

# Block Google Consumer Accounts Access in the SWA

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Reporting and Logs](#)

[Logs](#)

[Verify](#)

[Related Information](#)

---

## Introduction

This document describes the process of blocking Google Workspace or Google Consumer Accounts access in Secure Web Appliance (SWA).

## Prerequisites

### Requirements

Cisco recommends knowledge of these topics:

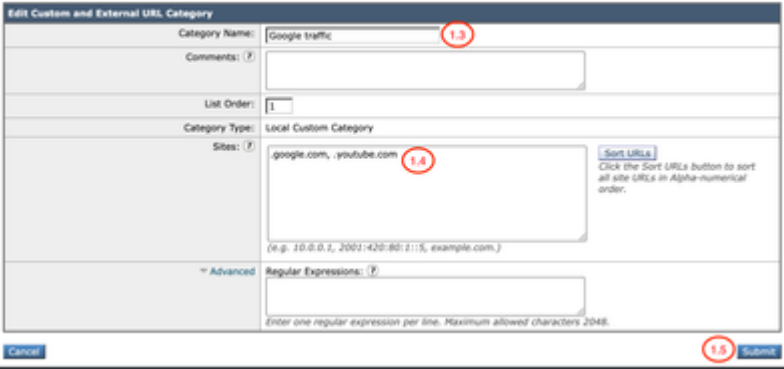

- Access to the Graphic User Interface (GUI) of SWA
- Administrative Access to the SWA.

### Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

# Configure

<p>Step 1. Create a Custom URL Category for the Google sites.</p>	<p>Step 1.1. From the GUI, navigate to <b>Web Security Manager</b> and choose <b>Custom and External URL Categories</b>.</p> <p>Step 1.2. Click <b>Add Category</b> to create a new Custom URL Category.</p> <p>Step 1.3. Enter <b>Name</b> for the new category.</p> <p>Step 1.4. Define these URLs in the Sites section:</p> <p>.google.com</p> <p>Step 1.5. <b>Submit</b> the changes.</p> <p><b>Custom and External URL Categories: Edit Category</b></p>  <p><i>Image - Custom URL Category</i></p> <p> <b>Tip:</b> For more information about how to configure Custom URL Categories, kindly visit: <a href="#">Configure Custom URL Categories in Secure Web Appliance</a>.</p>
<p>Step 2. Decrypt the traffic.</p>	<p>Step 2.1. From the GUI, navigate to <b>Web Security Manager</b> and choose <b>Decryption Policies</b>.</p> <p>Step 2.2. Click <b>Add Policy</b>.</p> <p>Step 2.3. Enter <b>Name</b> for the new policy.</p>

**Decryption Policy: Google account access**

**Policy Settings**

**Enable Policy**

Policy Name: ( ? )  **2.3**  
(i.e. my IT policy)

Description:   
(Maximum allowed characters: 256)

Insert Above Policy:  ▾

Policy Expires:

Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  :  :

Step 2.4. Select the **Identification Profile** that you need this policy to apply to.



**Tip:** If you bypassed the Authentications for Microsoft URLs and you are configuring this policy for All users, choose: **All Identification Profiles > All Users**.

Step 2.5. From **Policy Member Definition** section, click **URL Categories** links to add the Custom URL Category.

Step 2.6. Select the **URL Category** that was created in Step 1.

Step 2.7. Click **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:  ▾

Identification Profile:  ▾ **2.4** No Identification Profile selected

Authorized Users and Groups:

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 traffic **2.5**

**User Agents:** None Selected

**2.7**

Image - Configure Decryption Policy

Step 2.8. In **Decryption Policies** page, click the link from **URL Filtering** for the new policy.

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"/>

Image - Edit URL Filtering Action

Step 2.9. Choose **Decrypt** as the action for Custom URL Category.

Step 2.10. Click **Submit**.

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

Custom and External URL Category Filtering		Use Global Settings	Override Global Settings					
Category	Category Type	Select all	Pass Through	Monitor	Decrypt	Drop (?)	Quota-Based	Time-Based
Google traffic	Custom (Local)	—	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Image - Decrypt the Custom URL Category

Step 3.1. From the GUI, navigate to **Web Security Manager** and choose **HTTP ReWrite Profiles**.

Step 3.2. Click **Add Profile**.

Step 3.3. Enter **Name** for the new profile.

Step 3.4. Use **X-GoogApps-Allowed-Domains** for the first **Header Name**.

Step 3.5. For the **Restrict-Access-To-Tenants** setting, use a domain value of permitted tenant list, which must be a comma-separated list of the tenants that users are allowed to access.

Step 3. Create HTTP Rewrite Profile.

Step 3.9. Click **Submit**.

