

AUTOWORKLET

User Guide

Everything you need to sign in, work securely, and get the most out of your automations.

For everyone on your team • Version 3.0 • Updated 29 Sep 2026

Welcome

This guide walks you through everyday Autoworklet - from signing in and keeping your session safe to teaching and running worklets with confidence. Pick a topic below, or read it through.

In this guide

1

Signing in & keeping your account secure

p.2

How to sign in securely, keep your session safe, and recover access to Autoworklet.

2

Working across your organizations

p.10

Working across organizations, understanding role-based permissions, and requesting the right level of access.

3

Building & running worklets safely

p.18

Building and running worklets while protecting customer data, credentials and connected integrations.

4

Staying safe & getting help

p.25

Everyday security responsibilities for every Autoworklet user - and how to report a problem fast.

Signing in & keeping your account secure

This guide tells Autoworklet users how to authenticate securely and regain access if they are locked out - so that only verified individuals reach customer data.

What you'll learn

- ✓ Signing in with Google or with email and password.
- ✓ Password rules and password reset for email accounts.
- ✓ Account recovery through Google or Forgot password.
- ✓ Understanding automatic session timeout and log-off behavior.

Signing in to Autoworklet

1. Open the Autoworklet web app. Sign in with Google, or with the email and password you registered.
2. If you use Google, your Google account's own sign-in protections apply (including 2-Step Verification if you turned it on there).
3. If you use email and password, the password must include at least 8 characters, an uppercase letter, a lowercase letter, a number, and a special character.
4. On first sign-in Autoworklet creates your personal workspace and opens Home for that workspace. Use the organization switcher to move to any other organization you have been invited to.
5. Never share your password or one-time codes. Autoworklet staff will never ask for them.

Signing in to Autoworklet



**Automate your workflow,
amplify your impact.**

Join thousands of forward-thinking teams who are reclaiming their time with Autoworklet's intelligent automation platform.

 © 2025–2026 Autoworklet, LLC. All rights reserved.

Welcome back

Sign in to your account

 Sign in with Google

Or sign in with email

Email address

Password

[Forgot password?](#)

Sign in →

By signing in, you agree to our [Terms of Service](#) and [Privacy Policy](#).

Don't have an account? [Sign up](#)

Sign in with Google, or with email and password.

