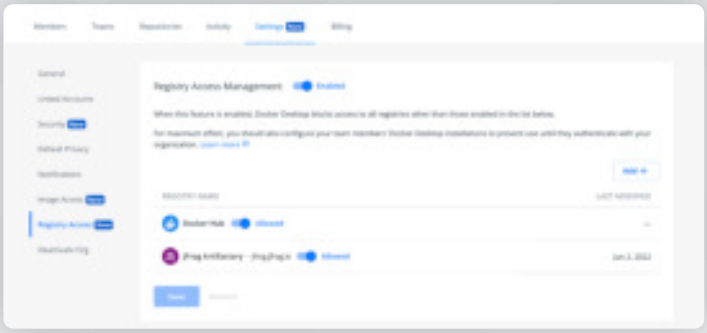
Registry Access Management with JFrog Artifactory

Reduce security risks through greater registry control

Registry Access Management for Docker Business gives organizations greater control over the registries their developers can access while using Docker Desktop. New registries can be spun up quickly, providing a way for developers to potentially pull malicious software or push sensitive data and intellectual property. When enabled, Registry Access Management can reduce the security risks associated with using public registries by ensuring that developers only access trusted registries such as a private registry on Artifactory.

JFrog Artifactory is a scalable, universal, binary repository manager that automatically manages your artifacts and dependencies throughout the application development and delivery process, it plays a central role in managing and automating your DevOps CI/CD pipeline. Using Artifactory to manage binaries enables software teams to collaborate with the same coherent and consistent set of binaries and dependencies through all phases of the development cycle.



Easy to enable

Protect your organization by restricting registry access through centralized controls via Docker Hub.

Improves productivity

Avoid setting firewalls and other overly restrictive mechanisms that can slow developer productivity.

Better visibility

Gain better visibility into your organization's registry access policy and clearer notifications when accessing barred registries.

Centralized controls make it easier for admins to manage their registries

Organization owners can set registry access policies through centralized controls on Docker Hub.

- Search, display, and add new registries in a single view.
- Set which registries developers can access while using Docker Desktop by simply toggling on and off each listed registry.
- Developers who try to access the affected registry on Docker Desktop will receive clear notifications that the registry is blocked by their organization.

For more information and best practices, check out our docs page.

A more secure developer experience without the compromise

By enabling both Registry Access Management and Image Access Management, organizations can have greater security over their Docker workflows. This empowers developers to do their best work with the confidence that the registries and images they use are compliant with their organization's policies. The result is a more secure developer experience that doesn't compromise on productivity, speed, or choice.

Registry Access Management is available to organizations with an active Docker Business subscription. Click here to learn more about how Docker Business supercharges developer productivity and collaboration without compromising on security and compliance.