SureCloud®

# Enterprise Identity Server

## SSO Setup Guide

Version 1.1

# Contents

# Introduction

The SureCloud Enterprise Identity Server allows a user to link a SureCloud account to their organisational user account and login through their organisation's portal. (e.g. Azure)

The steps to accomplish this are as follows:

- SureCloud need to configure a mapping for your domain (e.g. org1.com) to inform the platform that any user with this domain will be redirected to your authentication server.
- SureCloud need to configure a connector within the platform which will redirect a user to your identity server, depending on your identity server we will also need some information from you.

SureCloud supports the following authentication technologies:

- ADFS – Active Directory Federated Services
- SAMLP Identity Provider
- SharePoint Apps
- Google Apps
- Office 365
- Microsoft Azure AD

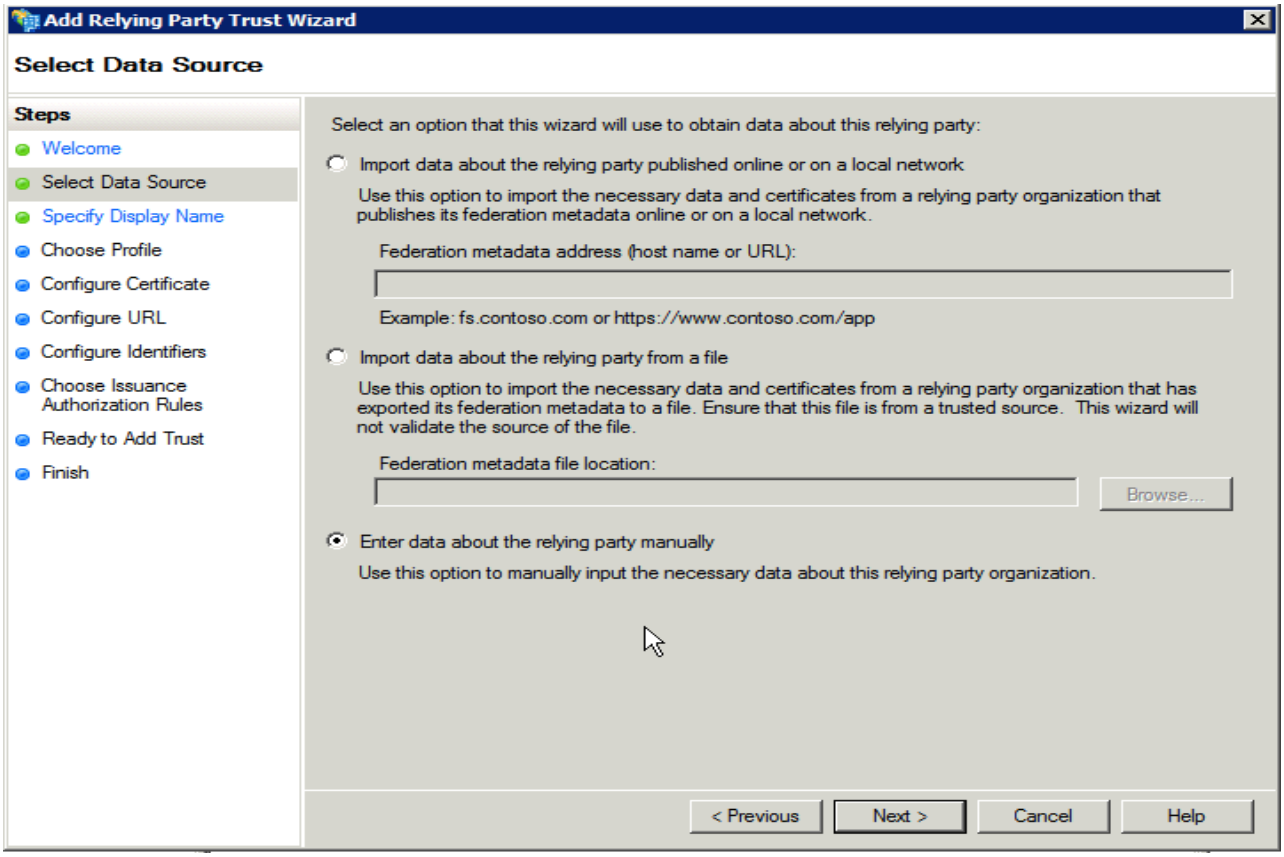
We provide connector configuration details for ADFS and Azure AD (see below) please contact us if you would like to configure any of the other technologies listed above and we can setup info for those as well.

We support both IdP and SP initiated login flows (**Note:** IdP initiated is only supported when using a SAML connector)

In IdP initiated SSO a.k.a. Unsolicited Web SSO, the federation process is initiated by the IdP sending an unsolicited SAML response to the SP. In SP initiated, the SP generates an request that is sent to the IdP as the first step in the federation process and the IdP then responds with a SAML response

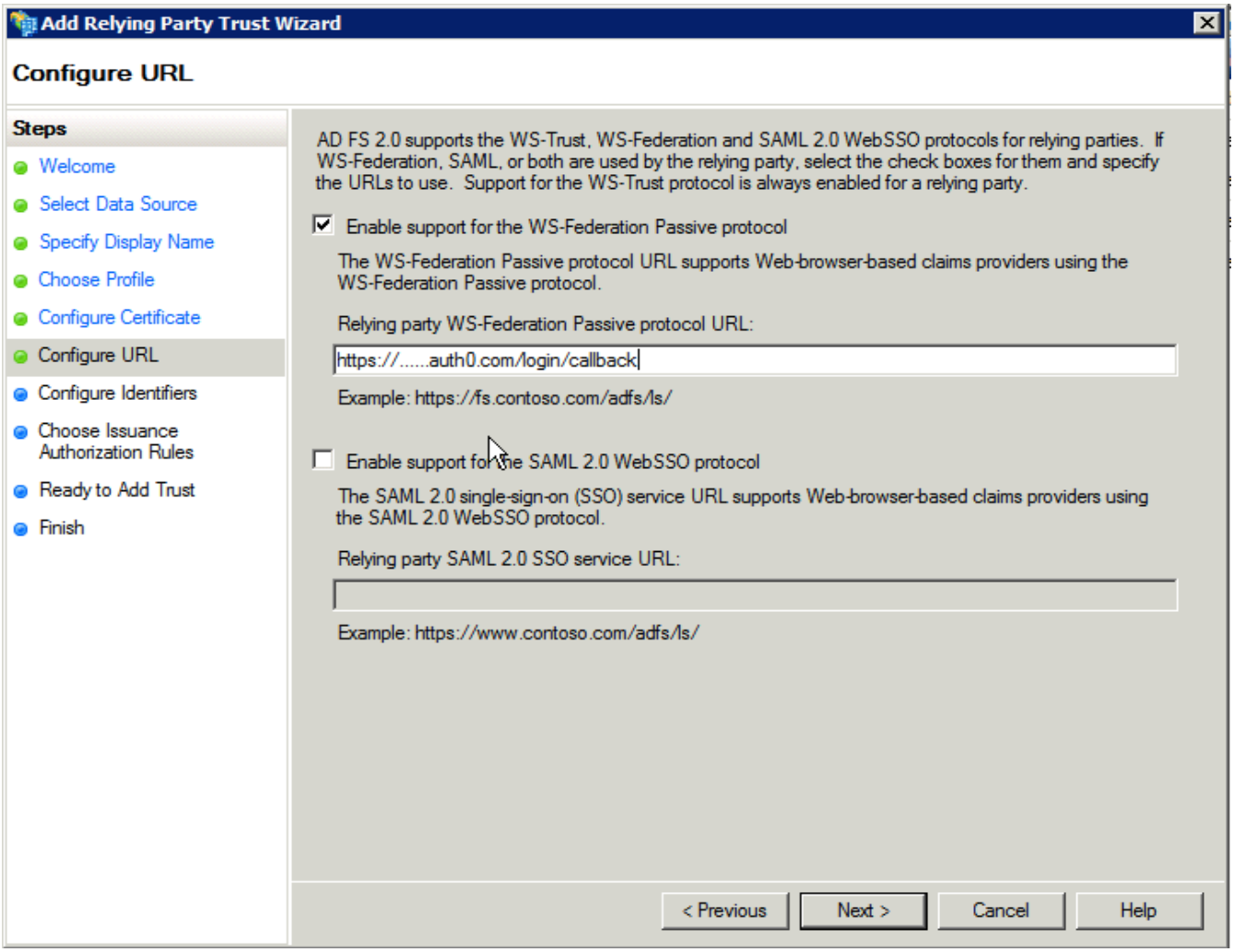
# ADFS Connector Configuration

1. Open the ADFS Management Console.
2. Click on Add Relying Party Trust.
3. Click Start on the first step.
4. Select Enter data about the relying party manually and click Next.



