How to Set Up Single Sign-On

Abstract

This document provides instructions on how to setup Single Sign-On (SSO) experience.

December 2023

Revisions

Date	Description
December 2023	Revision 4

Acknowledgments

Author: Vedam Venkateshwara

Support: NA

Other: NA

Table of contents

Executive summary

Note: This section is required for Reference Architectures, Best Practices guides, and Technical White Papers. It is optional for Deployment and Configuration guides.

The executive summary includes a problem statement and the Dell Technologies solution that is detailed in the remainder of the paper. It should include key findings and information that gives the reader insight as to why they would be interested in this solution.

1 Setting Up the Single Sign-On (SSO) Experience for your Organization’s identity Provider

The service provider or Dell identity group invites IAM expert. IAM expert receives an invitation email with a link to validate his credentials. For more information, refer to the Topic 1: **Sign In and Verify your Account** of Email Invitation document.

After your account is verified, you will be redirected to the External Federation Portal.

If the page **Manage Domain** appears, then follow **Section 1** of Domain Management document or else follow Step 1 of this document.

To enable an SSO experience for the user, perform the following steps:

1. Click **Create IdP Group**.

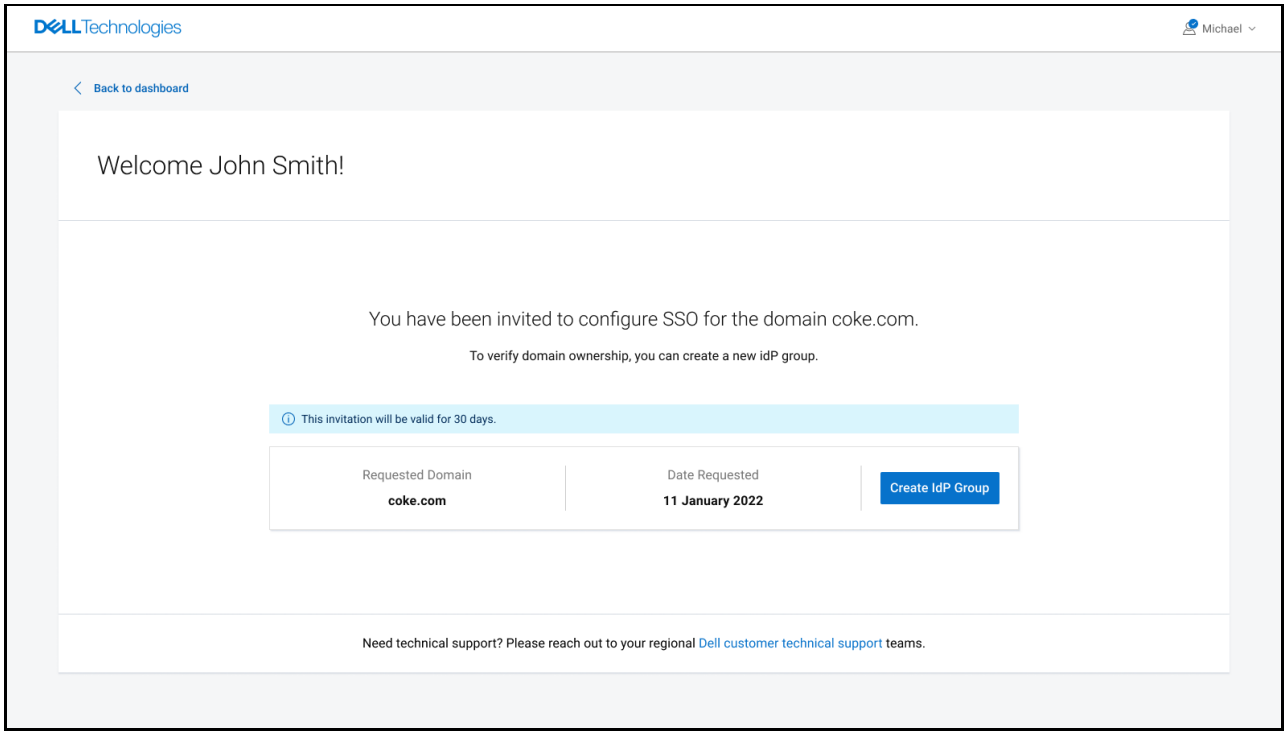

Figure 1 Create IdP Group

2. Perform the following:
   a. In the **IdP Group Name** field, enter the name of the IdP Group.
   b. Click **Create IdP Group**.

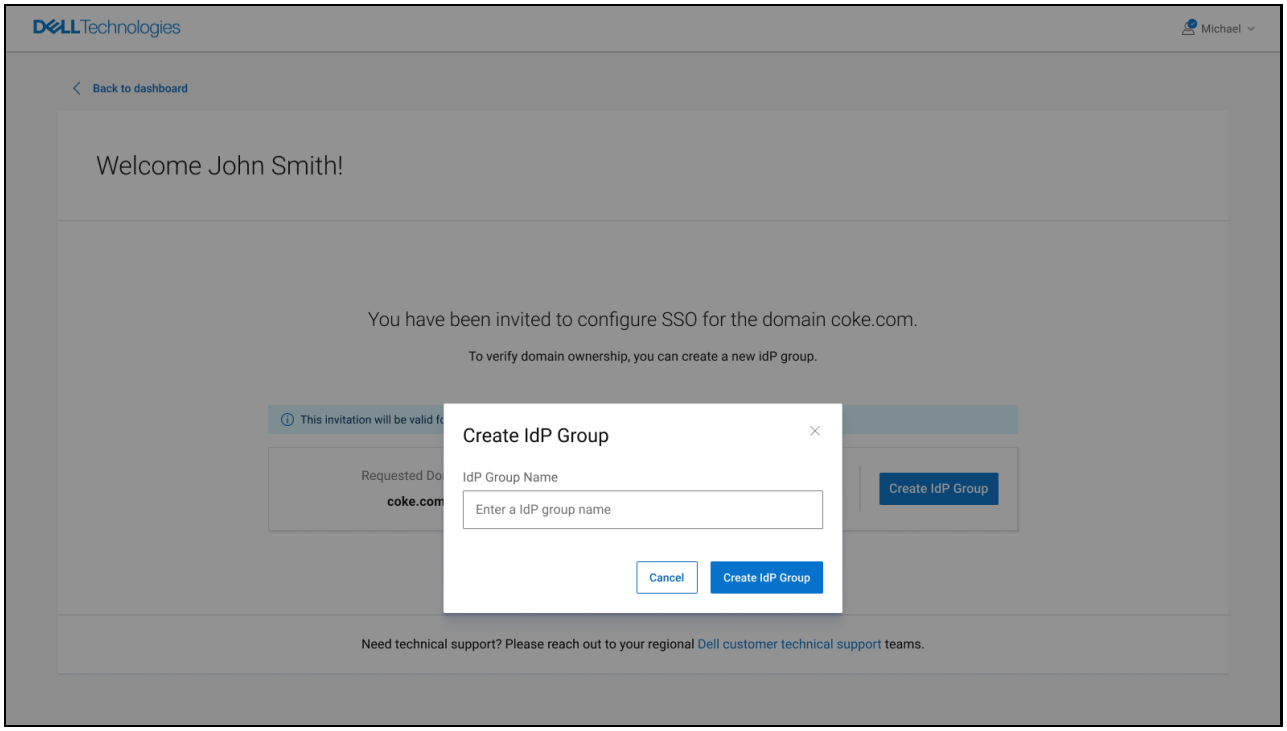

Figure 2 IdP Group Name

3. You will be redirected to the Manage Domain page as shown below. You can choose to either verify the primary domain or go to the dashboard by clicking on the "Back to Dashboard" button. To know more on how to verify a domain, refer **Section 2** of Domain Management document.

