LastPass •••|

Table of Contents

Set Up Federated Login for LastPass Using Okta

This guide provides setup instructions for using LastPass with Okta SCIM as your Identity Provider (IdP) for your LastPass Enterprise or LastPass Identity account.

Summary

LastPass supports the following provisioning features:

- Create Users
- Update User Attributes
- Deactivate Users
- Push Groups

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
  - Okta Lifecycle Management
  - API Access Management
- 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 Okta SCIM endpoint for federated login does not require any software installation.

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: Generate a Provisioning Token

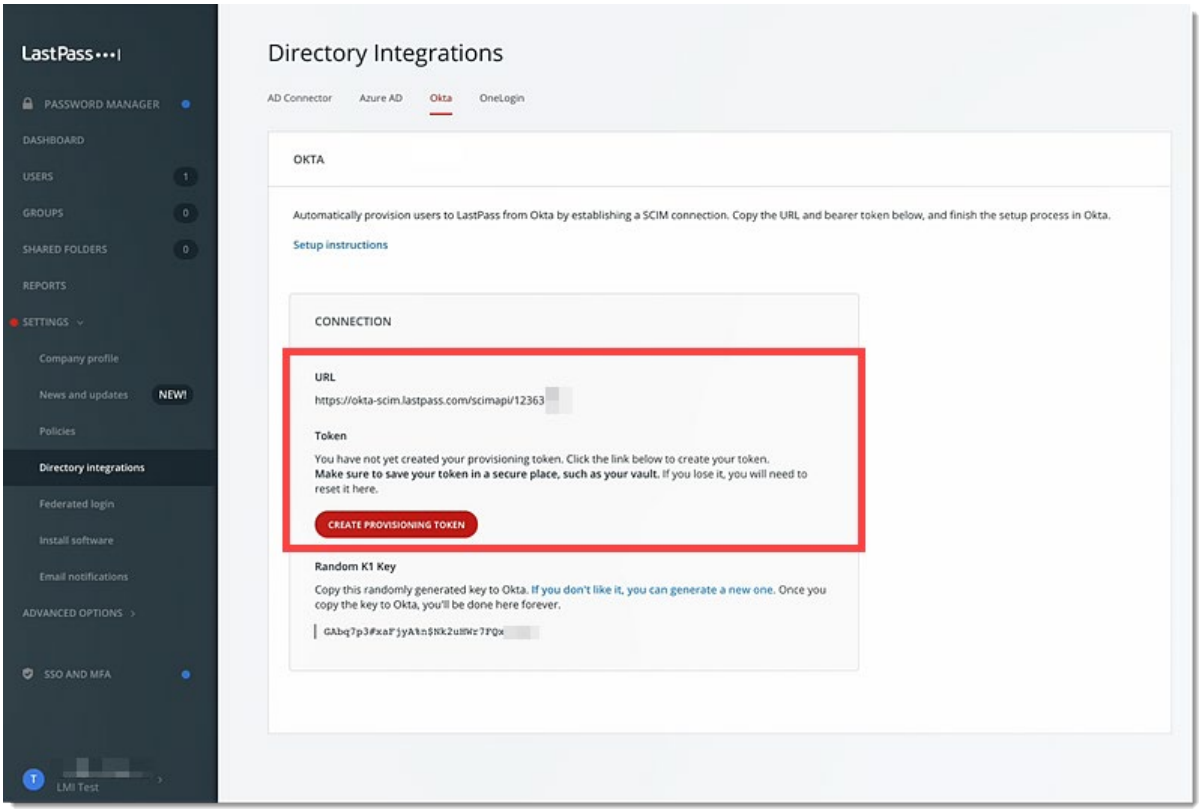
1. Access the LastPass Admin Console by opening a web browser and navigating to either of the following:

    - For accounts using US data centers: https://lastpass.com/company/#!/dashboard

    - For accounts using 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 **Okta** 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.

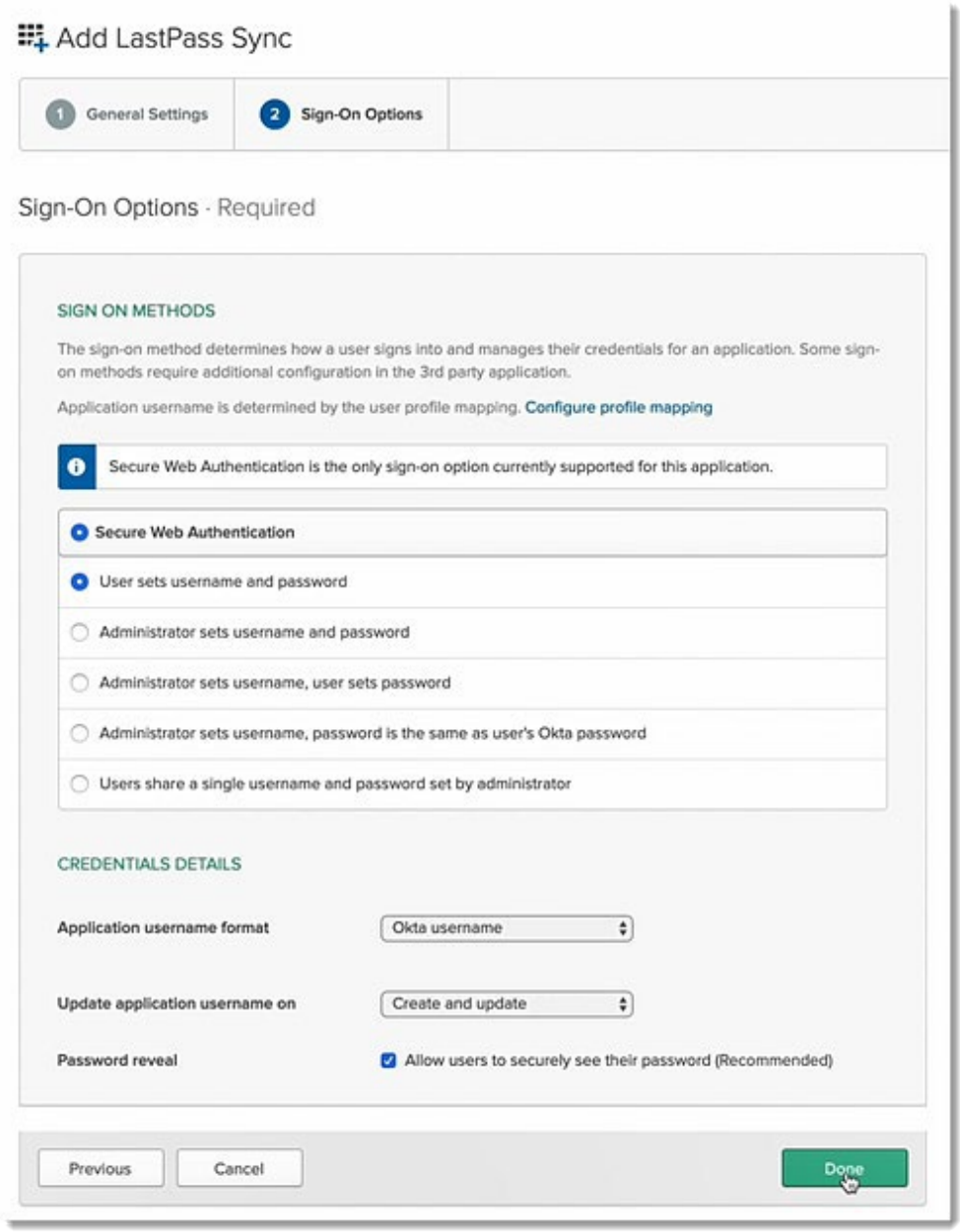
    Note: *If you navigate away from the Okta tab within the Directory Integrations page, the Provisioning Token will no longer be accessible through the LastPass Admin Console. If the Token is lost, a new one can be generated, but this will invalidate the previous code. Any process that used the old Token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



