VPNaaS SAML身份验证失败(")中继状态解密失败(")使用Duo IdP时出错

目录

问题

尝试使用具有SAML身份验证的安全客户端远程访问并将Duo用作身份提供程序(IdP)来建立VPNaaS连接时，观察到以下错误：

- 处理SSO身份验证请求时失败。请与系统管理员联系
- 解密中继状态失败

使用相同IdP和Duo配置的身份验证在ZTNA（零信任网络访问）中成功运行，但在VPN连接中失败。在Duo中为ZTNA和VPN配置了两个不同的应用程序，它们都使用相同的IdP。

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问 — 安全客户端远程访问（VPN、状态、专用资源）
- 认证方法:具有Duo IdP的SAML
- 配置了两个Duo应用程序：一个用于ZTNA，一个用于VPN
- 身份验证适用于ZTNA，对VPN失败
- 软件版本:全部
- 未指定最近的硬件/软件版本更改

分辨率

通过更正Duo应用程序上用于VPN的实体ID和声明使用者服务(ACS)URL的配置，解决了此问题。从Secure Access下载了正确的元数据并上传到VPN Duo应用程序，从而解决了SAML中继状态解密错误。

1. 登录到CSA仪表板。转到连接>终端用户连接 — >虚拟专用网络。找出您连接的配置文件。
2. 单击Profile 和Edit。转到Authentication 选项卡。
3. 下载用于安全访问的SAML元数据。
4. 检查entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml"和<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. 确保entityID和AssertionConsumerService与为VPN SSO身份验证配置的Duo应用相匹配。

原因

Duo VPN应用上的实体ID和ACS URL配置错误导致SAML中继状态解密失败。Duo for VPN中不存在正确的配置，即使ZTNA身份验证使用同一IdP也是如此。使用来自Secure Access的准确元数据更新Duo VPN应用程序解决了此问题。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。