

Kinvey MIC setup to common authsources

(Warning: this is an informal document only, 3rd-party information might be out-of-date. Use as reference example only)

Current as per April 2017

Changelog:

- 1.0: First version, SAML: ivo 2015-09-25
- 1.1: Updated for new console, Add google oauth: ivo 2016-12-20
- 1.2: Ping: ivo 2017-01-05
- 1.3: SFDC: ivo 2017-04-10
- 1.4: ADFS: ivo 2018-02-01
- 1.5 Azure OpenID: rlh 2018-02-06
- 1.6 Azure SAML: rlh 2018-02-09
- 1.7 Update ADFS: rlh 2018-02-15

Table of contents:

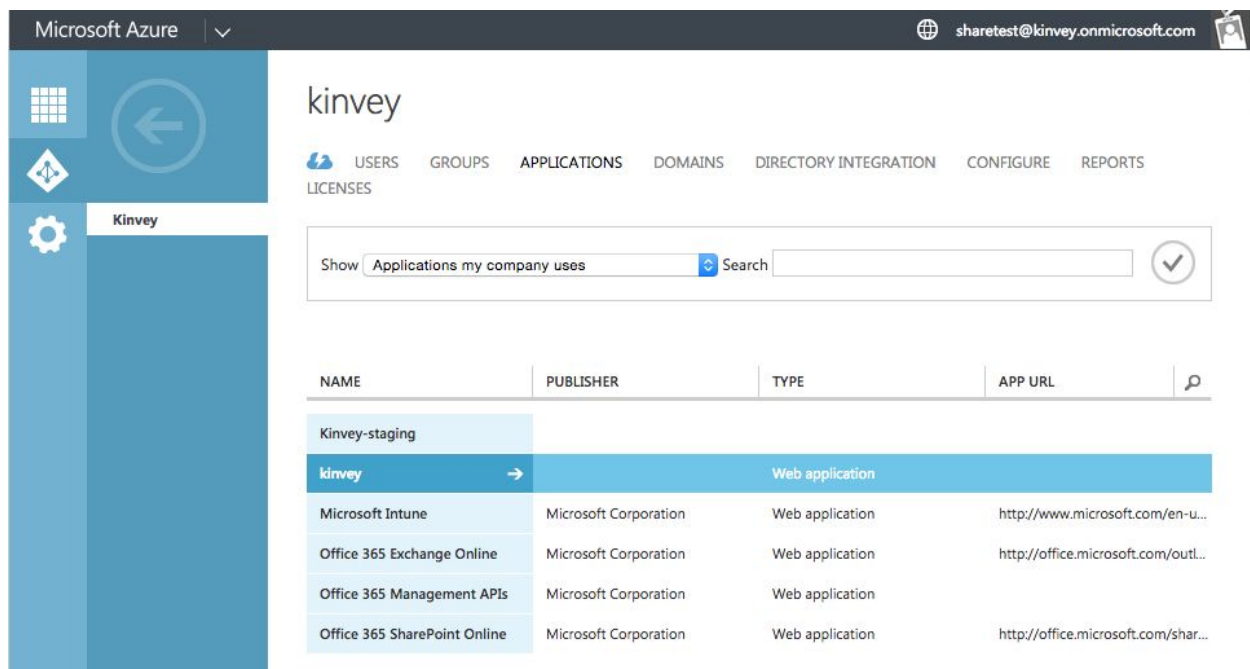
1. Azure SAML integration (old Azure console)	3
Set up connected application in the Azure console	3
Parameters in Kinvey Console	5
Assign users to use this connected app	6
2. ADFS SAML integration	8
Add a Relying Party Trust	8
3. Azure SAML integration	17
Create a new application	17
Configure App ID URI	19
Configure Reply URLs	20
Configure the permissions	21
Configure Kinvey	24
4. Azure OpenID connect integration	26
Create a new application	26
Configure Reply URLs	28
Configure the permissions	29
Create the Client Secret	31

Configure Kinvey	32
5. Google OAuth2 integration	34
Set up connected app in Google Developer Console	34
Parameters in Kinvey Console	35
Enable API's to use this Connected App	38
Testing the MIC config via the Console	40
6. Salesforce authentication integration	42
Set up connected app in Salesforce	42
Parameters in Kinvey Console	43
Forward Salesforce attributes to your datalink	45
Testing the MIC config via the Console	46
7. Ping integration (NOT WORKING CURRENTLY!)	48
Set up connected app in Google Developer Console	48
Parameters in Kinvey Console	48
In your app	49
Testing the MIC config via the Console	49

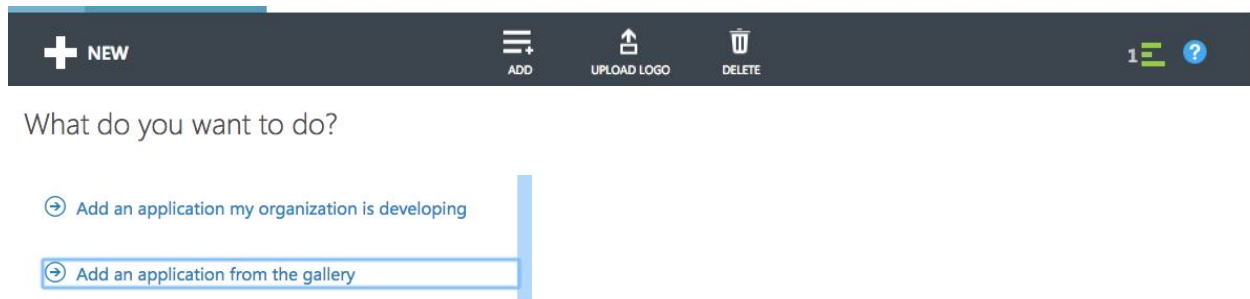
1. Azure SAML integration (old Azure console)

Set up connected application in the Azure console

In Azure (<https://manage.windowsazure.com/>), go to your AD instance, and click on "Applications"



At the bottom, click on "Add" and choose "Add an Application from the gallery"



Use "Custom" and give it a name.

APPLICATION GALLERY

Add an application for my organization to use

FEATURED APPLICATIONS (15)

CUSTOM

ALL (2496)

BUSINESS MANAGEMENT (97)

COLLABORATION (288)

CONSTRUCTION (3)

CONTENT MANAGEMENT (86)



Add an unlisted application my organization is using **PREVIEW**

NAME

Kinvey

Enter the name of an application you are using, and add it to explore single sign-on integration options.

Click on "Configure Single Sign-on"

Use "Microsoft Azure AD Single Sign-On"

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to Kinvey?

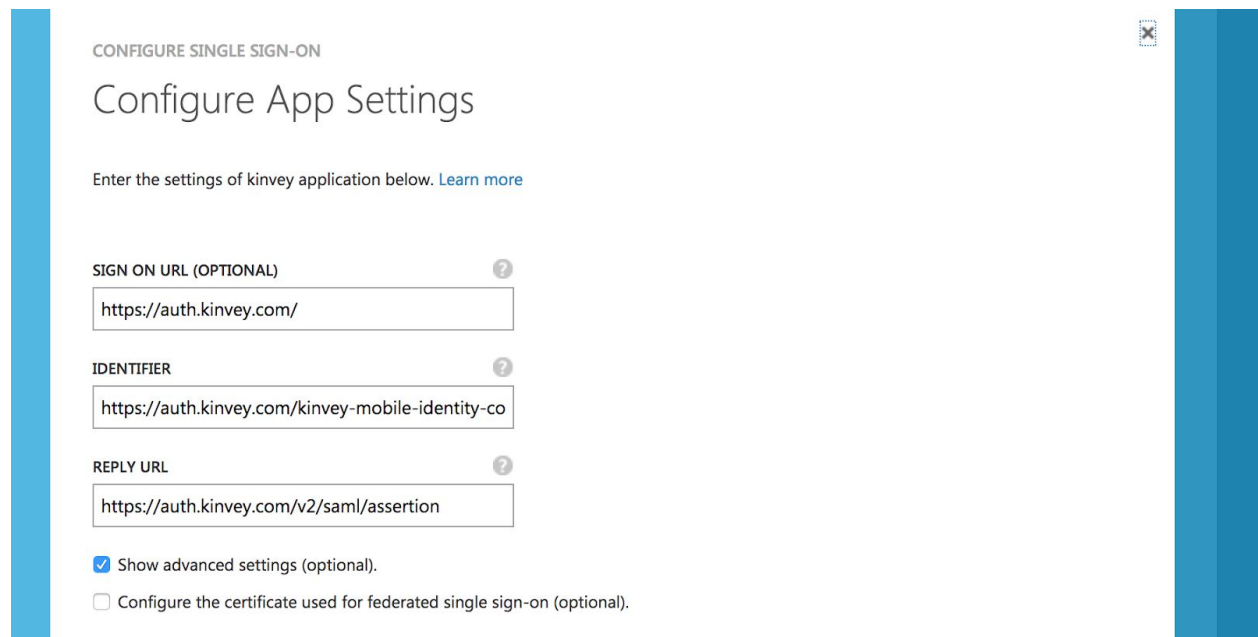
- ☒ Microsoft Azure AD Single Sign-On
Establish federation between Microsoft Azure AD and Kinvey
[Learn more](#)

In the "Configure App Settings" screen, check "Show Advanced Settings"

Use these urls:

- Sign On URL: <https://auth.kinvey.com/>
- Issuer/Identifier URL: <https://auth.kinvey.com/kinvey-mobile-identity-connect>
- Reply URL: <https://auth.kinvey.com/v2/saml/assertion>

NOTE: Replace with dedicated instance url if needed, e.g. `https://<instance>-auth.kinvey.com...`



CONFIGURE SINGLE SIGN-ON

Configure App Settings

Enter the settings of kinvey application below. [Learn more](#)

SIGN ON URL (OPTIONAL) ?

`https://auth.kinvey.com/`

IDENTIFIER ?

`https://auth.kinvey.com/kinvey-mobile-identity-co`

REPLY URL ?

`https://auth.kinvey.com/v2/saml/assertion`

☒ Show advanced settings (optional).

☐ Configure the certificate used for federated single sign-on (optional).

Parameters in Kinvey Console

In the next screen, observe the windows.net url and certificate you will now configure in the Auth Provider settings screen into the Kinvey console:

- Create a new SAML-Redirect configuration
- MS Issuer URL -> ignore in Kinvey console
- Kinve Provider URI -> MS Single Sign On Service URL
- Kinvey Logout URI -> MS Single Sign Out Service URL
- MS Certificate: Download Base64, open in text editor, paste certificate into Kinvey Certificate field
- Kinvey Name ID Format URI: literal:
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
- Set your redirect URI's as per your front-end requirements.
- Allowed attributes:
 - You must include "id" and "audience" minimally as allowed attributes

Provider Configuration

Type of Provider

Which auth service do you want to use?

SAML-Redirect

Provider URI

https://login.windows.net/631d3418-d713-4a95-bd54-636109555

Redirect URI's

The URI that is invoked to pass an authorization grant code back to your app.

https://console.kinvey.com

kinveyLetoTest://

+ ADD REDIRECT URI

Logout URI

The Logout URI provided by the SAML Identity Provider

https://login.windows.net/631d3418-d713-4a95-bd54-636109555

Certificate Text

The X.509 Certificate text provided by the SAML Identity Provider

-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQPKDr91GizKBL0tQnWTr02DANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEyINaWNyY2F0ZTAeFw0xNTA5MmMxODU0XJ0aWZnY2F0ZTAeFw0xNTA5MmMxODU0

Name ID Format URI

The format that Kinvey expects for the auth identifying NameID

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Enable Proxy?

No

Yes

Allowed attributes

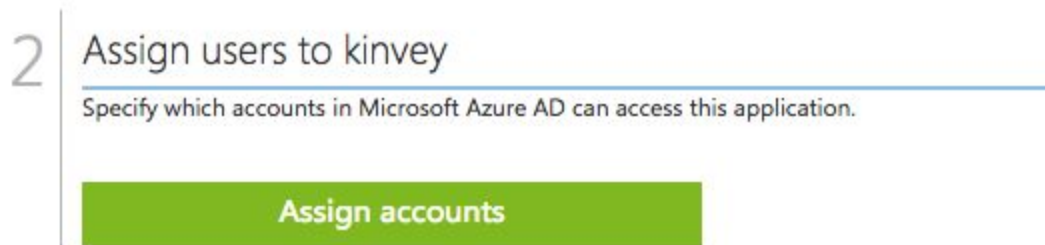
id

audience

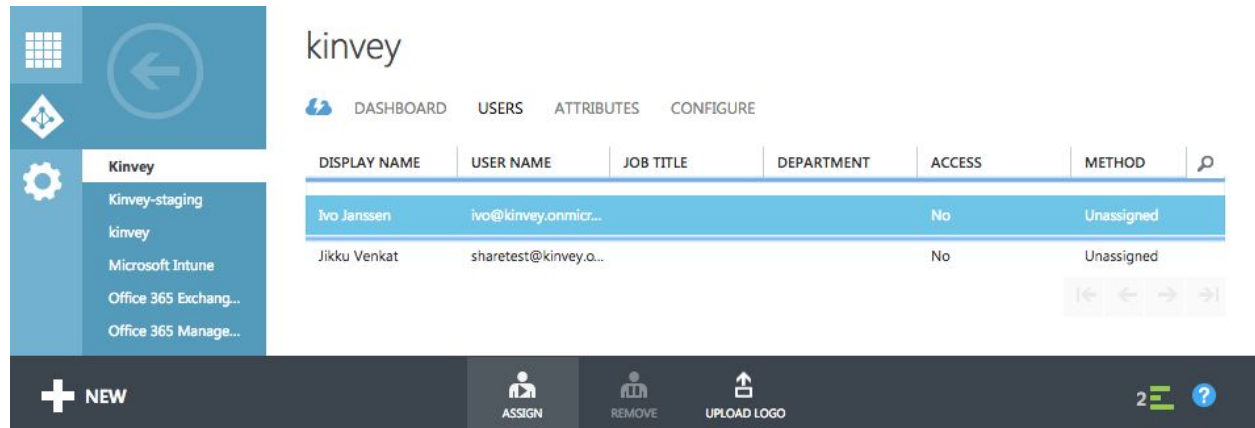
This completes the configuration.