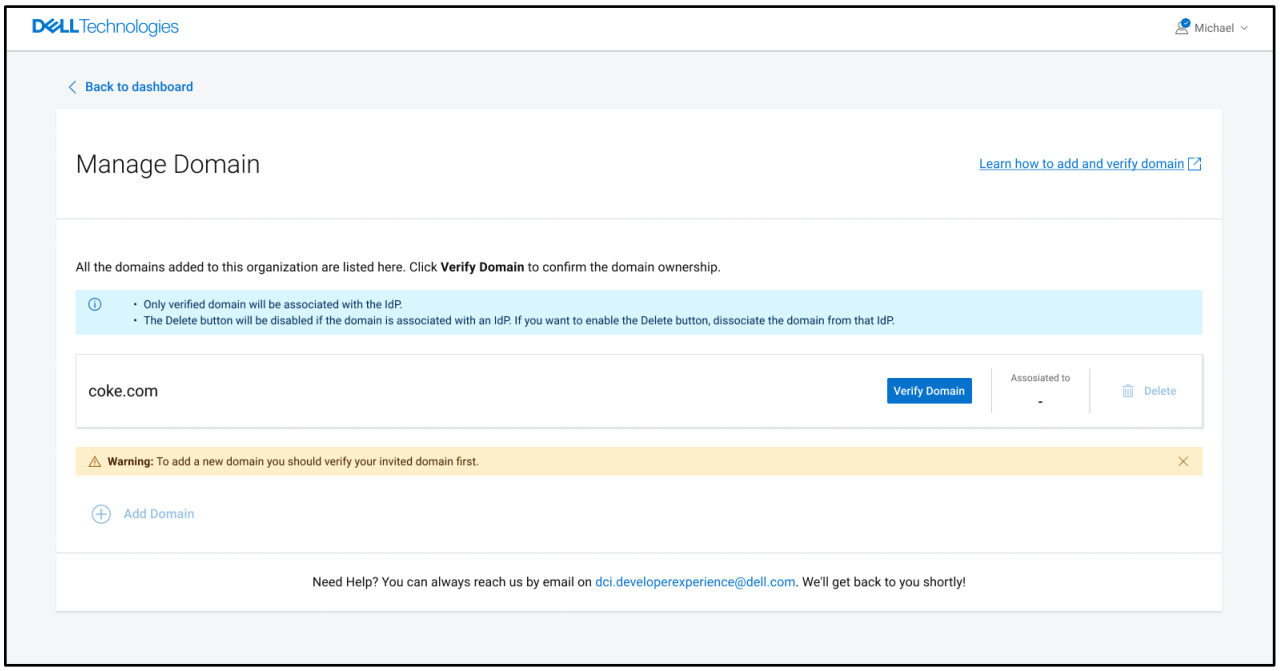

Figure 3 Verify Domain

4. Click **Register IdP for SSO**

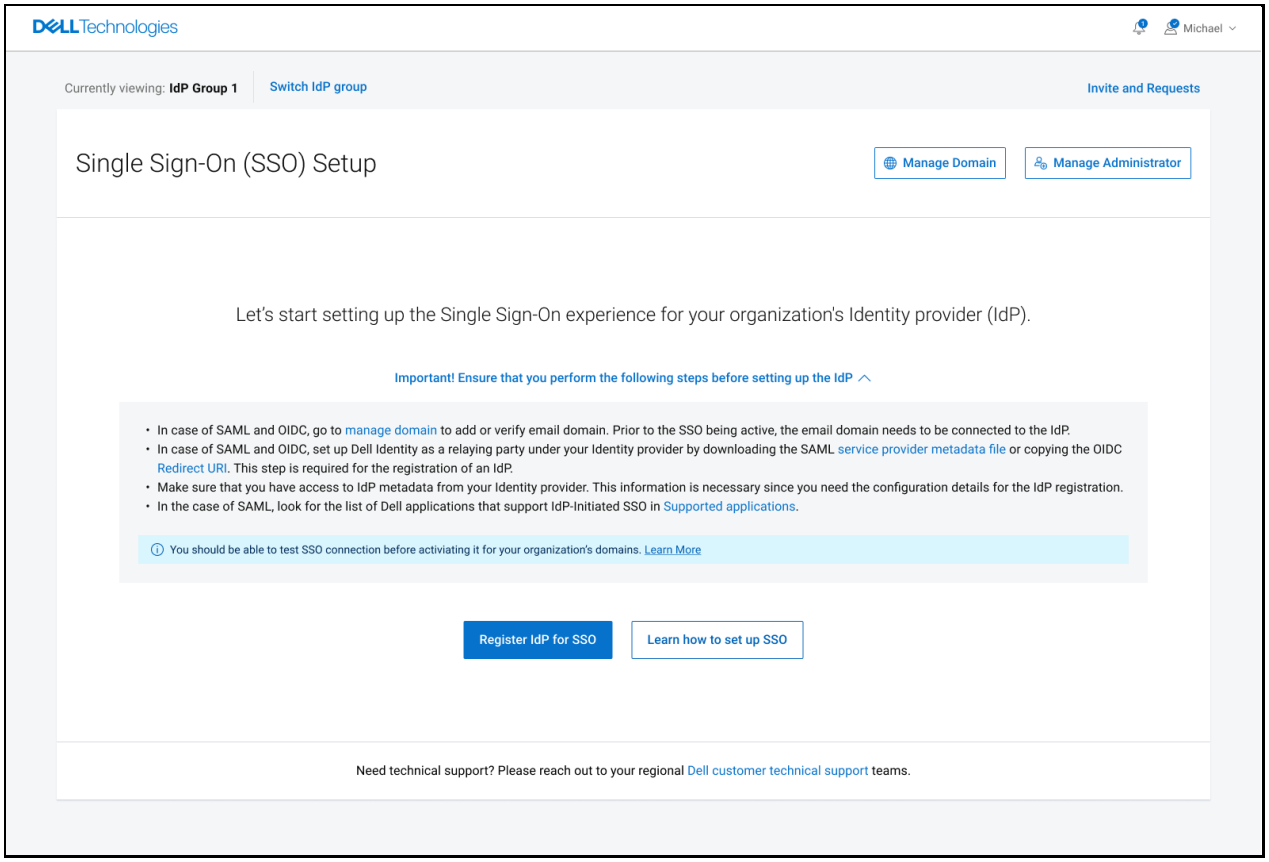

Figure 4 Register IdP for SSO

5. In the **Select Domain** Tab, perform the following:
   a. In the **SSO Configuration Name** field, enter the name for the SSO configuration record.
   b. Select the **Domain Name** associated with the IdP.
      If you cannot find the domain you want, then click **Manage Domain**. For more information on adding a domain, refer to the Step 2.a of Domain Management document.
   c. Click **Next**.

