Workshop

From Models to Operations: Understanding Autonomous Agents in Networking

Lab Guide

Learning Objectives

Upon completion of this lab, you will be able to:

- Create your own AI agent in the context of Network Automation.
- Extend your AI agent to add new network functions.
- Understand the difference between the two agent planning strategies: CoT and ReAct.
- Influence your agent to use a local knowledge database and a long-term memory.
- Design your agent to instantiate a single instance or multiple instances (agent swarm).

Disclaimer

This document aims to familiarize you with AI Autonomous Agents. Although the lab design and configuration examples could be used as a reference, it's not a real design, thus not all recommended features are used, or enabled optimally. For the design related questions please contact your representative at Cisco, or a Cisco partner.

Pre-requirements

For this lab we will require a VPN connection to Cisco dCloud and, optionally, a Remote Desktop connection.

1. If Cisco Secure Client is not installed on your laptop, please download the client from the following box folder:
   https://cisco.box.com/s/zpekvtyspebkoupk2z1id896ey9d0bud
   See instruction to install the Cisco Secure Client here.
2. For Mac and Linux users, use the Remote Desktop application of your preference. Suggested options are:
   - Mac: Windows App
   - Linux: Remmina

Notes:

- If you prefer not to use a Remote Desktop connection, you will also have the option to open the Agent playground UI on your own laptop, once connected to the VPN.
- If you prefer to install and run the Agent playground package on your own laptop, please follow instructions in **Appendix B**.

Run your Setup (All users)

During this lab, our AI agent will require to interact with a Large Language Model (LLM) via API.

- In the setup running on Cisco dCloud, we will have pre-defined credentials to use CIRCUIT as LLM Provider.

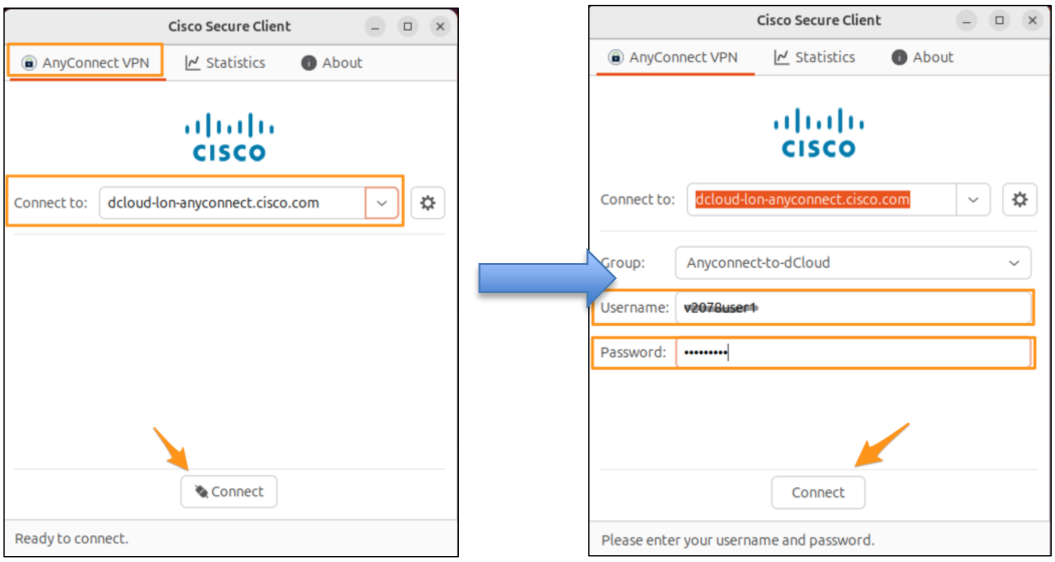
- If you prefer to use you own LLM Provider API keys (OpenAI and OpenRouter are supported), then please see instructions in **Appendix C.**

- If you want to use OpenAI or OpenRouter as LLM Provider but you have not created your API keys, then please see instruction in **Appendix B > Task 1 and Task 2** to create your keys. Then follow instructions in **Appendix C**.

