# Eenmalige aanmeldingsverificatie van Kerberos configureren in SWA

## Inhoud



## Inleiding

In dit document worden de stappen beschreven voor het configureren van proxygebruikers voor Single Sign-On (SSO)-verificatie via Kerberos in Secure Web Appliance (SWA).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-beheer.
- Basis Active Directory-beheer.

Cisco raadt u aan deze hulpprogramma's te installeren:

- Fysieke of virtuele SWA.

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

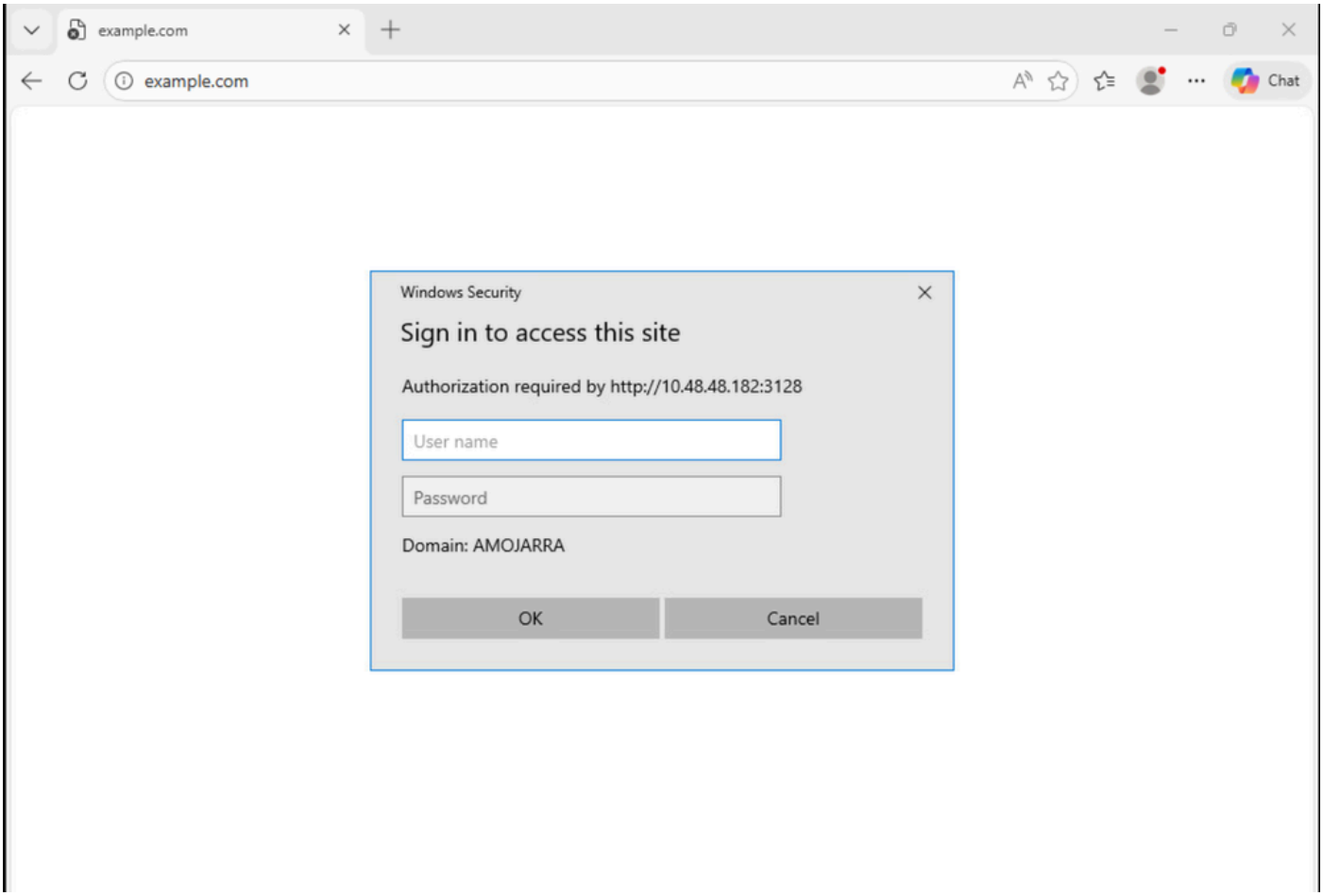
### Gebruikte componenten

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.

