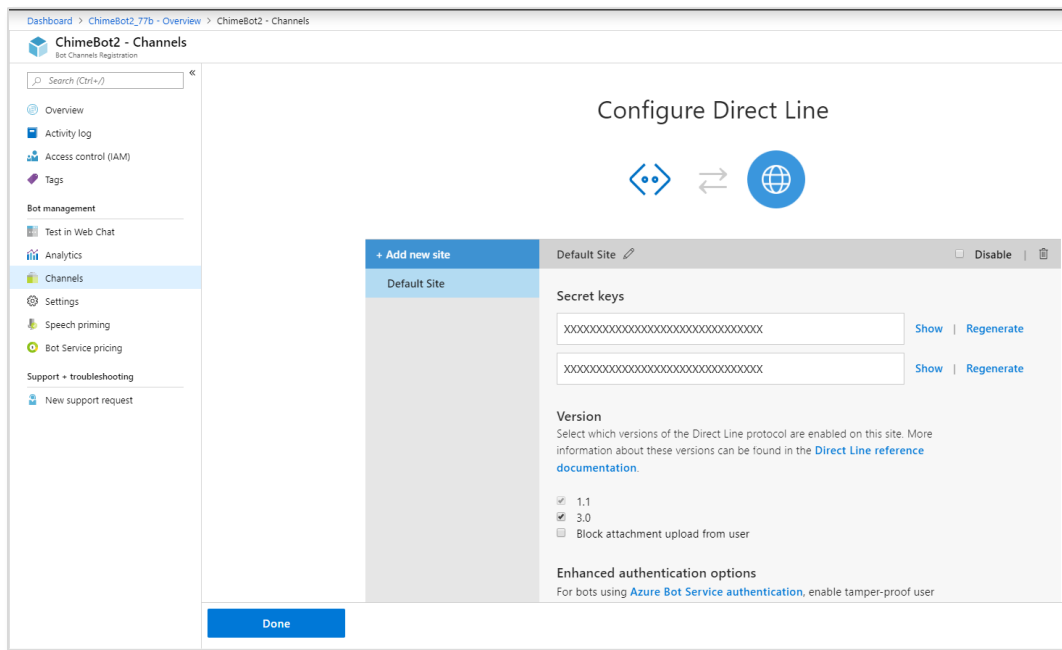


Figure 33: Configure Direct Line

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.

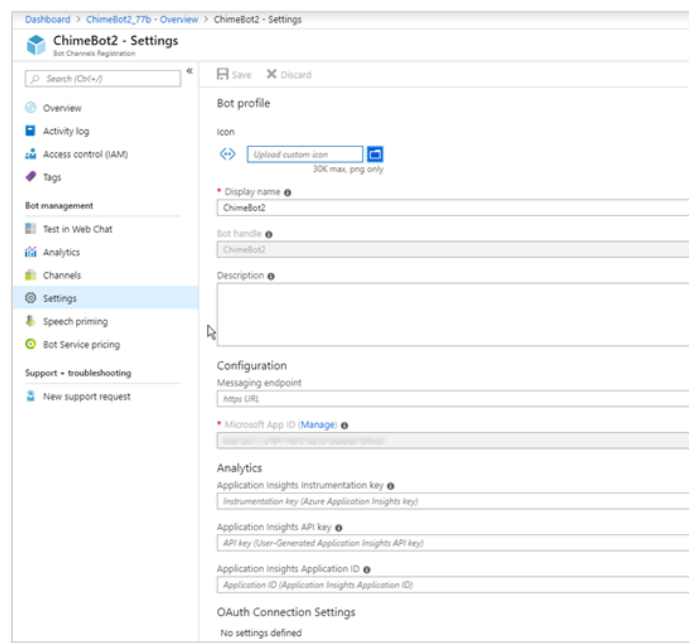
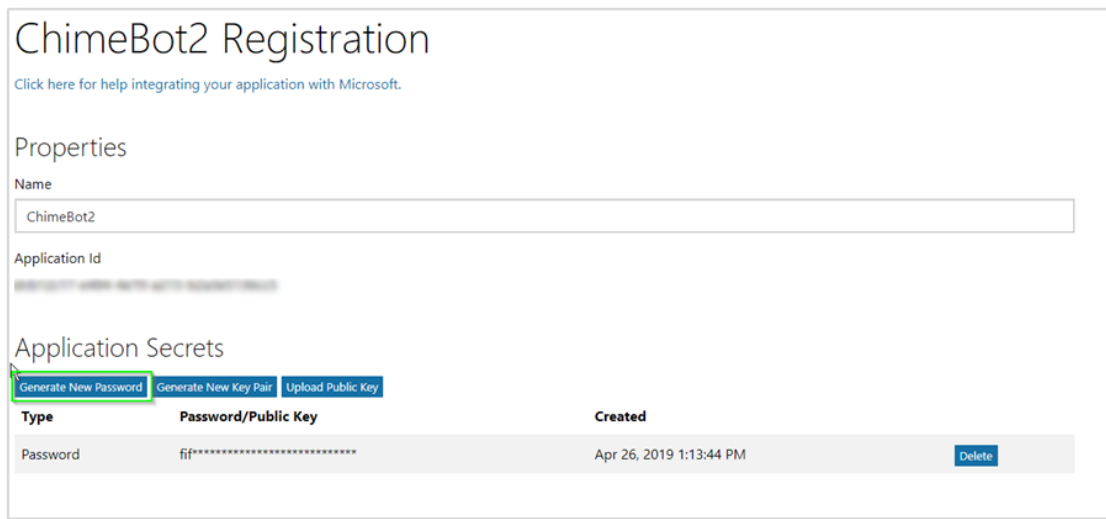


