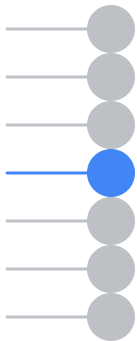


6. Set up user authentication

As an administrator, you can use single sign-on (SSO) profiles to control how users authenticate when using Password Sync. How you set it up depends on the number of profile assignments.

You're on step 6 of 7



Step 1: Provide instructions about password changes

1. Have users contact you or another admin if they need to reset their managed Google Account password.

For details, visit [Set up password recovery for users](/admin/users/set-up-password-recovery-for-users)
(/admin/users/set-up-password-recovery-for-users).

2. Create an internal webpage with instructions on how users should change their Windows password and not their managed Google Account password.

Step 2: Set user authentication

1. In the Google Admin console, go to Menu



Overview.

Go to Overview (<https://admin.google.com/ac/appsettings/352555445522>)

Requires having the [Security Settings](#)

(/admin/users/administrator-privilege-definitions#user_security) administrator privilege.

2. Click **Set up single sign-on (SSO) with a third party IdP**.
3. For **Manage SSO profile assignments**, go to the **SSO profile** column.
4. If there's only one assignment that relates to **SSO profile for organization**, go to Option 1 to set authentication by your organization's SSO profile.
5. If there are multiple SSO profiles and at least one assignment that relates to **None (Users will sign in with Google)**, go to Option 2 to set authentication by SSO profile assignments.

With this option, users that authenticate with SSO or with their Google credentials are directed to are directed to your internal webpage to change their Windows password.

Option 1: Set authentication by organization's SSO profile

This setting applies to your users even if you don't turn on SSO for your organization.

1. Click **SSO profile for your organization**.
2. For **Change password URL**, enter the URL of the internal webpage that you created in Step 1 to instruct users about changing their Windows password.
3. Click **Save**.

Option 2: Set authentication by SSO profile assignments

1. Click **Third-party SSO profile for your organization** and note any identity provider (IdP) settings.
2. Click **SSO with third-party IDPs**
>
Add SAML Profile.
3. Create a new SAML profile using the IdP settings from step 1.

4. For **Change password URL**, enter the URL of the internal webpage that you created in Step 1 to instruct users about changing their Windows password.

5. If there are no additional IdP settings to add, skip the remaining settings.

6. Click **Save**.

7. Click **Back** and change any profile assignments that reference **SSO profile for organization** to the new SAML profile.

Changes can take up to 24 hours but typically happen more quickly. [Learn more](#) (/admin/support/troubleshooting/how-changes-propagate-to-google-services)

8. Click **Third-party SSO profile for your organization** and uncheck the **Set up SSO with third-party identity provider** box.

9. Click **Save**.

With this option, even if you have no SSO profiles (SSO profile assignments set to **None** in the Admin console) and turned off the SSO profile for your organization, your users are directed to your internal webpage to change their Windows password.

Related topics

- [Set up SSO for your organization](#) (/admin/apps/setting-up-sso)
- [Google Sites training and help](https://support.google.com/a/users/answer/9282722) (https://support.google.com/a/users/answer/9282722)

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (https://creativecommons.org/licenses/by/4.0/), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (https://www.apache.org/licenses/LICENSE-2.0). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies) (https://developers.google.com/site-policies). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2026-07-17 UTC.