Install Docker Desktop on Windows

As part of this process, we'll be creating a sandbox environment for Splunk Enterprise using Docker, allowing you to test and explore Splunk in a contained setup without impacting your main system.

I recommend checking out the Docker Documentation: Docker Docs for Installing Docker Desktop for the installation steps on Mac, Windows, and Linux systems.

1
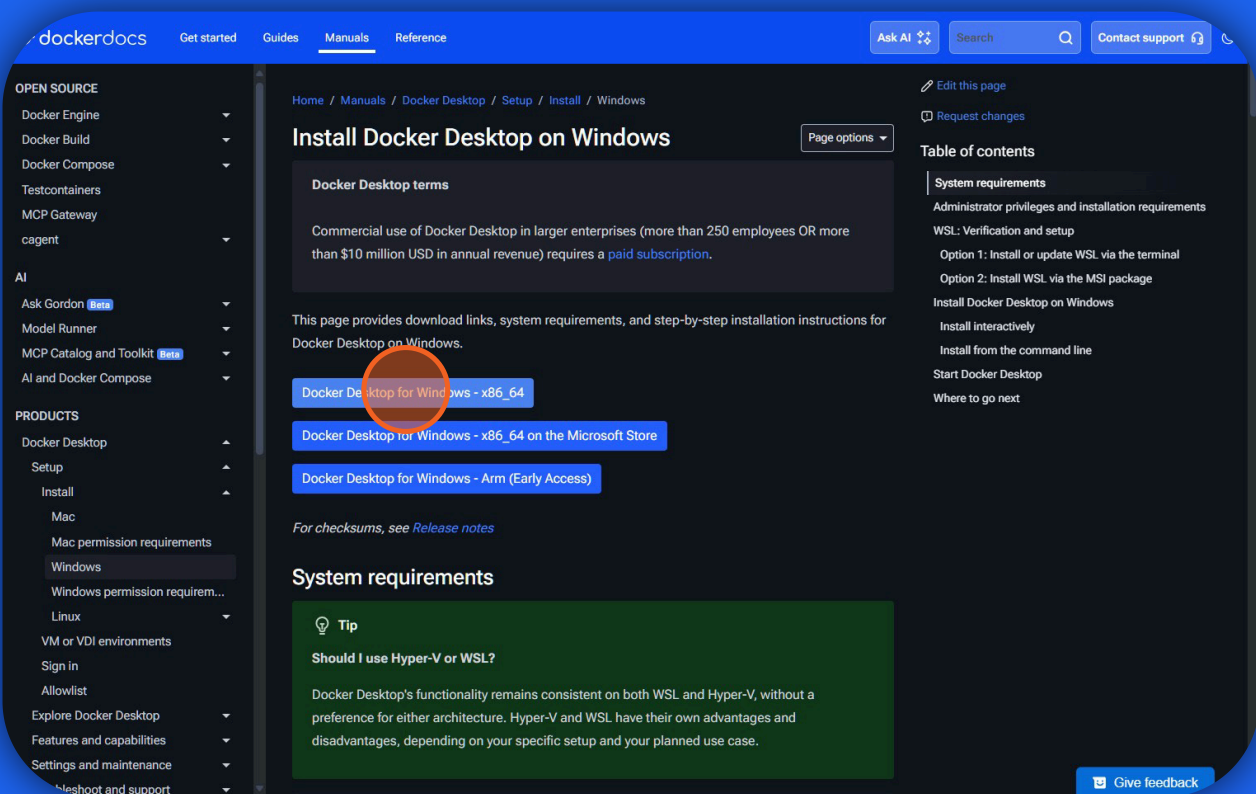
Navigate to Docker Docs for Installing Docker Desktop

Install Docker Desktop on Windows

Click "Docker Desktop for Windows - x86_64"

Install Docker Desktop interactively

1. Download the installer from the top of the page or release notes.
2. Run Docker Desktop Installer.exe (default location: C:\Program Files\Docker\Docker).
3. Choose your backend (WSL 2 or Hyper-V) if prompted.
4. Follow the wizard to authorize and complete the installation.
5. Click Close when finished and start Docker Desktop.

With Docker installed, the next step is to set up your Splunk Enterprise instance inside a container. Running Splunk in Docker provides a lightweight, isolated environment that you can start, stop, or reset as needed —perfect for testing, development, and sandbox experimentation.

In this part, you will:

Create a Splunk Enterprise instance within Docker container. Then be able to access the Splunk Web interface from your browser to access the console.
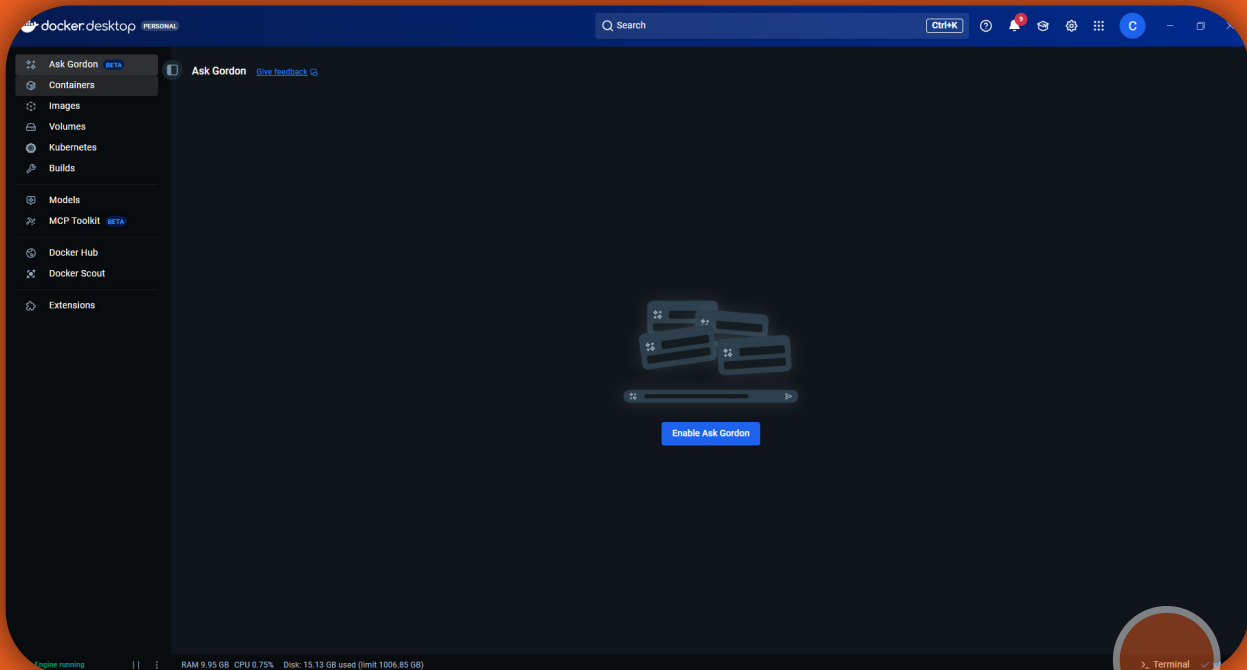
1

Launch Docker Desktop on your machine
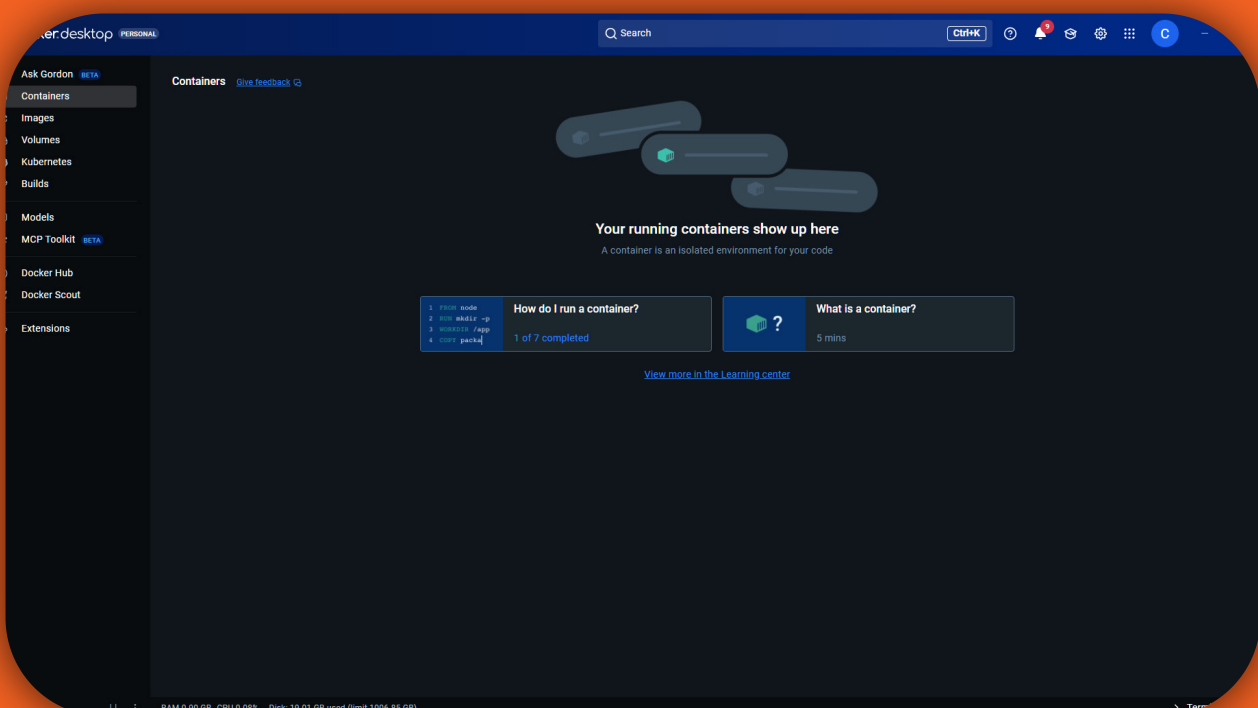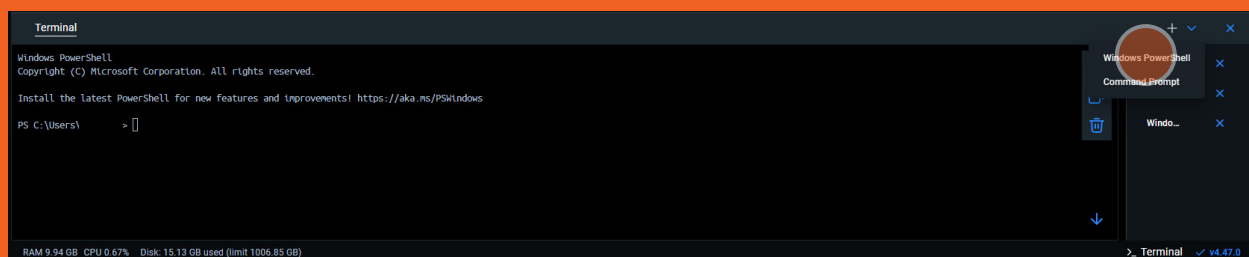
2

Click Terminal (bottom-right corner)

3

Select Windows PowerShell

Splunk Enterprise Sandbox

4

In Powershell, run:

Terminal

```
docker run -d `
-p 8080:8000 `
-e "SPLUNK_GENERAL_TERMS=--accept-sgt-current-at-splunk-com" `
-e "SPLUNK_START_ARGS=--accept-license" `
-e "SPLUNK_PASSWORD=Example123!" `
splunk/splunk:latest
```

5

Key Takeaways from Command

Terminal

Notes:
- Port 8080 → Splunk Web
- Password = Example123!
- Accepts license & terms
- Creates a Splunk image from splunk/splunk:latest under Image tab
- A Splunk instance appears under Containers once setup completes, the name of the instance is auto-generated

Splunk Enterprise Sandbox

Password Notes:
If you want to use your own, make sure it follows Splunk's password policy (e.g., minimum length, mix of uppercase, lowercase, numbers, and special characters).

Example of a compliant custom password:
MySecurePass2025!

Splunk Password Policy Docementation

6

Access Splunk Enterprise Instance

Terminal

- Paste http://localhost:8080 in web browser
- Username: admin
- Password: Example123! or custom password set by you