

# 對Umbrella自定義阻止頁面繞過或使用代碼進行故障排除

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [排解自訂封鎖頁面問題](#)

#### [常見方案](#)

[在「Web策略阻止」頁中未啟用HTTPS檢查](#)

[自定義阻止頁面未連結到正確的策略](#)

[診斷資訊中的組織ID =0，來源ID=30829397](#)

### [旁路代碼或使用者故障排除](#)

#### [常見方案](#)

[錯誤消息："找不到您輸入的旁路代碼"](#)

[「阻止」頁不顯示某些目標的管理旁路部分](#)

[錯誤消息："您輸入的登入憑據無效"](#)

[錯誤消息："您輸入的旁路代碼已過期"](#)

[使用旁路代碼/使用者時頁面載入不正確](#)

[阻止頁面繞過警告](#)

---

## 簡介

本文說明如何解決自定義阻止頁面上繞行或使用代碼的Cisco Umbrella問題。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 排解自訂封鎖頁面問題

自定義阻止頁面無法工作的原因有很多，文中介紹了一些常見的原因。

## 常見方案

在「Web策略阻止」頁中未啟用HTTPS檢查

要確保Web策略塊的功能，必須在規則集中啟用HTTPS檢查。

自定義阻止頁面未連結到正確的策略

建立[自定義阻止頁面後](#)，請確保該頁面連結到正確的策略：

1.擴展策略。

2.在Umbrella Default Block Page Applied下，選擇Edit。

The screenshot shows the configuration page for a policy named 'Default Policy'. The page is organized into several sections, each with a shield icon and a title. The sections are:

- Applied to All Identities**: A section with a shield icon and the text 'Applied to All Identities'.
- Security Setting Applied: Default Settings**: A section with a shield icon and the text 'Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked. No integration is enabled.' Below this are links for 'Edit' and 'Disable'.
- Content Setting Applied: Default Settings**: A section with a shield icon and the text 'Alcohol, Games, Advertisements, plus 3 more will be blocked.' Below this are links for 'Edit' and 'Disable'.
- Application Setting Applied: Default Settings**: A section with a shield icon and the text 'Nielsen, Acquia Cloud, AppNexus, plus 788 more will be blocked.' Below this are links for 'Edit' and 'Disable'.
- 2 Destination Lists Enforced**: A section with a shield icon and the text '1 Block List, 1 Allow List'. Below this is a link for 'Edit'.
- File Analysis Not Enabled**: A section with a shield icon and the text 'Requires Intelligent Proxy, File Inspection Not Enabled'.
- Umbrella Default Block Page Applied**: A section with a shield icon and the text 'Umbrella Default Block Page Applied'. Below this are links for 'Edit' and 'Preview Block Page'. This section is highlighted with a red rectangular box.

At the top of the page, there is a header with the following information:

Default Policy	Protection	Applied To	Contains	Last Modified
	DNS Policy	All Identities	4 Policy Settings	Aug 27, 2023

21385636885652

3.選擇使用自定義外觀，然後從下拉選單中選擇自定義塊頁：

2

Default Policy	Protection DNS Policy	Applied To All Identities	Contains 4 Policy Settings	Last Modified Aug 27, 2023	^
----------------	--------------------------	------------------------------	-------------------------------	-------------------------------	---

### Set Block Page Settings

Define the appearance and bypass options for your block pages.

Use Umbrella's Default Appearance  
[Preview Block Page »](#)

Use a Custom Appearance

**Choose an existing appearance** ▾

- Default Settings
- ▶ Byp  
▶ Byp  
test block

[CREATE NEW APPEARANCE](#)

[CANCEL](#) [SET & RETURN](#)

21385636888340

診斷資訊中的組織ID =0 , 來源ID=30829397



This site is blocked due to content filtering.

~~expense.certify.com~~

Sorry, expense.certify.com has been blocked by your network administrator.

