Azure AD integration with EloView (SAML)

This guide will teach you how to integrate EloView single sign-on (SSO) with Microsoft Azure Active Directory (Azure AD). It will also reference configuration steps for Hybrid Azure AD. When you integrate EloView with Azure AD, you can:

- Control in Azure AD who has access to EloView.
- Enable your users to sign in to EloView with their Azure AD account automatically.
- Manage your accounts in one central location - the Azure portal

Prerequisites

To get started, you will need the following items:

- Azure AD subscription with Global Administrator access or privilege to create enterprise applications.
- EloView subscription with Admin role access. If you don't have a subscription, you can sign-up for a free 45-day trial account from https://manage.eloview.com for your organization. If your organization already has an EloView account, ask a member to send an invite from the User Management page.

Note for Hybrid Azure AD
You will need to install Azure AD Connect (ADSync) as an on-premise service to synchronize user accounts and groups between Azure AD and Active Directory.

Collect EloView OrgID

1. *Sign in* to the **EloView** (https://manage.eloview.com) with an account with Admin privileges.

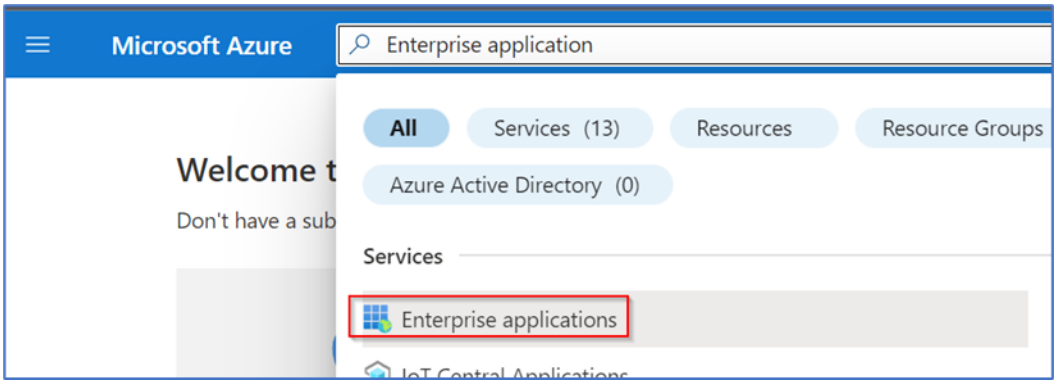
2. At the top navigation section, *click* **Accounts** and then **Account Settings**.

3. On the **Details** tab, *record* your **OrgID**

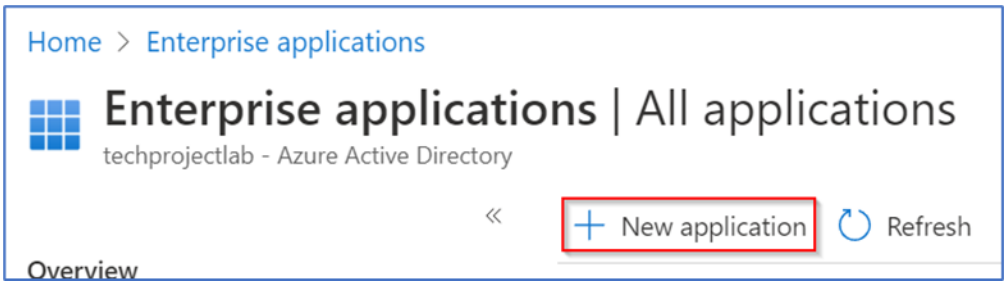
Create an enterprise app named EloView in Azure AD

4. *Sign into* your **Azure portal** (https://portal.azure.com) with an account with a Global Administrator role or privilege to create enterprise applications.

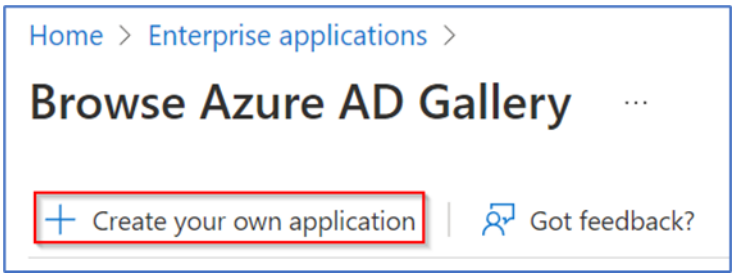
5. In the search bar, type in enterprise application, and then click the results **Enterprise application**.



