# Enable Specific YouTube Channel or Video and Block Rest of YouTube in SWA

## Contents


**Introduction**

**Prerequisites**

- Requirements
- Components Used

**Configuration Steps**

**Related Content**


## Introduction

This document describes how to allow specific YouTube channels or 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 to which you want 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**.

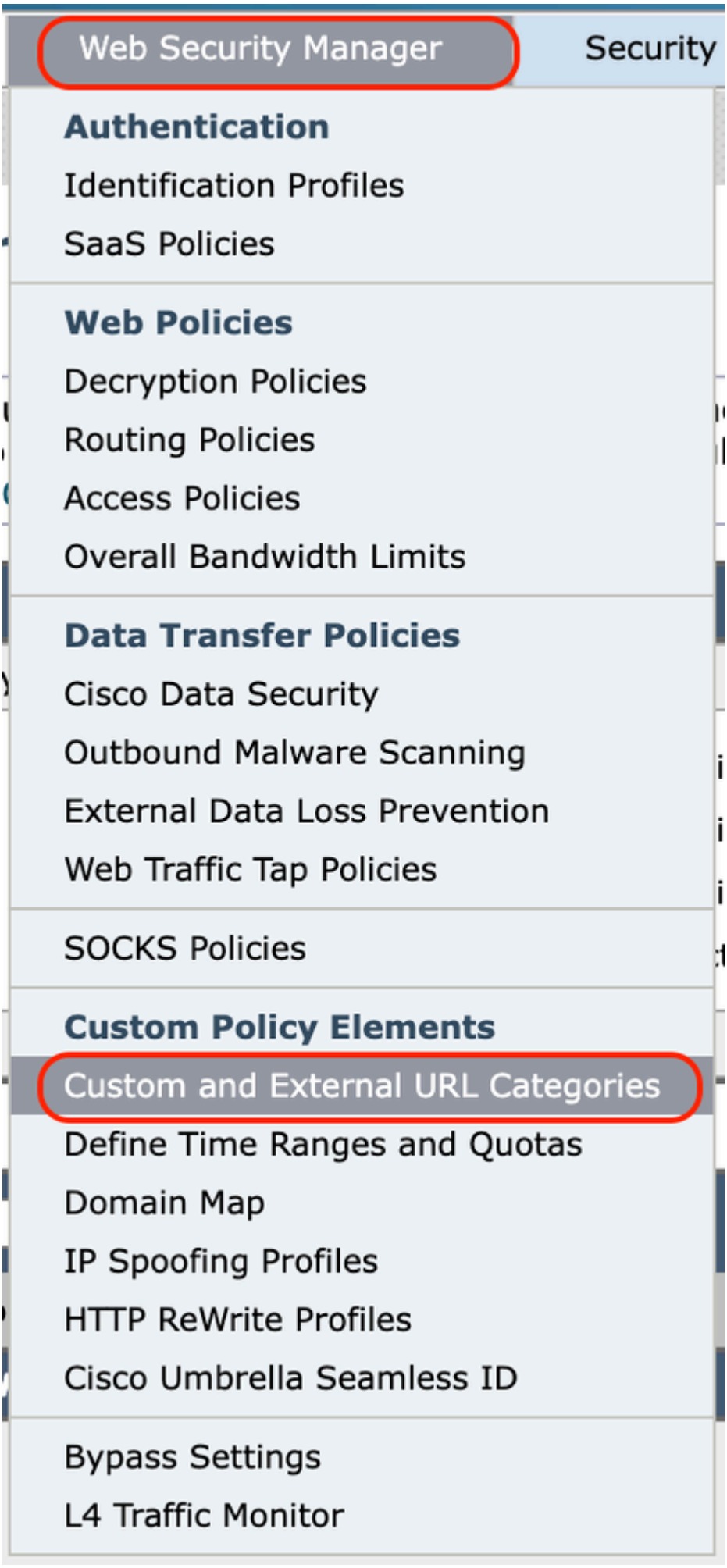

Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories
Define Time Ranges and Quotas
Domain Map
IP Spoofing Profiles
HTTP ReWrite Profiles
Cisco Umbrella Seamless ID
Bypass Settings
L4 Traffic Monitor

*Image- Choose Custom and External URL Categories*

Step 1.2. Choose **Add Category** and set the **Category Name**.

