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.

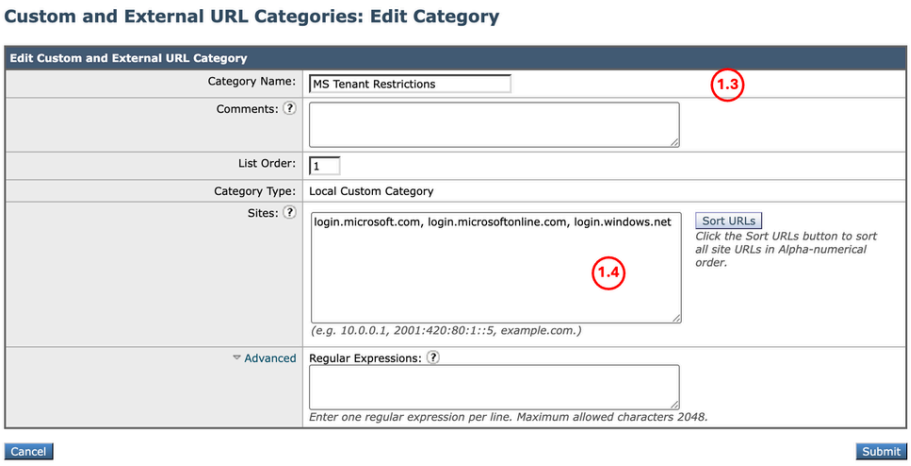
Gebruikte componenten

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

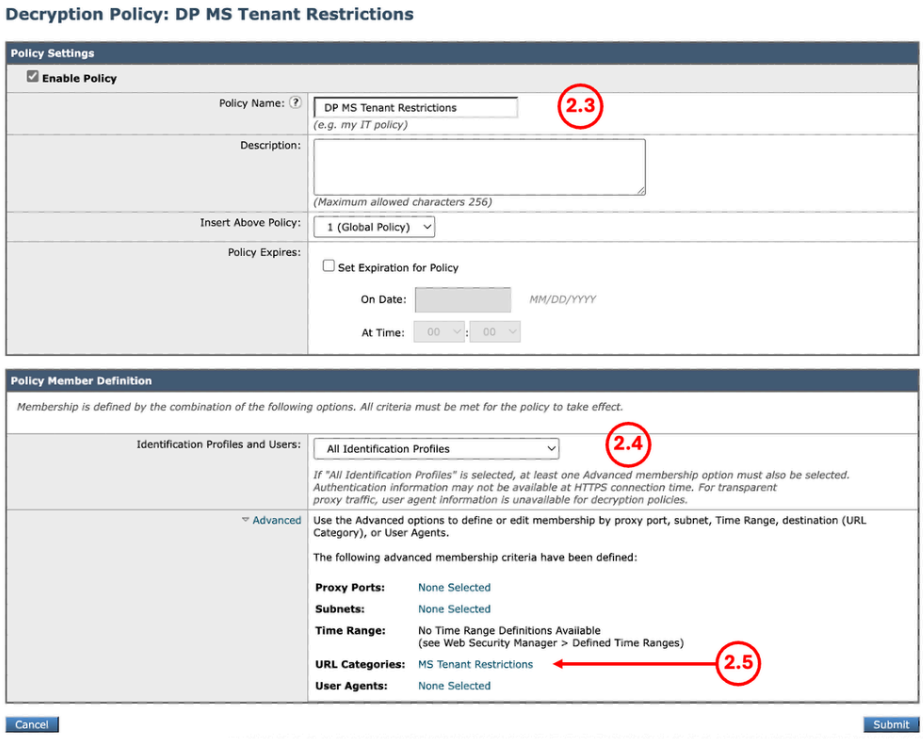
URL-categorie voor de website.	kies Aangepaste en Externe URL-categorieën. Stap 1.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken. Stap 1.3. Voer de naam voor de nieuwe rubriek in. Stap 1.4. Definieer deze URL's in de sectie Sites: `login.microsoft.com, login.microsoftonline.com, login.windows.net` Stap 1.5.Dien de wijzigingen in.  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.

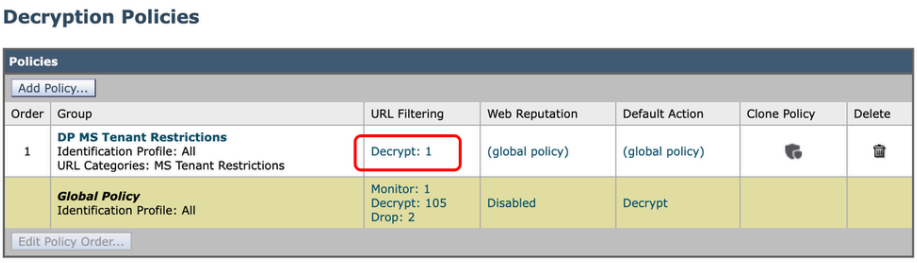
Stap 2.6. Selecteer de URL-categorie die is gemaakt in stap 1.