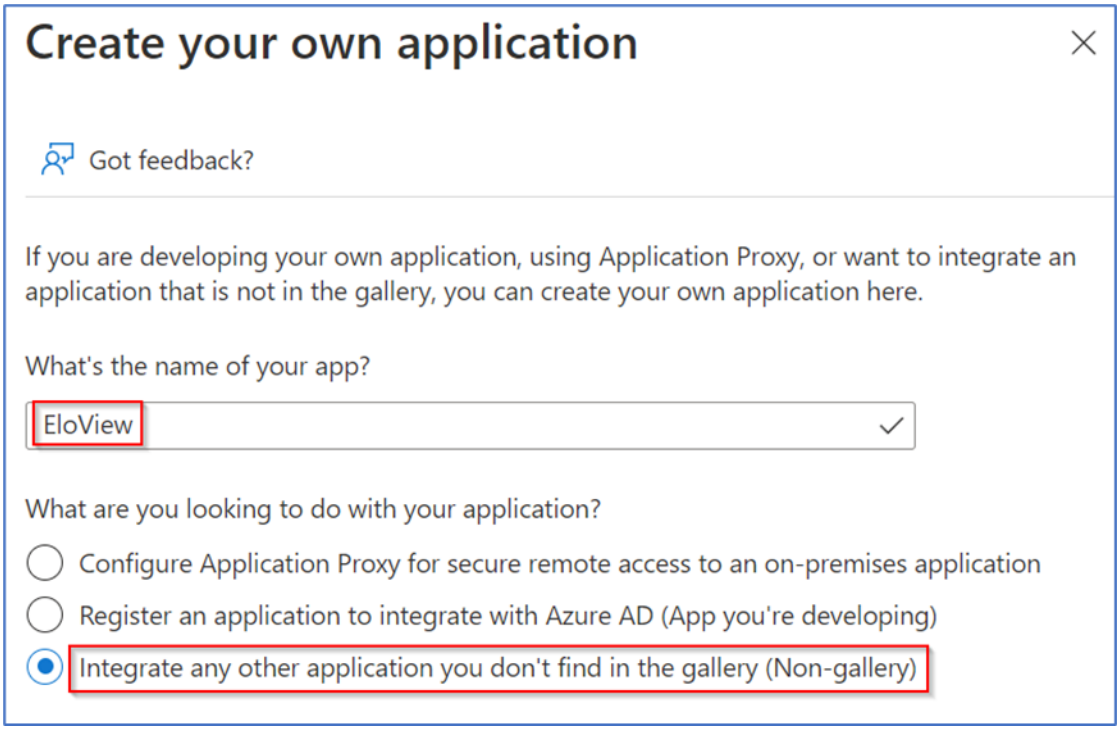
6. *Click* **New application**



7. *Click* **Create your own application**

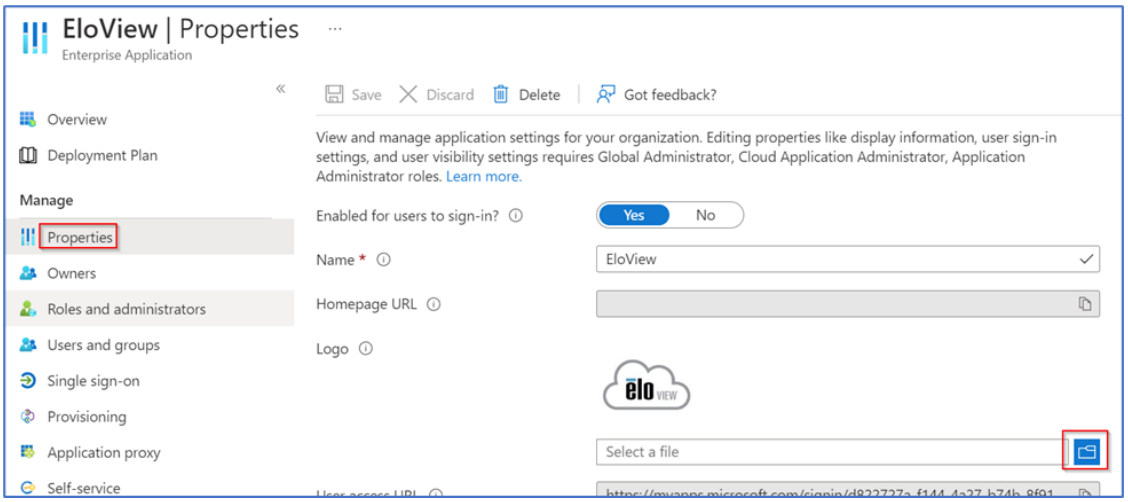


8. *Provide* a **name** for your application. For example, **EloView**
9. *Select* **Integrate any other application you don't find in the gallery (Non-gallery).**

