Secret Scanner

The Postman Secret Scanner scans public workspaces and published documentation to detect exposed secrets on all Postman plans. The Secret Scanner monitors the collections, global variables, environment variables, API specifications, and documentation in public workspaces. It safeguards your organization from potential threats and malicious users attempting to access any exposed secrets. It also scans the documentation your team has published, regardless of the type of workspace it's found in.

If you're on an Enterprise plan with the Advanced Security Administration add-on, Secret Scanner also scans internal workspaces and Partner Workspaces. With the add-on, Secret Scanner delivers results for public workspace, internal workspace, and Partner Workspace scans in Secret Scanner dashboard.

> You can also set up Postman's integration for Slack to alert you in Slack if the Secret Scanner detects exposed secrets in your workspaces.

How Secret Scanner works

Postman's Secret Scanner is turned on by default for public workspaces with all Postman plans and scans for:

- Exposed supported secrets in all HTTP and multi-protocol collections, including their requests and responses.
- The initial values of environment variables and global variables.
- API specifications in the Postman API Builder.
- Documentation published, regardless of the type of workspace it's found in.

Postman automatically replaces exposed secrets with placeholders if the Secret Scanner detects exposed supported secrets in your public workspaces. Team Admins and Workspace Admins are notified by email, Slack (if configured), and in-app notification if exposed secrets are automatically replaced.

Postman recommends using a vault secret as a placeholder for a real secret because each user can only access and use their own vault secrets. Vault secrets aren't synced to the Postman cloud. You can also use a variable as a placeholder if you'd like.

> Postman delivers scan results in the Secret Scanner dashboard for Enterprise plans.

Advanced Security Administration add-on

In addition to public workspaces, Secret Scanner is available for internal workspaces and Partner Workspaces for Enterprise plans with the Advanced Security Administration add-on. Secret Scanner delivers results in Secret Scanner dashboard.

Secret Scanner scans for exposed supported secrets in all HTTP and multi-protocol collections, in addition to API specifications in the Postman API Builder. For Partner Workspaces, the Secret Scanner also scans the initial values of environment and global variables.

Automatically replace secrets detected in public workspaces

If the Secret Scanner detects exposed supported secrets in your public workspaces, Postman automatically replaces each secret with a placeholder. Postman notifies Team Admins and Workspace Admins by email and in-app notification that the secrets were detected and replaced with placeholders.

If the Secret Scanner detects exposed secrets in your public workspaces during its regular scans, Postman notifies Team Admins and Workspace Admins by email, in-app notification, and workspace settings with a link to view the Secret Scanner results. There you can review and automatically replace all exposed secrets in your public workspace. If you don't replace secrets by the date specified in the email and workspace settings, Postman automatically replaces each secret with a placeholder.

Exposed secrets are automatically replaced with placeholders as follows:

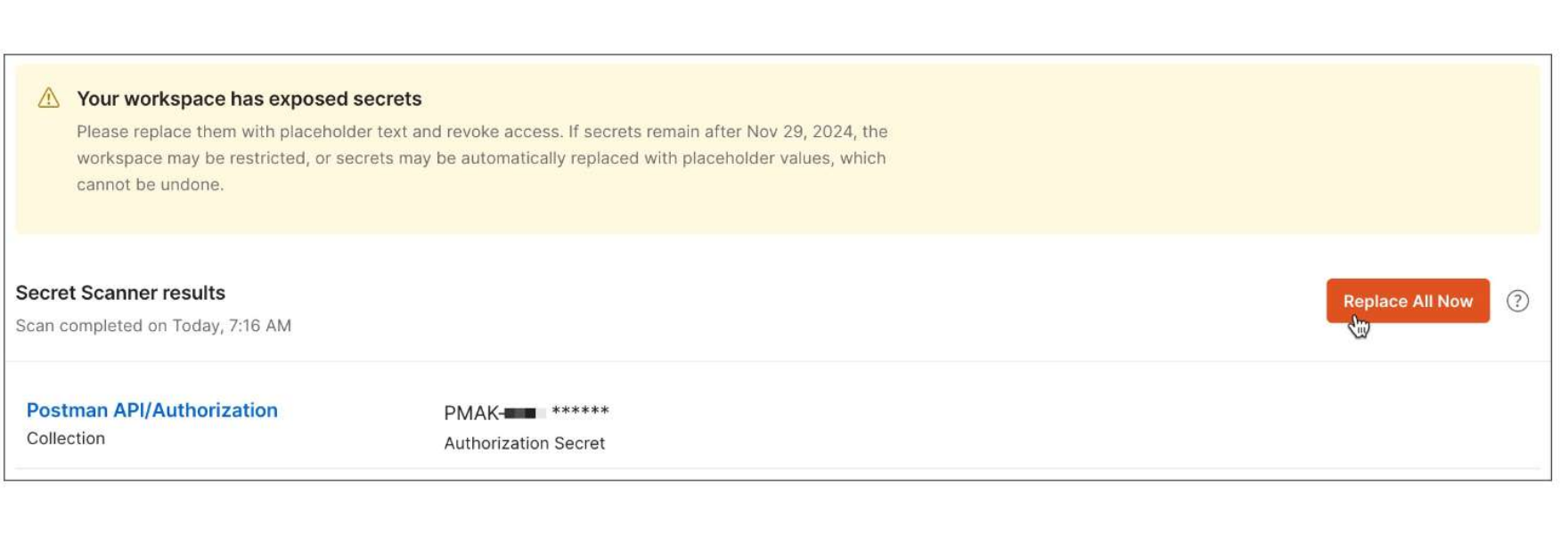
- For HTTP collections and requests, secrets will be replaced with a reference to a vault secret based on the detected key or token in lowercase, such as `{{vault:authorization-secret}}`.
- For all other Postman elements, secrets will be replaced with the detected key or token in uppercase with angle brackets around the text, such as `<AUTHORIZATION_SECRET>`.

Secrets exposed in multi-protocol collections won't be automatically replaced with placeholders. Secrets detected in multi-protocol collections must be removed or manually replaced with placeholders. Note that vault secrets aren't supported in multi-protocol collections.

> It's important that you also revoke exposed secrets the Secret Scanner detects.

