



Chime for Teams Installation Azure and Office 365 Prerequisites and Overview

June 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
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 Dispatcher Resource	20
Adding the Dispatcher into Chime.....	25

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. For the easiest setup, please acquire a certificate in the .pfx format as it will make adding it much easier.

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.

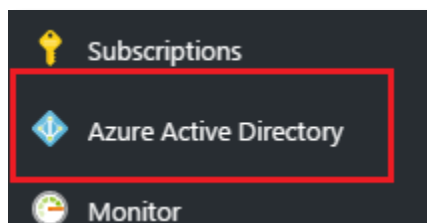


Figure 1: Begin Setting up Active Directory

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**

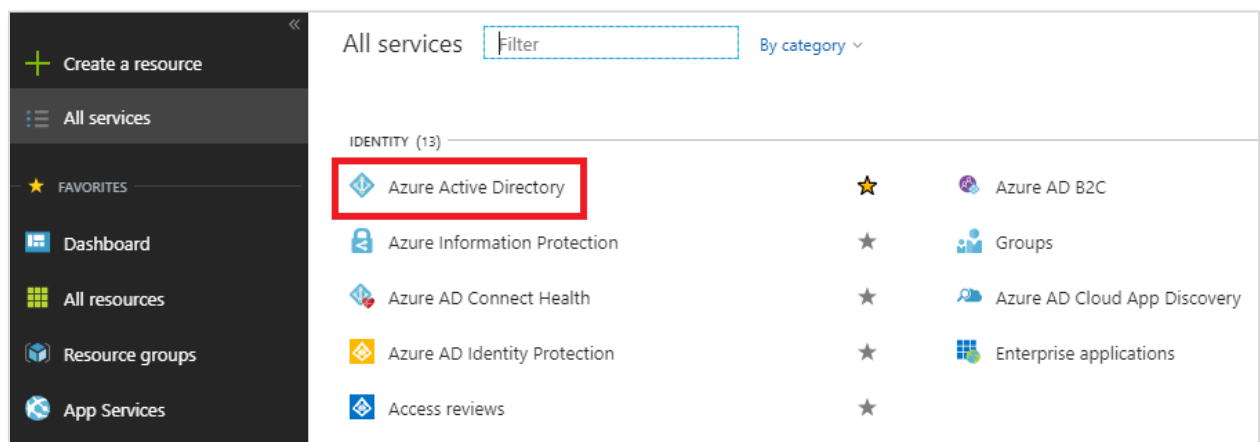

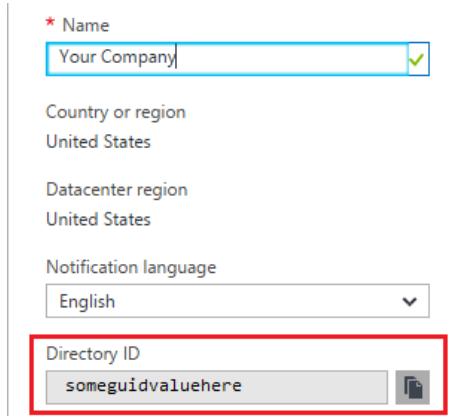


Figure 2: Secondary Option to Active Directory Setup

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.

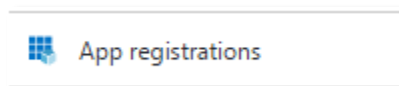


The screenshot shows the 'Properties' blade for an Azure Active Directory tenant. The 'Name' field contains 'Your Company'. The 'Country or region' and 'Datacenter region' are both set to 'United States'. The 'Notification language' is set to 'English'. The 'Directory ID' field contains 'someguidvaluehere'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

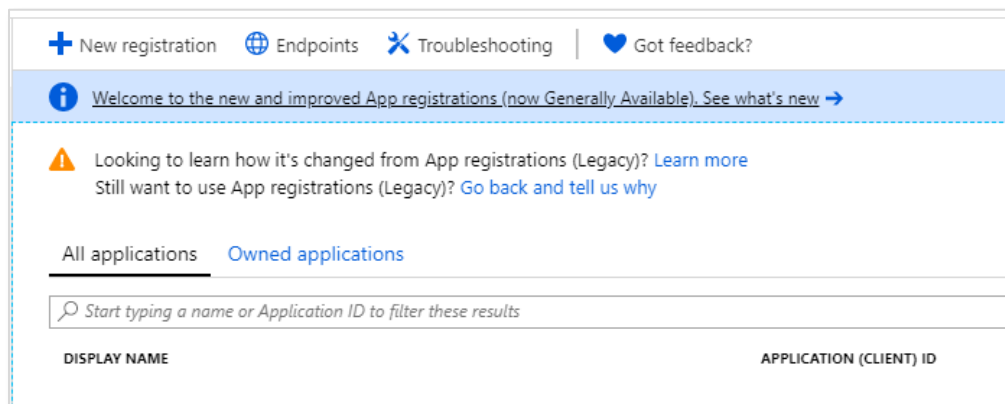
Figure 3: Copy Directory ID

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 →'. There is also 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'. Below this, there are tabs for '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 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

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
AppCatalog.ReadWrite.All	Delegated	Read and write to all app catalogs
Channel.ReadBasic.All	Application	Read the names and descriptions of all channels
Directory.Read.All	Application	Read directory data
Presence.Read.All	Delegated	Read presence information of all users in your organization
Team.ReadBasic.All	Application	Get a list of all teams
TeamMember.ReadWrite NonOwnerRole.All	Application	Add and remove members with non-owner role for all teams
TeamsApp.ReadWrite	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>
User.Read	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>
User.ReadBasic.All	Delegated	

