

在(SSO)证书和配置的统一的企业联络中心(UCCE)单个符号

Contents

[Introduction](#)

[Requirements](#)

[Components Used](#)

[部分A. SSO Message消息流](#)

[部分B.在IDP和IDS的Certificates Used](#)

[部分C. IDP详细Certification和配置](#)

[SSL认证\(SSO\)](#)

[配置SSO的\(有签字的内部CA的本地实验室SSL认证的步骤\)](#)

[令牌的签署的认证](#)

[Cisco IDS服务器如何获得令牌的唱歌认证公共密钥？](#)

[加密不是启用的](#)

[部分D. Cisco IDS边认证](#)

[SAML认证](#)

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

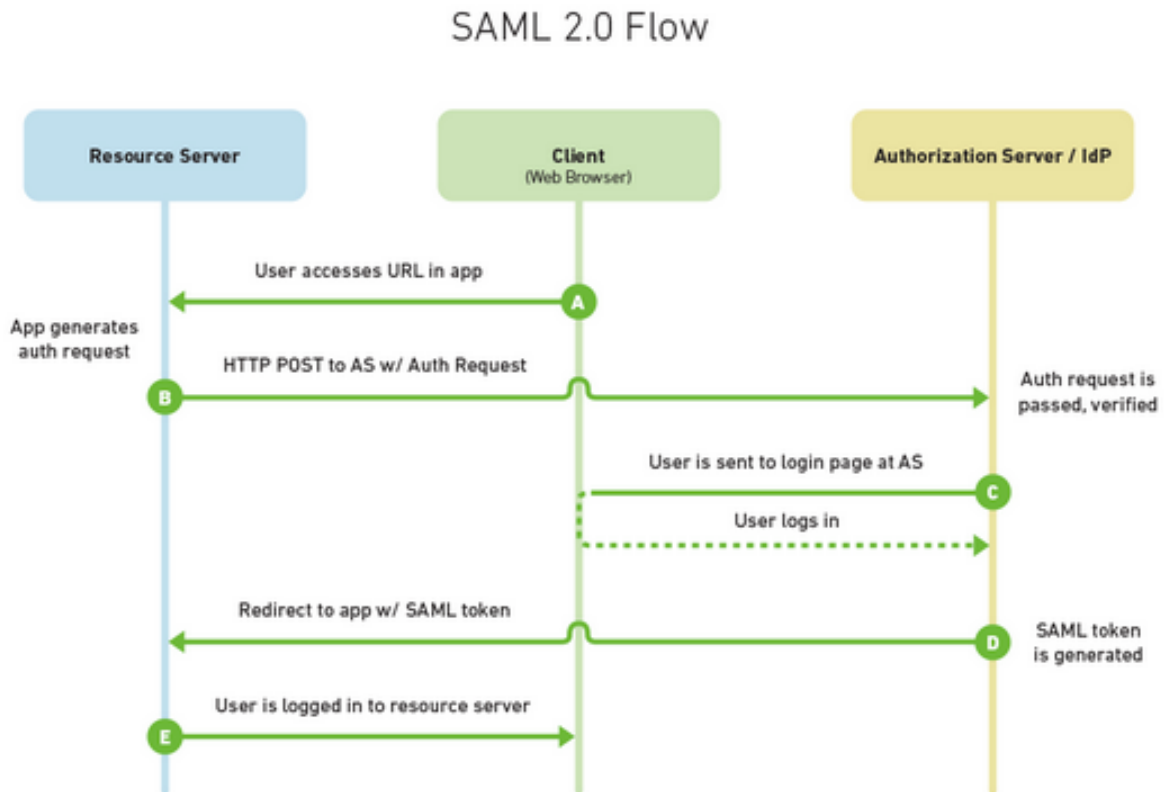
Components Used

UCCE 11.5

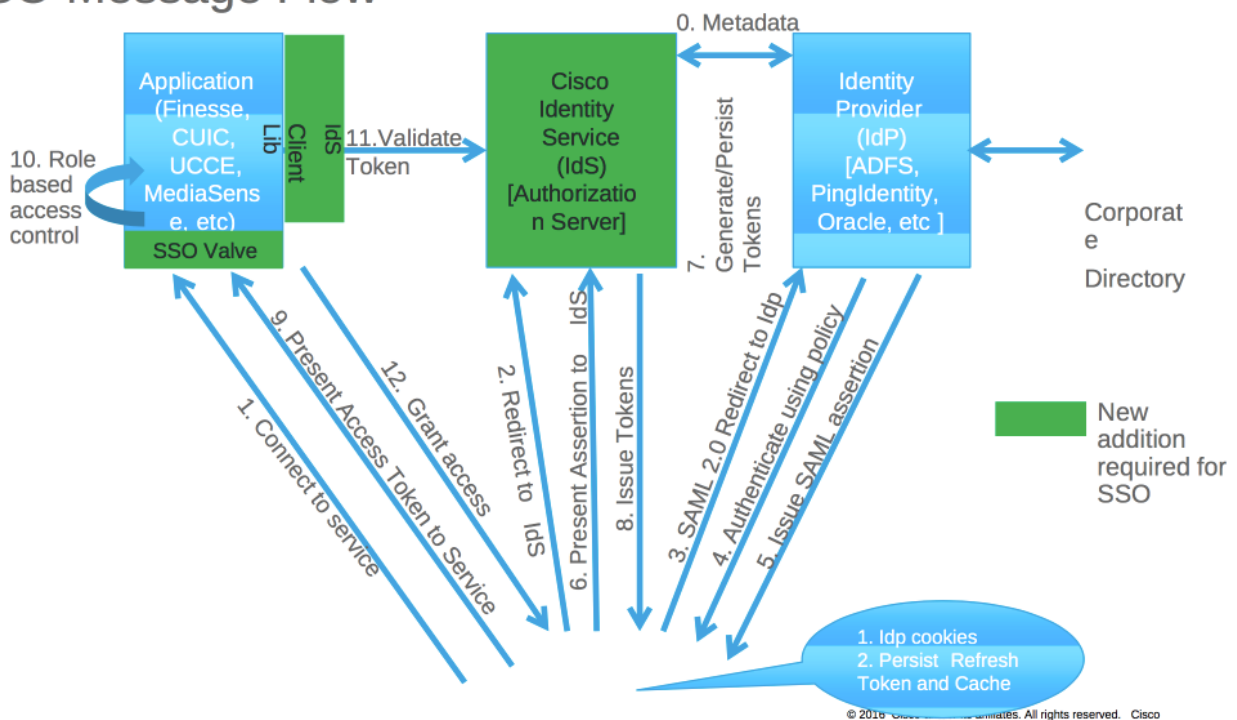
Windows 2012个R2

部分A. SSO Message消息流

The most common SAML flow is shown below:



