

Chime for Teams Installation Azure and Office 365 Prerequisites and Overview



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 Secrets1	2
Add Redirect URIs1	17
Azure Active Directory Accounts List1	8
Setup After Chime Install1	9
Install Wizard1	9
Creating Bots for Chime Dispatchers2	20
Creating a Dispatcher Resource2	20
Adding the Dispatcher into Chime2	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, 0365 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 <u>https://technet.microsoft.com/en-us/library/dn832618.aspx</u>.

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 (<u>https://portal.azure.com</u>).
- 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**

+	« Create a resource	All services Filter	By category ~	
i≡	All services	IDENTITY (13)		
- *	FAVORITES	Azure Active Directory	☆	Azure AD B2C
	Dashboard	Azure Information Protection	*	Groups
	All resources	🍫 Azure AD Connect Health	*	Azure AD Cloud App Discovery
()	Resource groups	Azure AD Identity Protection	*	Enterprise applications
۲	App Services	Access reviews	*	

Figure 2: Secondary Option to Active Directory Setup

CONFIGURE ACTIVE DIRECTORY AUTHENTICATION

RETRIEVE YOUR AZURE TENANT ID

11 Properties

1. Select

- in the navigation pane in the **Azure Active Directory** blade.
- 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.





REGISTER THE CHIME APPLICATION

- 1. Create a name for this application (Chime is a suitable name)
- 2. Select Accounts in this organizational directory only as the Supported account types
- 3. Enter the URL for the server that Chime will be hosted on, with the /Chime route in the URL (ex: https://yourserver.domain.com/Chime)

NOTE: Be sure that the /Chime is included in the URL, this will automatically configure the Reply URL to correctly work with the Chime application

Dashboard > instant technologies - App registrations > Register an application					
Register an application					
* Name					
The user-facing display name for this application (this can be changed later).					
CHime 🗸					
Supported account types					
Who can use this application or access this API?					
Accounts in this organizational directory only (instant technologies)					
Accounts in any organizational directory					
O 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 V https://yourwebserver.domain.com/chime V					

Figure 5: Create the Chime Web App / API

4. Click the

button in the bottom of the Register an Application blade.

CONFIGURE THE APPLICATION

Register

- 1. Click on the newly created application in the **App Registrations** blade. If you have many applications, you may need to search for it.
- 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	Туре	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. Without this permission, it is necessary for an administrator to manually upload Teams App packages for the queues.
User.Read	Delegated	OPTIONAL - Allows Chime to programmatically assign generated Teams App packages to the Team associated with a queue 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
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.

icrosoft APIs APIs my organization	uses My APIs					
ommonly used Microsoft APIs						
Microsoft Graph		🍊 🗖 🖬 🔬 🜆				
Take advantage of the tremendous amount of data in Office 385, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Unitune, OutlookExchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.						
Xarre Data Explorer						
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	Allow validated users to read and write protected content				
Azure Service Management	Data Export Service for Microsoft Dynamics 365	oco Dynamics 365 Business Central				
Programmatic access to much of the functionality available through the Azure portal	Export data from Microsoft Dynamics CRM organization to an external destination	Programmatic access to data and functionality in Dynamics 365 Business Central				
Dynamics CRM	Flow Service	Intune				
Access the capabilities of CRM business software and ERP systems	Embed flow templates and manage flows	Programmatic access to Intune data				
Office 365 Management APIs	OneNote	Power BI Service				
Retrieve information about user, admin, system, and policy actions and events	Create and manage notes, lists, pictures, files, and more in OneNote notebooks	Programmatic access to Dashboard resources such				

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.