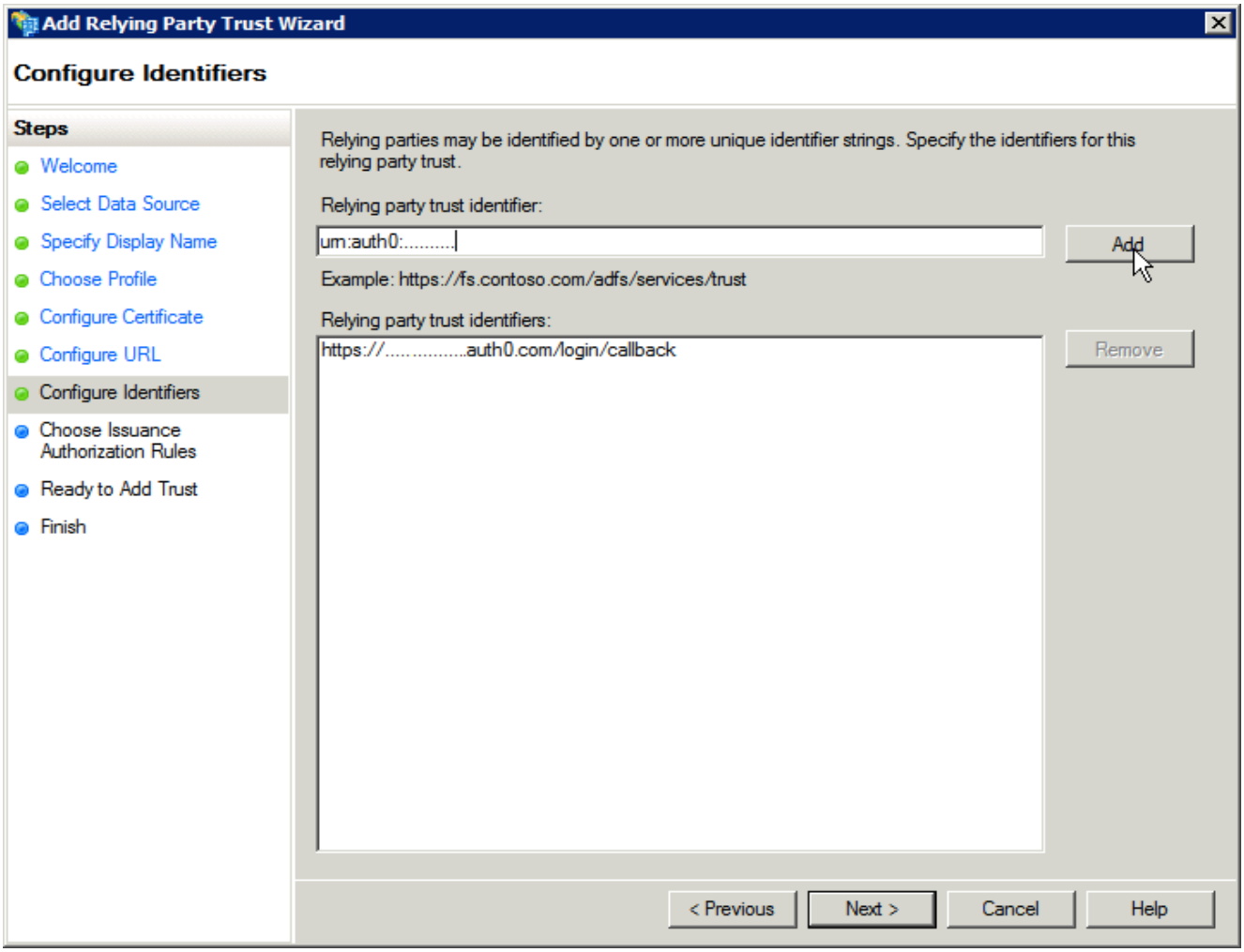

5. Enter an arbitrary name (e.g. "SureCloud Platform") and click Next.
6. Leave the default selection (*ADFS 2.0 profile*) and click Next.
7. Leave the default (*no encryption certificate*) and click Next.
8. Check Enable support for the WS-Federation..., enter the following value in the textbox and click Next.