Step #2: Create a LastPass Sync app in Okta

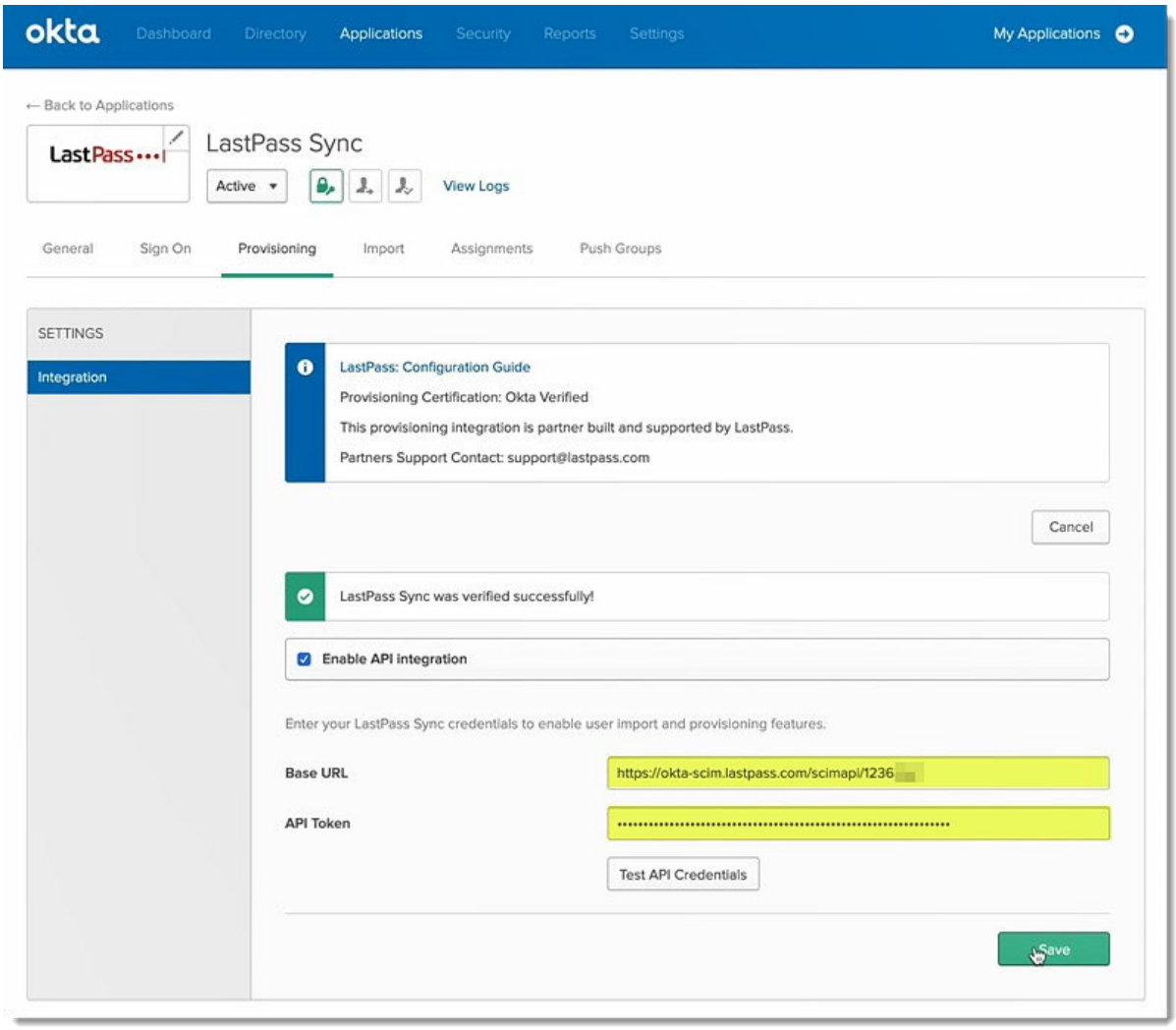
Once you have acquired the URL and Provisioning Token, you will need to enter them into the Okta Admin portal.

1. Log in to your Okta portal with your administrator account credentials.
2. Click the user account drop-down menu in the upper-right navigation, then select **Your Org**.
3. Access the Admin Dashboard by clicking **Admin** in the upper-right toolbar.
4. Under the **Applications** tab, select **Applications**.
5. Click **Add Application**.
6. Search for "LastPass Sync" then click **Add**.
7. Click **Next**, then click **Done** (leaving default values as-is).



