

Enable Specific YouTube Channel/Video and Block Rest of YouTube in SWA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Steps](#)

[Related Information](#)

Introduction

This document describes how to allow specific YouTube channels/videos and block the rest of YouTube in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access To 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.

Configuration Steps

Use these steps in order to allow a specific YouTube channel while access to YouTube is blocked:

Step 1. Create **Custom and External URL Categories** for the channel that needs to grant access, in this example, this URL category is called 'channel'.

Step 1.1. From GUI, navigate to **Web Security Manager** and choose **Custom URL and External Categories**.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

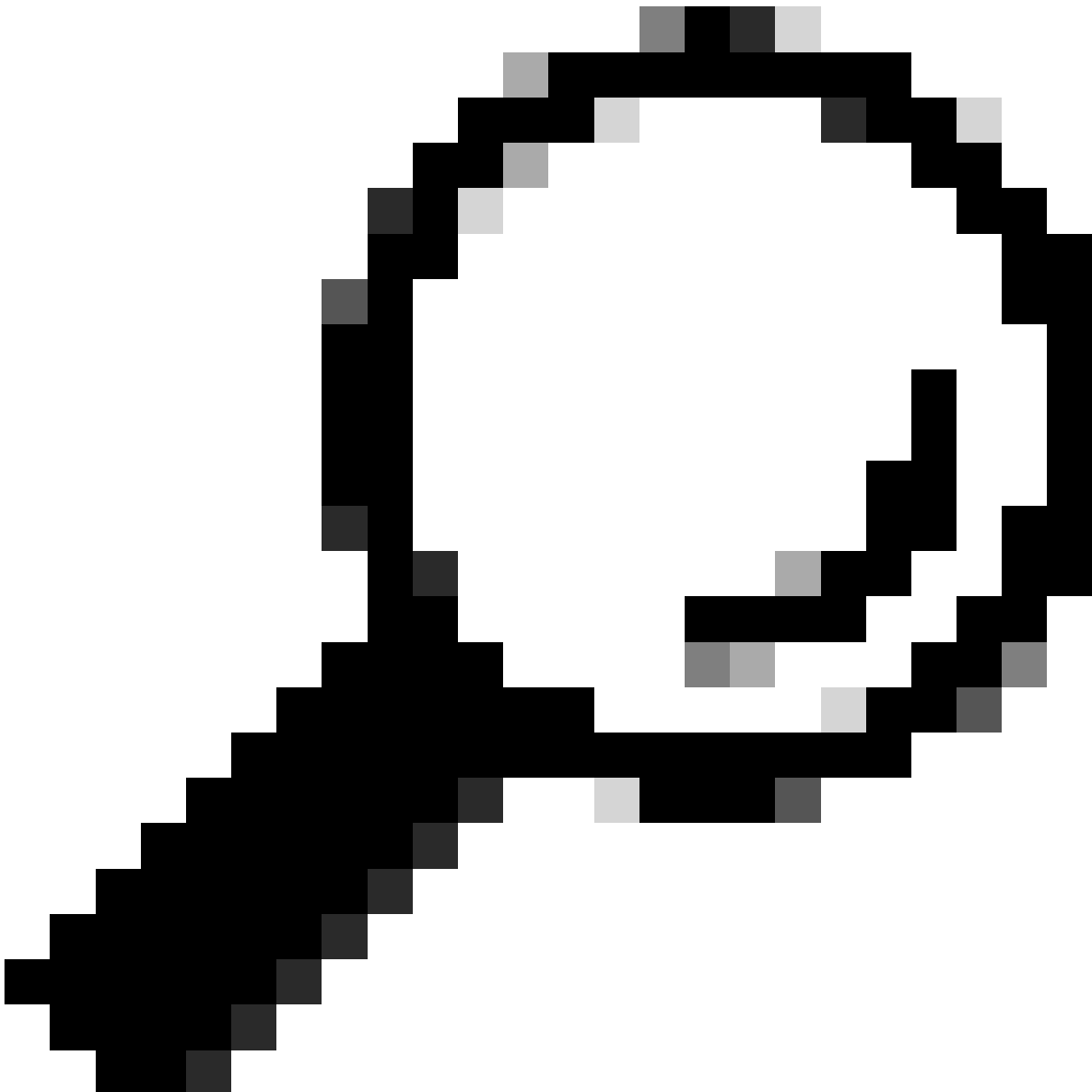
: Ensure the 'Channel' custom URL category has lower priority than the 'YouTube' custom URL category.