   https://surecloud.eu.auth0.com/login/callback

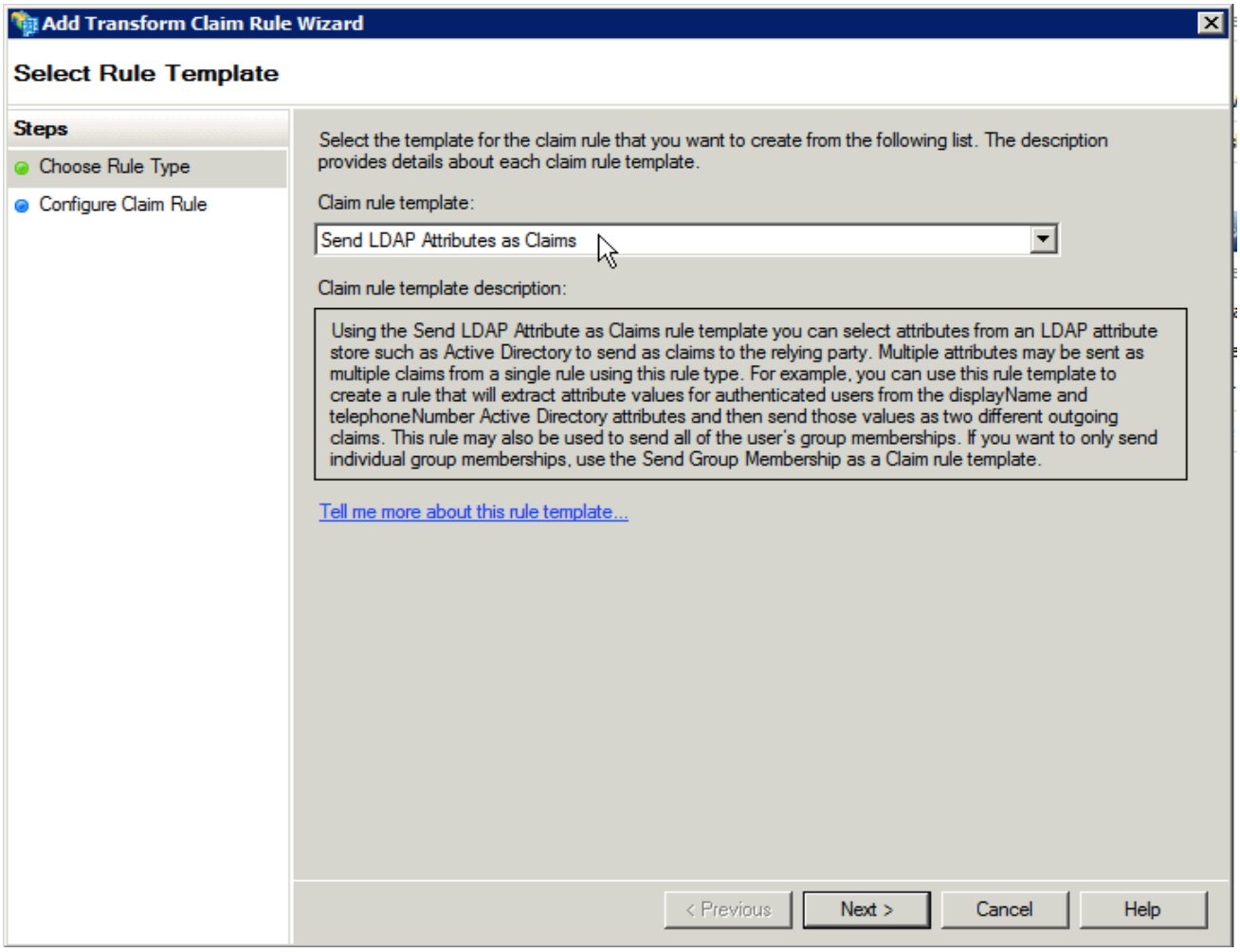



9. Add a *Relying party trust identifier* with the following value and click Add and then Next.

   ```
   urn:auth0:surecloud
   ```



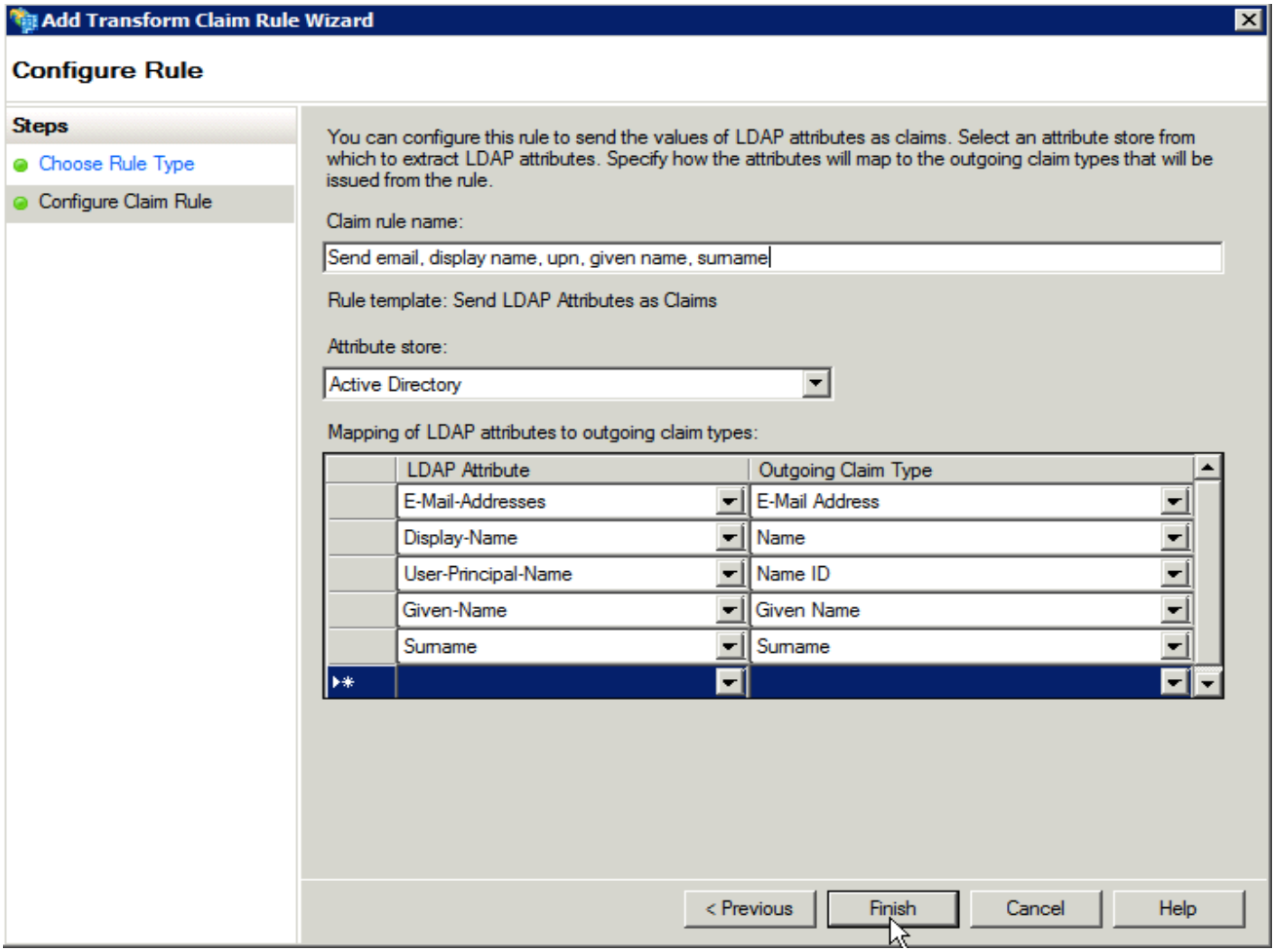

10. Leave the default option (*Permit all users...*) and click Next.
11. Click Next and then Close. The UI will show a new window to edit the Claim Rules.
12. Click on Add Rule....
13. Leave the default option (*Send LDAP Attributes as Claims*).




14. Give the rule an arbitrary name that describes what it does. For example:

    Map ActiveDirectory attributes (mail -> Mail, displayName -> Name, userPrincipalName -> NameID, givenName -> GiveName, sn -> Surname)

15. Select the mappings as shown in this image and click Finish.




Once the setup is complete you need to download the federation metadata.xml file.

This can be downloaded by browsing to

https://<adfs_server_name>/federationmetadata/2007-06/federationmetadata.xml

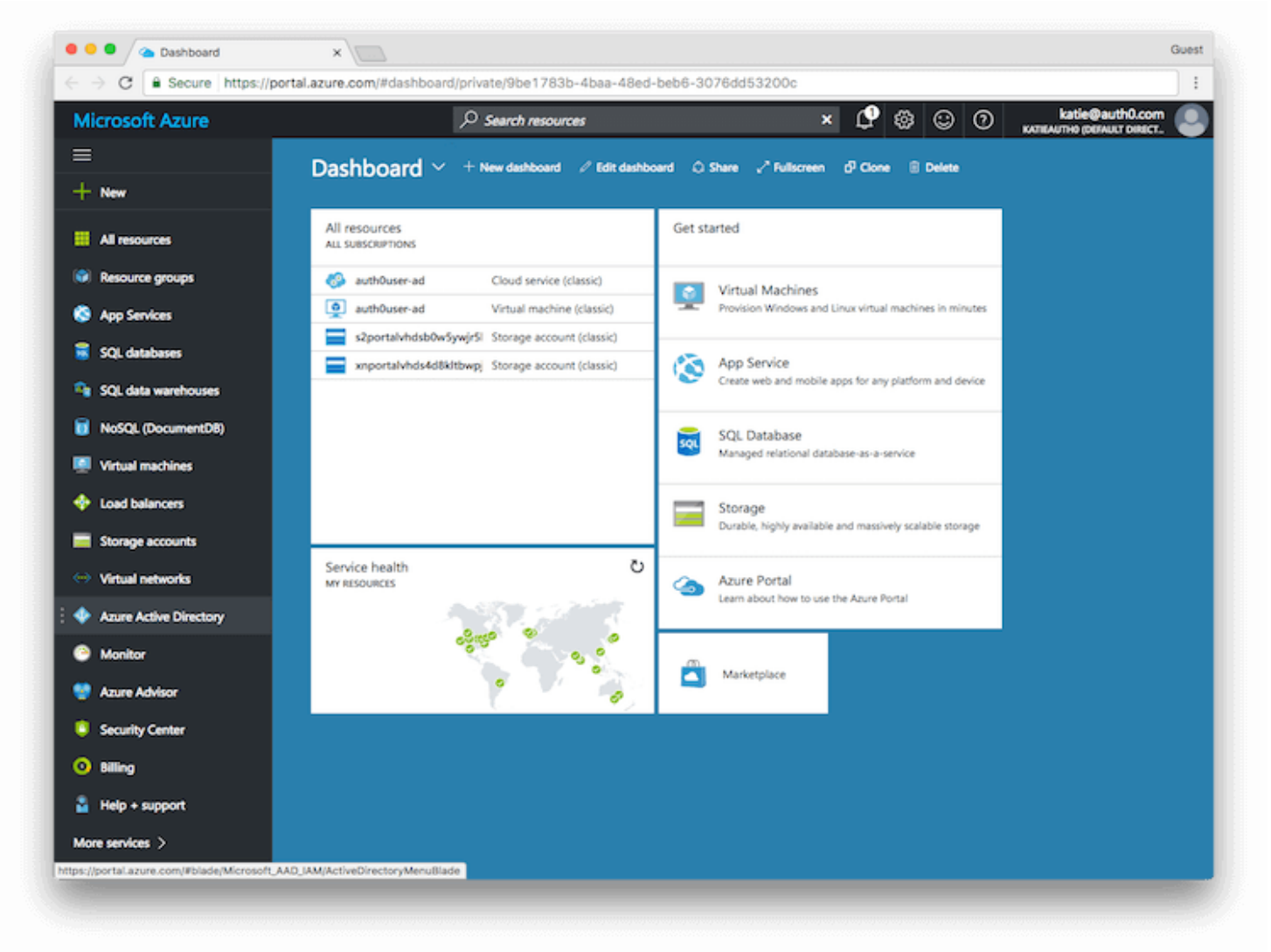
Save the file and send it to your designated SureCloud contact by email securely.

SureCloud will complete the connector setup and will inform you when it is ready for testing.

