

Implemente DLP en Secure Access para restringir el uso de Open AI ChatGPT para programación

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[1. Cree una clasificación de datos para utilizar el identificador de datos de código fuente](#)

[2. Cree una política DLP y llame al "Código fuente" de clasificación de datos que contiene.](#)

[3. Asegúrese de que dispone de una política de acceso a Internet para el tráfico hacia Chat GPT con el descifrado habilitado.](#)

[4. Utilizando Open AI ChatGPT intenta descargar o cargar cualquier programa.](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo implementar Data Loss Prevention (DLP) en Secure Access para restringir el uso de Open AI ChatGPT para programación y codificación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro
- DLP
- Abrir AI ChatGPT

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso seguro
- DLP

- Abrir AI ChatGPT

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

1. Cree una clasificación de datos para utilizar el identificador de datos de código fuente

Vaya a [Panel de acceso seguro](#).

- Haga clic en Secure > Data Classification > Add

The screenshot shows the Microsoft Secure console interface. On the left is a navigation sidebar with 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 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 bottom-right section. The 'Policy' column contains 'Access Policy' and 'Data Loss Prevention Policy'. The 'Profiles' column contains 'Endpoint Posture Profiles', 'IPS Profiles', and 'Web Profiles'. The 'Settings' column contains 'Threat Categories', 'Notification Pages', 'Do Not Decrypt Lists', and 'Certificates'. The bottom-right section, highlighted with a red box and arrow, contains 'Data Classification' with the description 'Manage rules to prevent sensitive data loss'.

- Ingrese el Data Classification Name > **Select Built-in Data Identifiers** > Search for Source Code y selecciónelo