Assign users to use this connected app

To allow specific users to use this SAML option, click on "Assign Users to Kinvey"



For each user you want to give access, highlight that user and click "Assign" at the bottom:



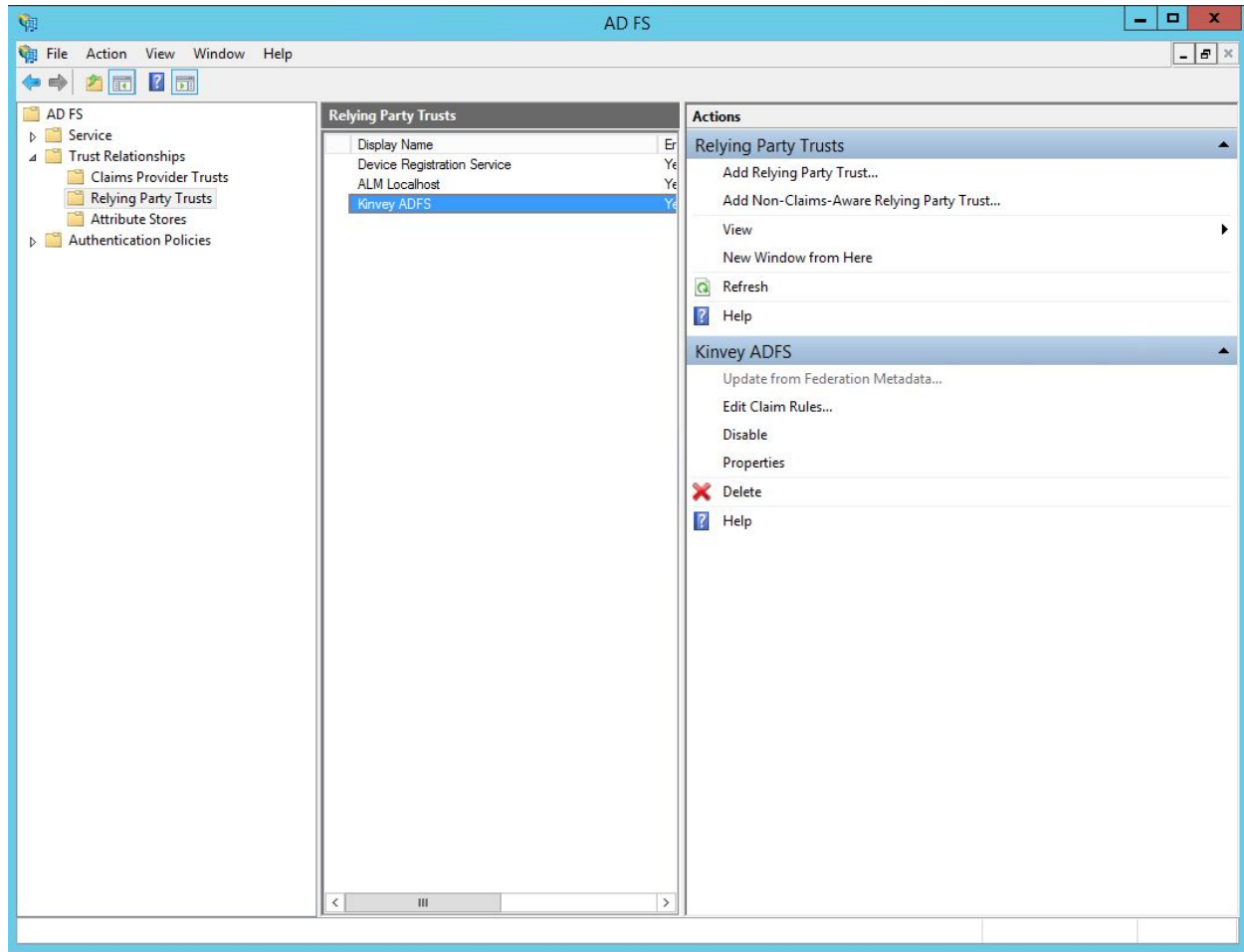
For Azure AD, you must use MIC API version 2

- iOS: `Client.sharedClient.micApiVersion = .v2`
- Xamarin: `Client.SharedClient.MICApiVersion = "v2";`
- Javascript: `user.loginWithMIC('http://localhost:8100',
$kinvey.AuthorizationGrant.AuthorizationCodeLoginPage, {version: "v2"});`

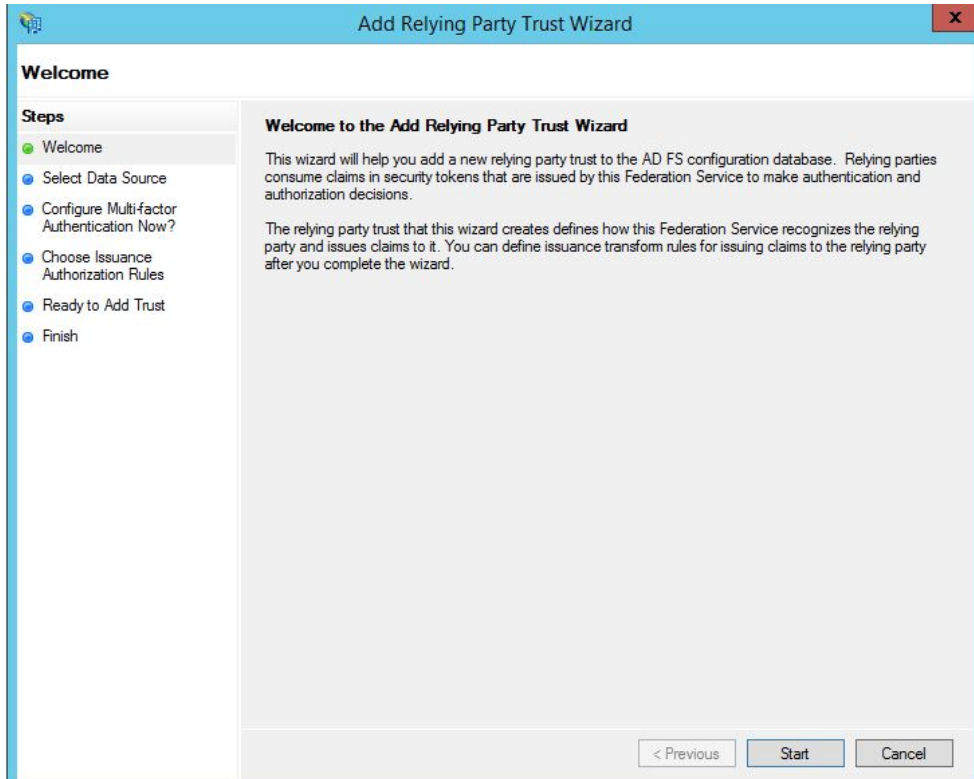
2. ADFS SAML integration

Add a Relying Party Trust

Begin by launching your instance of ADFS. Start the Add Relying Party Trust wizard.

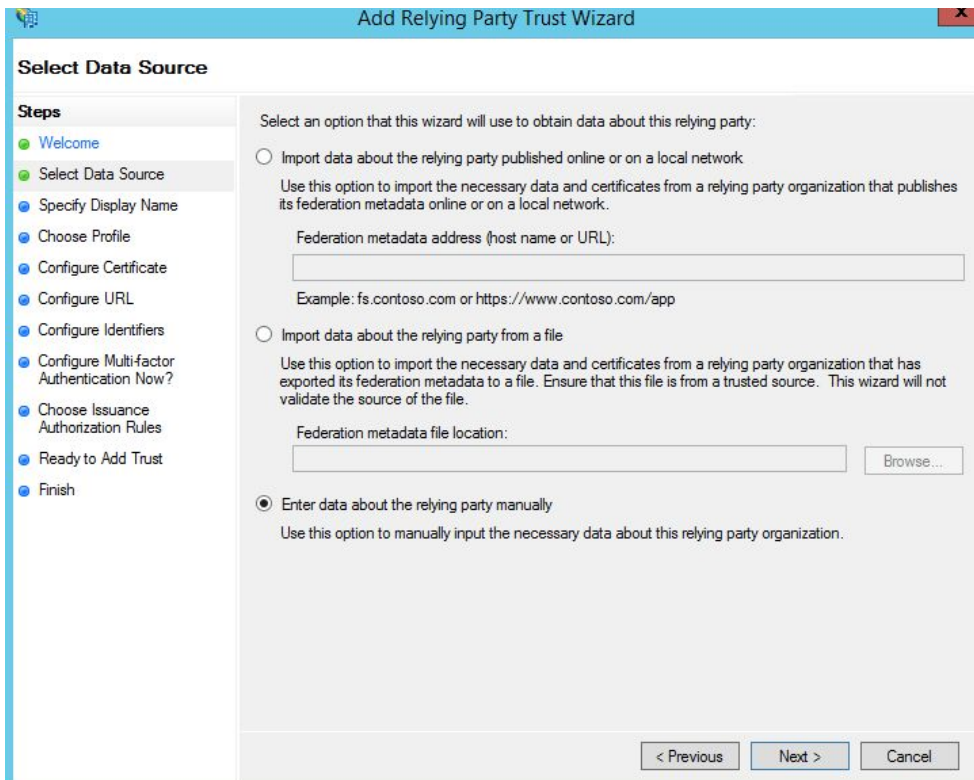


This starts the configuration wizard for a new trust. Press Start



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard'. The window is divided into two main sections. On the left, under the heading 'Steps', there is a list of steps: 'Welcome' (highlighted with a green dot), 'Select Data Source' (blue dot), 'Configure Multi-factor Authentication Now?' (blue dot), 'Choose Issuance Authorization Rules' (blue dot), 'Ready to Add Trust' (blue dot), and 'Finish' (blue dot). The main area on the right is titled 'Welcome to the Add Relying Party Trust Wizard'. It contains two paragraphs of text. The first paragraph states: 'This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.' The second paragraph states: 'The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.' At the bottom right of the main area, there are three buttons: '< Previous' (disabled), 'Start' (active), and 'Cancel'.

Enter data about relying part manually. Press Next>



The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Select Data Source' step. The title bar is blue with the text 'Add Relying Party Trust Wizard'. The window is divided into two main sections. On the left, under the heading 'Steps', there is a list of steps: 'Welcome' (green dot), 'Select Data Source' (highlighted with a green dot), 'Specify Display Name' (blue dot), 'Choose Profile' (blue dot), 'Configure Certificate' (blue dot), 'Configure URL' (blue dot), 'Configure Identifiers' (blue dot), 'Configure Multi-factor Authentication Now?' (blue dot), 'Choose Issuance Authorization Rules' (blue dot), 'Ready to Add Trust' (blue dot), and 'Finish' (blue dot). The main area on the right is titled 'Select Data Source'. It contains the text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options. The first option is 'Import data about the relying party published online or on a local network'. Below it is a text box for 'Federation metadata address (host name or URL):' with the example 'fs.contoso.com or https://www.contoso.com/app'. The second option is 'Import data about the relying party from a file'. Below it is a text box for 'Federation metadata file location:' with a 'Browse...' button. The third option is 'Enter data about the relying party manually', which is selected with a radio button. Below it is the text: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right of the main area, there are three buttons: '< Previous' (disabled), 'Next >' (active), and 'Cancel'.

Display name that you'll recognize in the future. Press Next>

The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. The wizard has a blue title bar with the text 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Specify Display Name' and contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'Kinvey ADFS'. Below the text box is a 'Notes:' label followed by a large text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Select AD FS profile. Press Next>

The screenshot shows the 'Choose Profile' step of the 'Add Relying Party Trust Wizard'. The wizard has a blue title bar with the text 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Choose Profile' and contains the instruction 'This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.' Below this, there are two radio button options. The first option is 'AD FS profile', which is selected. Below it is a description: 'This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.' The second option is 'AD FS 1.0 and 1.1 profile', which is not selected. Below it is a description: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Leave the certificate settings at their defaults. Press Next>

The screenshot shows the 'Configure Certificate' step of the 'Add Relying Party Trust Wizard'. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate (selected), Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains a text box with the following text: 'Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..'. Below this text are four input fields: 'Issuer:', 'Subject:', 'Effective date:', and 'Expiration date:'. Below these fields are three buttons: 'View...', 'Browse...', and 'Remove'. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

Enable support for the SAML 2.0 WebSSO protocol. Service URL provided by Kinvey Metadata URI. Press Next>

The screenshot shows the 'Configure URL' step of the 'Add Relying Party Trust Wizard'. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (selected), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains a text box with the following text: 'AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.' Below this text are two checkboxes. The first checkbox is 'Enable support for the WS-Federation Passive protocol'. Below it is a text box for 'Relying party WS-Federation Passive protocol URL:' with an example: 'https://fs.contoso.com/adfs/ls/'. The second checkbox is 'Enable support for the SAML 2.0 WebSSO protocol'. Below it is a text box for 'Relying party SAML 2.0 SSO service URL:' with the value 'https://auth.kinvey.com/v3/saml/assertion' and an example: 'https://www.contoso.com/adfs/ls/'. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

Enter Relying party trust identifier. Press Next>

The screenshot shows the 'Add Relying Party Trust Wizard' at the 'Configure Identifiers' step. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers (selected), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this is a text box for 'Relying party trust identifier:' with an 'Add' button. An example is provided: 'https://fs.contoso.com/adfs/services/trust'. Below that is a list box for 'Relying party trust identifiers:' containing 'https://auth.kinvey.com/kinvey-mobile-identity-connect' with a 'Remove' button. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

- https://auth.kinvey.com/kinvey-mobile-identity-connect

< Previous Next > Cancel

Leave the configure multi-factor at their defaults. Press Next>

The screenshot shows the 'Add Relying Party Trust Wizard' at the 'Configure Multi-factor Authentication Now?' step. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now? (selected), Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.' Below this is a table with columns 'Requirements', 'Users/Groups', and 'Global Settings'. The table shows 'Not configured' for all three. Below the table are two radio buttons: 'I do not want to configure multi-factor authentication settings for this relying party trust at this time.' (selected) and 'Configure multi-factor authentication settings for this relying party trust.' Below this is a paragraph: 'You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).' At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

Add Relying Party Trust Wizard

Configure Multi-factor Authentication Now?

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Requirements	Users/Groups	Global Settings
	Not configured	
	Device	Not configured
	Location	Not configured

☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

Select the Permit all users to access this relying party radio button. Press Next>

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main area is titled 'Choose Issuance Authorization Rules'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules (highlighted), Ready to Add Trust, and Finish. The main content area contains the following text: 'Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.' Below this, there are two radio button options: 'Permit all users to access this relying party' (selected) and 'Deny all users access to this relying party'. Each option has a descriptive paragraph. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

☒ Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

☐ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous Next > Cancel

On the final screen use the Close button to exit and open the Claim Rules editor.

The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Finish' step. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main area is titled 'Finish'. On the left, the 'Steps' pane lists the same steps as the previous window, with 'Finish' highlighted. The main content area contains the following text: 'The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.' Below this, there is a checkbox labeled 'Open the Edit Claim Rules dialog for this relying party trust when the wizard closes', which is checked. At the bottom right, there is a 'Close' button.

