VPNaaS SAML-verificatie mislukt met " decodering van relaystatus mislukt" fout met Duo IdP

Inhoud

uitgeven

Wanneer u probeert een VPNaaS-verbinding tot stand te brengen met behulp van Secure Client Remote Access met SAML-verificatie en Duo als Identity Provider (IdP), wordt deze fout waargenomen:

- Er is een fout opgetreden bij het verwerken van de SSO-verificatieaanvraag. Neem contact op met de systeembeheerder
- Decodering van relaisstaat mislukt

Verificatie met dezelfde IdP- en Duo-configuratie werkt met succes voor ZTNA (Zero Trust Network Access), maar mislukt voor VPN-verbindingen. Er zijn twee afzonderlijke toepassingen geconfigureerd in Duo voor ZTNA en VPN, beide met dezelfde IdP.

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- Subtechnologie: Veilige toegang - Veilige externe toegang voor clients (VPN, houding, persoonlijke bronnen)
- Verificatiemethode: SAML met Duo IdP
- Twee Duo-toepassingen geconfigureerd: één voor ZTNA, één voor VPN
- Authenticatie werkt voor ZTNA, mislukt voor VPN
- Softwareversie: ALLE
- Geen recente wijzigingen in de hardware-/softwareversie opgegeven

resolutie

Het probleem werd opgelost door de configuratie van de Entity ID en Assertion Consumer Service (ACS) URL op de Duo applicatie voor VPN te corrigeren. De juiste metagegevens werden gedownload van Secure Access en geüpload naar de VPN Duo-app, waardoor de SAML-relaystate-decoderingsfout werd opgelost.

1. Login op het CSA Dashboard. Ga naar Verbinden > Eindgebruikersconnectiviteit -> Virtuele privénetwerken. Bekijk het profiel waarmee u bent verbonden.
2. Klik op dat profiel en bewerk. Ga naar het tabblad Authenticatie.

3. Download de SAML-metagegevens voor veilige toegang.
4. Controleer entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml" en <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
5. Zorg ervoor dat entityID en AssertionConsumerService overeenkomen met de Duo-toepassing die is geconfigureerd voor VPN SSO-verificatie.

Oorzaak

Een verkeerde configuratie van de Entiteit-ID en ACS-URL op de Duo VPN-toepassing resulteerde in de SAML-relaystate-decoderingsfout. De juiste configuratie was niet aanwezig in Duo for VPN, hoewel ZTNA-verificatie met dezelfde IdP werkte. Het bijwerken van de Duo VPN-toepassing met nauwkeurige metagegevens van Secure Access heeft het probleem opgelost.

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.