Task 1: Connect to Cisco dCloud VPN

Connect to the dCloud VPN using Cisco Secure Client:

In the Cisco Secure Client, enter the host dcloud-rtp-anyconnect.cisco.com and select Connect. Next, enter the credentials (**Username / Password**).



Connect to: dcloud-lon-anyconnect.cisco.com

Ready to connect.

Connect to: dcloud-lon-anyconnect.cisco.com

Group: Anyconnect-to-dCloud

Username: [redacted]

Password: ••••••••

Please enter your username and password.

Note: Credentials to access the dCloud VPN will be shared by email.

Task 2: Connect to the Remote Workstation

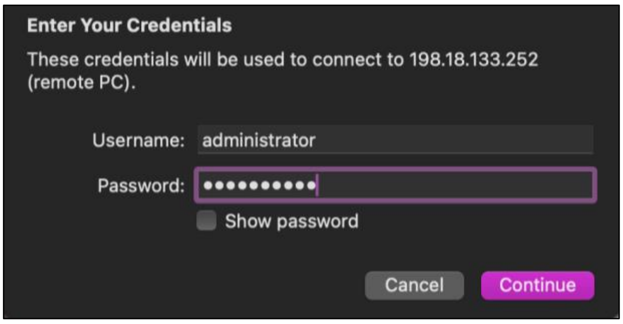
Skip this task if you prefer not to use a Remote Desktop connection and want to open the Agent playground UI on your own laptop.

Use your preferred Remote Desktop connection application to connect to the remote workstation in dCloud.

Use the following connection details:

- IP: 198.18.133.252
- User: administrator
- Password: C1sco12345

Example using Window App for Mac:



Enter Your Credentials

These credentials will be used to connect to 198.18.133.252 (remote PC).

Username: administrator

Password: ••••••••••

□ Show password

Task 3: Set your LLM Provider API Keys via REST API

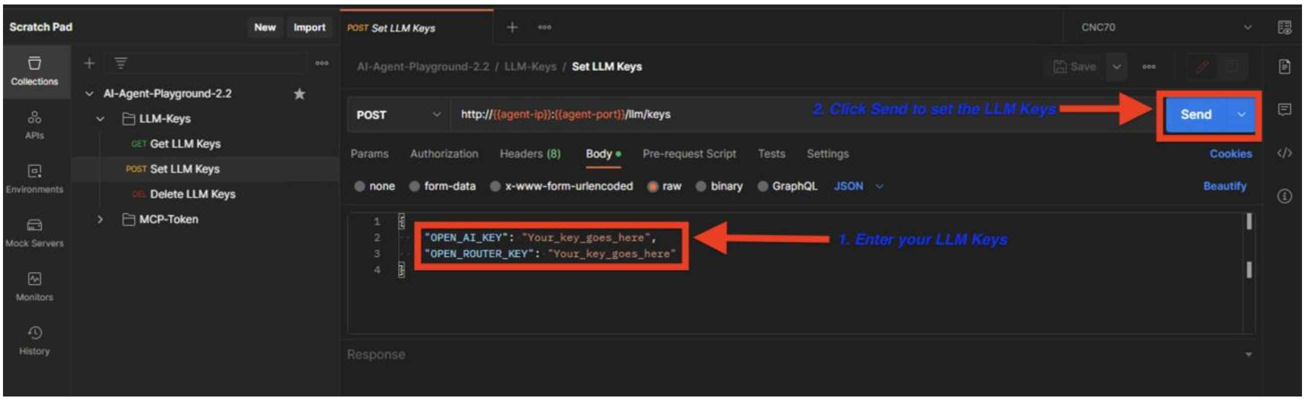
To accomplish this task, Students have the option to set the LLM Keys *(bring your LLM Keys)* using Postman **or** WebUI.

Note: Only OpenAI and OpenRouter are supported as LLM providers to configure the API keys via REST API.