To replace secrets detected during the Secret Scanner's regular scans, do the following:

1. In the email, in-app notification, or workspace settings, select **View Exposed Secrets** to open the Secret Scanner results in Postman.
2. In the Secret Scanner results, review the details for each exposed secret:
   - **Element name and location** - The name and location of the element type that has the exposed secret. You can select this to open the exposed secret in a new tab.
   - **Element type** - The element type that has the exposed secret.
   - **Secret value** - The partially masked value of the exposed secret.
   - **Secret name** - The authorization type of the exposed secret.
3. Select **Replace All Now** to replace each exposed secret in your public workspace with a placeholder. The syntax of the placeholder is based on the detected key or token and the Postman element it was found in.



Your workspace has exposed secrets

Please replace them with placeholder text and revoke access. If secrets remain after Nov 29, 2024, the workspace may be restricted, or secrets may be automatically replaced with placeholder values, which cannot be undone.

Secret Scanner results

Scan completed on Today, 7:16 AM

Postman API/Authorization Collection	PMAK-[redacted] ****** Authorization Secret

> You can also remove or replace each secret one at a time. Select the element name and location for each exposed secret to open it in a new tab. Remove each exposed secret, or replace each value with a placeholder that's relevant to your API.

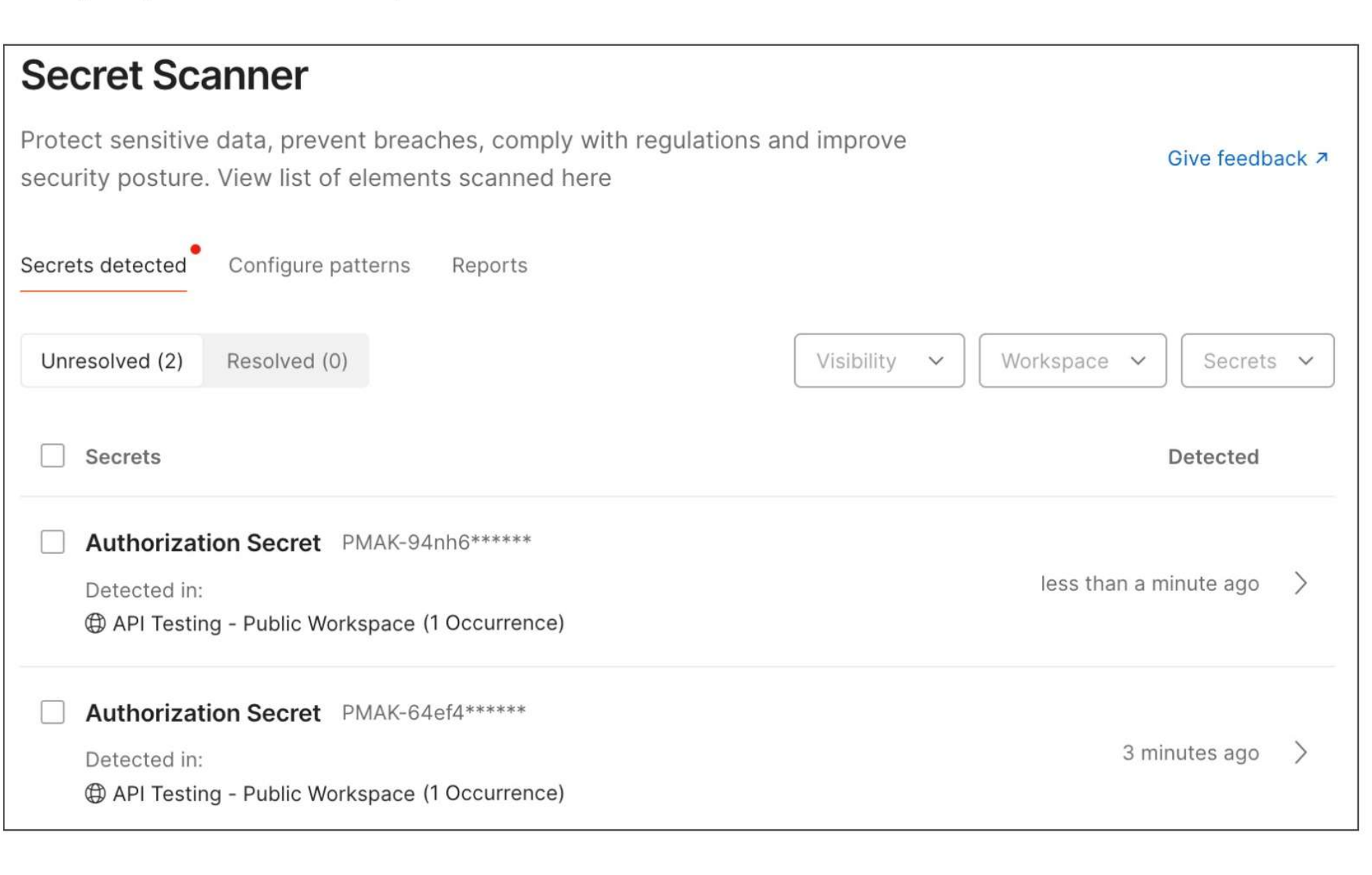
Secret Scanner dashboard

> The Secret Scanner dashboard is available with Postman Enterprise plans. Secret Scanner reports are available with the Enterprise plan with the Advanced Security Administration add-on.

Team Admins and Super Admins can view detected secrets, configure default and custom patterns, and review Secret Scanner reports in the Secret Scanner dashboard. To open the dashboard, select **Team > Team Settings** in the Postman header. Then, select **Secret Scanner** in the left sidebar.

By default, Secret Scanner scans public workspaces to detect and replace exposed secrets.

If you're on the Enterprise plan with the Advanced Security Administration add-on, Secret Scanner also monitors collections, API specifications, and documentation in your internal workspaces and Partner Workspaces. The Secret Scanner also scans the initial values of environment and global variables in Partner Workspaces. With the add-on, Secret Scanner delivers results for public workspace, internal workspace, and Partner Workspace scans in Secret Scanner dashboard.