Request API permissions		>				
< All APIs						
V TeamMember (1)						
TeamMember.Read.All ① Read the members of all teams	Yes					
TeamMember.ReadWrite.All ① Add and remove members from all teams	Ves					
TeamMember.ReadWriteNonOwnerRole.All ③ Add and remove members with non-owner role for all teams	Yes					
> TeamsActivity						
> TeamsAppInstallation						
> TeamsApp						
> TeamSettings						
> TeamsTab						
🗸 Team (1)						
Team.Create ① Create teams	Yes					
Team.ReadBasic.All ① Get a list of all teams	Yes					
、						
Add permissions Discard						

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

▼ User (1)					
-					
Yes					
-					

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

Configured permissions Applications are authorized to call AF III the permissions the application ne + Add a permission	Pls when they eds. Learn mo	are granted permissions by users/admins as part of the conser ore about permissions and consent t for Instant Technologies	nt process. The list of cont	figured permissions should include
API / Permissions name	Туре	Description	Admin consent requ	Status
∽ Microsoft Graph (9)				•••
AppCatalog.ReadWrite.All	Delegated	Read and write to all app catalogs	Yes	♂ Granted for Instant Tech ···
Channel.ReadBasic.All	Application	Read the names and descriptions of all channels	Yes	✓ Granted for Instant Tech ····
Directory.Read.All	Application	Read directory data	Yes	♂ Granted for Instant Tech ····
Presence.Read.All	Delegated	Read presence information of all users in your organization	No	♂ Granted for Instant Tech ···
Team.ReadBasic.All	Application	Get a list of all teams	Yes	♂ Granted for Instant Tech, ····
TeamMember.ReadWriteNonOw	Application	Add and remove members with non-owner role for all tea	Yes	♂ Granted for Instant Tech, ····
TeamsApp.ReadWrite	Delegated	Manage user's Teams apps	No	♂ Granted for Instant Tech ···
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Instant Tech ····
User.ReadBasic.All	Delegated	Read all users' basic profiles	No	♂ Granted for Instant Tech ···

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

Client secrets					
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.					
+ New client secret					
DESCRIPTION	EXPIRES	VALUE			
Chime	12/31/2299	1_xdz]6:*dUFscVX4P1[@z?JPMUrq33= [Ō		



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
- We provide a PowerShell script to create such a script, CreateAzureADCert.ps1, which is reproduced below:



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 certIm.msc
 - b. Expand the Personal\Certificates store in the left pane and find the certificate that has been generated for the client certificate

certIm - [Certificates - Local Computer\Personal\Certificates]							
File Action View Help							
🖈 Certificates - Local Computer	Issued To 📩	Issued By	Expiration Date	Intended Purposes	Friendly Name		
⊿ Personal	Contraction and some	Particular and Instant and a line	1. The second	terror and territoria	- Terrar		
Certificates	Weiner without	Caroline Replayering the field.	10000	interioristical.	Constanting of the		
Trusted Root Certification Au	The second second	Uniform PRE Incompany Of		Serve Reflective States	Styles, 201		
Enterprise Trust	vitga02.instant-tech.com	vitga02.instant-tech.com	1/29/2021	Client Authenticati	<none></none>		
Intermediate Certification Au	Contract of the local states of the local stat	March 1975 ALC	10 10 TOD	Republished in the	MARKET CO.		
Trusted Publishers	ЬÌ						

Figure 15: Chime Service Account

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

vitqa02.insta	Open	-	302.instant-tech.com	1/29/2021
	All Tasks	All Tasks		0/ 14/2020
	Cut Copy		Request Certifica Renew Certificate	te with New Key with New Key
	Delete		Manage Private K	(eys
	Properties		Advanced Operat	tions 🗟 🗟
	Help		Export	

Figure 16: Manage Private Keys

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

Permissions for vitqa02.instant-tech.com priv ×	Select Users, Computers, Service Accounts, or Groups
Security Group or user names: CREATOR OWNER SYSTEM Administrators Administrators Remove	Select this object type: Users, Groups, or Built-in security principals Object Types From this location:
Permissions Allow Deny Full control	Advanced OK Cancel

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 <u>https://portal.azure.com</u>, and then find the Azure AD App Registration that was previously created.

