

# Schakel specifieke YouTube Channel/Video en Blokkeer rest van YouTube in SWA

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[Gerelateerde informatie](#)

---

## Inleiding

In dit document wordt beschreven hoe u specifieke YouTube-kanalen/video's kunt toestaan en de rest van YouTube in Secure Web Appliance (SWA) kunt blokkeren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configuratiestappen

Gebruik deze stappen om een specifiek YouTube-kanaal toe te staan terwijl de toegang tot YouTube is geblokkeerd:

Stap 1. Maak Aangepaste en externe URL-categorieën voor het kanaal dat toegang moet verlenen. In dit voorbeeld wordt deze URL-categorie 'kanaal' genoemd.

Stap 1.1. Van GUI, navigeer aan de Manager van de Veiligheid van het Web en kies Aangepaste URL en Externe Categorieën.

**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

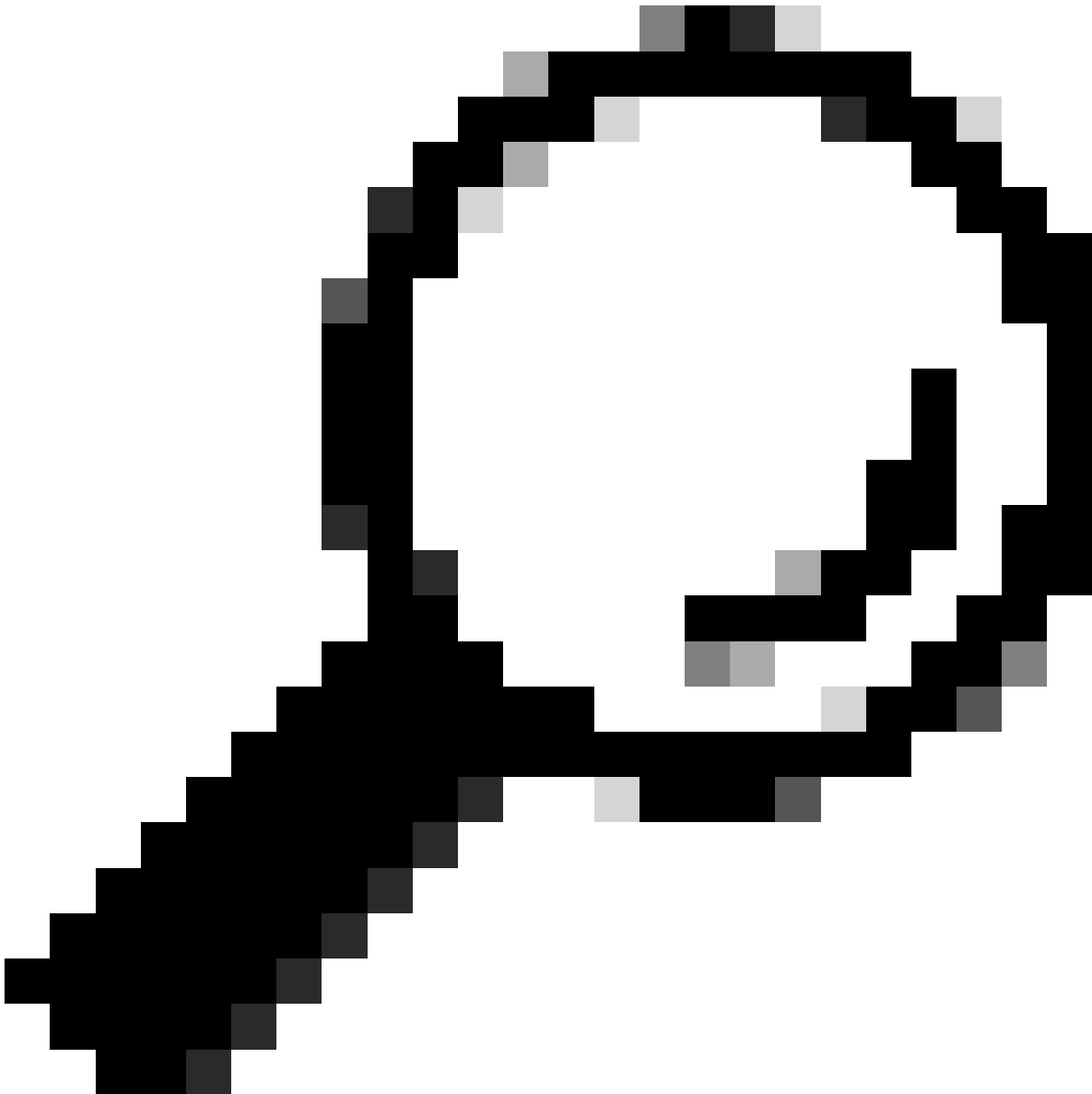
: Zorg ervoor dat de aangepaste URL-categorie 'Kanaal' een lagere prioriteit heeft dan de aangepaste URL-categorie 'YouTube'.

