# Google-toegang tot consumentenaccounts blokkeren in de SWA

## Inhoud



## Inleiding

Dit document beschrijft het proces van het blokkeren van Google Workspace of Google Consumer Accounts toegang in Secure Web Appliance (SWA).

## Voorwaarden

### Vereisten

Cisco raadt kennis van deze onderwerpen aan:

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

### Gebruikte componenten

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

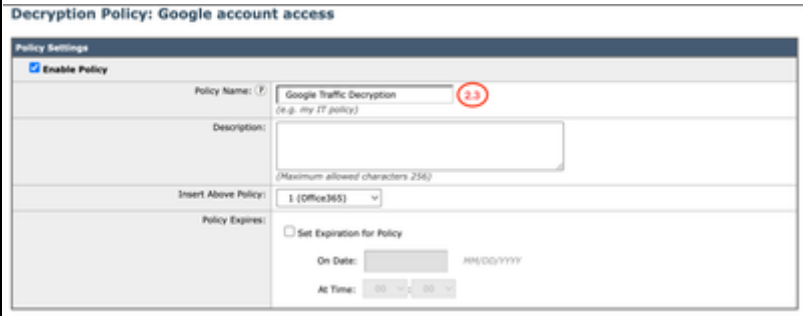
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

<table>
<tr>
<td>Stap 1. Maak een aangepaste URL-categorie voor de Google-sites.</td>
<td>Stap 1.1. Navigeer vanuit de GUI naar Web Security Manager en kies Aangepaste en Externe URL Categorieën.<br><br>Stap 1.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken.<br><br>Stap 1.3. Voer de naam voor de nieuwe rubriek in.<br><br>Stap 1.4. Definieer deze URL's in het gedeelte Sites:<br><br><code>.google.com</code><br><br>Stap 1.5. De wijzigingen indienen.<br><br>  <br><br>Afbeelding - Aangepaste URL-rubriek<br><br>Tip: Ga voor meer informatie over het configureren van aangepaste URL-categorieën naar: Aangepaste URL-categorieën configureren in Secure Web Appliance.</td>
</tr>
<tr>
<td>Stap 2.Decodeer het verkeer.</td>
<td>Stap 2.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid.</td>
</tr>
</table>

Stap 2.2. Klik op Beleid toevoegen.

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



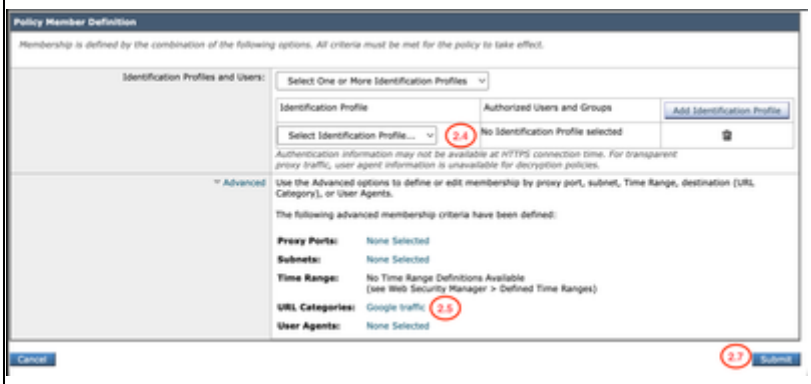

Stap 2.4. Selecteer het identificatieprofiel waarop u dit beleid wilt toepassen.

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-categorieënlinks om de aangepaste URL-categorie toe te voegen.

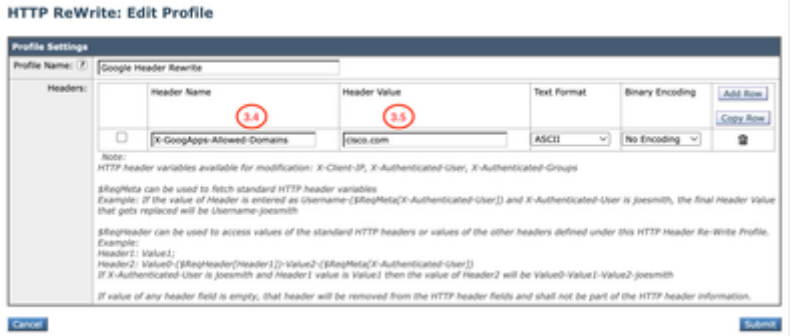
Stap 2.6.Selecteer de URL-categorie die is gemaakt in stap 1.

