Power Pages 1 Day

Power Platform WorkshopPLUS

Lab 2: Authentication

Conditions and Terms of Use

Microsoft Confidential - For Internal Use Only

This training package is proprietary and confidential and is intended only for uses described in the training materials. Content and software are provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2021 Microsoft Corporation. All rights reserved.

Copyright and Trademarks

© 2021 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

<http://www.microsoft.com/about/legal/permissions/>

Internet Explorer, Microsoft, Microsoft Dynamics, Microsoft Dynamics logo, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Table of Contents

[Lab 2: Authentication 5](#_Toc83307789)

[Part 1: Authentication 6](#_Toc83307790)

# Lab 2: Authentication

Introduction

Visitors who submit 311 tickets or apply for open employment opportunities will want to securely access their information. Pages allow visitors to register and securely access the data we want them to see.

Objectives

After completing this, you will be able to:

Configure pages user authentication.

Prerequisites

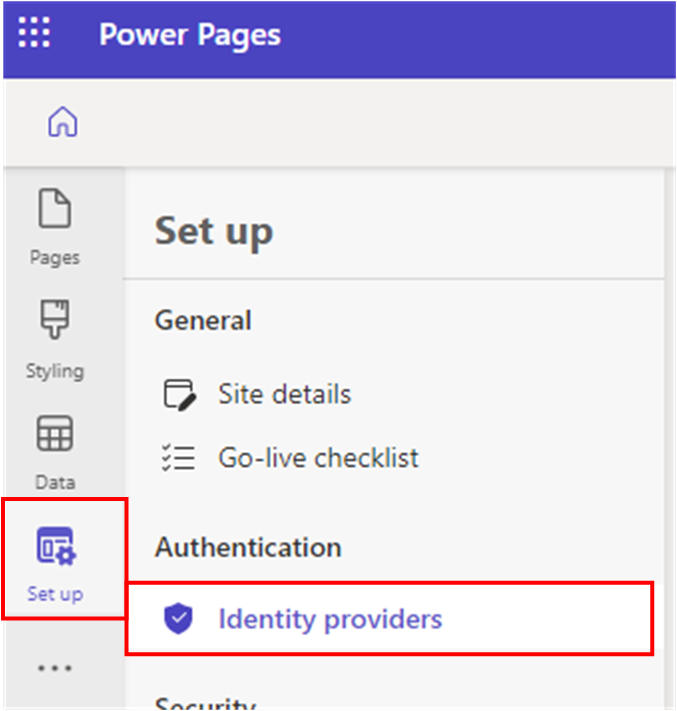
Completion of Lab 1

Estimated Time to Complete

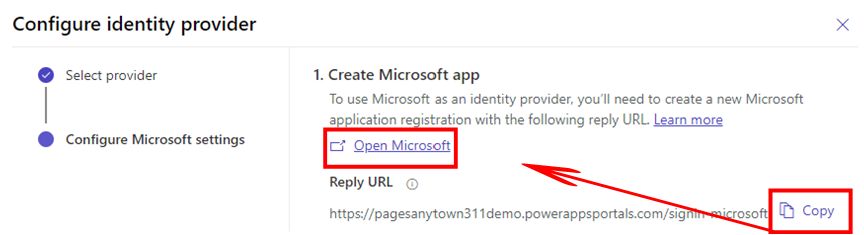
* 25 minutes for the following steps:

## Part 1: Authentication

1. Navigate to https://make.powerpages.microsoft.com and ensure you are in the Pages 1 Day Dataverse environment.
2. Click on the **Set up** icon via the left navigation bar, then select **Identity Providers** beneath **Authentication**.

