

Configuring Azure AD access for Chime for Lync

Configuring Chime for Lync to use a Microsoft Azure AD instance as its directory service requires a small amount of setup in Office 365 and the Azure Management Portal. These steps are listed below:

Contents

Authorizing Chime to access Azure AD (Nov 2015)	3
Prerequisites:	3
Steps:.....	3
Azure Active Directory Accounts List	17

Authorizing Chime to access Azure AD (Nov 2015)

Prerequisites:

- A.) You must have an Office365 tenant for your organization.
- B.) You must be an administrator of your Office 365 domain.

Steps:

- 1.) Sign into the Office365 website, and navigate to the Admin Center.

The screenshot displays the Office 365 Admin Center. At the top is a green header with the Office 365 logo and name. Below this is a navigation pane on the left containing categories like SETUP, USERS, COMPANY PROFILE, IMPORT, CONTACTS, SHARED MAILBOXES, MEETING ROOMS, GROUPS, DOMAINS, PUBLIC WEBSITE, BILLING, EXTERNAL SHARING, MOBILE MANAGEMENT, SERVICE SETTINGS, REPORTS, SERVICE HEALTH, SUPPORT, PURCHASE SERVICES, MESSAGE CENTER, TOOLS, and ADMIN. The main content area is titled 'Office 365 admin center' and includes a search bar. A banner at the top right says 'New Admin Center in the works - get a s'. The 'Service overview' section is active, showing 'Service health' with '1 issue', 'Service requests' with 'No open service requests', 'Mail protection' with '2557 messages received, 734 processed by filtering.', and 'Message center' with 'No new messages in the past 7 days'. The 'Current health' section lists services: Exchange, Identity Service, Office 365 Portal, Office Subscription, Rights Management Service, SharePoint, Skype for Business, Sway, and Yammer Enterprise (marked as 'Restoring service'). A 'Planned maintenance' section at the bottom states 'No planned maintenance scheduled.'

- 2.) In the left navigation panel, expand the **Admin** nav, and select **Azure AD**. This should open the Azure Management Portal in a new tab or window. If you have not setup an Azure account linked with your Office 365 identity, you will need to do so; see <https://technet.microsoft.com/en-us/library/dn832618.aspx>. In the Portal, you should see the Active Directory for your Office 365 subscription.

The screenshot displays the Microsoft Azure Management Portal interface. The top header shows 'Microsoft Azure' and the user's email 'erichards@instant-tech.com'. The left navigation pane includes 'ALL ITEMS', 'ACTIVE DIRECTORY 1', and 'SETTINGS'. The main content area is titled 'all items' and contains a table with the following data:

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
instant technologies	→ Directory	✓ Active	Shared by all instant tech...	United States

At the bottom of the interface, there is a dark blue bar with a '+ NEW' button, a 'DELETE' icon, and a help icon.

3.) Click on your Active Directory. This should load up the Quick Start view for your directory.

The screenshot displays the Microsoft Azure portal interface. At the top, the header shows 'Microsoft Azure' and a user profile 'erichards@instant-tech.com'. The left sidebar contains navigation icons for 'instant technologies' and a search bar. The main content area is titled 'instant technologies' and features a navigation menu with links to 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. A large banner states 'Your directory is ready to use. Here are a few options to get started.' with a checkbox to 'Skip Quick Start the next time I visit'. Below this, a section titled 'I WANT TO' includes buttons for 'Set Up Directory', 'Manage Access', and 'Develop Applications'. The 'GET STARTED' section lists three steps: 1. 'Improve user sign-in experience' with a description and an 'Add domain' button; 2. 'Integrate with your local directory' with a description and a 'Download Azure AD Connect' link; 3. 'Get Azure AD Premium' with a description and a 'Try it now' button. The 'EXPLORE' section is visible at the bottom. The footer includes a '+ NEW' button and a help icon.

Microsoft Azure

erichards@instant-tech.com

instant technologies

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS LICENSES

instant technolog...

Your directory is ready to use.
Here are a few options to get started.