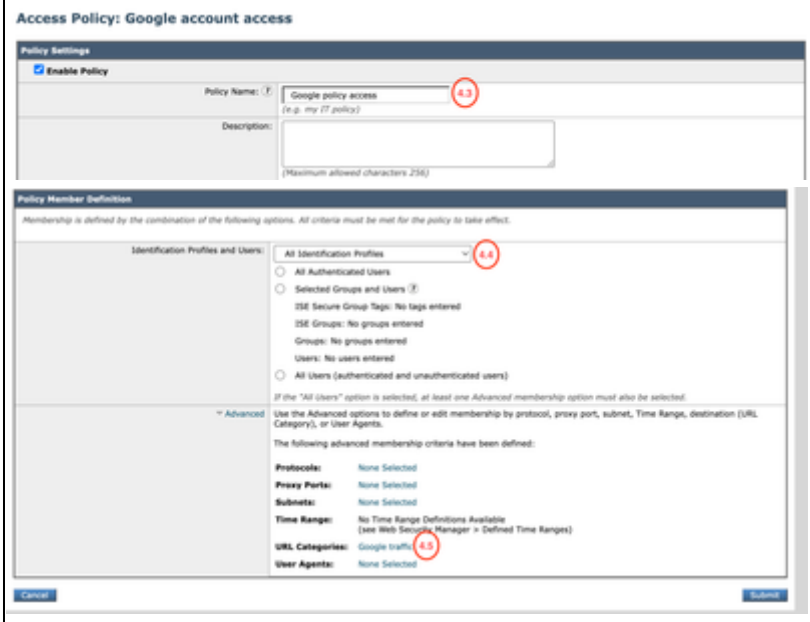
Stap 2.7.Klik op Indienen.

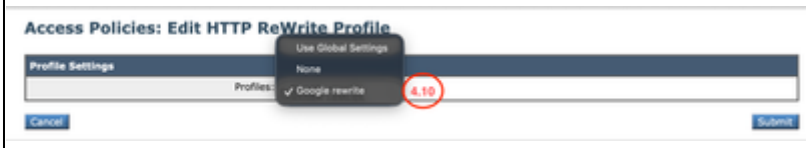



Afbeelding - Decryptiebeleid configureren

Stap 2.8. Klik in de pagina Decryptiebeleid op de link van URL-filtering voor het nieuwe beleid.

| | |
|---|---|
| | Afbeelding - Actie URL-filtering bewerken<br><br>Stap 2.9. Kies Decrypt als de actie voor Aangepaste URL-rubriek.<br><br>Stap 2.10.Klik op Indienen.<br><br>  <br><br><br>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.<br><br>Stap 3.2. Klik op Profiel toevoegen.<br><br>Stap 3.3. Voer een naam in voor het nieuwe profiel.<br><br>Stap 3.4. Gebruik X-GoogApps-Allowed-Domains voor de eerste naam van de koptekst.<br><br>Stap 3.5. Gebruik voor de instelling Toegang tot huurders beperken een domeinwaarde van de lijst met toegestane huurders, die een door komma's gescheiden lijst moet zijn van de huurders waartoe gebruikers toegang hebben.<br><br>Stap 3.9.Klik op Indienen.<br><br>  <br><br><br>Afbeelding - HTTP-herschrijfprofiel toevoegen |