Finish

The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☒ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Close

Click Add Rule... to launch the wizard. Use Send LDAP Attributes as Claims for your Claim rule template, and click Next to proceed.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: LDAP outgoing

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	E-Mail Address
*		

< Previous Finish Cancel

Add another Rule, this time selecting Transform an Incoming Claim as the template.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Email transform

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

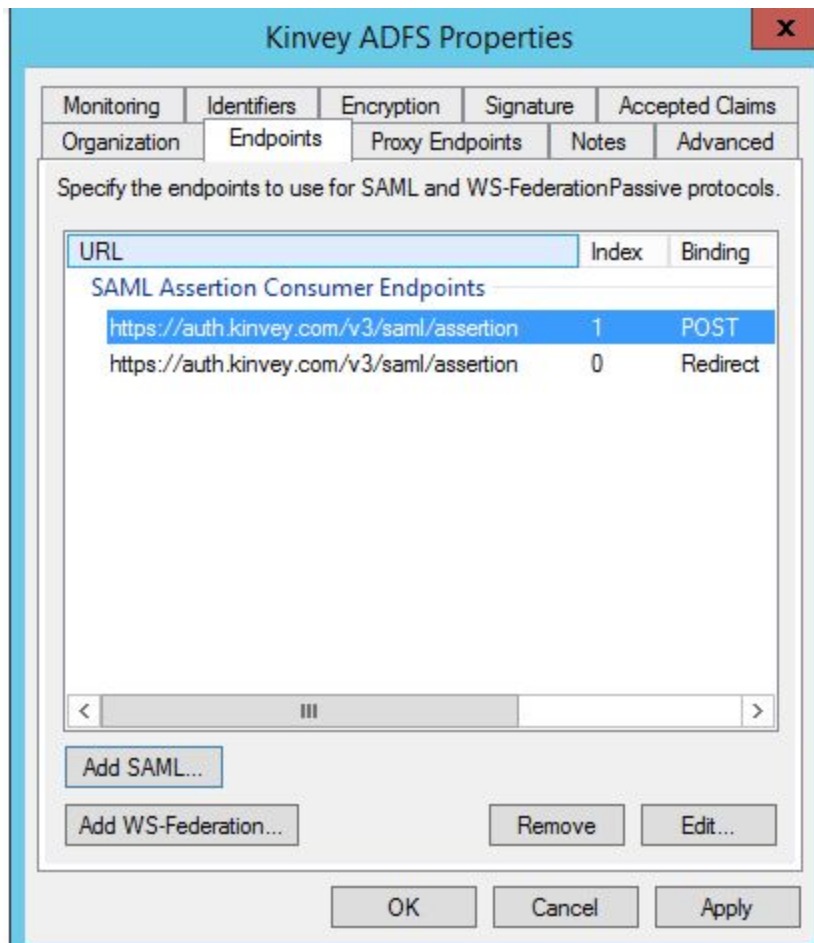
☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

< Previous Finish Cancel

Finally, click **Finish** to create the claim rule. In the Endpoints tab, click on add SAML to add a new endpoint.



Edit Endpoint

✕

Endpoint type:

SAML Assertion Consumer

Binding:

Redirect

☐ Set the trusted URL as default

Index:

0

^

v

Trusted URL:

https://auth.kinvey.com/v3/saml/assertion

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK

Cancel

Edit Endpoint

✕

Endpoint type:

SAML Assertion Consumer

Binding:

POST

☐ Set the trusted URL as default

Index:

1

^

v

Trusted URL:

https://auth.kinvey.com/v3/saml/assertion

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

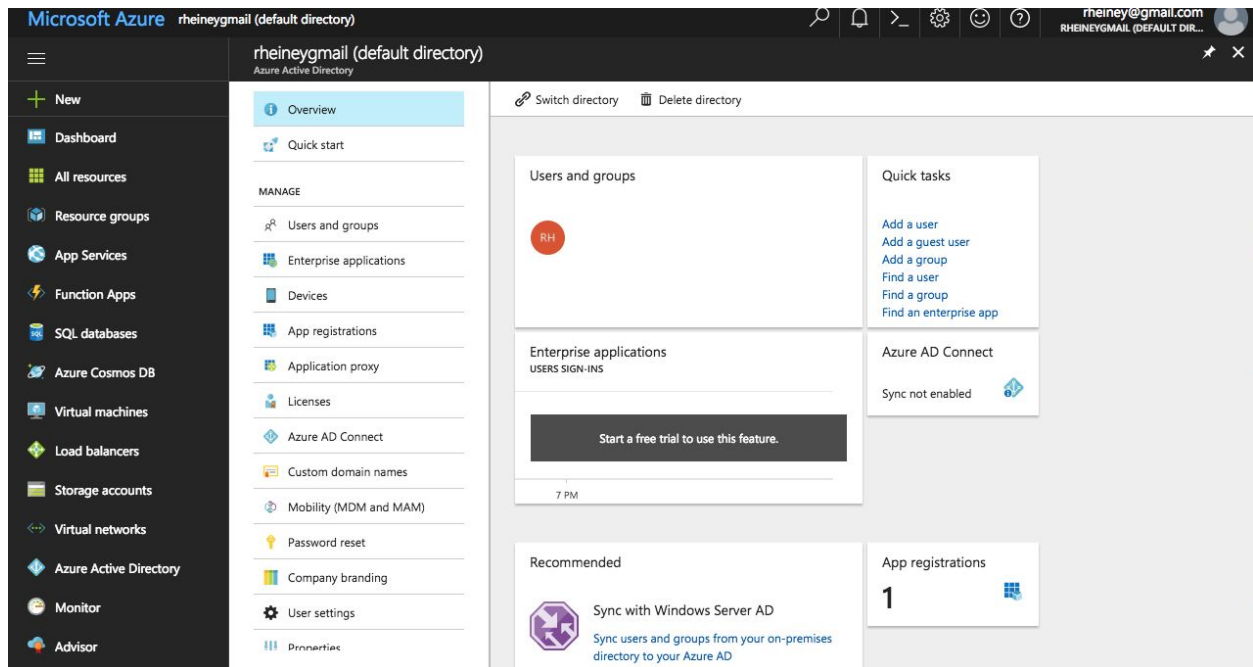
OK

Cancel

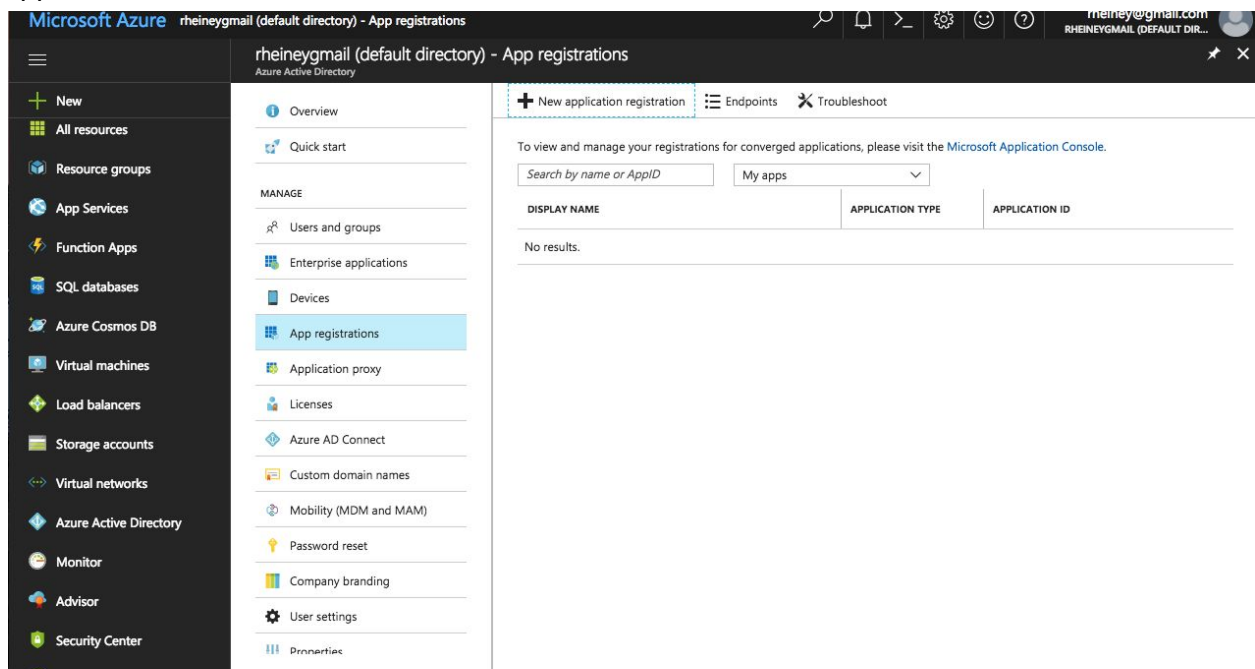
3. Azure SAML integration

Create a new application

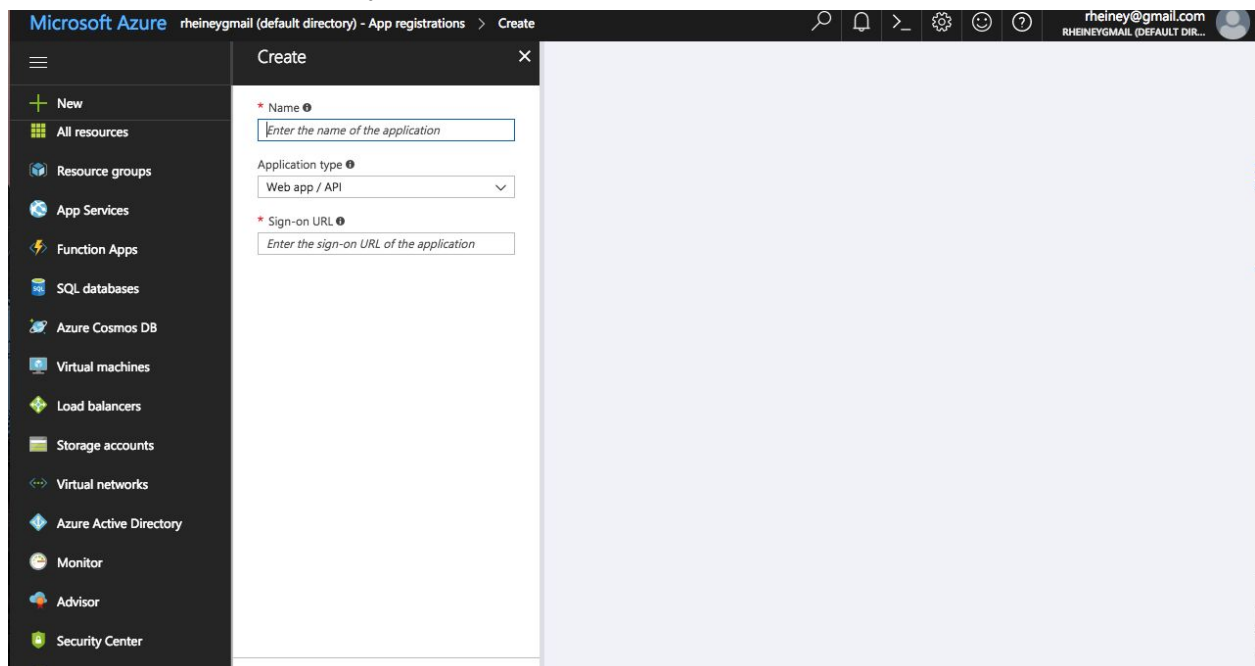
Login to Microsoft Azure at <https://portal.azure.com> and choose Azure Active Directory from the sidebar.



Select App registrations. Then click on the +New application registration button to add a new application.

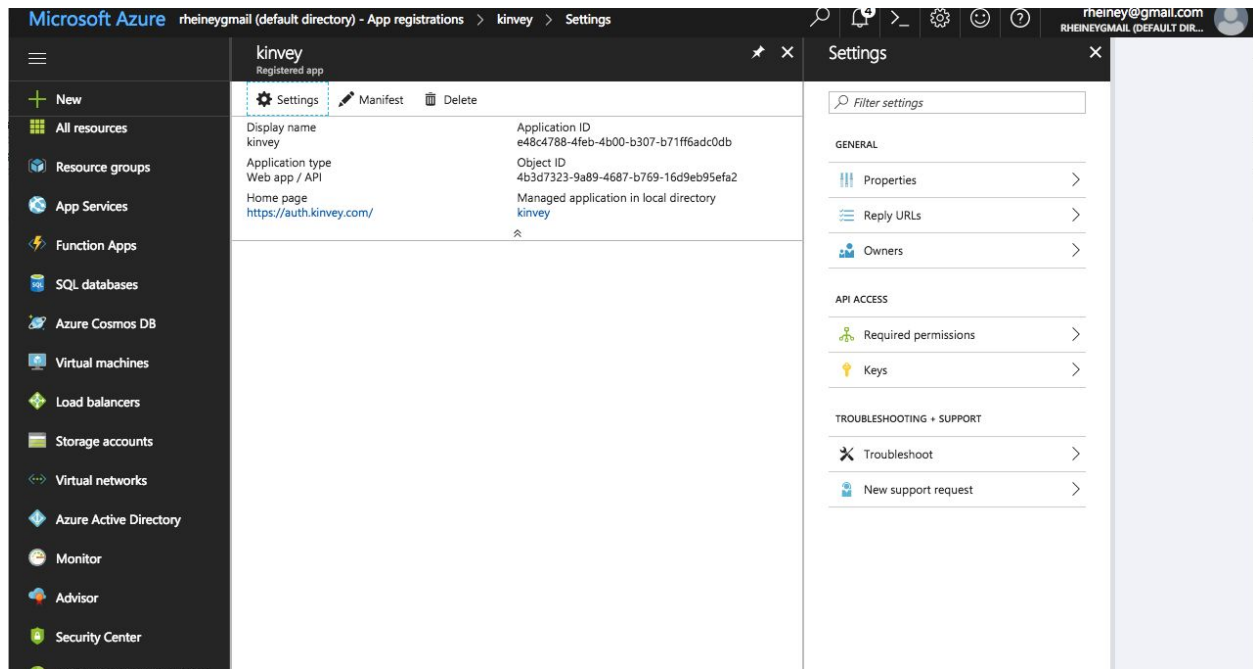


Enter a name for the application, select Web app/API as the Application Type, and for Sign-on URL enter https://auth.kinvey.com/.

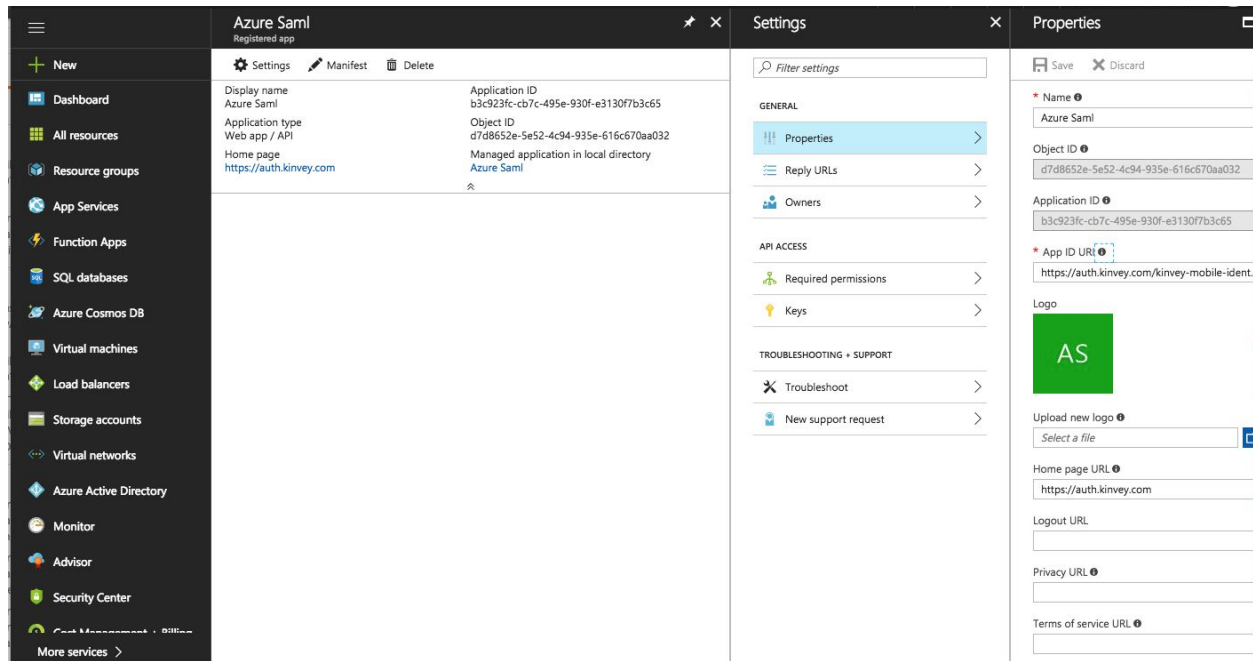


Configure App ID URI

Then click on Settings and Properties.