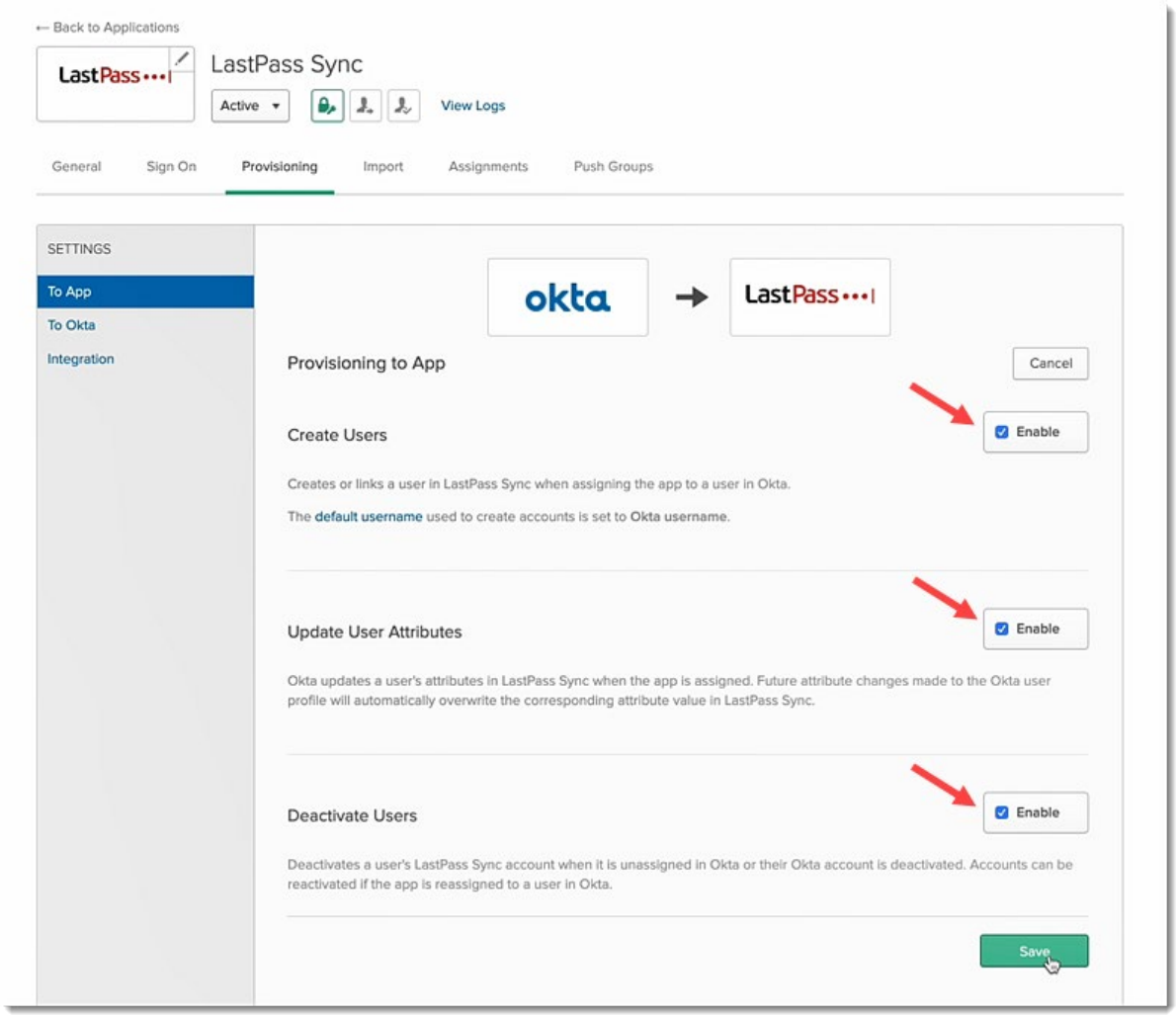
Step #3: Enter the Provisioning URL and Token into LastPass Sync

1. Click the **Provisioning** tab, then click **Configure API Integration**.
2. Check the box to enable the **Enable API integration** option.
3. Enter the following 2 values that you copied from **Step #1** (the Generate a Provisioning Token section) above:
    a. For the Base URL field, paste the Connection **URL** from **Step #1, Sub-step #5** above.
    b. For the API Token field, paste the **Provisioning Token** you copied from **Step #1, Sub-step #6** above.
4. Click **Test API Credentials** to validate the information you entered.
5. Click **Save** to finish setting up the application.



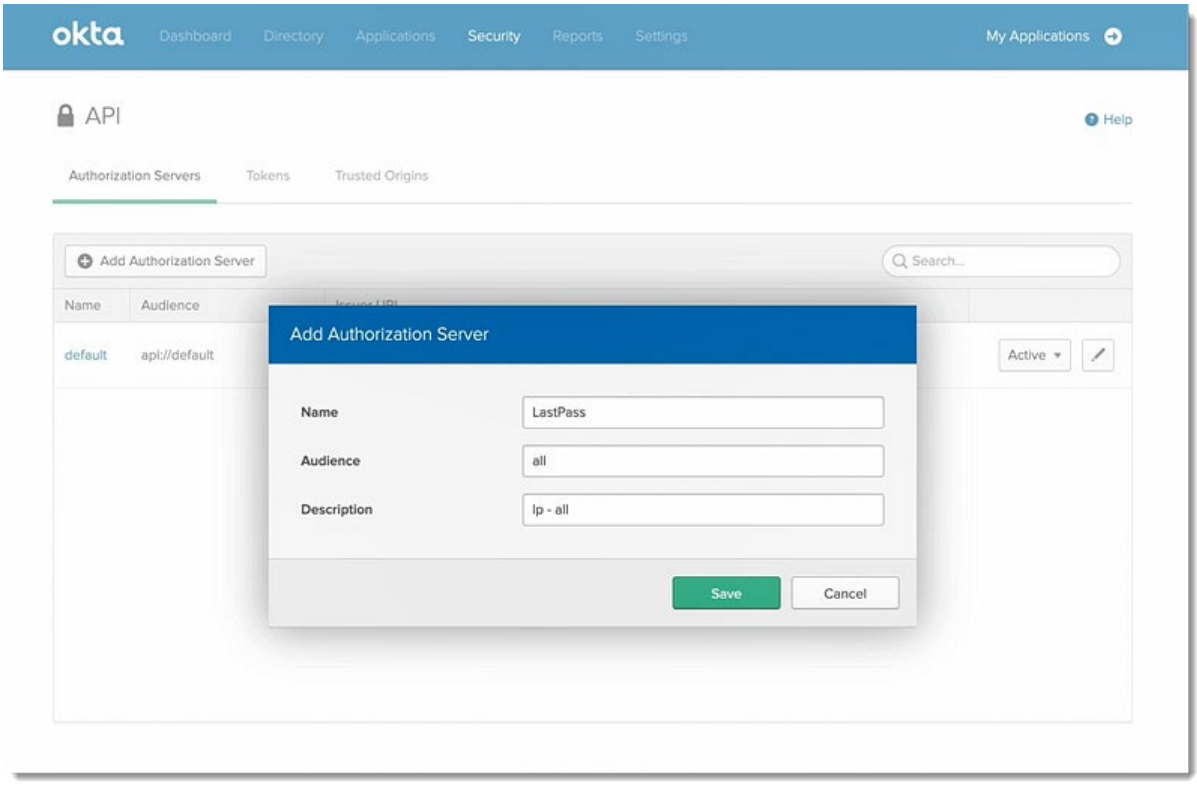
Step #4: Enable Provisioning to the LastPass Sync app in Okta

