SCIM Provisioning for LastPass Using Azure Active Directory

Table of Contents

Set Up SCIM Provisioning for LastPass Using Azure Active Directory 2

Summary 2

System Requirements 2

Before you begin 2

Step #1: Generate a Provisioning Token 3

Step #2: Configure Azure AD with LastPass 4

You’re all set! 9

Contact Us 9

Set Up SCIM Provisioning for LastPass Using Azure Active Directory

This guide provides setup instructions for using LastPass with Azure Active Directory (Azure AD) for your LastPass Enterprise or LastPass Identity account.

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 and LastPass Identity accounts do support federated login with Azure Active Directory, which allows users to log in to LastPass using their Azure Active Directory account (no separate Master Password required). To set up federated login with Azure Active Directory, please see Set Up Federated Login for LastPass Using Azure Active Directory article.

System Requirements

Syncing Azure Active Directory to LastPass requires the following:

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

The LastPass Azure AD SCIM endpoint for does not require any software installation.

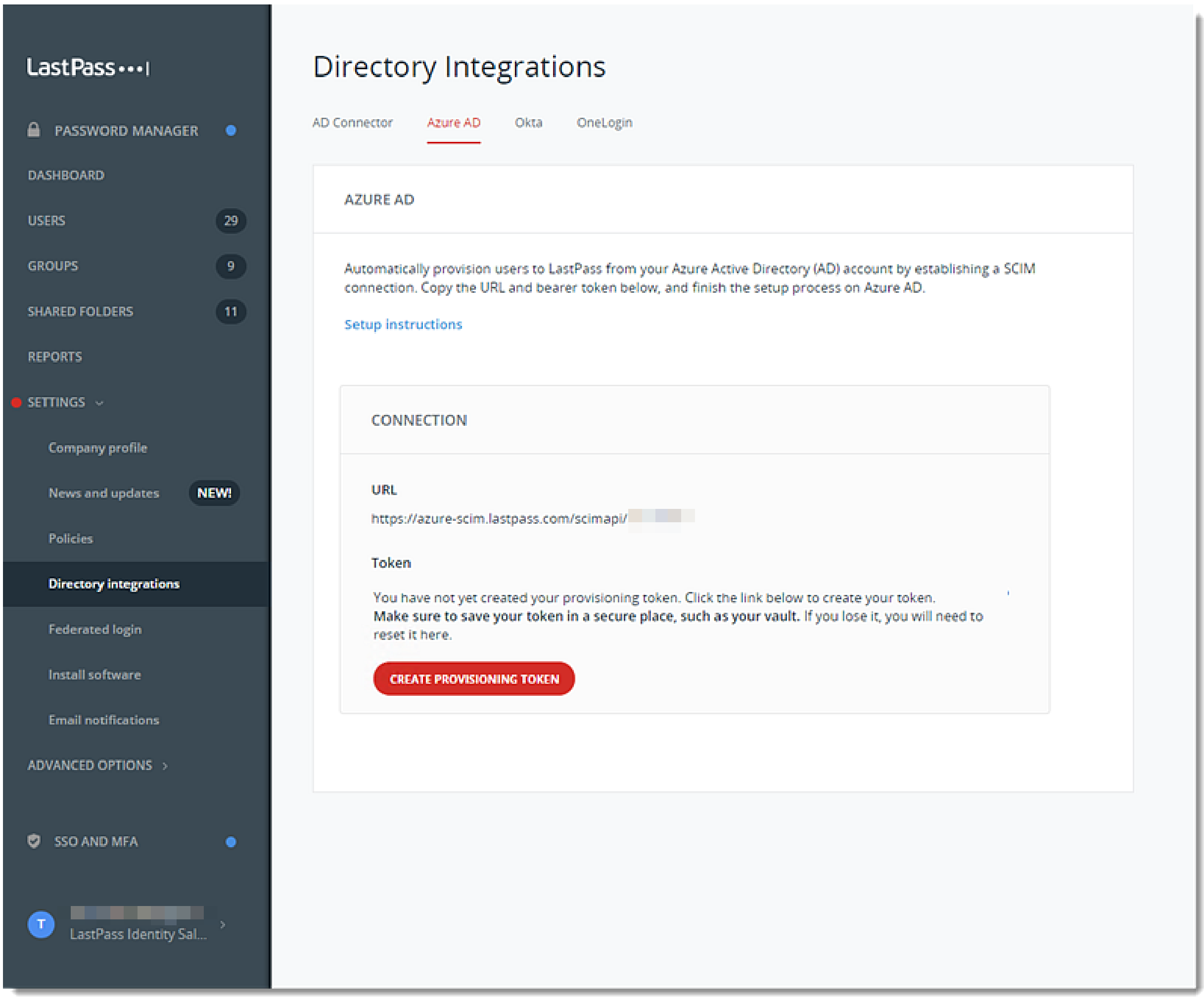
Before you begin