Figure 34: Bot Settings

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.

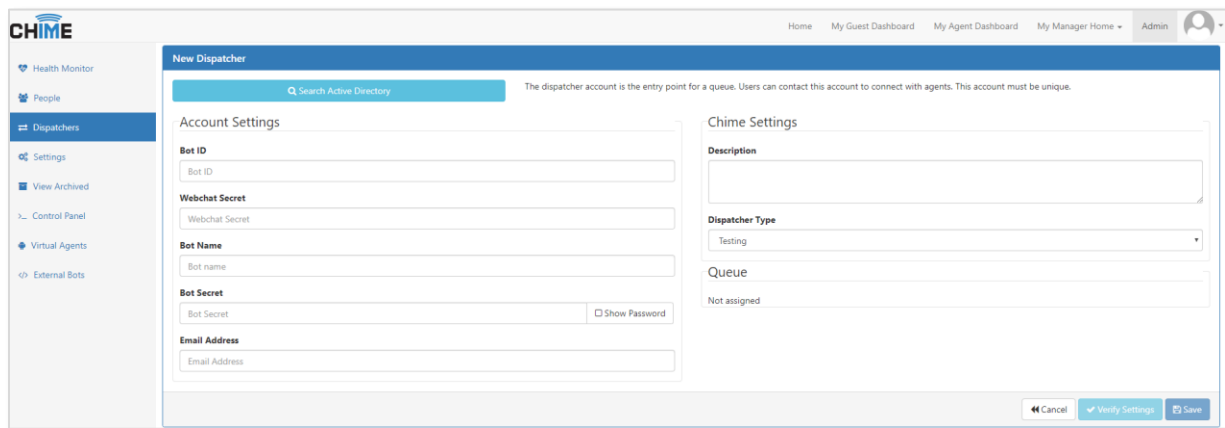


The screenshot shows the 'ChimeBot2 Registration' page. Under the 'Application Secrets' section, there are three buttons: 'Generate New Password' (highlighted with a green box), 'Generate New Key Pair', and 'Upload Public Key'. Below these buttons is a table with columns 'Type', 'Password/Public Key', and 'Created'. The table contains one row with 'Password' as the type, a masked password 'fif*****' as the value, and 'Apr 26, 2019 1:13:44 PM' as the creation date. A 'Delete' button is located at the end of this row.

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

Figure 35: 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.



The screenshot shows the 'New Dispatcher' form in the Chime Admin console. 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' field (set to 'Not assigned'). At the bottom right, there are 'Cancel', 'Verify Settings', and 'Save' buttons.