Step1: Set LLM keys via Postman

On your desktop, please find the postman App.

Use the **Set LLM Keys** request to set one or both API keys with your own keys. Use the **Body** payload to set the API key information, and then select **Send**. See screenshot below for reference:



POST http://{{agent-ip}}:{{agent-port}}/llm/keys

```
{
  "OPEN_AI_KEY": "Your_key_goes_here",
  "OPEN_ROUTER_KEY": "Your_key_goes_here"
}
```

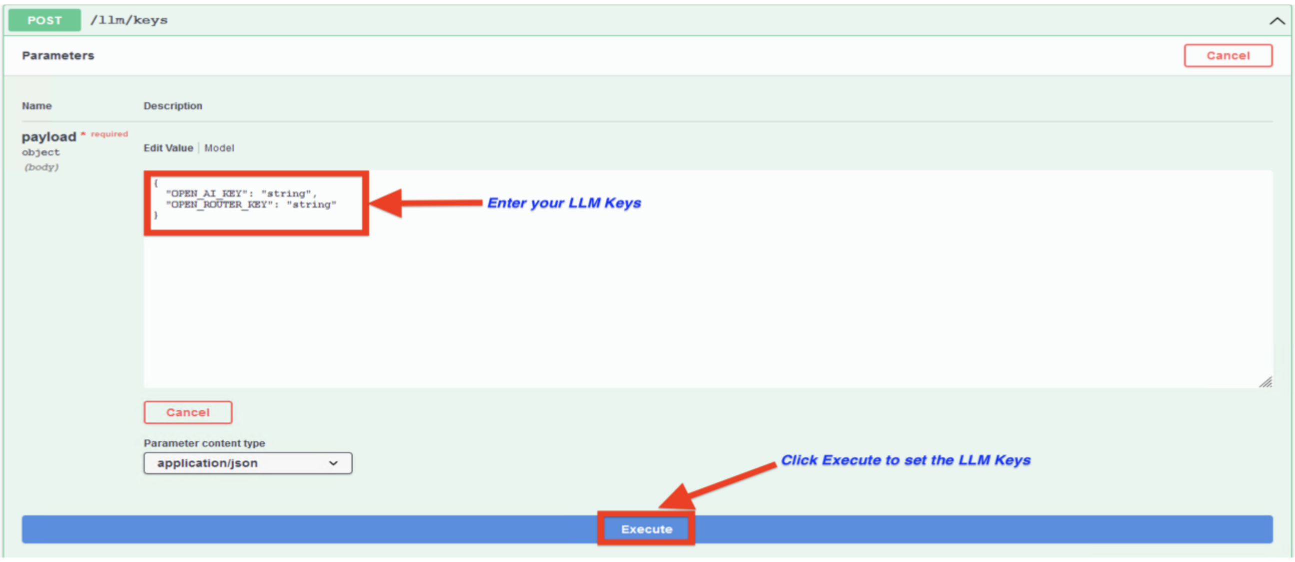
1. Enter your LLM Keys

2. Click Send to set the LLM Keys

Step 2: Set LLM Keys using WebUI

Please use the IP Address ‘http://198.18.134.201:4109/ to reach the application.

Enter your LLM Keys and Hit execute to set the LLM Keys.



```
{
  "OPEN_AI_KEY": "string",
  "OPEN_ROUTER_KEY": "string"
}
```