### 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	-	

Afbeelding - Aangepaste URL Categorie Order.png

Stap 3. Maak Identificatieprofielen voor de gebruikers die toegang hebben tot het YouTube-kanaal.



Tip: u kunt de aangepaste categorieën instellen in het beleid voor decryptie en toegang. In dit geval is het niet nodig om een afzonderlijk ID-profiel in te stellen.

Stap 3.1. Van GUI, navigeer aan de Manager van de Veiligheid van het Web en kies Identificatieprofielen.

Stap 3.2. Kies Identificatieprofiel toevoegen.

Stap 3.3. Voer de profielnaam in.

Stap 3.4. Kies de gebruiker(s) of definieer de leden via IP-subnet.

Stap 3.5. Klik op de sectie Geavanceerd en kies URL-categorieën.

### Identification Profiles: Users Allowed To View Channel

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> <b>Enable Identification Profile</b>	
Name: ?	Users Allowed To View Channel <small>(e.g. my IT Profile)</small>
Description:	Users Allowed to View Channel <small>(Maximum allowed characters 256)</small>
Insert Above:	1 (Global Profile) v

User Identification Method	
Identification and Authentication: ?	<small>For additional options, define an authentication realm (see Network &gt; Authentication) or enable ISE (see Network &gt; Identity Services Engine).</small>

Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	10.0.0.0/8 <small>(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)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> 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: <b>Proxy Ports:</b> None Selected <b>URL Categories:</b> None Selected <b>User Agents:</b> None Selected <small>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.</small>

Afbeelding - ID-profiel maken

Stap 3.6. Voeg beide URL-categorieën toe die zijn gemaakt in Stap 1 en Stap 2. en klik op Gereed.

## 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.

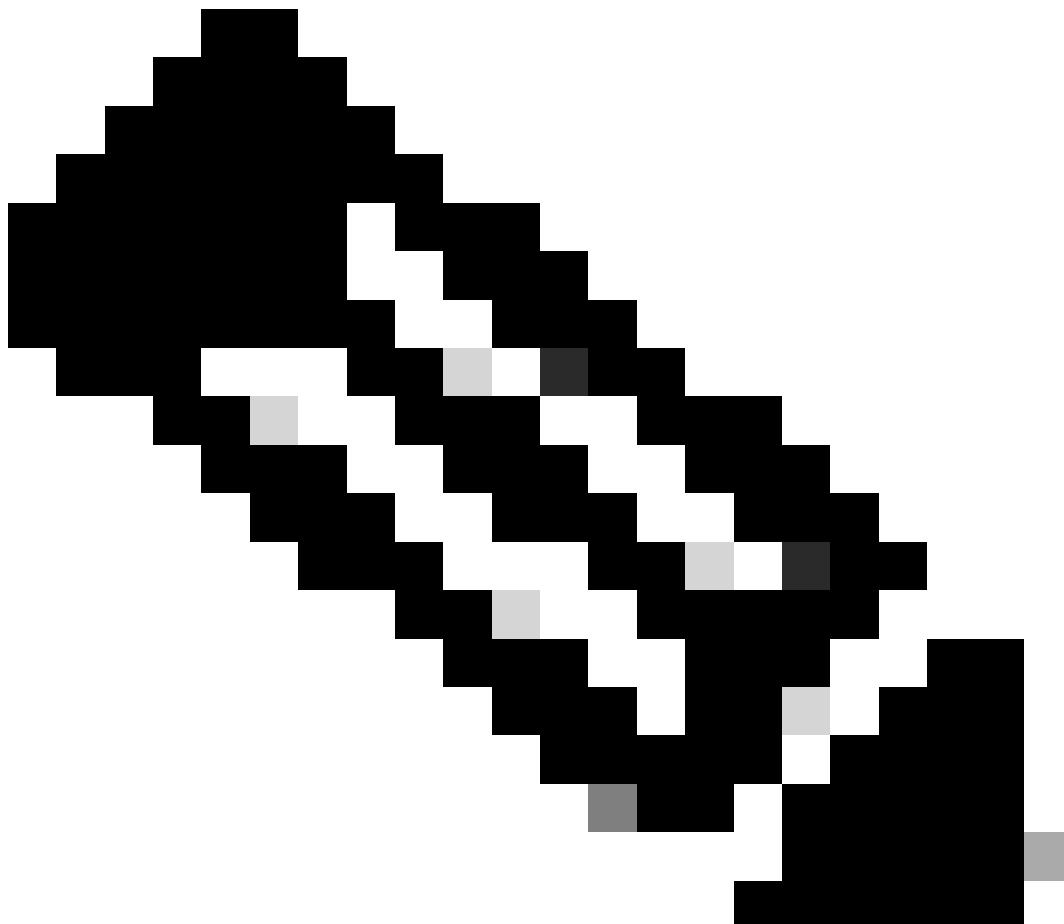
Custom and External URL Categories		
Category	Category Type	
Channel	Custom (Local)	<input type="checkbox"/>
YouTube	Custom (Local)	<input type="checkbox"/>

