# Secure Web Appliance configureren om gasttoegang toe te staan

## Inhoud



## Inleiding

In dit document worden de stappen beschreven die gebruikers die het decoderingscertificaat niet hebben geïnstalleerd, in staat moeten stellen toegang te krijgen tot het internet via Secure Web Appliance (SWA).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fysieke of virtuele SWA geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- De installatiewizard is voltooid.

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

## Overzicht van scenario

Dit artikel behandelt een scenario voor netwerktoegangscontrole binnen het 10.10.10.0/24 Wi-Fi-subnet. De omgeving bestaat uit twee verschillende gebruikersgroepen die een verschillend beveiligings- en toegangsbeleid vereisen:

- Managed Devices: door het bedrijf uitgegeven laptops die volledig zijn geverifieerd en waarop het SWA-decoderingscertificaat is geïnstalleerd. Deze apparaten zijn vertrouwd en doorgaans onderworpen aan het standaardbeleid voor bedrijfstoegang.
- Onbeheerde/gastapparaten: persoonlijke laptops en mobiele apparaten die niet zijn geverifieerd en waarvoor het SWA-decoderingscertificaat ontbreekt.

Doel:
Het bedrijf streeft ernaar om een restrictief beleid voor webtoegang te implementeren voor onbeheerde apparaten, waarbij hun connectiviteit wordt beperkt tot een specifieke subset van toegestane URL's, terwijl ervoor wordt gezorgd dat bedrijfsmiddelen veilig blijven.

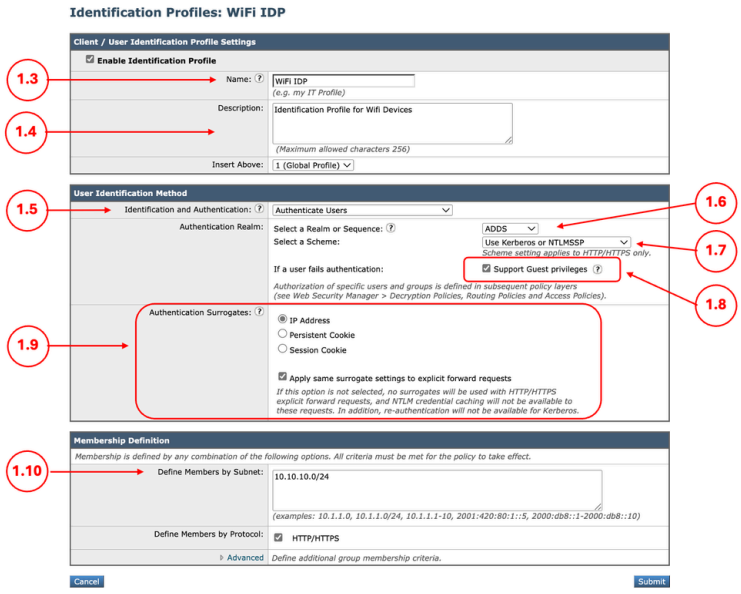
---

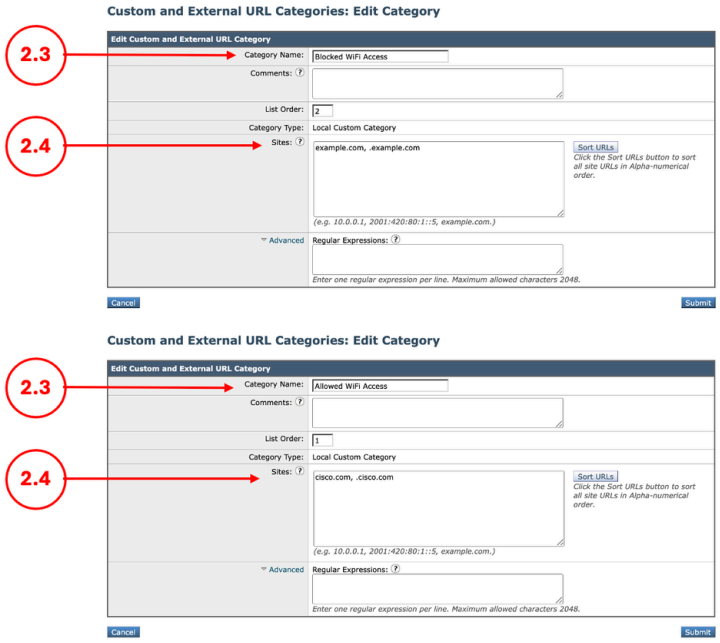
Opmerking: Aangezien het decryptiecertificaat niet wordt vertrouwd op de onbeheerde apparaten, kunt u het HTTPS-verkeer niet decoderen en moet de actie worden ingesteld om door te gaan.

