## LastPass ••••

### **Table of Contents**

Set Up Federated Login 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
Step #3: Capture the Application ID and OpenID Connect from Azure AD 1	0
Step #4: Configure Federated login settings in LastPass	.1
Step #5: Configure a Redirect URI in Azure AD 1	.2
Step #6: Configure API permissions in Azure AD1	.3
Step #7: Add users to the LastPass app in Azure AD	.5
Step #8: Set up Multifactor Authentication on Azure AD (optional)	.5
You're all set!	.6
Troubleshooting & Tips1	.6
Contact Us 1	.6

# Set Up Federated Login 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

Federated login for LastPass Enterprise and LastPass Identity accounts allows users to log in to LastPass using their Azure AD account (instead of a username and separate Master Password) to access their LastPass Vault.

### **System Requirements**

The enable federated login for LastPass using Azure AD, the following is required:

- 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 federated login does not require any software installation.

### Before you begin...

- It is <u>required</u> that you <u>enable the "Permit super admins to reset Master</u> <u>Passwords" policy</u> for at least 1 LastPass admin (who is also a non-federated admin) in the LastPass Admin Console. This ensures that all LastPass user accounts can still be recovered (via Master Password reset) if a critical setting is misconfigured or changed for federated login after setup is complete.
- 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 either of the following:
  - For accounts using US data centers: <u>https://lastpass.com/company/#!/dashboard</u>
  - For accounts using EU data centers: <u>https://lastpass.eu/company/#!/dashboard</u>
- 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. Under Connection, 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.

**Important:** 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**.

LastPass ••••	Directory Integrations
PASSWORD MANAGER	AD Connector Azure AD Okta OneLogin
DASHBOARD	
USERS 29	
GROUPS 9	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.
SHARED FOLDERS 11	Setup instructions
REPORTS	
🐞 SETTINGS 🕹	CONNECTION
Company profile	
News and updates NEW!	URL
Policies	nttps://azure-scim.iastpass.com/scimap/
Directory integrations	Token You have not yet created your provisioning token. Click the link below to create your token.
Federated login	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.
Install software	CREATE PROVISIONING TOKEN
Email notifications	
ADVANCED OPTIONS >	
SSO AND MFA O	
■ LastPass Identity Sal >	

LastPass ••••

### 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 <a href="https://portal.azure.com">https://portal.azure.com</a>.
- 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.

Home > LogMeIn USA Inc. > Enterprise a	Home > LogMeIn USA Inc. > Enterprise applications - All applications > Categories > Add an application > LastPass Adrian Test1 - Provisioning					
LastPass Adrian Test1 - Provisi	oning					
Oreniew     Deployment Plan     Diagnose and solve problems     Manage     III Properties	Save       > Discard         Test Connection					
<ul> <li>Owners</li> <li>Users and groups</li> <li>Single sign-on</li> <li>Provisioning</li> <li>Application proxy</li> <li>Setf-service</li> <li>Security</li> <li>Conditional Access</li> </ul>	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					
♣       Permissions         ♥       Token encryption         Activity       ●         ●       Sign-ins         mi       Usage & insights (Preview)         ■       Audit logs         ▲       Provisioning logs (Preview)         ■       Access reviews         Troubleshooting + Support         ❤       Virtual assistant (Preview)	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 User 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)				
urnietf:params:scim:schemas:extension:enter	rprise:2.0:User		~	
Target Object Actions				÷.
<ul> <li>✓ Create</li> <li>✓ Update</li> <li>✓ Delete</li> </ul>				1
Attribute Mappings Attribute mappings define how attributes a Directory and customappsso	are synchronized be	etween Azure A	Active	1
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 app this application.	ear in the source a	nd target attrib	oute lists for	
The attribute list for Azure Active Directory Request additional attributes you would like	is up to date with to see supported	all supported a here.	ttributes.	
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 Lis	t								×
🔒 Save 🗙 Discard									
customappsso Use	r Attributes								Â
NAME	TYPE	PRIMAR	REQUIR	MULTI	EXACT	APTEXPRESSION	REFERENCED OBJE		
id	String							Delete	
active	Boolean							Delete	
displayName	String							Delete	
userName	String		۲					Delete	
externalid	String		۲					Delete	

12. Under the "Attribute Mapping" section, Azure may have created mappings already, but those can be modified and/or deleted.