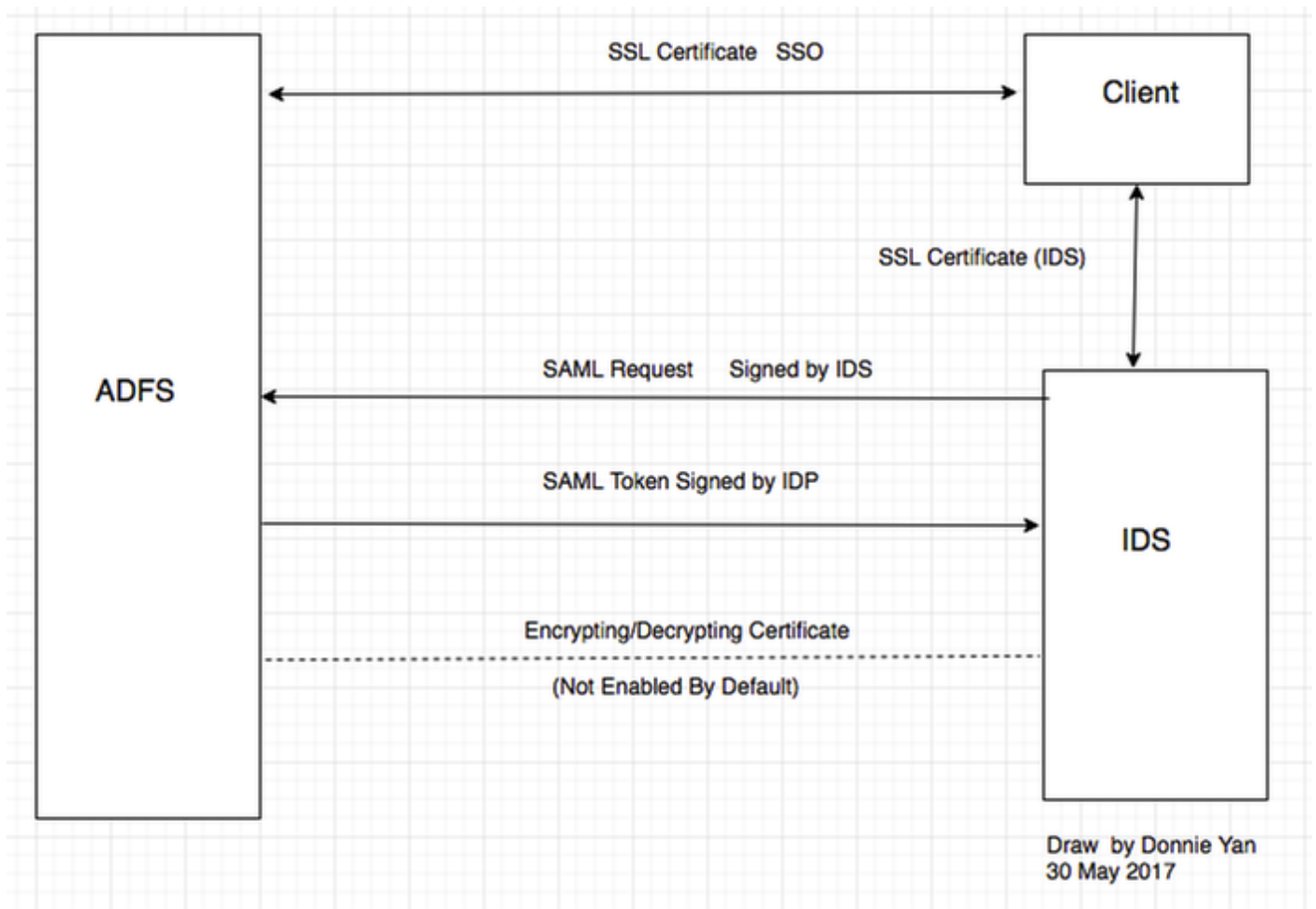
SSO Message Flow



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pplication时候，使用此有效令牌登录

部分B.在IDP和IDS的Certificates Used



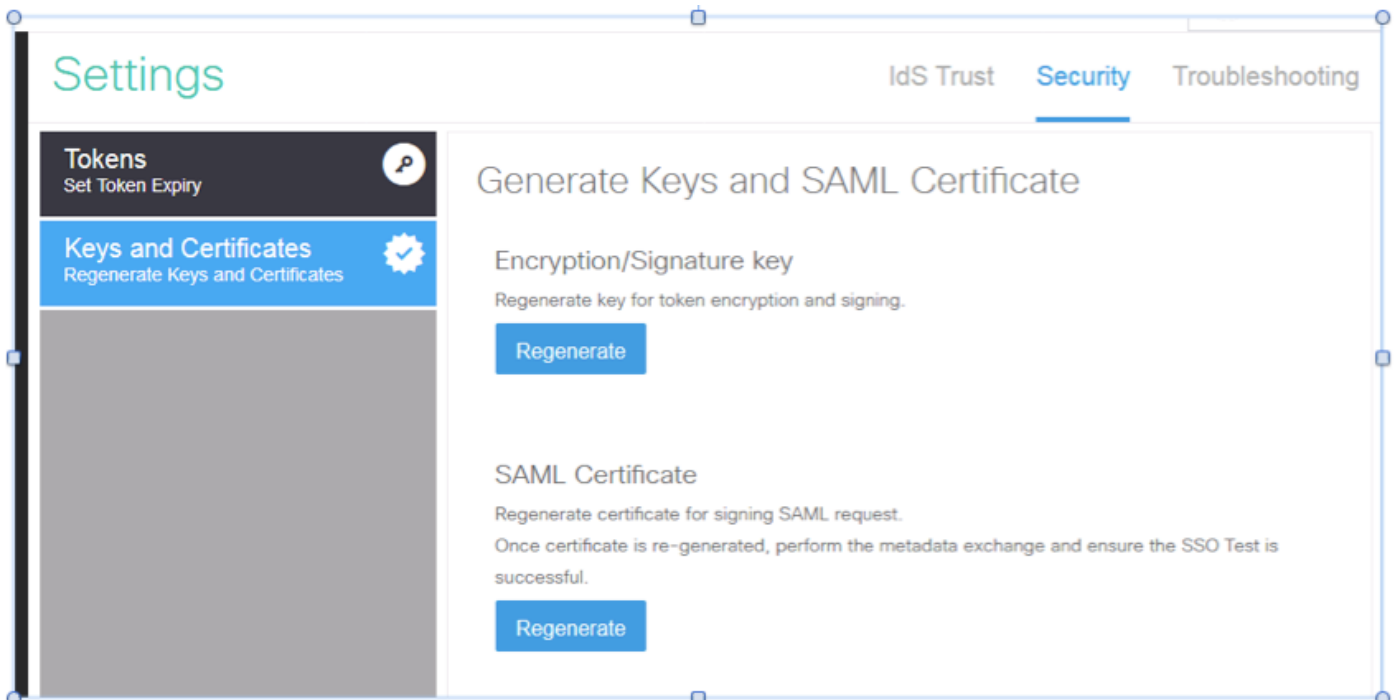
IDP证书

- SSL认证(SSO)
- 令牌的签署的认证
- 令牌-解码

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=col115dc.col115.org.au, OU=TAC, O=Cisco...	CN=col115-COL115-CA, ...	12/30/2016	12/30/2017		
Token-decrypting					
CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co...	12/30/2016	12/30/2017		Primary
Token-signing					
CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11...	12/30/2016	12/30/2017		Primary