☐ Skip Quick Start the next time I visit

I WANT TO **Set Up Directory** Manage Access Develop Applications

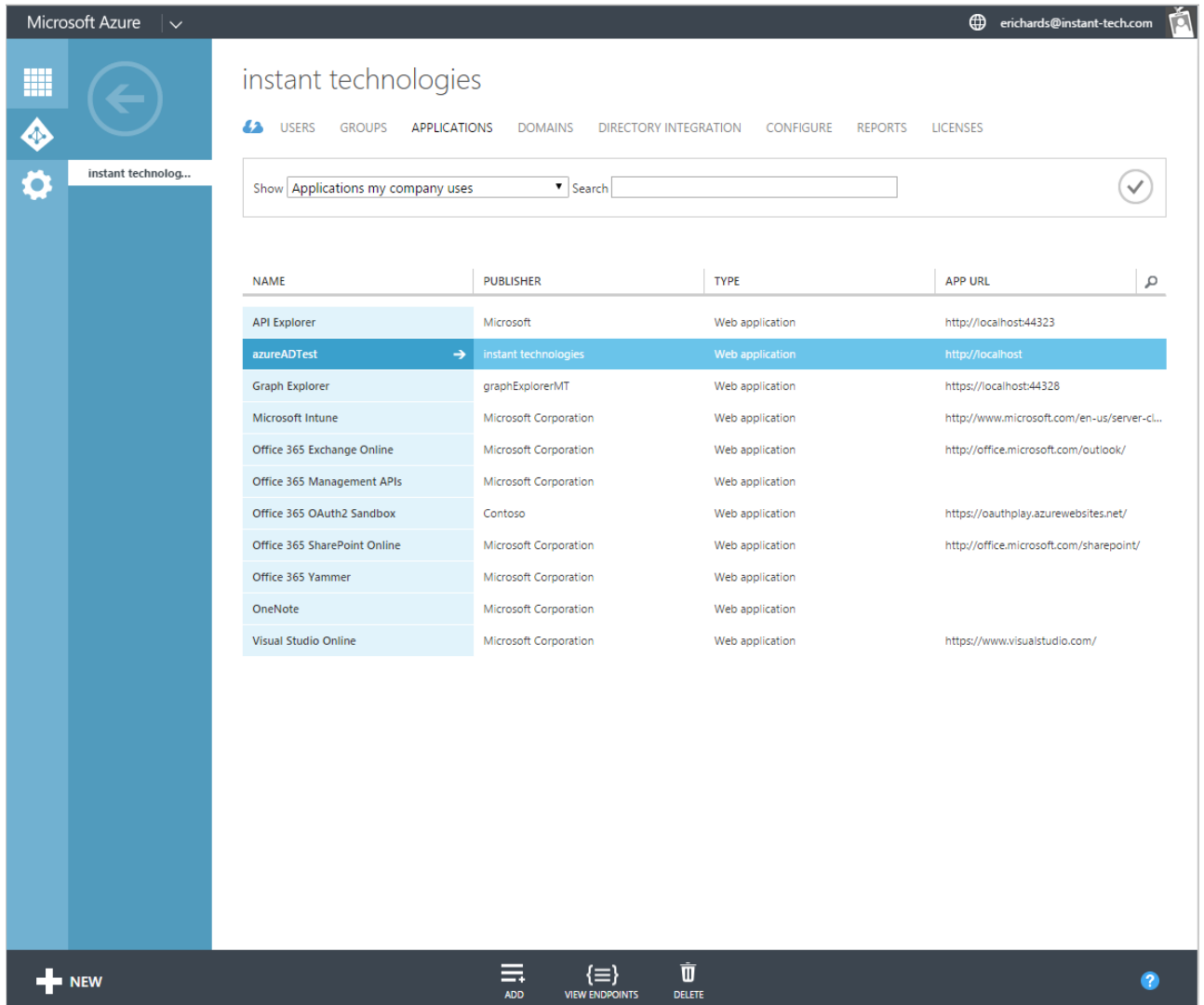
GET STARTED

- 1 Improve user sign-in experience
Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.
Add domain
- 2 Integrate with your local directory
Use the same user accounts and groups in the cloud that you already use on premises.
[Download Azure AD Connect](#)
- 3 Get Azure AD Premium
Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.
Try it now

EXPLORE

+ NEW

- 4.) In the top tab bar, select **Applications**. This will show a list of applications which have been configured to access your Azure Active Directory.