Step 1.3. Add these two **URLs** in the Sites section.

```
ytimg.com, .ytimg.com
```

Step 1.4. In this example, the Channel URL is Cisco Secure Web Appliance YouTube Channel. Add this Regular expressions for the channel:

```
\.youtube.*UCsl9s\_etl\_i6Hb2ilAl71Bw
```

Step 1.5. Add these **Regular Expressions**, which are general and not specific to your Channel URL.

```
youtube\.com/videoplayback
www\.youtube\.com/crossdomain\.xml
youtube\.com/generate
```

Step 1.6. **Submit** changes.

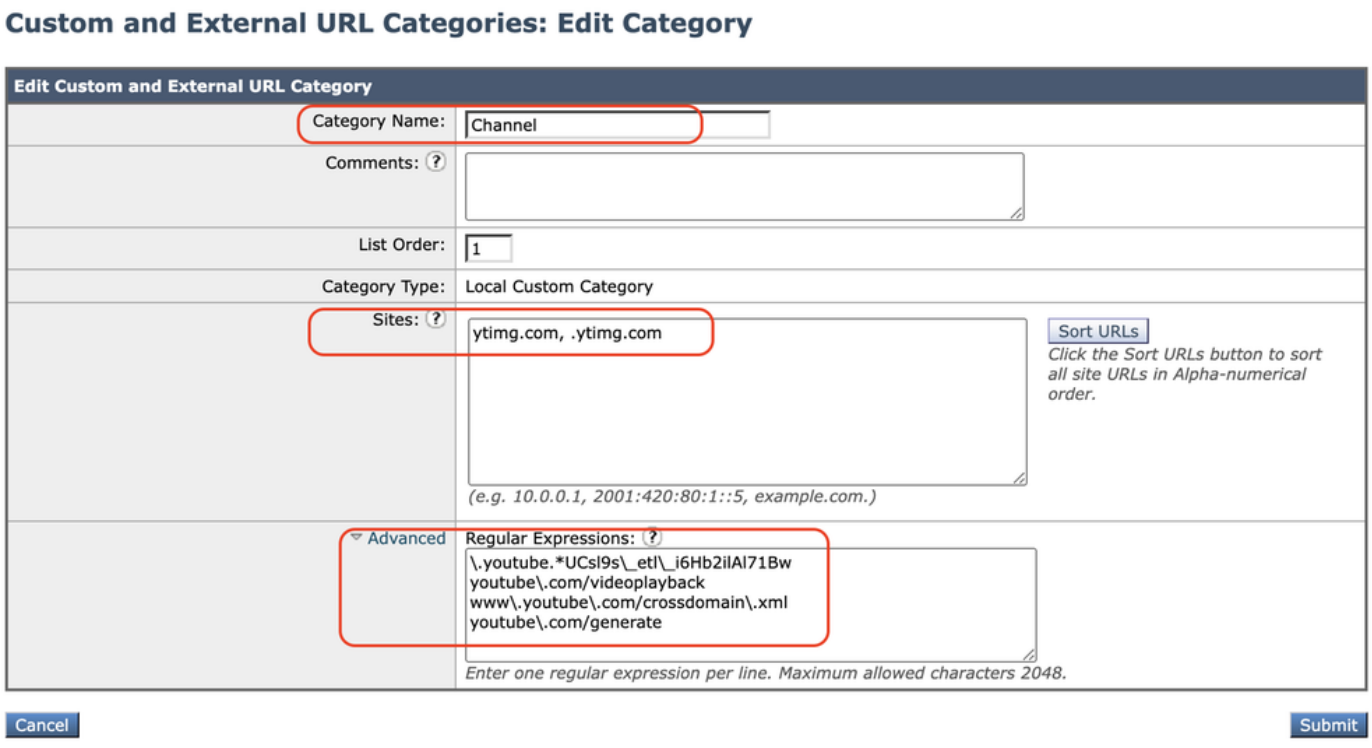



*Image- Configure Channel Custom URL Category*

Step 2. Create **Custom and External URL Categories** in order to block YouTube. (In this example, the category was named YouTube.)