IDS证书

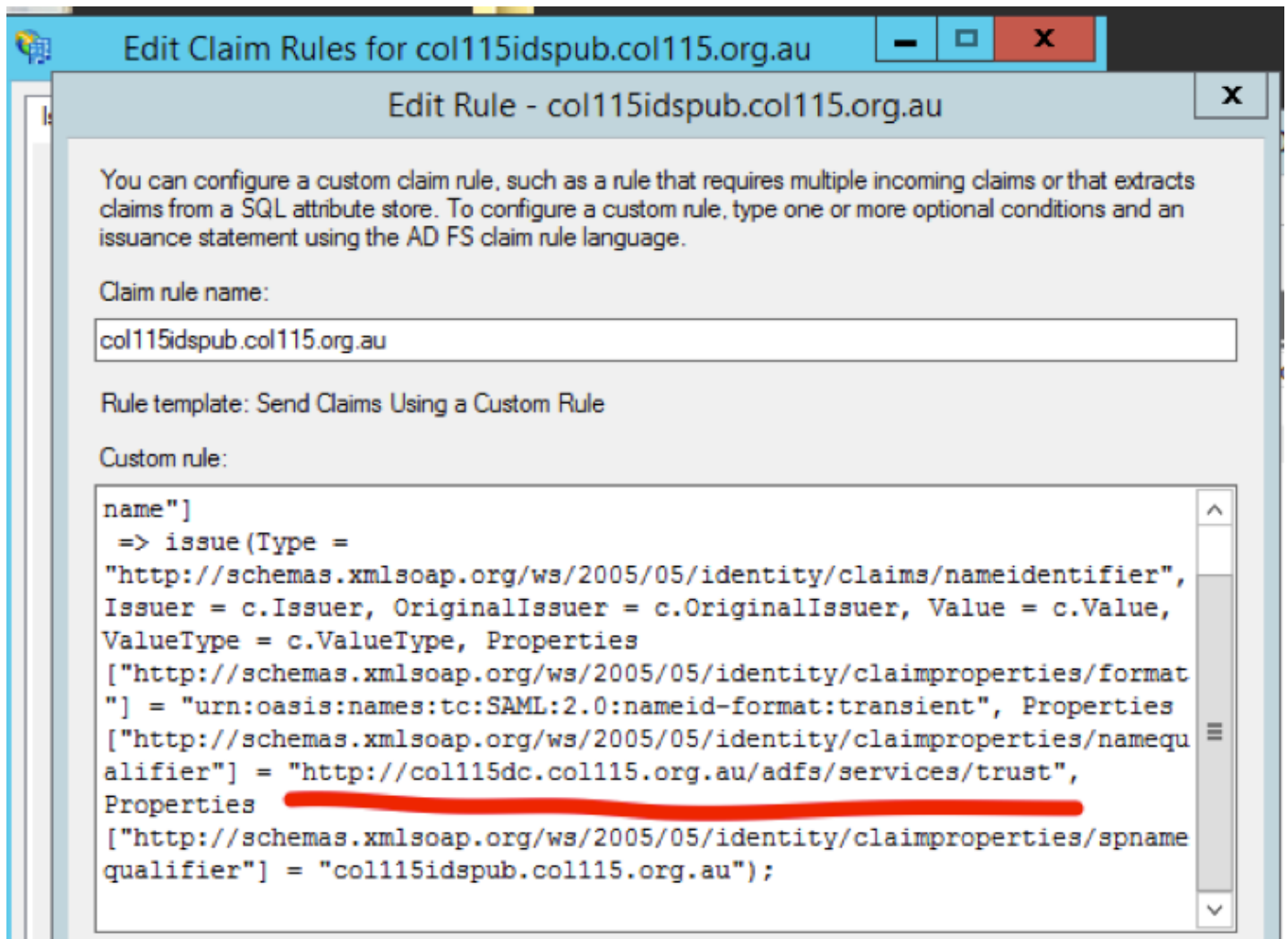
- SAML认证
- 签名键
- 加密密钥



部分C. IDP详细Certification和配置

SSL认证(SSO)

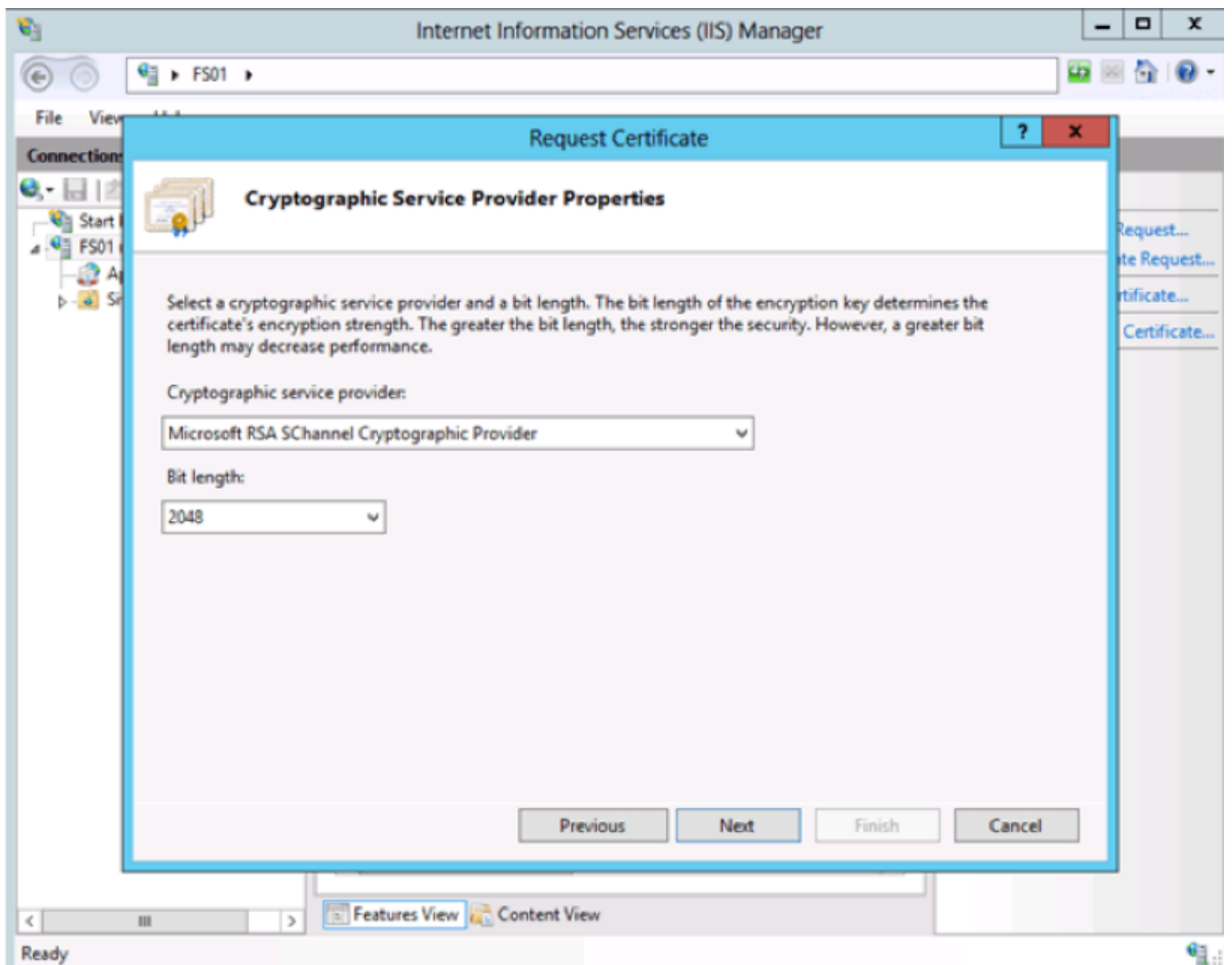
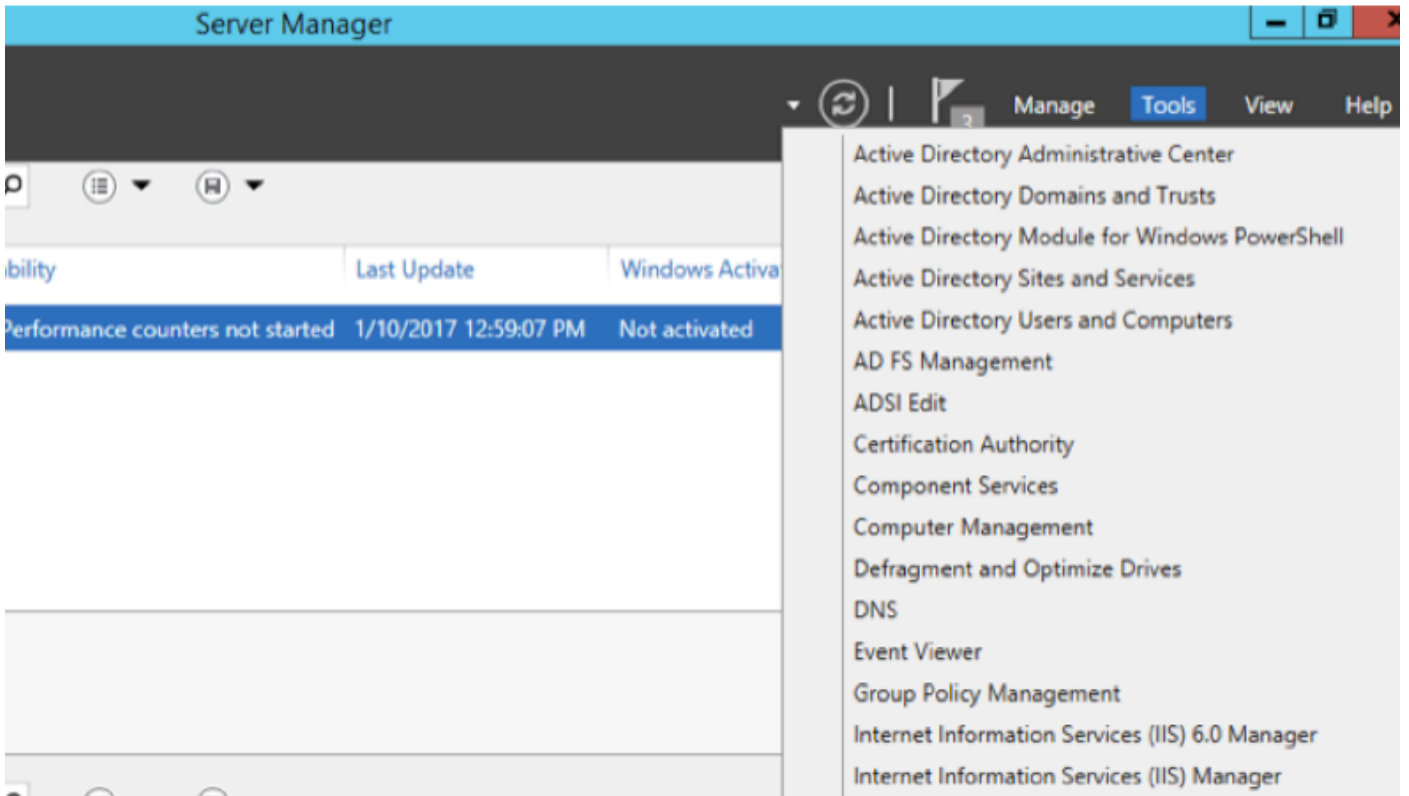
- 此认证使用在IDP和客户端之间。客户端必须委托SSO认证
- 放置SSL认证加密在客户端和IDP服务器之间的会话。此认证不是特定的对ADFS，然而特定对IIS
- SSL认证的主题必须与用于ADFS配置的名字配比



