

# Implementazione di DLP in accesso sicuro per limitare l'utilizzo di GPT per la programmazione tramite chat API aperta

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[1. Creare una classificazione dei dati per utilizzare l'identificatore dei dati del codice sorgente](#)

[2. Creare i criteri di prevenzione della perdita dei dati e chiamarli "Codice sorgente" per la classificazione dei dati.](#)

[3. Assicurarsi di disporre di criteri di accesso a Internet per il traffico verso Chat GPT con decrittografia abilitata.](#)

[4. Using Open AI ChatGPT provare a scaricare o caricare qualsiasi programma.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come implementare Data Loss Prevention (DLP) in Secure Access per limitare l'utilizzo di Open AI ChatGPT per la programmazione e la codifica.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso sicuro
- DLP
- Apri API ChatGPT

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Accesso sicuro

- DLP
- Apri API ChatGPT

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### 1. Creare una classificazione dei dati per utilizzare l'identificatore dei dati del codice sorgente

Passare a [Dashboard di accesso protetto](#).

- Fare clic su Secure > Data Classification > Add

Overview

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

## Data Classification

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

Data Classifications Exact Data Matches Indexed Document Matches

**Policy**

**Access Policy**  
Create rules to control and secure access to private and internet destinations

**Data Loss Prevention Policy**  
Prevent data loss/leakage with policy rules

**Profiles**

**Endpoint Posture Profiles**  
Configure requirements for end-user devices connecting to private resources

**IPS Profiles**  
Configure settings for intrusion prevention

**Web Profiles**  
Configure web security settings for use in internet access rules

**Settings**

**Threat Categories**  
Choose types of harmful destinations to restrict access to

**Notification Pages**  
Configure notifications to present to end users who try to access blocked or warned destinations.

**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

- Immettere il comando Data Classification Name > **Seleziona** Built-in Data Identifiers > Cerca Source Code e selezionarlo

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

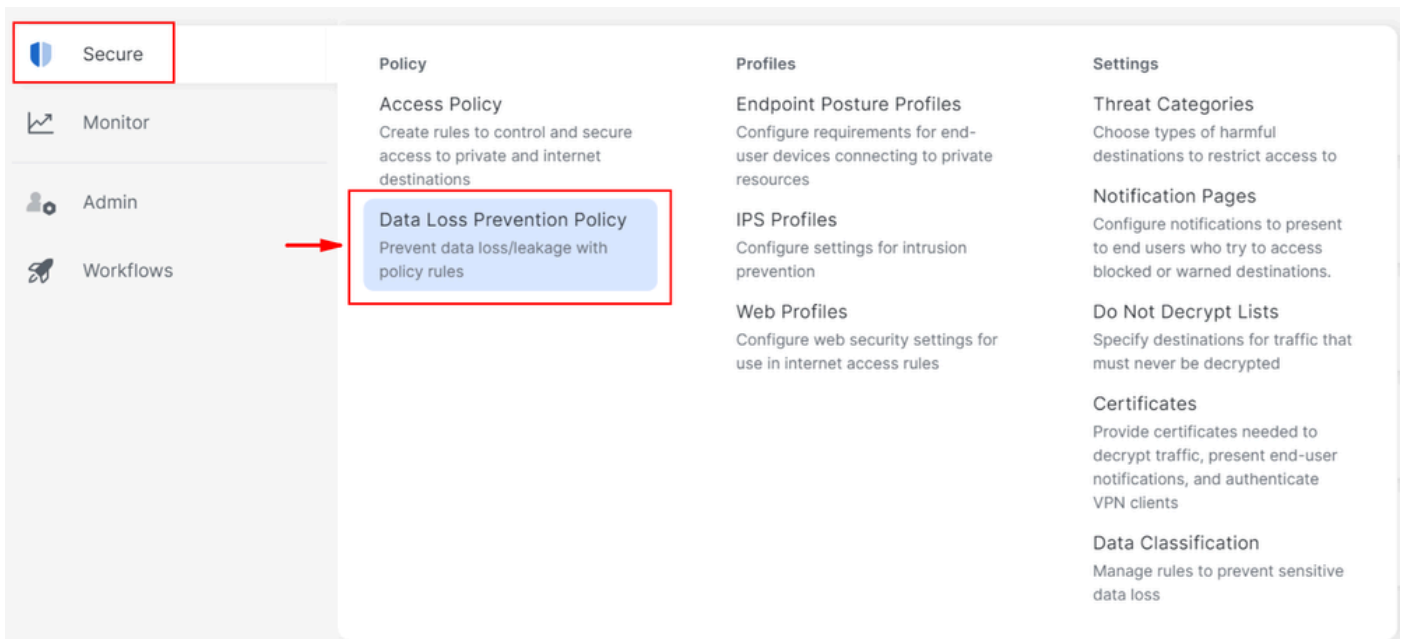
**Selected Data Identifiers**  
 Source Code

**Built-in Data Identifiers**  
  
No Data Identifiers found.

