Table of Contents

Set Up Federated Login for LastPass Using Okta SSO and Active Directory

This guide provides setup instructions for using LastPass with Okta SSO (single sign-on) as your Identity Provider (IdP) and Active Directory as your directory provider. This type of setup may be referred to as a "hybrid" configuration.

Summary

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

System Requirements

To enable federated login for LastPass using Okta, the following is required:

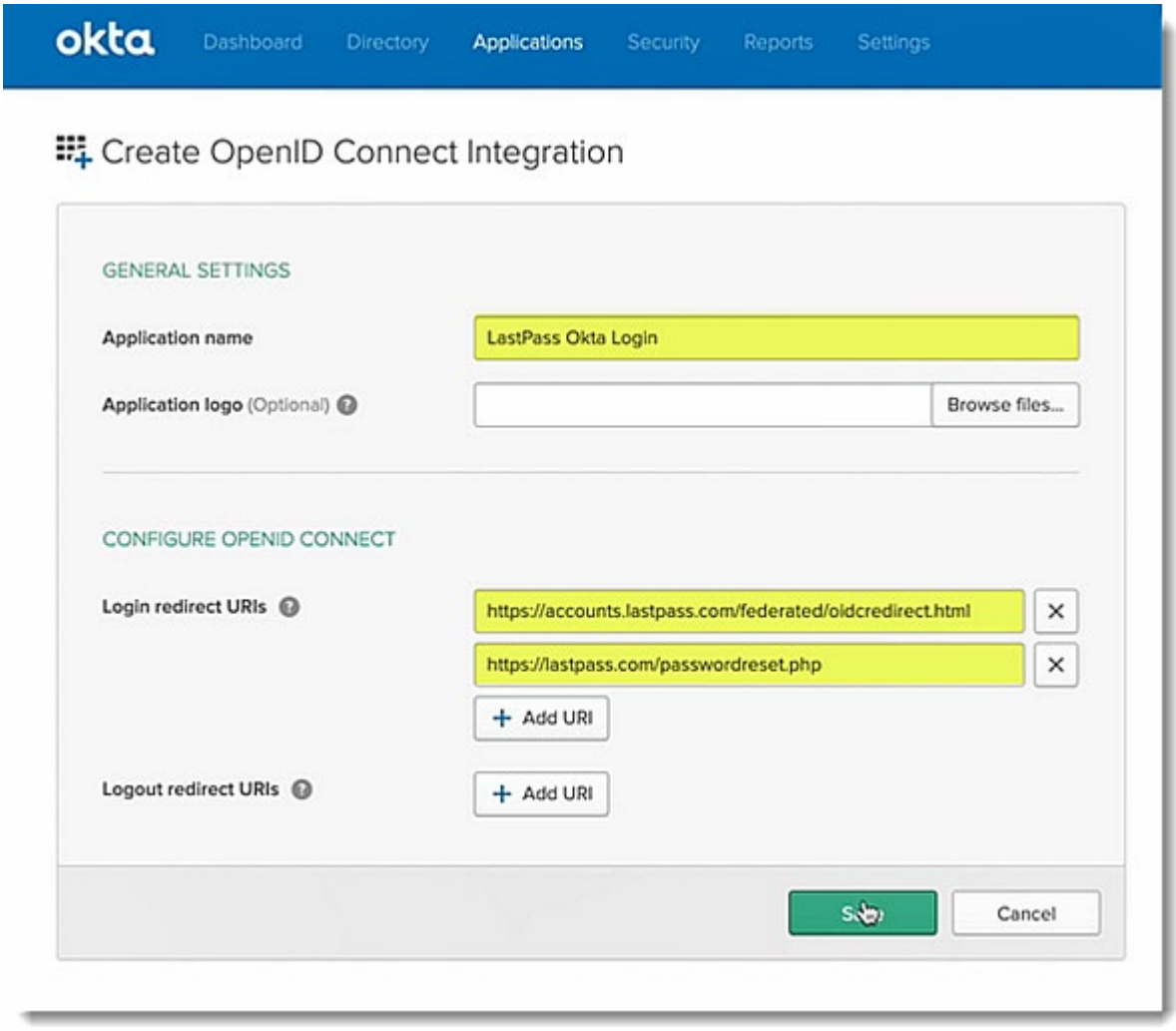
- You must be using **all** of the following:
  - Okta Single Sign-On
  - Active Directory
- An active trial or paid LastPass Enterprise or LastPass Identity account
- An active LastPass Enterprise or LastPass Identity admin (required when activating your trial or paid account)

Before you begin

- It is **required** that you enable the "Permit super admins to reset Master Passwords" policy 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 Okta Admin portal.

