

# 在SWA中阻止Google消費者帳戶訪問

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[報告和日誌](#)

[記錄檔](#)

[驗證](#)

[相關資訊](#)

---

## 簡介

本文描述在安全Web裝置(SWA)中阻止Google Workspace或Google消費者帳戶訪問的過程。

## 必要條件

### 需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)
- 對SWA的管理訪問。

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

# 設定

<p>步驟1.為Google網站建立自定義URL類別。</p>	<p>步驟1.1. 從GUI中，導覽至Web Security Manager，然後選擇Custom 和External URL。</p> <p>步驟1.2. 按一下Add Category以建立一個新的自訂URL類別。</p> <p>步驟1.3. 為新類別輸入Name。</p> <p>步驟1.4. 在「站點」部分定義以下URL：</p> <p>.google.com</p> <p>步驟1.5. 提交變更。</p>  <p>影象 — 自定義URL類別</p> <p> 提示：有關如何配置自定義URL類別的詳細資訊，請訪問：<a href="#">在Secure Web Appliance中配置自定義URL類別</a>。</p>
<p>步驟2.解密流量。</p>	<p>步驟2.1. 從GUI導航到Web Security Manager，然後選擇Decryption Policies。</p> <p>步驟2.2. 按一下Add Policy。</p> <p>步驟2.3. 輸入新策略的Name。</p>

**Decryption Policy: Google account access**

**Policy Settings**

Enable Policy

Policy Name: ( ? ) Google Traffic Decryption **2.3**  
(i.e. my IP policy)

Description:   
(Maximum allowed characters: 256)

Insert Above Policy: 1 (Office365) v

Policy Expires:

Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  : :

步驟2.4.選擇需要此策略應用的Identification Profile。



提示：如果您繞過Microsoft URL的身份驗證，並且正在為所有使用者配置此策略，請選擇：All Identification Profiles > All Users。

步驟2.5.從策略成員定義部分，按一下URL類別連結，新增自定義URL類別。

步驟2.6.選擇在步驟1中建立的URL類別。

步驟2.7.單擊提交。

**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: Select One or More Identification Profiles v

Identification Profile: Select Identification Profile... v **2.4** No Identification Profile selected

Authorized Users and Groups:

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 traffic: **2.5**

User Agents: None Selected

**2.7**

影象 — 配置解密策略

步驟2.8. InDecryption Policies頁面，點選新策略的URL Filtering連結。

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Google account access Identification Profile: Global All identified users URL Categories: Google traffic	Decrypt: 1 <b>2.8</b>	(global policy)	(global policy)	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>

影象 — 編輯URL過濾操作

步驟2.9. 選擇Decrypt作為Custom URL Category的操作。

步驟2.10.單擊提交。



影象 — 解密自定義URL類別

步驟3.1.在GUI中，導覽至Web Security Manager，然後選擇HTTP ReWrite Profiles。

步驟3.2.按一下「Add Profile」。

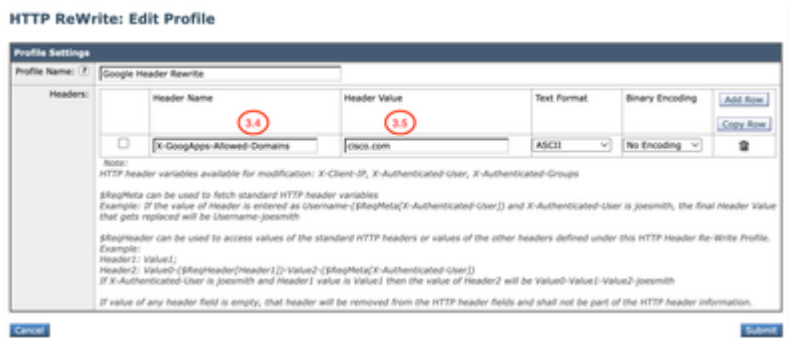
步驟3.3. 輸入新配置檔案的Name。

步驟3.4.將X-GoogApps-Allowed-Domains用於firstHeader名稱。

步驟3.5.對於Restrict-Access-To-Tenantssetting，使用允許的租戶清單的域值，該域值必須是允許使用者訪問的租戶的逗號分隔清單。

步驟3.建立HTTP重寫配置檔案。

步驟3.9.ClickSubmit。



影象 — 新增HTTP重寫配置檔案

步驟4.建立訪問策略。

步驟4.1.從GUI導航到Web Security Manager，然後選擇

Access Policies。

步驟4.2. 按一下Add Policy。

步驟4.3. 輸入新策略的Name。

步驟4.4。 ( 可選 ) 選擇需要此策略應用的Identification Profile。

第4.5步：從策略成員定義部分，按一下URL類別連結，新增自定義URL類別。

步驟4.6. 選擇URL Category，這是在第1步中建立的。

步驟4.7. 單擊提交。

Access Policy: Google account access

Policy Settings

Enable Policy

Policy Name: Google policy access

Description: (Maximum allowed characters: 256)