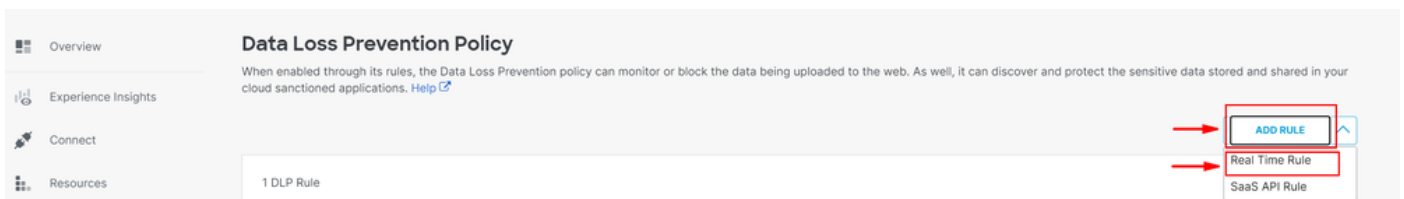
**Custom Identifiers**

2. Creare i criteri di prevenzione della perdita dei dati e chiamarli "Codice sorgente" per la classificazione dei dati.

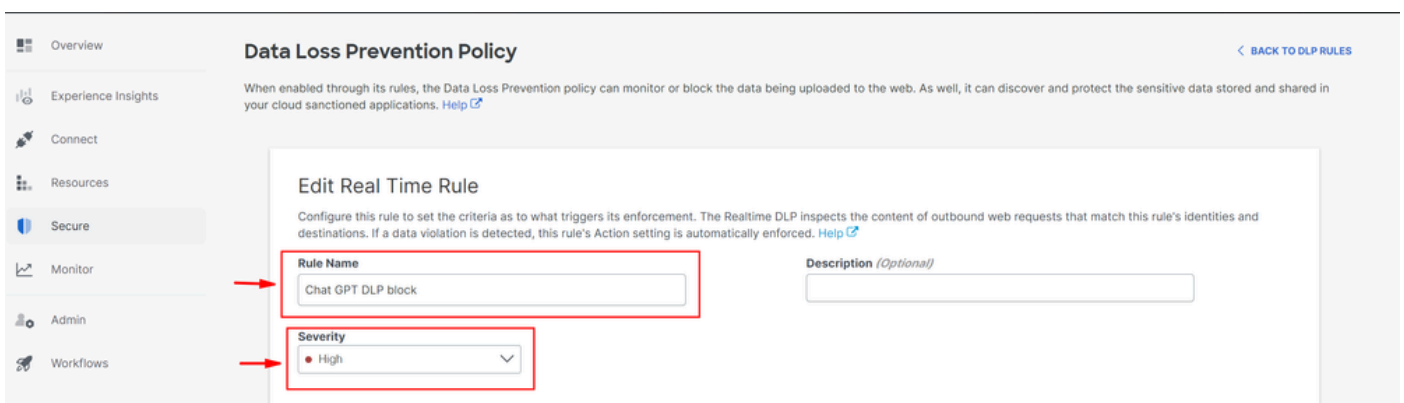
- Fare clic su Secure > Data Loss Prevention Policy



- Fare clic su Add Rule > Real Time Rule



- Fornire un Rule Name > Imposta appropriato Severity



- In Seleziona (Select) Data Classifications Content e selezionate 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.

- Built-in GDPR Classification PREVIEW
- Built-in HIPAA Classification PREVIEW
- Built-in PCI Classification PREVIEW
- Built-in PII Classification PREVIEW
- Source Code PREVIEW

- In Identitiesselazionare le identità desiderate

### Identities


Select identities to add them to this rule.

