Plan and roll out Docker

- Who needs to be involved
- Communication and information gathering
  - Communicate with your developers and IT teams
  - Identify Docker organizations
  - Gather requirements
- Finalize plans and begin setup
  - Send finalized settings files to the MDM team
  - Begin setup
- Testing
  - SSO and SCIM testing
  - Test Registry Access Management and Image Access Management
  - Deploy settings and enforce sign in to test group
- Deploy your Docker setup
  - Enforce SSO
  - Deploy configuration settings and enforce sign-in to users
  - Next steps

Use this workflow to plan a Docker rollout across your organization, test its settings with a pilot group, and coordinate deployment with your IT teams. For invitations and sign-in configuration, follow Onboard a Docker organization.

Who needs to be involved

Identify the people responsible for each part of the rollout:

- Organization owners to manage membership and organization settings
- DNS and identity provider teams to verify domains and configure single sign-on (SSO)
- IT and mobile device management (MDM) teams to distribute Docker Desktop and configuration files

- Development leads and security representatives to agree on settings and security requirements
- A small group of developers to test the configuration before wider deployment

Communication and information gathering

Communicate with your developers and IT teams

Notify existing Docker Desktop users before changing versions, settings, or sign-in requirements. Explain which changes they should expect, when the pilot and wider rollout will happen, and where to report problems. Ask users to use their business email for their Docker accounts.

Engage your MDM team early to understand deployment requirements and lead times. Agree on how to distribute configuration files, registry keys, or `.plist` files for your chosen deployment method.

Identify Docker organizations

Survey teams to find existing Docker organizations and decide which ones should be part of the rollout. If you need to administer multiple organizations together, consider a Docker company. A company groups Docker organizations; it is separate from the business deploying Docker Desktop.

Gather requirements

Work with organization owners, development leads, and security representatives to define a baseline that supports development workflows and company policies. Agree on:

- Docker Desktop versions and update policies
- Settings developers can change and settings administrators must control
- Sign-in requirements, identity provider integration, and user provisioning
- Approved image sources and registries
- Additional Docker products your teams need and the subscriptions they require

Review Settings Management and Hardened Docker Desktop to choose controls available with your subscription.

Finalize plans and begin setup

Send finalized settings files to the MDM team

Record the agreed baseline and configure it through Docker Home or an `admin-settings.json` file, as appropriate for your subscription and deployment method. Coordinate with your MDM team to prepare the configuration and your chosen method for enforcing sign-in. Deploy to the pilot group before applying the settings more widely.

Begin setup

Follow organization onboarding to identify users, invite owners and members, and configure sign-in and provisioning. SSO and SCIM require Docker Business. Plan authentication and provisioning together: SSO authenticates users, while provisioning controls how users are added, updated, and removed.

Choose a supported Docker Desktop version and agree with IT on how users will receive it through MDM, a software portal, or direct installation. See Docker Desktop deployment.

If your rollout includes other Docker products, confirm access and complete their setup before the pilot. For example, follow the setup documentation for Docker Build Cloud, Docker Scout, or Docker Hardened Images.

Testing

SSO and SCIM testing

If you configure SSO or SCIM, test sign-in, provisioning, role assignments, and team membership with pilot accounts. Include a user joining the organization and a user leaving it. Follow the

provisioning documentation for the behavior of your chosen method. Check CLI authentication as well as Docker Desktop and browser sign-in.

Test Registry Access Management and Image Access Management

If your subscription and rollout include Registry Access Management or Image Access Management, verify that pilot users can pull approved images and that configured restrictions block disallowed sources. Tell pilot users about these restrictions before testing them.

Deploy settings and enforce sign in to test group

Apply the baseline settings and sign-in requirements to the pilot group. Have developers run their normal projects on Docker Desktop and Docker Hub. Confirm that required settings apply and that developers can still build, pull, and run the containers they need. Use the pilot rollout tutorial for a focused settings policy test.

For each additional product in your rollout, have a pilot developer complete a representative task: build with a cloud builder, review Scout results, or pull a Hardened Image. Record problems and adjust the baseline before wider deployment.

Deploy your Docker setup

Communicate the rollout schedule and expected changes to users. Confirm that IT and MDM teams are ready to distribute the tested configuration and support users who encounter problems.

Enforce SSO

If your plan includes SSO enforcement, verify that your identity provider configuration covers all intended users before enforcing it. Follow Configure SSO for setup and enforcement. Enforcing SSO and enforcing Docker Desktop sign-in are separate controls.

Deploy configuration settings and enforce sign-in to users

Have the MDM team distribute the tested Docker configuration to the remaining users. Provide instructions for sign-in and a support contact. Review feedback after each deployment group before expanding the rollout.

Next steps

- Review organization Insights, if available for your subscription, to track Docker Desktop adoption and versions.
- Use the user access workflow to review membership and permissions after rollout.
- Monitor Docker Scout findings for repositories where you've configured Scout.

□□□ #2
□ □□□ □□□ 2026-10-31 18:52:57 UTC
□ □□□ □□□ 2026-10-31 18:52:58 UTC