Azure Delegated Permissions

Last Modified on 06/12/2019 7:07 pm AEDT

ReadiNow API Callouts can connect to Microsoft Azure APIs by using OAuth 2.0 authentication.

Azure offers two permission models:

- Application - where a software application such as ReadiNow connects to an API service on its own behalf
- Delegated - where a software application is connecting to an API service on behalf of a specific end user

This page describes how to configure API Callouts to connect using the **Delegated** model.

> Note that ReadiNow API Callout requests are made on behalf on a fixed nominated account, not on behalf of the currently logged in users. As such they are not truely delegated, and it is generally more appropriate to use the Application Permission model. However, the delegated model is still supported to handle cases where the API being called only offers support for delegated permissions.

Additional information can also be found in the Microsoft Azure reference at: Configuring a client application to access web APIs

Overview

The following sample demonstrates how to:

- configure Azure to receive connections using the delegated permission model
- configure ReadiNow API Callouts to authenticate with Azure

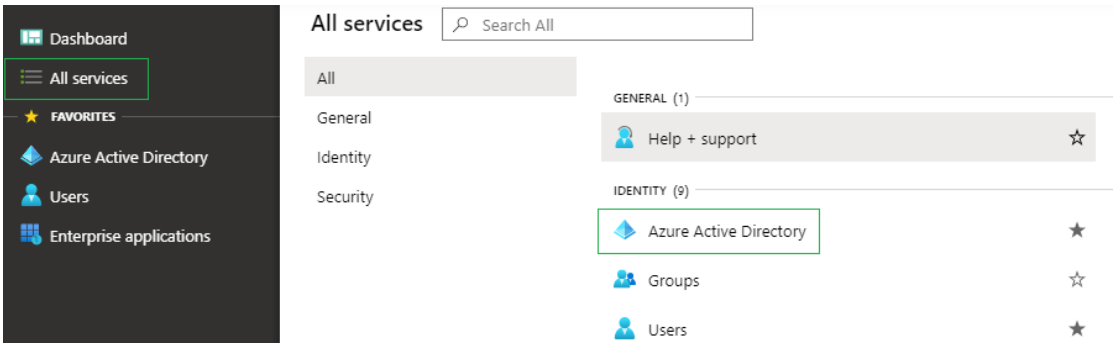
Once complete, refer to Connecting to Azure APIs to extend the sample to set up specific API endpoints and call them using a workflow.

Note: the following is provided as an example to illustrate connecting to the Azure APIs in general, and use the Azure 'users' API as an example. If you wish to achieve automatic provisioning, then use the single-sign-on provisioning mechanism.

