

DLP in Secure Access to Restricted Open AI ChatGPT-gebruik voor programmeren implementeren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[1. Maak een gegevensclassificatie om het identificatiecode van de broncode te gebruiken](#)

[2. Maak een DLP-beleid en noem de gegevensclassificatie "broncode" erin.](#)

[3. Zorg ervoor dat u een internettoegangsbeleid hebt voor verkeer naar Chat GPT met decryptie ingeschakeld.](#)

[4. Use Open AI ChatGPT proberen om een programma te downloaden of te uploaden.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u DLP (Data Loss Prevention) in Secure Access kunt implementeren om het gebruik van Open AI ChatGPT voor programmering en codering te beperken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beveiligde toegang
- DLP
- AI-chatGPT openen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Beveiligde toegang
- DLP
- AI-chatGPT openen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

1. Maak een gegevensclassificatie om het Identificatiecode van de broncode te gebruiken

Navigeer naar [het Secure Access Dashboard](#).

- Klik op Secure > Data Classification > Add

The screenshot displays the 'Data Classification' configuration page in the Secure Access Dashboard. The left sidebar contains navigation options: Overview, Experience Insights, Connect, Resources, Secure (highlighted with a red box and arrow), Monitor, Admin, and Workflows. The main content area is titled 'Data Classification' and includes a help link. Below the title, there are three tabs: 'Data Classifications' (selected), 'Exact Data Matches', and 'Indexed Document Matches'. The main content is organized into four columns: Policy, Profiles, Settings, and a highlighted 'Data Classification' section. The 'Data Classification' section is highlighted with a red box and arrow, showing the option to 'Manage rules to prevent sensitive data loss'.

Policy	Profiles	Settings	Data Classification
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 Classification Manage rules to prevent sensitive data loss
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	

- Voer het veld Data Classification Name > **Selecteren** Built-in Data Identifiers > Zoeken naar Source Code in en selecteer het