- It is helpful to open a text editor application so that you can copy and paste values that will be used between your LastPass Admin Console and the Azure AD Admin portal.

Step #1: Generate a Provisioning Token

1. Access the LastPass Admin Console by opening a web browser and navigating to one of the following:
   - Accounts using the US data centers: https://lastpass.com/company/#!/dashboard
   - Accounts using the EU data centers: https://lastpass.eu/?ac=1&lpnorefresh=1
2. Enter your administrator username and Master Password, then click **Log In**.
3. Select **Settings > Directory integrations** in the left navigation.
4. Click on the **Azure AD** tab.
5. Copy the URL and paste it into your text editor application.
6. Click the **Create Provisioning Token** to generate it, then copy the token and paste it into your text editor application.

   Note: *If you navigate away from the Azure AD tab within the Directory Integrations page, the Provisioning Token will no longer be accessible through the LastPass 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****.*



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

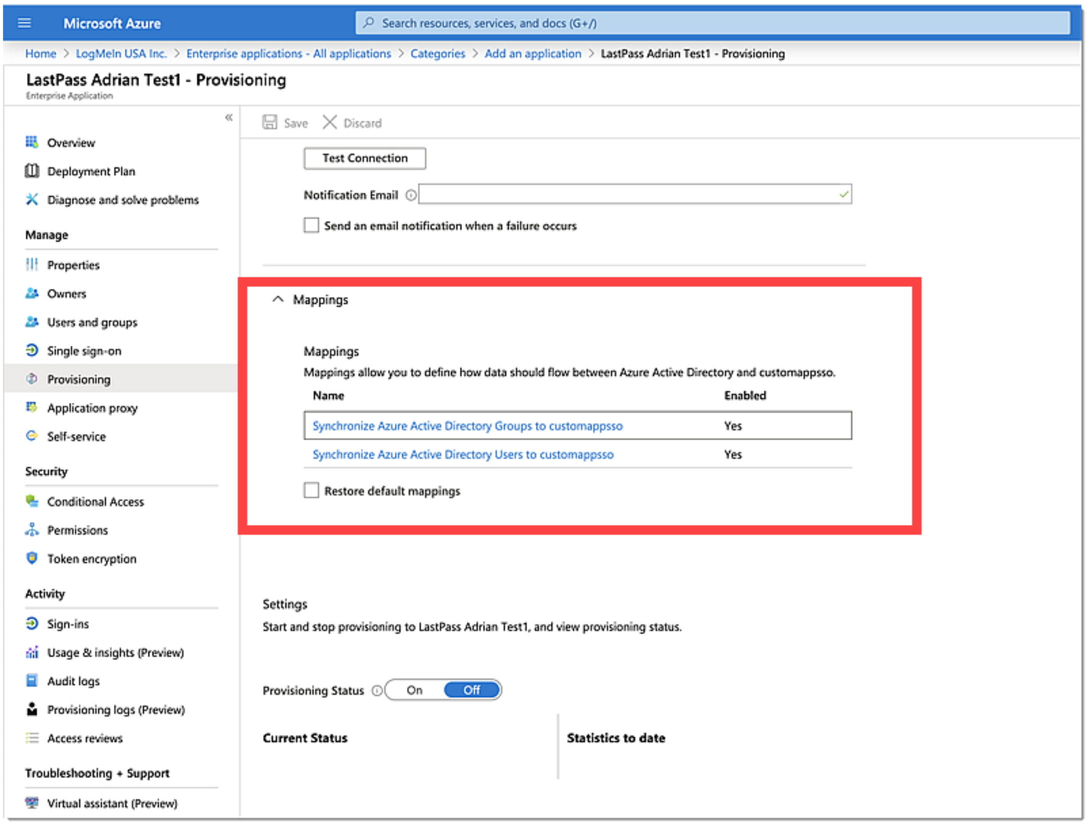
You have not yet created your provisioning token. Click the link below to create your token. **Make sure to save your token in a secure place, such as your vault.** If you lose it, you will need to reset it here.

