利用Umbrella的固定元数据URL进行SWG SAML身份验证

目录

简介

本文档介绍如何利用Umbrella的固定元数据URL进行安全Web网关(SWG)SAML身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella SWG。

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。

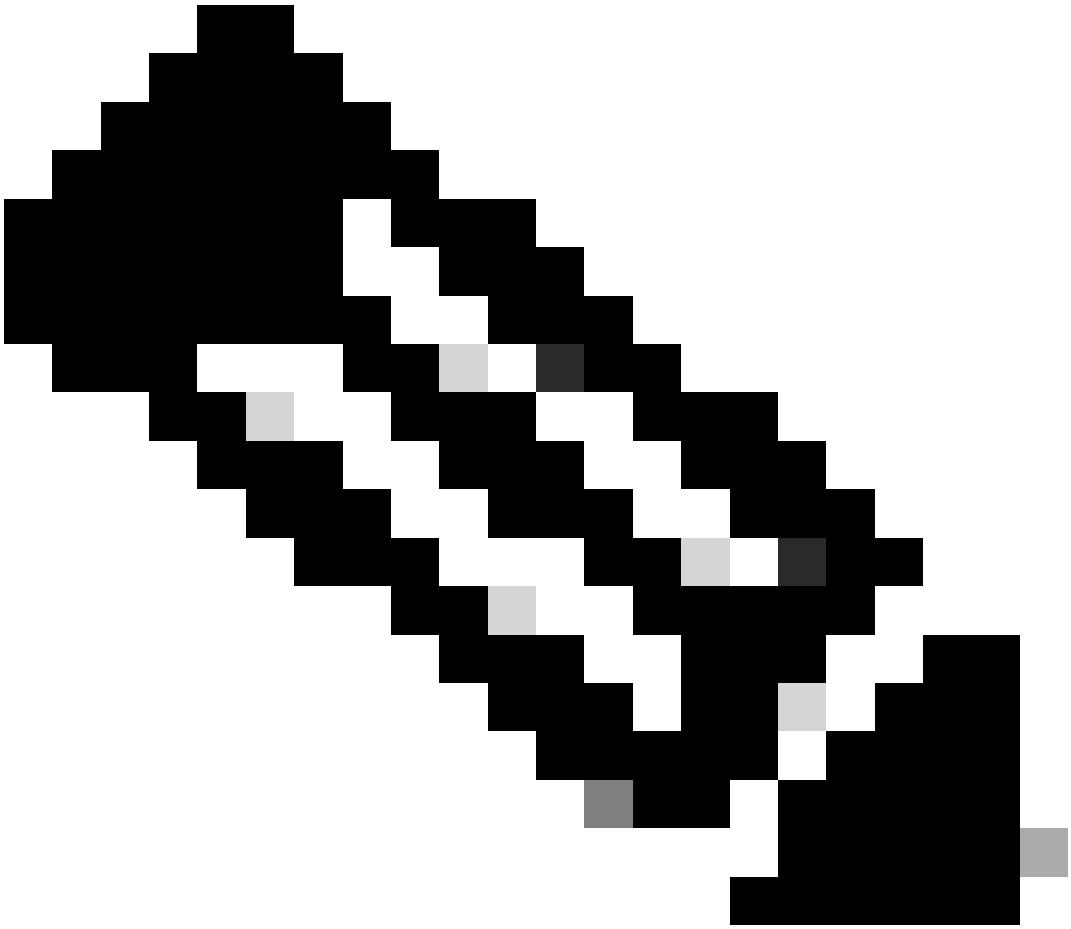
固定元数据URL

当对Umbrella SWG使用SAML身份验证时，我们提供两个选项，用于将我们的证书信息导入到您的身份提供程序(IdP)中。 对于验证请求签名证书的IdP，这是必需的。

1. 通过固定元数据URL进行自动配置：https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml
2. 手动导入我们的新签名证书。在替换证书时，需要每年执行此操作。

第一个选项现在是支持基于URL的元数据自动更新的身份提供程序(IdP)的首选配置方法。这包括常用的IdP，例如Microsoft ADFS和Ping身份。 其优势在于，IdP每年自动导入我们的新证书，无需人