  
**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)

- In Destinazioni selezionare Select Destination Lists and Applications for Inclusion
- Seleziona Application Categories> Seleziona Generative AI > Seleziona OpenAI API (Vetted) e 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 [×](#)

- In Actionseleziona Block
- In User Notifications, è possibile impostare notifiche e-mail per gli utenti finali quando la regola viene attivata (facoltativo)

## 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](#)

- Fare clic su Save

---

DELETE

CANCEL

SAVE



3. Assicurarsi di disporre di criteri di accesso a Internet per il traffico verso Chat GPT con decrittografia abilitata.

**Esempio:**

# Chat GPT



Internet

## General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

## Sources

Any

## Destinations

2 destinations



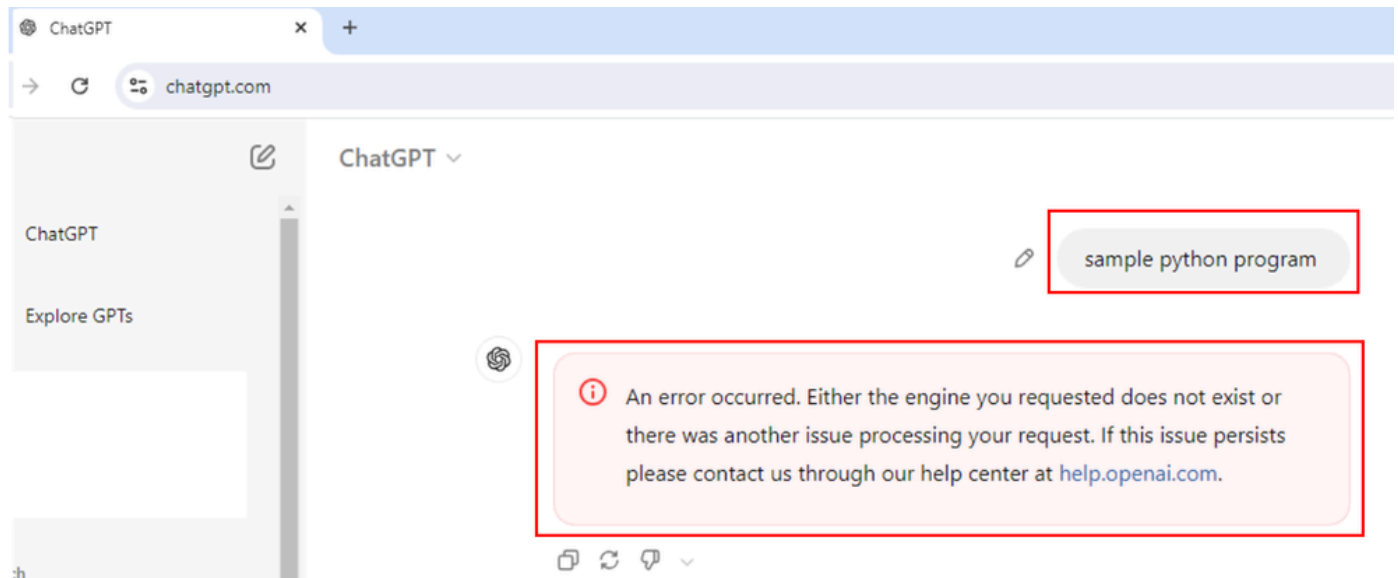
## Application Settings (2)

OpenAI API

OpenAI ChatGPT



- Chiedi un programma Python di esempio e questa richiesta viene bloccata.




- Chiedere se il programma è corretto o meno e questa richiesta viene bloccata.



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](https://help.openai.com).

< 2/2 >    

Verifica

Possiamo vedere quando l'utente cerca di chiedere a ChatGPT un programma Python di esempio, la richiesta viene bloccata.

Possiamo confermare che un evento DLP è stato attivato nei log di Secure Access Data Loss Prevention.

- Vai a 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
<input type="checkbox"/> Allowed <a href="#">Advanced</a>			

### 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

### Management

- Exported Reports
- Scheduled Reports
- Saved Searches
- Admin Audit Log

**Data Loss Prevention**  
Data violations detected through the Real Time and SaaS API rules

- Siamo in grado di vedere l'evento DLP.

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

- Fare clic sui tre punti alla fine del registro eventi per verificare ulteriori dettagli sull'evento.

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

- Fare clic su 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

- A questo punto è possibile visualizzare tutti i dettagli dell'evento.

## 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>

- Espandere la classificazione per visualizzare il contenuto corrispondente al classificatore.



## Rule

**Chat GPT DLP**

## Severity

● High

## Direction

Inbound

## Classification

Source Code

**8 Matches** Source Code

**def calculate\_year\_of\_century(age):, def main():...**



- Vediamo tutti i dettagli del contenuto che corrisponde al classificatore / classificazione dei criteri di prevenzione della perdita dei dati.

