# 在(SSO)证书和配置的统一的联络中心企业(UCCE)单个符号

## Contents



## Introduction

本文描述对于UCCE SSO是必需的认证配置。此功能的配置介入HTTPS、数字签名和加密的几证书。

### Requirements

Cisco 建议您了解以下主题：

- UCCE版本11.5
- Microsoft激活目录(AD) -在Windows服务器上安装的AD
- 激活目录联邦服务(ADFS)版本2.0/3.0

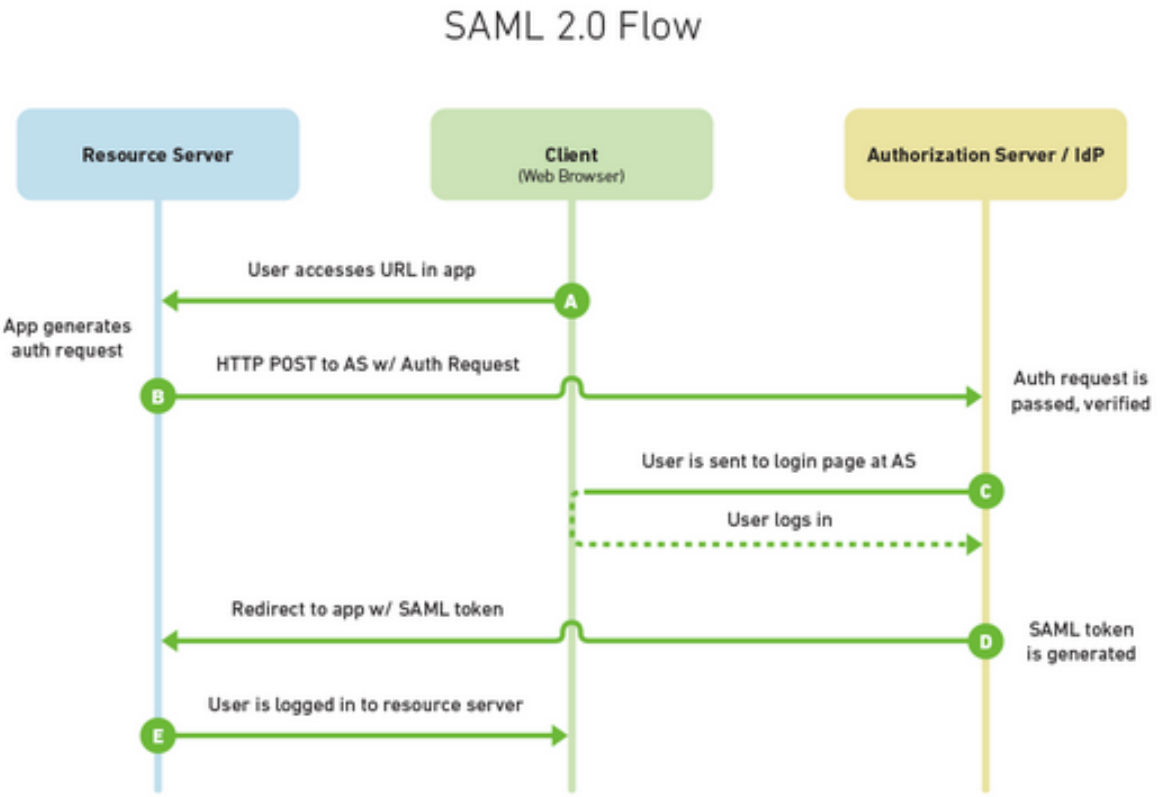
### Components Used

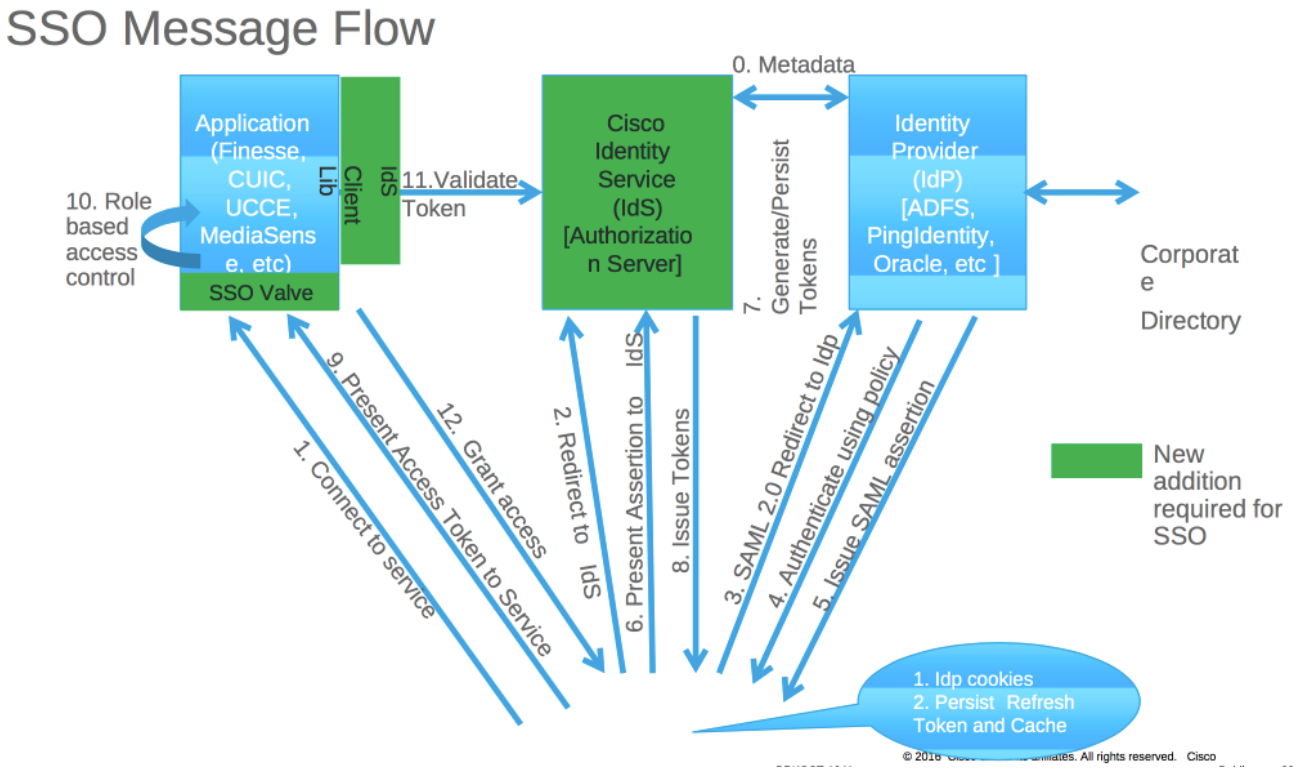
UCCE 11.5

Windows 2012个R2

### 部分A. SSO Message消息流

The most common SAML flow is shown below:

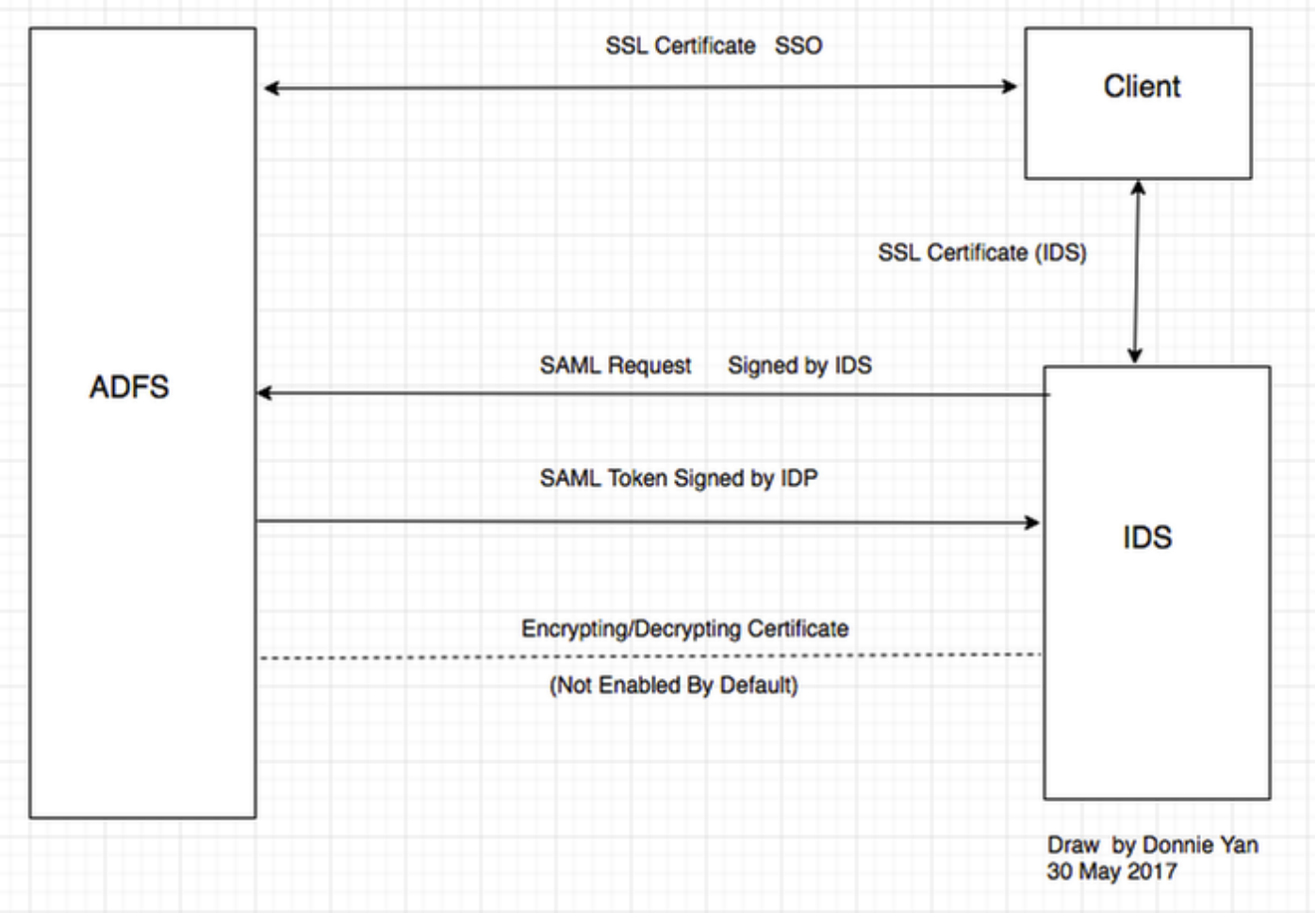



当SSO是启用的，当代理程序登录到精良桌面：

- 精良服务器重定向代理程序浏览器与身份服务(IDS)联络
- IDS重定向代理程序浏览器对身份供应商(IDP)与SAML请求
- IDP生成SAML令牌并且通过对IDS服务器
- 当令牌生成了，在代理程序访问对ppplication时候，使用此有效令牌登录

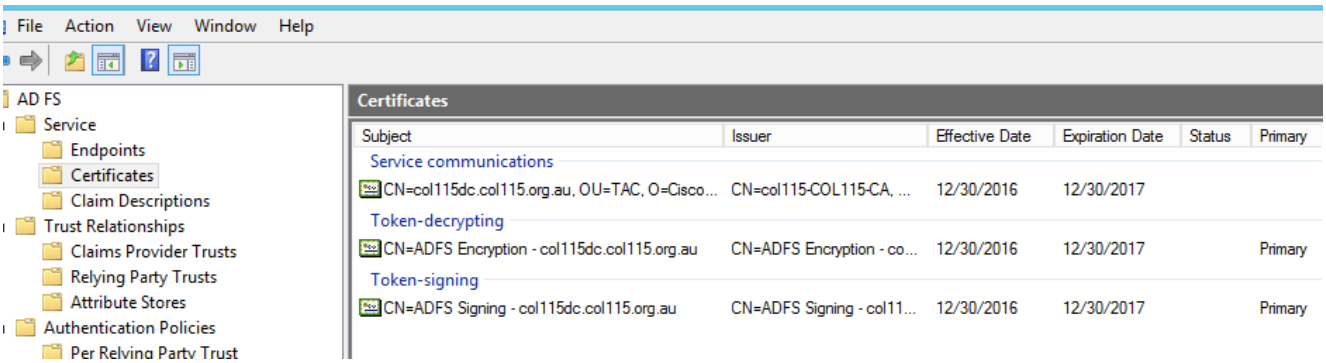
## 部分B.在IDP和IDS的Certificates Used




### IDP证书

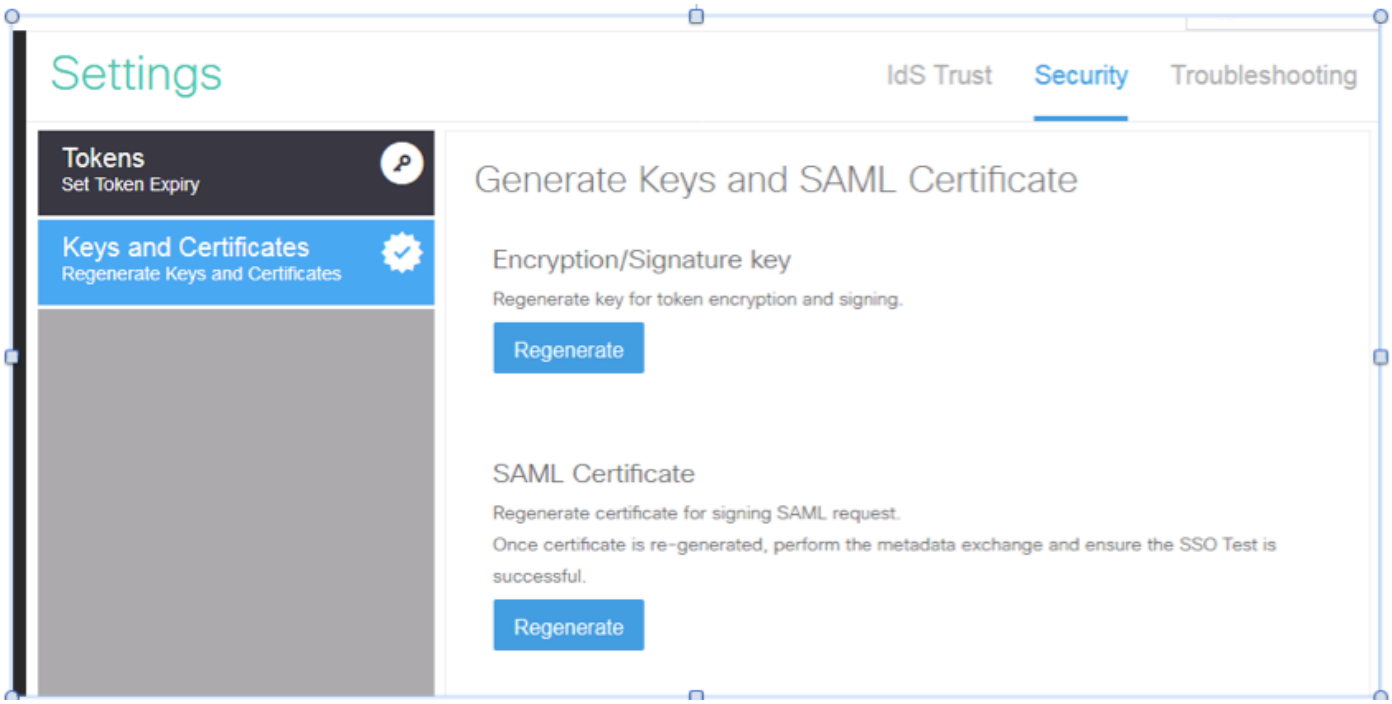
- SSL认证(SSO)
- 令牌的签署的认证
- 令牌–解码

1.




