AgenticAI Foundry

Student Quick Start Guide

MIT Professional Education | Applied Generative AI for Digital Transformation

This guide will get you from zero to running the course demos in the shortest possible time. Follow the steps in order and you'll see the app open in your web browser.

What You'll Be Running

Demo	Module	API Key?	What You'll Learn
■ LLM Cost Explorer	1	No	Why AI costs vary 200x by model
■ Multi-Agent Demo	2	Optional	How AI agents collaborate as a team
■ LangChain Agent	2	Optional	How a single agent uses tools
■ MCP Explorer	3	No	How agents connect to apps & services
■■ Agent Security Demo	4	Demo: No	Prompt injection attacks & guardrails

Good news: Modules 1 and 3 work immediately with zero setup. Start there and come back for Module 2 once you're comfortable.

Step 0 — Get the Code

You need a copy of the app files on your computer before anything else. The easiest way requires no account and no technical knowledge:

1. Open your web browser and go to: **https://github.com/dlwhyte/AgenticAI_foundry**
2. Click the green **"< > Code"** button (top-right area of the page)
3. Click **"Download ZIP"**
4. Find the downloaded file in your **Downloads** folder
5. Unzip/extract it: **Windows** — right-click → "Extract All" | **Mac** — double-click
6. Move the extracted folder somewhere easy to find, like your Desktop

■ **Tip:** The folder will be called **AgenticAI_foundry-main**. In later steps you'll need to navigate your terminal to this folder — knowing exactly where it is will save you time.

Choose Your Setup Path

Ask yourself one question:

> ***"Have I installed Docker Desktop before, or am I comfortable installing a new application from a website?"***

■ Path A — Docker

Recommended

Docker packages the entire app — Python, all libraries, everything — into a self-contained box. Fewer things can go wrong once it's running.

Best if: You want the most reliable setup
Time: ~20 minutes (mostly downloading)
One-time install: Docker Desktop (~500MB)

■ Path B — Python

Alternative

Run the app directly using Python. More steps and more things that can go wrong, but more visibility into how it works.

Best if: You already have Python installed
Time: ~15 minutes
One-time install: Python + libraries

Path A — Docker Setup

Step 1 — Install Docker Desktop

Download Docker Desktop from: **https://www.docker.com/products/docker-desktop/**

Windows	Mac
1. Download the Windows installer 2. Run **Docker Desktop Installer.exe** 3. Keep all default options 4. Restart your computer when asked 5. Open Docker Desktop from Start menu 6. Wait for the whale icon to stop animating	1. Check Apple menu → About This Mac for chip type (Intel or Apple Silicon M1/M2/M3) 2. Download the matching version 3. Open the .dmg file 4. Drag Docker to Applications 5. Open Docker from Applications 6. Wait for the whale icon in the menu bar to stop animating

■ **You'll know Docker is ready when:** the whale icon in your taskbar (Windows) or menu bar (Mac) has **stopped animating** and is showing a steady icon.

Step 2 — Open a Terminal

A terminal is a text-based window for typing commands. Don't worry — you only need a handful.

Windows	Mac	Linux

Press **Win + R**, type **powershell**, press Enter	Press **Cmd + Space**, type **Terminal**, press Enter	Press **Ctrl + Alt + T**

Step 3 — Navigate to the Project Folder

In the terminal, type **cd** followed by the path to the folder you extracted in Step 0. Replace the example path with the actual location on your computer:

Windows example:

```
cd C:\Users\YourName\Desktop\AgenticAI_foundry-main
```

Mac/Linux example:

```
cd ~/Desktop/AgenticAI_foundry-main
```

> ■ **Shortcut:** You can drag the project folder directly onto the terminal window and it will paste the full path for you. Then just add **cd** at the start.

Step 4 — Build the App (one-time only)

Type this command and press Enter. This downloads Python and all required libraries — it takes 2–5 minutes and shows a lot of output. That's normal.

```
docker build -t agenticai-foundry .
```

Wait until you see: **[+] Building X.Xs (13/13) FINISHED** — the last line will say **unpacking to docker.io/library/agenticai-foundry:latest**

Step 5 — Run the App

```
docker run -p 8501:8501 agenticai-foundry
```

You'll see output that includes: **You can now view your Streamlit app in your browser.**

Step 6 — Open the App in Your Browser

Open any web browser (Chrome, Safari, Edge, Firefox) and go to:

```
http://localhost:8501
```

> ■ You should see the AgenticAI Foundry home page! Click any demo in the sidebar to get started.

Step 7 — Stopping the App

When you're done, go back to the terminal and press **Ctrl + C** to stop the app.

> Next time you want to run the app, you only need Steps 5 and 6 — Steps 1 through 4 are one-time setup only.

Path B — Python Setup

Use this path if you prefer not to use Docker or already have Python 3.10+ installed.

> ■■ **Check your Python version FIRST before doing anything else.**
>
> Open a terminal and run: **python3 --version**
>
> If it shows **Python 3.9 or lower** — stop here and use Docker (Path A) instead. The agent demos (Module 2) require Python 3.10 or higher and will fail to install on older versions.
>
> Modules 1 and 3 will work on Python 3.9, but Module 2 will not.

Step 1 — Verify Python 3.10 or Higher

Run **python3 --version** in your terminal. You need to see Python 3.10, 3.11, 3.12, or 3.13.

If you need to upgrade, download from **https://www.python.org/downloads/** and run the installer. It installs alongside your existing Python — nothing gets deleted.

■■ **Windows users:** During installation, check **"Add Python to PATH"** — this box is easy to miss and causes problems later if skipped.
■■ **Mac users:** Your Mac may have Python 3.9 built in from Xcode. Download Python 3.11 from python.org — it installs separately without affecting anything else.

Step 2 — Open a Terminal

See Step 2 from Path A above.

Step 3 — Navigate to the Project Folder

See Step 3 from Path A above.

Step 4 — Install Required Libraries

> ■■ **Do not skip this step.** If you skip it, the app will crash with an error like *ModuleNotFoundError: No module named 'tiktoken'*. Run both commands below, one at a time:

```
pip3 install -r requirements.txt
pip3 install -r requirements-crewai.txt
```

Wait until your terminal prompt returns before moving on. This takes 2–5 minutes and shows a lot of output — that's normal.

Step 5 — Run the App

```
python3 -m streamlit run Home.py
```

Your browser should open automatically to **http://localhost:8501**. If it doesn't, open your browser and go there manually.

Step 6 — Stopping the App

Press **Ctrl + C** in the terminal when you're done.

Troubleshooting — Most Common Issues

Problem	Solution
Docker: "Cannot connect to Docker daemon"	Docker Desktop is not running. Open the Docker Desktop application and wait for the whale icon to stop animating, then try again.
Docker: "Port 8501 is already in use"	Another app is using that port. Try: docker run -p 8502:8501 agenticai-foundry then open http://localhost:8502 instead.
Docker: Build seems stuck	The first build downloads ~500MB. On slower connections this can take 10+ minutes. Wait it out — once complete, future runs take seconds.
Python: ModuleNotFoundError (any module name)	You skipped the install step. Run both of these: pip3 install -r requirements.txt then pip3 install -r requirements-crewai.txt then restart the app.
Python: "pip3 not found"	Try pip install -r requirements.txt instead (without the 3).
Python: "streamlit not found"	Use python3 -m streamlit run Home.py instead of streamlit run Home.py.
Python: "Permission denied" on pip install	Add --user to the command: pip3 install --user -r requirements.txt
Browser doesn't open automatically	Manually go to http://localhost:8501 in any web browser.

Need more help?
Run **python setup_check.py** in the project folder — it checks your environment and tells you exactly what's working and what's not. Bring the output to office hours or post it in the course forum.

■■ Module 4 · Agent Security Demo

Explore how AI agents can be attacked via prompt injection — and how guardrails defend against them.

Two Modes

Mode	API Key?	What You Can Do
Demo Mode	No	Pre-built attack scenarios with simulated responses — works immediately
Live Mode	Optional	Test real guardrails with OpenAI, Anthropic, or Ollama

What You'll See

Six attack scenarios including direct injection, role-playing (DAN), gradual escalation, system prompt extraction, and indirect injection. Five defense layers you can toggle on and off: input validation, scope enforcement, constitutional AI review, output filtering, and human-in-the-loop. A business impact

calculator showing breach costs vs. guardrail ROI by industry.

Key Insight

> No single guardrail catches every attack — AI security requires defense in depth. This demo shows you why layering multiple defenses matters.