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 >

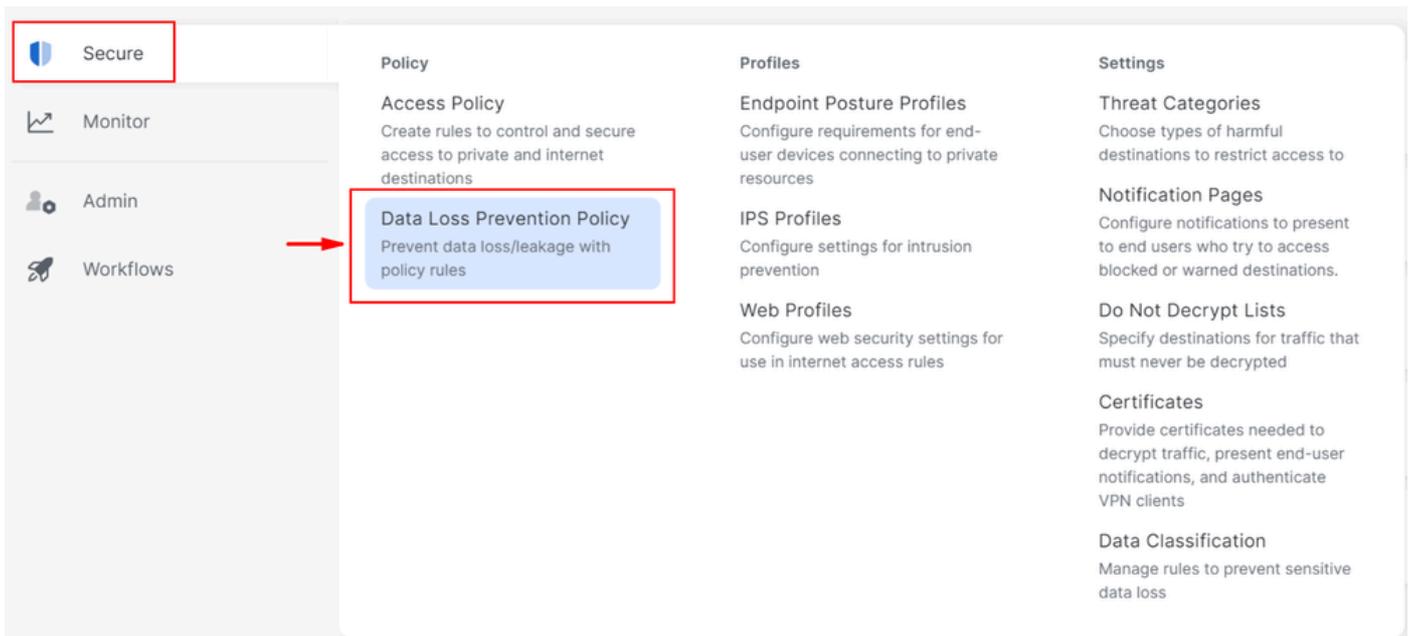
Built-in Data Identifiers

No Data Identifiers found.

Custom Identifiers

2. Cree una política DLP y llame al "Código fuente" de clasificación de datos que contiene.

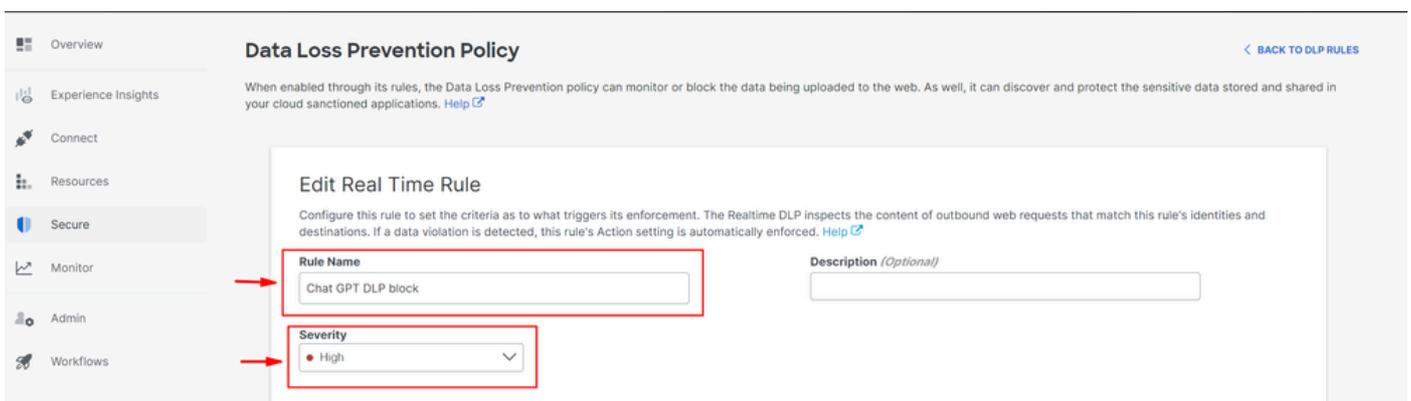
- Haga clic en Secure > Data Loss Prevention Policy



- Haga clic en Add Rule > Real Time Rule



- Proporcione un Rule Name > Set apropiado Severity



- En Data Classifications seleccionar Content y seleccionar 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

- En Identities seleccione las identidades deseadas según sea necesario

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)

- En Destinos, seleccione Select Destination Lists and Applications for Inclusion
- Select Application Categories > Select Generative AI > Select OpenAI API (Vetted) and OpenAI ChatGPT (Vetted) in Outbound and Inbound Direction

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 [×](#)

- En Actionseleccionar Block
- En User Notifications, puede configurar las notificaciones de correo electrónico para los usuarios finales, cuando se active la regla (opcional)

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 [▼](#)

- Haga clic en Save

DELETE

CANCEL

SAVE



3. Asegúrese de que dispone de una política de acceso a Internet para el tráfico hacia Chat GPT con el descifrado habilitado.