Custom and External URL Categories

Categories List						
Add Category...						
Order	Category	Category Type	Comments	Last Updated	Feed Content	Delete
1	Channel	Custom (Local)		N/A	-	
2	YouTube	Custom (Local)	Block Access to YouTube	N/A	-	

Image- Custom URL Category Order.png

Step 3. Create **Identification Profiles** for the users who are permitted to access the YouTube channel.



Tip: You can set the Custom Categories in the Decryption and Access Policy. In this case, there is no need to set a separate ID profile.

Step 3.1. From GUI, navigate to **Web Security Manager** and choose **Identification Profiles**.

Step 3.2. Choose **Add Identification Profile**.

Step 3.3. Enter the **Profile Name**.

Step 3.4. Choose the user(s) or define the members by IP Subnet.

Step 3.5. Click the **Advanced** section and choose **URL Categories**.

Identification Profiles: Users Allowed To View Channel

Client / User Identification Profile Settings

Enable Identification Profile

Name:
(e.g. my IT Profile)

Description:
(Maximum allowed characters 256)

Insert Above:

User Identification Method

Identification and Authentication: For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).

Membership Definition

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

Define Members by Subnet:
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: HTTP/HTTPS

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

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

URL Categories: None Selected

User Agents: None Selected

The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

Image- Create ID Profile

Step 3.6. Add both URL categories which were created in Step 1. and Step 2. and click **Done**.

Identity Profiles: Policy "Users Allowed To View Channel": Membership by URL Categories

Advanced Membership Definition: URL Category

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

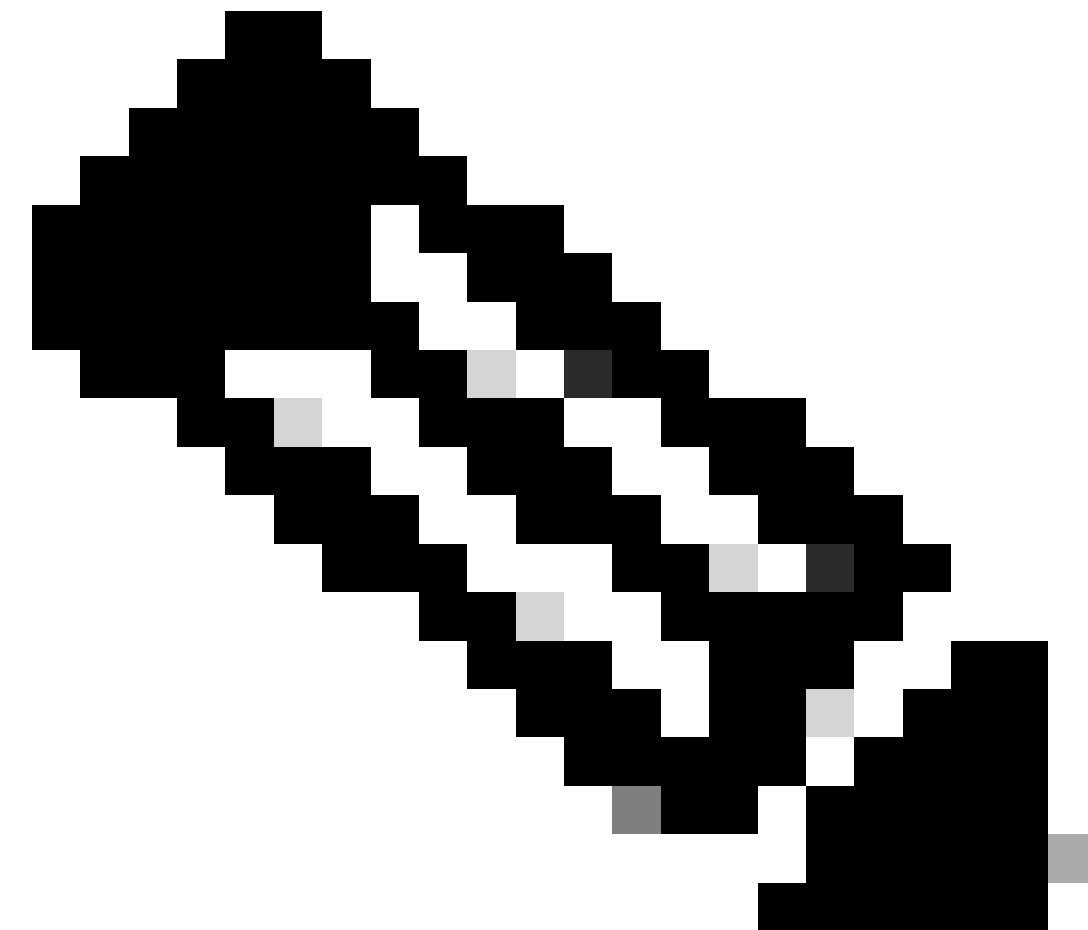
Custom and External URL Categories		
Category	Category Type	
Channel	Custom (Local)	<input checked="" type="checkbox"/>
YouTube	Custom (Local)	<input checked="" type="checkbox"/>

Note: In the original image, the 'Channel' and 'YouTube' rows in the table and the 'Add' and 'Select all' buttons in the right-hand column are highlighted with red boxes.