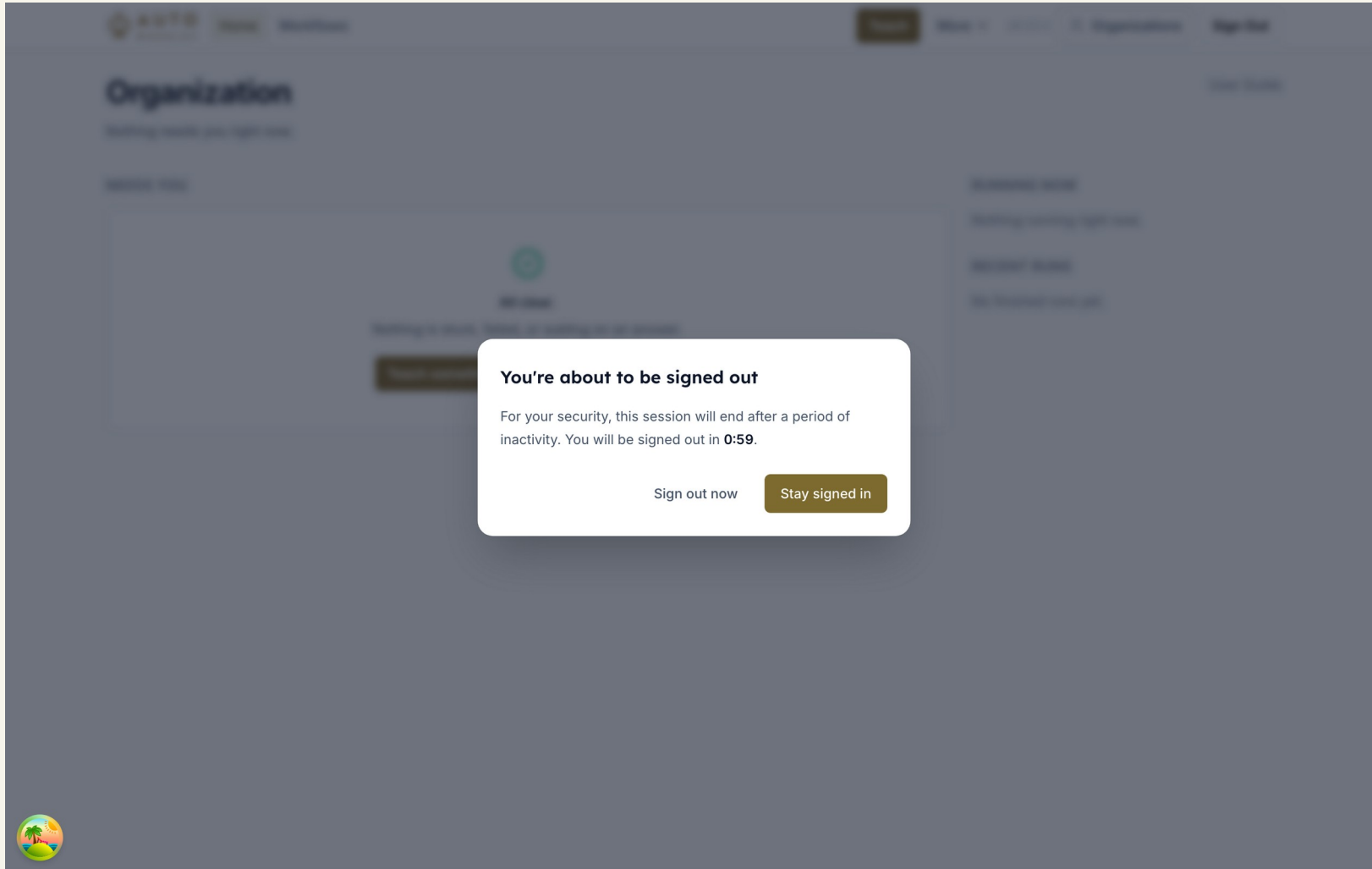
Protecting the account you sign in with

1. Google sign-in: turn on 2-Step Verification in your Google account settings. Autoworklet does not enroll a separate authenticator for your Autoworklet login.
2. Email and password: use a unique password and a reputable password manager. You can change it from your profile.
3. Login accounts that automations use to sign into other sites (password plus authenticator) belong in Secrets, not in your Autoworklet password. See Building and running worklets safely.

Session timeout and signing off

1. In the browser, after 2 hours of inactivity a warning appears one minute before automatic log-off; choose "Stay signed in" to extend.
2. A browser session is force-ended 24 hours after sign-in, regardless of activity.
3. Either timeout signs out that browser only; your other devices stay signed in.
4. The Sign out control in the header signs you out on every device. Use it on shared or public devices - do not rely on the timeout.
5. In the Autoworklet mobile app, the app locks after 15 minutes in the background and asks for a full sign-in every 30 days. Its Sign out ends the phone only.

Session timeout and signing off



One minute before idle log-off, choose Stay signed in or Sign out now.

Recovering access

1. Lost access to your Google account: recover it through Google's standard account-recovery process, then sign in.
2. Forgot an email-and-password login: use Forgot password on the sign-in page and follow the reset email.
3. Suspected account compromise: sign out and report it right away.
4. Admins re-verify identity out-of-band before restoring access - never approve a reset you did not initiate.

Recovering access



Reset your password

Remember your password? [Sign in](#) to your account.

Email address

Reset password →



Forgot password sends a reset email for email-and-password accounts.

Working across your organizations

This guide explains how access works across your organizations so you can work with the right level of access and know how to request changes.