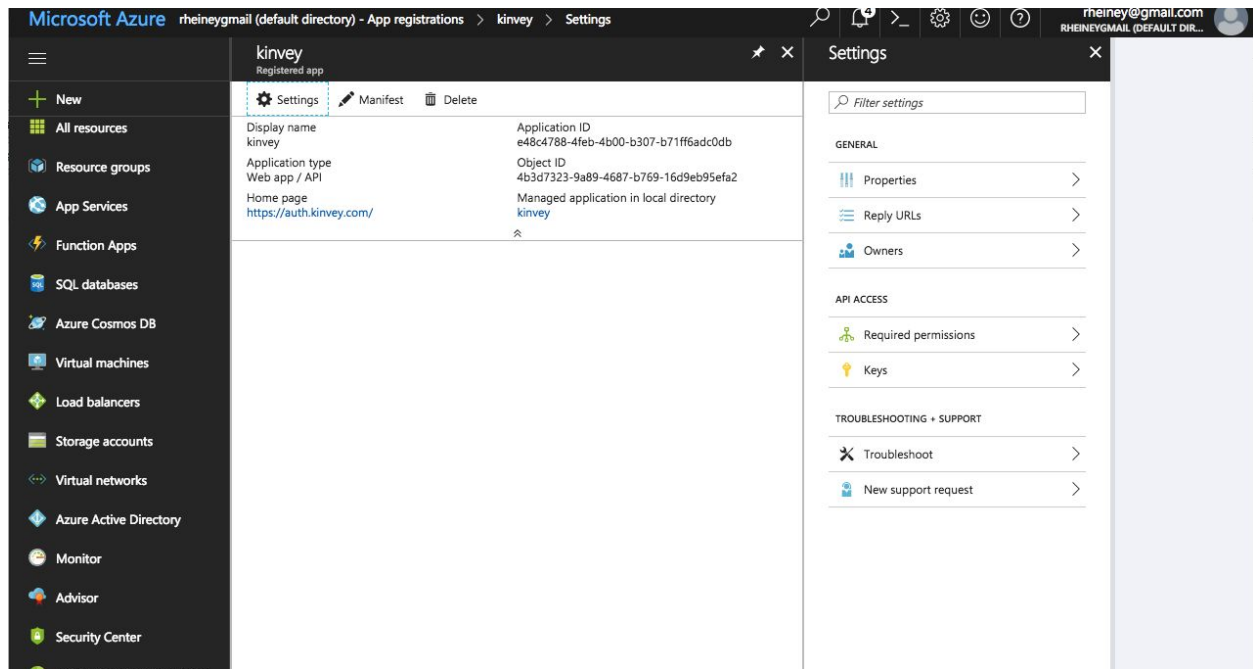


Set App ID URI to https://auth.kinvey.com/kinvey-mobile-identity-connect

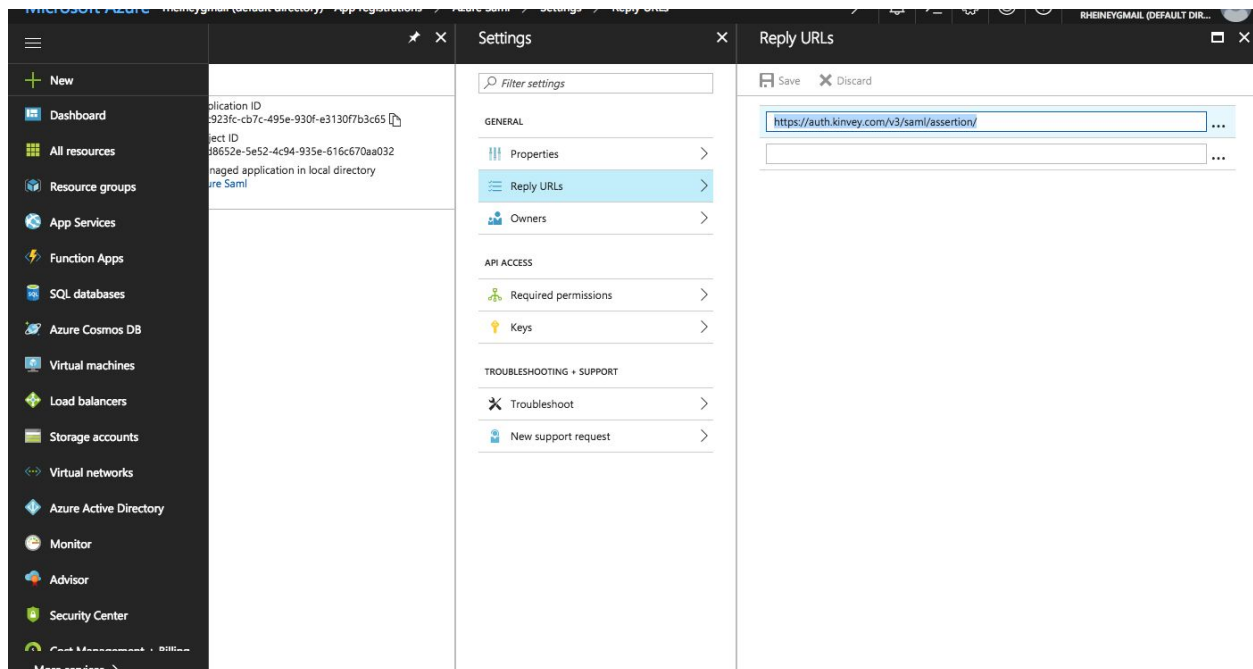


Configure Reply URLs

Then click on Settings and Reply URLs.

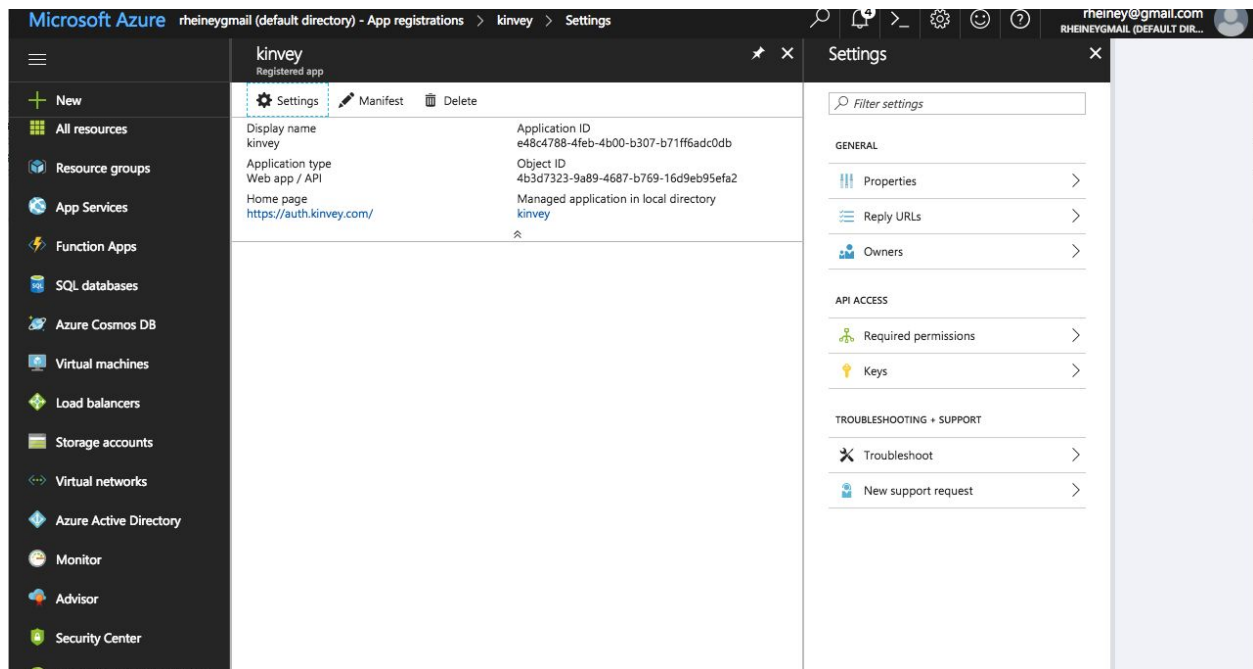


Set Reply URLs to <https://auth.kinvey.com/v3/saml/assertion/>

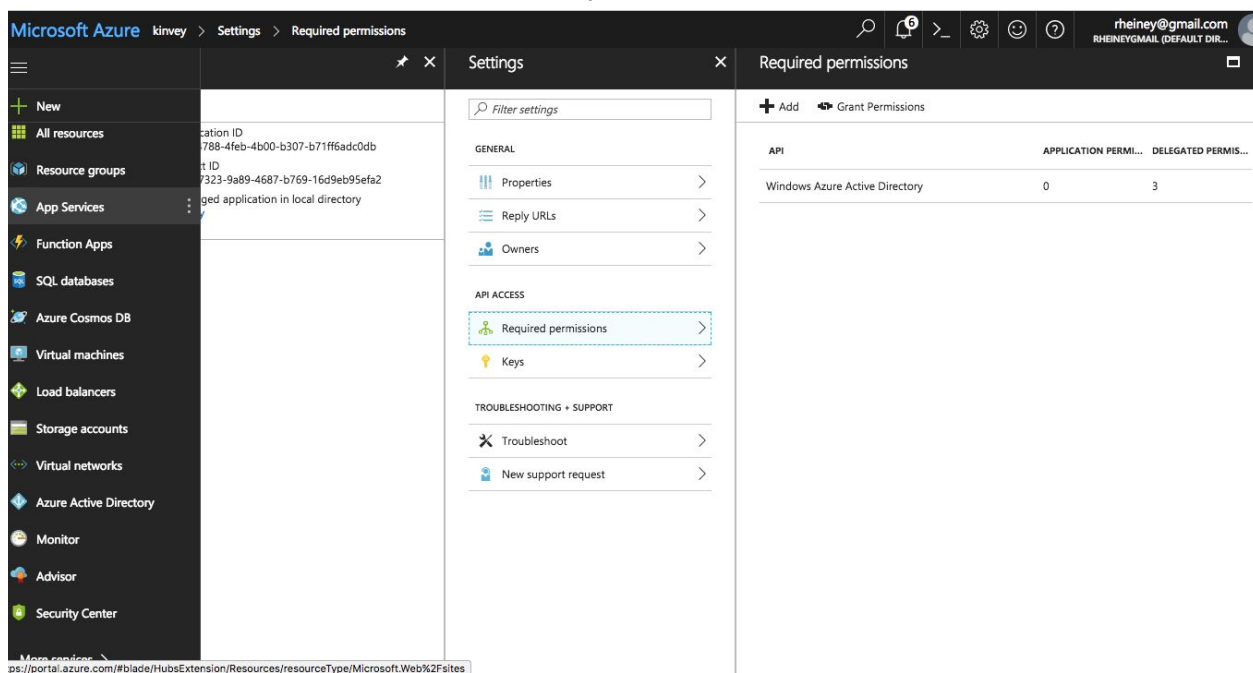


Configure the permissions

Then click on Settings and Required permissions.



Then click on Windows Azure Active Directory.



Check Access the directory as the signed-in user, Read all users basic profiles and Sign in and read user profile under Delegated Permissions.

The screenshot shows the 'Required permissions' and 'Enable Access' configuration for Windows Azure Active Directory. The left pane shows the 'Required permissions' section with a table of API permissions. The right pane shows the 'Enable Access' section with a list of permissions and their status.

API	APPLICATION PERM...	DELEGATED PERMIS...
Windows Azure Active Directory	0	3

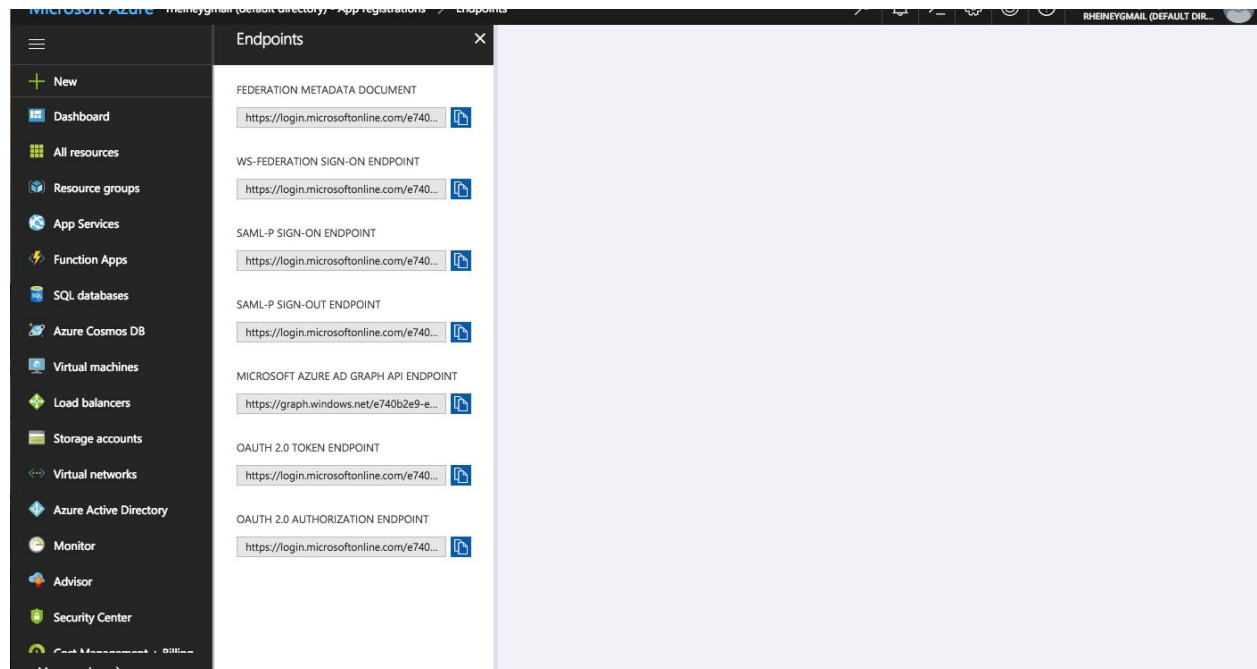
Permission	Status
Read and write directory data	Yes
Read and write devices	Yes
Read all hidden memberships	Yes
Manage apps that this app creates or owns	Yes
Read and write all applications	Yes
Read and write domains	Yes
DELEGATED PERMISSIONS	
<input checked="" type="checkbox"/> Access the directory as the signed-in user	No
Read directory data	Yes
Read and write directory data	Yes
<input type="checkbox"/> Read and write all groups	Yes
Read all groups	Yes
Read all users' full profiles	Yes
<input checked="" type="checkbox"/> Read all users' basic profiles	No
<input checked="" type="checkbox"/> Sign in and read user profile	No
Read hidden memberships	Yes

Select App registrations. Then click on the =Endpoints button to display urls for getting metadata.

The screenshot shows the 'App registrations' section in the Microsoft Azure portal. The left pane shows the 'App registrations' section with a list of app registrations. The right pane shows the 'Endpoints' tab with a table of endpoints.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
No results.		