[redacted]

Step #2: Configure Azure AD with LastPass

Once you have acquired the URL and Provisioning Token, you will need to enter them into the Azure AD Admin portal.

1. Log in to your Azure AD portal with your administrator account credentials at https://portal.azure.com.
2. Navigate to **Azure Active Directory** > **Enterprise Applications** > **New application** > **All** > **Non-gallery application**.
3. Enter a name for your application (LastPass) 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. Select the **Provisioning** tab in the left navigation.
5. For Provisioning Mode, use the drop-down menu and select **Automatic**.
6. Under Admin Credentials, enter the following:
    a. Locate the “Tenant URL” field and paste the **URL** you copied from the LastPass Admin Console.
    b. Locate the “Secret Token” field and paste the Provisioning **Token** you copied from the LastPass Admin Console.
7. Click **Test Connection** to have Azure AD attempt to connect to the SCIM endpoint. If the attempts fail, error information is displayed.
8. If the connection test succeeds, click **Save** to store the admin credentials.
9. Next, select **Mappings**.
10. Click **Synchronize Azure Active Directory Users to <app name>** to modify user object mappings.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > LogMeIn USA Inc. > Enterprise applications - All applications > Categories > Add an application > LastPass Adrian Test1 - Provisioning
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Troubleshooting + Support
Virtual assistant (Preview)
Save
Discard
Test Connection
Mappings
On
Off

LastPass Adrian Test1 - Provisioning
Enterprise Application

Notification Email

□ Send an email notification when a failure occurs

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Synchronize Azure Active Directory Groups to customappsso	Yes
Synchronize Azure Active Directory Users to customappsso	Yes

□ Restore default mappings

Settings

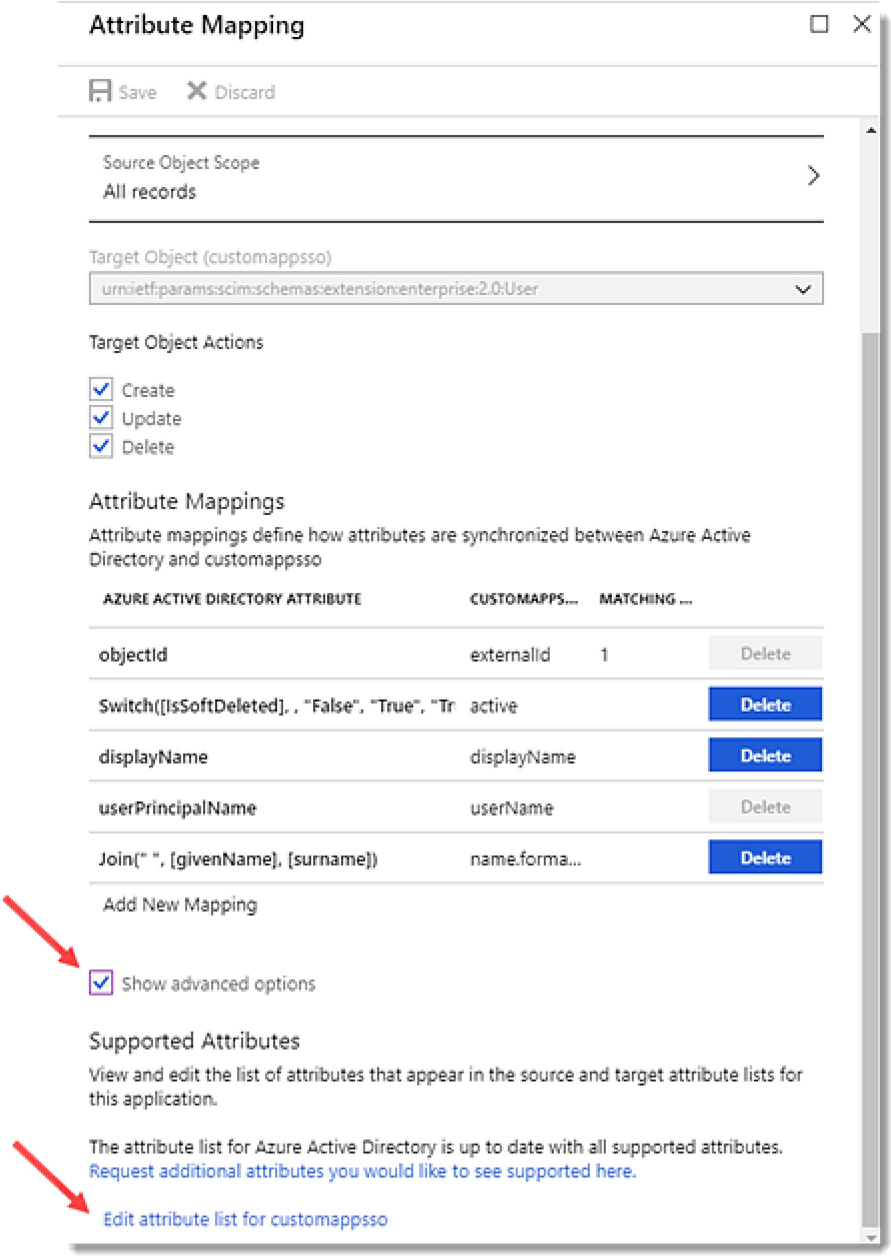
Start and stop provisioning to LastPass Adrian Test1, and view provisioning status.