工干预。



注意：许多IDP不执行SAML请求签名的验证，因此这些步骤不是必需的。 如有疑问，请联系您的身份提供商供应商进行确认。

要求

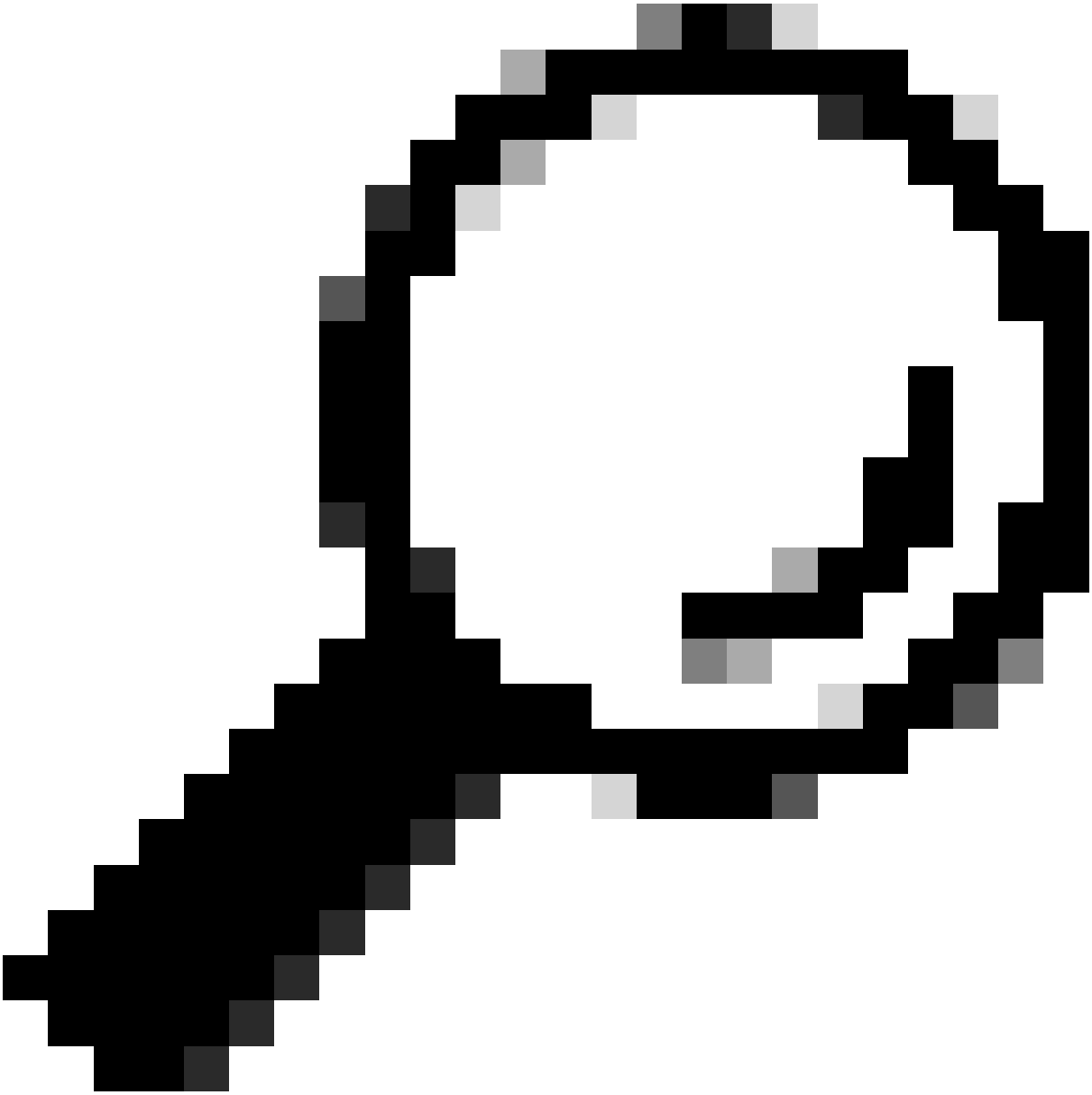
访问元数据URL的要求

- 支持从URL自动更新服务提供程序元数据（例如ADFS、Ping）的IdP
- 您的IdP平台必须能够访问我们的元数据URL以及关联的证书颁发机构URL
- 您的IdP平台还必须能够访问证书本身的证书颁发机构URL
- 您的IdP平台必须支持TLS 1.2，才能安全地连接到元数据URL。如果IDP应用程序使用.NET framework 4.6.1或更低版本，可能需要根据Microsoft文档进行一些进一步配置。