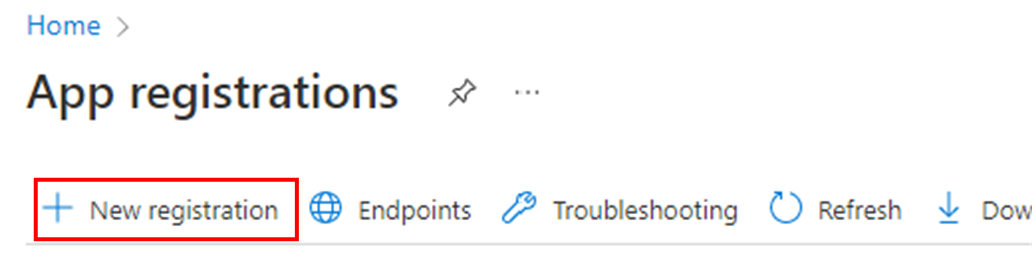


1. To the right of the **Microsoft** identity provider option, select **Configure**.
2. A window will slide out from the right margin.
3. Click **Next**
4. Copy the **Reply URL** and click **Open Microsoft**

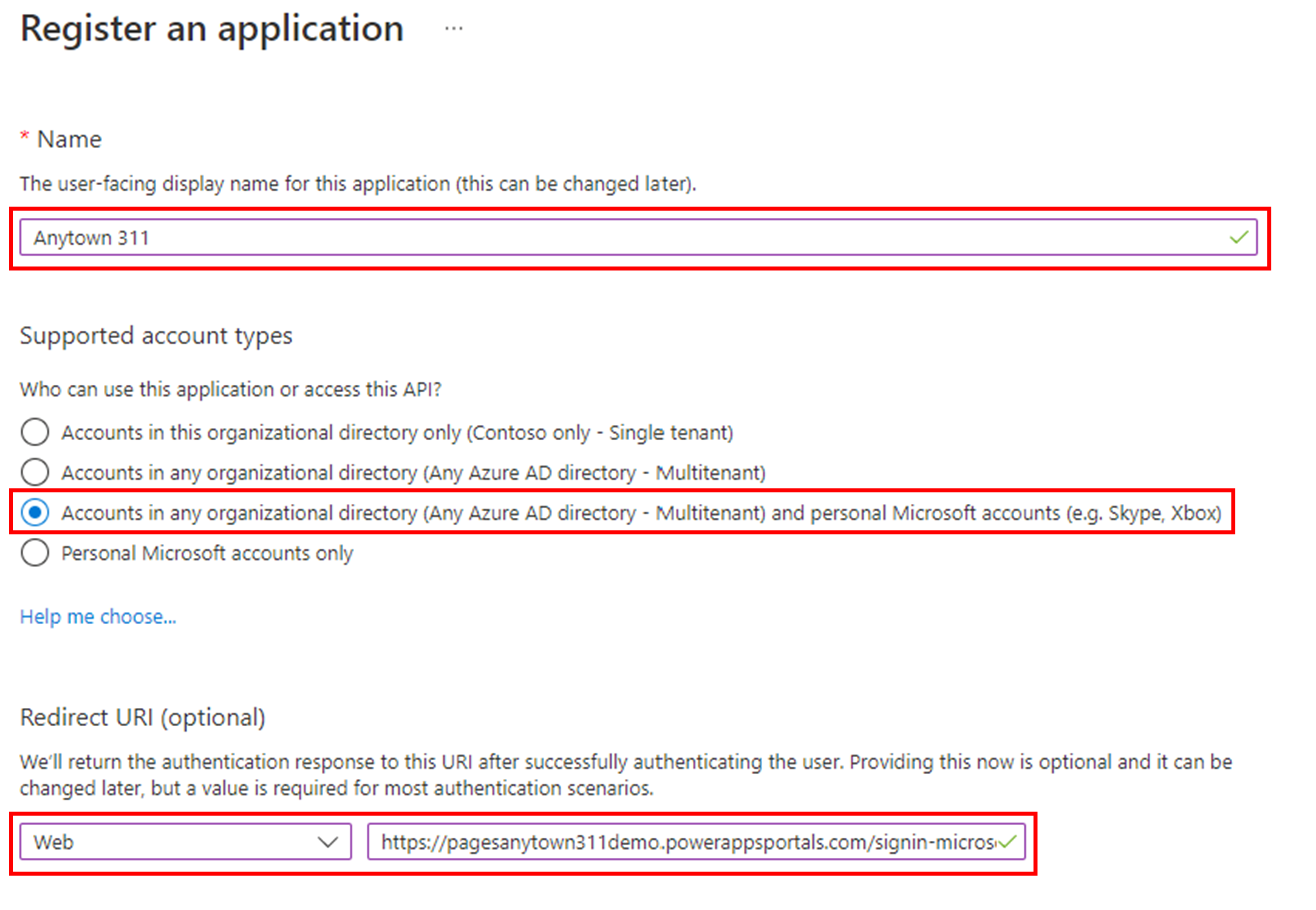


Azure App Registration Steps:

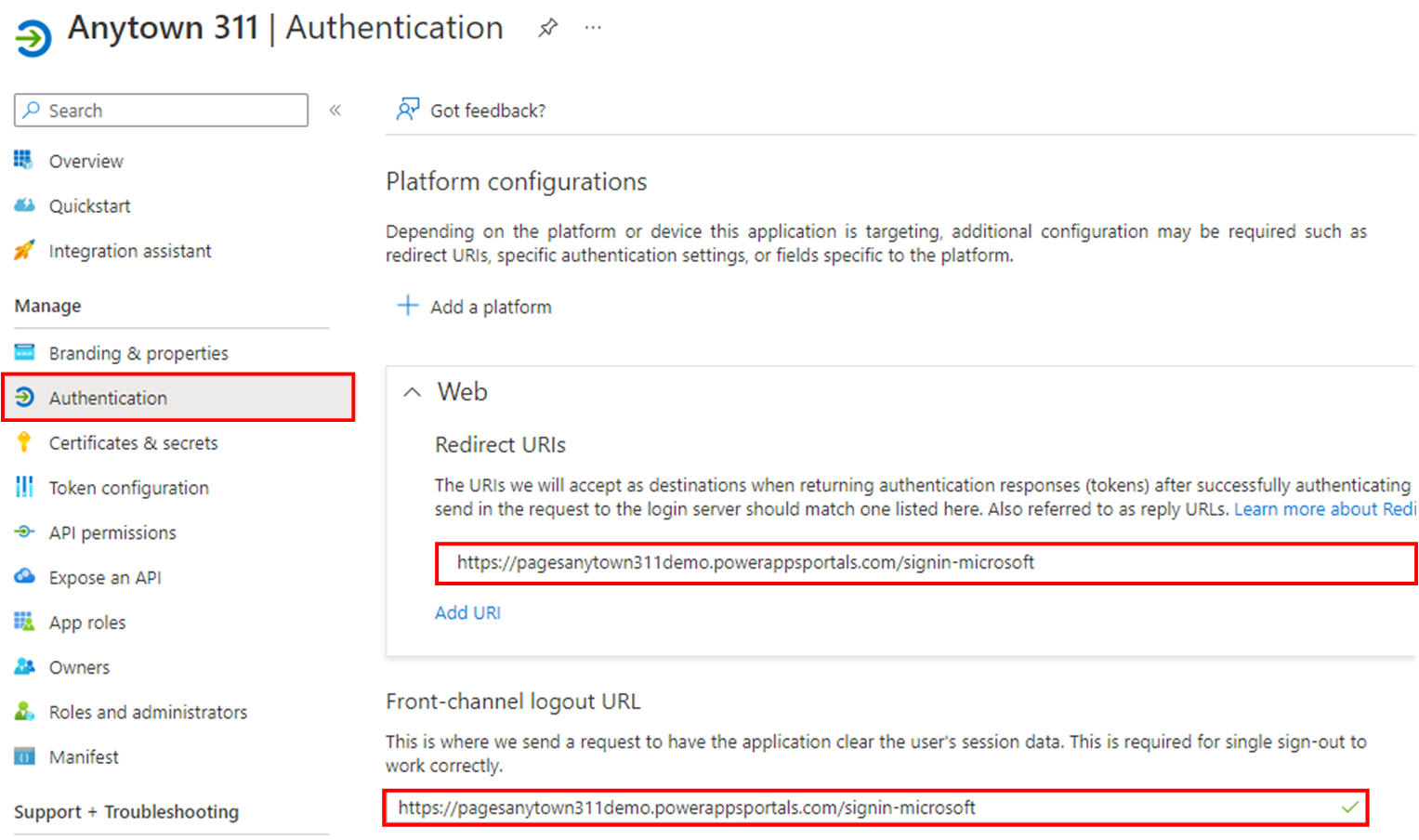
1. Navigate to: [App registrations - Microsoft Azure](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade)
2. Select **+** **New Registration**