**Important:** Only the required 4 mappings should be present after editing, and must be configured correctly. You **MUST** delete all extra mappings except for the ones listed below, otherwise you will encounter synchronization issues.

- 13. Modify the User Attributes as follows:
  - 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, then go back to ExternalID and set its Precedence to 1. 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).

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

Attribute Mapping ×	Edit Attribute
🕂 Save 🗙 Discard	Mapping type o
Source object (Azore Active Directory)	, Direct 🗸
User	Source attribute o
Source Object Scope	objectId V
All records	Default value if null (optional) O
Target Object (customappsso)	
umietf:params:scim:schemas:extension:enterprise:2.0:User	* Target attribute o
Target Object Actions	externalid 🗸
✓ Create	Match objects using this attribute
✓ Update	Yes 🗸 🗸
V Delete	Matching precedence o
Attribute Mappings	1
Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso	Apply this mapping <b>O</b>
	Always
ALONE ACTIVE DIRECTORY AT REDOLE COSTONARYS INFICUITO	
objectid externalid 1 Delete	
Switch([IsSoftDeleted], , "False", "True", "Tr_active Delete	
displayName displayName Delete	
userPrincipalName userName Delete	
Add New Mapping	

- 14. Click Save, then return to the Provisioning settings and select Mappings (from Step #9 above).
  15. 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							
LastPass Adrian Test1 - Provisi Enterprise Application	LastPass Adrian Test1 - Provisioning						
«	🗟 Save 🗙 Discard						
Overview	Tast Connection						
Deployment Plan	resconnector						
X Diagnose and solve problems	Notification Email 💿 🚽						
Manage	Send an email notification when a failure occurs						
Properties							
2 Owners	∧ Mappings						
Users and groups							
Single sign+on	Mappings						
Provisioning	Mappings allow you to define how data should flow between Azure Active Directory and customappsso.						
Application proxy	Name Enabled						
Self-service	Synchronize Azure Active Directory Groups to customappsso Yes						
Security	Synchronize Azure Active Directory Users to customappisso Yes						
Conditional Access	Restore default mappings						
🖧 Permissions							
Token encryption							
Activity							
Sign-ins	Settings Start and stop provisioning to LastPass Adrian Test1, and view provisioning status.						
前 Usage & insights (Preview)	·· · · · · · · · · · · · · · · · · · ·						
Audit logs							
Provisioning logs (Preview)							
E Access reviews	Current Status Statistics to date						
Troubleshooting + Support							
Virtual assistant (Preview)							

LastPass ••••

#### 16. Next, modify group object mappings as follows:

- 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	×	Edit Attribute Lis	t						ΟX
🕂 Save 🗙 Discard		🖪 Save 🗙 Discard							
Source Object (Azure Active Directory) Group	~	customappsso Grou NAME	up Attributes TYPE PRIM	IMAR REQUIR	MULTI	DACT	API EXPRESSION	REFERENCED OBJE.	
Source Object Scope		id	String 🗹			8			Delete
All records		externalid	String 🗌						Delete
Target Object (customappsso)		displayName	String 📃						Delete
umietfparamsscimschemas.core:2.0:Group	~	members	Reference 🗸 🗌	) Prim 📃 Requ	Mult	Exac		2 selected 👻	Delete
Target Object Actions	✓ urnietf:parame	scimschemas.core:2.0:Gro	up					^	¥
✓ Create     ✓ Update     ✓ Delete	urnietf:paramo urnietf:paramo urnietf:paramo	iscimischemasicorei2.0:Gro iscimischemasicorei2.0:Gro iscimischemasicorei2.0:Gro	up.id up.externalid up.displayName						
Attribute Mappings	urnietfparam	scimschemas.core:2.0:Gro	up.members						the schema of
Attribute mappings define how attributes are synchronized between Azure Act Directory and customappisso	urniettparam	escimeschemastextensionen escimeschemastextensionen	terprise:2.0:User terprise:2.0:User.id						
AZURE ACTIVE DIRECTORY ATTRIBUTE CUSTOMAPPS MATCHING	urnietfparam	scimschemastextensionen	terprise:2.0:User.active						
objectid externalid 1	Delete	<ul> <li>See the online door</li> </ul>	terprise:2.0:User.display! cumentation on attribute e	/Name editing.				-	]

17. Under the "Attribute Mapping" section, Azure may have created mappings already, but those can be modified and/or deleted.

