

# Configura restrizione tenant Microsoft O365 in SWA

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura di configurazione](#)

[Report e log](#)

[Log](#)

[Creazione di report](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto il processo di configurazione della limitazione del tenant Microsoft O365 in Secure Web Appliance (SWA).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'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. Creare una	Passaggio 1.1. Dalla GUI, passare a Web Security Manager e
-------------------------	--

categoria URL personalizzata per il sito Web.

scegliere Categorie URL personalizzate ed esterne.

Passaggio 1.2. Fare clic su Add Category per creare una nuova categoria di URL personalizzati.

Passaggio 1.3. Inserire il nome della nuova categoria.

Passaggio 1.4. Definire gli URL nella sezione Siti:

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

Passaggio 1.5. Sottomettere le modifiche.

#### Custom and External URL Categories: Edit Category

The screenshot shows a web form titled "Edit Custom and External URL Category". It has several sections: "Category Name" with a text input containing "MS Tenant Restrictions" (marked with a red circle 1.3); "Comments" with a text area; "List Order" with a dropdown menu set to "1"; "Category Type" set to "Local Custom Category"; "Sites" with a text area containing "login.microsoft.com, login.microsoftonline.com, login.windows.net" (marked with a red circle 1.4) and a "Sort URLs" button; and "Advanced" with a "Regular Expressions" text area. At the bottom are "Cancel" and "Submit" buttons.

Immagine - Categoria URL personalizzato



Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare: <https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Passaggio 2. Decrittare il traffico.

Passaggio 2.1. Dalla GUI, passare a Web Security Manager e scegliere Decryption Policies (Criteri di decrittografia)

Passaggio 2.2. Fare clic su Aggiungi criterio.

Passaggio 2.3. Immettere il nome del nuovo criterio.

Passaggio 2.4. Selezionare il profilo di identificazione a cui applicare il criterio.

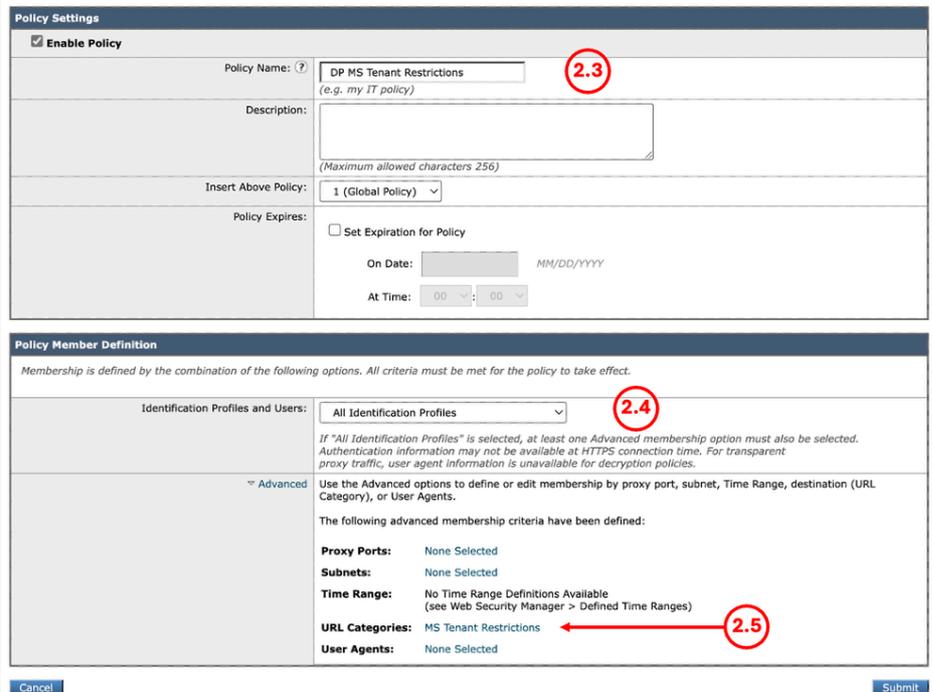
 Suggerimento: Se le autenticazioni per gli URL Microsoft sono state ignorate e si sta configurando questo criterio per Tutti gli utenti, scegliere: Tutti i profili di identificazione > Tutti gli utenti

Passaggio 2.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata.

Passaggio 2.6. Selezionare la categoria dell'URL creata nel Passaggio 1.

Passaggio 2.7. Fare clic su Sottometti.

#### Decryption Policy: DP MS Tenant Restrictions



**Policy Settings**

Enable Policy

Policy Name:  (e.g. my IT policy) **2.3**

Description:

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:  **2.4**

*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:** MS Tenant Restrictions **2.5**

**User Agents:** None Selected

Immagine - Configura criterio di decrittografia

Passaggio 2.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento Filtro URL per il nuovo criterio.

#### Decryption Policies



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

Immagine - Modifica azione filtro URL

Passaggio 2.9. Scegliere Decrittografa come azione per Categoria URL personalizzato.

Passaggio 2.10. Fare clic su Sottometti.

#### 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	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
MS Tenant Restrictions	Custom (Local)	—			✓		—	—

Cancel Submit

Immagine - Decrittografa la categoria dell'URL personalizzato

Passaggio 3.1. Dalla GUI, passare a Web Security Manager e scegliere HTTP ReWrite Profiles.

Passaggio 3.2. Fare clic su Aggiungi profilo.

Passaggio 3.3. Immettere il nome del nuovo profilo.

Passaggio 3.4. Utilizzare Restrict-Access-To-Tenant per il primo nome intestazione.