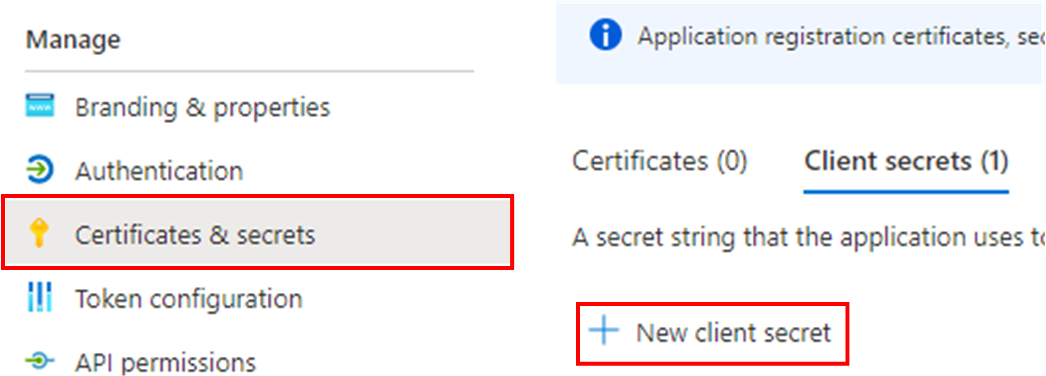
1. For **Name**, enter **Anytown 311.**
   * Note: The name entered here will be shown to end users during the sign-in/up
2. Within the Support Account Types section, select “**Accounts in any organizational directory (Any Azure AD – Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)**”
3. For **Redirect URI (optional)**: Select **Web** and paste the **Reply URL** (This was copied to your clipboard in the step 5/Configure identity provider form)



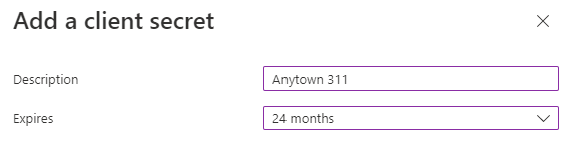
1. Click the **Register** button on the bottom left of the form.
2. From the left-hand navigation, select **Authentication** beneath the **Manage** section.
3. Paste the **Reply URL** that you copied into the **Redirect URIs** and **Front-channel logout URL** textboxes to ensure they are consistent with the one entered in step 11 above.

