在SWA中配置Kerberos单点登录身份验证

目录

简介

本文档介绍在安全网络设备(SWA)中通过Kerberos将代理用户配置为具有单点登录(SSO)身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。
- 基本Active Directory管理。

思科建议您安装以下工具：

- 物理或虚拟SWA。

- 对SWA图形用户界面(GUI)的管理访问。
- 对Active Directory的管理访问。

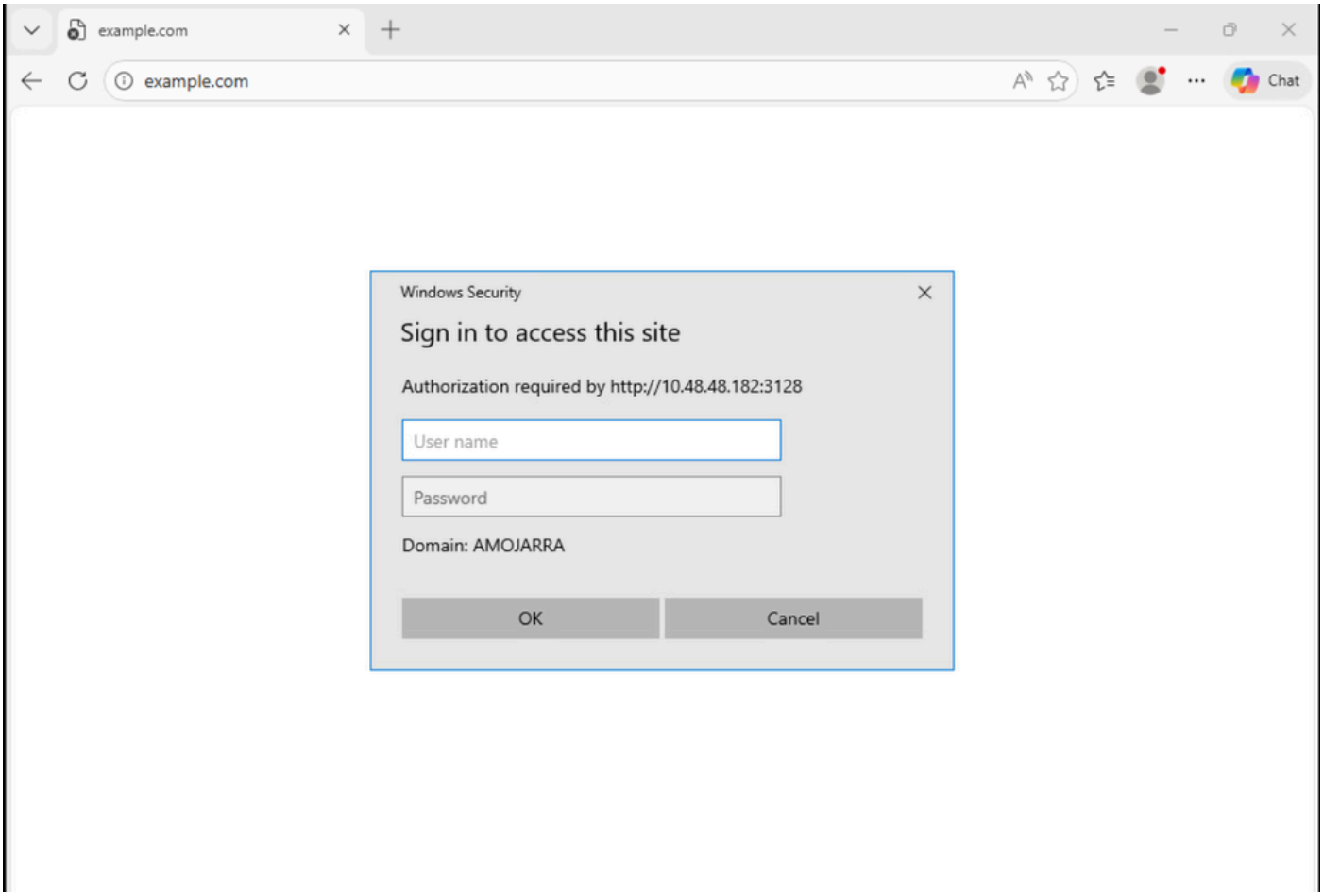
使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

如果代理客户端尝试访问网站并提示手动输入凭证，请使用以下步骤进行故障排除。



图像 — 用户身份验证提示

步骤1.检查与客户端相关的Acesslogs。

步骤1.1.登录到CLI。

步骤1.2.运行grep。

第1.3步：选择与关联的号码。访问日志。

第1.4步：在Enter the regular expression to grep中，键入客户端IP地址。

第1.5步：按Enter，直到您看到Do you want to tail the logs，键入“Y”并按Enter直到您看到Accesslogs。

步骤1.6.尝试从客户端PC访问任何网站以重现问题。

第1.7步：确认标识配置文件流量即将命中。

在本示例中，标识配置文件是Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

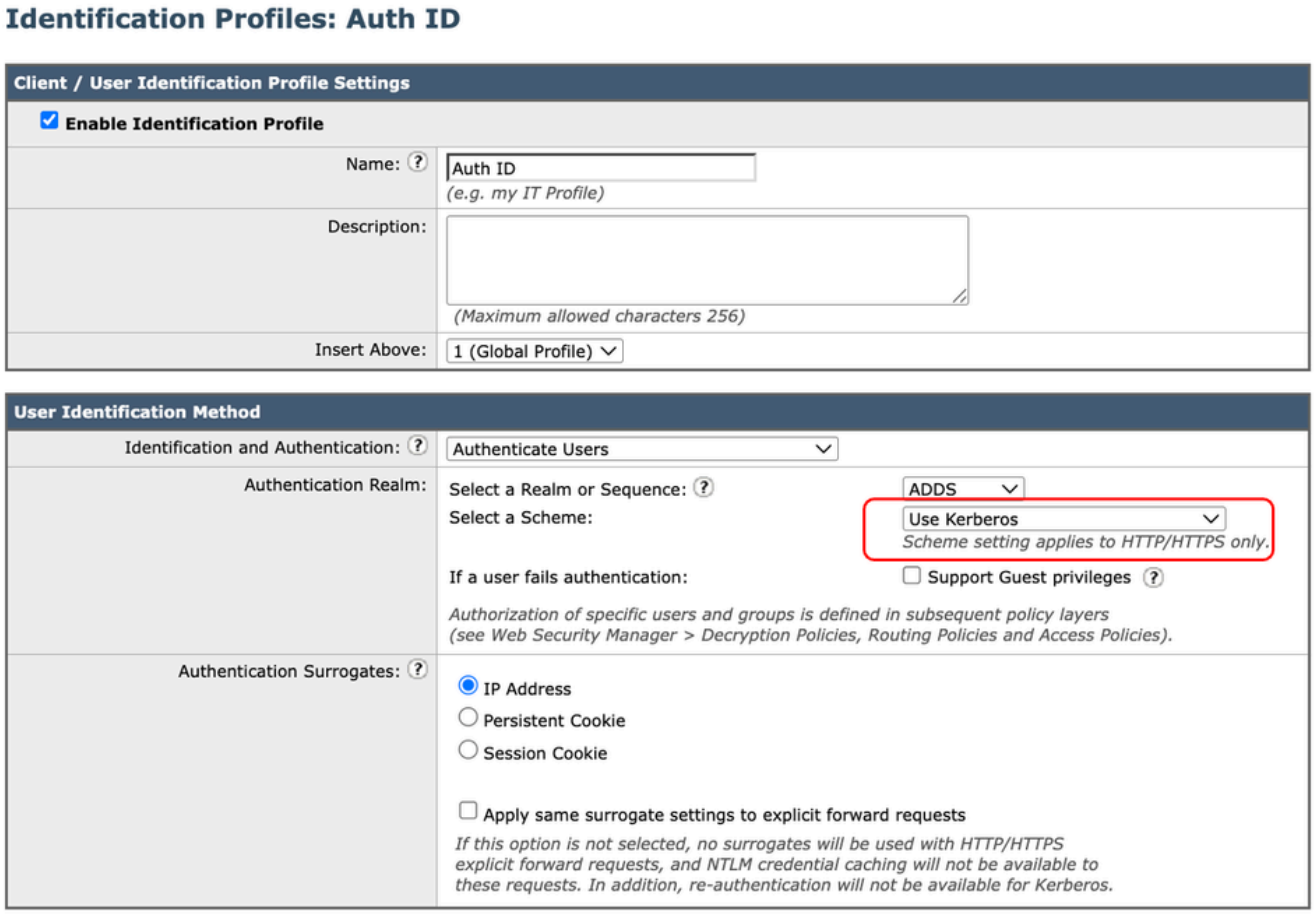
步骤2.检查标识配置文件。

第2.1步：登录到SWA的GUI。

第2.2步：从网络安全管理器，选择Identification Profiles。

第2.3步：点击流量命中时的标识配置文件的名称。

步骤2.4.确认身份验证方案未设置为基本。



图像 — 身份验证方案

步骤3.测试SWA和Active Directory连接。

第3.1步：从SWA GUI导航到网络并选择身份验证。

第3.2步：点击身份验证领域名称。

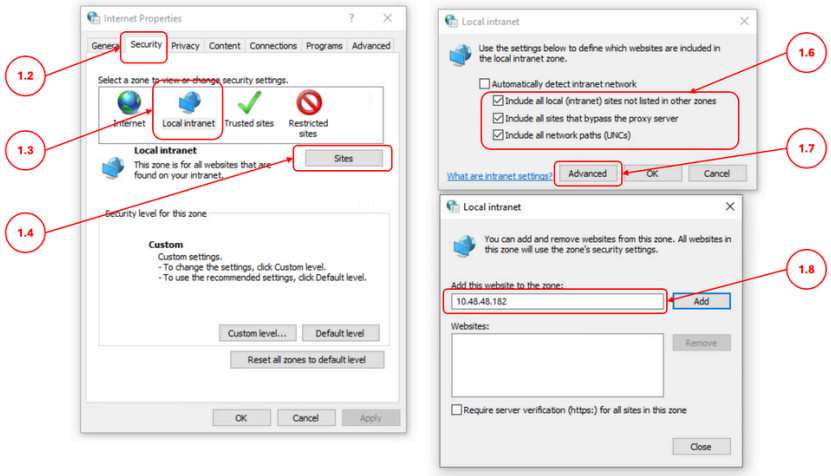
第3.3步：单击开始测试以查看SWA和Active directory连接状态。

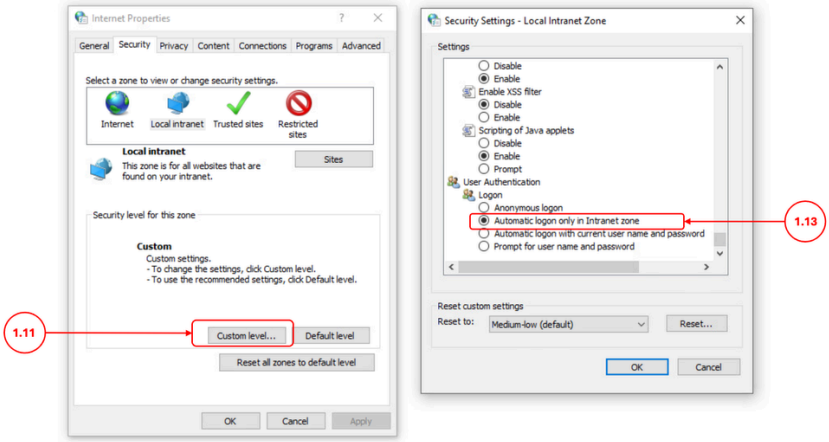
如果未发现错误，请验证客户端PC配置（如本文所述）。

配置客户端PC

使用以下步骤验证客户端PC配置：

步骤	详细信息

步骤1.本地内部网站点	第1.1步：在开始菜单中，键入Internet Option，然后按Enter键。 第1.2步：在“Internet属性”窗口中，单击“安全”选项卡。 第1.3步：选择本地Intranet。 步骤1.4.点击Sites。 步骤1.5.确保未选中Automatically detect intranet network复选框。 第1.6步：选择以下三个选项： • 包括未在其他区域中列出的所有本地（内部网）站点 • 包括绕过代理服务器的所有站点 • 包括所有网络路径(UNC) 第1.7步。单击高级。 第1.8步：输入SWA的FQDN或IP地址并添加到列表中。 第1.9步(可选)根据您的内部安全策略，您可以禁用Require Server Verification。  图像 — 配置本地Internet站点 第1.10步。单击Close和OK。 第1.11步：在Security选项卡中，点击Custom level。 步骤1.12.滚动到User Authentication。 步骤1.13.确保选中Automatic logon only in Intranet zone。

	 图像 — Intranet用户的自动登录
步骤2.收集日志	如果步骤1，则未通过Kerberos修复SSO身份验证： 第2.1步：将SWA身份验证日志更改为跟踪并检查日志。 第2.2步：将[Auth-Method = %m]作为自定义字段添加到访问日志中。有关更多信息，请访问：在访问日志中配置性能参数。 步骤2.3.运行客户端IP和Active Directory IP地址的数据包捕获过滤器，并确认客户端PC正在向SWA发送Kerberos服务票证。

注意：确保在浏览器代理设置中配置了SWA的FQDN。

相关信息

- 思科安全Web设备AsyncOS 15.0用户指南
- 为安全Web设备配置防火墙
- 在内容安全设备上配置数据包捕获
- 配置访问日志中的性能参数
- 访问安全Web设备日志
- 使用安全Web设备最佳实践 — 思科
- 绕过安全Web设备中的身份验证 — 思科

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）。