---

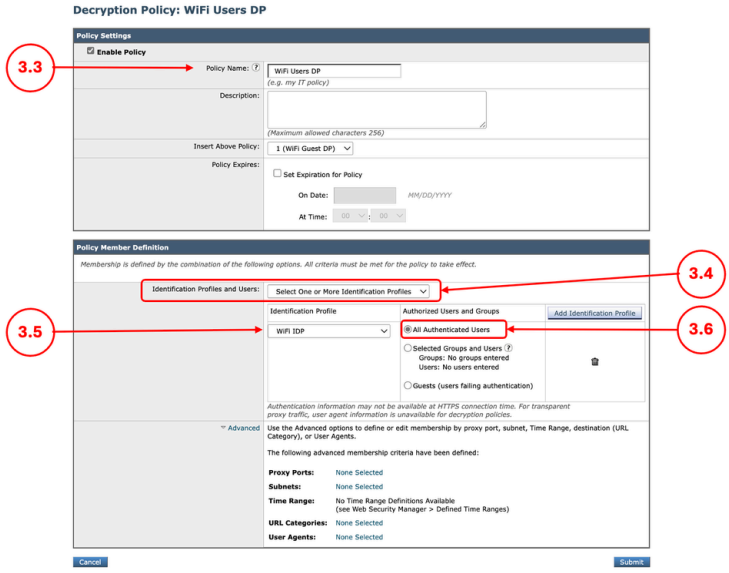
## Configuratiestappen

| | |
|---|---|
| Stap 1. Identificatieprofiel maken. | Stap 1.1. Navigeer vanuit de SWA GUI naar Web Security Manager en selecteer Identification Profile.<br><br>Stap 1.2. Klik op Identificatie toevoegen.<br><br>Stap 1.3. Geef een naam op voor het profiel.<br><br>Stap 1.4. (Optioneel) Definieer de beschrijving.<br><br>Stap 1.5. Kies Gebruikers verifiëren in identificatie en verificatie.<br><br>Stap 1.6. Kies het Active Directory-domein uit Selecteer een rijk of reeks.<br><br>Stap 1.7. Selecteer in Selecteer een schema de |

| | |
|---|---|
| | gewenste verificatieprotocollen.<br><br>Tip: kies geen basisverificatie in de lijst Een schema selecteren.<br><br>Stap 1.8. Schakel het selectievakje in voor Gastrechten voor ondersteuning.<br><br>Stap 1.9. (Optioneel) Afhankelijk van uw ontwerp, kunt u het surrogaat inschakelen door dezelfde surrogaatinstellingen toe te passen op expliciete doorstuurverzoeken.<br><br>Let op: Aangezien u het verkeer niet kunt decoderen, selecteert u in de transparante implementatie geen Persistent Cookie of Sessiecookie.<br><br>Stap 1.10. Definieer het IP-adres in subnet, Definieer leden op subnet.<br><br>Stap 1.11. Verzenden en vastleggen van de wijzigingen.<br><br>  <br><br>Afbeelding - Identificatieprofiel definiëren |
| Stap 2. (Optioneel) Maak de aangepaste URL-categorieën voor toegestane en geblokkeerde URL's | Stap 2.1.Navigeer van de GUI naar Web Security Manager en kies Aangepaste en Externe URL-categorieën.<br><br>Stap 2.2.Klik op Rubriek toevoegen om een nieuwe |

| | |
|---|---|
| | aangepaste URL-rubriek te maken.<br><br>Stap 2.3.Voer de naam in voor de nieuwe categorie.<br><br>Stap 2.4. Definieer het domein en/of de subdomeinen van de websites die u de toegang wilt blokkeren.<br><br>Stap 2.5.Wijzigingen indienen.<br><br>Stap 2.6. Gebruik dezelfde stappen om een URL-categorie te maken voor de website die u toegang verleent.<br><br>  <br>Afbeelding - Aangepaste URL-rubriek definiëren |
| Stap 3. Decoderingsbeleid maken voor beheerde apparaten | Stap 3.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid<br><br>Stap 3.2.Klik op Beleid toevoegen.<br><br>Stap 3.3.Voer een naam in voor het nieuwe beleid.<br><br>Stap 3.4. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.<br><br>Stap 3.5.Selecteer het identificatieprofiel dat is gemaakt in stap 1.<br><br>Stap 3.6. Selecteer Alle geverifieerde gebruikers. |

Stap 3.7.Klik op Indienen.



