Microsoft Azure
Active Directory Integration

Table of Contents

This guide provides setup instructions for using LastPass Enterprise with Microsoft Azure Active Directory as your Identity Provider (IdP).

Summary

LastPass supports the following provisioning features:

- Create Users
- Update User Attributes
- Sync User Groups
- Deactivate or Disable Users

Completing only the SCIM Provisioning steps for Azure Active Directory (outlined in this guide) will still require the user to create and remember a separate Master Password to log in to LastPass, which is used to create the unique encryption key for their LastPass Vault.

LastPass Enterprise does support federated login with Azure Active Directory, which allows users to log into LastPass using their Azure Active Directory account. To set up federated login with Azure Active Directory, you must first complete the steps outlined in this SCIM integration guide, then additionally complete the steps outlined in the Set Up Federated Login for LastPass Enterprise Using Azure Active Directory article.

System Requirements

Syncing users from Azure AD to LastPass requires:

- An active Premium subscription to Microsoft Azure AD
- An active trial or paid LastPass Enterprise account
- An active LastPass Enterprise admin (required when activating your trial)

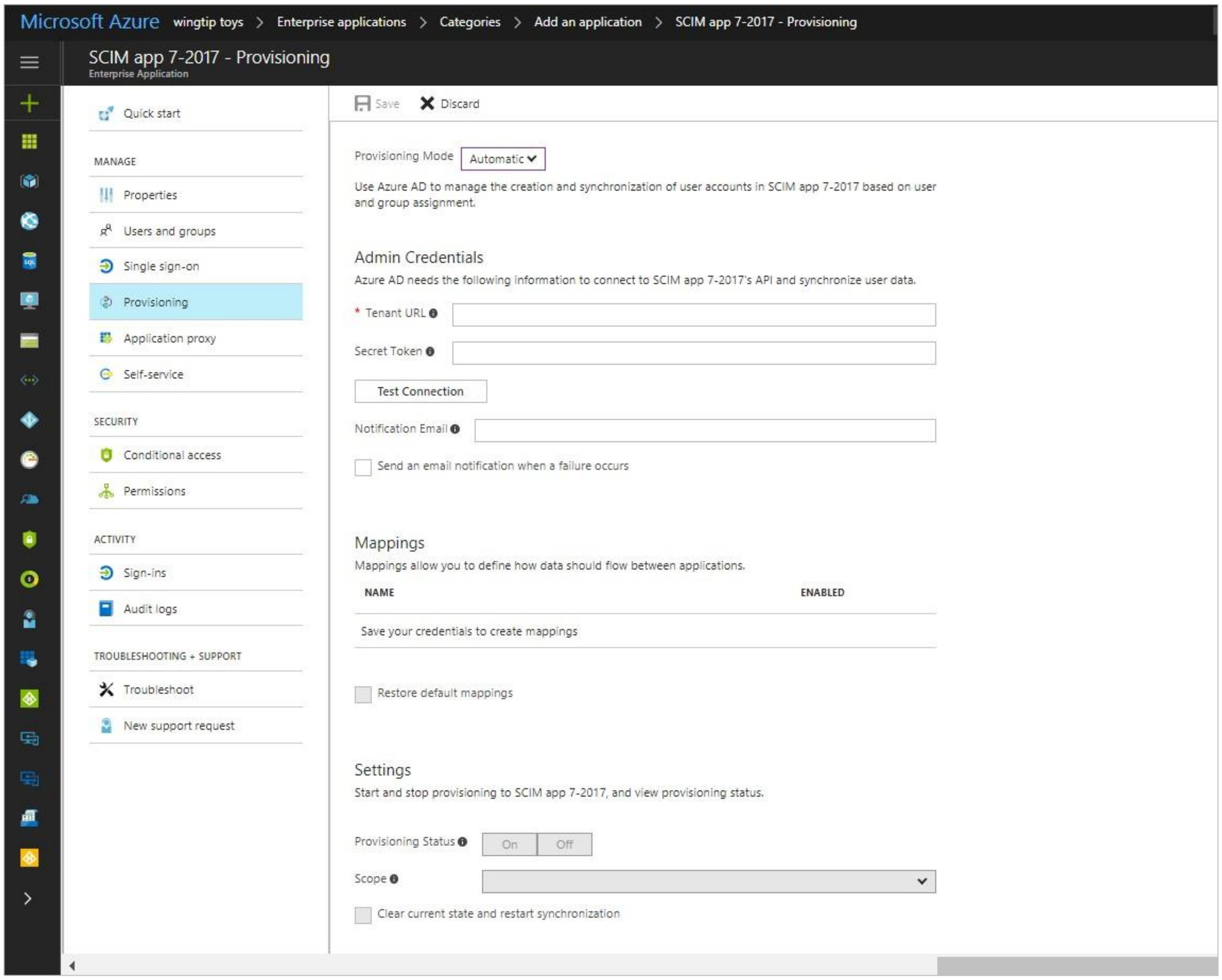
The LastPass Azure AD SCIM Provisioning does not require any software