**Buttons:** Add, Select all

Afbeelding - URL-categorieën toevoegen

Stap 3.7. Wijzigingen verzenden.

Stap 4. Maak een decryptie beleid om het YouTube verkeer te decrypteren. In dit voorbeeld is de beleidsnaam Decrypt Youtube.



Opmerking: Als u YouTube Traffic niet decodeert, kan SWA het kanaaladres niet bepalen

in Transparent-implementatie.

Stap 4.1. Van GUI, navigeer aan de Manager van de Veiligheid van het Web en kies het Beleid van de Decryptie.

Stap 4.2. Kies Beleid toevoegen en voer de beleidsnaam in.

Stap 4.3. Kies het Identificatieprofiel dat u in Stap 3 hebt gemaakt.

### Decryption Policy: Add Group

#### Policy Settings

Enable Policy

Policy Name:  (e.g. my 11 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	<input type="button" value="Add Identification Profile"/>
<input type="text" value="Users Allowed To View Channel"/>	No authentication required	<input type="button" value=""/>

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Define additional group membership criteria.

Afbeelding - Maak een decryptie beleid

Stap 4.4. Voeg de wijzigingen toe.

Stap 4.5. Op de pagina Decryptie Beleid klikt u op Monitor in de sectie URL-filtering.

## Decryption Policies

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

Afbeelding - Klik op URL-filtering

Stap 4.6. Kies Decrypt voor zowel URL-categorieën als Indienen.

### 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"/>		—	—

Afbeelding - Kies ontsleutelen

Stap 5. Maak een toegangsbeleid om de toegang tot YouTube Channel te configureren. In dit voorbeeld is de naam van het beleid Allow YouTube.

Stap 5.1. Ga van GUI naar Web Security Manager en kies Toegangsbeleid.

Stap 5.2. Klik op Beleid toevoegen en voer de beleidsnaam in.

Stap 5.3. Kies het Identificatieprofiel dat u in Stap 3 maakt.



## Access Policy: Add Group

**Policy Settings**

**Enable Policy**

Policy Name: ?

Allow YouTube

(e.g. my IT 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	<input type="button" value="Add Identification Profile"/> 

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

Afbeelding - Toegangsbeleid maken

Stap 5.4. Wijzigingen verzenden.

Stap 5.5. Op de pagina Toegangsbeleid klikt u op Monitor in de sectie URL-filtering.

## Access Policies

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

Afbeelding - Toegangsbeleid configureren

Stap 5.6. Kies de categorie Toestaan voor kanaal.

Stap 5.7. Kies Blok voor de categorie YouTube.

## Access Policies: URL Filtering: Allow YouTube

Custom and External URL Category Filtering		Use Global Settings		Override Global Settings										
Category	Category Type	Select all	Block	Select all	Redirect	Select all	Allow ?	Select all	Monitor	Select all	Warn ?	Select all	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		--	--

Afbeelding - Categorieactie instellen

Stap 5.8. Op dezelfde pagina gaat u naar Exceptions to Blocking voor ingesloten/doorverwezen inhoud en kunt u Referrer-uitzonderingen inschakelen.

Stap 5.9. Kies Alle ingesloten/doorverwezen inhoud.

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:

Afbeelding - Referrer inschakelen

Stap 5.10. Kies vanuit Set Exception for Content Referred by These Categories de **YouTube** aangepaste URL categorie.

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).