### IDS证书

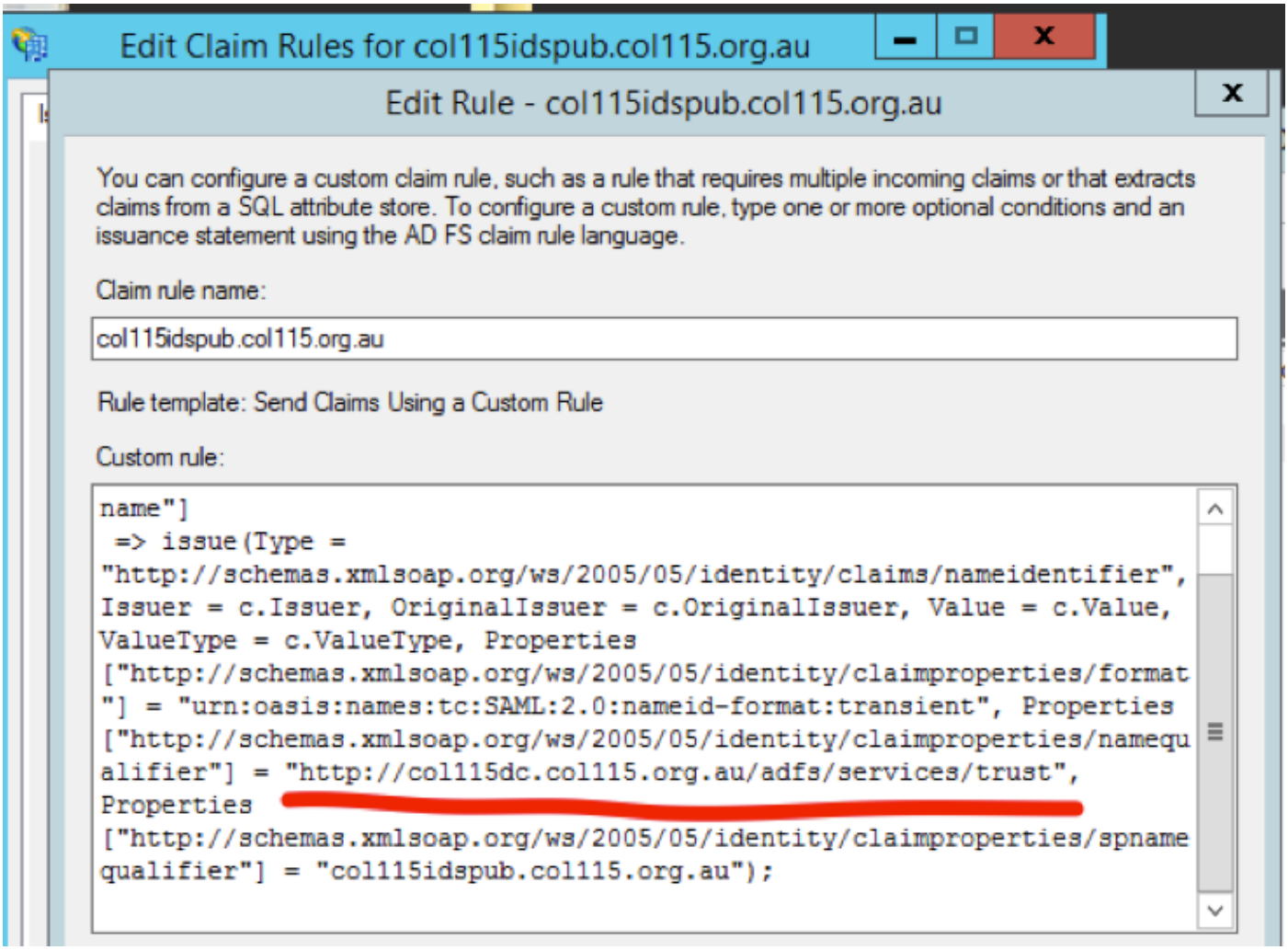
- SAML认证
- 签名键
- 加密密钥




## 部分C. IDP详细Certification和配置

### SSL认证(SSO)

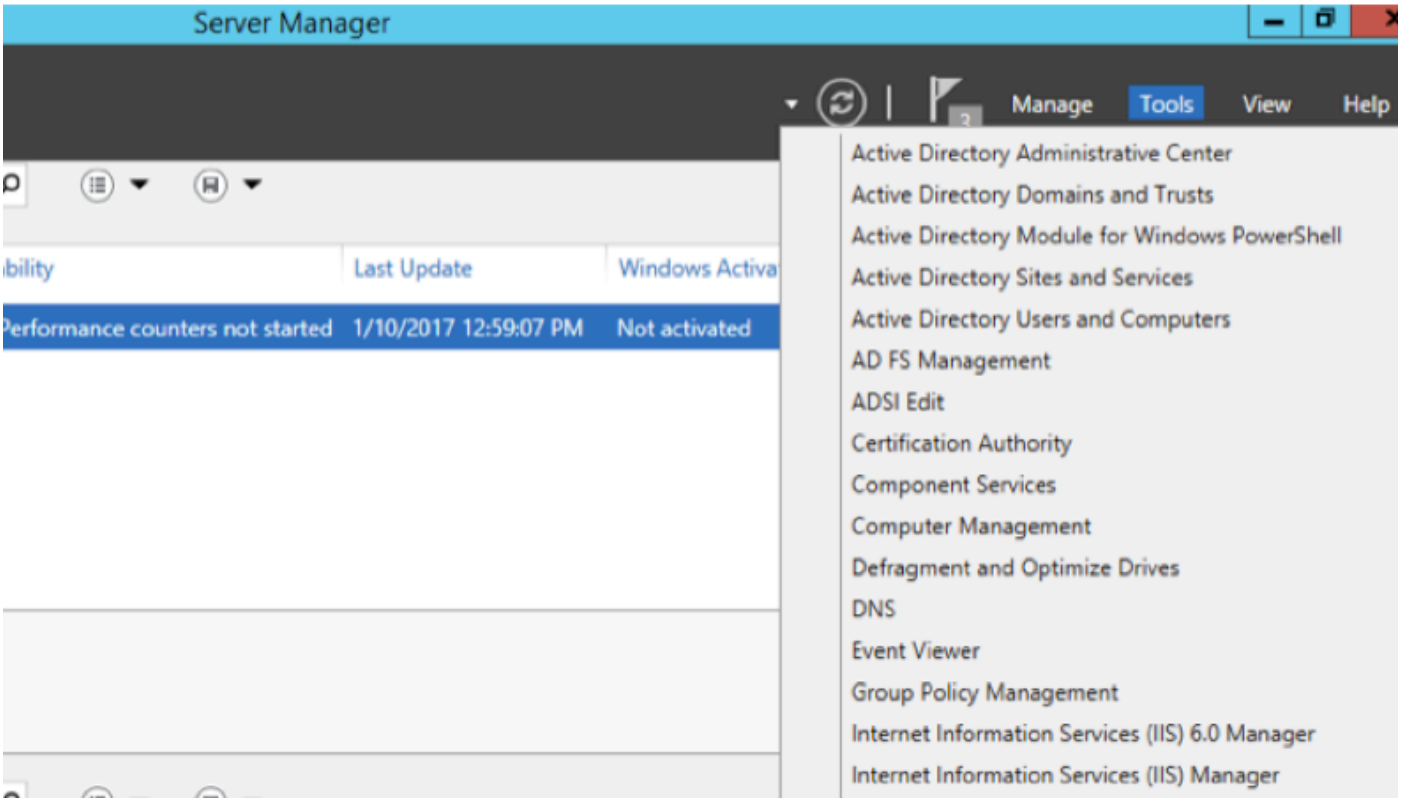
- 此认证使用在IDP和客户端之间。客户端必须委托SSO认证
- 放置SSL认证加密在客户端和IDP服务器之间的会话。此认证不是特定的对ADFS，然而特定对IIS
- SSL认证的主题必须与用于ADFS配置的名字配比