Secret Scanner

Protect sensitive data, prevent breaches, comply with regulations and improve security posture. View list of elements scanned here

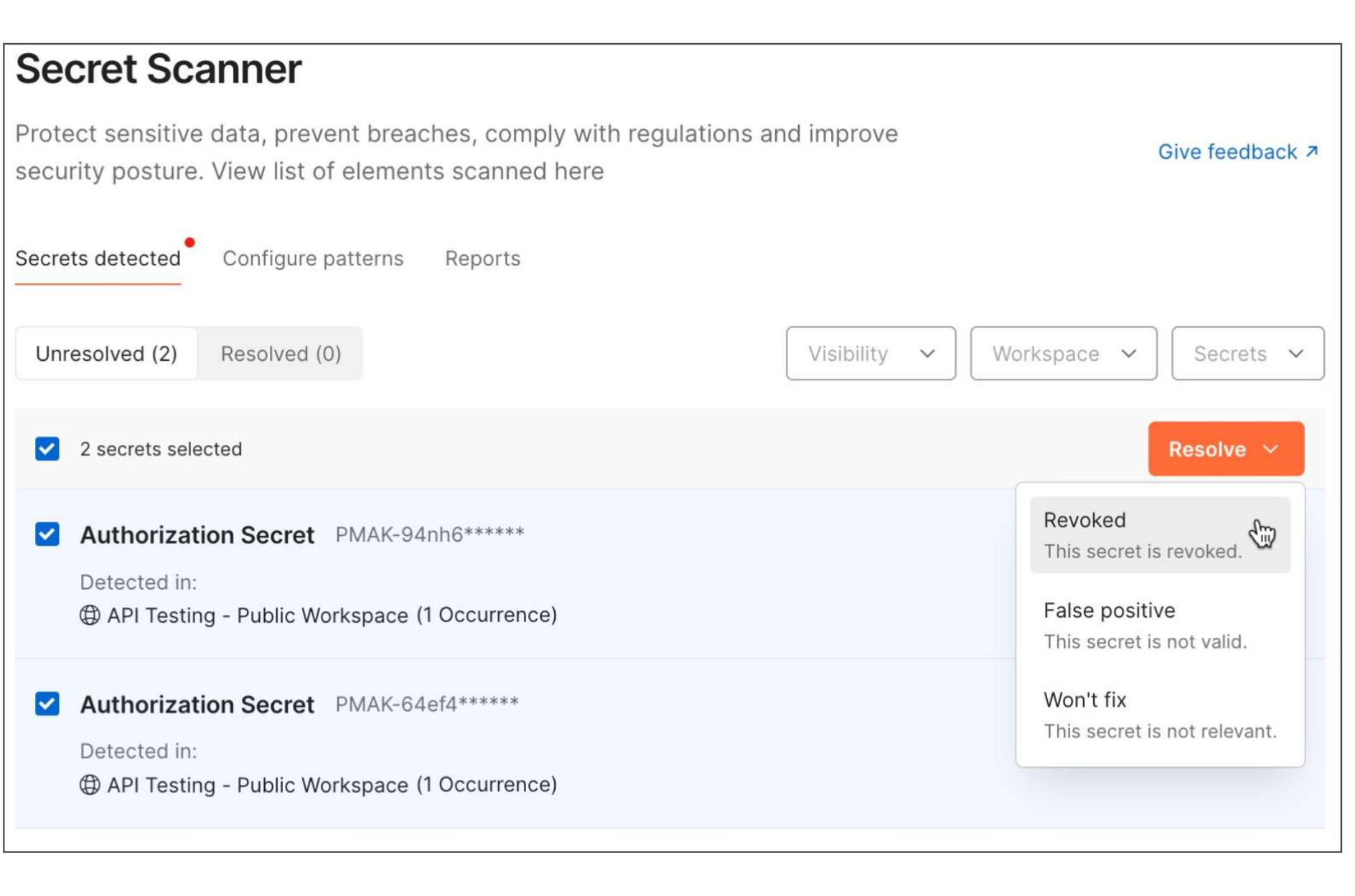
☐ Secrets	Detected
☐ **Authorization Secret** PMAK-94nh6****** Detected in: API Testing - Public Workspace (1 Occurrence)	less than a minute ago
☐ **Authorization Secret** PMAK-64ef4****** Detected in: API Testing - Public Workspace (1 Occurrence)	3 minutes ago

Resolve detected secrets

Team Admins and Super Admins can review the default and custom secrets that the Secret Scanner has found in the **Secrets detected** tab of the Secret Scanner dashboard. From the **Unresolved** tab, you can bulk resolve detected secrets, or you can select a detected secret to view details and resolve it. Filter findings by visibility type, workspace name, and secret type.

> Admins and Super Admins can access all identified secrets within a team, including ones in public workspaces. Workspace Admins can also view secrets within the workspaces they manage.

To bulk resolve detected secrets with the same status, select the checkbox next to each detected secret. You can also select the checkbox next to **Secrets** to select all detected secrets on the page. Select **Resolve** and then select a status to resolve the secrets.



