

在安全訪問中實施DLP以限制開放式AI ChatGPT用於程式設計

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

- [1. 建立資料分類以使用原始碼資料識別符號](#)
- [2. 建立DLP策略，並在其中呼叫資料分類「原始碼」。](#)
- [3. 確保您已為發往「聊天GPT」且已啟用解密的流量設定了Internet訪問策略。](#)
- [4. 使用Open AI ChatGPT嘗試下載或上傳任何程式。](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何在安全訪問中實施資料丟失防護(DLP)，以限制Open AI ChatGPT用於程式設計和編碼。

必要條件

需求

思科建議您瞭解以下主題：

- 安全存取
- DLP
- 開啟AI ChatGPT

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全存取
- DLP
- 開啟AI ChatGPT

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

1. 建立資料分類以使用原始碼資料識別符號

導航到[安全訪問控制台](#)。

- 點選Secure>Data Classification> Add

The screenshot shows the Microsoft Security Center interface. On the left sidebar, the 'Secure' menu item is highlighted with a red box and a red arrow pointing to it. The main content area is titled 'Data Classification' and contains a grid of configuration options. The 'Data Classification' option in the bottom right of the grid is highlighted with a red box and a red arrow pointing to it. The grid includes sections for Policy, Profiles, and Settings, each with sub-items and brief descriptions.

Policy	Profiles	Settings
Access Policy Create rules to control and secure access to private and internet destinations	Endpoint Posture Profiles Configure requirements for end-user devices connecting to private resources	Threat Categories Choose types of harmful destinations to restrict access to
Data Loss Prevention Policy Prevent data loss/leakage with policy rules	IPS Profiles Configure settings for intrusion prevention	Notification Pages Configure notifications to present to end users who try to access blocked or warned destinations.
	Web Profiles Configure web security settings for use in internet access rules	Do Not Decrypt Lists Specify destinations for traffic that must never be decrypted
		Certificates Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients
		Data Classification Manage rules to prevent sensitive data loss

- 輸入Data Classification Name > Select Built-in Data Identifiers > Search forSource Code並選擇它

Data Classifications Exact Data Matches Indexed Document Matches

For more information about data classification, see [Help](#)

[ADD CUSTOM IDENTIFIER](#)

Add New Data Classification

Data Classification Name

Description (Optional)

Select Boolean Operator
 OR AND

Built-in Data Identifiers

Built-in Identifiers
 Source Code >

Custom Identifiers

Data Classifications Exact Data Matches Indexed Document Matches

For more information about data classification, see [Help](#)

[ADD CUSTOM IDENTIFIER](#)

Add New Data Classification

Data Classification Name

Description (Optional)

Select Boolean Operator
 OR AND

Selected Data Identifiers
 Source Code >

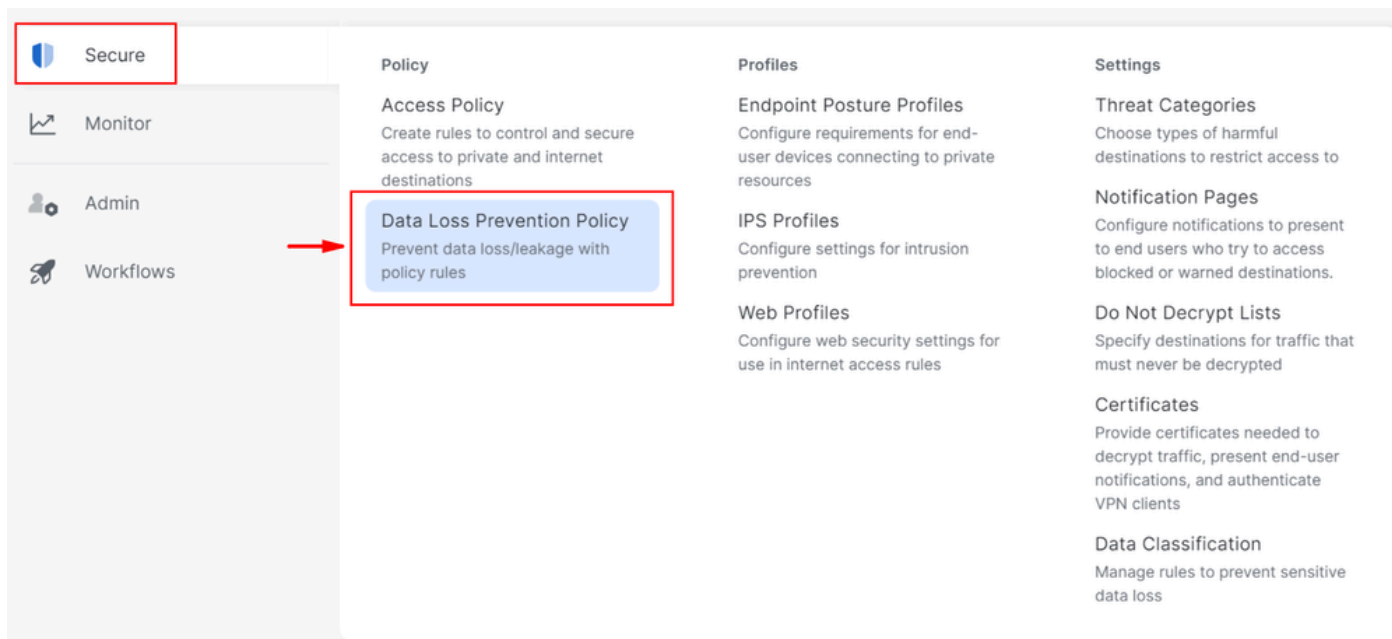
Built-in Data Identifiers

No Data Identifiers found.

Custom Identifiers

2. 建立DLP策略，並在其中呼叫資料分類「原始碼」。

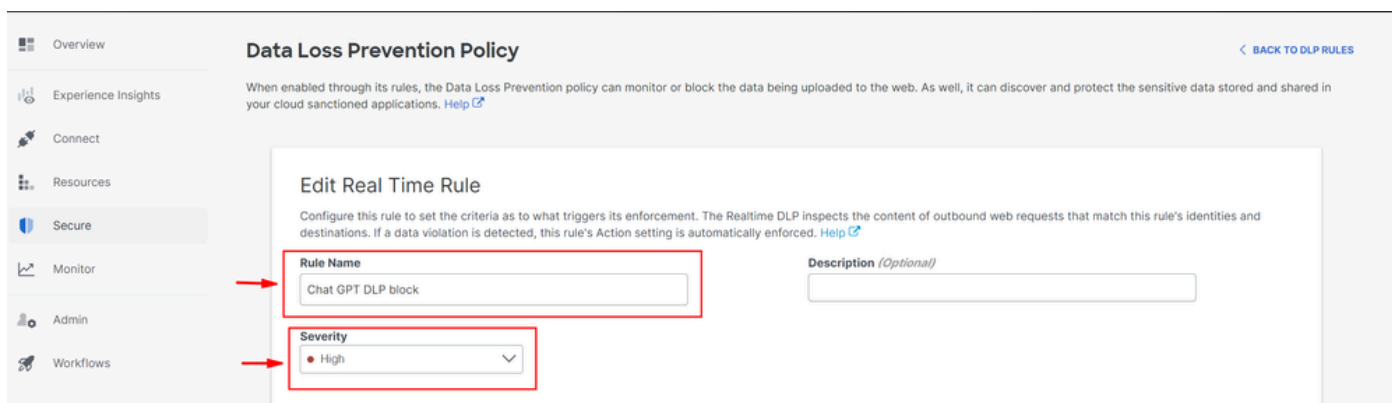
- 點選Secure> Data Loss Prevention Policy



- 點選Add Rule> Real Time Rule



- 提供Rule Name>設定適當的 Severity



- 在Data Classifications下，選擇Content，然後選擇 Source Code

Data Classifications

Select where to search for the selected data classifications.

- Content File Name Content and File Name

Select data classifications to add them to this rule.

Search Classifications

<input type="checkbox"/> Built-in GDPR Classification	PREVIEW
<input type="checkbox"/> Built-in HIPAA Classification	PREVIEW
<input type="checkbox"/> Built-in PCI Classification	PREVIEW
<input type="checkbox"/> Built-in PII Classification	PREVIEW
<input checked="" type="checkbox"/> Source Code	PREVIEW

- 在Identities選取所需的標識

Identities
Select identities to add them to this rule.

Search Identities

All Identities

<input type="checkbox"/> AD Groups	
<input checked="" type="checkbox"/> AD Users	4 >
<input type="checkbox"/> Network Tunnel Groups	6 >
<input type="checkbox"/> Networks	1 >
<input checked="" type="checkbox"/> Roaming Computers	4 >

5 Selected REMOVE ALL

<input checked="" type="checkbox"/> Roaming Computers	4
onmicrosoft.com)	

- 在目標下，選取 Select Destination Lists and Applications for Inclusion
- 選擇 Application Categories > Select Generative AI > Select OpenAI API (Vetted) and OpenAI ChatGPT (Vetted) in Outbound and InboundDirection

Destinations

Manage destination lists and vetted applications for this rule.

All Destinations

Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

Select Destinations Lists and Applications for Inclusion

Scans selected destination lists and vetted applications.

Destinations

Destination Lists 1 >

Application Categories

4802 (2 SELECTED) >

2 Selected for Inclusion

REMOVE ALL

Applications Categories

OpenAI API / Generative AI, Outbound & Inbound



OpenAI ChatGPT / Generative AI, Outbound & Inbound



- 在Actionselect下 Block
- 在User Notifications下，您可以在規則觸發時設定傳送給終端使用者的電子郵件通知（可選）

Action

Choose to monitor or block content for this rule.

Block

The Default Block Page Applied

User Notifications

When enabled, the system sends an email to recipients notifying them that this rule has been triggered.

User Notifications enabled

Email Message

Select the design of the email notification that will be sent to recipients.

Default Email

[Preview Default Email >](#)

Custom Email

Select template

- 按一下 Save

DELETE

CANCEL

SAVE



3. 確保您已為發往「聊天GPT」且已啟用解密的流量設定了Internet訪問策略。

範例：

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

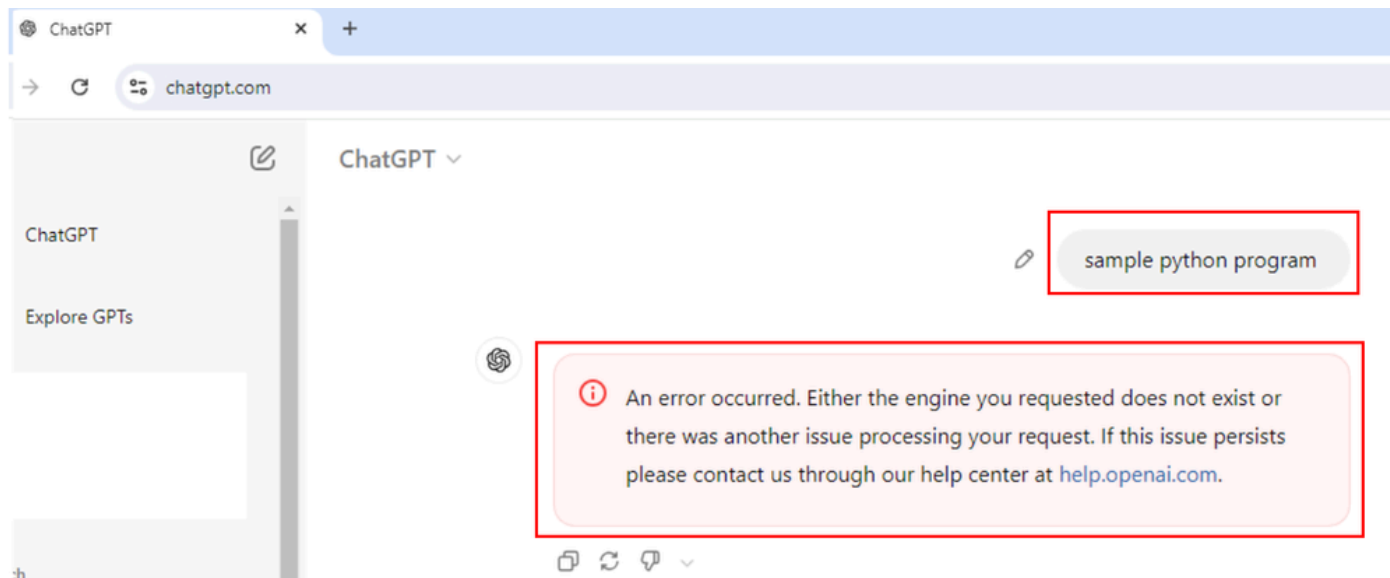


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- 請求一個python程式示例，此請求被阻止。




- 詢問程式是否正確，並封鎖此要求。



ChatGPT ▾

```
Is this program correct?  
# Python program to swap two variables  
  
x = 5  
y = 10  
  
# To take inputs from the user  
#x = input('Enter value of x: ')  
#y = input('Enter value of y: ')  
  
# create a temporary variable and swap the values  
temp = x  
x = y  
y = temp  
  
print('The value of x after swapping: {}'.format(x))  
print('The value of y after swapping: {}'.format(y))
```



 An error occurred. Either the engine you requested does not exist or there was another issue processing your request. If this issue persists please contact us through our help center at help.openai.com.

< 2/2 >    ▾

驗證

我們可以看到，當使用者嘗試向ChatGPT請求示例Python程式時，該請求被阻止。我們可以確認在安全訪問資料丟失防護日誌中觸發了DLP事件。

- 轉至Monitor> Data Loss Prevention

Overview

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Activity Search

FILTERS

Search by domain, identity, or URL

Search filters

1,965 Total

Response

Select All

Request

Source

Allowed Advanced

Reports

Remote Access Logs

Activity Search

Traffic logs

Security Activity

Security events and top threats

Total Requests

Activity Volume

App Discovery

Discover and analyze network applications

Top Destinations

Top domains visited by DNS

Top Categories

Top security and content categories by DNS

Third-Party Apps

Cloud Malware

View and manage detected malware events

Data Loss Prevention

Data violations detected through the Real Time and SaaS API rules

Management

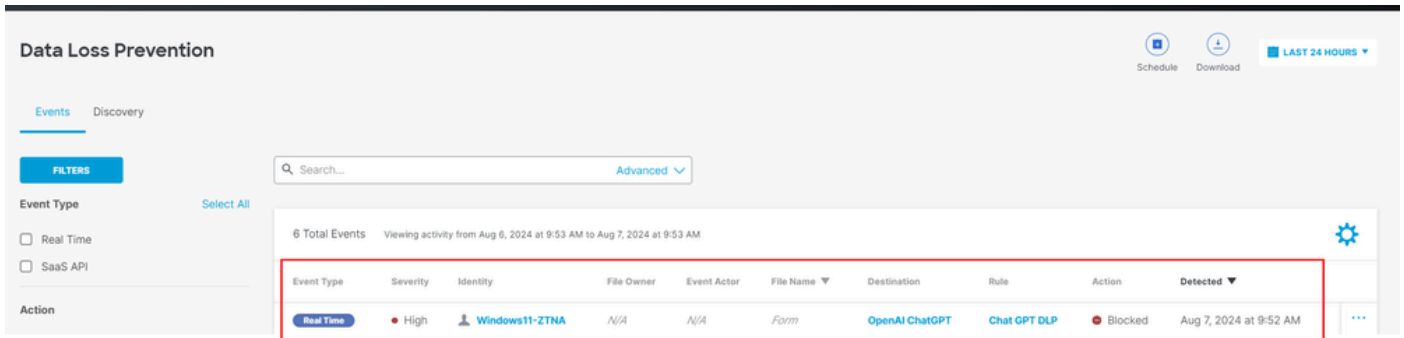
Exported Reports

Scheduled Reports

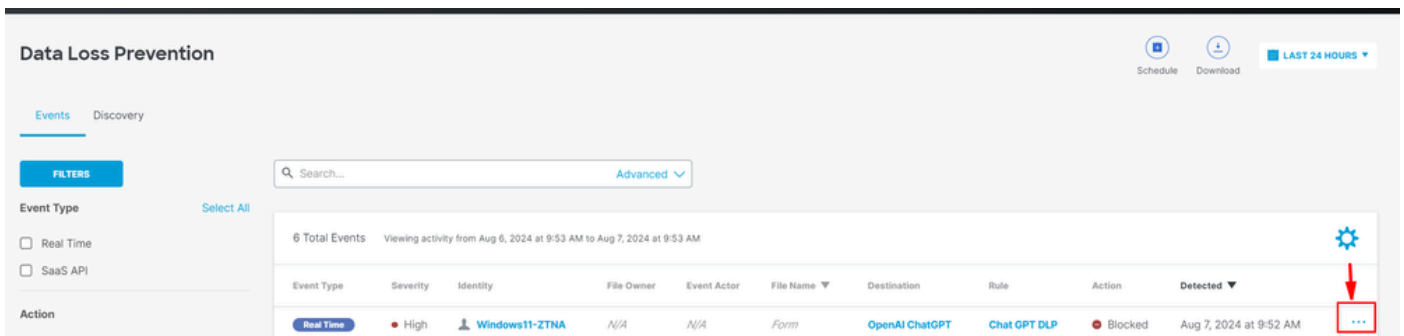
Saved Searches

Admin Audit Log

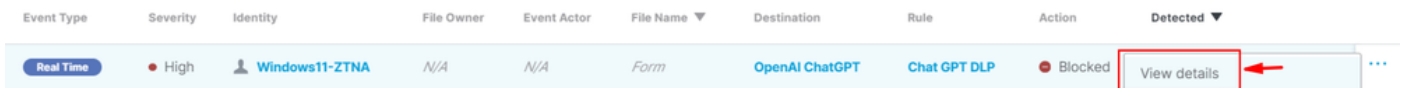
- 我們可以看到DLP事件。



- 按一下事件記錄檔結尾的三個點，以檢查事件的詳細資訊。



- 按一下 View details.



- 現在我們可以看到整個事件詳細資訊。

Event Details



Detected

Aug 7, 2024 at 9:52 AM

Action

 Blocked

File Name

Form

Identity

 **Windows11-ZTNA**

Application

OpenAI ChatGPT

Application Category

Generative AI

Destination URL

<http://chatgpt.com/backend-api/conversation>

- 展開分類以檢視與分類器匹配的內文。



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

def calculate_year_of_century(age):, def main():...



- 我們將檢視與DLP策略的分類器/分類相匹配的內容的所有詳細資訊。

Source Code

8 Matches Source Code

def calculate_year_of_century(age):, def main():...

age, then calculates the year they will turn 100 years old:\n\n`python`
def calculate_year_of_century(age):\n """Calculate the year the user will turn 100."""\n current_year =\n = 100 - age\n year_of_century = current_year + years_until_100\n return year_of_century\n\n**def main():**\n # Ask the user for their name and age\n name

疑難排解

- 確保與Open AI ChatGPT的Web請求匹配的訪問策略已啟用解密。
- 要快速檢查SSE是否解密了Open AI ChatGPT的流量，請檢查顯示常用名稱的網站證書，其中包含「Cisco Secure Access」關鍵字。

Certificate Viewer: chatgpt.com



General

Details

Issued To

Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>


Issued By


Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	<Not Part Of Certificate>



Validity Period



Issued On	Monday, August 5, 2024 at 10:14:04 PM
Expires On	Saturday, August 10, 2024 at 10:14:04 PM



ChatGPT x +

← → ↻  chatgpt.com

 chatgpt.com x


 ChatGPT  **Connection is secure** >


 Explore GP  **Cookies and site data** >


 **Site settings** 


Previous 30 Days


ChatGPT x +

← → ↻  chatgpt.com



 **Security** x
chatgpt.com

 ChatGPT

 Explore GP

 **Connection is secure**
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. [Learn more](#)

Previous 30 Days

Simple Python P  **Certificate is valid** 

Certificate Viewer: chatgpt.com



General

Details

Issued To

Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	<Not Part Of Certificate>

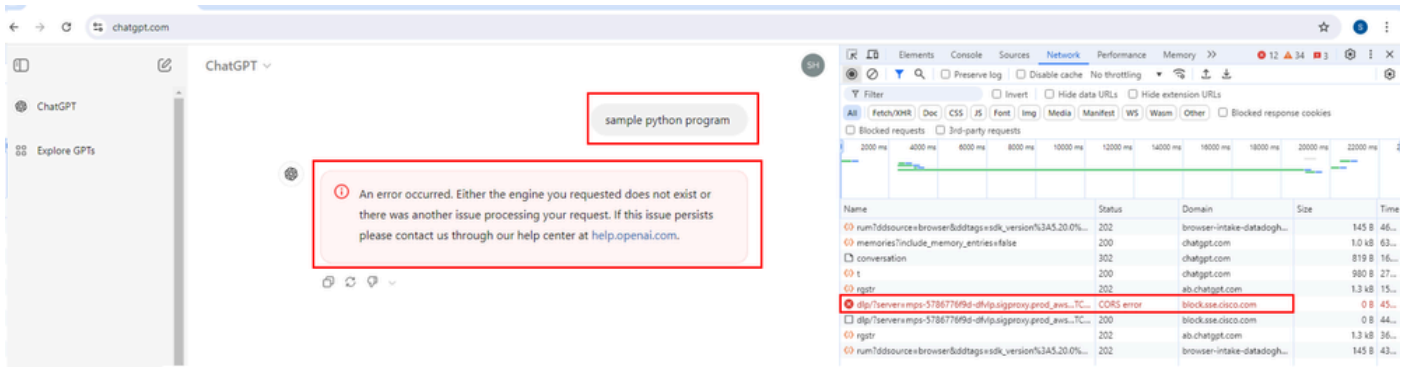
Validity Period

Issued On	Monday, August 12, 2024 at 10:52:16 PM
Expires On	Saturday, August 17, 2024 at 10:52:16 PM

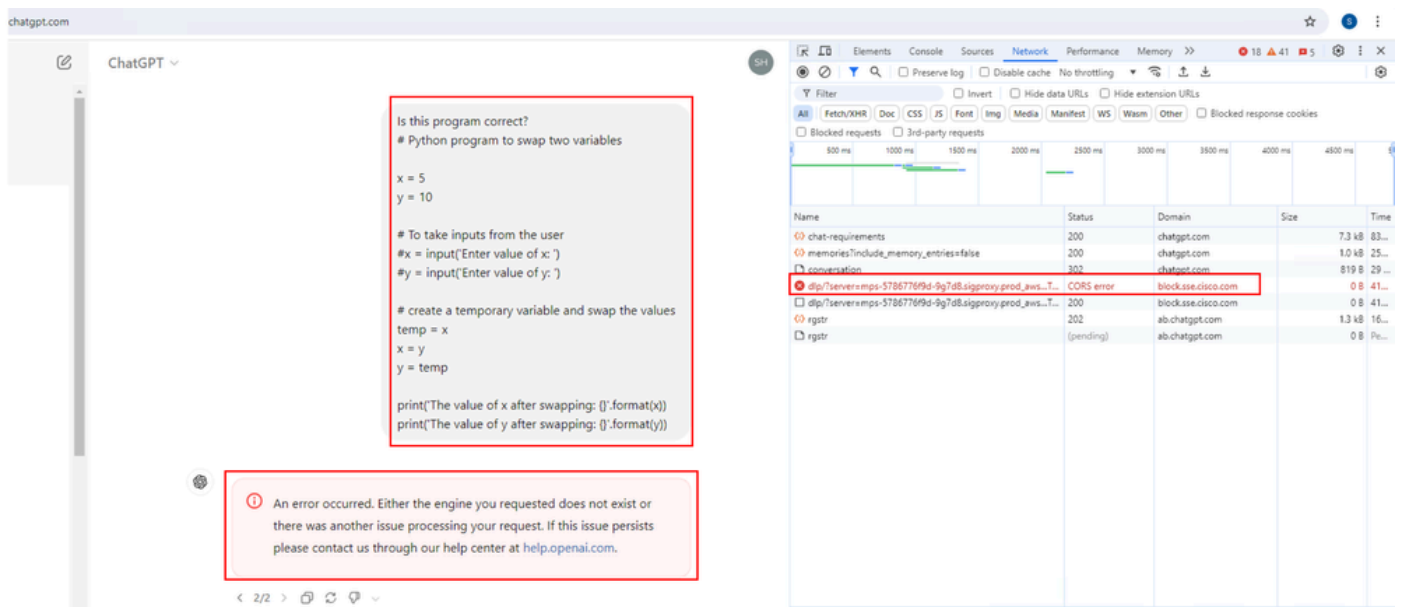
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- 打開ChatGPT >打開開發人員工具>選擇網路>下一步嘗試向ChatGPT詢問示例Python程式
- 請注意，該請求會生成一個塊。在域下，您將看到「block.sse.cisco.com」



- 詢問ChatGPT程式碼是否正確。
- 請注意，請求結果會生成一個塊，在「domain」下您會看到「block.sse.cisco.com」。



相關資訊

- [思科安全訪問使用手冊](#)
- [Cisco技術支援和下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。