Cisco Secure Client SAML-verificatie Vragen bij elke poging met Microsoft Entra ID SSO

Inhoud

uitgeven

Cisco Secure Client (AnyConnect) geïntegreerd met Microsoft Entra ID voor SAML-verificatie ondervond meerdere verificatiegerelateerde problemen die de Single Sign-On (SSO)-functionaliteit verstoorden:

- Gebruikers werden gevraagd om verificatie bij elke VPN-verbindingspoging, zelfs wanneer er een actieve Entra ID-sessie in de browser bestond
- De client lanceerde de ingesloten browser in plaats van de externe/systeembrowser, ondanks dat externe browserverificatie expliciet is ingeschakeld voor SAML
- Gebruikers kwamen vaak de fout tegen: "Verificatiefout vanwege probleem met omleiden naar SSO-URL"
- Het SSO-gedrag was veranderd ten opzichte van de vorige werkstatus, waarbij gebruikers verbinding konden maken met VPN door simpelweg op Verbinden te klikken zonder verificatieprompts

milieu

- Product: Cisco Secure Client (AnyConnect)
- Technologie: Secure Access VPN met SAML-verificatie
- Identiteitsprovider: Microsoft Entra ID (Azure AD)
- Verificatiemethode: SAML SSO-integratie
- Externe browserverificatie ingeschakeld voor SAML

resolutie

De oplossing betrof het aanpakken van de onderliggende problemen met de verbindingsstatus van het Azure AD-apparaat en de configuratie van de browser die de verificatieproblemen veroorzaakten:

Stap 1: De status van Azure AD Join vaststellen

Voer de volgende opdracht uit om de huidige Azure AD-join-status van het betreffende apparaat te controleren:

```
dsregcmd /status
```

Controleer de uitvoer om te bepalen of het apparaat AzureAdJoined = NO weergeeft, wat een onjuiste Azure AD-join-status aangeeft.

Stap 2: Azure AD Join State corrigeren

Voer de opdracht dsregcmd uit om de status van Azure AD-join op het getroffen apparaat te corrigeren. Na het uitvoeren van de juiste afgescheiden bewerkingen,

```
dsregcmd /status
dsregcmd /leave
dsregcmd /join`
```

Controleer of de apparaatstatus het volgende weergeeft:

```
AzureAdJoined = YES
```

Deze correctie lost het onderliggende probleem met de verificatiestatus op waardoor Cisco Secure Client bij elke verbinding om referenties vroeg.

Stap 3: Standaardbrowsertoepassingen opnieuw instellen

Om het probleem van de externe browser versus het ingesloten browsergedrag aan te pakken:

Stel de standaardinstellingen van de toepassingen van het apparaat opnieuw in om ervoor te zorgen dat Cisco Secure Client de externe/systeembrowser correct start voor SAML-verificatie in plaats van de ingesloten browser.

```
Settings → Apps → Default apps → Reset
```

Stap 4: Verificatie

Controleer na het doorvoeren van de bovenstaande wijzigingen het volgende gedrag:

- Cisco Secure Client vraagt niet langer om wachtwoord of Windows Hello-verificatie bij elke VPN-verbinding
- De client start correct de externe browser voor SAML-verificatie in plaats van de ingesloten browser
- De SSO-functionaliteit wordt hersteld, zodat gebruikers verbinding kunnen maken zonder herhaalde verificatievragen wanneer er een actieve Entra ID-sessie bestaat
- De fout "Verificatiefout vanwege probleem met omleiden naar SSO-URL" treedt niet meer op

Oorzaak

De verificatieproblemen werden veroorzaakt door een onjuiste Azure AD-join-status op het getroffen apparaat, waarbij het apparaat AzureAdJoined = NEE weergaf in plaats van de vereiste AzureAdJoined = JA-status. Deze onjuiste join-status verhinderde de juiste SSO-tokenvalidatie en dwong Cisco Secure Client om verificatie te vragen bij elke verbindingspoging.

Bovendien zijn de standaard toepassingsinstellingen van het apparaat verkeerd geconfigureerd, waardoor Cisco Secure Client de ingesloten browser in plaats van de externe browser voor SAML-verificatie heeft gestart, ondanks dat de externe browserinstelling is ingeschakeld in de

clientconfiguratie.

Verwante inhoud

- Cisco Technical Support en downloads

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.