# Certificati e configurazione Single Sign-On (SSO) UCCE (Unified Contact Center Enterprise)

## Sommario



## Introduzione

In questo documento vengono descritte le configurazioni dei certificati necessarie per UCCE SSO. La configurazione di questa funzionalità richiede diversi certificati per HTTPS, firma digitale e crittografia.

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE release 11.5
- Microsoft Active Directory (AD) - AD installato in Windows Server
- Active Directory Federation Service (ADFS) versione 2.0/3.0

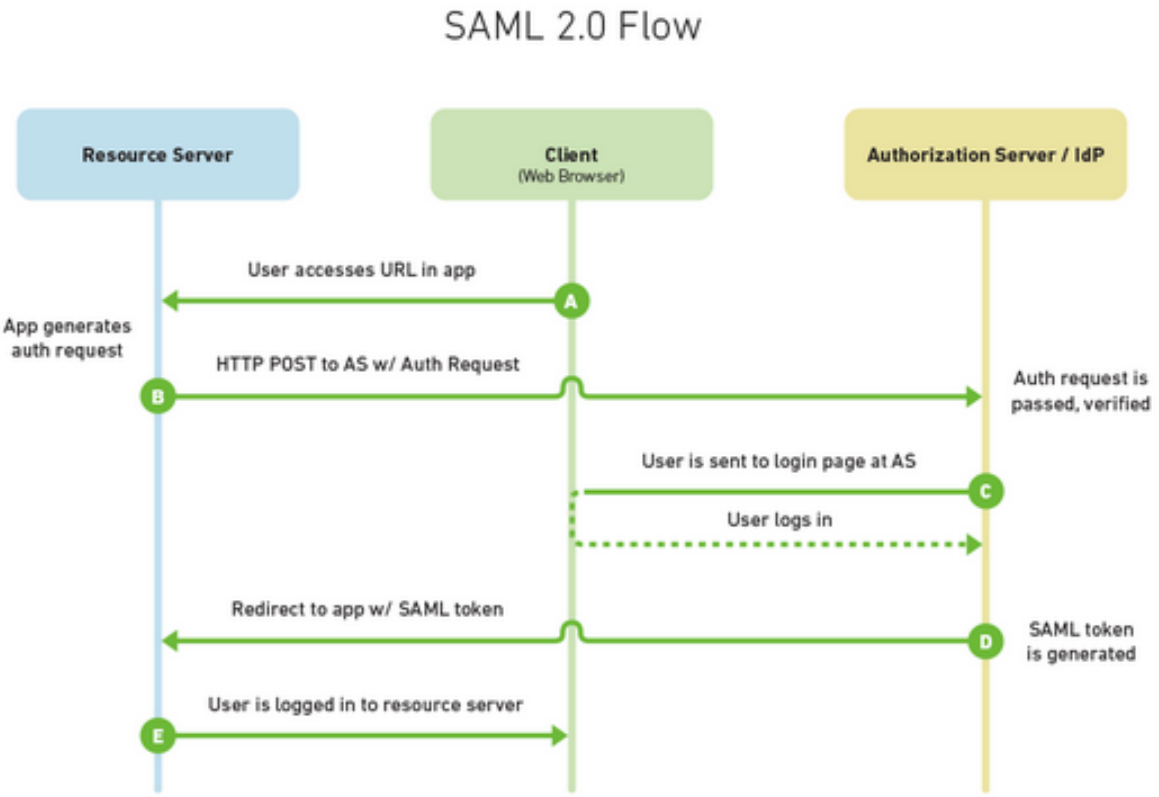
### Componenti usati

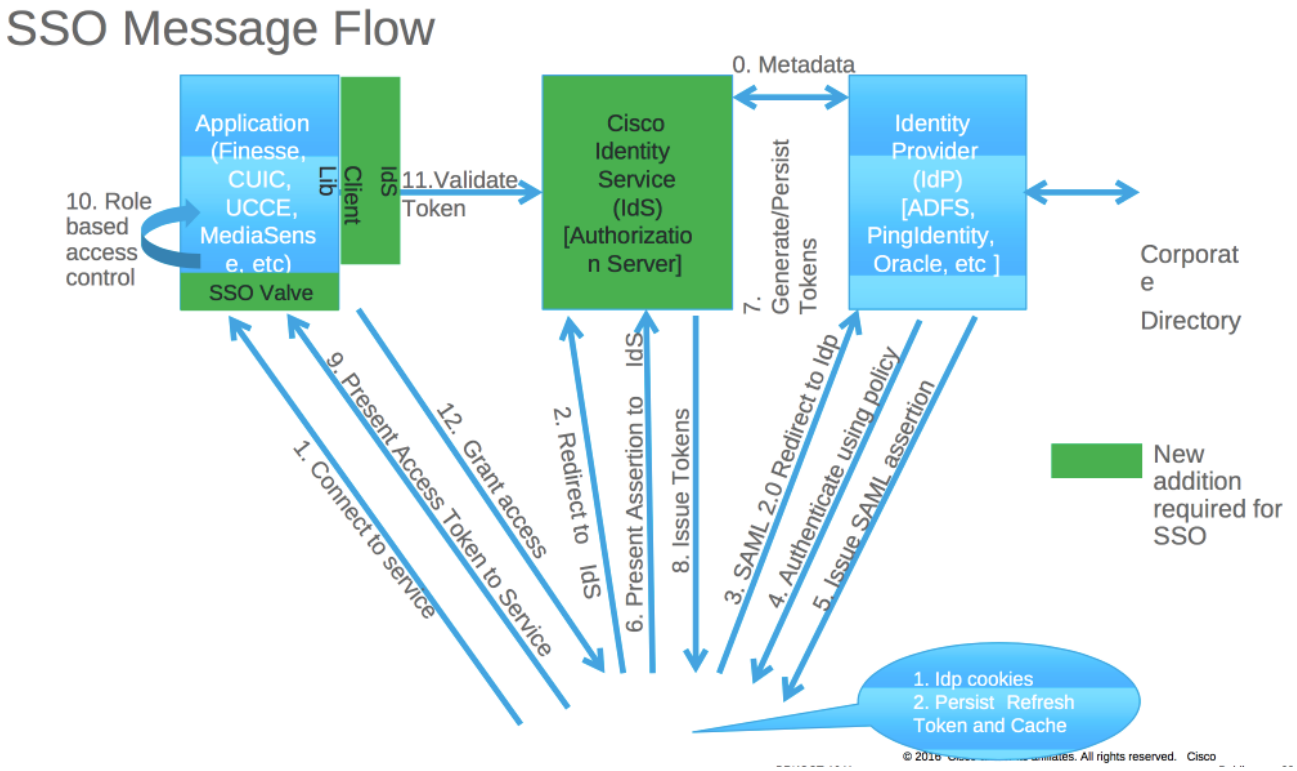
UCCE 11.5

Windows 2012 R2

### Parte A. Flusso messaggi SSO

The most common SAML flow is shown below:

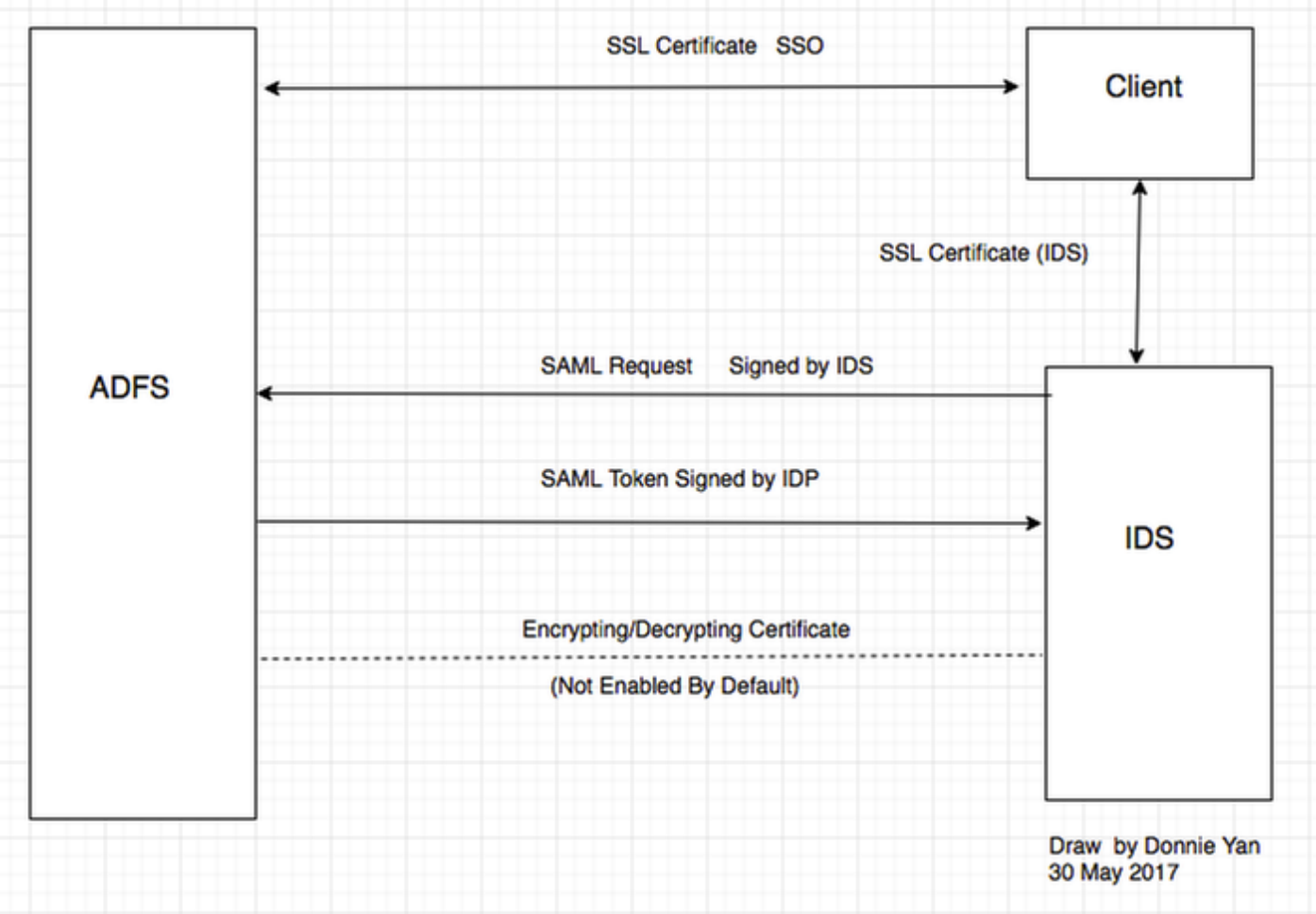



Quando SSO è abilitato, quando l'agente accede al desktop Finesse:

- Il server Finesse reindirizza il browser dell'agente per comunicare con Identity Service (IDS)
- IDS reindirizza il browser dell'agente al provider di identità (IDP) con richiesta SAML
- IDP genera il token SAML e lo passa al server IDS
- Al momento della generazione del token, ogni volta che l'agente passa all'applicazione, utilizza questo token valido per l'accesso

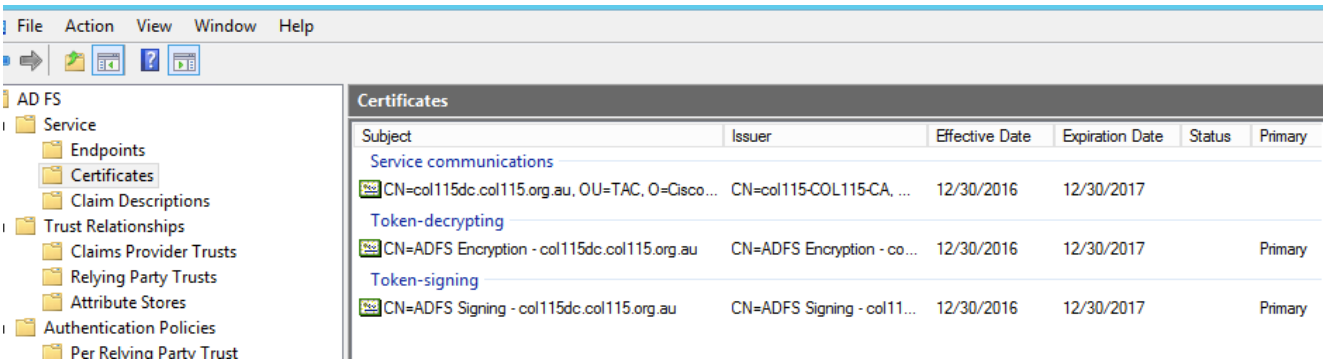
## Parte B. Certificati utilizzati in IDP e IDS




### Certificati IDP

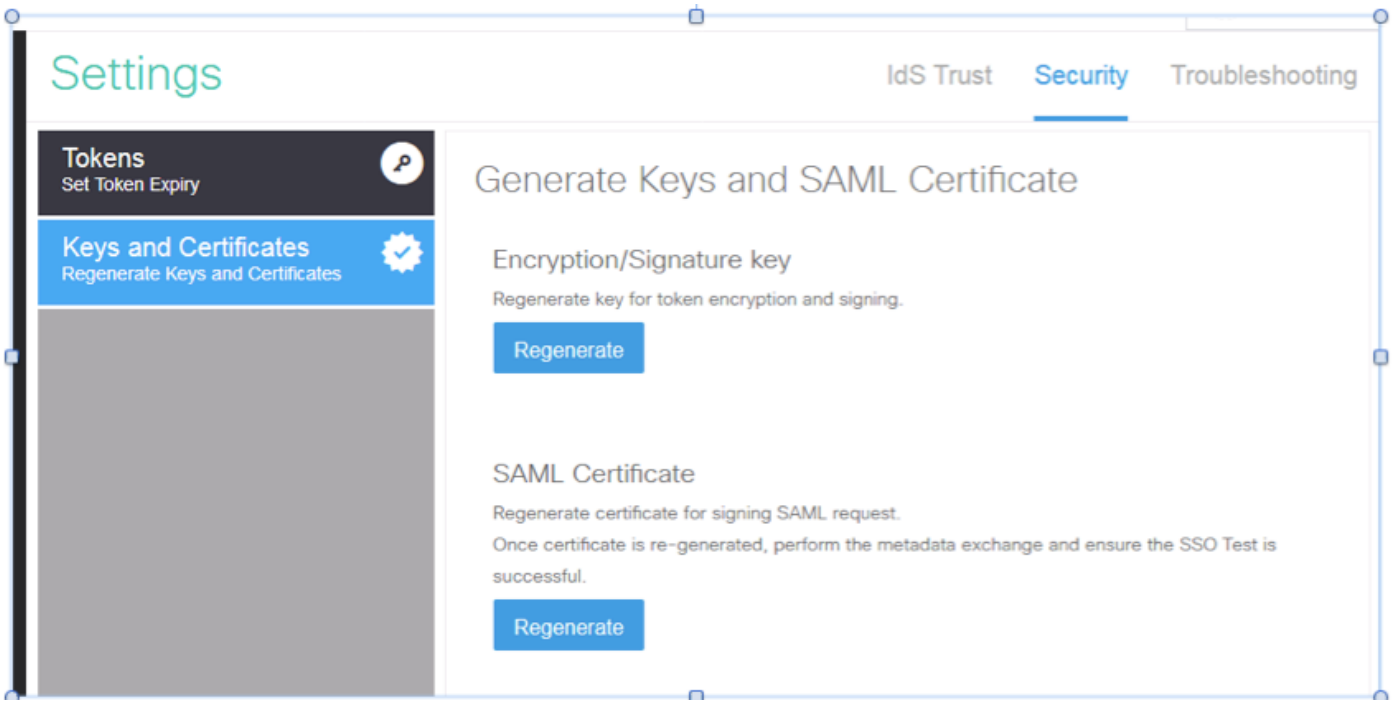
- Certificato SSL (SSO)
- Certificato per la firma di token
- Token - decrittografia

1.




