

在SWA中配置Microsoft O365租戶限制

目錄

簡介
必要條件
需求
採用元件
設定步驟
報告和日誌
記錄檔
報告
相關資訊

簡介

本文描述在安全Web裝置(SWA)中配置配置Microsoft O365租戶限制的過程。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

設定步驟

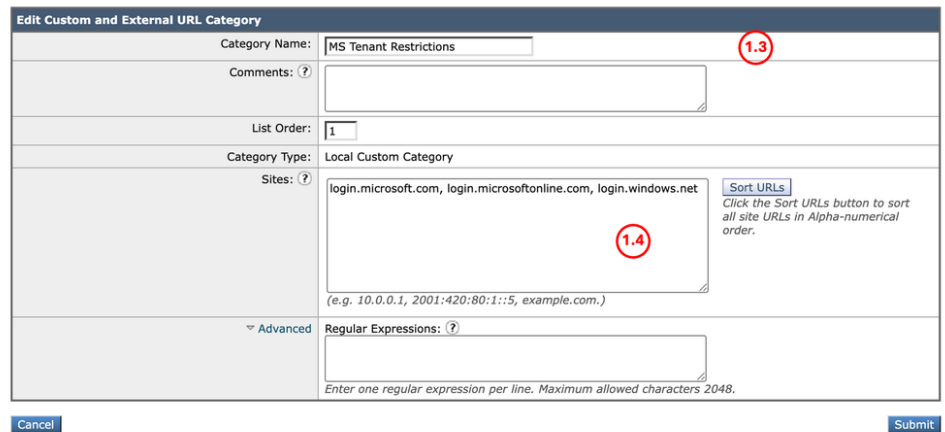
步驟1.為網站建立自定義URL類別。	步驟1.1.從GUI導覽至Web Security Manager並選擇Custom and External URL Categories。 步驟1.2.單擊Add Category以建立新的自定義URL類別。 步驟1.3.輸入Name作為新類別。
--------------------	---

步驟1.4.在「站點」部分中定義以下URL：

login.microsoft.com, login.microsoftonline.com, login.windows.net

步驟1.5.提交變更。

Custom and External URL Categories: Edit Category



影象 — 自定義URL類別



提示：有關如何配置自定義URL類別的詳細資訊，請訪問：
<https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

步驟2.解密流量。

步驟2.1.在GUI中，導覽至Web Security Manager，然後選擇Decryption Policies

步驟2.2.單擊Add Policy。

步驟2.3.輸入新策略的名稱。

步驟2.4.選擇需要應用此策略的Identification Profile。



提示：如果您繞過Microsoft URL的身份驗證，並且正在為所有使用者配置此策略，請選擇：All Identification Profiles > All Users

步驟2.5.在策略成員定義部分，按一下URL類別連結以新增自定義URL類別。

步驟2.6.選擇在步驟1中建立的URL類別。

步驟2.7.按一下Submit。

Decryption Policy: DP MS Tenant Restrictions

Policy Settings

☒ Enable Policy

Policy Name: ?

DP MS Tenant Restrictions

Description:

Insert Above Policy:

1 (Global Policy)

Policy Expires:

☐ Set Expiration for Policy

On Date:

MM/DD/YYYY

At Time:

00

:

00

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

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:

MS Tenant Restrictions

User Agents:

None Selected

Cancel

Submit

影象 — 配置解密策略

步驟2.8.在Decryption Policies頁面中，點選新策略的URL Filtering中的連結。

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP MS Tenant Restrictions Identification Profile: All URL Categories: MS Tenant Restrictions	Decrypt: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 105 Drop: 2	Disabled	Decrypt		
Edit Policy Order...						

影象 — 編輯URL過濾操作

步驟2.9.選擇Decrypt作為Custom URL Category的操作。

步驟2.10.單擊提交。

Decryption Policies: URL Filtering: DP MS Tenant Restrictions

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
		Select all	Select all	Select all	Select all	Select all	(Unavailable)
MS Tenant Restrictions	Custom (Local)	—			☒		—

Cancel

Submit

影象 — 解密自定義URL類別

步驟3.創建HTTP重寫配置檔案。

- 步驟3.1.在GUI中，導覽至Web Security Manager，然後選擇HTTP ReWrite Profiles。
- 步驟3.2.按一下「Add Profile」。
- 步驟3.3.輸入新配置檔案的名稱。
- 步驟3.4.將Restrict-Access-To-Tenants用於第一個標頭名稱。
- 步驟3.5.對於Restrict-Access-To-Tenants設定，使用<permitted tenant list>的值，該值必須是允許使用者訪問的租戶的逗號分隔清單。
- 步驟3.6.單擊Add Row
- 步驟3.7.使用Restrict-Access-Context作為第二個標頭名稱。
- 步驟3.8.對於Restrict-Access-Context設定，使用單個目錄ID的值指定定義租戶限制的租戶。
- 步驟3.9.按一下Submit。

HTTP ReWrite: Edit Profile

Profile Settings

Profile Name: ? Header Rewrite MS Tenant Restrictions

Header Name	Header Value	Text Format	Binary Encoding
☐ Restrict-Access-To-Tenants	9.onmicrosoft.com	ASCII	No Encoding
☐ Restrict-Access-Context	2-9505-4097-a69a-c1553ef	ASCII	No Encoding

Note:
HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups

\$ReqMeta can be used to fetch standard HTTP header variables
Example: If the value of Header is entered as Username-{\$ReqMeta[X-Authenticated-User]} and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith

\$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.
Example:
Header1: Value1;
Header2: Value0-{\$ReqHeader[Header1]}-Value2-{\$ReqMeta[X-Authenticated-User]}
If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith
If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.

