



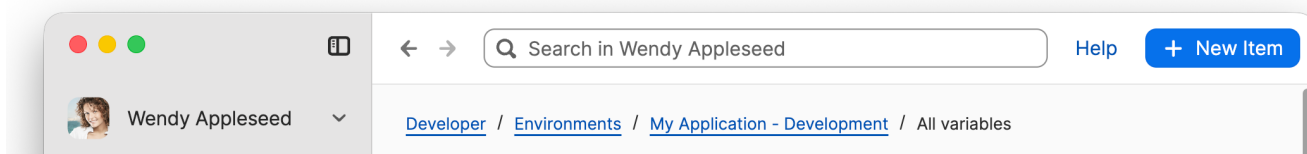
Environments

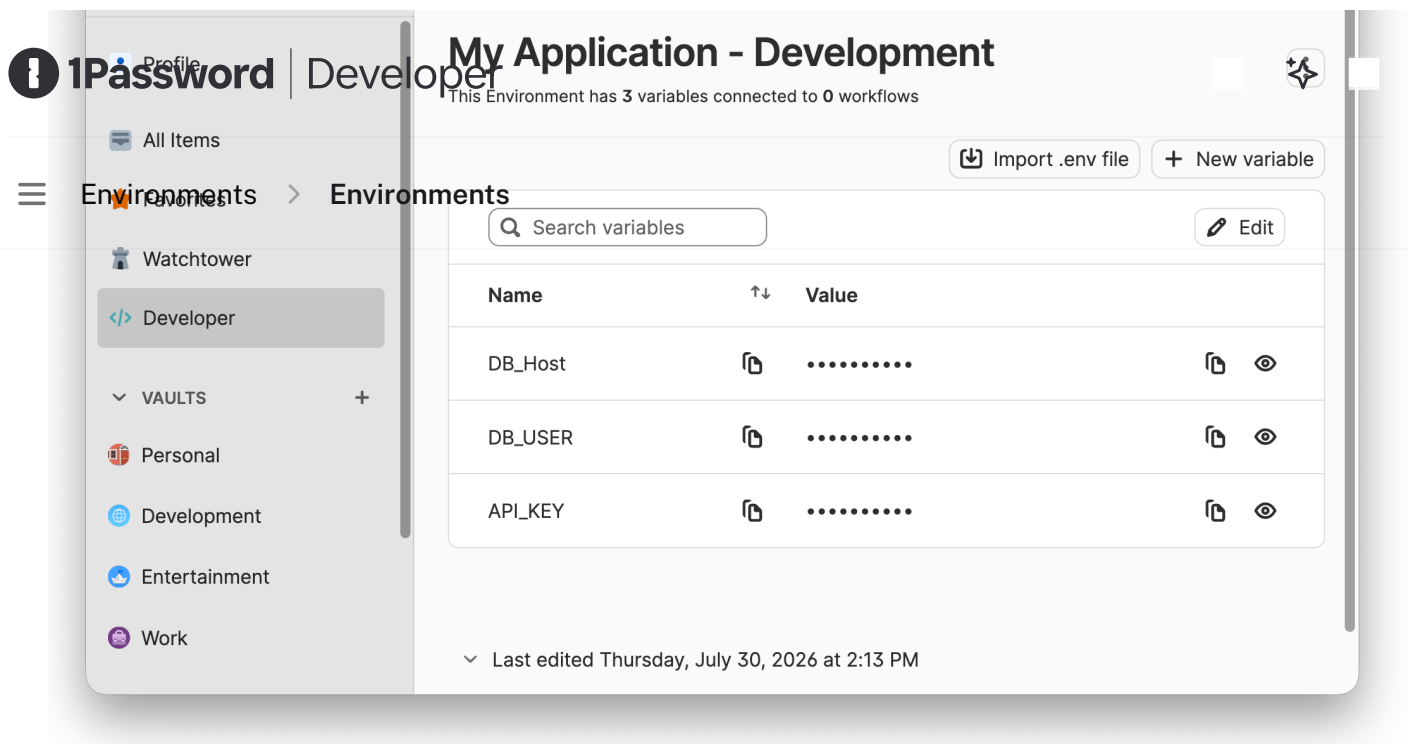
Environments

1Password Environments allow you to organize and manage your project's environment variables, separately from the rest of the items in your 1Password vaults. You can create an Environment for each project or development stage, then securely access your variables directly from 1Password when you need them. With Environments, you can:

- Make your Environment's variables available via [locally mounted .env files](#), without writing your credentials to disk.
- Validate your locally mounted .env file setup in supported agents and IDEs with [the 1Password agent hook](#).
- Programmatically [read your environment variables](#) from 1Password in your terminal or in your Go, JavaScript, or Python integrations.
- Securely sync your environment variables to [AWS Secrets Manager](#).
- [Share Environments with your team members](#) for easier collaboration and onboarding.
- [Connect an integration to your 1Password Business account](#), so your team can access their secrets in their machine workflows.

You can import your project variables to Environments from your existing .env files, or by manually adding key-value pairs for each variable.





⚠ When sharing an Environment with others and reading its contents outside of 1Password, review the Environment's values carefully before using them in any program or workflow. What you store in 1Password is exactly what we provide when you read your Environment.

Requirements

Before you can use Environments, you'll need to:

- [Sign up for 1Password.](#)
- Install and sign in to 1Password for [Mac](#), [Windows](#), or [Linux](#).
This feature is not available in 1Password for iOS or Android.
- Have an Owner or Administrator [turn the Environments policy on](#) from the 1Password admin console.

1Password | Developer

New to 1Password developer tools? Environments > Environments

Follow the developer quickstart to set up the CLI, create your first Environment, and add biometric SSH signing in one guide.

Create an Environment

1. In the 1Password desktop app, go to **Developer > View Environments**.
2. Select **New environment**.
3. Enter a name for the new environment, then select **Save**. If you have multiple 1Password accounts, you can select which account to save the environment to.



You can also use [1Password Developer Watchtower](#) to find `.env` files containing plaintext secrets on your device and [import them into Environments](#).

Add variables to an Environment

After you create an Environment, you can add your project secrets as variables. 1Password Environment variables map to conventional [environment variables](#). Each variable is a key-value pair that includes a name (for example, `DB_HOST`, `DB_USER`, or `API_KEY`) and a value that holds the corresponding secret.

To add variables to an Environment, open and unlock the 1Password desktop app, navigate to **Developer > View Environments**, then select the Environment you want to update.

You can add variables in two ways:

- If you have an existing `.env` file for your project, select **Import .env file**. 1Password will automatically import your environment variables.
- To manually add environment variables, select **New variable**. Enter the environment variable name in the **Name** field and its secret in the **Value** field. Repeat this process for

each environment variable you want to add.



 **Environments** > **Environments**

 Values are hidden by default, which means they'll be masked in the output of CLI and SDK operations. To change this, select the verticle ellipsis  next to the variable, then select **Show value by default**.

You can add, edit, or remove variables from your Environment at any time. To update your variables, open the Environment and select **Edit**.

Use your Environments in your workflows

In the 1Password desktop app, you can configure each Environment to fit your workflow:

- **Local .env file**: Create a locally mounted `.env` file to make your environment variables available during local development without writing plaintext secrets to disk.
- **Agent hook**: Use 1Password's hook to validate your locally mounted `.env` files with supported IDEs and agents like Cursor and GitHub Copilot.
- **Programmatically read Environments**: Read environments then pass environment variables to applications and scripts using 1Password CLI or 1Password SDKs.
- **AWS Secrets Manager**: Sync secrets from 1Password to AWS Secrets Manager.

Manage your Environments



1Password Environments return values exactly as they are entered. Format your values as you would in a standard `.env` file. For example:

- If a value contains a space, enclose the value in quotation marks: `"bar baz"`
- If a value contains special characters, escape them with a `\`: `\$100`

Values are hidden by default, but you can toggle the visibility on or off in the **Actions** column. You can also delete variables from this column. Select **Edit** within the environment to add, edit, or delete variables at a later time.