Step 2.1. In the **Custom URL and External Categories** choose **Add Category** and set the **Category Name**.

Step 2.2. Add these two **URLs** in the Sites section.

```
.youtube.com, youtube.com
```

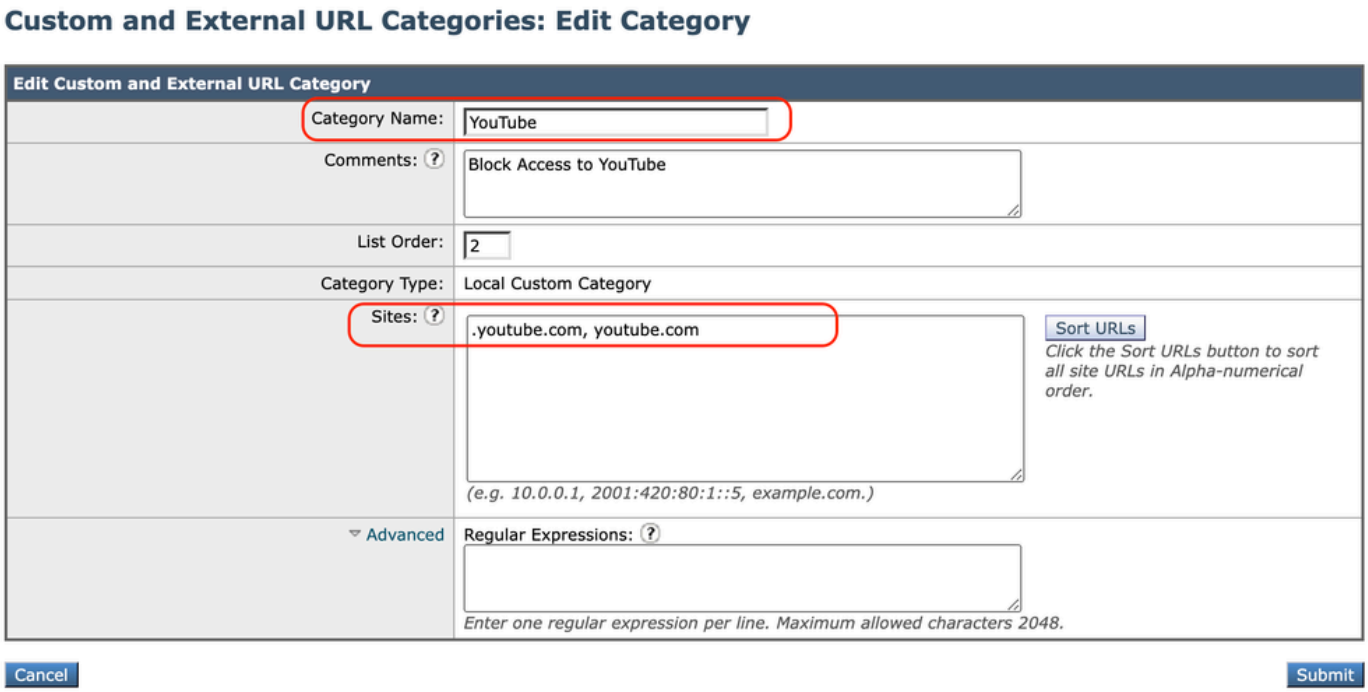



*Image- Configure Category to Block Access To YouTube*

Step 2.3. Click **Submit**.

---

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

---

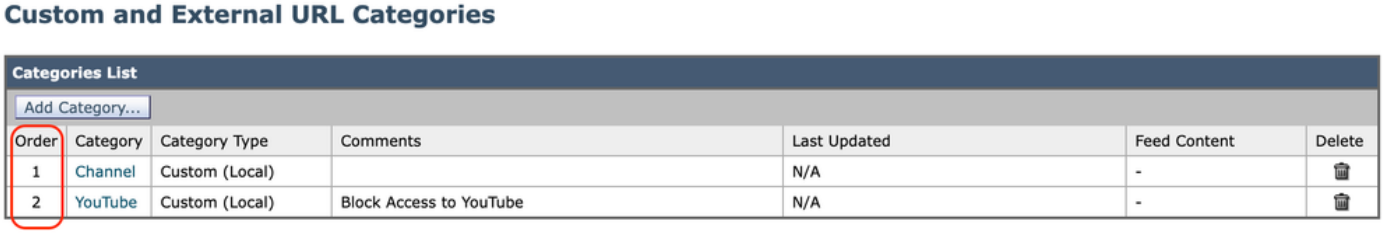


*Image- Custom URL Category Order.png*

Step 3. Create **Identification Profiles** for the users that 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**.