Microsoft Azure | erichards@instant-tech.com

instant technologies

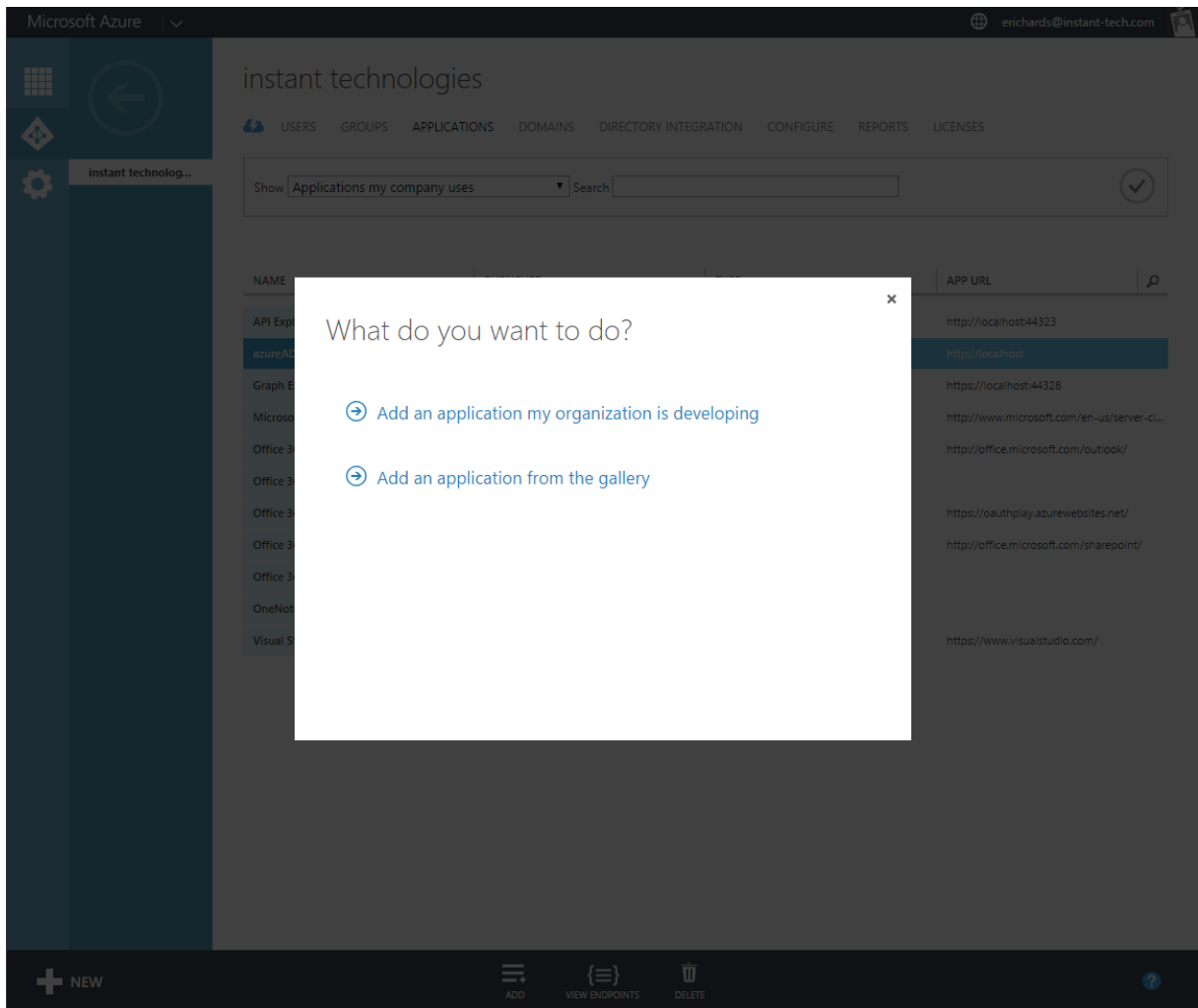
USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS LICENSES