Provisioning Status: On [✓ Off]

Current Status

Statistics to date

11. Modify the mappings with the following:
   a. Check the box for **Show advanced options** at the bottom of Attribute Mapping.
   b. Click **Edit attribute list for <app name>**



Attribute Mapping

Save Discard

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

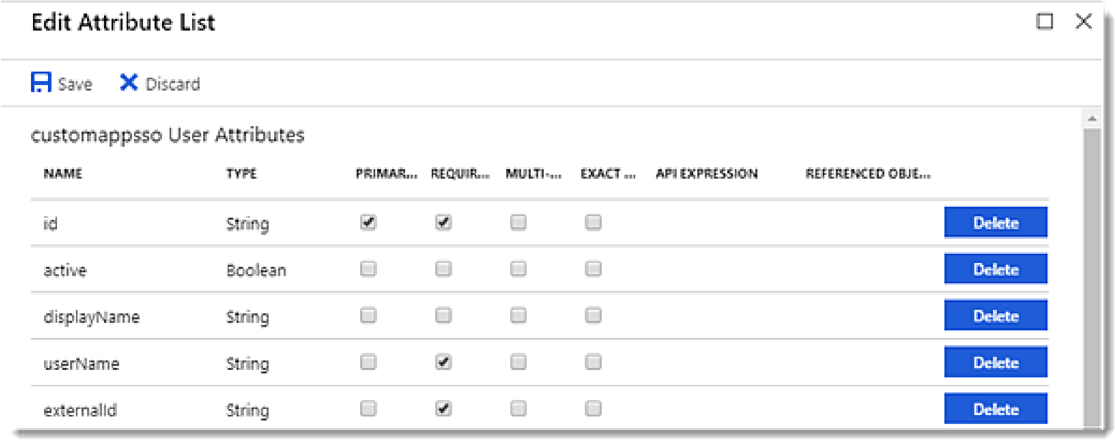
Supported Attributes

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.