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

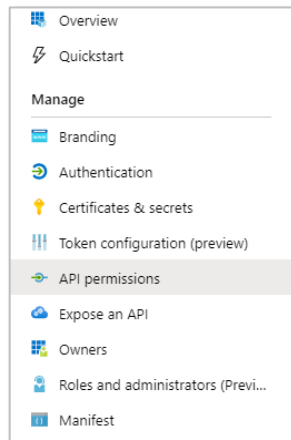


Figure 6: Access Required API Permissions

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

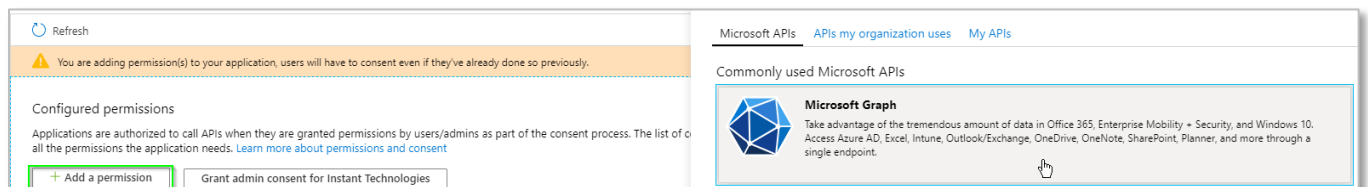


Figure 7: Manage Required Permissions

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

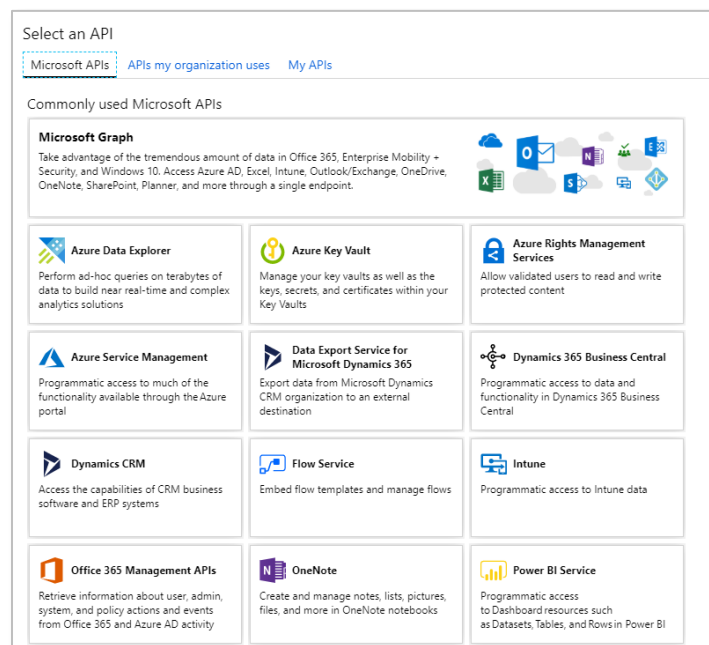


Figure 8: Configure Required Permissions

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

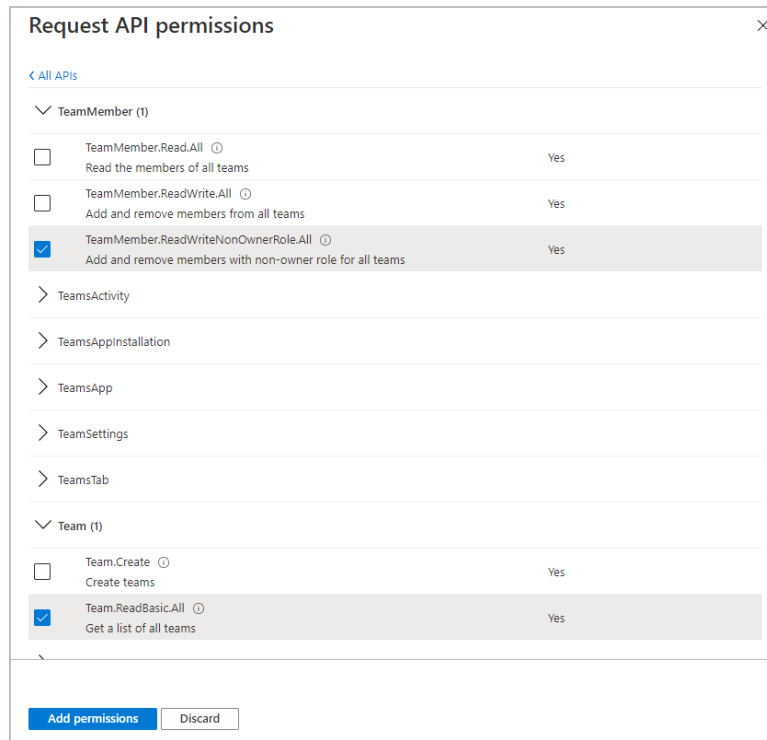


Figure 9: Select Permissions for Graph Api

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. AppCatalog.ReadWrite.All
 - b. Presence.Read.All
 - c. TeamsApp.ReadWrite
 - d. User.Read
 - e. User.ReadBasic.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