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。

Microsoft Active Directory Certificate Services -- col115-COL115-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity, communicate with others over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Additional Attributes:

Attributes:

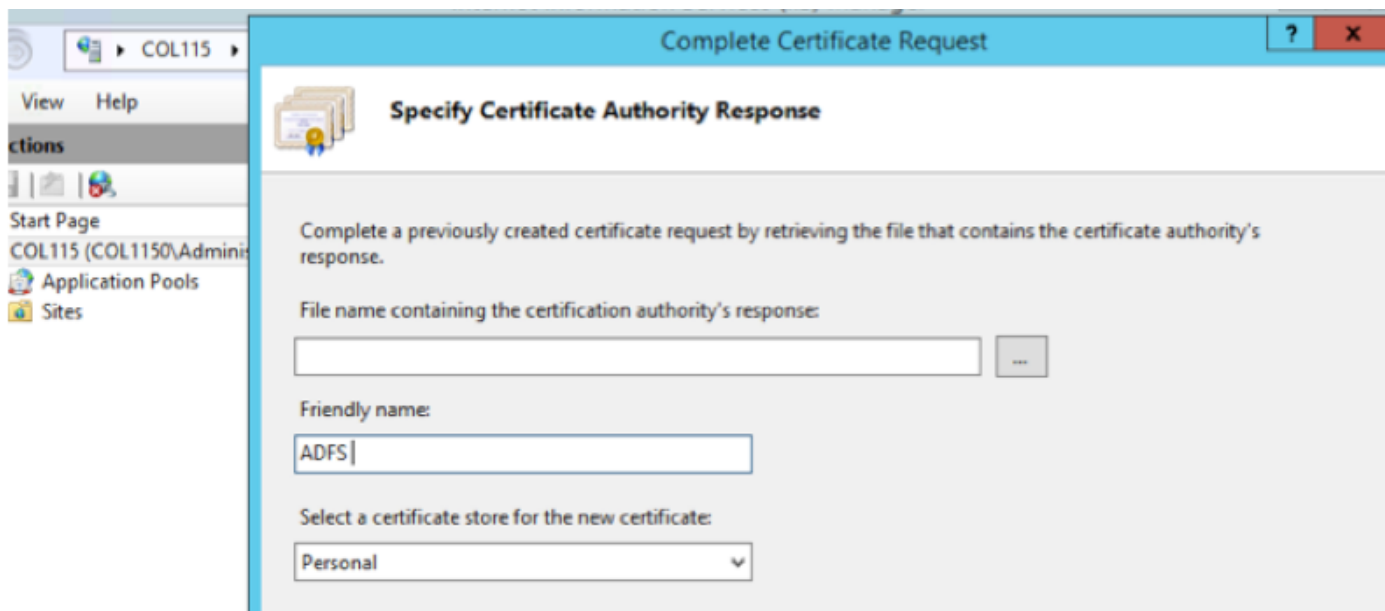
Submit >

步骤3.安装签名的证书回到ADFS服务器并且分配到ADFS功能。

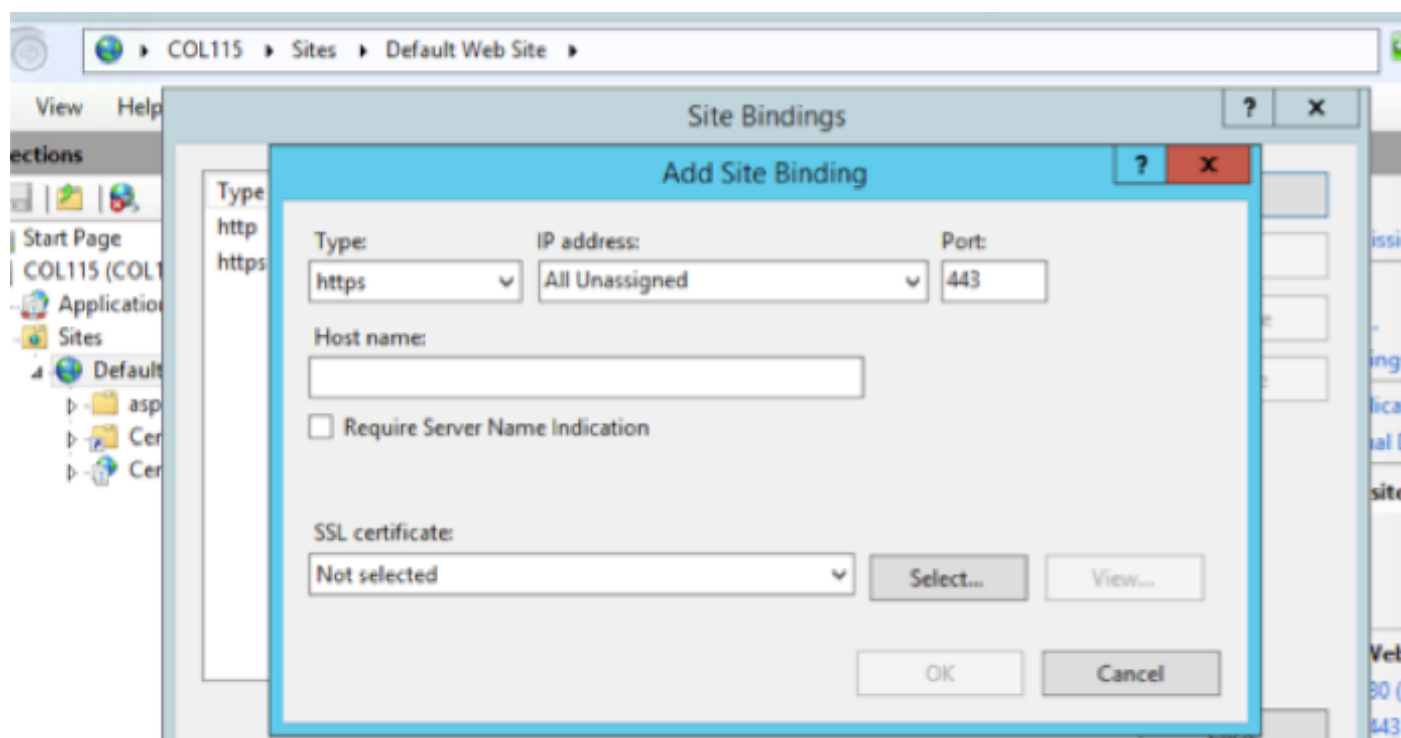
1. 安装签名的证书回到ADFS服务器。为了执行此，请打开服务器manager>Tools>Click互联网信息 Services(IIS) Manager>。