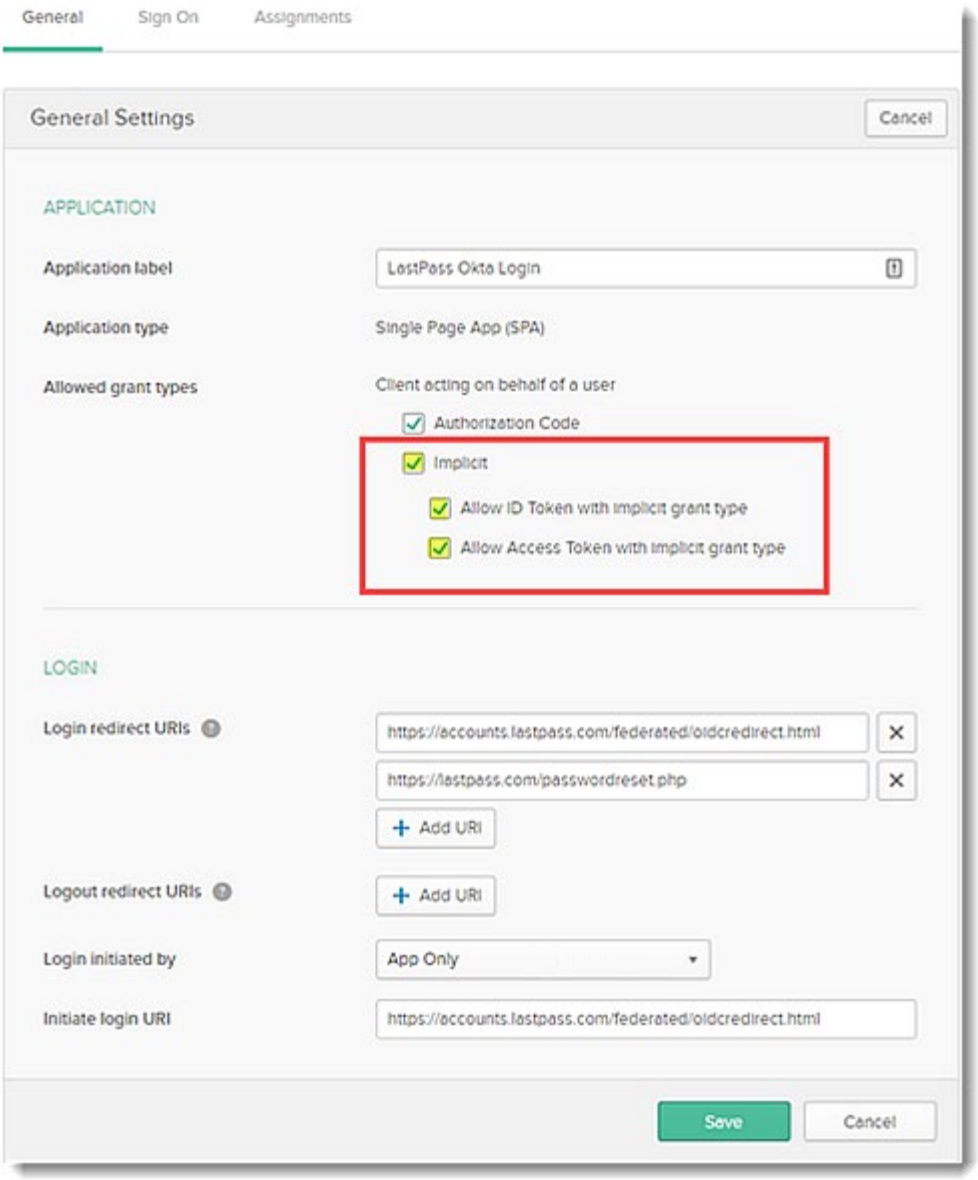
Step #1: Create a Single Page Application to Enable Login with Okta