Image- Add URL Categories

Step 3.7. **Submit** changes.

Step 4. Create a Decryption policy in order to decrypt the YouTube traffic. In this example, the policy name is **Decrypt Youtube**.



Note: If you do not decrypt YouTube Traffic, SWA is unable to determine the channel address in Transparent deployment.

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

Step 4.2. Choose **Add Policies** and enter the policy Name.

Step 4.3. Choose the **Identification Profile** that you created in Step 3.

Decryption Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy)

Description: (Maximum allowed characters 256)

Insert Above Policy:

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

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	Authorized Users and Groups	Add Identification Profile
<input type="text" value="Users Allowed To View Channel"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

Define additional group membership criteria.

Image- Create Decryption Policy

Step 4.4. **Submit** the changes.

Step 4.5. On the **Decryption Policies** page, click **Monitor** in the **URL Filtering** section.

Decryption Policies

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Decrypt Youtube Identification Profile: Users Allowed To View Channel All identified users	<input type="button" value="Monitor: 2"/>	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107	Enabled	Decrypt		

Image- Click on URL Filtering

Step 4.6. Choose **Decrypt** for both URL categories and **Submit**.

Decryption Policies: URL Filtering: Decrypt Youtube

Custom and External URL Category Filtering								
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>								
Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Channel	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—
YouTube	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—

Image- Choose Decrypt

Step 5. Create an **Access Policy** in order to configure YouTube Channel access. In this example, the policy name is **Allow YouTube**.

Step 5.1. From GUI, navigate to **Web Security Manager** and choose **Access Policies**.

Step 5.2. Click **Add Policy** and enter the policy name.

Step 5.3. Choose the **Identification Profile** that you create in Step 3.

Access Policy: Add Group

Policy Settings

Enable Policy

Policy Name: ?

Allow YouTube

(e.g. my 11 policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy:

1 (Global Policy) ▾

Policy Expires:

Set Expiration for Policy

On Date:

MM/DD/YYYY

At Time:

:

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 ▾

Identification Profile	Authorized Users and Groups	
Users Allowed To View Channel ▾	No authentication required	<div style="background-color: #2c3e50; color: white; padding: 2px 5px;">Add Identification Profile</div> <div style="text-align: center; font-size: small;">🗑️</div>

Advanced ▾

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:

HTTP/HTTPS/FTP over HTTP in Identification Profile Users Allowed To View Channel

Proxy Ports:

None Selected

Subnets:

None Selected

Time Range:

No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories:

URL Categories Channel, YouTube in Identification Profile Users Allowed To View Channel

User Agents:

None Selected

Image- Create Access Policy

Step 5.4. **Submit** changes.

Step 5.5. On the **Access Policies** page, click **Monitor** in the **URL Filtering** section.

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Allow YouTube Identification Profile: Users Allowed To View Channel All identified users	(global policy)	Monitor: 2	(global policy)	(global policy)	(global policy)	(global policy)	🔄	🗑️
	Global Policy Identification Profile: All	No blocked items	Monitor: 107	Monitor: 342	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Edit Policy Order...

Image- Configure Access Policy

Step 5.6. Choose **Allow** for **Channel** category.

Step 5.7. Choose **Block** for the **YouTube** category.

Access Policies: URL Filtering: Allow YouTube

Custom and External URL Category Filtering		Use Global Settings		Override Global Settings					
Category	Category Type	Select all	Block	Redirect	Allow ?	Monitor	Warn ?	Quota-Based	Time-Based
Channel	Custom (Local)	--	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
YouTube	Custom (Local)	--	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Image- Set Category Action

Step 5.8. On the same page, scroll to **Exceptions to Blocking for Embedded/Referred Content** and Enable **Referrer Exceptions**.

Step 5.9. Choose **All embedded/referred content**.

Exceptions to Blocking for Embedded/Referred Content

A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category / application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category representing your intranet).

Enable Referrer Exceptions

Set Exception for Content Referred by These Categories:

Set Exception for This Referred Content:

Image- Enable Referrer

Step 5.10. From Set Exception for Content Referred by These Categories, choose the **YouTube** custom URL category.

