

# Google reCAPTCHA zulassen, wenn der Zugriff auf Suchmaschinenportale gesperrt ist

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Referenzen](#)

---

## Einleitung

In diesem Dokument werden die Schritte beschrieben, um Google reCAPTCHA in Secure Web Appliance (SWA) zuzulassen, wenn Sie den Zugriff auf Suchmaschinenportale blockiert haben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Web Access und HTTPS-Entschlüsselung

Cisco empfiehlt außerdem Folgendes:

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.
- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA

### Verwendete Komponenten

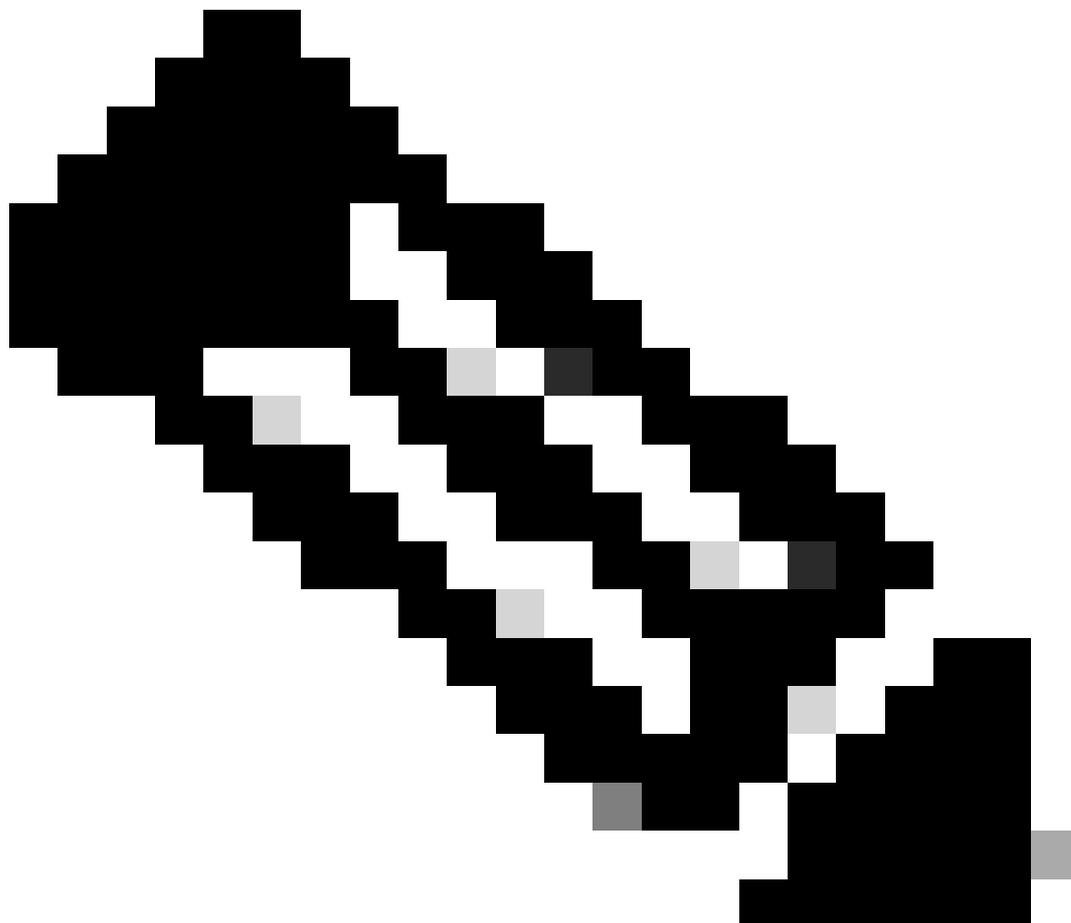
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

# Konfigurationsschritte

**Schritt 1:** Navigieren Sie in der GUI zu, Security Services HTTPS Proxy, und wählen Sie HTTPS-Entschlüsselung aktivieren aus, wenn diese nicht bereits aktiviert ist.

---



**Hinweis:** Für diese Konfiguration muss die HTTPS-Entschlüsselung aktiviert sein. Ist diese Funktion nicht aktiviert, lesen Sie den entsprechenden Artikel am Ende dieses Dokuments.

