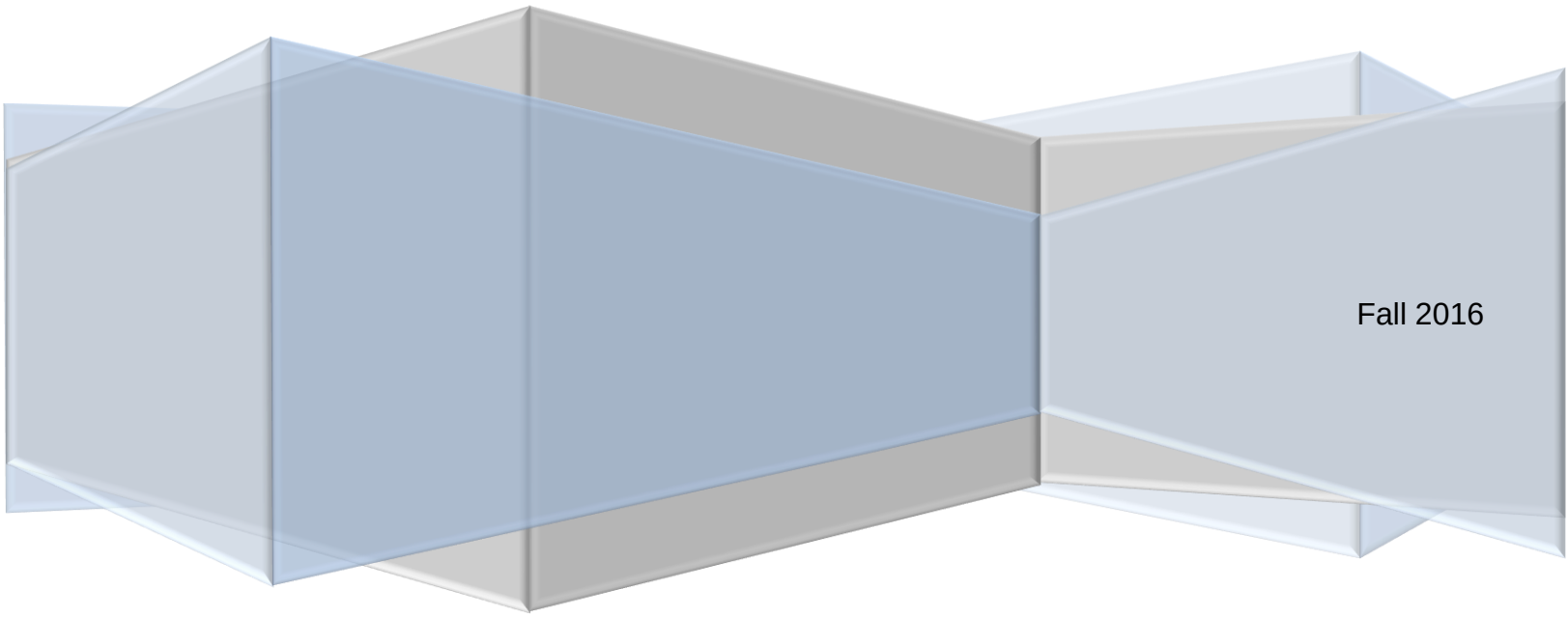
Chime Office 365 Prerequisites



Fall 2016

Copyright and Disclaimer

Trademarks

Contact Information

See our website for Customer Support information.

http://www.instant-tech.com/

Microsoft CERTIFIED Partner | ISV/Software Solutions

CONTENTS

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 (https://portal.azure.com).
Select the **Azure Active Directory** in the left-hand navigation pane.