Exceptions to Blocking for Embedded/Referred Content

A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category / application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category representing your intranet).

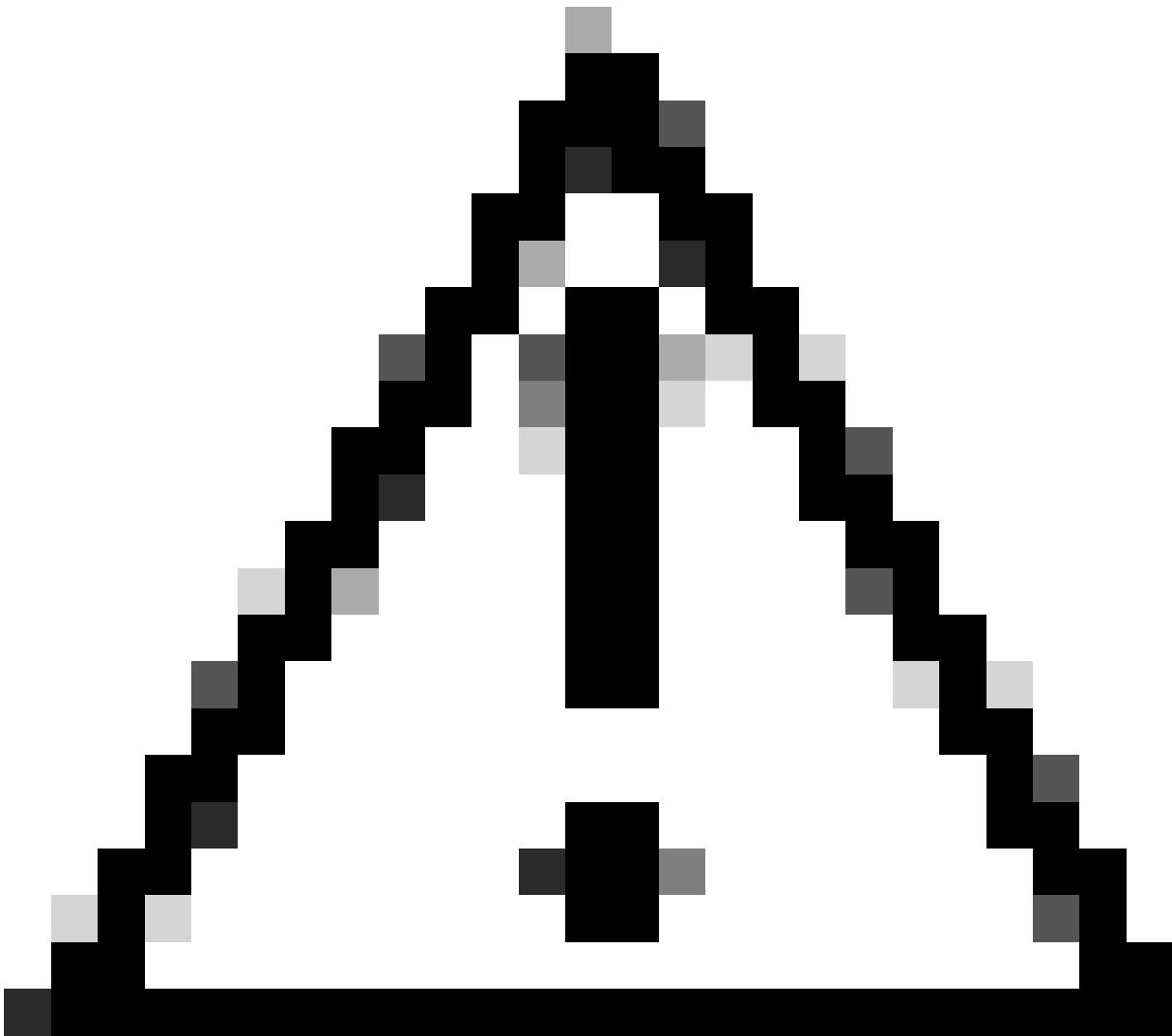
Enable Referrer Exceptions

Set Exception for Content Referred by These Categories:

Set Exception for This Referred Content:

Image- Configure Embedded Content

Step 5.11. **Submit** and **Commit** changes.



Caution: If users first access the Channel, then they can navigate to all YouTube videos.

Related Information

- [User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD\(General Deployment\) - Troubleshooting \[Cisco Secure Web Appliance\] - Cisco](#)
- [Cisco Technical Support & Downloads](#)