



Table of Contents

Summary.....	2
System Requirements.....	2
Before you begin.....	2
Step #1: Generate a Provisioning Token.....	3
Step #2: Create a LastPass Sync app in OneLogin.....	4
Step #3: Configure your LastPass Sync app.....	5
Contact Us.....	6

Set Up SCIM Provisioning for LastPass Using OneLogin

This guide provides set-up instructions for using LastPass with OneLogin as your Identity Provider (IdP).

Summary

LastPass supports the following provisioning features:

- Create Users
- Update User Attributes
- Deactivate Users

Completing only the SCIM Provisioning steps for OneLogin (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.

System Requirements

Syncing the OneLogin user directory to LastPass requires:

- An active OneLogin provisioning subscription
- An active trial or paid LastPass Business account
- An active LastPass Business admin (required when activating your trial or paid account)

The LastPass OneLogin SCIM endpoint does not require any software installation.

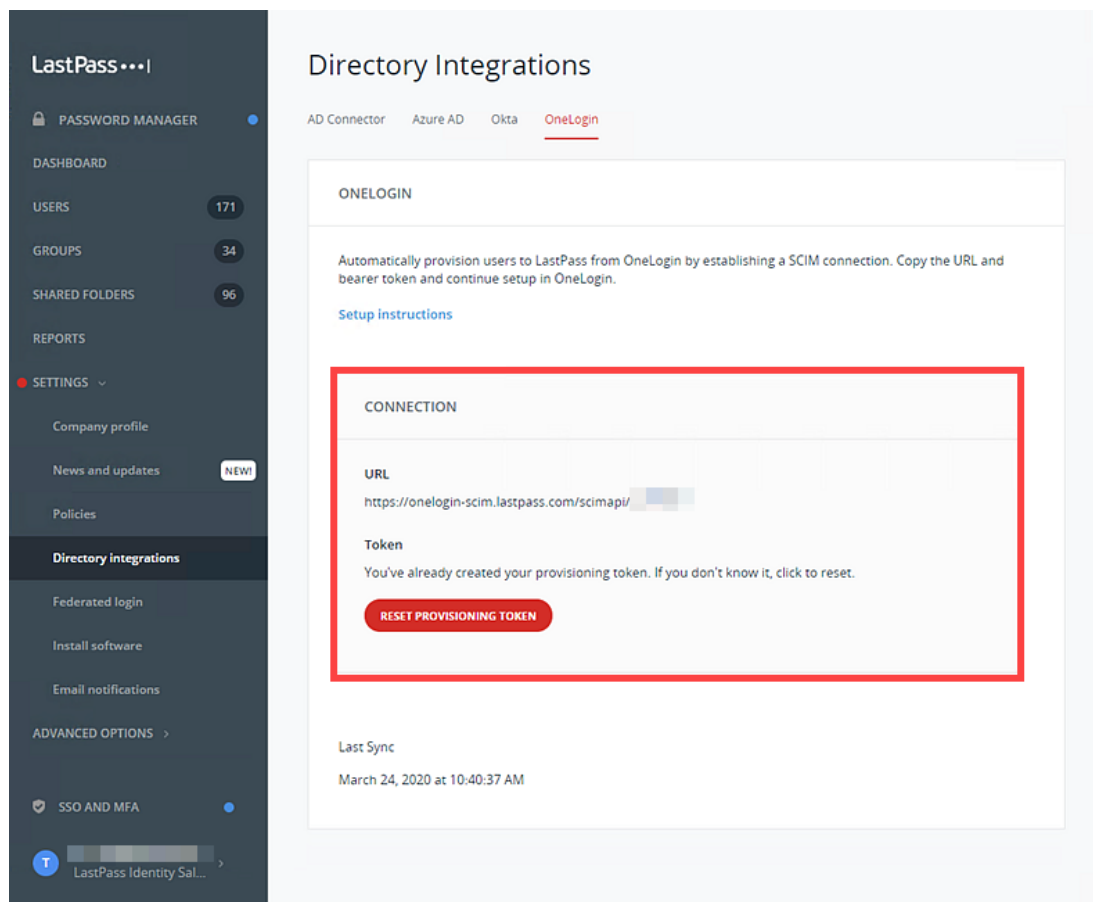
Before you begin

- It is **strongly recommended** that you [enable the “Permit super admins to reset Master Passwords” policy](#) for at least one (1) LastPass 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 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 OneLogin 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/company/#!/dashboard>
2. Enter your administrator username and Master Password, then click **Log In**.
3. Select **Settings** > **Directory integrations** in the left navigation.
4. Select the **OneLogin** 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.