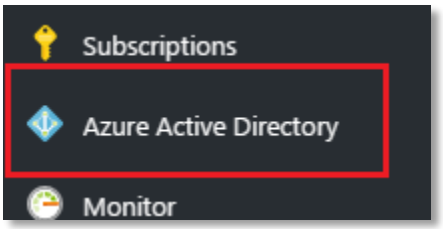
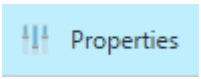


Figure 1

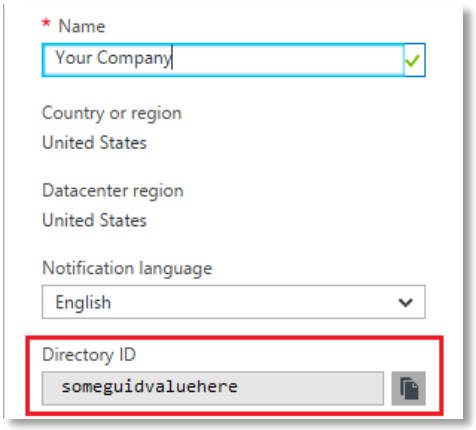
Dec 2, 2016
Rev 4 – PSM

CONFIGURE ACTIVE DIRECTORY AUTHENTICATION

RETRIEVE YOUR AZURE TENANT ID

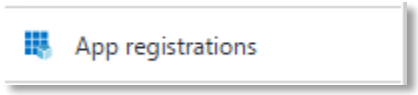
1. Select 

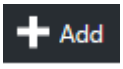
in the navigation pane in the **Azure Active Directory** blade.
2. Copy the **Directory ID** from the field, and save it somewhere convenient. You will need this value when configuring Chime.