Secret Scanner

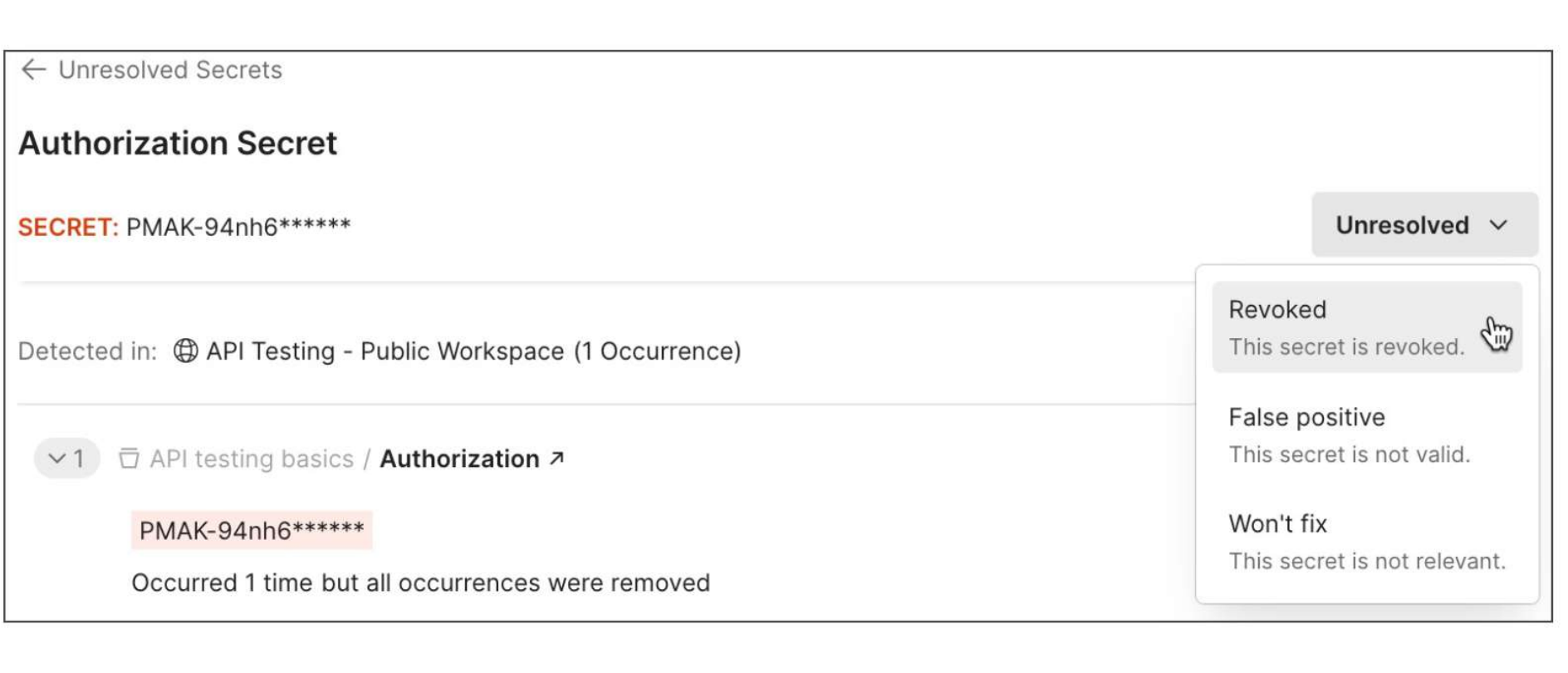
Protect sensitive data, prevent breaches, comply with regulations and improve security posture. View list of elements scanned here

☑ 2 secrets selected

☑ **Authorization Secret** PMAK-94nh6******
Detected in:
API Testing - Public Workspace (1 Occurrence)

☑ **Authorization Secret** PMAK-64ef4******
Detected in:
API Testing - Public Workspace (1 Occurrence)

You can also select a detected secret to view more details and resolve it. Each detected secret shows where it was found and when it was detected. To view the SHA256 hash value of a detected secret, hover over the partially hidden value and select ⓘ **Secret Details**. To resolve the secret, select **Unresolved** and then select a status.



Authorization Secret

SECRET: PMAK-94nh6******

Detected in: API Testing - Public Workspace (1 Occurrence)

1 API testing basics / **Authorization** ↗

PMAK-94nh6******

Occurred 1 time but all occurrences were removed

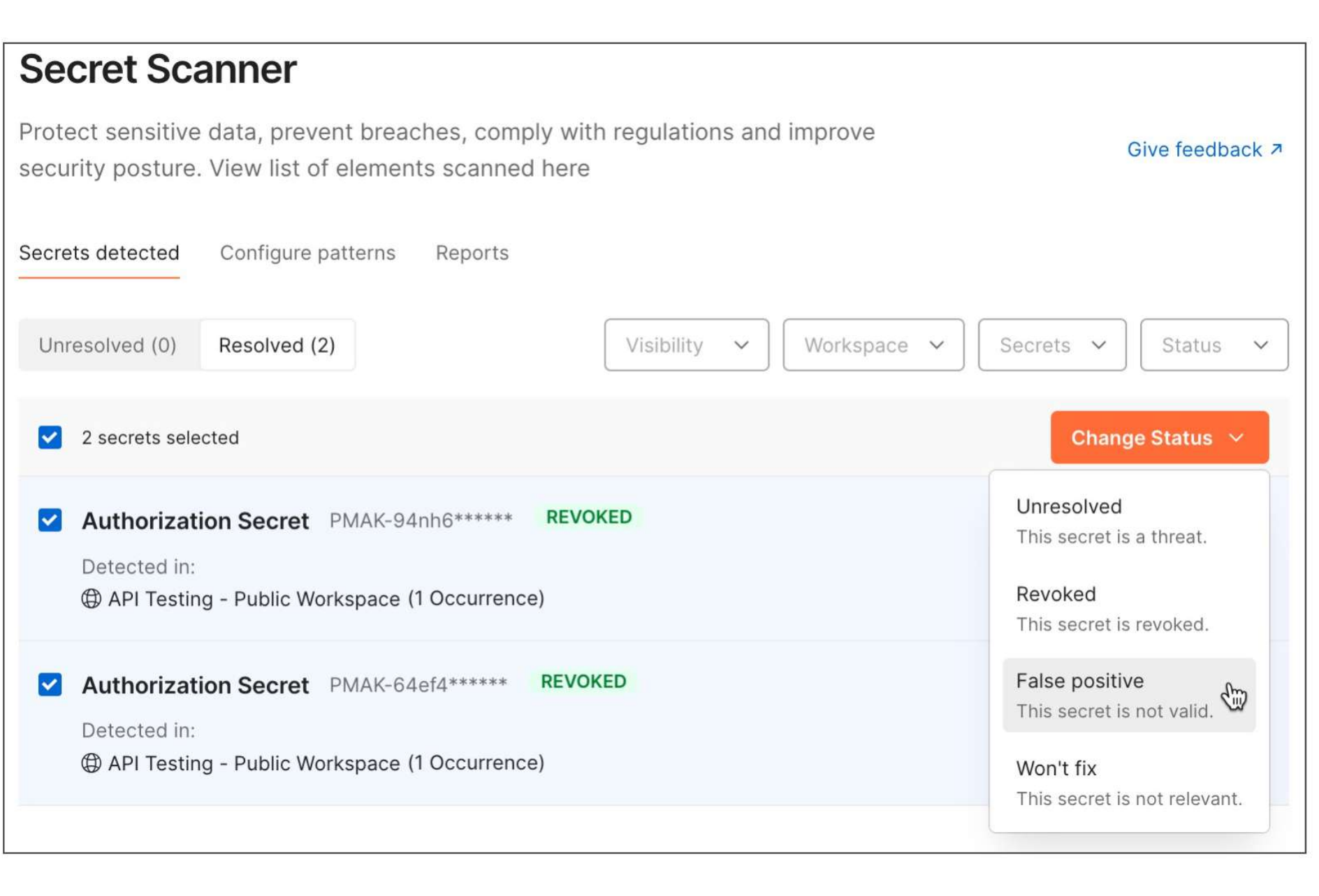
You can resolve a detected secret with the following statuses:

- **Revoked** - This secret has been revoked.
- **False positive** - This secret isn't valid.
- **Won't fix** - This secret isn't relevant.