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

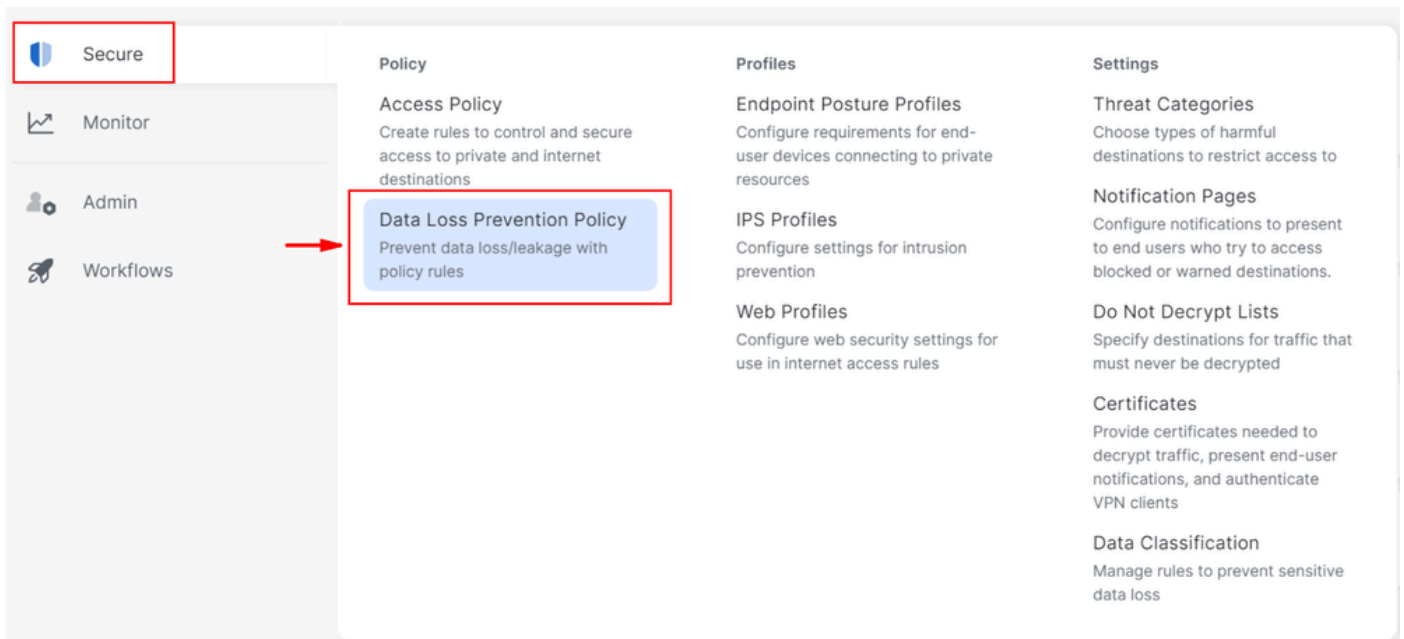
Built-in Data Identifiers

No Data Identifiers found.

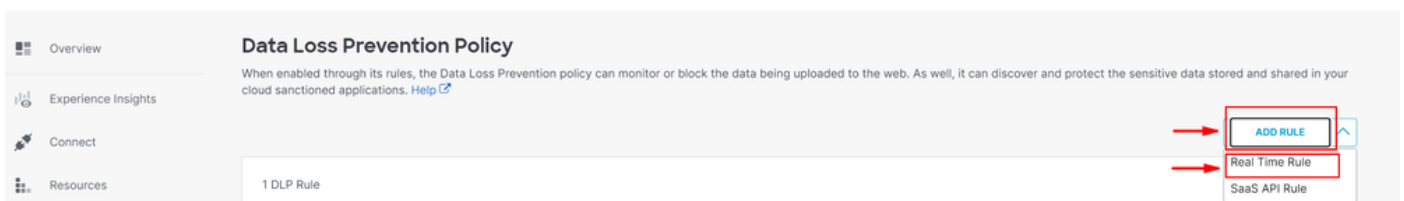
Custom Identifiers

2. Maak een DLP-beleid en noem de gegevensclassificatie "broncode" erin.

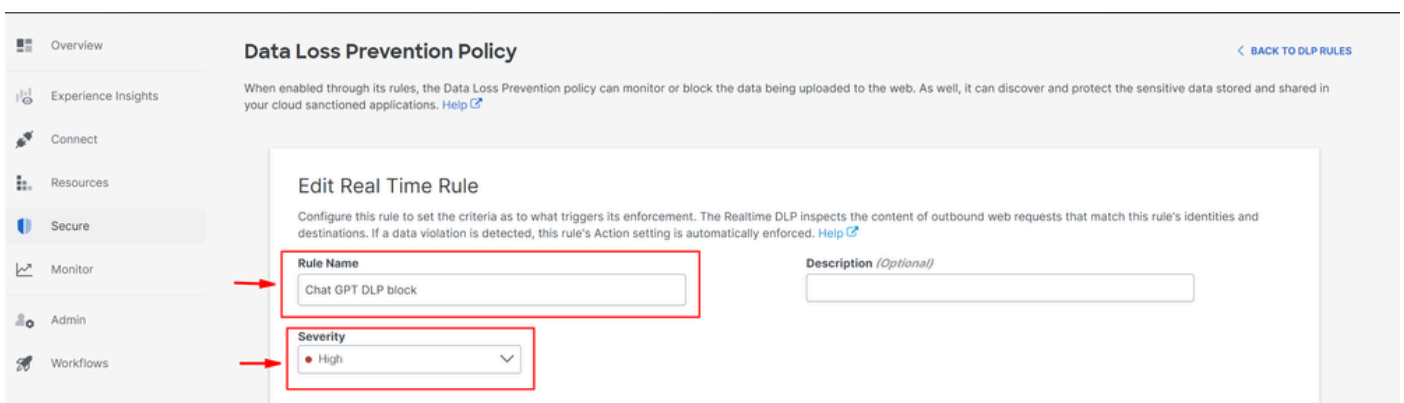
- Klik op Secure > Data Loss Prevention Policy



- Klik op Add Rule > Real Time Rule



- Geef een Rule Name > Stel de juiste waarde in Severity



- Selecteer onder Data Classifications ContentSelecteer 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

- Selecteer desgewenst de gewenste Identitiesidentiteiten

Identities
Select identities to add them to this rule.