示例：Microsoft ADFS

可以通过编辑Umbrella的信赖方信任设置来配置固定元数据URL:

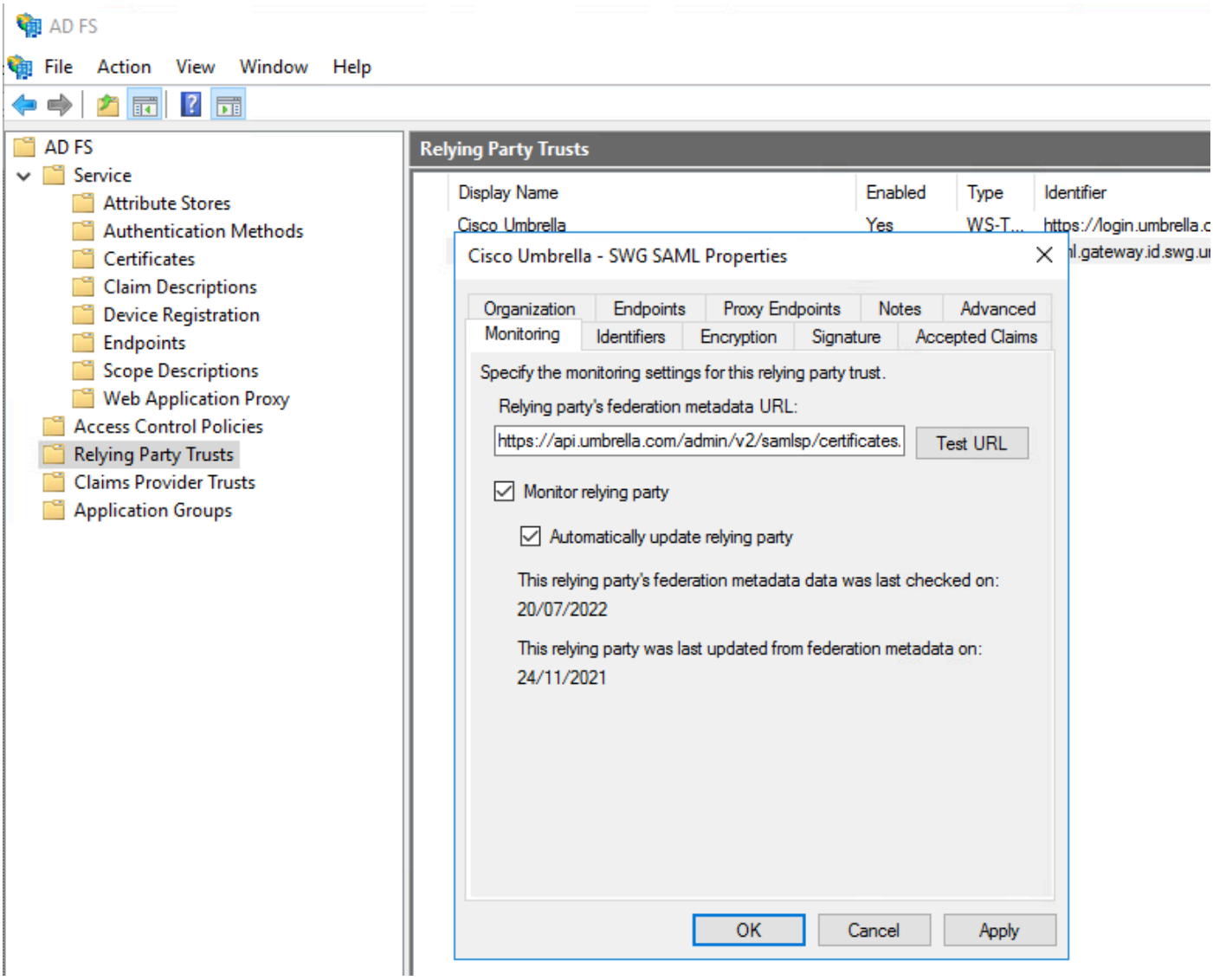
1. 导航到Monitoring选项卡并输入元数据URL。
2. 选择监控信赖方和自动更新信赖方。



