Install Skolon Pass (QR-code) as an IDP to Google Workspace

Skolon Support - 2025-10-01 - Google Workspace

Skolon SSO for Google Workspace: An Overview

This article provides a conceptual overview of how to set up Skolon as the primary login method (Single Sign-On or SSO) for pupils accessing Google Workspace. This integration allows pupils to use their familiar Skolon Pass (QR code) to securely access their Google accounts and services like Google Classroom.

In this setup:

- **Skolon** acts as the **Identity Provider (IdP)**. It is the authority that verifies the user's identity (e.g., by scanning a Skolon Pass QR code).
- **Google Workspace** acts as the **Service Provider (SP)**. It is the service the user wants to access.

When a pupil tries to log into their Google account, the following happens:

1. Google Workspace recognizes that the user belongs to a group that must log in via an external provider.
2. Google automatically redirects the user to the Skolon login page.
3. The pupil authenticates using their Skolon Pass (or username/password).
4. Once Skolon verifies the pupil's identity, it sends a secure confirmation back to Google.
5. Google accepts this confirmation and grants the pupil access to their account.

Installation steps

1. Install Skolon as an SAML IdP in Google Workspace
   Follow the steps in our how-to article here How-To: Configure Skolon SAML SSO in Google Workspace
2. Create Skolon Pass for the users (if you want to use the QR-code as SSO)
3. Assign the SAML SSO to one user to test the SSO as described below (Using Organizational Units (OUs) for Targeted Rollout)

4. Optional for Chrome Devices - configure force authentication as described below (Forcing Authentication on Chrome Devices)
5. Once you've completed the above steps and tested it with a user, assign the SAML SSO to the users you want in Google.

Using Organizational Units (OUs) for Targeted Rollout

A key advantage of this integration is the ability to control exactly who uses Skolon SSO. You don't have to enable it for everyone at once.

Within the Google Admin Console, you can create and manage Organizational Units (OUs). By assigning the Skolon SSO profile only to the OUs containing your pupil accounts, you can make this login method mandatory for them. Meanwhile, other users—such as teachers and staff—can remain in their own OUs and continue to log in directly to Google with their standard Google passwords. This ensures a smooth, phased rollout without disrupting staff workflows.

You can read more about how to assign the SAML SSO under the section "Decide which users should use SSO" on this support article from Google "Setting up SSO".

Configure SAML single sign-on for ChromeOS devices

For schools using Chromebooks, this integration can be extended to the device login screen. Within the Google Admin Console, you can configure a policy for specific OUs that forces authentication through an external identity provider. This means pupils can use their Skolon Pass not just to access Google services, but to log into the Chromebook itself, creating a seamless and unified login experience from the moment the device is opened.

You can find instructions on how to configure your ChromeOS Devices with a SAML Single Sign-On on this support article from Google:

Configure SAML single sign-on for ChromeOS devices