

在安全访问中实施DLP以限制开放式AI ChatGPT用于编程

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

- [1. 创建数据分类以使用源代码数据标识符](#)
- [2. 创建DLP策略，并在其中调用数据分类“源代码”。](#)
- [3. 确保您对发往“聊天GPT”且已启用解密的流量拥有适当的互联网访问策略。](#)
- [4. 使用Open AI ChatGPT尝试下载或上传任何程序。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在安全访问中实施防数据丢失(DLP)，以限制Open AI ChatGPT用于编程和编码。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全访问
- DLP
- 打开AI ChatGPT

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全访问
- DLP
- 打开AI ChatGPT

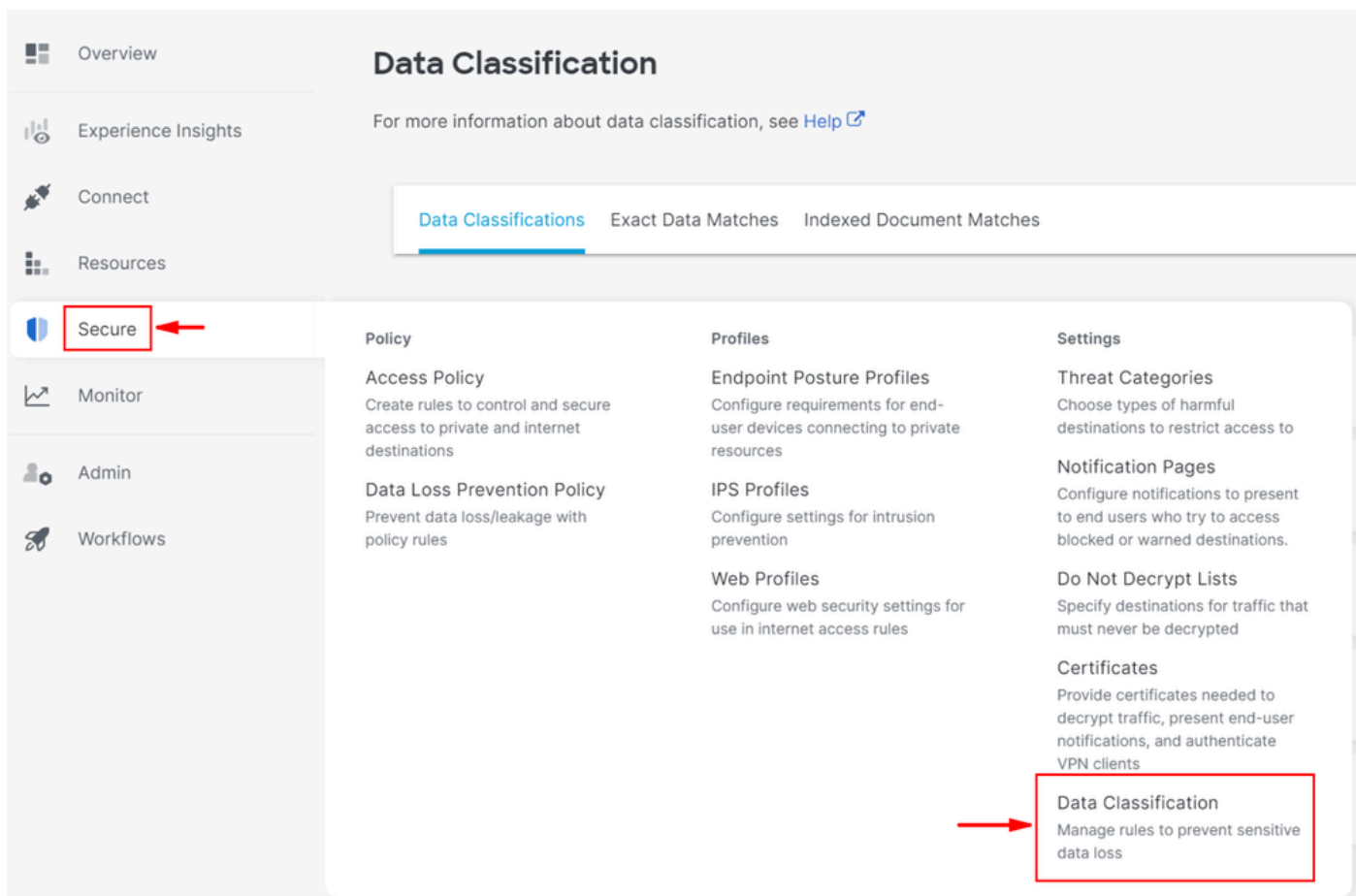
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

