使用身份服务(IdS)排除CCE单点登录故障 — 证书管理

目录

简介

本文档介绍在UCCE/PCCE中重新生成和交换SAML证书的详细步骤，以确保安全、清晰的流程。

作者：Nagarajan Paramasivam，Cisco TAC工程师。

先决条件

要求

思科建议您了解以下主题：

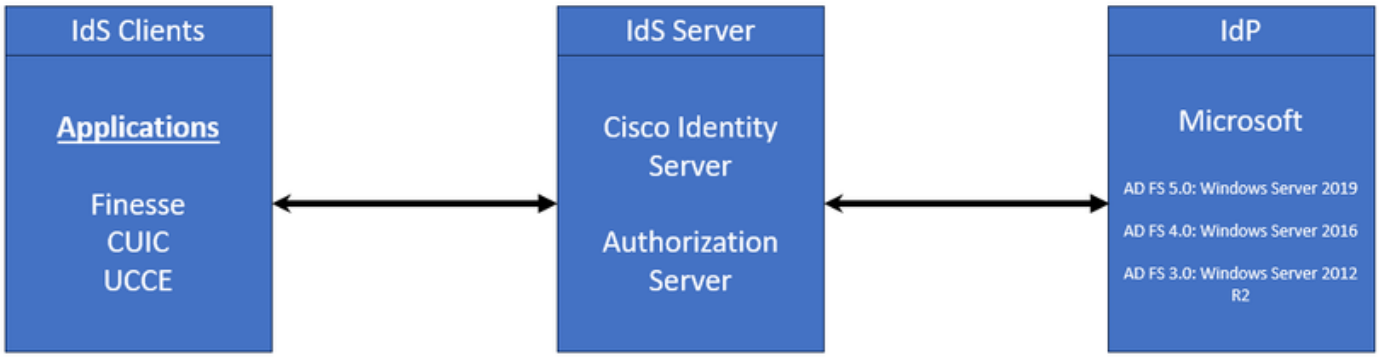
- 套装/统一联系中心企业版(PCCE/UCCE)
- 语音操作系统(VOS)平台
- 证书管理
- 安全断言标记语言(SAML)
- 安全套接字层 (SSL)

- Active Directory联合身份验证服务(AD FS)
- 单点登录(SSO)

使用的组件

本文档中的信息基于以下组件：

- 思科身份服务（思科Id）
- 身份提供程序(IdP)- Microsoft Windows ADFS



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。

背景信息

在UCCE/PCCE中，思科身份服务(Cisco IdS)提供身份提供商(IdP)和应用之间的授权。

配置思科IdS时，您可以在思科IdS和IdP之间设置元数据交换。此交换建立信任关系，然后允许应用使用思科ID进行SSO。您可以从Cisco IdS下载元数据文件并将其上传到IdP，从而建立信任关系。

SAML证书类似于SSL证书，当出现某些情况时，需要更新或更改它。在思科身份服务(IdS)服务器上重新生成或交换SAML证书时，可能导致与身份提供程序(IdP)的受信任连接中断。 此中断可能导致依靠单点登录的客户端或用户无法获得访问系统所需的授权的问题。

本文档旨在涵盖各种常见情况，在这些情况下，您必须在Cisco IdS服务器上创建新的SAML证书。它还说明如何将此新证书提供给身份提供程序(IdP)，以便重建信任。通过执行此操作，客户端和用户可继续使用单点登录，而不会出现任何问题。目标是确保您拥有顺利且无混淆地处理证书更新过程所需的所有信息。

需牢记的要点：

1. SAML证书默认在思科IdS服务器安装期间生成，有效期为3年

2. SAML证书是自签名证书

3. SAML证书是驻留在Cisco IDS发布者和用户上的SSL证书

4.只能在Cisco IDS Publisher节点中执行SAML证书重新生成

5.可用的SAML证书安全哈希算法类型是SHA-1和SHA-256

6. SHA-1算法用于IdS 11.6，而在早期版本中，SHA-256算法用于IdS 12.0及更高版本

7.身份提供程序(IdP)和身份服务(IdS)都必须使用相同的算法类型。

8.只能从Cisco IdS Publisher节点(sp-<Cisco IdS_FQDN>.xml)下载Cisco IdS SAML证书

9.请参阅此链接了解UCCE/PCCE单点登录配置。UCCE 12.6.1功能指南

SAML证书已过期

生成SAML证书的有效期为3年（1095天），到期前需要更新SAML证书。已过期的SSL证书被视为无效证书，它会破坏思科身份服务(IdS)和身份提供程序(IdP)之间的证书链。