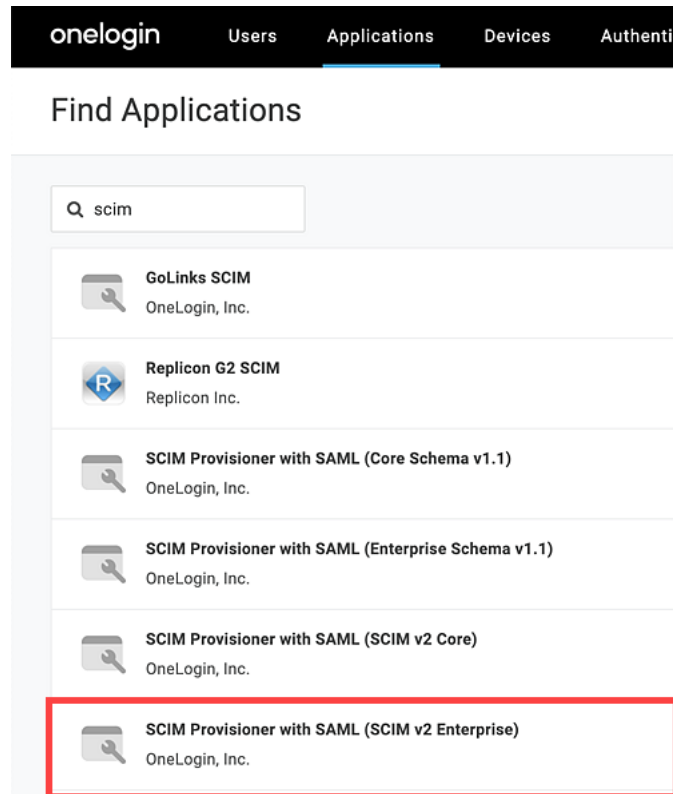
Note: If you navigate away from the OneLogin tab within the Directory Integrations page, the Provisioning Token will no longer be accessible through the LastPass Admin Console. If the Token is lost, a new one can be generated, but this will invalidate the previous code. Any process that used the old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



Step #2: Create a LastPass Sync app in OneLogin

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

1. Log in to the OneLogin admin portal with your administrator account credentials.
2. In the top toolbar, go to **Applications > Add App**.
3. Search for and select **SCIM Provisioner with SAML (SCIM v2 Enterprise)**.



4. Enter a name for the app (e.g., LastPass Sync).
5. Click **Save**.

Step #3: Configure your LastPass Sync app

1. Select the **Configuration** tab in the left navigation.
2. Scroll down and locate the “SCIM Base URL” field, then copy and paste the **URL** you captured (from **Step #1, sub-step 5** above) into the SCIM Base URL field.
3. Locate the “SCIM Bearer Token” field, then copy and paste the **Provisioning Token** you created and captured (from **Step #1, sub-step 6** above) into the SCIM Bearer Token field.
4. Under API Status, click **Enable**.

← SCIM Provisioner with SAML (SCIM ... MORE ACTIONS SAVE

Info **Configuration** Parameters Rules SSO Access Provisioning Users Privileges

SAML Consumer URL

API Connection

API Status

Disabled ENABLE

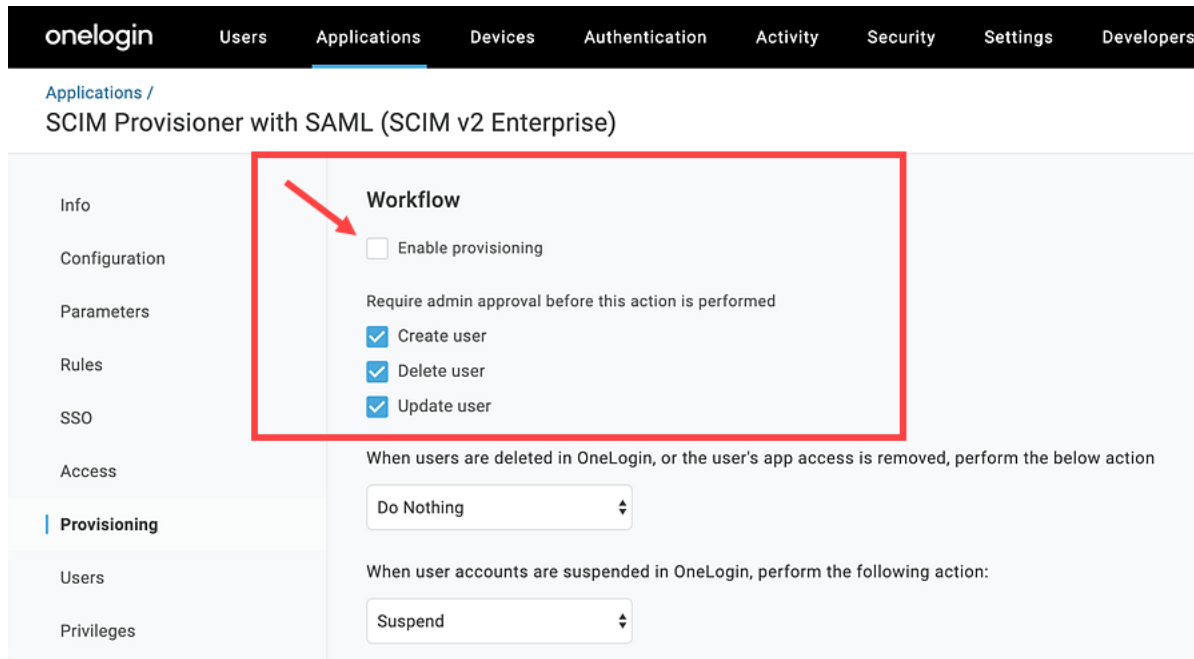
SCIM Base URL

SCIM JSON Template

Custom Headers

SCIM Bearer Token

5. Select the **Provisioning** tab.
6. If desired (based on the needs of your organization), under the “Require admin approval before this action is performed” section, uncheck the box(es) to disable the following options (which are checked and enabled by default):
 - **Create user**
 - **Delete user**
 - **Update user**
7. Check the box to enable the **Enable provisioning** setting when finished.



Contact Us

If you have not started a LastPass Business trial, please contact our Sales team at lastpass.com/contact-sales for more information.

For more details, please see [Set Up OneLogin Integration](#). For further assistance, you can contact our support team by select a contact option at the bottom of the article.