

instant

CHIME

Chime Office 365 Prerequisites

Fall 2016

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 - 2016 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

Prerequisites:	3
Configure Active DirectORy Authentication	4
Retrieve your Azure Tenant ID	4
Create Application	4
Create the Chime application	5
Configure the Application	5
Configure Application Permissions	6
Create a new API key	7
Azure Active Directory Accounts List	8
Configure UCWA Connection	9
Create the new application	9
Configure Manifest	10
Configure the application permissions	10

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.

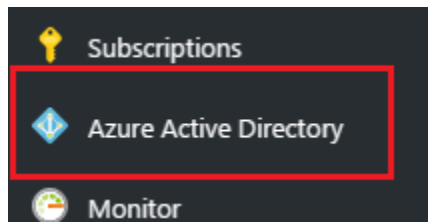

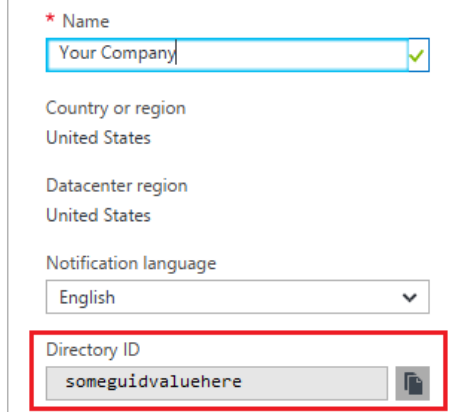


Figure 1

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

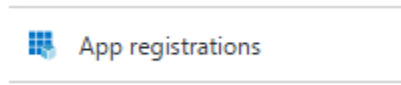
Datacenter region
United States


Notification language
English ▼

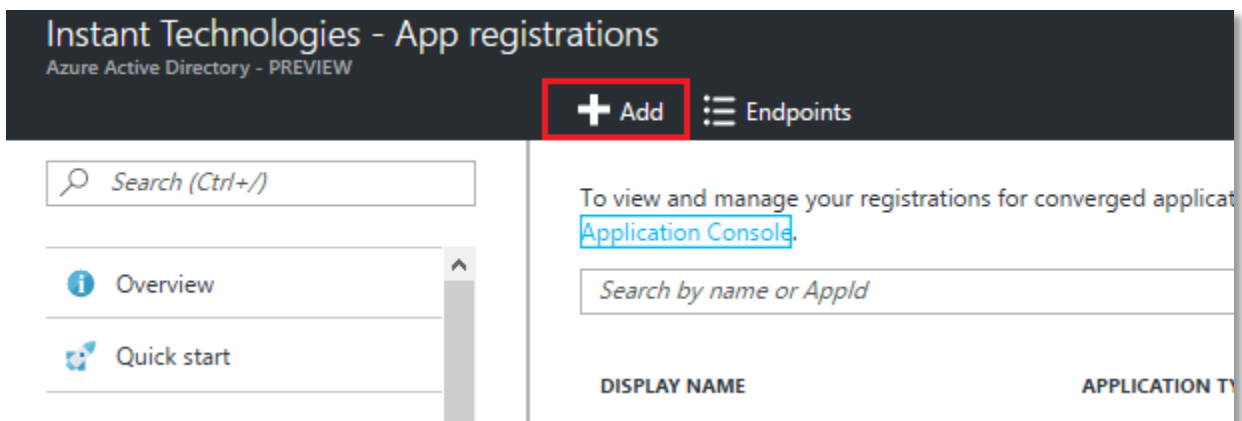
Directory ID
someguidvaluehere

CREATE APPLICATION



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



2. Click the  **Add** option in the **Azure Active Directory** blade.



Instant Technologies - App registrations
Azure Active Directory - PREVIEW

 **Add**  Endpoints

Search (Ctrl+/)

Overview

Quick start

To view and manage your registrations for converged applications, use the [Application Console](#).