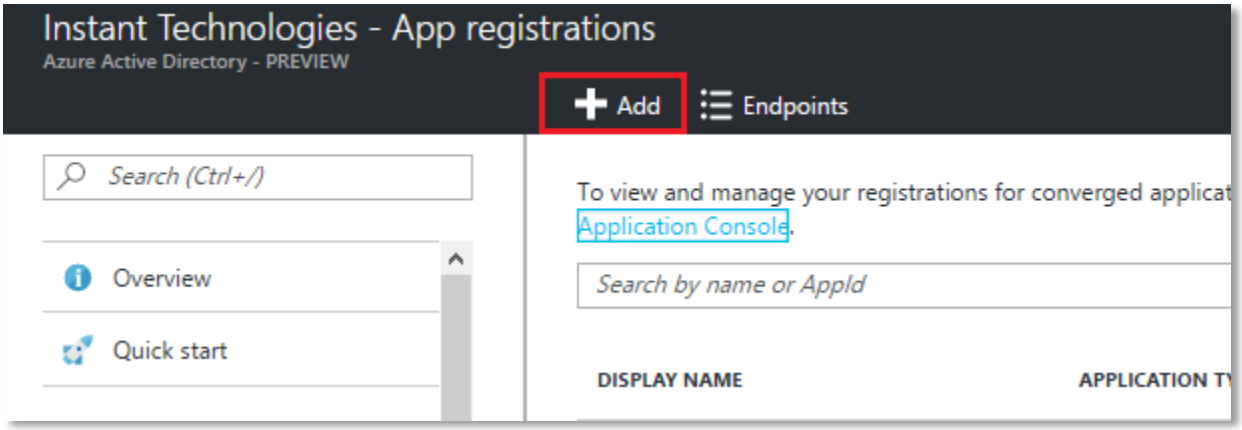
CREATE APPLICATION

1. Select **App Registrations** in the new navigation pane within the **Azure Active Directory** blade.



2. Click the 

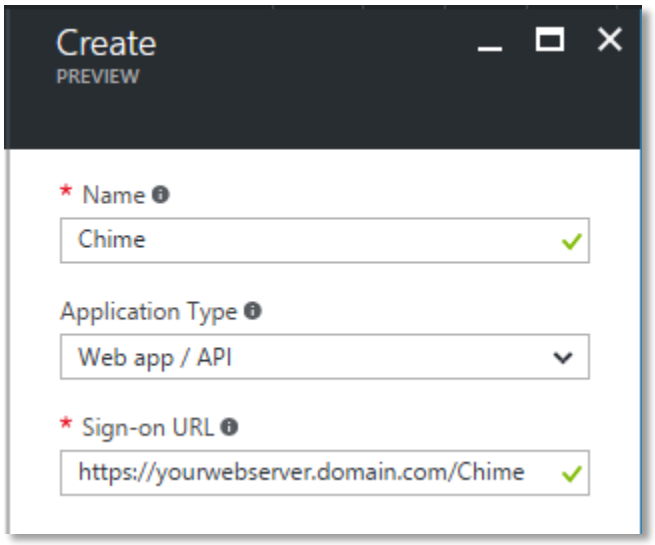
option in the **Azure Active Directory** blade.



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)

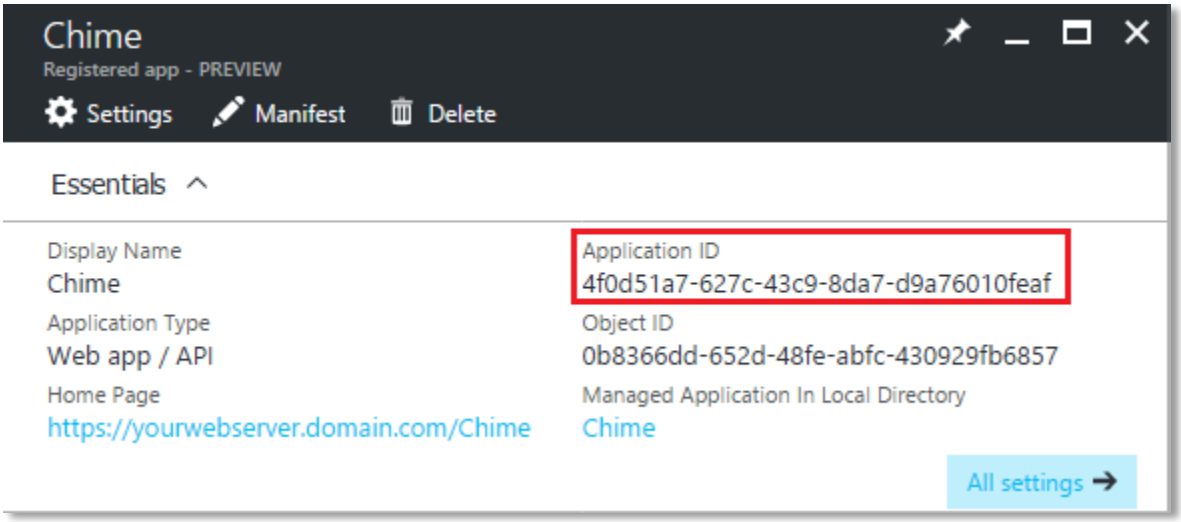
   NOTE: Be sure that the /Chime is included in the URL, this will automatically configure the Reply URL to correctly work with the Chime application



4. Click the  button in the bottom of the **Create** blade.

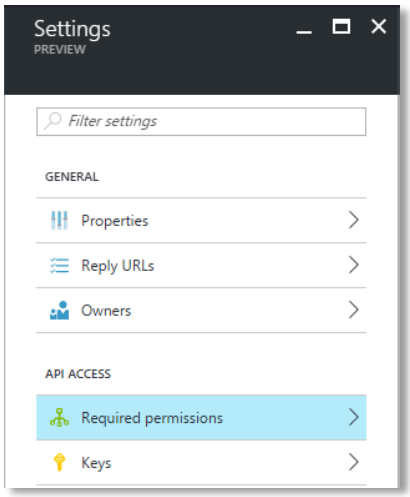
CONFIGURE THE APPLICATION

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.