Figure 36: 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:

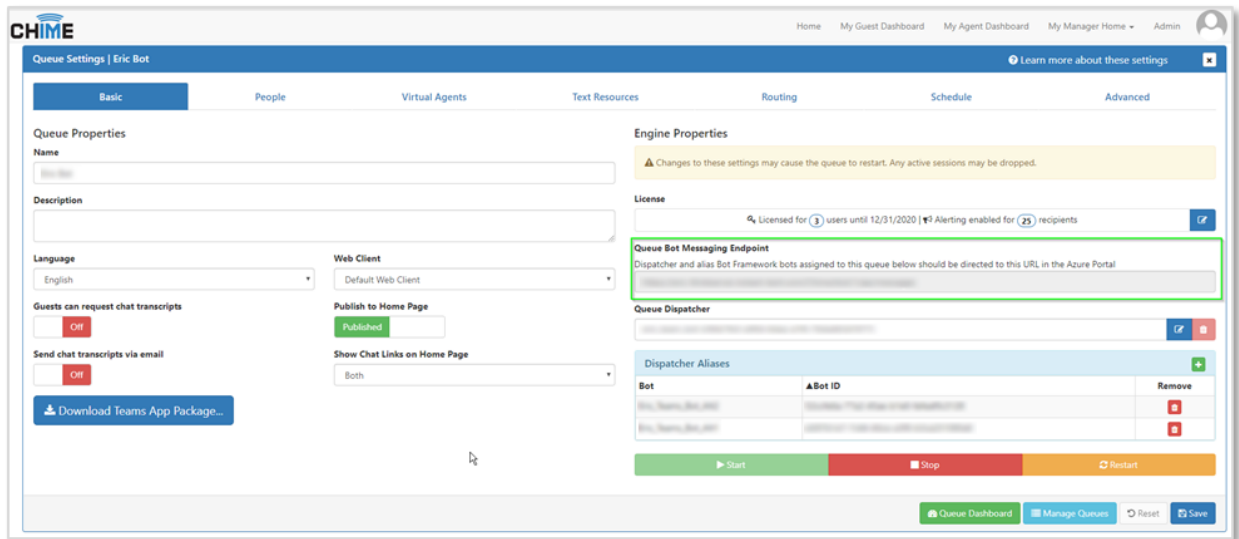


Figure 37: Chime Queue Settings

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.

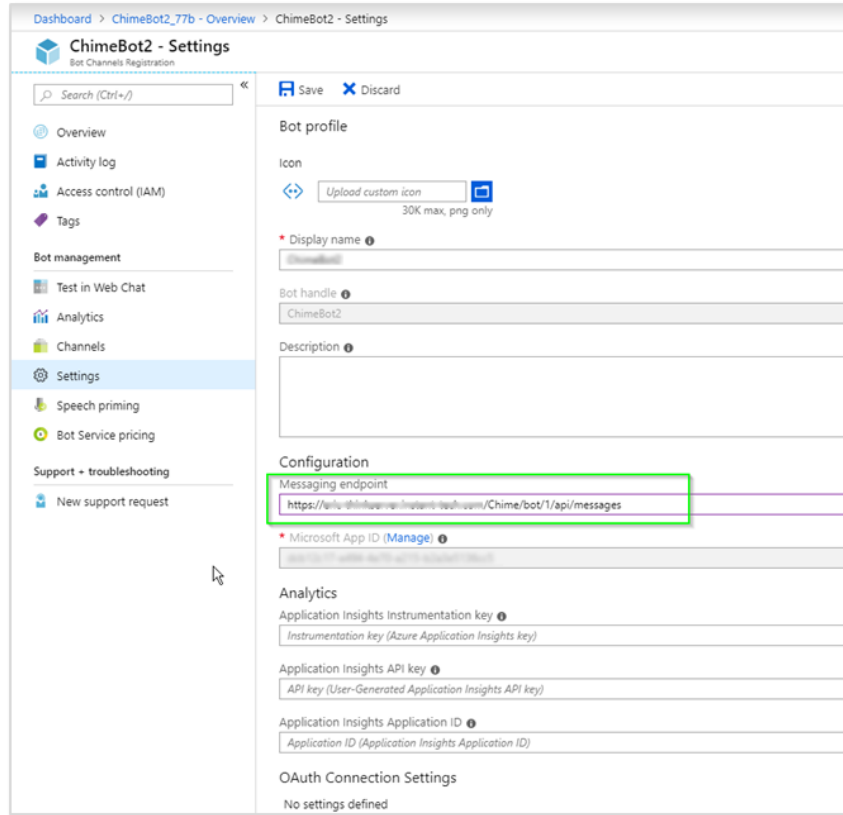


Figure 38: Settings - Configuration