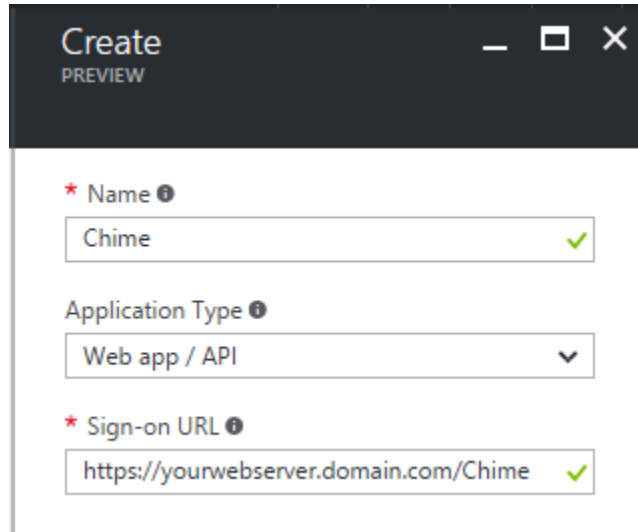
Search by name or AppId

DISPLAY NAME	APPLICATION TYPE
--------------	------------------

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>)

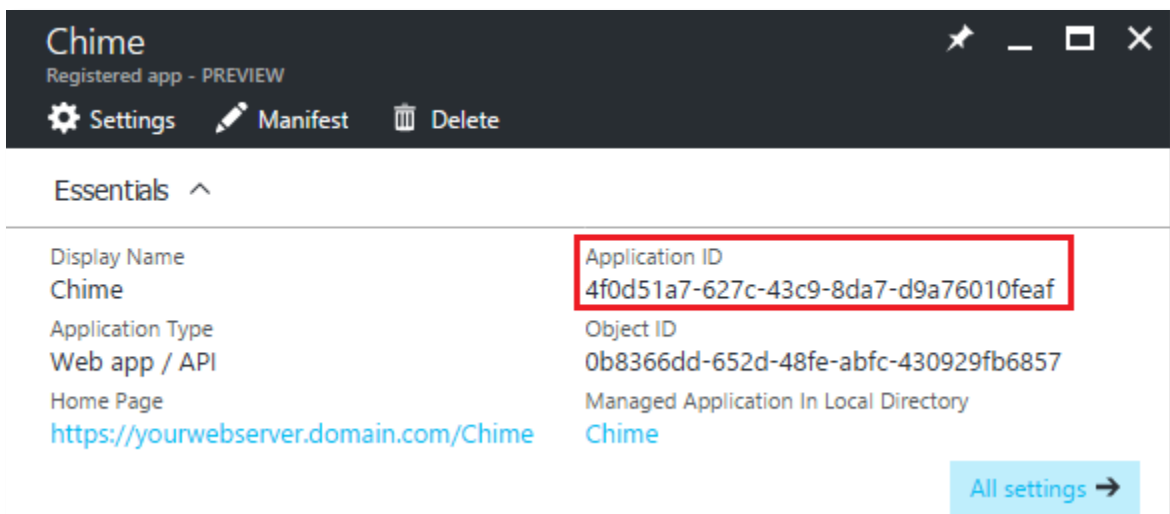
NOTE: Be sure that the /Chime is included in the URL, this will automatically configure the Reply URL to correctly work with the Chime application



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

CONFIGURE THE APPLICATION

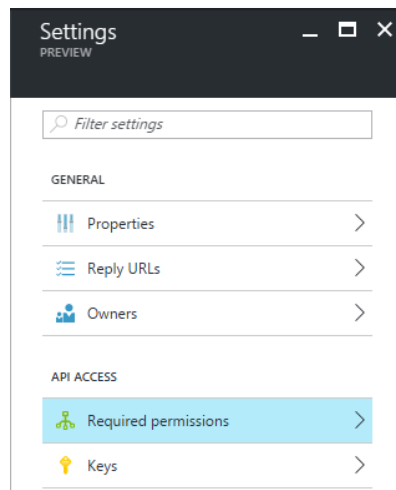
1. Click on the newly created application in the **App Registrations** blade. If you have many applications, you may need to search for it.
2. Record the **Application ID**. This value will be used when configuring Chime.



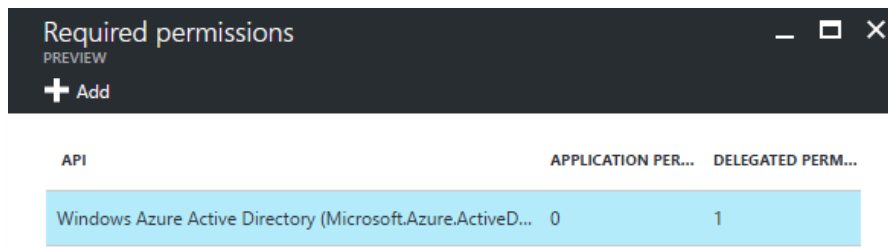
Display Name	Application ID
Chime	4f0d51a7-627c-43c9-8da7-d9a76010feaf
Application Type	Object ID
Web app / API	0b8366dd-652d-48fe-abfc-430929fb6857
Home Page	Managed Application In Local Directory
https://yourwebserver.domain.com/Chime	Chime

