Manage vulnerability exceptions

- Create exceptions
- View exceptions
  - View exceptions in Docker Scout Dashboard or Docker Desktop
  - View exceptions in the CLI

Vulnerabilities found in container images sometimes need additional context. Just because an image contains a vulnerable package, it doesn't mean that the vulnerability is exploitable. **Exceptions** in Docker Scout lets you acknowledge accepted risks or address false positives in image analysis.

By negating non-applicable vulnerabilities, you can make it easier for yourself and downstream consumers of your images to understand the security implications of a vulnerability in the context of an image.

In Docker Scout, exceptions are automatically factored into the results. If an image contains an exception that flags a CVE as non-applicable, then that CVE is excluded from analysis results.

Create exceptions

To create an exception for an image, you can:

- Create an exception in the GUI of Docker Scout Dashboard or Docker Desktop.
- Create a VEX document and attach it to the image.

The recommended way to create exceptions is to use Docker Scout Dashboard or Docker Desktop. The GUI provides a user-friendly interface for creating exceptions. It also lets you create exceptions for multiple images, or your entire organization, all at once.

View exceptions

To view exceptions for images, you need to have the appropriate permissions.

- Exceptions created using the GUI are visible to members of your Docker organization. Unauthenticated users or users who aren't members of your organization cannot see these exceptions.
- Exceptions created using VEX documents are visible to anyone who can pull the image, since the VEX document is stored in the image manifest or on filesystem of the image.

View exceptions in Docker Scout Dashboard or Docker Desktop

The **Exceptions** tab of the Vulnerabilities page in Docker Scout Dashboard lists all exceptions for for all images in your organization. From here, you can see more details about each exception, the CVEs being suppressed, the images that exceptions apply to, the type of exception and how it was created, and more.

For exceptions created using the GUI, selecting the action menu lets you edit or remove the exception.

To view all exceptions for a specific image tag:

{{< tabs >}} {{< tab name="Docker Scout Dashboard" >}}

1. Go to the Images page.
2. Select the tag that you want to inspect.
3. Open the **Exceptions** tab.

{{< /tab >}} {{< tab name="Docker Desktop" >}}

1. Open the **Images** view in Docker Desktop.
2. Open the **Hub** tab.
3. Select the tag you want to inspect.
4. Open the **Exceptions** tab.

{{< /tab >}} {{< /tabs >}}

View exceptions in the CLI

{{< summary-bar feature_name="Docker Scout exceptions" >}}

Vulnerability exceptions are highlighted in the CLI when you run `docker scout cves <image>`. If a CVE is suppressed by an exception, a `SUPPRESSED` label appears next to the CVE ID. Details about the exception are also displayed.

> [!IMPORTANT] In order to view exceptions in the CLI, you must configure the CLI to use the same Docker organization that you used to create the exceptions.
>
> To configure an organization for the CLI, run:
>
> ```
> $ docker scout configure organization <organization>
> ```
>
> Replace `<organization>` with the name of your Docker organization.
>
> You can also set the organization on a per-command basis by using the `--org` flag:
>
> ```
> $ docker scout cves --org <organization> <image>
> ```

To exclude suppressed CVEs from the output, use the `--ignore-suppressed` flag:

```
$ docker scout cves --ignore-suppressed <image>
```

□□□ #2
□ □□□ □□□ 2026-10-31 19:36:14 UTC
□ □□□ □□□ 2026-10-31 19:36:15 UTC