1. On the **Provisioning** tab, select **To App** in the left navigation.
2. Next to the "Provisioning to App" label, click **Edit**.
3. Check the boxes to enable the following 3 settings:
    - **Create Users**
    - **Update User Attributes**
    - **Deactivate Users**
4. Click **Save.**



Step #5: Create an Authorization Server for LastPass

1. Under the **Security** tab in the main toolbar, select **API**.
2. Click **Add Authorization Server** and enter your desired values into the Name, Audience, and Description fields. If you have no preference, enter the following values:
    - **Name**: LastPass
    - **Audience**: all
    - **Description**: lp – all
3. Click **Save** to finish adding your Authorization Server.



Step #5.1: Add a Generated LastPassK1 to Authorization Server Claims

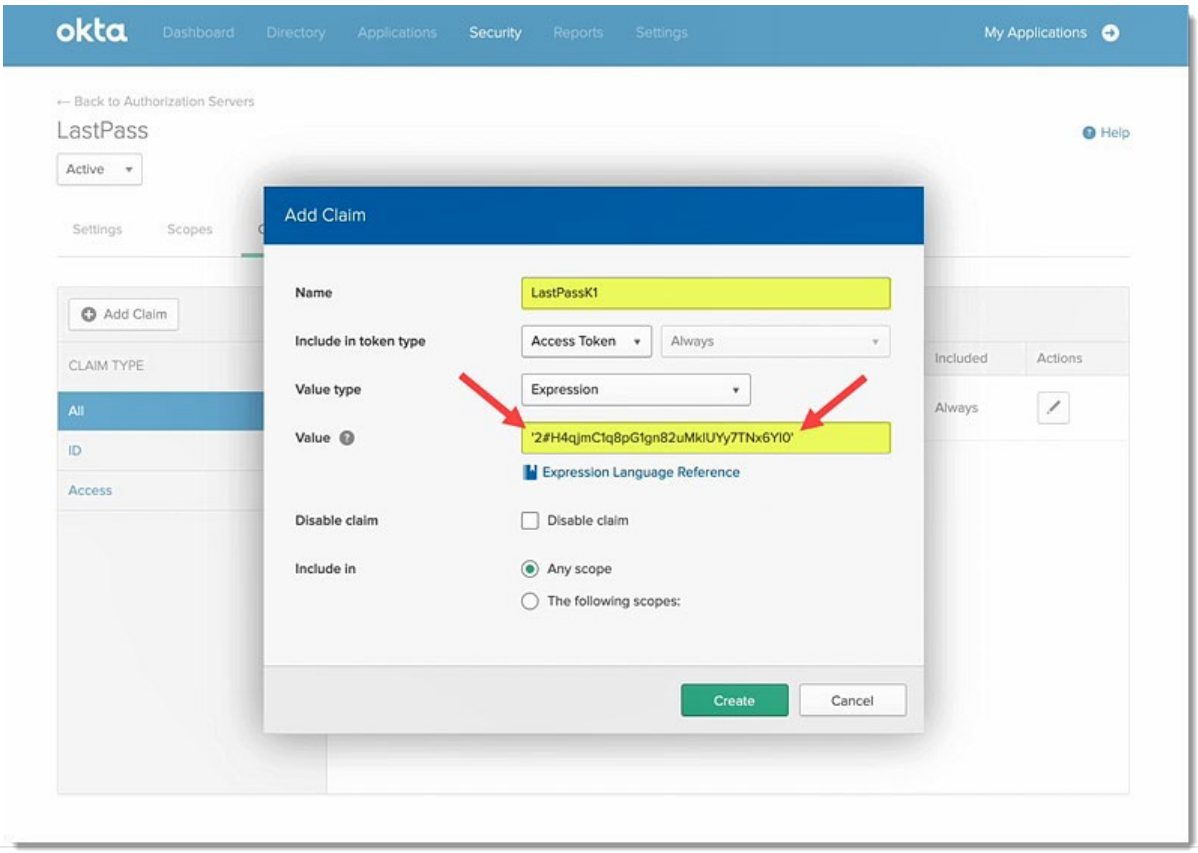
1. On the **Authorization Servers** tab, click the **Claims** tab.
2. Click **Add Claim** in the upper-left navigation.
3. For the Name field, enter **LastPassK1**.
4. Return to the LastPass Admin Console and click **Settings** > **Federated login** in the left navigation.
5. Click the **Okta** tab.
6. Copy the Random K1 Key (or click the hyperlink to generate a new one).
7. Once you have generated the Random K1 Key you would like to use, copy it and paste it into your text editor application.
8. Return to Okta and paste the **Random K1 Key** into the Value field between single quotes that you must add on each side of the key (e.g., 'r4nd0mk3y').
9. Click **Create** when finished.

WARNING!

It is of critical importance that you do not change the Random K1 Key once it has been saved in Okta.

