Secure Engine

Estimated reading time: 1 minute

This section discusses the security features you can configure and use within your Docker Engine installation.

- You can configure Docker's trust features so that your users can push and pull trusted images. To learn how to do this, see Use trusted images (https://docs.docker.com/engine/security/trust/) in this section.
- You can protect the Docker daemon socket and ensure only trusted Docker client connections. For more information, Protect the Docker daemon socket (https://docs.docker.com/engine/security/https/)
- You can use certificate-based client-server authentication to verify a Docker daemon has the rights to access images on a registry. For more information, see Using certificates for repository client verification (https://docs.docker.com/engine/security/certificates/).
- You can configure secure computing mode (Seccomp) policies to secure system calls in a container. For more information, see Seccomp security profiles for Docker (https://docs.docker.com/engine/security/seccomp/).
- An AppArmor profile for Docker is installed with the official *.deb* packages. For information about this profile and overriding it, see AppArmor security profiles for Docker (https://docs.docker.com/engine/security/apparmor/).

seccomp (https://docs.docker.com/glossary/?term=seccomp), security (https://docs.docker.com/glossary/?term=security), docker (https://docs.docker.com/glossary/?term=docker), documentation (https://docs.docker.com/glossary/?term=documentation)