\equiv Microsoft Azure	${\cal P}$ Search resources, services, and docs	(G+/)
Dashboard > Instant Technologies - App r	egistrations	
Instant Technologies - Ap	p registrations	
	+ New registration	otin Troubleshooting otin App registrations
Overview	Welcome to the new and improved A on how it's changed.	pp registrations (now Generally Available). See wh
💉 Getting started	All applications Owned application	ons
🗙 Diagnose and solve problems	₽ b53chdhai ind stile indes	10101
Manage	Display name	Application (client) ID Created On
🚨 Users	Chime Office365 QA	b53
A Groups	■ 1111	
🏮 Organizational relationships		
Boles and administrators		
Enterprise applications	\triangleright	
📮 Devices		
App registrations		



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

\equiv Microsoft Azure	𝒫 Search resources, services,	and docs (G+/)	
Dashboard > Instant Technologies - App	registrations > Chime Office365	QA - Certificates & secrets	
🔶 Chime Office365 QA - 0	Certificates & secrets		;
	Credentials enable application web addressable location (usi	ns to identify themselves to the authe ng an HTTPS scheme). For a higher le	entication service when receiving tokens at evel of assurance, we recommend using a
u Overview	certificate (instead of a client	secret) as a credential.	-
Quickstart	Certificates		
Manage	Certificates can be used as se referred to as public keys.	crets to prove the application's identi	ty when requesting a token. Also can be
Branding	↑ Upload certificate]	
Authentication	No certificates have been add	ed for this application.	
📍 Certificates & secrets			
III Token configuration (preview)	Thumbprint	Start Date	Expires
API permissions			
🙆 Expose an API	Client secrets		
R Owners	A secret string that the applic	ation uses to prove its identity when	requesting a token. Also can be referred to
Roles and administrators (Previ	application password.		

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.

	${\cal P}$ Search resources, services, and docs (G+	÷/)		
Dashboard > Instant Technologies - App	registrations > Chime Office365 QA - Certific	ates & secrets		
🔶 Chime Office365 QA - C	ertificates & secrets			۶¢
	Credentials enable applications to identify web addressable location (using an HTTPS	themselves to the auther	tication service when receiving tokens	; at a
Overview	certificate (instead of a client secret) as a cr	redential.	er or assurance, we recommend using	
🖗 Quickstart	Certificates			
Manage	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.			
🔤 Branding	↓ Upload certificate			- 1
Authentication				- 1
📍 Certificates & secrets	Thumborint	Start Date	Evniros	- 1
Token configuration (preview)	44021	Start Date	Expires	T ^e
- ADI pormissions	70001			

Figure 20: Verify Thumbprint

ADD REDIRECT URIS

1. To add Redirect URLs click the Authentication button.



Figure 21: Configure Reply URLs

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: <u>https://[yourwebserver].domain.com/chime</u> (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 r more about redirect URIs and the restrictions	eferred as reply URLs. Learn
https://[yourwebserver].domain.com/chime/?a	Û
https://[yourwebserver].domain.com/chime	Û
Add URI	
Logout URL	
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 correct	ily.
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 correct	ily.
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 correct e.g. https://myapp.com/logout	ly.
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 correct e.g. https://myapp.com/logout	ly.
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 correct e.g. https://myapp.com/logout Implicit grant	ly.
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 correct 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	tly. √]
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 correct 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:	
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 correct 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	tly. √]

Figure 22: Configure Reply URLs

- 3. In the text box below, add in a URI with this format: <u>https://[yourwebserver].domain.com/chime/?a</u>
- 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

Setup Azure AD Connection	<
Azure AD Tenant:	1
Azure AD Tenant ID:]
Azure AD ClientID:	1
Azure AD Client Secret Key:]
Test]
Save	

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.

Configuration Wizard		-		×
	Configure AD	Provide the basic information to connect to search your Microsoft Active C		
O DD	Configure SQL	Provide access to SQL Database		
Stc	Pick Admin	Pick a user as an administrator for Chime		
●	Setup SSL	Setup HTTPS and SSL support (REQUIRED for Office 365)		
6	Setup Mail	Setup SMTP Mail settings		
	Chime for Lync Service	Start Stop	STOP	
Furthe	r documentation and set	up information can be found at <u>http://addchime.com/faq.html</u>		
Logs Advanced			Close	

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.

