Muestra unificada de la empresa del Centro de contacto sola (UCCE) en los Certificados (SSO) y la configuración

Contenido

Introducción

Este documento describe las configuraciones del certificado que se requieren para UCCE SSO. La configuración de esta característica implica varios Certificados para el HTTPS, la firma digital y el cifrado.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 11.5 UCCE
- Microsoft Active Directory (AD) - AD instalado en el Servidor Windows
- Versión 2.0/3.0 del servicio de la federación del Active Directory (ADFS)

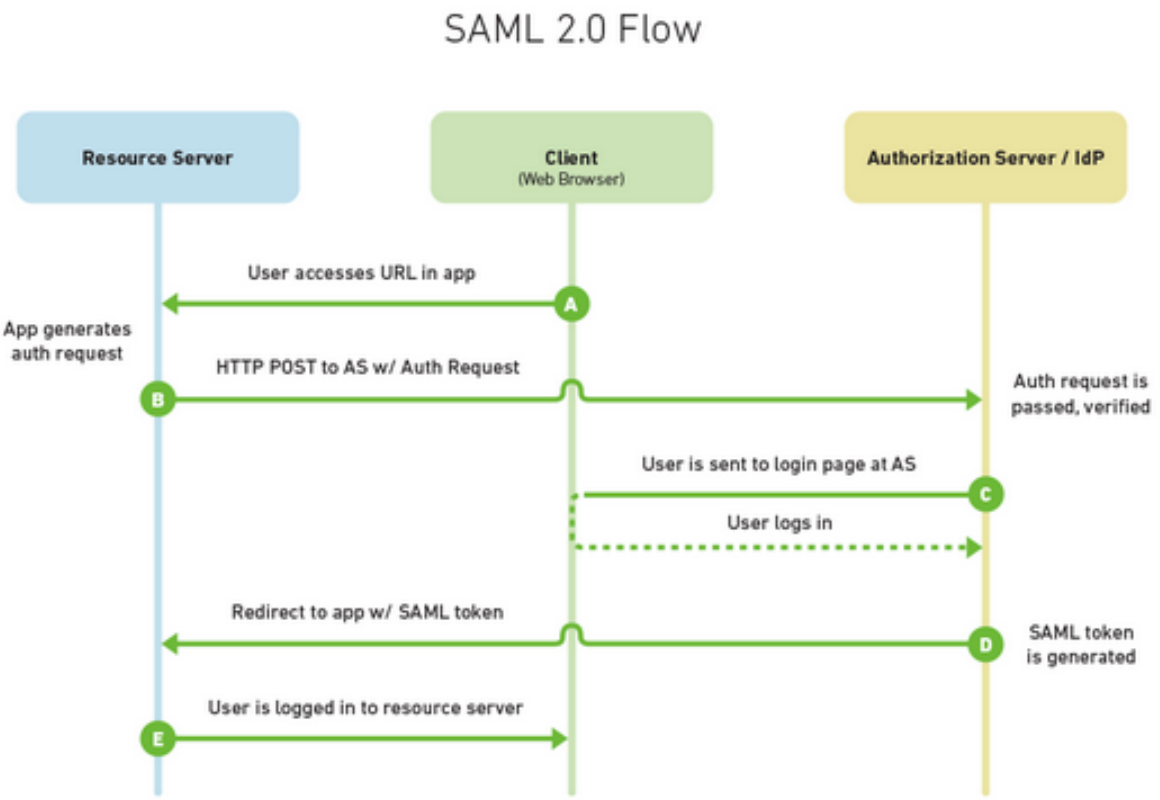
Componentes Utilizados

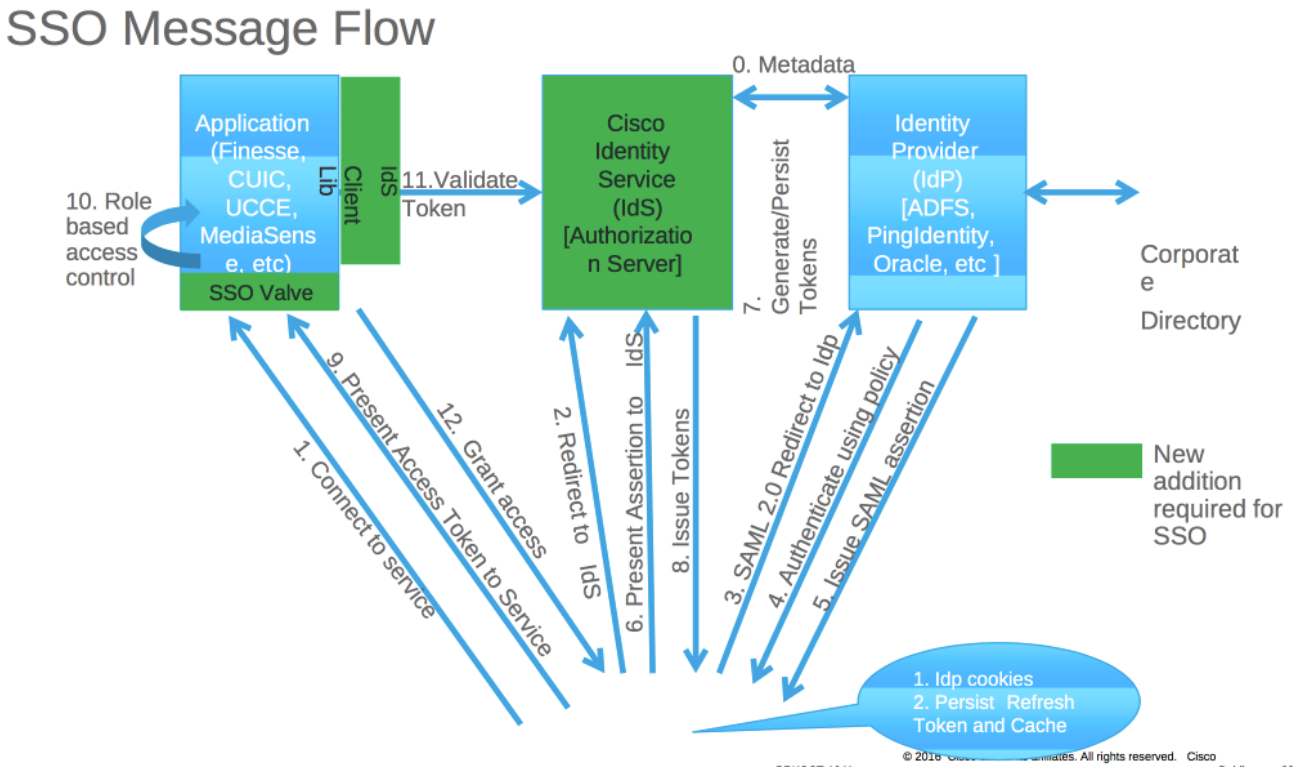
UCCE 11.5

R2 de Windows 2012

Parte A. SSO Message Flow

The most common SAML flow is shown below:



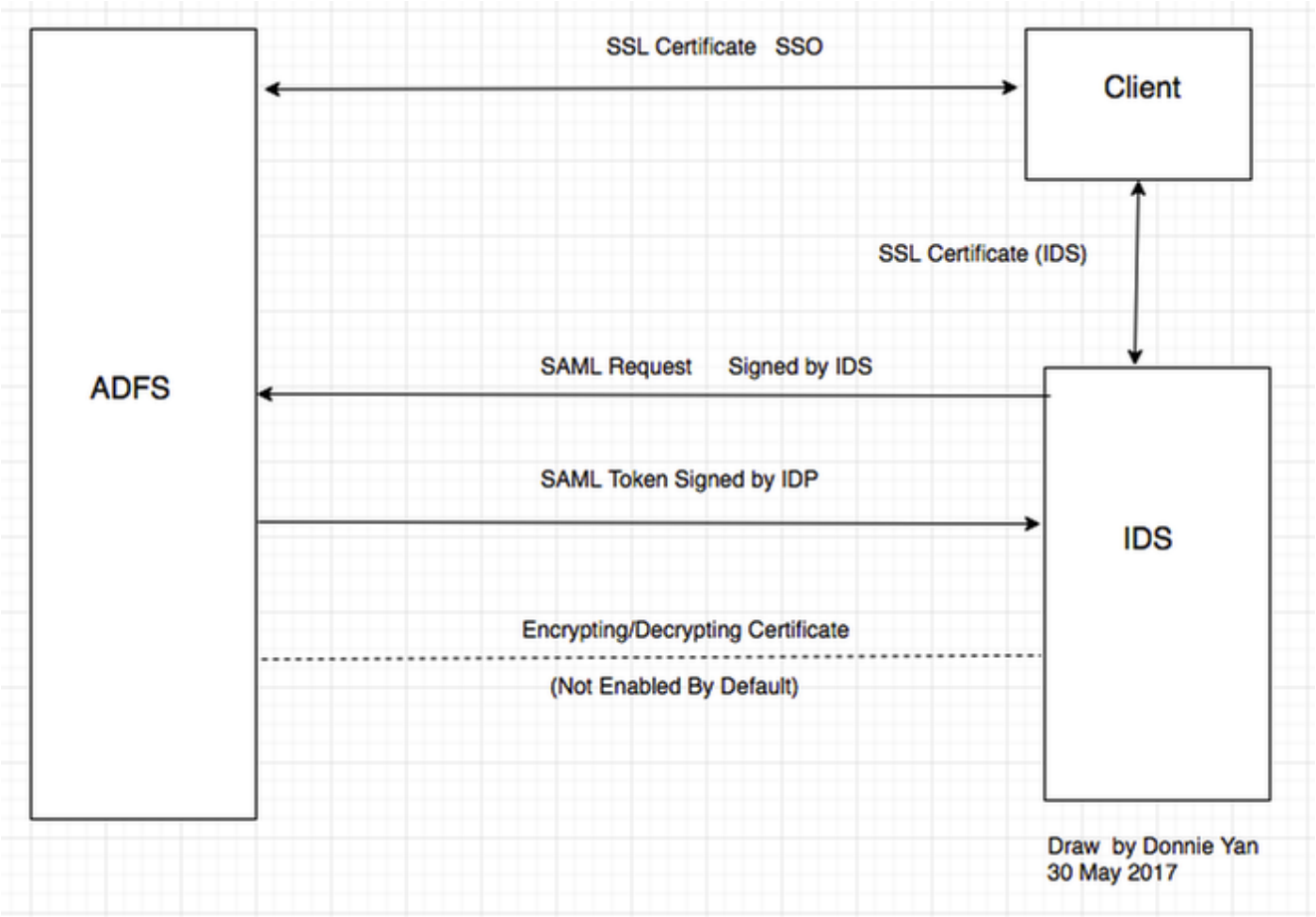


Cuando se habilita el SSO, cuando el agente abre una sesión al escritorio de la delicadeza:

- El servidor de la delicadeza reorienta al navegador del agente para comunicar con el servicio de la identidad (el IDS)
- El IDS reorienta al navegador del agente al proveedor de la identidad (IDP) con la petición de SAML
- IDP genera SAML el token y pasa al Servidor IDS

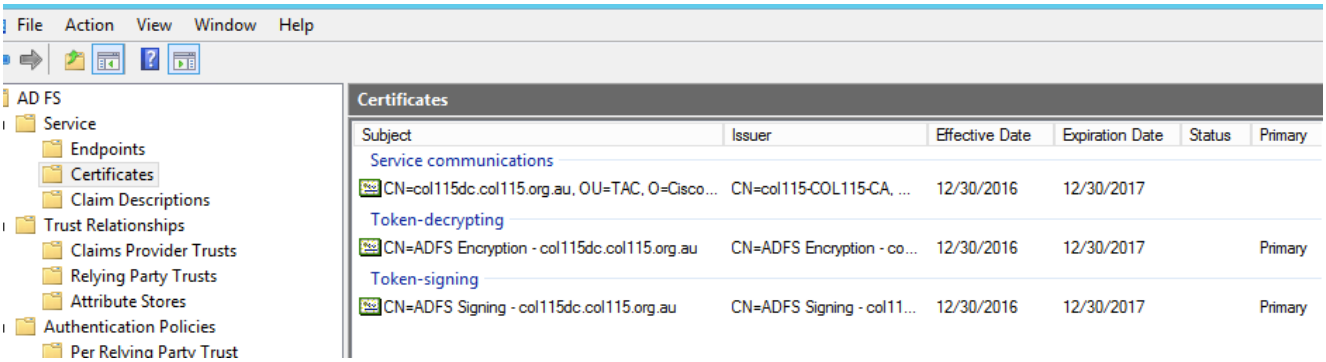
- Cuando el token fue generado, cada vez que el agente hojea al ppplication, utiliza este token válido para el login

Parte B. Certificates Used en IDP y el IDS



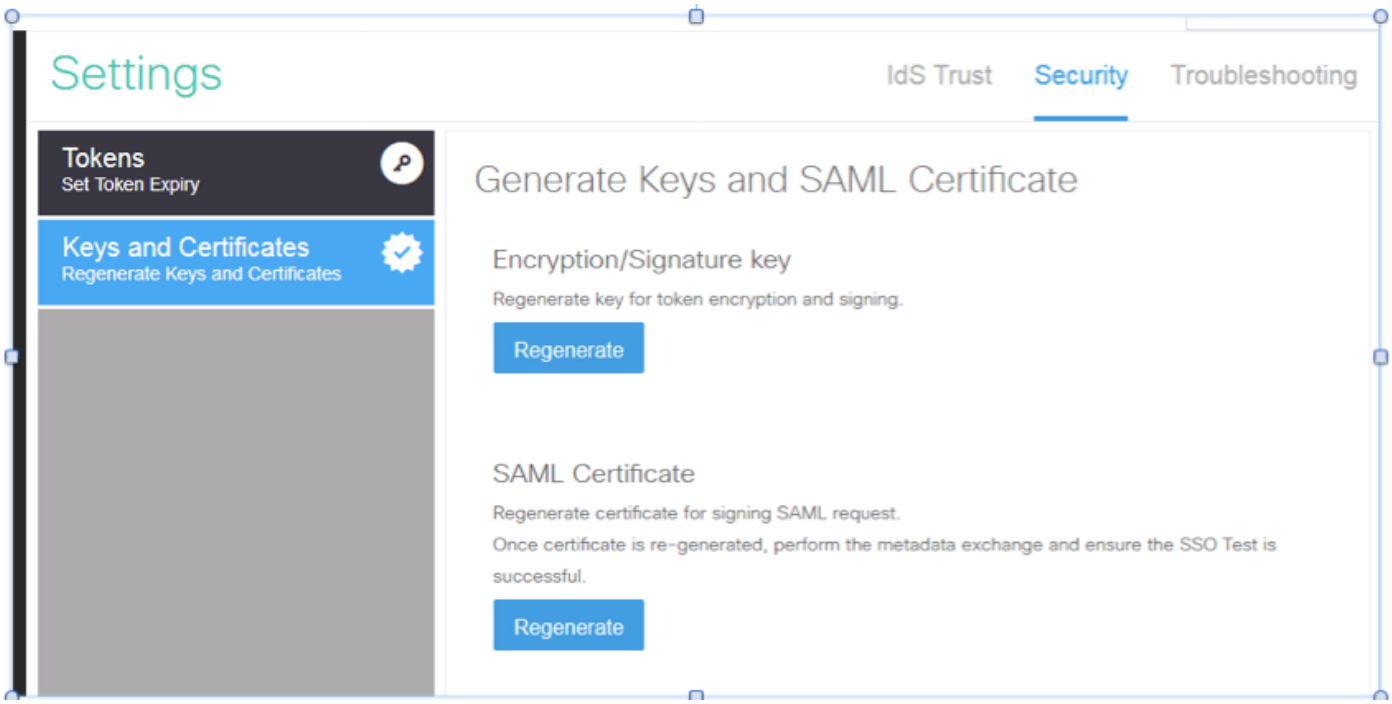
Certificados IDP

- Certificado SSL (SSO)
- Certificado de firma simbólico
- Token – desencriptando

1. 