### HTTP ReWrite: Edit Profile

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

Image - Add HTTP ReWrite Profile

Step 4.1. From the GUI, navigate to **Web Security Manager** and choose **Access Policies**.

Step 4.2. Click **Add Policy**.

Step 4.3. Enter **Name** for the new policy.

Step 4.4. (Optional) Select the **Identification Profile** that you need this policy to apply to.

Step 4.5. From **Policy Member Definition** section, click **URL Categories** links to add the Custom URL Category.

Step 4.6. Select the **URL Category** that was created in Step 1.

Step 4.7. Click **Submit**.

Step 4. Create Access Policy.

Access Policy: Google account access

Policy Settings

Enable Policy

Policy Name: Google policy access (4.3)  
(e.g. my IP policy)

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 (4.4)

All Authenticated Users

Selected Groups and Users (2)

ISE Secure Group Tags: No tags entered

ISE Groups: No groups entered

Groups: No groups entered

Users: No users entered

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: Google traffic (4.5)

User Agents: None Selected

Cancel Submit

Image - Create Access Policy

Step 4.8. In **Access Policies** page, make sure the action of the **URL Filtering** is set to **Monitor**.

Step 4.9. Click the link in **HTTP ReWrite Profile** to add the HTTP Header Profile to this policy.

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

Image - Access Policy Properties

Step 4.10. Choose the **HTTP ReWrite Profiles**, created in Step [3].

Access Policies: Edit HTTP ReWrite Profile

Use Global Settings

Profile Settings

Profiles: Google rewrite (4.10)

Cancel Submit

	<p><i>Image - Add HTTP ReWrite Profile</i></p> <p>Step 4.11. Click <b>Submit</b>.</p> <p>Step 4.12. Click <b>CommitChanges</b>.</p>
--	---

## Reporting and Logs

### Logs

You can add custom fields to the access logs or the W3C logs to view the HTTP header rewrite profile name.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%]	x-http-rewrite-profile-name	HTTP header rewrite profile name.

You can generate Web Tracking report to view the reports of the traffic by the Access Policy name.

Use these steps to generate the reports:

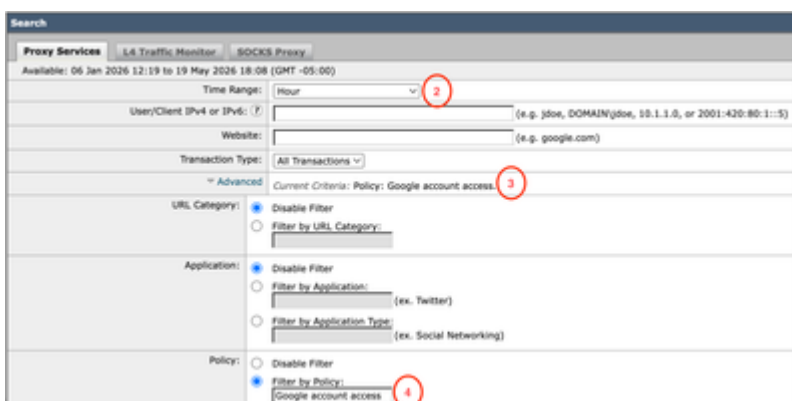
Step 1. From the GUI, select **Reporting** and choose **Web Tracking**.

Step 2. Choose your desired **Time Range**.

Step 3. Click the **Advanced** link to search transactions using advanced criteria.

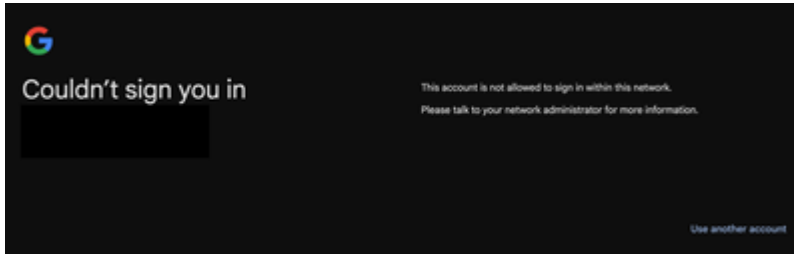
Step 4. In the **Policy** section, select **Filter by Policy** and type the name of the **Access Policy** that was created previously.

Step 5. Click **Search** to review the report.



# Verify

When the Google domain restriction configuration is completed, the user is only able to access the accounts which are under the domain configured on the Header Rewrite profile on Step 3. If the user tries accessing an account on a different domain, or, a different, personal, Google account, the access is restricted with this notice:



## Related Information

[Define Custom URL Categories in WSA](#)

[User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance](#)

[Configure Decryption Certificate in Secure Web Appliance](#)

[WSA HTTP Header Rewrite](#)

[Block Access to Consumer Accounts \(Google Documentation\)](#)