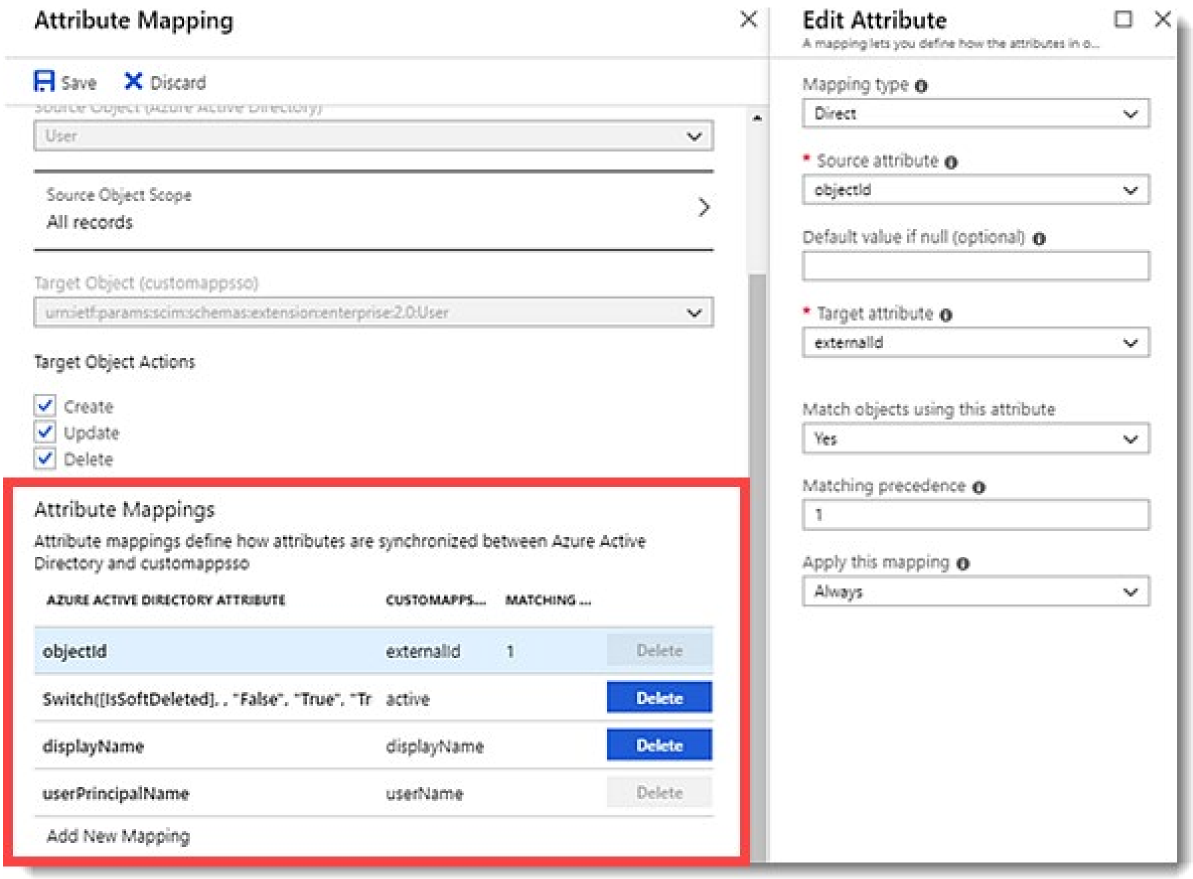
Edit Attribute List

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. Under the ”Attribute Mapping” section, 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. Delete all extra mappings except for the ones listed below, and make sure you edit them accordingly by clicking on each of them:
    a. **ExternalID** – Use the objectID attribute from Azure AD and set this as a matching attribute with Precedence set as **1**.
        - ***Note:*** *This should be the only mapping with any Precedence set. In order to change the ExternalID Precedence to 1, you may need to modify another attribute that might already have a Precedence set to 1.* ***After you find such attribute, you can change its precedence from 1 to 2, <u>then go back to ExternalID and set its Precedence to 1</u>.*** *Finally, to remove the Precedence entirely from the other attribute (now set to 2), you can now edit it once again and set the ”Match objects using this attribute” to* ***No****.*
    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).