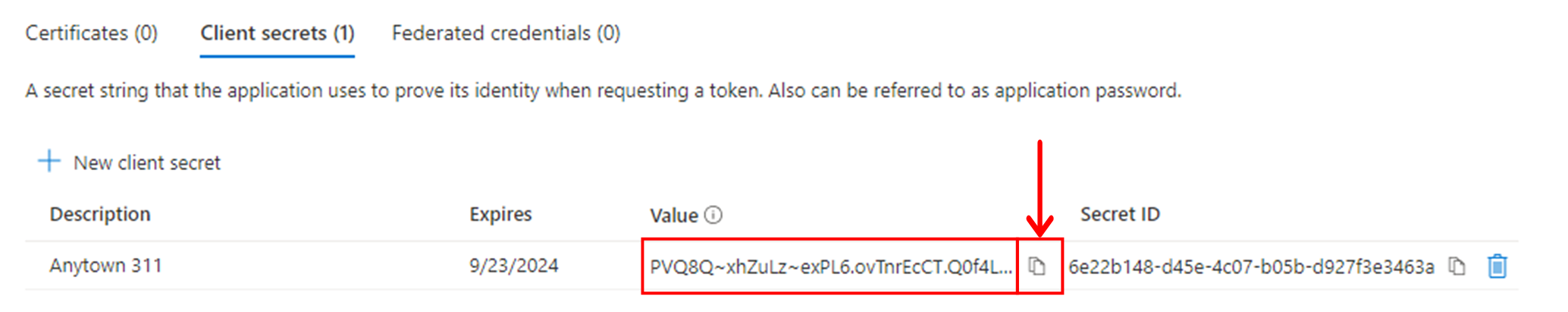


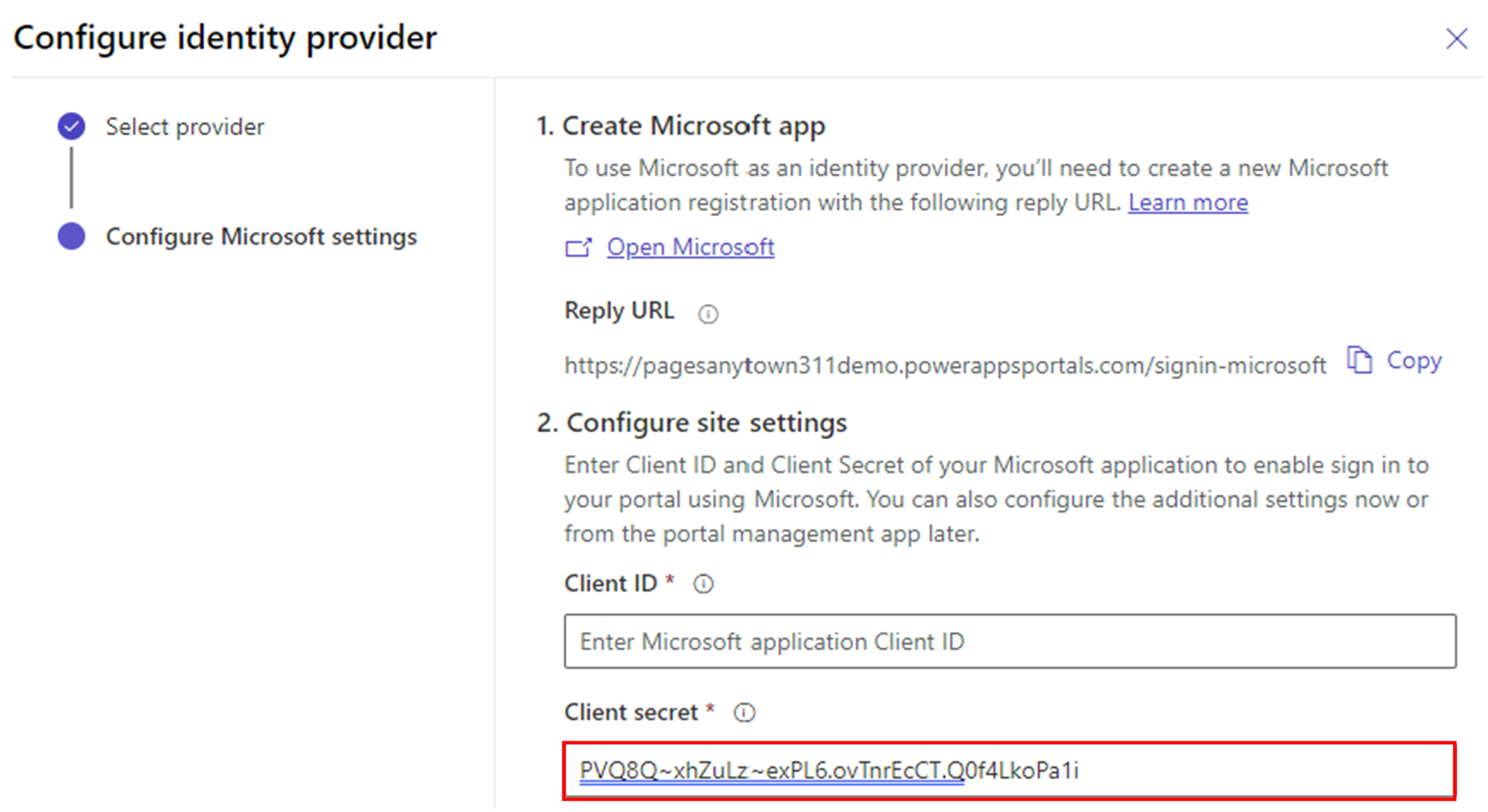
1. Click the **Save** button on the bottom left of the screen.
2. From the left-hand navigation, select **Certificates & secrets** beneath **Manage.**
3. On the **Client Secrets** tab, select **+ New client secret.**