CONFIGURE APPLICATION PERMISSIONS

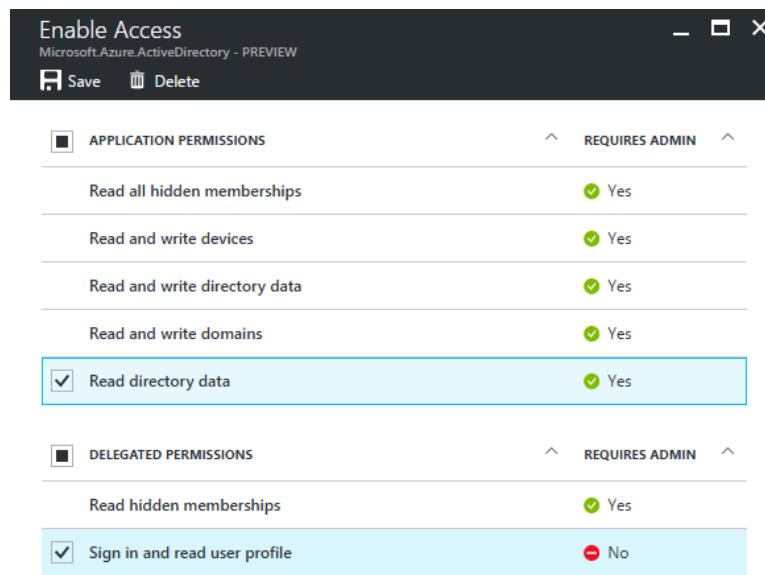
1. Click on the **Required permissions** option in the **Settings** blade



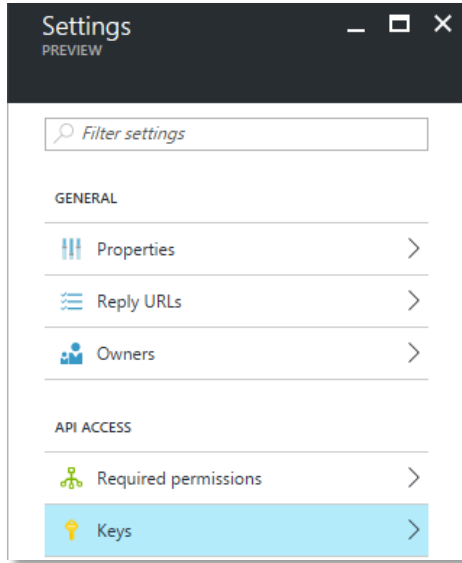
2. Click Windows Azure Active Directory in the list of APIs in the **Required permissions** blade



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.

