

オープンAIチャットを制限するためのセキュアアクセスでのDLPの実装プログラミングのためのGPTの使用

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[1. ソースコードデータ識別子を使用するためのデータ分類の作成](#)

[2. DLPポリシーを作成し、その中のデータ分類を「ソースコード」と呼びます。](#)

[3. 復号化を有効にしたチャットGPTへのトラフィック用のインターネットアクセスポリシーが設定されていることを確認します。](#)

[4. Open AI ChatGPTを使用して、任意のプログラムをダウンロードまたはアップロードしてみてください。](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、プログラミングおよびコーディング用にオープンAI ChatGPTの使用を制限するために、セキュアアクセスにデータ損失防止(DLP)を実装する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアなアクセス
- DLP
- AI ChatGPTを開く

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアなアクセス
- DLP

- AI ChatGPTを開く

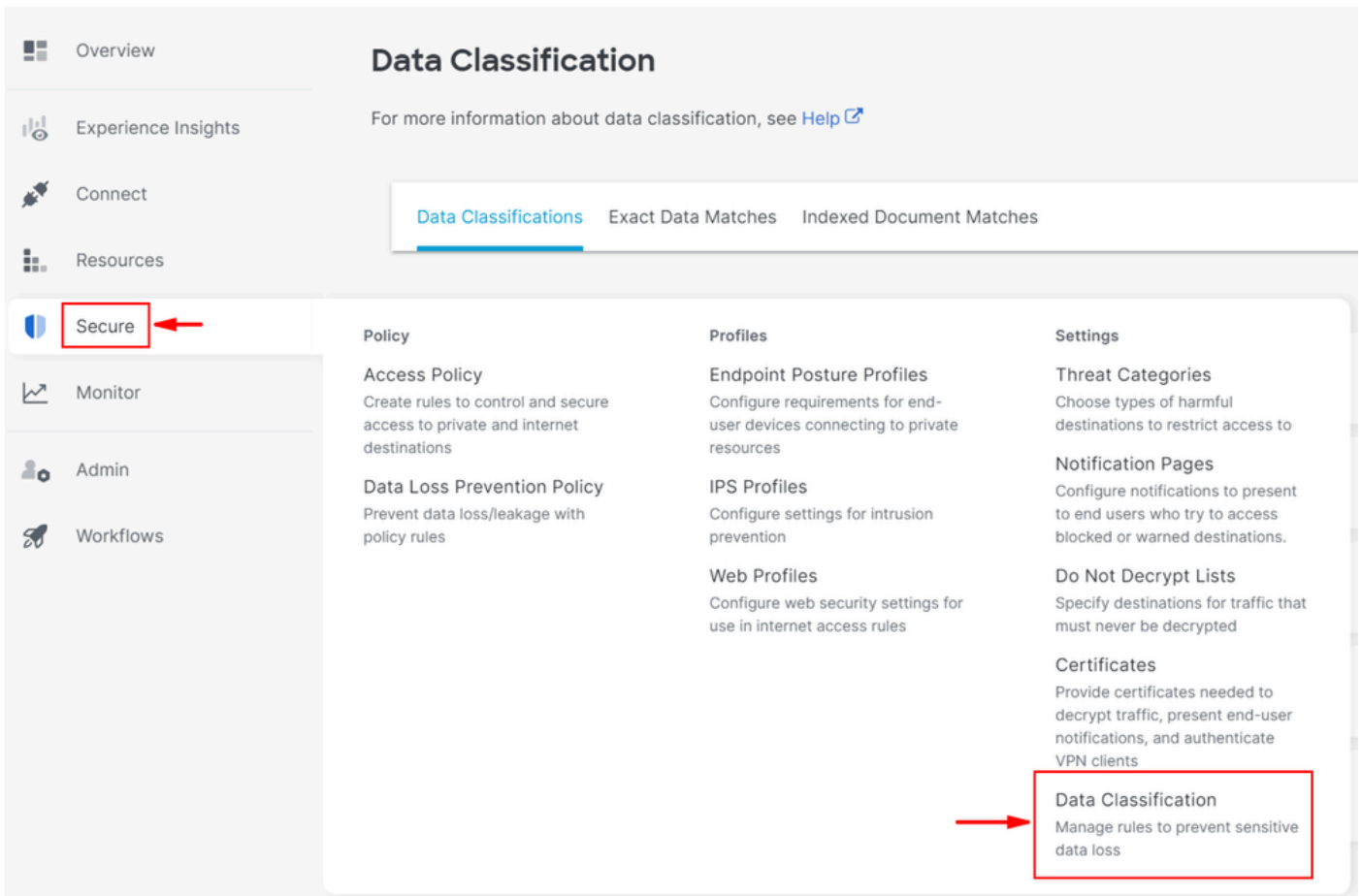
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