解决方案

1.检查SAML证书到期日期

2.重新生成SAML证书

3.下载sp.xml文件

4.从sp.xml文件检索SAML证书

5.将旧的SAML证书替换为IdP中的新SAML证书

6.有关详细步骤，请参阅参考部分

(注意: {由于只更改了SAML证书，因此不需要将元数据交换到IdP})

身份提供程序(IdP)中的安全哈希算法更改

假设在采用单点登录的现有PCCE/UCCE环境中。IdP和思科IdS服务器均配置了SHA-1安全哈希算法。考虑到SHA-1的弱点需要将安全散列算法更改为SHA-256。

解决方案

1.更改AD FS信赖信任方中的安全哈希算法（SHA-1到SHA-256）

2.在IdS发布器中的“密钥和证书”（SHA-1到SHA-256）下更改安全散列算法

3.在IdS发布器中重新生成SAML证书

4.下载sp.xml文件

5.从sp.xml文件检索SAML证书

6.将旧的SAML证书替换为IdP中的新SAML证书

7.有关详细步骤，请参阅参考部分

Cisco IdS服务器IP地址或主机名更改 — 重建了共存的CUIC/LiveData/IdS发布服务器或独立IdS发布服务器 — 重建了共存的CUIC/LiveData/IdS订阅服务器或独立IdS订阅服务器

这些情况很少发生，强烈建议您重新开始单点登录(SSO)设置，以确保生产环境中的SSO功能得到快速而有效的恢复。必须优先执行此重新配置，以尽量减少对用户所依赖的SSO服务的任何中断。

解决方案

1.从AD FS中删除现有信赖方

2.上传Cisco IdS服务器tomcat trust中的AD FS SSL证书

3.下载sp.xml文件

4.有关详细步骤，请参阅《参考部分和功能指南》

5.在AD FS中配置信赖信任方

6.添加索赔规则

7.启用签名的SAML断言

8.下载AD FS联合元数据

9.将联合元数据上传到Cisco IdS服务器

10.执行测试SSO

参考

如何在ADFS或

如何启用已签名的SAML断言

有关详细步骤，请参阅本文档：UCCE 12.6.1功能指南

如何将AD FS SSL证书上传到Cisco IdS tomcat信任

1.下载或检索AD FS SSL证书

2.访问Cisco IdS Publisher OS Administration页面

3.使用操作系统管理员凭证登录

4.导航至“安全”>“证书管理”

5.点击“上传证书/证书链”，系统将显示弹出窗口

6.单击“下拉菜单”，然后在“证书用途”上选择tomcat-trust

7.单击“浏览”并选择AD FS SSL证书

8.单击“上传”

(注:{信任证书会复制到订阅服务器节点。您不需要上载到订阅服务器节点。})

