

# Sperrung des Zugriffs auf Google-Privatkundenkonten in den SWAs

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Berichte und Protokolle](#)

[Protokolle](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

---

## Einleitung

Dieses Dokument beschreibt den Prozess der Blockierung des Zugriffs auf Google Workspace oder Google Consumer Accounts in Secure Web Appliance (SWA).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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

Schritt 1.1: Navigieren Sie in der GUI zum Web Security Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus.

Schritt 1.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen.

Schritt 1.3: Geben Sie einen Namen für die neue Kategorie ein.

Schritt 1.4. Definieren Sie diese URLs im Abschnitt Sites:

.google.com

Schritt 1.5. Änderungen übermitteln.

Schritt 1. Erstellen Sie eine benutzerdefinierte URL-Kategorie für die Google-Websites.

### Custom and External URL Categories: Edit Category

Category Name: Google traffic

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ? .google.com, .youtube.com

Sort URLs  
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Regular Expressions: ?

Enter one regular expression per line. Maximum allowed characters: 2048.

Cancel Submit

Bild - Benutzerdefinierte URL-Kategorie



Tipp: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter: [Konfigurieren benutzerdefinierter URL-Kategorien in der sicheren Webappliance.](#)

Schritt 2.1. Navigieren Sie in der GUI zu Websicherheits-Manager, und wählen Sie Entschlüsselungsrichtlinien aus.

Schritt 2.2. Klicken Sie auf Richtlinie hinzufügen.

Schritt 2.3: EnterName für die neue Richtlinie.

Decryption Policy: Google account access

Schritt 2.4: Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.



Tip: Wenn Sie die Authentifizierungen für Microsoft-URLs umgangen haben und diese Richtlinie für Alle Benutzer konfigurieren, wählen Sie: Alle Identifizierungsprofile > Alle Benutzer.

Schritt 2:Entschlüsseln des Datenverkehrs

Schritt 2.5. Klicken Sie im Abschnitt "Policy Member Definition" auf URL-KategorienLinks, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 2.6. Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde.

Schritt 2.7: Klicken Sie auf Senden.

Image: Konfigurieren der Entschlüsselungsrichtlinie

Schritt 2.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung

für die neue Richtlinie.

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]		

Bild - URL-Filterungsaktion bearbeiten

Schritt 2.9. Wählen Sie Entschlüsseln als Aktion für die benutzerdefinierte URL-Kategorie aus.

Schritt 2.10. Klicken Sie auf Senden.

**Decryption Policies: URL Filtering: Google account access**

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 (F)	Quota-Based	Time-Based
Google traffic	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

**2.9** **2.10** **Submit**

Bild: Entschlüsseln der benutzerdefinierten URL-Kategorie

Schritt 3.1. Navigieren Sie in der GUI zu Web Security Manager und wählen Sie HTTP ReWrite Profiles.

Schritt 3.2. Klicken Sie auf Profil hinzufügen.

Schritt 3.3: Geben Sie einen Namen für das neue Profil ein.

Schritt 3.4: Verwenden Sie X-GoogApps-Allowed-Domains als ersten Header-Namen.

Schritt 3.5. Für die Einstellung "Restrict-Access-To-Tenants" verwenden Sie einen Domänenwert der Liste zulässiger Tenants, bei der es sich um eine kommasetrennte Liste der Tenants handeln muss, auf die Benutzer zugreifen dürfen.

Schritt 3.9. Klicken Sie auf Senden.

Schritt 3: Erstellen eines HTTP Rewrite Profile

**HTTP ReWrite: Edit Profile**

Profile Settings

Profile Name: Google Header Rewrite

Header Name	Header Value	Text Format	Binary Encoding
X-GoogApps-Allowed-Domains	1900.com	ASCII	No Encoding

**3.6** **3.5**

Note:  
HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Group  
\$ReqMeta can be used to fetch standard HTTP header variables  
Example: If the value of Header is entered as Username-(\$ReqMeta[X-Authenticated-User]) and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith  
\$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.  
Example:  
Header 1: Value1;  
Header 2: Value2-(\$ReqHeader[Header1])-Value3-(\$ReqMeta[X-Authenticated-User]);  
If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith  
If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.

**Cancel** **Submit**

Bild - HTTP ReWrite-Profil hinzufügen

Schritt 4: Erstellen einer Zugriffsrichtlinie

Schritt 4.1. Navigieren Sie in der GUI zu Websicherheits-Manager, und wählen Sie Zugriffsrichtlinien aus.

Schritt 4.2. Klicken Sie auf Richtlinie hinzufügen.

Schritt 4.3: EnterName für die neue Richtlinie.

Schritt 4.4 (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.

Schritt 4.5. Klicken Sie im Abschnitt "Policy Member Definition" auf URL-Kategorien Links, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 4.6. Wählen Sie die in Schritt 1 erstellte URL-Kategorie aus.

Schritt 4.7. Klicken Sie auf Senden.