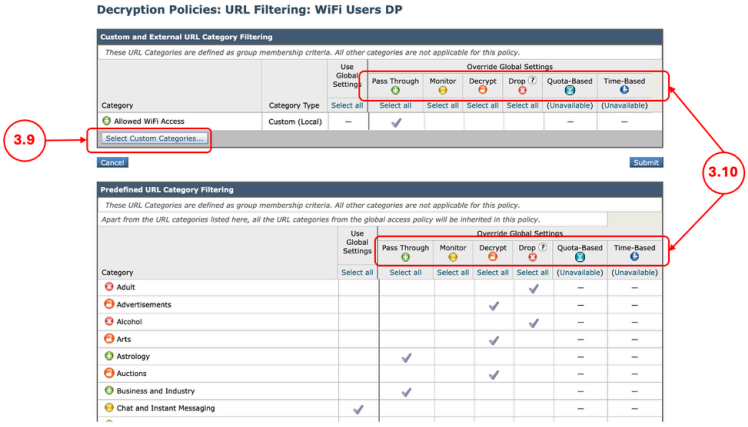

Decoderingsbeleid maken voor beheerde apparaten

Stap 3.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid.

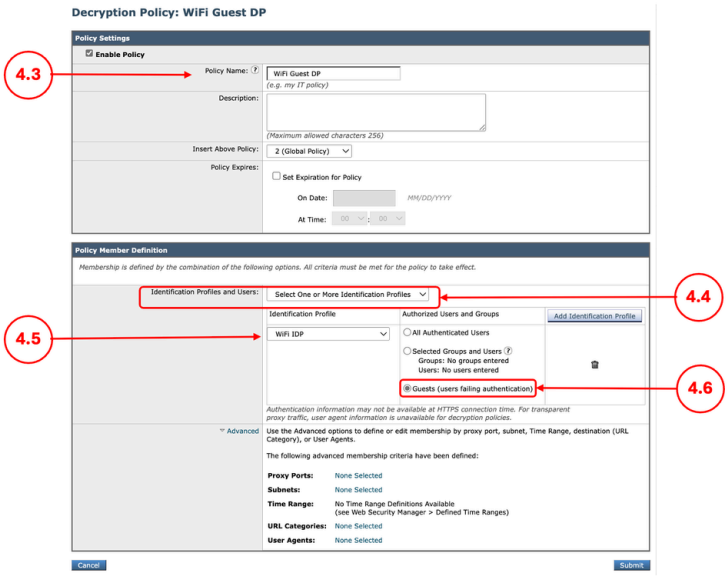
Stap 3.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen

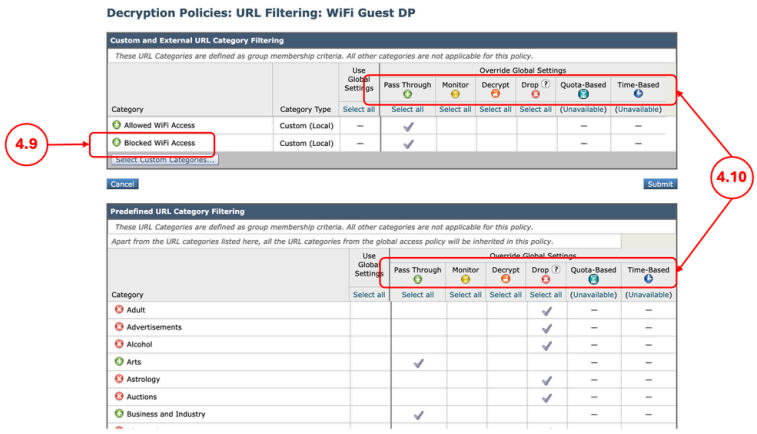
Stap 3.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering.