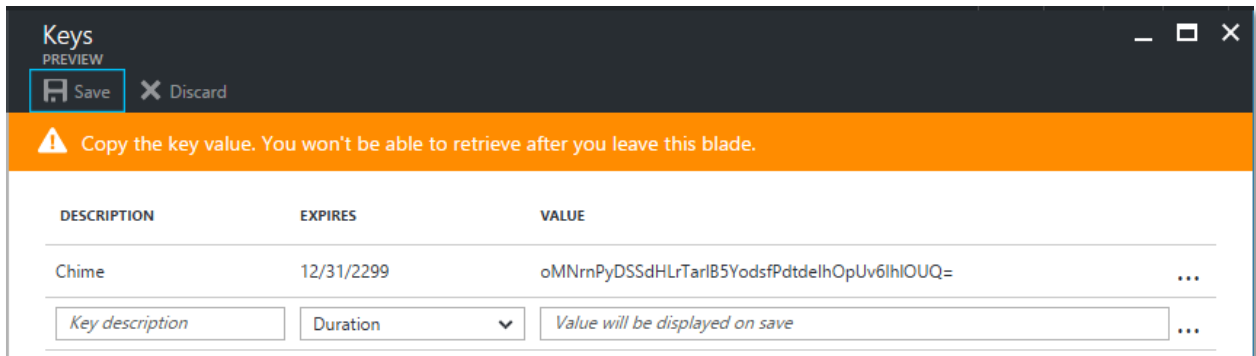


4. Close the **Required permissions** blade.
5. Click **Keys** in the **Settings** blade.

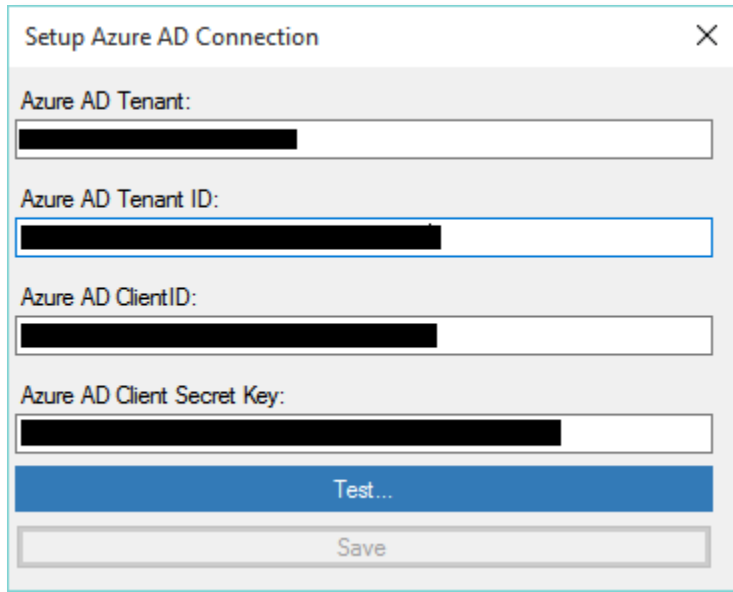


CREATE A NEW API KEY

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



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

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)


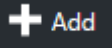
Azure AD Client Secret Key _____

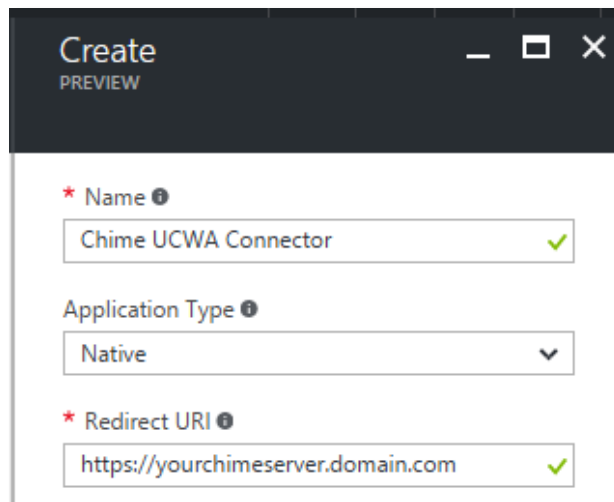
This value is from Page 8

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  **App registrations** in the Azure Active Directory blade.
2. Click  **Add** 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.




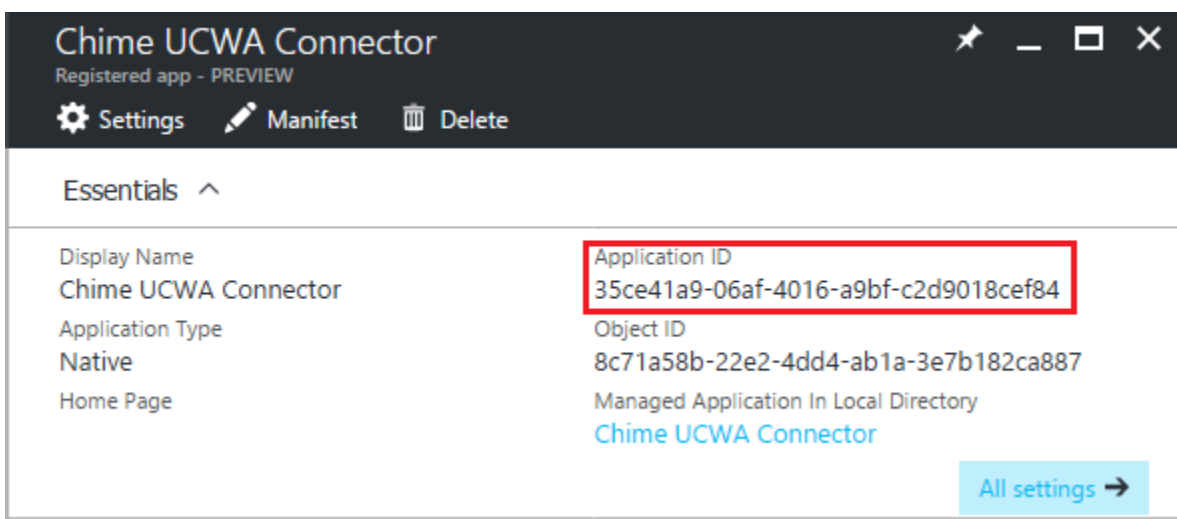
Create
PREVIEW

* Name ⓘ
Chime UCWA Connector ✓

Application Type ⓘ
Native ▼

* Redirect URI ⓘ
https://yourchimeserver.domain.com ✓

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


1. Click  **Manifest** in the application blade
2. Find the value for **allowOauth2ImplicitFlow**

```
13 "oauth2AllowImplicitFlow": false,
```