1. ソースコードデータ識別子を使用するためのデータ分類の作成

[Secure Access Dashboard](#)に移動します。

- Secure > Data Classificationの順にクリックします。 Add
Data Classification Name



- > **Select Built-in Data Identifiers** > Search forと入力してSource Code、これを選択します

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

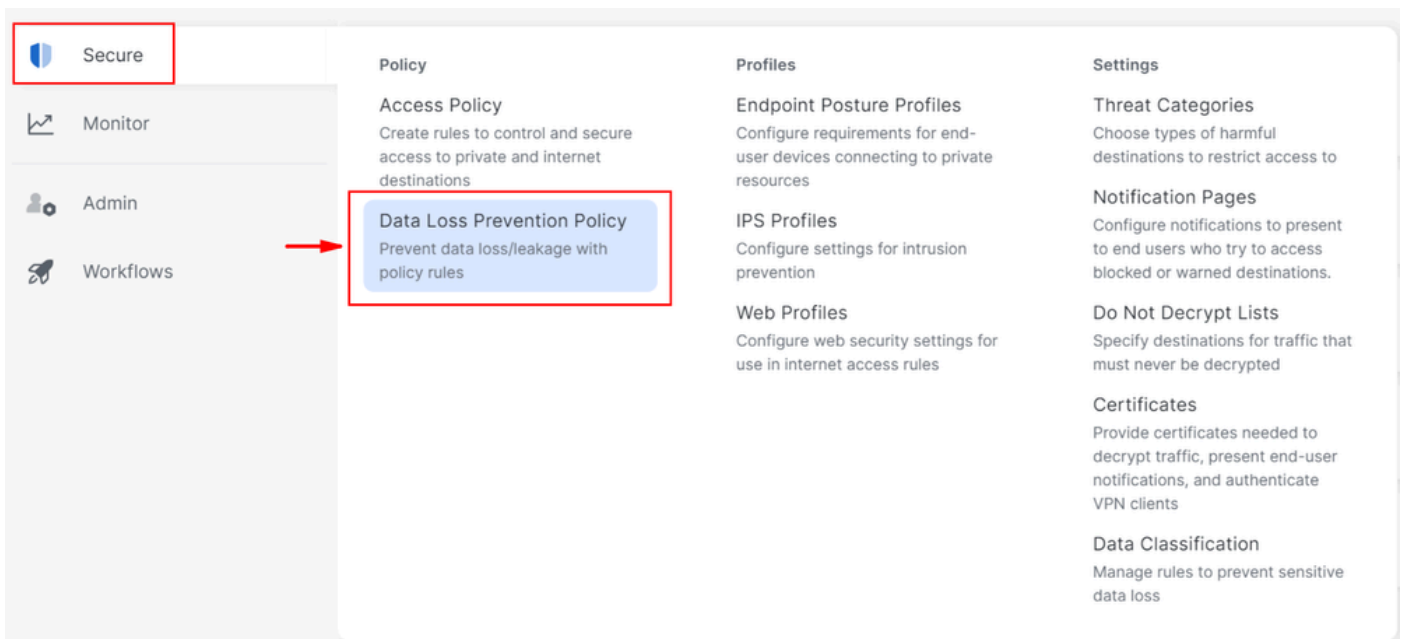
No Data Identifiers found.