Stap 3.11. Klik op Submit (Verzenden)




Afbeelding - Actie voor decoderingsbeleid configureren

| | |
|---|---|
| Stap 4. Decoderingsbeleid maken voor niet-beheerde apparaten | Stap 4.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid<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. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.<br><br>Stap 4.5.Selecteer het identificatieprofiel dat is gemaakt in stap 1.<br><br>Stap 4.6. Selecteer Gasten (gebruikers zonder verificatie).<br><br>Stap 4.7.Klik op Indienen.<br><br>  <br><br>Decoderingsbeleid maken voor niet-beheerde apparaten<br><br>Stap 4.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid.<br><br>Stap 4.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen<br><br>Stap 4.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering. |

| | |
|---|---|
| | Opmerking: Gebruik Decrypt niet als actie, omdat het SWA-decoderingscertificaat niet wordt vertrouwd op de niet-beheerde apparaten.<br><br>  <br>Afbeelding - Decoderingsactie voor niet-beheerde apparaten<br><br>Stap 4.11. Scroll naar beneden in het gedeelte Uncategorized URL's en kies de juiste actie.<br><br>  <br>Afbeelding - Niet-gecategoriseerde URL's<br><br>Tip: Voor het beveiligingsperspectief is het het beste om de actie in te stellen op Drop, in het geval dat een URL toegang nodig heeft, kunt u deze toevoegen in de aangepaste URL-categorie die aan het beleid is toegewezen.<br><br>Stap 4.12. Klik op Submit (Verzenden) |
| Stap 5. Toegangsbeleid voor beheerde apparaten maken | Stap 5.1. Navigeer vanuit de GUI naar Web Security Manager en kies Access Policies<br><br>Stap 5.2.Klik op Beleid toevoegen.<br><br>Stap 5.3.Voer een naam in voor het nieuwe beleid.<br><br>Stap 5.4. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.<br><br>Stap 5.5.Selecteer het identificatieprofiel dat is |

gemaakt in stap 1.

Stap 5.6. Selecteer Alle geverifieerde gebruikers.

Stap 5.7.Klik op Indienen.

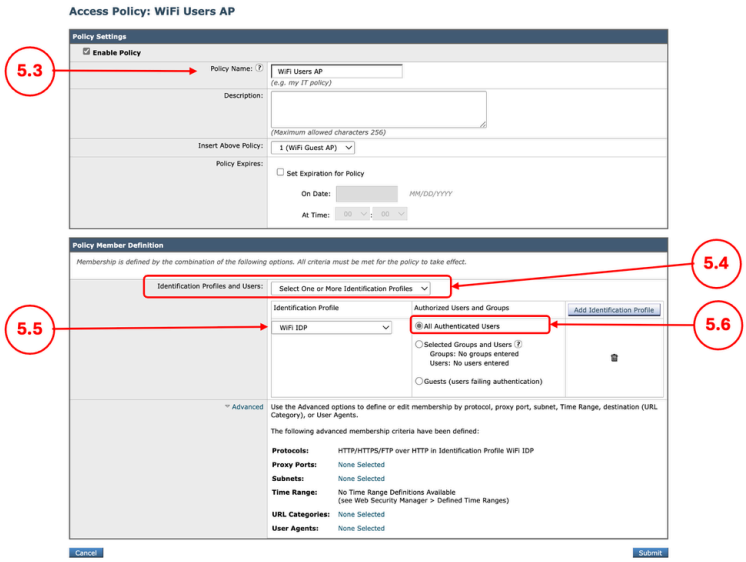
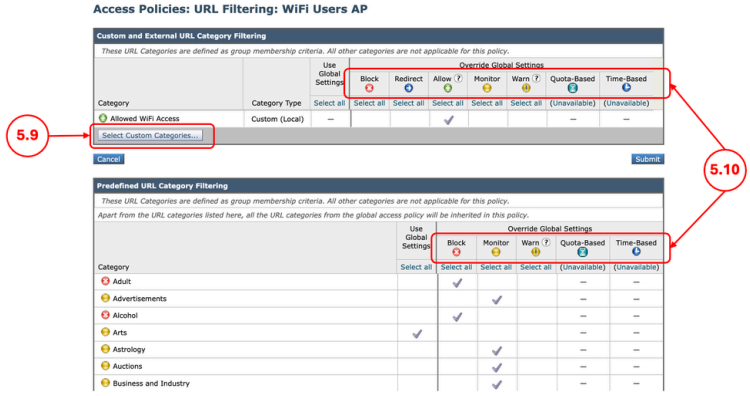



Image - Toegangsbeleid voor beheerde apparaten

Stap 5.8. Klik op de pagina Toegangsbeleid op de koppeling URL-filtering voor het nieuwe beleid.