Stap 2.7. Klik op Indienen.



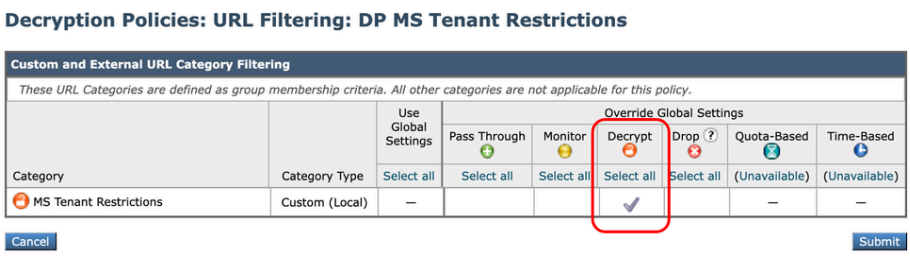
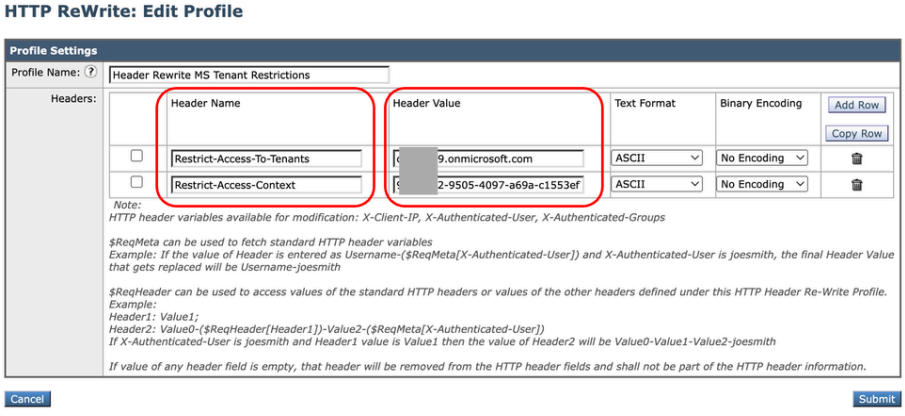
Afbeelding - Decryptiebeleid configureren

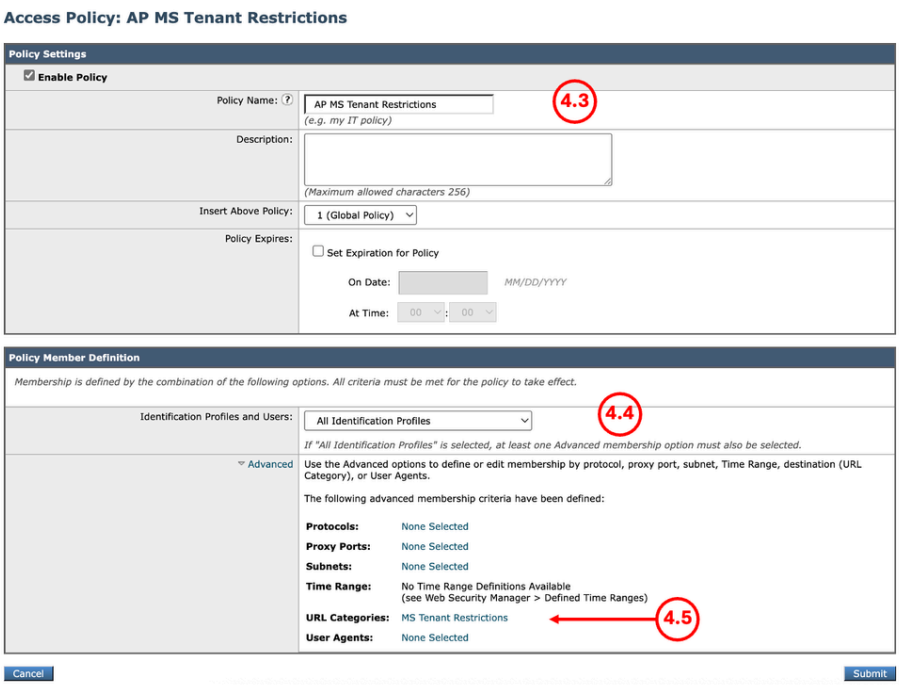
Stap 2.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid.