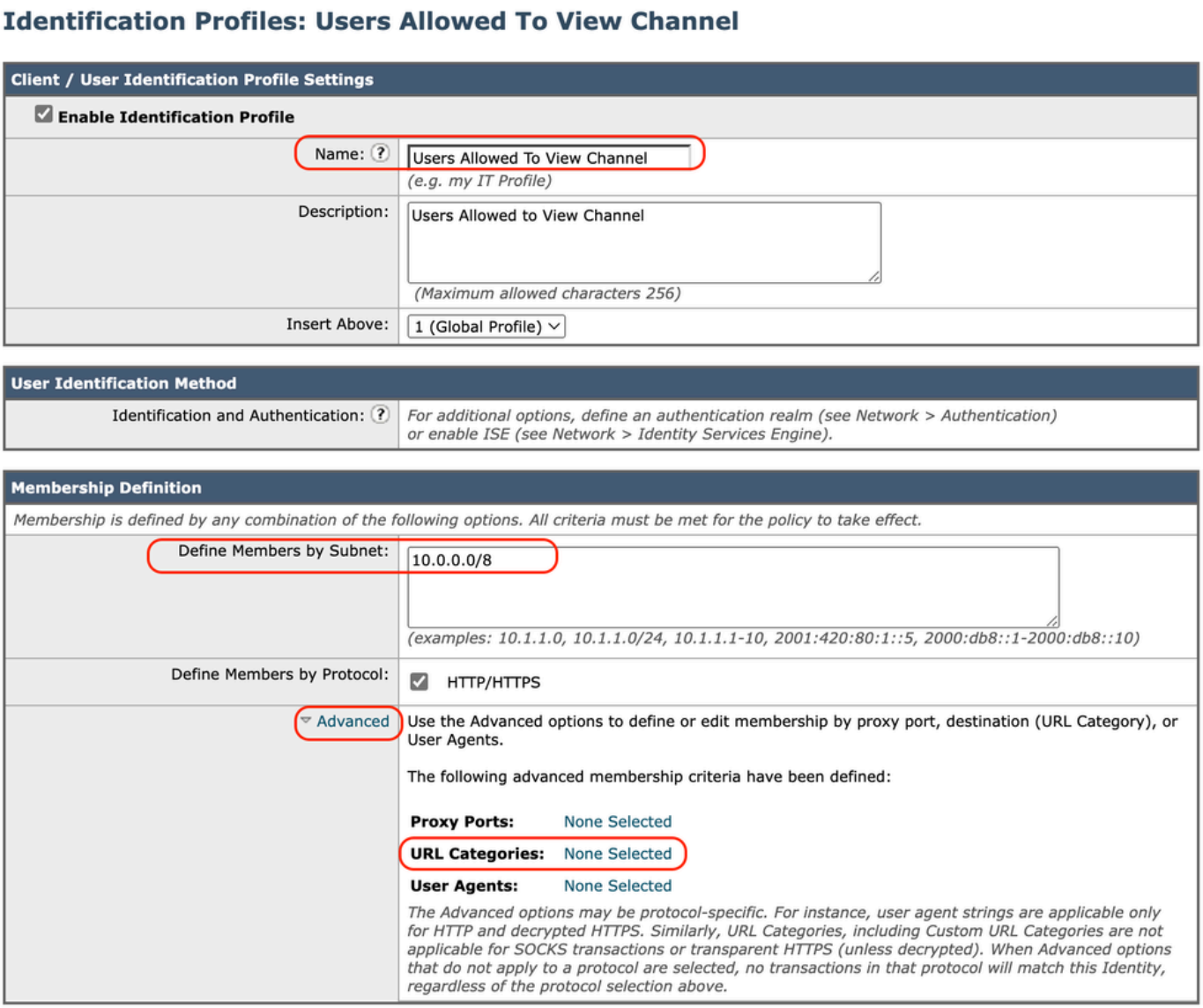



*Image- Create ID Profile*

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

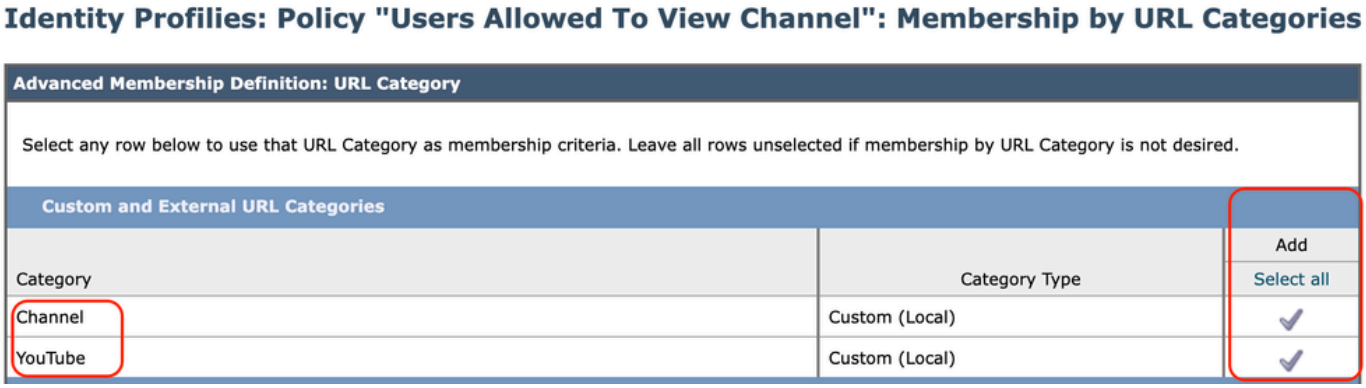



*Image- Add URL Categories*

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.