**Important:** Only the required 3 mappings should be present after editing, and must be configured correctly. You **MUST** delete all extra mappings except for the ones listed below, otherwise you will encounter synchronization issues.

18. Modify the Group Attribute Mapping rules as follows:

- a) **ExternallD** 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.

ttribute Mapping			
Save 🗙 Discard			
Name			
Synchronize Azure Active Directory Groups	s to customappsso		
nabled	_		
Yes		No	)
ource Object (Azure Active Directory)			
Group			~
Source Object Scope			>
All records			
irget Object (customappsso)			
urnietf:params:scim:schemas:core:2.0.Grou	ip.		~
Create Update Delete ttribute Mappings ttribute mappings define how attributes irectory and customappsso AZURE ACTIVE DIRECTORY ATTRIBUTE	s are synchronized b CUSTOMAPPS	etween Azure .	Active
objectId	externalid	1	Delete
displayName	displayName		Delete
displayName nembers	displayName members		Delete Delete

- 19. Click **Save**, then return to the Provisioning settings.
- 20. 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/or groups assigned in the Users and groups tab.
  - **Note:** 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.
- 21. Once your configuration is complete, enable the Provisioning Status by clicking **On**.
- 22. Click **Save** to start the Azure AD provisioning service.

### Step #3: Capture the Application ID and OpenID Connect from Azure AD

- 1. In the Azure AD portal, navigate to your directory.
- 2. Select **App registrations** in the left navigation, then select **the name of your app**. You will then be redirected to the **Overview** page.
- 3. With **Overview** selected in the left navigation, copy the *Application* (*client*) *ID* field contents and paste it into your open text editor.
- 4. Click **Endpoints** in the top navigation to expand the menu on the right.
- 5. Copy *OpenID Connect metadata document* field contents and paste it into your open text editor.
- 6. Proceed to the next step below where these items will be used.

Microsoft Azure	,P Search resources, services, and docs (G+/)	E & O O O O O O O O O O O O O O O O O O
Home > App registr.	ations > UPEUA1	Endpoints ×
LP EU A1		
🖉 Search (Cind+/)	Delete     Delete     Delete	OAuth 2.8 authorization endpoint (v2)
Cvenview	Got a second? We would love your feedback on Microsoft identity platform:	OAuth 2.0 token endpoint (v2)
Guidstart	Display name 3 LP EU A1	0
Manage	Application (clent) ID :	OAuth 2.8 authorization endpoint (vf)
E Branding	Otard D 1	6
Authentication		OAuth 2.8 token endpoint (vf)
† Certificates & secrets	Welcome to the new and incomved Ace resisturions. Looking to learn hose	Parallel Faces of matching designed
11 Token configuration (preview)	•	https://togin.microsoftonine.com/
<ul> <li>API permissions</li> </ul>	Call APIs	Microsoft Graph All endpoint
👄 Expose an API		https://graph.microsoft.com
K Owners		Federation metadata document
Roles and administrators (Previ		6
Manifest		WS-Federation sign-on endpoint
Support - Troubleshooting	Build more powerful apps with rich user and business data from Microsoft services and your own company's data	0
P Troubleshooting	SOURCES.	SAML P sign-on endpoint
New support request	View API permissions	0
		SAML P sign-out endpoint
	Sign in users in 5 minutes	6
	866661+6114	

### **Step #4: Configure Federated login settings in LastPass**

- 1. Go back to the LastPass Admin Console, then select **Settings** > **Federated login** in the left navigation.
- 2. Select the **Azure AD** tab, then enter the following:
  - In the "Directory (tenant) ID" field, paste the **OpenID Connect metadata document** from **Step #3** (in the previous section).
  - In the "Application (client) ID" field, paste the **Application (client) ID** from **Step #3** (in the previous section).
- 3. Check the box for **Enabled**.
- 4. Click Save Settings when finished.

