

instant

CHIME

## Chime Office 365 Prerequisites

April 2018

## 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 .....	4
Prerequisites:.....	4
Configure Active Directory Authentication .....	5
Retrieve your Azure Tenant ID .....	5
Create Application .....	5
Create the Chime Application .....	6
Configure the Application .....	6
Configure Application Permissions .....	7
Create a New API Key.....	9
Azure Active Directory Accounts List .....	10
Configure UCWA Connection .....	11
Create the New Application .....	11
Configure Manifest .....	12
Configure the Application Permissions.....	12
SSL Certificate .....	14
Setup Before Chime Install.....	14
Setup After Chime Install.....	14

## 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:

- You must have an Office365 tenant for your organization.
- You must be an administrator of your Office 365 domain.
- 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 (<https://portal.azure.com>).  
Select the **Azure Active Directory** in the left-hand navigation pane.

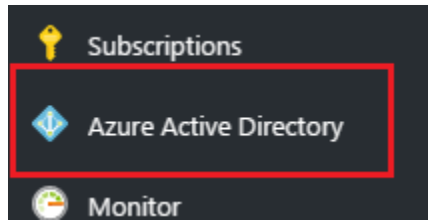


Figure 1 – Begin Setting up Active Directory

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**

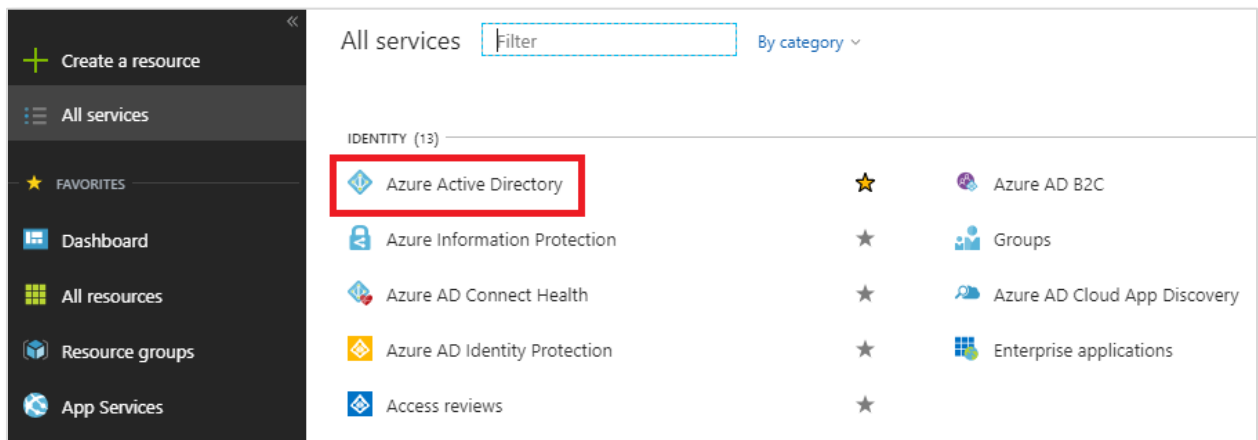

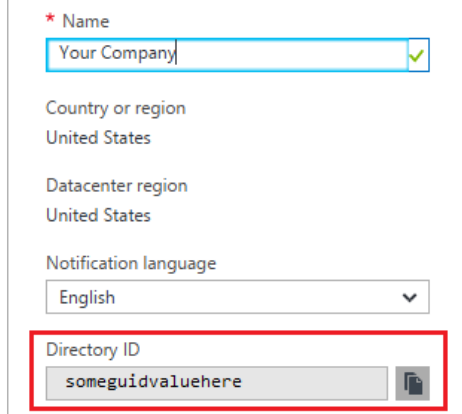


Figure 2 – Secondary Option to Active Directory Setup

## 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.



\* Name  
Your Company ✓

Country or region  
United States

Datacenter region  
United States

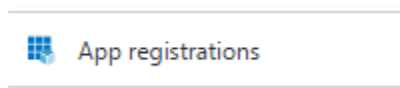
Notification language  
English ▼

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.

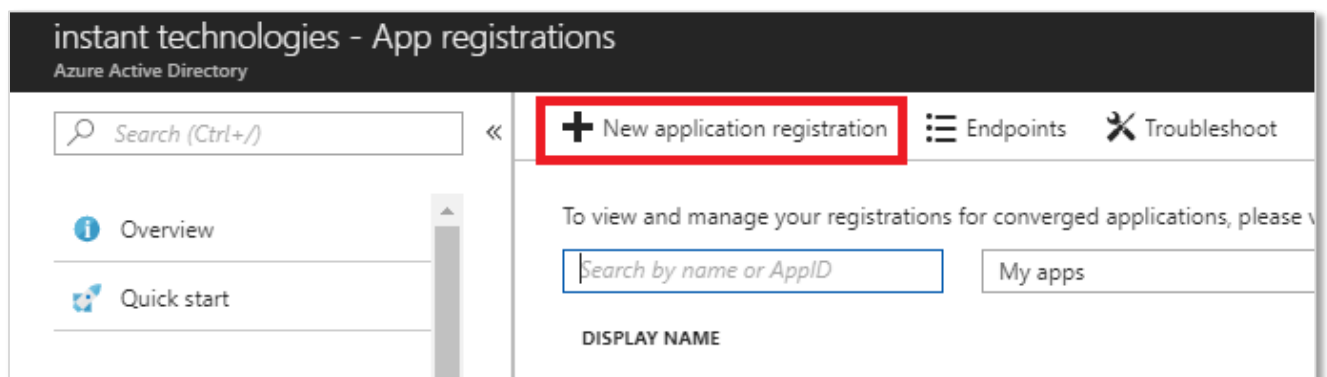


Figure 4 – Create New Application Registration

## 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: <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*

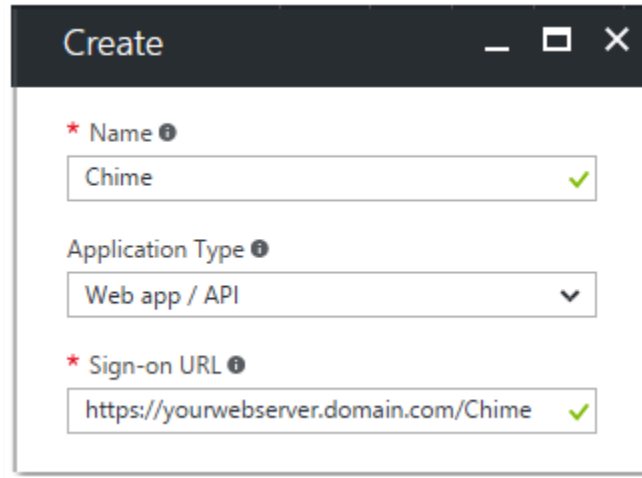


Figure 5 – Create the Chime Web App / API

4. Click the **Create** button in the bottom of the **Create** 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. Record the **Application ID**. This value will be used when configuring Chime.

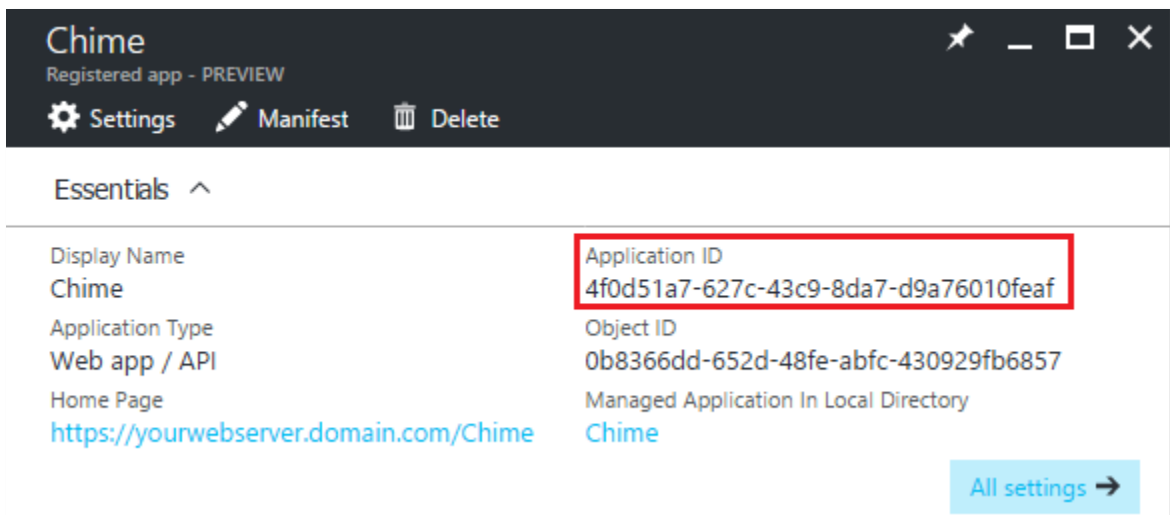


Figure 6 – Record Application ID

## CONFIGURE APPLICATION PERMISSIONS

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

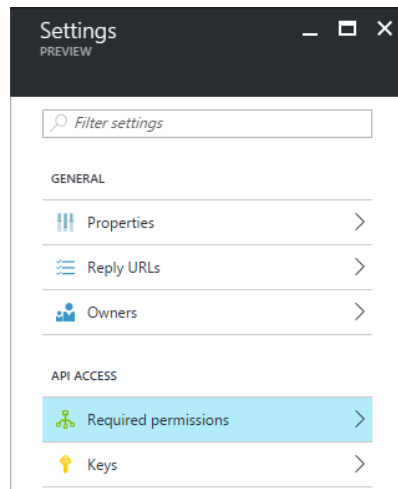


Figure 7 – Access Required Permissions

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

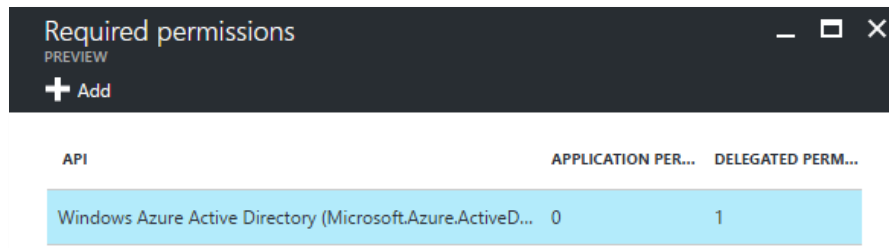


Figure 8 – Manage Required Permissions

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.

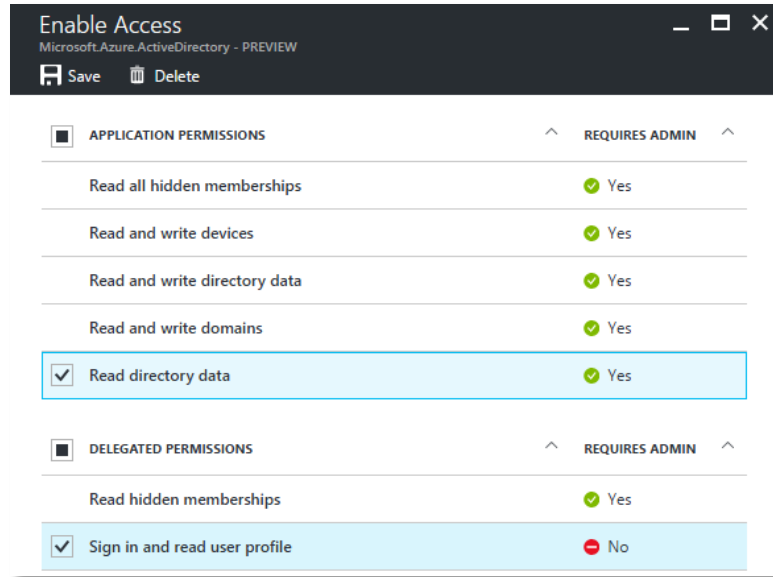


Figure 9 – Configure Required Permissions

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

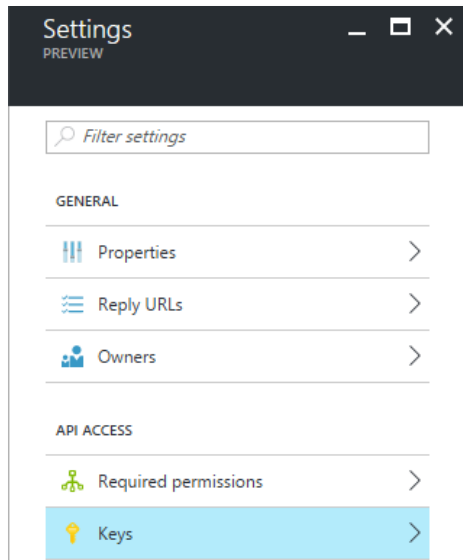


Figure 10 – Setup Keys



## 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

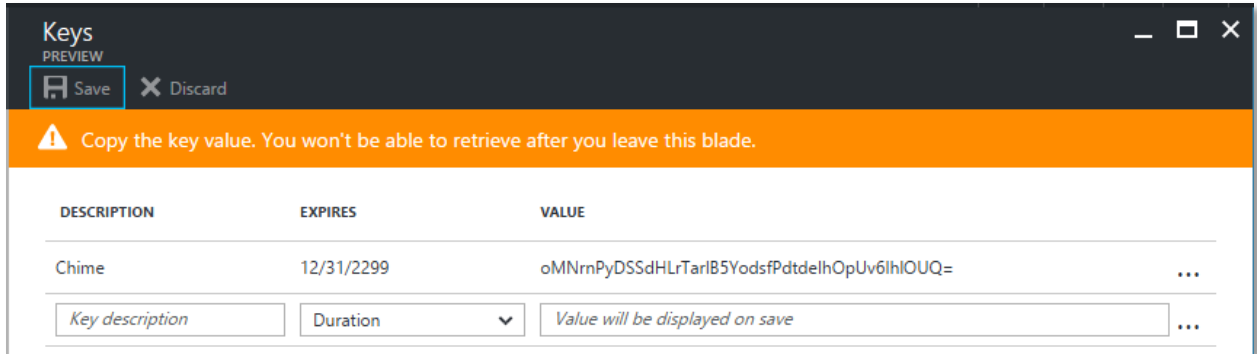
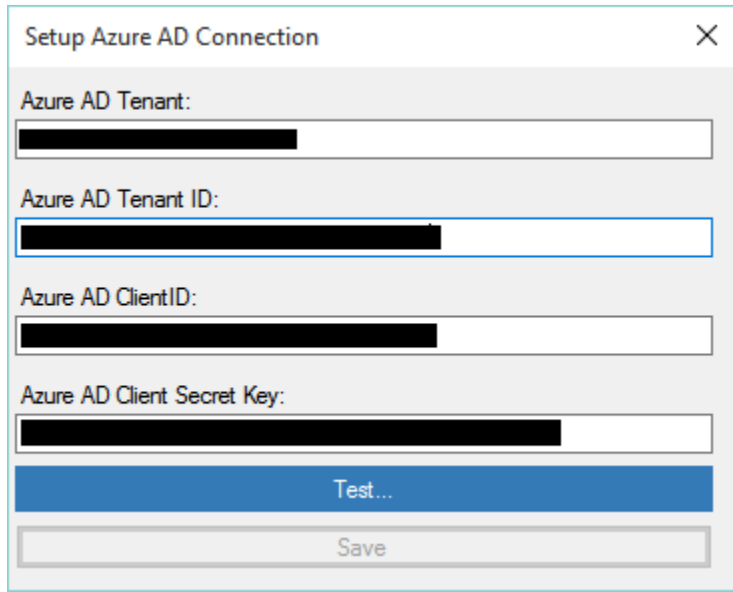


Figure 11 – Setup API Key

## AZURE ACTIVE DIRECTORY ACCOUNTS LIST



Setup Azure AD Connection

Azure AD Tenant:  
[Redacted]

Azure AD Tenant ID:  
[Redacted]

Azure AD Client ID:  
[Redacted]

Azure AD Client Secret Key:  
[Redacted]

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.

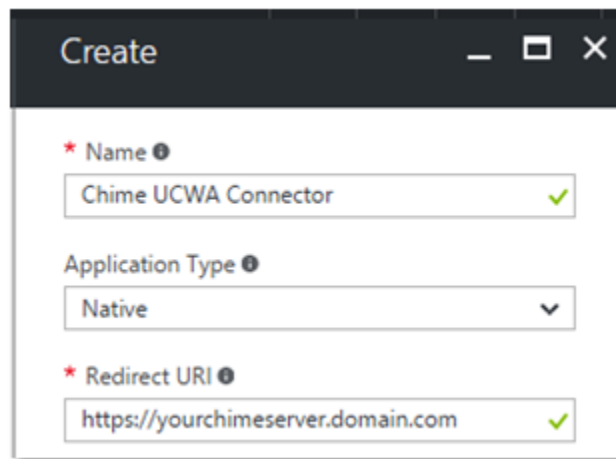



Figure 13 – Create New App Registration

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

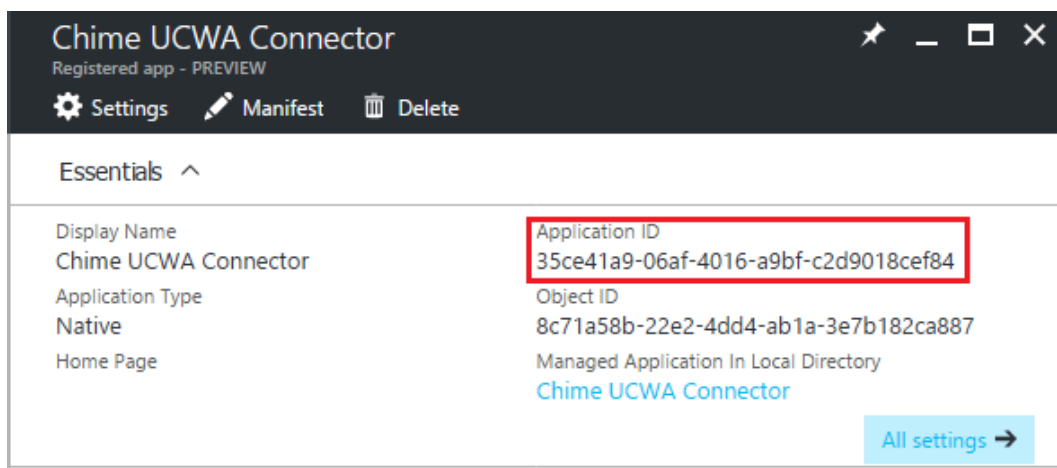
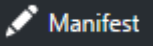


Figure 14 – Record Application ID

## CONFIGURE MANIFEST


1. Click  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**

```
13 "oauth2AllowImplicitFlow": true,
```

4. Click  in the Edit manifest blade

## CONFIGURE THE APPLICATION PERMISSIONS

1. Click the **Settings** button in the Edit manifest blade

 Required permissions >

2. Click > under API ACCESS in the Settings blade.

3. Click  in the **Required permissions** blade

4. Click **Select an API** in the Add API access blade

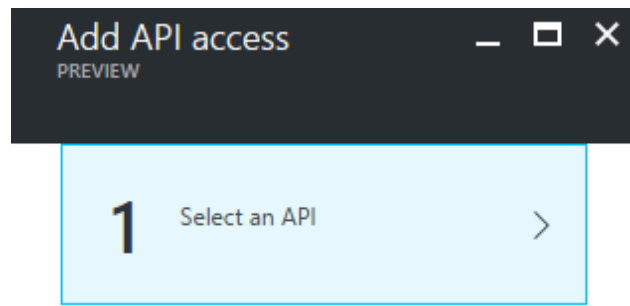


Figure 15 – Setup Required Permissions for App Registration

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

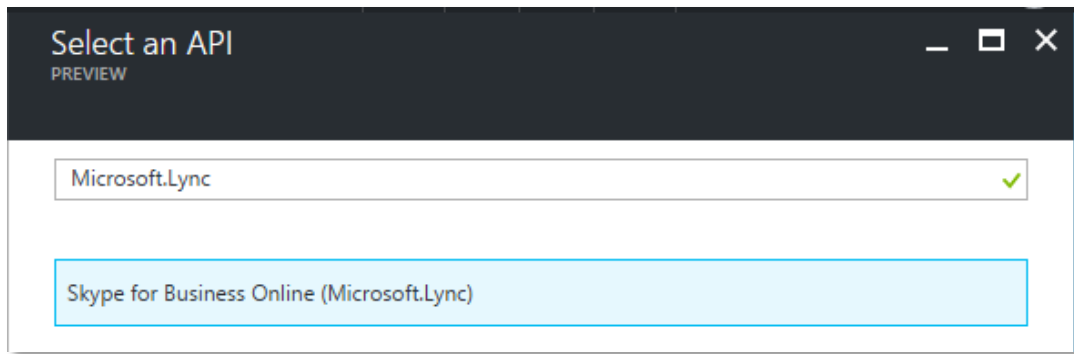


Figure 16 – Select Skype for Business API

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

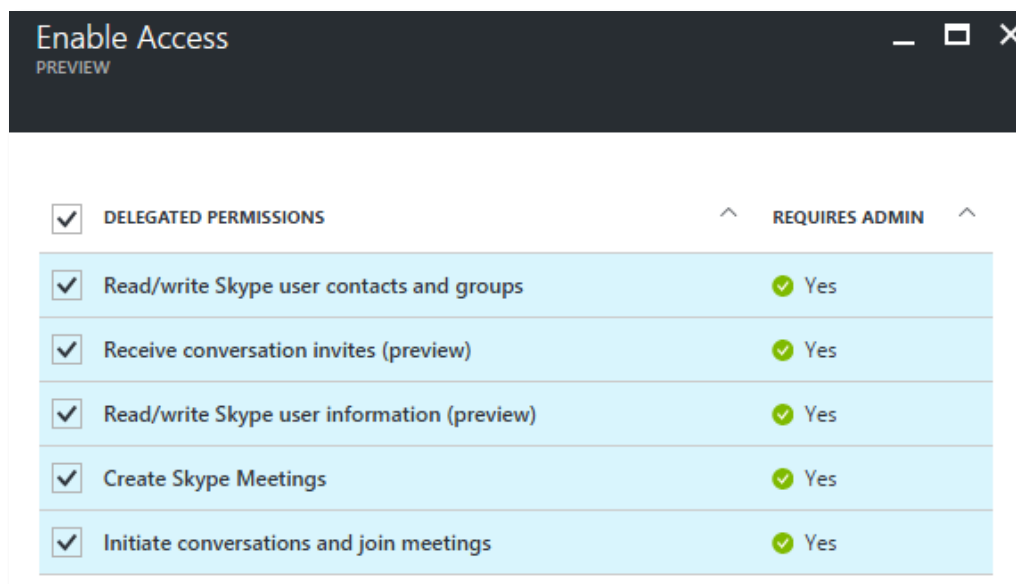


Figure 17 – Select Required Permissions

9. Click **Select** to assign the required permissions.
10. Click **Done** in the Add API Access pane to save the updated 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.

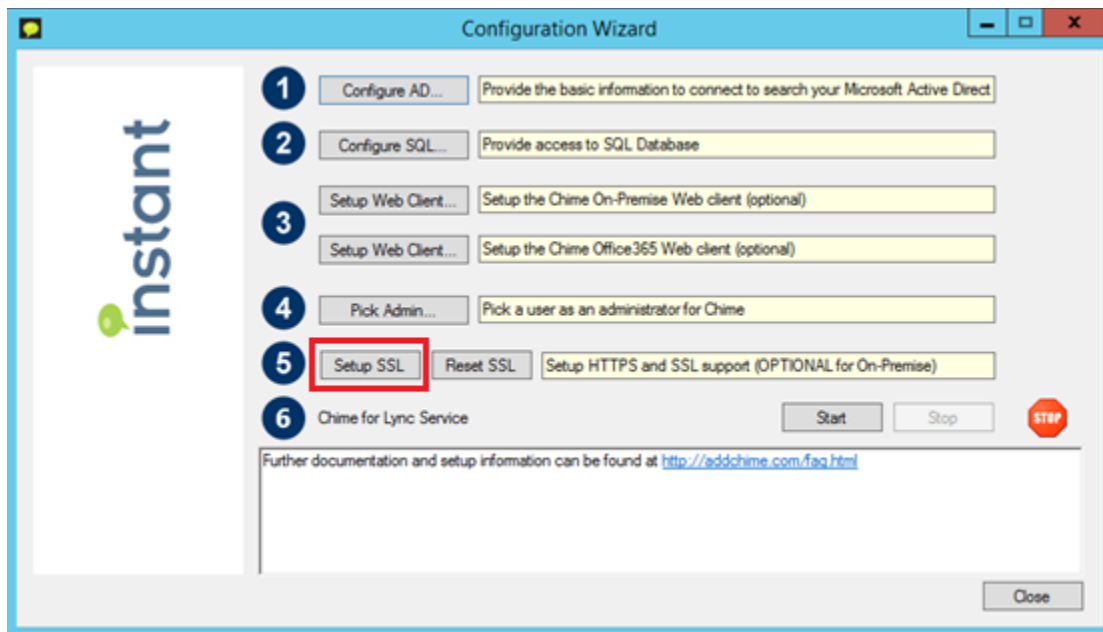


Figure 18: Configuration Wizard

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).

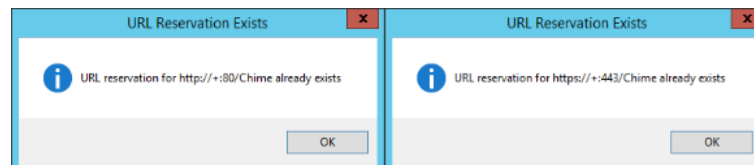


Figure 19: URL Reservations

3. 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.

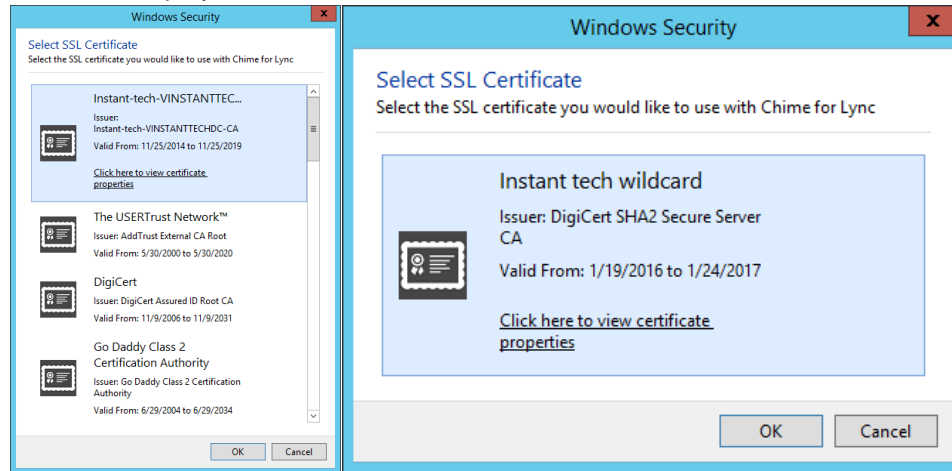


Figure 20: Selecting SSL Certificates

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

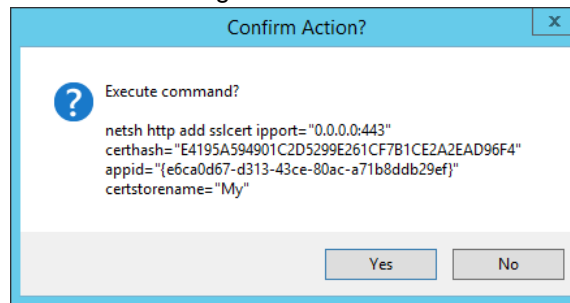


Figure 21: Executing SSL Command

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