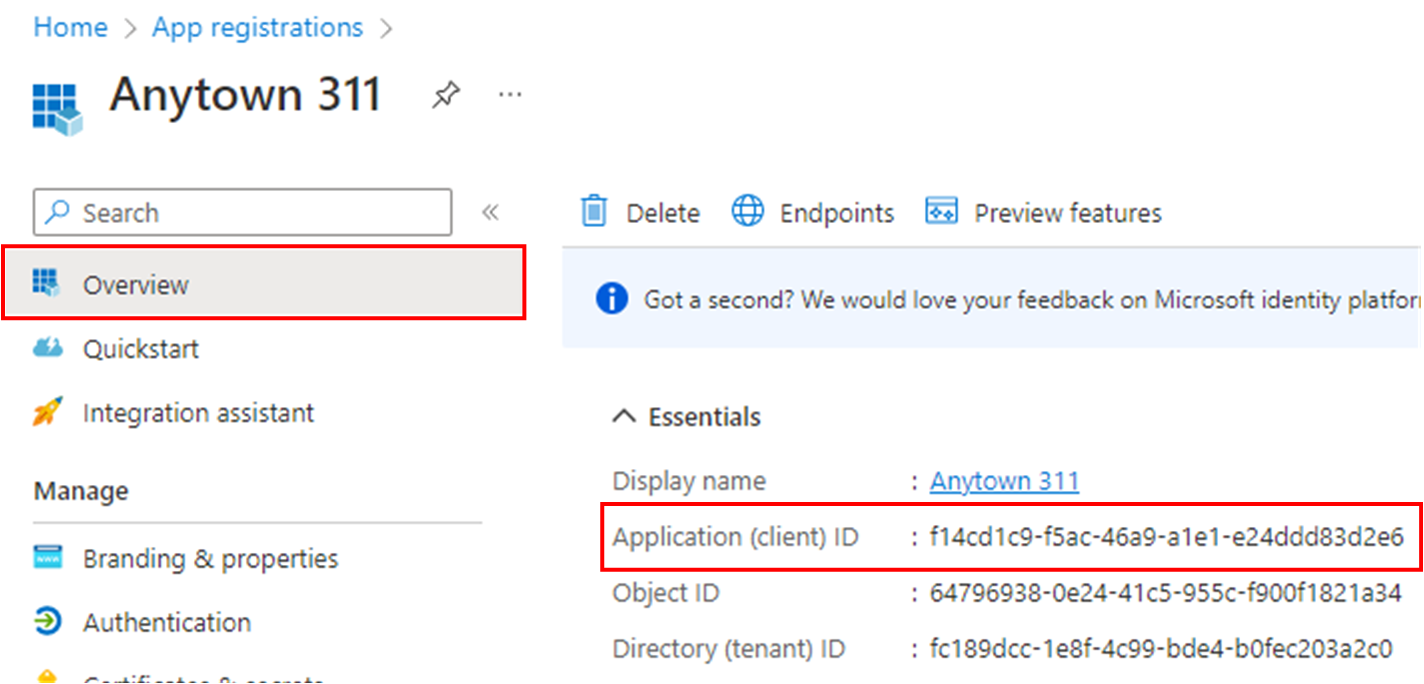
1. Enter **Anytown 311** into the **Description**
2. For **Expires**, select **24 months.**
3. Click the **Add** button on the bottom left of this pop-out window.