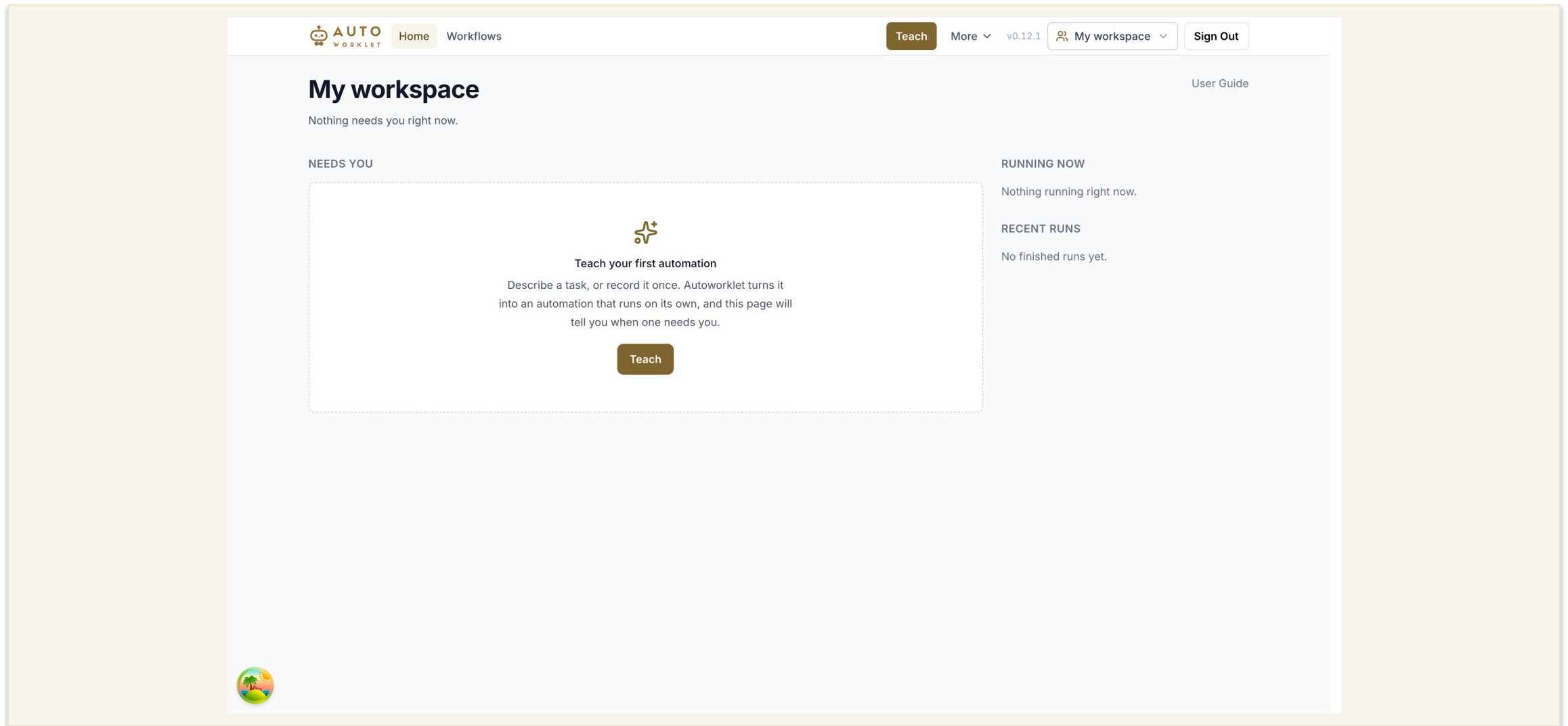
What you'll learn

- ✓ The personal workspace created for you at sign-up.
- ✓ Switching between organizations you belong to.
- ✓ Understanding member, manager and admin roles.
- ✓ Requesting access to an organization or a higher role.
- ✓ Inviting members (admins and managers) and removing access when people leave.

Your personal workspace

1. The first time you sign in, Autoworklet creates a personal workspace named for you and opens Home there.
2. You are an admin of that workspace. Use it for your own automations, or switch to a shared organization you have been invited to.
3. Shared organizations are created by an admin. You join them by accepting an invite.

