

# Bloquer le mode AI de Google dans l'appareil Web sécurisé

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Étapes de configuration](#)

[Vérifier](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les étapes nécessaires pour que l'apppliance Web sécurisé soit configurée pour bloquer les requêtes HTTPS au mode AI de Google.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- administration SWA
- Protocoles réseau et proxy de base
- Processus de décryptage de la SWA
- Expressions régulières

Cisco recommande d'installer les outils suivants :

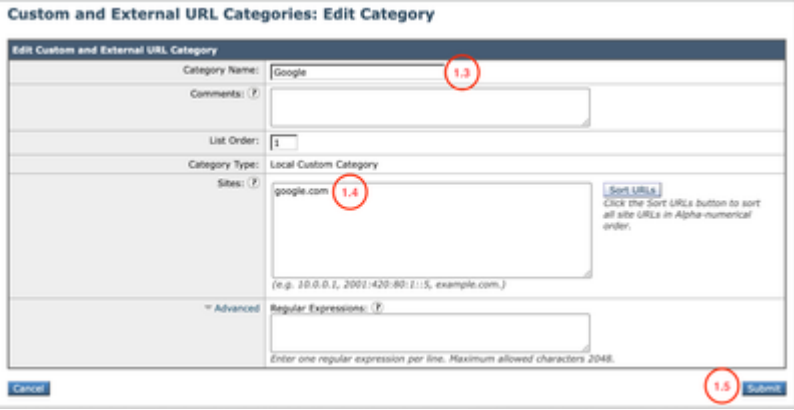
- SWA physique ou virtuel
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Étapes de configuration

<p>Étape 1 : création d'une catégorie d'URL personnalisée pour le site Web de Google</p>	<p>Étape 1.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories.</p> <p>Étape 1.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée.</p> <p>Étape 1.3. Saisissez le nom de la nouvelle catégorie.</p> <p>Étape 1.4. Définissez ces URL dans la section Sites :</p> <p>google.com</p> <p>Étape 1.5. Soumettre les modifications</p> 
<p>Étape 2. Créez une catégorie d'URL personnalisée pour le mode AI de Google.</p>	<p>Étape 2.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories.</p> <p>Étape 2.2. Cliquez sur Add Category pour créer une nouvelle catégorie d'URL personnalisée.</p> <p>Étape 2.3. Entrez le nom de la nouvelle catégorie.</p>

Étape 2.4. Définissez ces URL dans la section Expressions régulières :

google\\*.com.\*udm=50

Étape 2.5. Soumettre les modifications



Conseil : Pour plus d'informations sur la façon de configurer des catégories d'URL personnalisées, consultez : [Configurer des catégories d'URL personnalisées dans Appareil Web sécurisé - Cisco](#)

#### Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' interface. It contains the following fields and elements:

- Category Name:** GoogleModeAllBlock (highlighted with a red circle 2.3)
- Comments:** Testing
- List Order:** 3
- Category Type:** Local Custom Category
- Sites:** (Empty text area)
- Regular Expressions:** google\\*.com.\*udm=50 (highlighted with a red circle 2.4)
- Buttons:** Cancel (bottom left) and Submit (bottom right, highlighted with a red circle 2.5)
- Sort URLs button:** Located on the right side of the Sites field.

Étape 3. Déchiffrez le trafic pour Google.

Étape 3.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies

Étape 3.2. Cliquez sur Add Policy.

Étape 3.3. Entrez le nom de la nouvelle stratégie.

The screenshot shows the 'Policy Settings' interface. It contains the following fields and elements:

- Policy Name:** Google All Block (highlighted with a red circle 3.3)
- Description:** (Empty text area)
- Insert Above Policy:** 1 (getserver access policy)
- Policy Expires:**  Set Expiration for Policy
- On Date:** MM/DD/YYYY
- All Time:** (Time selection controls)

Étape 3.4. (Facultatif) Sélectionnez le profil d'identification auquel vous souhaitez que cette stratégie s'applique.

Étape 3.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour

ajouter la catégorie d'URL personnalisée.

Étape 3.6. Sélectionnez la catégorie d'URL créée à l'étape 1.

Étape 3.7. Cliquez sur Submit.