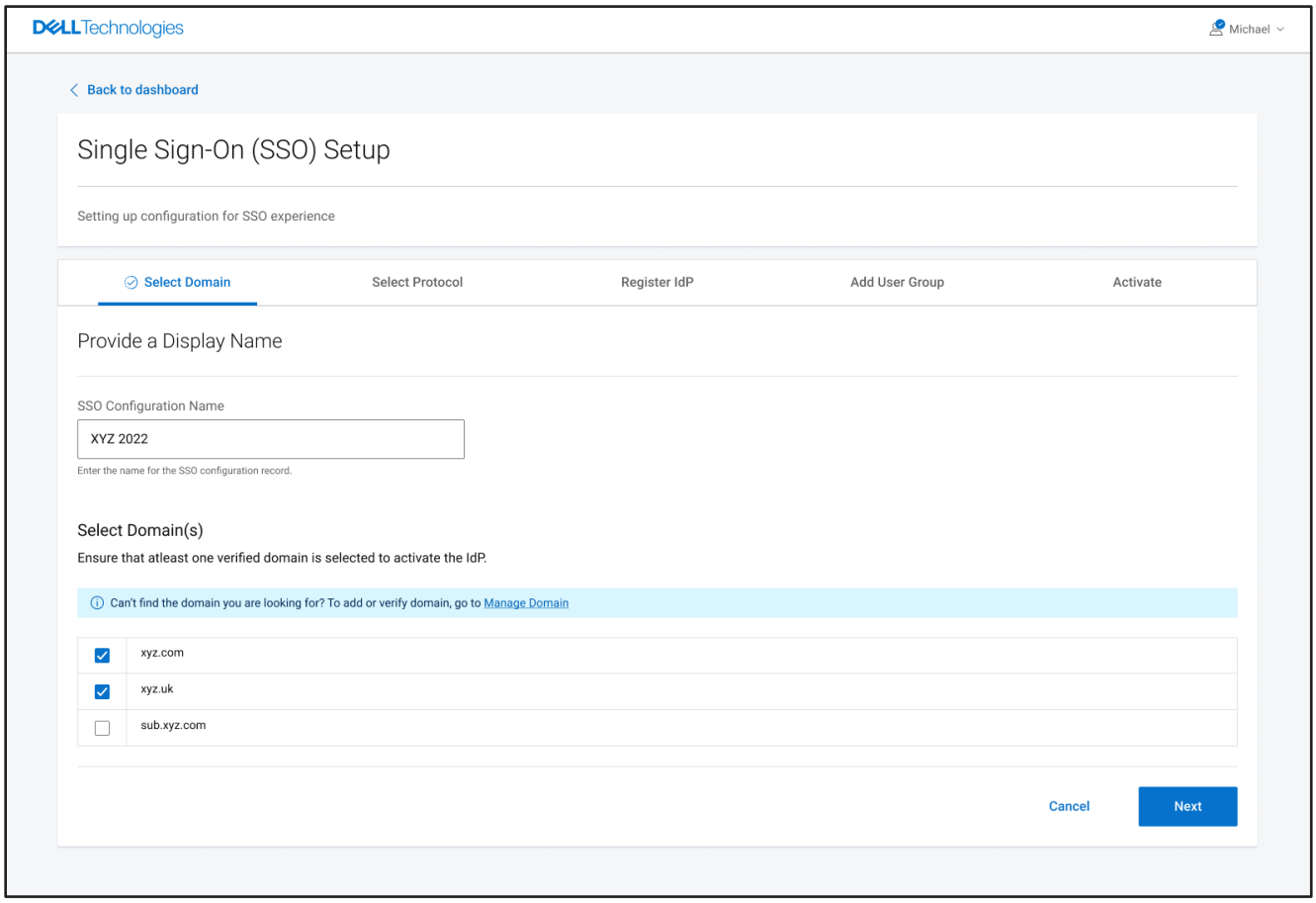

Figure 5 Single Sign-On Setup

Note: Ensure that at least one domain is selected to activate the IdP.

6. In the **Select Protocol** tab, perform the following:
   By default, SAML 2.0 is selected. For more information about SAML, click on **Learn more about SAML here.**
   For OIDC, refer Page 17.

   a. Select the authentication method.
      SP--initiated SSO is selected as the authentication method by default, and it cannot be changed.
      You can select IdP initiated SSO if your applications are listed in supported applications.
      For more information on SP-initiated SSO and IdP-initiated SSO, click on Learn more about SP & IdP initiated flow.
   b. Import the Identity Provider Metadata in one of the following ways:
      - **Upload IdP metadata**: If you have an IdP Metadata file, select **Upload IdP Metadata,** and click **Upload File.** Browse to the location where the IdP Metadata XML file is located and click **Open.** The IdP metadata file is uploaded.
      - **SAML Endpoint URL**: Enter the URL of the XML file that holds the federation metadata.
      - **Manually Enter Values**: If you do not have an IdP Metadata file, select **Manually Enter Values.**
   c. Click **Download SP Metadata (XML)** to download the metadata file and to set up Dell Identity as your Identity provider. For more information, click on **Learn more how to use SP metadata.**
   d. Copy all the SP metadata values and paste it in the respective fields at your IdP.
   e. After setting Dell Identity as your identity provider, click on **I have set up SP metadata and have uploaded to my Identity provider** check box.
   f. Click **Next**

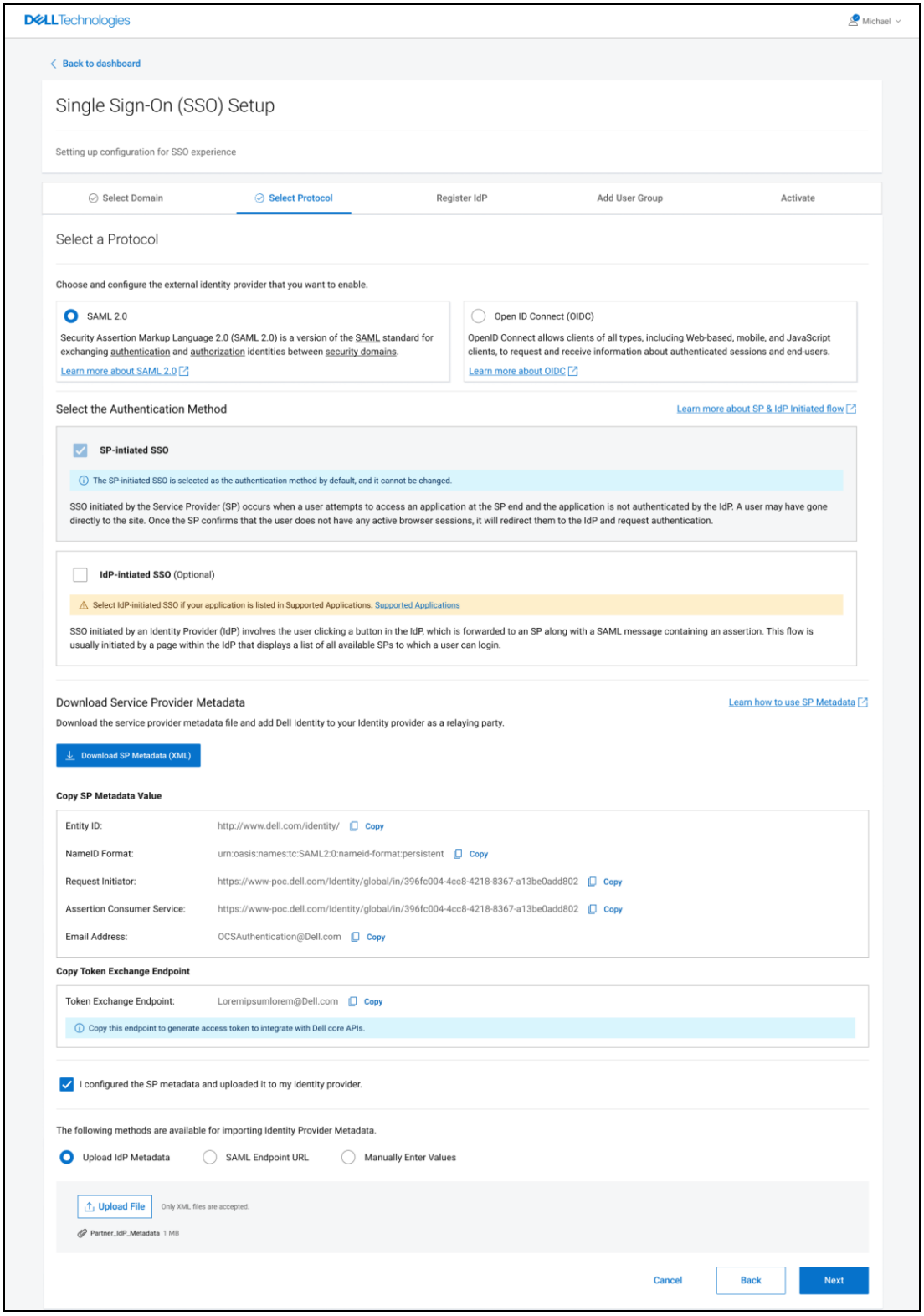

Figure 6 Select Protocol

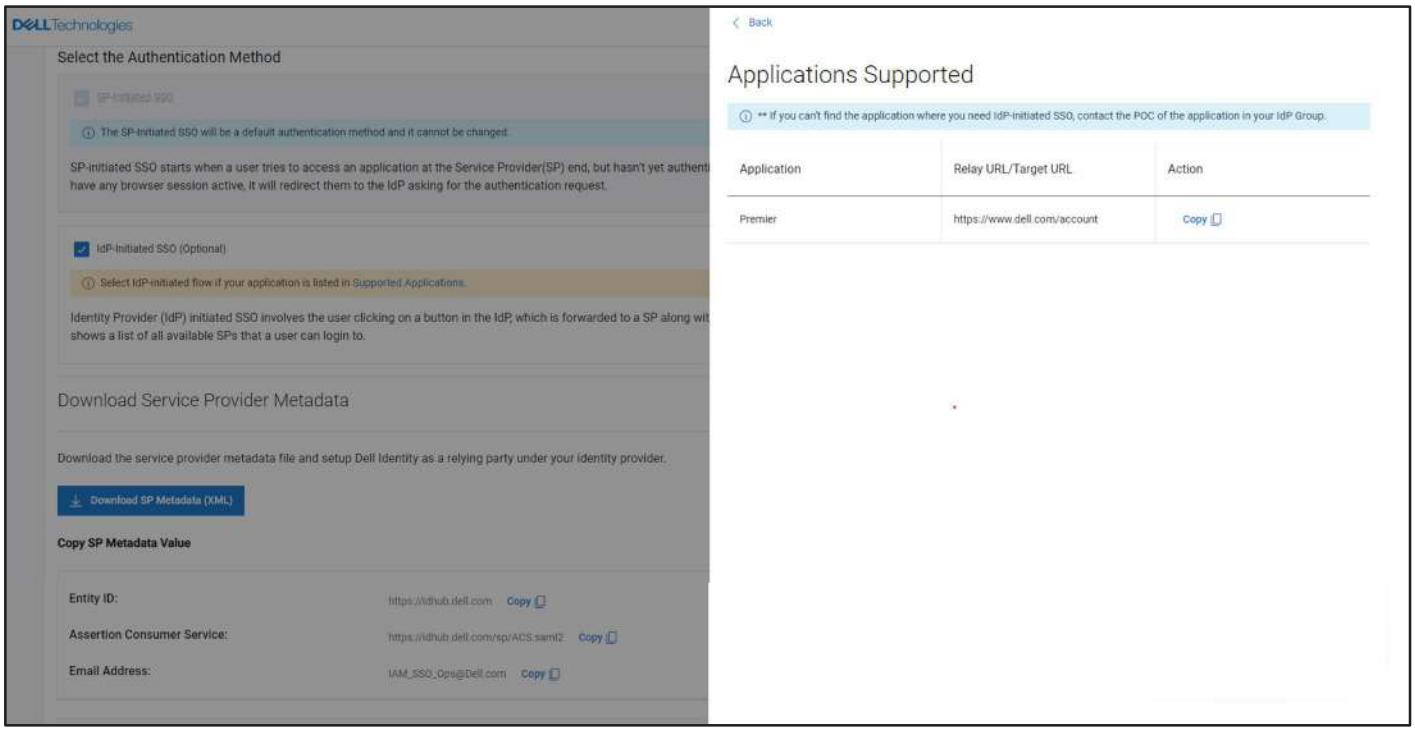

Figure 7 IdP Initiated SSO

7. In the **Register IdP** tab, all the fields in the Basic SAML information, Endpoints and Certificate section are auto populated if the IdP metadata file is uploaded.

   Claim section.

   a. In the Required Claims section, select the appropriate URLs from the drop-down list in the next fields.
   b. If necessary, select the claim list from the drop-down list for Member Of, Country Code, and Employee Type in the Optional Claims section.
   c. Click **Register**

Note: If any of the IdP Metadata sections contain errors, you will receive an error message. Ensure That you fix the errors before you register your IdP.

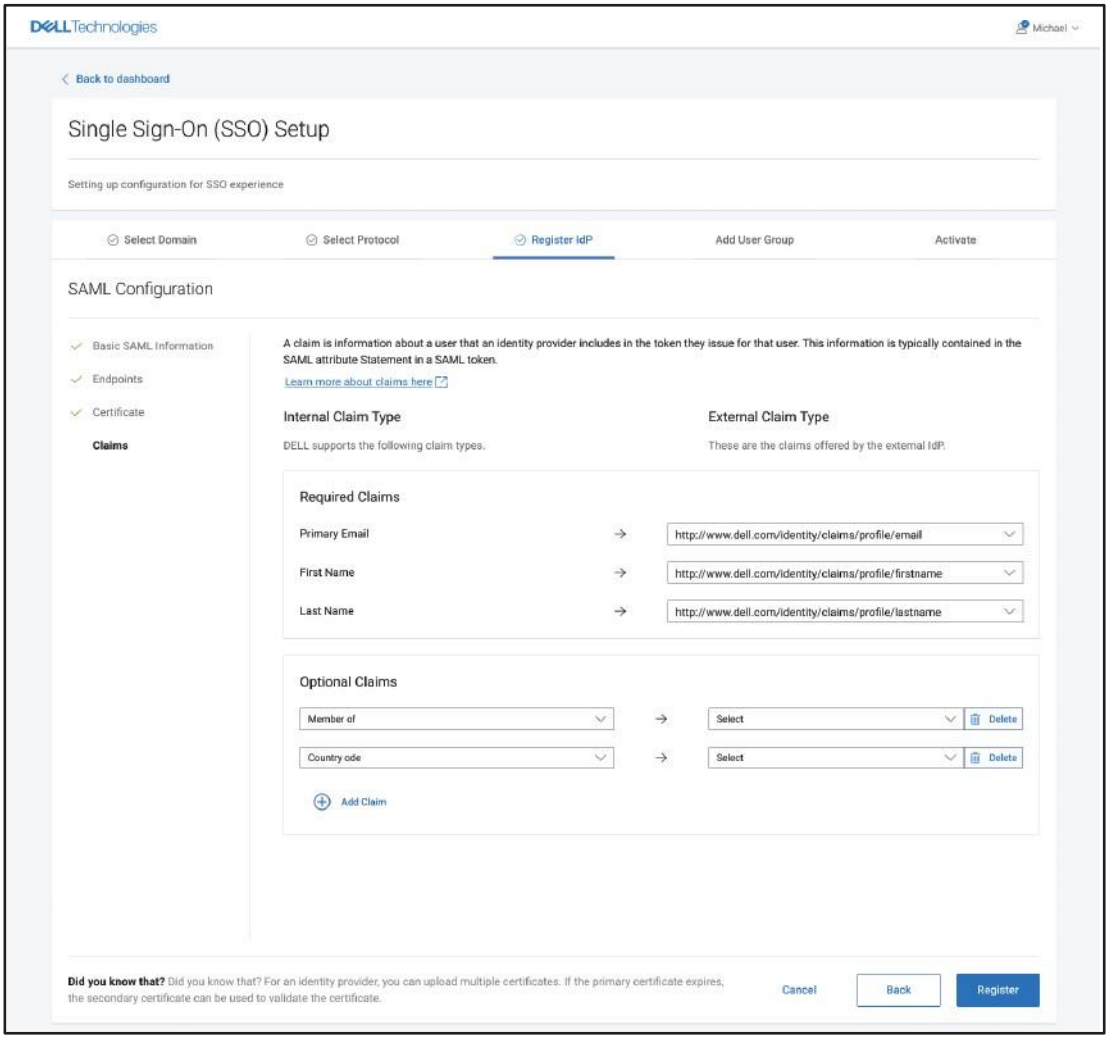

Figure 8 Register IdP

8. The **Add User Groups** tab is displayed. This is an optional step. If you do not want to update the user group, you can skip Step 7 and click **Next**.
   Even after activating the IdP, you can add User Groups.

9. In the Add User Groups, perform the following:
   a. To edit or delete an existing user group, click on the **Edit** or **Delete** icon with the respective user groups.
      OR
      To add new user groups, click on the **Add New User Group** button. Enter the name of the user group in the **Enter a group name** field and click **Save**.

Note: The groups set up will be effective only if the Member Of has been mapped.

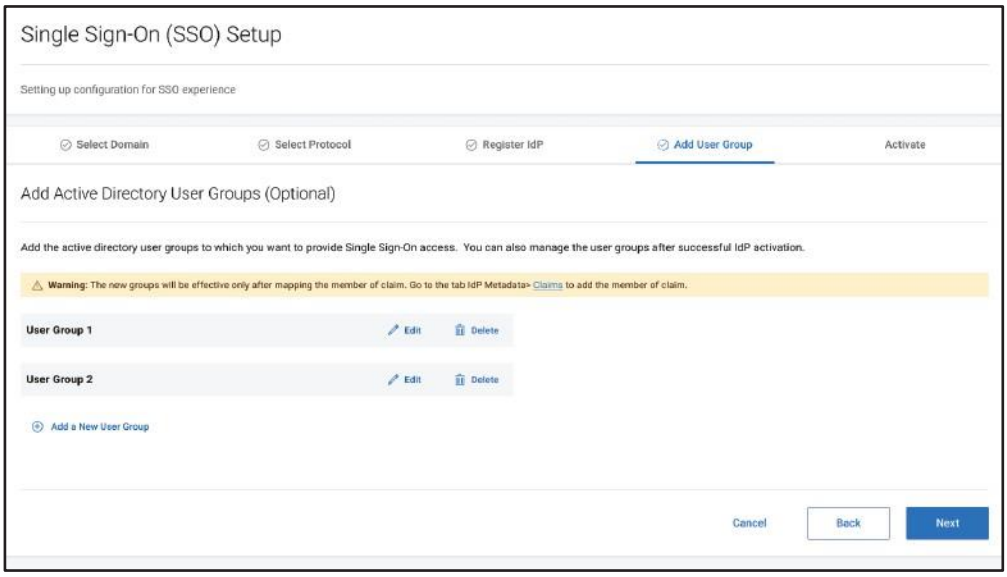

Figure 9 Add User Groups

   b. Click **Next**.

10. It is recommended to test the IdP connection and perform an end-to-end SSO testing to activate the IdP. This helps in detecting issues or if there is any break in connection. Click **Activate**.

    To test the IdP connection,

    a. Click **Test IdP Connection**. This will open an SSO session in a browser window with Dell Identity using your IdP. When prompted, Sign in using your corporate credentials, and the test results will appear on the page.
    b. If the setup is tested successful, navigate to the tab **Test Connection** on the **Single Sign-on Setup page,** and invite a user to test SSO. If the test fails, check the IdP configuration. If you require assistance, please contact the Dell Identity team.

    To invite users to Test SSO experience,

    a. Click **Enable Test SSO** to test the SSO experience.
       - Enabling Test SSO generates a unique email address for this IdP.
       - SSO is activated only for the users that are using this unique IdP email address.
    b. Share the unique email address that is generated with trusted users allowed to test the SSO.
    c. Share the application URL with the user to test the SSO.
       For SP Initiated SSO, users are required to access their specific application from Dell.com page to test the SSO.
       For IdP Initiated SSO, use the URL generated by your IdP and share the URL with your users to authenticate it with your IdP. On successful authentication, the user is redirected to the application using the relay URL mentioned in the table.
    d. Once Test SSO has been successfully confirmed, click **Activate**.