Your personal workspace

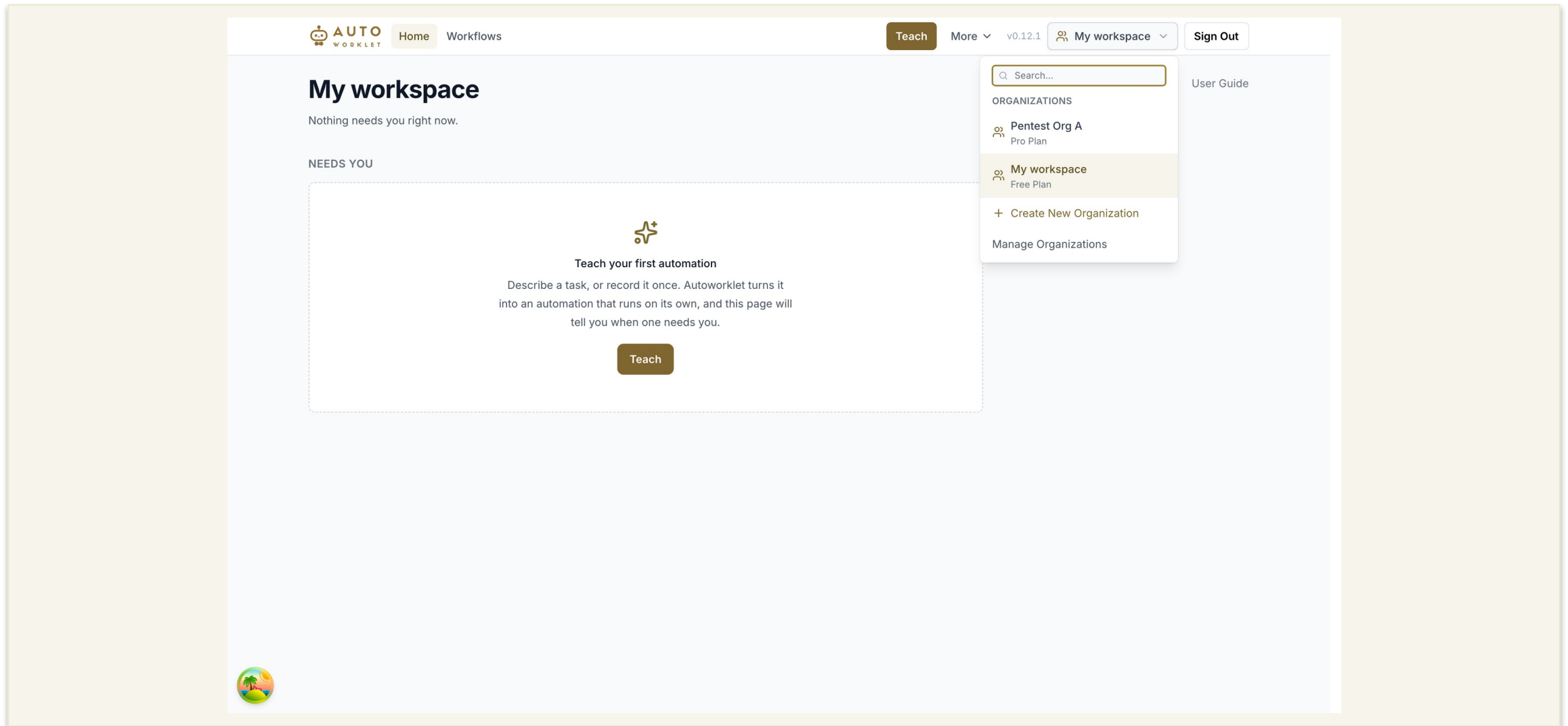


Home for your personal workspace. Teach starts an automation; this page lists what needs you.

Switching organizations

1. Use the organization switcher in the header to change your active organization.
2. Automations, data and run history belong to the active organization. Confirm you are in the right one before you run or share anything.
3. You only see organizations where you hold a role. If an organization is missing, you have not been granted access.

Switching organizations



The organization switcher lists every workspace you can open.

Understanding roles

1. Member: day-to-day use of automations and data the role permits; cannot invite people or change roles.
2. Manager: member capabilities plus inviting people, changing roles, and managing workflows.
3. Admin: full organization control, including billing and deleting the organization.
4. Ask for the lowest role that lets you do your job. Elevate only when a task requires it.

Requesting access or a role change

1. Ask an organization admin or manager, stating the business reason and the role you need.
2. They verify your identity and need, then send an invite or change your role.
3. Accept the invite from your verified account.
4. Keep requests specific. Ask only for the access you actually need.

Leaving or changing teams

1. Notify an admin or manager promptly when you no longer need access.
2. They remove membership the same business day for departures and immediately for terminations.
3. Once your access is removed, you can no longer open that organization.

Building & running worklets safely

This guide helps users create and run worklets safely - classifying data correctly, storing credentials in the right place, and limiting exposure of confidential information.