Ejemplo:

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

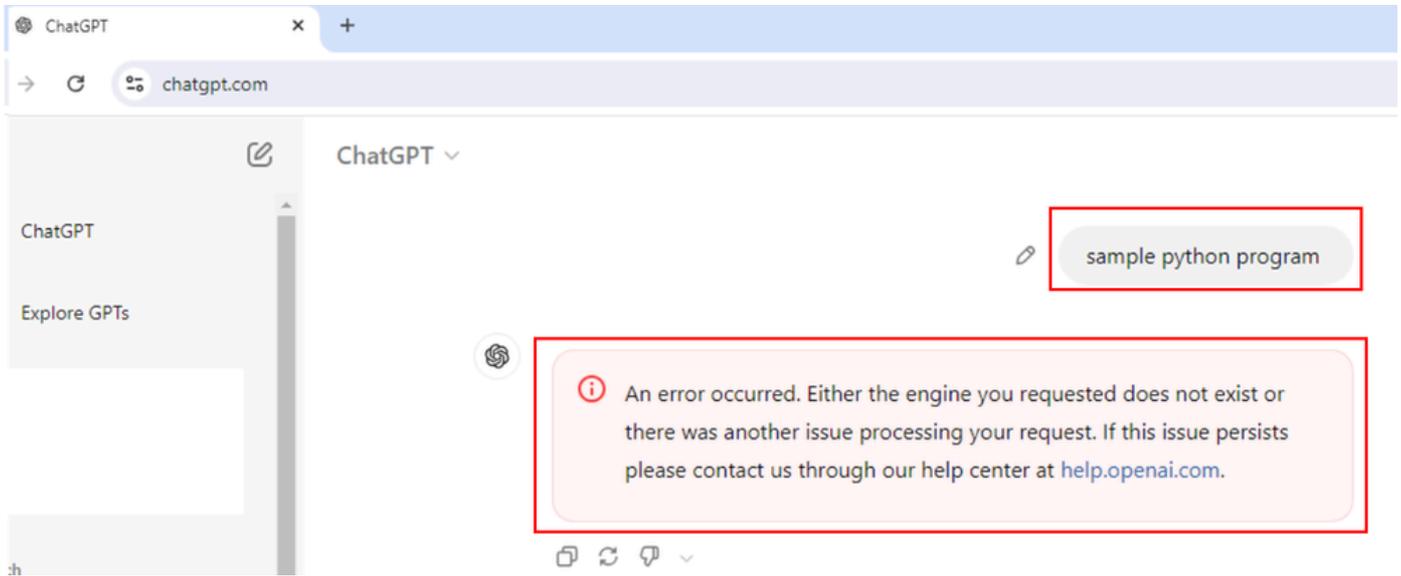


Application Settings (2)