Enter your LLM Keys

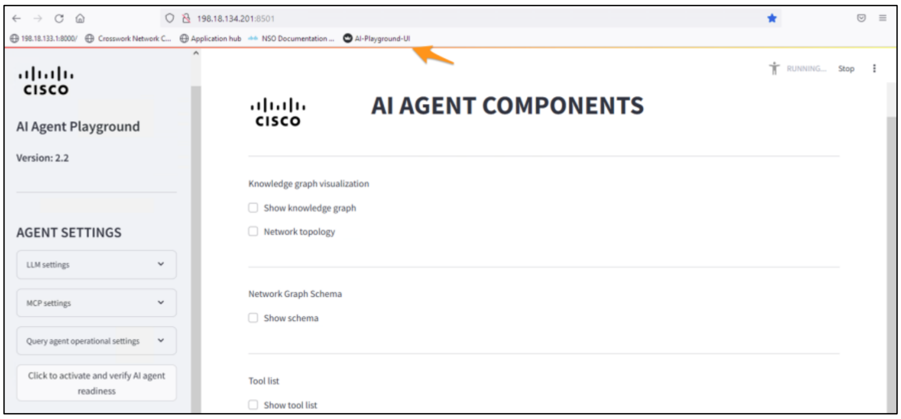
Click Execute to set the LLM Keys

Task4: Get familiar with the AI Agent playground UI

Step 1: Access the web UI

If you are not using a Remote Desktop connection, then just open a web-browser (Chrome or Mozilla are recommended) and go to the following URL: http://198.18.134.201:8501/

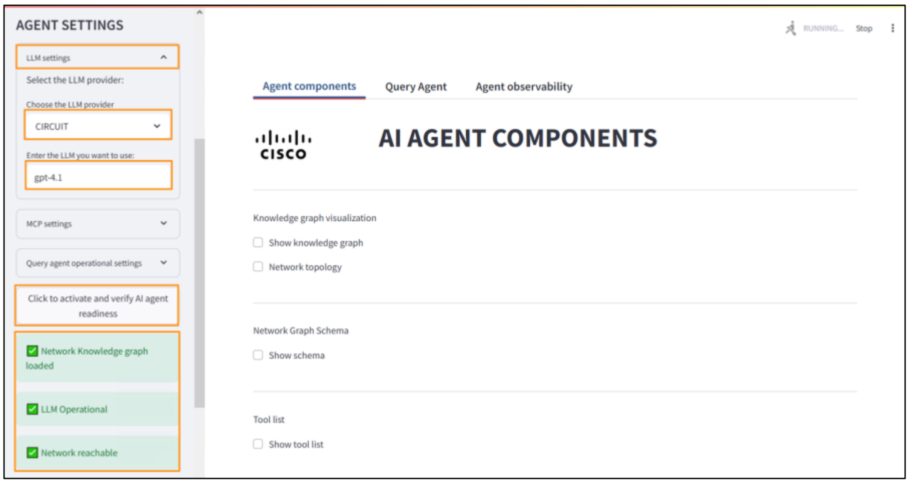
From the remote workstation, launch Mozilla and the Agent UI should be automatically opened. There is also a bookmark “AI-Playground-UI” that you can select:



Step 2: Verify the AI agent readiness

In the **Agent Settings** to the left-hand side, select **LLM settings > LLM provider** (use CIRCUIT by default or use your preferred LLM provider – see instructions in **Appendix C**). Then enter the **LLM** you will use (e.g. gpt-4.1) and **press Enter**. Keep all other settings at their default values and select **Click to activate and verify AI agent readiness**. You should see three validations in green color, meaning that your AI agent is ready to be used.

See picture below for reference:



Select the LLM provider:

Choose the LLM provider: CIRCUIT

Enter the LLM you want to use: gpt-4.1

☑ Network Knowledge graph loaded

☑ LLM Operational

☑ Network reachable

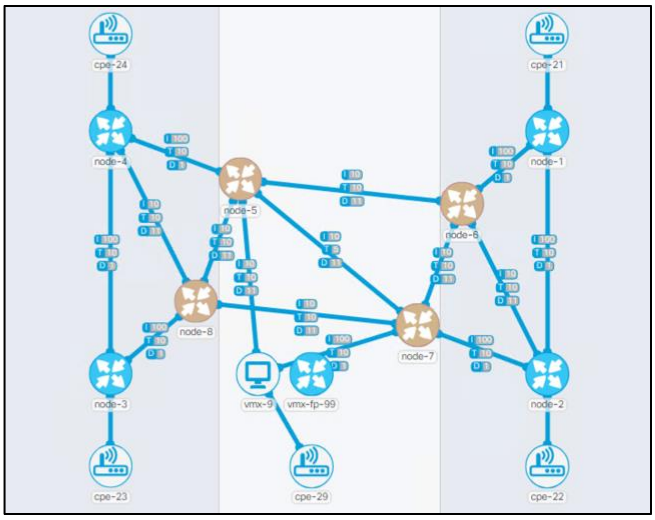
Note: If the last check is in red color (failed state) then it means the network topology is unreachable. Please raise your hand to call one of the proctors.