Show Applications my company uses Search

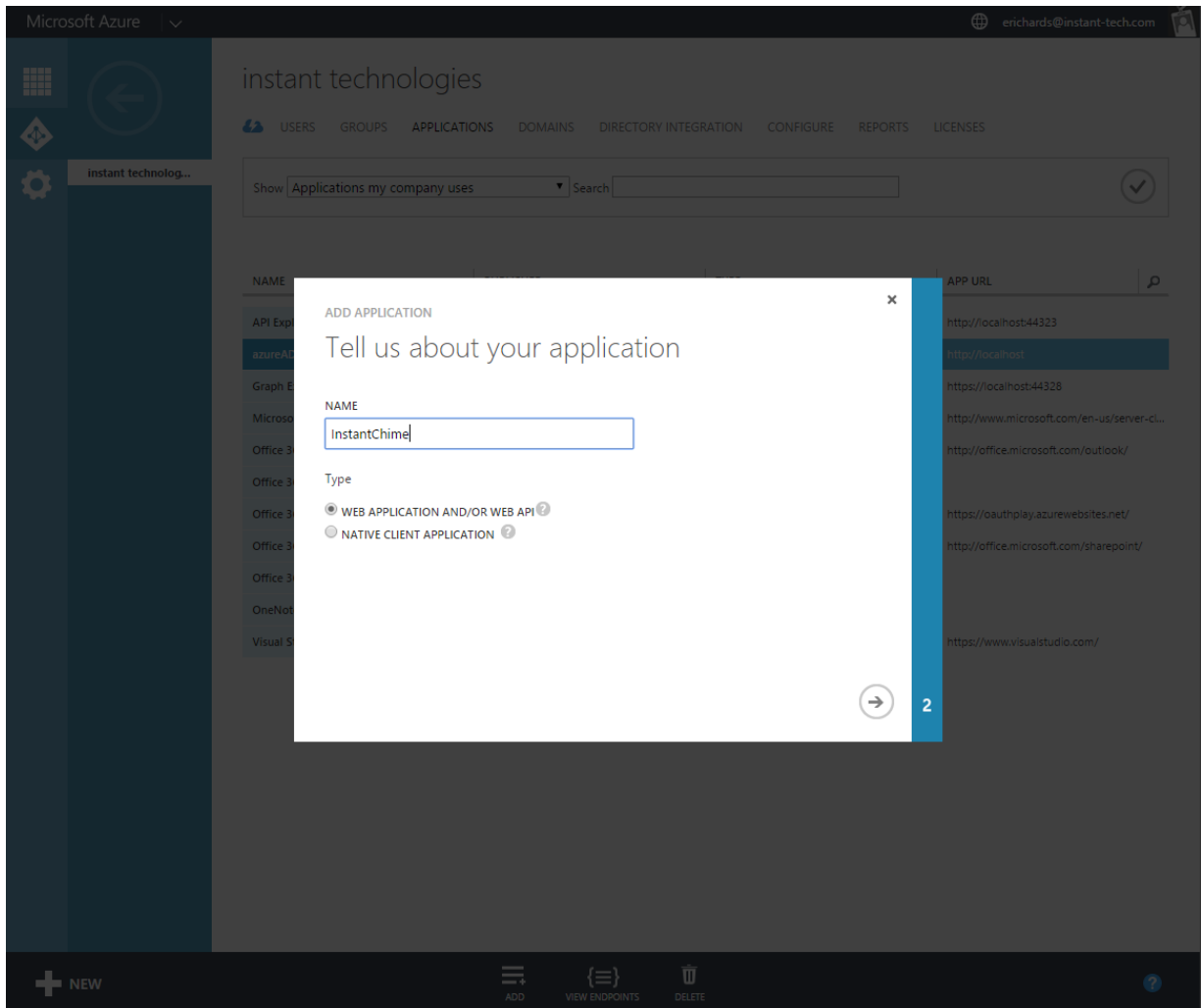
NAME	PUBLISHER	TYPE	APP URL
API Explorer	Microsoft	Web application	http://localhost:44323
azureADTest	instant technologies	Web application	http://localhost
Graph Explorer	graphExplorerMT	Web application	https://localhost:44328
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 OAuth2 Sandbox	Contoso	Web application	https://oauthplay.azurewebsites.net/
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	
OneNote	Microsoft Corporation	Web application	
Visual Studio Online	Microsoft Corporation	Web application	https://www.visualstudio.com/

+ NEW ADD VIEW ENDPOINTS DELETE ?

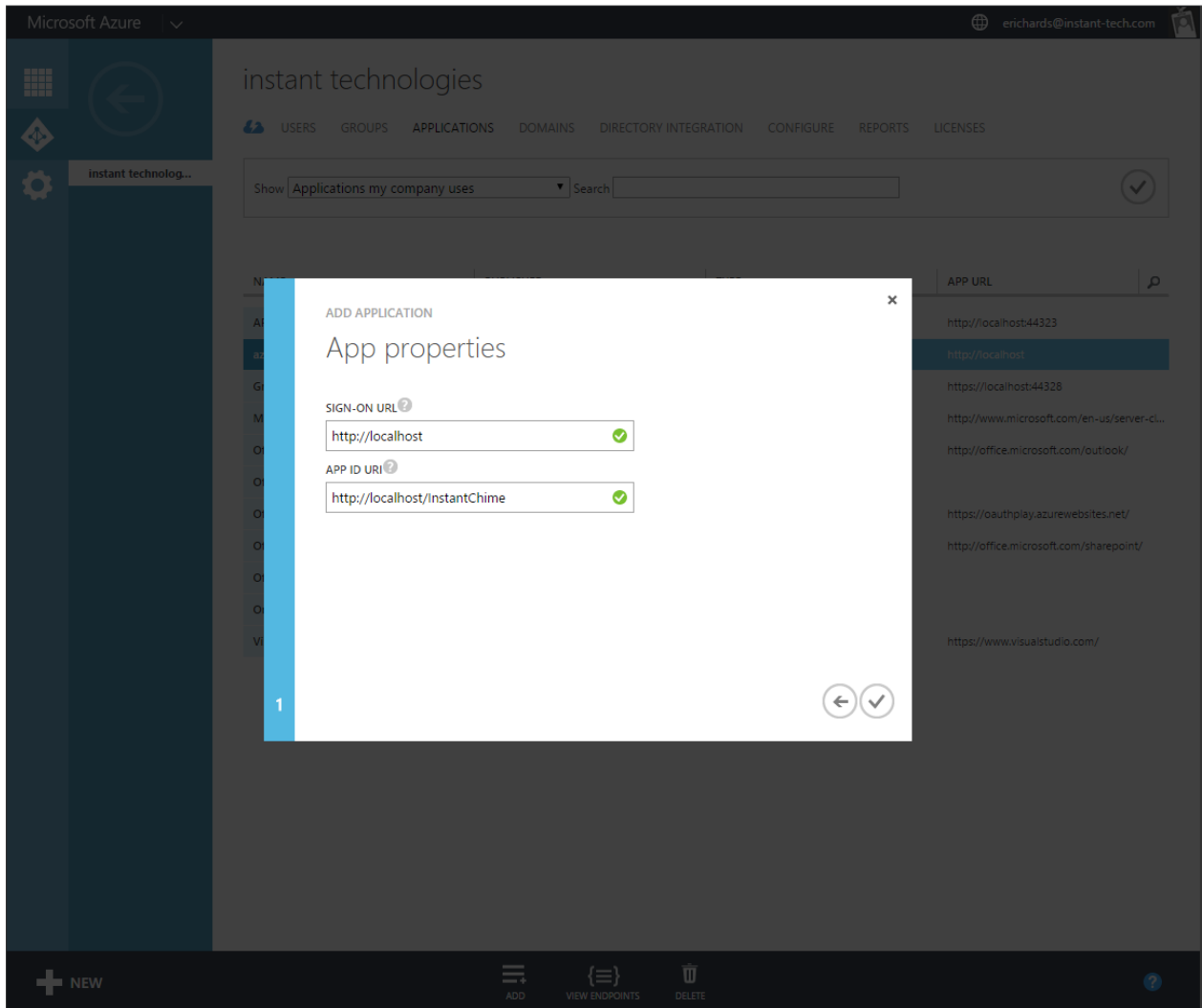
- 5.) To configure access to Azure Active Directory for Chime, select **Add** from the bottom toolbar. This will bring up a modal window. In this window, select **Add an application my organization is developing**.