Passaggio 3.5. Per l'impostazione Restrict-Access-To-Tenants, utilizzare il valore <elenco tenant consentiti>, che deve essere un elenco separato da virgole dei tenant a cui gli utenti possono accedere.

Passaggio 3.6. Fare clic su Aggiungi riga

Passaggio 3.7. Utilizzare Restrict-Access-Context come secondo nome intestazione.

Passaggio 3.8. Per l'impostazione Restrict-Access-Context, utilizzare il valore di un singolo ID directory per specificare il tenant che definisce le restrizioni tenant.

Passaggio 3.9. Fare clic su Sottometti.

Passaggio 3. Creare il profilo di riscrittura HTTP.

### HTTP ReWrite: Edit Profile

Profile Settings				
Profile Name: ?	Header Rewrite MS Tenant Restrictions			
Headers:	Header Name	Header Value	Text Format	Binary Encoding
<input type="checkbox"/>	Restrict-Access-To-Tenants	9.onmicrosoft.com	ASCII	No Encoding
<input type="checkbox"/>	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

Immagine - Aggiungi profilo ReWrite HTTP



Suggerimento: Per ulteriori informazioni sulle Restrizioni tenant e su come raccogliere le informazioni sul tenant, visitare: [Microsoft Learn - Limita l'accesso a un tenant.](#)

Passaggio 4. Creazione dei criteri di accesso.



Suggerimento: Se le autenticazioni per gli URL Microsoft sono state ignorate e si sta configurando questo criterio per Tutti gli utenti, scegliere: Tutti i profili di identificazione > Tutti gli utenti.

Passaggio 4.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata.

Passaggio 4.6. Selezionare la categoria dell'URL creata nel Passaggio 1.

Passaggio 4.7. Fare clic su Sottometti.

### Access Policy: AP MS Tenant Restrictions

**Policy Settings**

Enable Policy

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

Description:

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:

Advanced

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:

User Agents: None Selected

Immagine - Crea criteri di accesso

Passaggio 4.8. Nella pagina Criteri di accesso, verificare che l'azione del filtro URL sia impostata su Monitor.

Passaggio 4.9. Fare clic sul collegamento in Profilo di riscrittura HTTP per aggiungere il profilo di intestazione HTTP al criterio.

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		

Immagine - Proprietà criteri di accesso

Passaggio 4.10. Scegliere i profili di riscrittura HTTP, creati nel passaggio [3].

### Access Policies: Edit HTTP ReWrite Profile

**Profile Settings**

Profiles:  Use Global Settings

None

Header Rewrite MS Tenant Restrictions

Immagine - Aggiungi profilo ReWrite HTTP

Passaggio 4.11. Fare clic su Sottometti.

Passaggio 4.12. Esecuzione del commit delle modifiche.

# Report e log

## Log

È possibile aggiungere un campo personalizzato ai log degli accessi o ai log W3C per visualizzare il nome del profilo di riscrittura dell'intestazione HTTP.

Identificatore formato nei log degli accessi	Campo di log nei log W3C	Descrizione
%]	x-http-rewrite-profile-name	Nome profilo di riscrittura intestazione HTTP.

## Creazione di report

È possibile generare un report di verifica Web per visualizzare i report del traffico in base al nome del criterio di accesso.

Per generare i rapporti, effettuare le operazioni riportate di seguito.

Passaggio 1. Dalla GUI, selezionare Reporting e scegliere Tracciamento Web.

Passaggio 2. Scegliere l'intervallo di tempo desiderato.

Passaggio 3. Fare clic sul collegamento Avanzate per cercare le transazioni utilizzando criteri avanzati.

Passaggio 4. Nella sezione Criterio selezionare Filtra per criterio e digitare il nome del criterio di accesso creato in precedenza.

Passaggio 5. Fare clic su Cerca per esaminare il report.

## 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:	Hour <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span>
User/Client IPv4 or IPv6: ?	<input type="text"/> (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)
Website:	<input type="text"/> (e.g. google.com)
Transaction Type:	All Transactions ▾
▼ Advanced Search transactions using advanced criteria. <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">3</span>	
URL Category:	<input checked="" type="radio"/> Disable Filter <input type="radio"/> Filter by URL Category: <input type="text"/>
Application:	<input checked="" type="radio"/> Disable Filter <input type="radio"/> Filter by Application: <input type="text"/> (ex. Twitter) <input type="radio"/> Filter by Application Type: <input type="text"/> (ex. Social Networking)
Policy:	<input type="radio"/> Disable Filter <input checked="" type="radio"/> Filter by Policy: <input type="text"/> AP MS Tenant Restrictor <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">4</span>

Immagine - Report di verifica Web

## Informazioni correlate

- [Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)
- [Guida all'installazione di Cisco Secure Email e Web Virtual Appliance](#)
- [Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco](#)
- [Utilizzare le procedure ottimali per Secure Web Appliance](#)
- [Configurare il firewall per Secure Web Appliance](#)
- [Configura certificato di decrittografia in Appliance Web sicura](#)
- [Configurazione e risoluzione dei problemi di SNMP in SWA](#)
- [Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server](#)
- [Abilita canale/video YouTube specifico e blocca resto di YouTube in SWA](#)
- [Informazioni sul formato HTTPS Accesslog in Secure Web Appliance](#)
- [Accesso ai registri protetti di Web Appliance](#)
- [Ignora autenticazione in Secure Web Appliance](#)
- [Blocca il traffico in Secure Web Appliance](#)
- [Ignora traffico aggiornamenti Microsoft in Secure Web Appliance](#)

## 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).