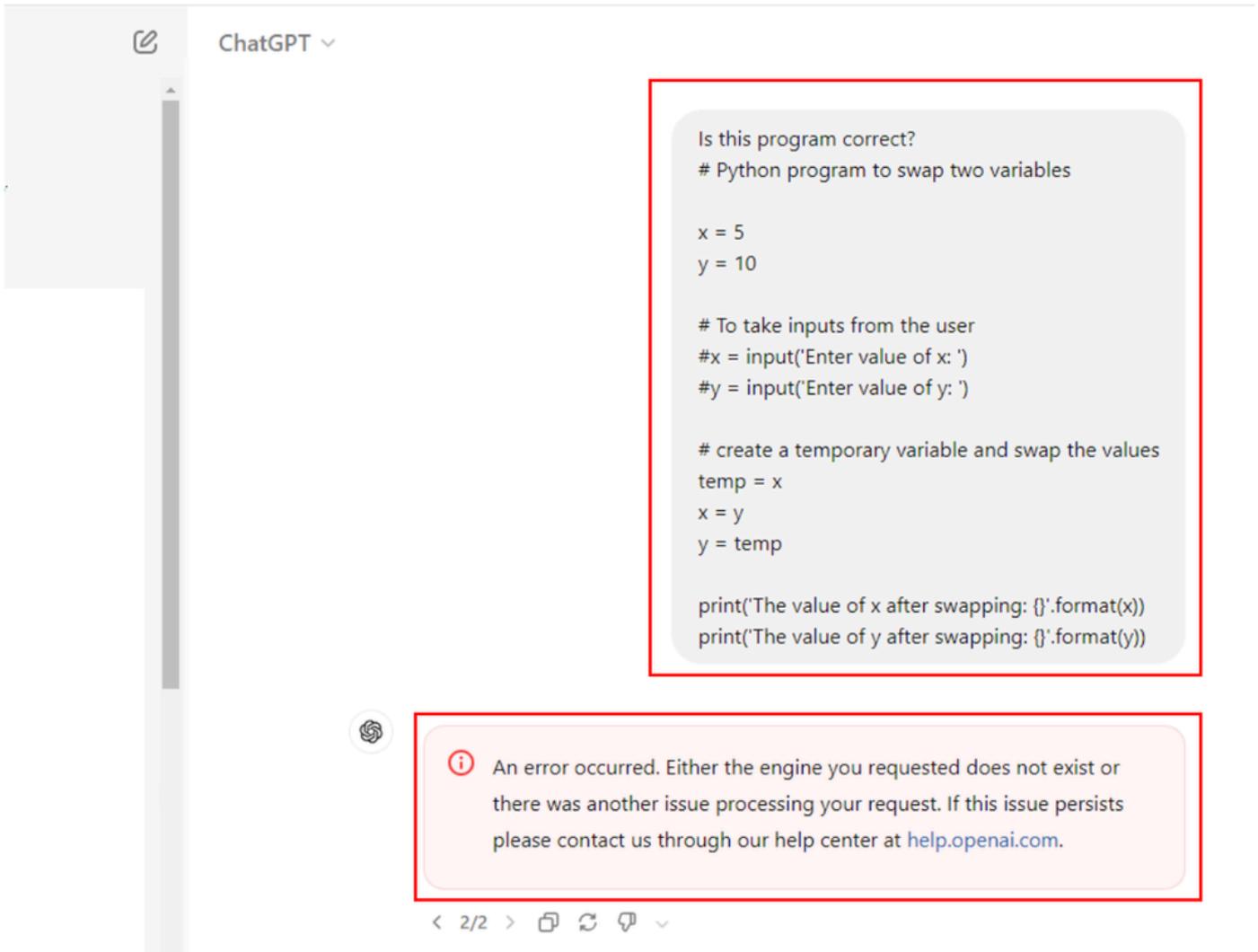
OpenAI API

OpenAI ChatGPT

- Solicite un programa python de muestra y esta solicitud se bloqueará.



- Pregunte si el programa es correcto o no y esta solicitud se bloqueará.



Verificación

Podemos ver que cuando un usuario intenta pedir a ChatGPT un programa de Python de muestra, la solicitud se bloquea.

Podemos confirmar que se ha desencadenado un evento de DLP en los registros de prevención de pérdida de datos de acceso seguro.