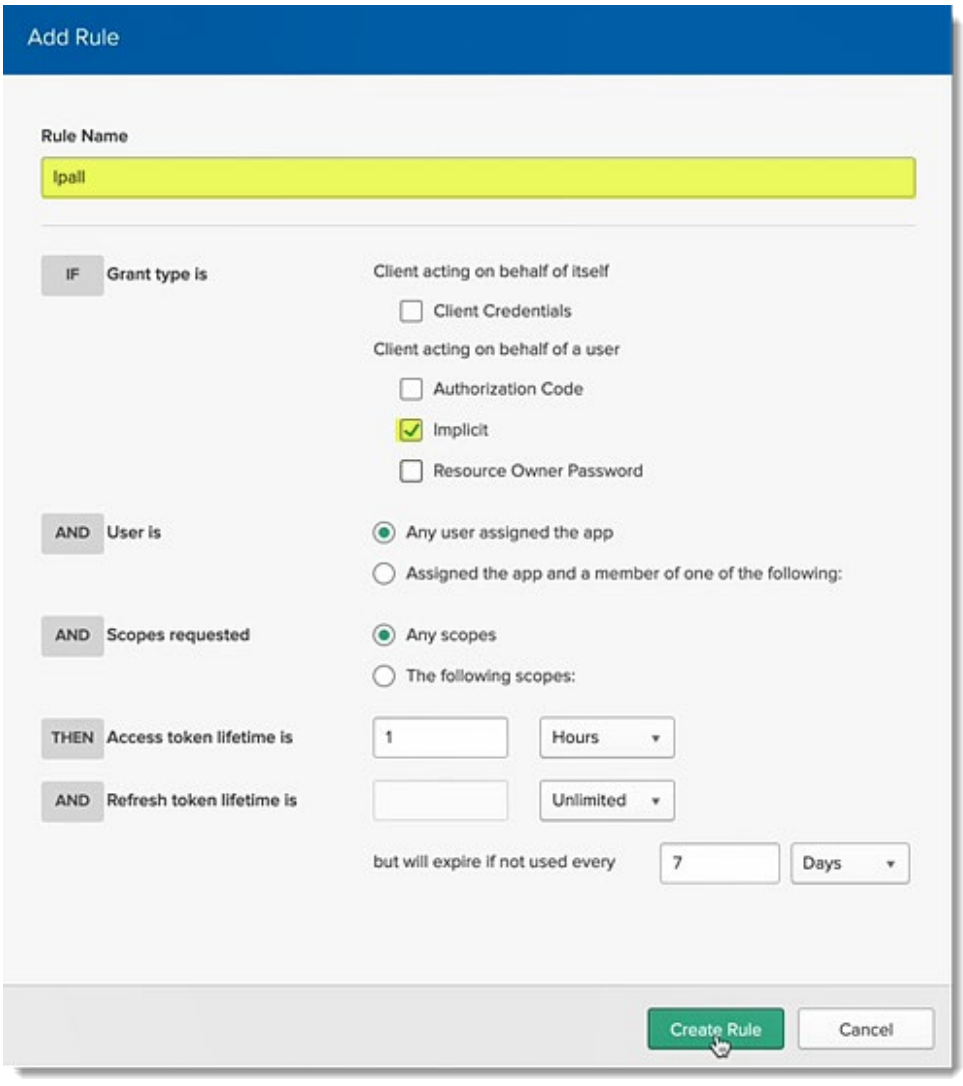
If you modify the LastPassK1 Key that you use to set up federated login for your organization:

- **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).**



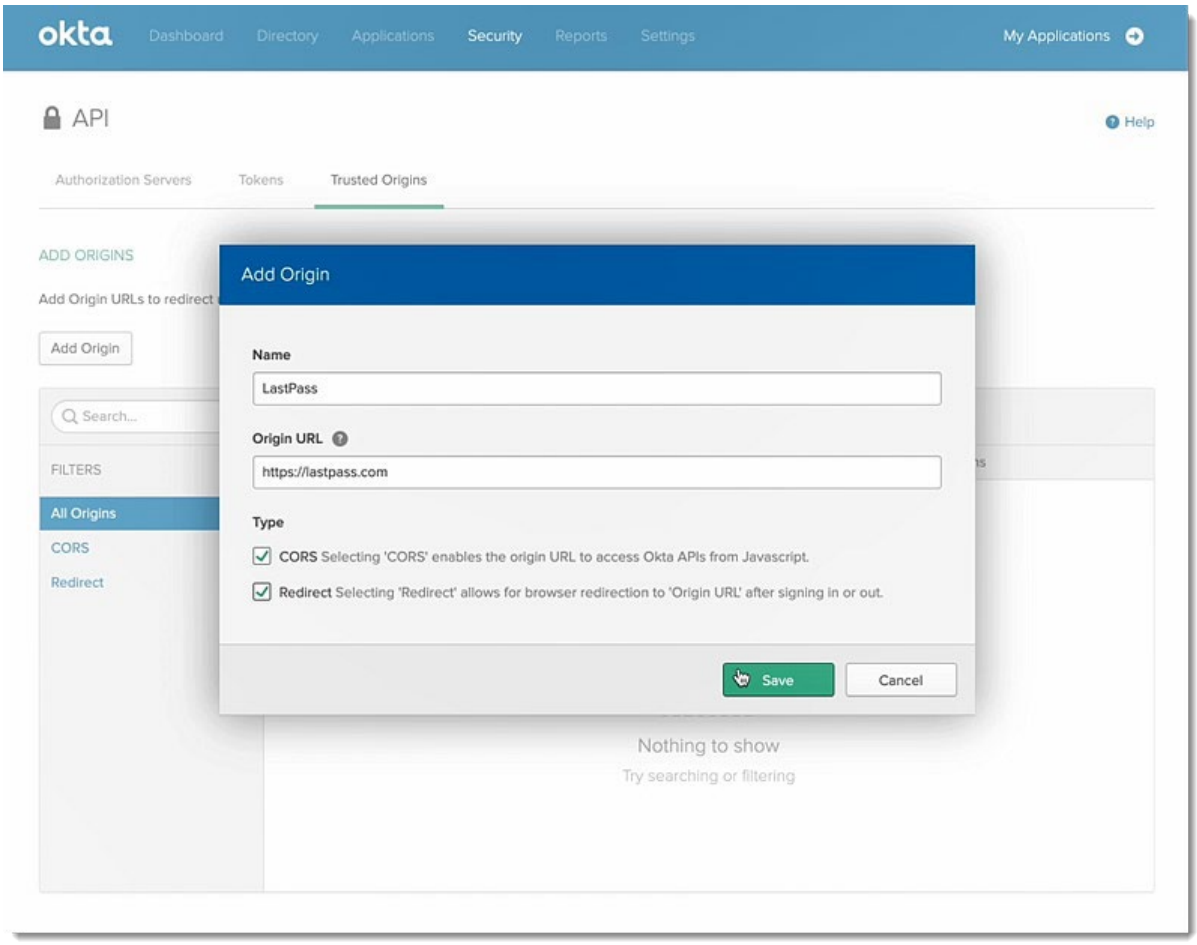
Step #5.2: Add a New Access Policy for the Authorization Server

1. On the LastPass Authorization Server page, click the **Access Policies** tab.
2. Click **Add Policy**.
3. Enter your desired values for the Name and Description fields. If you have no preference, enter the following values:
    - **Name**: LastPass
    - **Description**: lpall
4. Click **Create Policy**.
5. Click **Add Rule**.
6. Enter your desired value for the Rule Name field. If you have no preference, enter **lpall**.
7. Under the "If Grant type is" section, **uncheck** the boxes for the following:
    - Client Credentials
    - Authorization Code
    - Resource Owner Password
8. Confirm that the checkbox is enabled for the **Implicit** option, as it is a required setting.
9. Click **Create Rule**.