ederated Login 🗉	
tive Directory Federated Services (ADFS) Azure AD Okta Federated Users	
Provision users to LastPass from your Azure Active Directory. They'll log in to LastPass with their AD credentials instead of their master password.	
Follow these instructions.	
CONFIGURE AZURE AD	
Complete this form using information from your Azure portal.	
OpenID Connect metadata document URL (ends with: .well-known/openid-configuration) https://login.microsoftonline.com/	
Application (client) ID	
Enabled	
SAVE SETTINGS	

### Step #5: Configure a Redirect URI in Azure AD

- 1. In the Azure AD portal, select **App Registrations**, then select your **<app name>**.
- 2. Click Authentication, then click Switch to the Old Experience.
- 3. Select **Overview** in the left navigation.
- 4. Under Redirect URI in the upper-right navigation, click Add a Redirect URI.
- 5. Add the first Redirect URI, as follows:
  - For the Type column, use the drop-down menu and select Web
  - For the Redirect URI column, enter either of the following:
    - i. For accounts using US data centers: https://lastpass.com/passwordreset.php
    - ii. For accounts using **EU data centers**: https://lastpass.eu/passwordreset.php
- 6. Add the second Redirect URI, as follows:
  - For the Type column, use the drop-down menu and select Web
  - For the Redirect URI column, enter <u>https://accounts.lastpass.com/federated/oidcredirect.html</u>
- 7. Under the Implicit Grant settings, check the boxes to enable the following settings:
  - Access tokens
  - ID tokens
- 8. Click **Save** when finished.



### Step #6: Configure API permissions in Azure AD

- 1. In the Azure AD portal, select **API permissions** in the left navigation.
- 2. Click the Add a permission button, then select Microsoft Graph.
- 3. In the right navigation, select **Delegated permissions**.
- 4. Under the Permission menu, check the boxes to enable the following permission settings:
  - email
  - openid
  - profile

E Microsoft Azure 🖉 Search	resources, services, and docs (G+/)		N 67 4 0
Microsoft Azure     Autores     Microsoft Azure     Acure     P EU A1 - API permissions     P EU A1 - API permission     P Search (Cmd+/)     «      Goverview     Quickstart Manage     Branding	resources, services, and docs (G+/)    Configured permissions  Applications are authorized to call APIs when they are g all the permissions the application needs, Learn more al  + Add a permission Grant admin conserv	Request API permissions Microsoft Graph https://graph.microsoft.com/ Docs C* What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user. Select permissions	Application permissions Your application runs as a signed-in user.
<ul> <li>Authentication</li> <li>Certificates &amp; secrets</li> <li>Token configuration (preview)</li> <li>API permissions</li> <li>Expose an API</li> <li>Owners</li> <li>Roles and administrators (Previ</li> <li>Manifest</li> <li>Support + Troubleshooting</li> <li>Youbleshooting</li> <li>New support request.</li> </ul>	API / Permissions name Type ✓Microsoft Graph (5) email Delega openid Delega User,Rea3 Delega User,Rea3 Delega	Type to search  Permission  email view users' email address  offine_access Maintain access to data you have given it access to  offine_access Maintain access to data you have given it access to  offine_access Maintain access to data you have given it access to  offine_access Maintain access to data you have given it access to  offine_access AccessReview > AdministrativeUnit > Agreement > Agreement > Analytics	bA I
		> AppCatalog > Application > AppRoleAssignment > ApprovalRequest > AuditIon Add permission Discard	

- 5. Under the User menu, check the boxes to enable the following user settings:
  - User.Read
  - User.ReadWrite
- 6. When finished, click **Add permissions**.

■ Microsoft Azure	resources, services, and docs (G+/)	
Home > LP EU A1 - API permissions		Request API permissions
LP EU A1 - API permission	s	Taxantan
O. Comb (Code A	C Refresh	> TeamsApp
> search (cmu+/) «	0	> Teamstab
Overview	Configured permissions	> inreatAssessment
Quickstart	Applications are authorized to c	all APIs when they are g
Manage	all the permissions the applicab	> Irust-rameworkkeyset
🗮 Branding	+ Add a permission	Grant admin consen > UserActivity
Authentication	API / Permissions name	> UserAuthenticationMethod Type
📍 Certificates & secrets	Microsoft Graph (5)	> UserNotification
Token configuration (preview)	email	> UserTimelineActivity Delega
<ul> <li>API permissions</li> </ul>	openid	V User (2) Delega
Expose an API	profile	Delega Export user's data ()
Owners	User Read	Delega User Invite All
Roles and administrators (Previ	User.ReadWrite	Delega
Manifest		Manage user identities O
Support + Troubleshooting		User.Read Sign in and read user profile ①
7 Troubleshooting New support request		User Read All Read all users' full profiles ①
		User.ReadBasic.All Read all users' basic profiles ③
		Viser.ReadWrite Read and write access to user profile ③
		User.ReadWrite.All Read and write all users' full profiles ③
		> WorkforceIntegration
		Add permissions Discard