Change the status of resolved detected secrets

After you resolve a detected secret, Team and Super Admins can change the status of a resolved secret. From the **Resolved** tab, you can bulk change the status of resolved secrets, or you can select a resolved secret to view details and change its status. You can also unresolve a secret if Team and Super Admins need to review it again. Filter findings by visibility type, workspace name, secret type, and status type.

To bulk change resolved detected secrets to the same status, select the checkbox next to each resolved detected secret. You can also select the checkbox next to **Secrets** to select all resolved detected secrets on the page. Select **Change Status** and then select a different status to resolve the secrets.



Secret Scanner

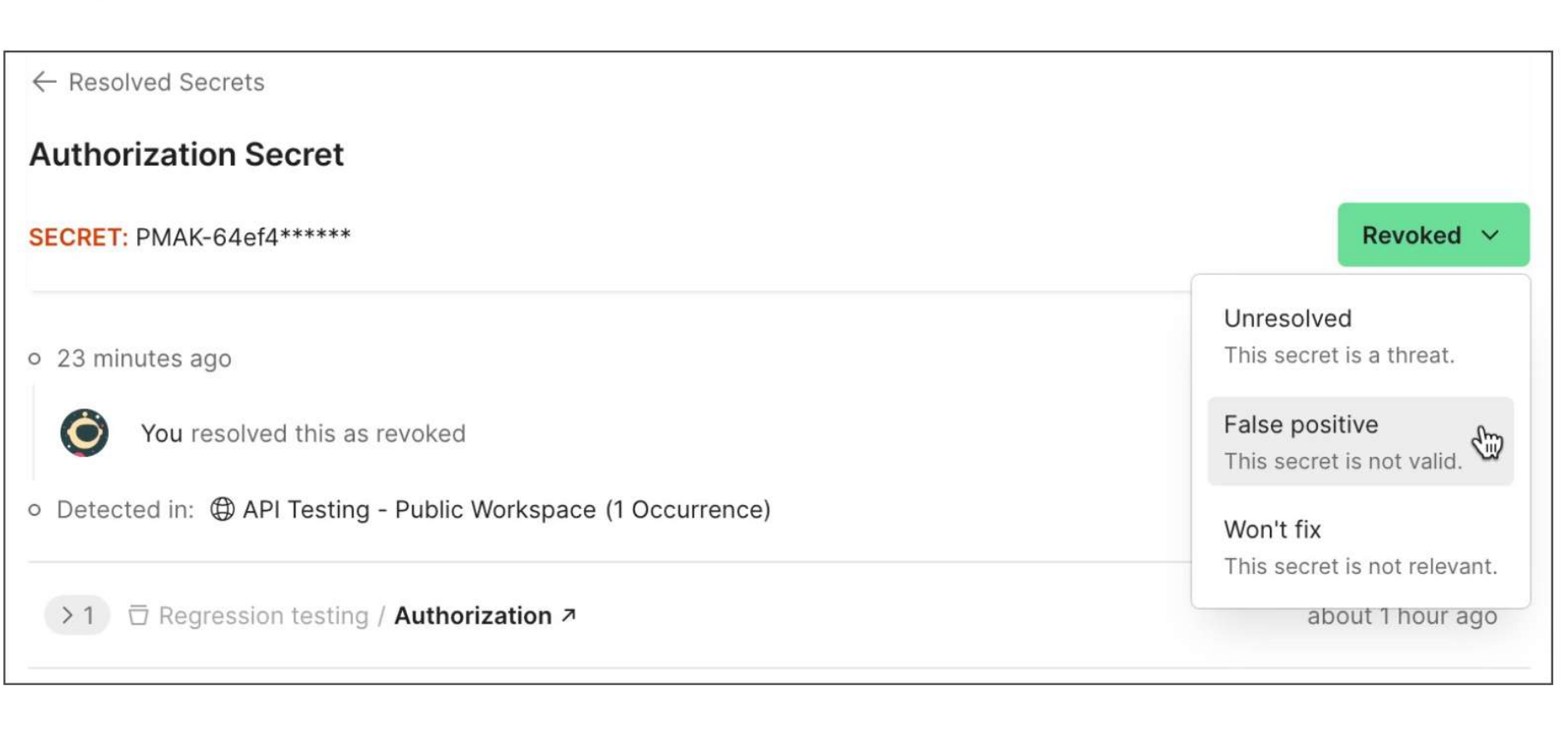
Protect sensitive data, prevent breaches, comply with regulations and improve security posture. View list of elements scanned here

☑ 2 secrets selected

☑ **Authorization Secret** PMAK-94nh6****** REVOKED
Detected in:
API Testing - Public Workspace (1 Occurrence)

☑ **Authorization Secret** PMAK-64ef4****** REVOKED
Detected in:
API Testing - Public Workspace (1 Occurrence)

You can also select a resolved detected secret to view more details and change its status. Each detected secret shows where it was found and when it was detected. To view the SHA256 hash value of a detected secret, hover over the partially hidden value and select ⓘ **Secret Details**. To change the resolved secret's status, select the status chosen earlier and then select a different status.



Authorization Secret

SECRET: PMAK-64ef4******

23 minutes ago

You resolved this as revoked

Detected in: API Testing - Public Workspace (1 Occurrence)

1 Regression testing / **Authorization** ↗

You can select **Unresolved** instead of changing the status for the detected secret. This moves the detected secret back to the **Unresolved** tab where Team and Super Admins can review and resolve the secret again.

Secret Scanner summary emails

Team Admins, Super Admins, and Workspace Admins can stay informed about Secret Scanner findings by subscribing to daily, weekly, or monthly summary emails. You'll receive the following based on your selections:

- A daily summary email every day at 12:00 AM UTC.
- A monthly summary email on the first of every month.
- A weekly summary email every Monday.

