

# Consenti a Google reCAPTCHA quando l'accesso ai portali del motore di ricerca è bloccato

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura di configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

---

## Introduzione

In questo documento viene descritto come consentire a Google reCAPTCHA in Secure Web Appliance (SWA) di bloccare l'accesso ai portali del motore di ricerca.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Web Access e decrittografia HTTPS.

Cisco consiglia inoltre di:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Installazione guidata completata.
- Accesso amministrativo all'interfaccia grafica (GUI) SWA.

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

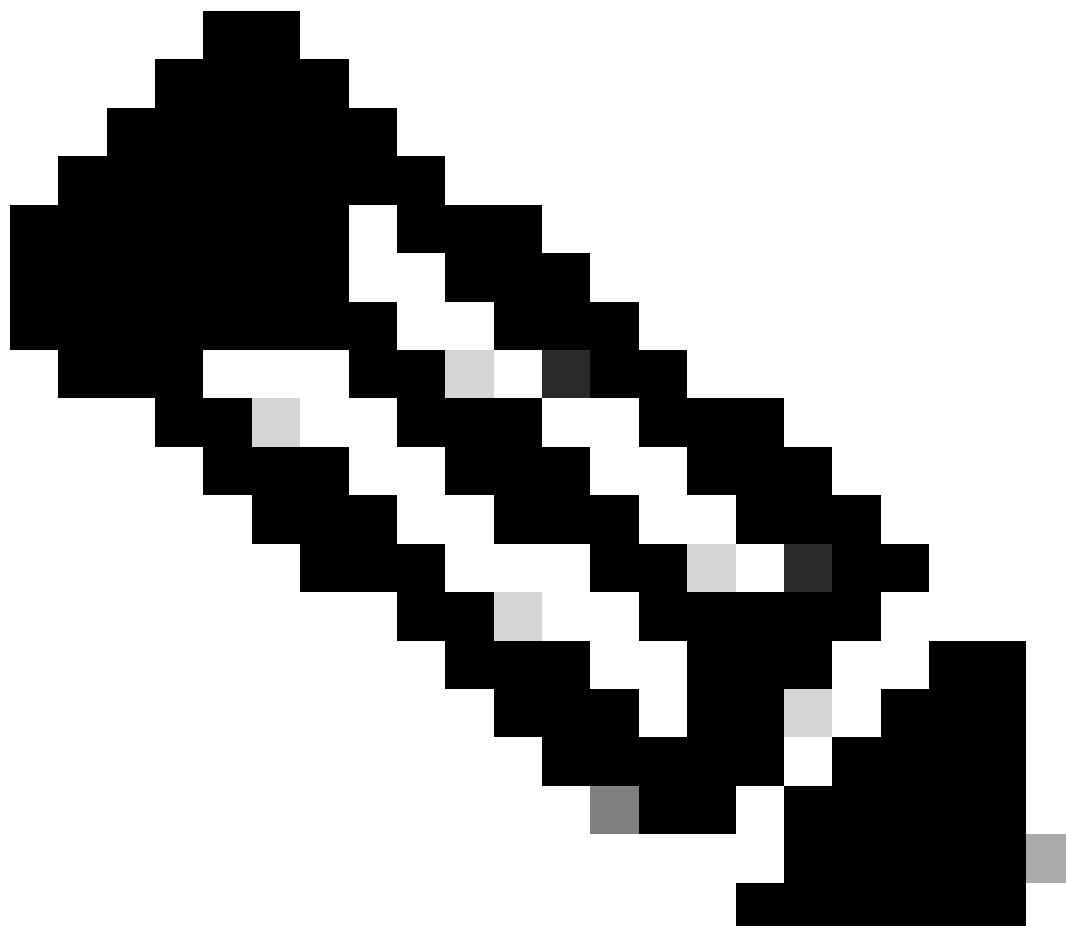
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

## Procedura di configurazione

Passaggio 1. Dalla GUI, passare alla Security Services schermata e scegliere HTTPS Proxy, abilita decrittografia HTTPS se non è già abilitata.