[> Report an incorrect block](#)

▼ Diagnostic Info

ACType:	2
Block Type:	aup
Bundle ID:	-
Domain Tagging:	-
Host:	block.opendns.com
IP Address:	<input type="text"/>
Org ID:	0
Origin ID:	30829397
Prefs:	-
Query:	<input type="text"/>
Server:	<input type="text"/>
Time:	<input type="text"/>

21386106915476

此問題通常是由於Umbrella阻止頁面IP「146.112.0.0/16」的上游阻止或在瀏覽器設定上啟用DoH所導致的。如果您使用的是Meraki MX並且已啟用內容過濾，則可以考慮在Meraki控制面板中禁用內容過濾，並合併Umbrella塊頁面IP「146.112.0.0/16」，「155.190.0.0/16」、「umbrella.com」和「opendns.com」新增到您的允許/排除清單中，與以下螢幕截圖類似：

## Content Filtering

Content filtering set here becomes a default. Deliberately allowing content access or matching [Active Directory](#) group policy supersedes the default.

### Check content and threat categories

Find out what content and threat categories that a URL has.

Type in the URL

### Category blocking

Block URLs by website and threat category. See the [full category list](#).

Block

Content categories

Threat categories

### URL filtering

Enter specific URLs to block or allow. You can use **Category blocking** to block a large number of sites by category rather than entering a list of specific URLs here. [Learn more](#)

Block

Blocked URL list

Targets specific URLs to block

Allow

Allowed URL list

Targets specific URLs to allow

21417585172628

## 旁路代碼或使用者故障排除

旁路代碼或使用者工作不正常，或您收到不同的錯誤消息的原因有很多，

### 常見方案

錯誤消息："找不到您輸入的旁路代碼"

與阻止頁面外觀相似，必須確保建立的旁路代碼/使用者與相應的策略正確關聯。如果旁路代碼或使用者連線到其他策略，嘗試使用旁路代碼或使用者可能導致此錯誤消息。閱讀Umbrella文檔中的詳細資訊：

- [建立塊頁旁路代碼](#)
- [在策略中啟用阻止頁面繞行](#)

## 「阻止」頁不顯示某些目標的管理旁路部分

如果阻止頁面未顯示特定目標的「管理繞行」部分，則應用阻止設定可以阻止該頁面。「繞過代碼/使用者」僅適用於「內容類別」和「阻止目標清單」塊型別。要解決此問題，請考慮刪除該應用程式並將域/內容類別新增到此策略中。

錯誤消息："您輸入的登入憑據無效"

如果啟用了儀表板SSO，則以旁路使用者身份登入時，預計會出現收到此錯誤的行為。阻止頁面繞過(BPB)使用者不再繞過阻止頁面或以任何容量向Umbrella進行身份驗證。BPB使用者與Umbrella中的任何其他使用者一樣，也是使用者，但是由於SSO處理身份驗證的方式，它不能用於繞過阻止頁面。您必須改用BPB代碼。

錯誤消息："您輸入的旁路代碼已過期"

您遇到此錯誤訊息的原因如下：

- 如果繞過代碼的過期日期已過，則繞過代碼已過期。
- 如果將旁路代碼到期日期設定為2038年1月19日星期二03:14:07 UTC以後的日期，則會發生此錯誤。

## 使用旁路代碼/使用者時頁面載入不正確

當使用者訪問被阻止的域並輸入代碼以取消阻止該域時，將在具有該域的使用者裝置上建立cookie。

例如，如果使用者繞過YouTube，則會為「youtube.com」建立一個cookie，並且僅為此域建立cookie。在本例中，YouTube服務請求來自不同域(如「youtube-nocookie.com」、「ytimg.l.google.com」和「googlesyndication.com」)的資訊，此使用者策略不允許使用這些資訊。這會導致YouTube無法正確載入。

解決方案：如果仍希望使用旁路代碼/使用者，則可以新增頁面所依賴的所有域，以將此資訊檢索到允許清單。您可以在本文中找到最常用的服務：[Block Page Bypass:要允許的域](#)

## 阻止頁面繞過警告

- 如果被阻止的內容是嵌入在頁面中的內容(如影象、樣式表、指令碼)，則使用者無法看到BPB頁面以輸入代碼(即使Umbrella嘗試顯示代碼)。
- BPB代碼可以配置為僅取消阻止某些類別或目標。這可能會導致問題，即頁面的部分內容被解除阻止，而嵌入的內容未被阻止。如有疑問，請嘗試使用「bypass everything」代碼測試。
- BPB受到網站上的內容安全策略的嚴重影響，這些策略可以阻止Umbrella的cookie，因此會阻止BPB處理嵌入內容。您需要將其中一些嵌入域列入白名單才能使其正常工作。請參閱「阻止頁面繞行：要允許的域。」
- BPB旁路事件當前未記錄在Umbrella報告中。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。