    Note: - If the user activates the IdP without disabling the test SSO, the test SSO will be automatically disabled.
    - After clicking on Activate, the IdP is activated but the SSO experience will be enabled after 40 minutes.
    - If you click Skip Activation, your IdP will be in 'Pending Activation' state. In case you want to activate your IdP, click Edit IdP and update the required information.

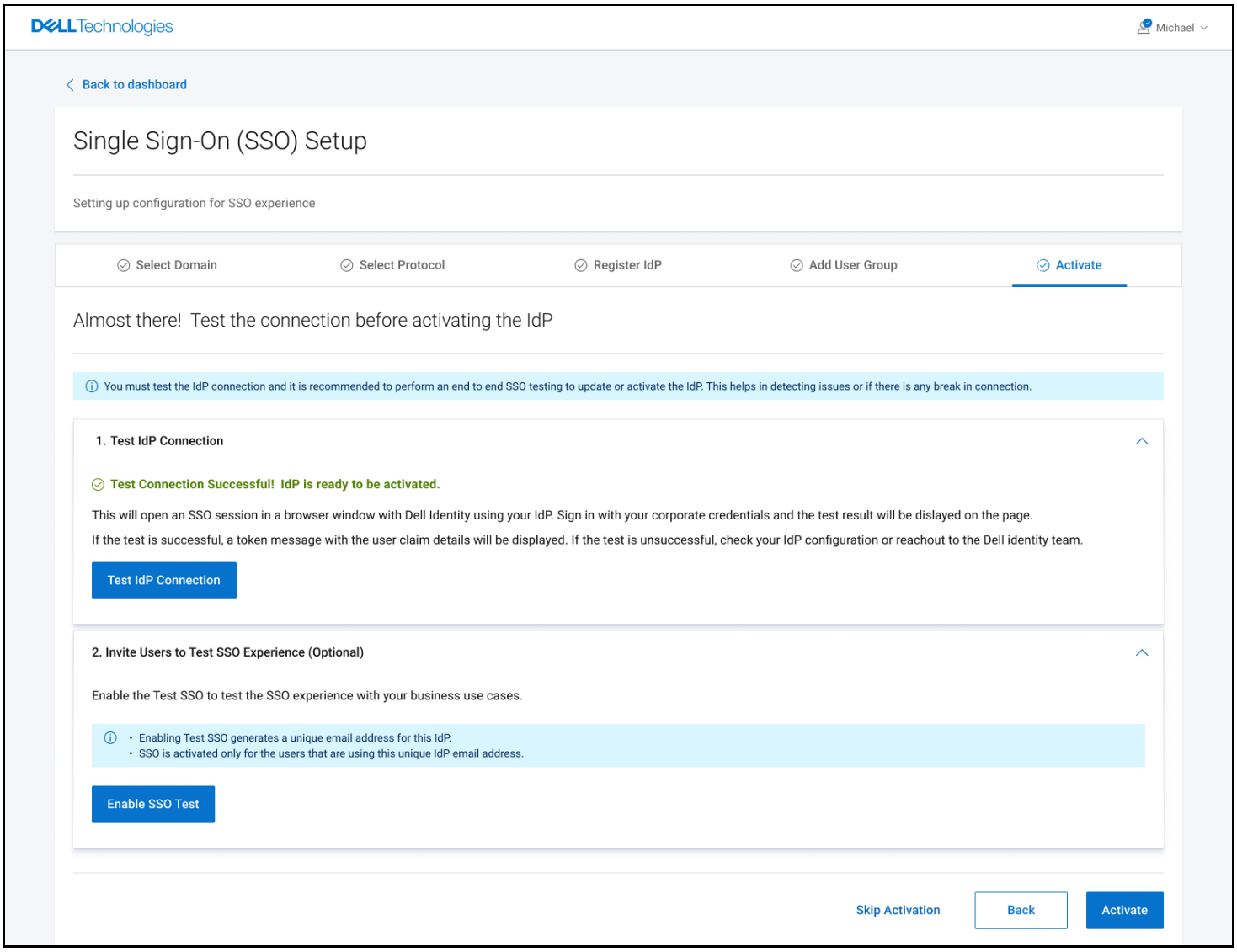

Figure 10 Activate

11. If you want to disable your registered IdP, click **Disable** on the IdP configuration page.
    A confirmation message dialog box will appear to confirm if you want to disable your IdP. Click **Yes**.
    Your registered IdP will be disabled.

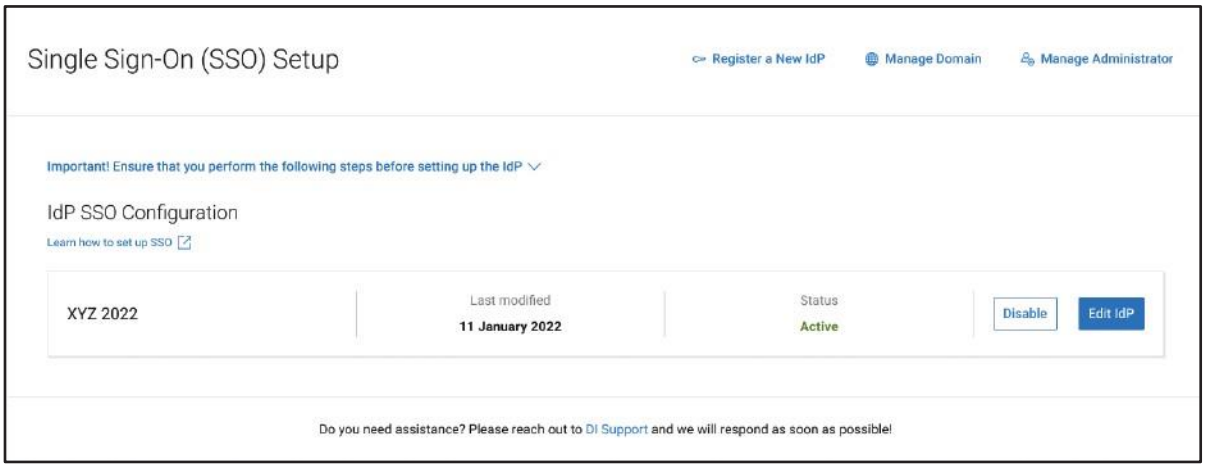

Figure 11 Registered IdP - Disabled

Note: Ensure that at least one domain is selected to activate the IdP.

