

Problemen oplossen UPN niet geconfigureerd

Fout na vernieuwing van paraplu-certificaat in SWG SAML

Inhoud

[Inleiding](#)

[Overzicht](#)

[Impact](#)

[Scenario 1 - Fout na importeren nieuw paraplu-certificaat](#)

[Zorg ervoor dat zowel de huidige als de nieuwe overkoepelende certificaten worden geïmporteerd](#)

[Zorg ervoor dat de attribuutclaims-map juist is](#)

[Scenario 2 - Fout na verlopen paraplu-certificaat](#)

[Zorg ervoor dat het nieuwe certificaat is geïmporteerd bij de Identity Provider](#)

[\(AANBEVOLEN\) Automatische metagegevensupdates configureren](#)

[Ervoor zorgen dat de adressen van de CRL-server \(Certificate Revocation List\) toegankelijk zijn voor de Identity Provider](#)

[Microsoft ADFS - Voorbeeld van handmatig importeren van certificaten](#)

Inleiding

In dit document wordt beschreven hoe u een fout "UPN niet geconfigureerd" kunt oplossen na het vernieuwen van het SAML-ondertekeningscertificaat van de paraplu.

Overzicht

"UPN niet geconfigureerd" is een algemene fout die om een aantal redenen kan optreden. Een mogelijke oorzaak houdt verband met het verstrijken van het SAML-ondertekeningscertificaat van de paraplu dat jaarlijks wordt verlengd. Voor de meest recente informatie over de vervaldatum van certificaten, kunt u onze portal Mededelingen lezen.

Als het Umbrella-certificaat verloopt en u geen actie hebt ondernomen, worden gebruikers geblokkeerd voor internettoegang met deze mogelijke fouten:

- Fout "UPN niet geconfigureerd" met overkoepelend merk bij het surfen op het web via SWG
- Een andere fout die wordt weergegeven door uw identiteitsprovider



Failed when processing the SAML authentication request. Please contact your System Administrator

UPN is not configured, please check claim rules in your IDP

[Terms](#) | [Privacy Policy](#) | [Contact](#)

Dit artikel bespreekt 2 verschillende scenario's die de fout veroorzaken:

- Scenario 1 - Fout na importeren nieuw paraplucertificaat
- Scenario 2 - Fout na verlopen paraplucertificaat

Impact

Nieuwe gebruikersaanmeldingen voor SWG mislukken, waardoor de toegang tot internet wordt geblokkeerd. Dit geldt niet noodzakelijkerwijs voor alle gebruikers, maar wordt geactiveerd wanneer:

- Een gebruikerssessie verloopt door onze herverificatie-instelling (bijvoorbeeld dagelijks)
- Een nieuwe gebruiker meldt zich aan
- Een gebruiker wist de cache van de browser of gebruikt een nieuwe browser.

Scenario 1 - Fout na importeren nieuw paraplucertificaat

Als de fout direct optreedt na het aanbrengen van een wijziging (bijvoorbeeld ter voorbereiding op de verlenging van het Umbrella-certificaat), is het waarschijnlijk dat er een fout is gemaakt met het invoercertificaat.

Zorg ervoor dat zowel de huidige als de nieuwe overkoepelende certificaten worden geïmporteerd

Ter voorbereiding op certificaatvernieuwing stelt Umbrella een nieuw certificaat beschikbaar, maar het nieuwe certificaat wordt pas na afloop van de geldigheidsduur voor ondertekening gebruikt.

Daarom moet uw IdP-configuratie twee certificaten bevatten die zijn vermeld in de configuratie Serviceverlener / Vertrouwende partij. Configureer opnieuw vanuit [metagegevens](#) om dit op te lossen.

- Huidig certificaat - met een aankomende vervaldatum
- Toekomstig certificaat - dat geldig is voor het volgende jaar.

Zorg ervoor dat de attribuutclaims-map juist is

Als u de Serviceverlener / Vertrouwende partij opnieuw hebt geconfigureerd, moet u aanvullende configuratiewijzigingen aanbrengen om ervoor te zorgen dat de IdP de attributen verzendt die we nodig hebben om de SAML-reactie te valideren. Dit komt vaak voor bij Microsoft ADFS waarbij onze claimkaart opnieuw moet worden gemaakt.

Scenario 2 - Fout na verlopen paraplucertificaat

Als de fout optreedt nadat het Umbrella-certificaat is verlopen en er geen wijzigingen in de IdP zijn aangebracht.

Controleer of het nieuwe certificaat is geïmporteerd in de Identity Provider

Om het probleem op te lossen Importeer het nieuwe certificaat handmatig in uw identiteitsprovider. Wanneer ons certificaat de verlenging nadert, wordt het nieuwe certificaat beschikbaar gesteld in onze aankondigingsportal.

(AANBEVOLEN) Automatische metagegevensupdates configureren

Umbrella biedt nu een vaste metadata-URL die kan worden gebruikt voor naadloze metadata-updates. We raden u aan deze methode te configureren om handmatige actie tijdens de volgende certificaatrollover te voorkomen.

Ervoor zorgen dat de adressen van de CRL-server (Certificate Revocation List) toegankelijk zijn voor de Identity Provider

Umbrella maakt nu gebruik van een andere certificeringsinstantie, zodat deze CRL/OCSP-adressen beschikbaar zijn voor de IdP-server:

- <http://validation.identrust.com>
- <http://commercial.ocsp.identrust.com>

Microsoft ADFS - Voorbeeld van handmatig importeren van certificaten

Microsoft ADFS is een populaire IdP waarvan bekend is dat het aanvragen van handtekeningen valideert. Het certificaat kan als volgt worden bijgewerkt:

- Open AD FS-beheer
- Breid Relying Party Trusts uit en zoek de RP voor Umbrella SWG
- Rechtsklik op de vertrouwende partij in ADFS en selecteer Eigenschappen
- Upload het nieuwe certificaat op het tabblad Ondertekening

SWG Properties
✕

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Claims

Specify the signature verification certificates for requests from this relying party.

Subject	Expiration Date
Current Umbrella Certificate	Date
Future Umbrella Certificate	Date

Check Expiration Dates

Add..
View...
Remove...

OK
Cancel
Apply

Bij het naderen van de vervaldatum van het certificaat bevatten de door Cisco verstrekte metagegevens meerdere certificaten om zich voor te bereiden op een naadloze rollover. Verwijder het huidige certificaat niet zolang het nog geldig is. Cisco blijft ondertekenen met het huidige certificaat tot de vervaldatum/tijd.

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.