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

All Authenticated Users

Selected Groups and Users

All Users (authenticated and unauthenticated users)

Advanced

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

URL Categories: Google traffic

User Agents: None Selected

映像 — 建立訪問策略

步驟4.8. 在Access Policies頁面中，確保URL Filtering的操作設定為Monitor。

步驟4.9. 按一下HTTP重寫配置檔案中的連結將HTTP標頭配置檔案新增到此策略中。

Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile
(global policy)	Monitor	Restrict: 1 Monitor: 320	(global policy)	(global policy)	Google rewrite

影象 — 訪問策略屬性

步驟4.10. 選擇HTTP ReWrite Profiles ( 在步驟[3]中建立 )。

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Name: Google rewrite

Profiles:  Google rewrite

	影象 — 新增HTTP重寫配置檔案  步驟4.11.單擊提交。  步驟4.12.CommitChanges。
--	--

## 報告和日誌

### 記錄檔

您可以將自定義欄位新增到訪問日誌或W3C日誌，以檢視HTTP報頭重寫配置檔名稱。

訪問日誌中的格式說明符	W3C日誌中的日誌欄位	說明
%]	x-http-rewrite-profile-name	HTTP標頭重寫配置檔名稱。

您可以生成Web跟蹤報告，以便按訪問策略名稱檢視流量報告。

使用以下步驟生成報告：

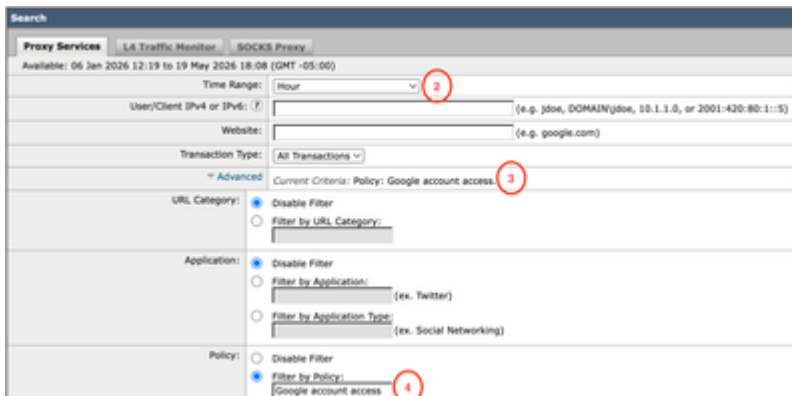
步驟1. 在GUI中選擇Reporting，然後選擇Web Tracking。

步驟2.選擇所需的時間範圍。

步驟3.按一下Advanced連結以使用高級條件搜尋事務處理。

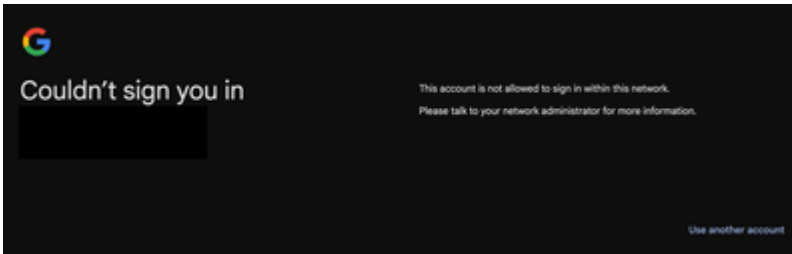
步驟4.在Policy部分，選擇Filter by Policy，然後鍵入先前建立的Access Policy的名稱。

步驟5.按一下Search以檢視報告。



## 驗證

完成Google域限制配置後，使用者只能訪問第3步的「標題重寫」配置檔案中配置的域下的帳戶。如果使用者嘗試訪問其他域上的帳戶，或者不同的、個人的Google帳戶，則訪問受此通知限制：



## 相關資訊

[在WSA中定義自定義URL類別](#)

[Cisco Secure Web Appliance AsyncOS 15.2使用手冊](#)

[在安全Web裝置中配置解密證書](#)

[WSA HTTP標頭重寫](#)

[阻止訪問消費者帳戶 \( Google文檔 \)](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。