---

**Schritt 2:** Navigieren Sie von der GUI zum **Web Security Manager**, und wählen Sie **Benutzerdefinierte und externe URL-Kategorien**, erstellen Sie zwei benutzerdefinierte URL-Kategorien, eine für google.com und die andere für Google reCAPTCHA. Klicken Sie auf **Senden**.

### 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](#)

Benutzerdefinierte URL-Kategorie für Google erstellen

### 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](#)

Benutzerdefinierte URL-Kategorie für Google erstellen

**Schritt 3:** Navigieren Sie in der GUI zum **Websicherheits-Manager**, und wählen Sie **Entschlüsselungsrichtlinien aus**, erstellen Sie eine Entschlüsselungsrichtlinie, um google.com zu entschlüsseln. Klicken Sie neben den **URL-Kategorien auf Keine ausgewählt**, und wählen Sie

die benutzerdefinierte **Google-URL-Kategorie** aus. Klicken Sie auf **Senden**.

## Decryption Policy: Add Group

**Policy Settings**

**Enable Policy**

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

Description:   
(Maximum allowed characters 256)

Insert Above Policy: 1 (dropiscospecific) ▾

Policy Expires:  Set Expiration for Policy

On Date:

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

Entschlüsselungsrichtlinie zum Entschlüsseln von Google

**Schritt 3.1:** Navigieren Sie zu **Entschlüsselungsrichtlinien**, und klicken Sie in der Zeile der **GoogleDecrypt**-Richtlinie auf **Überwachen**.

**Schritt 3.2:** Wählen Sie **Entschlüsseln** in Zeile zu **Google-Kategorie** und klicken Sie auf **Senden**.

## 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

Wählen Sie die erstellte benutzerdefinierte **URL-Kategorie für Google** aus, um sie in der **Entschlüsselungsrichtlinie** zu entschlüsseln.

**Schritt 4:** Navigieren Sie von der GUI zum **Web Security Manager**, und wählen Sie **Zugriffsrichtlinien** aus, erstellen Sie eine Zugriffsrichtlinie, um Google reCAPTCHA zuzulassen, und wählen Sie **captchallow** als **URL-Kategorien** aus.

## 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

Zugriffsrichtlinie für Google RECAPTCHA

**Schritt 4.1:** Navigieren Sie zu **Zugriffsrichtlinien**, und klicken Sie in der Zeile der **GoogleCaptchaAccessPolicy**-Richtlinie auf **Überwachen**. Wählen Sie **Zulassen** in Zeile zu **Captchaallow** Category. **Senden** und **bestätigen Sie Änderungen**.

### 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	Ove		
			Block	Redirect	Allow
Captchaallow	Custom (Local)	—	Select all	Select all	Select all

Wählen Sie die erstellte benutzerdefinierte URL-Kategorie für Google RECAPTCHA aus, um sie in der Zugriffsrichtlinie zuzulassen.

**Schritt 5:** Stellen Sie sicher, dass **Suchmaschinen und Portale** in der **vordefinierten URL-Kategoriefilterung** in der globalen Zugriffsrichtlinie blockiert sind:

## 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	

Standardrichtlinie zur Blockierung des Zugriffs auf Suchmaschinen

## Überprüfung

Sie können sehen, dass der Zugriff auf Google reCAPTCHA funktioniert, aber der Zugriff auf die Suchmaschine (Google) wird weiterhin verweigert, nachdem Sie die HTTPS-Entschlüsselung aktiviert und den Zugriff auf Google reCAPTCHA in der Zugriffsrichtlinie zugelassen haben:



Google CAPTCHA funktioniert

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

*Google-Website wird blockiert*

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

### Fehlerbehebung

Wenn der Zugriff auf das Google reCAPTCHA gesperrt ist, können Sie die Zugriffsprotokolle in der SWA-CLI überprüfen. Wenn Sie die Google-URL und nicht die Google reCAPTCHA-URL sehen, kann es sein, dass die Entschlüsselung nicht aktiviert ist:

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

### Referenzen

- [Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD \(Allgemeine Bereitstellung\) - Verbinden, Installieren und Konfigurieren \[Cisco Secure Web Appliance\] - Cisco](#)
- [WSA-Zertifikatverwendung für HTTPS-Entschlüsselung](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.