1. 创建数据分类以使用源代码数据标识符

导航到[安全访问控制面板](#)。

- 点击Secure>>Data Classification> Add



- 输入Data Classification Name>选择 Built-in Data Identifiers>搜索并选定Source Code

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

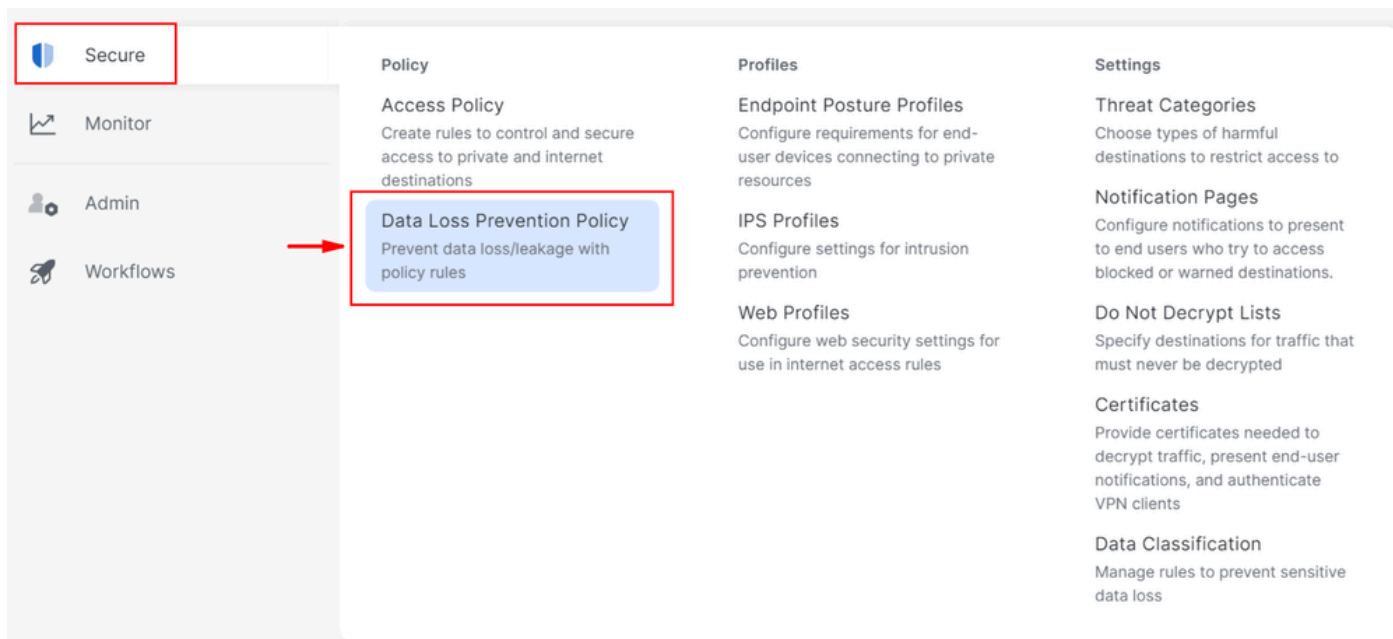
Built-in Data Identifiers

No Data Identifiers found.

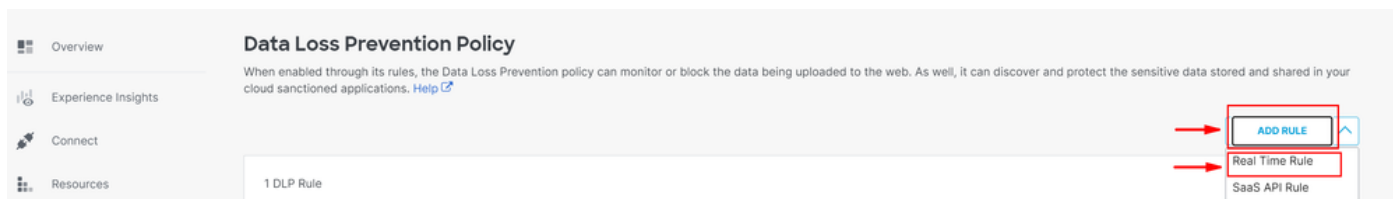
Custom Identifiers

2. 创建DLP策略，并在其中调用数据分类“源代码”。

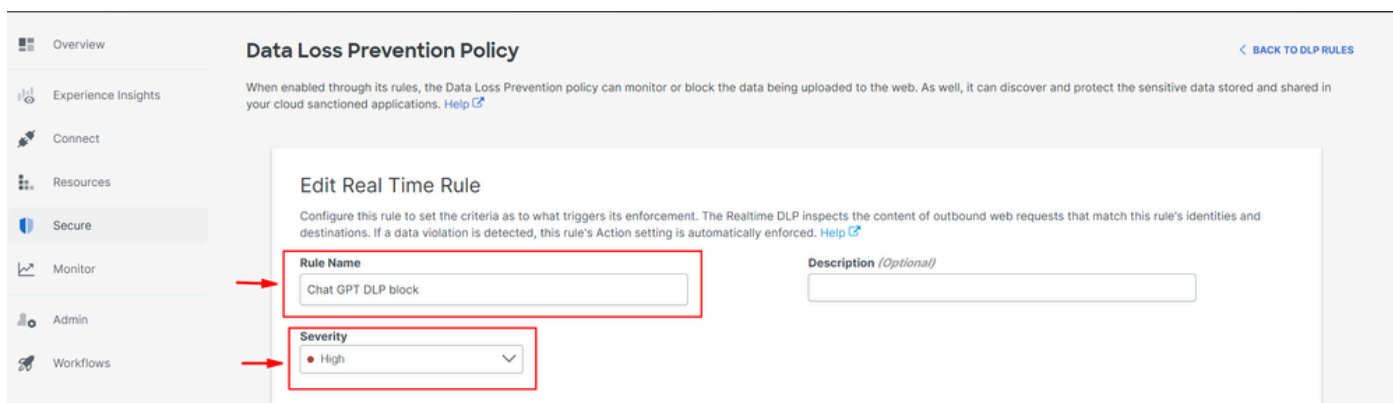
- 点击Secure> Data Loss Prevention Policy



- 点击Add Rule> Real Time Rule



- 输入Rule Name>设置适当的 Severity



- 在Data Classifications下，选择Content 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下，根据需要选择所需的身份

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Destinations下，选择 Select Destination Lists and Applications for Inclusion
- 选择Application Categories>选择 Generative AI>选择OpenAI API (Vetted)和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，您可以在触发规则时设置发送给最终用户的邮件通知（可选）

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

- 点击 Save

DELETE

CANCEL

SAVE



3. 确保您对发往“聊天GPT”且已启用解密的流量拥有适当的互联网访问策略。

示例：

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

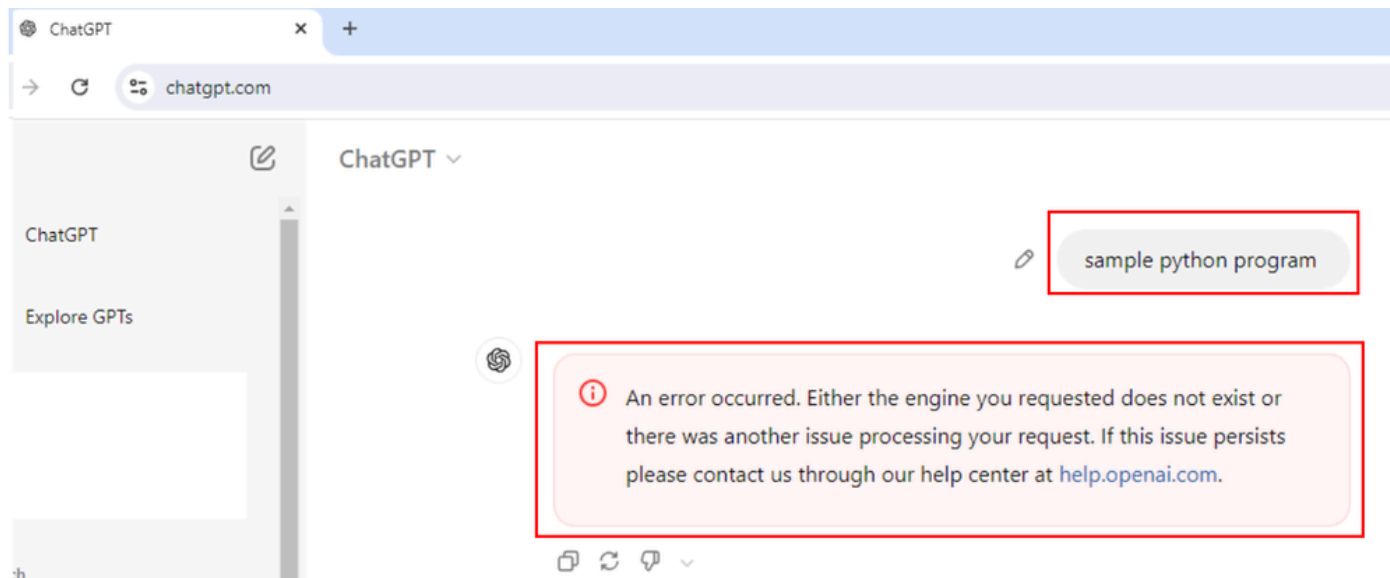


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- 请求一个示例python程序，此请求被阻止。




- 询问程序是否正确并阻止此请求。



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 >    ▾

验证

我们可以看到，当用户尝试向ChatGPT请求示例python程序时，请求会被阻止。
我们可以确认安全访问防数据丢失日志中是否触发了DLP事件。

- 转至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



View

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

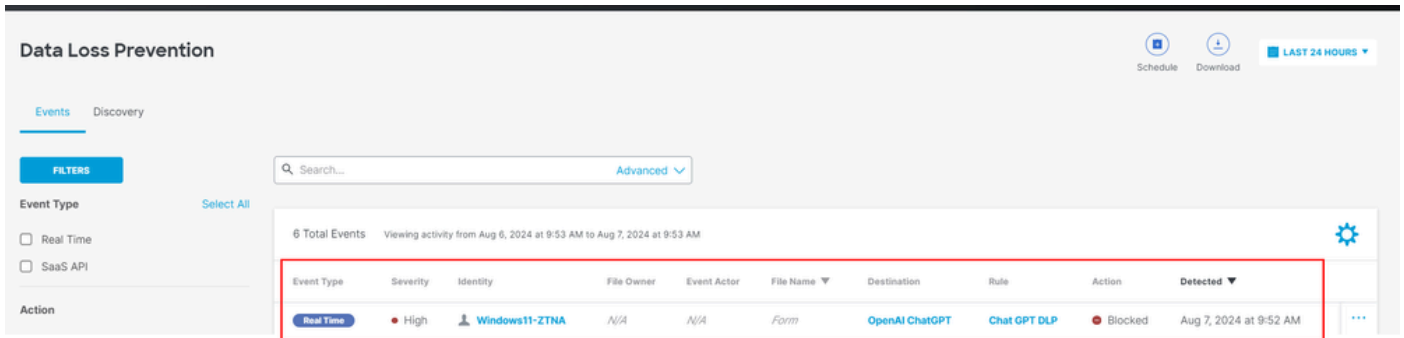
Exported Reports

Scheduled Reports

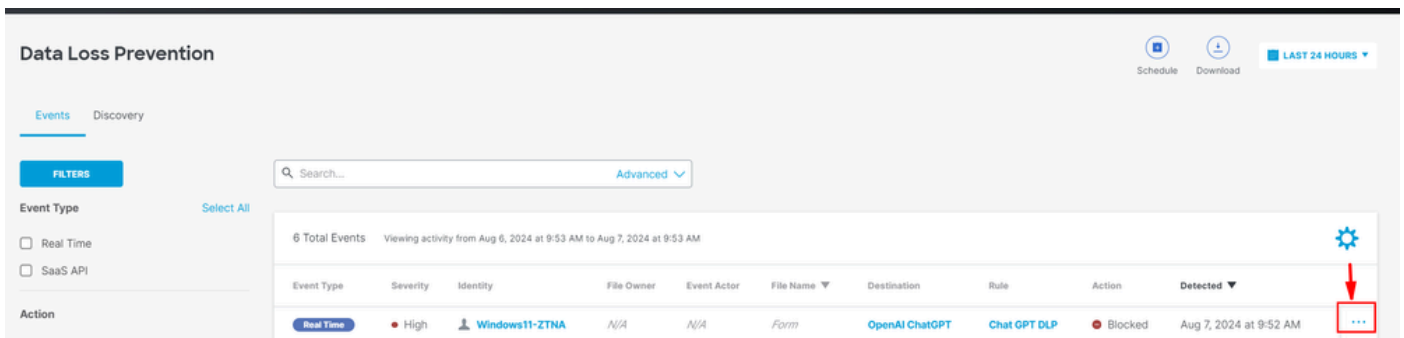
Saved Searches

Admin Audit Log

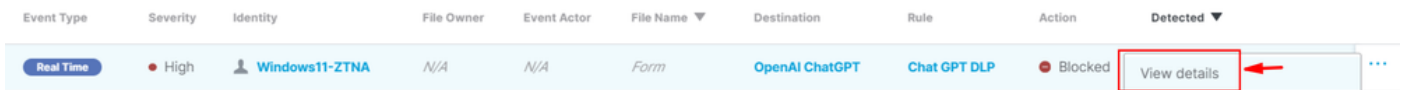
- 我们可以看到DLP事件。



- 单击事件日志末尾的三个点，查看事件的详细信息。



- 点击 View details.



- 现在，我们可以看到整个活动详细信息。

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>

- 展开分类以查看与分类器匹配的内容。



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- 我们将看到匹配分类器/DLP策略分类的所有内容详细信息。

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```\npython\n**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

故障排除

- 确保与Open AI ChatGPT的Web请求匹配的访问策略已启用解密。
- 要快速检查SSE是否解密了Open AI ChatGPT的流量，请检查显示常用名称的网站证书，其中包含关键字“Cisco Secure Access”。

Certificate Viewer: chatgpt.com



General

Details

Issued To

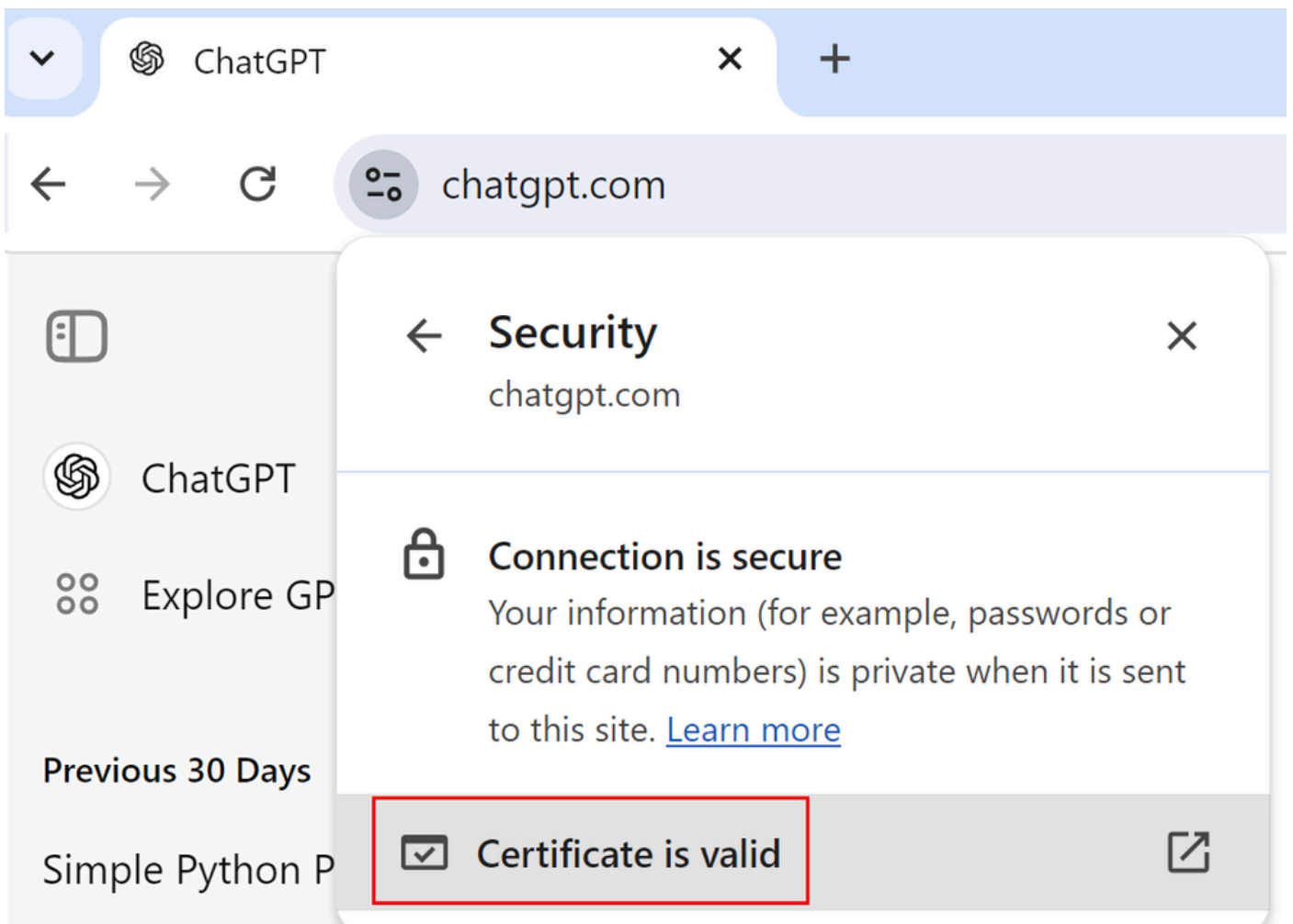
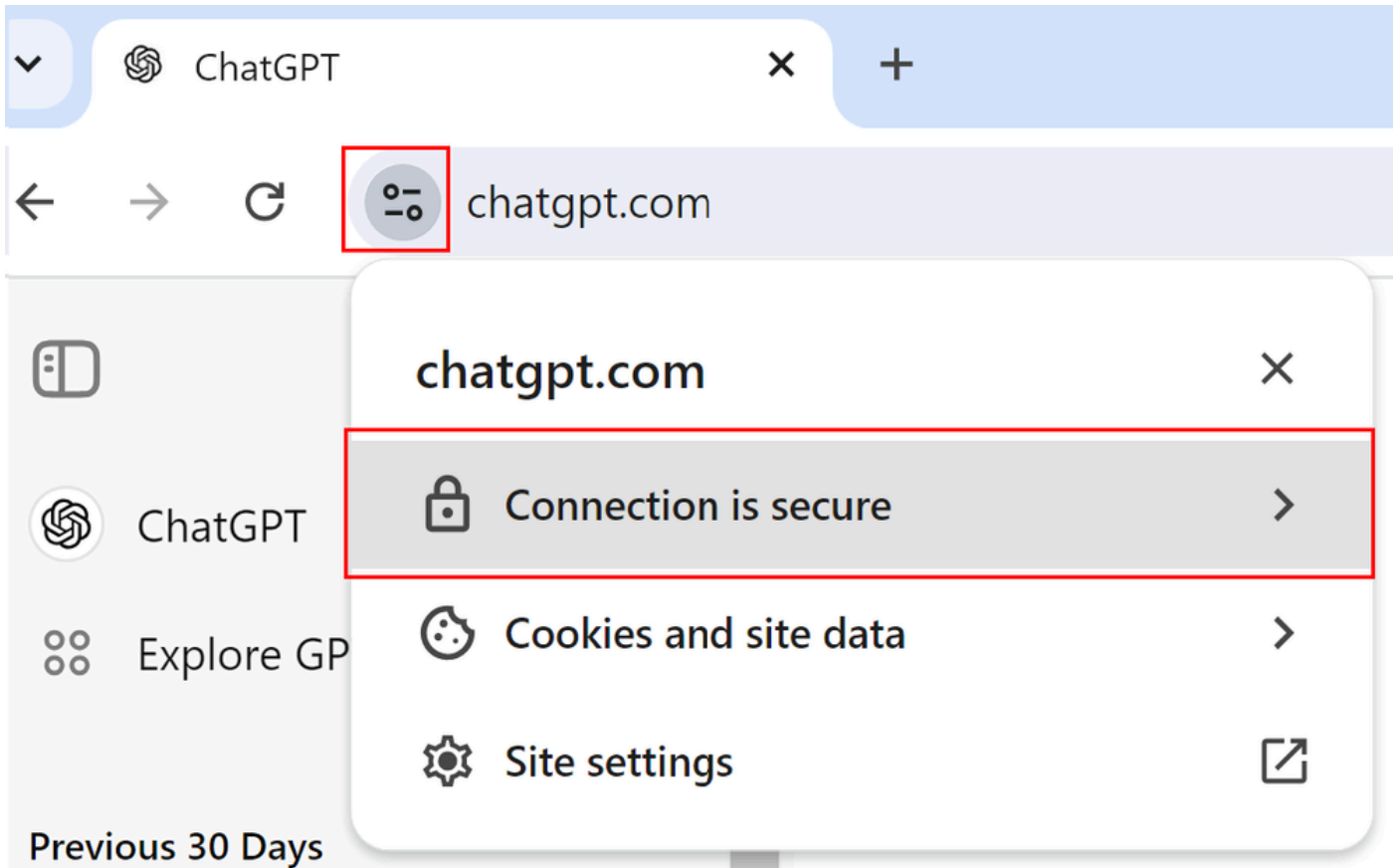
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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



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>

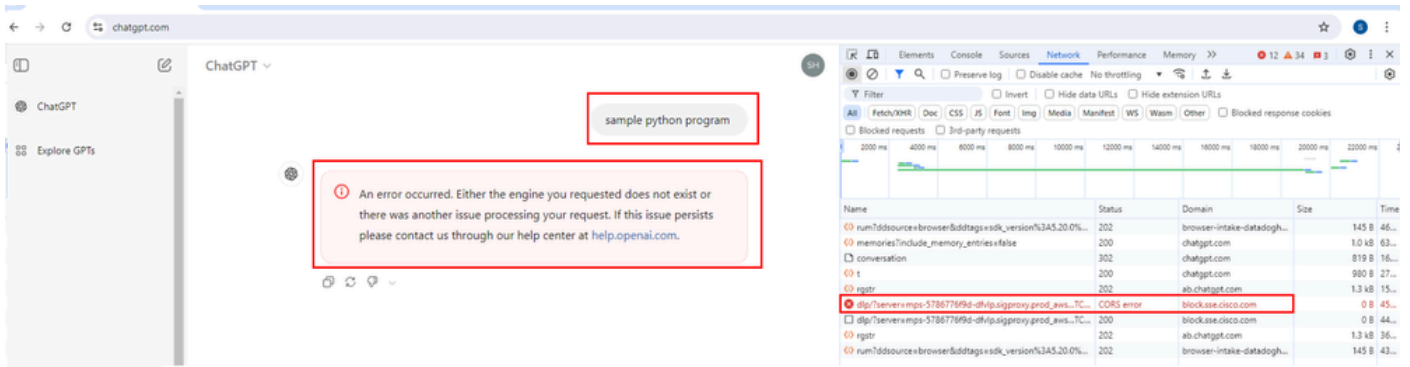
Validity Period

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

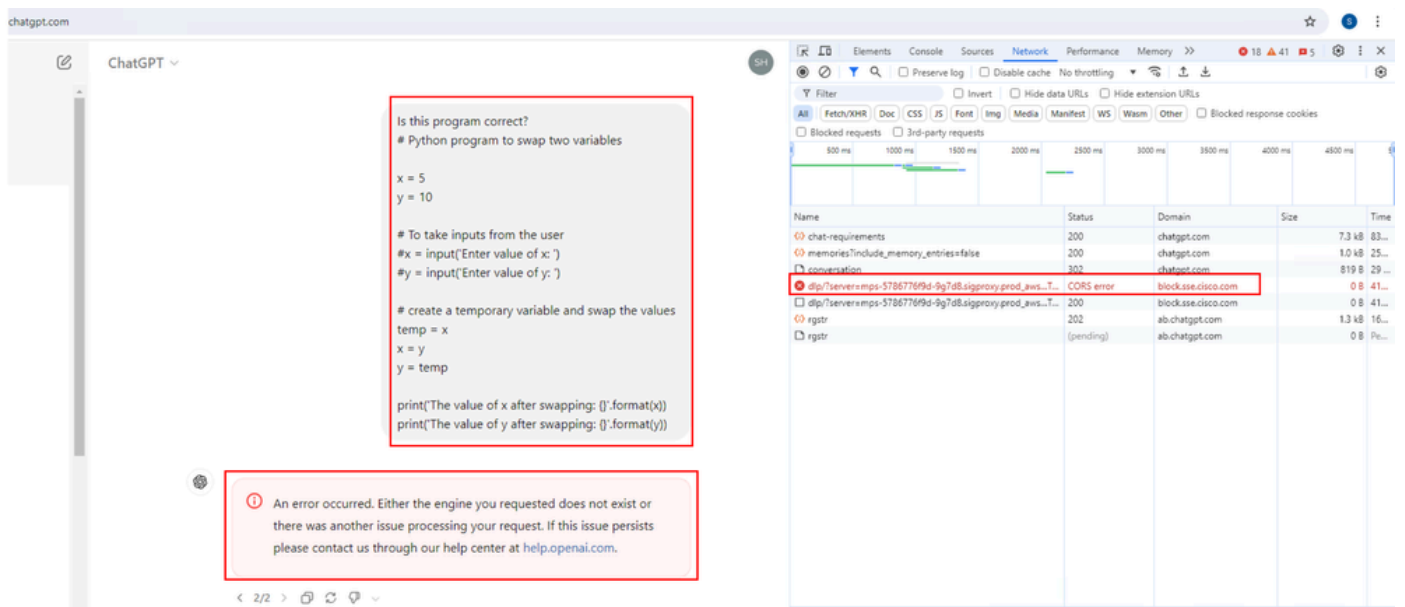
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- 打开ChatGPT > Open developer tools > Select Network > Next to ask ChatGPT for a sample python program
- 请注意，请求会导致阻止。在域下，您可以看到“block.sse.cisco.com”



- 询问ChatGPT程序代码是否正确。
- 请注意，请求会导致阻止，在“domain”下您会看到“block.sse.cisco.com”。



相关信息

- [思科安全访问用户指南](#)
- [Cisco技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。