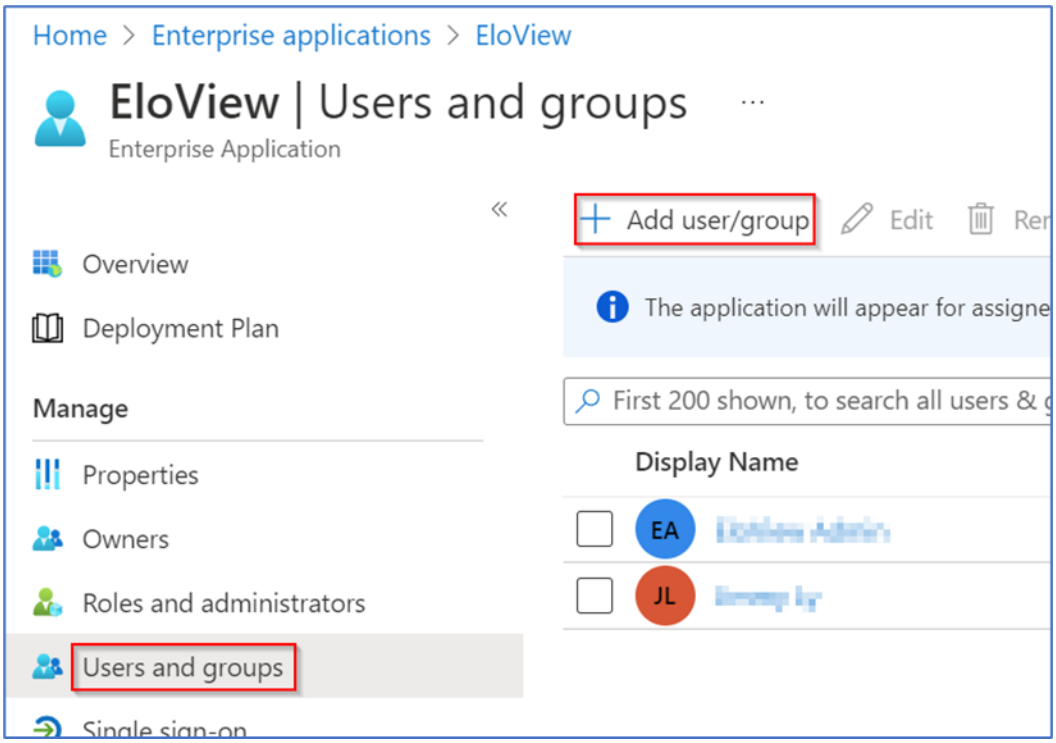


10. At the left navigation pane, *click* **Properties**. *Upload* an image file for your application, and then *click* **Save**. This is the application logo that users will see on My Apps, in the Office 365 application launcher, and when admins view this application in the application gallery.

Right-click on image save logo



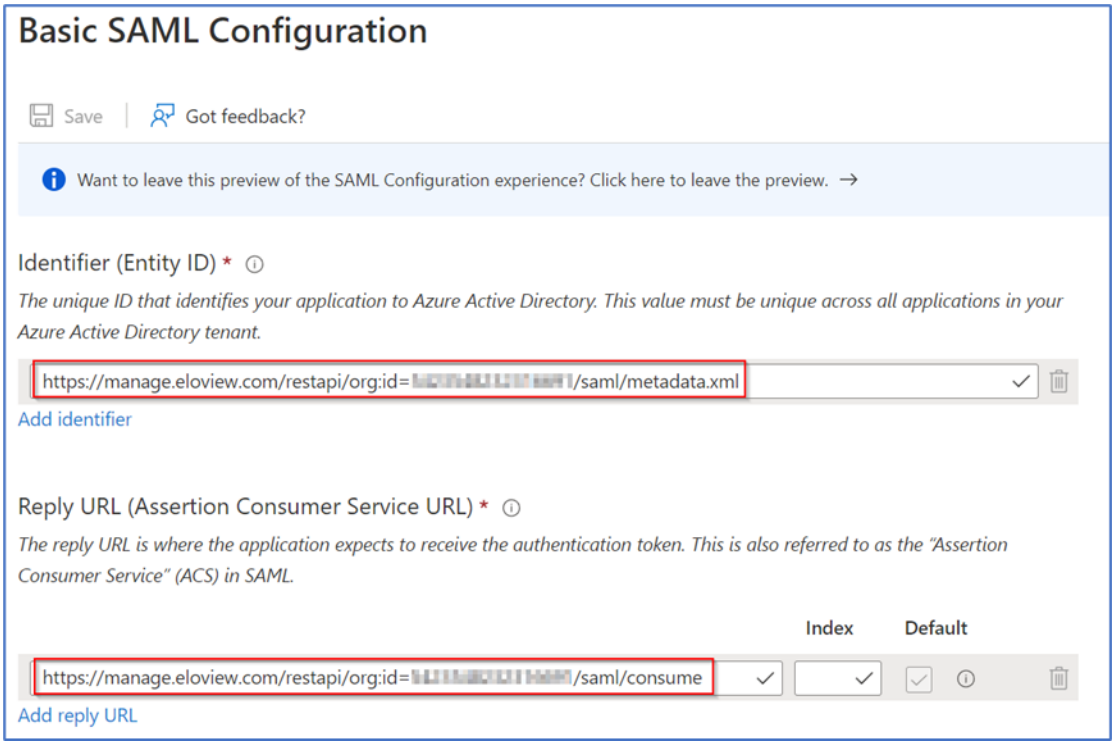
11. At the left navigation pane, *click* **Users and group**. *Click* **Add user/group**, *click* **None selected**, *choose* **users**, *click* **Select**, and then **Assign**.