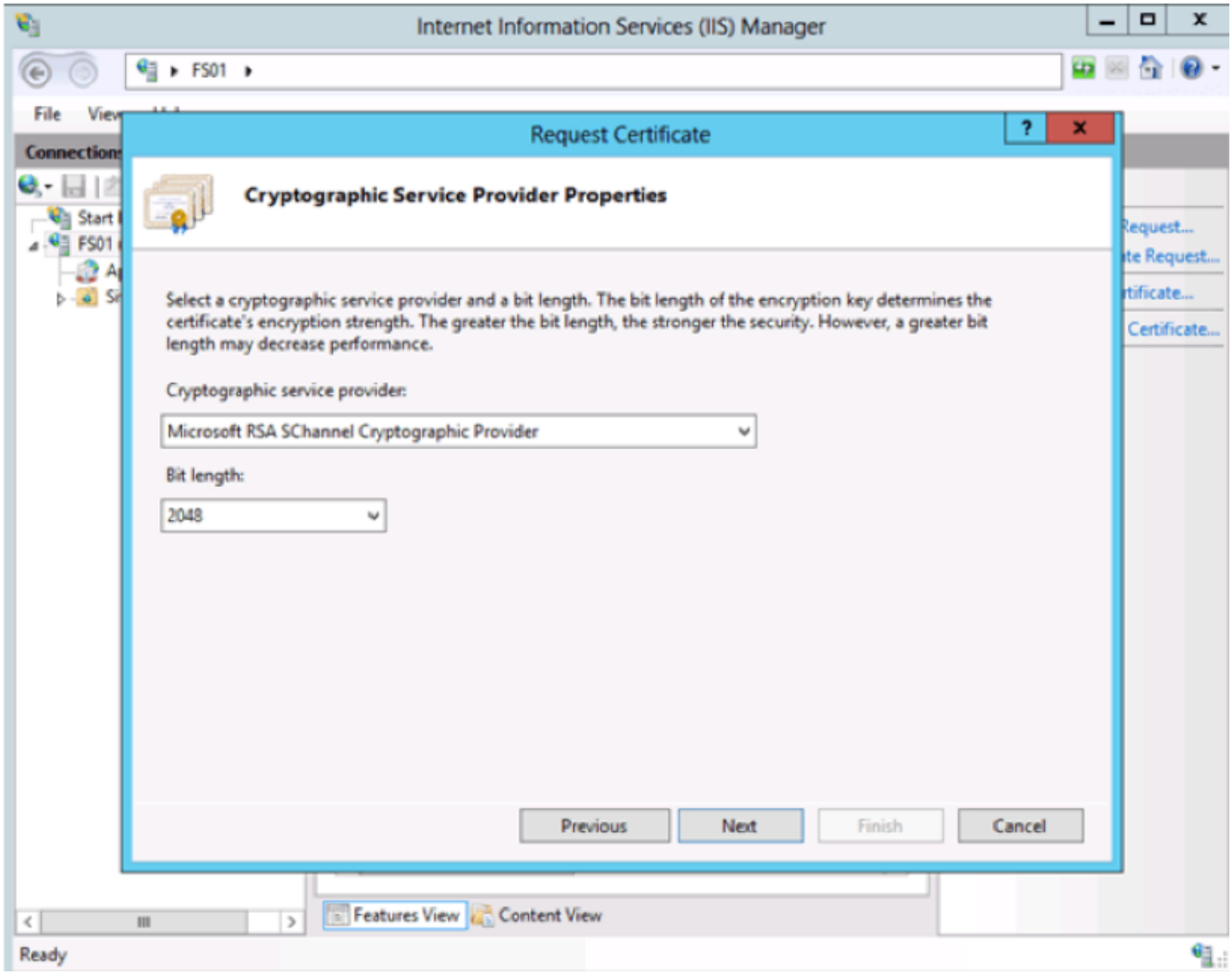



**配置SSO的(有签字的内部CA的本地实验室SSL认证的步骤)**

**步骤1.**用认证署名请求(CSR)**创建**SSL认证和符号由ADFS的内部CA。

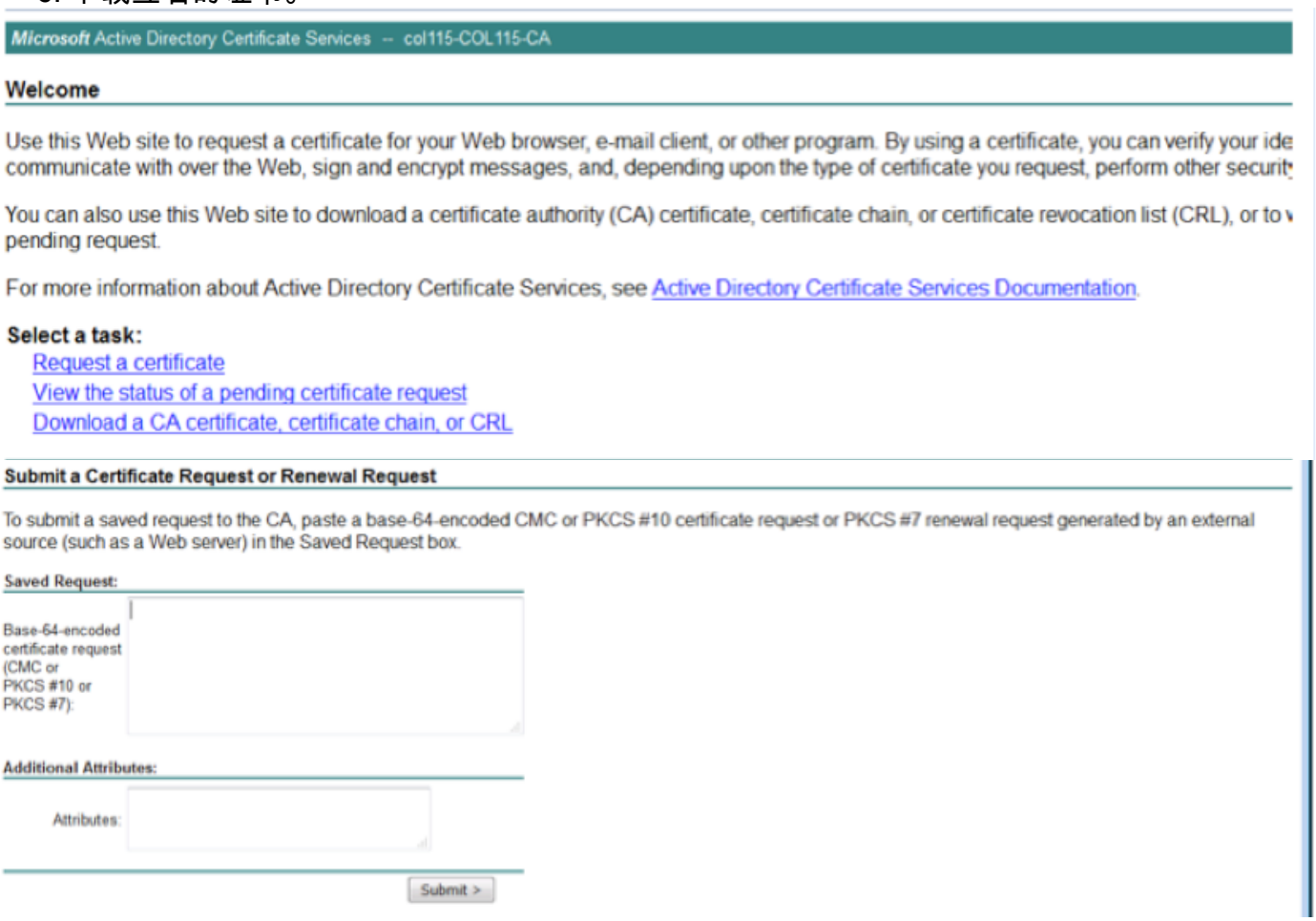
1. 打开服务器管理器。
2. 点击工具。
3. 点击互联网信息服务(IIS)管理器。
4. 选择当地服务器。
5. 选择服务器证明。
6. 点击开放功能(动作面板)。
7. 点击**创建**证书请求。
8. 留下密码服务提供商在默认值。
9. 更改**比特长度到2048**。
10. 单击 **Next**。
11. 选择一个位置保存请求的文件。
12. 单击 **完成**。




**步骤2.** CA签署从step1生成的CSR。

1. **打开**CA服务器唱此CSR **http ：<CA服务器IP地址>/certsrv/**。
2. 点击请求认证。
3. 点击先进的证书请求。
4. **复制**CSR到Based-64编码的证书请求。
5. **提交**。
6. 下载签名的证书。




**步骤3.**安装签名的证书回到ADFS服务器并且分配到ADFS功能。

1. 安装签名的证书回到ADFS服务器。为了执行此，请**打开服务器manager>Tools>Click互联网信息Services(IIS) Manager>**。