What you'll learn

- ✓ Teaching a new automation and watching Home for items that need you.
- ✓ Connecting third-party integrations (Sheets, Drive, Slack, GitHub).
- ✓ Storing login accounts for automations in Secrets.
- ✓ Handling and classifying the data worklets read and write.

Classifying data before you build

1. Identify whether the worklet touches public, internal or confidential/PII data.
2. Process only the data the task needs; avoid copying confidential data into logs or outputs.
3. Prefer references (IDs, links) over duplicating sensitive values inside worklet data.

Storing credentials and secrets safely

1. Never paste API keys, passwords or tokens directly into a worklet script or parameter.
2. Open More, then Secrets. Store each site login (website, username, password) there so automations can sign in without the secret living in a script.
3. If the site uses an authenticator app, add that authenticator to the same Secrets entry. This is for the automation's login, not for your Autoworklet account.
4. Connect Google Sheets, Drive, Slack or GitHub from More, then Settings, so Autoworklet holds scoped, revocable access rather than a pasted password.

Storing credentials and secrets safely

+ Add account

Website / service

e.g. github.com

Username / email

e.g. user@example.com

Password (optional)

Leave blank to skip

Description (optional)

e.g. shared ops account

MFA

None

QR / URI

Manual seed

+ Password generator

+ Save account

Add a site login in Secrets. Password and authenticator stay on the same account.

Autoworklet User Guide

21

Teaching and running worklets

1. Use Teach to describe a task or record it once. Autoworklet turns that into an automation.
2. Confirm the active organization and target data before you run, especially for write actions.
3. Home lists items that need you (a question, a stuck teach, a failed run). Open the item to handle it.
4. Dismiss hides an item on your Home only. It does not delete the work. Use Restore all if you hid something by mistake.

Teaching and running worklets

The screenshot shows the 'Teach a task' interface in the AUTO WORKLET application. At the top, there is a navigation bar with the 'AUTO WORKLET' logo, 'Home', and 'Workflows' links. On the right side of the navigation bar are buttons for 'Teach', 'More', 'v0.12.1', 'Organizations', and 'Sign Out'. Below the navigation bar, a progress indicator shows four steps: 1. Show (active), 2. Clarify, 3. Build, and 4. Ready. The main heading is 'Teach a task', followed by the instruction 'Describe what you want done, or record your screen. Up to 5 minutes.' There are two main sections for input: 'Describe the task' and 'Or record your screen'. The 'Describe the task' section includes a text input field with the placeholder text 'e.g. open example.com and read the main heading' and a 'Continue with a description' button. The 'Or record your screen' section includes a video recording icon and a placeholder for a screen recording.

Teach a task with a short description or a screen recording.

Sharing and embedding

1. Embed widgets only on trusted surfaces. Embedding exposes the configured worklet to that audience.
2. Revoke integrations you no longer use from More, then Settings.
3. Disconnecting immediately revokes Autoworklet's access to that integration.

Staying safe & getting help

This guide states the security responsibilities every user accepts when using Autoworklet, and the fast path for reporting anything suspicious.