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。

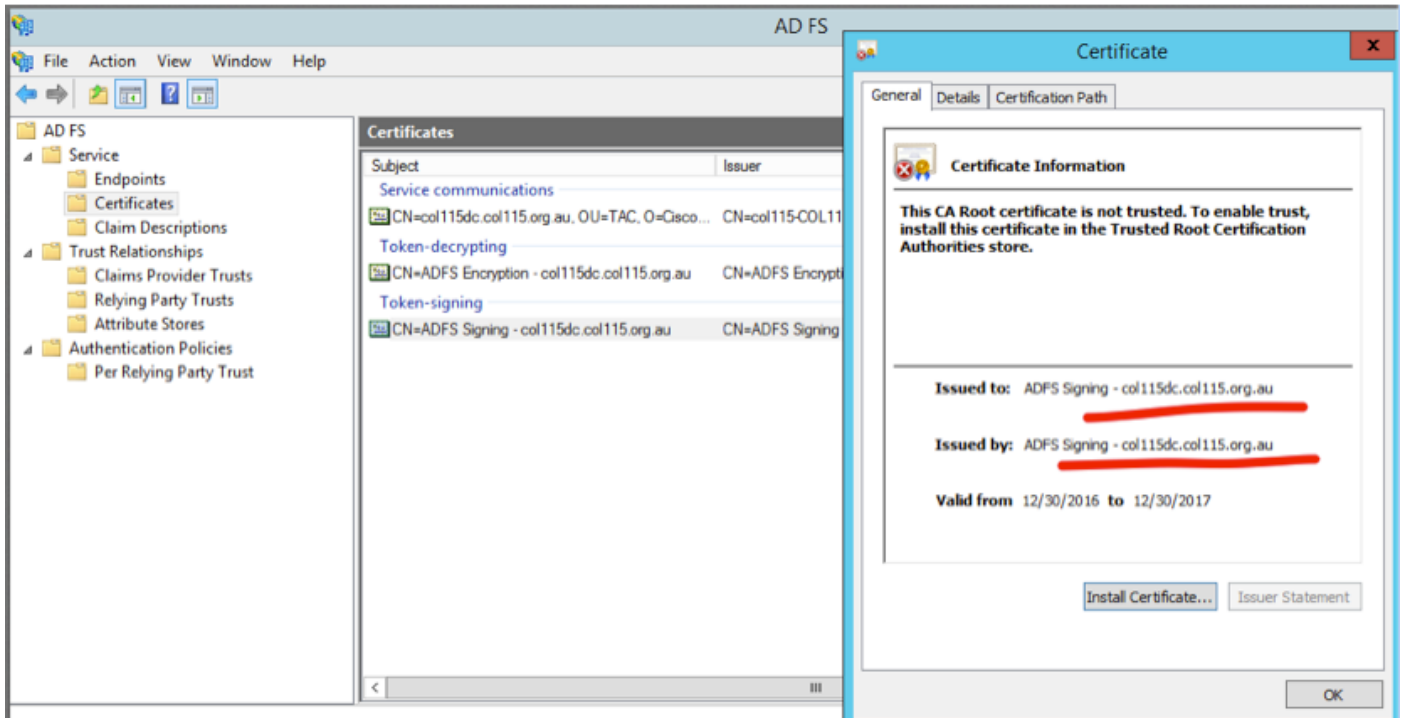
Note:在ADFS功能的安装时，必须使用早先SSL认证。

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)。



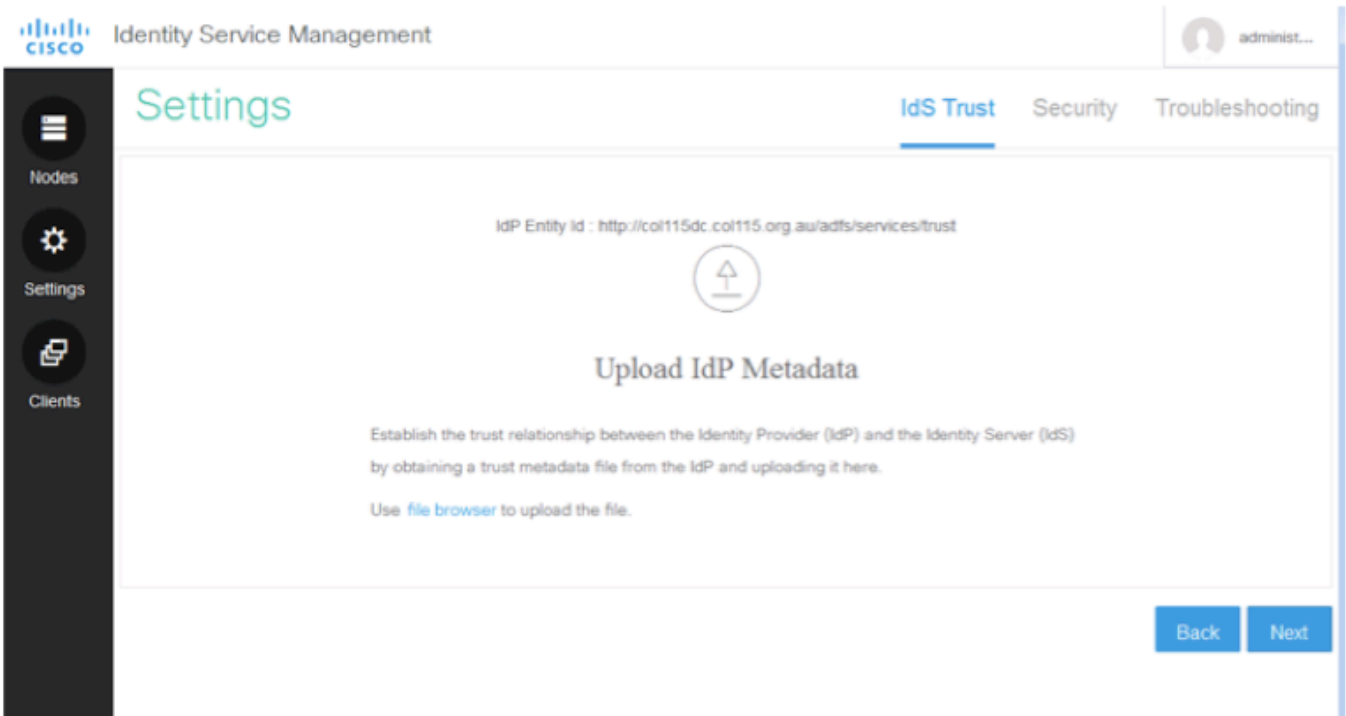
Cisco IDS服务器如何获得令牌的唱歌认证公共密钥？

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>。

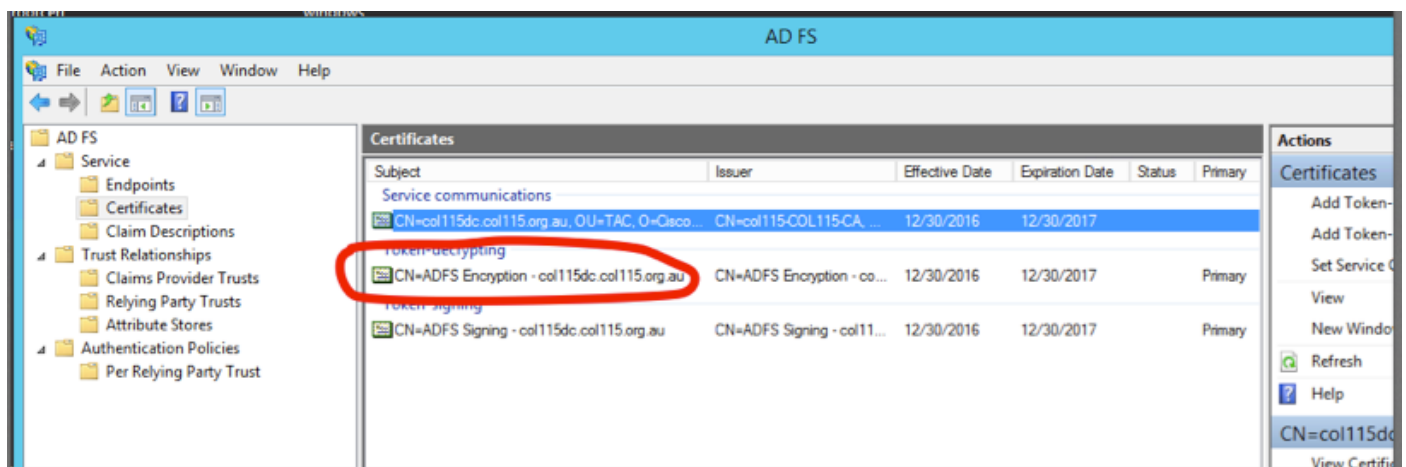
```
35
36 --<KeyDescriptor use="signing">
37
38
39 --<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
40
41
42 --<X509Data>
43
44 <X509Certificate>MIIC6DCCAdCgAwIBAgIQFpYJVv99CK9LN50rMdF5nDANBgkqhkiG9w0BAQsFADAwMS4wL5Y2Z295MTE1Lm9yZy5hdTCCASIwDQYJKoZIhvcNAQEBBQADggE...