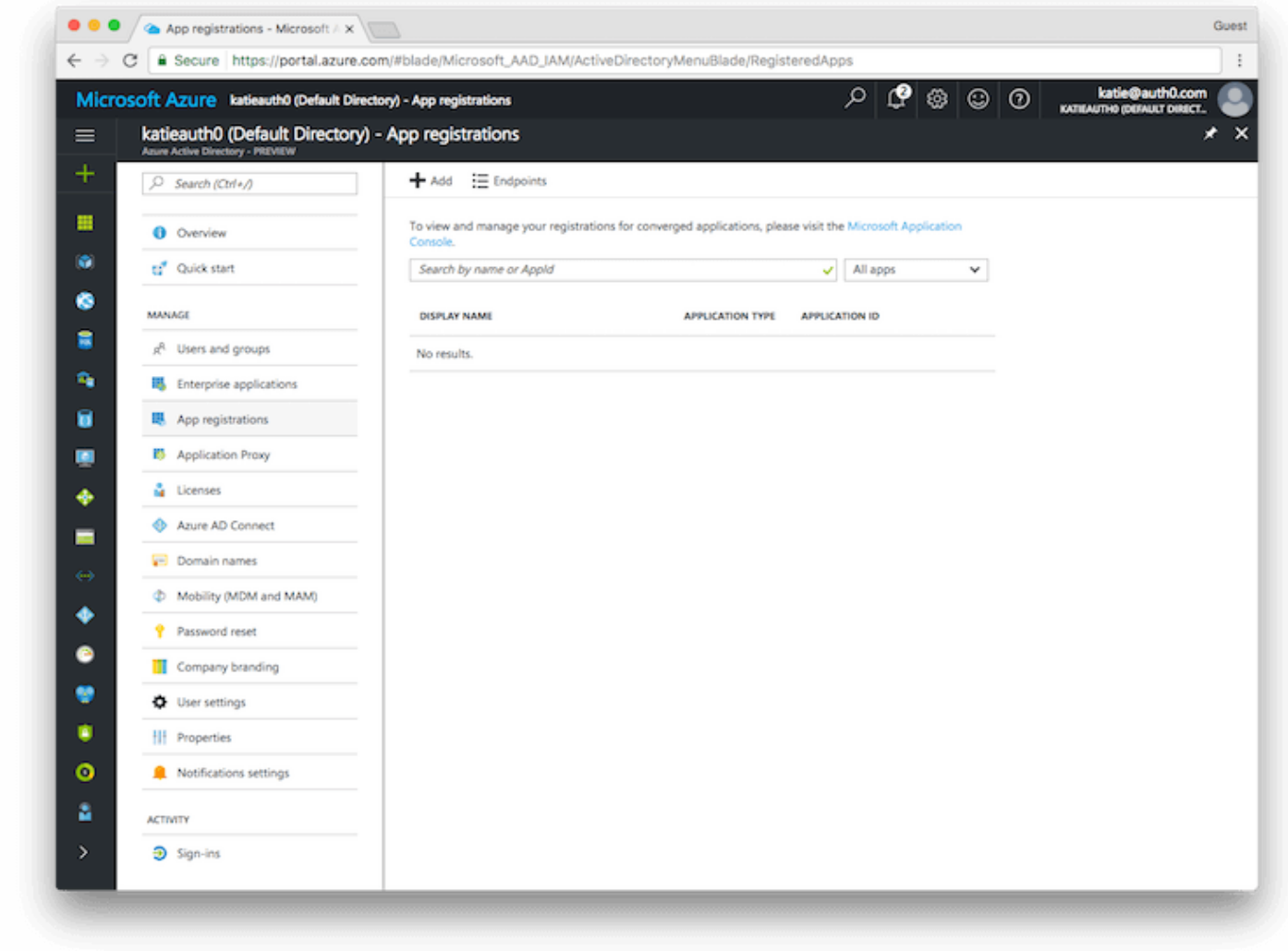
# Azure AD Connector Configuration

## 1. Create a new application

Login to Microsoft Azure and choose **Azure Active Directory** from the sidebar.

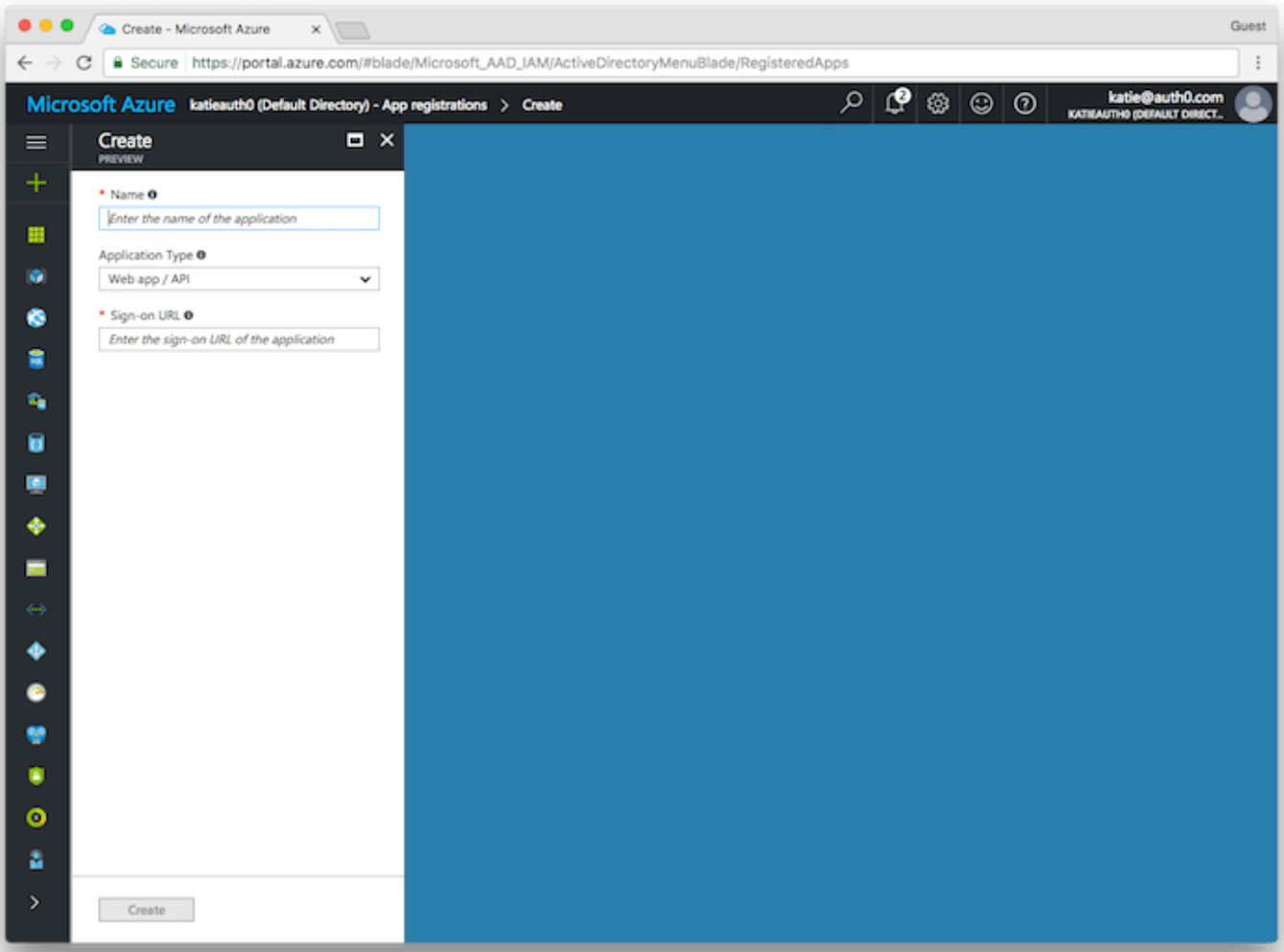



Then under **MANAGE**, select **App registrations**.



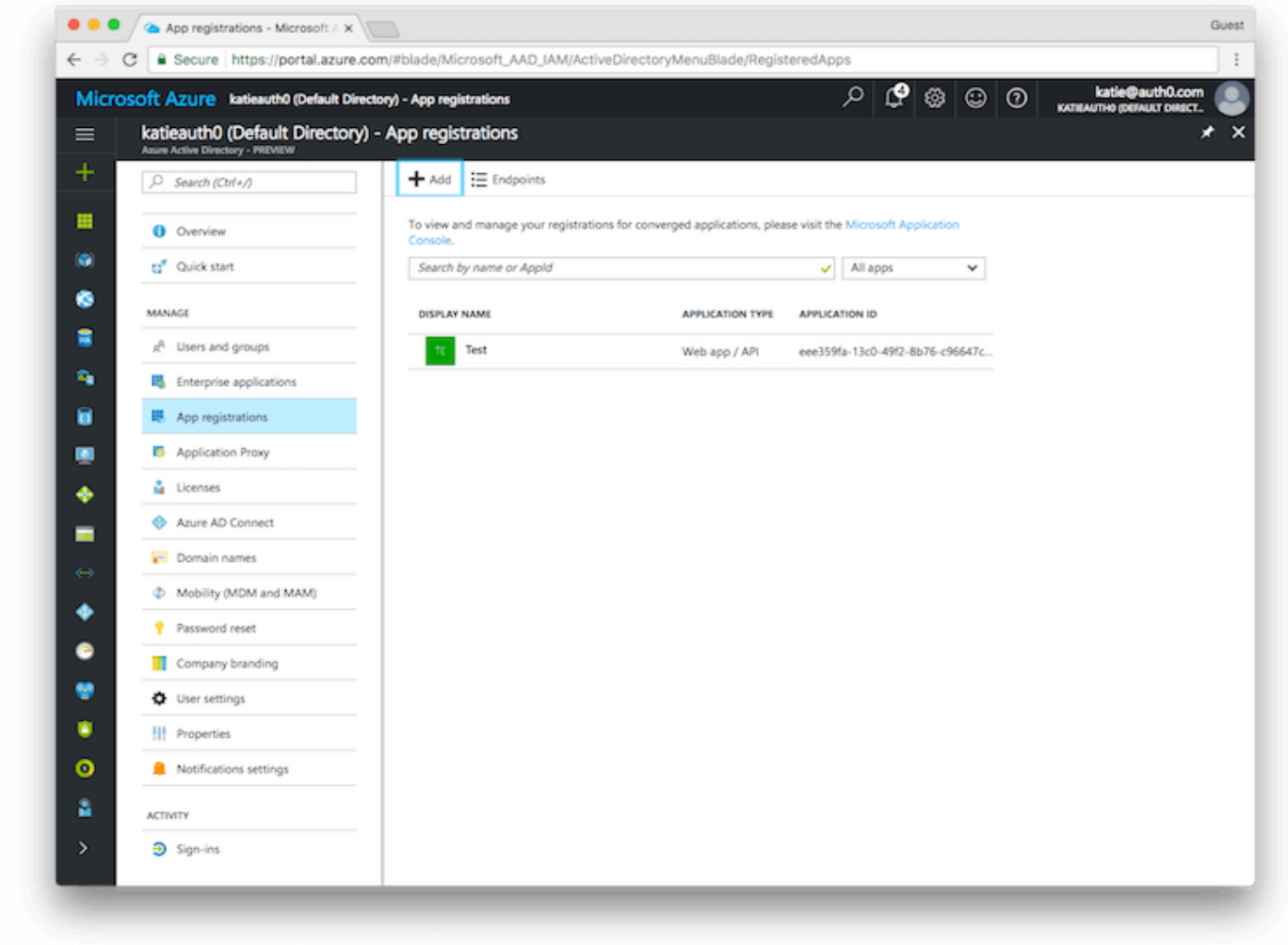

Then click on the + **ADD** button to add a new application.