1. Log in to your Okta Admin portal with your administrator account credentials.
2. Under **Applications** on the main toolbar, click **Applications**.
3. Click **Add Application** in the upper-left navigation.
4. Click **Create New App** in the upper-left navigation.
5. Under the "Platform" section, use the drop-down menu to select **Single Page App (SPA)**.
6. Click **Create.**
7. Under General Settings, enter the following information:
    - **Application name:** LastPass Okta Login
8. Under Configure OpenID Connect, add the following Redirect URIs:
    - https://accounts.lastpass.com/federated/oidcredirect.html
    - https://lastpass.com/passwordreset.php
    - For accounts using EU data centers only, also add: https://lastpass.eu/passwordreset.php
9. Click **Save** when finished.



Step #2: Enable the Implicit Grant Type for ID and Access Tokens

1. On the LastPass Okta Login application page, click the **General** tab.
2. Under "Allowed grant types" confirm that the following checkboxes are enabled:
    - **Implicit**
        - **Allow ID Token with implicit grant type**
        - **Allow Access Token with implicit grant type**
3. If the checkboxes are not enabled already, click **Edit**, then check the boxes to enable all 3 settings and click **Save**.



Step #3: Add a Company-Wide Key as a Group Claim

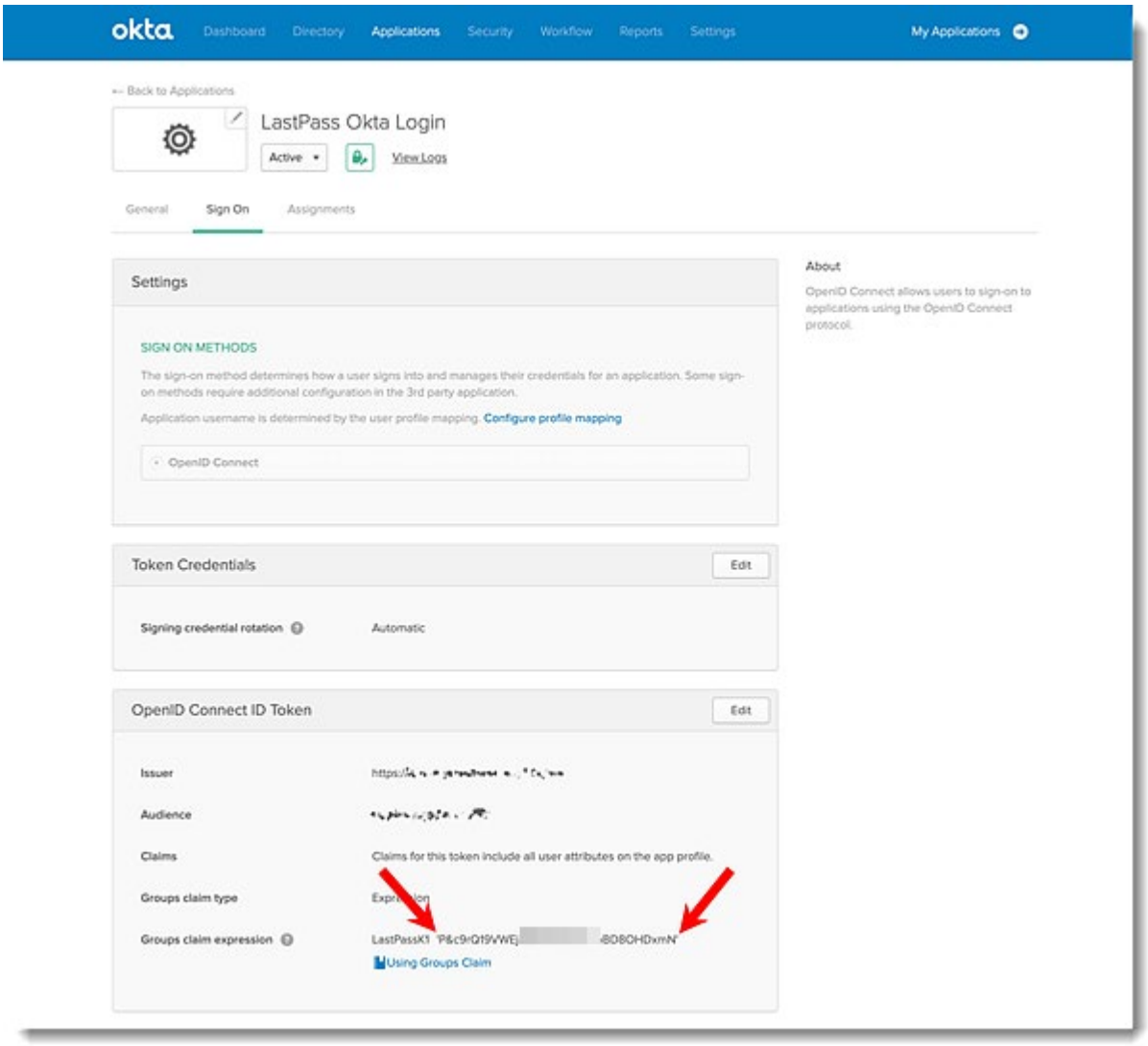
1. Under the newly created Application, click **Sign On** tab.
2. In the **OpenID Connect ID Token** section click **Edit**.
3. In the **Groups claim type** dropdown select **Expression**
4. For the **Claim name** field, enter **LastPassK1**.
5. Access the LastPass Admin Console by navigating to either of the following:
    - For accounts using US data centers: https://lastpass.com/company/#!/dashboard
    - For accounts using EU data centers: https://lastpass.eu/company/#!/dashboard
6. Log in with your LastPass admin username and Master Password.
7. Click **Settings** in the left navigation, then select **Federated login**.
8. Click the **Okta** tab.
9. Copy the Random Company-Wide Key (or click the hyperlink to generate a new one).
10. Once you have copied your Random Company-Wide Key, paste it into your text editor application.
11. Return to Okta and within the "OpenID Connect ID Token" section, paste the **Random Company-Wide Key** into the **Group claim expression** field between single quotes that you must add on each side of the key (e.g., 'r4nd0mk3y').
12. Click **Save** when finished.