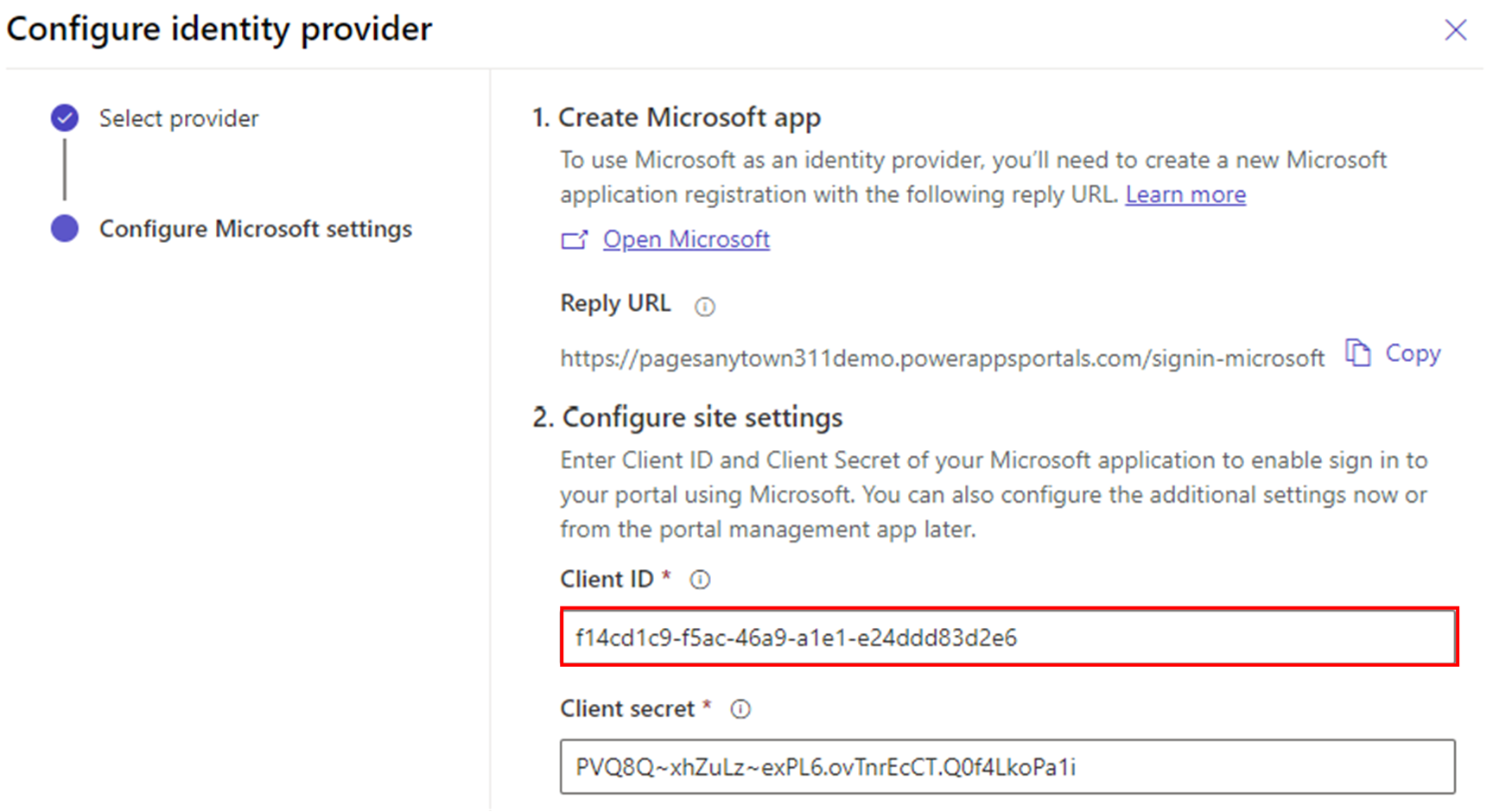
1. Locate the Client secret you just added. Click the **Copy to clipboard** button next to the value within the **Value** column. 
2. Navigate back to the **Power Pages** tab in your browser.
3. Paste the client secret value from your clipboard into the **Client secret** field on the form.