Enter a name for the application, select **Web app/API** as the **Application Type**, and for **Sign-on URL** enter your application URL.

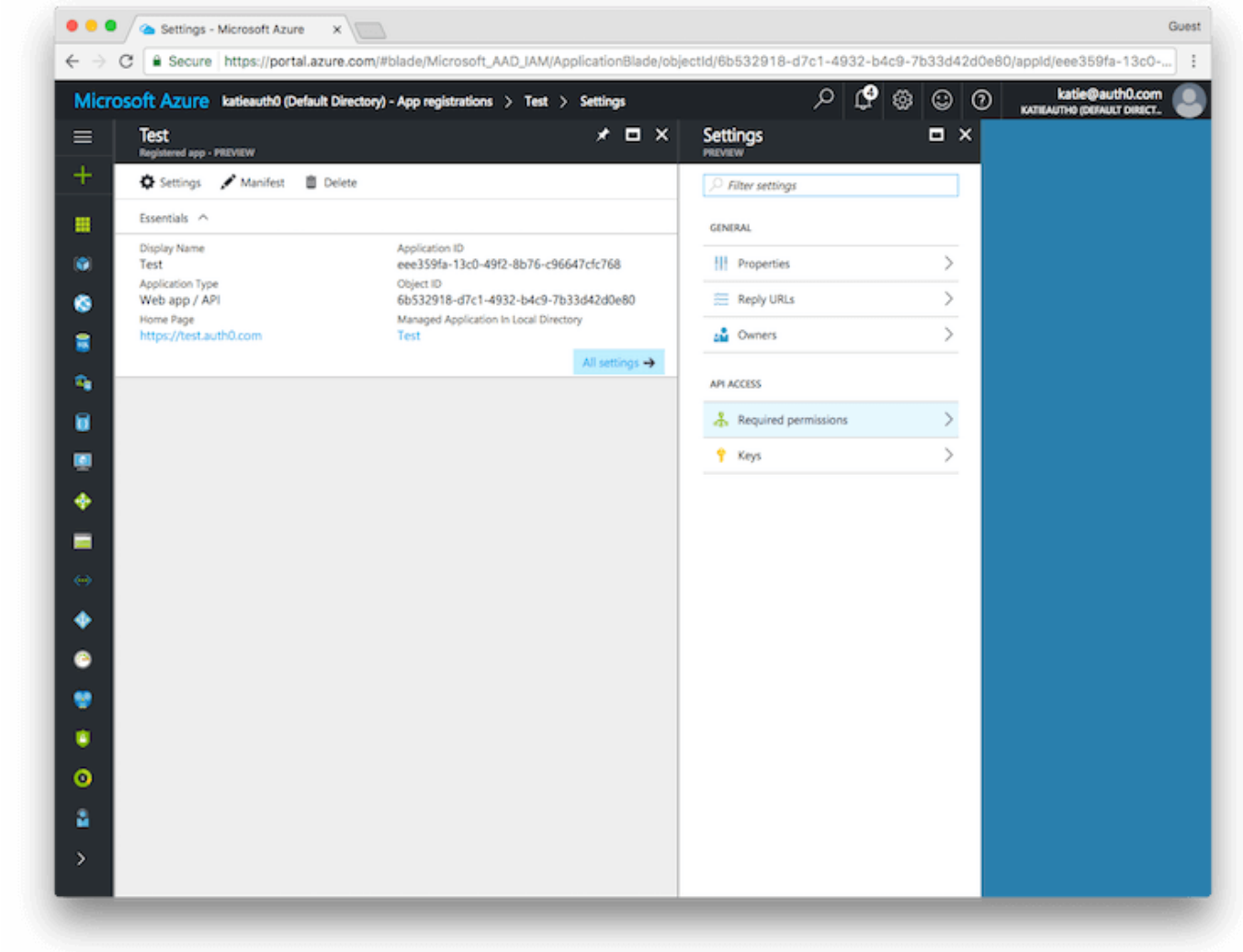



## 2. Configure the permissions

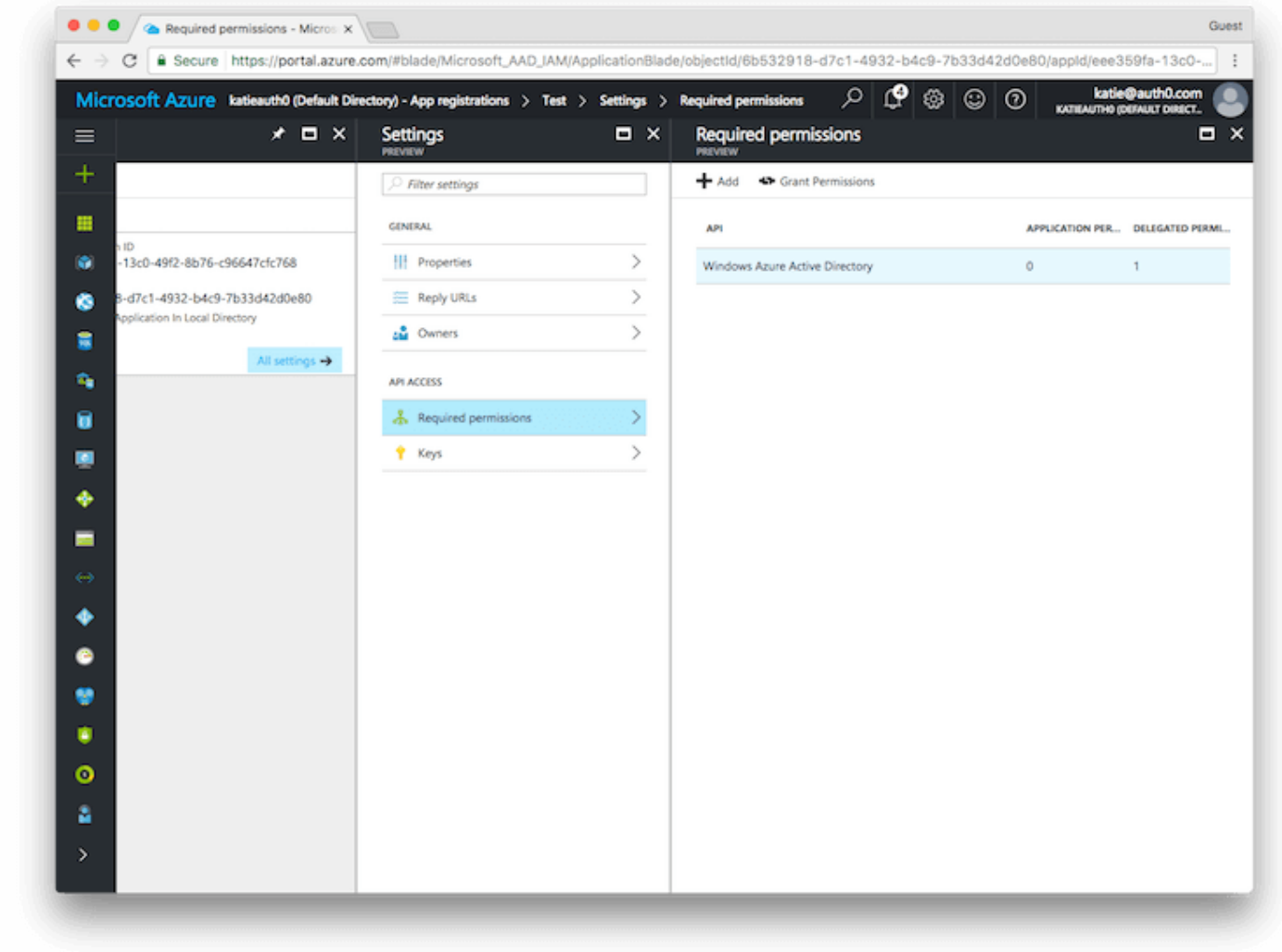
Once the application has been created, you will have to configure the permissions. Click on the name of the application to open the **Settings** section.