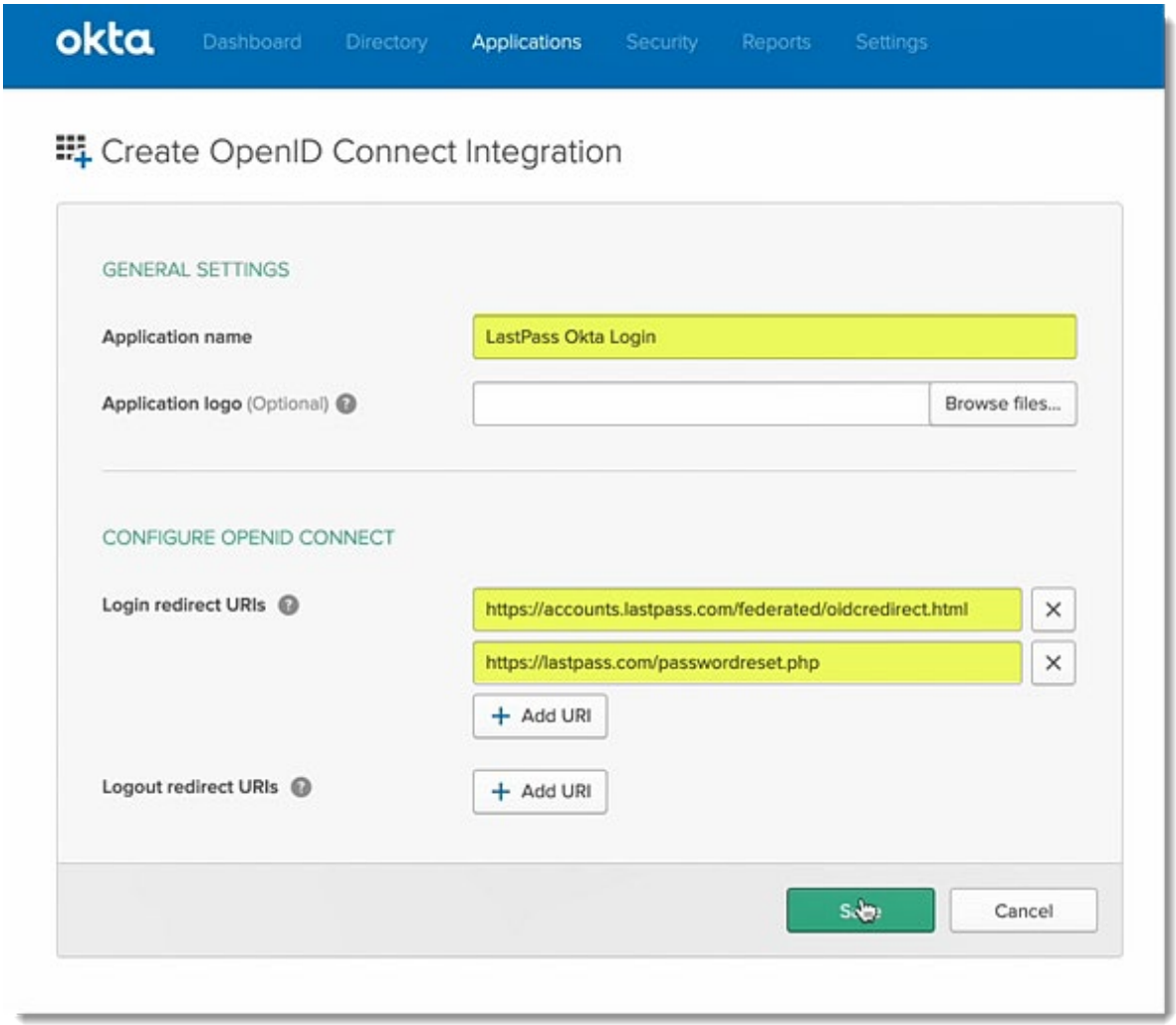
Step #6: Enable CORS for LastPass

1. Click **Back to Authorization Servers** in the upper-left navigation.
2. Click the **Trusted Origins** tab, then click **Add Origin**.
3. Enter the following values:
    - **Name**: LastPass
    - **Origin URL**: https://lastpass.com
4. Under Type, check both of the boxes to enable the following options:
    - **CORS**
    - **Redirect**
5. Click **Save**.



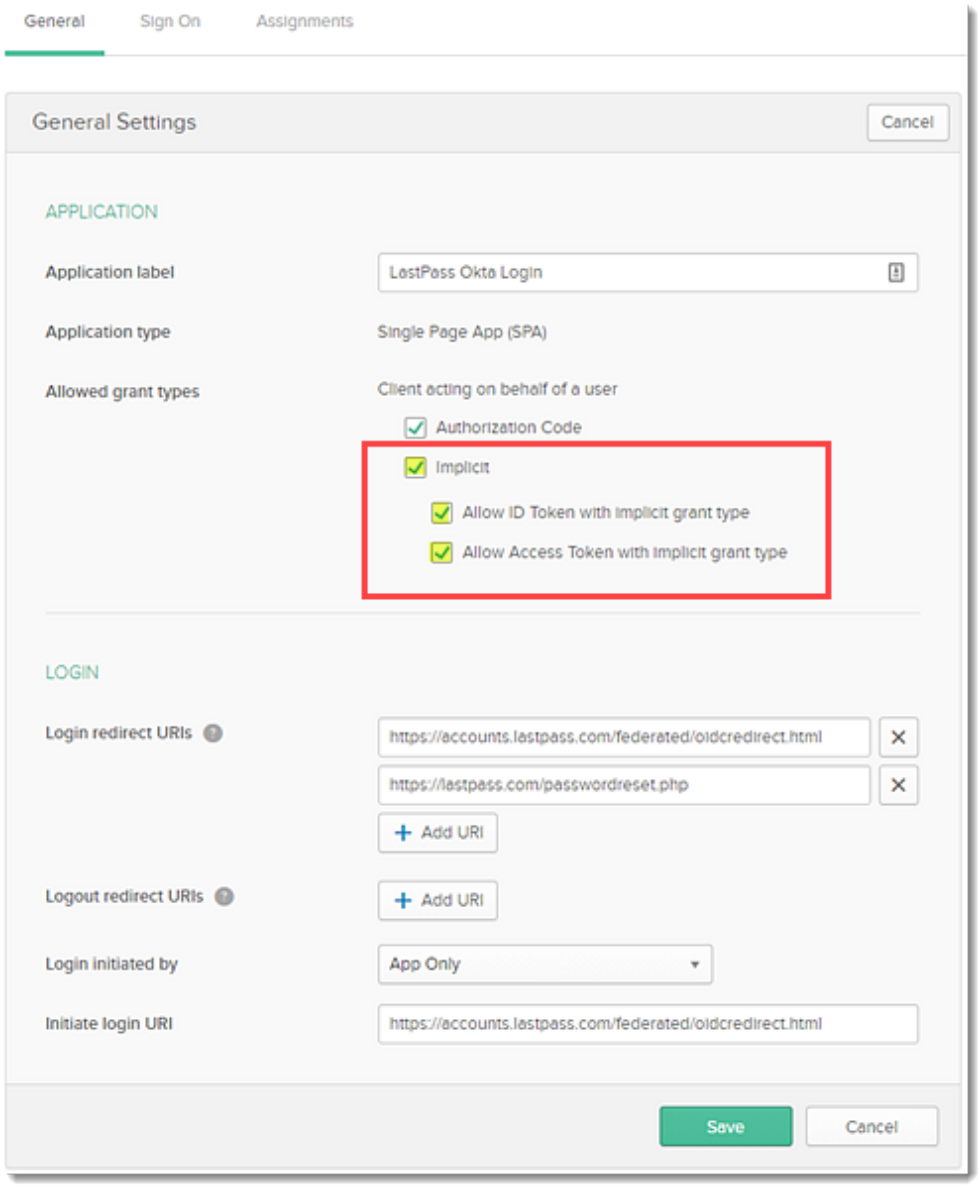
Step #7: Create a Single Page Application to Enable Login with Okta