---

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

Risoluzione dei problemi

- Verificare che il criterio di accesso corrispondente alle richieste Web per Open API ChatGPT abbia la decrittografia abilitata.
- Per verificare rapidamente se SSE sta decrittografando il traffico per Open AI ChatGPT, controllare il certificato del sito web che mostra il nome comune che include le parole chiave "Cisco Secure Access" in esso.

## 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>

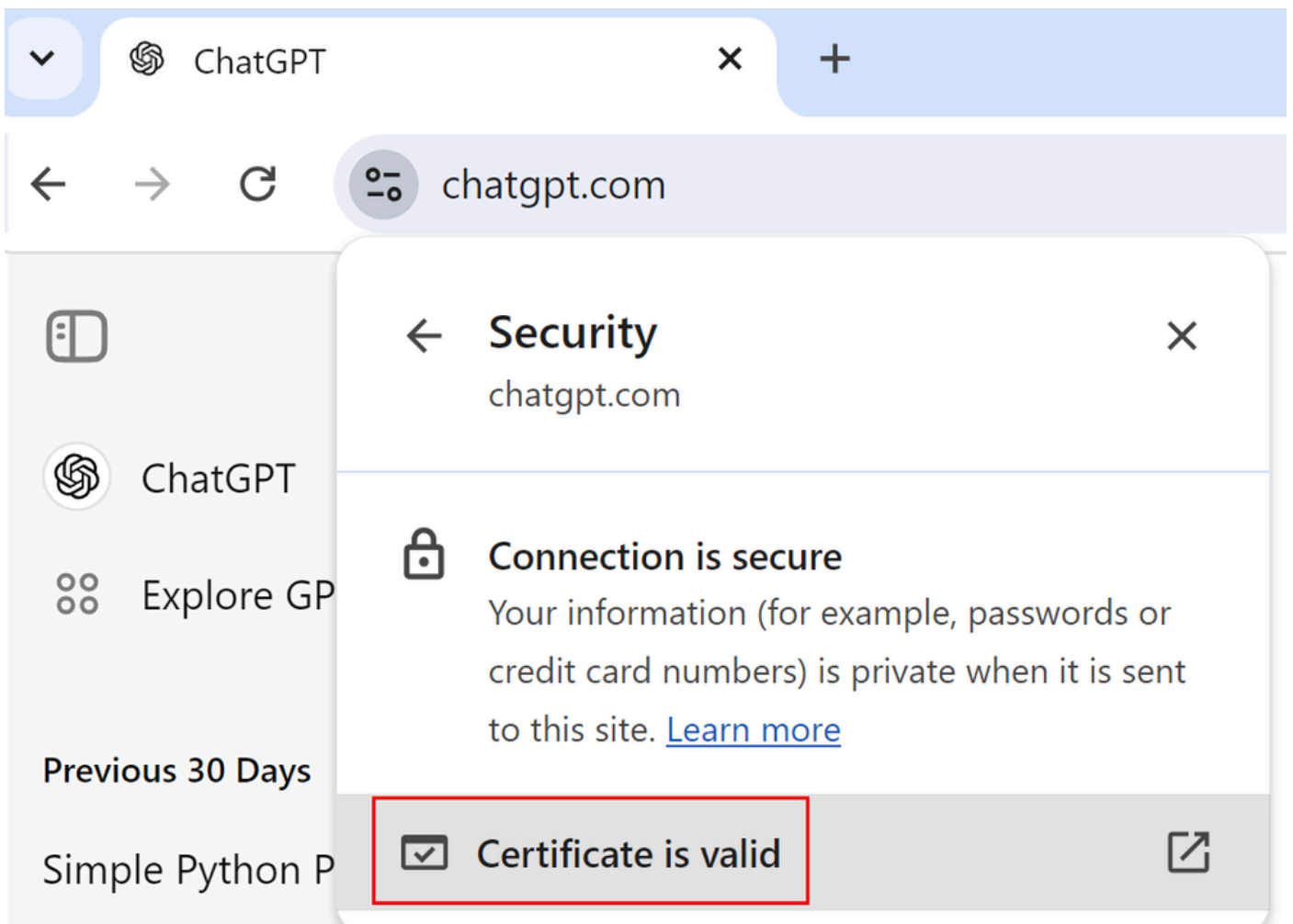
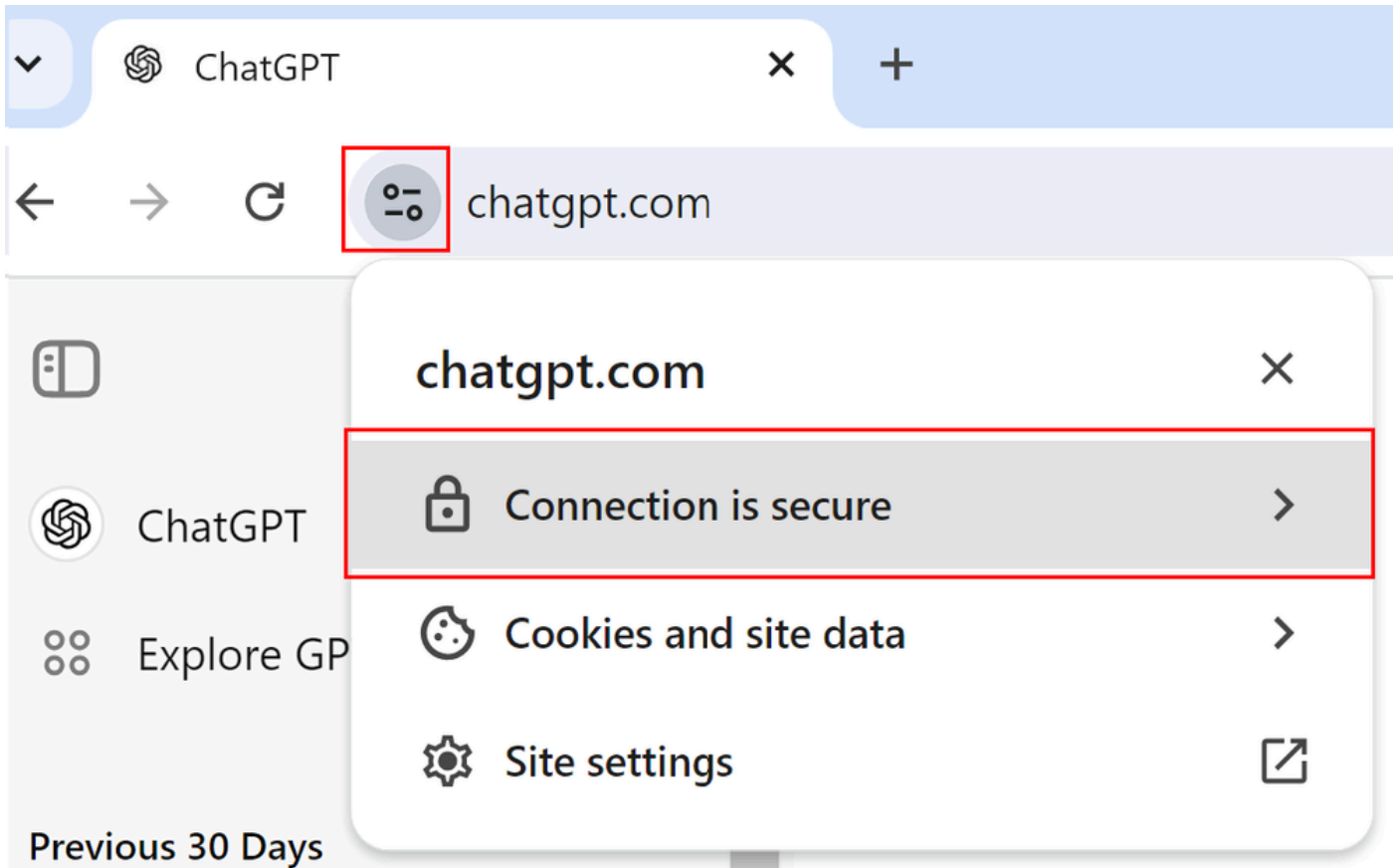
#### Issued By