1Password | Developer Rename or remove an Environment



If you want to rename or remove an Environment:

≡ Environments > Environments

1. In the 1Password desktop app, go to **Developer > View Environments**.
2. Select the Environment you want to manage, then select **Manage Environment**.
3. Choose **Rename environment** or **Delete environment**.



Deleted Environments cannot be restored and any associated integrations will stop working. 1Password will prompt you to confirm whether or not you want to delete your Environment before proceeding.

Share an Environment

If you're using a shared account, such as for a team or business, you can share Environments with your team members. Each Environment remains independent, allowing you to work across multiple environments in different accounts while keeping environment variables separate. Access must be granted for each Environment.

To share an Environment:

1. In the 1Password desktop app, go to **Developer > View Environments**.
2. Select the Environment you want to share, then select **Manage environment > Manage access**. You'll be redirected to the Admin Console.
3. Select **Manage**, then search for and select the team members or groups you want to add to your Environment.
4. To adjust permissions for team members or groups added to your Environment, select the People or Groups tab in the "Environment access" screen. Next to the team member or group name, select the ellipsis and choose to allow viewing, allow editing, or allow managing.

To remove a team member or group from an Environment, return to the "Manage access" screen. Select the People or Groups tab in the "Environment access" screen, then select the

ellipsis next to the team member or group name you want to remove and select **Remove**



Environments > Environments Sort and search Environments

You can curate your Environments view to surface information you need in the way that best supports your work. From the Environments page in the 1Password desktop app (**Developer > View Environments**), select the arrow next to the **Name** column to organize Environments alphabetically or reverse-alphabetically.

Search for Environments from anywhere in the 1Password app [using the top-level search bar](#) to navigate to your Environments directly. Enter the name of an Environment in the search, then select it to go directly to that Environment's details page.

You can also sort or search for specific variables within Environments. Within an Environment's details page, select the arrow next to the variables **Name** column to organize variables alphabetically or reverse-alphabetically. To search variables, select + **Add variable** then enter a variable name in the **Search variables** bar.

Turn the Environments policy on or off

Owners and Administrators can turn Environments on or off from the 1Password Admin Console. This controls whether all users in an account have access to the Environments feature. If Environments are turned off, any previously created Environments and integrations will become inaccessible to users until the policy is re-enabled.

No data is deleted when the policy is turned off. Full access to all previously created Environments will be restored if the policy is turned back on.

If a user tries to access previously available Environments after the policy is turned off, they'll see a message that the policy has been turned off with instructions to contact an Administrator if they need access.

To turn the Environments policy on or off:

1. Sign in to 1Password.com with your administrator or owner account.

2. From the sidebar, go to **Policies** then select **Sharing and permissions**.
3. Select **Developer permissions**.

4. Scroll to the **Environments** toggle, then turn it on or off.

5. Follow the confirmation steps, then scroll to the bottom of the page and select **Save**.

Learn more

- [Access secrets from 1Password through local .env files](#)
- [Use 1Password's agent hook to validate local .env files from 1Password Environments](#)
- [Sync secrets between 1Password and AWS Secrets Manager \(beta\)](#)
- [Programmatically read Environments with 1Password CLI or 1Password SDKs](#)
- [1Password Developer Watchtower](#)
- [Workflow: Secure your developer secrets](#)
- [Workflow: Secure local development](#)
- [Workflow: Secure your deployments](#)

Related topics

-  [environment](#)
-  [Load secrets into the environment](#)
-  [Programmatically read 1Password Environments](#)

Was this page helpful?

 Yes

 No

[Local .env files](#) >

Terms of Service

 [Privacy Policy](#) > **Environments**

Cookie Policy

Accessibility

Resources

1Password University

Blog RSS

Newsletter

Community



Developer community

Code of Conduct

Community projects
disclaimer