Certificados IDS

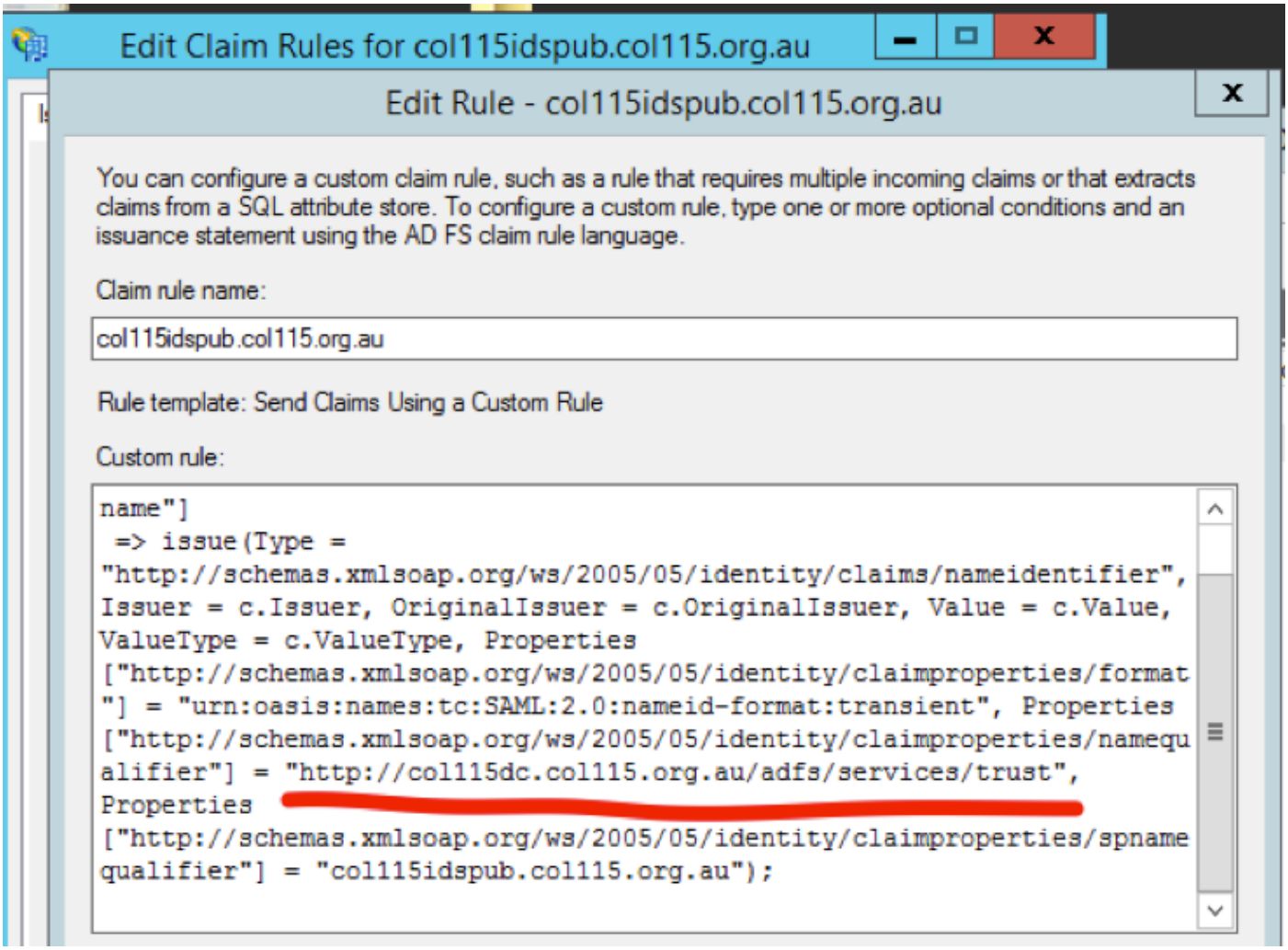
- SAML certificado
- Clave de la firma
- Clave de encripción



Parte C. IDP Certification detalladamente y configuración

Certificado SSL (SSO)

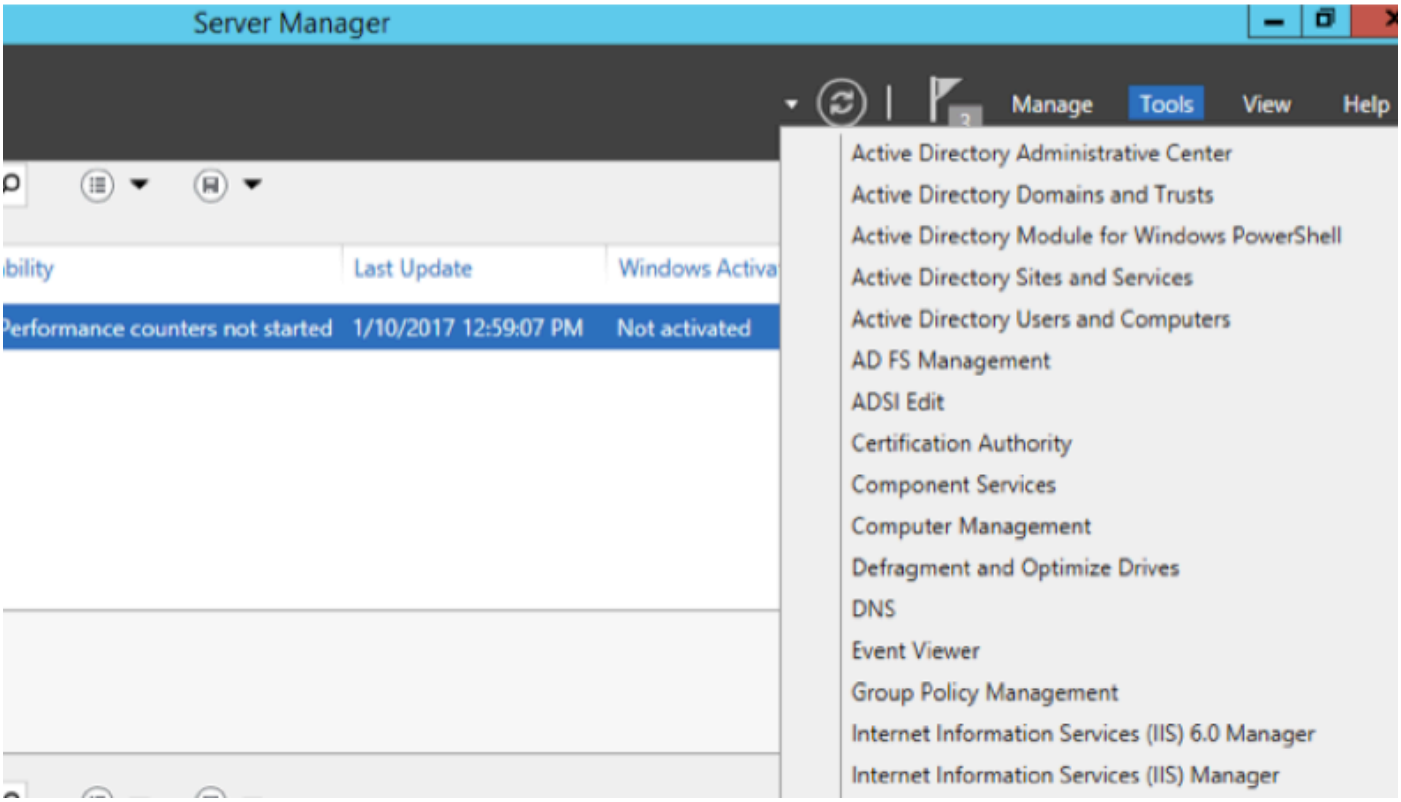
- Este certificado se utiliza entre IDP y el cliente. El cliente debe confiar en el certificado SSO
- El certificado SSL se coloca para cifrar la sesión entre el cliente y el servidor IDP. Este certificado no es específico a ADFS, sino al específico al IIS
- El tema del certificado SSL debe hacer juego con el nombre usado en configuración ADFS

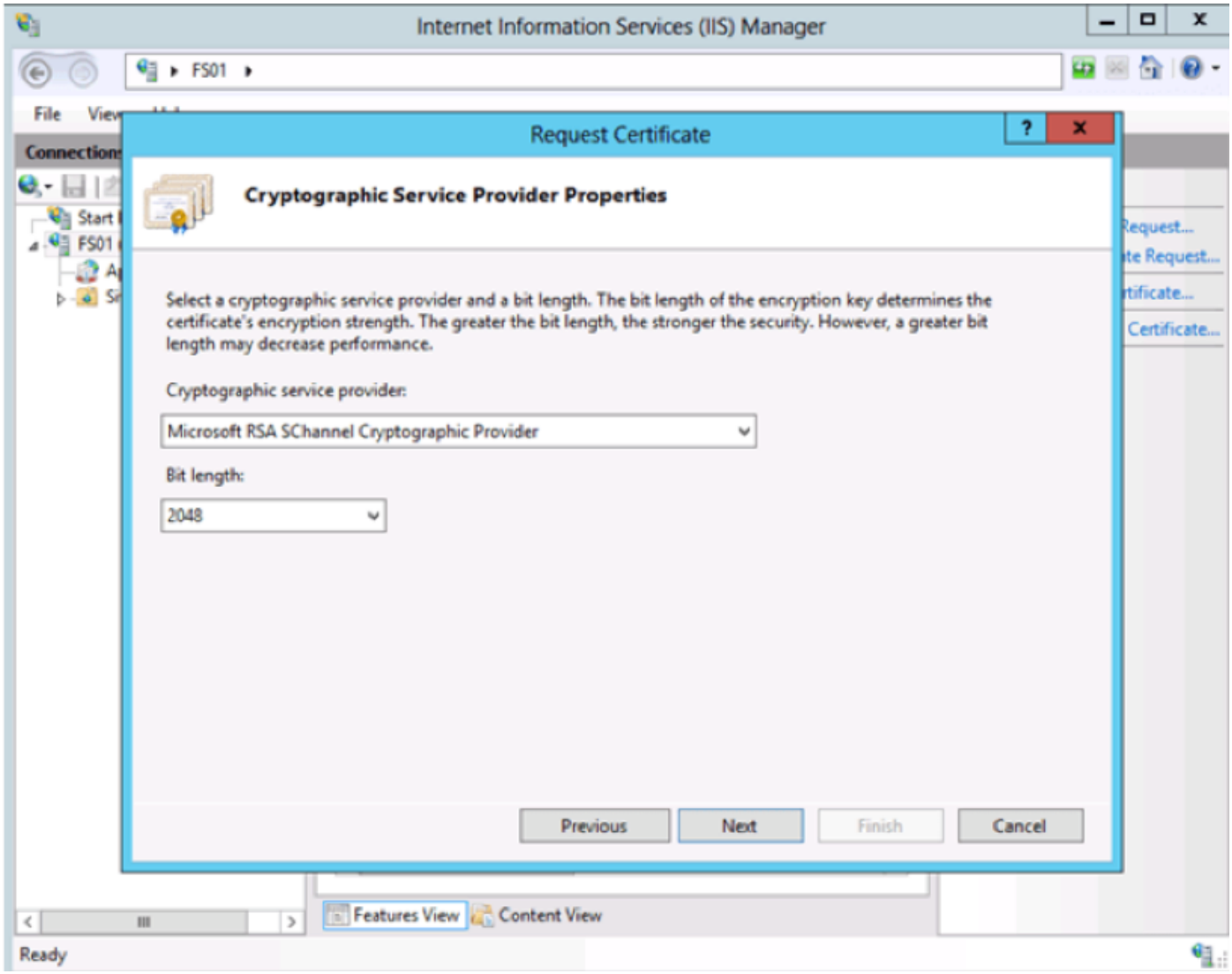


Pasos para configurar el certificado SSL para el SSO (el laboratorio local con CA interno firmó)

Paso 1. Cree el certificado SSL con el pedido de firma de certificado (CSR) y la muestra por CA interno para ADFS.