Navigate to Notification preferences or select your avatar in the Postman header, then select **Settings > Notifications** to view the Secret Scanner summary options. From there, you can select the box for either daily, weekly, or monthly summaries—or all—and save your preferences.

Manage Secret Scanner findings with the Postman API

> The Secret Scanner Postman API endpoints are available with the Postman Enterprise plan with the Advanced Security Administration add-on.

Team Admins, Super Admins, and Workspace Admins can access Secret Scanner findings through the Postman API. Using the Postman API enables you to create custom automated workflows to retrieve and resolve identified secrets. To learn more, see the Postman API documentation.

Supported secrets

The Secret Scanner searches for a variety of secrets by default. You can also add your team's proprietary third-party app tokens that aren't supported yet using custom patterns.

Default patterns

By default, the Secret Scanner checks for tokens issued by common service providers including Amazon, Google, GitHub, Stripe, and Twilio. To view the complete list of default patterns, open the Secret Scanner dashboard and select **Configure patterns**.

Custom patterns

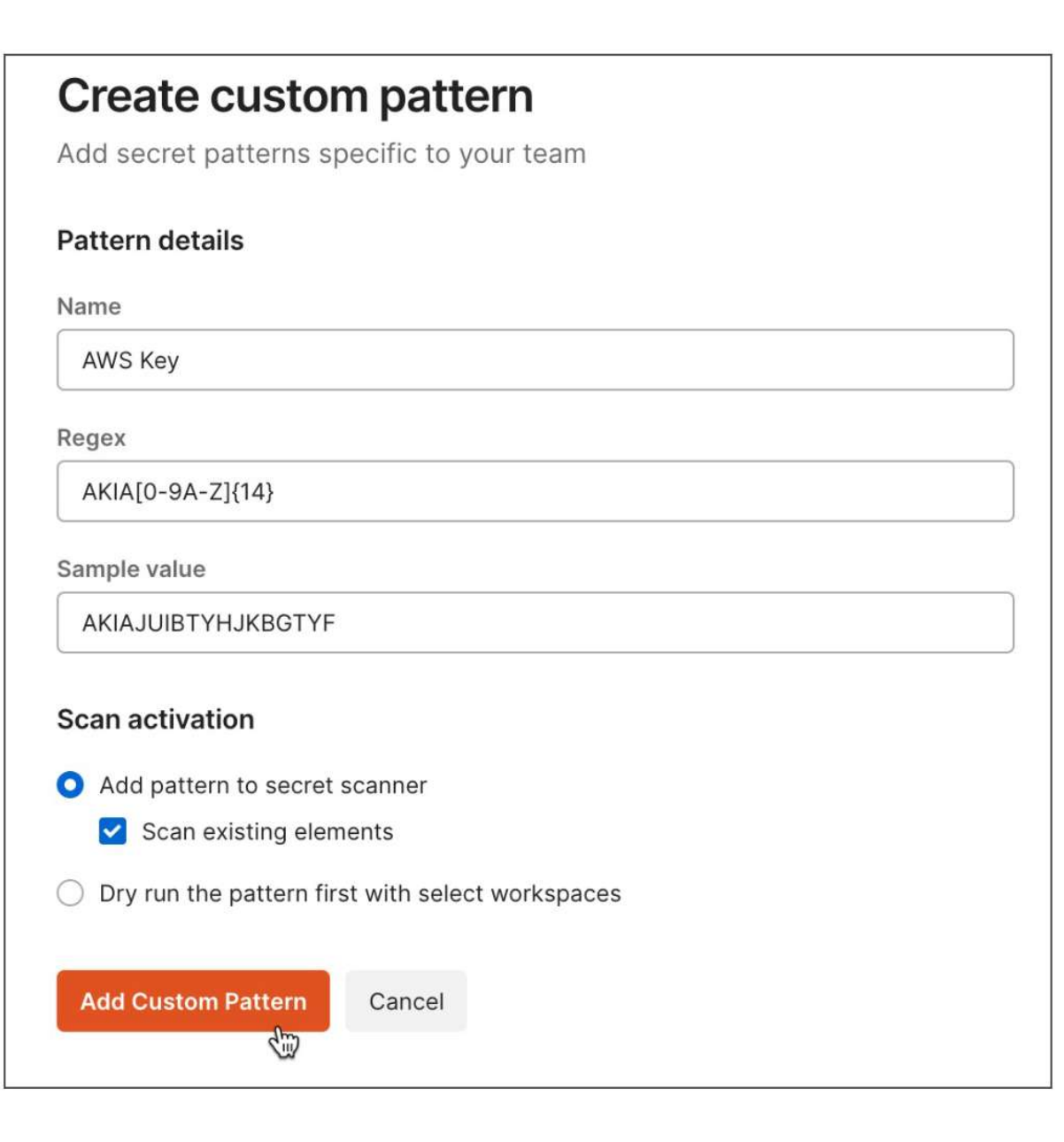
> Custom patterns are available with Postman Enterprise plans.

You can use custom patterns to scan your team's proprietary tokens and any third-party app tokens that aren't scanned by default. You can also dry run custom patterns before adding them to the Secret Scanner, enabling you to test the results that the custom pattern returns.

Your team can add a total of five patterns. You must be a Community Manager or team member with both Developer and Admin roles to add custom patterns.

To add custom patterns, do the following:

1. Open Postman and select **Team > Team Settings** in the Postman header. Select **Secret Scanner** in the left sidebar, then select the **Configure patterns** tab.
2. In the **Custom patterns** section, select + **Add**.
3. In the **Pattern details** section, add the following details for the custom token:
   - **Name** - The name of your custom pattern.
   - **Regex** - The regular expression that specifies the pattern of the secrets you want to find a match for.
   - **Sample value** - A sample value used to validate the regular expression pattern.
4. In the **Scan activation** section, select one of the following:
   - **Add pattern to secret scanner** - Add the secrets the Secret Scanner finds to the **Secrets detected** tab in the dashboard. By default, the **Scan existing elements** checkbox is selected, meaning the Secret Scanner will use the custom pattern to scan existing elements. If you'd like to only scan new elements, clear the **Scan existing elements** checkbox.
   - **Dry run the pattern first with select workspaces** - Dry run the custom pattern before adding it to the Secret Scanner. You can select up to 20 public workspaces, internal workspaces, or Partner Workspaces for the dry run. The results of the dry run won't be added to the **Secrets detected** tab in the dashboard. Learn more about creating a custom pattern dry run.
5. Select **Add Custom Pattern** or **Dry Run Pattern**, depending on the option you selected in the **Scan activation** section.