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

- All Identification Profiles (3.6)
- All Authenticated Users (3.6)
- Selected Groups and Users (X)
- Groups: No groups entered
- Users: No users entered
- Guests (users failing authentication)
- All Users (Authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL, Category), or User Agents.

The following advanced membership criteria have been defined:

- Proxy Ports: None Selected
- Subnets: None Selected
- Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
- URL Categories: Google (3.8)
- User Agents: None Selected

Cancel (3.7) Submit

Étape 3.8. Dans la page Decryption Policies, cliquez sur le lien de URL Filtering pour la nouvelle stratégie.

Étape 3.9. Choisissez Decrypt comme action pour Custom URL Category.

Étape 3.10. Cliquez sur Envoyer.

#### Decryption Policies: URL Filtering: Decrypting Google Traffic

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop (X)	Quota-Based	Time-Based
Google	Custom (Local)	---	Select all	Select all	Select all (3.9)	Select all	(Unavailable)	(Unavailable)

Cancel (3.10) Submit

Étape 4.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies.

Étape 4.2. Cliquez sur Add Policy.

Étape 4.3. Entrez le nom de la nouvelle stratégie.

Étape 4 : blocage du trafic en mode AI de Google

Policy Settings

Enable Policy

Policy Name: (Y) Google AI Block (4.3)  
(e.g. my IT policy)

Description:   
(Maximum allowed characters 256)

Insert Above Policy: 1 (petter server access policy)

Policy Expires:

Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time: 00:00

Étape 4.4. (Facultatif) Sélectionnez le profil d'identification auquel vous souhaitez que cette stratégie s'applique.

Étape 4.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée.

Étape 4.6. Sélectionnez la catégorie d'URL créée à l'étape 2.

Étape 4.7. Cliquez sur Submit.

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: All Identification Profiles (4.4)  
All Authenticated Users  
Selected Groups and Users (0)  
Groups: No groups entered  
Users: No users entered  
Guests (users failing authentication)  
All Users (authenticated and unauthenticated users)

If the 'All Users' option is selected, at least one Advanced membership option must also be selected.  
Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: None Selected  
Proxy Ports: None Selected  
Subnets: None Selected  
Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)  
URL Categories: GoogleModeAIBlock (4.5)  
User Agents: None Selected

Cancel Submit (4.7)

Étape 4.8. Dans la page Stratégies d'accès, cliquez sur le lien du filtrage d'URL pour la nouvelle stratégie.

Étape 4.9. Choisissez Block comme action pour Custom URL Category.

Étape 4.10. Cliquez sur Submit.

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Rewrite Profile	Clone Policy	Delete
1	Google AI Block Identification Profile: All All identified users URL Categories: GoogleModeAIBlock	(global policy)	Block: 1 (4.8)	Monitor: 321	(global policy)	(global policy)	(global policy)		

Access Policies: URL Filtering: Google AI Block

Custom and External URL Category Filtering

Category	Category Type	Block	Deny	Allow	Monitor	Warn	Warn	Warn	Warn	Warn	Warn
GoogleModeAIBlock	Custom-Defined	Block	Deny	Allow	Monitor	Warn	Warn	Warn	Warn	Warn	Warn

Cancel Submit (4.10)

Étape 4.11. Valider les modifications

## Vérier

Lorsque les paramètres de configuration sont terminés, le trafic Google AI est traité sur les journaux d'accès comme Bloquer, car il est détecté par la catégorie personnalisée que nous avons créée pour Google AI Block.

<#root>

1779219170.427 101 10.184.103.26

TCP\_DENIED\_SSL/403

0 GET https://www.google.com:443/search?q=cisco+live+&sca\_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo

BLOCK\_CUSTOMCAT\_12-Google\_AI\_Block

-ciscotest-NONE-NONE-NONE-NONE-NONE <"C\_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,-,"IW\_srch"

Une requête de recherche en mode Google AI est bloquée et affiche cette notification de l'utilisateur final.



Tout autre trafic Google continue d'être autorisé.

## Informations connexes

[Définir des catégories d'URL personnalisées dans WSA](#)

[Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance](#)

[Configurer le certificat de déchiffrement dans l'appareil Web sécurisé](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.