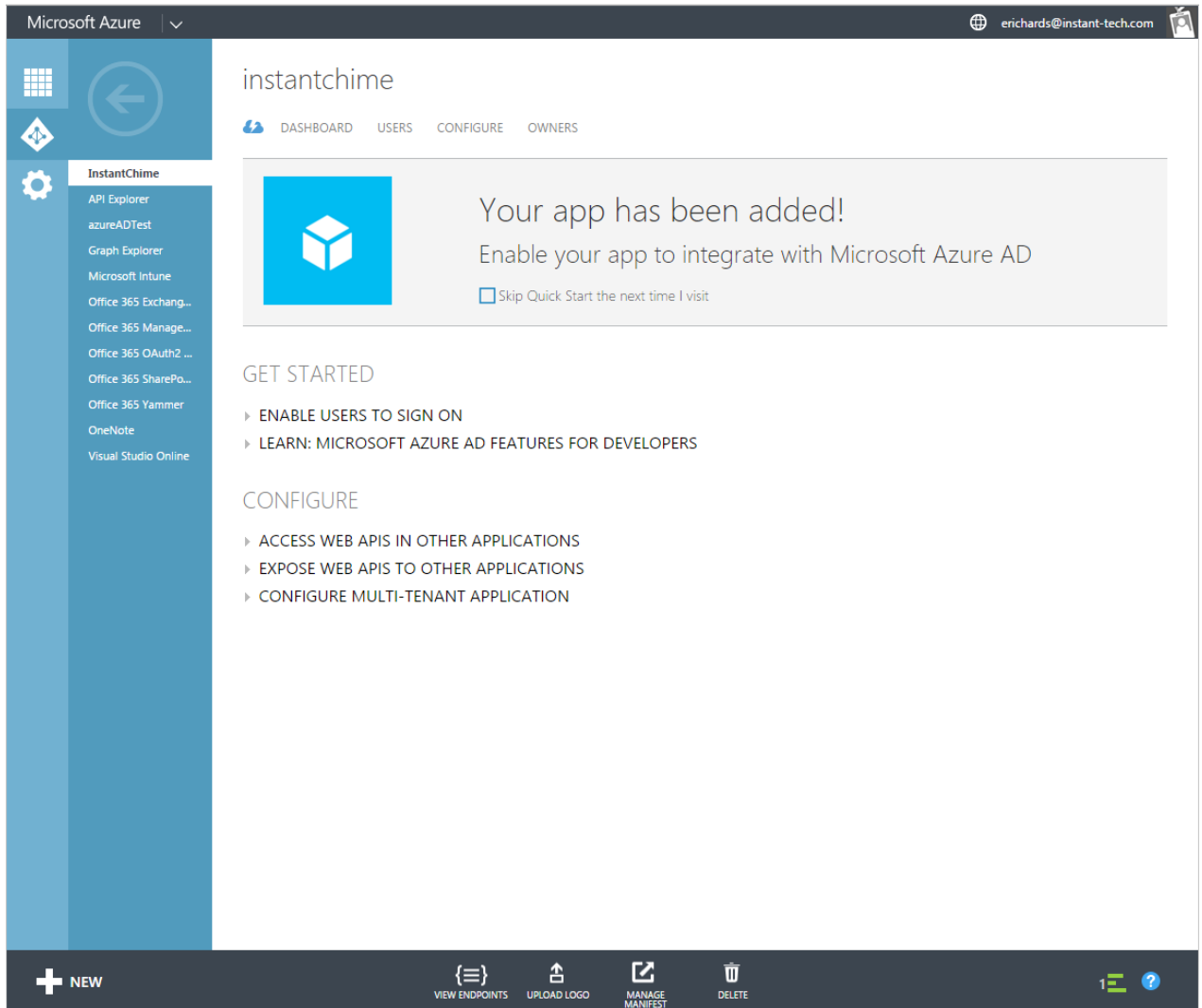
- 6.) This will start a wizard to create the new application access. You will need to enter a name to identify this application, e.g. InstantChime. This name can be whatever you choose. Be sure to select the radio button for **Web Application And/Or Web API**. When you have done this, click the right-arrow button to move onto the next step.