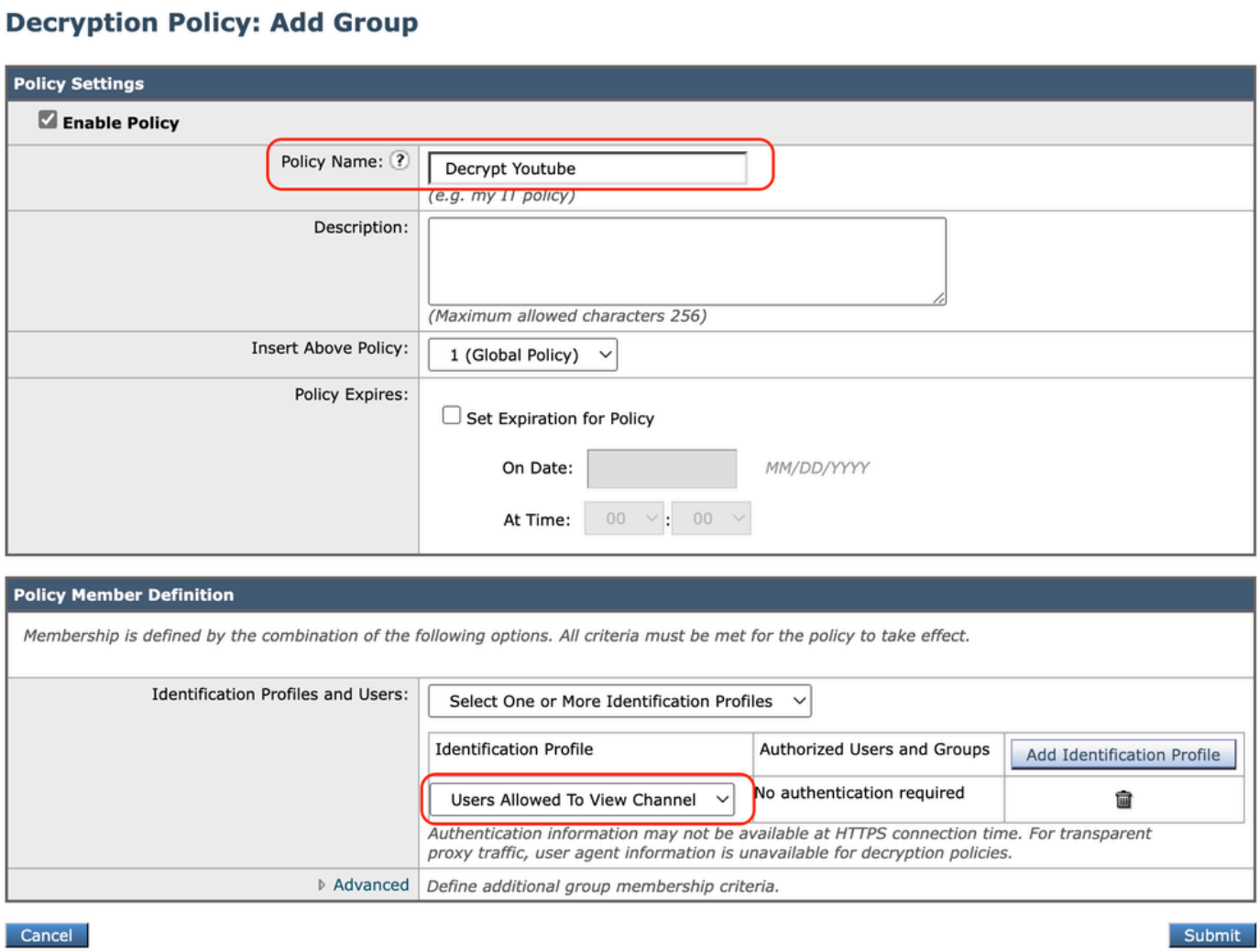



*Image- Create Decryption Policy*

Step 4.4. **Submit** the changes.