Search Identities

All Identities

- AD Groups
- AD Users 4 >
- Network Tunnel Groups 6 >
- Networks 1 >
- Roaming Computers 4 >

5 Selected REMOVE ALL

- Roaming Computers 4
- onmicrosoft.com)

- Selecteer onder Bestemmingen Select Destination Lists and Applications for Inclusion
- Selecteer Application Categories> Selecteren Generative AI > Selecteren OpenAI API (Vetted) en 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 [×](#)

- Onder Acties selecteren Block
- Onder User Notifications, kunt u e-mailberichten aan eind - gebruikers opstellen, wanneer de regel wordt teweeggebracht (facultatief)

Action

Choose to monitor or block content for this rule.

Block [v](#)

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 [v](#)

- Klik op Save

DELETE

CANCEL

SAVE



3. Zorg ervoor dat u een internettoegangsbeleid hebt voor verkeer naar Chat GPT met decryptie ingeschakeld.

Voorbeeld:

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

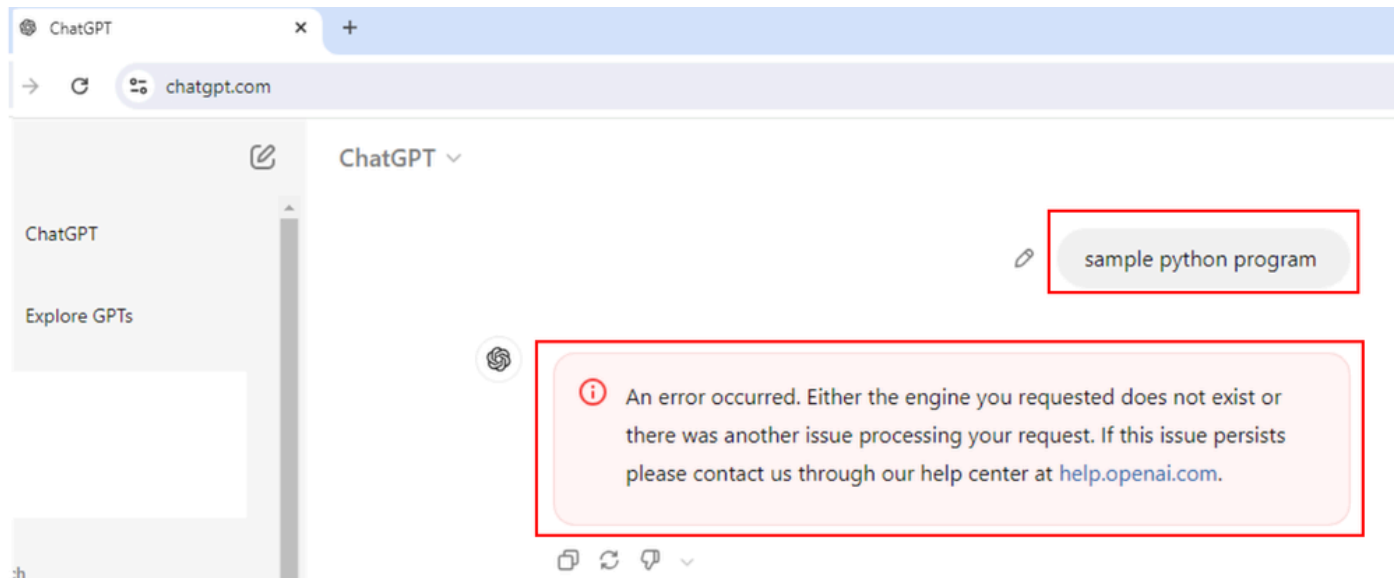


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- Vraag om een voorbeeldpython programma en dit verzoek wordt geblokkeerd.