       WARNING! If you already have users in LastPass, their email address **MUST** match the Azure AD attribute mapped to the userName value. **<u>If this is not mapped correctly, a duplicate user will be created for every existing user in LastPass.</u>**



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):

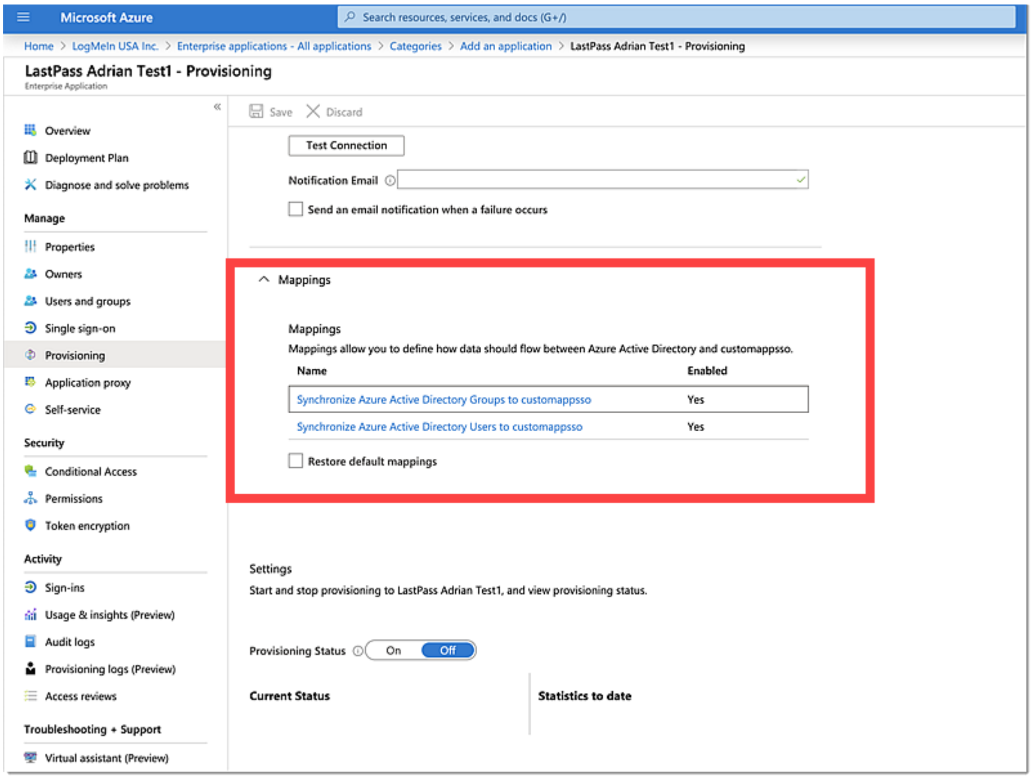
* Target attribute: externalId

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 #9** above).
14. Click **Synchronize Azure Active Directory Groups to <app name>** to modify group object mappings.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > LogMeIn USA Inc. > Enterprise applications - All applications > Categories > Add an application > LastPass Adrian Test1 - Provisioning
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Troubleshooting + Support
Virtual assistant (Preview)
Save
Discard
Test Connection

LastPass Adrian Test1 - Provisioning
Enterprise Application

Notification Email

□ Send an email notification when a failure occurs

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Synchronize Azure Active Directory Groups to customappsso	Yes
Synchronize Azure Active Directory Users to customappsso	Yes

□ Restore default mappings

Settings

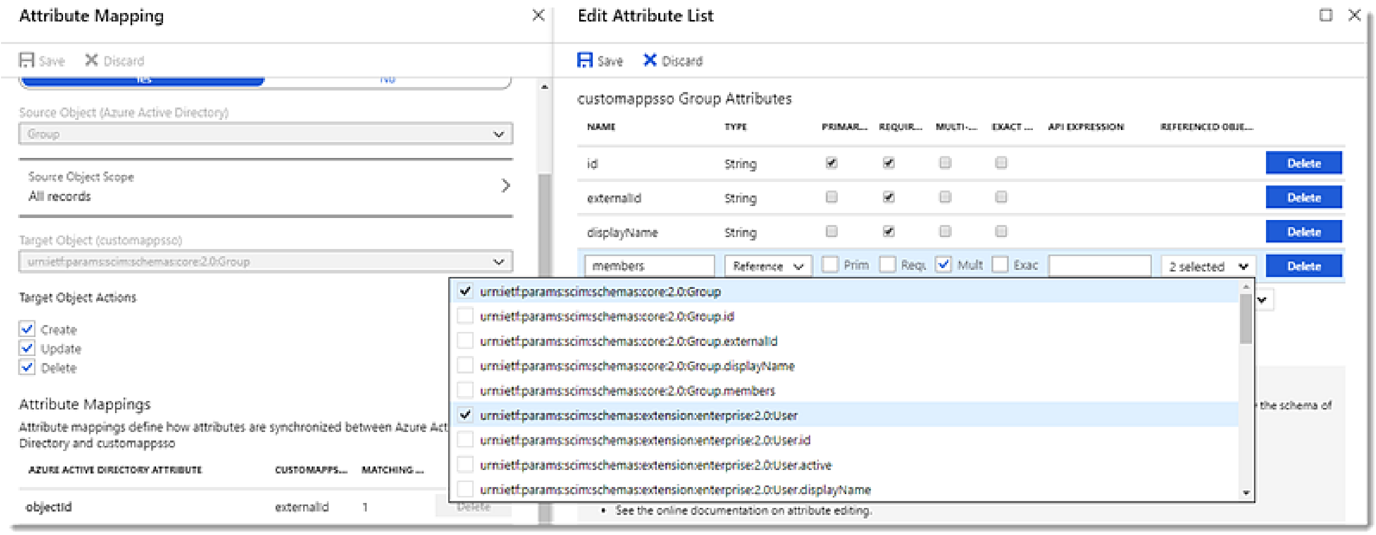
Start and stop provisioning to LastPass Adrian Test1, and view provisioning status.