Copy FEDERATION METADATA DOCUMENT and paste url into browser window or Postman to view metadata. Also copy SAML-P SIGN-ON ENDPOINT this url is used for Provider URI in next section.

[illegible]

Add Auth Service for SAML redirect.

Apps

Service Catalog

Learn

Support

R

S

Starting the Jo...
Development

Dashboard

Live Service

IDENTITY

Users

Mobile Identity Connect

Roles

DATA

Collections

Files

API Console

BUSINESS LOGIC

Collection Hooks

Custom Endpoints

Common Code

Scheduled Code

Mobile Identity Connect

Environment

Active

OAuth2

sdoauth

Make Default

salesforce mic

AUTH SERVICE ID: 6e7dd48808f64efaa39c76b5aa94f23f

OpenID Connect

Azure AD

Default

AUTH SERVICE ID: 55e054cabacd4f90abb610628646862c

+ Add Auth Service

Users of this app can authenticate with:

Username & Password

view docs

Google

view docs

Facebook

view docs

Twitter

view docs

LinkedIn

view docs

Salesforce

view docs

Auth Services allow you to integrate Kinvey with your own authentication provider (e.g. Active Directory, SAML, LDAP, etc.) so users can log in to your app via your existing identity management system.

+ Add Auth Service

SAML R

Azure AD Saml

« Return to environment

Description

Provider URI

https://login.microsoftonline.com/e740b2e9-edad-44d4-9ec5-733

Scope

ENVIRONMENT
Starting the Journey : Development

Redirect URI's

The URI that is invoked to pass an authorization grant code back to your app.

http://localhost:3000

+ ADD REDIRECT URI

Certificate Text

The X.509 Certificate text provided by the SAML Identity Provider

MIIDBTCCAe2gAwIBAgIQHU7yHxNEM7lBeqfRTMBhhtANBgkqhkiG9w0BAQsFADAIMSswKQYDVQQDEyhhY2NvdW50cy5kY2Nnc3RpZDQ5cm99LnRpbmRvdzQ3MubmVOMB4XDTA4MDAwODAwMDAwMFoXDTIwMDEwOTAwMDAwMFowLTERMAkGA1UEAxMiYWVWb3VudHMtYWNjaXNzY29udHJvbm93aW5kb3Q

Name ID Format URI

The format that Kinvey expects for the auth identifying NameID

urn:oasis:names:tc:SAML:1:1nameid-format:emailAddress

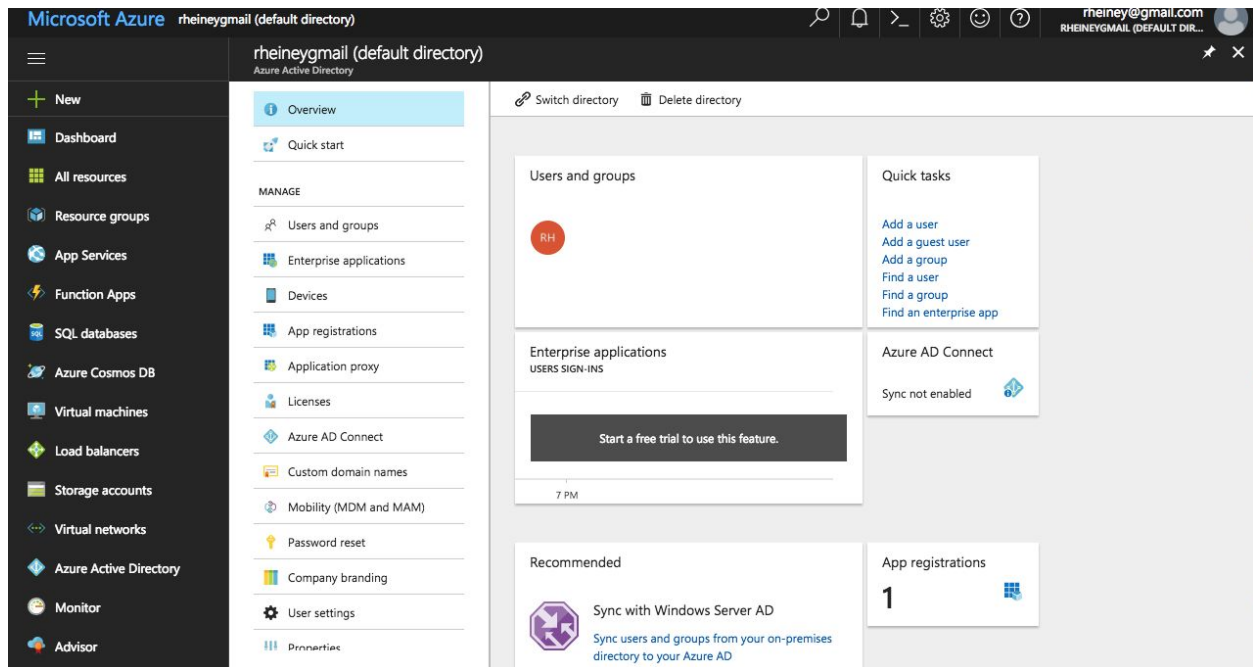
Feedback

Provider URI	The single sign-on service URL provided by the SAML Identity Provider in the endpoint section SAML-P SIGN-ON ENDPOINT
Redirect URI's	The OAuth 2.0 redirect URI to be used by the client app - example http://localhost:3000
Certificate Text	The X.509 Certificate text provided by the SAML Identity Provider from FEDERATION METADATA DOCUMENT located in previous endpoint section. <KeyDescriptor use="signing"> in metadata.
Name ID Format URI	The format that Kinvey expects for the auth identifying NameID urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

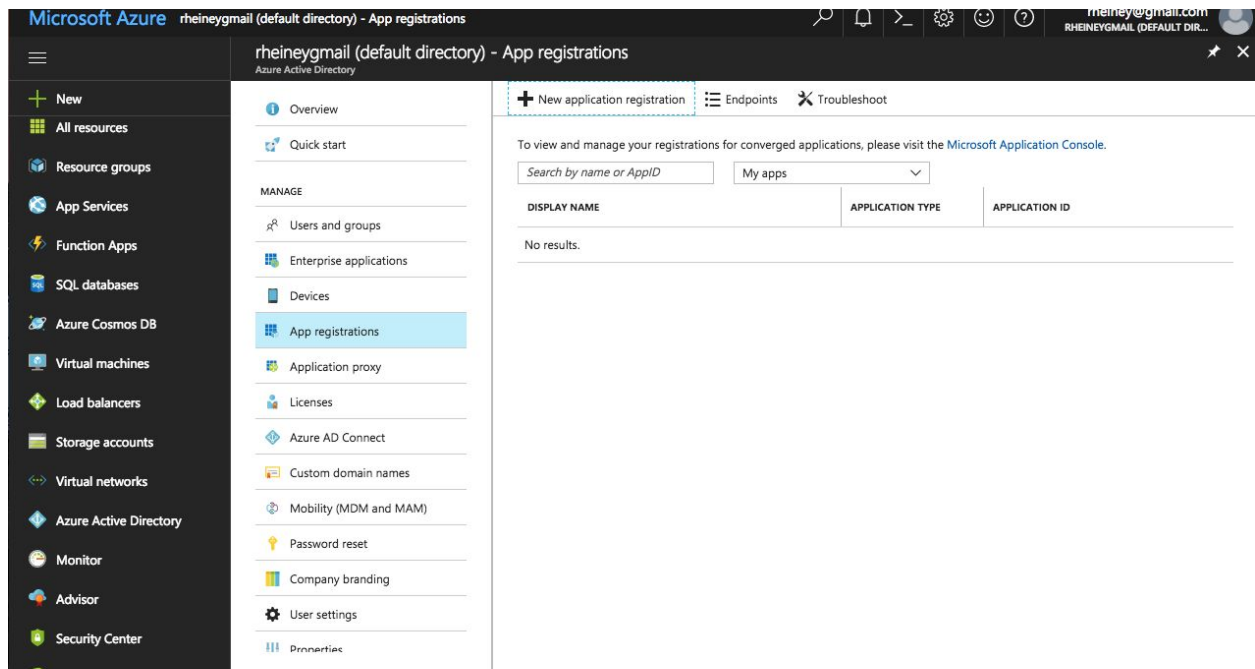
4. Azure OpenID connect integration

Create a new application

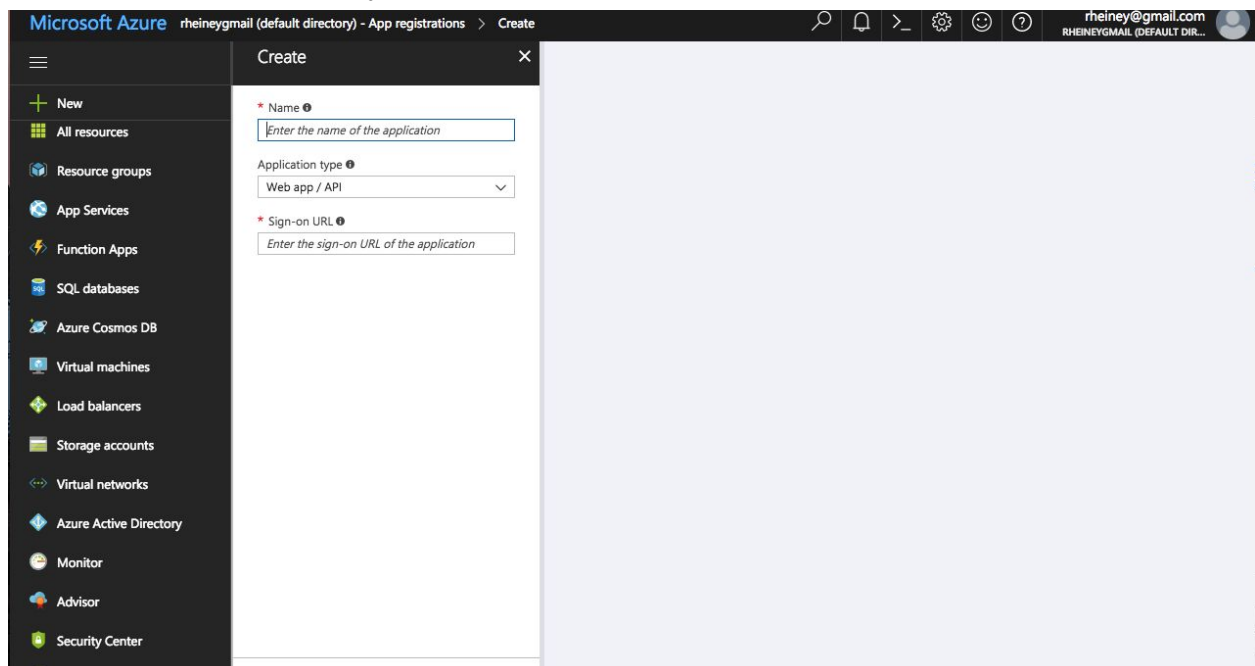
Login to Microsoft Azure at <https://portal.azure.com> and choose Azure Active Directory from the sidebar.



Select App registrations. Then click on the +New application registration button to add a new application.

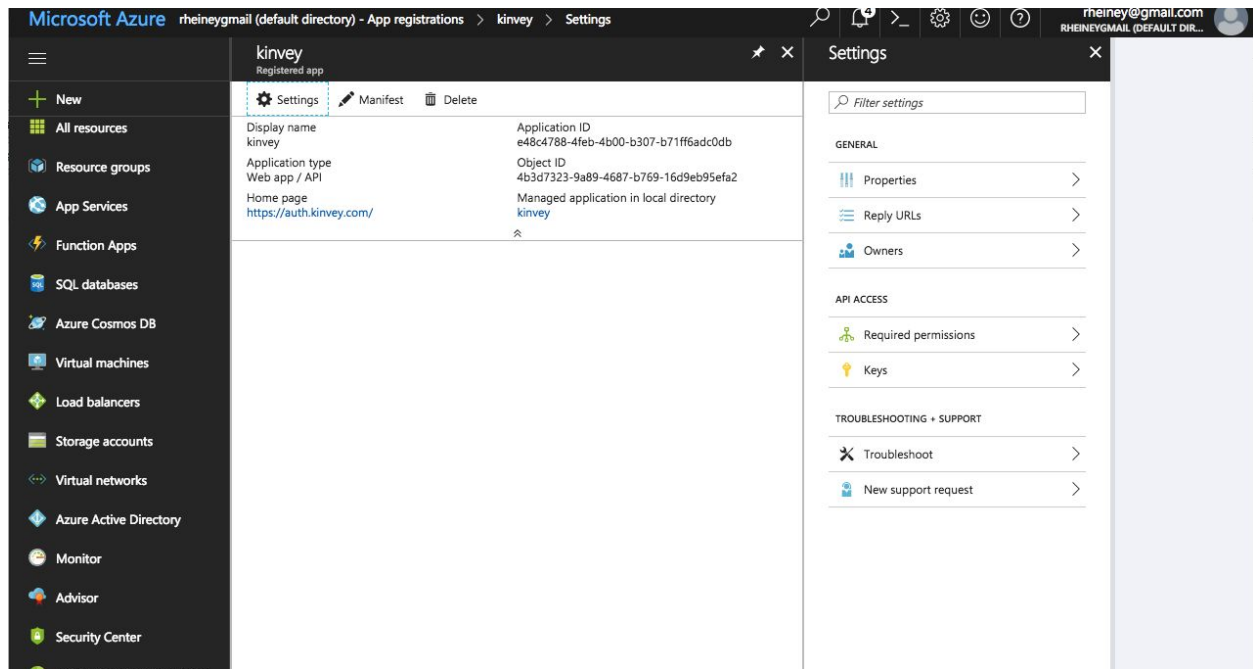


Enter a name for the application, select Web app/API as the Application Type, and for Sign-on URL enter https://auth.kinvey.com/.

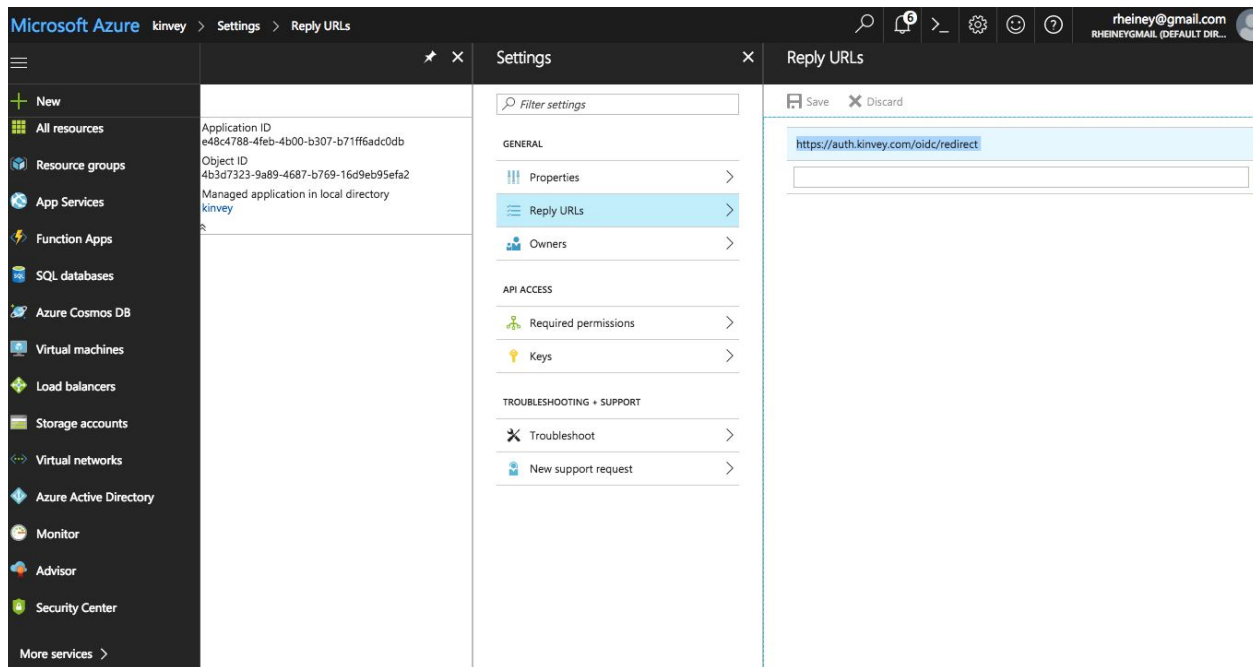


Configure Reply URLs

Then click on Settings and Reply URLs.