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

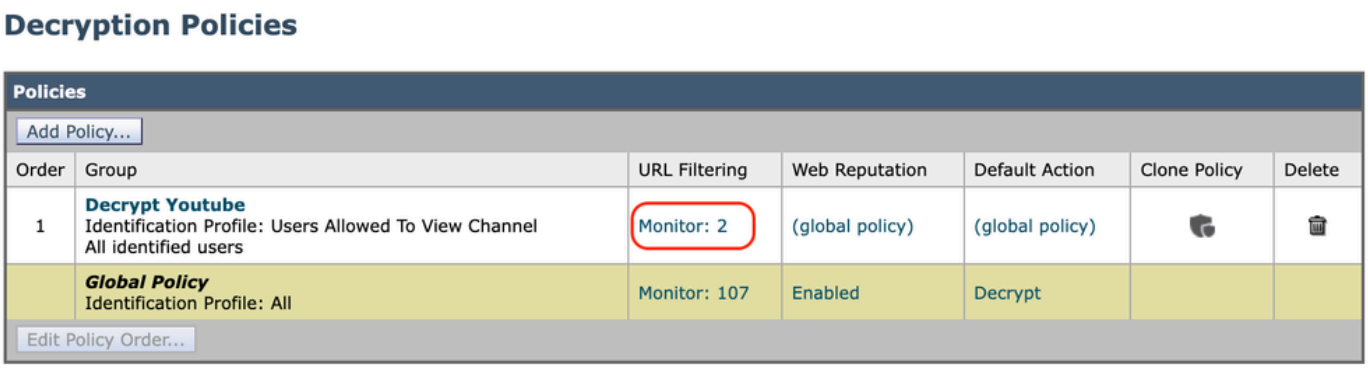



*Image- Click on URL Filtering*

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

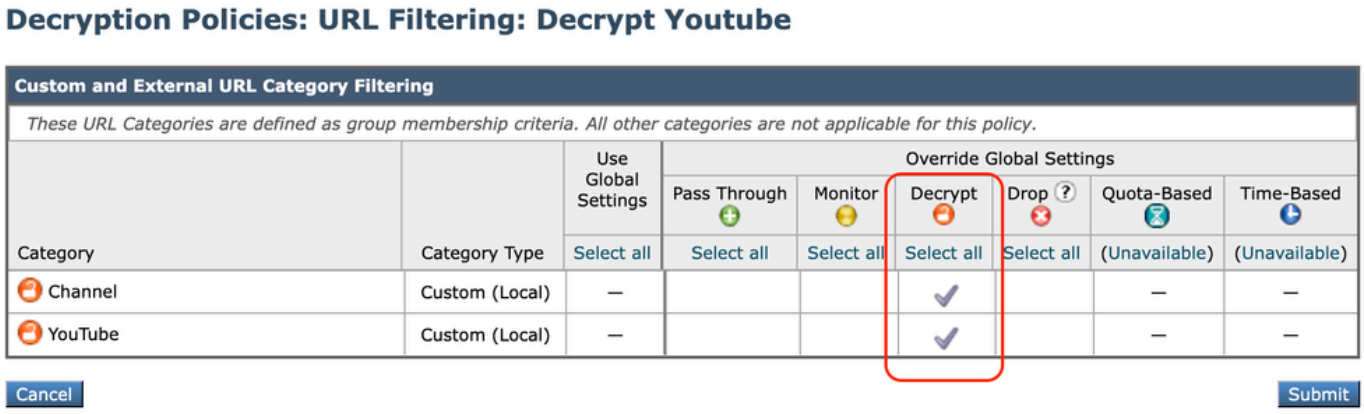



*Image- Choose Decrypt*

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 created in Step 3.