**本地Server>Server Certificate>Open功能(动作面板)**。

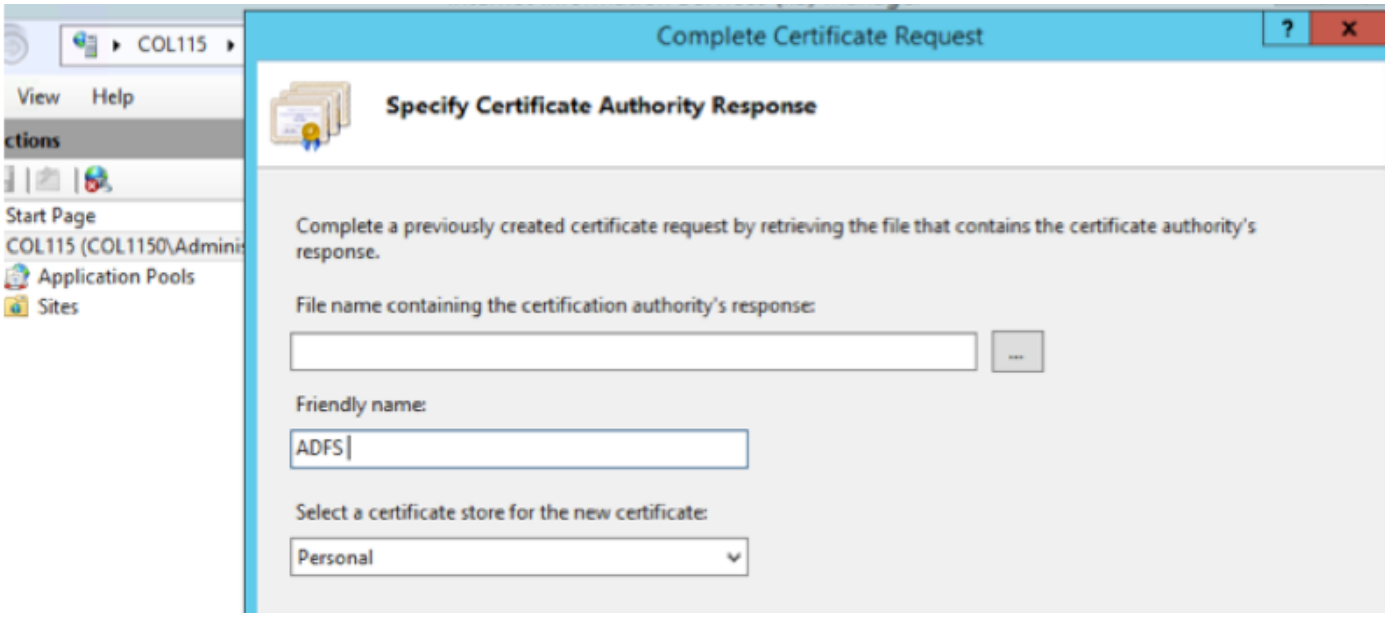
2. 点击完全证书请求。

3. 选择路径对您从第三方认证供应商完成并且下载的完全CSR文件。

4. **进入**认证的友好名称。

5. 选择私有作为证书存储。

6. 单击 **Ok**。




7. 在此阶段，所有认证被添加了。现在， SSL需要认证分配。

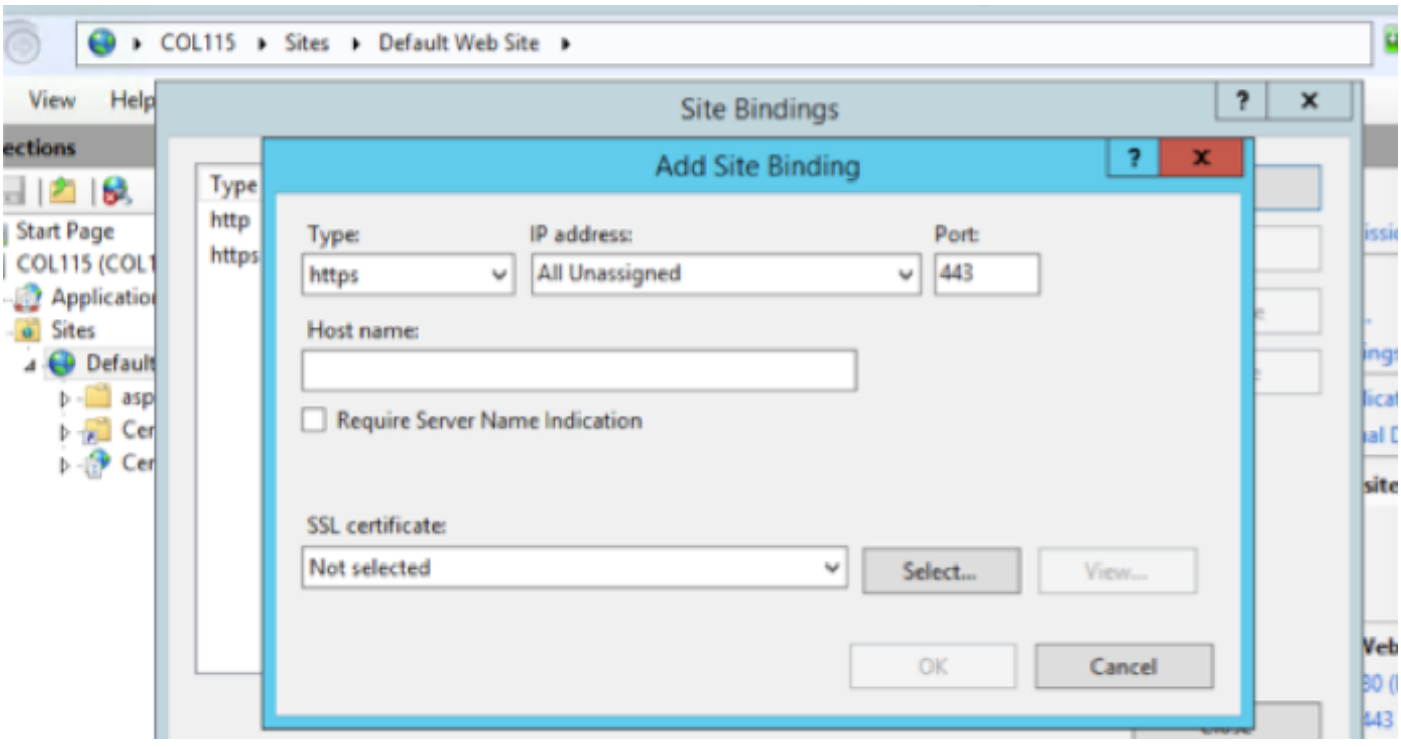
8. **扩展本地server>Expand Sites>Select默认网站>Click捆绑**(动作面)。