The screenshot displays the configuration interface for an access policy. The top section, 'Policy Settings', includes a checkbox for 'Enable Policy' and a text field for 'Policy Name' containing 'Google policy access'. Below this is a 'Description' field. The bottom section, 'Policy Member Definition', contains radio buttons for 'All Identification Profiles', 'All Authenticated Users', 'Selected Groups and Users', and 'All Users'. The 'Advanced' section lists various criteria: 'Protocols', 'Proxy Ports', 'Subnets', 'Time Range', 'URL Categories' (set to 'Google traffic'), and 'User Agents'. Red circles highlight the 'Policy Name' field, the 'All Identification Profiles' radio button, and the 'Google traffic' option under 'URL Categories'.

Bild: Erstellen einer Zugriffsrichtlinie

Schritt 4.8. Stellen Sie auf der Seite Access Policies (Zugriffsrichtlinien) sicher, dass die Aktion der URL-Filterung auf Monitor (Überwachen) festgelegt ist.

Schritt 4.9: Klicken Sie auf den Link in HTTP ReWrite Profile, um dieser Richtlinie das HTTP-Header-Profil hinzuzufügen.

Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	C
(global policy)	Monitor: 4.8	Restrict: 1 Monitor: 320	(global policy)	(global policy)	Google rewrite 4.9	

Bild - Eigenschaften der Zugriffsrichtlinie

Schritt 4.10: Wählen Sie die HTTP-ReWrite-Profile, die in Schritt [3] erstellt wurden.

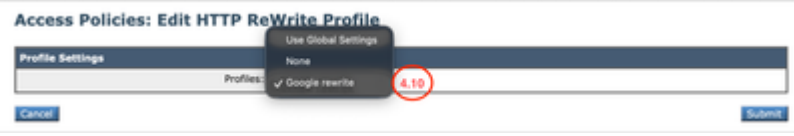


Bild - HTTP ReWrite-Profil hinzufügen

Schritt 4.11. Klicken Sie auf Senden.

Schritt 4.12. Änderungen bestätigen.

## Berichte und Protokolle

### Protokolle

Sie können den Zugriffsprotokollen oder den W3C-Protokollen benutzerdefinierte Felder hinzufügen, um den Namen des HTTP-Header-Umschreibprofils anzuzeigen.

Formatangabe in Zugriffsprotokollen	Protokollfeld in W3C-Protokollen	Beschreibung
%]	x-http-rewrite-profilname	Profilname für HTTP-Header umschreiben.

Sie können einen Web-Tracking-Bericht erstellen, um die Berichte des Datenverkehrs nach dem Namen der Zugriffsrichtlinie anzuzeigen.

Gehen Sie folgendermaßen vor, um Berichte zu erstellen:

Schritt 1: Wählen Sie in der GUI Reporting aus, und wählen Sie Web Tracking aus.

Schritt 2: Wählen Sie den gewünschten Zeitraum.

Schritt 3: Klicken Sie auf den Link Erweitert, um Transaktionen nach erweiterten Kriterien zu suchen.

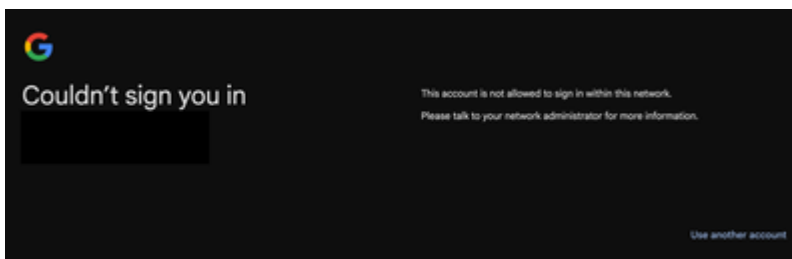
Schritt 4. Wählen Sie im Abschnitt Policy (Richtlinie) die Option Filter by Policy (Nach Richtlinie filtern) aus, und geben Sie den Namen der zuvor erstellten Zugriffsrichtlinie ein.

Schritt 5: Klicken Sie auf Suchen, um den Bericht zu überprüfen.

The screenshot shows the 'Search' interface of a Cisco Secure Web Appliance. It includes tabs for 'Proxy Services', 'L4 Traffic Monitor', and 'SOCKS Proxy'. The 'Advanced' section is expanded, showing search criteria for 'URL Category', 'Application', and 'Policy'. The 'Policy' section has 'Filter by Policy' selected, with 'Google account access' entered in the text field. Red circles are placed around the 'Time Range' dropdown (2), the 'Current Criteria' dropdown (3), and the 'Filter by Policy' radio button (4).

## Überprüfung

Wenn die Konfiguration der Google-Domänenbeschränkung abgeschlossen ist, kann der Benutzer nur auf die Konten zugreifen, die sich unter der im Header Rewrite-Profil in Schritt 3 konfigurierten Domäne befinden. Wenn die Benutzer versuchen, auf ein Konto in einer anderen Domäne oder, in einem anderen, persönlichen Google-Konto zuzugreifen, wird der Zugriff mit diesem Hinweis eingeschränkt:



## Zugehörige Informationen

[Benutzerdefinierte URL-Kategorien in WSA definieren](#)

[Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance](#)

[Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren](#)

[WSA HTTP Header Rewrite](#)

[Zugriff auf Verbraucherkonten blockieren \(Google-Dokumentation\)](#)

## 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.