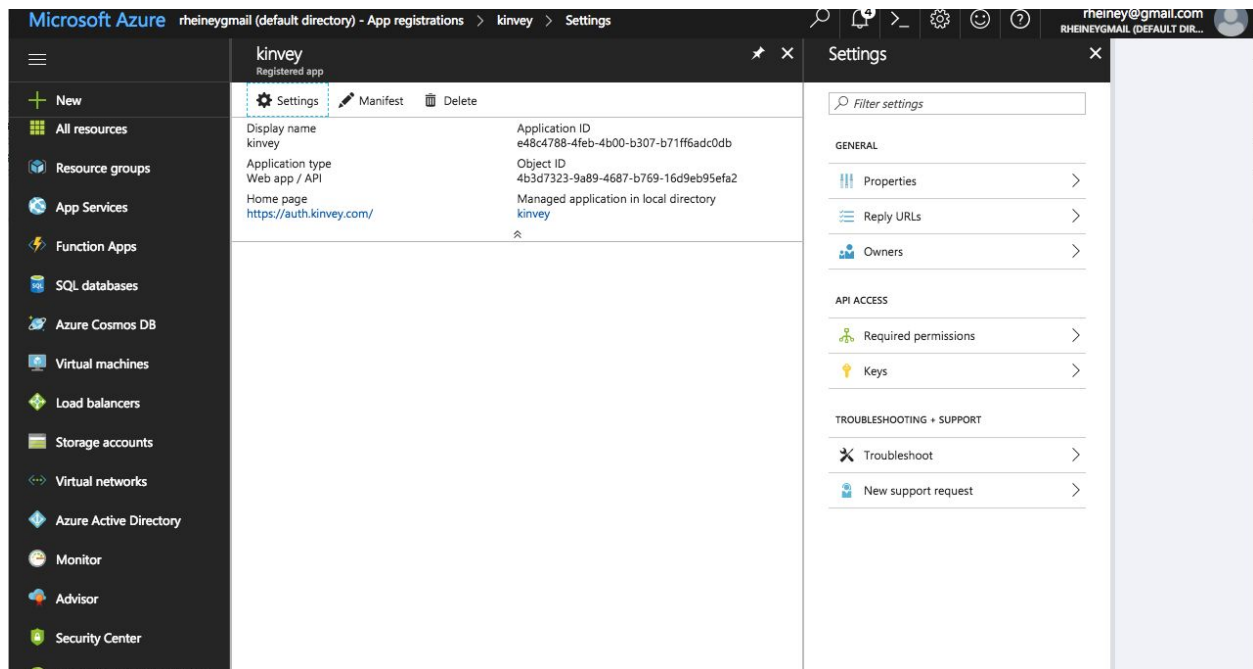


Set Reply URLs to <https://auth.kinvey.com/oidc/redirect>

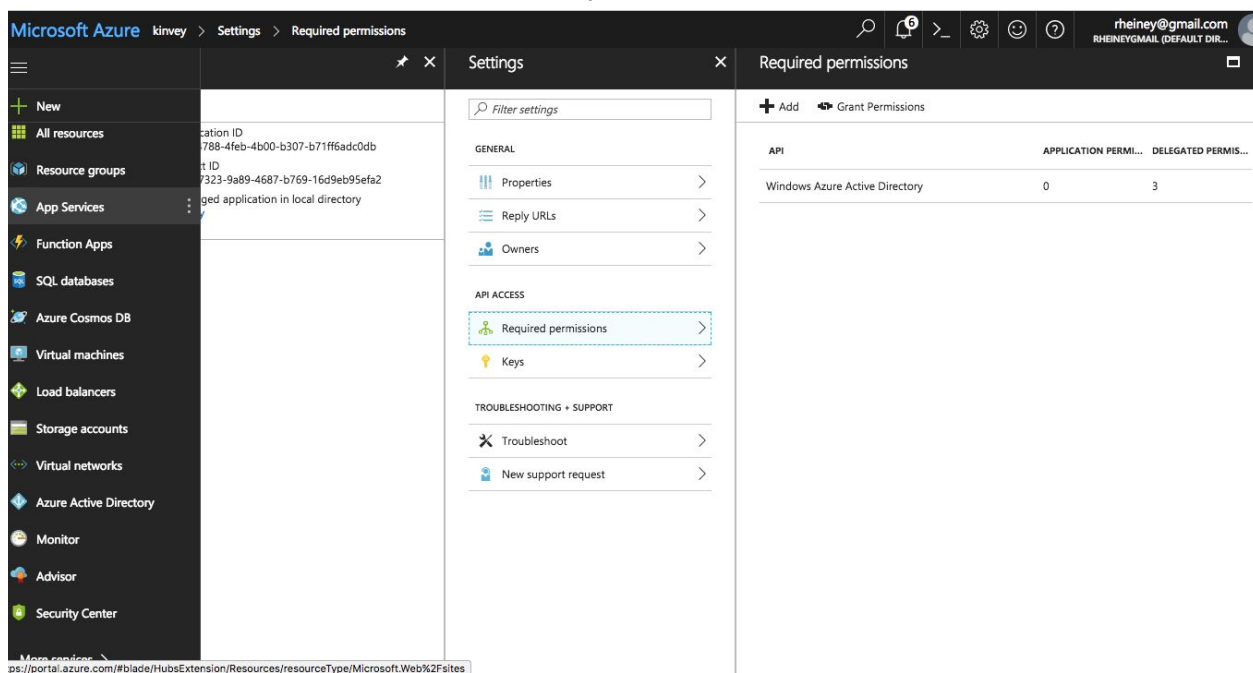


Configure the permissions

Then click on Settings and Required permissions.



Then click on Windows Azure Active Directory.



Check Access the directory as the signed-in user, Read all users basic profiles and Sign in and read user profile under Delegated Permissions.

The screenshot displays the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', and 'Security Center'. The main area is divided into two panels: 'Required permissions' and 'Enable Access'.

Required permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	3

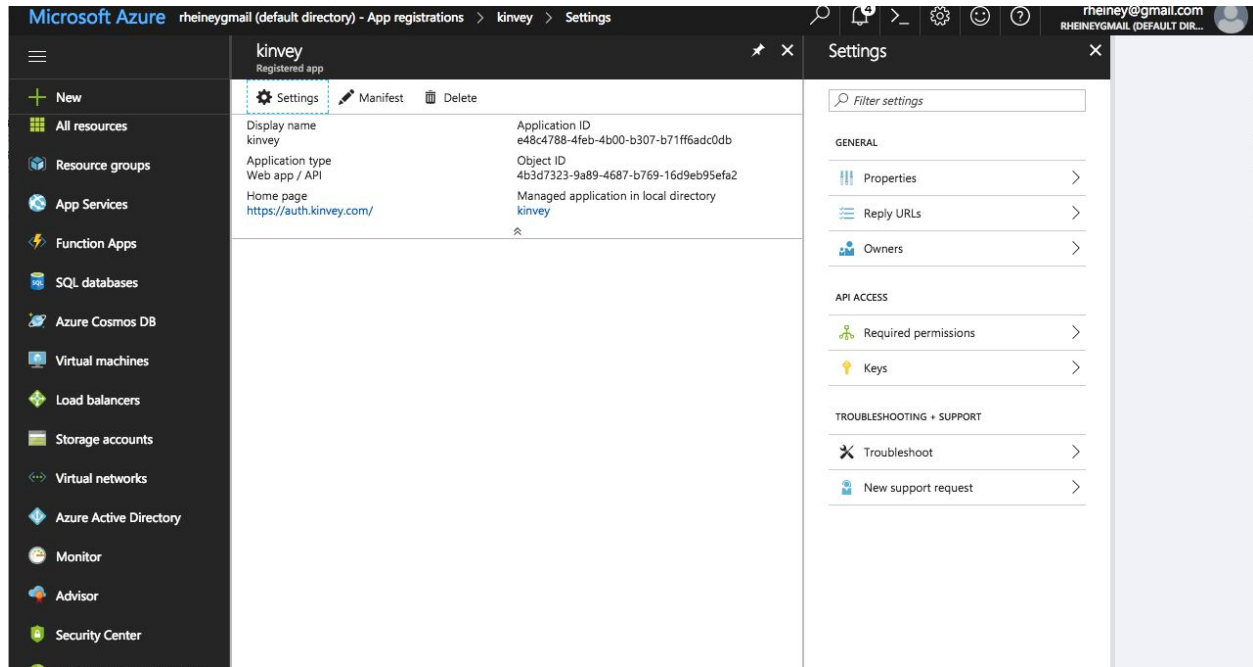
Enable Access
Windows Azure Active Directory

Save Delete

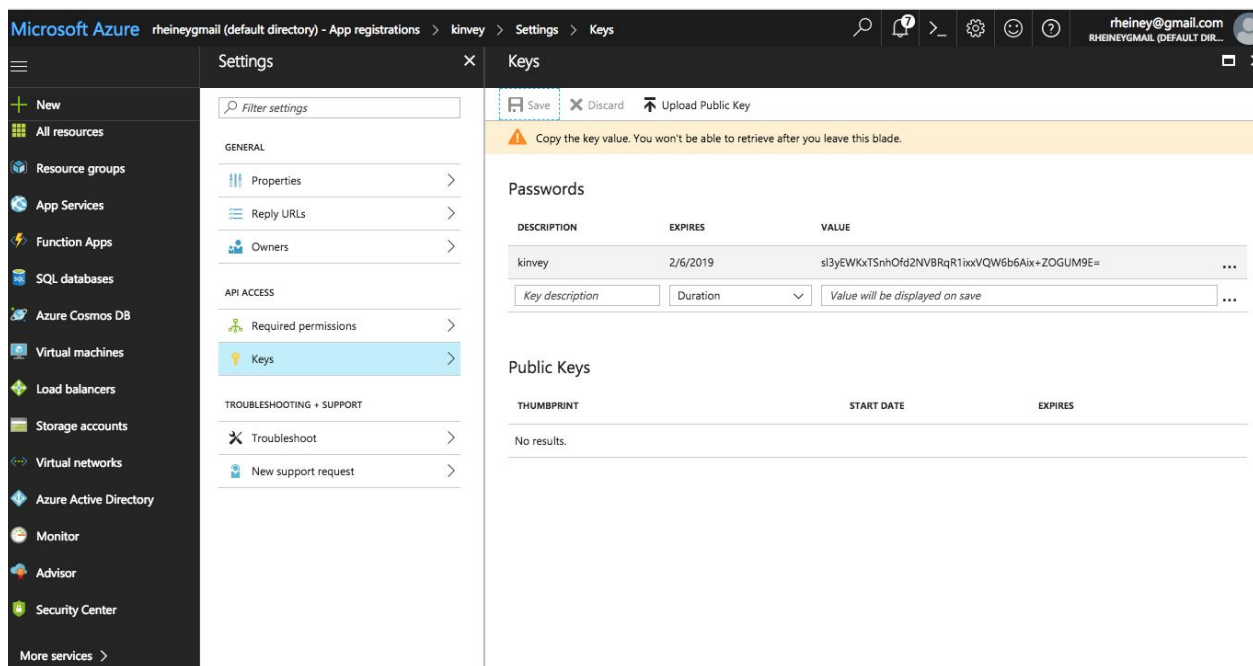
Read and write directory data	Yes
Read and write devices	Yes
Read all hidden memberships	Yes
Manage apps that this app creates or owns	Yes
Read and write all applications	Yes
Read and write domains	Yes
DELEGATED PERMISSIONS <small>Requires Admin</small>	
<input checked="" type="checkbox"/> Access the directory as the signed-in user	No
Read directory data	Yes
Read and write directory data	Yes
<input type="checkbox"/> Read and write all groups	Yes
Read all groups	Yes
Read all users' full profiles	Yes
<input checked="" type="checkbox"/> Read all users' basic profiles	No
<input checked="" type="checkbox"/> Sign in and read user profile	No
Read hidden memberships	Yes

Create the Client Secret

Next you will need to create a key which will be used as the Client Secret in Provider Configuration. Press Keys from the Settings menu



Set description and expiration. Press Save and the key will be displayed. Make sure to copy the value of this key before leaving this screen.



Configure Kinvey

Add Auth Service for OpenID Connect.

The screenshot shows the Kinvey Mobile Identity Connect interface. On the left is a sidebar with navigation options: Dashboard, Live Service, IDENTITY (Users, Roles), DATA (Collections, Files, API Console), and BUSINESS LOGIC (Collection Hooks, Custom Endpoints, Common Code, Scheduled Code). The main area is titled 'Mobile Identity Connect' and shows an 'Environment' section with a green 'Active' status. Two authentication services are listed: 'sdoauth' (Salesforce mic) with AUTH SERVICE ID: 6e7dd48808f64efaa39c76b5aa94f23f, and 'Azure AD' (OpenID Connect) with AUTH SERVICE ID: 55e054cabacd4f90abb610628646862c. A green '+ Add Auth Service' button is at the bottom of the list. On the right, a section titled 'Users of this app can authenticate with:' lists various providers: Username & Password, Google, Facebook, Twitter, LinkedIn, and Salesforce, each with a 'view docs' link. Below this is a paragraph explaining that Auth Services allow integration with external authentication providers like Active Directory, SAML, or LDAP.

Add the following fields specified on next page.

The screenshot shows the 'New OpenID Connect Service' setup form. The left sidebar has a 'Setup' button. The main form has four sections: 'Provider Configuration' with a 'Name *' field (placeholder: 'Service name'), 'Description' field (placeholder: 'Description'), 'Provider URI' field (placeholder: 'e.g. ldap-service.my-company.com'), and 'Scope *'. The 'Scope *' section includes explanatory text: 'Choosing an environment will make this service accessible to only that environment.' and 'Choosing an organization will make it accessible to any app in that organization.' It also features a radio button for 'Environment' (selected), an 'App' dropdown menu (currently showing 'Starting the Journey'), and an 'Environment' field.