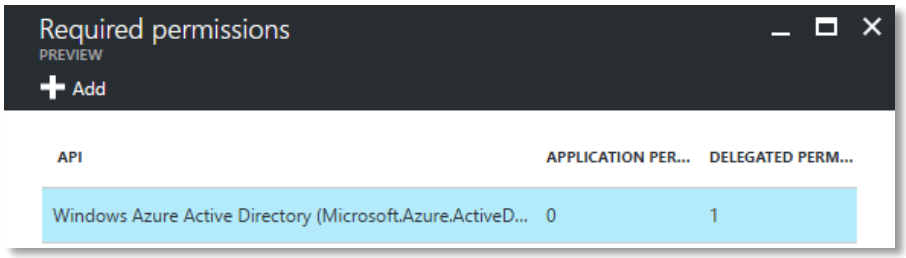


CONFIGURE APPLICATION PERMISSIONS

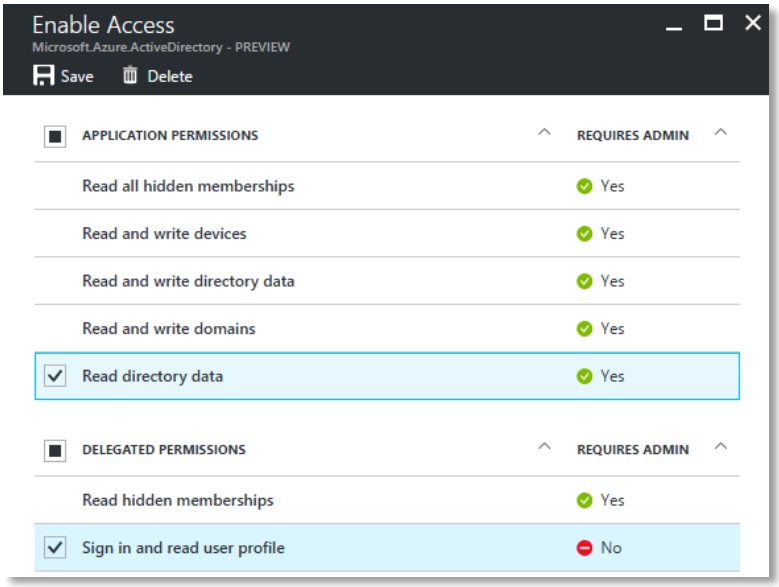
1. Click on the **Required permissions** option in the **Settings** blade



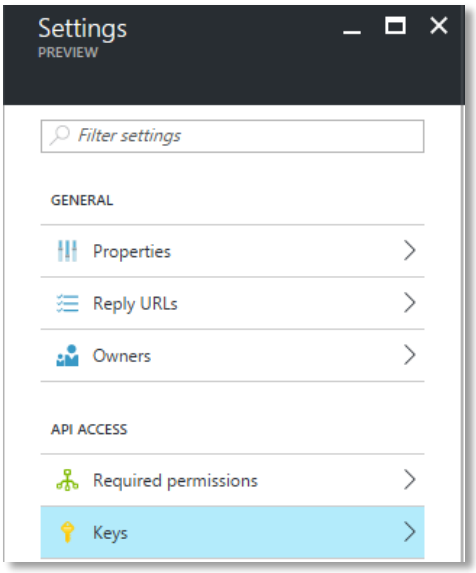
2. Click Windows Azure Active Directory in the list of APIs in the **Required permissions** blade



3. 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.

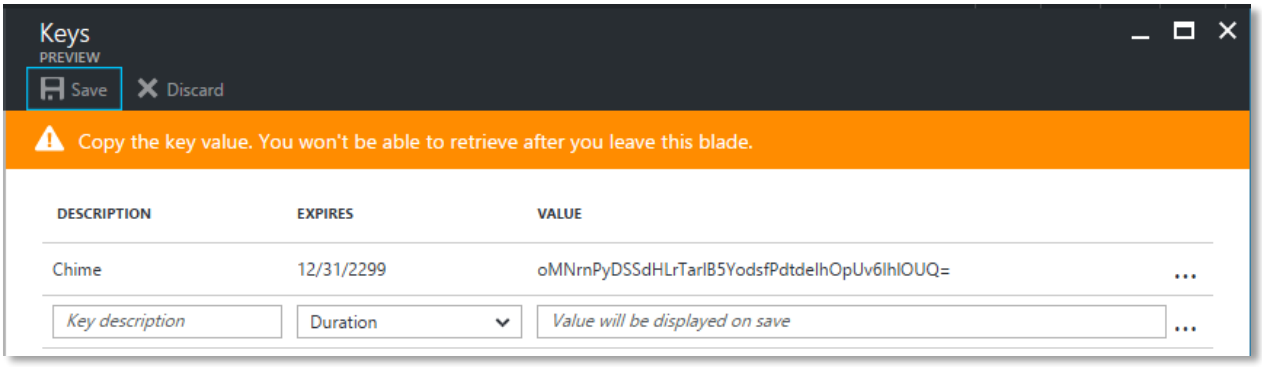


4. Close the **Required permissions** blade.
5. Click **Keys** in the **Settings** blade.

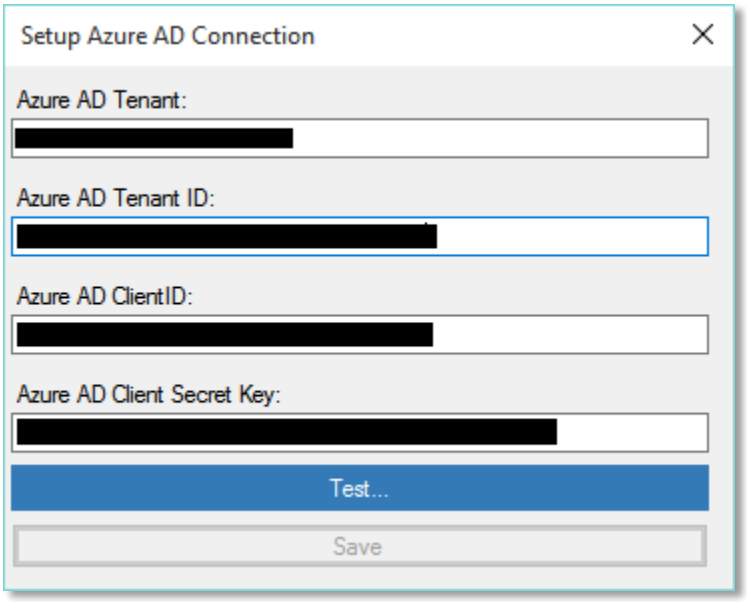


CREATE A NEW API KEY

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



AZURE ACTIVE DIRECTORY ACCOUNTS LIST



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)

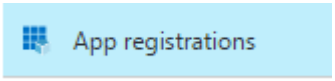
Azure AD Client Secret Key _____

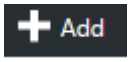
This value is from Page 8

CONFIGURE UCWA CONNECTION

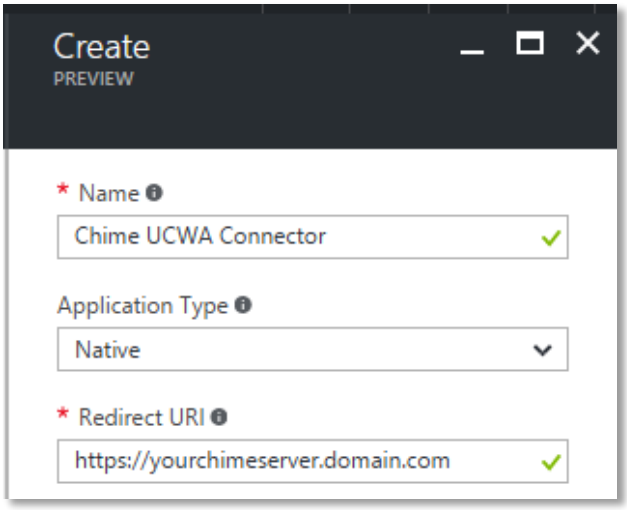
The UCWA connection is required in order for Chime to login and connect to Skype for Business on behalf of the dispatcher accounts.

CREATE THE NEW APPLICATION.

1. Click 

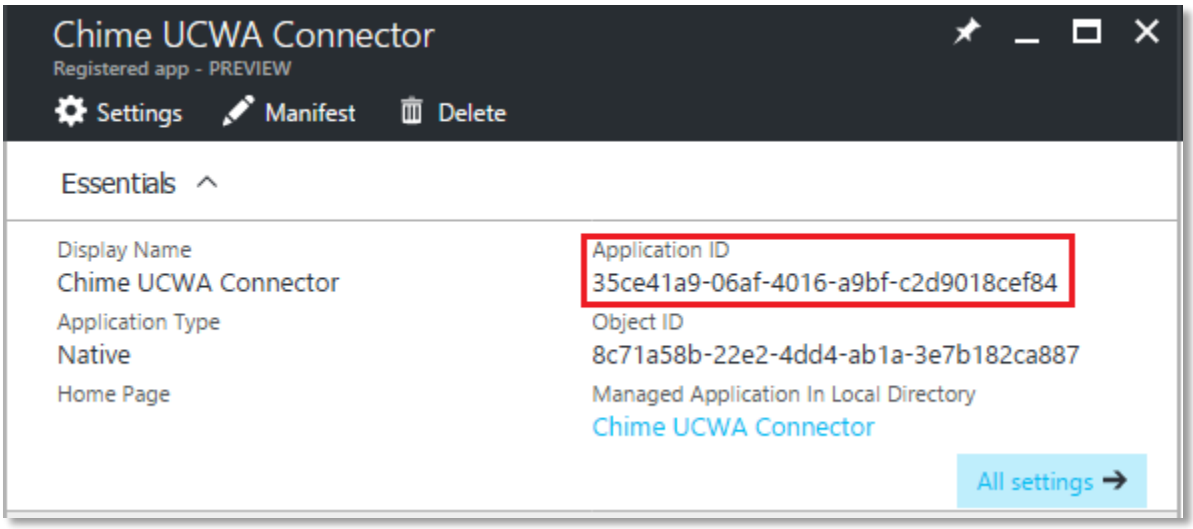
in the Azure Active Directory blade.
2. Click 

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.

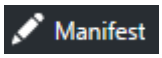


6. Click 

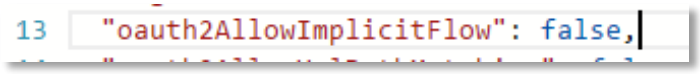
at the bottom of the Create blade
7. Record the **Application ID**. This will be required when configuring Chime (Skype SDK ID)



CONFIGURE MANIFEST

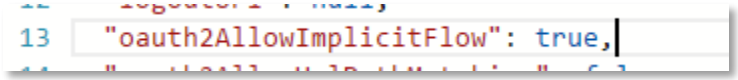
1. Click 

in the application blade
2. Find the value for **allowOauth2ImplicitFlow**



NOTE: This should be around line 13

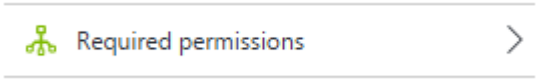
3. Change the value from **false** to **true**