### Certificati IDS

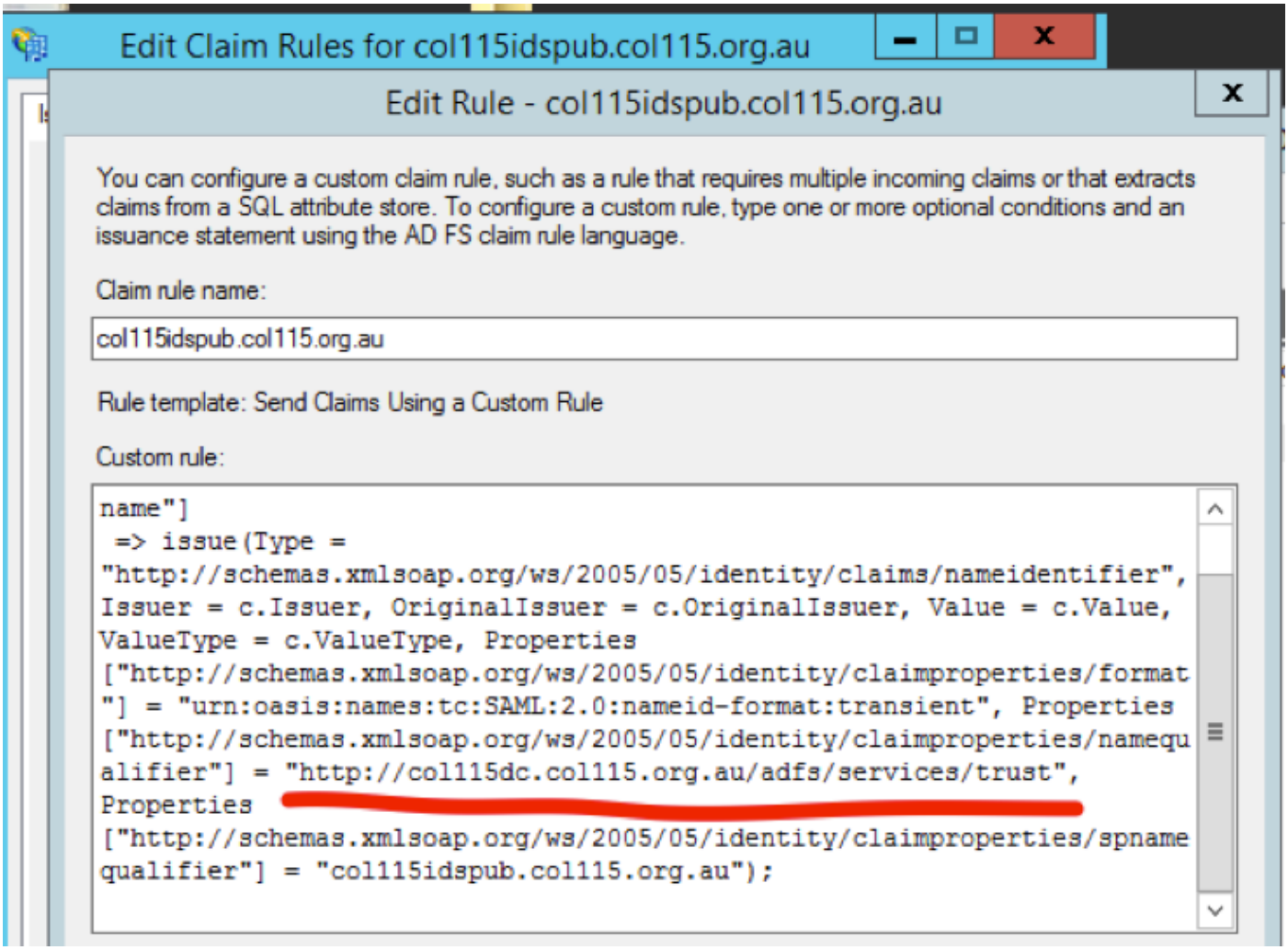
- Certificato SAML
- Chiave firma
- Chiave di crittografia




## Parte C. Certificazione IDP in dettaglio e configurazione

### Certificato SSL (SSO)

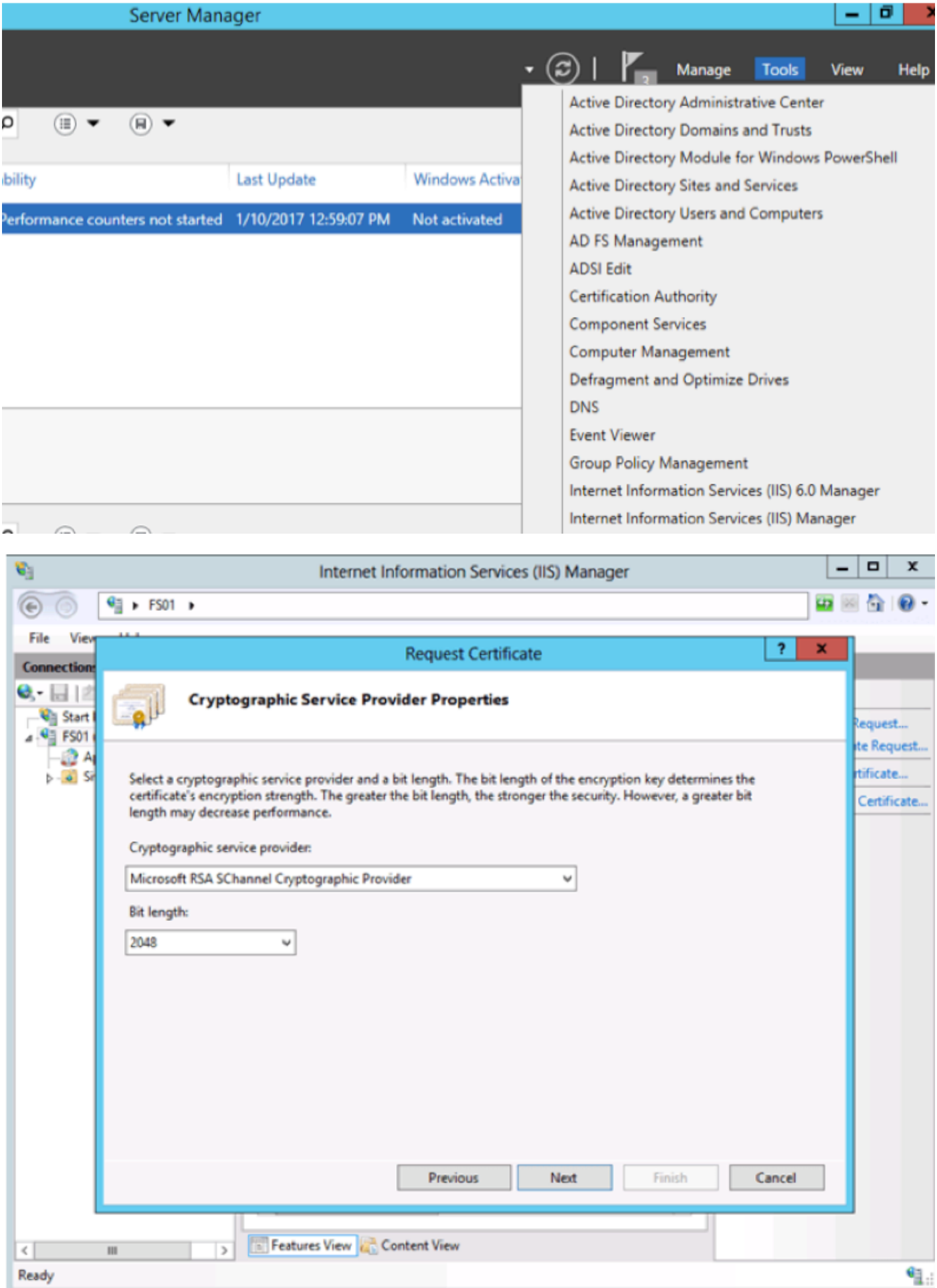
- Questo certificato viene utilizzato tra IDP e il client. Il client deve considerare attendibile il certificato SSO
- Il certificato SSL viene posizionato per crittografare la sessione tra il client e il server IDP. Questo certificato non è specifico di ADFS, ma specifico di IIS
- Il soggetto del certificato SSL deve corrispondere al nome utilizzato nella configurazione ADFS