- Vaya 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

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

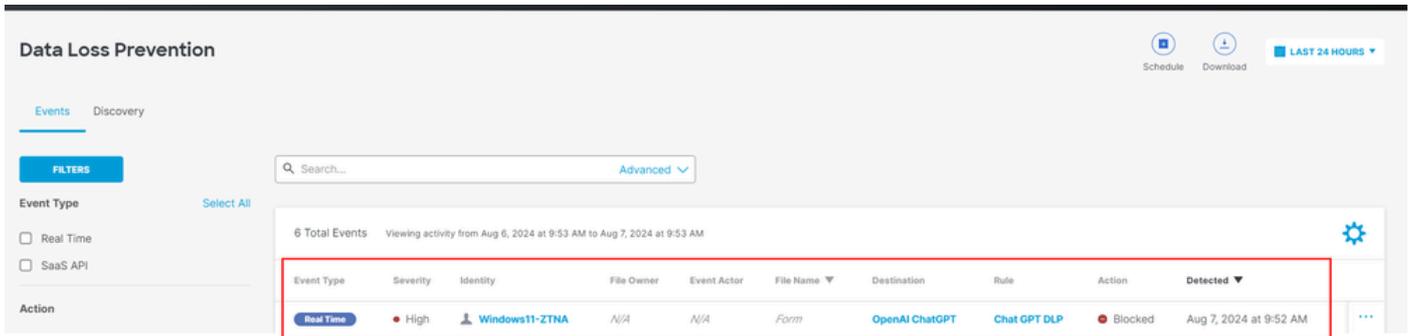
Exported Reports

Scheduled Reports

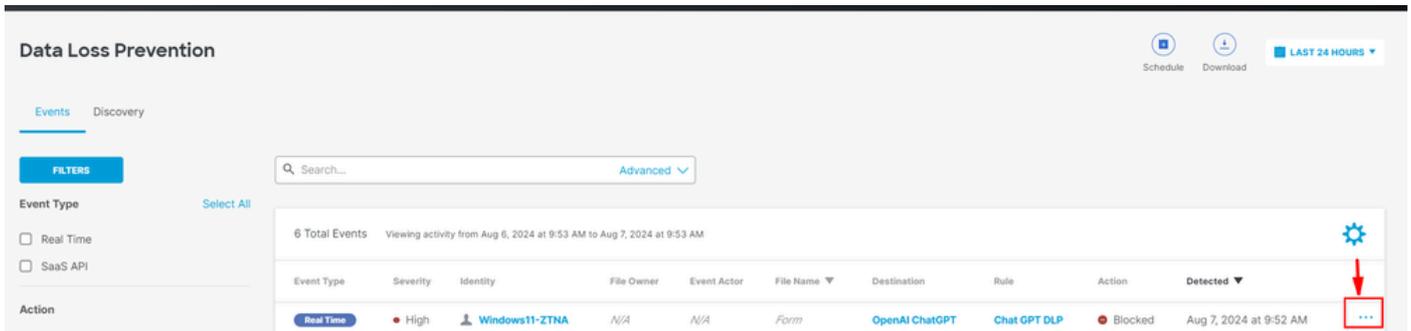
Saved Searches

Admin Audit Log

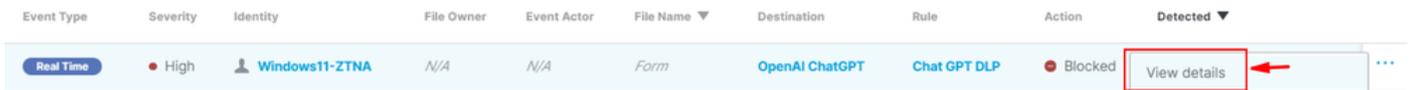
- Podemos ver el evento de DLP.



- Haga clic en los tres puntos situados al final del registro de eventos para comprobar si hay más detalles sobre el evento.



- Haga clic en View details.



- Ahora vemos todos los detalles del 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>

- Expanda la clasificación para ver qué contenido coincide con el clasificador.



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- Vemos todos los detalles del contenido que coinciden con el clasificador/clasificación de la política DLP.

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

Troubleshoot

- Asegúrese de que la política de acceso que coincide con las solicitudes web para Open AI ChatGPT tenga el descifrado habilitado.
- Para verificar rápidamente si SSE está descifrando el tráfico para Open AI ChatGPT, verifique el certificado del sitio web que muestra que el nombre común incluye las palabras clave "Cisco Secure Access".