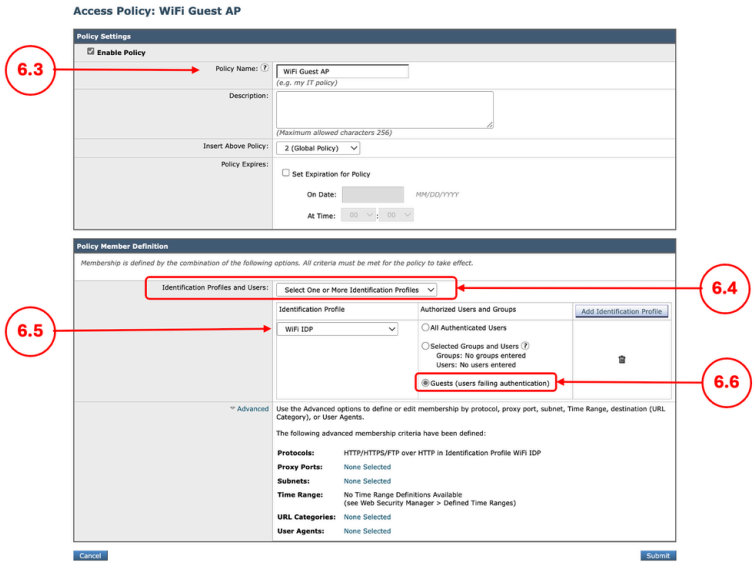
Stap 5.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen

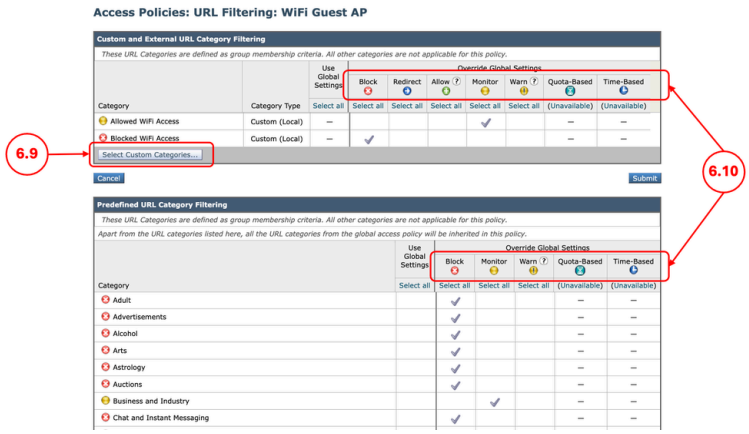
Stap 5.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering.




Afbeelding - URL-filters voor toegangsbeleid voor beheerde apparaten

Stap 5.11. Klik op Indienen.

| | |
|---|---|
| Stap 6. Toegangsbeleid voor niet-beheerde apparaten maken | Stap 6.1. Navigeer vanuit de GUI naar Web Security Manager en kies Access Policies<br><br>Stap 6.2.Klik op Beleid toevoegen.<br><br>Stap 6.3.Voer een naam in voor het nieuwe beleid.<br><br>Stap 6.4. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.<br><br>Stap 6.5.Selecteer het identificatieprofiel dat is gemaakt in stap 1.<br><br>Stap 6.6. Selecteer Gasten (gebruikers zonder verificatie).<br><br>Stap 6.7.Klik op Indienen.<br><br>  <br>Image - Toegangsbeleid voor niet-beheerde apparaten<br><br>Stap 6.8. Klik op de pagina Toegangsbeleid op de koppeling URL-filtering voor het nieuwe beleid.<br><br>Stap 6.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen<br><br>Stap 6.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering. |




Afbeelding - URL-filters voor toegangsbeleid voor niet-beheerde apparaten

Stap 6.11. Scroll naar beneden in het gedeelte Uncategorized URL's en kies de juiste actie.


Afbeelding - Toegangsbeleid URL's zonder rubriek

Tip: Voor het beveiligingsperspectief is het het beste om de actie in te stellen op Blokkeren, in het geval dat een URL toegang nodig heeft, kunt u deze toevoegen in de aangepaste URL-categorie die aan het beleid is toegewezen.

