

DeepL login wall: Two steps to strengthen data security across your business

A simple solution that guarantees the highest level of confidentiality and streamlines user navigation

What is the login wall?

The login wall is a feature designed to help enforce maximum data security. It redirects your employees to the DeepL login page when they are connected to the internal network.

Why use the login wall?

With the login wall, your employees benefit from DeepL Pro’s enhanced confidentiality and data protection—allowing your company to get the most out of your subscription.



Enterprise-grade data protection

DeepL Pro safeguards your information with transport layer security (TLS) encrypted data transmission and guarantees text deletion after successful processing. Plus, DeepL Pro texts are never used to train our AI models or accessed by third parties. [Learn more about how we protect your data here.](#)



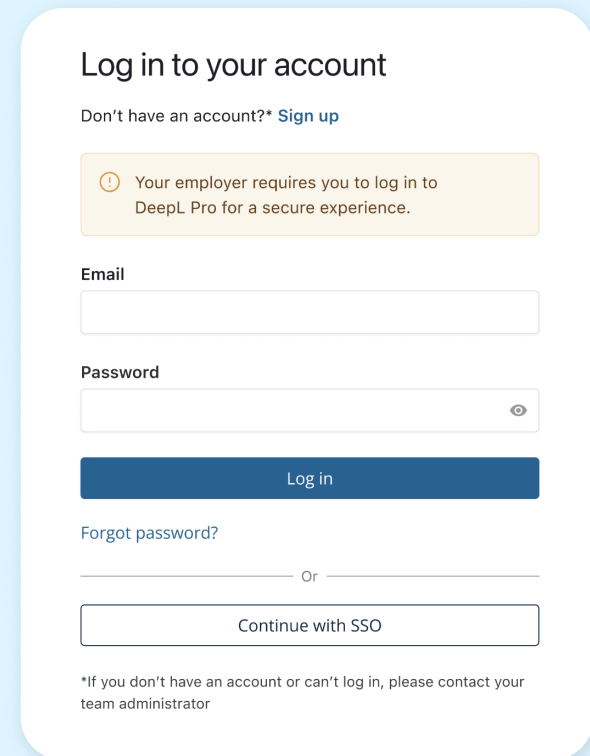
Best user experience

Once they log in, your employees get [all the perks of DeepL Pro](#): no character limit, easy document translation, and shared glossaries for consistent messaging. Simplify workflows, boost productivity, and offer the best user experience—all with your existing subscription.



Improved return on investment

Choosing the right Language AI solution can be challenging and costly. By taking advantage of all the features and licenses at your disposal, you’ll capitalize on the full value of your DeepL Pro subscription and improve your ROI.



How to set it up

Your IT department can implement the login wall and adapt it to your network in a few simple steps:



Step 1

Set up your proxy or firewall to respond to any request to `login-wall.deepl.com` with a **902 HTTP status code**

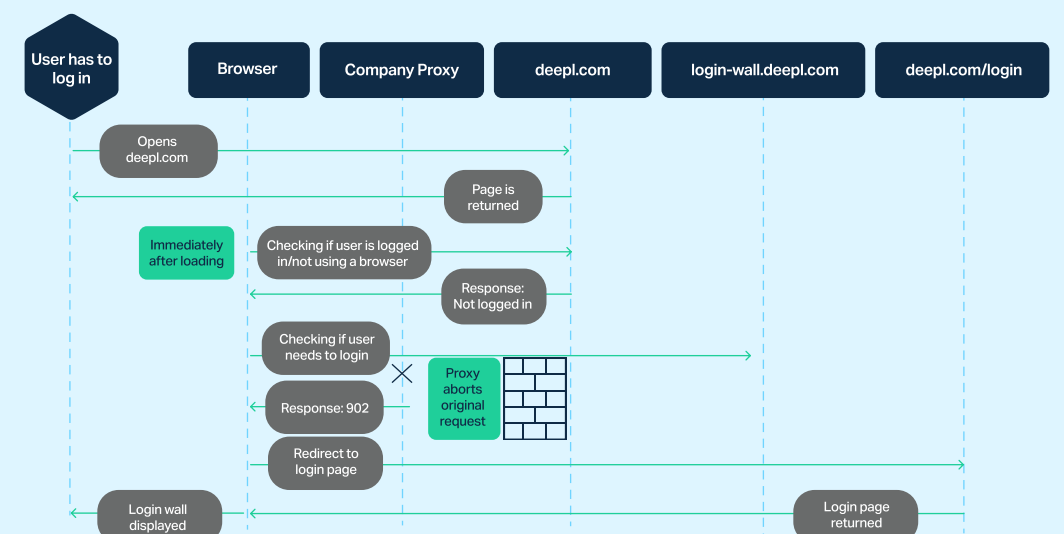
Important! The HTTP response must contain a certificate signed by your internal certificate authority. If your organization uses a web/content filtering proxy or firewall solution, you can configure this rule within them, as they typically handle SSL inspection using internally signed certificates.



Step 2

When your proxy or firewall responds with the 902 HTTP status code, our frontend will automatically redirect the user to <https://www.deepl.com/login>

Important! Allow Cross-Origin Resource Sharing (CORS) preflight requests. Our application performs preflight checks using the OPTIONS HTTP method before sending GET or POST requests to different subdomains of `deepl.com`. Please make sure that your firewall or proxy is configured to allow OPTIONS requests in addition to the standard GET and POST methods. This setup is critical for the proper functioning of the application across different subdomains.



Take control of your data security and make the most of DeepL Pro today