思科安全访问 — 使用IDP的SAML证书续订 (Microsoft Entra ID)

目录

问题

将SSO身份验证与Microsoft Entra ID SAML用作思科安全访问的身份提供程序(IdP)时，SAML验证证书即将到期。

组织需要了解正确的证书续订流程，以避免身份验证中断，并确定续订Entra ID SAML证书时，是否必须在安全访问中创建新的单点登录配置。

环境

- 配置了SSO身份验证的思科安全访问
- 作为身份提供程序的Microsoft Entra ID SAML
- 具有即将到期日期的SAML验证证书
- SWG（安全网络网关）和ZTNA（零信任网络访问）的现有SSO配置

分辨率

第1步 — 检测证书续订

- 身份提供程序(IdP)更新或轮换其SAML签名证书。
- 当证书接近到期时，通常会发生这种情况。

第2步 — 获取更新的IdP元数据

- 从IdP导出新IdP元数据XML或新签名证书。

第3步 — 检验证书更改

确认证书已实际更改。

检查：

- 指纹
- 到期日期
- 签发方

这样可以确保SP使用正确的证书进行更新

更新服务提供商配置

登录到Cisco Secure Access Dashboard并更新配置。

导航至Connect - User and Groups。

点击Configuration Management

在SSO Authentication - Edit the SSO Authentication Profile下 — 使用新证书上传元数据文件，或上传证书（如果手动配置）。

第5步 — 保存并应用配置

- 保存更新的配置

第6步 — 验证SSO身份验证

执行SSO登录测试。

原因

服务提供程序使用身份提供程序(IdP)签名证书验证SAML断言签名，当IdP更新证书时，SP必须更新其受信任证书以继续验证身份验证请求

相关内容

- 思科安全访问 — SAML单点登录概述和配置
- 为思科安全访问配置SAML SSO（Microsoft Entra ID示例）
- 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）。