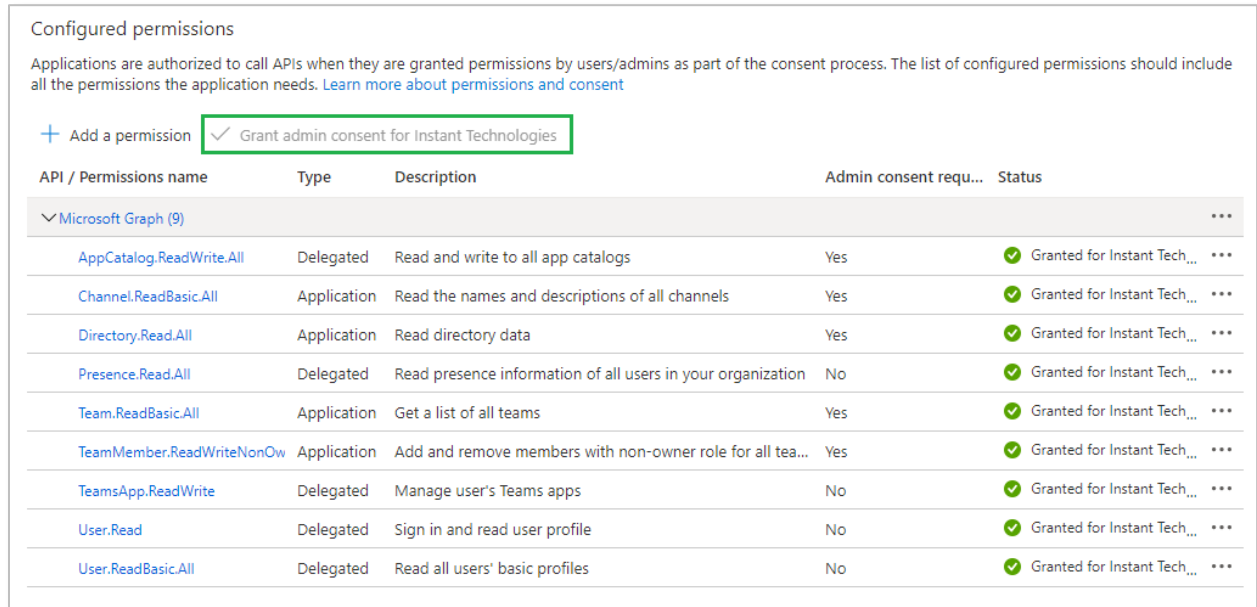


Figure 11: Grant Admin Consent

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.

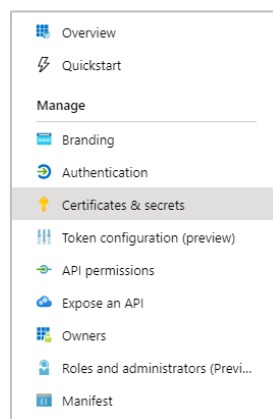


Figure 12: Access Certificates & Secrets

2. Click the **New client secret** button.
3. Enter a description for your client secret.
4. Select a duration for this API key. Recently Microsoft changed this so that you are not able to set it to never expire. **Note:** make sure this secret key is updated before it expires. If this expires, none of your users will be able to log into Chime. When updating this every 2 years you will need to also add the new value into the install wizard.
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