Certificate Viewer: chatgpt.com



General

Details

Issued To

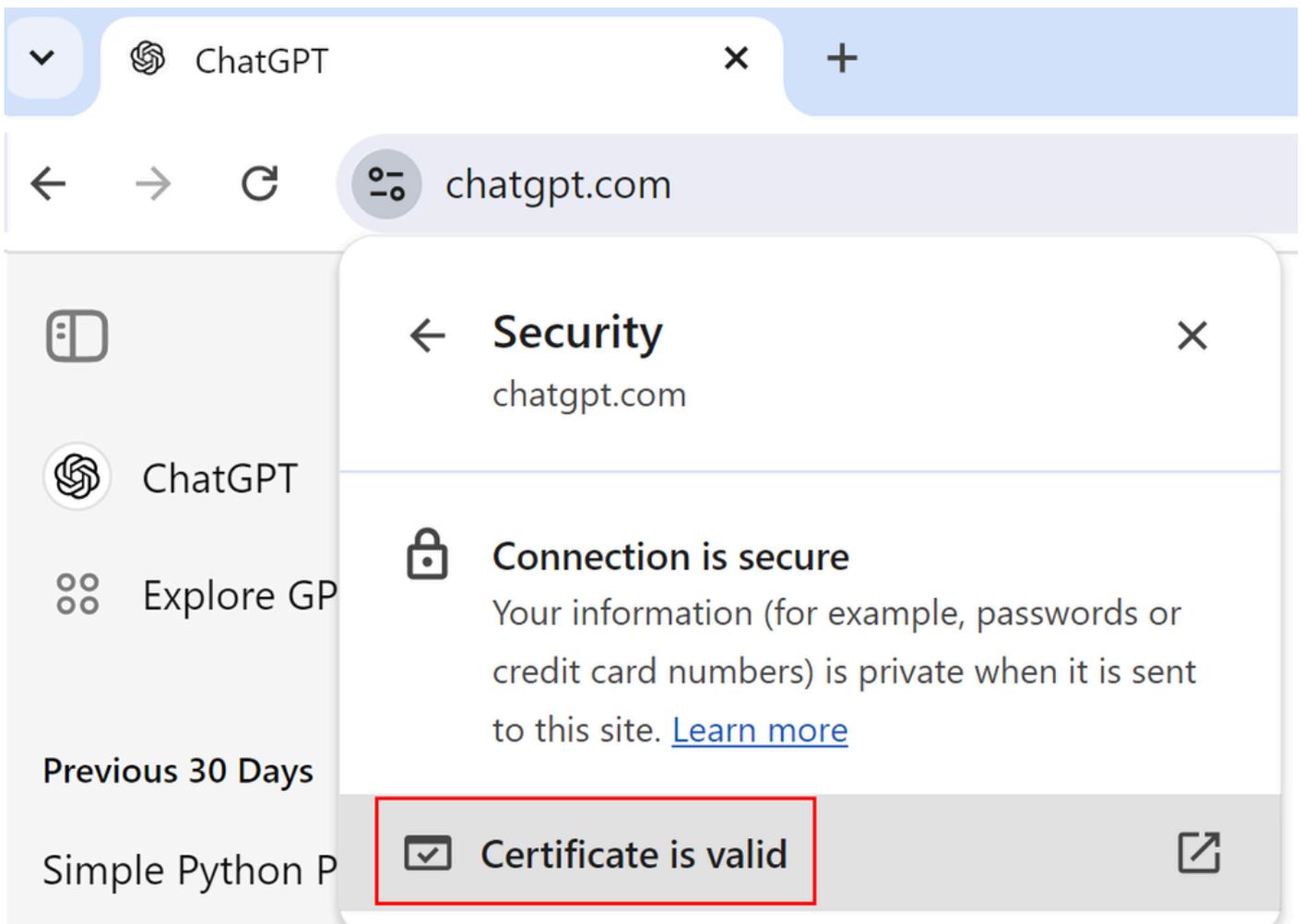