This information can be obtained by the send a request using your tenant
<https://login.microsoftonline.com/{tenant}/.well-known/openid-configuration>

For more information see

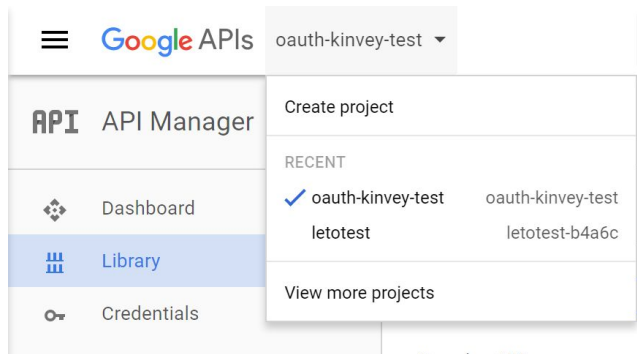
<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-openid-connect-code>

Provider URI	The token endpoint provided by the OpenID Connect Provider - token_endpoint in openid-configuration
Redirect URI's	The OAuth 2.0 redirect URI to be used by the client app - example http://localhost:3000
Grant Endpoint	The authorization grant endpoint provided by the OpenID Connect provider - authorization_endpoint in openid-configuration
Client Id	The client id supplied by the OpenID Connect provider - Application ID from Azure settings
Client Secret	The client secret supplied by the OpenID Connect provider - Client Secret saved previously in Azure settings
Issuer Identifier	The issuer identifier supplied by the OpenID Connect provider - issuer in openid-configuration
Scope	Any scope attributes as defined by the OpenID Connect provider. Include multiple scopes by inserting a space between each scope. profile email

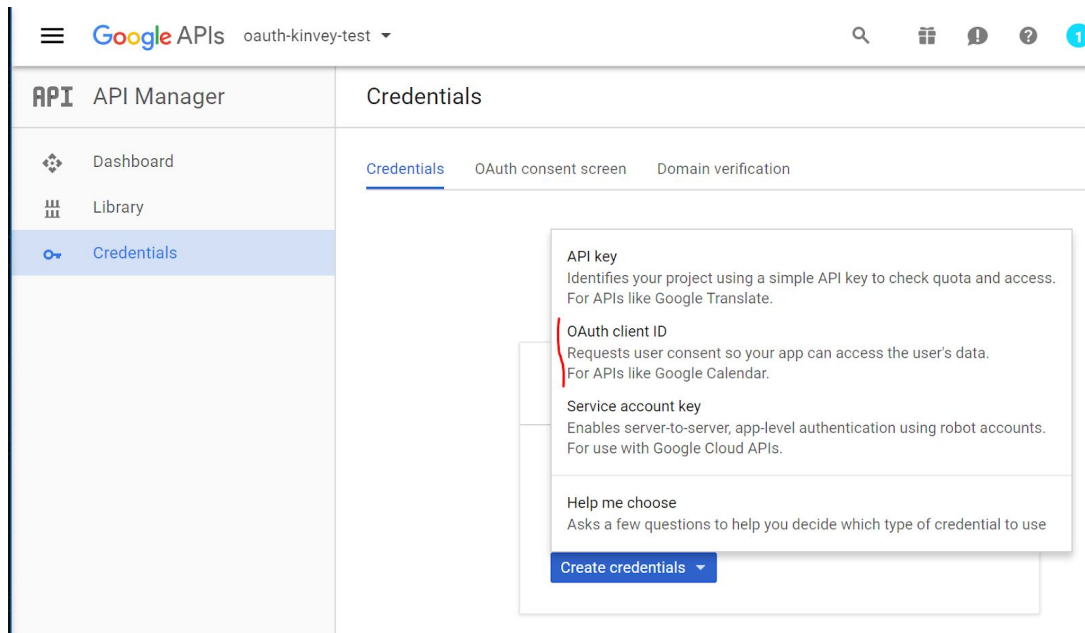
5. Google OAuth2 integration

Set up connected app in Google Developer Console

- Go to the Google developer portal at <https://console.developers.google.com/>
- Optionally, create new project



- Click on "Credentials" on the left, then "Create Credentials" and "OAuth Client ID"



- If needed, follow the Configure Consent Screen. There are no Kinvey-required settings here, you can fill out the consent screen as you like
- Select "Web Application", and set the Authorized Redirect URI to: <https://auth.kinvey.com/oauth2/redirect> (or use the appropriate uri for your dedicated instance, e.g. <https://com-us1-auth.kinvey.com/oauth2/redirect>)

API

API Manager

Dashboard

Library

Credentials

Credentials

←

Create client ID

Application type

☒ Web application
 ☐ Android [Learn more](#)
☐ Chrome App [Learn more](#)
☐ iOS [Learn more](#)
☐ PlayStation 4
 ☐ Other

Name

Kinvey test

Restrictions

Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI or (http://*.example.com) or a path (http://example.com/subdir) the origin URI.

http://www.example.com

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that will be used to receive the OAuth 2.0 response. The path will be appended with the query string. Cannot contain URL fragments or relative paths. Cannot be a

https://auth.kinvey.com/oauth2/redirect

http://www.example.com/oauth2callback

Create

Cancel

- Now copy down your client ID and secret from the result screen.

OAuth client

Here is your client ID

377503800353-qgcskrj9ssb1ckhrodi3kticgdj8t5.apps.googleusercontent.com

Here is your client secret

M1bjnZH5EpVoCZCSafRE6six

OK

Parameters in Kinvey Console

Now you can fill out the Kinvey MIC configuration screen:

- Type of provider: OAuth2
- Provider URI: <https://www.googleapis.com/oauth2/v3/token>
- Redirect URI: <https://console.kinvey.com> (or use your dedicated console url, e.g. <https://com-us1-console.kinvey.com>). DO NOT add a trailing slash.

- Grant Type: Authorization Code
- Grant Endpoint: <https://accounts.google.com/o/oauth2/auth>
- Client ID / Client Secret: As per the parameters received in the previous section
- User ID Attribute: leave blank
- User ID Endpoint: leave blank
- Scope: Add the API's that you have enabled for use with this MIC setup, e.g. "https://mail.google.com/ openid profile email". (see next section)
- Include client ID/secret in token request?: No
- Allowed attributes:
 - You must include "id" and "audience" minimally as allowed attributes

Provider Configuration

Type of Provider

Which auth service do you want to use?

OAuth2



Provider URI

https://www.googleapis.com/oauth2/v3/token

Redirect URI's

The URI that is invoked to pass an authorization grant code back to your app.

https://console.kinvey.com



kinveyTest://



[+ ADD REDIRECT URI](#)

Grant Type

The OAuth 2.0 Grant Type to be used.

Authorization Code



Grant Endpoint

The OAuth 2.0 authorization grant endpoint provided by the OAuth2 provider

https://accounts.google.com/o/oauth2/auth

Client ID

The client id supplied by the OAuth2 provider.

377503800353-qgcskrj9ssb1ckhrodij3kticgdj8t5.apps.googleusercontent.com

Client Secret

The client secret supplied by the OAuth2 provider

MlbjnZH5EpVoCZCSafRE6six

User ID Attribute

The attribute to be used to obtain the userid. If no User Id endpoint is supplied, the service will look for the specified attribute in the id_token attribute of the token response. If a User Id endpoint is supplied, a request will be made to that endpoint and the User Id will be obtained from the specified attribute.

adminbob

User ID Endpoint An endpoint from which to obtain the User Id, found in many OAuth2 implementations.	<input type="text" value="http://adminbob.example.com"/>
Scope Any scope attributes as defined by the OAuth2 provider.	<input type="text" value="https://mail.google.com/ openid profile email https://www.googleapis"/>
Include client id in token request? This will include the client id in the body of the OAuth2 token request instead of in the Authorization header.	No <input checked="" type="radio"/> Yes
Include client secret in token request? This will include the client secret in the body of the OAuth2 token request instead of in the Authorization header.	No <input checked="" type="radio"/> Yes

Allowed attributes	<input type="text" value="id"/> × <input type="text" value="audience"/> ×
---------------------------	--

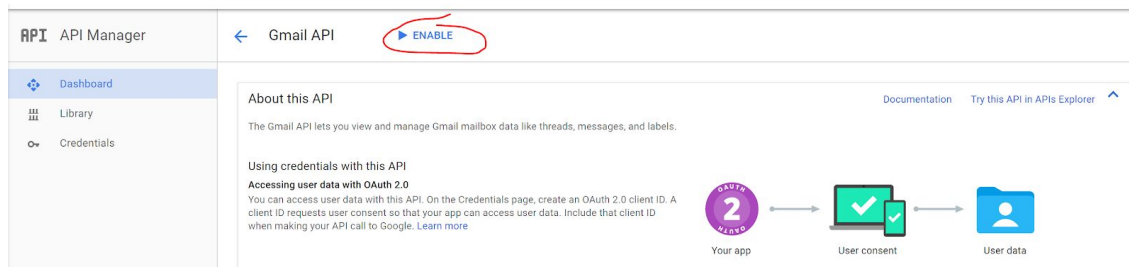
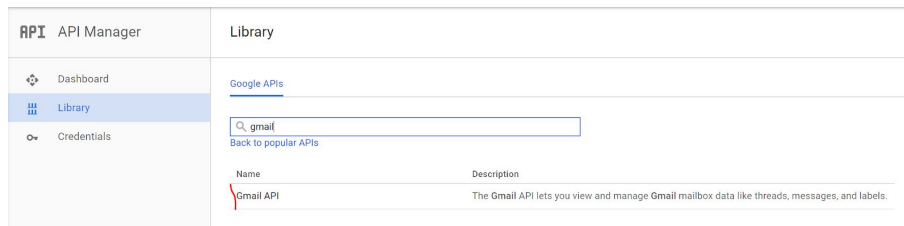
Enable API's to use this Connected App

- Go back to your main Dashboard by clicking on "Dashboard" in the left tab
- Enable some API's

API API Manager	Dashboard + ENABLE API
Dashboard	Enabled APIs No APIs are enabled
Library	
Credentials	

Each API has a corresponding "scope" that can be found in the documentation. This scope must be added to the "scope" list in the MIC config if you want to use this API in subsequent data access.

As an example, we'll enable the GMail API so that you can see your google mail via Kinvey connectors:



Click on the "Try this API in APIs Explorer" to quickly learn about scopes. In the APIs Explorer screen, click on "Authorize requests using OAuth 2.0". You will be presented with an overview of all scopes relevant to the GMail API. Confusingly enough, some of these scopes start with `https://`. Copy these scopes into your MIC config screen.

Select OAuth 2.0 scopes:

Scopes are used to grant an application different levels of access to data on behalf of the end user. Each API may declare one or more scopes. [Learn more about OAuth 2.0](#)

Gmail API declares the following scopes. Select which ones you want to grant to APIs Explorer.

- ☐ <https://mail.google.com/>
View and manage your mail
- ☐ <https://www.googleapis.com/auth/gmail.compose>
Manage drafts and send emails
- ☐ <https://www.googleapis.com/auth/gmail.insert>
Insert mail into your mailbox
- ☐ <https://www.googleapis.com/auth/gmail.labels>
Manage mailbox labels
- ☐ <https://www.googleapis.com/auth/gmail.metadata>
View your email message metadata such as labels and headers, but not the email body
- ☐ <https://www.googleapis.com/auth/gmail.modify>
View and modify but not delete your email
- ☐ <https://www.googleapis.com/auth/gmail.readonly>
View your emails messages and settings
- ☐ <https://www.googleapis.com/auth/gmail.send>
Send email on your behalf
- ☐ <https://www.googleapis.com/auth/gmail.settings.basic>
Manage your basic mail settings
- ☐ <https://www.googleapis.com/auth/gmail.settings.sharing>
Manage your sensitive mail settings, including who can manage your mail

Add additional scopes (optional):

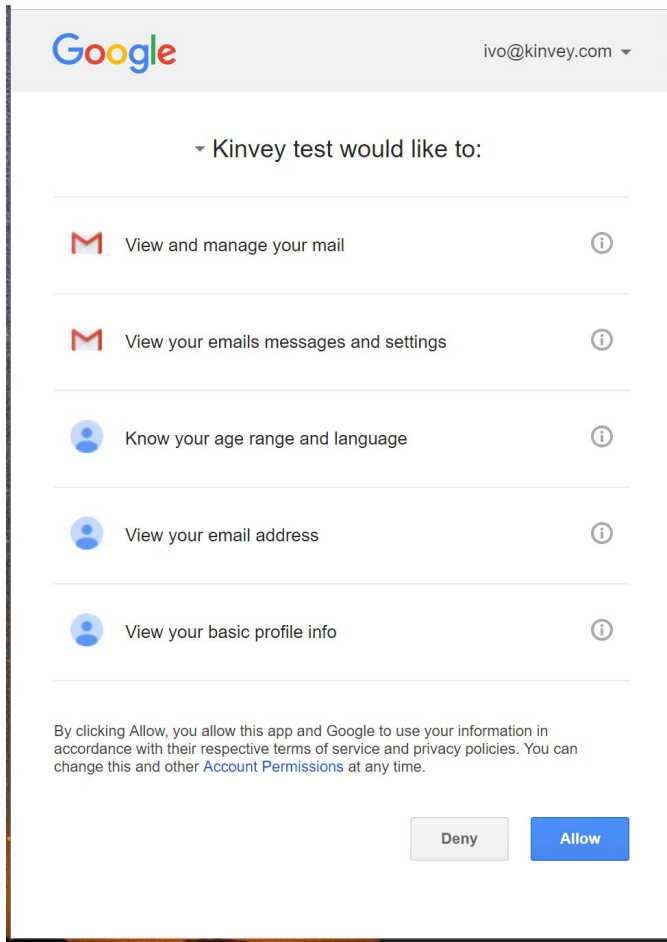
Authorize

Cancel

Testing the MIC config via the Console

In the API console, you can attempt a MIC login:

- Go to the API console.
- Click on "Show Options"
- Click on "Authentication", and select "Mobile Identity Connect".
 - You can leave the API version to its default (currently v3)
- Click "Login with Mobile Identity Connect"
- You will now be entered into a MIC login flow utilizing your new setup. You should see your "connected app name" near the top, and the scopes you selected are available for review in the consent screen:



- Click "Allow". You are now logged in to Kinvey via MIC.
- You can verify the successful login by inspecting your user record in the Users collection:

ivotest

oauthtest

Dashboard

IDENTITY

Users

Users

Collect

Filter collections...

1 of 1 users

+ Column

+ User

_id	_acl	_kmd	_socialIdentity	username
586be4543260b045382a420	{ "creator": "586be454326"	{ "lmt": "2017-01-03T17:5	{ "kinveyAuth": { "access_	"6d69529f-4b4d-4e6a-b99!