NOTE: This should be around line 13

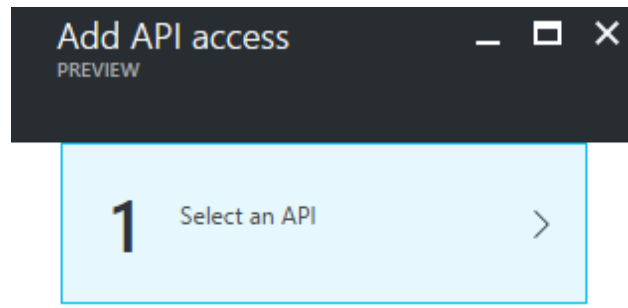
3. Change the value from **false** to **true**

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

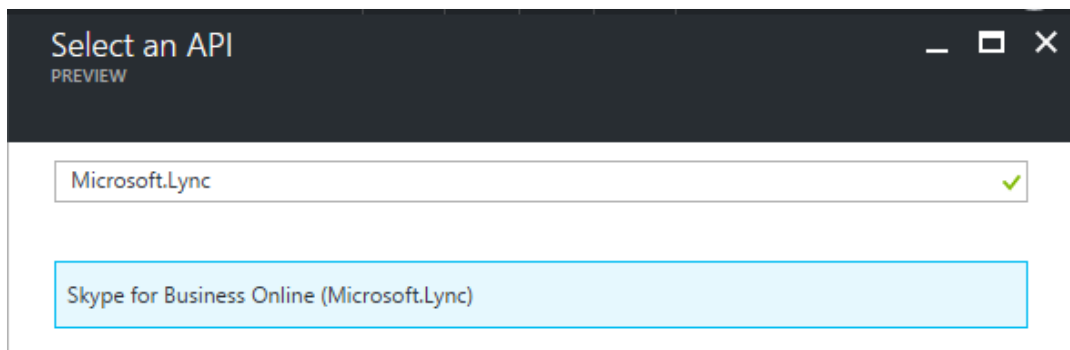
4. Click  **Save** in the Edit manifest blade

CONFIGURE THE APPLICATION PERMISSIONS

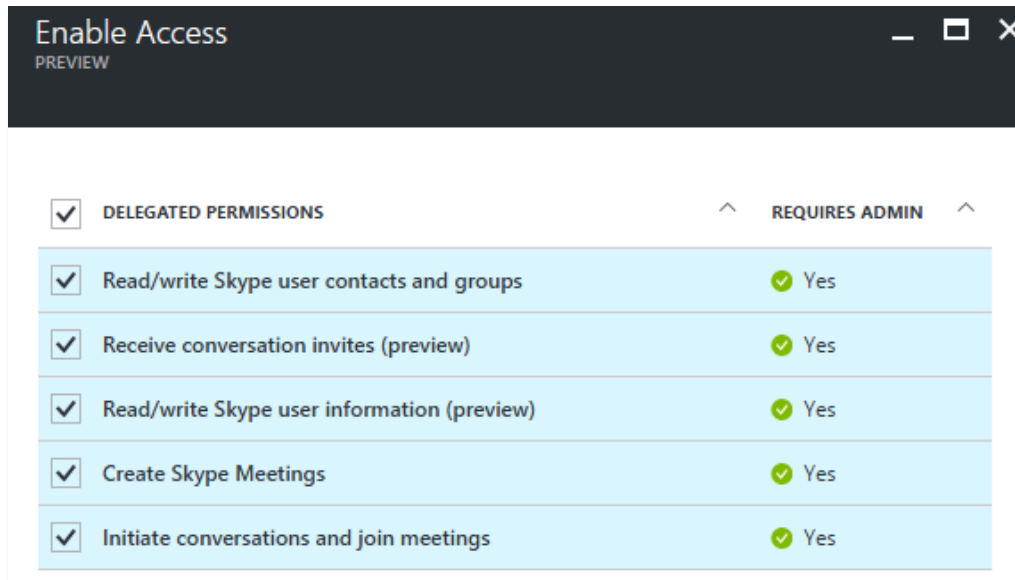
1. Click  **Required permissions** under API ACCESS in the Settings blade.
2. Click  **Add** in the **Required permissions** blade
3. Click **Select an API** in the Add API access blade



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.