- Vraag of het programma juist is of niet en deze aanvraag wordt geblokkeerd.



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 >    ▾

Verifiëren

We kunnen zien wanneer de gebruiker probeert om ChatGPT te vragen voor een voorbeeldpython-programma, het verzoek wordt geblokkeerd. We kunnen bevestigen dat een DLP-gebeurtenis is geactiveerd in Secure Access Data Loss Prevention-logboeken.

- Ga naar 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

- We kunnen het DLP-evenement zien.

Data Loss Prevention

Schedule Download LAST 24 HOURS

Events Discovery

FILTERS

Search... Advanced

6 Total Events Viewing activity from Aug 6, 2024 at 9:53 AM to Aug 7, 2024 at 9:53 AM

Event Type	Severity	Identity	File Owner	Event Actor	File Name	Destination	Rule	Action	Detected
Real Time	High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52 AM

- Klik op de drie punten aan het einde van het gebeurtenissenlogboek om meer details over de gebeurtenis te controleren.

Data Loss Prevention

Schedule Download LAST 24 HOURS

Events Discovery

FILTERS

Search... Advanced

6 Total Events Viewing activity from Aug 6, 2024 at 9:53 AM to Aug 7, 2024 at 9:53 AM

Event Type	Severity	Identity	File Owner	Event Actor	File Name	Destination	Rule	Action	Detected
Real Time	High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52 AM

- Klik op View details.

Event Type	Severity	Identity	File Owner	Event Actor	File Name	Destination	Rule	Action	Detected
Real Time	High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	Blocked	View details

- Nu zien we de volledige eventdetails.

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>

- Breid de classificatie uit om te zien welke inhoud overeenkomt met de classificator.



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- We zien alle details van de inhoud die overeenkwam met de classificator / classificatie van het DLP-beleid.

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\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

Problemen oplossen

- Zorg ervoor dat het toegangsbeleid dat overeenkomt met webaanvragen voor Open AI ChatGPT heeft decryptie ingeschakeld.
- Als u snel wilt controleren of SSE verkeer decodeert voor Open AI ChatGPT, controleert u het certificaat van de website waarop de veelvoorkomende naam "Cisco Secure Access" bevat.

Certificate Viewer: chatgpt.com



General

Details

Issued To

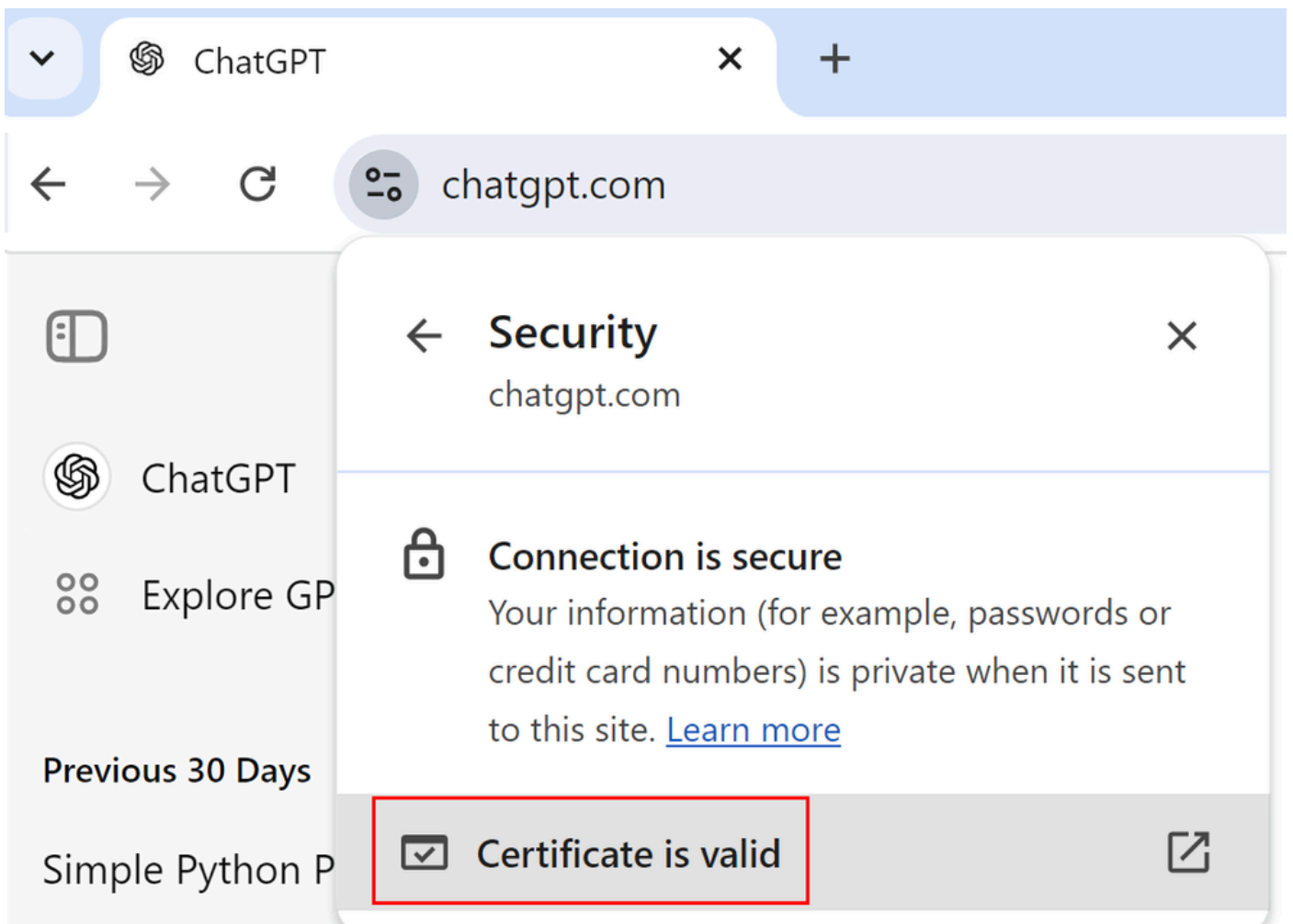
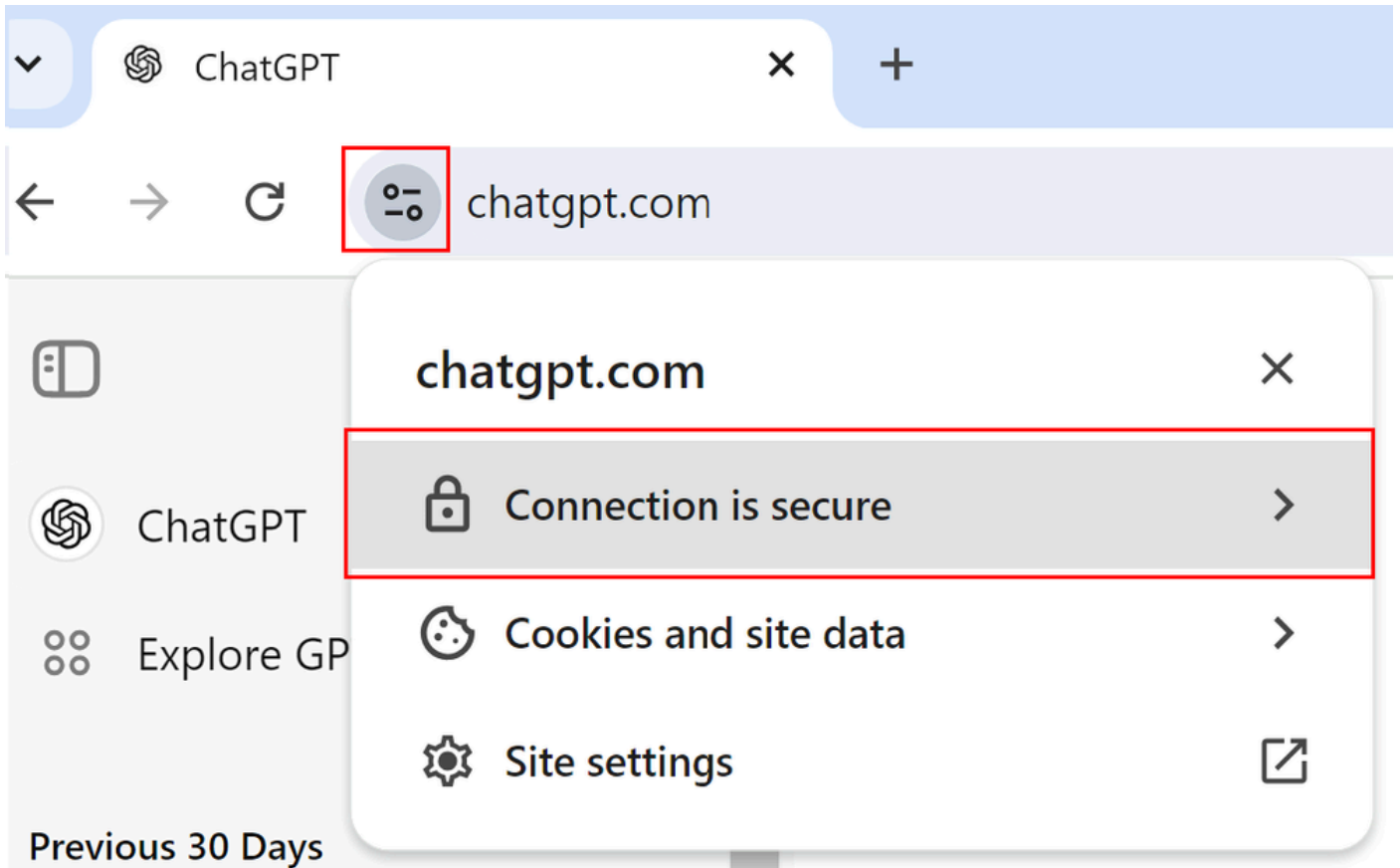
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

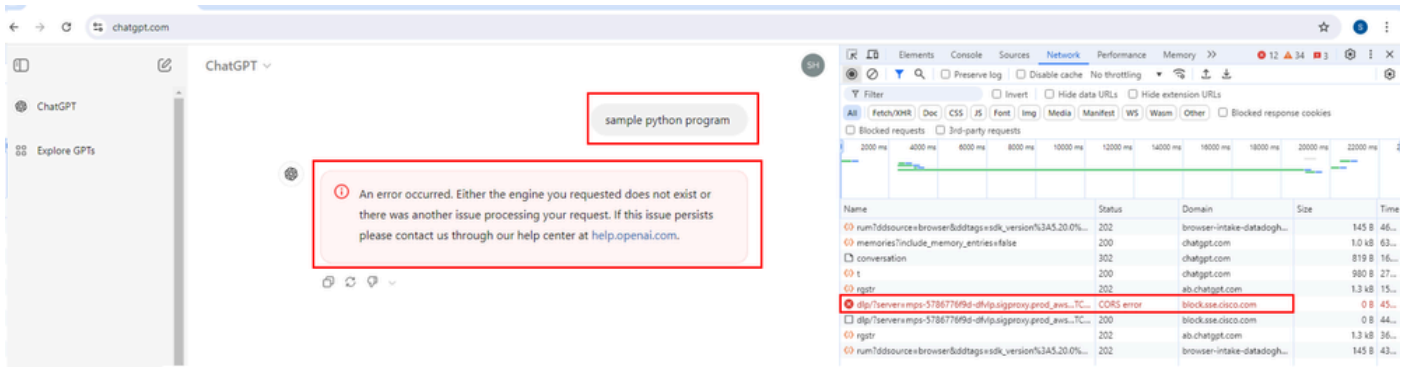
Validity Period

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

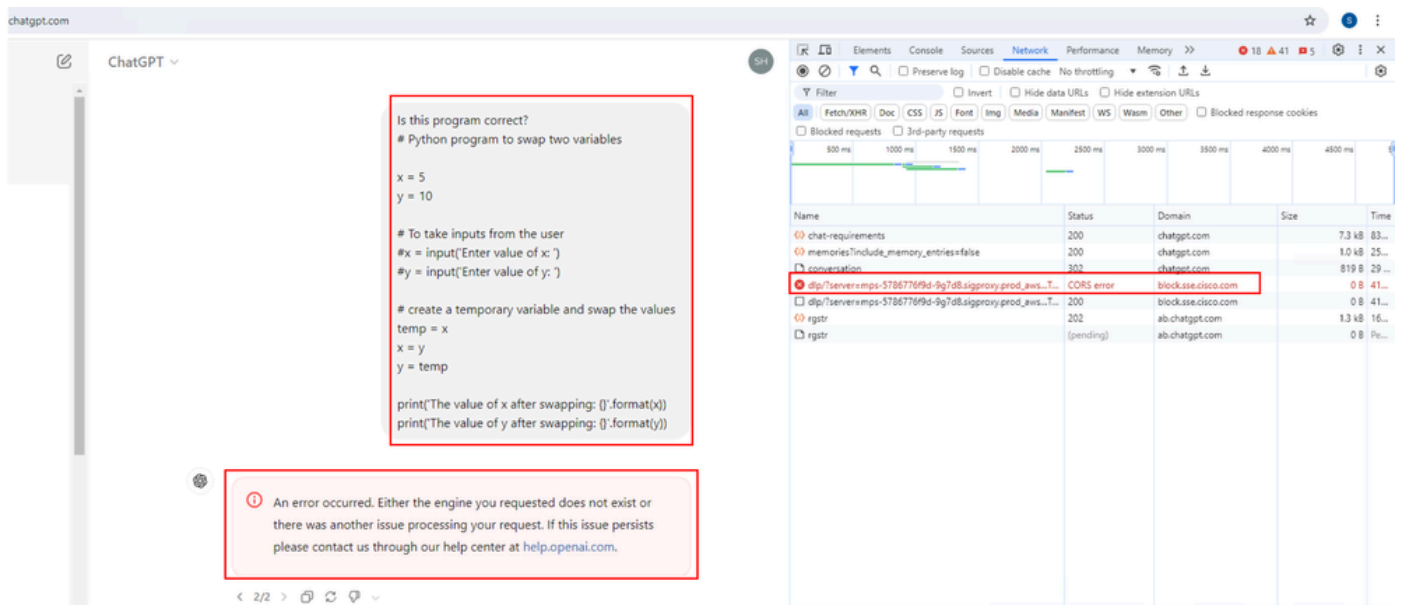
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bddd3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- Open ChatGPT > Open developer tools > Selecteer Netwerk > Volgende poging om ChatGPT te vragen voor een voorbeeldpython programma
- Merk op dat het verzoek resulteert in een blokkering. Onder het domein zie je "block.sse.cisco.com"



- Vraag ChatGPT of de programmacode correct is.
- Merk op dat het verzoek resulteert in een blok en onder "domein" zie je "block.sse.cisco.com".



Gerelateerde informatie

- [Gebruikershandleiding voor Cisco Secure Access](#)
- [Cisco technische ondersteuning en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.