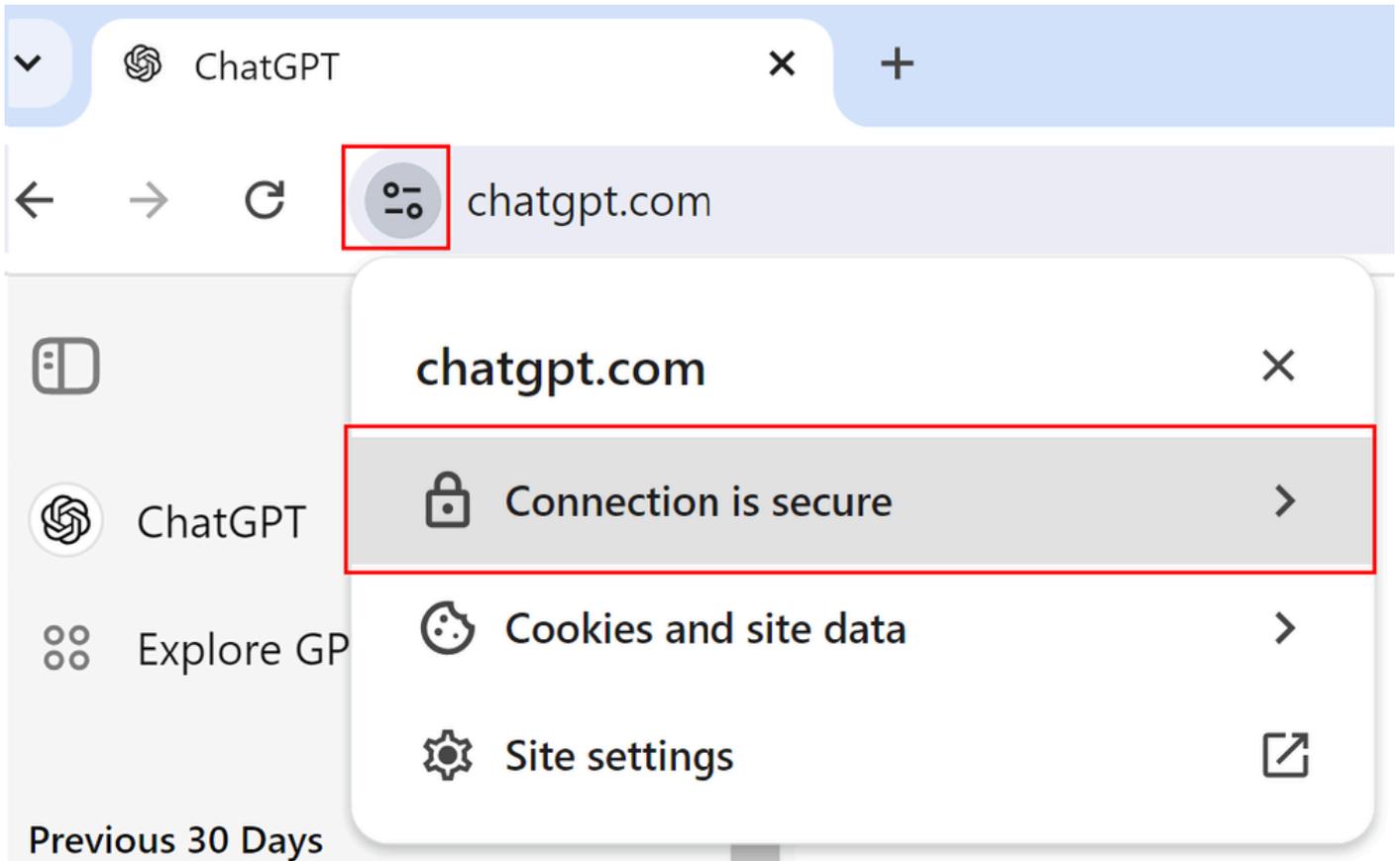
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