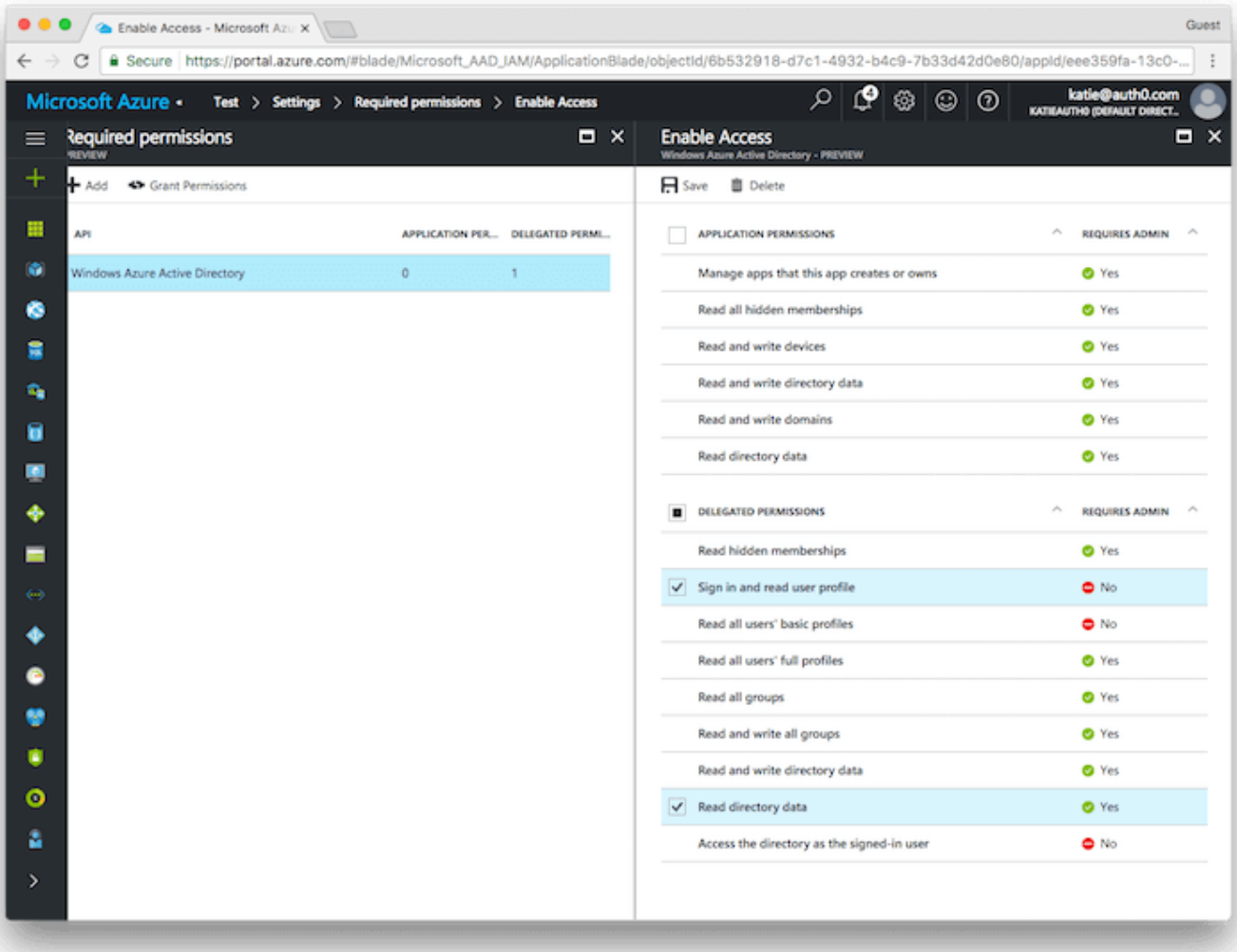

Click **Required permissions.**




Then click on **Windows Azure Active Directory** to change the access levels.



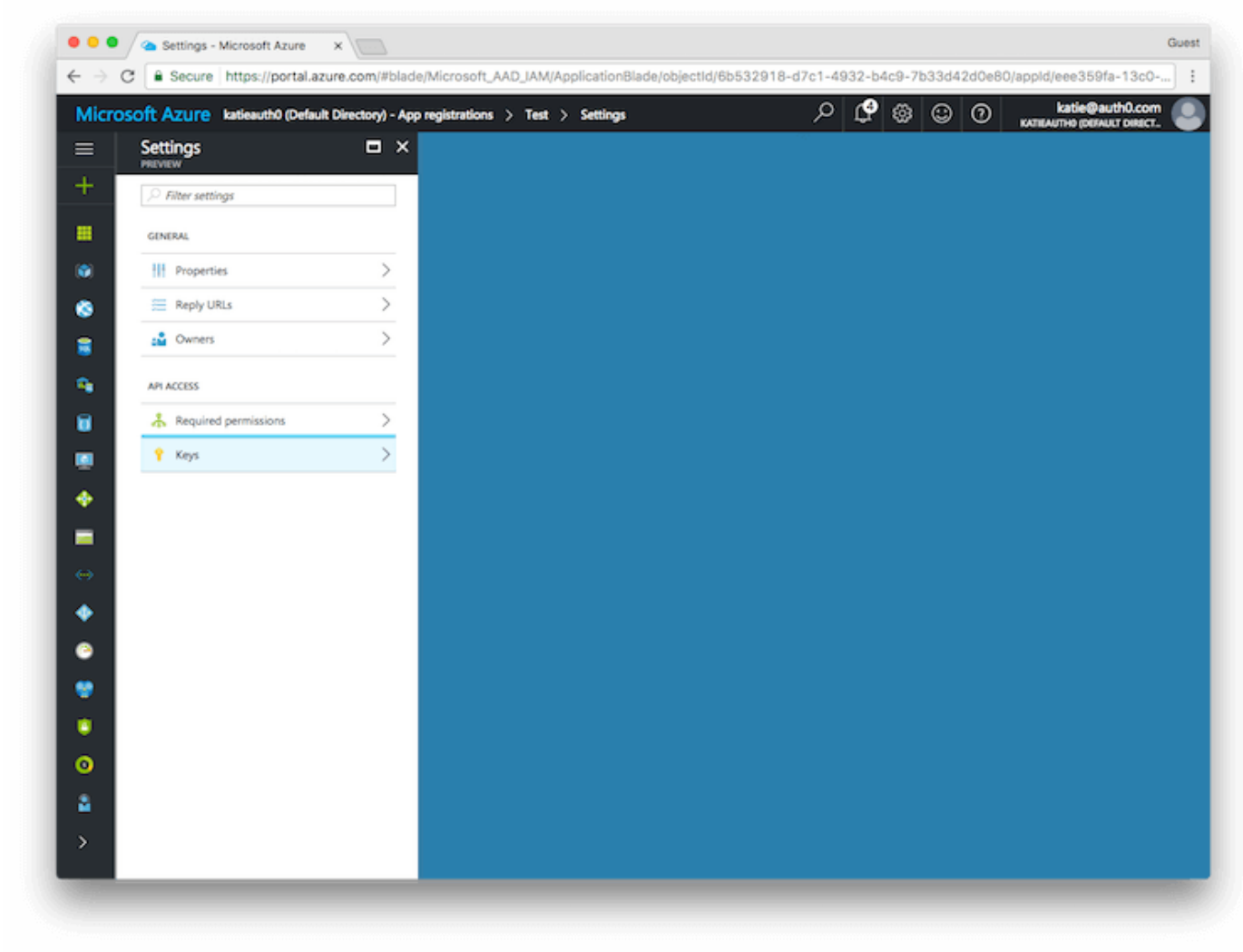

The next step is to modify permissions so your app can read the directory. Under **DELEGATED PERMISSIONS** check next to **Sign in and read user profile** and **Read directory data**.




Click the **SAVE** button at the top to save these changes.

