对显示带有EntraID的空白白屏的安全访问基于浏览器的SAML身份验证进行故障排除

目录

问题

当配置思科安全访问以在未安装思科安全客户端的设备上强制进行基于浏览器的SAML身份验证时，身份验证过程重定向到空白的白色屏幕，而不是显示EntraID身份验证页面。此问题专门发生在Microsoft Edge正常（非InPrivate）模式和Google Chrome浏览器中。使用Edge InPrivate模式时，身份验证工作正常。SAML身份验证配置文件同时启用了解密和SSO身份验证。

配置的策略结构包括：

- 允许身份验证后用户的策略。(来源：任何用户，目标：any)
- 允许使用SAML身份验证配置文件的SAML身份验证策略。(来源：终端IP，目标：0.0.0.0(TCP 80,443)
- 允许使用SAML身份验证配置文件的SAML身份验证帮助程序策略。(来源：终端IP，目标：any)
- 阻止策略。(来源：终端IP，目标：any)

环境

- 思科安全接入（Internet接入模块）
- EntraID作为身份提供程序(IdP)
- 基于浏览器的SAML身份验证，适用于没有思科安全客户端的设备
- 启用解密和SSO身份验证的SAML身份验证配置文件
- Microsoft Edge和Google Chrome浏览器

分辨率

通过将特定的EntraID相关域添加到SAML身份验证配置文件配置中的解密排除列表可以解决此问题。这可防止SSL/TLS解密进程干扰EntraID身份验证流程。

步骤 1：将EntraID域添加到解密排除列表

在SAML身份验证配置文件的解密排除列表中配置以下四个EntraID域：

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

步骤 2：将配置应用于SAML策略

确保解密排除设置同时应用于以下两者：

- 允许SAML身份验证策略。(来源：终端IP，目标：0.0.0.0(TCP 80,443)
- 允许SAML身份验证助手策略。(来源：终端IP，目标：any)

步骤 3：检验分辨率

应用解密排除配置后，测试身份验证流程：

- Microsoft Edge（正常模式）：可以成功重定向到EntraID身份验证页面。
- Google Chrome:可以成功重定向到EntraID身份验证页面。
- 两种浏览器都可以一致地显示EntraID身份验证输入屏幕。

原因

出现空白白屏的原因是，当对SAML身份验证配置文件启用解密时，思科安全访问中的SSL/TLS解密过程会干扰EntraID身份验证流程。解密过程会中断浏览器和EntraID身份验证服务器之间的安全通信，导致身份验证页面无法正确加载。InPrivate模式工作正常，因为它以不同方式处理SSL/TLS会话，从而绕过解密干扰。将EntraID域添加到解密排除列表允许身份验证流量在不解密的情况下通过，从而保持安全身份验证流的完整性。

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）。