45
```

从ADFS元数据



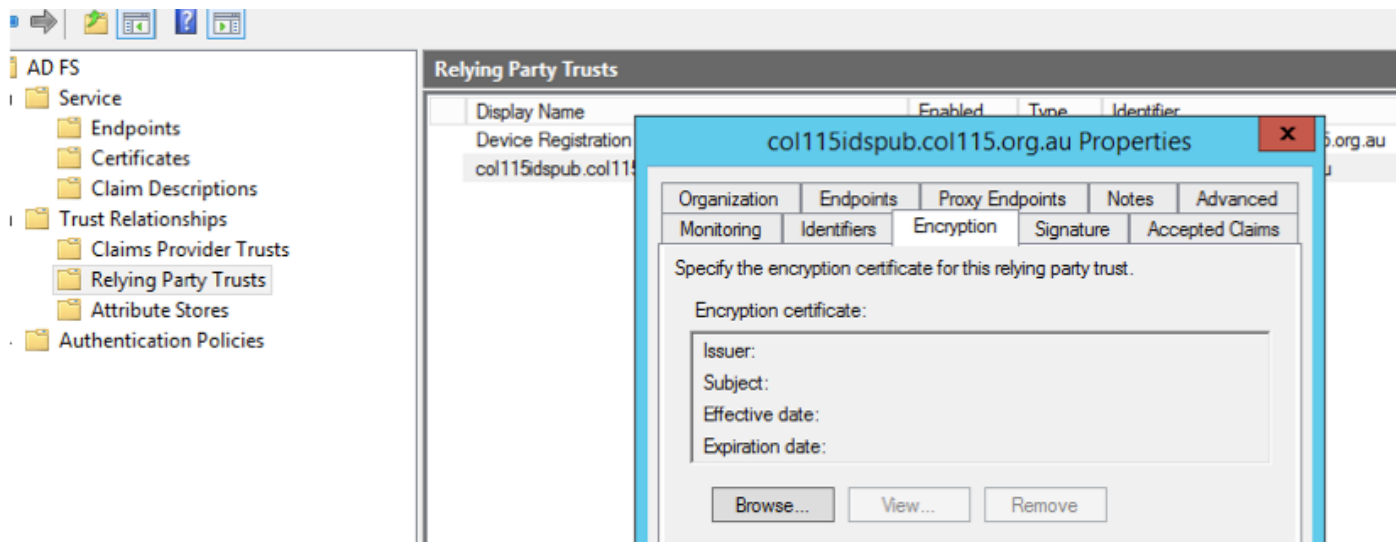
加载ADFS元数据到IDS 令牌的解密

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decrypting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。

Identity Service Management

Nodes

Node	Status	SAML Certificate Expiry
col115idspub.col115.org.au ★	In Service	12-14-2019 18:58 (930 days left)

col115idspub.col115.org.au Properties

Subject	Issuer	Effective Date	Expiration Date
CN=col115de...	CN=col115dspu...	12/14/2016 6:5...	12/14/2019

Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: col115idspub.col115.org.au