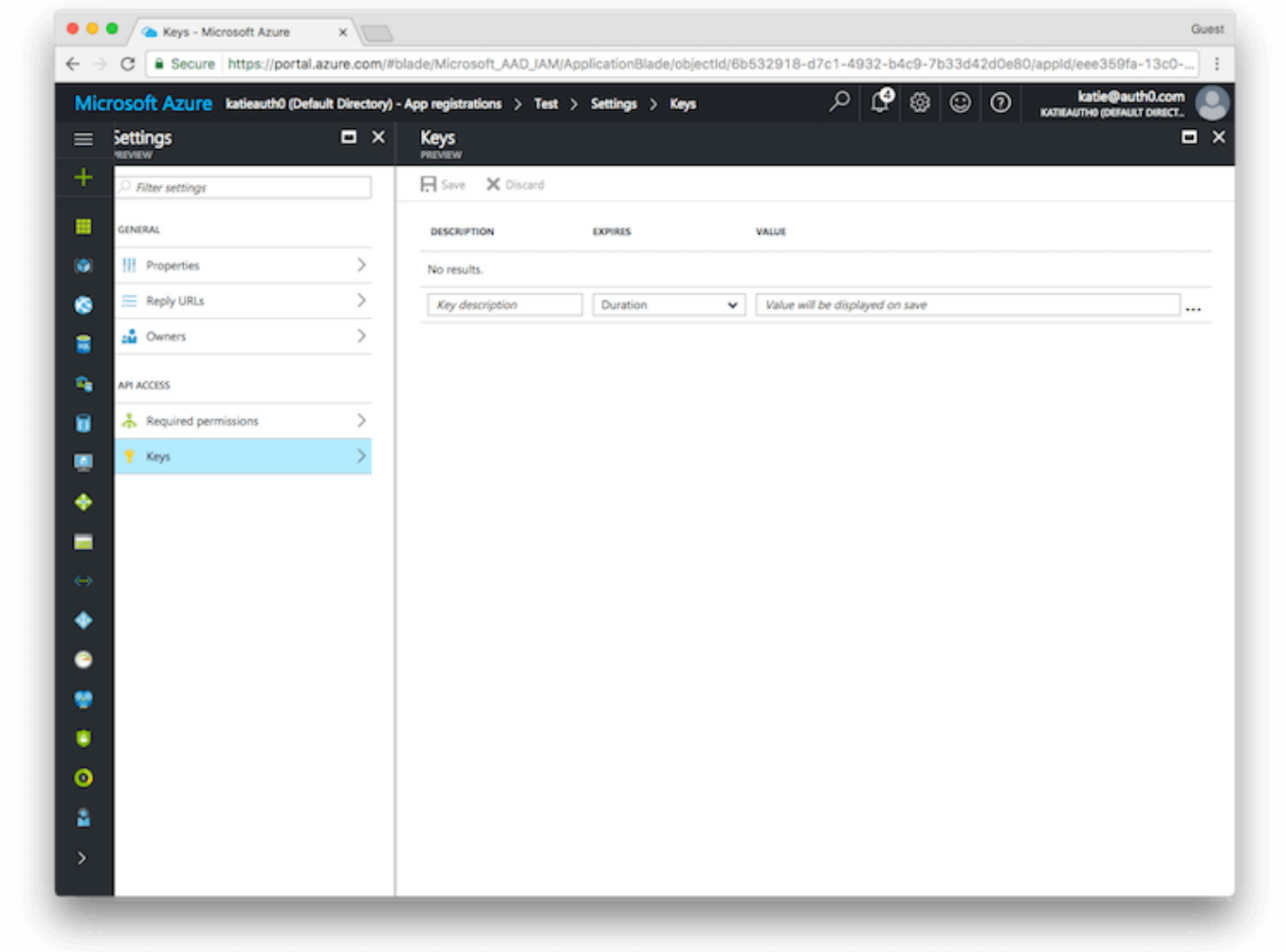
# 4. Create the key

Next you will need to create a key which will be used as the **Client Secret** in the connector. Click on **Keys** from the **Settings** menu.

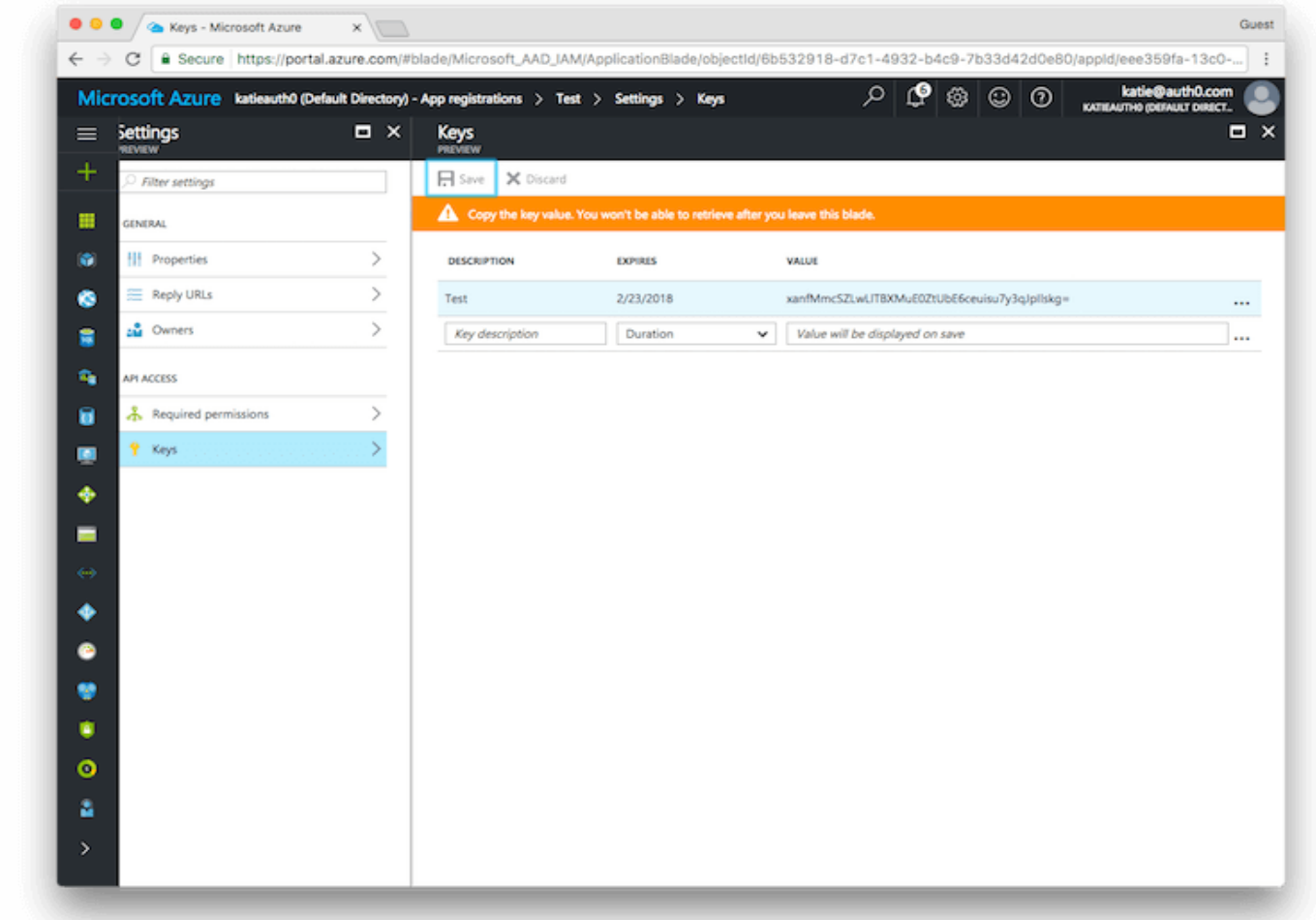



Enter a name for the key and choose the desired duration.

If you choose an expiring key, make sure to record the expiration date in your calendar, as you will need to renew the key (get a new one) before that day in order to ensure users don't experience a service interruption.



