

Microsoft O365-huurdersbeperking configureren in SWA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[Rapportage en logboeken](#)

[Logboeken](#)

[verslaggeving](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt het proces beschreven voor het configureren van Microsoft O365 Tenant Restriction in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratiestappen

Stap 1. Maak een aangepaste	Stap 1.1. Navigeer vanuit de GUI naar Web Security Manager en
-----------------------------	---

URL-categorie voor de website.

kies Aangepaste en Externe URL-categorieën.

Stap 1.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken.

Stap 1.3. Voer de naam voor de nieuwe rubriek in.

Stap 1.4. Definieer deze URL's in de sectie Sites:

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

Stap 1.5. Dien de wijzigingen in.

Custom and External URL Categories: Edit Category

Category Name: MS Tenant Restrictions 1.3

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ?
login.microsoft.com, login.microsoftonline.com, login.windows.net 1.4
(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

[Sort URLs](#)
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Advanced Regular Expressions: ?
Enter one regular expression per line. Maximum allowed characters 2048.

[Cancel](#) [Submit](#)

Afbeelding - Aangepaste URL-rubriek



Tip: Ga voor meer informatie over het configureren van aangepaste URL-categorieën naar:
<https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Stap 2. Decodeer het verkeer.

Stap 2.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid

Stap 2.2. Klik op Beleid toevoegen.

Stap 2.3. Voer een naam in voor het nieuwe beleid.

Stap 2.4. Selecteer het identificatieprofiel waarop dit beleid van toepassing is.



Tip: Als u de verificaties voor Microsoft-URL's hebt omzeild en dit beleid voor alle gebruikers configureert, kiest u: Alle identificatieprofielen > Alle gebruikers

Stap 2.5. Klik in de sectie Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen.

Stap 2.6. Selecteer de URL-categorie die is gemaakt in stap 1.

Stap 2.7. Klik op Indienen.

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**

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

Afbeelding - Decryptiebeleid configureren

Stap 2.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid.

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...						

Afbeelding - Actie URL-filtering bewerken

Stap 2.9. Kies Decrypt als de actie voor Aangepaste URL-rubriek.

Stap 2.10. Klik op Indienen.

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)	—			☒		—	—

Afbeelding - De aangepaste URL-rubriek decoderen

Stap 3.1. Navigeer vanuit de GUI naar Web Security Manager en kies HTTP ReWrite Profiles.

Stap 3.2. Klik op Profiel toevoegen.

Stap 3.3. Voer de naam in voor het nieuwe profiel.

Stap 3.4. Gebruik Restrict-Access-To-Tenants voor de eerste naam van de koptekst.

Stap 3.5. Gebruik voor de instelling Toegang tot huurders beperken een waarde van <lijst met toegestane huurders>, die een Kommagescheiden lijst moet zijn van de huurders waartoe gebruikers toegang hebben.

Stap 3.6. Klik op Rij toevoegen

Stap 3.7. Gebruik Restrict-Access-Context als tweede naam van de koptekst.

Stap 3.8. Gebruik voor de instelling Restrict-Access-Context de waarde van een enkele directory-ID om de tenant op te geven die de tenant-beperkingen definieert.

Stap 3.9. Klik op Indienen.

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	Add Row
☐ Restrict-Access-Context	2-9505-4097-a69a-c1553ef	ASCII	No Encoding	Copy Row

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.

Stap 3. Maak een HTTP-herschrijfprofiel.

Afbeelding - HTTP-herschrijfprofiel toevoegen



Tip: Ga voor meer informatie over huurdersbeperking en het verzamelen van uw huurdersinformatie naar: [Microsoft Learn - Toegang tot een huurder beperken.](#)

Stap 4.1. Navigeer vanuit de GUI naar Web Security Manager en kies Toegangsbeleid

Stap 4.2. Klik op Beleid toevoegen.

Stap 4.3. Voer een naam in voor het nieuwe beleid.

Stap 4.4. Selecteer het identificatieprofiel waarop dit beleid van toepassing is.



Tip: Als u de verificaties voor Microsoft-URL's hebt omzeild en dit beleid voor alle gebruikers configureert, kiest u: Alle identificatieprofielen > Alle gebruikers.

Stap 4.5. Klik in de sectie Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen.

Stap 4.6. Selecteer de URL-categorie die is gemaakt in stap 1.

Stap 4.7. Klik op Indienen.

Stap 4. Toegangsbeleid maken.

Access Policy: AP MS Tenant Restrictions

Policy Settings	
☒ Enable Policy	
Policy Name: ?	AP MS Tenant Restrictions 4.3 (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: :

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 4.4
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 4.5
User Agents:	None Selected

Cancel Submit

Afbeelding - Toegangsbeleid maken

Stap 4.8. Zorg ervoor dat op de pagina Toegangsbeleid de actie URL-filtering is ingesteld op Bewaken.

Stap 4.9. Klik op de link in HTTP ReWrite Profile om het HTTP Header Profile aan dit beleid toe te voegen.

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...									

Afbeelding - Eigenschappen toegangsbeleid

Stap 4.10. Kies de HTTP-herschrijfprofielen, gemaakt in stap [3].

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles: ☒ Use Global Settings ☐ None ☐ Header Rewrite MS Tenant Restrictions

Cancel Submit

Afbeelding - HTTP-herschrijfprofiel toevoegen

Stap 4.11. Klik op Indienen.

Stap 4.12. Wijzigen doorvoeren.

Rapportage en logboeken

Logboeken

U kunt een aangepast veld toevoegen aan de toegangslogs of de W3C-logs om de naam van het HTTP-herschrijfprofiel voor de header weer te geven.

Opmaakspecificatie in toegangslogboeken	Logboekveld in W3C-logboeken	Beschrijving
%]	x-http-rewrite-profile-name	HTTP header herschrijf profielnaam.

verslaggeving

U kunt een webtrackingrapport genereren om de rapporten van het verkeer weer te geven met de naam AccessPolicy.

Gebruik deze stappen om de rapporten te genereren:

Stap 1. Selecteer in de GUI Rapportage en kies Webtracking.

Stap 2. Kies het gewenste tijdsbereik.

Stap 3. Klik op de Geavanceerde link om transacties te zoeken met behulp van geavanceerde criteria.

Stap 4. Selecteer in het gedeelte Beleid de optie Filter op beleid en typ de naam van het toegangsbeleid dat eerder is gemaakt.

Stap 5. Klik op Zoeken om het rapport te bekijken.

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 (2)

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: All Transactions

Advanced (3) 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: (4) AP MS Tenant Restrictor

Afbeelding - Rapport voor webtracking

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)
- [Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance](#)
- [Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco](#)
- [Best practices voor veilige webapparaten gebruiken](#)
- [Firewall configureren voor Secure Web Appliance](#)
- [Decryptiecertificaat configureren in Secure Web Appliance](#)
- [SNMP configureren en oplossen in SWA](#)

- [SCP Push Logs configureren in Secure Web Appliance met Microsoft Server](#)
- [Specifieke YouTube-kanaal / video inschakelen en de rest van YouTube blokkeren in SWA](#)
- [Inzicht in HTTPS-toegangslogindeling in Secure Web Appliance](#)
- [Toegang tot beveiligde logbestanden van webapparaten](#)
- [Verificatie omzeilen in Secure Web Appliance](#)
- [Verkeer blokkeren in Secure Web Appliance](#)
- [Microsoft Updates-verkeer omzeilen in Secure Web Appliance](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.