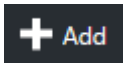


4. Click 

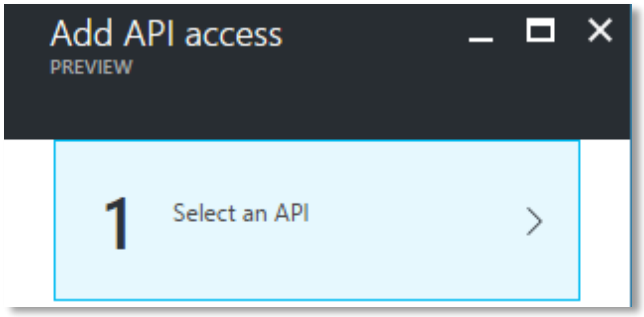
in the Edit manifest blade

CONFIGURE THE APPLICATION PERMISSIONS

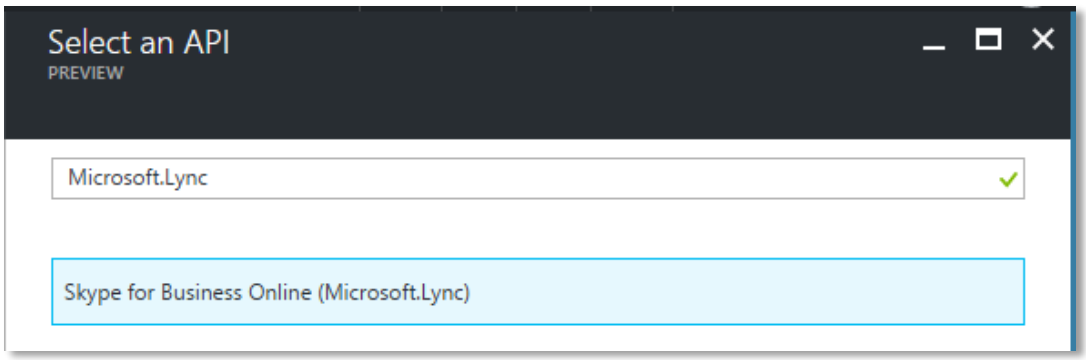
1. Click 

under API ACESS in the Settings blade.
2. Click 

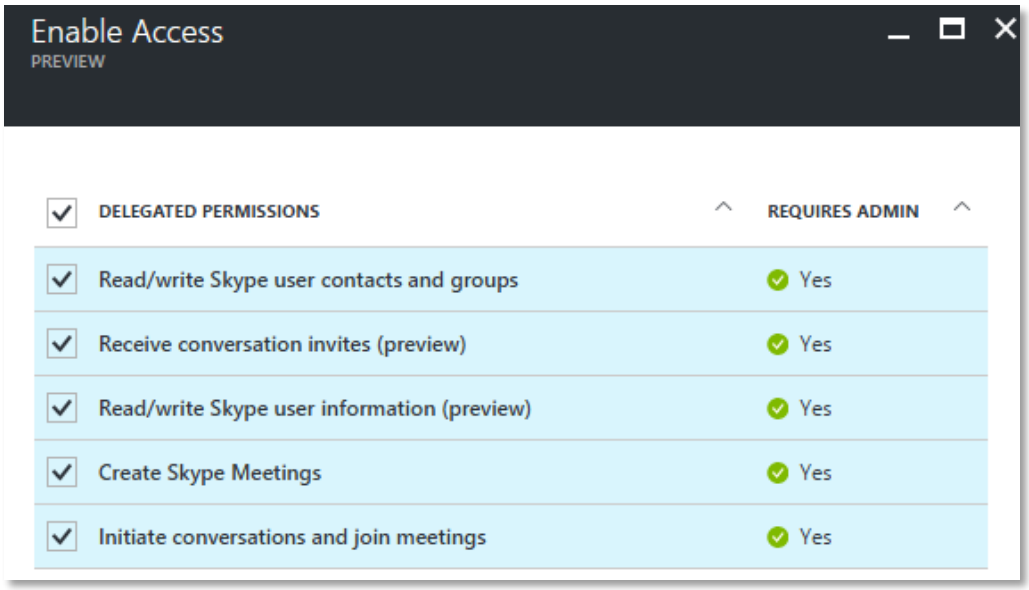
in the **Required permissions** blade
3. Click **Select an API** in the Add API access blade



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



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



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