1. In the **Select Protocol** tab, select OIDC as protocol.
   For more information about OIDC, click on **Learn more about OIDC**.
   a. There are two ways in which configuration can be enabled
   Well known Endpoint
   Manually Enter Values
   Select either **Well known Endpoint** or **Manually Enter Values**,
   b. Enter either Well known Endpoint or Manually Enter Values as per the selection.
   c. Click **Next**

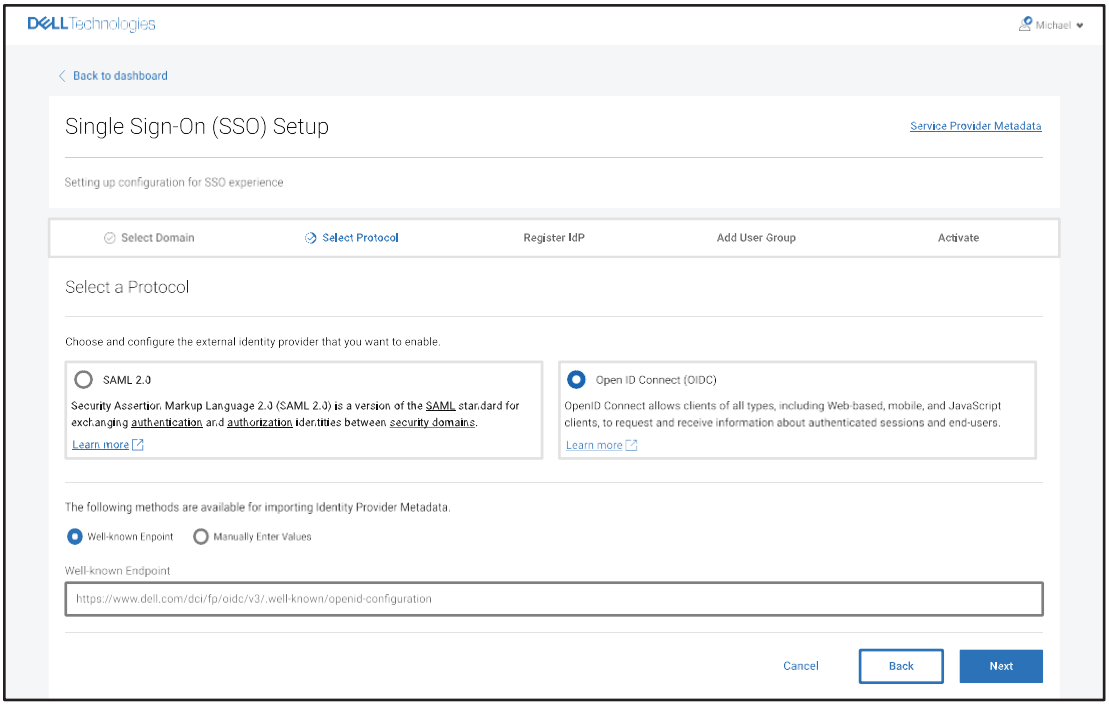

Figure 12 OIDC - Select Protocol

2. In the **Register IdP** tab, Issuer and Redirect URI, and all the fields in the Endpoint are auto populated.
   Basic Information
   a. Enter **Client ID**, which you will find on your Identity Provider.
   b. Enter **Client Secret**, which you will find on your Identity Provider.
   c. Copy the **Redirect URI** and configure with your application.

Note: Changes to the issuer will update the Redirect URI

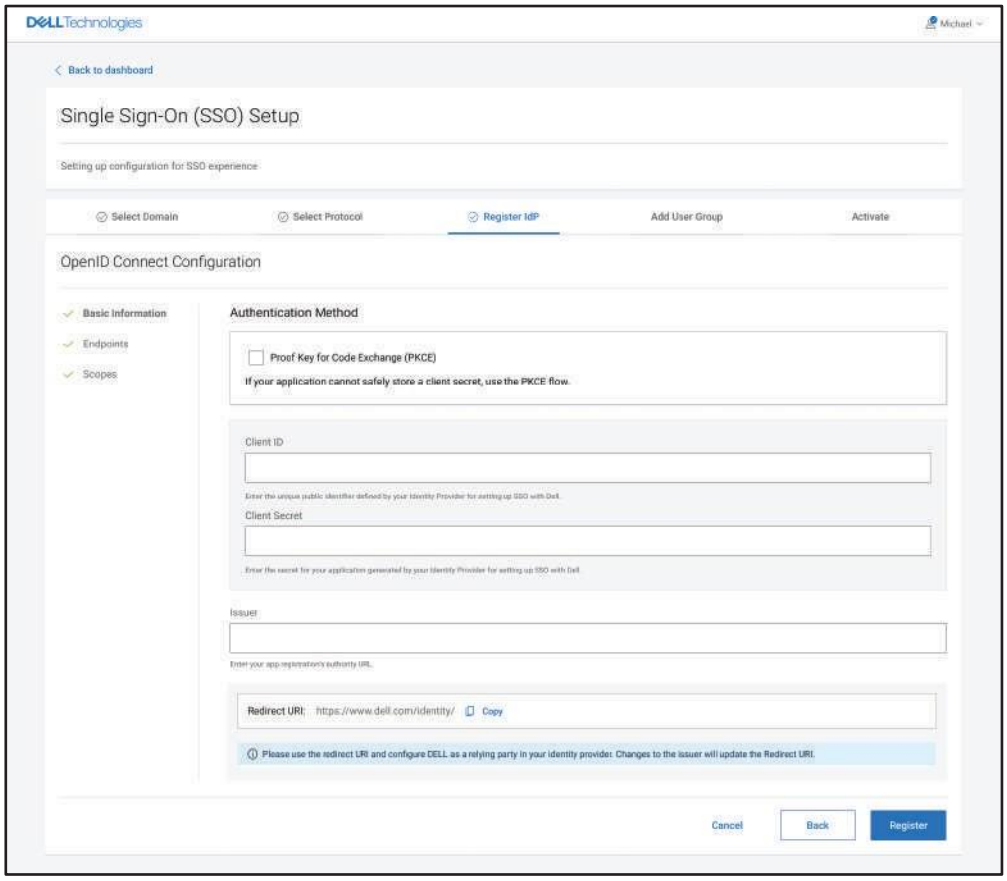

Figure 13 OIDC - Register IdP - Basic Information

Endpoints

Endpoints are auto populated from the Well Known Endpoints or Manually Entered Values.