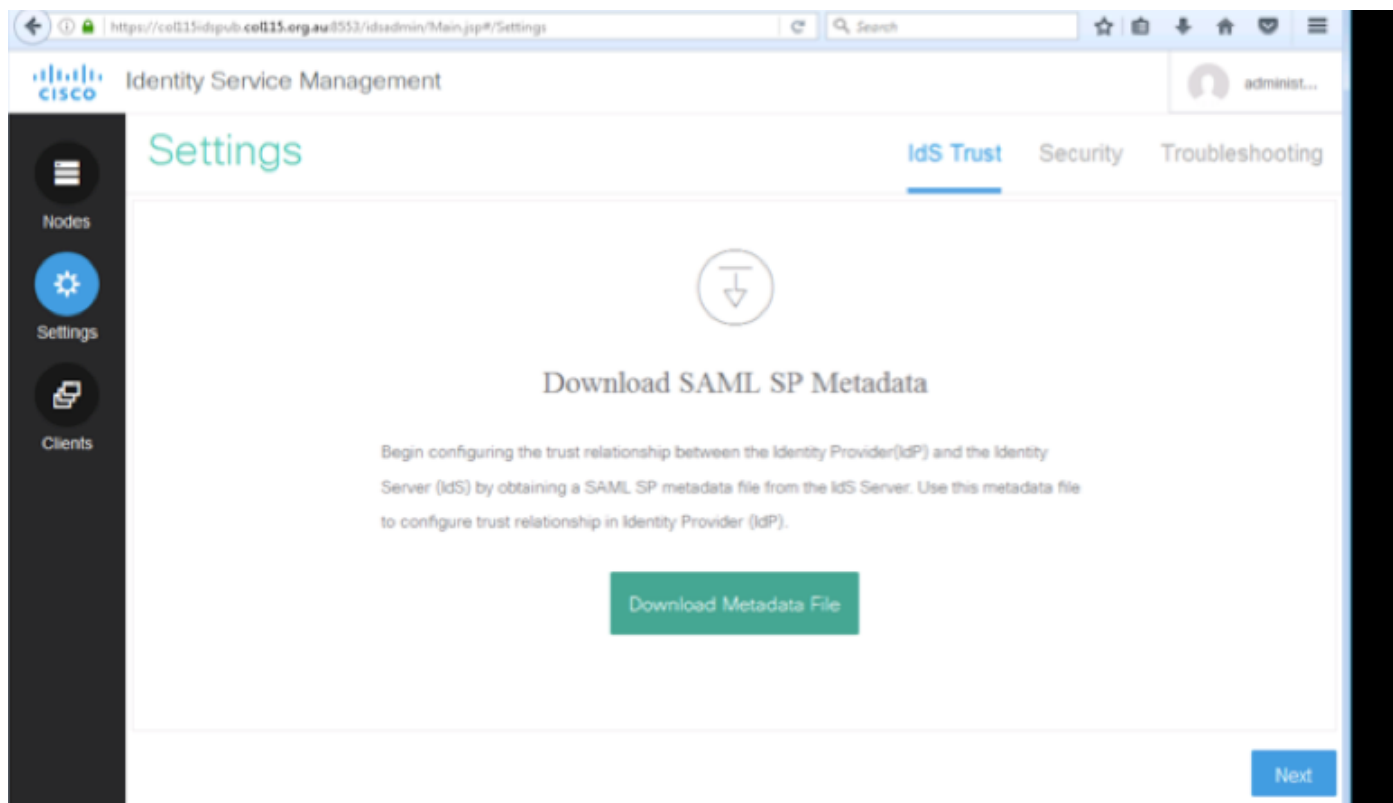
Issued by: col115idspub.col115.org.au

Valid from 12/14/2016 to 12/14/2019

Install Certificate... Issuer Statement

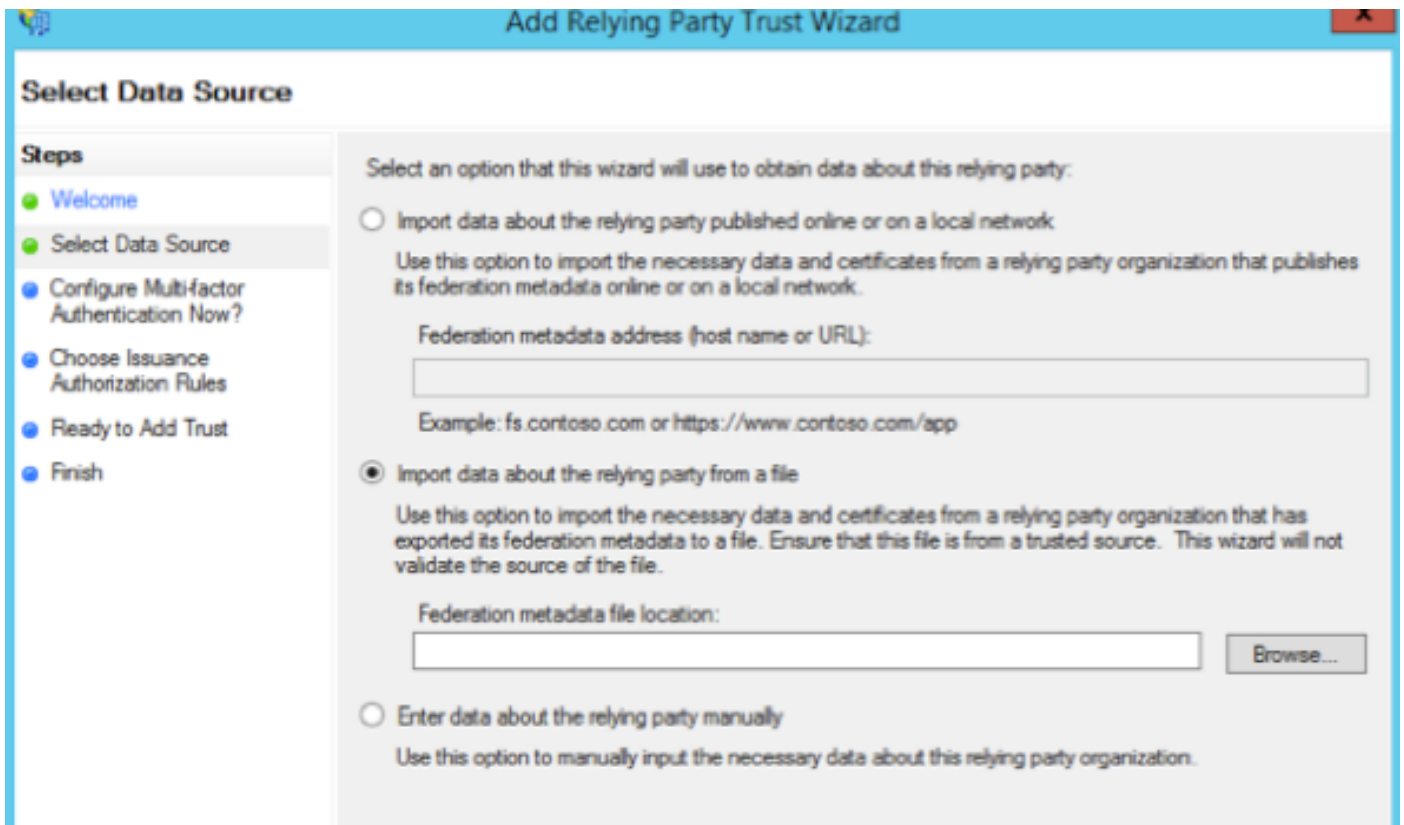
此认证用于签署SAML请求，并且发送到IDP (ADFS)。此公共密钥在IDS元数据，并且必须导入ADFS服务器。