Create custom pattern

Add secret patterns specific to your team

Pattern details

Name: AWS Key

Regex: AKIA[0-9A-Z]{14}

Sample value: AKIAJUIBTYHJKBGTYF

Scan activation

● Add pattern to secret scanner

☑ Scan existing elements

○ Dry run the pattern first with select workspaces

To edit a custom pattern, select the edit icon ✎ next to a custom pattern. Edit the name or regular expression, update the sample value, then select **Save**. If you edited the regular expression, select one of the following to confirm your changes:

- **Keep Existing Leaks** - Show detected secrets in the **Secrets detected** tab that are associated with earlier iterations of this custom pattern.
- **Remove Existing Leaks** - Remove detected secrets from the **Secrets detected** tab that are associated with earlier iterations of this custom pattern.

> When you edit a regular expression in a custom pattern, the updated regular expression is used to scan new elements only. To scan existing elements with the changes to the pattern, create a new custom pattern and make sure the **Scan existing elements** checkbox is selected.

To delete a custom pattern, select the delete icon 🗑 next to a custom pattern. Then select **Delete** to confirm. When you delete a custom pattern, all detected secrets associated with this pattern will be removed from the **Secrets detected** tab in the dashboard.

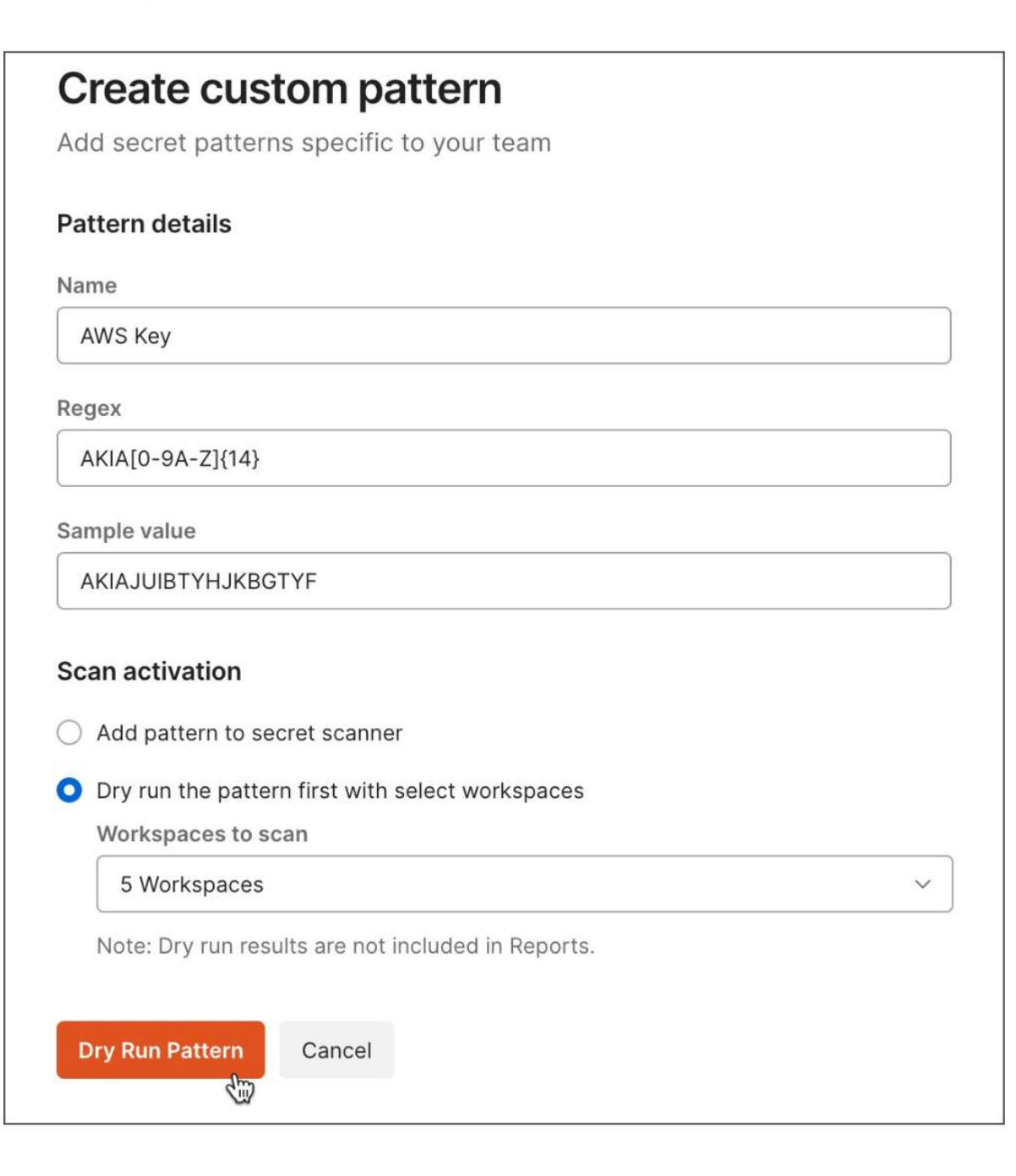
Dry run custom patterns

When you create a custom pattern, you can choose to dry run the regular expression pattern before adding it to the Secret Scanner. This enables you to test the results that the regular expression pattern returns. You can dry run the pattern on up to 20 public workspaces, internal workspaces, or Partner Workspaces. If the dry run works as expected, you can add the custom pattern to the Secret Scanner, enabling your team to review the results in your dashboard.

> The results of the dry run won't be added to the **Secrets detected** tab in the dashboard. You must manually add the custom pattern to the Secret Scanner.

To dry run a custom pattern, do the following:

1. Add a custom pattern, and select **Dry run the pattern first with select workspaces** in the **Scan activation** section.
2. Select public workspaces, internal workspaces, or Partner Workspaces to scan. You can select up to 20 workspaces.
3. Select **Dry Run Pattern**.