WARNING!

It is of critical importance that you do not change the Random Company-Wide Key once it has been saved in Okta.

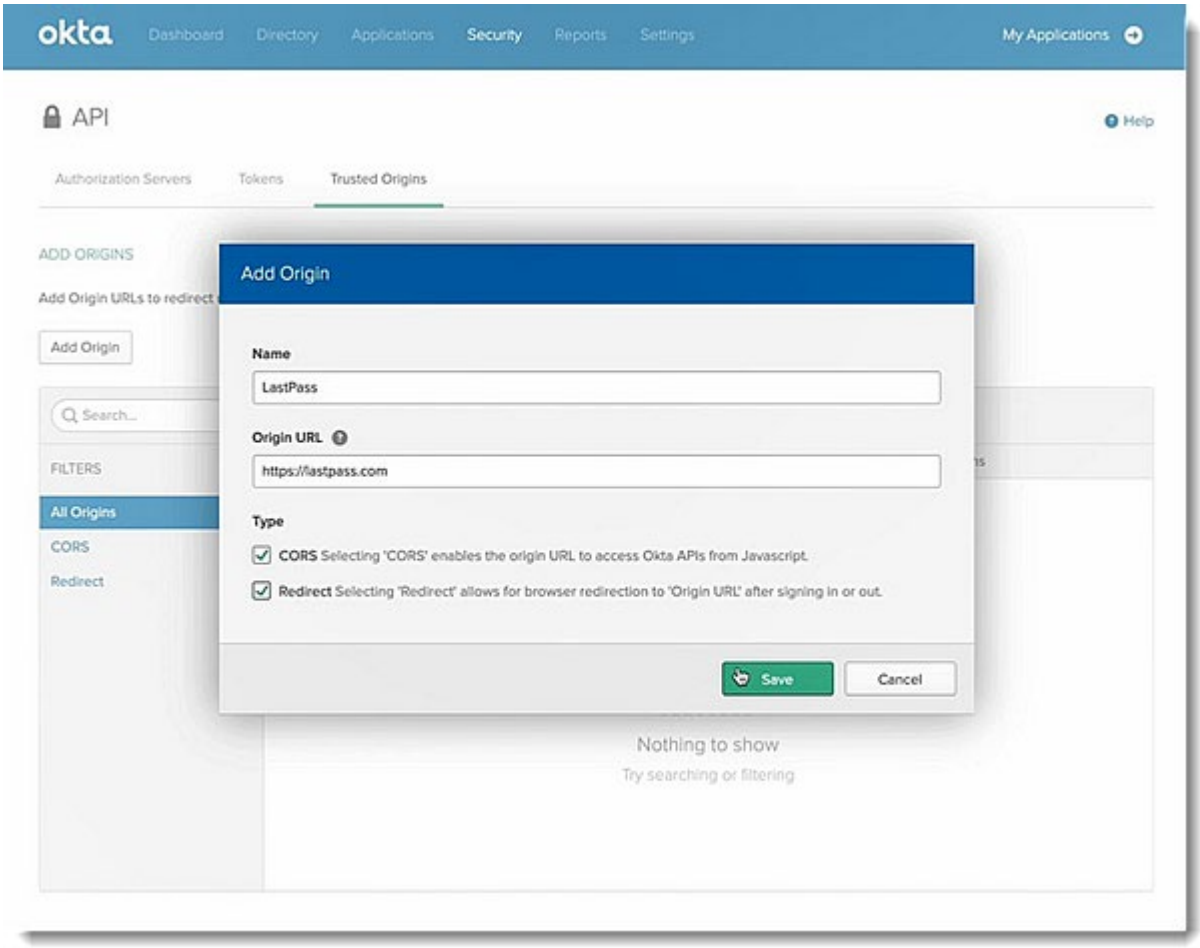
If you modify the LastPassK1 Key that you use to set up federated login for your organization:

- **All of your LastPass users will instantly lose access to their Vaults**
- **The only way to restore their access is to reset the Master Password for each individual LastPass user by utilizing the Super Admin Master Password Reset policy (strongly recommended before beginning setup).**


okta
Dashboard
Directory
Applications
Security
Workflow
Reports
Settings
My Applications
Back to Applications
LastPass Okta Login
Active
View Logs
General
Sign On
Assignments
Settings
SIGN ON METHODS
The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.
Application username is determined by the user profile mapping. Configure profile mapping
OpenID Connect
About
OpenID Connect allows users to sign-on to applications using the OpenID Connect protocol.
Token Credentials
Edit
Signing credential rotation
Automatic
OpenID Connect ID Token
Edit
Issuer
Audience
Claims
Claims for this token include all user attributes on the app profile.
Groups claim type
Groups claim expression
Using Groups Claim