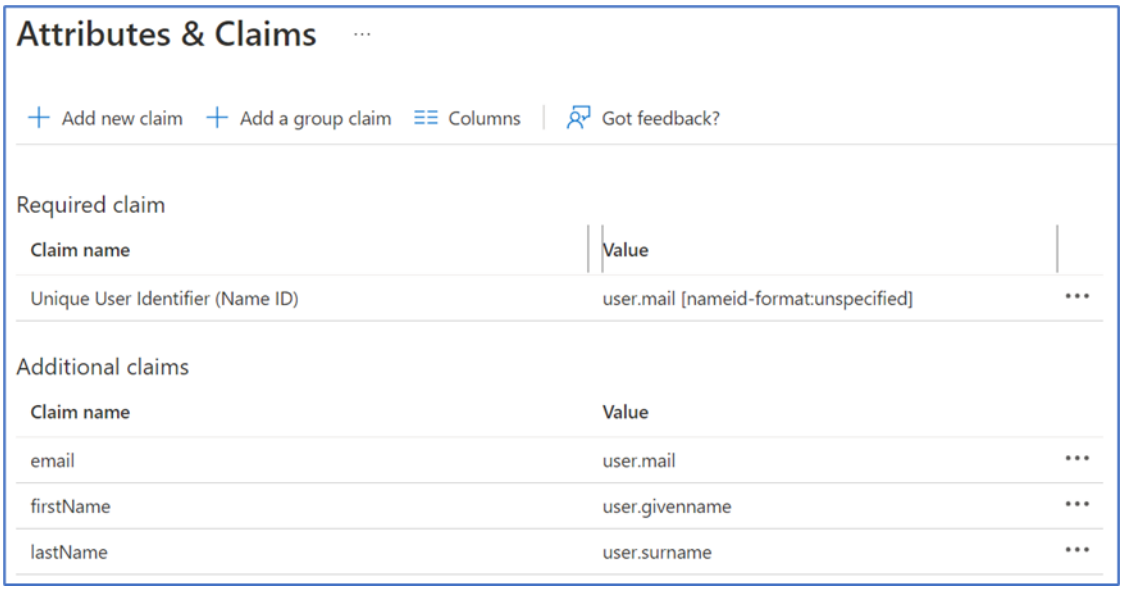
12. At the left navigation pane, *click* **Single sign-on**. The next following section will cover configuring boxes 1-4. In **Box 1**, *click* **Edit**.

13. *Enter* the following values after replacing **bold sections** with your **OrgID #**. Refer to steps 1-3 to collect your unique OrgID from EloView. Click Save when finished.

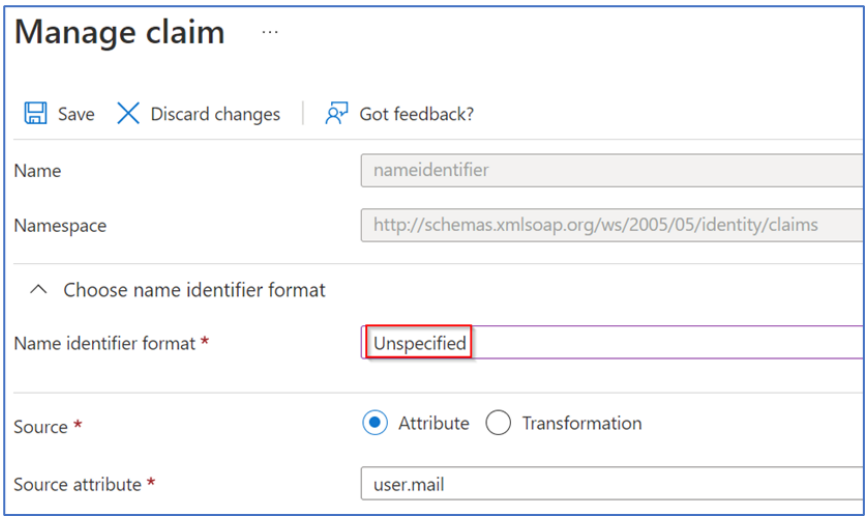
Identifier (Entity ID)
*https://manage.eloview.com/restapi/org:id=**1234567XXXXXXXX1**/saml/metadata.xml*
Reply URL (Assertion Consumer Service URL)
*https://manage.eloview.com/restapi/org:id=**1234567XXXXXXXX1**/saml/consume*
*Leave the index value blank.



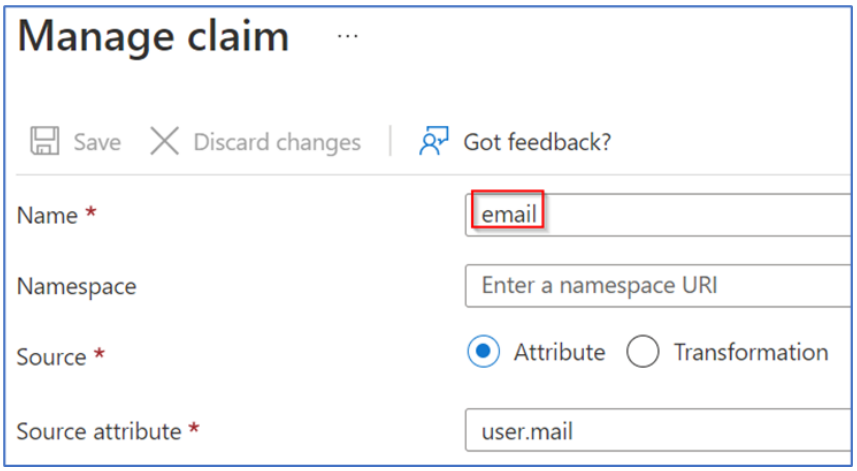
14. In **Box 2**, *click* **Edit**. Match the following **claims** and **values** shown in the image below.



15. *Click* **user.mail [nameid-format:emailAddress]**, *change* the Name identifier format to **Unspecified** and then *click* **Save**.