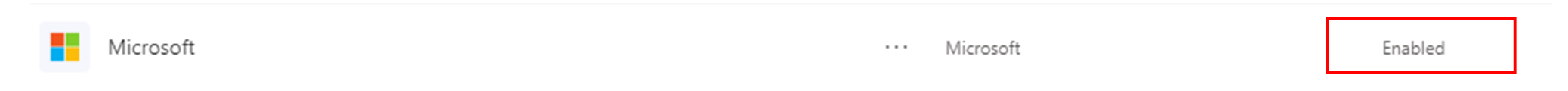
1. Navigate back over to the **Anytown 311 – Microsoft Azure** tab in your browser.
2. Select **Overview** from the left-hand navigation in your app.
3. Locate the **Application (client) ID** and copy to your clipboard.



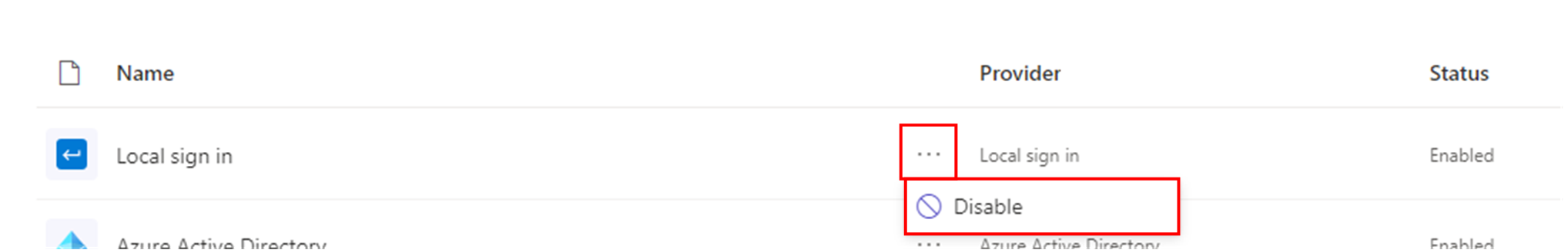
1. Navigate back to the **Power Pages** tab in your browser.
2. Paste the **Application (client) ID** from your clipboard into the **Client ID** field in the form.



1. Click the **Confirm** button on the bottom left of the pop-out window.
2. Once configuration has completed, click the **Close** button.
3. You will now see the **Status** of the Microsoft identity provider is set to **Enabled.**



1. Click **Preview > Desktop** from the top right of the page.
2. Click **Sign in** on the main navigation bar.
3. Click **Microsoft** beneath **External SignIn.**
4. When prompted, login with your admin credentials, check the **Consent on behalf of your organization** box, and click **Accept**.
   1. Validate you can successfully log in.
   2. Note: If you receive an error stating that the user ID is already taken, you will need to add your trial account email to your Contact record. This can be done through the Portal Management application.
5. **Sign out.**
6. Navigate to your **Power Pages** tab. Click the **Ellipses** button next to the **Local sign in** identity provider, then select **Disable**.



1. Click **Preview > Desktop** from the top right of the page.
2. Notice that there is no longer an option to login using username and password. We have disabled this option because users are going to login using a **Microsoft** account. If you click **register**, you can also no longer register using a username and password.

 You have completed Lab 2.