Up to this point you have successfully completed the Quick Start Lab Guide for this workshop. **Next tasks and steps will be provided by the presenter. Enjoy your lab!**

Appendix A – Network Topology

The following topology will be used during the lab.

- The routers are configured to mimic a core-network, with P and PE routers. node-1, node-2, node-3 and node-4 are PEs and node-5, node-6, node-7 and node-8 are P routers. Node-9 is a hybrid P/PE. They are interconnected with point2point links and are running ISIS as their Interior Gateway Protocol (IGP). They are also peering BGP Link-state (BGP-LS) with the routers pce-11 and pce-12, which are the SR-PCEs in the network. They are the Path Computation Elements (PCEs) which handle path computation of delegated LSPs and learn topology via BGP Link State. All other nodes are Path Computation Clients (PCCs).
- The SR-PCE is deployed off-path (i.e. external to the ISIS domain), as it is not intended to forward any traffic. Its role is only to be the SR-PCE, to build link-state topology, and act as a route-reflector for the network.



Equipment details

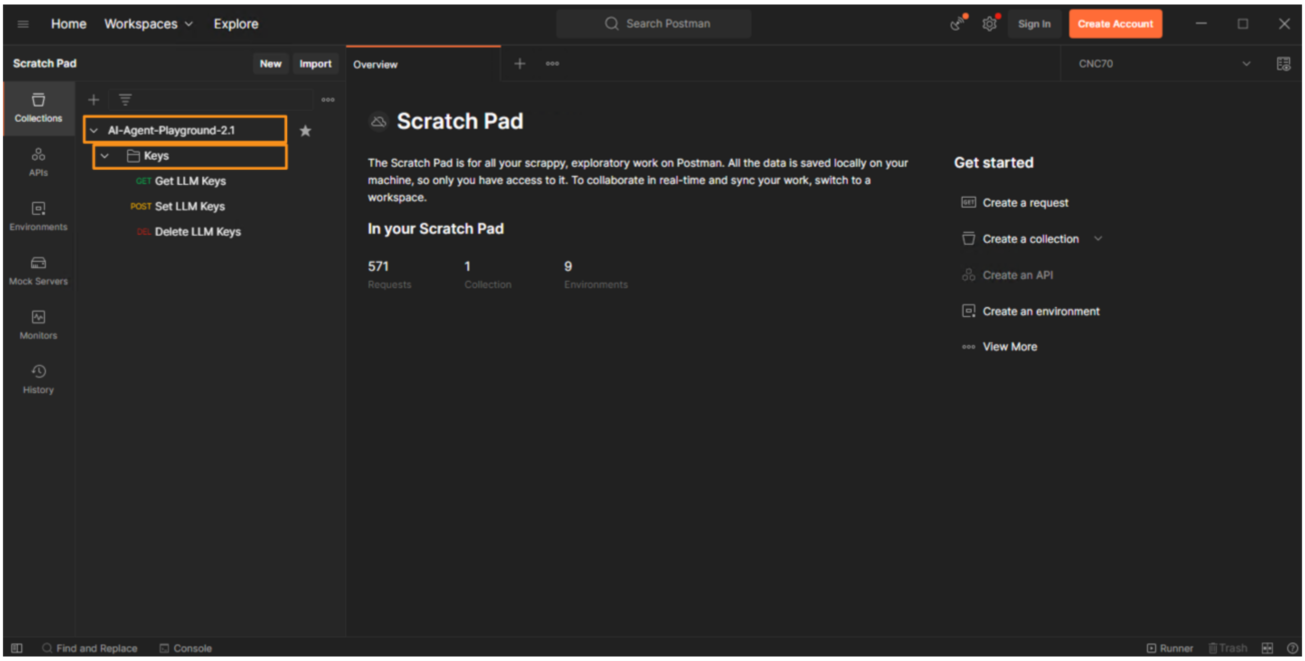
Name	Description	Host Name (FQDN)	IP Address	Username	Password
node-1 - node-8	Cisco IOS XRv	name.demo.dcloud.cisco.com	198.18.1.41-48, 198.19.1.1-8	cisco	cisco
pce-11 – pce-12	Cisco SR-PCE, RR on IOS XR	name.demo.dcloud.cisco.com	198.18.1.51-52, 198.19.1.11-12	cisco	cisco
cpe-11-14	Cisco IOSv, telnet	name.demo.dcloud.cisco.com	198.18.1.61-64, 198.19.1.21-64	cisco	cisco