Step #4: Enable CORS for LastPass

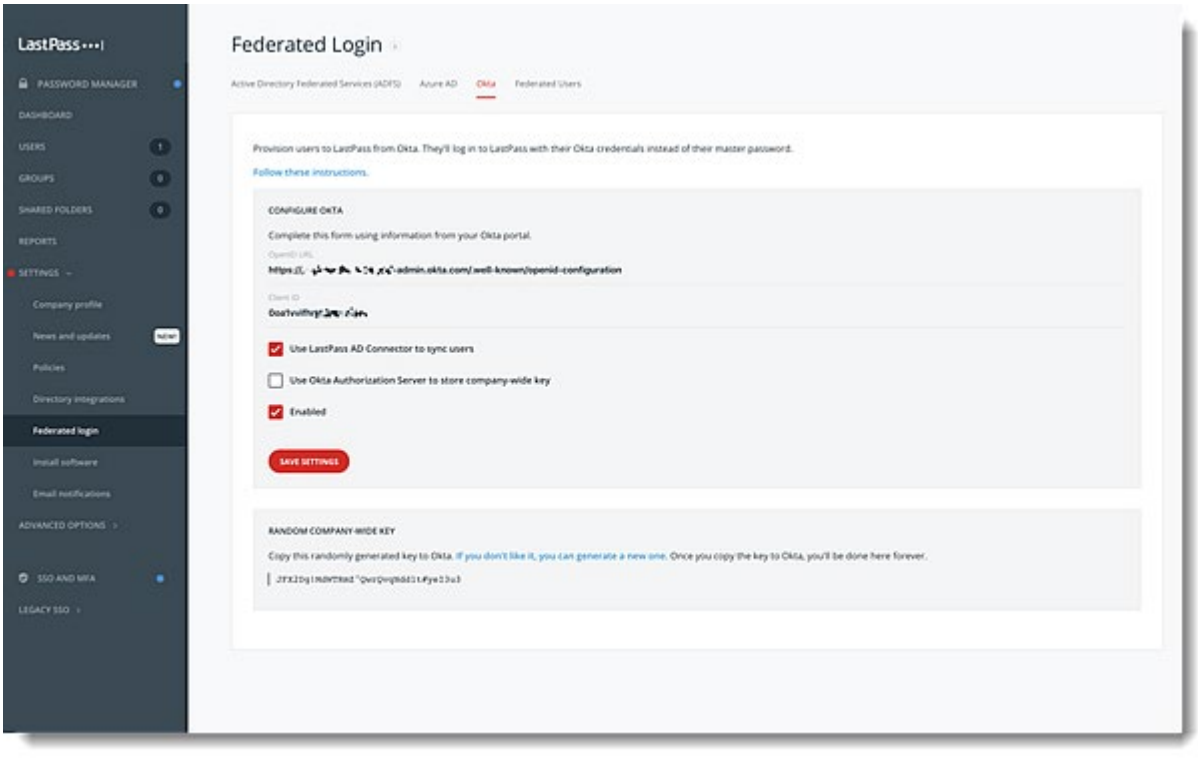
1. Click the **Security** tab, then click **API**.
2. Click the **Trusted Origins** tab, then click **Add Origin**.
3. Enter the following values:
    - **Name**: LastPass
    - **Origin URL**
        - For accounts using US data centers: https://lastpass.com
        - For accounts using EU data centers: https://lastpass.eu
4. Under Type, check both of the boxes to enable the following options:
    - **CORS**
    - **Redirect**
5. Click **Save**.



Step #5: Set Up Okta in LastPass

1. In Okta, click on the **Applications** tab, then click **Applications**.

2. Click on the LastPass Okta Login application, then on the **General** tab, scroll down to the "Client Credentials" section.
3. Copy the **Client ID** and paste it into your text editor application.
4. Return to the LastPass Admin Console, then select **Settings** > **Federated Login** in the left navigation.
5. Click the **Okta** tab.
6. Paste the **Client ID** (that you copied from **Sub-Step #2** this section) into the Client ID field.
7. Open a new web browser tab and navigate to the Okta Admin portal.
8. Edit the current URL to end with '.well-known/openid-configuration' which will look like this: https://<yourcompany>-admin.okta.com/.well-known/openid-configuration
9. Hit enter to the modified URL, which will confirm that the requested page is valid and exists.
10. Copy the modified URL and paste it into your text editor application.
11. Return to the LastPass Admin Console's Federated Login page with the **Okta** tab still selected, then paste the **modified Metadata URI** (that you copied from **Sub-Step #9** in this section) into the OpenID URL field.
12. Check the box to enable the **Use LastPass AD Connector to sync users** setting.
13. Uncheck the **Use Okta Authorization Server to store company-wide key** setting.
14. Check the box for the **Enabled** setting.
15. Click **Save Settings** when finished.



Step #6: Provision Users to LastPass Using the LastPass AD Connector

The users in this configuration are synchronized from your Active Directory, not Okta. As a result, the LastPass AD Connector must be configured to synchronize users from your Active Directory environment to LastPass. Please follow the setup instructions to configure the LastPass AD Connector at https://support.logmeininc.com/lastpass/help/set-up-the-lastpass-active-directory-connector-lp010057.