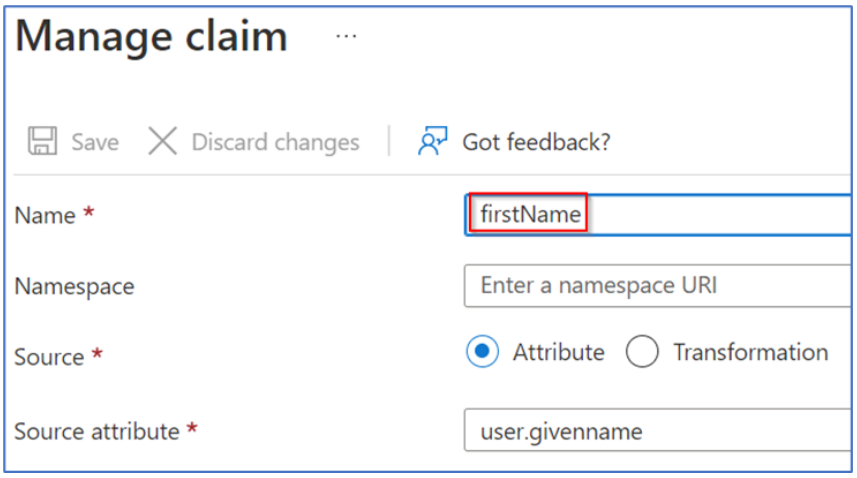


16. *Click* **user.mail**, *change* Name to **email**, *clear* the value in **Namespace**, and then *click* **Save**.



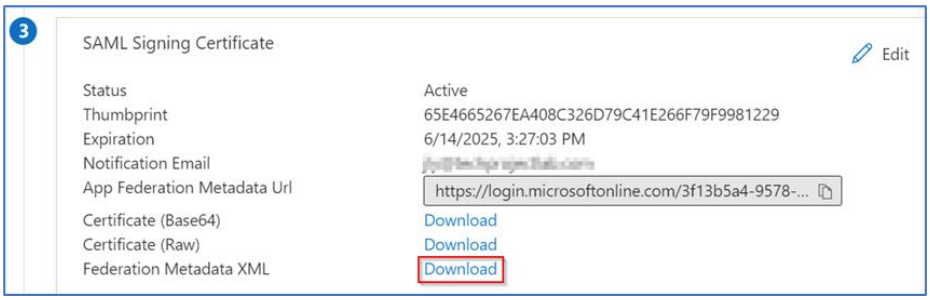
17. *Click* **user.givenname**, *change* Name to **firstName**, *clear* the value in **Namespace**, and then *click* **Save**.

18. *Click* **user.surname**, *change* Name to **lastName**, *clear* the value in **Namespace**, and then *click* **Save**.



19. Next to **user.userprincipalname**, *click* the **...** (dots), and then *click* **Delete**. Confirm Delete.

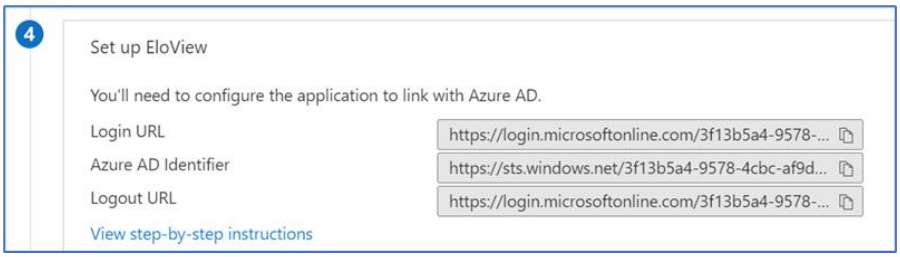
20. In **Box 3**, *click* the **Federation Metadata XML** download link.



21. *Open* the XML file with a text editor and then *search* for the text string **X509Certificate**.

22. Record the long string of text between **<X509Certificate>** and **</X509Certificate>** for later use.

23. In **Box 4**, record the **Login URL** and the **Logout URL** for later use.

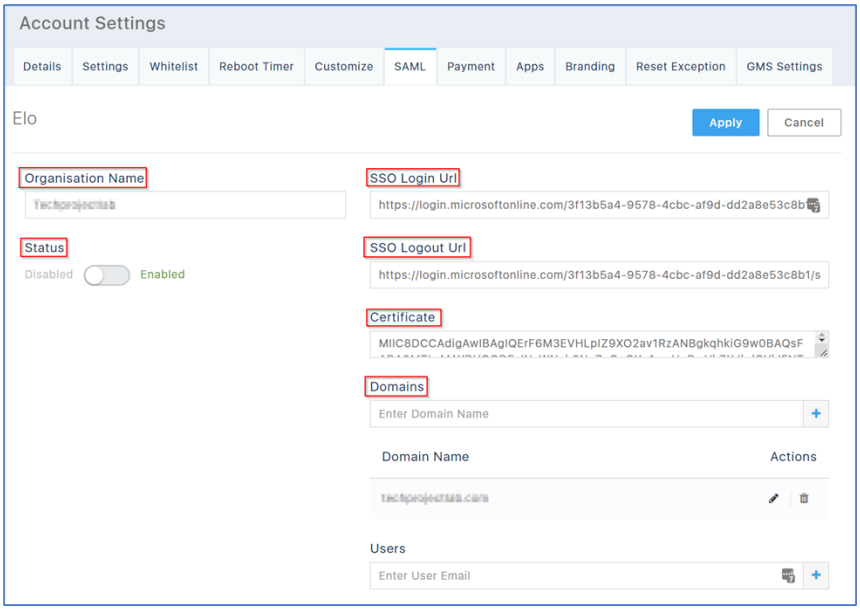


Configure SAML settings in EloView

24. *Sign in* to the **EloView** (https://manage.eloview.com) with an account with Admin privileges.