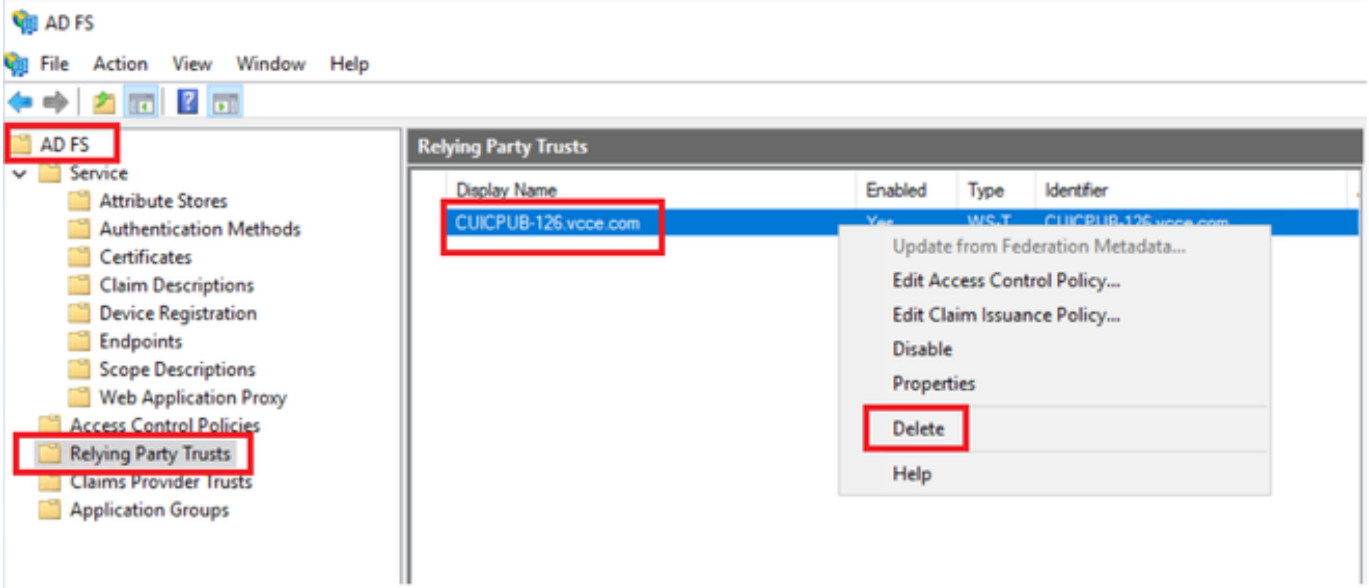
如何删除AD FS中的信赖方

1.使用管理员特权凭据登录到身份提供程序(IdP)服务器

2.打开服务器管理器，然后选择AD FS >工具> AD FS管理

3.在左侧树中，选择AD FS下的信赖方信任

4.右键单击Cisco IdS服务器并选择“删除”