🔁 SSL Configuratio	n		-	-		×
Configure SSL b This is required	ndings for Chime if you are using Office 365 Skype for Business					
Server Address:						
all and a second		Edit			e	
HTTP Port Bindin	j:					
http://+:80/Chime	8	3	Add			e
HTTPS Port Bindi	ıg:					
https://+:443/Chi	ne 🗧	3	Add			е
SSL Binding: NOTE: Certifica Friendly Name:	e Subject should match Chime Server Address	a –	Add			2
Cubiecte	• • • • • • • • • • • • • • • • • • •					
Subject:						
Issuer:						
Expires:						
	Details					



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

Windows	Security		×
Select	SSL Certificate		
Select the SSL certificate you would like to use with Chime for Lync			
9 	*. Authority - G2 Valid From: 9/7/2018 Click here to view cert	ure Certificate to 9/7/2019 ificate properties	
	ОК	Cancel	

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 <u>https://portal.azure.com</u>

Create a resource		
Get started		
Recently created	Azure Bot	

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 deplo manage all your resources.	oyed resources and costs. Use resource groups like folders to organize a	and
Bot handle * ①	Support-Dispatcher	~
Subscription * ①	Pay-As-You-Go Dev/Test	~
Resource group * ①	(New) Chime-Test-RG	\sim
	Create new	
New resource group location ①	East US	\sim
management. Learn more about availab Azure Bot Services pricing Pricing tier *	le options, or request a pricing quote, by visiting the	
-	Change plan	
Microsoft App ID		
A Microsoft AppID is required to create can manually create your own, then retu Manually create App ID	an Azure Bot resource. An App ID can be automatically created below, urn here to input your new App ID and password.	or you
() The app secret will be stored in Azu	are Key Vault in the same resource group as your Azure bot. Learn more $\sigma^{\rm c}$	
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

Home > Support-Dispatcher			
Support-Dispatcher Cha	nnels		
Overview	Connect to channels		
Activity log			
Access control (IAM)			
Tags	Name	Health	Published
Settings	Web Chat	Running	
🔓 Bot profile			
a Configuration			
Channels			
Channels (Preview)			
• Pricing	Add a featured channel		
Test in Web Chat			
🔁 Properties			

Figure 30: Configure Azure Bot Channels

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

Support-Dispatche	r Channels …
Overview	Configure Microsoft Teams
Activity log	configure microsoft realits
Access control (IAM)	
🗳 Tags	
Settings	
💄 Bot profile	
Configuration	
Channels	Messaging Calling Publish
👾 Channels (Preview)	
Pricing	
Test in Web Chat	Messaging Learn more
A Encryption	Messaging is available by default for your bot.
😂 Properties	Microsoft Teams Commercial (most common).
🔒 Locks	O Microsoft Teams for Government. Learn more
Monitoring	Delete channel to change the selection.
M Conversational analytics	
Alerts	
👬 Metrics 🗸	Cancel Save

Figure 31: Set up Teams Channel

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

Home > Support-Dispatcher			
Support-Dispatcher	Channels		
Overview		$\langle \bullet \rangle \rightarrow \oplus$	
 Activity log 			
Access control (IAM)			
Tags	+ Add new site	Default Site 🖉	🖸 Disable F 🗐
Settings	Default Site		
🍰 Bot profile			
Configuration		Secret keys	
Channels		****	Show Regenerate
Channels (Preview)			
Pricing		XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Show Regenerate
Test in Web Chat			
A Encryption		Version	
🔁 Properties		Select which versions of the Direct Line protocol are enabled on this sit	te. More
🔒 Locks		information about these versions can be found in the Direct Line refe documentation.	rence
Monitoring			
M Conversational analytics		3.0	
Alerts			
Metrics	Done		

Figure 32: Set up Direct Line and Reccord Secret

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

Support-Dispatcher	Configuration	
✓ Search (Ctrl+/) «	Messaging endpoint	
Overview	https URL	
Activity log	Enable Streaming Endpoint	
Access control (IAM)	Арр Туре	
🗳 Tags	MultiTenant	
Catting	Microsoft App ID (Manage) ①	
Settings	4f59a763-c351-4b49-920a-38c70e46cae8	
🤰 Bot profile	Application Insights Instrumentation key 💿	
a Configuration	Instrumentation key (Azure Application Insights key)	
Channels	Application Insights API key ①	
👾 Channels (Preview)		~
• Pricing	Application Insights Application ID 🛈	
Test in Web Chat	Application ID (Application Insights Application ID)	
A Encryption	Schema Transformation Version	
😂 Properties	V1.3	~
🔒 Locks	This determines how Bot Service converts messages sent between your bot and channels. Learn more	
Monitoring	No OAuth Connection settings defined	
Gonversational analytics	Add OAuth Connection Settings	
Alerts		
Metrics 🗸	Apply Discard changes	

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.