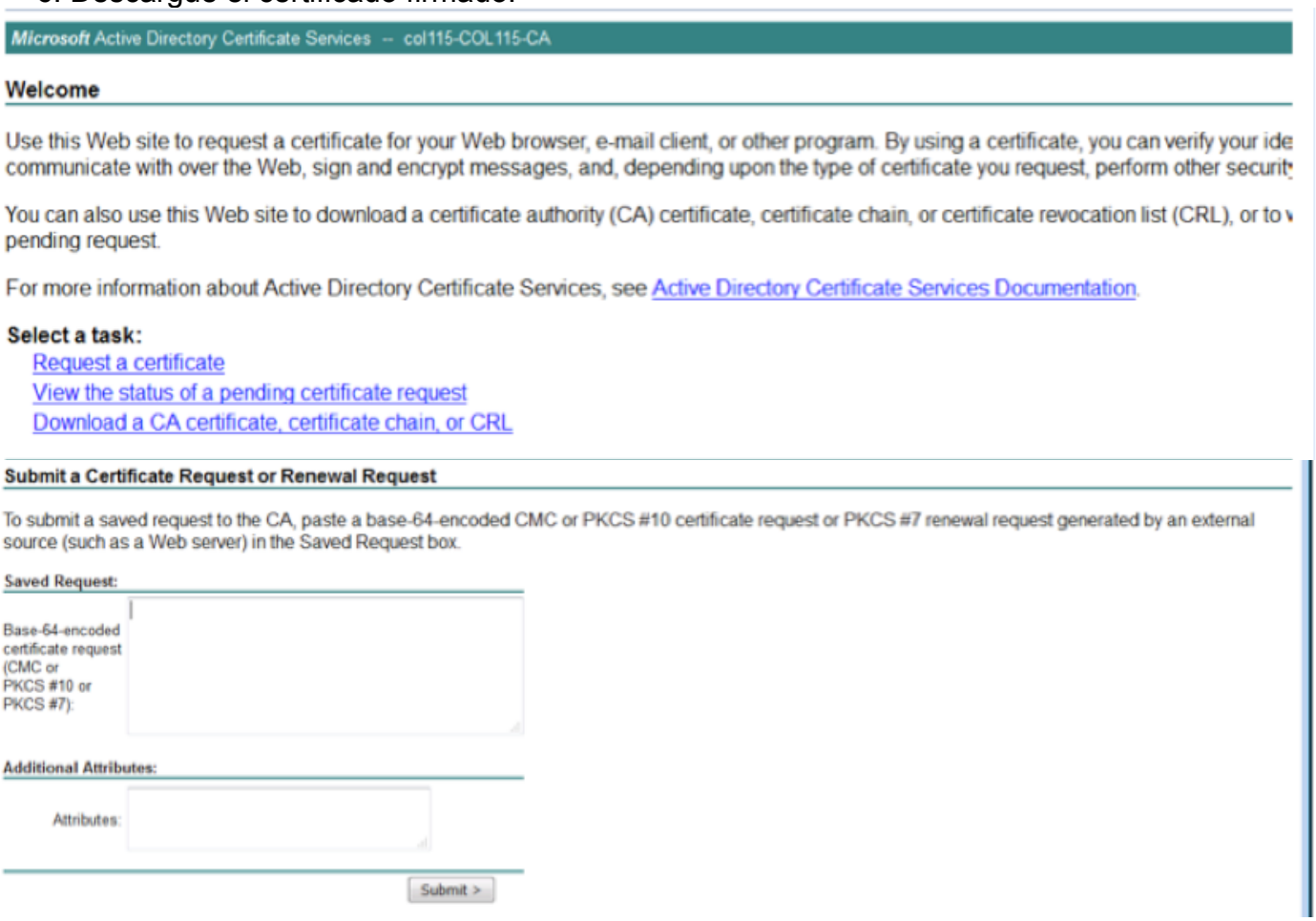
1. Abra al administrador de servidor.
2. Haga clic las herramientas.
3. Haga clic al administrador de los Servicios de Internet Information Server (IIS).
4. Seleccione al servidor local.
5. Seleccione los certificados de servidor.
6. Haga clic la característica abierta (el panel de la acción).
7. El tecleo **crea el** pedido de certificado.
8. Deje el proveedor de servicio criptográfico en el valor por defecto.
9. Cambie la **longitud de bit a 2048**.
10. Haga clic en Next (Siguiente).
11. Seleccione una ubicación para salvar el Archivo solicitado.
12. Haga clic en Finish (Finalizar).





Paso 2. CA firma el CSR que fue generado del paso 1.

1. **Abra el** servidor de CA para cantar este **HTTP** CSR**: Dirección IP del servidor >/certsrv/<CA**.
2. Petición del tecleo un certificado.
3. Pedido de certificado avanzado del tecleo.
4. **Copie el** CSR en el pedido de certificado codificado Based-64.
5. **Someta**.
6. Descargue el certificado firmado.



Paso 3. Instale el certificado firmado de nuevo al servidor ADFS y asígnelo a la característica ADFS.

1. Instale el certificado firmado de nuevo al servidor ADFS. Para hacer esto, **abra la información sobre Internet Services(IIS) Manager> del manager>Tools>Click del servidor**.

Característica local de Server>Server Certificate>Open (el panel de la acción).

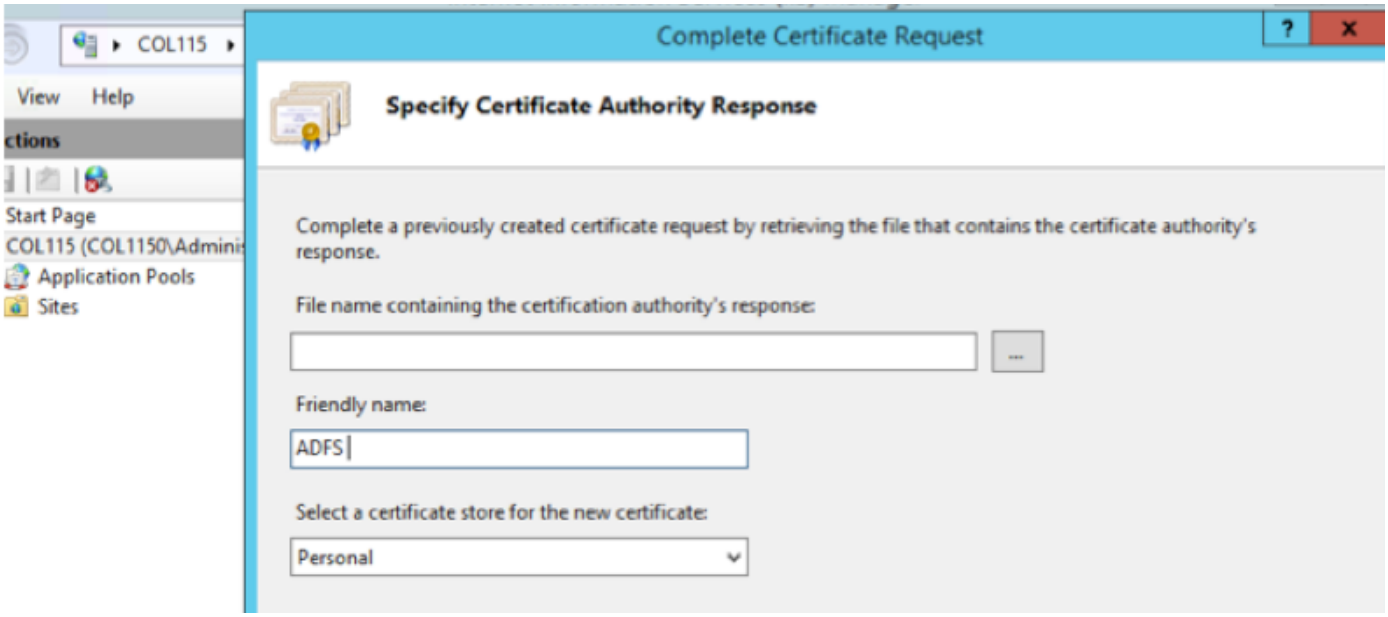
2. Pedido de certificado completo del tecleo.