25. At the top navigation section, *click* **Accounts** and then **Account Settings**.
26. On the **SAML** tab, *click* **Edit**.

27. *Enter* a **nickname** for your identity provider (Idp). For example, **Azure AD**.



28. *Paste in* **SSO Login URL** taken from the **Login URL**. Refer to step 23 to obtain the Login URL.

29. *Paste in* **SSO Logout URL** taken from the **Logout URL**.

30. *Paste in* the **Certificate string** taken from the **Federation Metadata XML** file.

31. *Enter* the **domain names** associated with your user's email addresses, and then *click* **(+)** to add.

32. Leave the Users field blank.

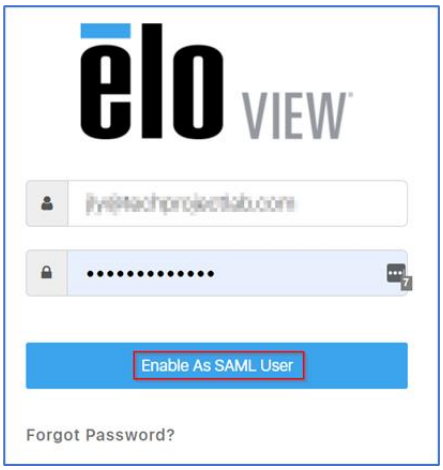
33. *Switch* the **Status** to **Enable**, and then *click* **Apply** when finished. After enabling SAML, optionally *enable* **Login via SAML only** after successfully verifying single sign-in.

Verify EloView SSO from the Microsoft My Apps Portal

34. *Sign into* the **Microsoft My Apps portal** (https://myapps.microsoft.com) with your organization user account to access the application library. This user account should have EloView admin account access.

35. *Click on* your new **EloView** enterprise application.

36. On the **EloView sign-in page**, *click* **Enable as SAML User**. *Refresh* the page if needed.



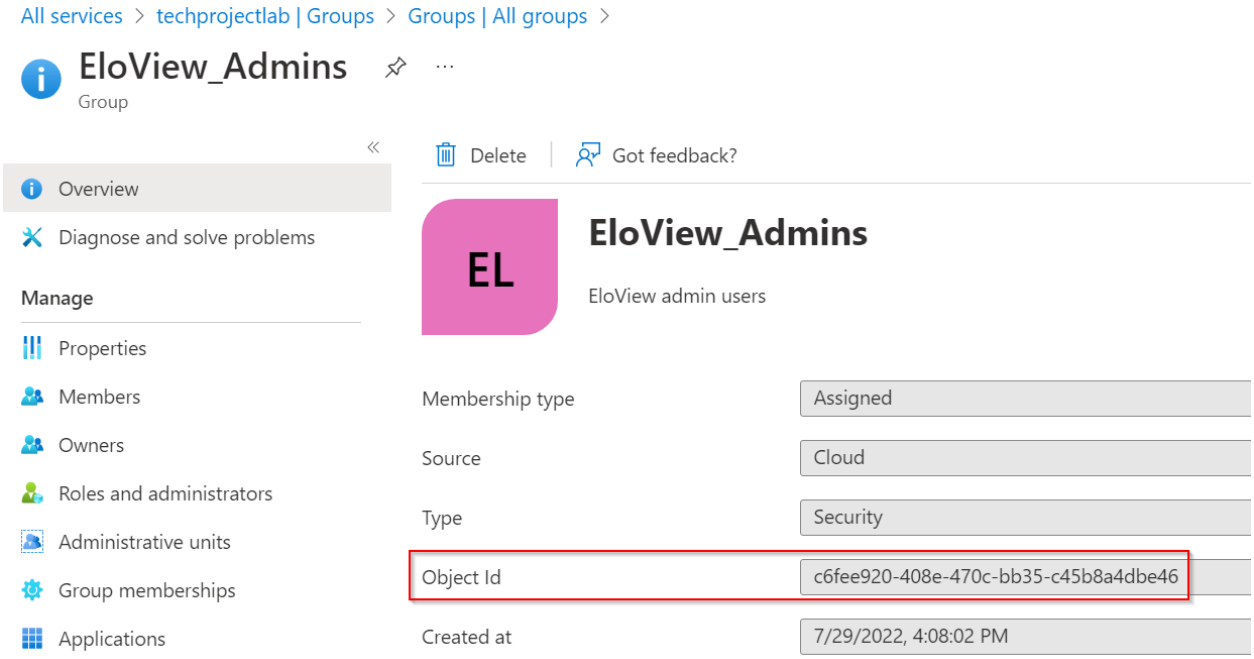
37. At the top navigation section, *click* **Accounts** and then **Manage Users**. If the Account Type for the admin account has changed to **(SAMLUser) Account Admin**, SAML configuration was successful.

Configuring access roles with security group claims in SAML token

38. *Sign into* the **Azure portal**.

39. *Create* a **new security group** in **Azure AD** or **Active Directory**. For example, EloView_Admins or EloView Admins.

40. *Go into* the **security group properties** and collect the **Object Id**.



41. *Add* **users** to the **security group** you want to have access to this role.

42. *Sign into* **EloView**. *Go to* **Accounts, Manage Users**, and then the **Roles tab**.

43. *Click* **Add New Role**

44. *Paste in* the **Object Id** of the **security group**. At this time, using the display name of the security group to name the custom role is not supported.

45. Using the toggles, **enable permissions** for the role, then *scroll* towards the bottom of the page, and finish assigning permissions by *clicking* **Done**.

46. *Go back* to the **Azure portal**.

47. *Go to* your **"EloView" enterprise application**.

48. *Click* **single sign-on**, and then the **edit button** under **Attributes & Claims**

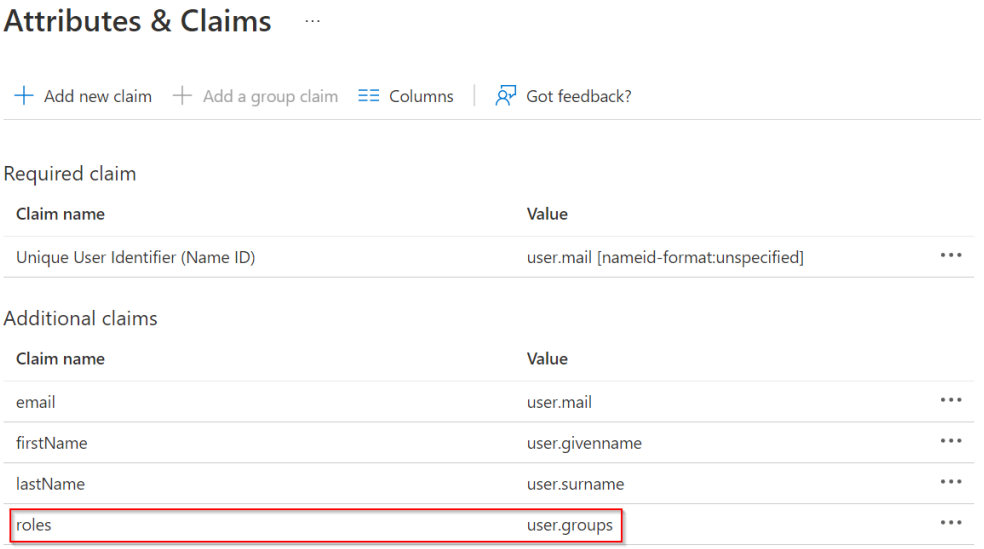
49. *Click* **Add a group claim**

50. From the **Group Claims** windows, *choose* **All groups**.

51. *Leave* **Source attribute** as **Group ID**.

52. Optionally, use the filter group advance option to limit the scope of the search when there are many security group associations. For example, set Attribute to match as Display name, Match with as Contains, and then String as EloView. This will search security groups associated with the user that contain "EloView" in the name.

53. Under **Customize the name of the group claim**, for the **Name** field type in the value **roles**. This should be lowercase. Leave the **Namespace** field blank and the two **checkboxes** unchecked. *Click* **Save** when finished.



54. Use the **Test single sign-on with "EloView"** to verify the configuration. You can also download the SAML response to inspect the XML for the presence of the security group Object ID.

55. *Log into* **EloView**, then *go to* **Accounts, Manage Users, Users** tab. Verify user has been assigned the correct role.

56. *Go back* to your **"EloView" enterprise application** in the **Azure portal**, then *go to* **Users and groups**.

57. *Add in* your **security group**. Assigned users and groups will be able to access the EloView app from My Apps.

Configuring access roles by specifying a role for a claim in a SAML token.

58. *Log into* **Azure AD** or **Active Directory**.

59. *Designate* an **attribute property** under the **user account profile** to specify an **EloView access role**. For example, I can use the attribute EmployeeID for an Azure AD user or ExtensionAttribute1 for an Active Directory user to specify one of the following default system roles for the user: **Admin, Registered User**, or **Viewer**.

60. *Go to* your "**EloView" enterprise application**.

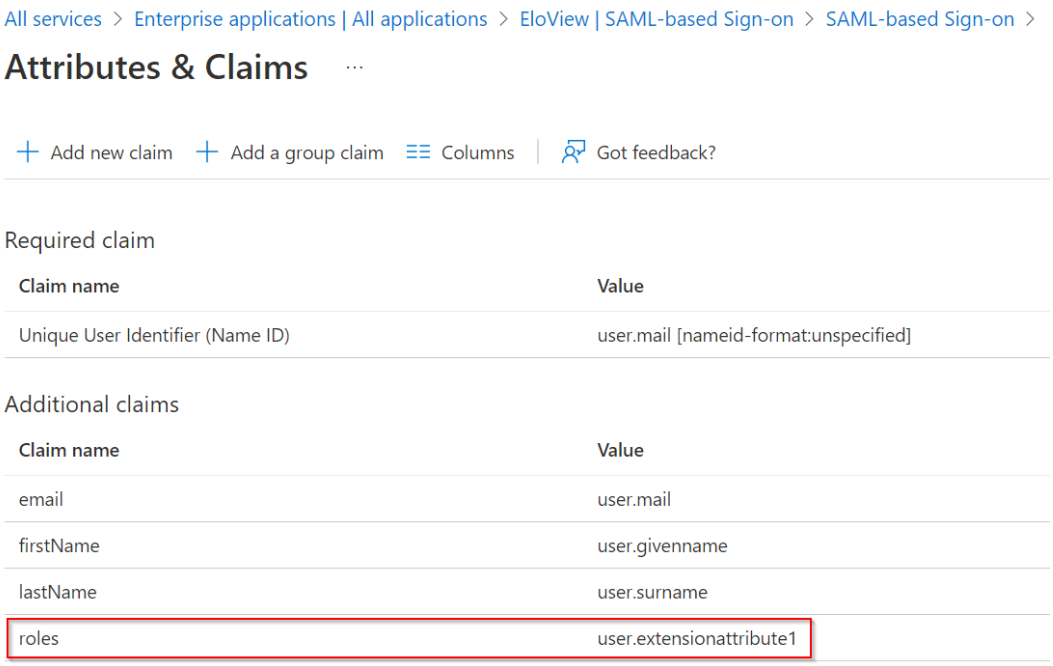
61. *Click* **single sign-on**, and then the **edit** button under **Attributes & Claims**.

62. *Click* **Add new claim**.

63. In the **Name field**, *type in* **roles**. This should be lowercase. Leave the **Namespace field** blank.

64. For the **Source**, *choose* **Attribute**.

65. For the **Source attribute**, *choose* **user.employeeid** or **user.extensionattribute1**. *Click* **Save** when done.



66. *Use* the **Test single sign-on with "EloView"** to verify the configuration. You can also download the SAML response to inspect the XML for the presence of the security group Object ID.

67. *Log into* **EloView**, then *go to* **Accounts, Manage Users, Users** tab. Verify user has been assigned the correct role.

Adding additional users to EloView

*If the user has an existing EloView account, you will need to set up an email alias.

68. *Create* a **new user** in **Azure AD** or **Active Directory** (if required).

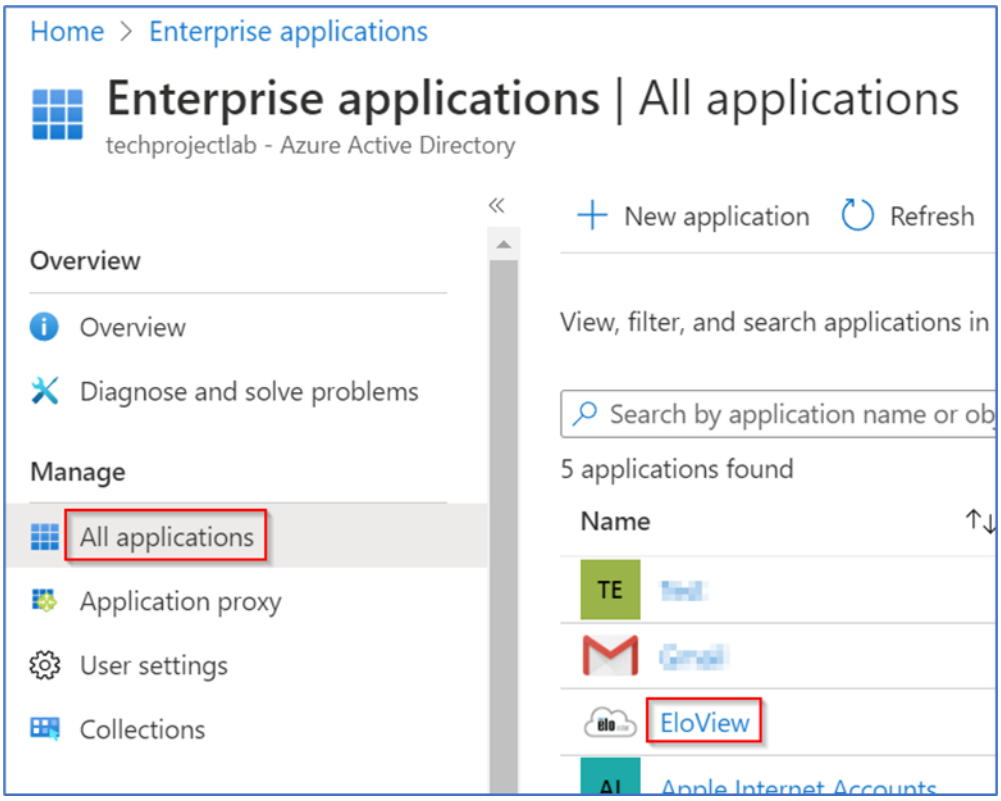
Note for Hybrid Azure AD
Create the user account in Active Directory then wait for Azure AD Connect (ADSync) to synchronize the user account to Azure AD.

69. *Sign into* your **Azure portal** (https://portal.azure.com) with an account with a Global Administrator role or privilege to create enterprise applications.

70. In the search bar, *type in* **Enterprise application**, and then *click* the **results Enterprise application**.

71. At the left navigation pane, *click* **All Applications** and then *click on* your **EloView enterprise application**.

72. At the left navigation pane, *click* **Users and group**. *Click* **Add user/group**, *click* **None selected**, *choose* **users**, *click* **Select**, and then **Assign**. After a few minutes, the recently added users will find the EloView enterprise application added to their Microsoft My App portal.


Home > Enterprise applications
Enterprise applications | All applications
techprojectlab - Azure Active Directory
New application
Refresh
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Collections
View, filter, and search applications in
Search by application name or ob
5 applications found
Name
TE
EloView

000003931