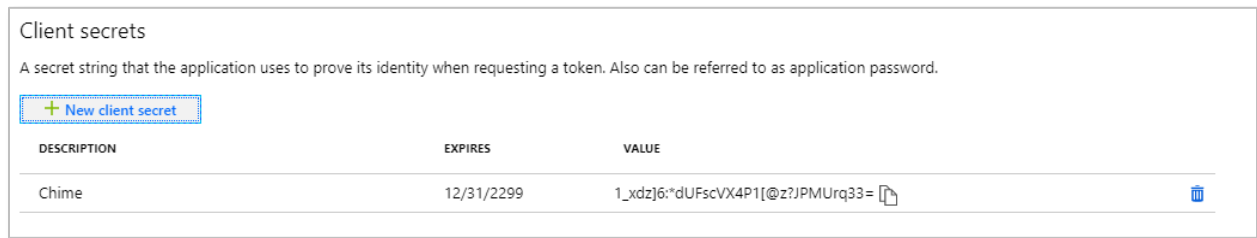


Figure 13: Setup API Key

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

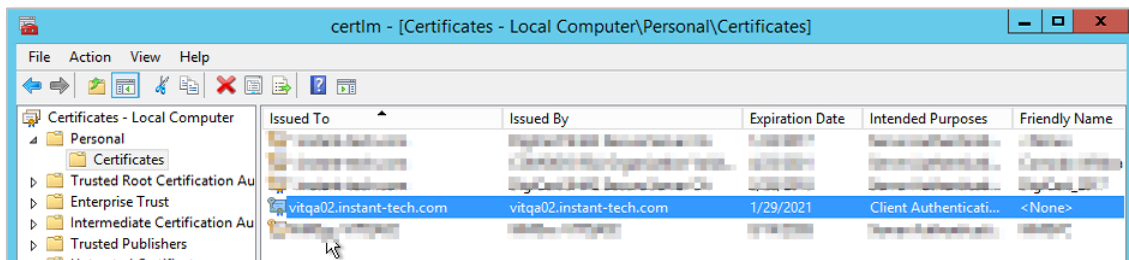


Figure 15: Chime Service Account

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

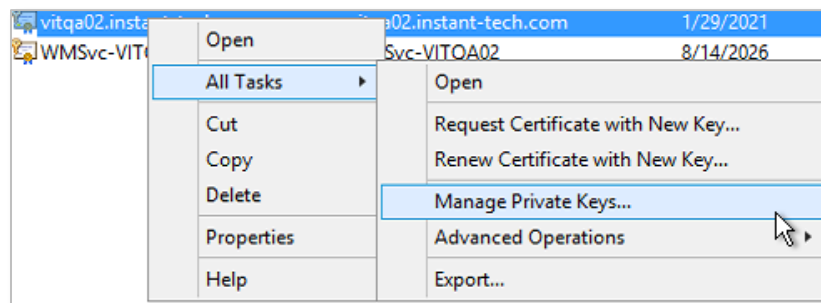


Figure 16: Manage Private Keys

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

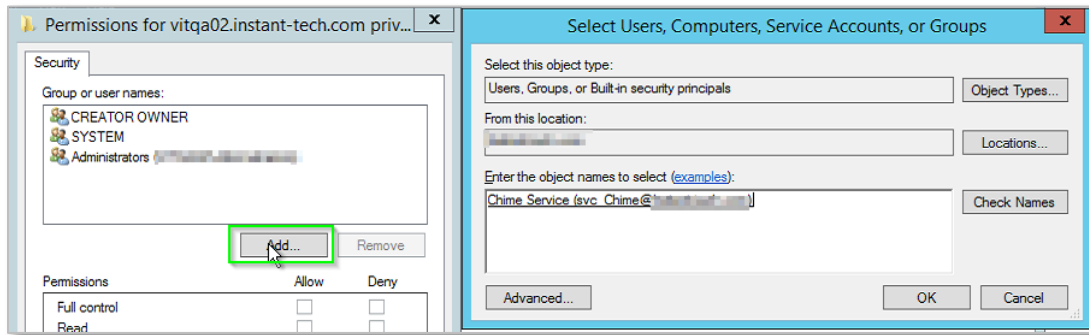


Figure 17: Add Account to Permissions

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.

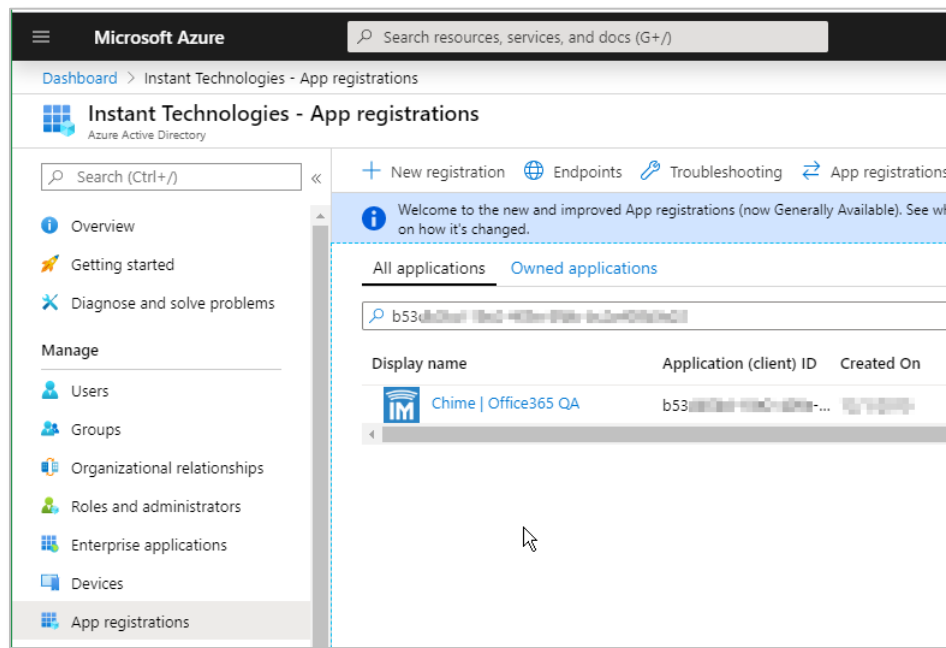


Figure 18: Navigate to App Registration

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

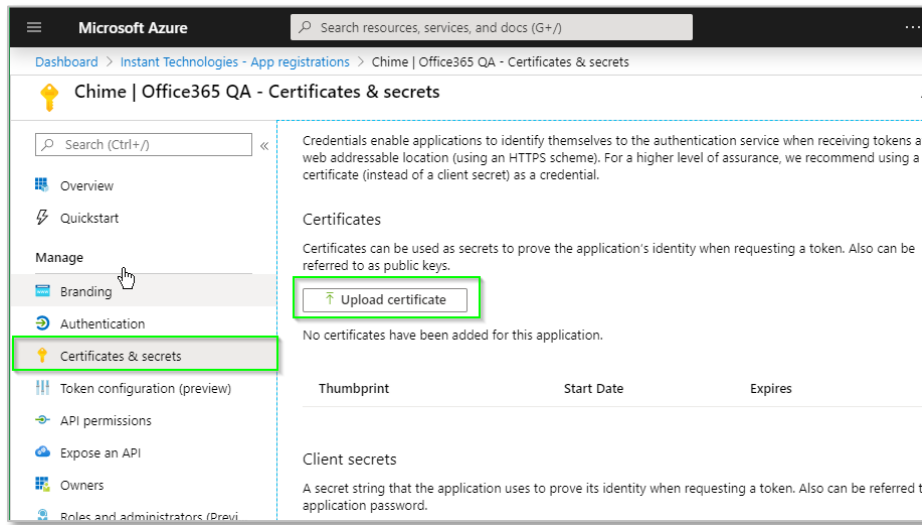


Figure 19: Upload Certificate

- 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.

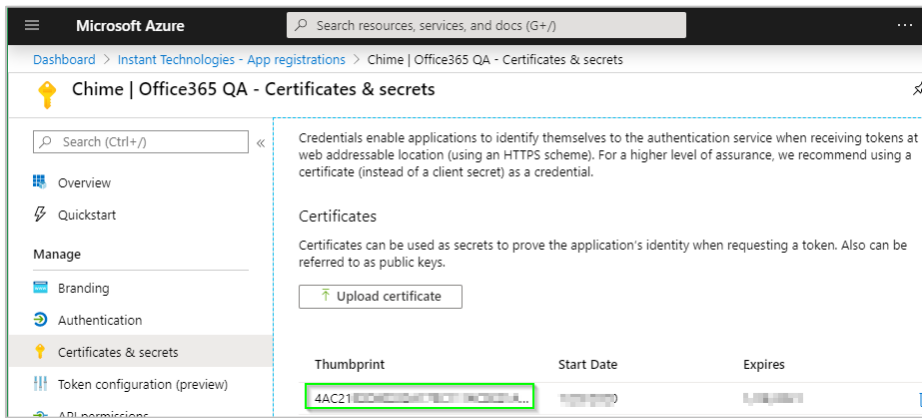


Figure 20: Verify Thumbprint

ADD REDIRECT URIS

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

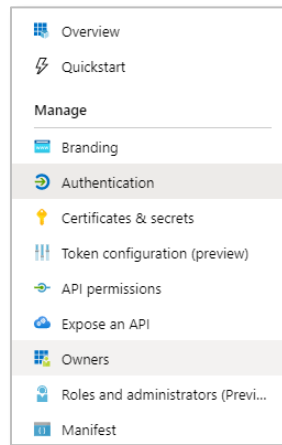


Figure 21: Configure Reply URLs

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)

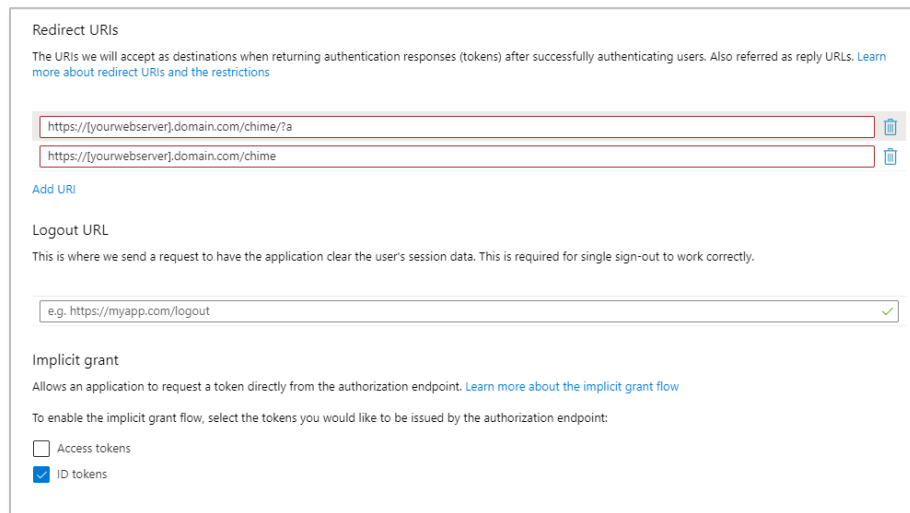
A screenshot of a web configuration page titled 'Redirect URIs'. It contains a list of two URIs: 'https://[yourwebserver].domain.com/chime/?a' and 'https://[yourwebserver].domain.com/chime', each with a delete icon. Below this is an 'Add URI' link. The 'Logout URL' section has a text input field with 'e.g. https://myapp.com/logout' and a checkmark. The 'Implicit grant' section has a description and a link. At the bottom, there are two checkboxes: 'Access tokens' (unchecked) and 'ID tokens' (checked).

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.

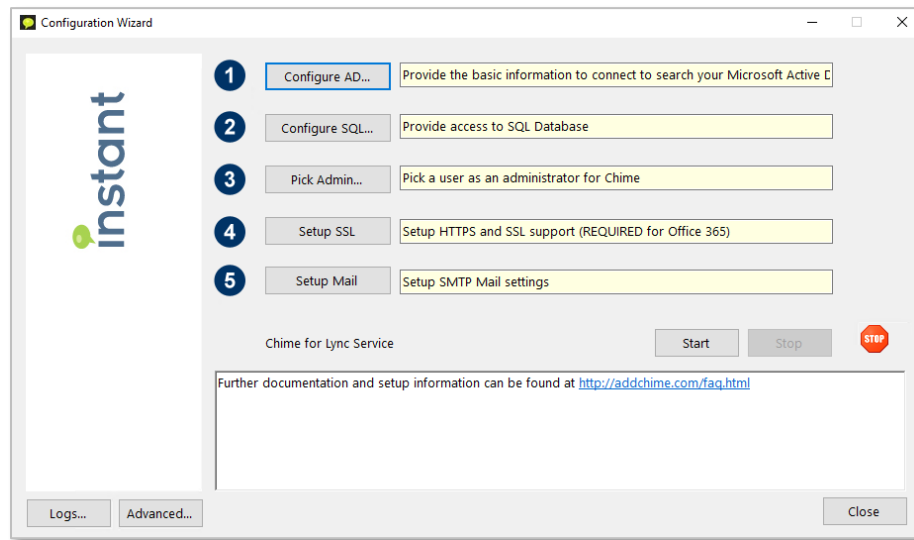


Figure 24: Configuration Wizard

When adding the certificate onto the server, make sure that it is in the .pfx format. This will make it much easier to setup SSL. Additionally, when adding it, make sure it is stored in the personal rather than local machine. 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**.

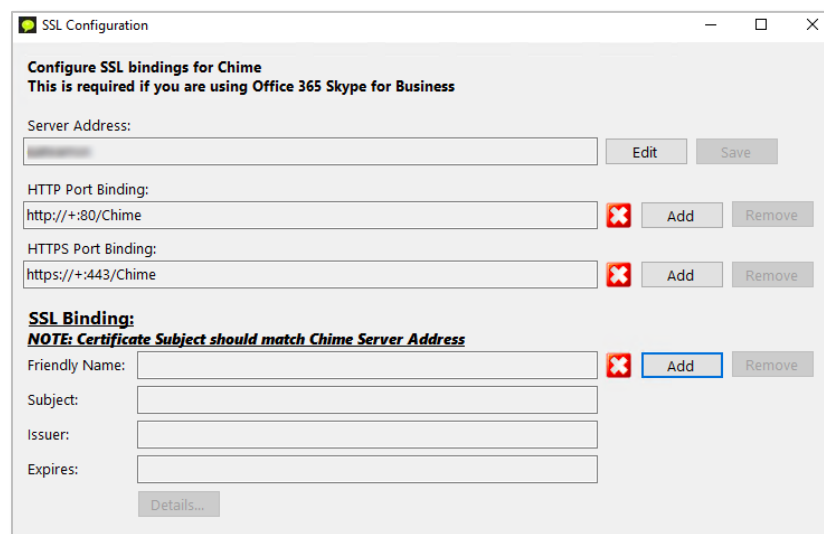


Figure 25: Setup SQL Connection

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

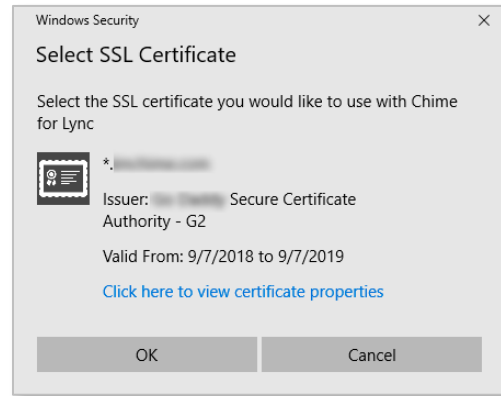


Figure 26: Select SSL Certificate

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.

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>

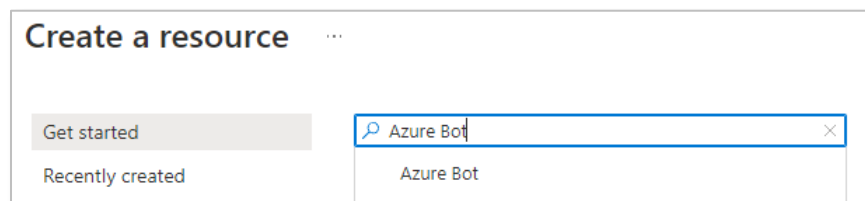


Figure 27: Searching for Azure Bot

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.

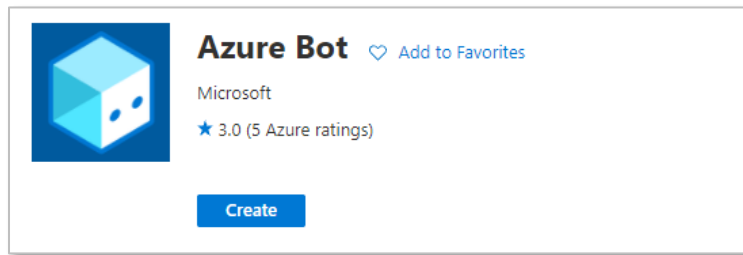


Figure 28: Create Azure Bot Resource

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](#)

i 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 29: Create Azure Bot - Basics

- a. **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.
 - 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.
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.
 - e. **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