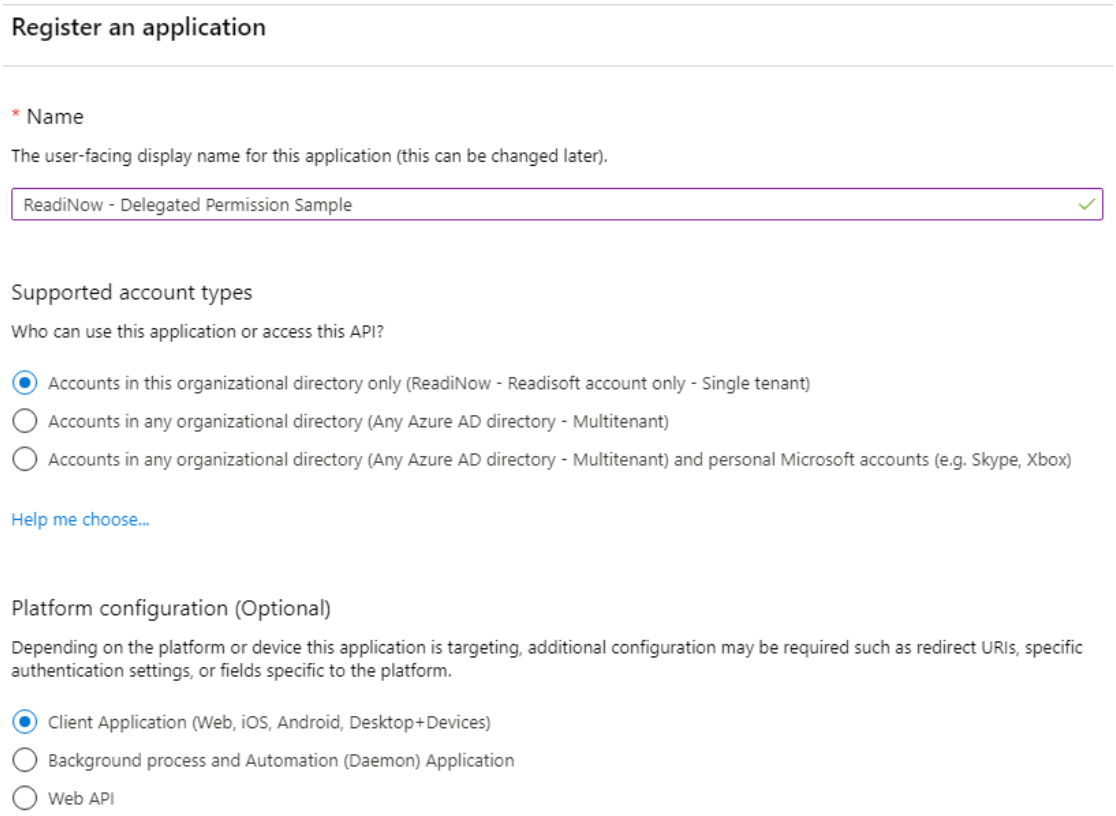
Configure Azure

The following steps will configure Azure to receive a connection from the ReadiNow platform, and grant sufficient permission for the ReadiNow API Callout to request information about users.

1. Register an application
    1. Log into the Azure portal
    2. Select **Azure Active Directory** on left, or locate it under **All services**



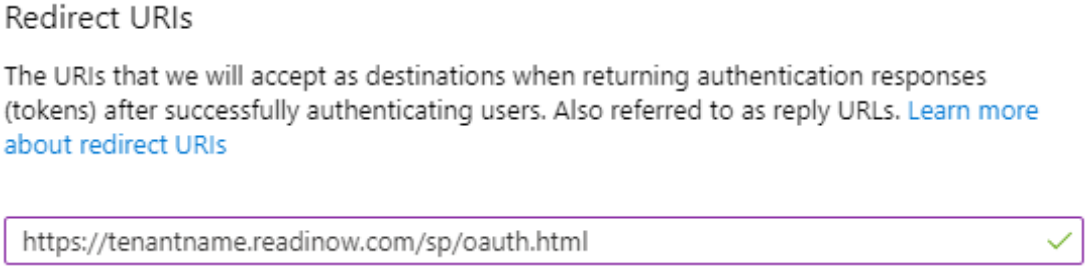
    3. Select **App Registrations**
    4. Click the **New Application Registration** button
    5. Enter a name for the application registration, such as "ReadiNow - Delegated Permission Sample"



6. Leave **Supported account types** as the default optionand blank options respectively.
7. Select **Client Application** for the Platform configuration - this corresponds to
8. Click the **Register** button at the bottom of the screen