Custom Identifiers

2. DLPポリシーを作成し、その中のデータ分類を「ソースコード」と呼びます。

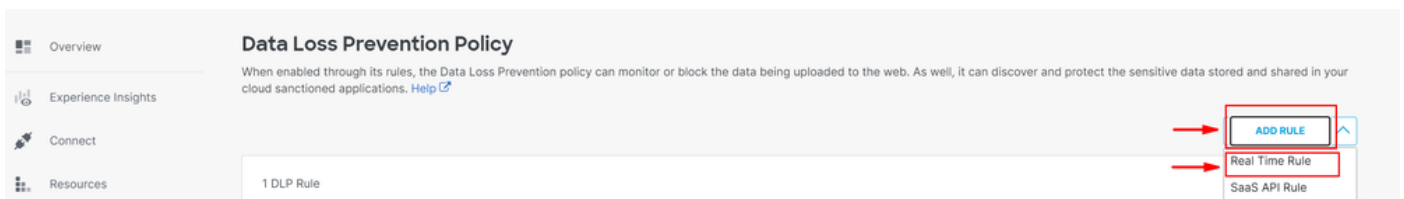
- Secureをクリックします。 Data Loss Prevention Policy

Add Rule



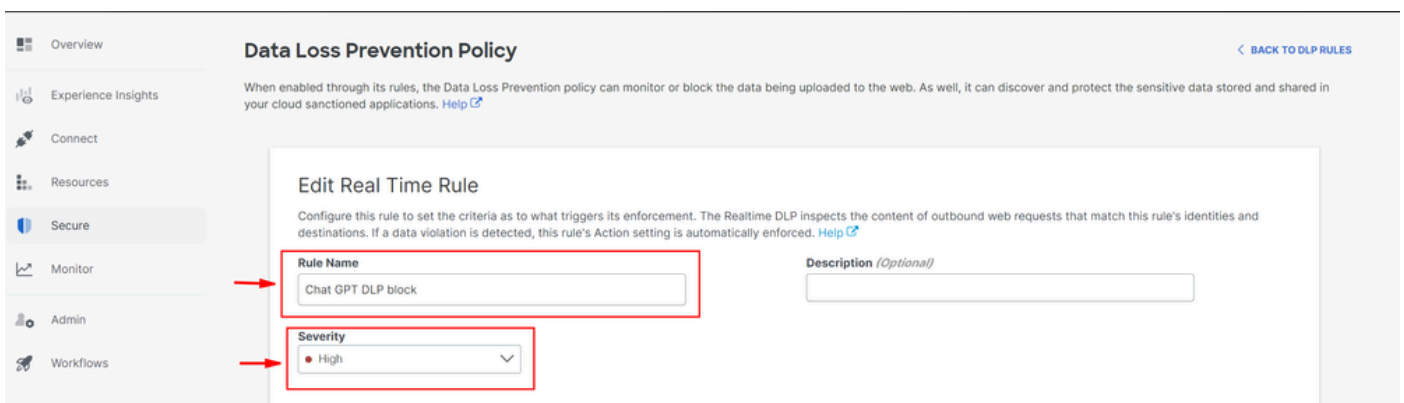
- ををクリックします。 Real Time Rule

Rule Name



- を入力し、適切な値に設定します Severity

Data ClassificationsContent



- selectで次を選択します。 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

- 必要に応じて必要なIDをIdentities選択します

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)	

- [通知先]で、次の項目を選択します Select Destination Lists and Applications for Inclusion
Application Categories
 - > SelectGenerative AI > SelectOpenAI API (Vetted)を選択し、「OpenAI ChatGPT (Vetted)」で 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 ×

- 選Action 下 Block

User Notifications

- では、ルールがトリガーされたときにエンドユーザーに送信される電子メール通知を設定できます (オプション)

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 ▼

- クリック Save

DELETE

CANCEL

SAVE



3. 復号化を有効にしたチャットGPTへのトラフィック用のインターネットアクセスポリシーが設定されていることを確認します。

以下に例を挙げます。

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

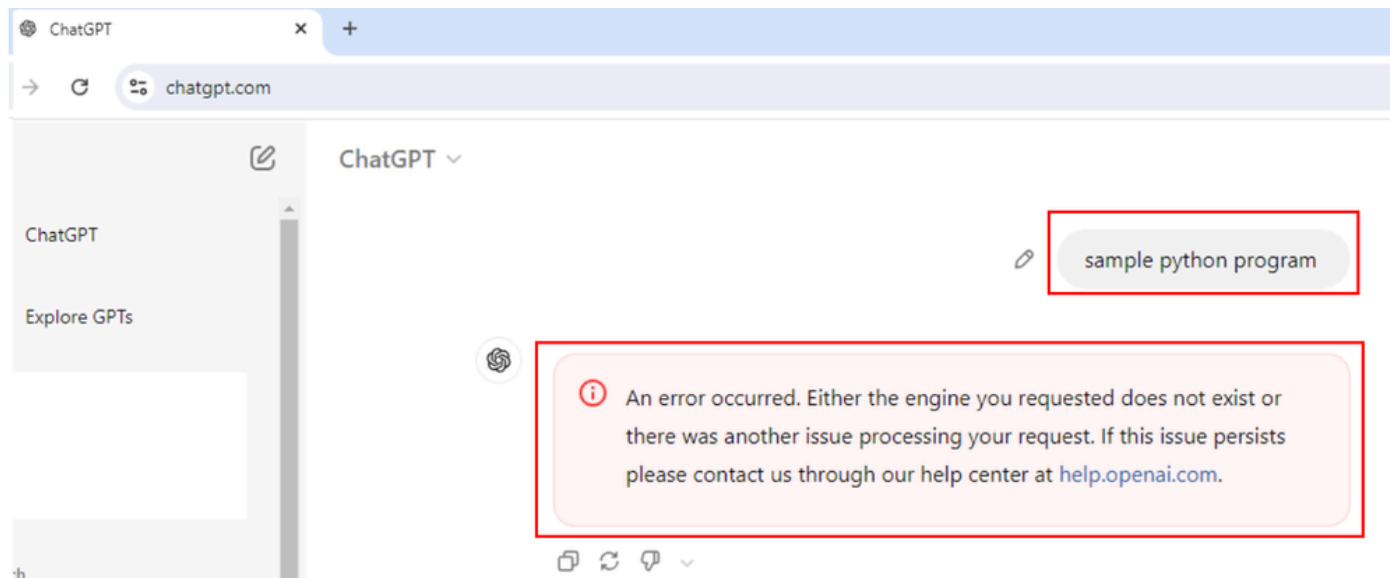


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- サンプルのPythonプログラムを要求すると、この要求はブロックされます。




- プログラムが正しいかどうかを尋ねると、この要求はブロックされます。



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 >    ▾

確認

ユーザがサンプルPythonプログラムをChatGPTに要求しようとする、要求がブロックされます。Secure Access Data Loss PreventionログでDLPイベントがトリガーされたことを確認できます。

- Monitorに移動します。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

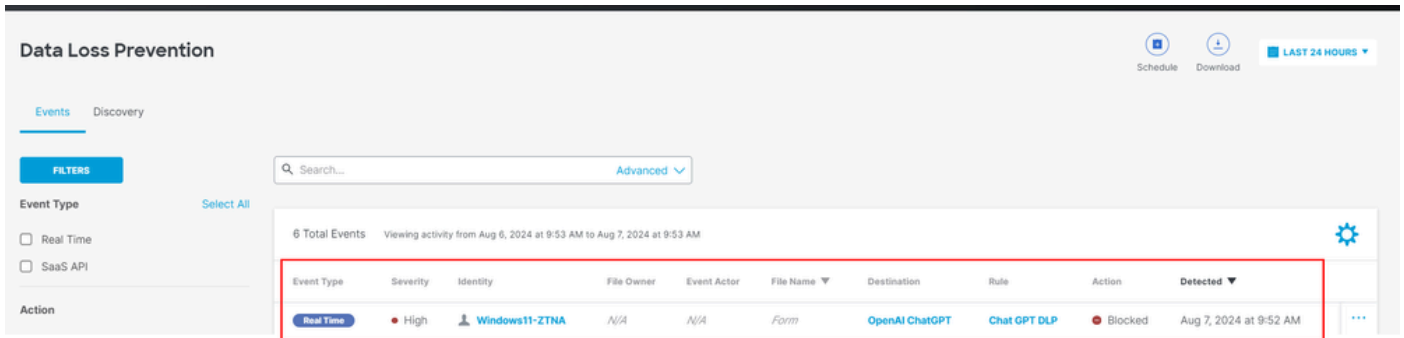
Exported Reports

Scheduled Reports

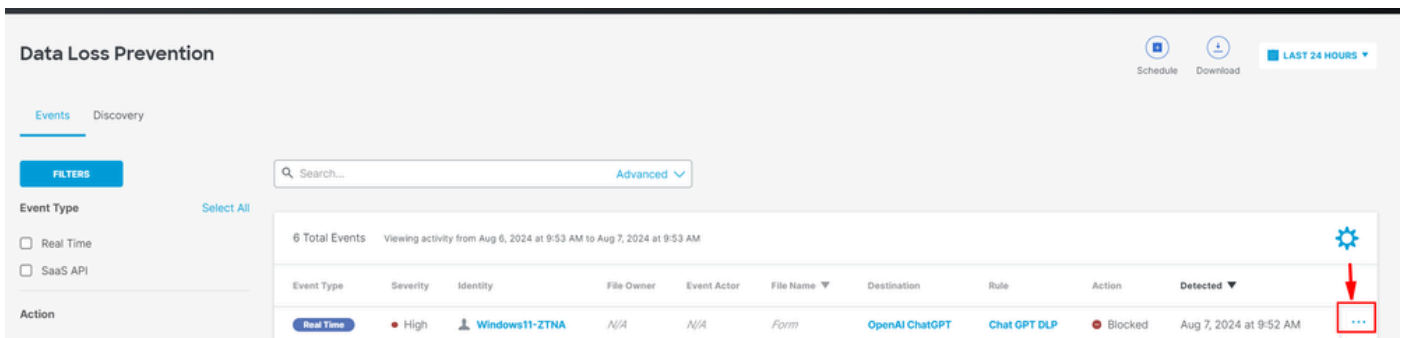
Saved Searches

Admin Audit Log

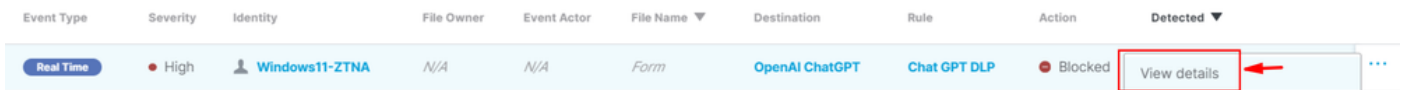
- DLPイベントが表示されます。



- イベントログの最後にある3つのドットをクリックして、イベントの詳細を確認します。



- クリック View details.



- これで、イベントの詳細全体が表示されます。

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>

- 分類を展開して、分類子に一致したコンテンツを確認します。



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- DLPポリシーの分類子/分類に一致したコンテンツのすべての詳細が表示されます。

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

トラブルシューティング

- Open AI ChatGPTのWeb要求を照合するアクセスポリシーで復号化が有効になっていることを確認します。
- SSEがOpen AI ChatGPTのトラフィックを復号化しているかどうかをすばやく確認するには、共通名にキーワード「Cisco Secure Access」が含まれていることを示すWebサイトの証明書を確認します。

Certificate Viewer: chatgpt.com



General

Details

Issued To

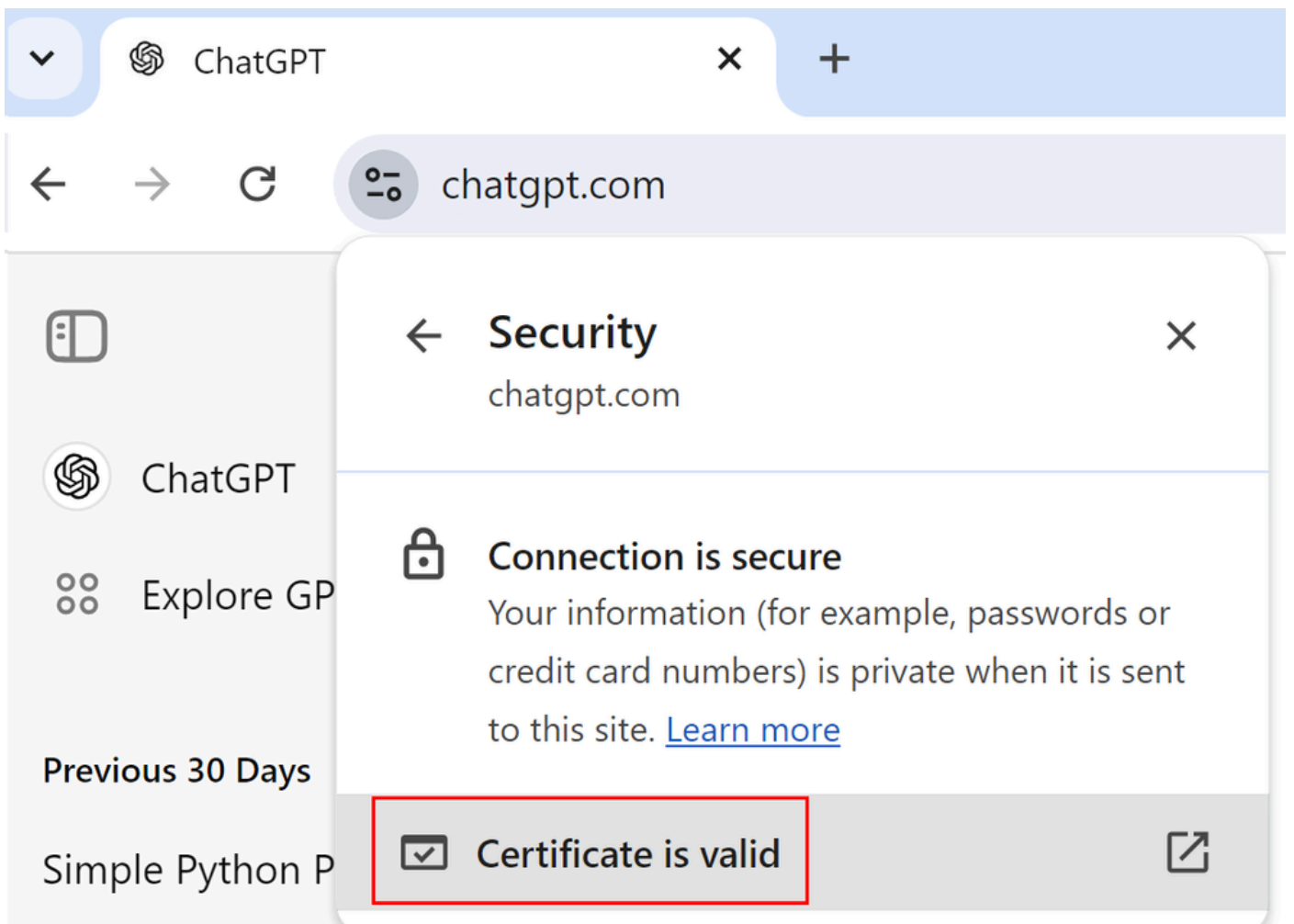
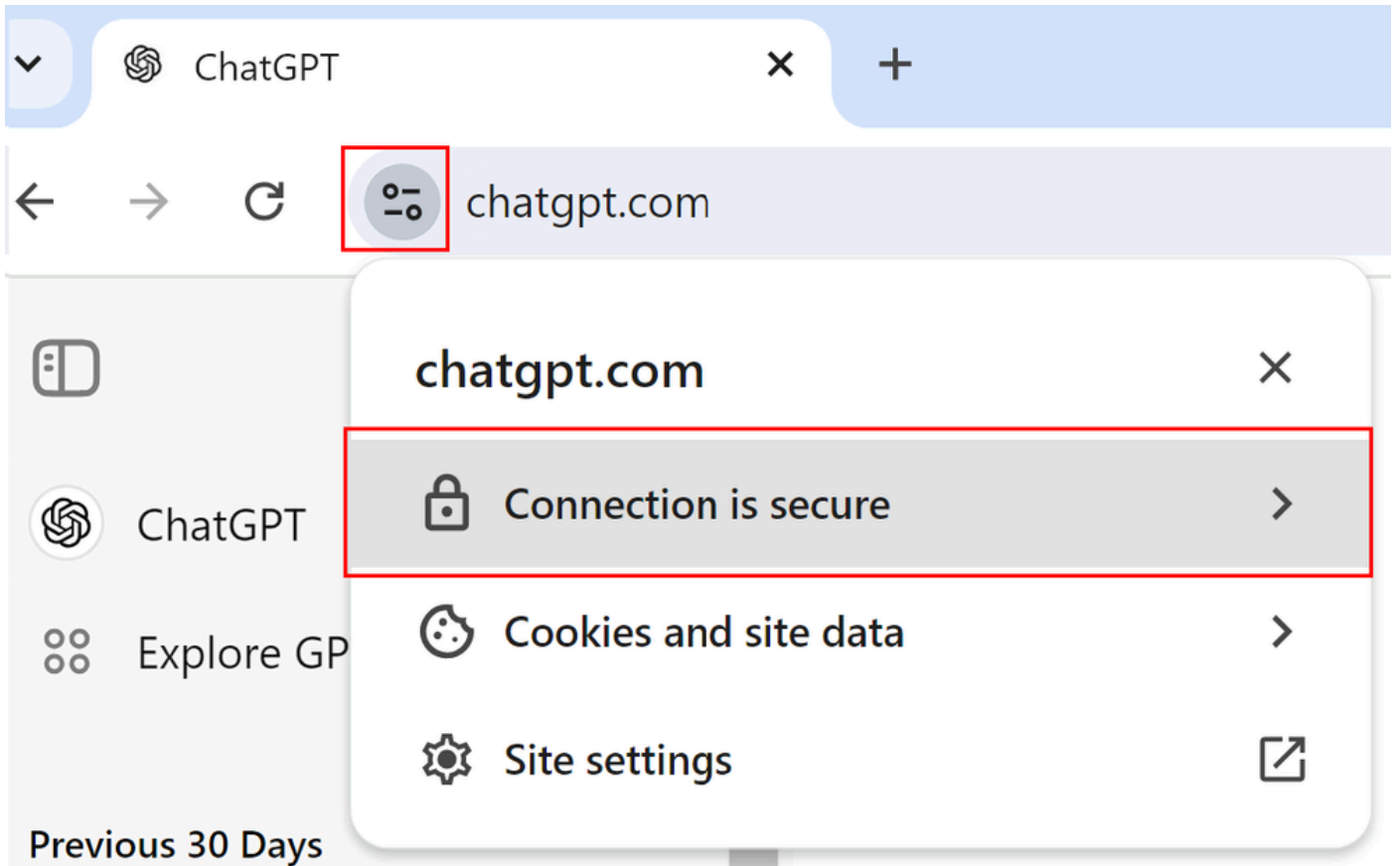
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

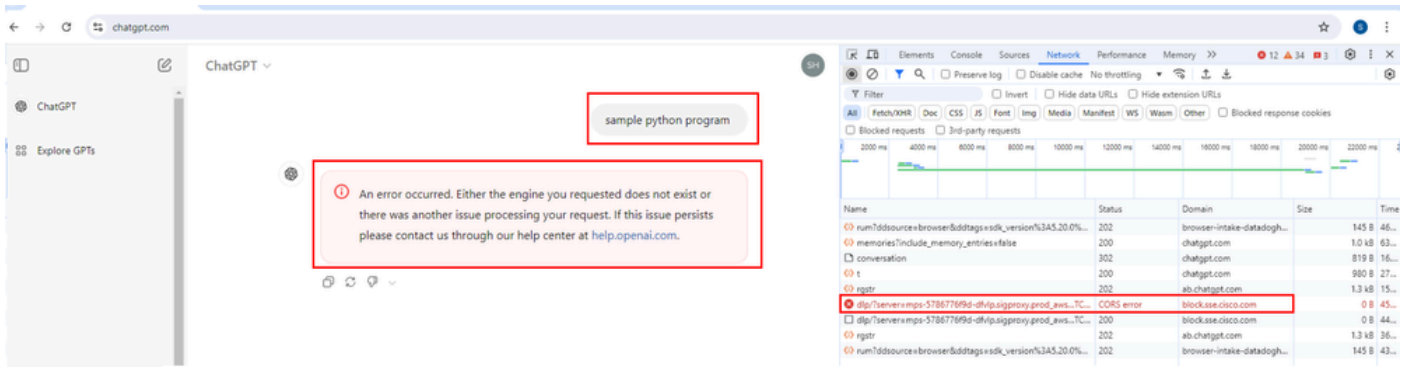
Validity Period

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

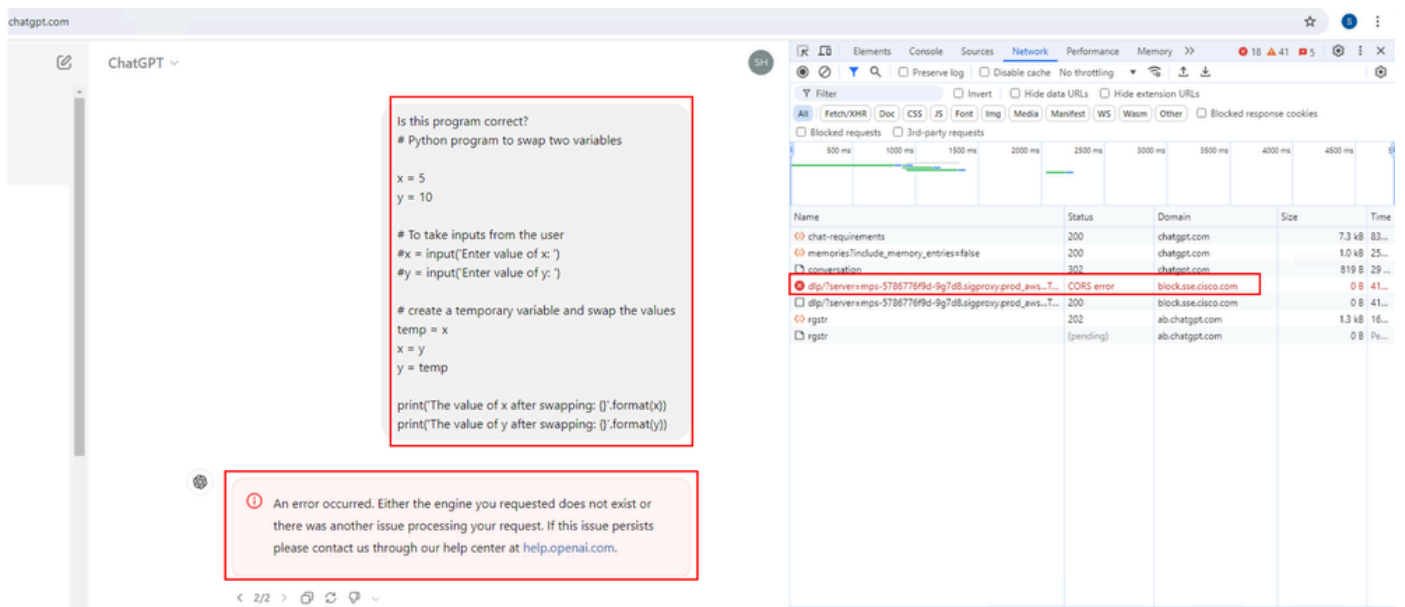
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- ChatGPTを開く > Open developer tools > Select Network > Next サンプルのPythonプログラムをChatGPTに要求する
- 要求の結果がブロックされることを確認します。ドメインの下に「block.sse.cisco.com



- プログラムコードが正しいかどうかをChatGPTに確認します。
- 要求の結果がブロックになり、「domain」の下に「block.sse.cisco.com」と表示されることを確認します。



関連情報

- [Cisco Secure Accessユーザガイド](#)
- [シスコテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。