---



**Nota:** per questa configurazione è necessario abilitare la decrittografia HTTPS. In caso contrario, fare riferimento all'articolo di riferimento alla fine di questo documento.

---

Passaggio 2. Dalla GUI, selezionare **Web Security Manager** e scegliere **Custom and External URL Categories**, quindi creare due categorie di URL personalizzate, una per google.com e l'altra per Google reCAPTCHA. Fare clic su **Invia**.

### Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Google"/>
Comments: (?)	<input type="text" value="Custom URL Category for Google"/>
List Order:	<input type="text" value="4"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text" value="google.com, .google.com"/> <div style="float: right; text-align: right;"> <a href="#">Sort URLs</a>  <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small> </div> <p><small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small></p>
Advanced	Regular Expressions: (?) <input type="text"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Cancel](#)

[Submit](#)

Crea categoria URL personalizzata per Google

### Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Captchaallow"/>
Comments: (?)	<input type="text" value="Custom URL Category for Google RECAPTCHA"/>
List Order:	<input type="text" value="5"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text"/> <div style="float: right; text-align: right;"> <a href="#">Sort URLs</a>  <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small> </div> <p><small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small></p>
Advanced	Regular Expressions: (?) <input type="text" value="www\.google\.com/recaptcha/"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Cancel](#)

[Submit](#)

Crea categoria URL personalizzata per Google

**Passaggio 3.** Dalla GUI, passare a **Web Security Manager** e scegliere **Criteri di decrittografia**, quindi creare i criteri di decrittografia per decrittografare google.com. Fare clic su **None Selected** (Nessuno) accanto a **URL Categories** (Categorie URL), quindi selezionare **Google**

custom URL category (Categoria URL personalizzata Google). Fare clic su **Invia**.

## Decryption Policy: Add Group

**Policy Settings**

**Enable Policy**

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

Description:  (Maximum allowed characters 256)

Insert Above Policy: 1 (dropciscospecific) ▾

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: All Identification Profiles ▾

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. 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

**User Agents:** None Selected

Cancel
Submit

Criteria di decrittografia per decrittografare Google

**Passaggio 3.1.** Passare a **Criteri di decrittografia** e fare clic su **Monitor** in linea con il criterio **GoogleDecrypt**.

**Passaggio 3.2.** Selezionare **Decrypt** in linea to **Google Category** e fare clic su **Submit (Invia)**.

## Decryption Policies: URL Filtering: GoogleDecrypt

**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	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Google	Custom (Local)	—			✓		—	—

Cancel
Submit

Selezionare la categoria URL personalizzato creato per Google per decrittografarlo nei criteri di decrittografia

**Passaggio 4.** Dalla GUI, selezionare **Web Security Manager**, quindi **Access Policies**, creare i criteri di accesso per consentire a Google reCAPTCHA e selezionare **captchaallow** come **categorie URL**.

## Access 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:

*If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.*

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:** 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:** [Captchaallow](#)

**User Agents:** None Selected

Criteri di accesso per consentire a Google RECAPTCHA

**Passaggio 4.1.** Passare a **Criteri di accesso** e fare clic su **Monitoraggio** in linea con il criterio **GoogleCaptchaAccessPolicy**. Selezionare **Allow** in line to **Captchaallow** Category (Consenti in linea alla categoria Captchaallow). **Invia e conferma modifiche.**

### Access Policies: URL Filtering: GoogleCaptchaAccessPolicy

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	Block	Redirect	Allow (?)	Over
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Captchaallow	Custom (Local)	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Selezionare la categoria URL personalizzato creato per Google RECAPTCHA per consentirlo nei criteri di accesso

**Passaggio 5.** Verificare che i motori di ricerca e i portali in **Filtro categoria URL predefinito** siano bloccati nei criteri di accesso globale:

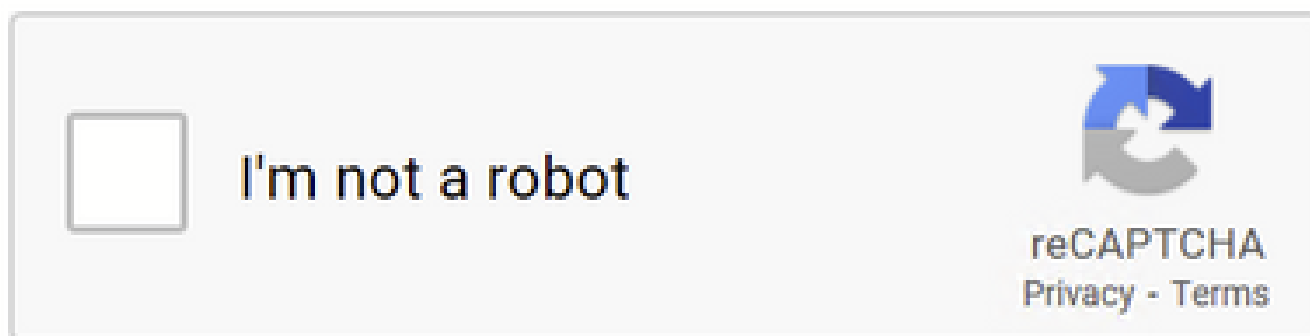
## Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering	
No Custom Categories are included for this Policy.	
<input type="button" value="Select Custom Categories..."/>	
Predefined URL Category Filtering	
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.	
Category	<input type="checkbox"/> Block <input type="checkbox"/> Select all
<input checked="" type="radio"/> Regional Restricted Sites (Poland)	
<input checked="" type="radio"/> Religion	
<input checked="" type="radio"/> SaaS and B2B	
<input checked="" type="radio"/> Safe for Kids	
<input checked="" type="radio"/> Science and Technology	
<input checked="" type="radio"/> Search Engines and Portals	<input checked="" type="checkbox"/>
<input checked="" type="radio"/> Sex Education	

Criterion predefinito per bloccare l'accesso ai motori di ricerca

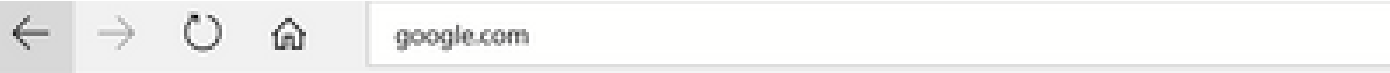
### Verifica

È possibile vedere l'accesso a Google reCAPTCHA funziona, ma l'accesso al motore di ricerca (Google) è ancora negato, dopo aver abilitato la decrittografia HTTPS e consentito l'accesso a Google reCAPTCHA nei criteri di accesso:



Google CAPTCHA Works

1675880489.667 279 10.106.40.203 TCP\_MISS\_SSL/200 23910 GET <https://www.google.com:443/recaptcha/api2/anchor?ar=1&k=6LdN4qUZAAAAA>



## This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site ( <http://google.com/> ) has been blocked because the web category "Search Engines and Portals" is not allowed.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Wed, 08 Feb 2023 18:23:01 GMT

Username:

Source IP: 10.106.40.203

URL: GET <http://google.com/>

Category: Search Engines and Portals

Reason: BLOCK-WEBCAT

Notification: WEBCAT

*Sito Google bloccato*

1675880581.157 0 10.106.40.203 TCP\_DENIED/403 0 GET "<https://google.com/favicon.ico>" - NONE/- - BLOCK\_WEBCAT\_12-DefaultGroup-DefaultC

### Risoluzione dei problemi

Se l'accesso a Google reCAPTCHA è bloccato, è possibile controllare i log degli accessi nella CLI SWA. Se vedi Google URL e non l'URL di Google reCAPTCHA, è possibile che la decrittografia non sia abilitata:

1675757652.291 2 192.168.100.79 TCP\_DENIED/403 0 CONNECT tunnel://[www.google.com:443/](http://www.google.com:443/) - NONE/- - BLOCK\_WEBCAT\_12-DefaultGroup-F

### Riferimenti

- [Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD \(General Deployment\) - Connessione, installazione e configurazione \[Cisco Secure Web Appliance\] - Cisco](#)
- [Utilizzo certificato WSA per decrittografia HTTPS](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).