installation.

Installation & Setup

To register and integrate your LastPass Enterprise Directory with your organization’s Azure AD:

1. Sign in to the Azure AD portal at https://portal.azure.com.
2. Go to **Azure Active Directory** > **Enterprise Applications** > **New application** > **All** > **Non-gallery application**.
3. Enter a name for your application and click **Add** to create an app object. The application object created is intended to represent the target app (for which you would be provisioning and setting up single sign-on, not just as the SCIM endpoint).
4. In the resulting screen, select **Provisioning** tab in the left column.
5. For Provisioning Mode, use the drop-down menu to select **Automatic**.



SCIM app 7-2017 - Provisioning
Enterprise Application

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM app 7-2017 based on user and group assignment.

Admin Credentials

Azure AD needs the following information to connect to SCIM app 7-2017's API and synchronize user data.

* Tenant URL

Secret Token

Notification Email

□ Send an email notification when a failure occurs

Mappings

Mappings allow you to define how data should flow between applications.

Save your credentials to create mappings

□ Restore default mappings

Settings

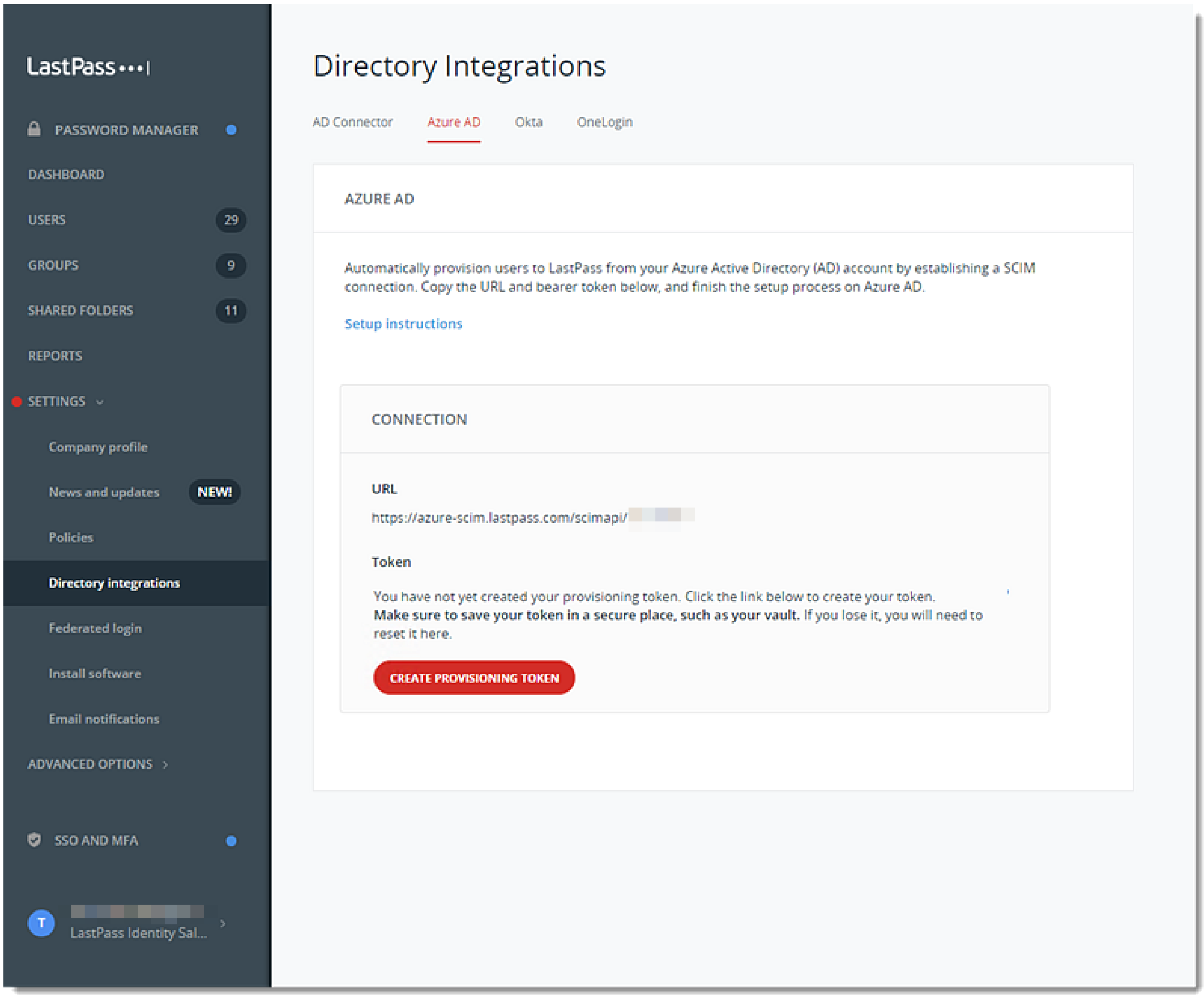
Start and stop provisioning to SCIM app 7-2017, and view provisioning status.