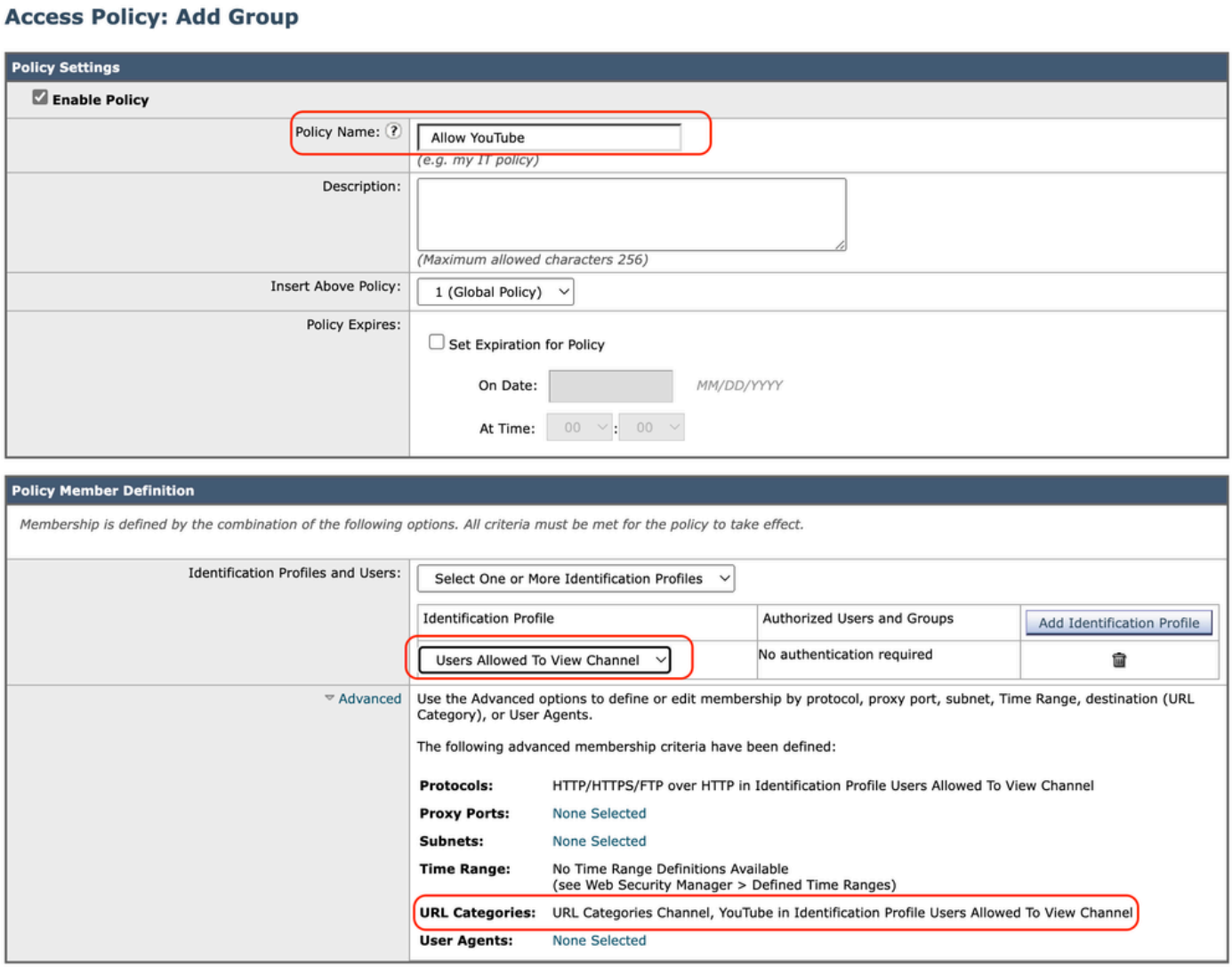



*Image- Create Access Policy*

Step 5.4. **Submit** changes.

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

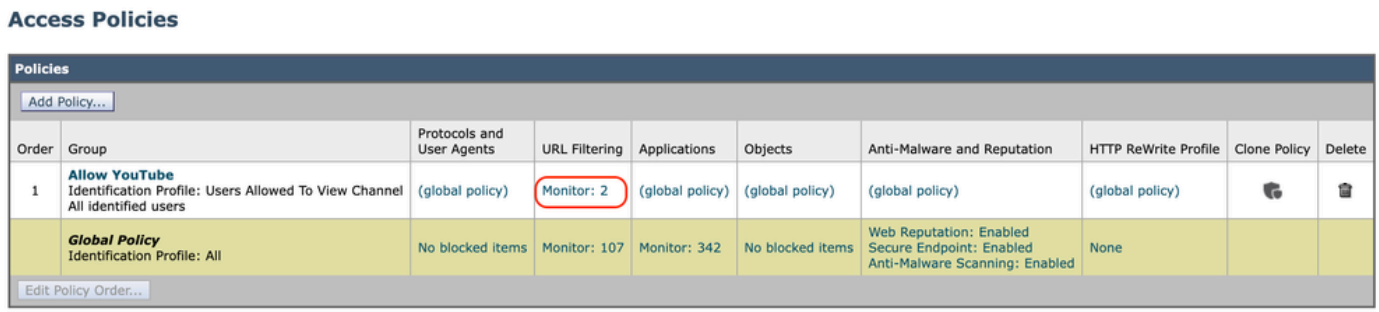



*Image- Configure Access Policy*

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

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

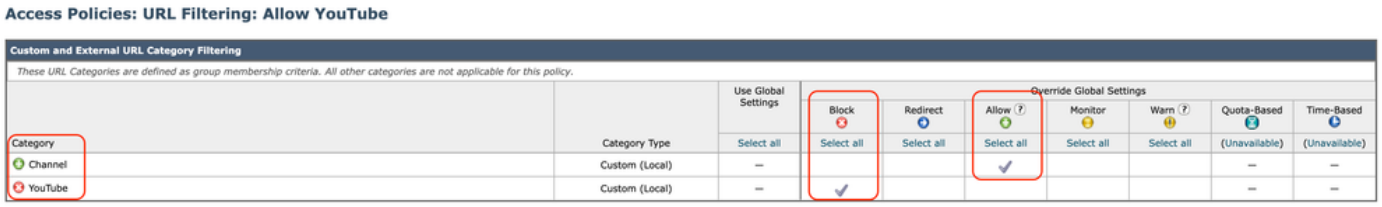



*Image- Set Category Action*

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**.




***Image- Enable Referrer***

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




*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 Content

[User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD(General Deployment) - Troubleshooting [Cisco Secure Web Appliance] - Cisco]

Cisco Technical Support & Downloads