**Passaggi per la configurazione del certificato SSL per SSO (laboratorio locale con CA interna firmata)**

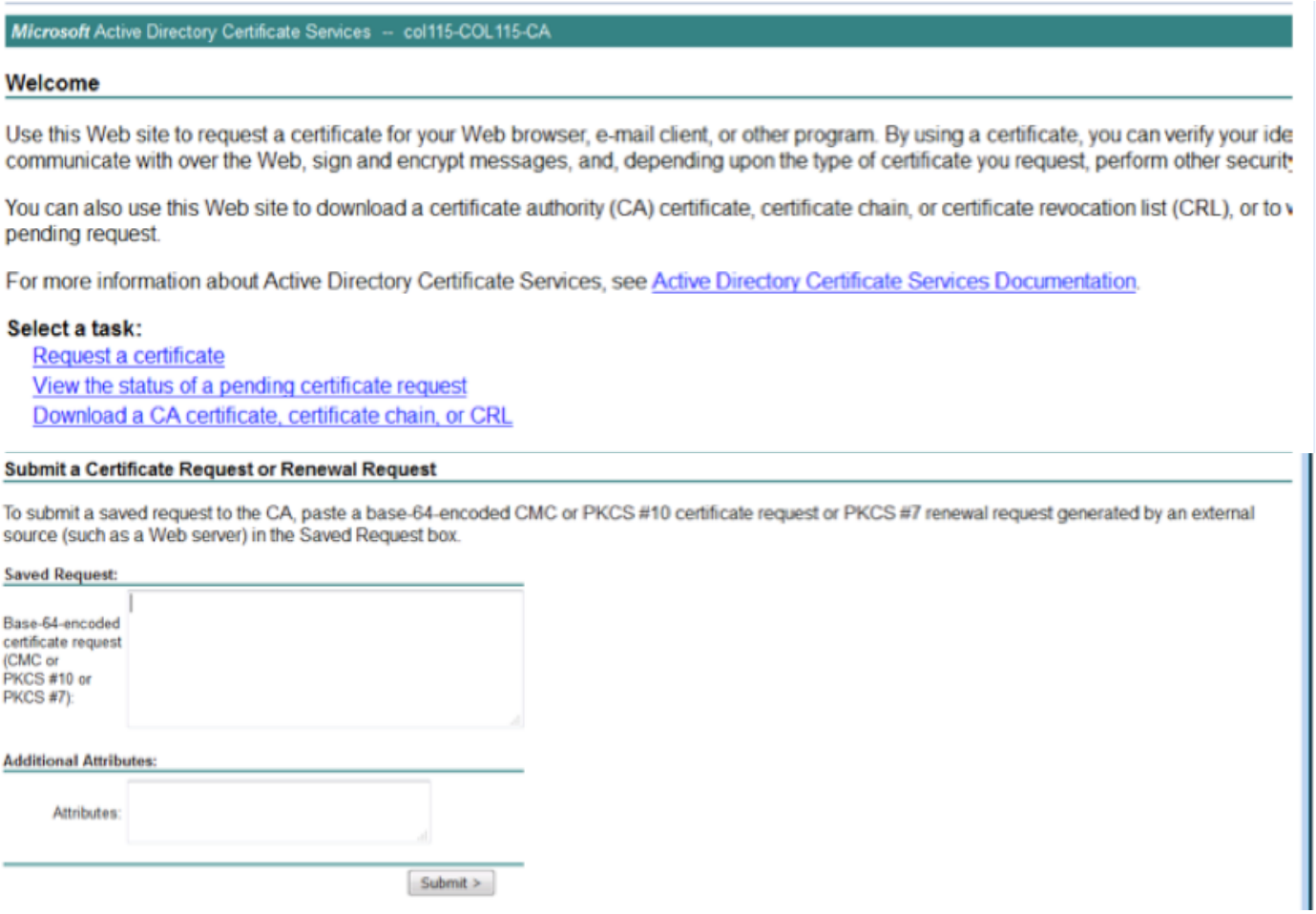
**Passaggio 1**. **Creare un** certificato SSL con CSR (Certificate Signing Request) e firmarlo con la CA interna per ADFS.

1. Aprire Server Manager.
2. Fare clic su Strumenti.
3. Fare clic su Gestione Internet Information Services (IIS).
4. Selezionare il server locale.
5. Selezionare Certificati server.
6. Fate clic su Apri feature (Open Feature) nel pannello azioni.
7. Fare clic su **crea** richiesta certificato.
8. Non modificare il provider del servizio di crittografia come predefinito.
9. Impostate **Lunghezza bit (Bit Length) a 2048**.
10. Fare clic su Next (Avanti).
11. Selezionare un percorso in cui salvare il file richiesto.
12. Fare clic su **Finish** (Fine).




**Passaggio 2.** CA firma il CSR generato dal passaggio 1.

1. **Aprire** il server CA per utilizzare questo CSR **http:<indirizzo IP server CA>/certsrv/**.
2. Fare clic su Richiedi certificato.
3. Fare clic su Richiesta avanzata certificati.
4. **Copiare** il CSR nella richiesta di certificato con codifica Based-64.
5. **Invia**.
6. Scaricare il certificato firmato.




**Passaggio 3.** Reinstallare il certificato firmato nel server ADFS e assegnarlo alla funzionalità ADFS.

1. Reinstallare il certificato firmato nel server ADFS. A tale scopo, **aprire Server manager>Strumenti>Fare clic su Gestione Internet Information Services (IIS)>**.

**Server locale>Certificato server>Apri funzionalità (pannello azioni)**.

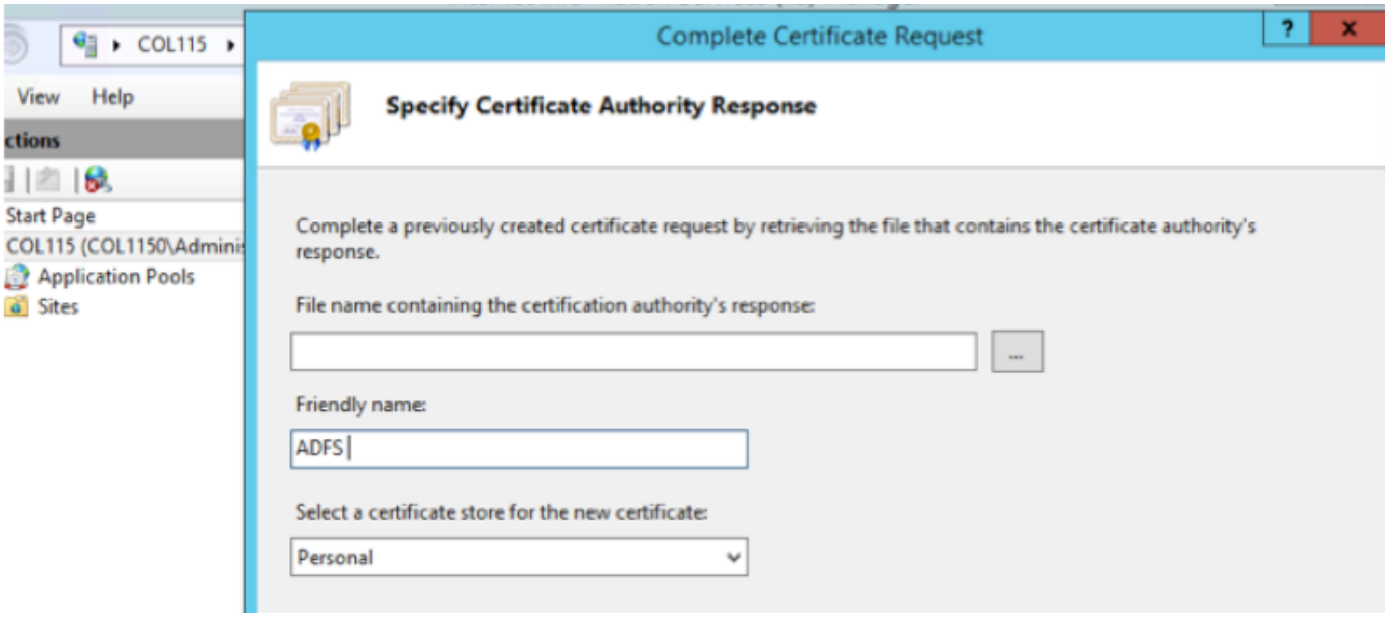
2. Fare clic su Completa richiesta certificato.

3. Selezionare il percorso del file CSR completo completato e scaricato dal provider di certificati di terze parti.

4. **Inserire** il nome descrittivo del certificato.

5. Selezionare Personale come archivio certificati.

6. Fare clic su **OK**.




7. In questa fase sono stati aggiunti tutti i certificati. A questo punto è necessario assegnare il certificato SSL.

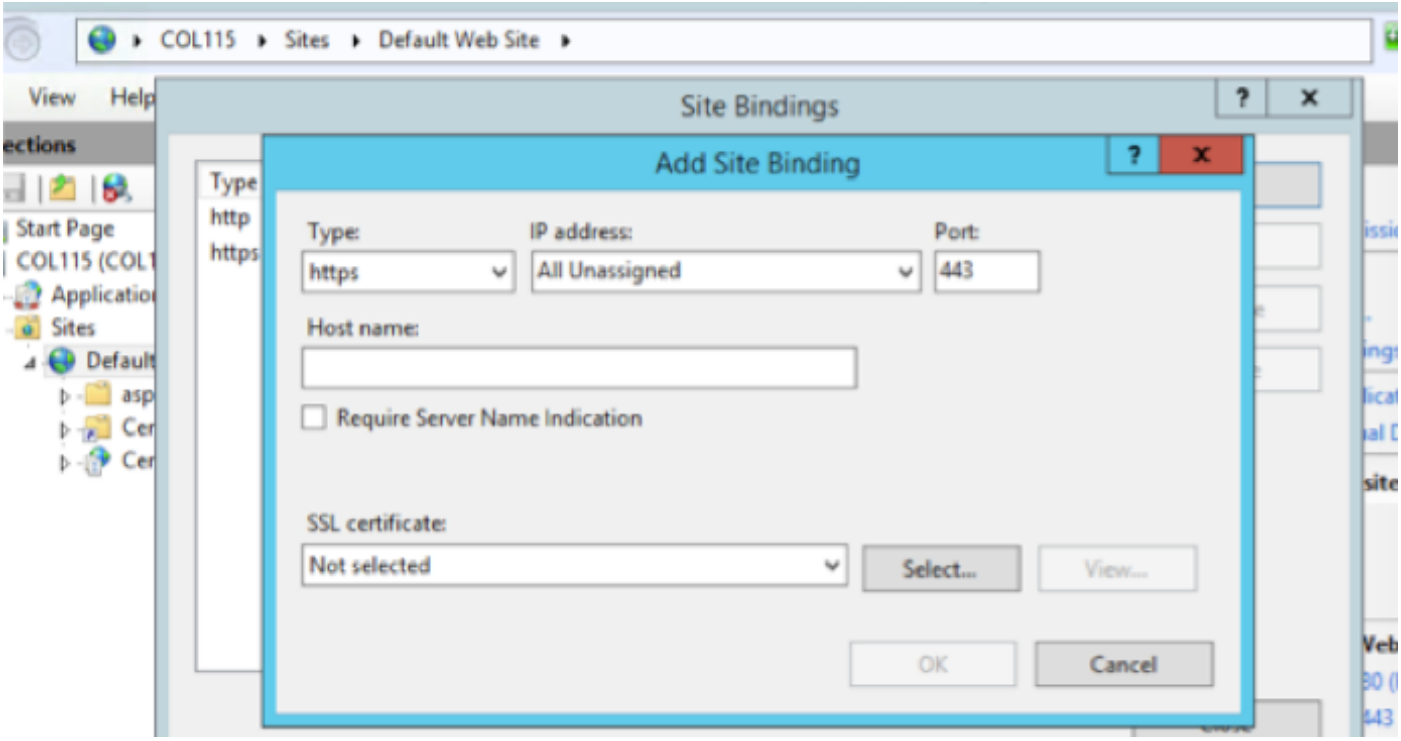
8. **Espandere** il **server locale>Espandi siti>Seleziona sito Web predefinito >Associazioni clic** (riquadro delle azioni).