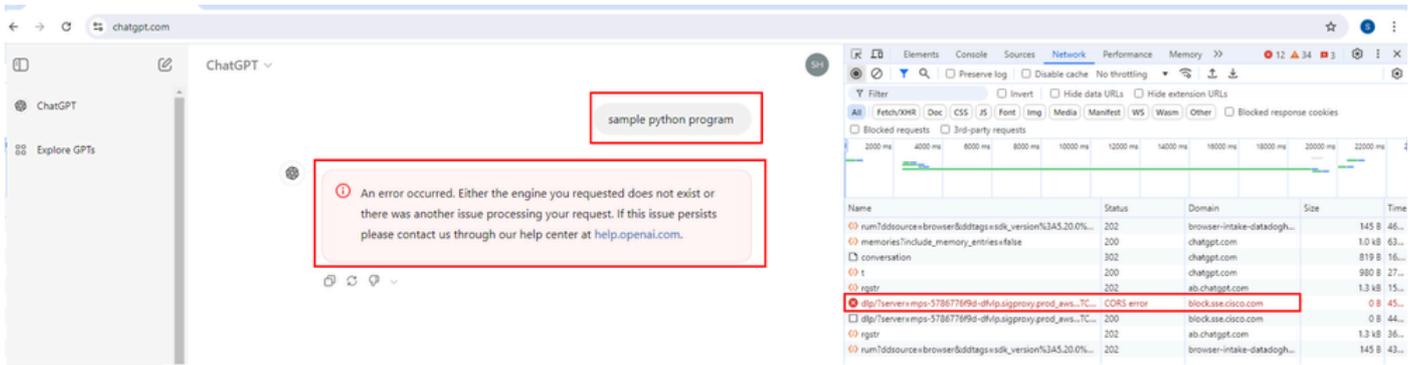
Validity Period

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

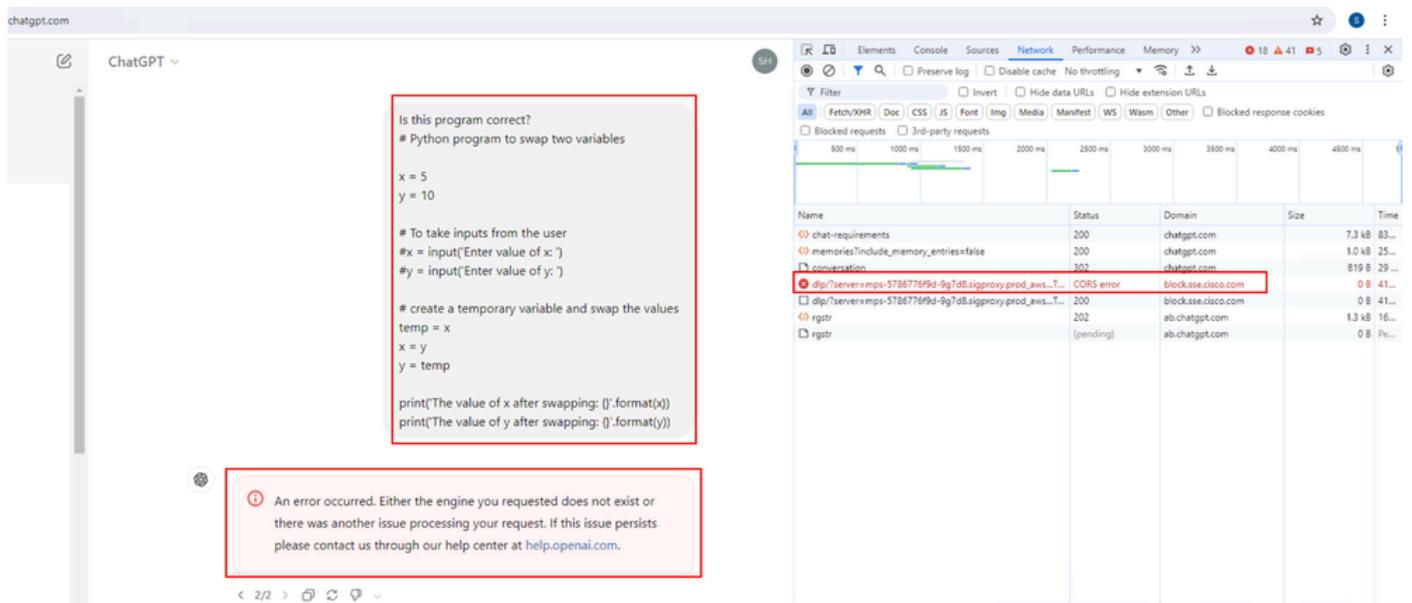
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- Abra ChatGPT > Open developer tools > Select Network > A continuación, intente solicitar a ChatGPT un programa python de ejemplo
- Observe que la solicitud da como resultado un bloque. En domain (dominio), verá "block.sse.cisco.com"



- Pregunte a ChatGPT si el código del programa es correcto.
- Observe que la solicitud da como resultado un bloque y bajo "domain" verá "block.sse.cisco.com".



Información Relacionada

- [Guía del usuario de Cisco Secure Access](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).