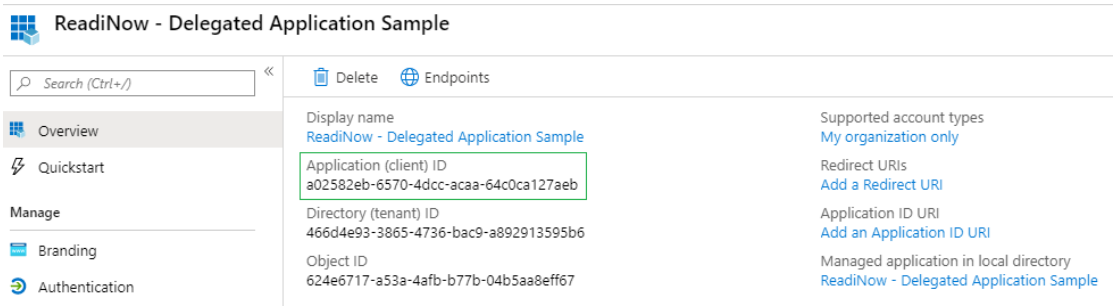
2. Configure the authorization
    1. You should automatically be redirected to the Authentication page (or select **Authentication** on the left)
    2. Click the **Add a platform** button (under the Platform configurations section)
    3. On the right, click the **Web** tile (Single page apps, Web apps)
    4. Enter a Redirect URL value of:

       https://*tenantname*.readinow.com/sp/oauth.html (where tenantname is your ReadiNow tenant name, or more generally use the same host name that you use to connect open ReadiNow in a web browser)



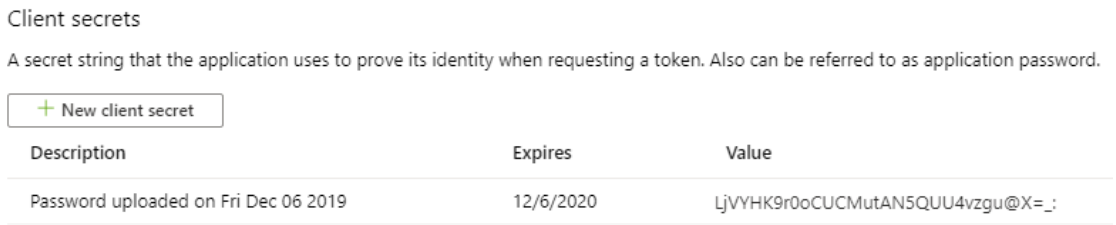
5. Click the **Configure** button at the bottom right

3. Configure the application
    1. An application information screen such as the following will be presented



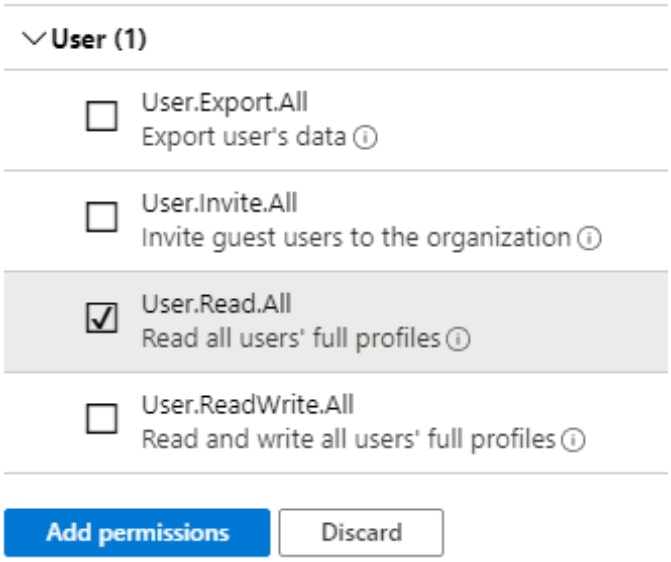
    2. Make a note of the **Application (client) ID -** you will need this in a later step

4. Configure a Client Secret
    1. A *client secret* can be thought of as a password for an application, such as the ReadiNow platform, rather than a person.
    2. Click **Certificates & secrets** on the left hand margin
    3. Click the **New Client secret** button
    4. Select an expiry date and click the **Add** button
    5. A new value will appear such as: LjVYHK9r0oCUCMutAN5QUU4vzgu@X=_: in the client secrets table