| | |
|---|---|
| Stap 4.Toegangsbeleid maken. | Stap 4.1. Navigeer vanuit de GUI naar Web Security Manager en kies Access Policies.<br><br>Stap 4.2. Klik op Beleid toevoegen.<br><br>Stap 4.3. Voer een naam in voor het nieuwe beleid.<br><br>Stap 4.4. (Optioneel) Selecteer het identificatieprofiel waarop u dit beleid wilt toepassen.<br><br>Stap 4.5.Klik in het gedeelte Definitie van beleidslid op URL-categoriekoppelingen om de aangepaste URL-categorie toe te voegen.<br><br>Stap 4.6.Selecteer de URL-categorie die is gemaakt in stap 1.<br><br>Stap 4.7. Klik op Indienen.<br><br>  <br><br>Afbeelding - Toegangsbeleid maken<br><br>Stap 4.8.InAccess Policies pagina, zorg ervoor dat de actie van de URL Filtering is ingesteld op Monitor.<br><br>Stap 4.9.Klik op de link in HTTP ReWrite Profile om het HTTP Header Profile aan dit beleid toe te voegen.<br><br>  <br><br>Afbeelding - Eigenschappen toegangsbeleid<br><br>Stap 4.10. Kies de HTTP-herschrijfprofielen, gemaakt in |

| | |
|---|---|
| | stap [3].<br>  <br><br>Afbeelding - HTTP-herschrijfprofiel toevoegen<br>Stap 4.11. Klik op Indienen.<br>Stap 4.12. Wijzigen vastleggen. |

# Rapportage en logboeken

## Logboeken

U kunt aangepaste velden 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. |

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

Gebruik deze stappen om de rapporten te genereren:

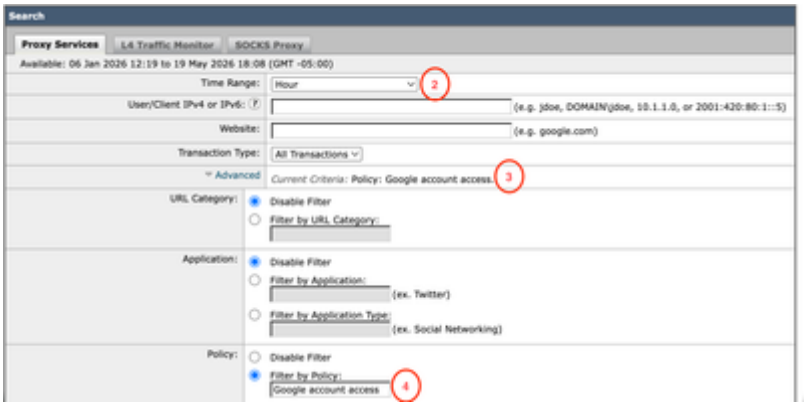
Stap 1. Selecteer Rapportage in de GUI en kies Webtracking.

Stap 2. Kies het gewenste tijdsbereik.

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

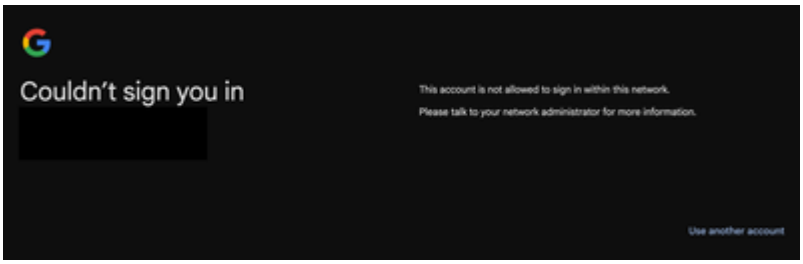
Stap 4. Selecteer in het gedeelte Beleid de optie Filter op beleid en typ de naam van het toegangsbeleid dat eerder is gemaakt.

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




## Verifiëren

Wanneer de configuratie van de Google-domeinbeperking is voltooid, heeft de gebruiker alleen toegang tot de accounts die onder het domein vallen dat is geconfigureerd in het profiel Herschrijven van koptekst in stap 3. Als het gebruik probeert toegang te krijgen tot een account op een ander domein, of een ander, persoonlijk Google-account, wordt de toegang beperkt met deze kennisgeving:




## Gerelateerde informatie

[Aangepaste URL-categorieën definiëren in WSA]

[Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance]

[Decryptiecertificaat configureren in Secure Web Appliance]

[WSA HTTP Header Rewrite]

[Toegang tot consumentenaccounts blokkeren (Google-documentatie)]

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.