提示：选择测试URL按钮以验证ADFS是否成功联系了URL。

---

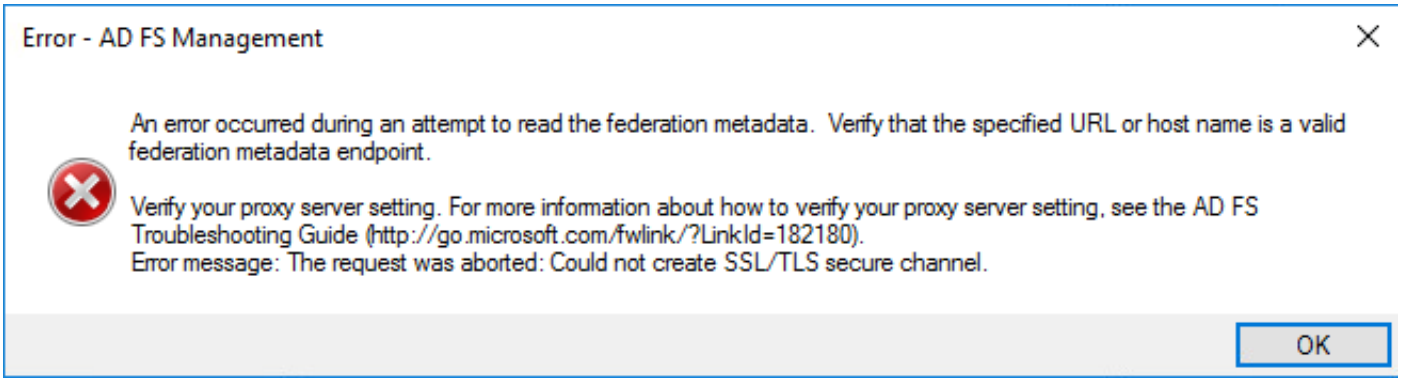
3. 选择Apply。



ADFS_RelyingPartyTrust.png

故障排除错误

如果收到错误消息“An error occurred during to read the federation metadata.测试URL时，验证指定的URL或主机名是否是有效的联合元数据终结点“，这通常表示需要更改注册表才能设置.NET Framework版本以使用强加密并支持TLS 1.2。



ADFS元数据_TLS_error.png

有关这些更改的完整详细信息由Microsoft发布在Microsoft文档的.Net Framework部分。

但是，通常这需要创建此密钥，然后关闭并重新打开ADFS管理控制台：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

限制:组织特定实体ID功能

如果使用Umbrella SAML Org-Specific EntityID功能，则不得使用基于URL的元数据更新机制。仅当多个伞状组织链接到同一身份提供者时，组织特定实体ID才适用。在这种情况下，您必须手动将证书添加到每个IDP配置。

手动证书导入（备选）

如果IdP不支持基于URL的更新，则必须每年手动将新的Umbrella请求签名证书导入到身份提供程序。

- 每年在到期日前不久，证书都会在我们的公告门户上提供。订阅通知门户
- 将新证书添加到IdP中的服务提供商/信赖方证书列表中。
  - 请勿删除任何当前证书。 Umbrella继续使用旧证书签名，直到到期为止。
- 如果您的IdP不包含导入服务提供商/信赖方证书的功能，则表明它不会验证SAML请求，并且无需进一步操作。 请与您的IdP供应商联系以确认。

如果在导入新证书后遇到“UPN is not configured”错误，则表示已发生错误。 请参阅本文进行故障排除：SWG SAML - UPN Not Configured错误

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）。