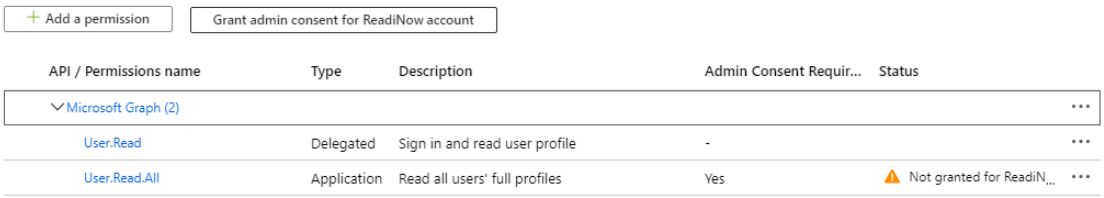


    6. Immediately copy it to a notepad document, or similar. This is the OAuth*client secret*. It cannot be recovered later.

5. Configure permissions that are needed to access the API
    1. Click on **API permissions** in the left margin
    2. Click the **Add a permission** button
    3. Click on the **Microsoft Graph** tile (or whichever API service you wish to access via ReadiNow API Callouts)
    4. Select **Delegated permissions**
    5. Locate and enable the **User.Read.All** permission (or whichever permissions are required for the API you intend to call)



6. Click the **Add permissions** button at the bottom of the panel
7. The new permission will appear in the permissions table
8.



9. Certain API permissions, such as User.Read.All, require explicit consent to be granted by an administrator.
10. Click the **Grant admin consent for account** button
11. A Microsoft login window will appear
12. Login, review the permissions granted, and click the **Accept** button
13. Keep the Azure window open for further configuration steps later

Configure ReadiNow API Callouts

The following steps will start to prepare a new API Callout library in ReadiNow to connect to Azure.

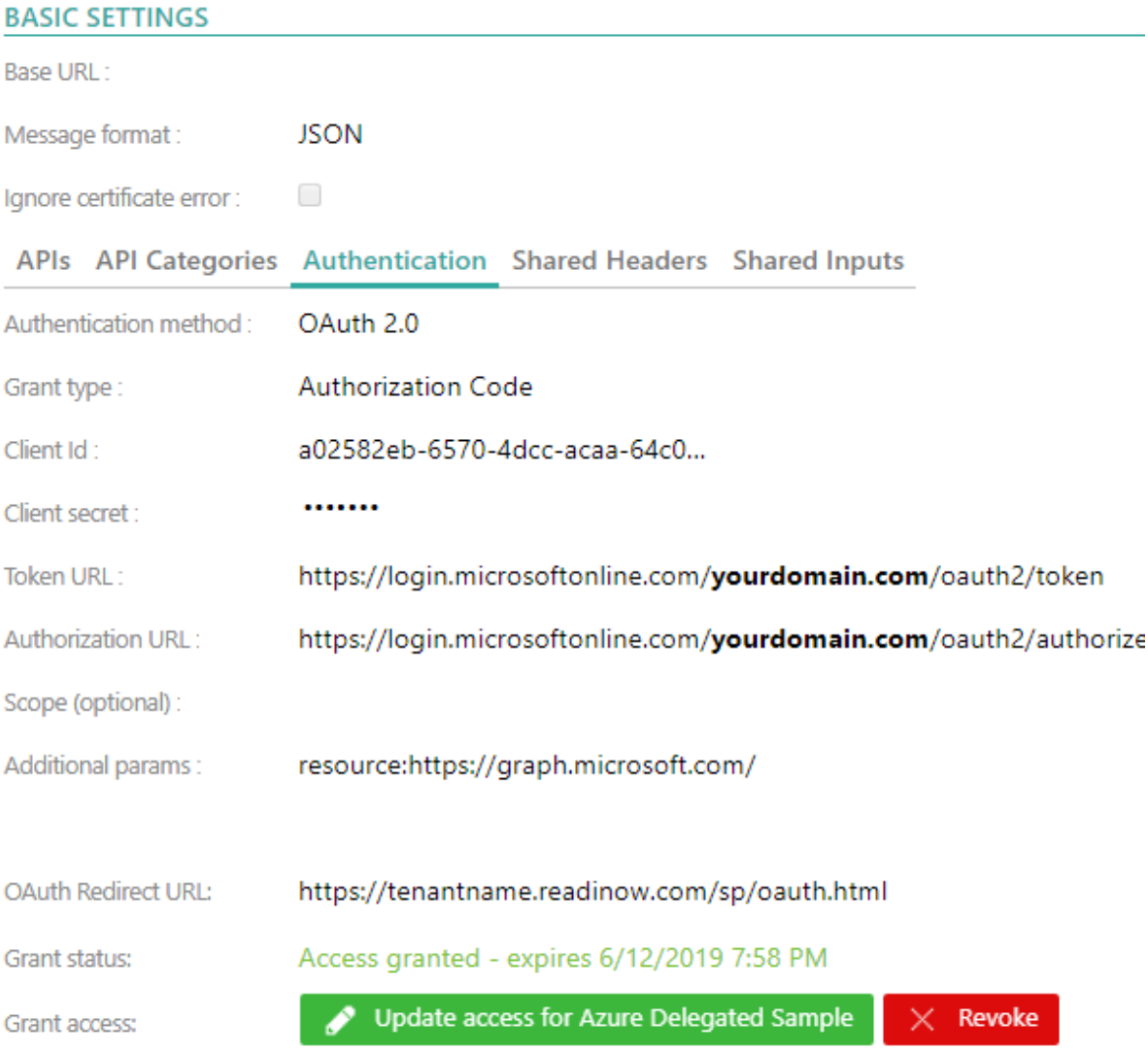
1. Create a new API Callout
    1. Log into ReadiNow
    2. Go to Administration / Integration / API Callouts

3. Click the **New** button to create a new API Callout
4. Name it "Azure Delegated Sample"
5. Leave the **Base URL** blank
6. Set the message format to JSON

2. Configure authentication
    1. On the Authention tab, set the **Authentication method** to **OAuth 2.0**
    2. Ensure that the **Grant Type** is set to **Client Credentials** - this corresponds to the Azure 'Application permission' type
    3. Set the **Client ID** to the **Application (client) ID** value provided by Azure in previous steps
    4. Set the **Client Secret** to the value provided by Azure in previous steps
    5. Set the **Token URL** to: https://login.microsoftonline.com/*yourdomain.com*/oauth2/token (where yourdomain.com is your ActiveDirectory domain, such as company.com)
    6. Set the **Authorization URL** to: https://login.microsoftonline.com/*yourdomain.com*/oauth2/authorize (where yourdomain.com is your ActiveDirectory domain, such as company.com)
    7. Set the **Additional params** to: resource:https://graph.microsoft.com/ This indicates to Azure which Azure API service the authentication token will be allowed to access.
    8. Click the **Save** button - do not click the Update Access button yet
    9. Check that the **OAuth Redirect URL** shown is the same as was provided to Azure in previous steps
3. Perform the OAuth grant
    1. Click on the green **Grant access** button
    2. An Azure login page might pop-up (or more likely it will remember that you are already logged into the portal).
    3. Log in using the account that should be used for the purpose of making API calls (which is ideally not the same as your admin account).
    4. If you are not prompted for login details, and you need to use a different account, then log out of the Azure portal now and try again.

5. You should then be presented with an Azure "Allow Access?" screen.
6. Click **Accept**, at the bottom. Note: this might not appear either if you're re-granting.

4. You should see a message saying that you are now authorized.



Next Steps

Azure and ReadiNow are now both configured so that ReadiNow callouts can connect to Azure.

Read Connecting to Azure APIs to continue building the sample to:

- create a API Callout endpoint to request user details
- create a workflow that uses the API Callout and processes results