Cisco Secure Access - SAML-certificaatvernieuwing met IDP (Microsoft Entra ID)

Inhoud

uitgeven

Wanneer SSO-verificatie wordt gebruikt met Microsoft Entra ID SAML als Identity Provider (IdP) voor Cisco Secure Access, lopen SAML-verificatiecertificaten bijna af.

Organisaties moeten het juiste proces voor het vernieuwen van certificaten begrijpen om verificatieonderbrekingen te voorkomen en te bepalen of een nieuwe Single Sign On-configuratie moet worden gemaakt in Secure Access bij het vernieuwen van Entra ID SAML-certificaten.

milieu

- Cisco Secure Access met SSO-verificatie geconfigureerd
- Microsoft Entra ID SAML als Identity Provider
- SAML-verificatiecertificaten met aankomende vervaldata
- Bestaande SSO-configuratie voor SWG (Secure Web Gateway) en ZTNA (Zero Trust Network Access)

resolutie

Stap 1 – Certificaatvernieuwing detecteren

- Identity Provider (IdP) vernieuwt of roteert het SAML-ondertekeningscertificaat.

- Dit gebeurt meestal wanneer het certificaat de vervaldatum nadert.

Stap 2 – Bijgewerkte IDp-metagegevens verkrijgen

- Exporteer de nieuwe IdP-metagegevens XML of het nieuwe ondertekeningscertificaat vanuit de IdP.

Stap 3 – Certificaatwijziging controleren

Bevestig dat het certificaat daadwerkelijk is gewijzigd.

Controleren:

- vingerafdruk
- Vervaldatum
- uitgever

Dit zorgt ervoor dat de SP wordt bijgewerkt met het juiste certificaat

Configuratie van serviceprovider bijwerken

Meld u aan bij het Cisco Secure Access Dashboard en werk de configuratie bij.

Navigeer naar Verbinden - Gebruikers en groepen.

Klik op Configuratiebeheer

Onder SSO-verificatie - Bewerk het SSO-verificatieprofiel - uploadt u het metagegevensbestand met een nieuw certificaat of uploadt u het certificaat als u handmatig configureert.

Stap 5 – Configuratie opslaan en toepassen

- De bijgewerkte configuratie opslaan

Stap 6 – SSO-verificatie valideren

Voer een SSO-inlogtest uit.

Oorzaak

Het identiteitscertificaat van de identiteitsleverancier (Identity Provider, IdP) wordt door de Serviceverlener gebruikt om de SAML-handtekening te verifiëren en wanneer de IdP het certificaat verlengt, moet de SP zijn vertrouwde certificaat bijwerken om de authenticatieverzoeken te blijven valideren

Verwante inhoud

- Cisco Secure Access – SAML Single Sign-On Overzicht en configuratie
- SAML SSO configureren voor Cisco Secure Access (voorbeeld Microsoft Entra ID)
- 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.