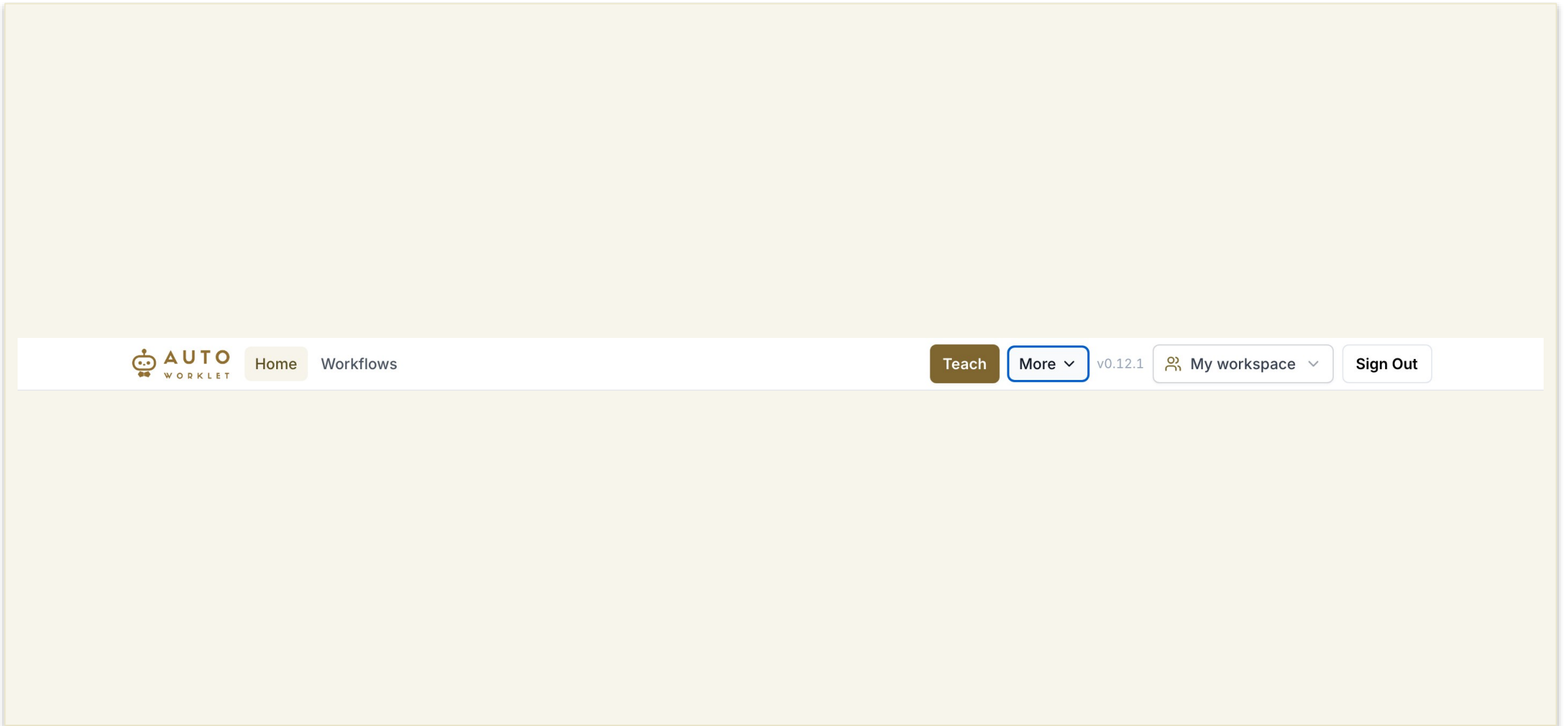
What you'll learn

- ✓ Acceptable use of accounts, data and integrations.
- ✓ Device and credential hygiene.
- ✓ Recognizing and reporting phishing and account compromise.
- ✓ The incident reporting path and expected response.

Protect your access

1. Never share passwords or one-time codes with anyone.
2. Lock your device and sign out on shared or public computers. Do not rely solely on the idle timeout.
3. If you sign in with Google, turn on 2-Step Verification there. If you sign in with email and password, use a unique password and a reputable password manager.
4. Only access data and organizations you are authorized to use.

Protect your access



Sign Out is always visible in the header.

Recognize phishing & social engineering

Always

1. Be wary of unexpected links or urgent requests to "verify" your account.
2. Autoworklet will never ask for your password or one-time code by email, chat or phone.
3. Verify the domain before entering credentials; report look-alike sites.

Report a security concern

1. If you suspect compromise, sign out of all sessions and change credentials where possible.
2. Report to security immediately via the published security contact / channel, with what happened and when.
3. Preserve evidence (screenshots, messages); do not delete suspicious items.
4. The security team acknowledges your report, investigates, and follows up as needed.

Acceptable use

[Reference](#)

1. Use Autoworklet only for authorized business purposes.
2. Do not attempt to bypass access controls, scrape other tenants' data, or disrupt the service.
3. Do not store data in Autoworklet that your organization prohibits from cloud processing.

Need a hand?

- > Open More, then User Guide, or read this PDF from Home.
- > Ask an organization admin or manager for access, roles, or integrations.
- > Spot something suspicious? Report it right away - see "Staying safe & getting help".
- > Protect the account you sign in with: Google 2-Step Verification, or a unique password in a password manager.

Thanks for using Autoworklet.