9.Click**添加**。

10. **更改**类型到HTTPS。

11. 选择您的认证从下拉菜单。

12. 单击 **Ok**。




现在， ADFS服务器的SSL认证分配。

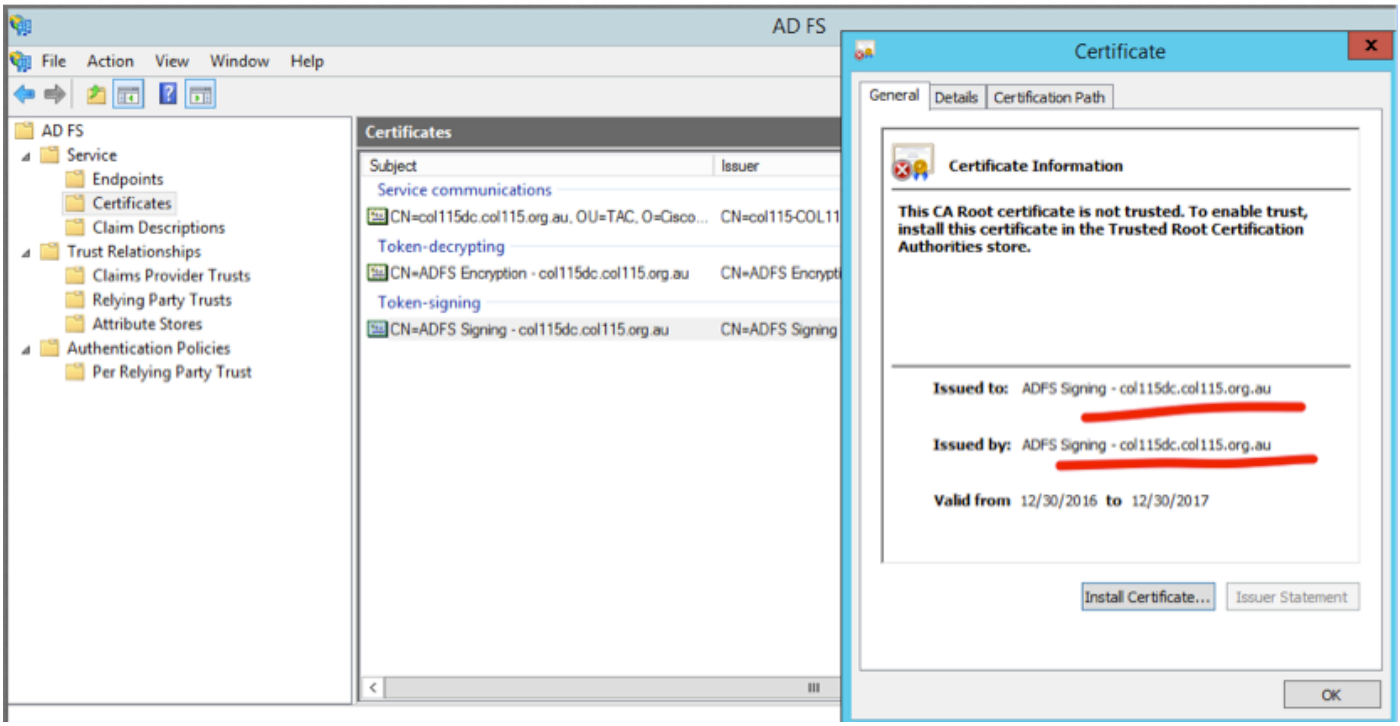
**Note**:在ADFS功能的安装时，必须使用早先SSL认证。

**令牌的签署的认证**

ADFS生成令牌的签署的认证的自签证书。默认情况下它是有效在一年内。

IDP生成的SAML令牌由ADFS专用密钥(令牌的签署的认证专用部分)烧焦。然后， IDS使用ADFS公共密钥验证。这保证签字的令牌不是获得修改。

用户需要获得访问到一个取决于的当事人应用程序每次使用的令牌的签署的认证(Cisco IDS)。

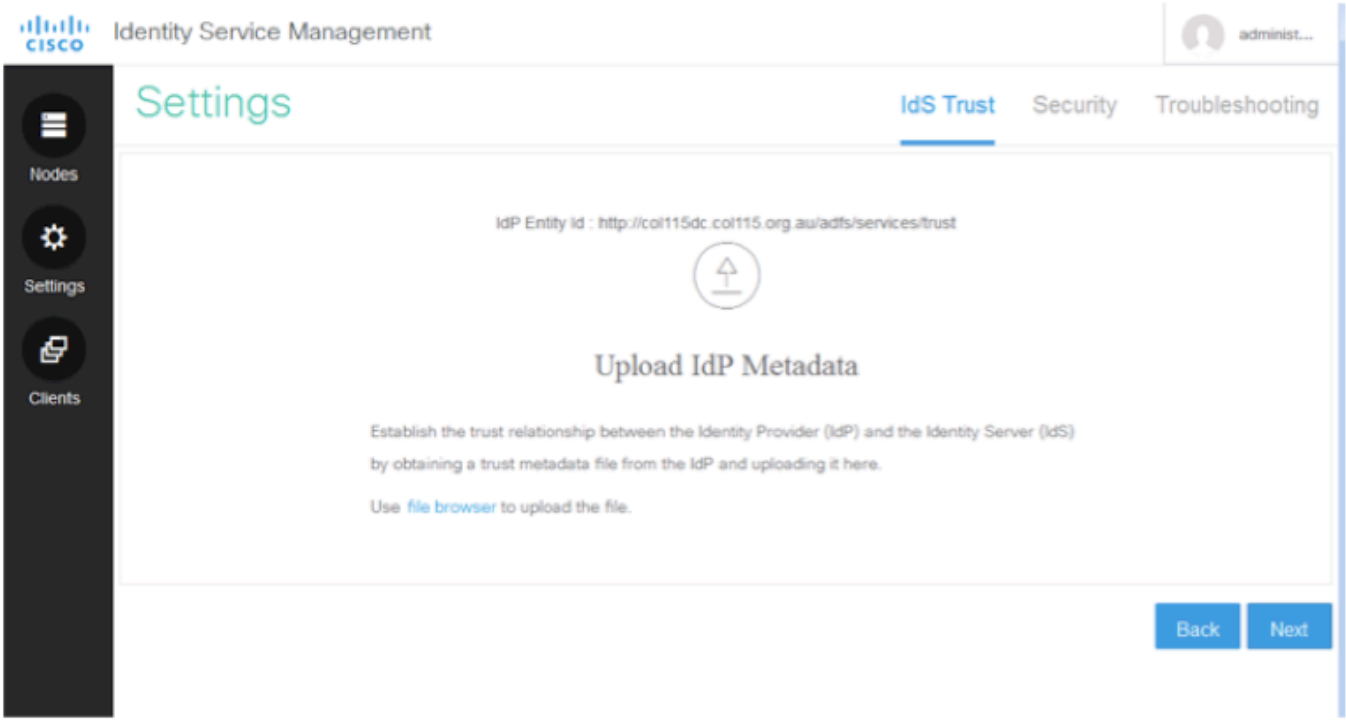



**Cisco IDS服务器如何获得令牌的唱歌认证公共密钥？**

这由加载ADFS元数据到IDS服务器，然后通过ADFS的公共密钥完成对IDS服务器。这样， IDS获取ADFS服务器公共密钥。

您需要从ADFS**下载**IDP元数据。为了下载IDP元数据，请参见链路**https://ADFS>/federationmetadata/2007-06/federationmetadata.xml <FQDN**。

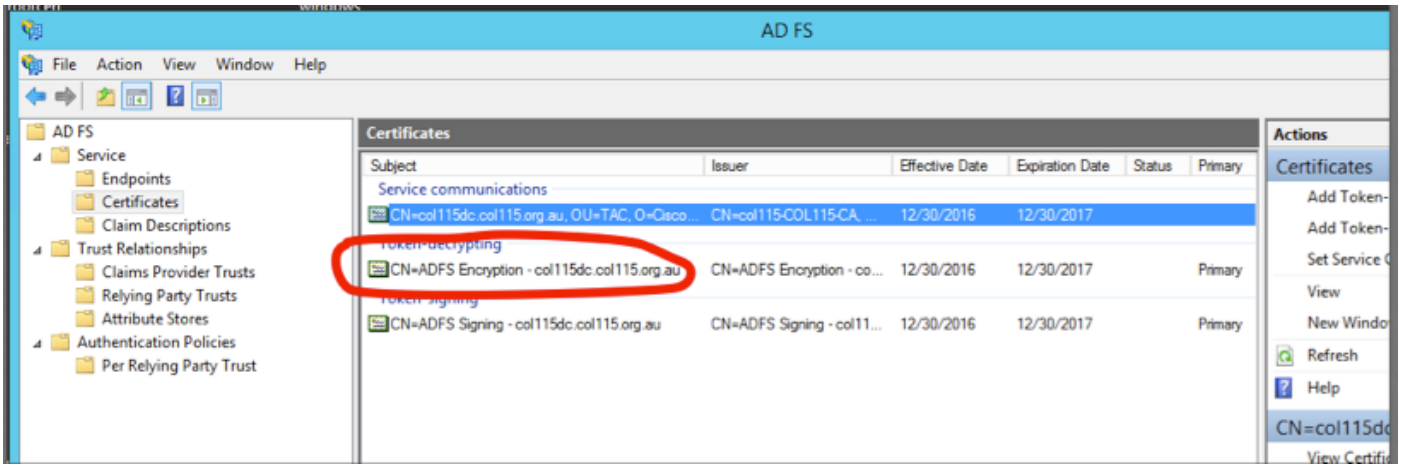

从ADFS元数据




加载ADFS元数据到IDS

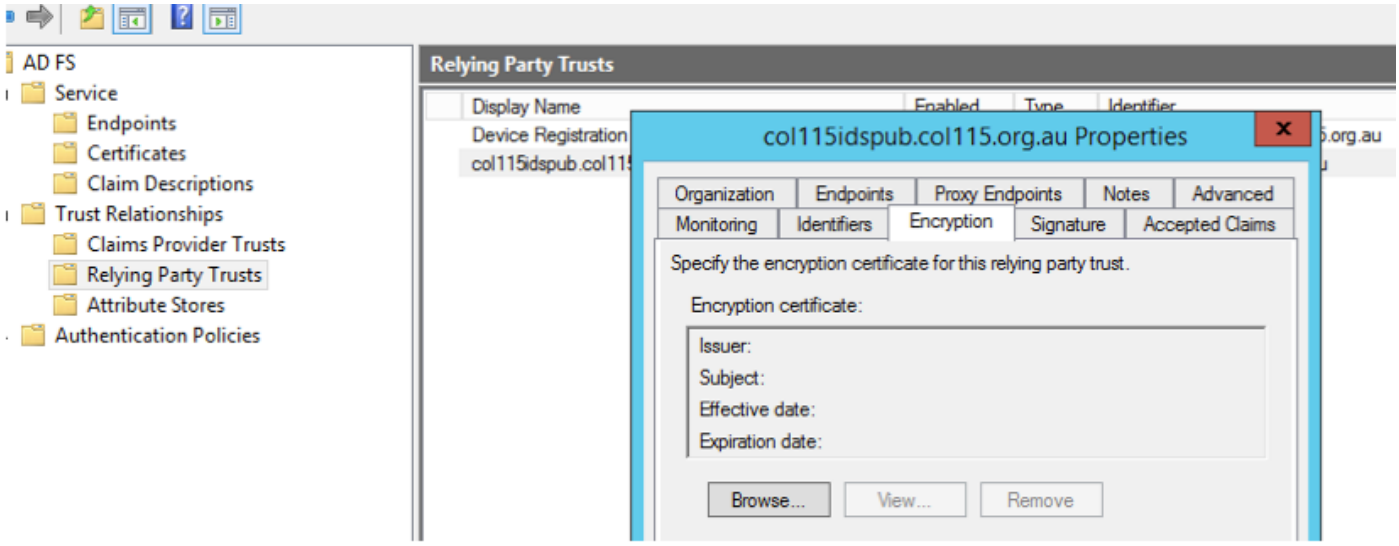
**令牌的解密**

此认证由ADFS服务器自动地生成(自己签署的)。如果令牌需要加密， ADFS使用IDS公共密钥解码它。但是，当您看到ADFS令牌dcrypting时，不意味着令牌被加密。




如果要发现令牌的加密是否为一个特定取决于的当事人应用程序是启用的，您需要检查在一个特定取决于的当事人应用程序的Encryption选项。

此镜像显示，令牌的加密不是启用的。



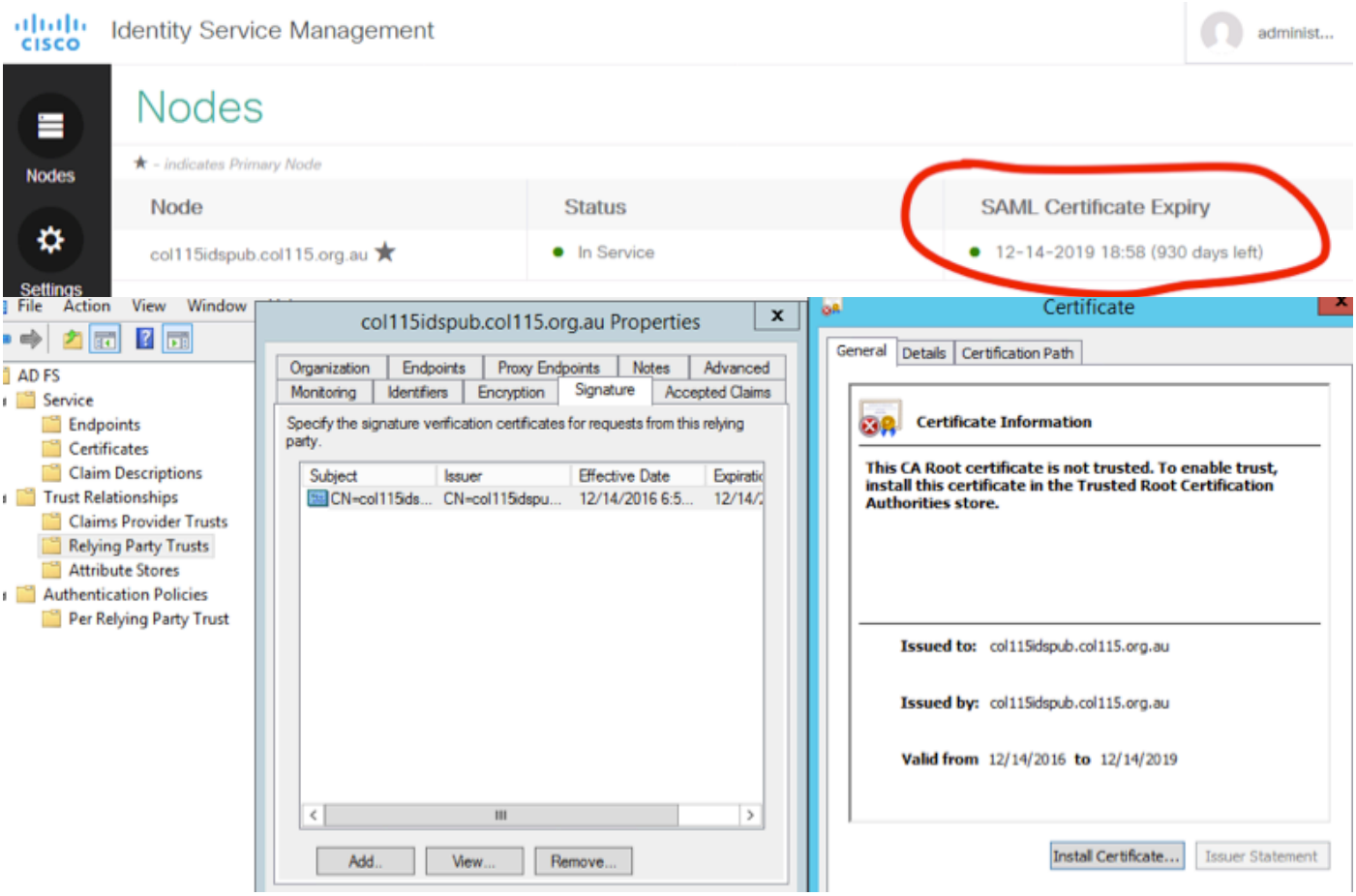

## 加密不是启用的

## 部分D. Cisco IDS边认证

- SAML认证
- 加密密钥
- 签名键

### SAML认证

此认证是由IDS服务器生成的(自己签署的)。默认情况下它是有效在3年内。

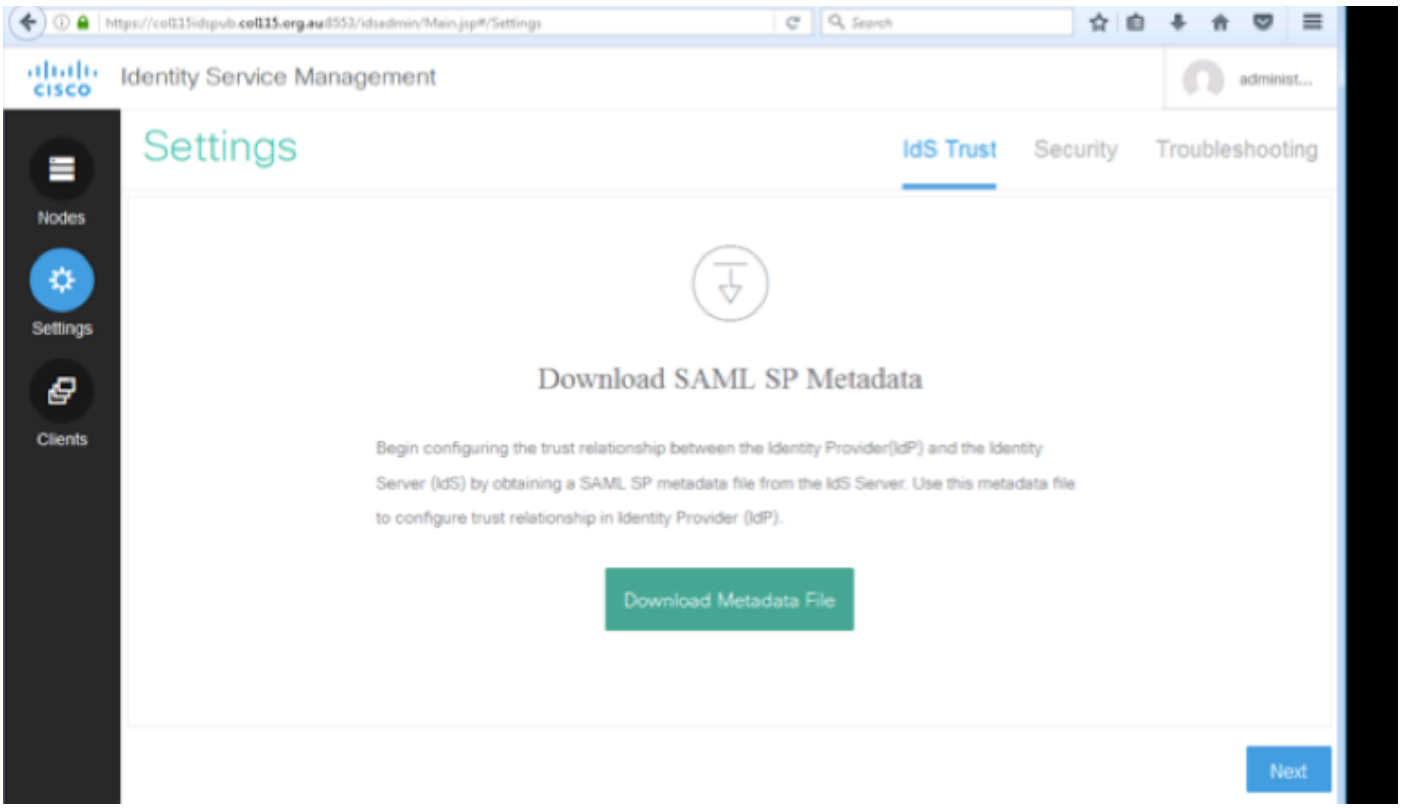


此认证用于签署SAML请求，并且发送到IDP (ADFS)。此公共密钥在IDS元数据，并且必须导入ADFS服务器。

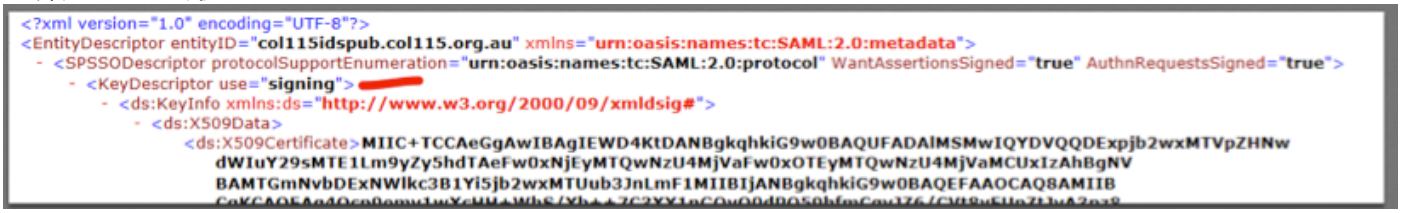
1.Download SAML从IDS服务器的SP元数据。

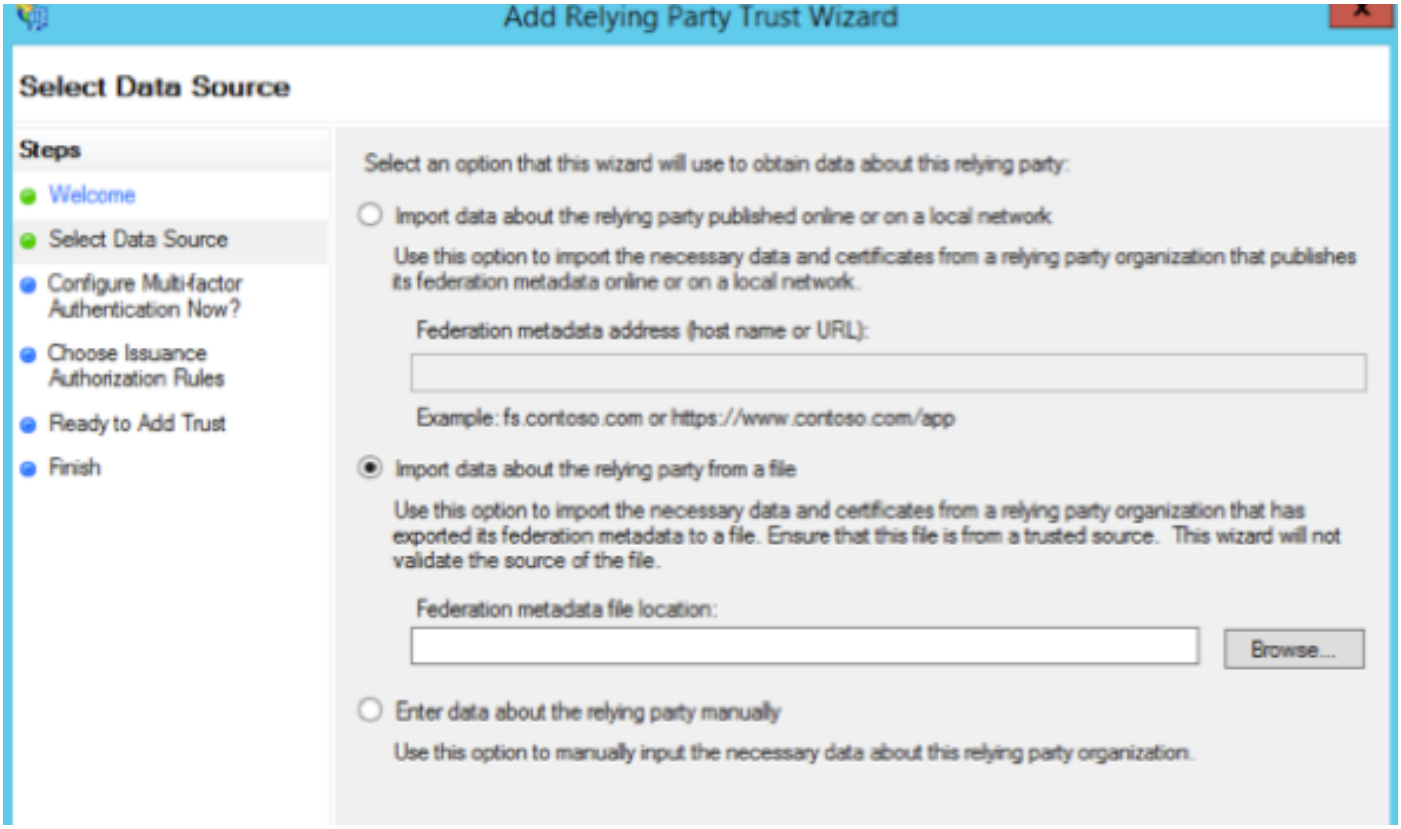
2. 对**https:// <ids服务器FQDN>:8553/idsadmin/的**Broswer。

3. 选择设置和下载SAML SP元数据并且**保存**它。

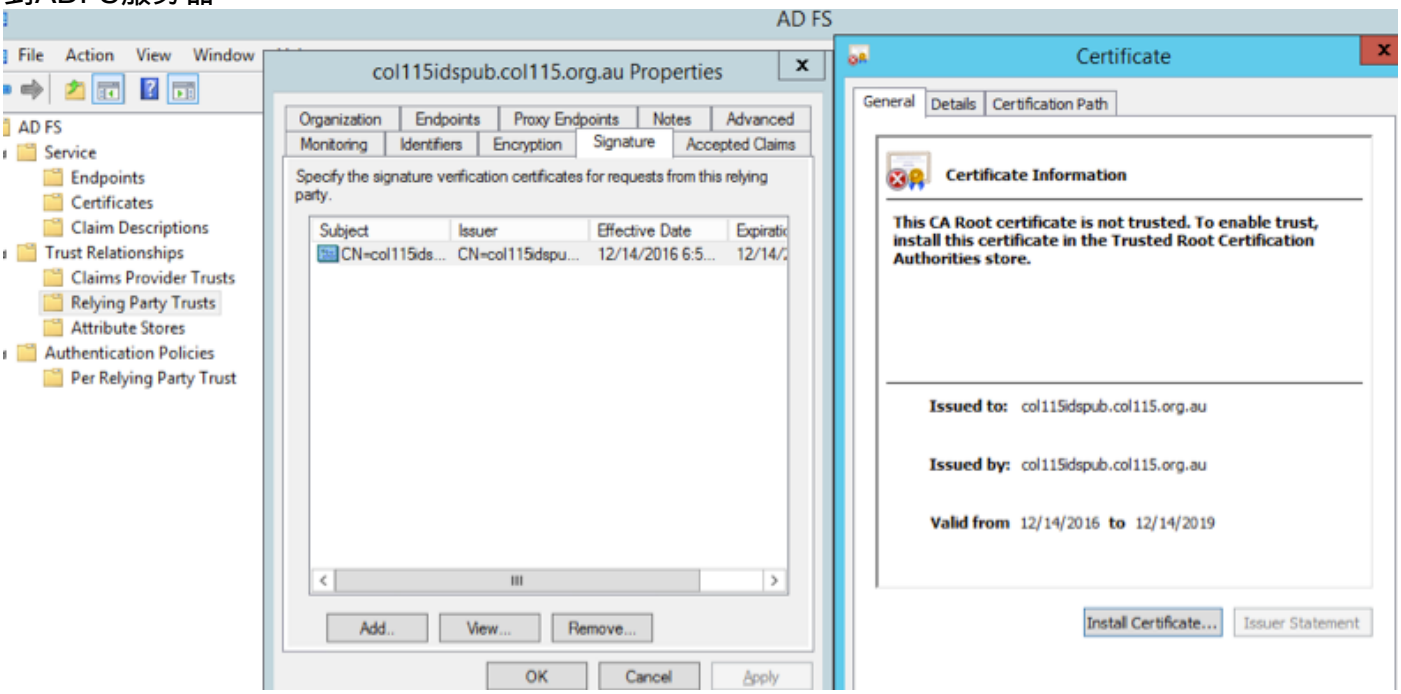



元数据从IDS服务器导入






到ADFS服务器

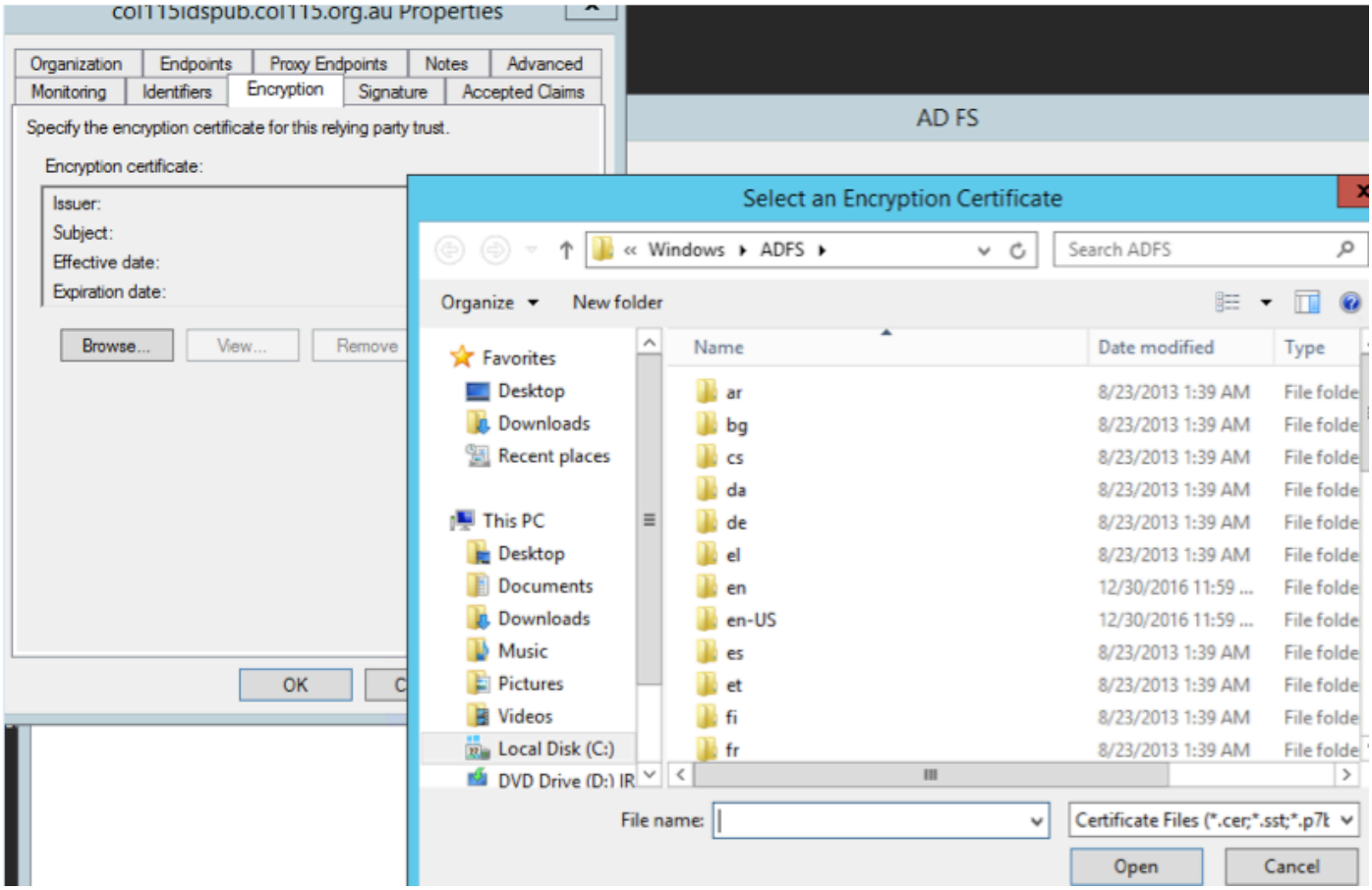



从ADFS边验证

当IDS重新生成时进行元数据交换的SAML认证这一用于签署SAML请求。

**加密/签名键**

默认情况下加密没有被启用。如果加密是启用的，需要被加载到ADFS。




Referecne :

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf