在思科安全访问中具有个人Google帐户的访客用户的ZTNA注册失败

目录

问题

在使用ZTNA（零信任网络访问）部署私有访问期间，在Entra ID中成功注册并在安全访问中进行调配后，使用个人Google帐户的访客用户注册失败。遇到的特定症状包括：

- 基于客户端的注册:注册过程达到SSO身份验证，提供凭证，但ZTNA显示“I/O错误”，且注册过程停滞
- 无客户端访问:返回错误消息“Cisco Secure Access Login failure.检查IDP配置”以及事务ID

这些故障会阻止对私有资源的访问，并影响对使用非公司身份的承包商式访问的ZTNA功能的测试。

环境

- 采用ZTNA部署的思科安全访问
- 作为身份提供程序的Microsoft Entra ID（以前称为Azure AD）
- 在Entra ID中注册为访客用户的个人Google帐户(@gmail.com)
- 访客帐户已调配并在安全访问中可见
- 在Entra ID和思科安全访问之间配置SAML身份验证

分辨率

通过修改Microsoft Entra ID中的SAML属性映射配置解决了注册失败。为了解决这一问题，采取了以下步骤：

步骤 1：分析DART捆绑包和客户端行为

查看DART捆绑包，确认Cisco安全客户端和ZTA组件正常运行。分析应验证注册流是否成功到达思科安全访问，以及是否在与身份提供程序进行SAML身份验证期间发生故障。

步骤 2：检查Entra ID身份验证日志

检查Entra ID身份验证日志，确认身份验证过程从身份提供程序角度成功完成。日志应显示身份验证成功，但安全访问因属性不匹配而拒绝登录。

步骤 3：确定SAML属性映射问题

确定Entra ID颁发UPN（用户主体名称）作为SAML声明，该声明与Secure Access预期的个人Gmail帐户身份不匹配。断言的IdP属性与预期的用户标识符不一致。

步骤 4：修改SAML属性映射

将Microsoft Entra ID中的SAML属性映射从UPN更改为Email Address。这可确保电子邮件地址声明与个人Google帐户身份匹配。

步骤 5：验证注册成功

在实施属性映射更改后，请重试ZTNA注册过程。Cisco Secure Access ZTA现在应能识别Gmail地址并允许成功完成注册。

原因

注册失败是由于Microsoft Entra ID声明的SAML属性与Cisco安全访问中的预期用户标识符之间不匹

配。Entra ID配置为将UPN（用户主体名称）作为SAML声明发送，但对于个人Google帐户(@gmail.com)，此UPN与实际的电子邮件地址标识不一致。思科安全访问预计接收邮件地址作为标识属性，以匹配已调配的访客用户帐户，导致身份验证被拒绝，尽管IdP身份验证成功。

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）。