Stap 6.12. Klik op Submit (Verzenden)

## Stap 7. (Optioneel) Cisco-gegevensbeveiligingsbeleid voor beheerde apparaten maken

Opmerking: als u het uploadverkeer voor beheerde apparaten niet wilt filteren, kunt u deze stap overslaan.

Stap 7.1. Navigeer vanuit de GUI naar Web Security Manager en kies Cisco Data Security.

Stap 7.2.Klik op Beleid toevoegen.

Stap 7.3.Voer een naam in voor het nieuwe beleid.

Stap 7.4. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.

Stap 7.5.Selecteer het identificatieprofiel dat is gemaakt in stap 1.

Stap 7.6. Selecteer Alle geverifieerde gebruikers..

Stap 7.7.Klik op Indienen.

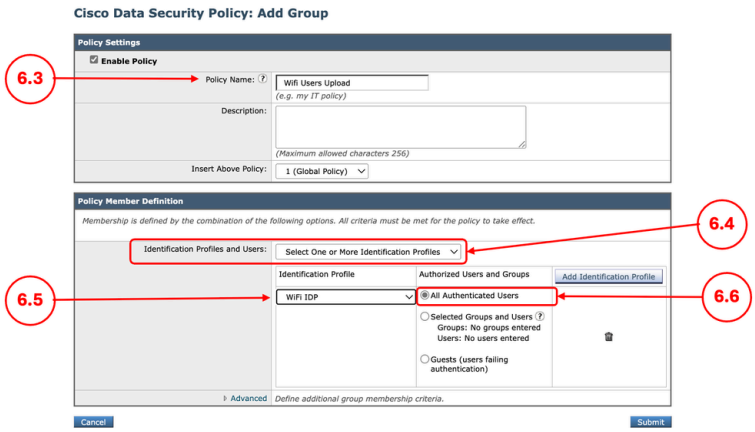
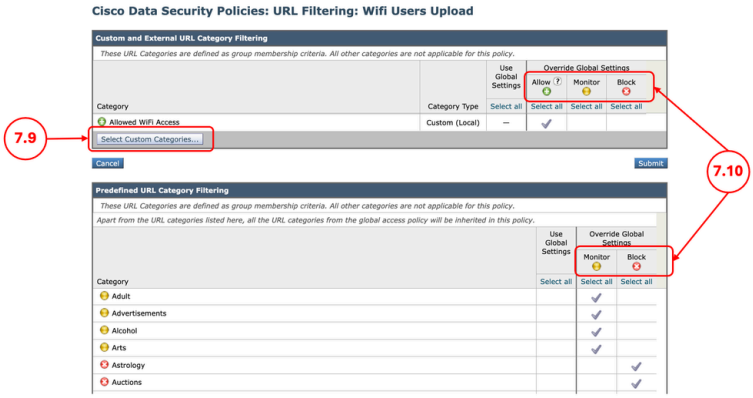
<table>
<tr>
<td></td>
<td>


Image - Cisco-gegevensbeveiligingsbeleid voor beheerde apparaten<br><br>
Stap 7.8. Klik op de pagina Gegevensbeveiligingsbeleid van Cisco op de koppeling URL-filtering voor het nieuwe beleid.<br><br>
Stap 7.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen<br><br>
Stap 7.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering.<br><br>


Afbeelding - Actie voor beheerde apparaten uploaden<br><br>
Stap 7.11. Klik op Indienen.</td>
</tr>
<tr>
<td>Stap 8. (Optioneel) Cisco-gegevensbeveiligingsbeleid maken voor niet-beheerde apparaten</td>
<td>Stap 8.1. Navigeer vanuit de GUI naar Web Security Manager en kies Cisco Data Security.<br><br>
Stap 8.2.Klik op Beleid toevoegen.<br><br>
Stap 8.3.Voer een naam in voor het nieuwe beleid.</td>
</tr>
</table>

Opmerking: als u het uploadverkeer voor niet-beheerde apparaten niet wilt filteren, kunt u deze stap overslaan.

Stap 8.4. Kies Een of meer identificatieprofielen selecteren in het vervolgkeuzemenu Identificatieprofielen en Gebruikers.

Stap 8.5.Selecteer het identificatieprofiel dat is gemaakt in stap 1.

Stap 8.6. Selecteer Alle geverifieerde gebruikers..

Stap 8.7.Klik op Indienen.

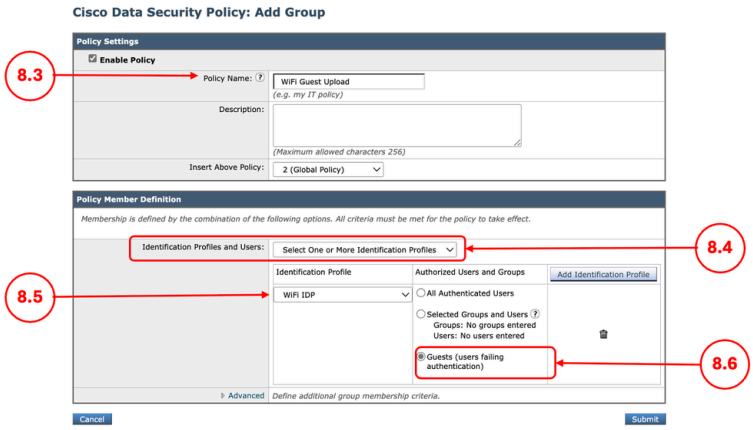
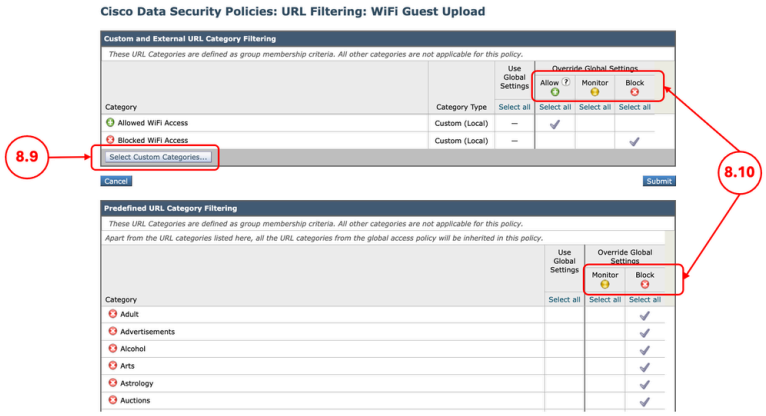


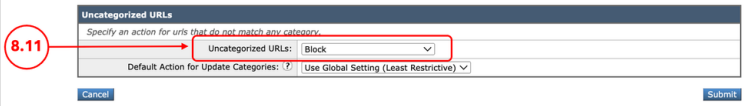

Image - Cisco-gegevensbeveiligingsbeleid voor niet-beheerde apparaten

Stap 8.8. Klik op de pagina Gegevensbeveiligingsbeleid van Cisco op de koppeling URL-filtering voor het nieuwe beleid.

Stap 8.9. (Optioneel) U kunt een aangepaste URL-rubriek toevoegen door op Aangepaste rubrieken selecteren te klikken en Opnemen in beleid voor de rubrieknamen te kiezen

Stap 8.10. Configureer de actie voor elke aangepaste en externe URL Category Filtering en Vooraf gedefinieerde URL Category Filtering.



| | |
|---|---|
| | Afbeelding - Actie uploaden voor niet-beheerde apparaten<br><br>Stap 8.11. Scroll naar beneden in het gedeelte Uncategorized URL's en kies de juiste actie.<br><br>  <br><br>Afbeelding - Actie uploaden voor URL's zonder rubriek<br><br>Tip: Voor het beveiligingsperspectief is het het beste om de actie in te stellen op Blokkeren, in het geval dat een URL toegang nodig heeft, kunt u deze toevoegen in de aangepaste URL-categorie die aan het beleid is toegewezen.<br><br>Stap 8.12. Klik op Submit (Verzenden) |
| Stap 9. De wijzigingen opslaan | Stap 9.1. De wijzigingen vastleggen |

## Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance - LD (Limited Deployment) - Probleemoplossing...
- Executable File Download blokkeren in SWA
- Uploadverkeer blokkeren in Secure Web Appliance
- Verkeer blokkeren in Secure Web Appliance
- Verificatie omzeilen in Secure Web Appliance
- Microsoft O365-huurdersbeperking configureren in SWA
- Beveiligde eerste installatie van webtoestel configureren
- 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.