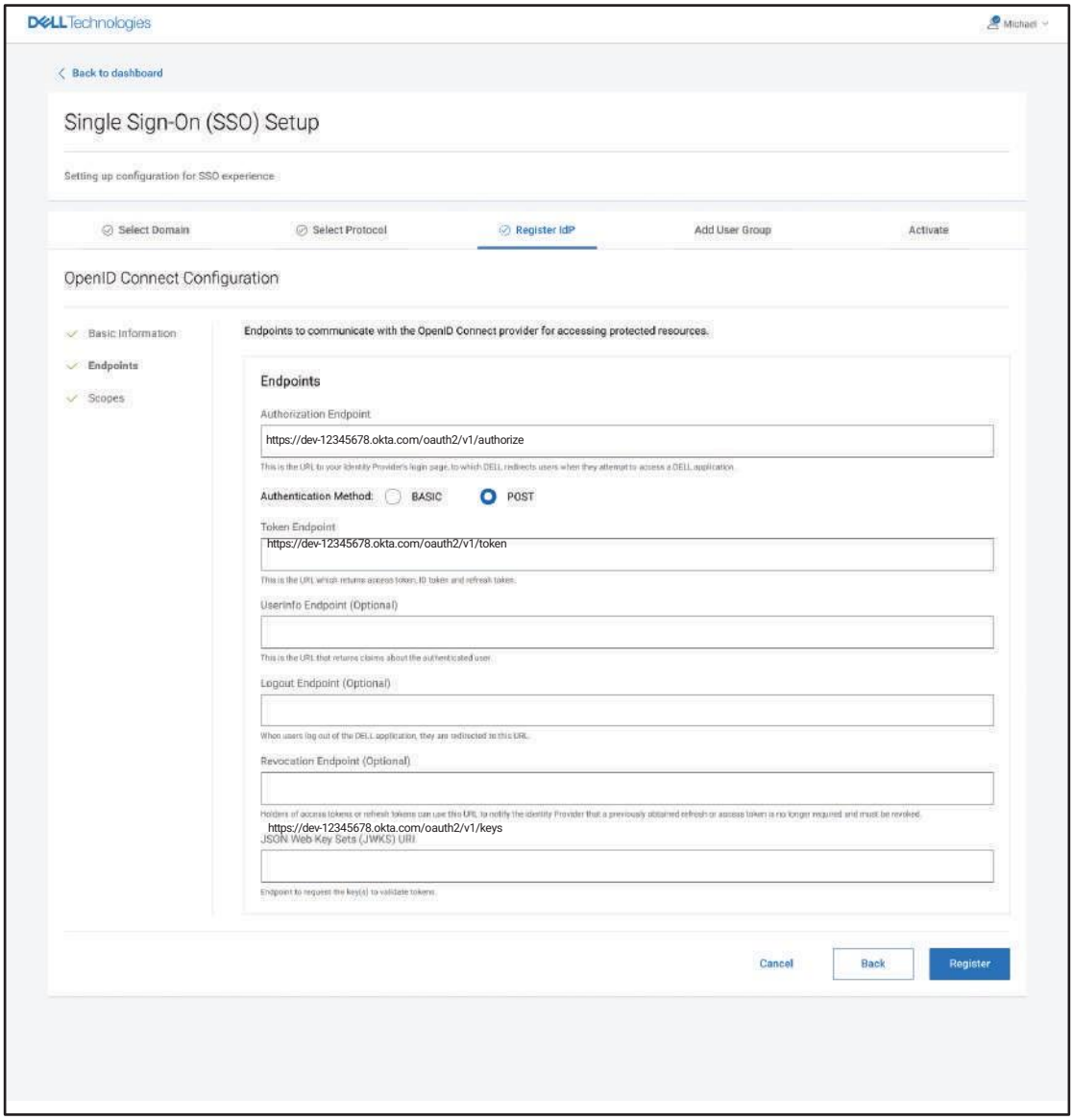

Figure 14 OIDC - Register IdP - Endpoints

Scopes
a. Some of the predefined scopes are auto populated based on the Well Known Endpoint or Manually Entered Endpoints
b. Enter or Select Claim for UUID
c. Click **Register IdP**

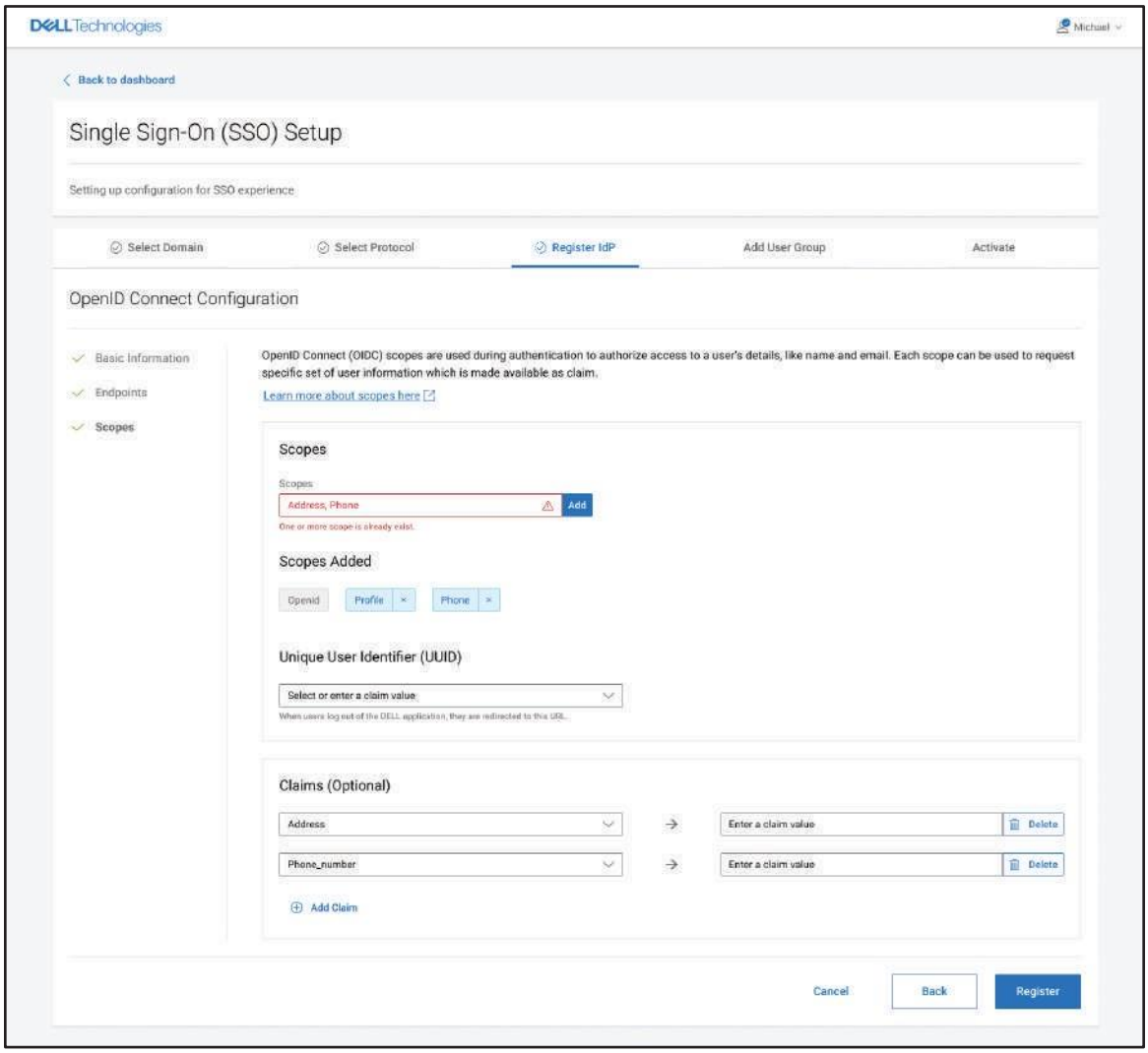

Figure 15 OIDC - Register IdP - Scopes

For **Add User Group** and **Activate** refer to Page 9 – Page 11.

1 Managing Identity Administrator

To invite a new Identity Administrator from dell identity portal, perform the following:

a. In the IdP configuration page, click **Manage Identity Administrator**.
b. Enter your First name, Last name, and Email address.
c. Click **Invite**.
   The requested user will receive a welcome email along with the steps to be followed. For more information, refer to Topic 1: **Sign In and Verify your Account** of Email Invitation document.