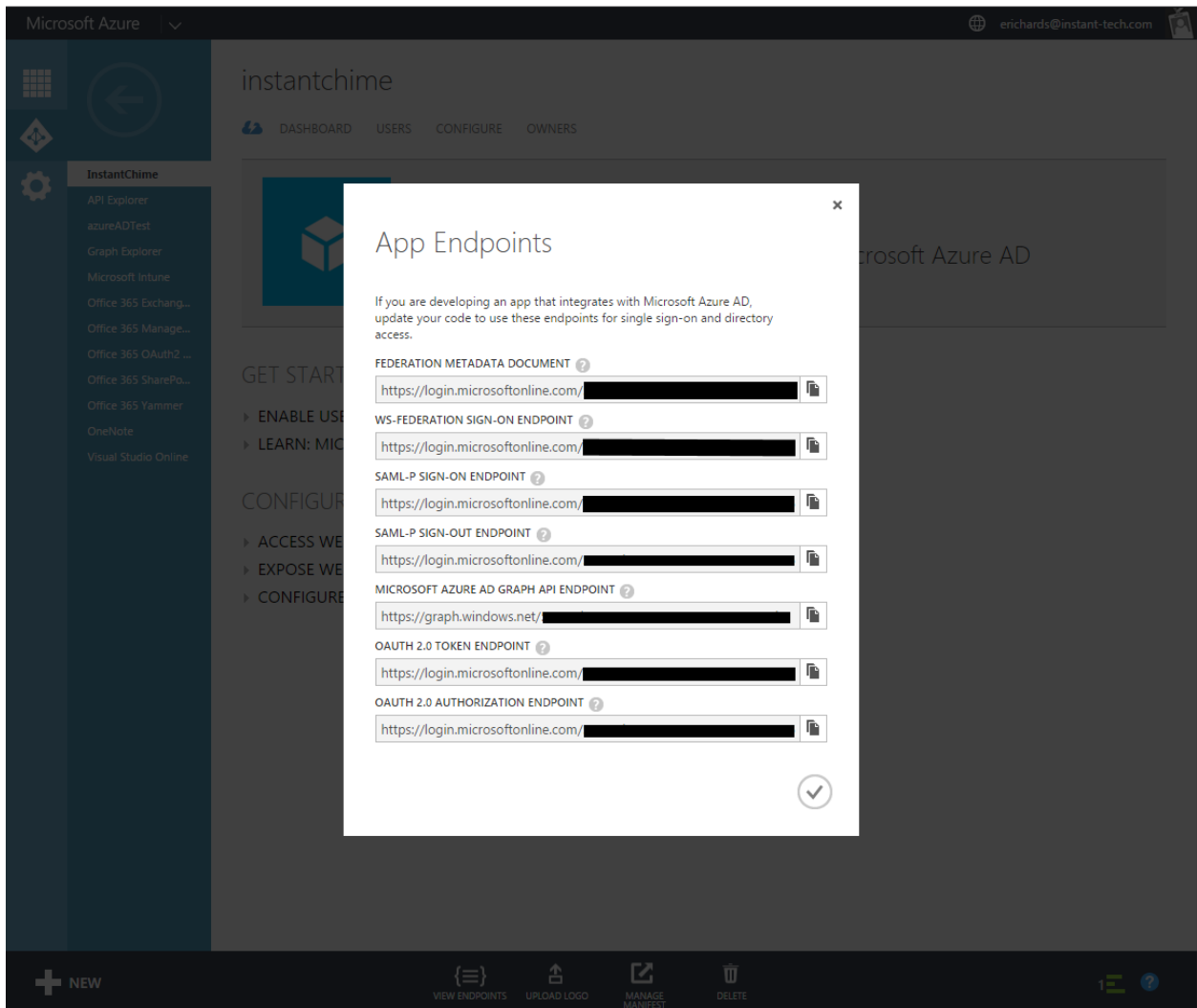
- 7.) In the second step, you will need to provide a **Sign-on Url** and an **App ID URI**. For Chime, these values are not really significant – using <http://localhost> for the **Sign-on URL** should be sufficient, and the **App ID URI** simply needs to be a URL that is not already used by another application in your Azure AD. When you have provided these values, click the check-mark button to create the new application. After a short time, the application will be created and you can continue with configuring it such that Chime can use this application to read from your Azure Active Directory.