9.Fare clic su **Add** (Aggiungi).

10. **Modificare** il tipo in HTTPS.

11. Selezionare il certificato dal menu a discesa.

12. Fare clic su **OK**.




A questo punto è stato assegnato il certificato SSL per il server ADFS.

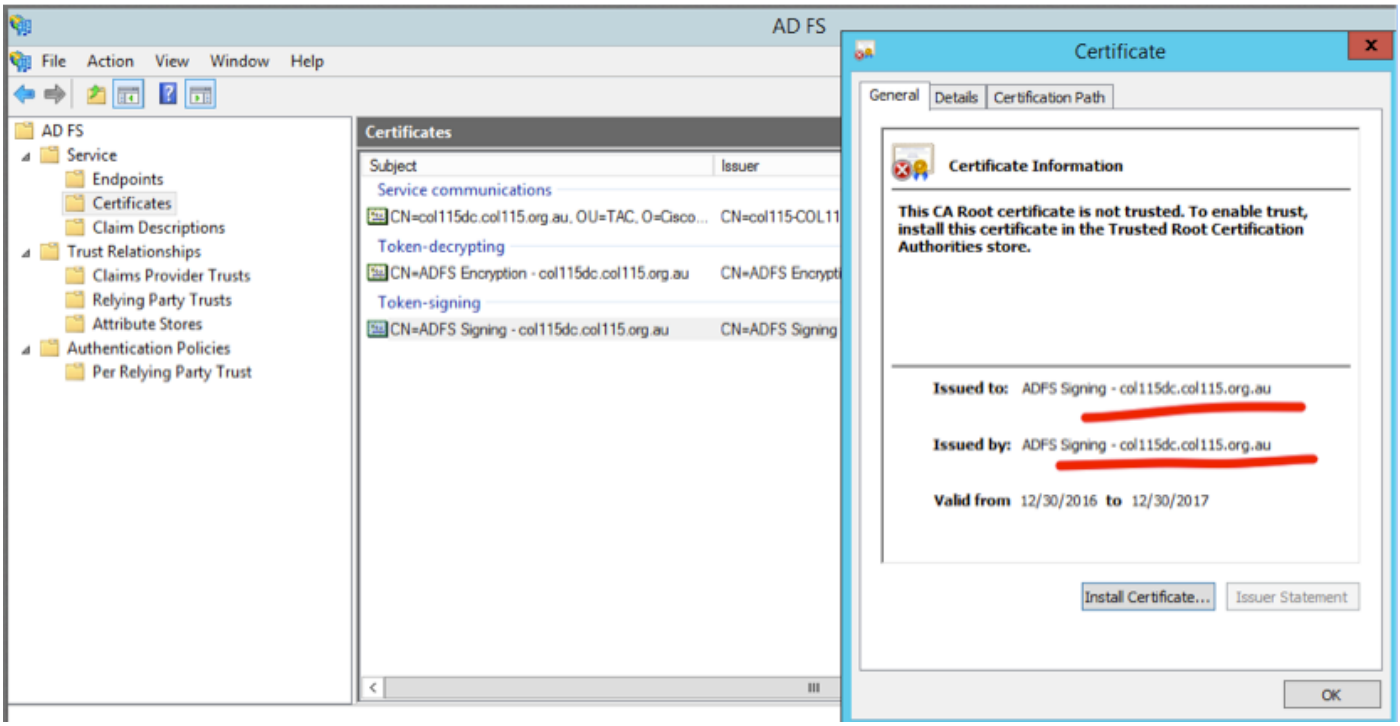
**Nota:** Durante l'installazione della funzionalità ADFS, è necessario utilizzare un certificato SSL precedente.

### Certificato per la firma di token

ADFS genera un certificato autofirmato per il certificato per la firma di token. Per impostazione predefinita è valido per un anno.

Il token SAML generato da IDP è firmato dalla chiave privata ADFS (parte privata del certificato per la firma di token). IDS quindi utilizza la chiave pubblica ADFS per la verifica. Il token firmato con garanzia non viene modificato.

Il certificato per la firma di token viene utilizzato ogni volta che un utente deve accedere a un'applicazione relying party (Cisco IDS).

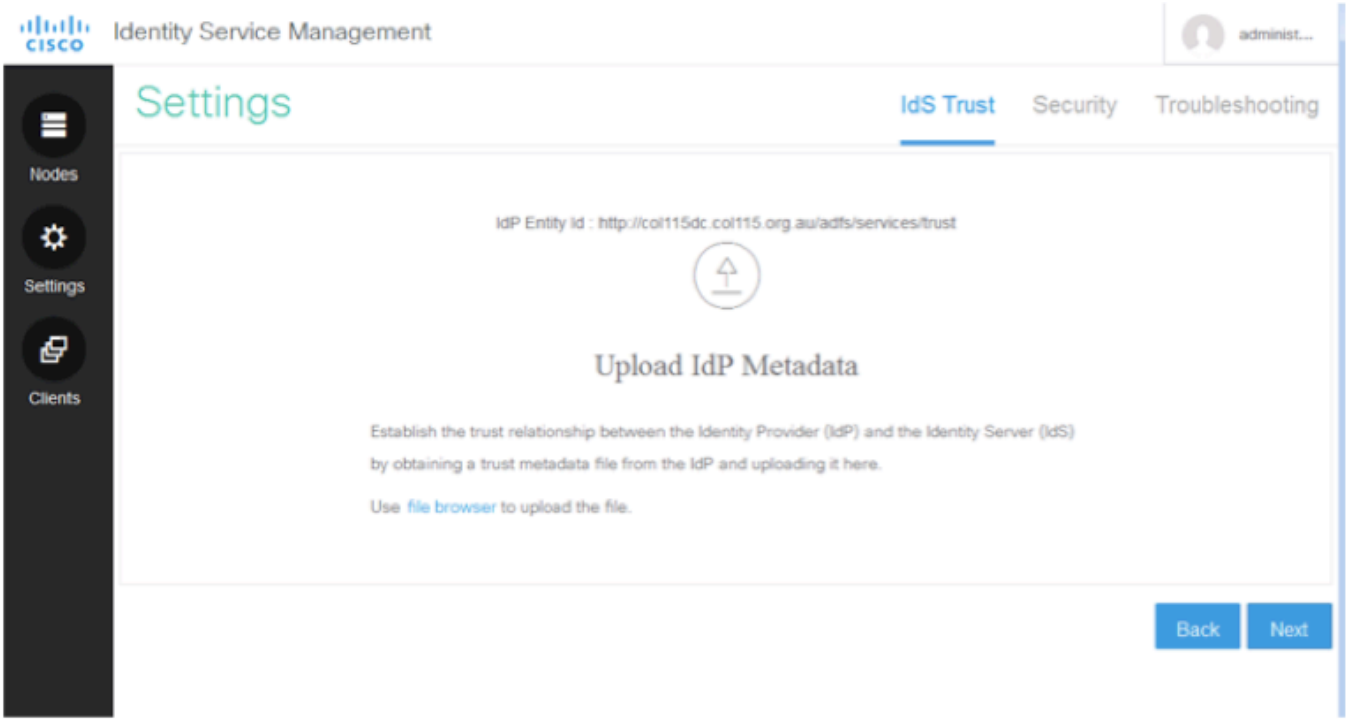



### In che modo il server Cisco IDS ottiene la chiave pubblica del certificato Token Singing?

A tale scopo, caricare i metadati ADFS nel server IDS e quindi passare la chiave pubblica di ADFS al server IDS. In questo modo IDS ottiene la chiave pubblica del server ADFS.

Ènecessario **scaricare** i metadati IDP da ADFS. Per scaricare i metadati IDP, fare riferimento al collegamento **https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

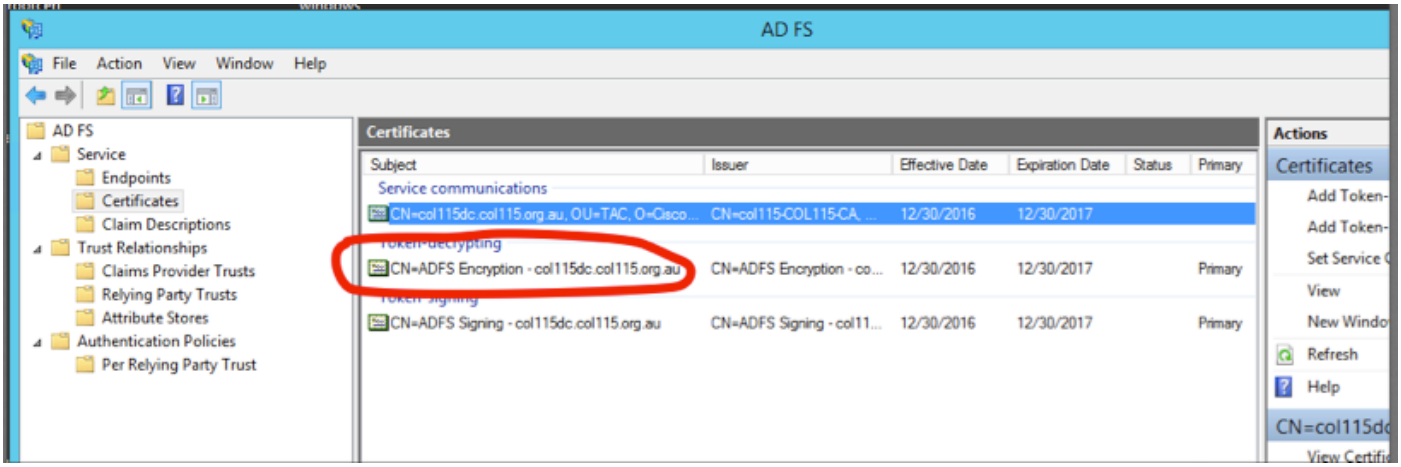

Da metadati
ADFS




carica metadati ADFS in IDS

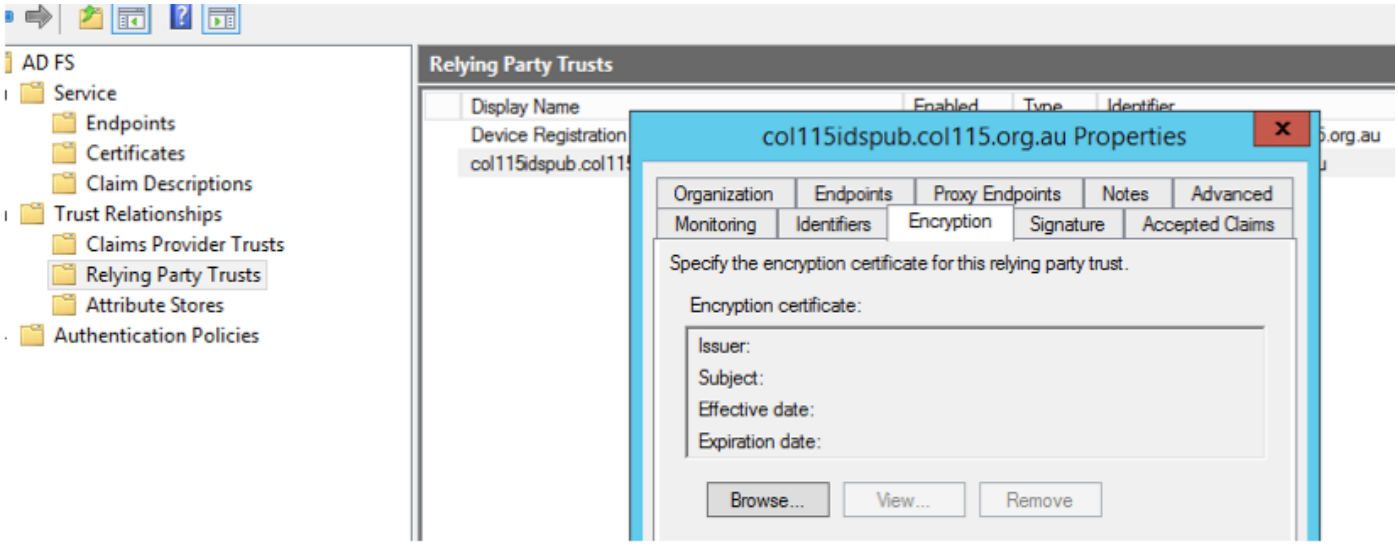
**Decrittografia token**

Questo certificato viene generato automaticamente dal server ADFS (autofirmato). Se il token richiede la crittografia, ADFS utilizza la chiave pubblica IDS per decrittografarlo. Tuttavia, quando viene visualizzata la crittografia token ADFS, NON significa che il token sia crittografato.




Se si desidera verificare se la crittografia del token è stata abilitata per un'applicazione relying party specifica, è necessario selezionare la scheda crittografia in un'applicazione relying party specifica.

Nell'immagine viene mostrato come la crittografia del token NON sia stata abilitata.



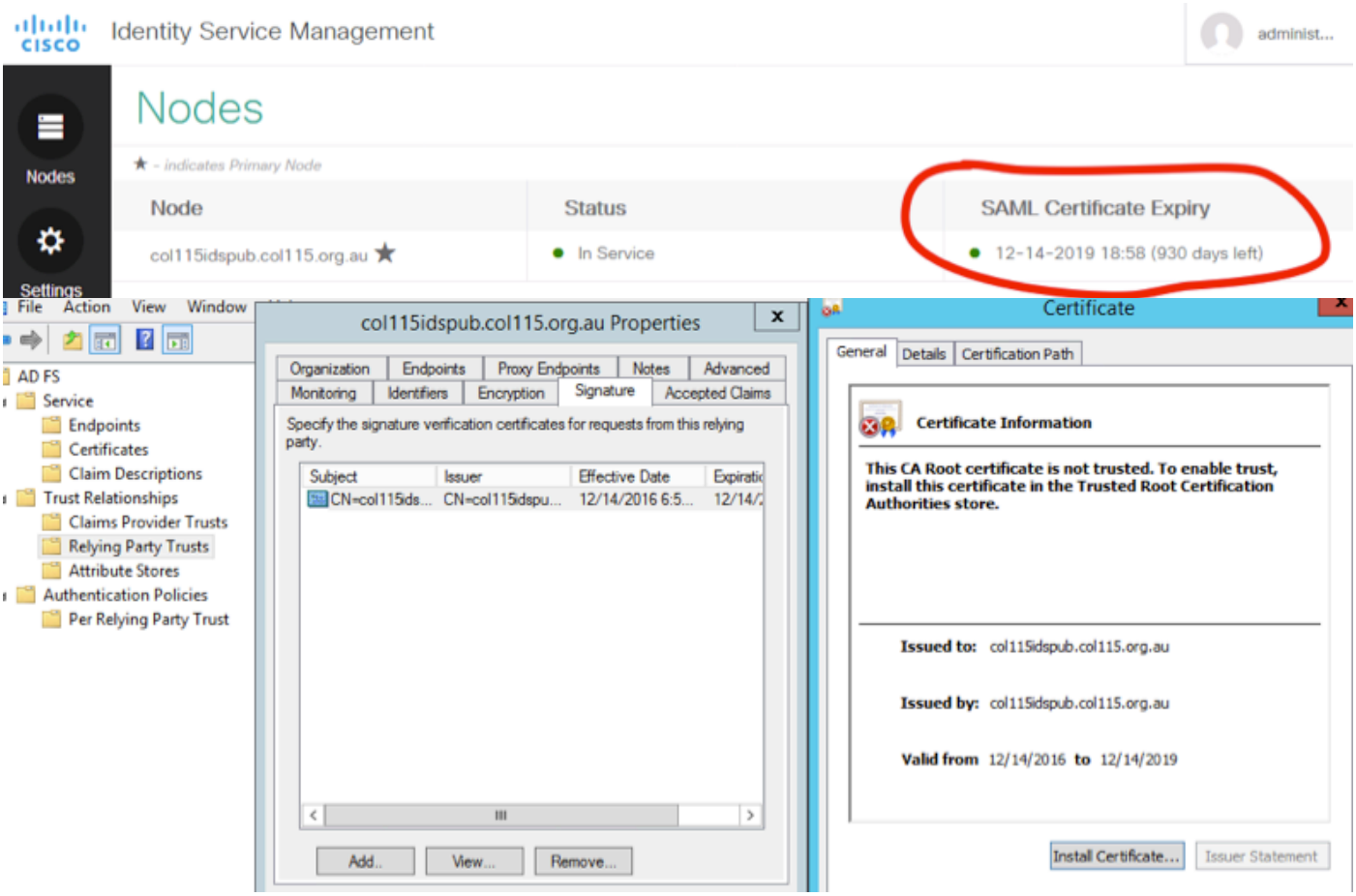

## Crittografia NON abilitata

## Parte D. Certificato laterale Cisco IDS

- certificato SAML
- Chiave di crittografia
- Chiave firma

### Certificato SAML

Questo certificato viene generato dal server IDS (autofirmato). Per impostazione predefinita è valido per 3 anni.

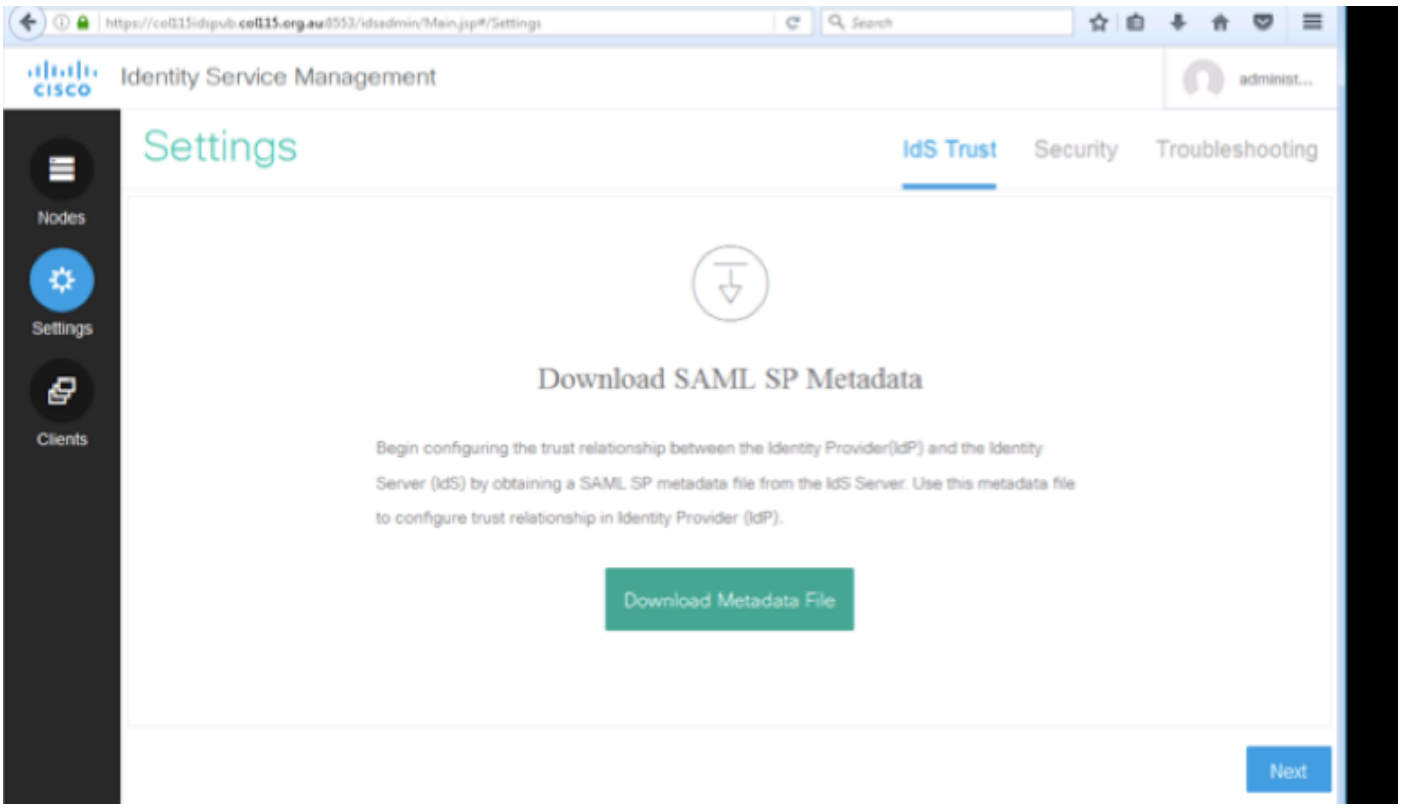


Questo certificato viene utilizzato per firmare la richiesta SAML e inviarla all'IDP (ADFS). La chiave pubblica è inclusa nei metadati IDS e deve essere importata nel server ADFS.

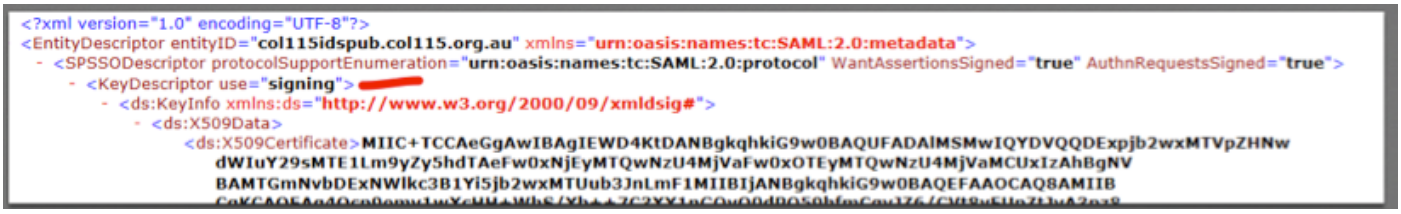
1.**Scaricare** i metadati SAML SP dal server IDS.

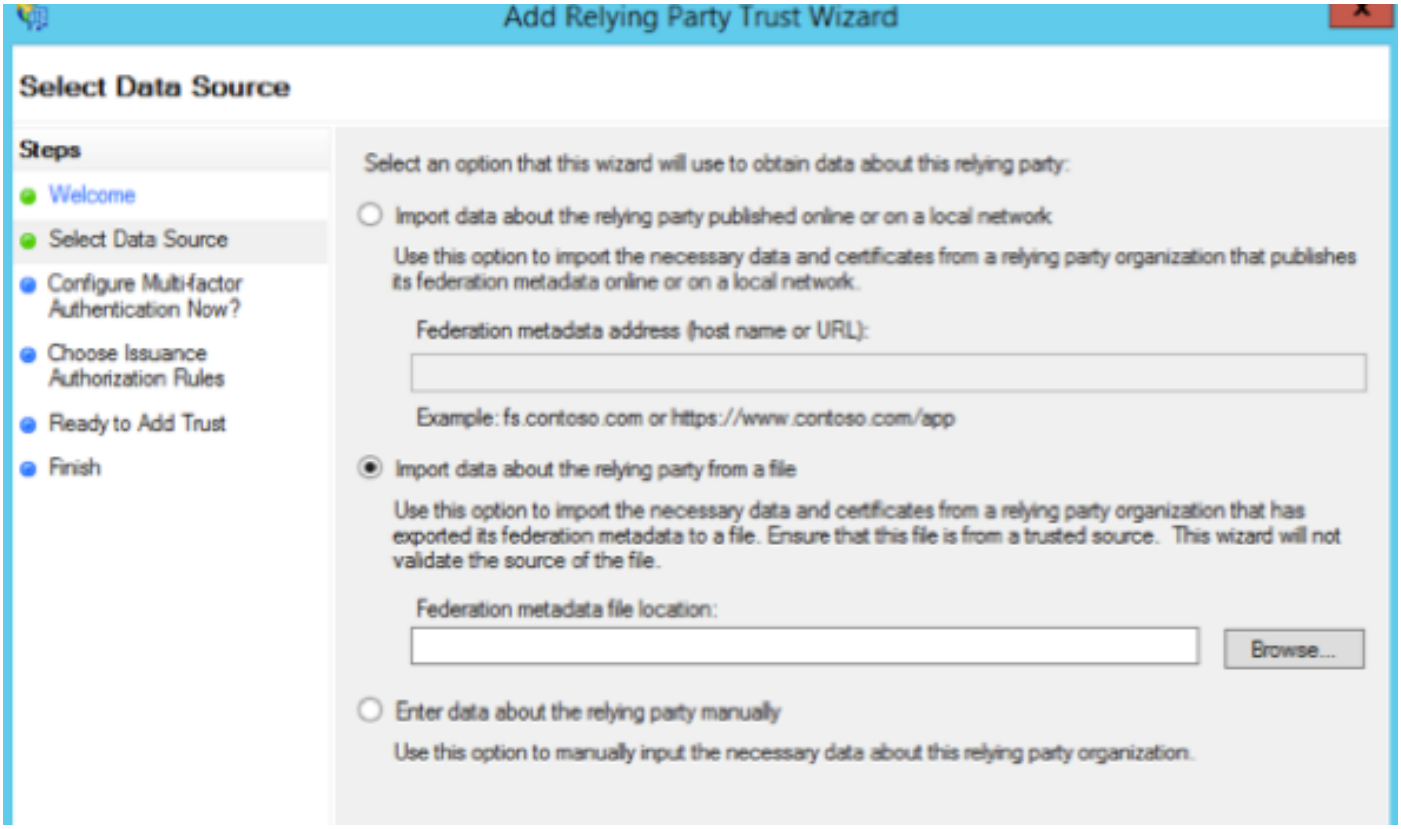
2. Passare a **https://<FQDN server ids>:8553/idsadmin/**.

3. Selezionare le impostazioni, scaricare i metadati SAML SP e **salvarli**.

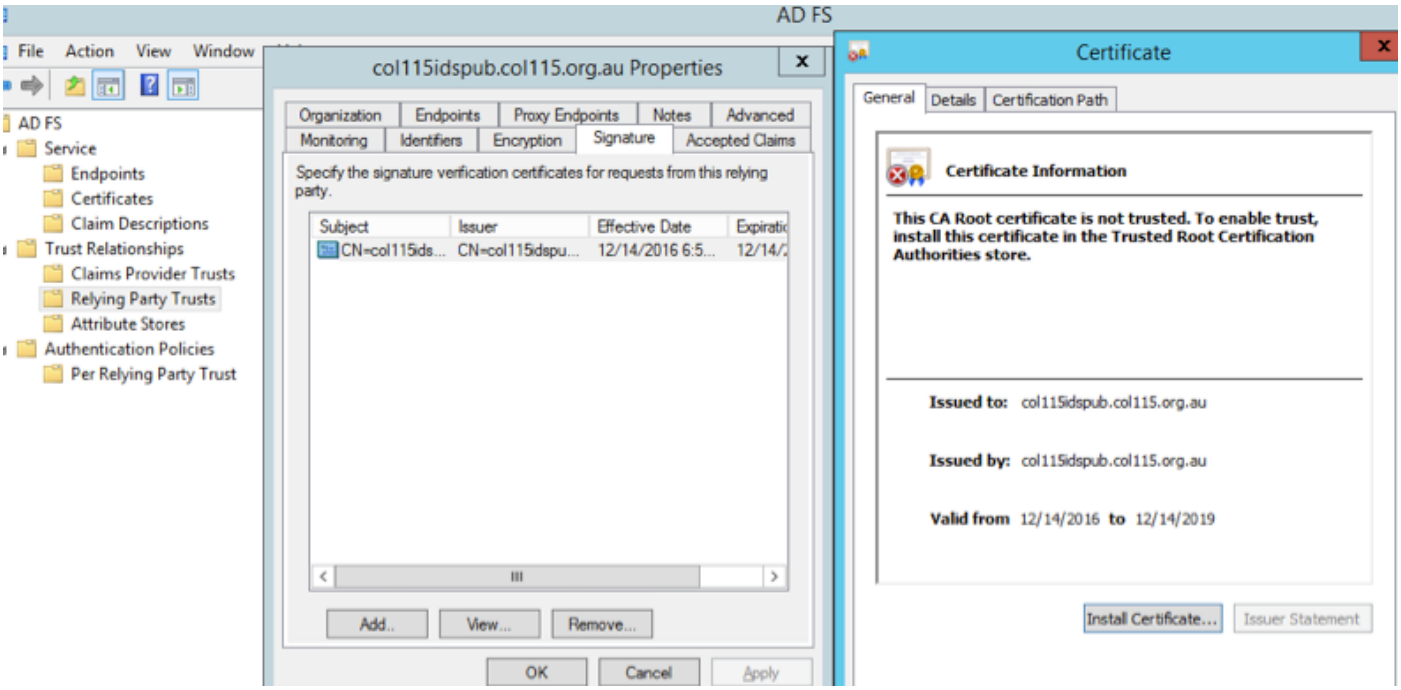



Metadati dal server IDS






importa nel server ADFS

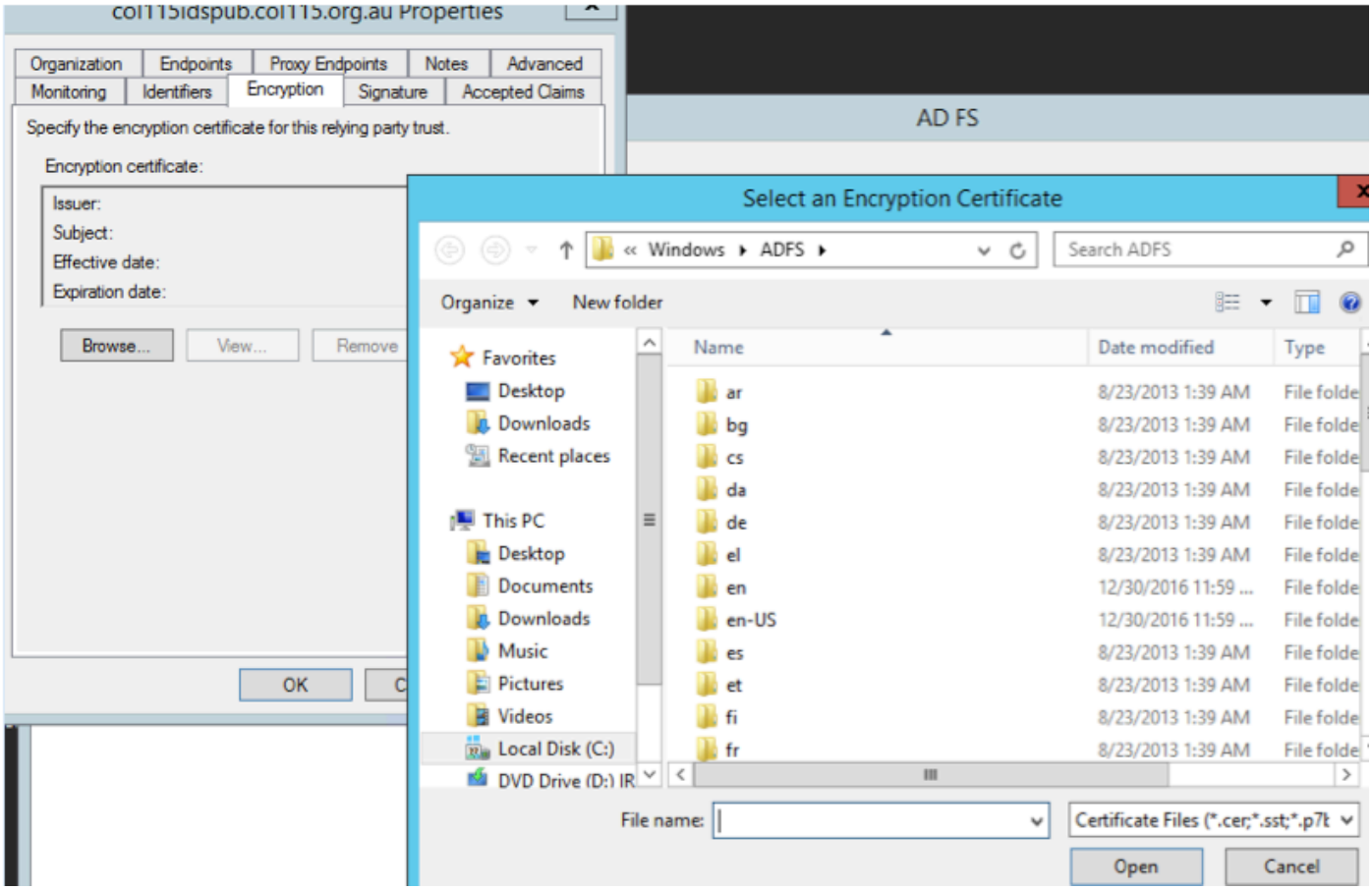



Verifica dal lato ADFS

Quando IDS rigenera il certificato SAML (quello utilizzato per firmare la richiesta SAML), esegue lo scambio di metadati.

### Chiave di crittografia/firma

Per impostazione predefinita, la crittografia non è attivata. Se la crittografia è abilitata, deve essere caricata in ADFS.




Riferimento:

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