3. Seleccione la trayectoria al archivo completo CSR que usted completó y descargó del proveedor del certificado del otro vendedor.

4. **Ingrese el** nombre cómodo para el certificado.

5. Seleccione personal como el almacén de certificados.

6. Click OK.



7. En esta etapa, todo el certificado fue agregado. Ahora, se requiere la asignación del certificado SSL.

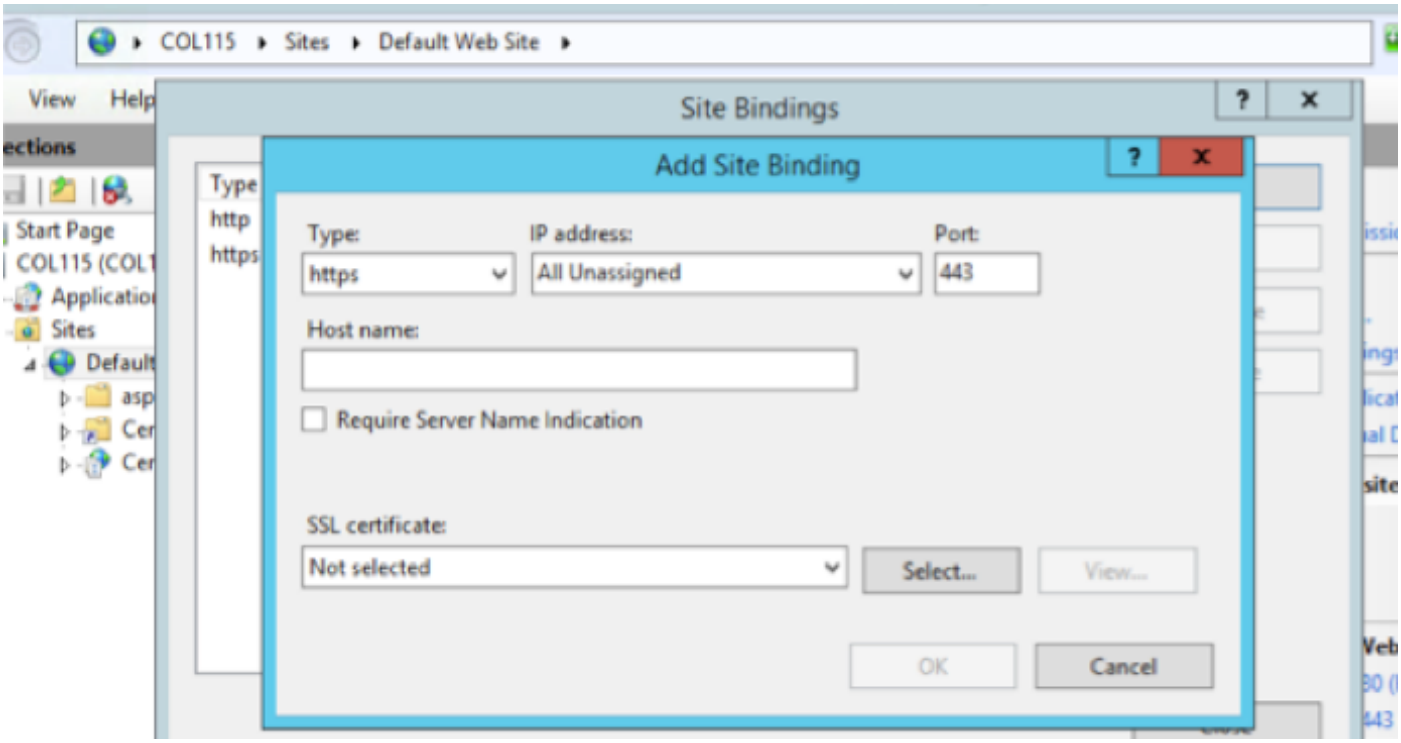
8. **Amplíe los atascamientos locales del >Click del Sitio Web predeterminado de Sites>Select del server>Expand** (panel de acciones).

9.Click **agregan**.

10. **Cambie el** tipo al HTTPS.

11. Seleccione su certificado del menú desplegable.

12. Click OK.



Ahora, el certificado SSL para el servidor ADFS fue asignado.

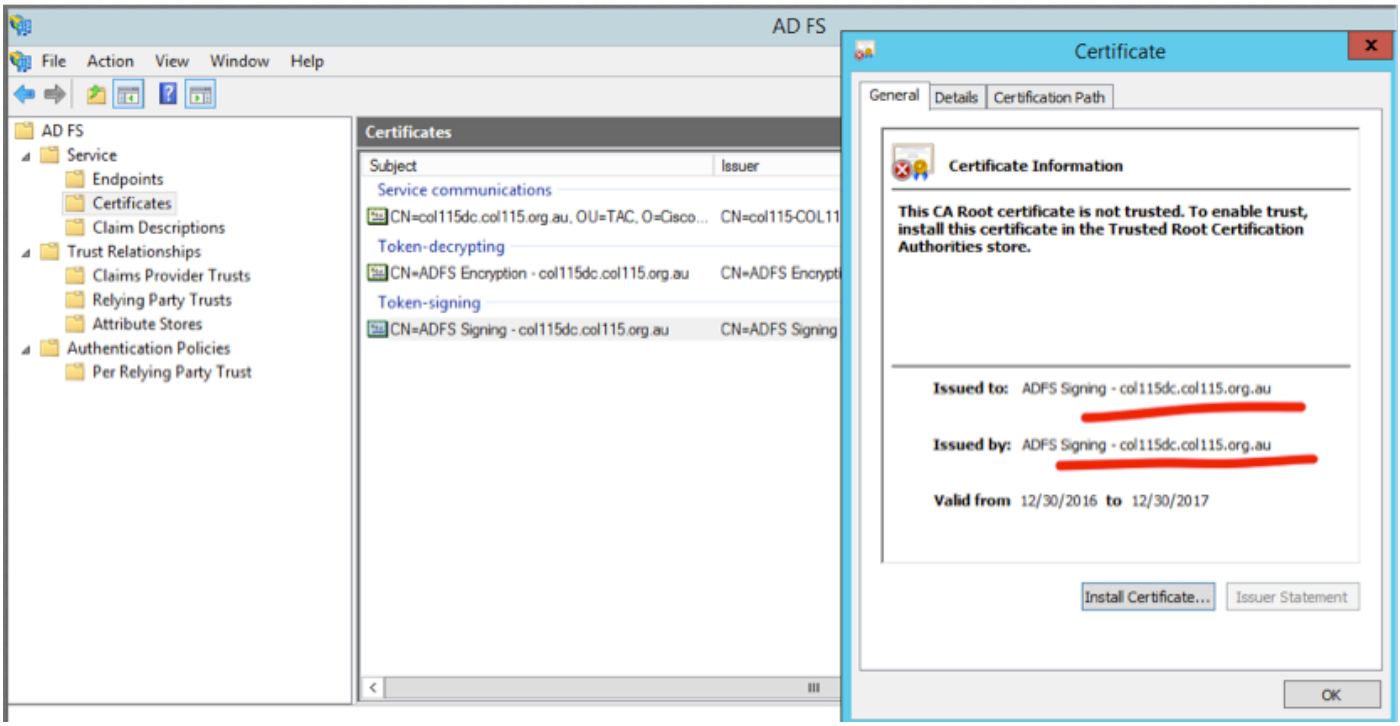
Note: Durante la instalación de la característica ADFS, el certificado anterior SSL debe ser utilizado.

Certificado de firma simbólico

ADFS genera el certificado autofirmado para el certificado de firma simbólico. Por abandono es válido por un año.

SAML el token generado por IDP es chamuscado por la clave privada ADFS (parte privada de firma simbólica del certificado). Entonces, el IDS utiliza la clave pública ADFS para verificar. Esto garantiza que el token firmado no es conseguir modificado.

El certificado de firma simbólico se utiliza cada vez que un usuario necesita para acceder a una aplicación de confianza del partido (Cisco IDS).

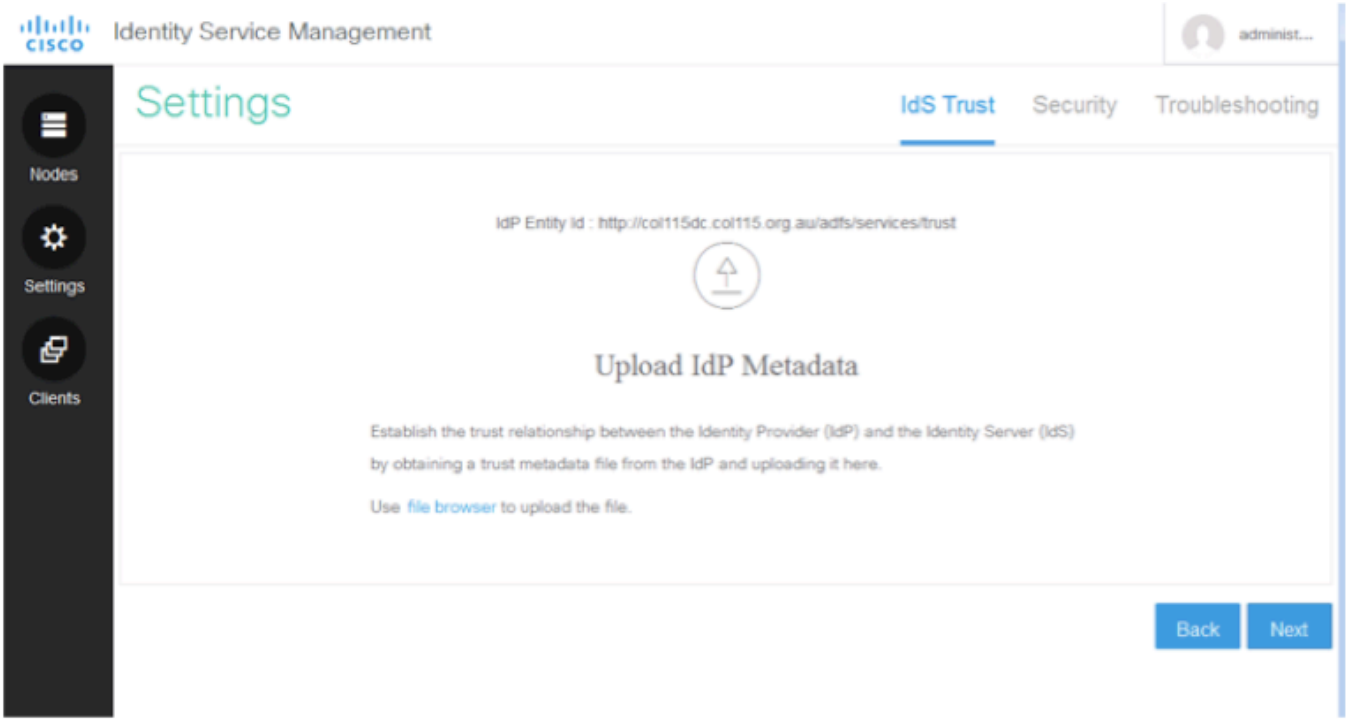


¿Cómo el servidor del Cisco IDS consigue la clave pública del certificado simbólico del canto?

Esto es hecha cargando los meta datos ADFS al Servidor IDS, y después pasando la clave pública ADFS al Servidor IDS. De esta manera, el IDS gana la clave pública del servidor ADFS.

Usted necesita **descargar los** meta datos IDP de ADFS. Para descargar los meta datos IDP, refiera al link **https:// <FQDN de ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

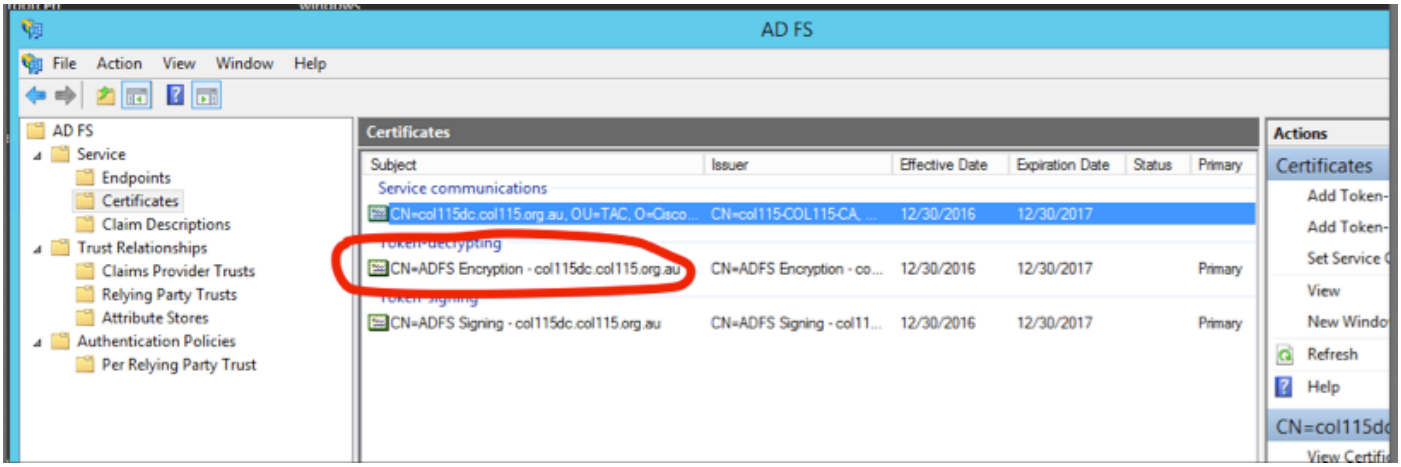
De ADFS los meta datos



cargan los meta datos ADFS al IDS

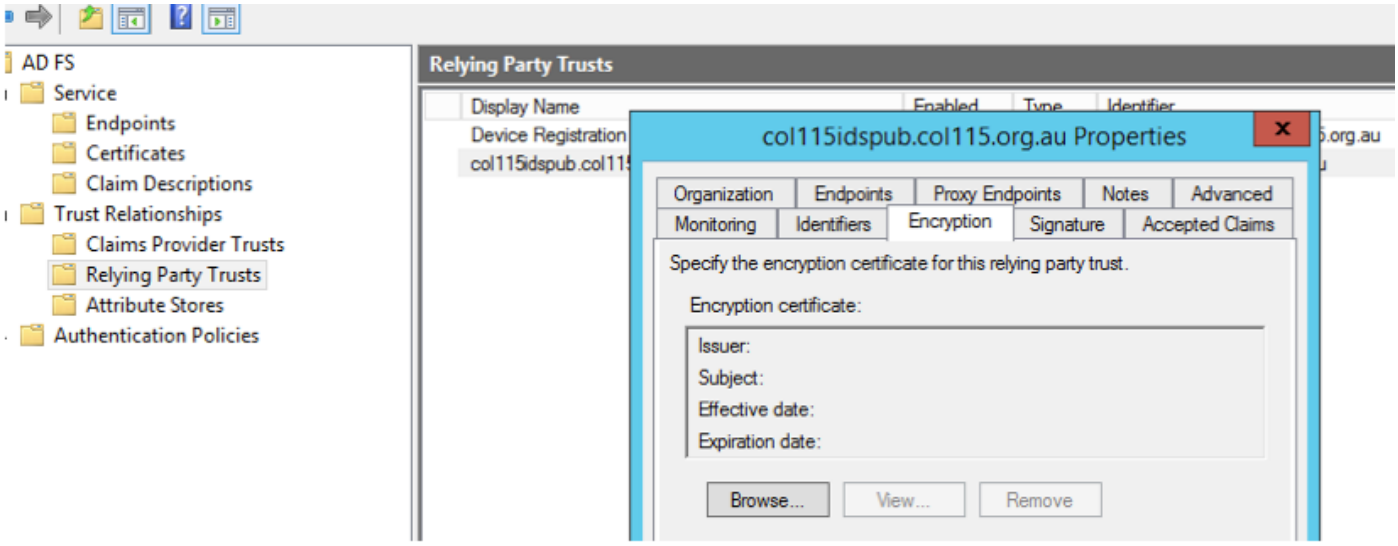
Desciframiento simbólico

Este certificado genera automáticamente por el servidor ADFS (uno mismo-firmado). Si el token necesita el cifrado, ADFS utiliza la clave pública IDS para desencriptarla. Pero, cuando usted ve el token-dcrypting ADFS, no significa que el token está cifrado.



Si usted quiere ver si el cifrado simbólico fue habilitado para una aplicación de confianza específica del partido, usted necesita marcar la lengueta del cifrado en una aplicación de confianza específica del partido.

Esta imagen muestra, el cifrado simbólico no fue habilitada.



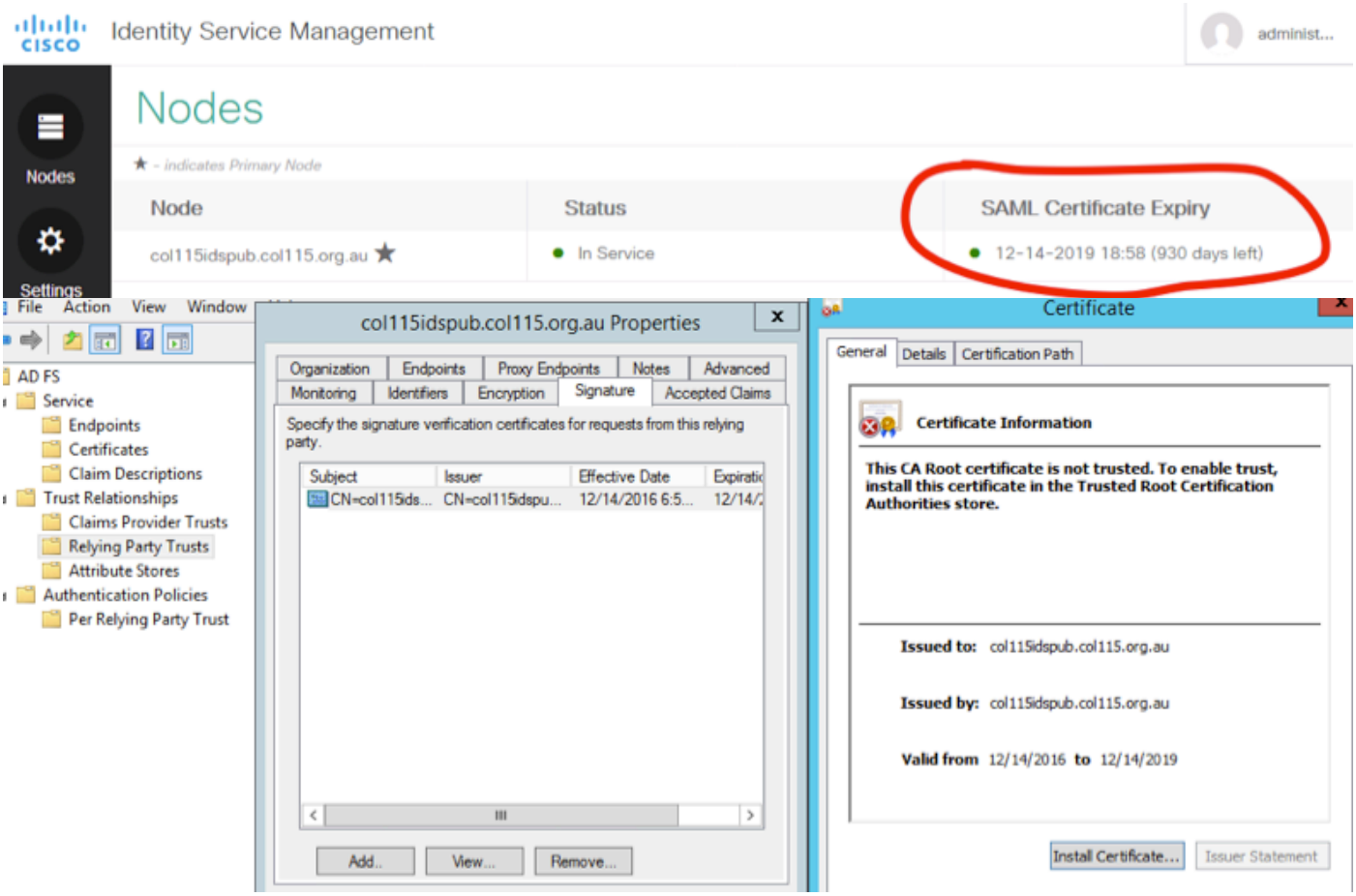
El cifrado no se habilita

Certificado del lado del Cisco IDS de la parte D.

- SAML certificado
- Clave de encripción
- Clave de la firma

SAML certificado

Este certificado es generado por el Servidor IDS (uno mismo-firmado). Por abandono es válido por 3 años.

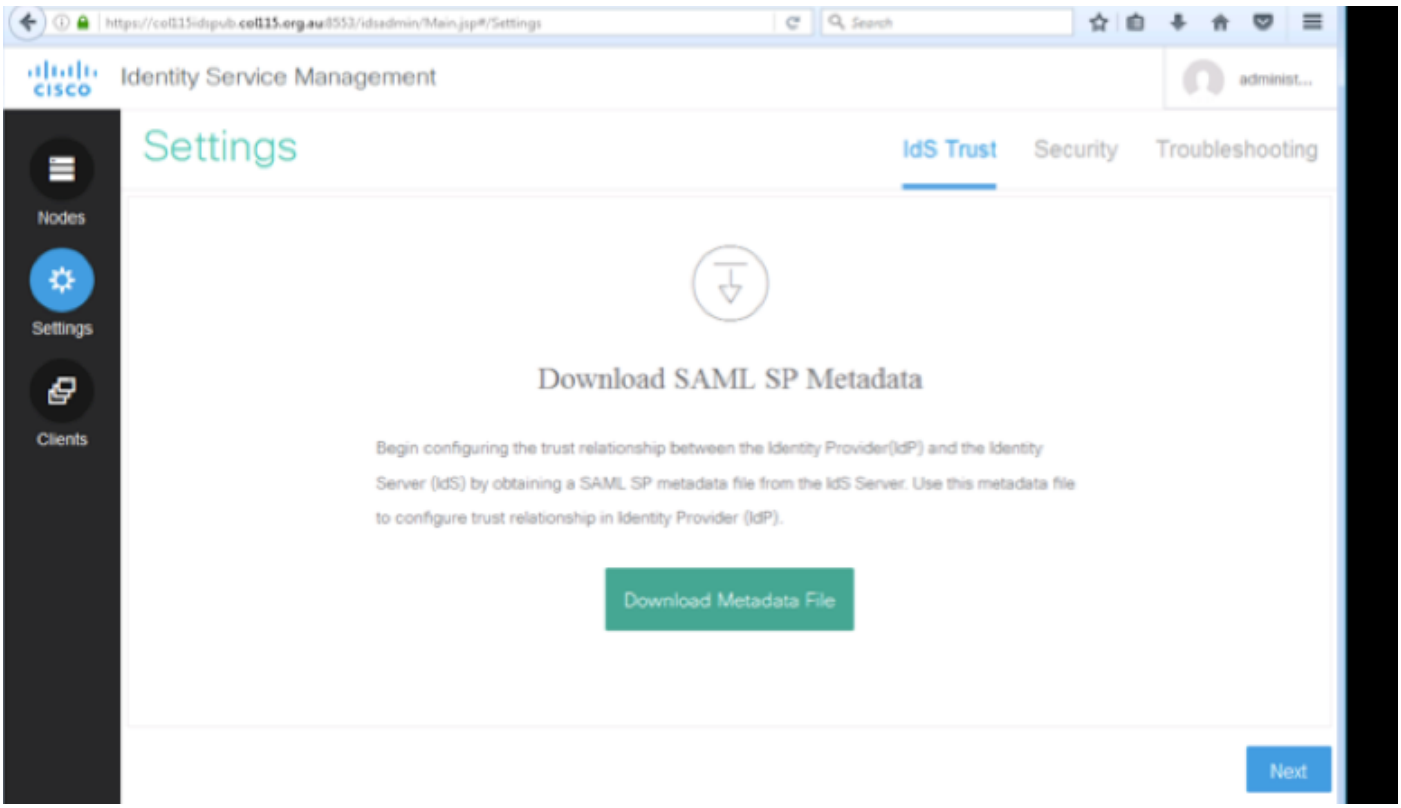


Este certificado se utiliza para firmar SAML la petición, y envía a IDP (ADFS). Esta clave pública está en los meta datos IDS, y se debe importar al servidor ADFS.

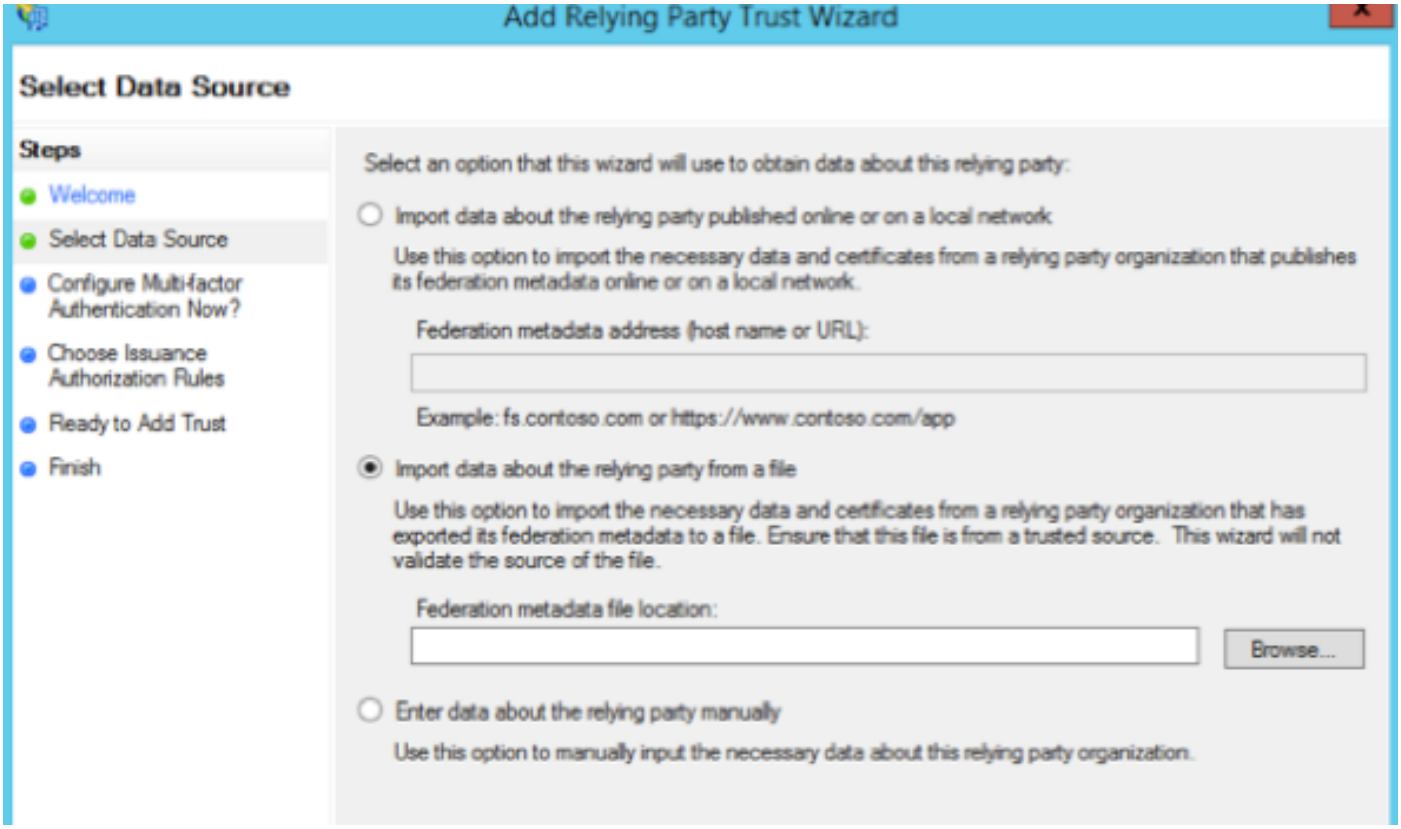
1.Download meta datos SAML SP del Servidor IDS.

2. Broswer al **servidor FQDN>:8553/idsadmin/ de los <ids de https://**.

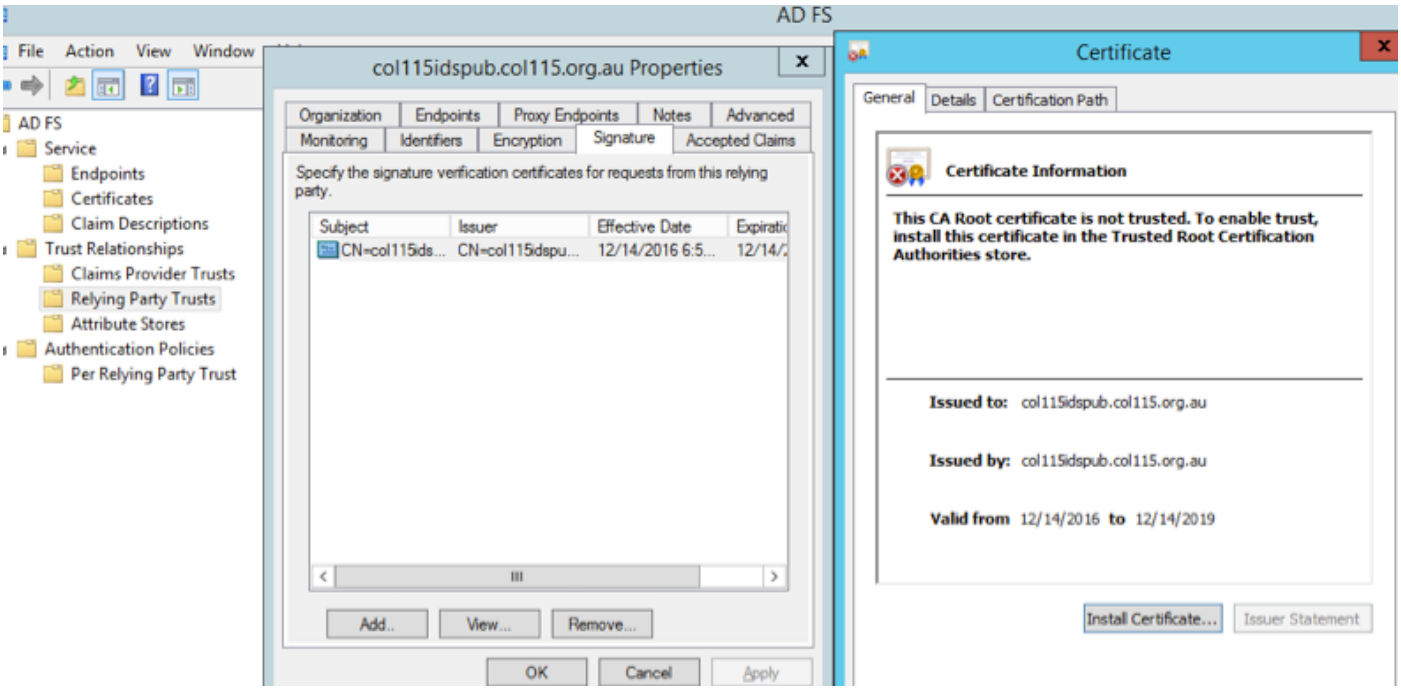
3. Seleccione las configuraciones y los meta datos de la descarga SAML SP y **sálvelos**.



Los meta datos de la importación



del Servidor IDS al servidor ADFS

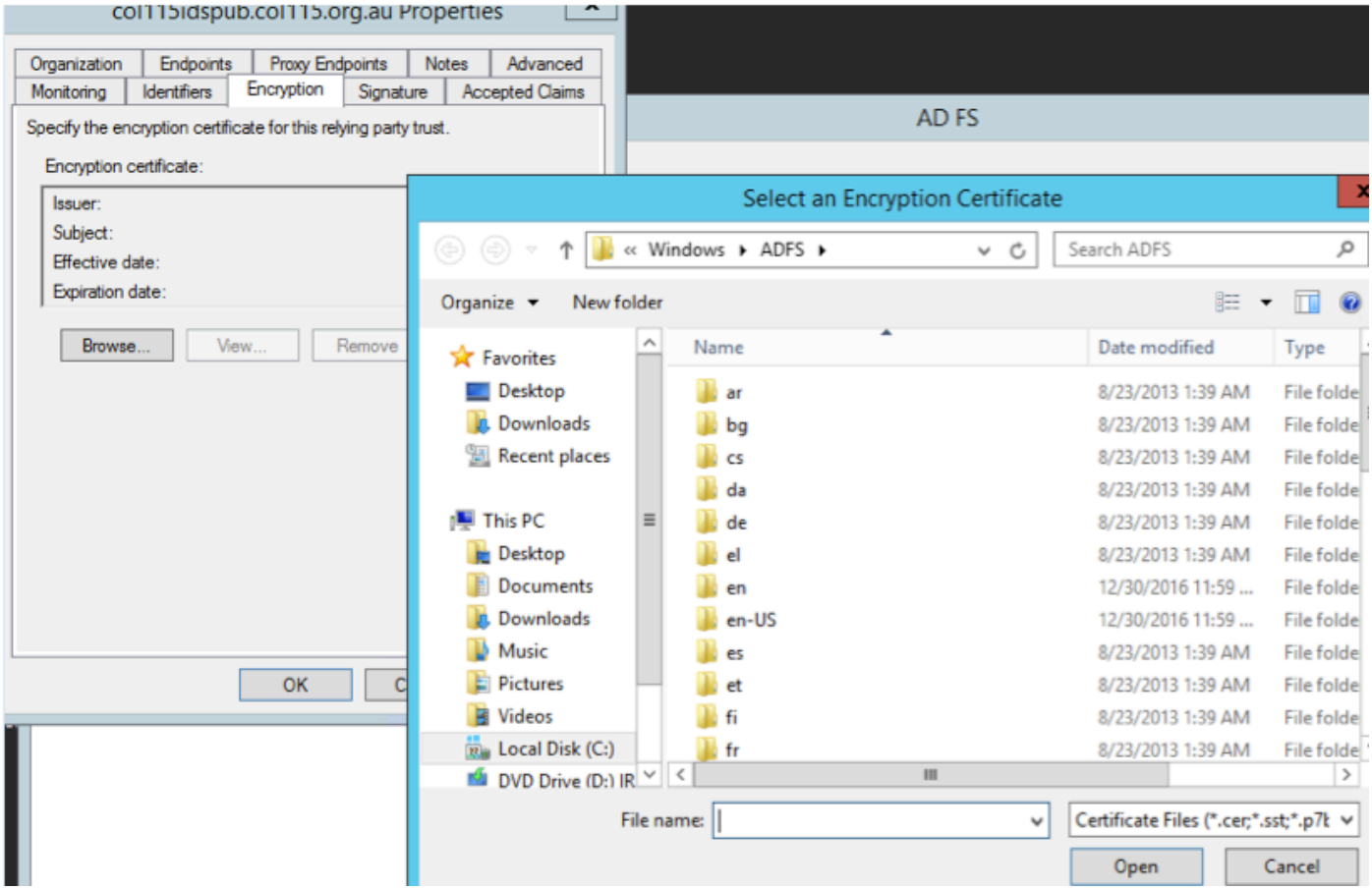


verifican del lado ADFS

Cuando el IDS regenera el certificado- uno de SAML se utiliza para firmar la petición de SAML que realiza el intercambio de los meta datos.

Cifrado/clave de la firma

El cifrado no se habilita por abandono. Si se habilita el cifrado, necesita ser cargado a 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