8.) After the application has been created in Azure, the portal should bring you to the Quick Start page for the new application.



- 9.) Next, click the **View Endpoints** icon in the bottom toolbar. This will show a number of API endpoints that can be used with this application for various purposes. Each of these endpoint URLs will contain the Azure AD tenant URI ID for your active directory instance. For example: <https://login.microsoftonline.com/00000000-0000-0000-0000-000000000000/federationmetadata/2007-06/federationmetadata.xml>. In this case, the tenant URI ID would be **00000000-0000-0000-0000-000000000000**. **Save this value, as it will be needed later to configure Chime to use Azure Active Directory.** Once you have noted this value, you may close the endpoint modal.



- 10.) Next, select **Configure** from the top tab bar, to continue configuring the new application. The first thing to do is to note the **Client ID**. This is a GUID that identifies this application. In the example below, this is **b53db5bd-18e2-409a-8fbb-bc2a400b0e20**. Save this value, as it will also be needed when configuring Azure AD access for Chime.

The screenshot displays the Microsoft Azure portal interface for configuring an application. The top navigation bar shows 'Microsoft Azure' and the user 'erichards@instant-tech.com'. The left sidebar contains a list of applications, with 'InstantChime' selected. The main content area is titled 'instantchime' and has tabs for 'DASHBOARD', 'USERS', 'CONFIGURE', and 'OWNERS'. The 'CONFIGURE' tab is active, showing the 'properties' section. The 'NAME' field is 'InstantChime'. The 'SIGN-ON URL' field is 'http://localhost'. The 'LOGO' field displays a blue square with a white cube icon. The 'APPLICATION IS MULTI-TENANT' field has a 'YES' button and a 'NO' button. The 'CLIENT ID' field displays the GUID 'b53db5bd-18e2-409a-8fbb-bc2a400b0e20'. At the bottom, there is a '+ NEW' button and a row of icons for 'VIEW ENDPOINTS', 'UPLOAD LOGO', 'MANAGE MANIFEST', and 'DELETE'.

Microsoft Azure | erichards@instant-tech.com

instantchime

DASHBOARD USERS CONFIGURE OWNERS

properties

NAME InstantChime

SIGN-ON URL http://localhost

LOGO

APPLICATION IS MULTI-TENANT YES NO

CLIENT ID b53db5bd-18e2-409a-8fbb-bc2a400b0e20

+ NEW

VIEW ENDPOINTS UPLOAD LOGO MANAGE MANIFEST DELETE

11.) Scroll down the page to see the rest of the settings for the application. Make sure that the option **User Assignment Required To Access App** is set to **NO**.

The screenshot displays the Microsoft Azure portal interface for configuring an application. The left-hand navigation pane lists various services, with 'InstantChime' selected. The main content area shows the application's settings, including the 'APPLICATION IS MULTI-TENANT' toggle set to 'NO', the 'CLIENT ID' field containing a GUID, and the 'USER ASSIGNMENT REQUIRED TO ACCESS APP' toggle also set to 'NO'. Below these are sections for 'keys', 'single sign-on' (with 'APP ID URI' and 'REPLY URL' fields), and 'permissions to other applications'. A table shows 'Windows Azure Active Directory' with 'Application Permissions: 0' and 'Delegated Permissions: 1'. A green 'Add application' button is visible at the bottom of the permissions section. The bottom of the screen features a dark navigation bar with icons for 'NEW', 'VIEW ENDPOINTS', 'UPLOAD LOGO', 'MANAGE MANIFEST', and 'DELETE', along with a user profile icon and a help icon.

Microsoft Azure

enrichards@instant-tech.com

APPLICATION IS MULTI-TENANT YES NO

CLIENT ID b53db5bd-18e2-409a-8fbb-bc2a400b0e20

USER ASSIGNMENT REQUIRED TO ACCESS APP YES NO

keys

Select du... VALID FROM EXPIRES ON THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.

single sign-on

APP ID URI http://localhost/InstantChime

REPLY URL http://localhost
(ENTER A REPLY URL)

permissions to other applications

Application	Application Permissions	Delegated Permissions
Windows Azure Active Directory	0	1

Add application

NEW VIEW ENDPOINTS UPLOAD LOGO MANAGE MANIFEST DELETE

12.) Next, it is necessary to grant permissions to the application to read data from Active Directory. Under the section **permissions to other applications**, click **Application Permissions**, and from the dropdown, check the checkbox for **Read directory data**. This will allow Chime to use this application to perform lookups and searches against your Azure Active Directory instance.

The screenshot displays the Microsoft Azure portal interface for configuring an application named "InstantChime". The left-hand navigation pane lists various services, with "InstantChime" currently selected. The main content area is divided into several sections:

- APPLICATION IS MULTI-TENANT:** A toggle switch set to "NO".
- CLIENT ID:** A text field containing the value "b53db5bd-18e2-409a-8fbb-bc2a400b0e20".
- USER ASSIGNMENT REQUIRED TO ACCESS APP:** A toggle switch set to "NO".
- keys:** A section for managing application keys, featuring a "Select du..." dropdown, "VALID FROM" and "EXPIRES ON" fields, and a note: "THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT."
- single sign-on:** A section for configuring single sign-on, including an "APP ID URI" field with the value "http://localhost/InstantChime" and a "REPLY URL" field with the value "http://localhost".
- permissions to other applications:** A section for granting permissions to other applications. It shows a dropdown menu with "Windows Azure Active Directory" selected. The "Application Permissions" list includes:
 - ☐ Read and write directory data
 - ☒ Read directory data
 - ☐ Read and write devices

At the bottom of the page, there is a green "Add application" button and a footer bar with icons for "NEW", "VIEW ENDPOINTS", "UPLOAD LOGO", "MANAGE MANIFEST", "DELETE", "SAVE", "DISCARD", and a help icon.

13.) Finally, it is necessary to configure an application key that Chime can use to authenticate itself with the Azure AD application. Under the **keys** section, create a new key, by selecting **2 years** from the dropdown. You could also select 1 year, but then the key will expire sooner, and a new key will need to be provisioned when the original key expires.

Microsoft Azure | erichards@instant-tech.com

APPLICATION IS MULTI-TENANT: YES NO

CLIENT ID: b53db5bd-18e2-409a-8fbb-bc2a400b0e20

USER ASSIGNMENT REQUIRED TO ACCESS APP: YES NO

keys

Duration	Valid From	Expires On	Key Value
2 years	2015-12-01	2017-12-01	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.
Select duration			THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.
1 year			
2 years			

single sign-on

APP ID URI: http://localhost/InstantChime ✓

REPLY URL: http://localhost
(ENTER A REPLY URL)

permissions to other applications

Application	Application Permissions	Delegated Permissions
Windows Azure Active Directory	1	1

Add application

+ NEW | VIEW ENDPOINTS | UPLOAD LOGO | MANAGE MANIFEST | DELETE | SAVE | DISCARD | 1 ?

14.) When you have completed these steps, click the Save icon from the bottom toolbar. Azure will save the changed settings and generate the API key that will be needed to access this application with Chime. **Be sure to record this value, as it will be required to configure Chime to use Azure AD.**

BEFORE NAVIGATING AWAY FROM THE PAGE, MAKE SURE THAT YOU HAVE RECORDED THE API KEY THAT IS GENERATED. IT WILL NOT BE POSSIBLE TO OBTAIN THIS KEY VALUE ONCE YOU HAVE LEFT THE PAGE.

Microsoft Azure | erichards@instant-tech.com

InstantChime

- API Explorer
- azureADTest
- Graph Explorer
- Microsoft Intune
- Office 365 Exchang...
- Office 365 Manage...
- Office 365 OAuth2 ...
- Office 365 SharePo...
- Office 365 Yammer
- OneNote
- Visual Studio Online

CLIENT ID: b53db5bd-18e2-409a-8fbb-bc2a400b0e20

USER ASSIGNMENT REQUIRED TO ACCESS APP: YES NO

keys

BE SURE TO SAVE THE API KEY THAT IS DISPLAYED HERE!
(Where the black bar is displayed here)

2 years 2015-12-01 2017-12-01 [Redacted API Key]

Select du... VALID FROM EXPIRES ON THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.

Copy and store the key value. You won't be able to retrieve it after you leave this page.

single sign-on

APP ID URI: http://localhost/InstantChime

REPLY URL: http://localhost
(ENTER A REPLY URL)

permissions to other applications

Windows Azure Active Directory Application Permissions: 1 Delegated Permissions: 1

+ NEW { } VIEW ENDPOINTS UPLOAD LOGO MANAGE MANIFEST DELETE 2 ?

Azure Active Directory Accounts List

Setup Azure AD Connection

Azure AD Tenant:
[Redacted]

Azure AD Tenant ID:
[Redacted]

Azure AD ClientID:
[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 Step 9

Azure AD Client ID

This value is from Step 10

Azure AD Client Secret Key

This value is from Step 14