如何检查或更改身份提供程序(IdP)中配置的安全哈希算法

1.使用管理员特权凭据登录到身份提供程序(IdP)服务器

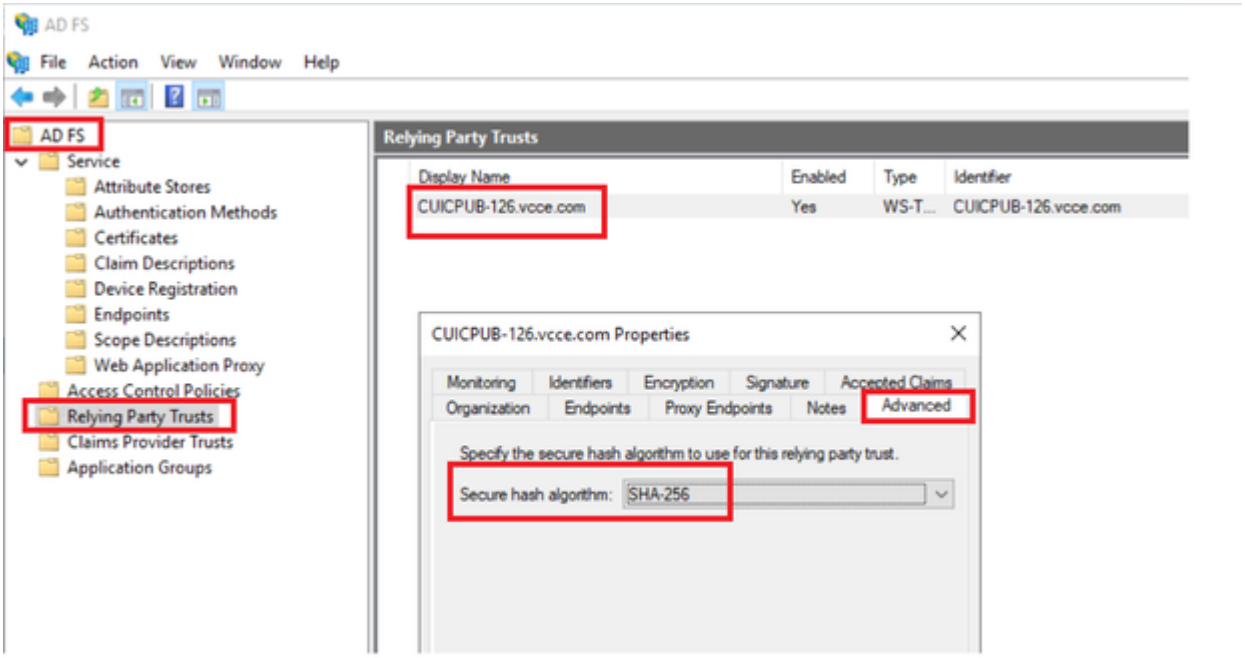
2.打开服务器管理器，然后选择AD FS >工具> AD FS管理

3.在左侧树中，选择AD FS下的信赖方信任

4.右键单击Cisco IdS服务器并选择属性

5.定位至“高级”标签

6.安全哈希算法选项显示AD FS服务器中配置的安全哈希算法。



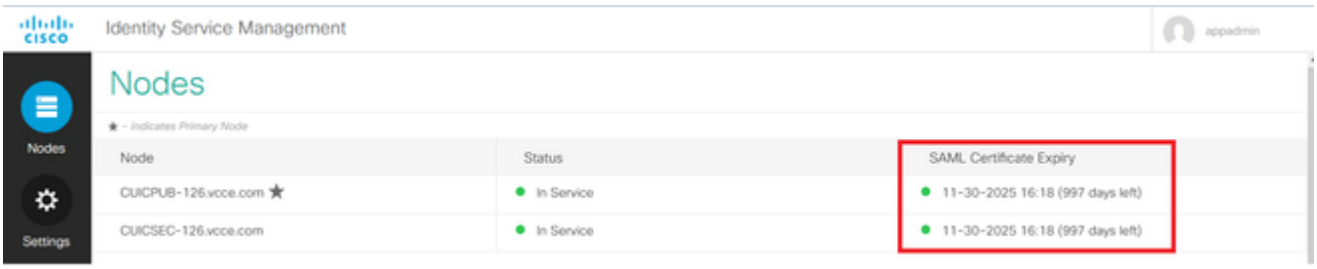
7.单击“下拉菜单”并选择所需的安全散列算法。

如何检查Cisco IdS服务器SAML证书到期日期

1.使用应用用户凭证登录到Cisco IdS服务器发布服务器或订用服务器节点

2.成功登录后，页面将转至“身份服务管理”>“节点”

3.显示Cisco IdS发布服务器和订用服务器节点、状态和SAML证书到期



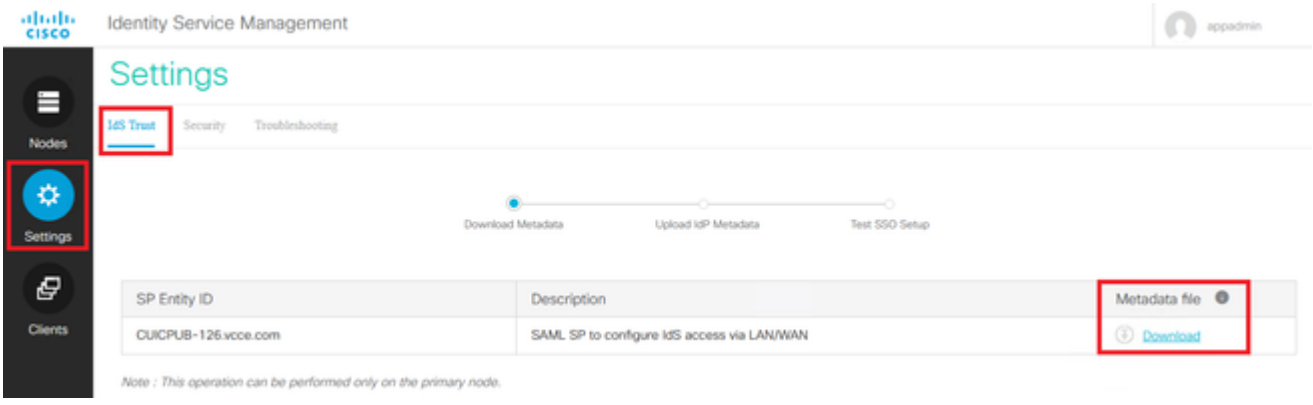
如何下载Cisco IdS服务器的元数据

1.使用应用用户凭证登录到Cisco IdS Publisher节点

2.单击设置图标

3.定位至“IDS信任”标签

4.点击“下载”链接以下载Cisco IdS集群的元数据



如何从sp.xml文件检索SAML证书

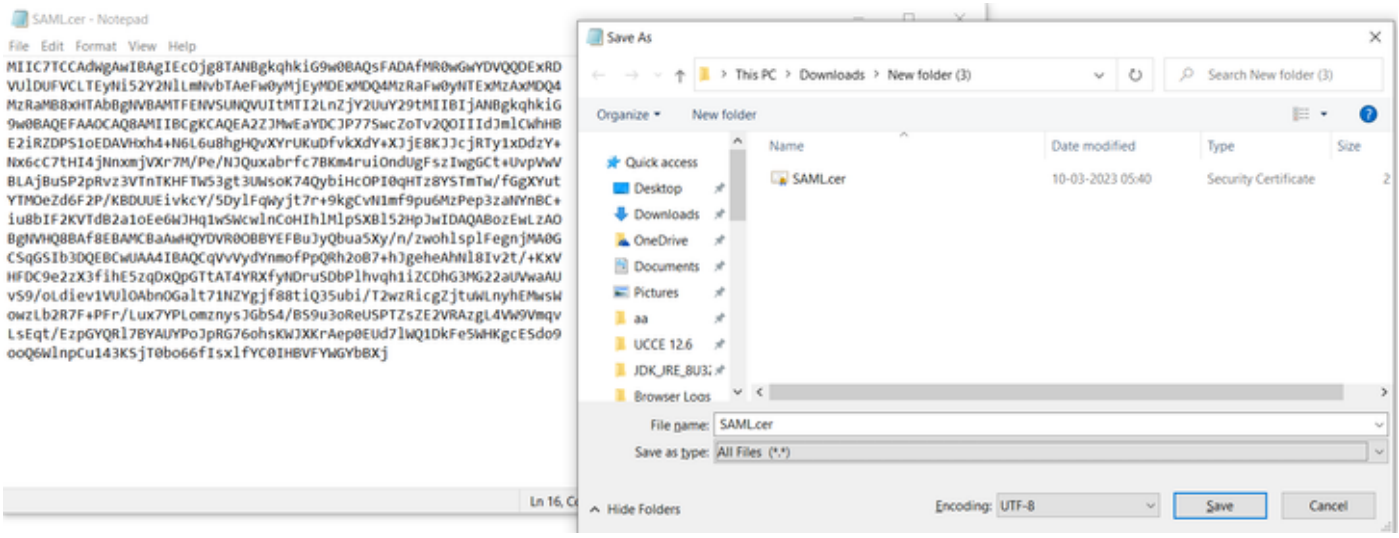
1.使用文本编辑器打开sp.xml文件

2.在信头<ds:X509Certificate></ds:X509Certificate>之间复制原始数据

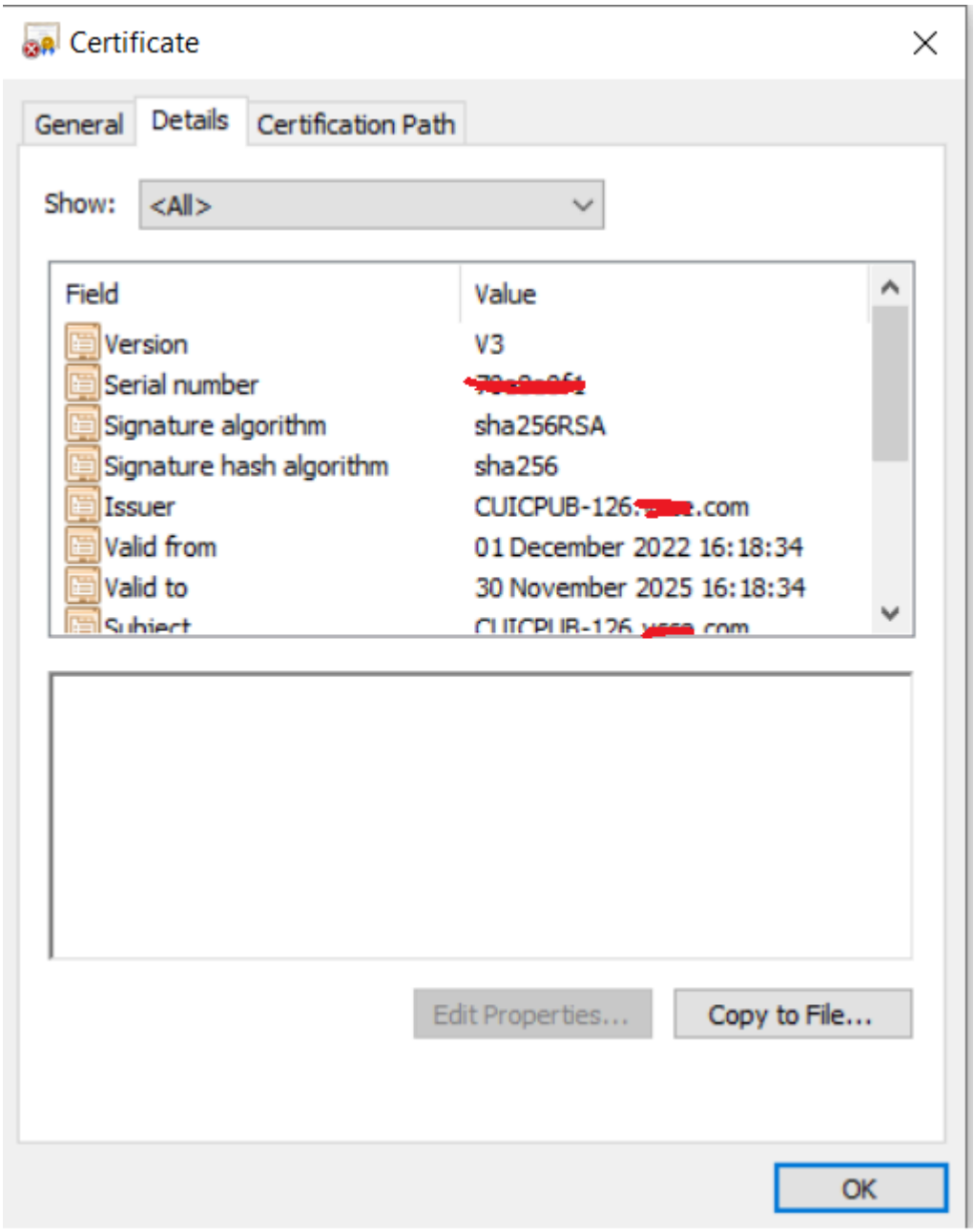
```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VUlDUFVCLTEyNi52Y2NlLmNvbTAeFw0yMjEyMDExMDQ4MzRaFw0yNTExMzAxMDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUItMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ZJMwEaYDCJP77SwcZoTv2QOIIIdJmlCWhHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJcjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabrfc7BKm4ruiOndUgFszIwgGCt+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyjt7r+9kgCvN1mf9pu6MzPep3zaNYnBC+
iu8bIF2KVTdB2a1oEe6WJHq1wSWcwlnCoHIhlMlpSXBl52HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBuJyQbua5Xy/n/zwohlsplFegnjMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhNl8Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGTtAT4YRXfyNDruSDbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdiev1VUlOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnyhEMwsW
owzLb2R7F+PFr/Lux7YPLomznysJGbS4/BS9u3oReUSPTZsZE2VRAzgL4VW9Vmqv
LsEqt/EzpGYQRl7BYAUYPoJpRG76ohsKWJXKrAep0EUd7lWQ1DkFe5WHKgcESdo9
ooQ6WlnpCu143KSjT0bo66fIsxlfYC0IHBVFYWGYbBXj</ds:X509Certificate>
```

3.打开另一个文本编辑器并粘贴复制的数据

4.保存文件.CER格式



5.打开证书以查看证书信息



如何替换AD FS中的SAML证书

1.将SAML证书文件复制到从sp.xml检索的AD FS服务器

2.打开服务器管理器，然后选择AD FS >工具> AD FS管理

3.在左侧树中，选择AD FS下的信赖方信任

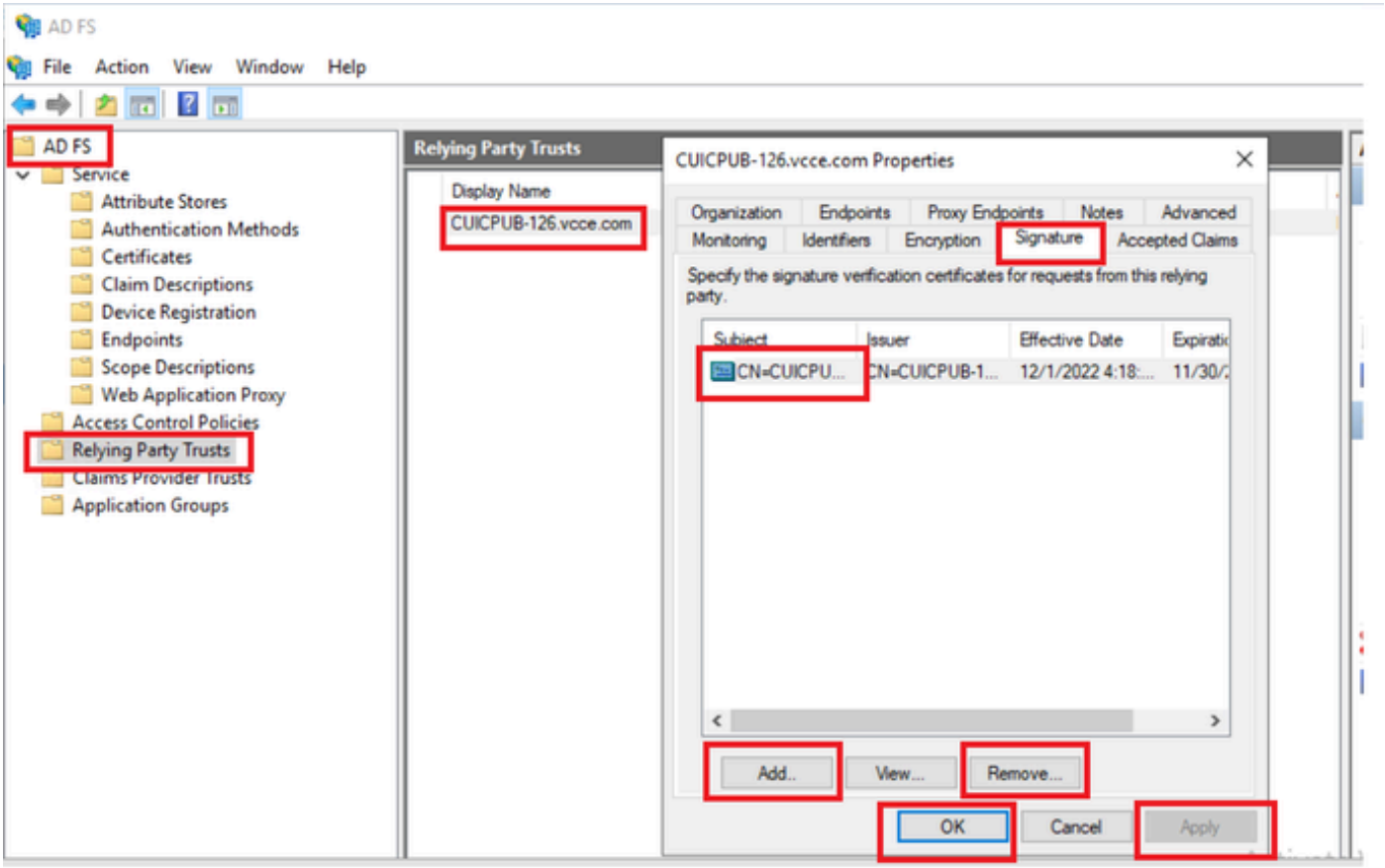
4.右键单击Cisco IdS服务器并选择属性

5.定位至“签名”标签

6.点击Add并选择新生成的SAML证书

7.选择旧SAML证书，然后单击“删除”

8.应用并保存



如何在Cisco IdS服务器中重新生成SAML证书

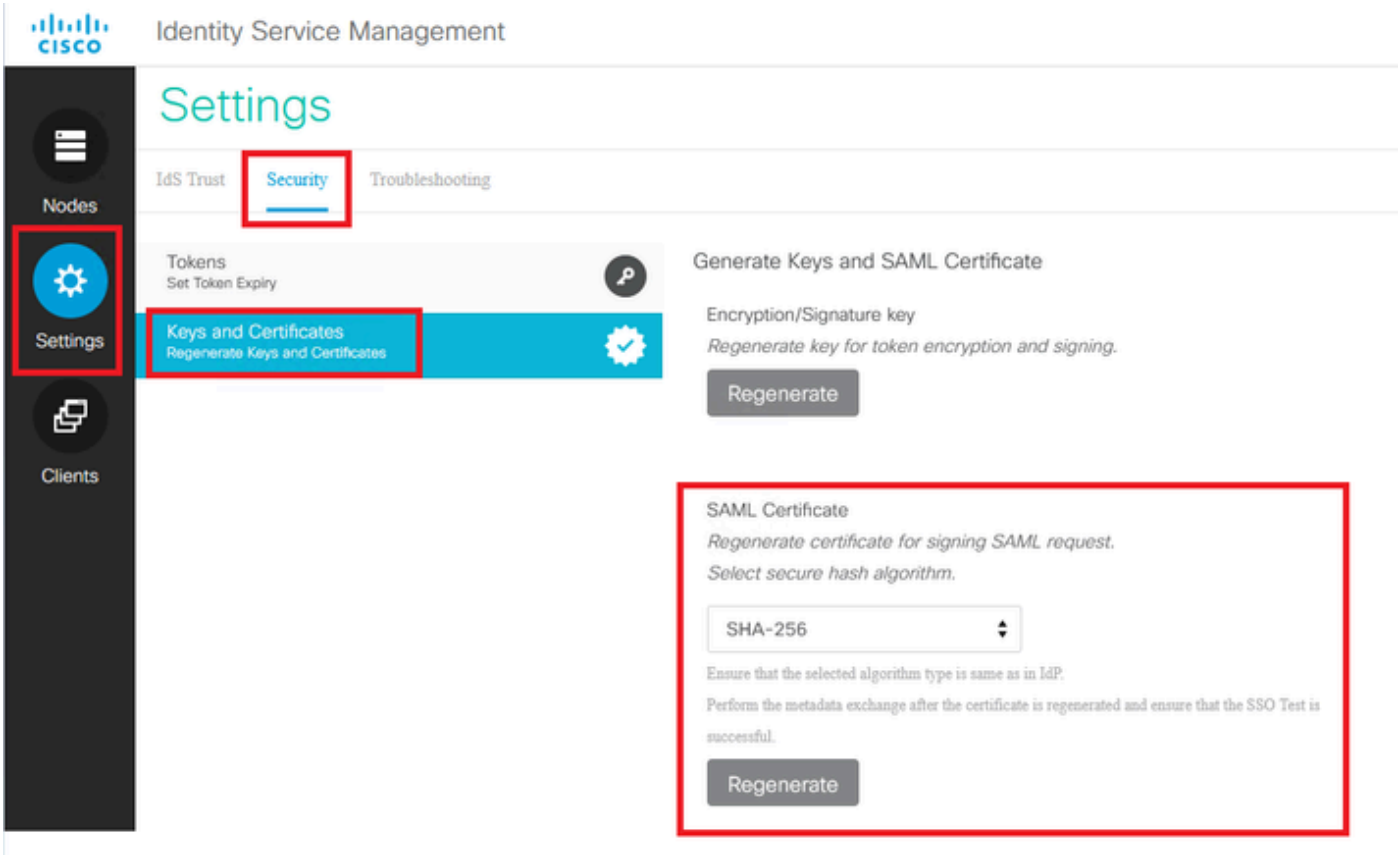
1.使用应用用户凭证登录到Cisco IdS Publisher节点

2.单击设置图标

3.定位至“安全性”标签

4.选择“密钥和证书”选项

5.点击SAML证书部分下的Regenerate按钮（突出显示）



测试SSO

每当SAML证书发生更改时，请确保TEST SSO在Cisco IdS服务器中成功并且从CCEAdmin页面重新注册所有应用。

1.从承担者AW服务器访问CCEAdmin页面

2.使用管理员级别的权限登录CCEAdmin门户

3.定位至“概览”>“功能”>“单点登录”

4.点击“向思科身份服务注册”下的“注册”按钮

5.执行测试SSO

Azure证书再生

1.从IDS重新生成证书（仅在发布服务器中），这将为发布服务器和订阅服务器自动生成证书
2.从IDS下载元数据并上传到IDP/Azure
3.从IDP/Azure续订证书，这将完全更改Azure中的元数据，并将从Microsoft Azure对其进行签名，从而解决.pfx的需求
4.将元数据从IDP/Azure上传到Cisco IDS，仅在发布服务器上进行
5.从IDS测试SSO

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）。