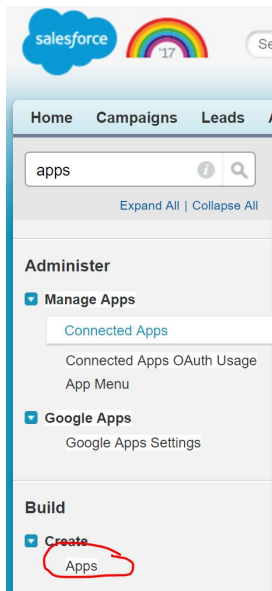
- Click on the "_socialIdentity" pop-out to inspect further properties of your login:

```
{ "kinveyAuth": {
  "access_token": "926ade9081a27e78ccbac0f54ce06399658d5bef", "refresh_token": "09f549069b55d0841b210a5c8b5e6e3d7e7c3452", "audience": "kid_ZKbrghVtUe", "id": "104144628994578148602", "client_token": "
  { "access_token": "ya29.C1IA9e1NyghVaDy3Mx7n3tw10Hg14eIdFr25_AWRawvynJRSegYMKtw52qDC8bHxg", "token_type": "Bearer", "expires_in": 3599, "id_token": "
  { "iss": "accounts.google.com", "iat": 1483465810, "exp": 1483469410, "at_hash": "nab2hByV9orgesc0Mah_4g", "aud": "377503800353-
  qgcskrj9ssb1ckhrodij3kticdgdj8t5.apps.googleusercontent.com", "sub": "104144628994578148602", "email_verified": true, "azp": "377503800353-
  qgcskrj9ssb1ckhrodij3kticdgdj8t5.apps.googleusercontent.com", "hd": "kinvey.com", "email": "ivo@kinvey.com"}}, "access_token_secret": null}}
```


6. Salesforce authentication integration

Set up connected app in Salesforce

- Log in to Salesforce (Classic Mode explained here) as a System Administrator role
- Search for "Apps" in the QuickFind menu. Click "Build -> Create -> Apps"



- Scroll down to "Connected Apps" near the bottom and click "New"
- Fill out Basic Information.
- Click "Enable OAuth Settings". Use these settings:
 - Enable for Device Flow: no
 - Callback URL: <https://auth.kinvey.com/oauth2/redirect> (or use the appropriate uri for your dedicated instance, e.g. <https://com-us1-auth.kinvey.com/oauth2/redirect>)
 - Use digital signatures: no
 - Selected OAuth Scopes: minimum required
 - Access and manage your data (api)
 - Access your basic information (id, profile, email, address, phone)
 - Allow access to your unique identified (openid)
 - Require Secret for Webserver: yes
 - Include ID token: yes
 - Include Standard claims: yes
 - Enable Asset tokens: no

Your screen will look like this:

▼ API (Enable OAuth Settings)

Enable OAuth Settings ☒

Enable for Device Flow ☐

Callback URL

Use digital signatures ☐

Selected OAuth Scopes

Available OAuth Scopes

- Access and manage your Chatter data (chatter_api)
- Access and manage your Eclair data (eclair_api)
- Access and manage your Wave data (wave_api)
- Access custom permissions (custom_permissions)
- Full access (full)
- Perform requests on your behalf at any time (refresh_token, offline_access)
- Provide access to custom applications (visualforce)
- Provide access to your data via the Web (web)

Add

Remove

Selected OAuth Scopes

- Access and manage your data (api)
- Access your basic information (id, profile, email, address, phone)
- Allow access to your unique identifier (openid)

Require Secret for Web Server Flow ☒

Include ID Token ☒

Enable Asset Tokens ☐

Include Standard Claims ☒

Include Custom Attributes ☐

Include Custom Permissions ☐

- In the resulting screen, copy the "Consumer Key" and "Consumer Secret"

▼ API (Enable OAuth Settings)

Consumer Key 3MVG9K12HHAq33RwE.RGCS1JtHX4AuZnbdLnVsfbaetuRopFO7jByf.X3z4AO3LyEukTYFtzR8lCqnMLZB3

Consumer Secret 6149602006980979952

Selected OAuth Scopes

- Access your basic information (id, profile, email, address, phone)
- Access and manage your data (api)
- Allow access to your unique identifier (openid)

Callback URL https://auth.kinvey.com/oauth2/redirect

Enable for Device Flow ☐

Require Secret for Web Server Flow ☒

Token Valid for 0 Hour(s)

Include Custom Attributes ☐

Include Custom Permissions ☐

Parameters in Kinvey Console

Now you can fill out the Kinvey MIC configuration screen:

- Type of provider: OAuth2
- Provider URI: <https://login.salesforce.com/services/oauth2/token>
- Redirect URI: <use your redirect URI that you define in the MIC SDK call in your app here>
- Grant Type: Authorization Code
- Grant Endpoint: <https://login.salesforce.com/services/oauth2/authorize>
- Client ID / Client Secret: As per the parameters received in the previous section
- User ID Attribute: leave blank

- User ID Endpoint: leave blank
- Scope: Add the API's that you have enabled for use with this MIC setup, e.g. "id api openid". (see next section)
- Include client ID/secret in token request?: YES on both
- Allowed attributes:
 - You must include "id" and "audience" minimally as allowed attributes

Your screen will look like this:

Provider Configuration	
Type of Provider Which auth service do you want to use?	OAuth2 ▼
Provider URI	https://login.salesforce.com/services/oauth2/token
Redirect URI's The URI that is invoked to pass an authorization grant code back to your app.	http://localhost:8100 × + ADD REDIRECT URI
Grant Type The OAuth 2.0 Grant Type to be used.	Authorization Code ▼
Grant Endpoint The OAuth 2.0 authorization grant endpoint provided by the OAuth2 provider	https://login.salesforce.com/services/oauth2/authorize
Client ID The client id supplied by the OAuth2 provider.	3MVG9K12HHAq33RwE.RGCS1JtHX4AuZnbdLNvSfgbauetuRopF07jByf.X3z4AO3LyEukTYFi
Client Secret The client secret supplied by the OAuth2 provider	6149602006980979952
User ID Attribute The attribute to be used to obtain the userId. If no User Id endpoint is supplied, the service will look for the specified attribute in the id_token attribute of the token response. If a User Id endpoint is supplied, a request will be made to that endpoint and the User Id will be obtained from the specified attribute.	adminbob

User ID Endpoint
An endpoint from which to obtain the User Id, found in many OAuth2 implementations.

http://adminbob.example.com

Scope
Any scope attributes as defined by the OAuth2 provider.

id api openid

Include client id in token request?
This will include the client id in the body of the OAuth2 token request instead of in the Authorization header.

No ☒ Yes

Include client secret in token request?
This will include the client secret in the body of the OAuth2 token request instead of in the Authorization header.

No ☒ Yes

Allowed attributes

id

audience

Forward Salesforce attributes to your datalink

- If you use RAPID, then you can simply enable "Use MIC" in the RAPID definition.

Kinvey needs to be able to connect to Salesforce to use it as a Data Source. Add your connection info below. If you aren't sure what these settings are, try contacting Salesforce administrator.

Host *
Enter the host address

https://login.salesforce.com

Kinvey also needs to be able to authenticate with Salesforce to ensure it can access the relevant data.

Authenticate via

☒ Mobile Identity Connect (MIC)
☐ Service Account
☐ Service Account OAuth

Destroy

Save

- If you use a custom datalink, and you need to forward the Salesforce token and instance_url to the backend, then you'll need to map these two attributes for forwarding to the DLC:

- `client_token` to X-Kinvey-AuthToken
- `Instance_url` to X-Kinvey-Salesforce-eURL

Data Link Header Mappings	
<code>client_token</code>	X-Kinvey-AuthToken
<code>instance_url</code>	X-Kinvey-Salesforce-eURL

[+ ADD HEADER MAPPING](#)

Testing the MIC config via the Console

In the API console, you can attempt a MIC login:

- Go to the API console.
- Click on "Show Options"
- Click on "Authentication", and select "Mobile Identity Connect".
 - You can leave the API version to its default (currently v3)
- Click "Login with Mobile Identity Connect"
- You will now be entered into a MIC login flow utilizing your new setup. You should see your "connected app name" near the top (in this case just "test"), and the scopes you selected are available for review in the consent screen:

The left screenshot shows the Salesforce login page. The username field contains 'ivo@kinvey.com.demo'. The password field is masked with dots. Below the password field is a 'Log In' button. There are also links for 'Forgot Your Password?' and 'Use Custom Domain'.

The right screenshot shows the 'Allow Access?' screen. It lists the permissions requested by the 'test' app: 'Access your basic information', 'Allow access to your unique identifier', and 'Access and manage your data'. Below the list, it asks 'Do you want to allow access for ivo@kinvey.com.demo? (Not you?)' and provides 'Deny' and 'Allow' buttons. At the bottom, it says 'To revoke access at any time, go to your personal settings.'

- Click "Allow". You are now logged in to Kinvey via MIC.
- You can verify the successful login by inspecting your user record in the Users collection:

_ivotest

sfdc-mic

Dashboard

IDENTITY

Users

Users

Q

Filter users...

Adv. ▾

1 of 1 users

_id ▾	_acl	_kmd	_socialIdentity	username
58ebdfa248cb8a1a42884729	{\"creator\": \"58ebdfa248cb8a1a42\", \"lmt\": \"2017-04-10T19:40:18.75\", \"kinveyAuth\": {\"access_token\": \"9e30e8fa-65df-4f5c-8847-c029c\"}}			

- Click on the "_socialIdentity" pop-out to inspect further properties of your login:

```

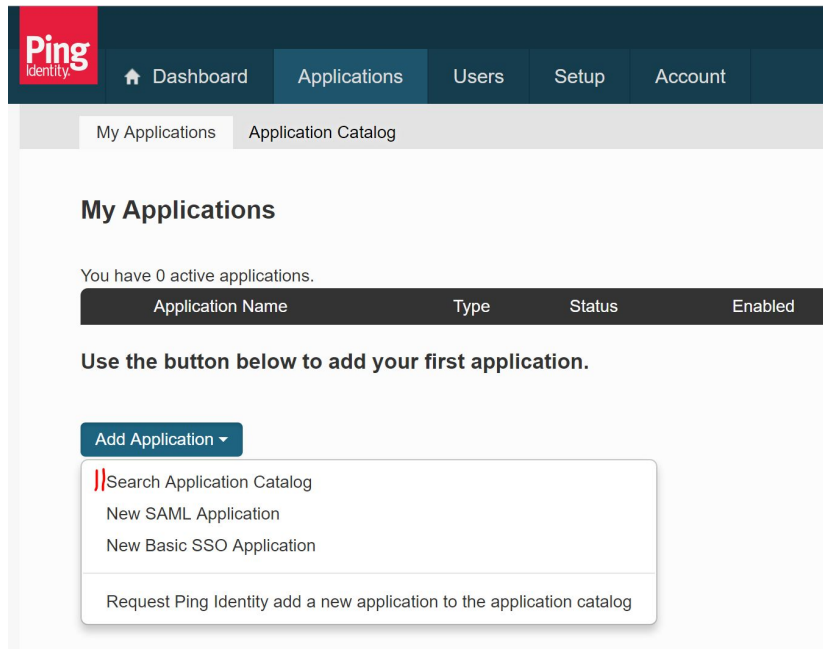
1 {
2   "kinveyAuth": {
3     "access_token": "678cb5e287ae1c0c39dd095af087ab6e2247a5b61",
4     "refresh_token": "6b717f1bc79a3af0507a2b46767f24474ecb8253",
5     "id": "https://login.salesforce.com/id/00D61000000IOxjEAG/00561000002L5qxAAC",
6     "audience": "kid_B1VsiQFT1",
7     "client_token": "
8     {\\"access_token\\":\\"00D61000000IOxjIASAAQIBsw0bf0vk5_eaM_618Zn9DshsdMuO.FBcPkjtUHFjISixHAR5dz0.5CpatVnjdS_tz7eNGaMiShz0P1fLZALN
9     openid id api\\",\\"id_token\\":{\\"at_hash\\":\\"ad7etdSUTPL5J-
10    PHb5LG0g\\",\\"sub\\":\\"https://login.salesforce.com/id/00D61000000IOxjEAG/00561000002L5qxAAC\\",\\"zoneinfo\\":\\"America/El_Salvador\\
11    region=null, country=null, postal_code=null\\",\\"profile\\":\\"https://kinveydemo-dev-
12    ed.my.salesforce.com/00561000002L5qxAAC\\",\\"iss\\":\\"https://login.salesforce.com\\",\\"preferred_username\\":\\"ivo@kinvey.com.demo
13    dev-ed--c.na34.content.force.com/profilephoto/005/F\\",\\"custom_attributes\\":{\\"ivoinstanceurl\\":\\"https://kinveydemo-dev-
14    ed.my.salesforce.com/services/Soap/c/38.0/00D61000000IOxjivo@kinvey.com.demo\\",\\"aud\\":\\"3MVG9KI2HHaq33RwE.RGCS1JtHc.L2XN9j8iV
15    16:40:12 GMT 2017\\",\\"nickname\\":\\"ivo\\",\\"name\\":\\"Ivo
16    Janssen\\",\\"phone_number\\":null,\\"exp\\":1491853335,\\"iat\\":1491853215,\\"family_name\\":\\"Janssen\\",\\"email\\":\\"ivo@kinvey.com\\",
17    ed.my.salesforce.com\\",\\"id\\":\\"https://login.salesforce.com/id/00D61000000IOxjEAG/00561000002L5qxAAC\\",\\"token_type\\":\\"Bearer\\
18    \"access_token_secret\\": null
19  }
20 }

```

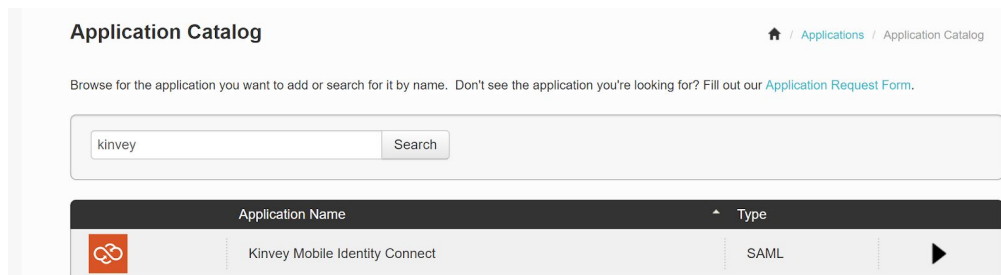

7. Ping integration (*NOT WORKING CURRENTLY!*)

Set up connected app in Google Developer Console

- Go to the Ping admin portal at <https://admin.pingone.com>
- Click on Applications in the top navbar and select "Add Application", and click on "Search Application Catalog"



- Search for the Kinvey connector in the catalog



- Click "Setup"
- <NEED MORE INFO HERE>

Parameters in Kinvey Console

Now you can fill out the Kinvey MIC configuration screen. From the PingOne details screen for your newly created application, download the "Signing Certificate" and the "SAML Metadata".

Open both in a text editor.

- Type of provider: SAML-Redirect
- Provider URI: Use "*SingleSignOnService*" from the metadata. It looks like this:
<https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=abc123-a...>
- Redirect URI: <https://console.kinvey.com> (or use your dedicated console url, e.g. <https://com-us1-console.kinvey.com>). DO NOT add a trailing slash.
- Logout URI: Use "https://sso.connect.pingidentity.com/sso/SLO.saml2"
- Certificate text: Copy paste text from the Signing Certificate (including the "-----" header and footer) into the textbox in the Kinvey console
- Name ID Format URI: Use
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
- Allowed attributes:
 - You must include "id" and "audience" minimally as allowed attributes

In your app

- Make sure to leave the MICApiVersion set to v1 (which is the default for most SDK's, but you must specifically set it to v1 in the Kinvey Console)

Testing the MIC config via the Console

In the API console, you can attempt a MIC login:

- Go to the API console.
- Click on "Show Options"
- Click on "Authentication", and select "Mobile Identity Connect".
 - What is the MIC API versions?
- Click "Login with Mobile Identity Connect"
- You will now be entered into a MIC login flow utilizing your new setup. You should see your "connected app name" near the top, and the scopes you selected are available for review in the consent screen:

(screenshot needed)

- Click "Allow". You are now logged in to Kinvey via MIC.
- You can verify the successful login by inspecting your user record in the Users collection:

(screenshot needed)

- Click on the "_socialIdentity" popup to inspect further properties of your login:

(screenshot needed)