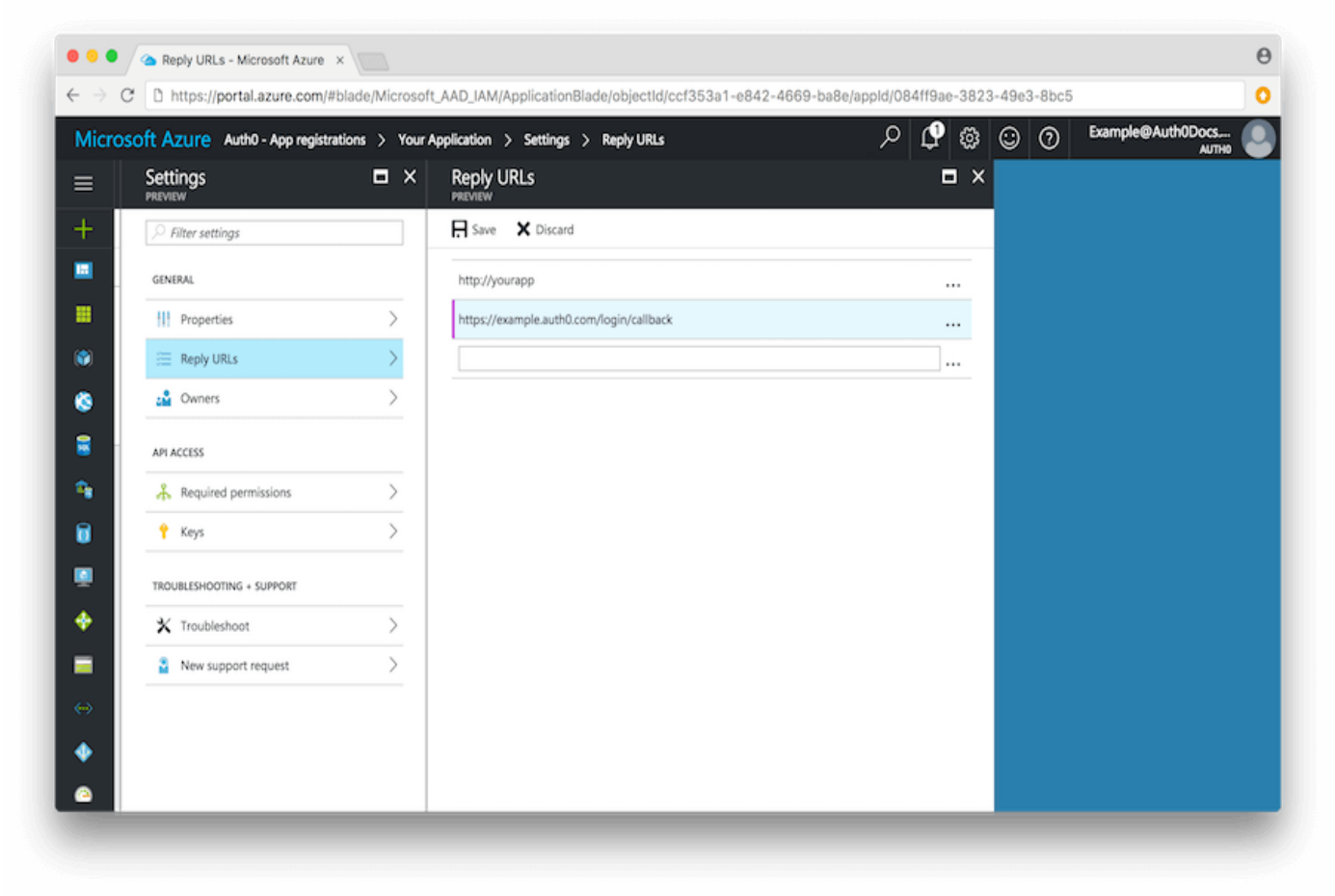

Click on **Save** and the key will be displayed. **Make sure to copy the value of this key before leaving this screen**, otherwise you may need to create a new key. This value is used as the **Client Secret** in the next step.




# 5. Configure Reply URLs

Next you need to ensure that your callback URL is listed in allowed reply URLs for the created application. Navigate to **Azure Active Directory** -> **Apps registrations** and select your app. Then click **Settings** -> **Reply URLs** and add:

https://surecloud.eu.auth0.com/login/callback

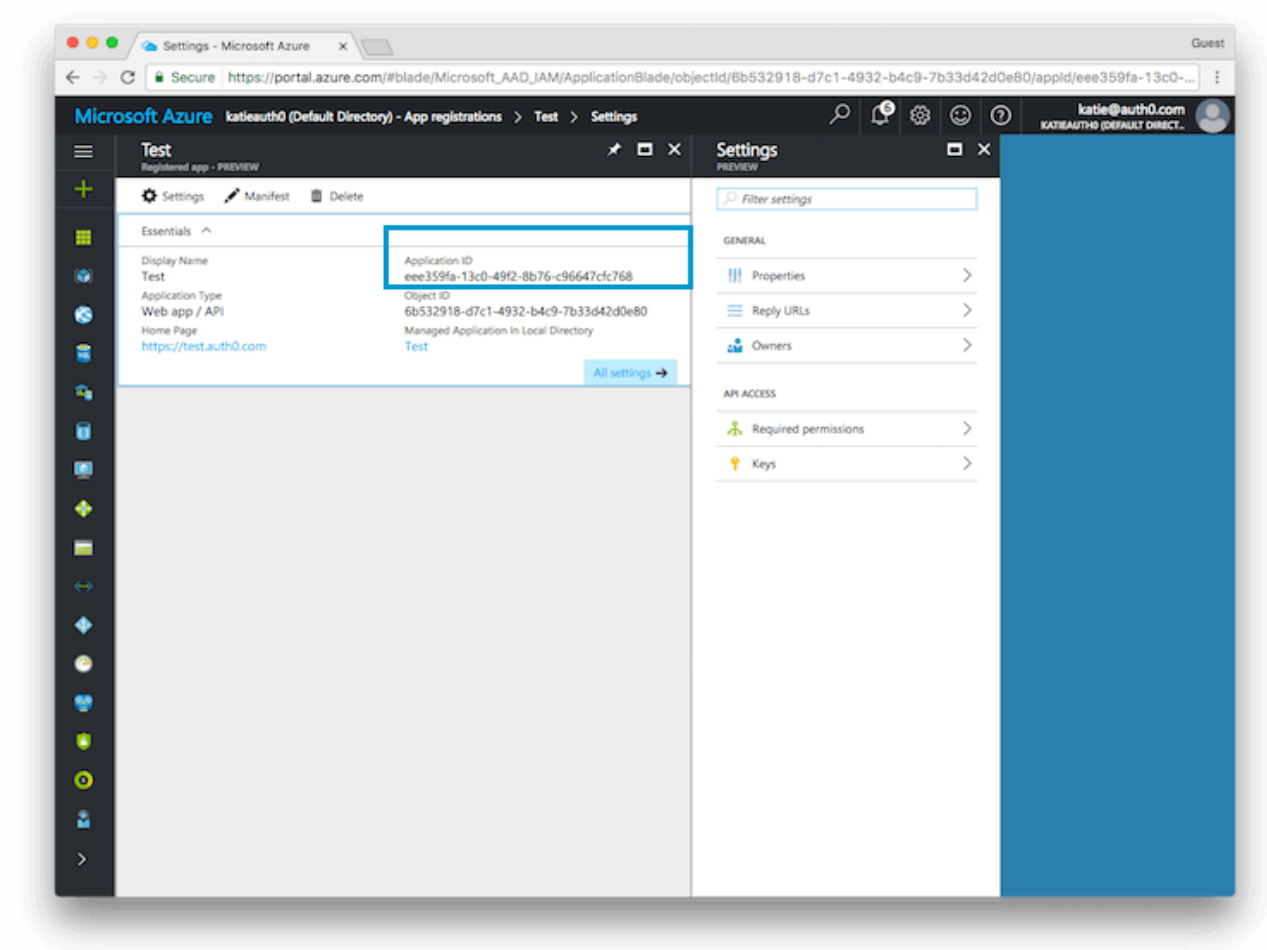



Without this step the App consent page will return a "Bad request" error. The fine print in the footer of this error page can be used to identify the exact tenant name and missing callback url.

You now need to retrieve the following information from the application you have just configured and provide to SureCloud:

- Client ID
- Client Secret
- Microsoft Azure AD Domain (e.g. org1.onmicrosoft.com)

For the Client ID, this value is stored as the Application ID in Azure AD.




For the **Client Secret** use the value that was shown for the key when you created it in the previous step.

Send these 3 pieces of information to your assigned SureCloud contact by email securely.

Once the connector configuration is complete then SureCloud will provide you with an URL that you will need to give to the Azure AD administrator. This URL will allow the administrator to *give consent* to the application so that users can log in.

# Troubleshooting

- Make sure you are in the desired directory to add your application. If you do not have an existing directory you will need to create one.
- When granting access, make sure to use an *Incognito/InPrivate* window and a Global Administrator user.
- If you get *Access cannot be granted to this service because the service listing is not properly configured by the publisher*, try enabling **Multi Tenanted** in the Windows Azure AD application under **Settings** -> **Properties**.

# SAML Connector Configuration

To configure a SAML connector, the following information should be configured on your SAML IDP:

```
SP Entity ID (Audience URI):
urn:auth0:surecloud:<connector>

Single Signon URL (Assertion Consumer Service URI):
https://surecloud.eu.auth0.com/login/callback?connection=<connector>

Single Logout URL:
https://surecloud.eu.auth0.com/logout
```

where ***<connector>*** is specific to the organisation and provided by SureCloud.

**Please Note.** If IDP initiated login is required, then the entity id is used when browsing to your IDP link to initiate the login which will identify the connector to use.

# Testing

We recommend using a test domain for the user mapping , otherwise all users with that domain will be redirected to the organisation's identity provider without testing being performed against the connector.

So for example, we would setup a domain mapping for test-org1.com , which would redirect any user with a email or user id that had the domain test-org1.com would be redirected.

Then we would set the user id for users who have been elected to test to be e.g. user1@test-org1.com, there email address would still be the same as before. They would then use that user id to login and would be redirected through the connector allowing testing to be performed.

Once the testing is completed to the client's satisfaction we would then configure the actual domains so that all users with that domain/s would be redirected. The test domain mapping would then be removed. (Please note the test domain requires no changes at the client end).

We provide another document **SureCloud Enterprise Identity Server Test Scenarios.doc** to provide some common test scenarios and expected results, these are based on an Azure configuration but can be adapted to suit different configuration options.

# Document Control

## Change Record

| Date | Author | Version | Change Reference |
|---|---|---|---|
| 01/08/2017 | David Atkins | 1.0 | |
| 19/6/2019 | David Atkins | 1.1 | Added iDP initiated login support details |

## Reviewers

| Name | Position |
|---|---|
| David Atkins | Senior Software Engineer |
| Chris Tandy | Senior Architect |
| Alex Brown | Product Director |