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>

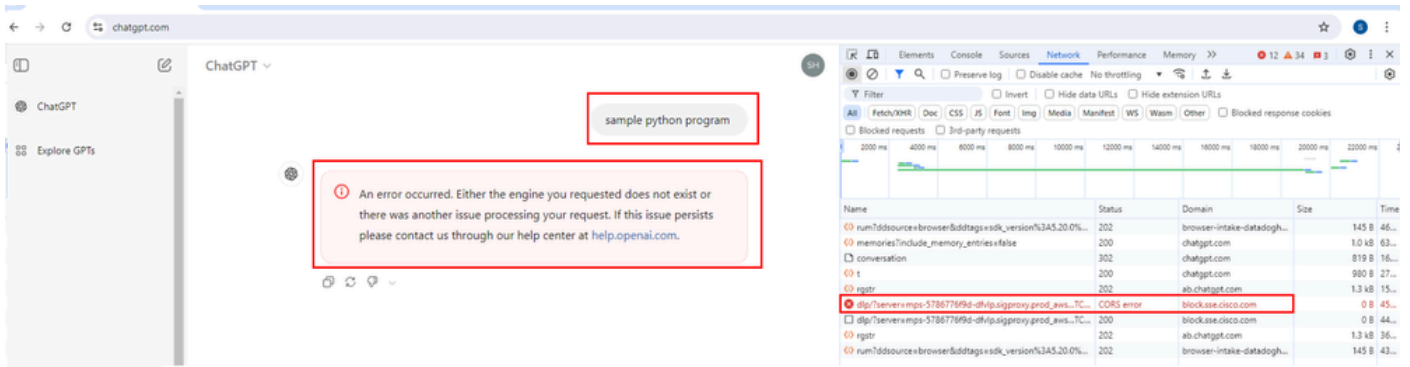
### Validity Period

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

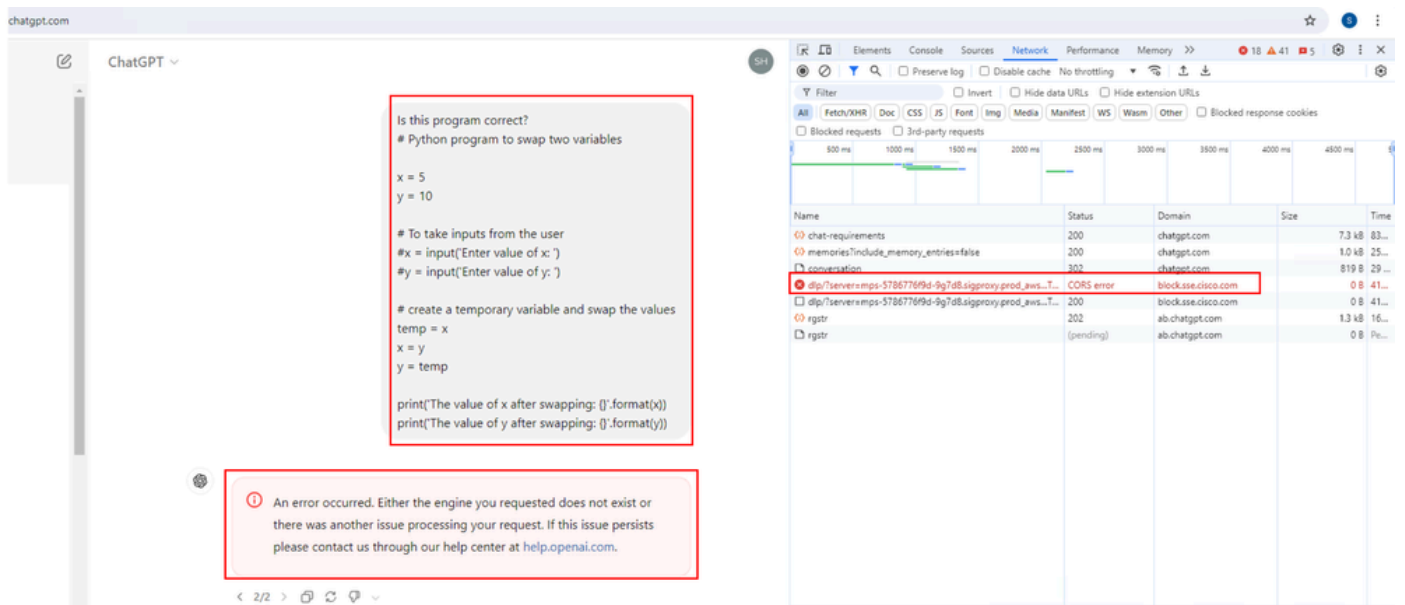
### SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- Apri ChatGPT > Apri strumenti di sviluppo > Seleziona Rete > Avanti prova a chiedere a ChatGPT un programma Python di esempio
- La richiesta genera un blocco. Sotto dominio si vede "block.sse.cisco.com"



- Chiedere a ChatGPT se il codice del programma è corretto.
- Si noti che la richiesta genera un blocco e sotto "dominio" viene visualizzato "block.sse.cisco.com".



#### Informazioni correlate

- [Guida per l'utente di Cisco Secure Access](#)
- [Supporto tecnico Cisco e download](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).