Provisioning Status: On [✓ Off]

Current Status

Statistics to date

15. Modify the group mappings with the following:
    a. Check the box for **Show advanced options** at the bottom of Attribute Mapping.
    b. Click **Edit attribute list for <app name>**.
    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

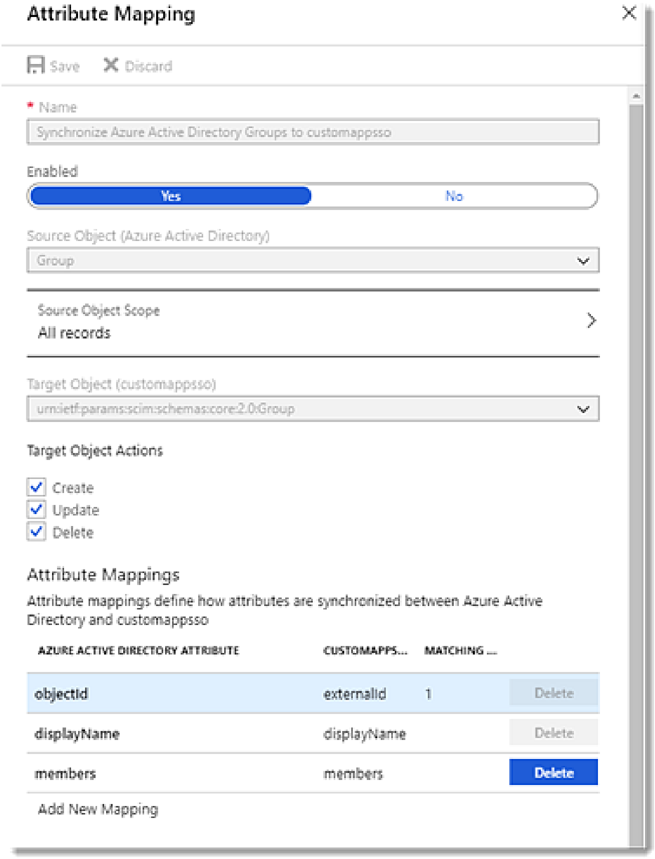
NAME	TYPE	PRIMAR...	REQUIR...	MULTI-...	EXACT ...	API EXPRESSION	REFERENCED OBJE...	
id	String	☑	☑	□	□			Delete
externalId	String	□	☑	□	□			Delete
displayName	String	□	☑	□	□			Delete
members	Reference	□ Prim	□ Req	☑ Mult	□ Exac		2 selected	Delete

☑ 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.

16. 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

17. Click **Save**, then return to the Provisioning settings.
18. 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.
    - **IMPORTANT:** *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.*
19. Once your configuration is complete, enable the Provisioning Status by clicking **On**.
20. Click **Save** to start the Azure AD provisioning service.

You're all set!

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.

Contact Us

If you have not started a LastPass Enterprise or LastPass Identity trial, please contact our Sales team 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.