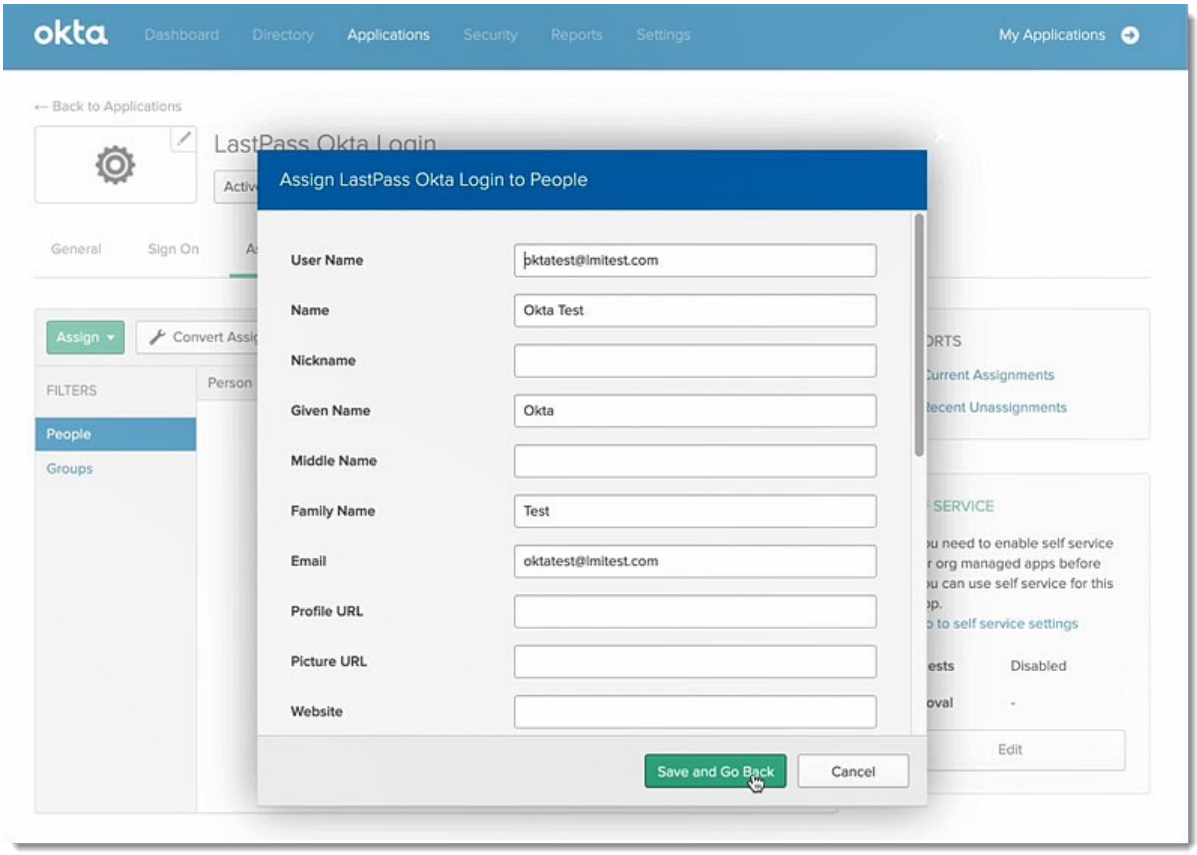
Please be sure that you sync the same users and groups from your Active Directory to LastPass as you do between Okta and your Active Directory, otherwise your users will be unable to authenticate.

Tip! *Use both the* ***LastPass AD Connector*** *and* ***Okta Active Directory agent*** *to sync the same set of users.*

Step #7: Assign the User to the Single Page Application

1. On the Okta Admin portal, under the **Applications** menu on the main toolbar, click **Applications**.
2. Click the **LastPass Okta Login** app.
3. Click the **Assign** drop-down menu in the upper-left navigation, then select **Assign to People**.
4. Locate your desired user, then click **Assign**.
5. When prompted, click **Save and Go Back**.
6. Click **Done** when finished.

Note: *Please be sure that the same users and groups are synchronized to LastPass and Okta from your Active Directory environment.*



Troubleshooting & Tips

- It is **required** that you enable the "Permit super admins to reset Master Passwords" policy 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 lastpass.com/contact-sales for more information.