1. Under **Applications** on the main toolbar, click **Applications**.
2. Click **Add Application** in the upper-left navigation.
3. Click **Create New App** in the upper-left navigation.
4. Under the "Platform" section, use the drop-down menu to select **Single Page App (SPA)**.
5. Click **Create**.
6. Under General Settings, enter the following information:
    - **Application name**: LastPass Okta Login
7. 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
8. Click **Save** when finished.



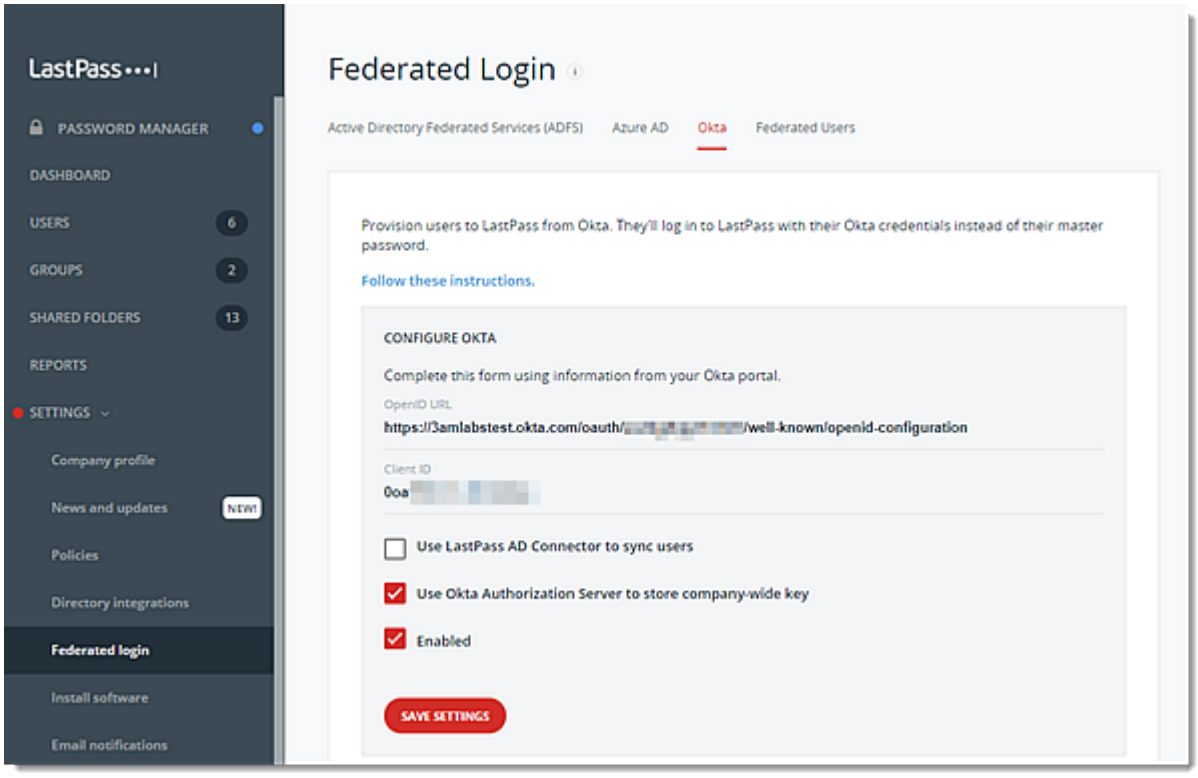
Step #8: Enable the Implicit Grant Type for ID and Access Tokens

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**.



