Create an exception using the GUI

- Prerequisites
- Steps

The Docker Scout Dashboard and Docker Desktop provide a user-friendly interface for creating exceptions for vulnerabilities found in container images. Exceptions let you acknowledge accepted risks or address false positives in image analysis.

Prerequisites

To create an in the Docker Scout Dashboard or Docker Desktop, you need a Docker account with **Editor** or **Owner** permissions for the Docker organization that owns the image.

Steps

To create an exception for a vulnerability in an image using the Docker Scout Dashboard or Docker Desktop:

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

1. Go to the Images page.
2. Select the image tag that contains the vulnerability you want to create an exception for.
3. Open the **Image layers** tab.
4. Select the layer that contains the vulnerability you want to create an exception for.
5. In the **Vulnerabilities** tab, find the vulnerability you want to create an exception for. Vulnerabilities are grouped by package. Find the package that contains the vulnerability you want to create an exception for, and then expand the package.
6. Select the **Create exception** button next to the vulnerability.

{{% create_panel.inline %}} Selecting the **Create exception** button opens the **Create exception** side panel. In this panel, you can provide the details of the exception:

- **Exception type**: The type of exception. The only supported types are:
  - **Accepted risk**: The vulnerability is not addressed due to its minimal security risk, high remediation costs, dependence on an upstream fix, or similar.
  - **False positive**: The vulnerability presents no security risk in your specific use case, configuration, or because of measures in place that block exploitation
    If you select **False positive**, you must provide a justification for why the vulnerability is a false positive:
- **Additional details**: Any additional information that you want to provide about the exception.
- **Scope**: The scope of the exception. The scope can be:
  - **Image**: The exception applies to the selected image.
  - **All images in repository**: The exception applies to all images in the repository.
  - **Specific repository**: The exception applies to all images in the specified repositories.
  - **All images in my organization**: The exception applies to all images in your organization.
- **Package scope**: The scope of the exception. The package scope can be:
  - **Selected package**: The exception applies to the selected package.
  - **Any packages**: The exception applies to all packages vulnerable to this CVE.

When you've filled in the details, select the **Create** button to create the exception.

The exception is now created and factored into the analysis results for the images that you selected. The exception is also listed on the **Exceptions** tab of the Vulnerabilities page in the Docker Scout Dashboard.

{{% /create_panel.inline %}}

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

1. Open the **Images** view in Docker Desktop.
2. Open the **Hub** tab.
3. Select the image tag that contains the vulnerability you want to create an exception for.
4. Select the layer that contains the vulnerability you want to create an exception for.
5. In the **Vulnerabilities** tab, find the vulnerability you want to create an exception for.
6. Select the **Create exception** button next to the vulnerability.

{{% create_panel.inline / %}}

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

□□□ #2
□ □□□ □□□ 2026-10-31 19:36:37 UTC
□ □□□ □□□ 2026-10-31 19:36:38 UTC