7. Under Configured Permissions, click **Grant <your LastPass application name>** to finish configuring API permissions for your LastPass app.

-9	LP EU A1 - API permissions						
2	Search (Cmd+/) «	C Refresh					
K S Ma	Overview Quickstart nage	Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part configured permissions should include all the permissions the application needs. Learn more about					
	Branding	Grant admin consent for Logmein USA Inc.					
€	Authentication	API / Permissions na	Туре	Description	Admin Consent Req		
۲	Certificates & secrets	Microsoft Graph (5)					
H	Token configuration (preview)	email	Delegated	View users' email address			
٠	API permissions	openid	Delegated	Sign users in	-		
۵	Expose an API	profile	Delegated	View users' basic profile			
4	Owners	User.Read	Delegated	Sign in and read user pro	-		
2	Roles and administrators (Previ	User.ReadWrite	Delegated	Read and write access to	-		
Ð	Manifest						

### Step #7: Add users to the LastPass app in Azure AD

- 1. In the Azure AD portal, with your LastPass application selected, go to **Overview > Enterprise applications** in the left navigation.
- 2. Select your newly created LastPass application.
- 3. Select **Users and groups** in the left navigation.
- 4. Click Add user.
- 5. Locate each of the users and/or groups in the list, then click **Select** to grant access to the LastPass app.

LP EU A1 - Users and grou	ips	nova 🦉 Undato Gradantials 🛛 🎫 Columns		
Overview     Deployment Plan	Add user     Edit     Remove     Dydate Credentials     ==     Columns     The application will appear on the Access Panel for assigned users. Set 'visible to users?'     First 100 shown, to search all users & groups, enter a display name.			
Manage	Display Name Object Type No application assignments found			
Owners     Users and groups				
<ul> <li>Single sign-on</li> <li>Provisioning</li> </ul>				
Application proxy     Self-service				
Security				

### Step #8: Set up Multifactor Authentication on Azure AD (optional)

If desired, you can <u>set up Multifactor Authentication at the Azure AD (Identity</u> <u>Provider) level</u>.

### You're all set!

You have successfully set up your LastPass Enterprise or LastPass Identity account to use federated login with your Azure Active Directory. All of your newly populated federated users will receive a Welcome email informing them that they can now log in to use LastPass. Please note that your LastPass users must log in using the LastPass web browser extension in order to use federated login for their Azure AD account with LastPass.

- To learn more about deploying the LastPass web browser extension to your organization, please see <u>Install LastPass Software Using the Admin Console</u>.
- To see your end users' experience, please see <u>Federated Login Experience for</u> <u>LastPass Users</u>.
- If your end users have linked personal accounts associated with their federated login account, please see <u>How do I verify my linked personal account?</u>
- To convert a non-federated user to a federated user, please see <u>How do</u> <u>I convert an existing LastPass user to a federated (Azure AD) user?</u>

### **Troubleshooting & Tips**

• It is <u>required</u> that you <u>enable the "Permit super admins to reset Master</u> <u>Passwords" policy</u> for at least 1 LastPass admin (who is also a non-federated admin) in the LastPass Admin Console. This ensures that all LastPass user accounts can still be recovered (via Master Password reset) if a critical setting is misconfigured or changed for federated login after setup is complete.

### **Contact Us**

If you have not started a LastPass Enterprise or LastPass Identity trial, please contact our Sales team at <u>lastpass.com/contact-sales</u> for more information.

For additional help, please see <u>Set Up Federated Login for LastPass Using Azure</u> <u>Active Directory</u>, and if desired, select a contact option at the bottom of the article.