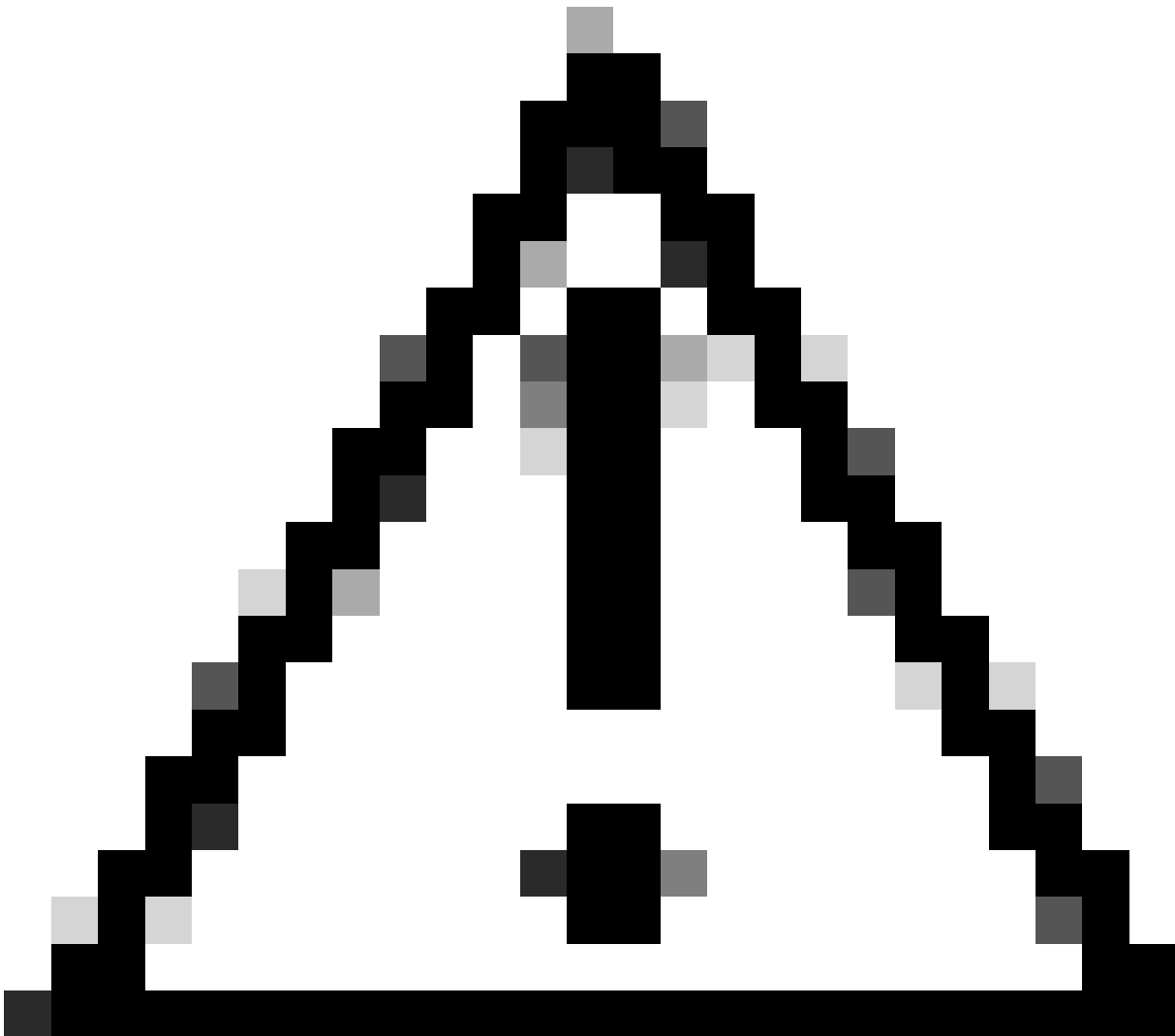
Enable Referrer Exceptions

Set Exception for Content Referred by These Categories:

Set Exception for This Referred Content:

Afbeelding - Ingesloten inhoud configureren

Stap 5.11. Wijzigingen **verzenden** en **vastleggen**



**Let op:** als gebruikers het kanaal voor het eerst gebruiken, kunnen ze naar alle YouTube video's navigeren.

---

#### Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - GD \(Algemene implementatie\) - Problemen oplossen \[Cisco Secure Web Applicatie\] - Cisco](#)
- [Cisco Technical Support en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.