**Docker Scout**



Docker Scout is an advanced image analysis by docker (Deprecating docker scan). As you may already know, images are made up of many layers stacked together. The software packages embedded in the layers might have weaknesses that could make your image vulnerable to attacks.

Imagine Docker Scout as a smart detective for your container images! It carefully checks every part of your Docker pictures to find any weak spots that could be risky. By spotting these problems early on, Docker Scout helps you make your apps stronger and safer from online dangers. It's like having a guardian that keeps your containers safe by finding and fixing problems before they cause trouble.

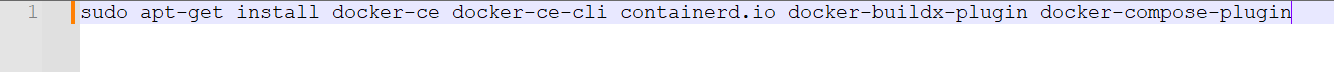
Docker Scout can proactively help you find and fix these vulnerabilities, helping you create a more secure software supply chain. It does this by analysing your images and creating a full inventory of the packages and layers

called a It then correlates this

[Software bill of materials (SBOM)open\_in\_new](https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf).

inventory with a continuously updated vulnerability database to identify vulnerabilities in your images.

Scout Workflow



[Docker Scout quickstart](https://docs.docker.com/scout/quickstart/)

**Docker CLI**

https://docs.docker.com/engine/install/ubuntu/

**Docker Installation**

**Install Docker**

|  |  |  |
| --- | --- | --- |
| <https://docs.docker.com/scout/image-analysis/> | | |
| **Note** |  | |
| You must have the **Editor** or **Owner** role in the Docker organization to activate image analysis on a repository.  **Login to docker** | | |
| A white and purple rectangle  Description automatically generated | |  |
| There is a 3 GB size limit on images analyzed by Docker Scout in Docker Desktop.  To install Scout plugin on Instance | | |
|  | | |
| **Note** |  | |
| Always examine scripts downloaded from the internet before running them locally. Before installing, make yourself familiar with potential risks and limitations of the convenience script.    To See Docker scout manual | | |

|  |  |  |
| --- | --- | --- |
| A screenshot of a computer  Description automatically generated | | |
| **[Quickview](https://docs.docker.com/scout/image-analysis/" \l "quickview)** |  | |
| The docker scout quickview command provides an overview of the vulnerabilities found in a given image and its base image. | | |
| A close-up of a computer screen  Description automatically generated | |  |
| Example: | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A screenshot of a computer  Description automatically generated  If your the base image is out of date, the quickview command also shows how updating your base image would change the vulnerability exposure of your image. | | | | |
| **[CVEs](https://docs.docker.com/scout/image-analysis/" \l "cves)** |  | | | |
|  | | | | |
| The Common Vulnerabilities and Exposures (CVE) system provides a reference | | |  | |
| method for publicly known information-security vulnerabilities and exposures. | | | |  |
| The docker scout cves command gives you a complete view of all the vulnerabilities in the image. | | | | |
| A close-up of a word  Description automatically generated | |  | | |
| Example | | | | |



It provides us with the vulnerability ID, affected versions, and fixed version, enabling us to take appropriate measures to mitigate this vulnerability.

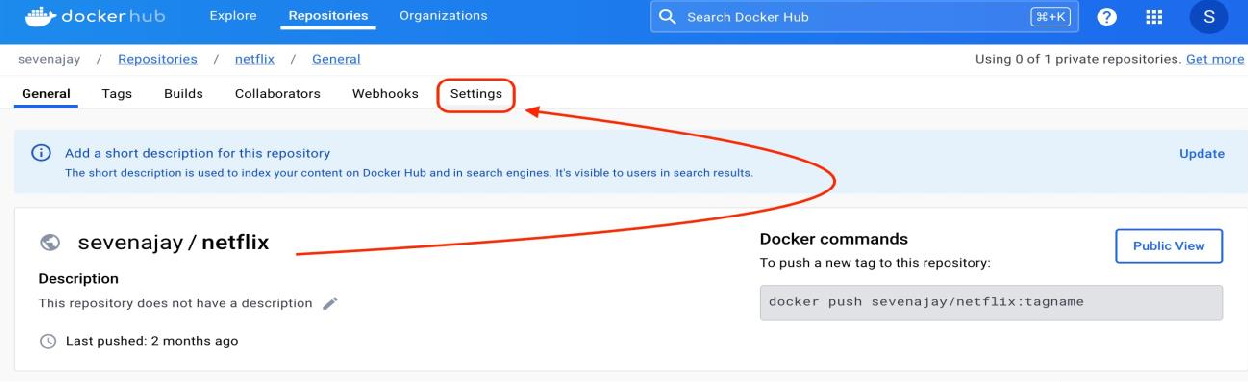
Report in Simple

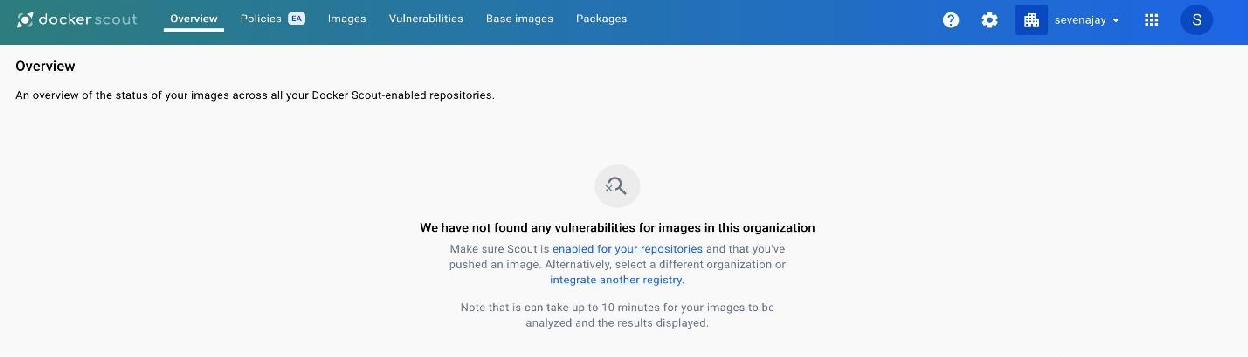
|  |  |  |
| --- | --- | --- |
| This command supports several flags that lets you specify more precisely which vulnerabilities you're interested in, for example, by severity or package type | | |
|  | |  |
| Example | | |
| A screenshot of a computer  Description automatically generated | | |
| Sample    A screenshot of a computer  Description automatically generated  The vulnerabilities in your base image should be aware of and not overlooked. Scout can also help us in this case with the command **docker scout** | | |
| **reccomendations.** |  | |
| A close-up of a computer screen  Description automatically generated | | |

|  |  |
| --- | --- |
| Sample | |
| A close-up of a sign  Description automatically generated |  |
| A computer screen with text and numbers  Description automatically generated  **Docker GUI** | |

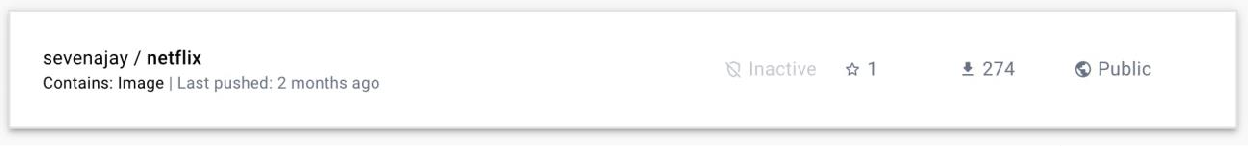
* If you're using Docker Desktop version 4.14 or above, Docker Scout is already installed and readily available.
* This is the simplest and most recommended method for most users.
* Login to Docker hub
* Click on Docker scout

Click On profile beside like in below image

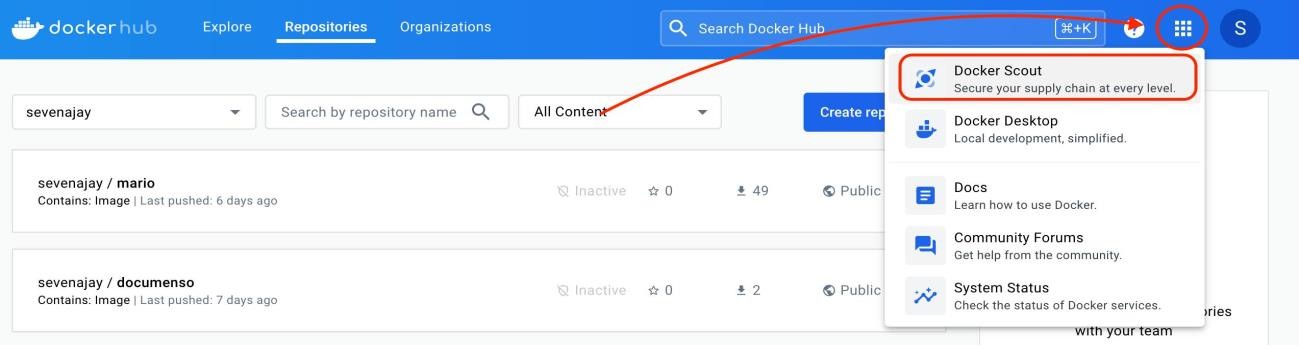










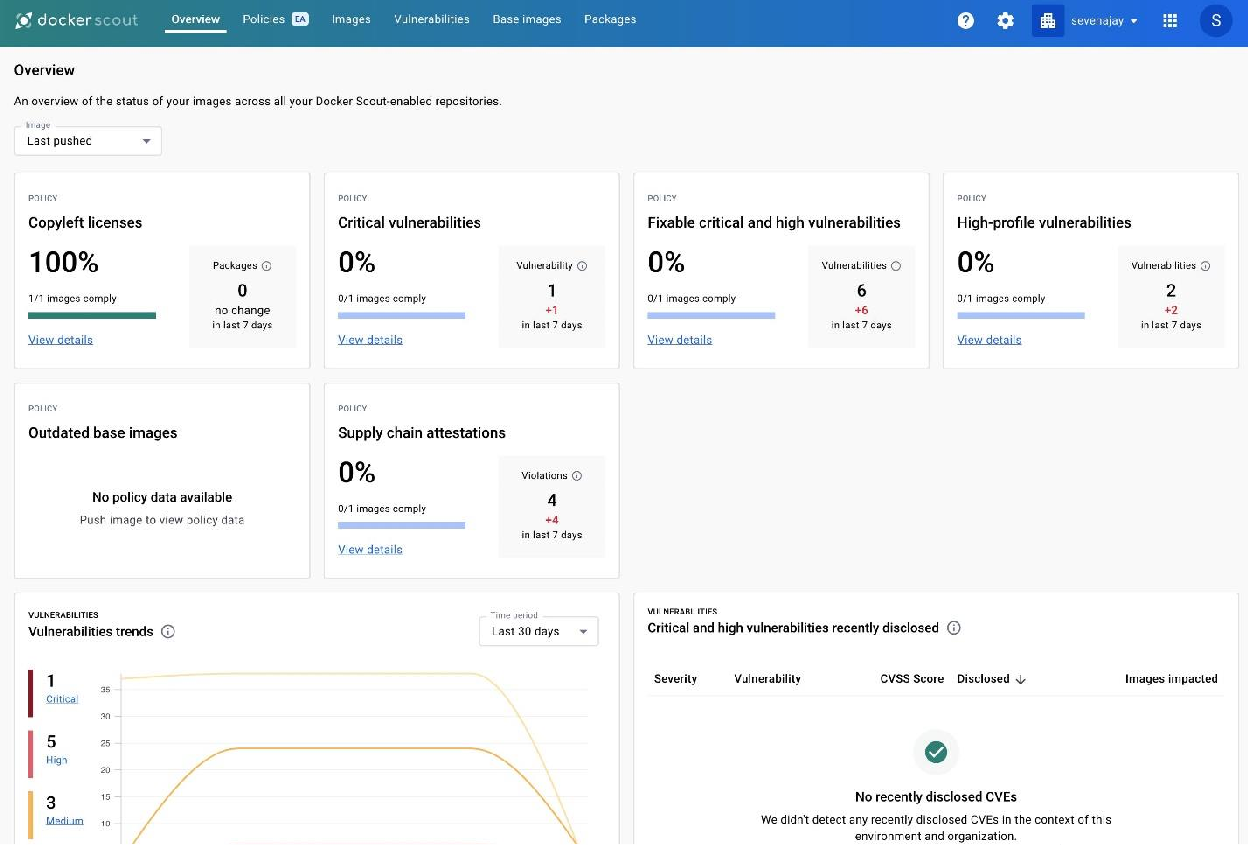


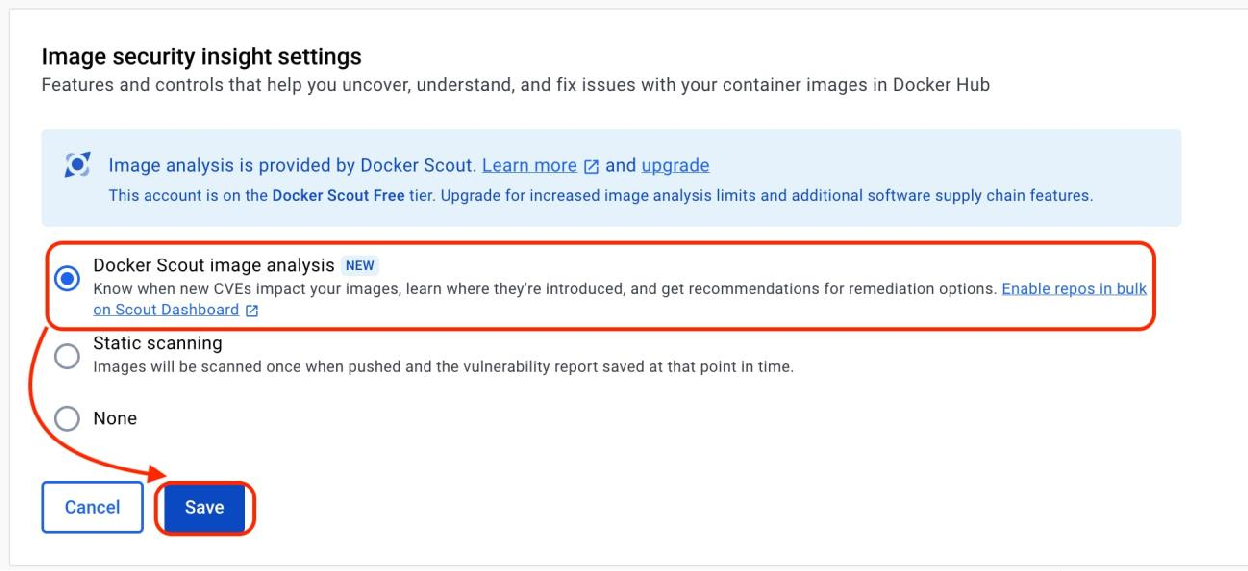
You will see page like this (As of now we dont have any images added to docker scout)

Let's Add some images to see the report, come back to docker- hub again

Iam selecting my netflix image to scout

Now click on settings



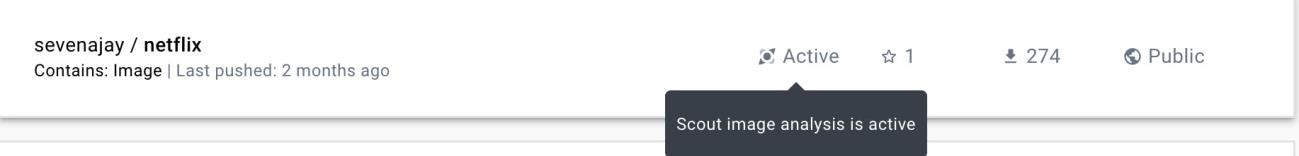




Now select Radio box of Docker scout and click on save.

Again, go back to Docker scout from hub

You will see image report and analysis like this



You can see scout is active for netflix image in Docker hub

Done.

|  |  |  |  |
| --- | --- | --- | --- |
| **Integrating Docker Scout with other systems** | | |  |
| By default, Docker Scout integrates with your Docker organization and your Docker Scout-enabled repositories on Docker Hub. You can integrate Docker Scout with additional third-party systems to get access to even more insights, including real-time information about you running workloads. | | | |
| **[Integration categories](https://docs.docker.com/scout/integrations/" \l "integration-categories)** | |  | |
| You'll get different insights depending on where and how you choose to integrate Docker Scout. | | | |
| **[Container registries](https://docs.docker.com/scout/integrations/" \l "container-registries)** |  | | |
| Integrating Docker Scout with third-party container registries enables Docker Scout to run image analysis on those repositories, so that you can get insights into the composition of those images even if they aren't hosted on Docker Hub.  The following container registry integrations are available: | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|      | [Artifactory](https://docs.docker.com/scout/integrations/registry/artifactory/) |  | | | | |
| [Amazon Elastic Container Registry](https://docs.docker.com/scout/integrations/registry/ecr/) | | | | |  |
| [Azure Container Registry](https://docs.docker.com/scout/integrations/registry/acr/) | |  | **Beta** |  | |

**[Continuous Integration](https://docs.docker.com/scout/integrations/" \l "continuous-integration)**

Integrating Docker Scout with Continuous Integration (CI) systems is a great way to get instant, automatic feedback about your security posture in your inner loop. Analysis running in CI also gets the benefit of additional context that's useful for getting even more insights.

The following CI integrations are available:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|          | [GitHub Actions](https://docs.docker.com/scout/integrations/ci/gha/) | | | |  | |
| [GitLab](https://docs.docker.com/scout/integrations/ci/gitlab/) |  | | | | |
| [Microsoft Azure DevOps Pipelines](https://docs.docker.com/scout/integrations/ci/azure/) | | | | |  |
| [Circle CI](https://docs.docker.com/scout/integrations/ci/circle-ci/) | | |  | | |
| [Jenkins](https://docs.docker.com/scout/integrations/ci/jenkins/) | |  | | | |

|  |  |  |
| --- | --- | --- |
| **[Environment monitoring](https://docs.docker.com/scout/integrations/" \l "environment-monitoring)** | |  |
| Environment monitoring refers to integrating Docker Scout with your deployments. This can give you information in realtime about your running container workloads.  Integrating with environments lets you compare production workloads to other versions, in your image repositories or in your other environments.  For more information about environment integrations, see [Environments.](https://docs.docker.com/scout/integrations/environment/) | | |
| **[Code quality](https://docs.docker.com/scout/integrations/" \l "code-quality)** |  | |
| Integrating Docker Scout with code analysis tools enables quality checks directly on source code, helping you keep track of bugs, security issues, test coverage, and more. In addition to image analysis and environment monitoring, code quality gates let you shift left your supply chain management with Docker Scout.  Once you enable a code quality integration, Docker Scout includes the code quality assessments as policy evaluation results for the repositories where you've enabled the integration.  The following code quality integrations are available: | | |

|  |  |  |
| --- | --- | --- |
|  | [SonarQube](https://docs.docker.com/scout/integrations/code-quality/sonarqube/) |  |

|  |  |
| --- | --- |
| **Overview for multiple images** | |
| **Benefits of using Docker Scout:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Enhanced security:** | Docker Scout helps you proactively identify and |
| address vulnerabilities in your images, mitigating security risks and preventing potential exploits.   * **Improved efficiency:** By automating vulnerability scanning, Docker Scout saves you time and effort compared to manual processes. * **Greater transparency:** Gain detailed information about the dependencies within your images, allowing for better understanding and control. * **Seamless integration:** Docker Scout integrates seamlessly with Docker Desktop, making it readily accessible and easy to use. | | |

|  |  |  |
| --- | --- | --- |
|  | **Understanding the reports:** |  |

After scanning, Docker Scout generates a detailed report that includes:

|  |  |  |
| --- | --- | --- |
|  | **Vulnerability details:** | Information about identified vulnerabilities, |
| such as their severity, CVSS score, affected packages, and historical references.   * **Dependency list:** A breakdown of all libraries and packages used within the image, including their versions and historical dependencies. * **Actionable recommendations:** Guidance on how to address   vulnerabilities and improve your image security, including historical patches and mitigation strategies. | | |

|  |  |
| --- | --- |
| **Advanced features:** |  |
| Docker Scout also offers several advanced features, including: | |

|  |  |  |
| --- | --- | --- |
|  | **Policy creation:** | Define custom rules and checks to ensure your image |
| adheres to specific security standards and historical guidelines.   * **Integration with CI/CD pipelines:** Automate vulnerability scanning within your development workflow for continuous monitoring. * **Vulnerability prioritization:** Focus on addressing the most critical vulnerabilities first based on historical risk assessments. | | |

|  |  |  |
| --- | --- | --- |
|  | **Conclusion:** |  |
| Docker Scout is a valuable tool for enhancing the security and reliability of your containerized applications. By leveraging its vulnerability scanning and dependency analysis capabilities, you can gain insights into your images, identify potential risks, and make informed decisions  about how to secure your software. | | |