## Voordat u begint

Als de proxyclient probeert toegang te krijgen tot een website en wordt gevraagd om de referenties handmatig in te voeren, gebruikt u deze stappen om problemen op te lossen.




Afbeelding - Prompt voor gebruikersverificatie

Stap 1. Controleer de toegangslogs die betrekking hebben op de client.

Stap 1.1. Log in bij de CLI.

Stap 1.2. Run grep.

Stap 1.3. Selecteer het nummer dat is gekoppeld aan de toegangslogs.

Stap 1.4. Typ in het vak Enter the regular expression to grep het IP-adres van de client.

Stap 1.5. Druk op Enter totdat u ziet Wilt u de logs volgen, typ "Y" en druk op enter totdat u de Accesslogs ziet.

Stap 1.6. Reproduceer het probleem door te proberen toegang te krijgen tot elke website vanaf de client-pc.

Stap 1.7. bevestig het identificatieprofiel dat het verkeer raakt.

In dit voorbeeld is het identificatieprofiel Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

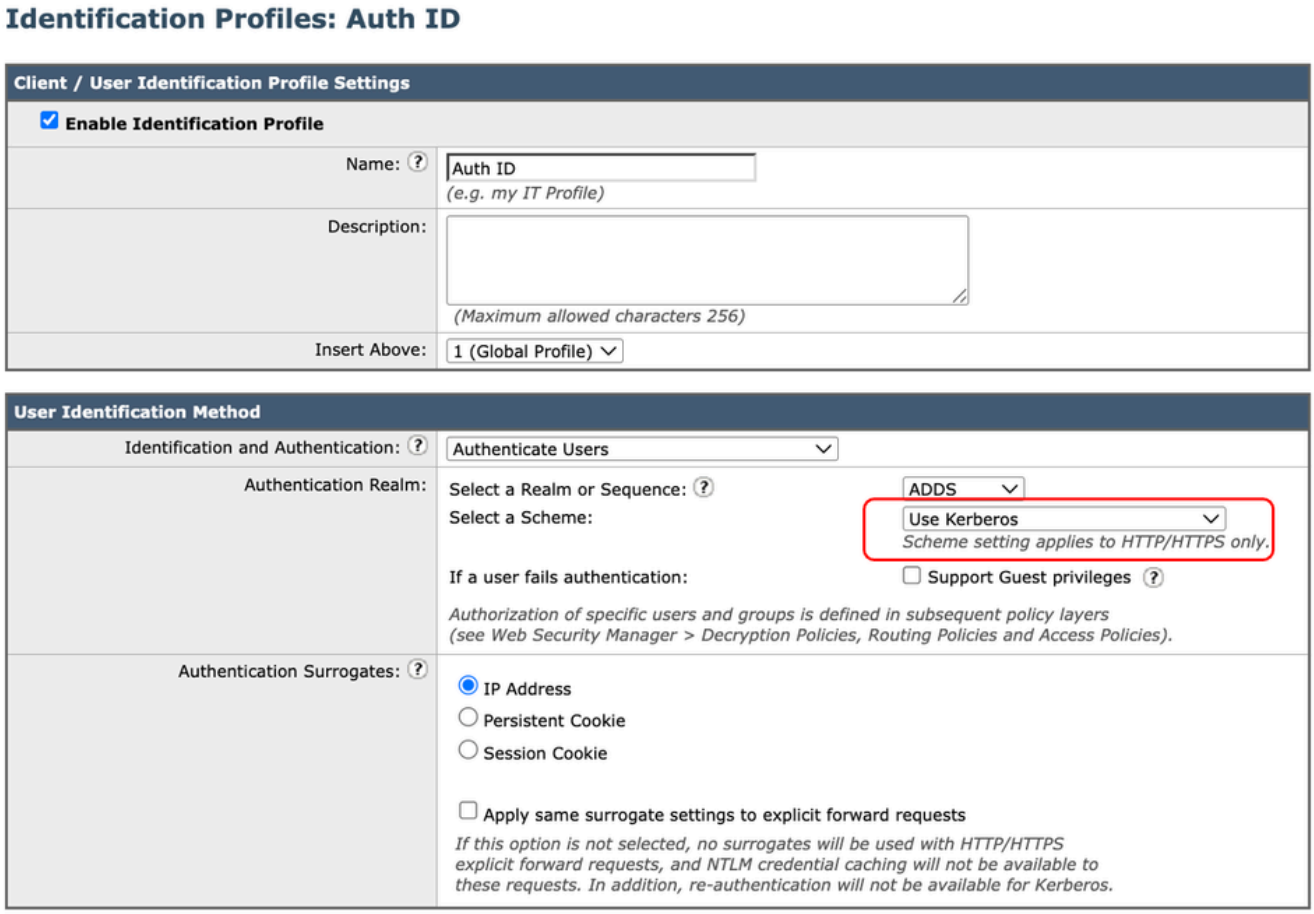
Stap 2. Controleer het identificatieprofiel.

Stap 2.1. Log in op de GUI van de SWA.

Stap 2.2. Selecteer Identificatieprofielen in Web Security Manager.

Stap 2.3. Klik op de naam van het identificatieprofiel dat het verkeer raakte.

Stap 2.4. Bevestig dat het verificatieschema niet is ingesteld op Basis.




Afbeelding - Authenticatieschema

Stap 3. SWA- en Active Directory-connectiviteit testen.

Stap 3.1. Navigeer vanuit de SWA GUI naar Netwerk en selecteer Authenticatie.

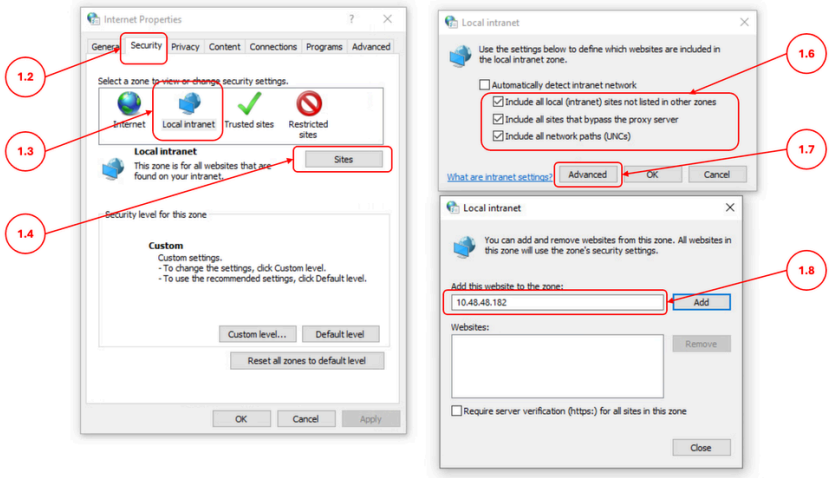
Stap 3.2. Klik op de naam van het verificatiegebied.

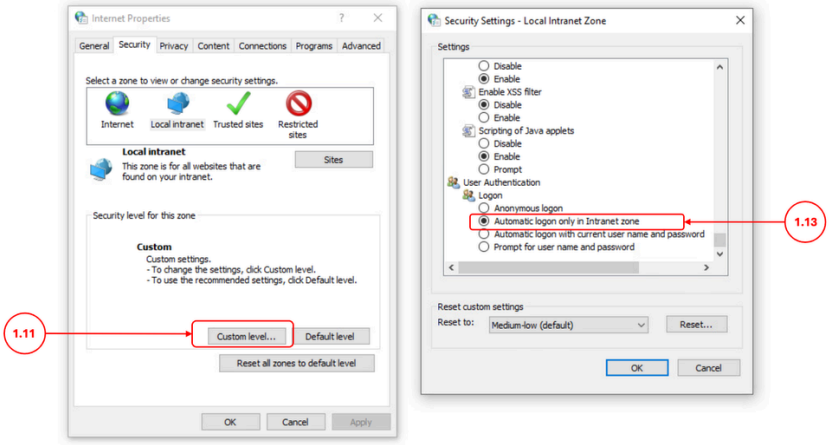
Stap 3.3. Klik op Test starten om de status van de SWA- en Active Directory-connectiviteit te bekijken.

Als er geen fouten worden gevonden, controleert u de configuratie van de client-pc zoals beschreven in dit artikel.

## De client-pc configureren

Gebruik deze stappen om de configuratie van de client-pc te controleren:

| Stappen | Details |
| --- | --- |
| Stap 1. Lokale intranetsites | Stap 1.1. Typ Internet Option in het menu Start en druk op Enter.<br><br>Stap 1.2. Klik in het venster Internet-eigenschappen op het tabblad Beveiliging.<br><br>Stap 1.3. Selecteer Lokaal intranet.<br><br>Stap 1.4. Klik op de sites.<br><br>Stap 1.5. Controleer of het selectievakje Intranetnetwerk automatisch detecteren niet is ingeschakeld.<br><br>Stap 1.6. Selecteer al deze drie opties:<br><br>• Alle lokale (intranet)sites opnemen die niet in andere zones worden vermeld<br>• Inclusief alle sites die de proxyserver omzeilen<br>• Alle netwerkpaden (UNC's) opnemen<br><br>Stap 1.7. Klik op Advanced (Geavanceerd).<br><br>Stap 1.8. Voer het FQDN- of IP-adres van uw SWA in en voeg dit toe aan de lijst.<br><br>Stap 1.9. (Optioneel) Afhankelijk van uw interne beveiligingsbeleid kunt u Verificatie van server vereisen uitschakelen.<br><br>  <br><br>Afbeelding - De lokale internetsites configureren<br><br>Stap 1.10. Klik op Sluiten en OK.<br><br>Stap 1.11. Klik op het tabblad Beveiliging op Aangepast |

| | |
|---|---|
| | niveau.<br><br>Stap 1.12. Blader naar Gebruikersverificatie.<br><br>Stap 1.13. Zorg ervoor dat de optie Alleen automatische aanmelding in de zone Intranet is geselecteerd.<br><br>  <br>Afbeelding - Automatische aanmelding voor intranetgebruikers |
| Stap 2. Verzamel de logs | Als stap 1 de SSO-authenticatie niet via Kerberos heeft opgelost:<br><br>Stap 2.1. Wijzig de SWA Auth-logs in Overtrekken en bekijk de logs.<br><br>Stap 2.2. Voeg [Auth-Method = %m ] toe als een aangepast veld aan de toegangslogboeken. voor meer informatie, bezoek: Prestatieparameter configureren in toegangslogboeken.<br><br>Stap 2.3. Voer een pakketopnamefilter uit voor het IP-adres van de client en het IP-adres van Active Directory en bevestig dat de client-pc het Kerberos-serviceticket naar de SWA verzendt. |

Opmerking: zorg ervoor dat u de FQDN van de SWA hebt geconfigureerd in de proxy-instellingen van uw browser.

## Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance
- Firewall configureren voor Secure Web Appliance

- Packet Capture configureren op Content Security Appliance
- Prestatieparameter configureren in toegangslogboeken
- Toegang tot beveiligde logbestanden van webapparaten
- Best practices voor veilige webapparaten gebruiken - Cisco
- Verificatie omzeilen in Secure Web Appliance - Cisco

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.