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.

www.docker.com