

Falla la autenticación SAML de VPNaaS con "Falla el descifrado del estado de retransmisión" Error al utilizar Duo IdP

Contenido

Problema

Cuando se intenta establecer una conexión VPNaaS utilizando Secure Client Remote Access con autenticación SAML y Duo como proveedor de identidad (IdP), se observa este error:

- Error al procesar la solicitud de autenticación de SSO. Póngase en contacto con el administrador del sistema
- Error al descifrar el estado de retransmisión

La autenticación con la misma configuración IdP y Duo funciona correctamente para ZTNA (acceso a red de confianza cero), pero falla para las conexiones VPN. Hay dos aplicaciones separadas configuradas en Duo para ZTNA y VPN, ambas con el mismo IdP.

Entorno

- Tecnología: Asistencia para soluciones (SSPT, contrato necesario)
- Subtecnología: Acceso seguro: acceso remoto seguro con cliente (VPN, estado, recurso privado)
- método de autenticación: SAML con Duo IdP
- Dos aplicaciones Duo configuradas: uno para ZTNA, otro para VPN
- La autenticación funciona para ZTNA, falla para VPN
- Versión del software: ALL
- No se han especificado cambios recientes en la versión de hardware/software

Resolución

El problema se resolvió al corregir la configuración de la URL de Entity ID y Assertion Consumer Service (ACS) en la aplicación Duo para VPN. Los metadatos correctos se descargaron de Secure Access y se cargaron en la aplicación VPN Duo, lo que resolvió el error de descifrado del estado de retransmisión SAML.

1. Inicie sesión en el panel de CSA. Vaya a Conexión > Conectividad del usuario final -> Redes privadas virtuales. Descubra el perfil al que está conectado.
2. Haga clic en ese perfil y edite. Vaya a la pestaña Authentication.
3. Descargue los metadatos SAML para Secure Access.

4. Compruebe entityID="<https://X.vpn.sse.cisco.com/saml/sp/metadata/saml>" y
<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?tname=ProfileName>"></AssertionCo
5. Asegúrese de que entityID y AssertionConsumerService coincidan con la aplicación Duo configurada para la autenticación SSO de VPN.

Causa

La configuración incorrecta del ID de entidad y la URL ACS en la aplicación Duo VPN dio lugar a la falla de descifrado del estado de retransmisión SAML. La configuración correcta no estaba presente en Duo para VPN, a pesar de que la autenticación ZTNA funcionaba con el mismo IdP. La actualización de la aplicación Duo VPN con metadatos precisos de Secure Access resolvió el problema.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).