Appendix B – Set your LLM Provider API Keys via REST API

Use Postman

In the remote workstation, from the Windows task bar launch Postman. The collection “**AI-Agent-Playground-2.2**” is pre-loaded. Open the collection and the **Keys** folder. You will see three API requests to perform the following operations:

- Get LLM Keys
- Set LLM Keys
- Delete LLM Keys



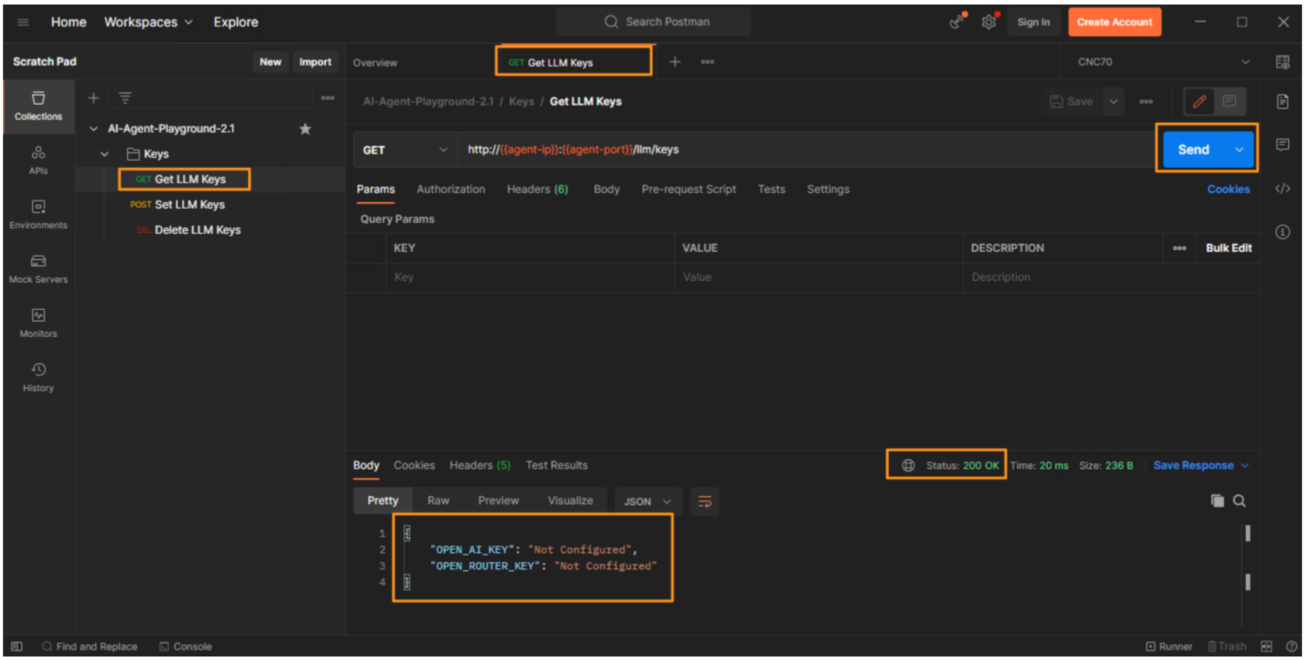
Scratch Pad

The Scratch Pad is for all your scrappy, exploratory work on Postman. All the data is saved locally on your machine, so only you have access to it. To collaborate in real-time and sync your work, switch to a workspace.

In your Scratch Pad

571 Requests
1 Collection
9 Environments

Use the **Get LLM Keys** request to validate if the API keys are in “**Configured**” or “**Not Configured**” state. In the following example, none of the API keys are configured:



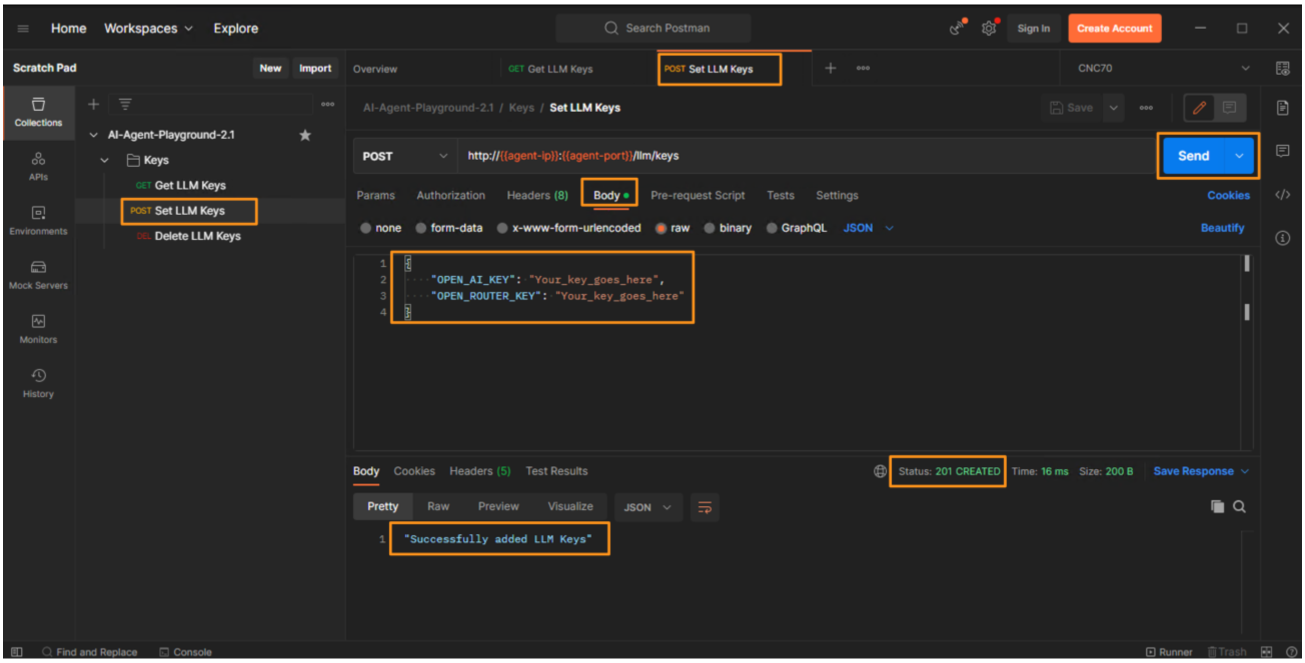
AI-Agent-Playground-2.1 / Keys / Get LLM Keys

GET http://{{agent-ip}}:{{agent-port}}/llm/keys

Status: 200 OK Time: 20 ms Size: 236 B

```
{
    "OPEN_AI_KEY": "Not Configured",
    "OPEN_ROUTER_KEY": "Not Configured"
}
```

Use the **Set LLM Keys** request to set one or both API keys with your own keys. Use the **Body** payload to set the API key information, and then select **Send**. See screenshot below for reference:



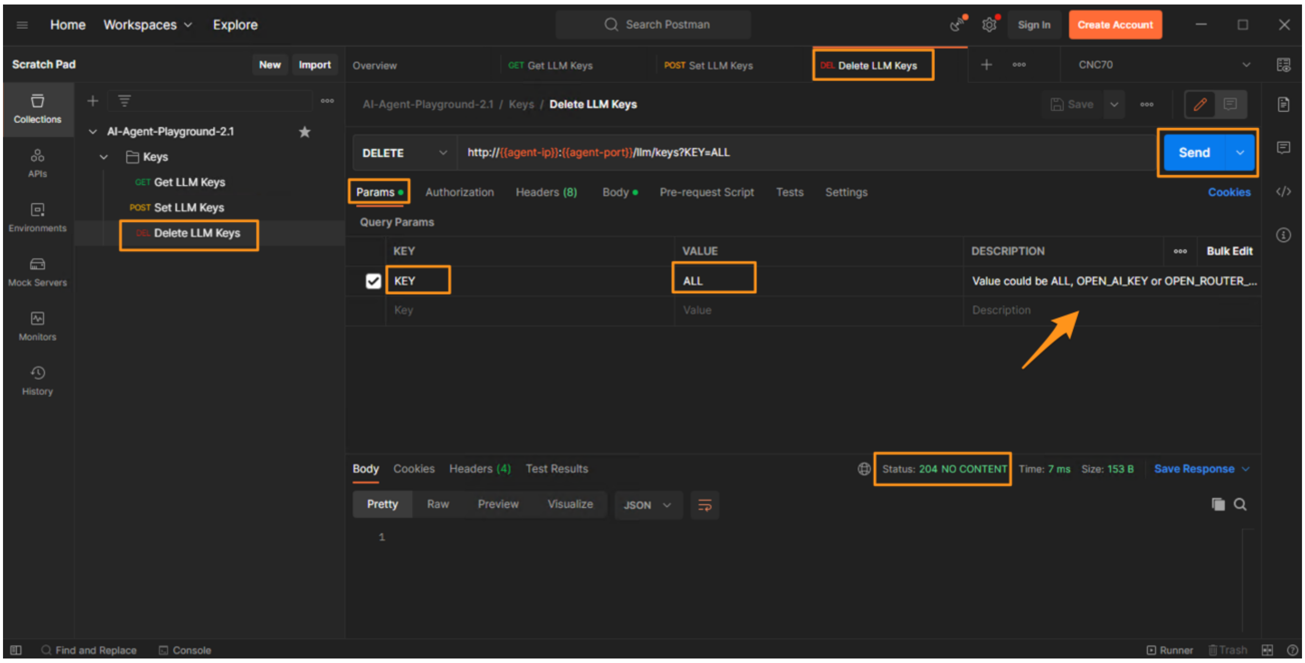
```
POST http://{{agent-ip}}:{{agent-port}}/llm/keys
```

```
{
    "OPEN_AI_KEY": "Your_key_goes_here",
    "OPEN_ROUTER_KEY": "Your_key_goes_here"
}
```

Status: 201 CREATED Time: 16 ms Size: 200 B

```
"Successfully added LLM Keys"
```

Use the **Delete LLM Keys** request to delete one or both API keys. A **KEY** parameter can be passed, and accepted values are: ALL (default), OPEN_AI_KEY or OPEN_ROUTER_KEY. See screenshot below for reference:



```
DELETE http://{{agent-ip}}:{{agent-port}}/llm/keys?KEY=ALL
```

Query Params

	KEY	VALUE	DESCRIPTION
☑	KEY	ALL	Value could be ALL, OPEN_AI_KEY or OPEN_ROUTER_...

Status: 204 NO CONTENT Time: 7 ms Size: 153 B

Note: even though values are not deleted with the Delete request, this information lives in memory only and will be automatically removed once the agent playground is stopped, or the dCloud session ends.