

# 使用身份服务(IdS)证书管理排除CCE单点登录故障

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [SAML证书已过期](#)

### [解决方案](#)

#### [身份提供程序\(IdP\)中的安全哈希算法更改](#)

### [解决方案](#)

#### [Cisco IdS服务器IP地址或主机名更改-已重建并存CUIC/LiveData/IdS发布服务器或独立IdS发布服务器-已重建并存CUIC/LiveData/IdS订阅服务器或独立IdS订阅服务器](#)

### [解决方案](#)

### [参考](#)

#### [如何在ADFS或](#)

#### [如何启用签名的SAML断言](#)

#### [如何将AD FS SSL证书上传到Cisco IdS tomcat trust](#)

#### [如何删除AD FS中的信赖信任方](#)

#### [如何检查或更改身份提供程序\(IdP\)中配置的安全哈希算法](#)

#### [如何检查Cisco IdS服务器SAML证书到期日期](#)

#### [如何下载Cisco IdS服务器的元数据](#)

#### [如何从sp.xml文件检索SAML证书](#)

#### [如何替换AD FS中的SAML证书](#)

#### [如何在Cisco IdS服务器中重新生成SAML证书](#)

#### [测试SSO](#)

---

## 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

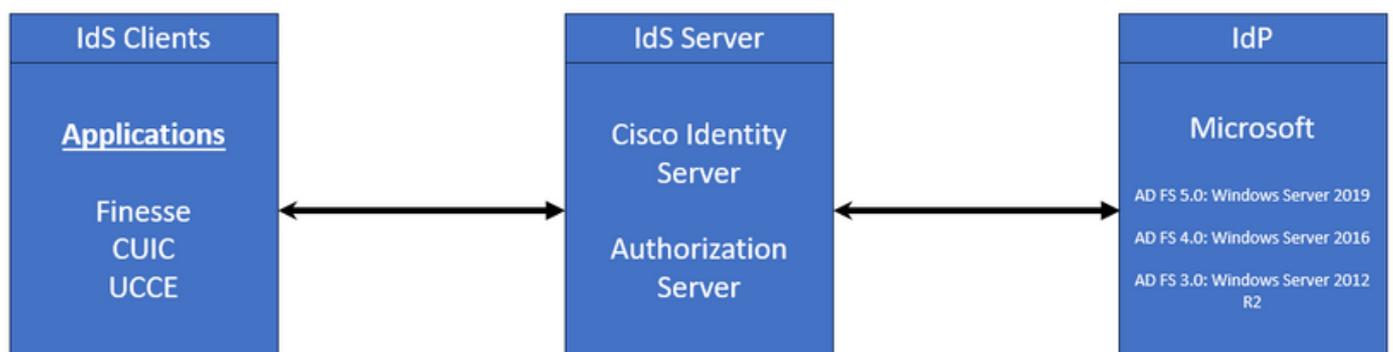
思科建议您了解以下主题：

- 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)提供身份提供程序(IdP)和应用之间的授权。

在配置思科ID时，您可以在思科ID和IDp之间建立元数据交换。此交换建立信任关系，然后允许应用使用思科ID进行SSO。您可以通过从思科ID下载元数据文件并将其上传到IDp来建立信任关系。

SAML证书类似于SSL证书，当出现某些情况时，需要更新或更改该证书。在思科身份服务(IdS)服务器上重新生成或替换SAML证书时，可能导致与身份提供程序(IdP)的受信任连接中断。此中断会导致依赖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。

本文档旨在介绍需要在思科IdS服务器上创建新的SAML证书的各种常见情况。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无误地处理证书更新过程所需的所有信息。

需牢记的要点：

1. 默认情况下，SAML证书在思科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发布服务器和用户上的SSL证书
4. 只能在Cisco IDS Publisher节点中执行SAML证书重新生成
5. SAML证书的安全散列算法的可用类型是SHA-1和SHA-256
6. SHA-1算法用于IdS 11.6，在以前的版本中，SHA-256算法用于IdS 12.0和更高版本
7. 身份提供程序(IdP)和身份服务(IdS)必须使用相同的算法类型。
8. 只能从Cisco IdS发布服务器节点(sp-<Cisco IdS\_FQDN>.xml)下载Cisco IdS SAML证书
9. 请参阅此链接以了解UCCE/PCCE单点登录配置。 [UCCE 12.6.1功能指南](#)

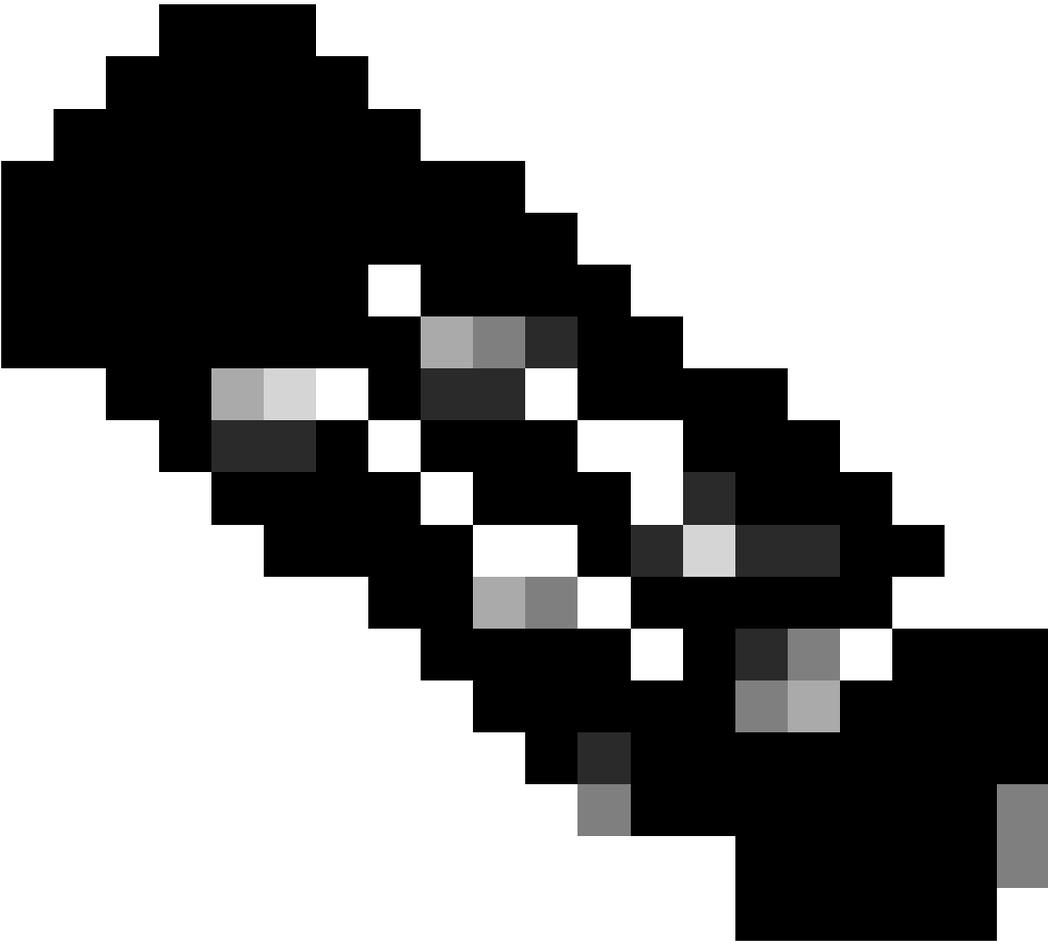
## SAML证书已过期

SAML证书的生成有效期为3年（1095天），并且需要在SAML证书到期之前续订。过期的SSL证书被视为无效证书，它将破坏思科身份服务(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. 用IdP中的新SAML证书替换旧SAML证书
6. 有关详细步骤，请参阅参考部分

---



(注意：{由于仅更改了SAML证书，因此不需要将IdS元数据交换为IdP})

---

## 身份提供程序(IdP)中的安全哈希算法更改

假设在具有单点登录的现有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在将安全散列算法更改为SHA-256时所需的弱点。

### 解决方案

1. 更改AD FS信赖信任方中的安全哈希算法 ( 将SHA-1更改为SHA-256 )
2. 将IdS发布服务器中的安全哈希算法在Keys and Certificate ( 密钥和证书，从SHA-1更改为SHA-256 ) 下更改
3. 在IdS发布服务器中重新生成SAML证书

4. 下载sp.xml文件
5. 从sp.xml文件检索SAML证书
6. 用IdP中的新SAML证书替换旧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-已重建并存 CUIC/LiveData/IdS发布服务器或独立IdS发布服务器-已重建并存 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，强烈建议重新开始使用单点登录(SSO)设置，以确保生产环境中的SSO功能得到迅速而有效的恢复。必须确定此重新配置的优先级，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“参考部分及功能指南”
5. 在AD FS中配置信赖方
6. 添加申请规则
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思科IdS服务器
10. 执行测试SSO

### 参考

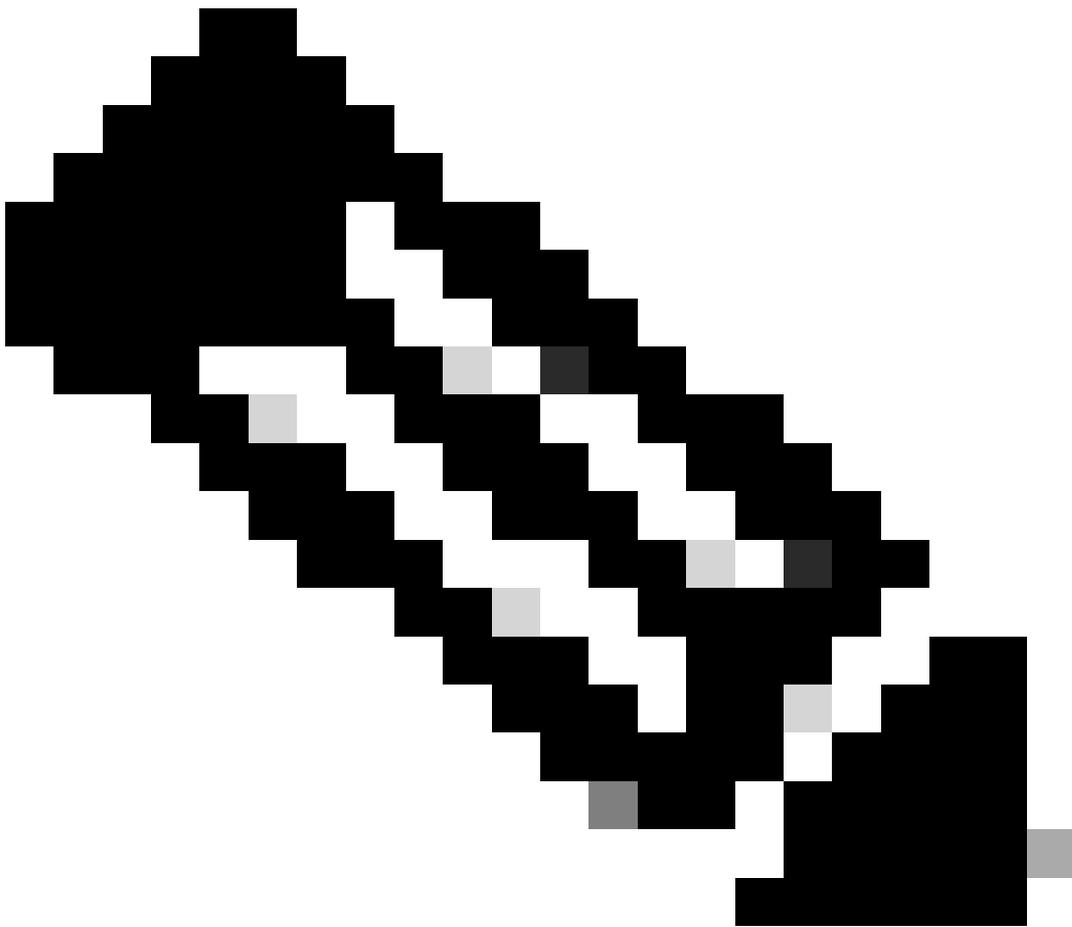
如何在ADFS或

如何启用签名的SAML断言

请参阅本文档了解详细步骤：[UCCE 12.6.1功能指南](#)

## 如何将AD FS SSL证书上传到Cisco IdS tomcat trust

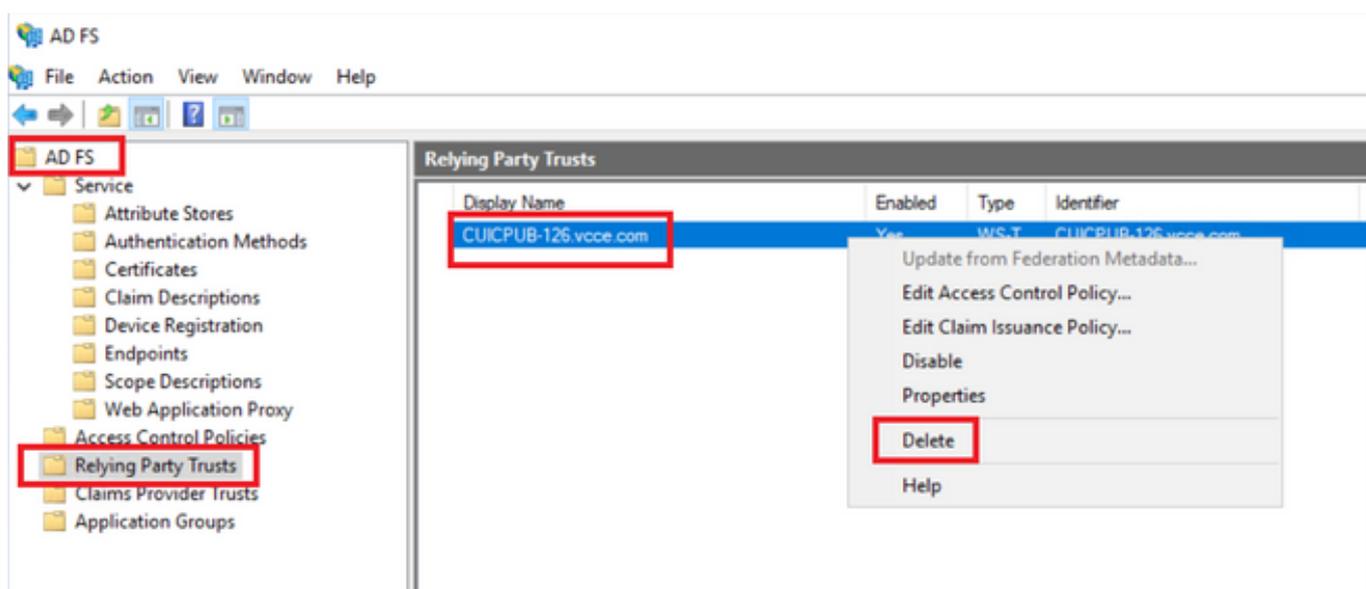
1. 下载或检索AD FS SSL证书
  2. 访问Cisco IdS Publisher OS Administration页面
  3. 使用操作系统管理员凭证登录
  4. 导航至“安全”>“证书管理”
  5. 点击“上传证书/证书链”，系统将显示弹出窗口
  6. 点击下拉菜单并选择“证书用途”上的tomcat-trust
  7. 单击“浏览”并选择AD FS SSL证书
  8. 点击上传
- 



(注意：{信任证书将复制到订阅服务器节点。您不需要在“订户”节点上上传。})

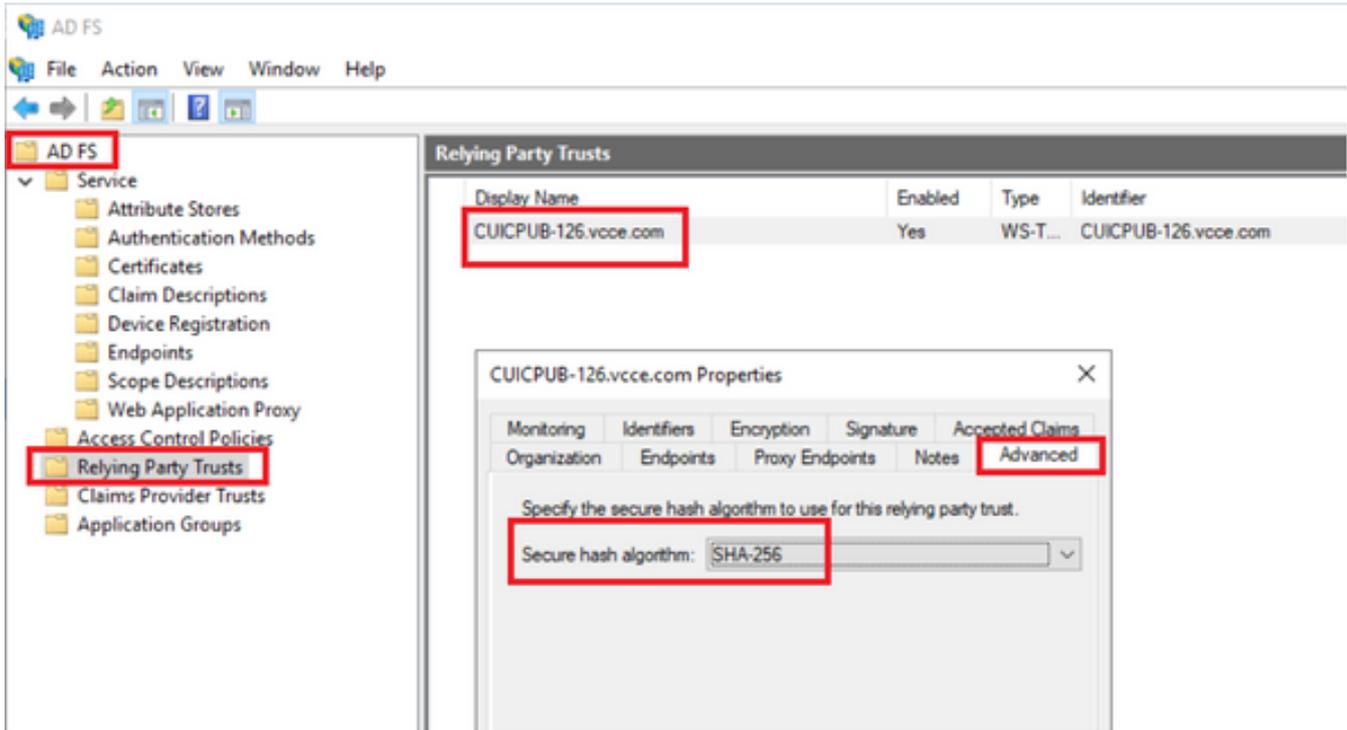
## 如何删除AD FS中的信赖信任方

1. 使用管理员特权凭证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

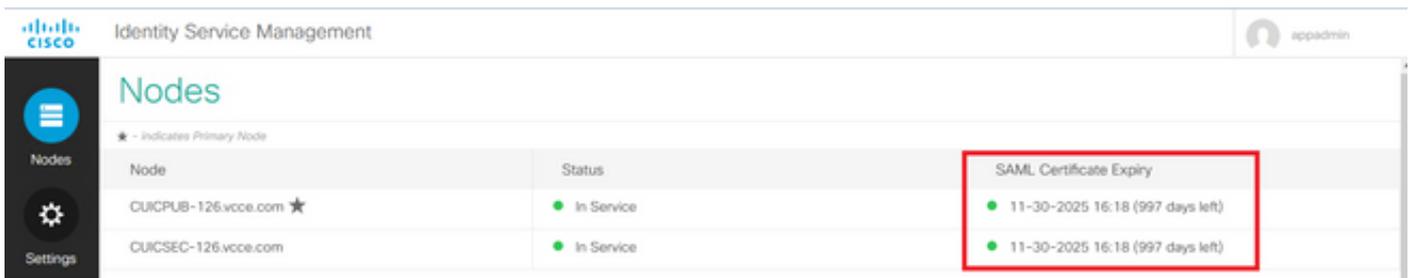
1. 使用管理员特权凭证登录到身份提供程序(IdP)服务器
2. 打开服务器管理器，然后选择AD FS >工具> AD FS管理
3. 在左侧树中，选择AD FS下的信赖方信任
4. 右键单击Cisco IdS服务器并选择属性
5. 定位至“高级”标签
6. Secure Hash Algorithm选项显示AD FS服务器中配置的安全散列算法。



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

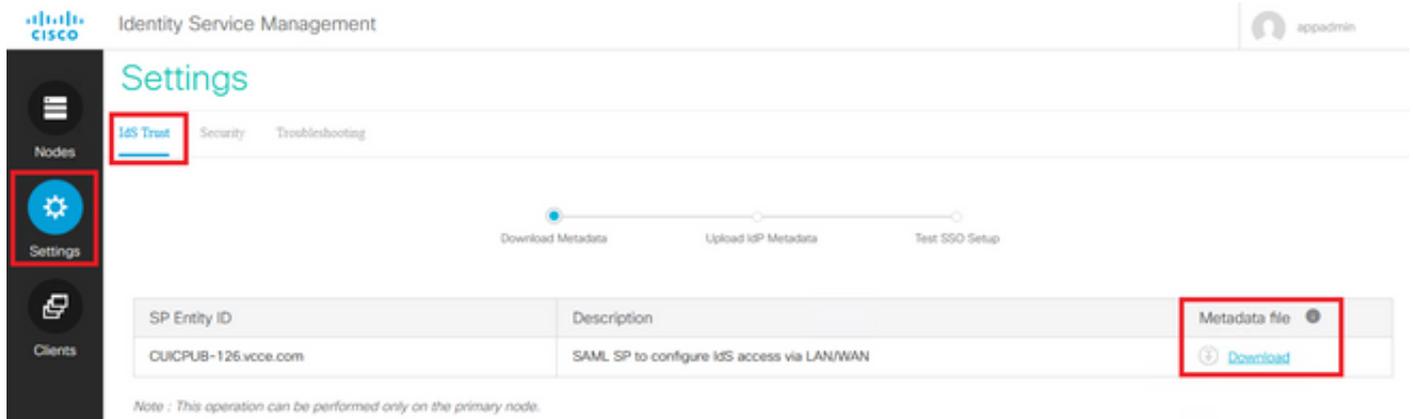
1. 使用应用用户凭证登录到Cisco IdS服务器发布方或订用方节点
2. 成功登录后，该页面将转至Identity Service Management > Nodes
3. 显示Cisco IdS发布服务器和订阅服务器节点、状态和SAML证书到期



## 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，下载Cisco IdS集群的元数据

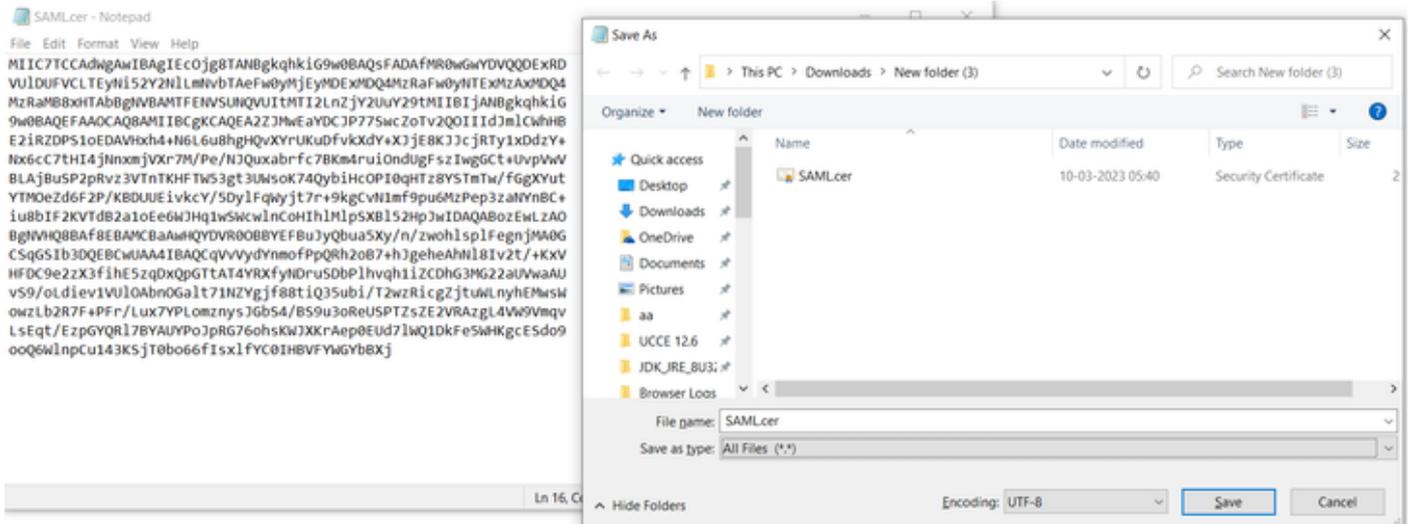


#### 如何从sp.xml文件检索SAML证书

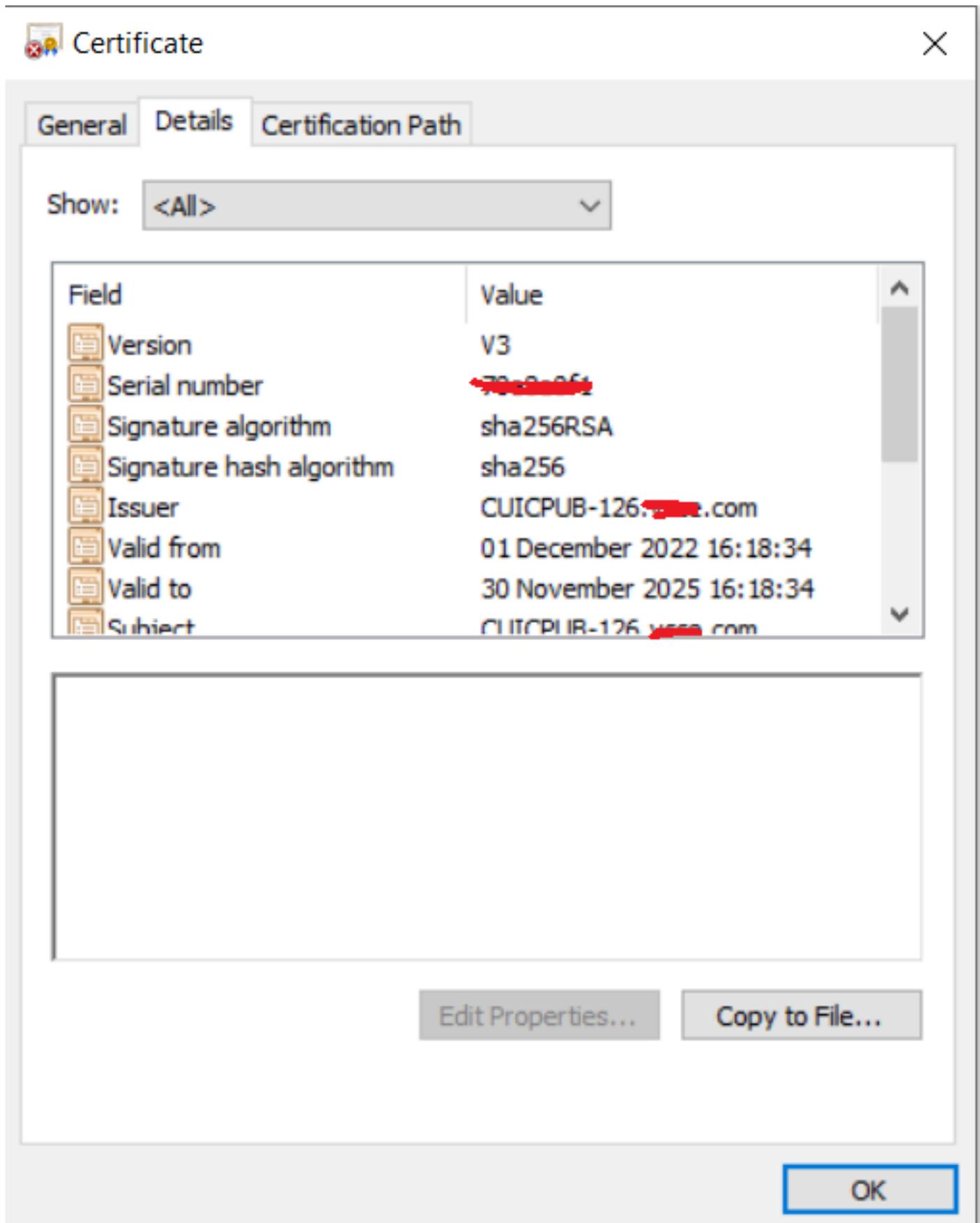
1. 使用文本编辑器打开sp.xml文件
2. 在信头<ds : X509Certificate></ds : X509Certificate>之间复制原始数据

```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VU1DUFVCLTEyNi52Y2N1LmNvbTAeFw0yMjE5MDExMDQ4MzRaFw0yNTE5MDExMDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUI tMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2ZJMwEaYDCJP77SwcZoTv2QOIIdJmlCWjHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJCjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabrFc7BKm4ruiOndUgFsZlwgGct+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyjt7r+9kgCvNlmf9pu6MzPep3zaNYnBC+
iu8bIF2KVTdB2a1oEe6WJHq1wSwcWlnCoHIh1MlpSXB152HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBuJyQbua5Xy/n/zwohlSplFegnJMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhN18Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGTtAT4YRXfyNDruSdbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdievlVULOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnYhEMwsW
owzLb2R7F+Pfr/Lux7YPLomznysJGbs4/BS9u3oReUSPTZsZE2VRAZg4VW9Vmqv
LsEqT/EzpgYQR17BYAUYPoJpRG76ohsKWJXKrAep0EUd71WQ1DkFe5WHKgcESdo9
ooQ6WlnpCul43KSjt0bo66fIsxlFYC0IHBVfYWGyBxj</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

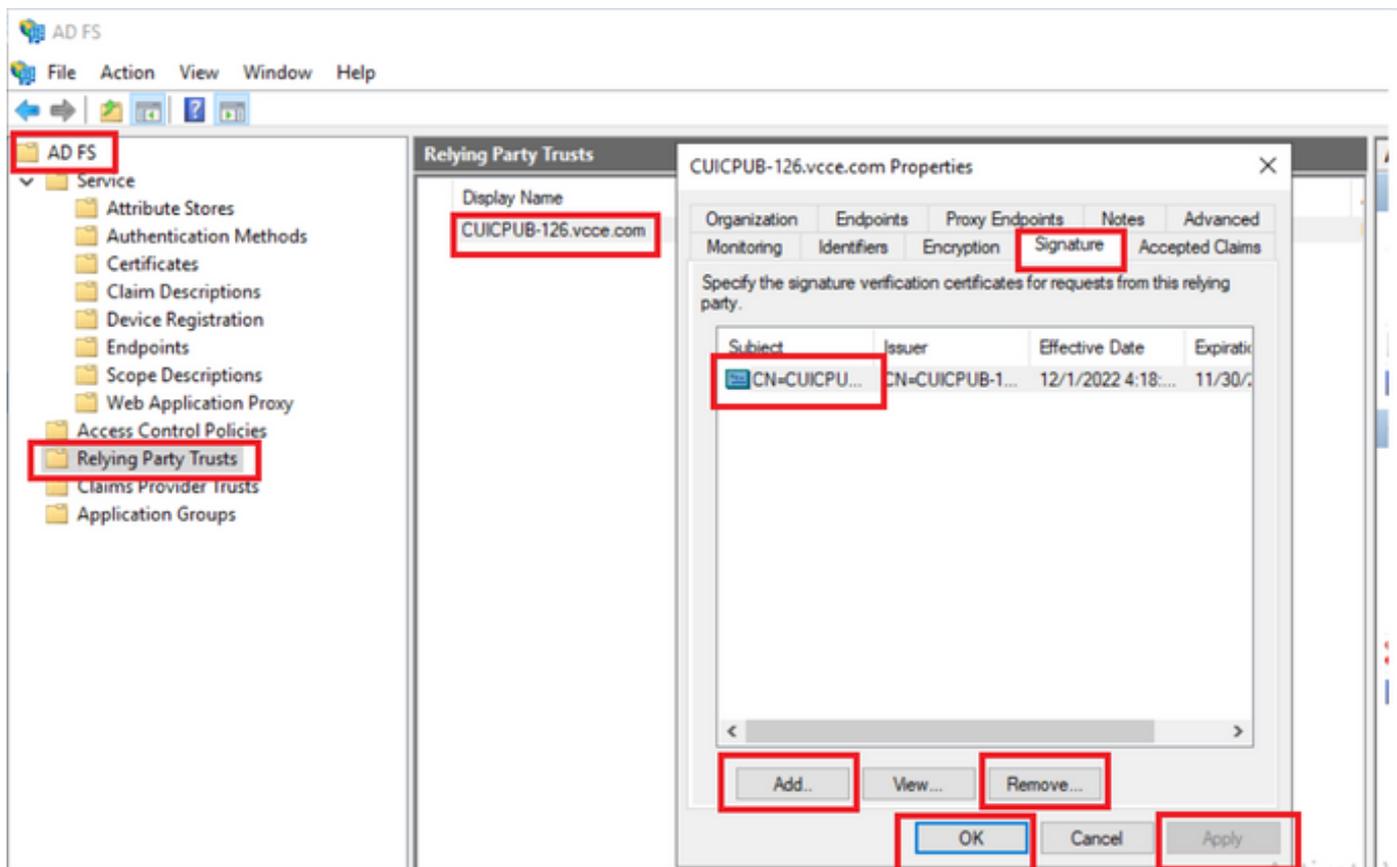


## 5. 打开证书以查看证书信息



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. 单击Add ( 添加 ) 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证书部分下方的“重新生成”按钮（突出显示）

The screenshot shows the Cisco Identity Service Management (IdSM) interface. The left sidebar contains navigation options: Nodes, Settings (highlighted with a red box), and Clients. The main content area is titled 'Settings' and has three tabs: IdS Trust, Security (highlighted with a red box), and Troubleshooting. Under the Security tab, there are two sub-sections: 'Tokens' (Set Token Expiry) and 'Keys and Certificates' (Regenerate Keys and Certificates, highlighted with a red box). The 'Keys and Certificates' section contains two 'Regenerate' buttons. The first is for 'Encryption/Signature key' with the instruction 'Regenerate key for token encryption and signing.' The second is for 'SAML Certificate' with the instruction 'Regenerate certificate for signing SAML request. Select secure hash algorithm.' Below this is a dropdown menu set to 'SHA-256' and a note: 'Ensure that the selected algorithm type is same as in IdP. Perform the metadata exchange after the certificate is regenerated and ensure that the SSO Test is successful.'

## 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，并从CCEAdmin页面重新注册所有应用。

1. 从主体AW服务器访问“CCEAdmin”页
2. 使用管理员级别权限登录到CCEAdmin门户
3. 导航至“概览”>“功能”>“单点登录”
4. 点击Register with Cisco Identity Service下的Register按钮
5. 执行测试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）。