Provisioning Status

Scope

□ Clear current state and restart synchronization

6. In the Tenant URL field, enter the URL provided in the LastPass Enterprise Admin Console (go to **Settings** > **Directory Integrations** and select the **Azure AD** tab.



Directory Integrations

AZURE AD

Automatically provision users to LastPass from your Azure Active Directory (AD) account by establishing a SCIM connection. Copy the URL and bearer token below, and finish the setup process on Azure AD.

CONNECTION

URL

https://azure-scim.lastpass.com/scimapi/[redacted]

Token

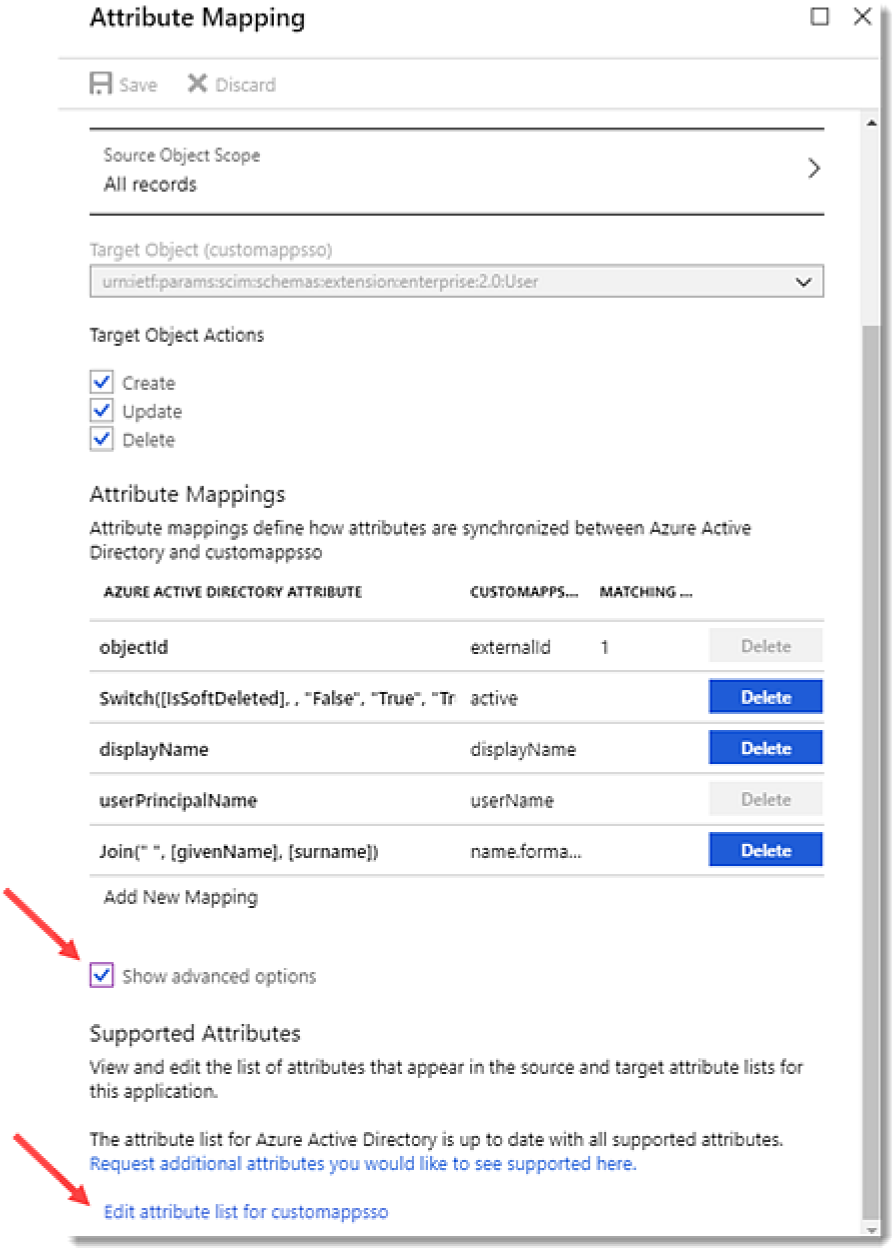
You have not yet created your provisioning token. Click the link below to create your token. **Make sure to save your token in a secure place, such as your vault.** If you lose it, you will need to reset it here.

[redacted]

7. The SCIM endpoint requires an OAuth bearer token from LastPass. In the LastPass Enterprise Admin Console, click **Create Provisioning Token**, then copy the provided token. In the Azure AD portal, paste the copied token into the Secret Token field.

   NOTE: *Once the admin navigates away from the Azure AD tab within the Directory Integrations page, the Provisioning Token will no longer be accessible through the Admin Console. If the Token is lost, a new one can be generated, but this will invalidate the previous code. Any process that used the old Token will need to be updated with the new one. A new Provisioning Token can be generated by navigating back to the Azure AD tab and clicking* ***Reset Provisioning Token****.*

8. Click **Test Connection** to have Azure Active Directory attempt to connect to the SCIM endpoint. If the attempts fail, error information is displayed.
9. If the connection test succeeds, click **Save** to save the admin credentials.
10. In Provisioning settings, select **Mappings**.
11. First, modify user object mappings:
    a) Check the box for **Show advanced options** at the bottom of Attribute Mapping.
    b) Click **Edit attribute list for ….**



Attribute Mapping

Source Object Scope
All records

Target Object (customappsso)
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Target Object Actions

☑ Create
☑ Update
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPS...	MATCHING ...	
objectId	externalId	1	Delete
Switch([IsSoftDeleted], , "False", "True", "Tr	active		Delete
displayName	displayName		Delete
userPrincipalName	userName		Delete
Join(" ", [givenName], [surname])	name.forma...		Delete

Add New Mapping

☑ Show advanced options

Supported Attributes

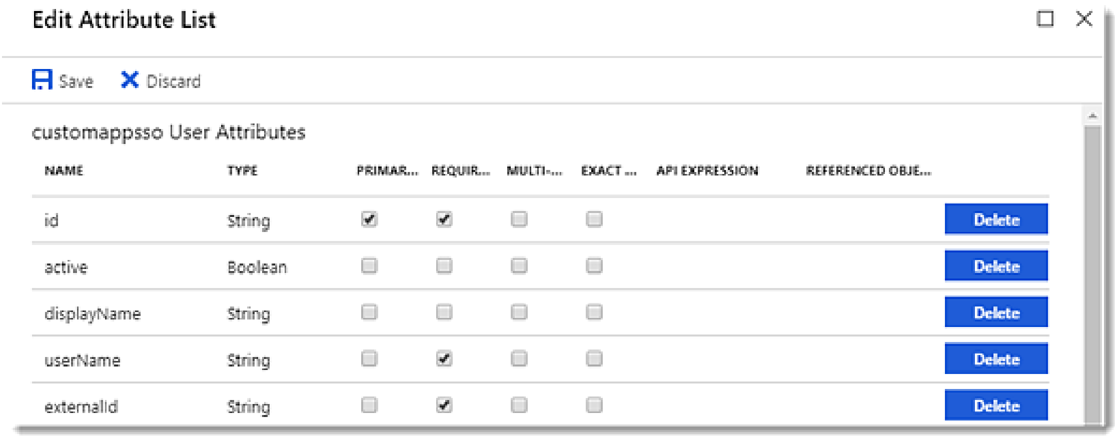
View and edit the list of attributes that appear in the source and target attribute lists for this application.

The attribute list for Azure Active Directory is up to date with all supported attributes. Request additional attributes you would like to see supported here.

Edit attribute list for customappsso

c) In the **Edit Attribute List**, make the following selections:
- Name = id, Type = String – Check the boxes for **Primary** and **Required**
- Name = userName, Type = String – Check the box for **Required**
- Name = externalID, Type = String – Check the box for **Required**

d) Click **Save** and return to Attribute Mapping.



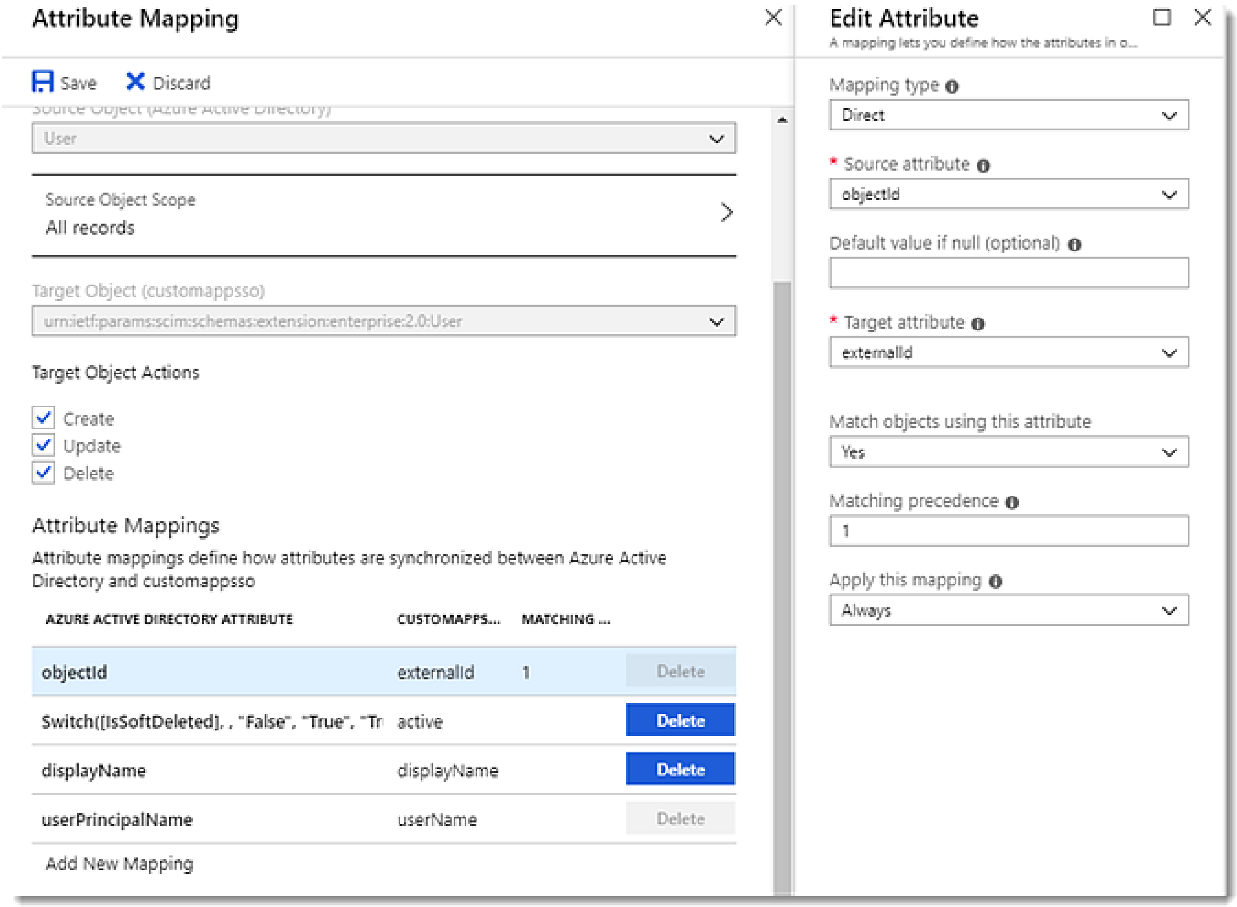
Edit Attribute List

Save Discard

customappsso User Attributes

NAME	TYPE	PRIMAR...	REQUIR...	MULTI-...	EXACT ...	API EXPRESSION	REFERENCED OBJE...	
id	String	☑	☑	☐	☐			Delete
active	Boolean	☐	☐	☐	☐			Delete
displayName	String	☐	☐	☐	☐			Delete
userName	String	☐	☑	☐	☐			Delete
externalId	String	☐	☑	☐	☐			Delete

12. Set 4 Attribute Mapping rules. By default, Azure may have created mappings already, but those can be modified or deleted if needed. Only the required 4 mappings should be present after editing, and must be configured correctly:
    a) **ExternalID** – Use the objectID attribute from Azure AD and set this as a matching attribute with Precedence set as **1**.
        - **TIP!** This should be the only mapping with any Precedence set. For any existing mapping you have set with a Precedence, set that mapping's Precedence to greater than 1, then create the ExternalID mapping outlined above and delete all unneeded mappings.
    b) **Active** – The default Azure AD mapping can be used, or a custom one which will be used to set the user as enabled/disabled in LastPass.
    c) **DisplayName** – Use any property from Azure AD. This should be a string which will be the synchronized user's name in LastPass.
    d) **UserName** – Map the user's email address from Azure AD. Please note that the userPrincipalName might not be equal to the email address. In this case, use an attribute from Azure AD which contains the email address the user will utilize and can read (e.g., Mail or in most cases, userPrincipalName should be fine).



Attribute Mapping

Save · Discard

Source Object (Azure Active Directory)

User

Source Object Scope
All records

Target Object (customappsso)

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Target Object Actions

☑ Create
☑ Update
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPS...	MATCHING ...	
objectId	externalId	1	Delete
Switch([IsSoftDeleted], , "False", "True", "Tr	active		Delete
displayName	displayName		Delete
userPrincipalName	userName		Delete

Add New Mapping

Edit Attribute

A mapping lets you define how the attributes in o...

Mapping type: Direct

* Source attribute: objectId

Default value if null (optional):

* Target attribute: externalId

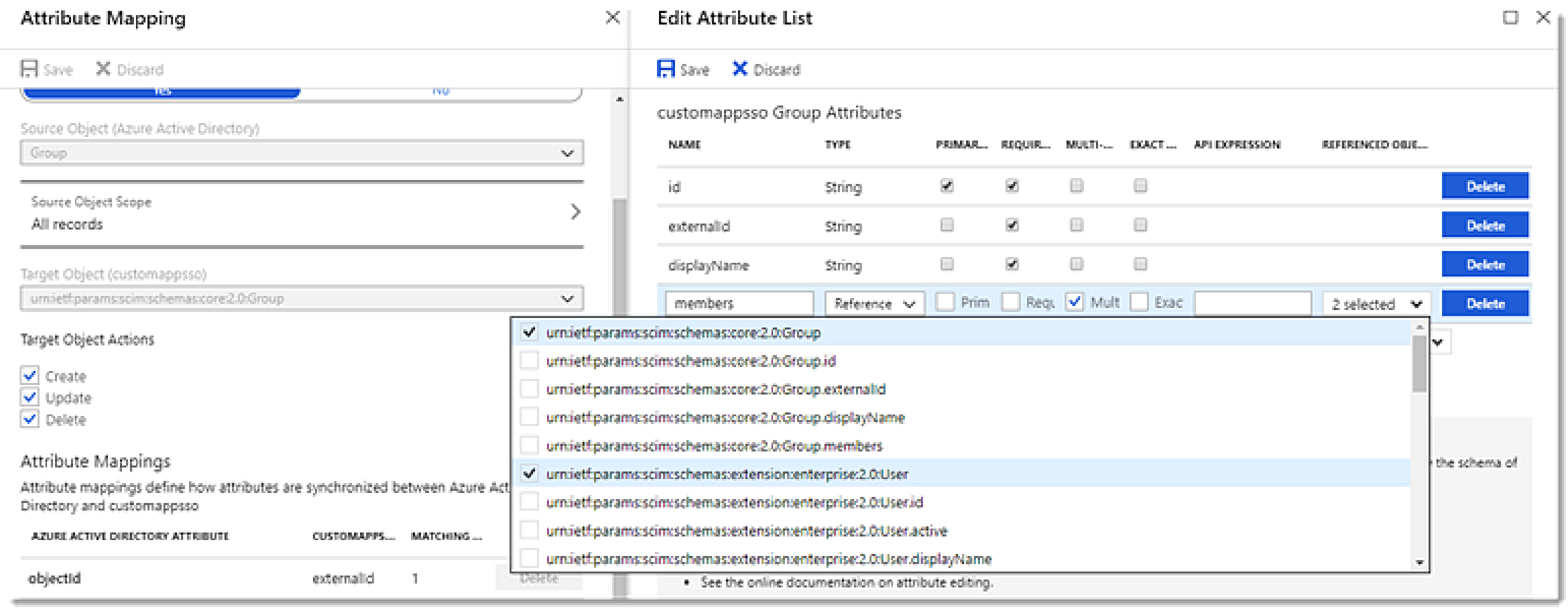
Match objects using this attribute: Yes

Matching precedence: 1

Apply this mapping: Always

13. Click **Save**, then return to the Provisioning settings and select **Mappings** (from **Step #10** above).
14. Next, modify group object mappings:
    a) Check the box for **Show advanced options** at the bottom of Attribute Mapping.
    b) Click **Edit attribute list for…**.
    c) In the Edit Attribute List, make the following selections:
       - Name = id, Type = String – Check the boxes for **Primary** and **Required**
       - Name = externalID, Type = String – Check the box for **Required**
       - Name **=** displayName, Type = String – Check the box for **Required**
       - Name **=** members, Type = Reference – Check the box for **Multi-Valued**, then set referenced objects for:
         - **urn:ietf:params:scim:schemas:core:2.0:Group**
         - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User**

    d) Click **Save** and return to Attribute Mapping.



Attribute Mapping

Save Discard

Source Object (Azure Active Directory)

Group

Source Object Scope
All records

Target Object (customappsso)

urn:ietf:params:scim:schemas:core:2.0:Group

Target Object Actions

☑ Create
☑ Update
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Act
Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPS...	MATCHING ...	
objectId	externalId	1	Delete

Edit Attribute List

Save Discard

customappsso Group Attributes

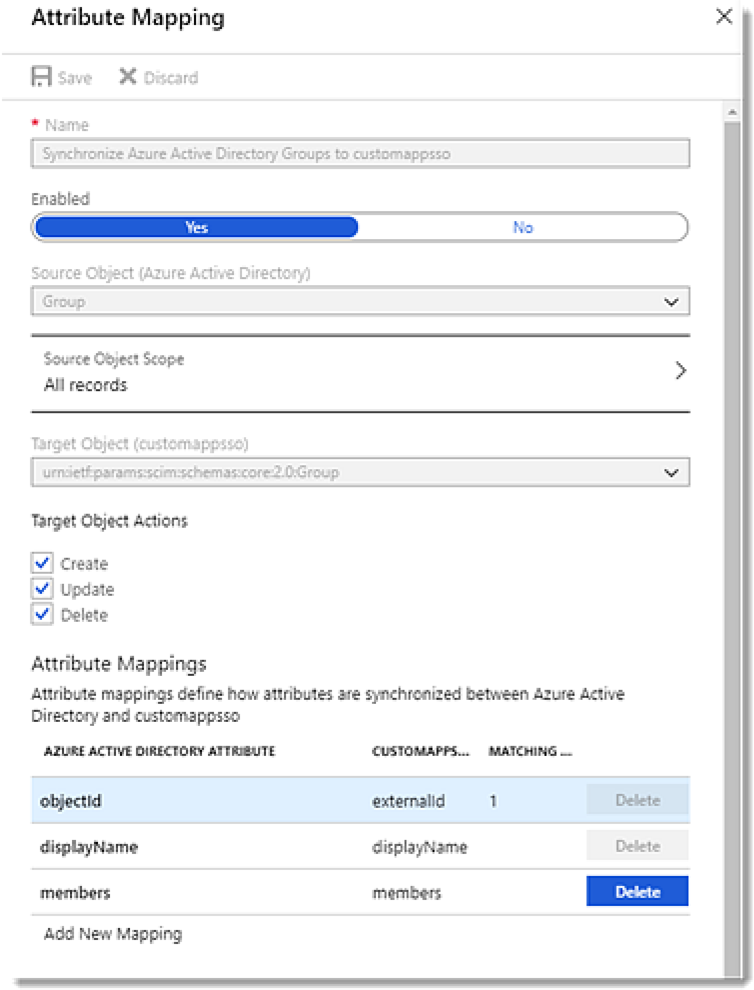
NAME	TYPE	PRIMAR...	REQUIR...	MULTI-...	EXACT ...	API EXPRESSION	REFERENCED OBJE...	
id	String	☑	☑	□	□			Delete
externalId	String	□	☑	□	□			Delete
displayName	String	□	☑	□	□			Delete
members	Reference	□ Prim	□ Req.	☑ Mult	□ Exac		2 selected	Delete

☑ urn:ietf:params:scim:schemas:core:2.0:Group
□ urn:ietf:params:scim:schemas:core:2.0:Group.id
□ urn:ietf:params:scim:schemas:core:2.0:Group.externalId
□ urn:ietf:params:scim:schemas:core:2.0:Group.displayName
□ urn:ietf:params:scim:schemas:core:2.0:Group.members
☑ urn:ietf:params:scim:schemas:extension:enterprise:2.0:User
□ urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.id
□ urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.active
□ urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.displayName

the schema of

- See the online documentation on attribute editing.

15. Set 3 Attribute Mapping rules, as follows:
    a) **ExternalID** – Use the objectID attribute from Azure AD and set this as a matching attribute with Precedence set as **1**. This should be the only mapping with any Precedence set.
    b) **DisplayName** – Use any attribute for group name.
    c) **Members** – User members from Azure AD.



Attribute Mapping

Save Discard

* Name

Synchronize Azure Active Directory Groups to customappsso

Enabled

Yes | No

Source Object (Azure Active Directory)

Group

Source Object Scope
All records

Target Object (customappsso)

urn:ietf:params:scim:schemas:core:2.0:Group

Target Object Actions

☑ Create
☑ Update
☑ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPS...	MATCHING ...	
objectId	externalId	1	Delete
displayName	displayName		Delete
members	members		Delete

Add New Mapping

16. Click **Save**, then return to the Provisioning settings.

17. Under Settings, the Scopefield defines which users and or groups are synchronized. Selecting **Sync only assigned users and groups** (recommended) will only sync users and groups assigned in the Users and groups tab.
18. Once your configuration is complete, enable the Provisioning Status by clicking **On**.
19. Click **Save** to start the Azure AD provisioning service.
20. If syncing only assigned users and groups (recommended), be sure to select the Users and groups tab and assign the users and/or groups you wish to sync.

Once the initial synchronization has started, you can use the Audit logs tab to monitor progress, which shows all actions performed by the provisioning service on your app. For more information on how to read the Azure AD provisioning logs, see Generate Enterprise Reports.

If you are interested in setting up federated login using Azure AD (to allow your users to log in to LastPass with their Azure Active Directory account), please see Set Up Federated Login for LastPass Enterprise using Azure Active Directory for next steps.

Contact Us

If you haven't started a trial, contact our team today at lastpass.com/contact-sales for more information.

For additional information, please see Set Up Azure Active Directory Integration. For further assistance, you can contact our support team by selecting a contact option at the bottom of the article.