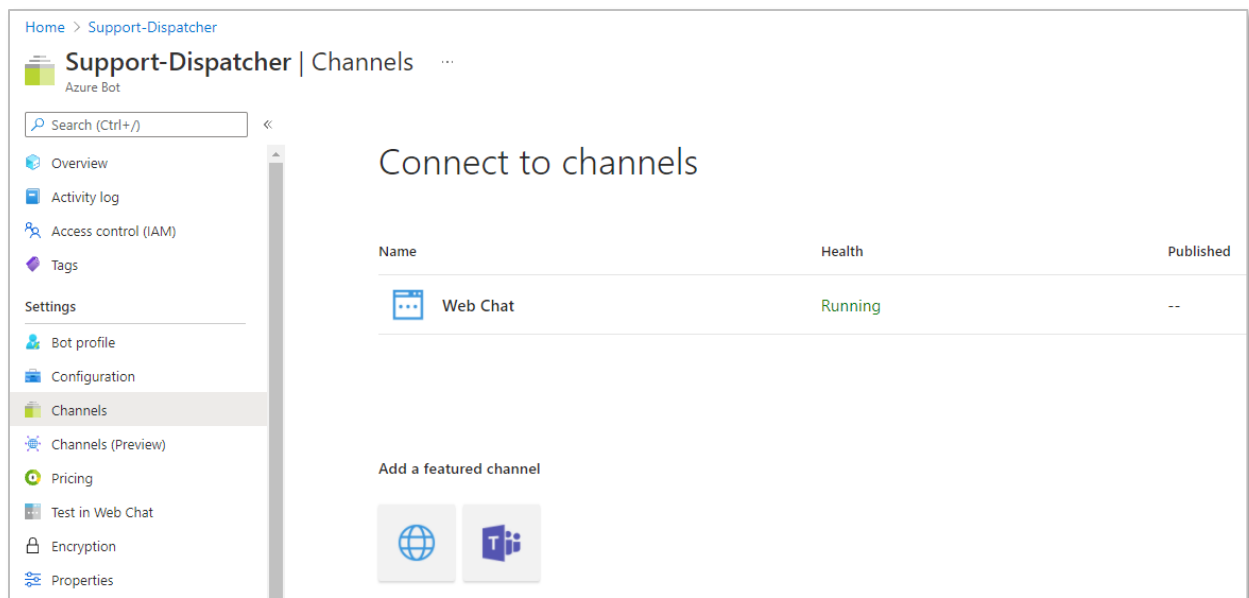


Figure 30: Configure Azure Bot Channels

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

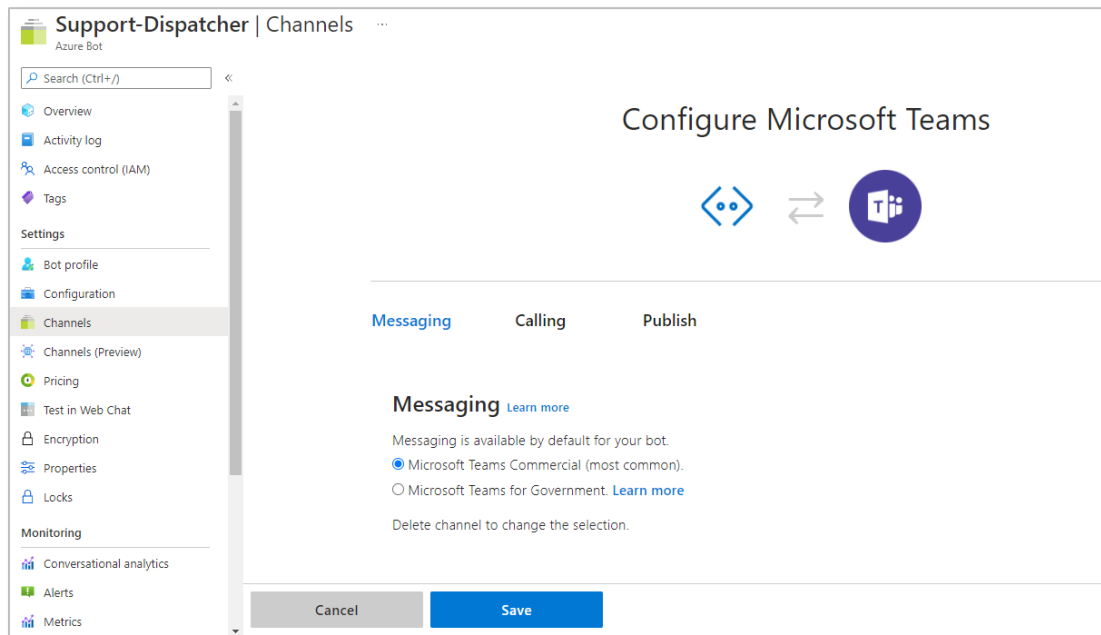


Figure 31: Set up Teams Channel

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

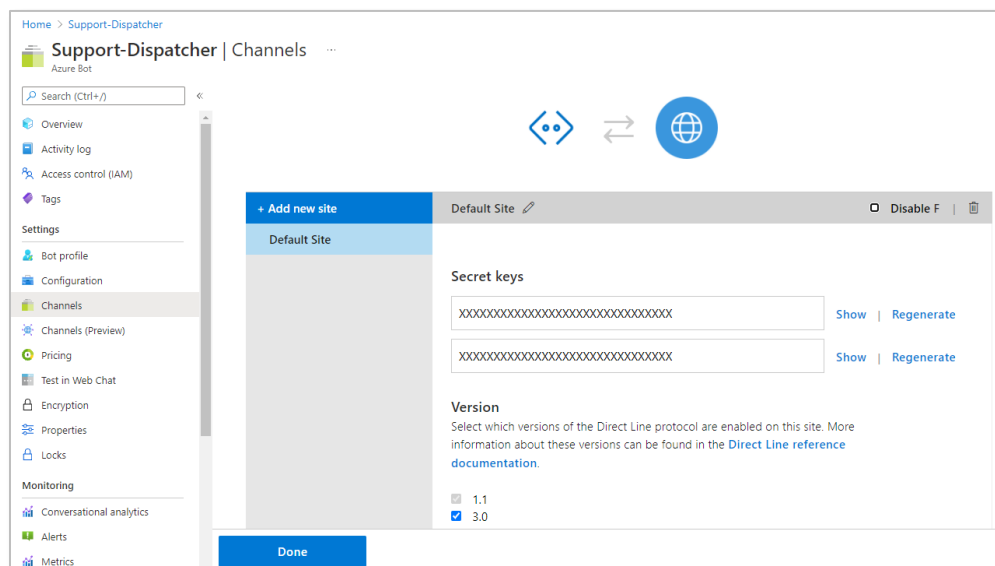


Figure 32: Set up Direct Line and Record Secret

- 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 Configuration tab on the bot registration. Record the **Microsoft App ID** fields here, as they will be needed to configure the bot in Chime.

The screenshot shows the 'Support-Dispatcher | Configuration' page in the Azure Bot portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Settings (Bot profile, Configuration, Channels, Channels (Preview), Pricing, Test in Web Chat), Encryption, Properties, Locks, Monitoring (Conversational analytics, Alerts, Metrics). The main content area is the 'Configuration' tab, which includes the following fields and sections:

- Messaging endpoint:** A text box containing 'https URL'.
- Enable Streaming Endpoint:** A checkbox that is currently unchecked.
- App Type:** A dropdown menu showing 'MultiTenant'.
- Microsoft App ID (Manage):** A text box containing the ID '4f59a763-c351-4b49-920a-38c70e46cae8'.
- Application Insights Instrumentation key:** A text box containing 'Instrumentation key (Azure Application Insights key)'.
- Application Insights API key:** A text box containing a masked key '.....' with a green checkmark on the right.
- Application Insights Application ID:** A text box containing 'Application ID (Application Insights Application ID)'.
- Schema Transformation Version:** A dropdown menu showing 'V1.3'.
- Footer text:** 'This determines how Bot Service converts messages sent between your bot and channels. [Learn more](#)'.
- No OAuth Connection settings defined:** A section with an 'Add OAuth Connection Settings' button.
- Buttons:** 'Apply' and 'Discard changes' buttons at the bottom.

Figure 33: Record App ID

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.

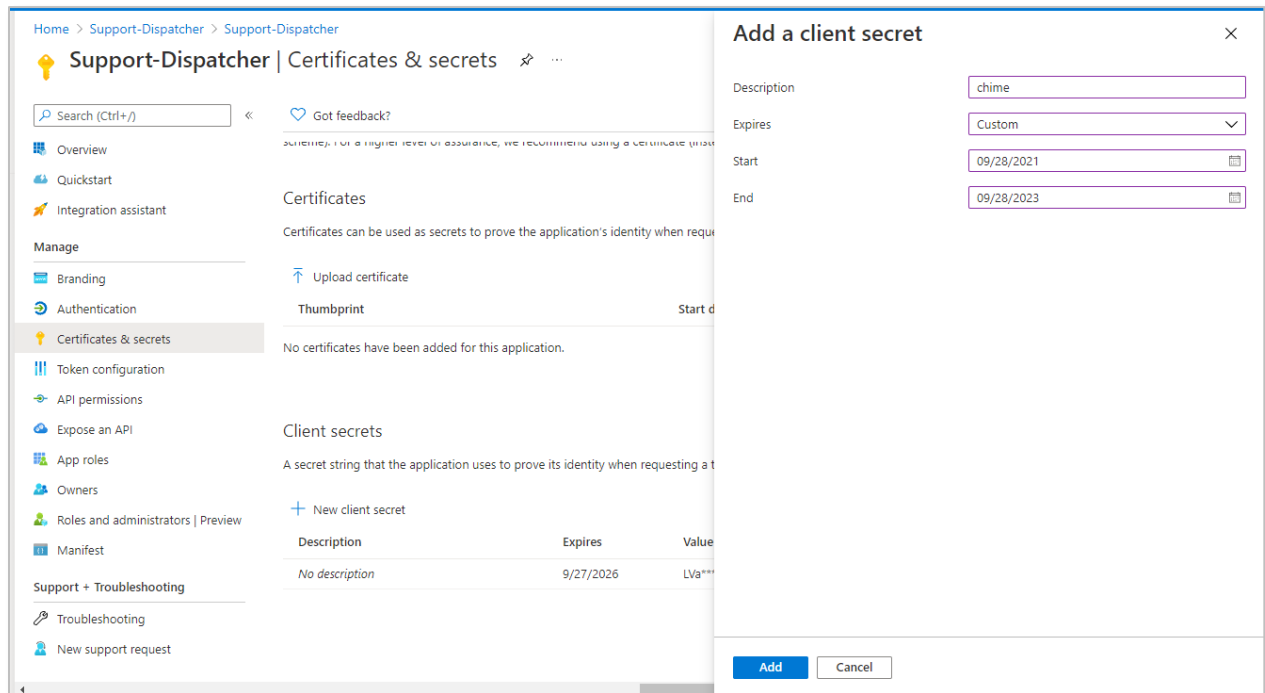


Figure 34: Add Client Secret

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. **Note**: make sure this secret key is updated before it expires. If this expires, none of your users will be able to log into Chime. When updating this every 2 years you will need to also add the new value into the install wizard.
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.

Figure 35: 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 36: 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.

Dashboard > ChimeBot2_77b - Overview > ChimeBot2 - Settings

ChimeBot2 - Settings

Bot Channels Registration

Search (Ctrl+/)

Save Discard

Bot profile

Icon [Upload custom icon](#) 30K max, png only

* Display name [ChimeBot2](#)

Bot handle [ChimeBot2](#)

Description

Configuration

Messaging endpoint [https://api.chimebot2.com/Chime/bot/1/api/messages](#)

* Microsoft App ID ([Manage](#))

Analytics

Application Insights Instrumentation key [Instrumentation key \(Azure Application Insights key\)](#)

Application Insights API key [API key \(User-Generated Application Insights API key\)](#)

Application Insights Application ID [Application ID \(Application Insights Application ID\)](#)

OAuth Connection Settings

No settings defined

Figure 37: Settings - Configuration