Create custom pattern

Add secret patterns specific to your team

Pattern details

Name: AWS Key

Regex: AKIA[0-9A-Z]{14}

Sample value: AKIAJUIBTYHJKBGTYF

Scan activation

○ Add pattern to secret scanner

● Dry run the pattern first with select workspaces

Workspaces to scan: 5 Workspaces

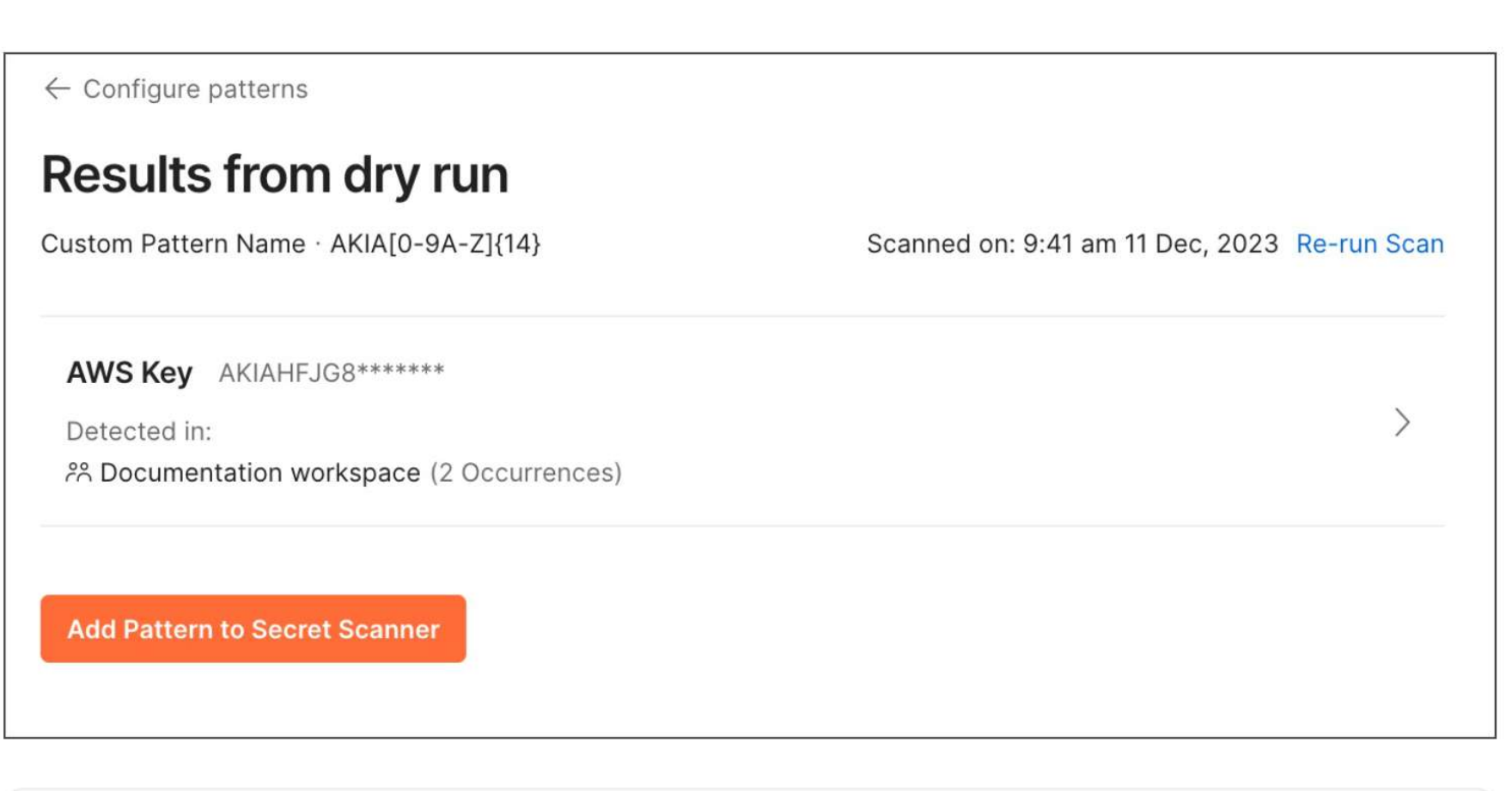
Note: Dry run results are not included in Reports.

To view the dry run results and add the custom pattern, do the following:

1. Select the **Configure patterns** tab.
2. In the **Custom patterns** section, select **View results** next to the custom pattern when the dry run is completed. You can select results from the dry run to view more details.

   > To run the dry run again, select **Re-run Scan** in the top right of **Results from dry run** page.

3. If the dry run performed as expected, you can add the custom pattern to the Secret Scanner, enabling you to view the results in the dashboard. In the **Results from dry run** page, select **Add Pattern to Secret Scanner**.



Results from dry run

Custom Pattern Name · AKIA[0-9A-Z]{14}

Scanned on: 9:41 am 11 Dec, 2023

AWS Key AKIAHFJG8*******

Detected in:

Documentation workspace (2 Occurrences)

> If you want to make changes to the dry run, select the delete icon 🗑 next to the custom pattern in the dashboard. Then add the custom pattern and dry run it with your changes.

4. To confirm, select one of the following:
   - **Ignore Existing Elements** - Scan only new elements with this custom pattern.
   - **Scan Existing Elements** - Scan new and existing elements with this custom pattern.

Protect Postman API keys in GitHub

Postman also works with GitHub to ensure that your Postman API keys are secure for free and paid Postman plans. If you commit a valid Postman API key to a public GitHub repository, Postman notifies you by email and in-app notification. You can also set up Postman's integration for Slack to alert you in Slack if this occurs.

It's recommended you delete the exposed API key in your API keys dashboard. You can then generate a new API key to continue working with the Postman API.

Protect Postman API keys in GitLab

> This feature is available with GitLab Ultimate plans.

Postman works with GitLab to protect your Postman API keys in GitLab public repositories for free and paid Postman plans. If you accidentally commit a valid Postman API key to a public GitLab repository, Postman notifies you by email and in-app notification.

It's recommended you delete the exposed API key in your API keys dashboard immediately. You can then generate a new API key to continue working with the Postman API.

Last modified: 2025/04/17

← Manage API keys
BYOK Encryption →