Afbeelding - Actie URL-filtering bewerken

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

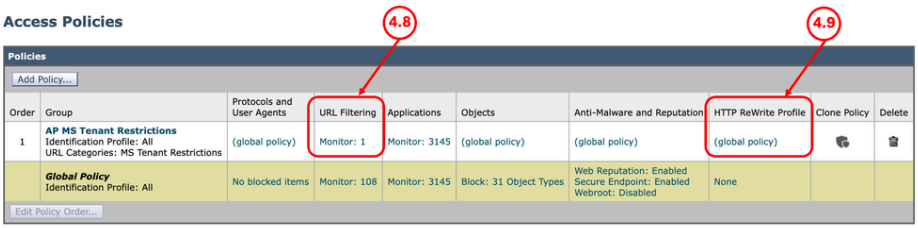
	Stap 2.10. Klik op Indienen.  Afbeelding - De aangepaste URL-rubriek decoderen
Stap 3. Maak een HTTP-herschrijfprofiel.	Stap 3.1. Navigeer vanuit de GUI naar Web Security Manager en kies HTTP ReWrite Profiles. Stap 3.2. Klik op Profiel toevoegen. Stap 3.3. Voer de naam in voor het nieuwe profiel. Stap 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. 

	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. Toegangsbeleid maken.	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. 

Afbeelding - Toegangsbeleid maken

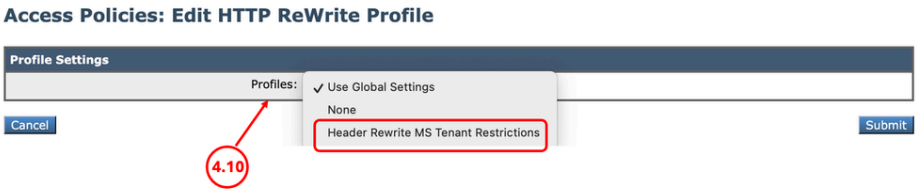
Stap 4.8. Zorg ervoor dat op de pagina Toegangsbeleid de actie URL-filtering is ingesteld op Bewaken.

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



Afbeelding - Eigenschappen toegangsbeleid

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



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:

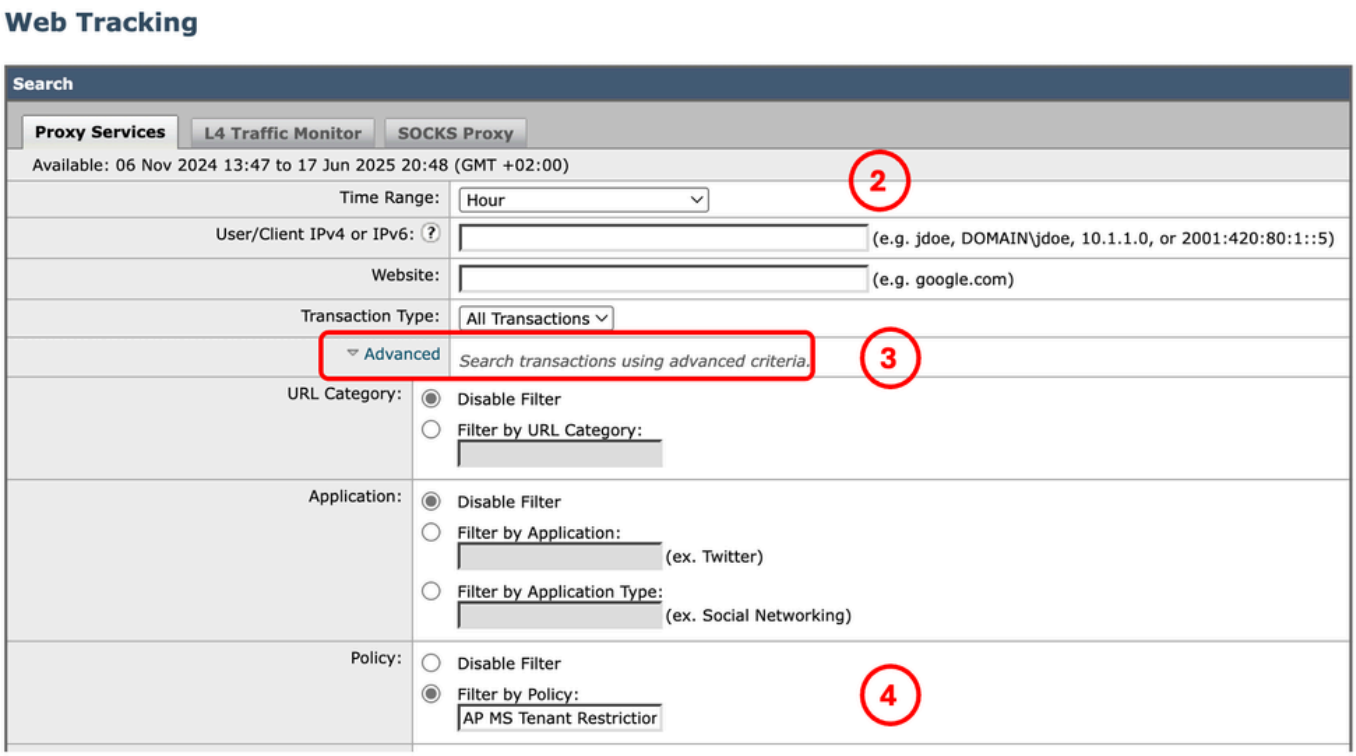
Stap 1. Selecteer in de GUI Rapportage en kies Webtracking.

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.



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.