1. Download SAML从IDS服务器的SP元数据。
2. 对https:// <ids服务器FQDN>:8553/idsadmin/的Browser。
3. 选择设置和下载SAML SP元数据并且保存它。

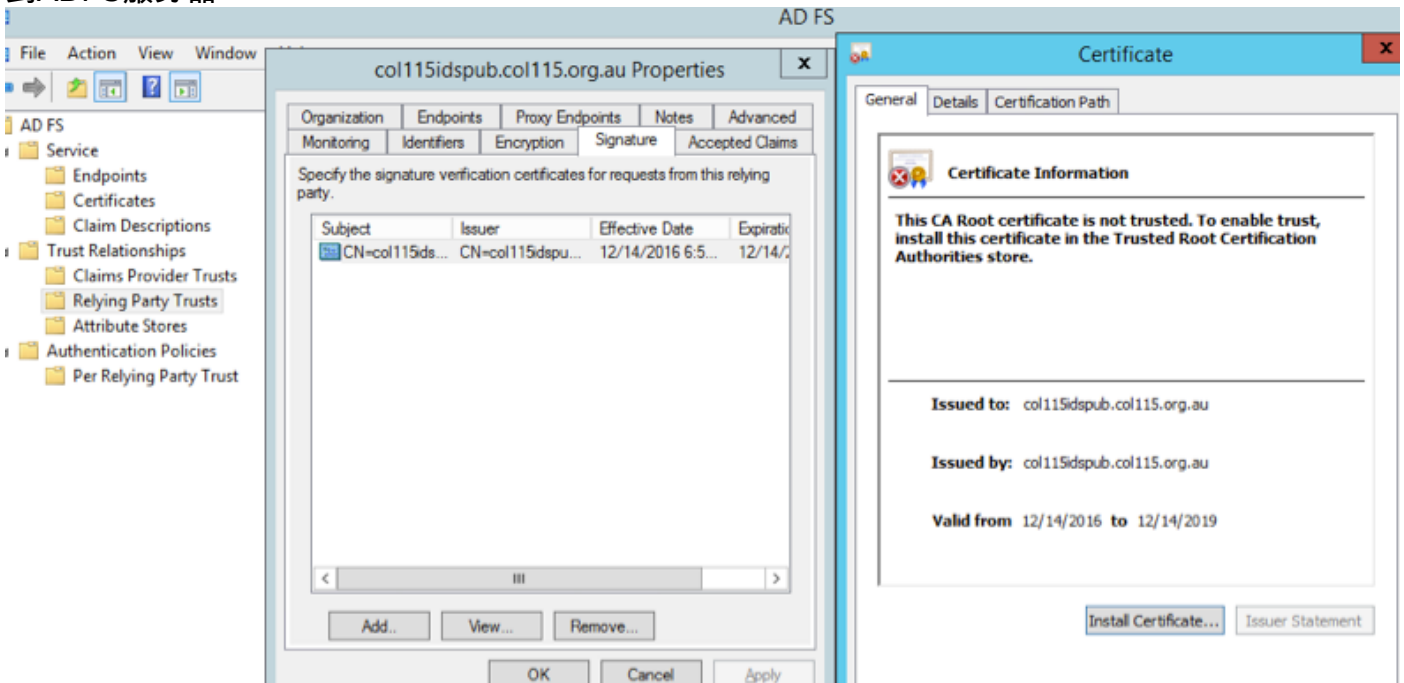


元数据从IDS服务器导入

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="col115idspub.col115.org.au" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
    - <KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
          <ds:X509Certificate>MIIC+TCC AeGgAwIBAgIEWD4KIDANBgkqhkiG9w0BAQUFADAISMwIQYDVQQDExpjb2wxMTVpZHNw
          dWIuY29sMTE1Lm9yZy5hdTAeFw0xNjEyMTQwNzU4MjVhFw0xOTEyMTQwNzU4MjVhMCUxIzAhBgNV
          BAMTGmNvbDExNWlkc3B1Yi5jb2wxMTUub3JnLmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
          CoKCAQEAa4Qca9euyTuxYcHM+MhS/Yb+K3CZY1eCQw00d0G50hfwCaw176/CVRuFHu713vA2e3
```



到ADFS服务器

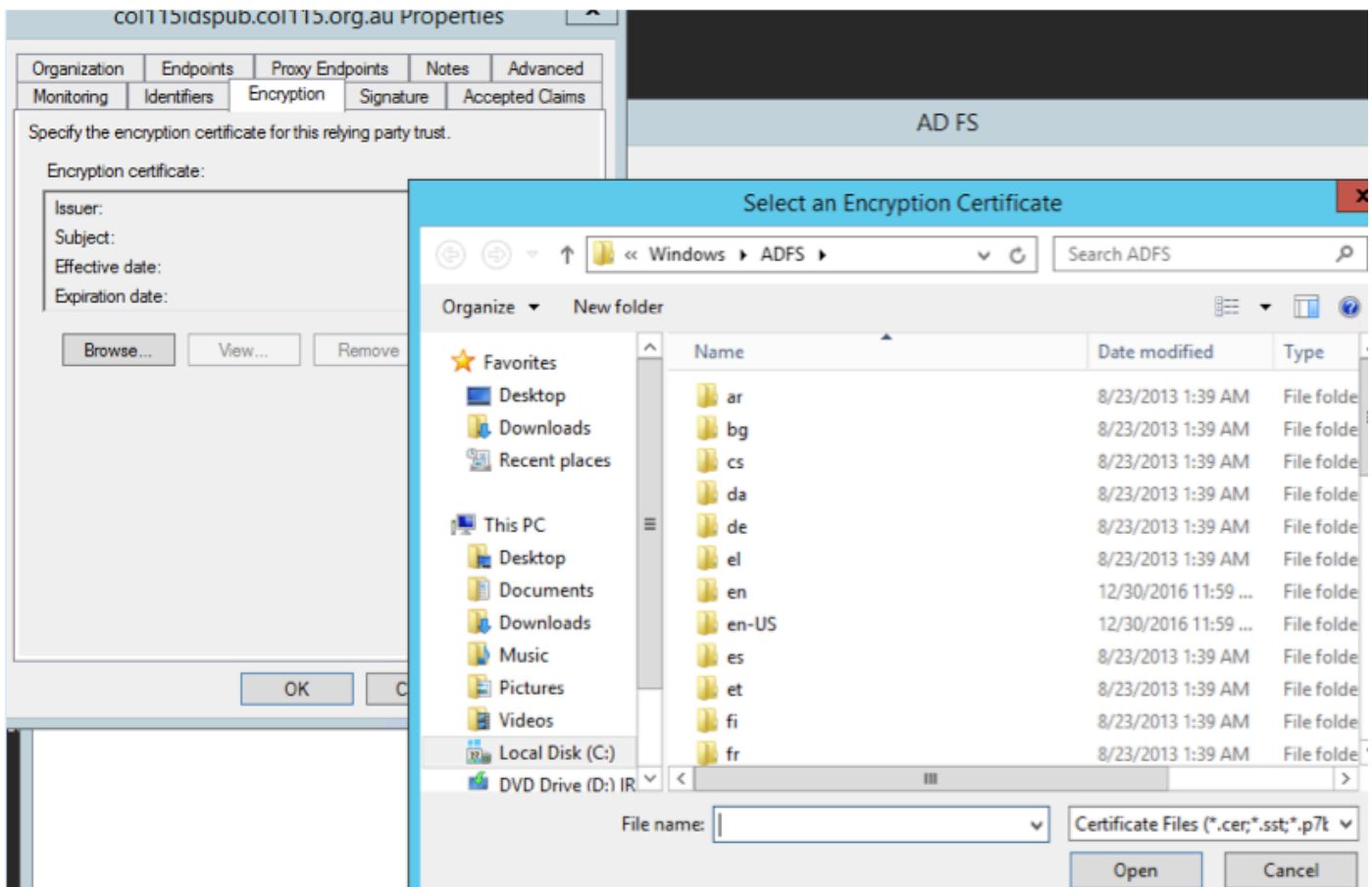


从ADFS边验证

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/cm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf