

Implementierung von DLP in Secure Access zur Beschränkung der Verwendung von Open AI ChatGPT für die Programmierung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[1. Erstellen einer Datenklassifizierung zur Verwendung der Quellcodedaten-ID](#)

[2. Erstellen Sie eine SvD-Policy, und rufen Sie die Datenklassifizierung als "Quellcode" auf.](#)

[3. Stellen Sie sicher, dass Sie über eine Internet-Zugangsrichtlinie für den Datenverkehr in Richtung Chat-GPT mit aktivierter Entschlüsselung verfügen.](#)

[4. Using Open AI ChatGPT versuchen, jedes Programm herunterzuladen oder hochzuladen.](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Data Loss Prevention (DLP) in Secure Access implementiert wird, um die Verwendung von Open AI ChatGPT für Programmierung und Codierung einzuschränken.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff
- SvD
- AI-ChatGPT öffnen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sicherer Zugriff

- SvD
- AI-ChatGPT öffnen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

1. Erstellen einer Datenklassifizierung zur Verwendung der Quellcodedaten-ID

Navigieren Sie zum [Dashboard für sicheren Zugriff](#).

- Klicken Sie auf Secure > Data Classification > Add

The screenshot shows the Microsoft Secure dashboard. On the left is a navigation sidebar with 'Secure' highlighted by a red box and a red arrow pointing to it. The main content area is titled 'Data Classification' and includes a 'Help' link. Below the title 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 'Data Classification'. The 'Data Classification' item at the bottom right is highlighted with a red box and a red arrow pointing to it. The 'Data Classification' item description is 'Manage rules to prevent sensitive data loss'.

- Geben Sie Data Classification Name > **Select** Built-in Data Identifiers > Search for Source Code ein, und wählen Sie es aus.

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

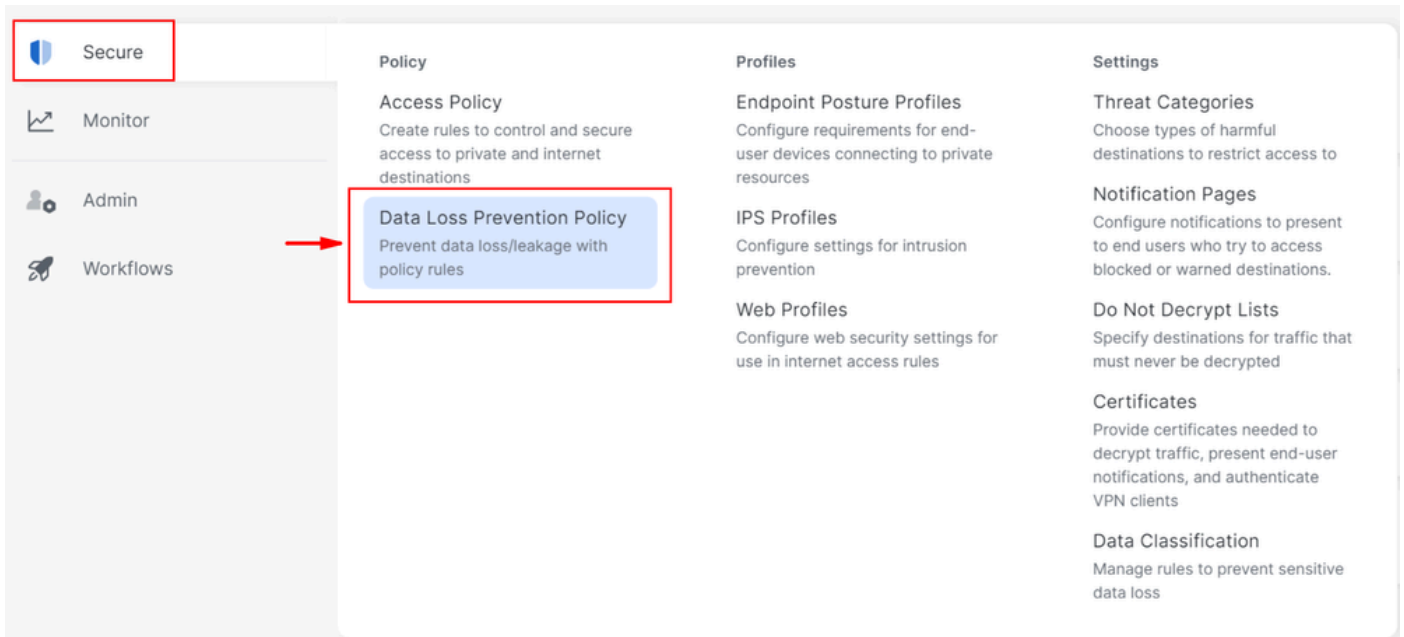
Built-in Data Identifiers

No Data Identifiers found.

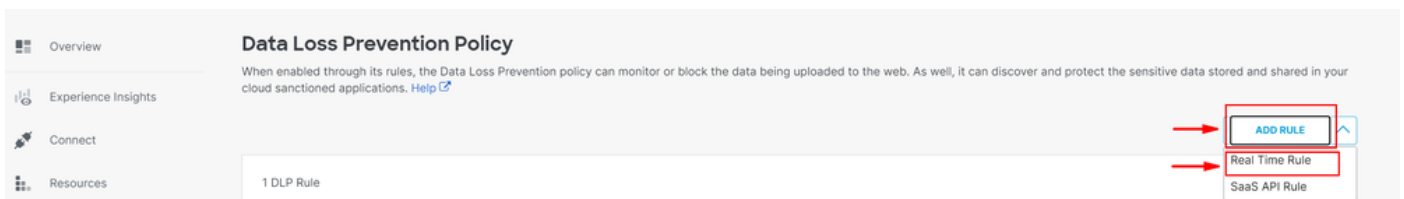
Custom Identifiers

2. Erstellen Sie eine SvD-Policy, und rufen Sie die Datenklassifizierung als "Quellcode" auf.

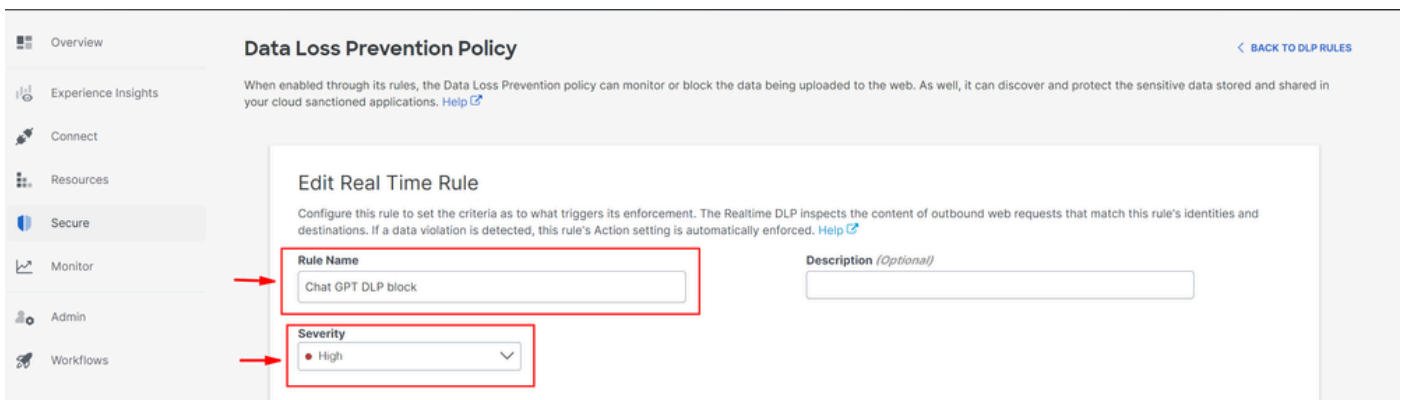
- Klicken Sie auf Secure > Data Loss Prevention Policy



- Klicken Sie auf Add Rule > Real Time Rule



- Geben Sie ein Rule Name > Festlegen der entsprechenden Severity



- Wählen Data Classifications Sie unter Content und 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

- Wählen Sie bei Bedarf die gewünschten Identitäten aus

Identities
Select identities to add them to this rule.

Search Identities

All Identities

- AD Groups
- AD Users
- Network Tunnel Groups
- Networks
- Roaming Computers

5 Selected REMOVE ALL

- Roaming Computers 4
- onmicrosoft.com)

- Wählen Sie unter Ziele Select Destination Lists and Applications for Inclusion
- Auswählen Application Categories> Auswählen Generative AI > Auswählen OpenAI API (Vetted) und 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



- Unter ActionAuswählen Block

- Unter User Notifications können Sie E-Mail-Benachrichtigungen an Endbenutzer einrichten, wenn die Regel ausgelöst wird (optional)

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



- Klicken Sie Save

DELETE

CANCEL

SAVE



3. Stellen Sie sicher, dass Sie über eine Internet-Zugangsrichtlinie für den Datenverkehr in Richtung Chat-GPT mit aktivierter Entschlüsselung verfügen.

Beispiel:

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

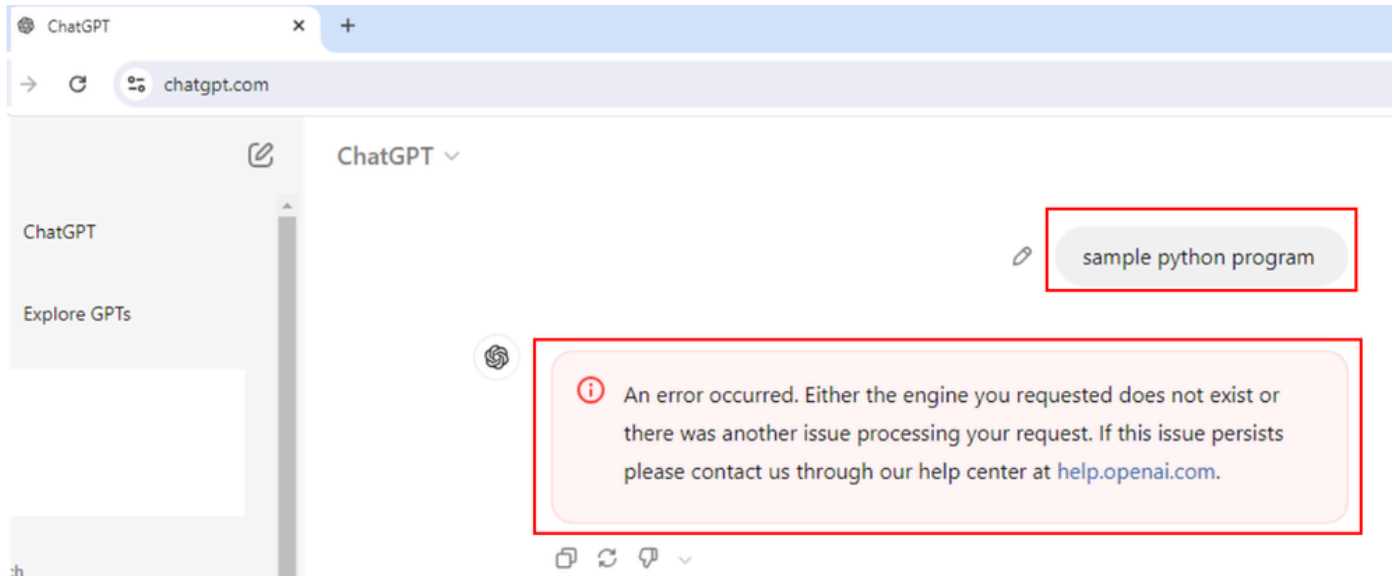


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- Fragen Sie nach einem Python-Beispielprogramm, und diese Anfrage wird blockiert.




- Fragen Sie, ob das Programm korrekt ist und diese Anfrage blockiert wird.



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 >    ▾

Überprüfung

Wenn ein Benutzer versucht, ChatGPT nach einem Python-Beispielprogramm zu fragen, wird die Anfrage blockiert.

Wir können bestätigen, dass in den Protokollen zum Schutz vor Datenverlust für sicheren Zugriff ein SvD-Ereignis ausgelöst wurde.

- Gehe zu 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

- Das SvD-Ereignis wird angezeigt.

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

- Klicken Sie auf die drei Punkte am Ende des Ereignisprotokolls, um weitere Details zum Ereignis anzuzeigen.

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

- Klicken Sie 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

- Jetzt werden alle Ereignisdetails angezeigt.

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>

- Erweitern Sie die Klassifizierung, um festzustellen, welcher Inhalt mit der Klassifizierung übereinstimmt.



Rule

Chat GPT DLP

Severity

● High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- Es werden alle Details der Inhalte angezeigt, die mit der Klassifizierung/Klassifizierung der SvD-Richtlinie übereinstimmen.

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

Fehlerbehebung

- Stellen Sie sicher, dass für die Zugriffsrichtlinie, die Webanfragen für Open AI ChatGPT entspricht, die Entschlüsselung aktiviert ist.
- Um schnell zu überprüfen, ob SSE den Datenverkehr für Open AI ChatGPT entschlüsselt, überprüfen Sie das Zertifikat der Website, das den gebräuchlichen Namen zeigt und die Schlüsselwörter "Cisco Secure Access" enthält.

Certificate Viewer: chatgpt.com



General

Details

Issued To

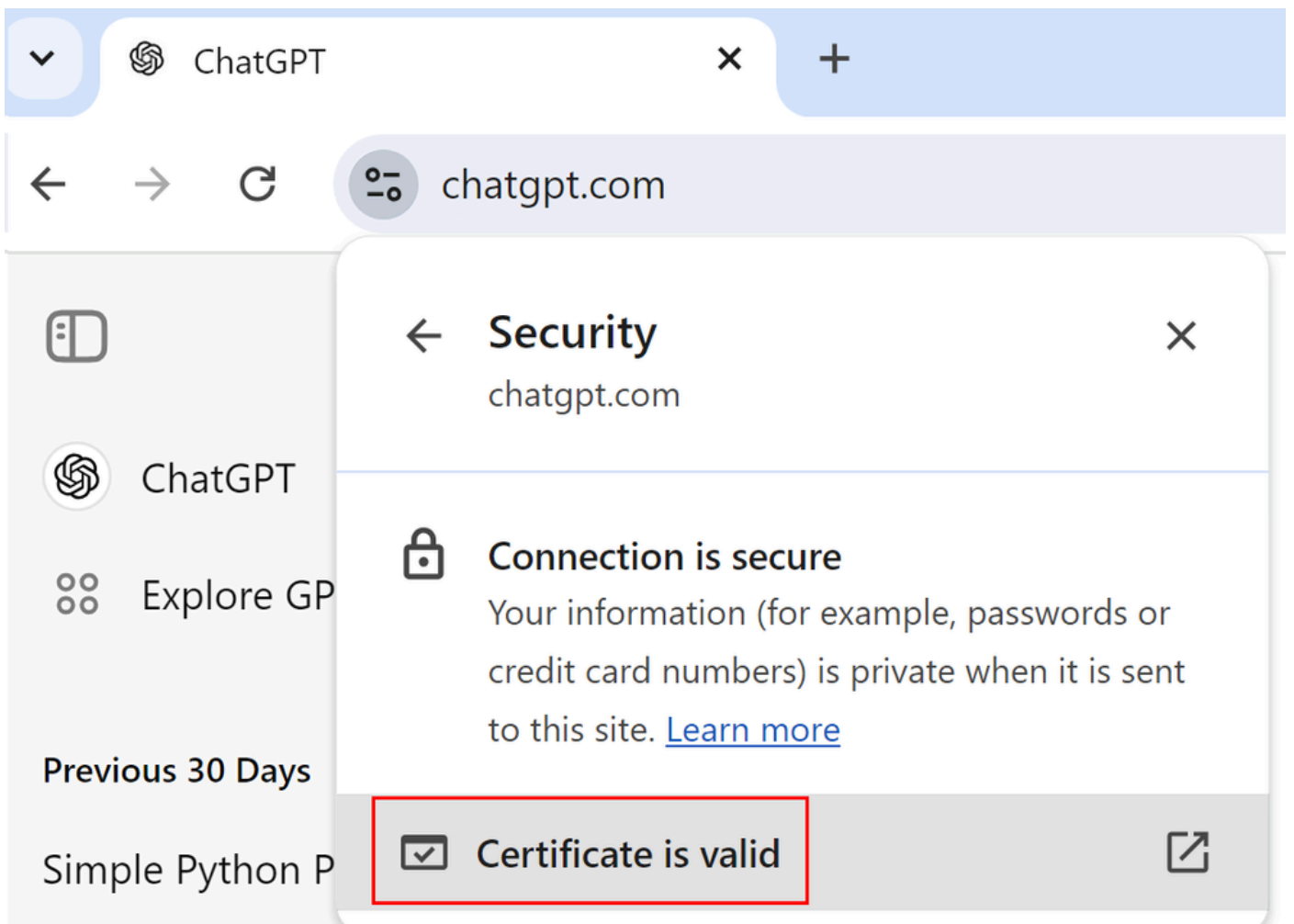
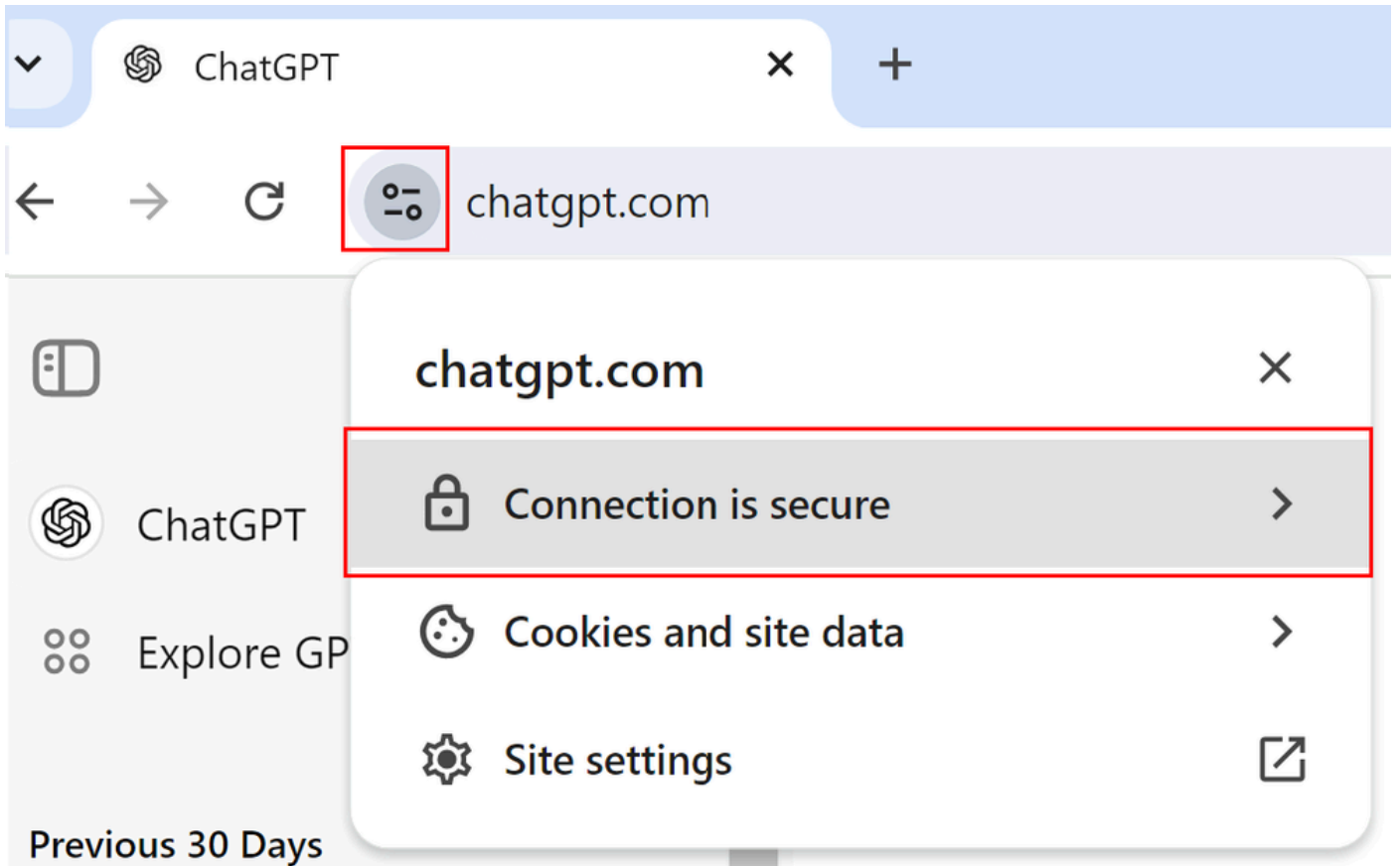
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

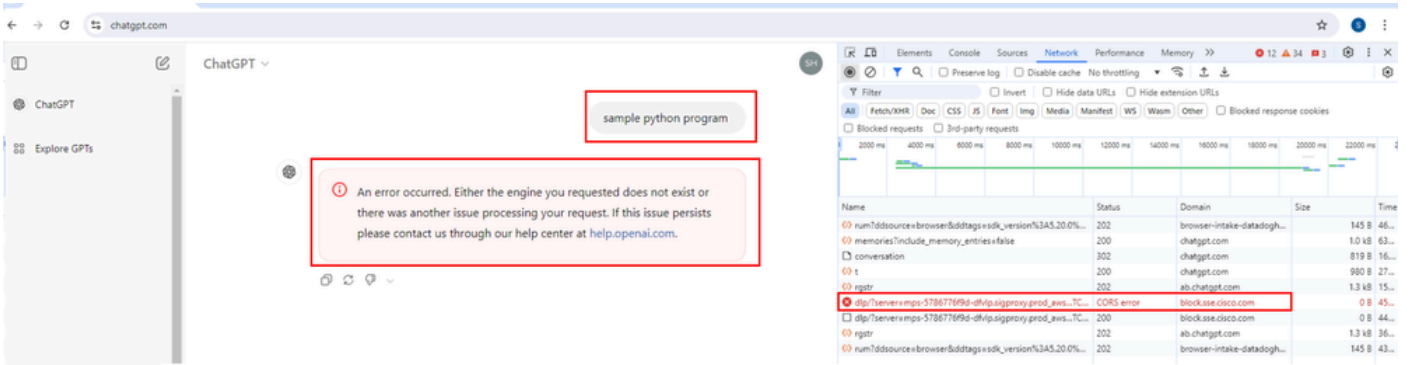
Validity Period

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

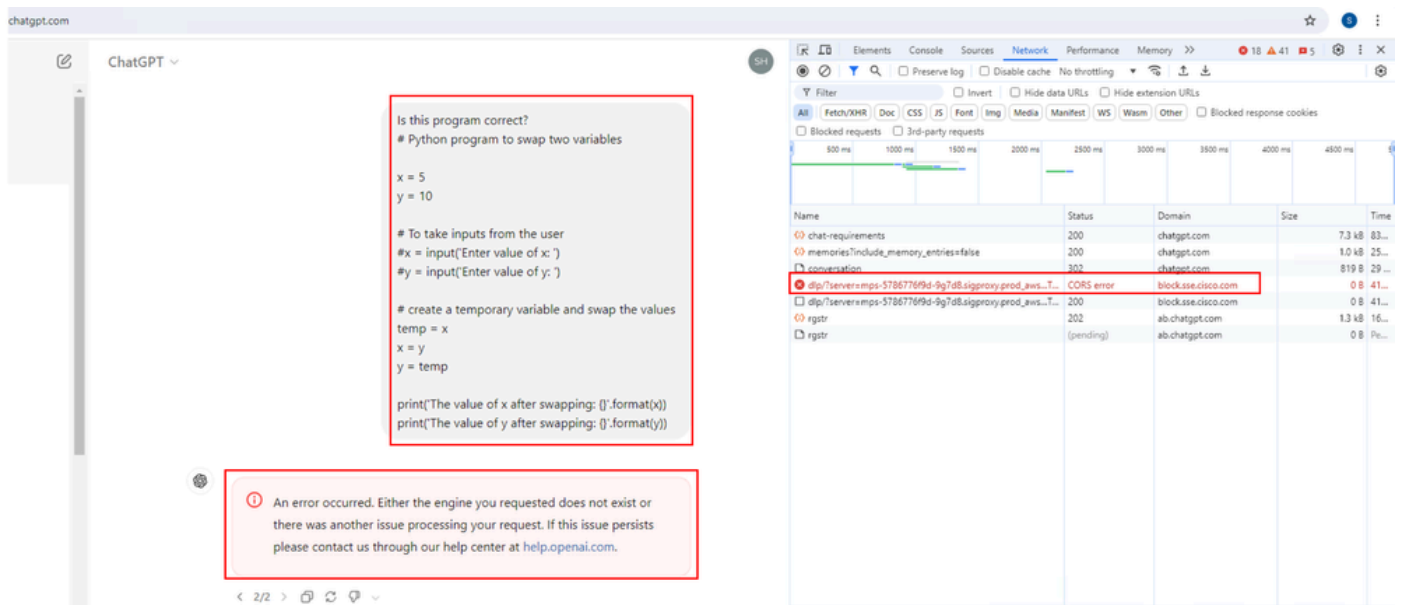
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- Öffnen Sie ChatGPT > Entwicklertools öffnen > Netzwerk auswählen > Weiter versuchen, ChatGPT nach einem Python-Beispielprogramm zu fragen.
- Beachten Sie, dass die Anforderung zu einer Blockierung führt. Unter Domäne wird Folgendes angezeigt: "block.sse.cisco.com"



- Fragen Sie ChatGPT, ob der Programmcode korrekt ist.
- Beachten Sie, dass die Anfrage zu einem Block führt und unter "domain" "block.sse.cisco.com" angezeigt wird.



Zugehörige Informationen

- [Cisco Secure Access Benutzerhandbuch](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.