Home > Support-Dispatcher > Support	t-Dispatcher			Add a client se	cret	×
💡 Support-Dispatcher	· Certificates & secrets ≉			Description	chime	
₽ Search (Ctrl+/) «	♡ Got feedback?			Expires	Custom	
Uverview	scheme), i or a higher lever or association, we re	commenta using a cer	runcate (more	Start	09/28/2021	Ē
 Quickstart Integration assistant 	Certificates			End	09/28/2023	
Manage	Certificates can be used as secrets to prove the	application's identity	y when reque			
🔤 Branding	↑ Upload certificate					
Authentication	Thumbprint		Start d			
📍 Certificates & secrets	No certificates have been added for this applic	ation.				
Token configuration						
 API permissions 						
Expose an API	Client secrets					
App roles	A secret string that the application uses to pro	ve its identity when re	equesting a t			
A Owners	+ New client secret					
Roles and administrators Preview	Description	Expires	Value			
 Manifest Support + Troubleshooting 	No description	9/27/2026	LVa***			
<i>Troubleshooting</i>						
New support request				Add Cancel]	

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.

CHIME			Home	My Guest Dashboard	My Agent Dashboard	My Manager Home 👻	Admin	0.
😻 Health Monitor	New Dispatcher							
嶜 People	Q Search Active Directory The dispatcher account in	the entry point fo	r a queue. Users can contact this	s account to connect with	agents. This account mus	t be unique.		
≓ Dispatchers	Account Settings		Chime Settings					
0° Settings	Bot ID		Description					
View Archived	Bot ID							
>_ Control Panel	Webchat Secret		Dienstcher Tyne					
Virtual Agents	Bot Name		Testing					•
External Bots	Bot name		Queue					
	Bot Secret		Not assigned					
	Bot Secret	Password						
	Email Address							
	Email Address							
						40 mm	autore D.C	
						Turner Venty S	ettings 835	ave

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:

CHIME					Home My Guest Dashboard	d My Agent Dashboard	My Manager Home +	Admin
Queue Settings Eric Bot						Learn	more about these setting	ngs 🗶
Basic	People	Virtual Agents	Text Resources	Rout	ting	Schedule	Advanced	
Queue Properties			Engi	ine Properties				
Name			A	Changes to these settings may	cause the queue to restart. Any acti	ive sessions may be dropped.		
Description			Licen	se				
				a _{e Licen}	sed for (3) users until 12/31/2020	♣ ⁴ Alerting enabled for 25 re	ecipients	œ
Language		Web Client	Queu Dispa	Queue Bot Messaging Endpoint Dispatcher and alias Bot Framework bots assigned to this queue below should be directed to this URL in the Azure Portal				
English	•	Default Web Client	•	Internet former and and former and another and the set of the				
Guests can request chat transcripts	Guests can request chat transcripts Publish to Home Page			e Dispatcher				R
Send chat transcripts via email		Show Chat Links on Home Page	Di	Direstehar Alisser				
Off		Both	* Bot	porter conses	▲Bot ID			Remove
A Download Teams App Package			100	Name, Box, 1982	11-160 - 161 - Kap 17-16 - 16	1		
			Res.	Same, Brit, MC	1011 C 100 D 100 D			
		₽¢		► Start		Stop	C Restart	
							1	. Down
						A Quede Dashboard	U Res	a save

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 - Overvier	w > ChimeBot2 - Settings
ChimeBot2 - Settings Bot Channels Registration	
,> Search (Ctrl+/)	R Save X Discard
Ø Overview	Bot profile
Activity log	lcon
🝰 Access control (IAM)	⟨→ Upload custom icon
🛷 Tags	30K max, png only
Pot management	* Display name 🕐
bot management	(hmdet)
Test in Web Chat	Bot handle 👩
iii Analytics	ChimeBot2
Channels	Description 💿
Settings	
Ispeech priming	
 Bot Service pricing 	
Support + troubleshooting	Configuration
New support request	Messaging endpoint
	 Microsoft App ID (Manage) 0
R	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