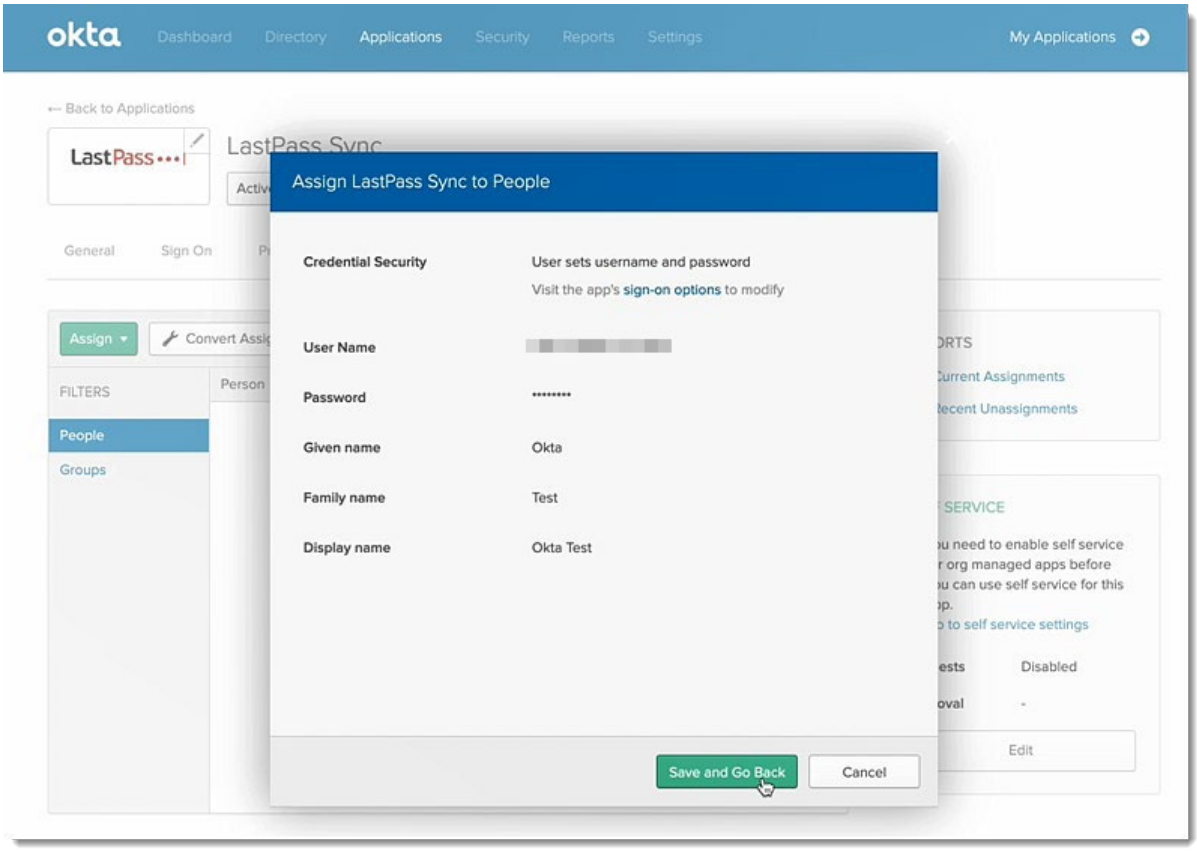
Step #9: Set Up Okta in LastPass

1. On the LastPass Okta Login application details page, scroll down to the “Client Credentials” section.
2. Copy the **Client ID** and paste it into your text editor application.
3. Return to the LastPass Admin Console, then select **Settings** > **Federated Login** in the left navigation.
4. Click the **Okta** tab.
5. Paste the **Client ID** (that you copied from **Sub-step #2** in this section) into the Client ID field.
6. Return LastPass Okta Login application details page. Under **Security** on the main toolbar bar, click **API**.
7. Click the name of Authorization Server you created from **Step #5, Sub-step #2** (in the Create an Authorization Server for LastPass section) above.
8. Open the **Metadata URI** in a new tab.
9. At the end of the Metadata URL (in the address bar of your web browser tab), replace “**oauth-authorization-server**” with “**openid-configuration**”.
10. Hit enter or open a new web browser tab to navigate to the modified URL, which will confirm that the requested page is valid and exists.
11. Copy the modified URL and paste it into your text editor application.
12. 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 #11** in this section) into the OpenID URL field.
13. Check the box for 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.



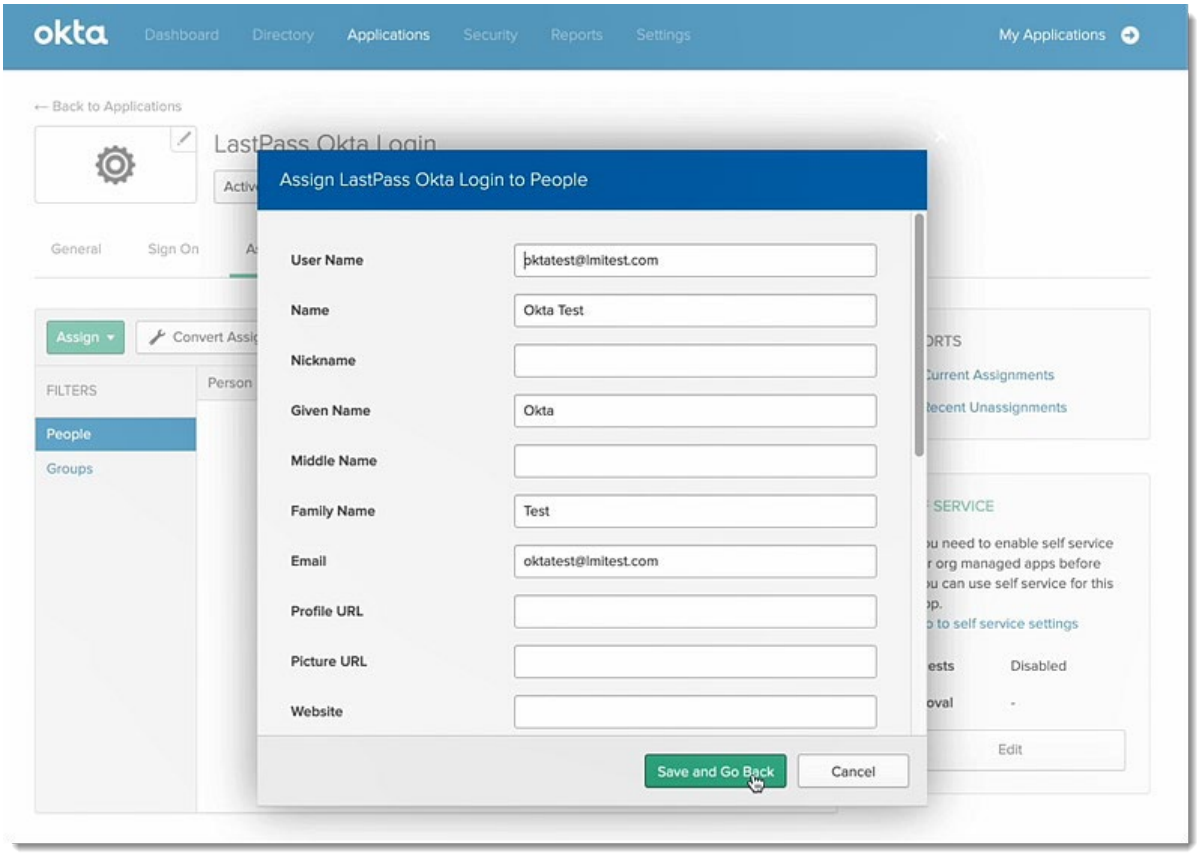
Step #10: Assign the user to the LastPass Sync application

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



Step #11: 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.



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.

For additional help, please see Set Up Federated Login for LastPass Using Okta, and if desired, select a contact option at the bottom of the article.