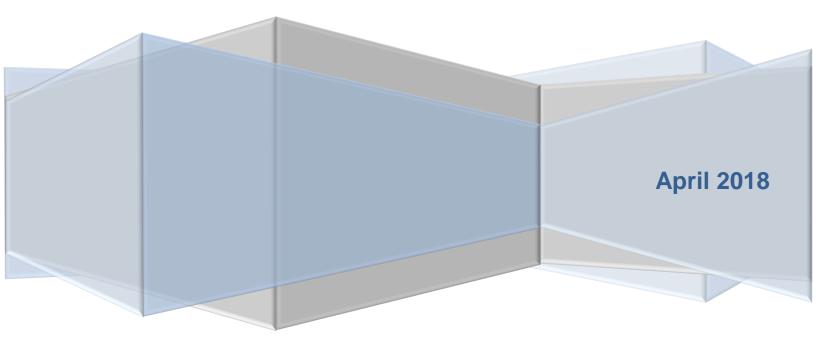


# **Chime Office 365 Prerequisites**



#### **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 - 2018 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

Configuring Azure AD Access for Chime for Lync
Prerequisites:4
Configure Active Directory Authentication5
Retrieve your Azure Tenant ID5
Create Application5
Create the Chime Application6
Configure the Application6
Configure Application Permissions7
Create a New API Key9
Azure Active Directory Accounts List
Configure UCWA Connection11
Create the New Application11
Configure Manifest
Configure the Application Permissions12
SSL Certificate
Setup Before Chime Install14
Setup After Chime Install14

### CONFIGURING AZURE AD ACCESS FOR CHIME FOR LYNC

Chime for Skype for Business Online (Office 365) requires the configuration of two Azure applications in order to allow Chime to leverage Office 365 for user authentication, and to communicate with your Skype for Business 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.

Sign into the Azure AD portal (<u>https://portal.azure.com</u>). Select the **Azure Active Directory** in the left-hand navigation pane.

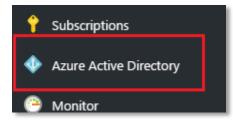


Figure 1 – Begin Setting up Active Directory

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 rese	« ource	All services	Filter	By category ~		
i∃ All services		IDENTITY (13)				
— 🛨 Favorites —			ve Directory	☆	4	Azure AD B2C
🔲 Dashboard		Azure Info	rmation Protection	*	:	Groups
All resources		Nzure AD 🤇	Connect Health	*	2	Azure AD Cloud App Discovery
📦 Resource gr	oups	\land Azure AD I	Identity Protection	*	14	Enterprise applications
🔇 App Service:	;	Access revi	iews	*		



## CONFIGURE ACTIVE DIRECTORY AUTHENTICATION

### RETRIEVE YOUR AZURE TENANT ID

### II Properties

- 1. Select in the navigation pane in the **Azure Active Directory** blade.
- 2. Copy the **Directory ID** from the field, and save it somewhere convenient. You will need this value when configuring Chime.

* Name
Your Company
Country or region
United States
Datacenter region
United States
Notification language
English 🗸
Directory ID
someguidvaluehere

Figure 3 – Copy Directory ID

CREA	TE APPLICATION	
1.	Select App Registrations i	n the new navigation pane within the <b>Azure Active Directory</b> blade.
		App registrations
2.	Click the New application	registration option in the Azure Active Directory blade.

instant technologies - App regist Azure Active Directory	rations	
	New application registration	🗄 Endpoints 🛛 🗙 Troubleshoot
Overview     Quick start	To view and manage your registra Search by name or AppID DISPLAY NAME	ations for converged applications, please v

Figure 4 – Create New Application Registration

### CREATE THE CHIME APPLICATION

- 1. Create a name for this application (Chime is a suitable name)
- 2. Select Web App / API as the type
- 3. Enter the URL for the server that Chime will be hosted on, with the /Chime route in the URL (ex: <a href="https://yourserver.domain.com/Chime">https://yourserver.domain.com/Chime</a>)

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

Create –		×
* Name 🛛 Chime	~	]
Application Type <b>0</b>		
Web app / API	۷	]
* Sign-on URL 🛛		
https://yourwebserver.domain.com/Chime	~	]

Figure 5 – Create the Chime Web App / API

4. Click the

button in the bottom of the Create blade.

### CONFIGURE THE APPLICATION

Create

- 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. Record the Application ID. This value will be used when configuring Chime.

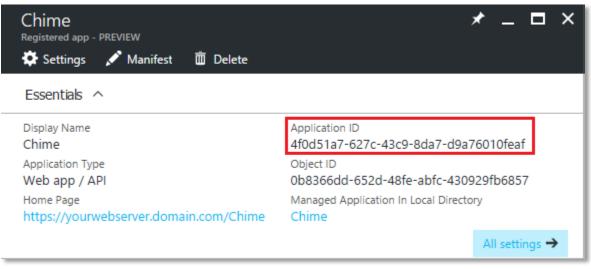


Figure 6 – Record Application ID

### CONFIGURE APPLICATION PERMISSIONS

- 1. Click the **Settings** button in the preview.
- 2. Click on the **Required permissions** option in the **Settings** blade

Settings PREVIEW	_ 🗆 ×
○ Filter settings	
GENERAL	
Properties	>
🚝 Reply URLs	>
Owners	>
API ACCESS	
Required permissions	>
📍 Keys	>

Figure 7 – Access Required Permissions

3. Click Windows Azure Active Directory in the list of APIs in the Required permissions blade

Required permissions PREVIEW Add		_	<
API	APPLICATION PER	DELEGATED PERM	
Windows Azure Active Directory (Microsoft.Azure.ActiveD	0	1	



- 4. Configure the required permissions
  - a. Click the checkbox to enable the ability to **Read Directory Data** in Application Permissions. *This will allow Chime to use this application to perform lookups and searches against your Azure Active Directory instance.*
  - b. Verify that the checkbox to Sign in and read user profile is checked in Delegated permissions
  - c. Click Save in the Enable Access blade once the settings are configured.

Enable Access Microsoft Azure ActiveDirectory - PREVIEW R Save 🛍 Delete	_ <b>-</b> ×
APPLICATION PERMISSIONS	^ REQUIRES ADMIN ^
Read all hidden memberships	🔮 Yes
Read and write devices	🔮 Yes
Read and write directory data	🔮 Yes
Read and write domains	🔮 Yes
✓ Read directory data	🥑 Yes
DELEGATED PERMISSIONS	REQUIRES ADMIN
Read hidden memberships	🕑 Yes
Sign in and read user profile	O No

Figure 9 – Configure Required Permissions

- 5. Close the **Required permissions** blade.
- 6. Click **Keys** in the **Settings** blade.

Setti			×
, <i>P F</i>	ilter settings		
GENE	RAL		
H	Properties	>	
≔	Reply URLs	>	
2 <b>8</b>	Owners	>	
API A	CCESS		
ሔ	Required permissions	>	
Ŷ	Keys	>	

Figure 10 – Setup Keys

### CREATE A NEW API KEY

- 1. Enter a name for the key
- 2. Select a duration for this API key.
- 3. Click **Save** to create a new API key.
- 4. Copy the newly created API key somewhere you can retrieve it. You will need this API key when configuring the Chime application

Keys PREVIEW R Save X Discard			_ 🗖 ×
▲ Copy the key val	ue. You won't be able to	retrieve after you leave this blade.	
DESCRIPTION	EXPIRES	VALUE	
Chime	12/31/2299	oMNrnPyDSSdHLrTarlB5YodsfPdtdelhOpUv6lhIOUQ=	
Key description	Duration	✓ Value will be displayed on save	

Figure 11 – Setup API Key

### AZURE ACTIVE DIRECTORY ACCOUNTS LIST

Setup Azure AD Connection X
Azure AD Tenant:
Azure AD Tenant ID:
Azure AD ClientID:
Azure AD Client Secret Key:
Test
Save

Figure 12 – 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 3 (Directory ID)

# Azure AD Client ID

This value is from Page 5 (Application ID)

# Azure AD Client Secret Key \_\_\_\_\_

This value is from Page 8

### CONFIGURE UCWA CONNECTION

The UCWA connection is required in order for Chime to login and connect to Skype for Business on behalf of the dispatcher accounts.

### CREATE THE NEW APPLICATION.

#### App registrations

1. Click

in the Azure Active Directory blade.

- 2. Click to create the new application.
- 3. Enter a name for the application (Chime UCWA Connector)
- 4. Choose Native as the application type
- 5. Enter a reply URL. This should be your Chime server, but this is not currently used within the Chime application.

Create –		
* Name 🖲		
Chime UCWA Connector	~	1
	•	1
Application Type <b>0</b>	~	]
Application Type <b>0</b>	~	]

#### Figure 13 – Create New App Registration

- 6. Click
- Create at the bottom of the Create blade
- 7. Record the Application ID. This will be required when configuring Chime (Skype SDK ID)

Chime UCWA Connector Registered app - PREVIEW	* _ ¤ ×
🍄 Settings 💉 Manifest 🗴 🟛 Delete	
Essentials ^	
Display Name Chime UCWA Connector	Application ID 35ce41a9-06af-4016-a9bf-c2d9018cef84
Application Type Native	Object ID 8c71a58b-22e2-4dd4-ab1a-3e7b182ca887
Home Page	Managed Application In Local Directory Chime UCWA Connector
	All settings 🗲



### CONFIGURE MANIFEST

4.

- 1. Click Manifest in the application blade
- 2. Find the value for **oauth2AllowImplicitFlow** NOTE: This should be around line 13
- 3. Change the value from false to true



### CONFIGURE THE APPLICATION PERMISSIONS

- 1. Click the Settings button in the Edit manifest blade
- 2. Click Under API ACESS in the Settings blade.
- 3. Click **Add** in the **Required permissions** blade
- 4. Click Select an API in the Add API access blade

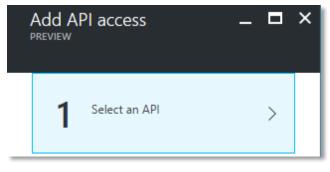


Figure 15 – Setup Required Permissions for App Registration

5. Search for the required API using the searing input field in the pane. You will need to search for Microsoft.Lync

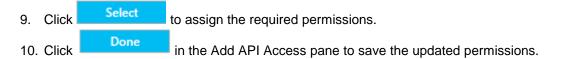
Select an API PREVIEW	_   ×
Microsoft.Lync	✓
Skype for Business Online (Micros	oft.Lync)



- 6. Select Skype for Business Online (Microsoft.Lync) in the API list
- 7. Click
- Select 8. Select the required permissions

Enable Access PREVIEW		-		×
	^	REQUIRES ADMIN	^	
✓ Read/write Skype user contacts and groups		🥑 Yes		
Receive conversation invites (preview)		🥑 Yes		
✓ Read/write Skype user information (preview)		🕑 Yes		
✓ Create Skype Meetings		🕑 Yes		
✓ Initiate conversations and join meetings		🕗 Yes		

#### Figure 17 – Select Required Permissions



### SSL CERTIFICATE

#### SETUP BEFORE CHIME INSTALL

To set up a Chime deployment with Office 365, you will need to acquire a SSL certificate. This certificate will be installed on the server on the same server that the Chime instance will be on. Without this certificate installed, no users will be able to authenticate into the web app.

### SETUP AFTER CHIME INSTALL

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 Direct
ž	Configure SQL Provide access to SQL Database
D	Setup Web Client Setup the Chime On-Premise Web client (optional)
nstant	Setup Web Client Setup the Chime Office 365 Web client (optional)
⊒_₀	Pick Admin Pick a user as an administrator for Chime
	5 Setup SSL Reset SSL Setup HTTPS and SSL support (OPTIONAL for On-Premise)
	6 Chime for Lync Service Start Stop 5100
	Further documentation and setup information can be found at http://addchime.com/fac.html
	Cose
	Cose

Figure 18: Configuration Wizard

Once the certificate has been installed on the server, you can follow these steps.

- 1. Click Setup SSL.
- 2. Click through the prompts to register listeners for ports 80 and 443 (or click OK if already reserved).



Figure 19: URL Reservations

 Select the desired SSL Certificate from the list provided. Click on the desired certificate and click OK to try and use that certificate. If you don't see the certificate desired, click Cancel, and another list will be displayed.

Windows Security	Windows Security X
Select SSL Certificate Select the SSL certificate you would like to use with Chime for Lync	Select SSL Certificate
Instant-tech-VINSTANTTEC	Select the SSL certificate you would like to use with Chime for Lync
<u>Click here to view certificate.</u> properties	Instant tech wildcard
The USERTrust Network™ Issuer: AddTrust External CA Root Valid From: 5/30/2000 to 5/30/2020	Issuer: DigiCert SHA2 Secure Server
DigiCert Issuer: DigiCert Assured ID Root CA	Valid From: 1/19/2016 to 1/24/2017
Valid From: 11/9/2006 to 11/9/2031 Go Daddy Class 2	Click here to view certificate properties
Certification Authority Issuer: Go Daddy Class 2 Certification Authority	
Valid From: 6/29/2004 to 6/29/2034	OK Cancel
OK Cancer	

Figure 20: Selecting SSL Certificates

4. Click to OK to execute the command to register the SSL Certificate.

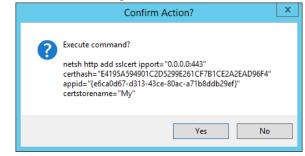


Figure 21: Executing SSL Command

5. The SSL certificate has now been successfully linked to Chime and users will be able to authenticate into the web application.