Cancel Submit

影象 — 新增HTTP重寫配置檔案

 提示：有關租戶限制以及如何收集租戶資訊的更多資訊，請訪問：[Microsoft學習 — 限制對租戶的訪問。](#)

步驟4.建立存取原則。

- 步驟4.1.在GUI中，導覽至Web Security Manager，然後選擇Access Policies
- 步驟4.2.單擊Add Policy。
- 步驟4.3.輸入新策略的名稱。
- 步驟4.4.選擇需要應用此策略的Identification Profile。

 提示：如果您繞過Microsoft URL的身份驗證，並且正在為所有使用者配置此策略，請選擇：所有標識配置檔案 > 所有使用者。

步驟4.5.在Policy Member Definition部分中，按一下URL Categories連結以新增自定義URL類別。

步驟4.6.選擇在步驟1中建立的URL類別。

步驟4.7.按一下Submit。

Access Policy: AP MS Tenant Restrictions

Policy Settings

☒ Enable Policy

Policy Name: ?

AP MS Tenant Restrictions
(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:

00:00

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.

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:

MS Tenant Restrictions

User Agents:

None Selected

映像 — 建立訪問策略

步驟4.8.在Access Policies頁中，確保URL Filtering的操作設定為Monitor。

步驟4.9.單擊HTTP ReWrite Profile中的連結，將HTTP Header Profile新增到此策略中。

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP MS Tenant Restrictions Identification Profile: All URL Categories: MS Tenant Restrictions	(global policy)	Monitor: 1	Monitor: 3145	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 3145	Block: 31 Object Types	Web Reputation: Enabled Secure Endpoint: Enabled Webroot: Disabled	None		
Edit Policy Order...									

影像 — 訪問策略屬性

步驟4.10.選擇在步驟[3]中建立的HTTP ReWrite Profiles。

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles:

✓ Use Global Settings

None

Header Rewrite MS Tenant Restrictions

Cancel

Submit

4.10

影象 — 新增HTTP重寫配置檔案

步驟4.11。單擊提交。

步驟4.12.提交更改。

報告和日誌

記錄檔

您可以在訪問日誌或W3C日誌中新增自定義欄位，以檢視HTTP報頭重寫配置檔名稱。

訪問日誌中的格式說明符	W3C日誌中的日誌欄位	說明
%]	x-http-rewrite-profile-name	HTTP標頭重寫配置檔名稱。

報告

可以生成Web跟蹤報告，以便按AccessPolicy名稱檢視流量報告。

使用以下步驟生成報告：

步驟1.在GUI中選擇Reporting，然後選擇Web Tracking。

步驟2.選擇所需的時間範圍。

步驟3.單擊Advanced連結以使用高級條件搜尋事務。

步驟4.在Policy部分，選擇Filter by Policy，並鍵入先前建立的Access Policy的名稱。

步驟5.按一下Search以檢視報告。

Web Tracking

Search

Proxy Services **L4 Traffic Monitor** **SOCKS Proxy**

Available: 06 Nov 2024 13:47 to 17 Jun 2025 20:48 (GMT +02:00)

Time Range:

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type:

☒ **Advanced** *Search transactions using advanced criteria.*

URL Category: ☒ Disable Filter
☐ Filter by URL Category:

Application: ☒ Disable Filter
☐ Filter by Application: (ex. Twitter)
☐ Filter by Application Type: (ex. Social Networking)

Policy: ☐ Disable Filter
☒ Filter by Policy:

影象 — Web跟蹤報告

相關資訊

- [Cisco Secure Web Appliance AsyncOS 15.2使用手冊](#)
- [思科安全電子郵件和網路虛擬裝置安裝指南](#)
- [在Secure Web Appliance中配置自定義URL類別 — Cisco](#)
- [使用安全Web裝置最佳做法](#)
- [為安全Web裝置配置防火牆](#)
- [在安全Web裝置中配置解密證書](#)
- [在SWA中配置SNMP並對其進行故障排除](#)
- [使用Microsoft Server在安全Web裝置中配置SCP推送日誌](#)
- [在SWA中啟用特定的YouTube頻道/影片並阻止YouTube的其餘部分](#)
- [瞭解Secure Web Appliance中的HTTPS訪問日誌格式](#)
- [訪問安全Web裝置日誌](#)
- [繞過安全Web裝置中的身份驗證](#)
- [阻止安全Web裝置中的流量](#)
- [繞過安全Web裝置中的Microsoft更新流量](#)

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）。