Unified Contact Center Enterprise (UCCE) Single Sign On (SSO)-Zertifikate und -Konfiguration

Inhalt

Einführung

Dieses Dokument beschreibt Zertifikatskonfigurationen, die für UCCE SSO erforderlich sind. Die Konfiguration dieser Funktion umfasst mehrere Zertifikate für HTTPS, digitale Signatur und Verschlüsselung.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCCE-Version 11.5
- Microsoft Active Directory (AD) - AD installiert auf Windows Server
- Active Directory Federation Service (ADFS) Version 2.0/3.0

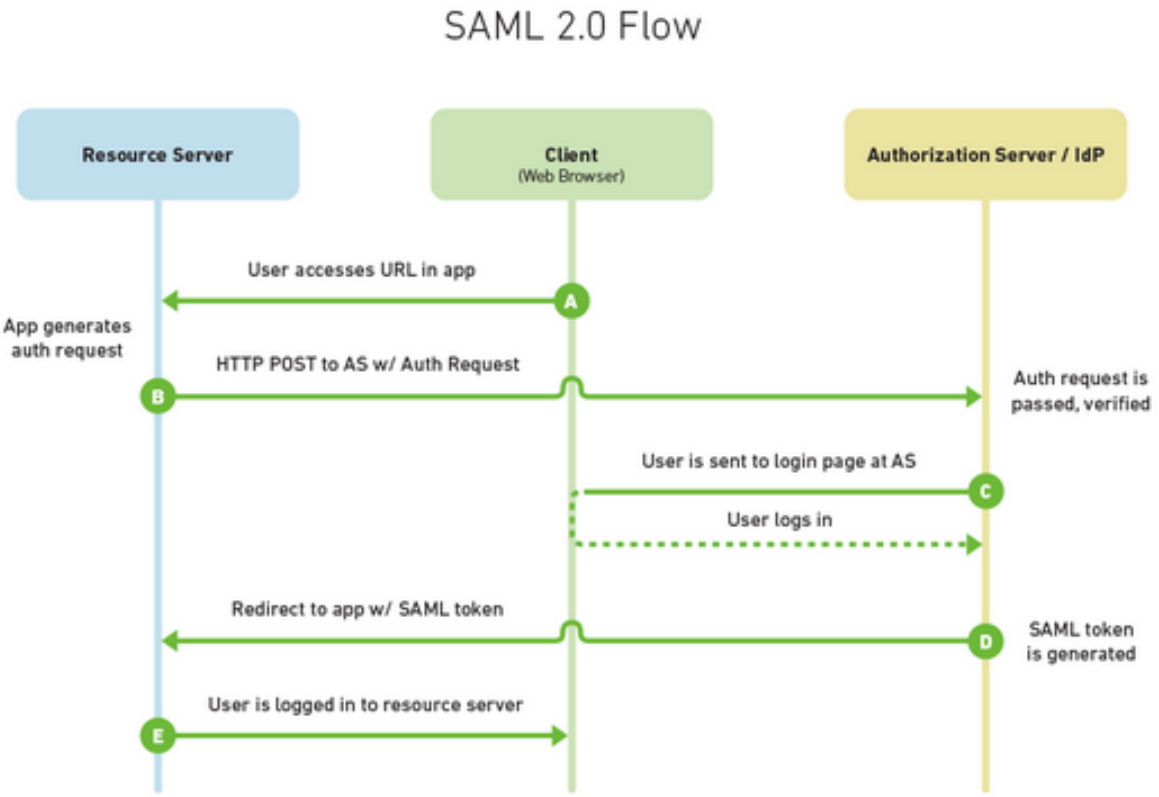
Verwendete Komponenten

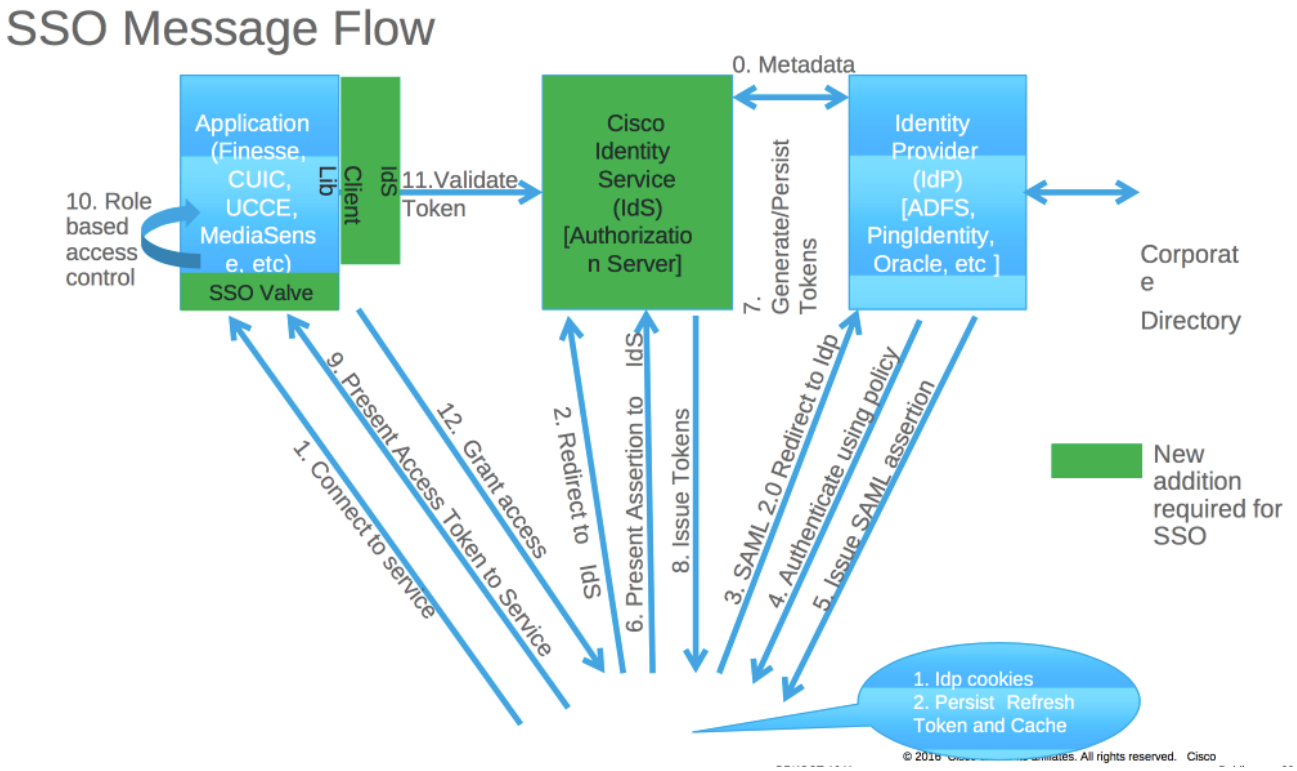
UCCE 11,5

Windows 2012 R2

Teil A. SSO-Nachrichtenfluss

The most common SAML flow is shown below:

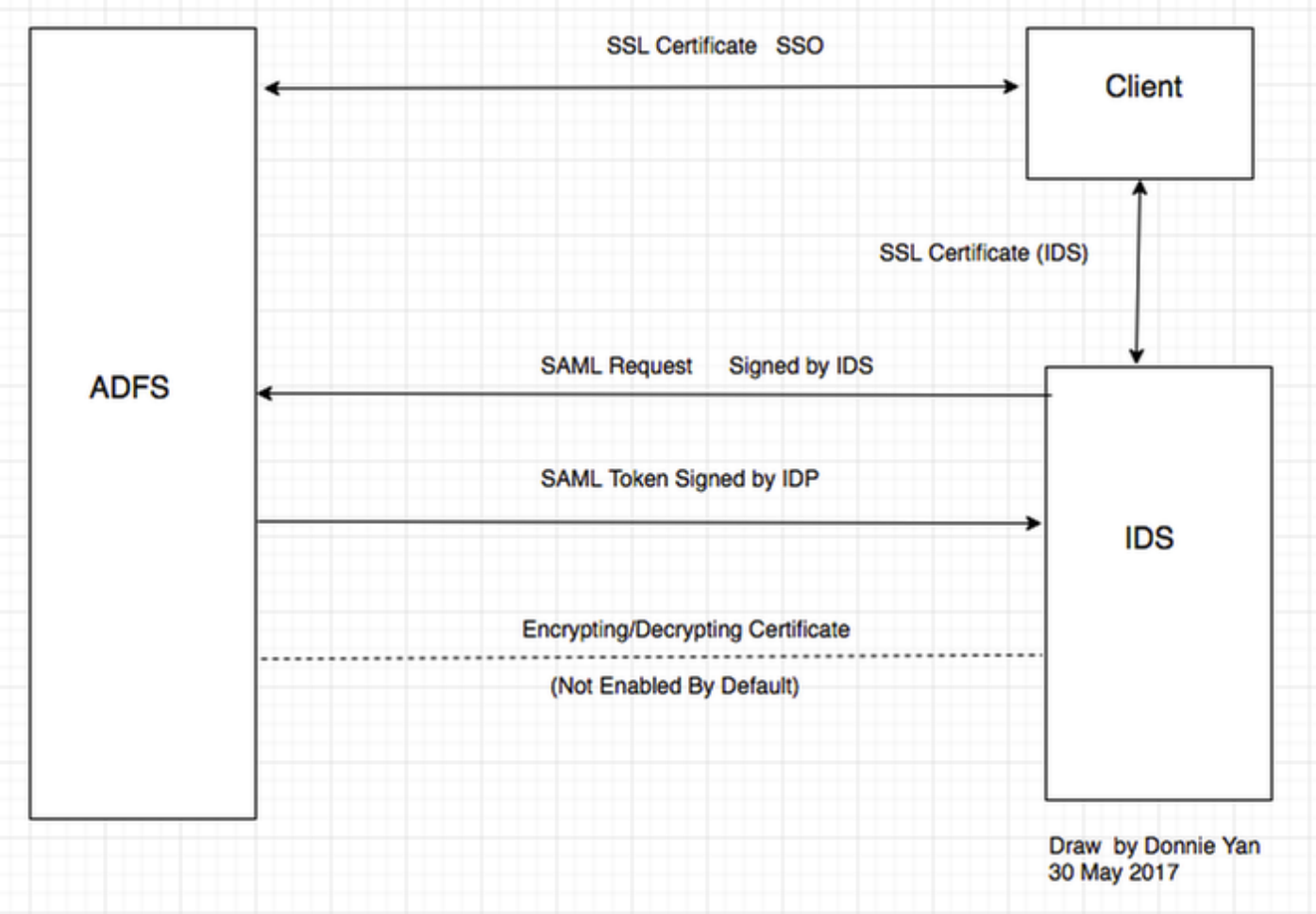




Wenn SSO aktiviert ist, meldet sich der Agent bei Finesse Desktop an:

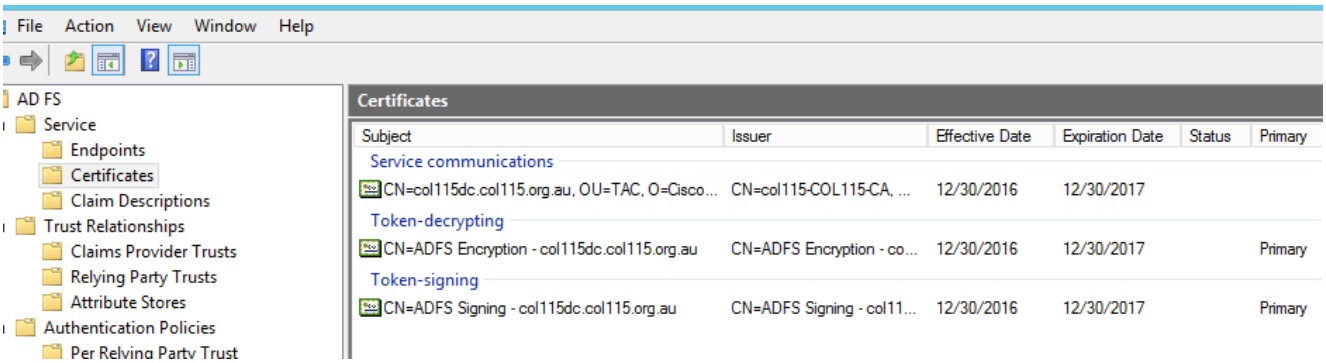
- Finesse-Server leitet Agent-Browser um, um mit Identity Service (IDS) zu kommunizieren
- IDS leitet Agent-Browser mit SAML-Anforderung an Identitätsanbieter (IDP) weiter
- IDP generiert SAML-Token und wird an den IDS-Server weitergeleitet.
- Wenn Token generiert wurde, verwendet der Agent bei jedem Durchsuchen der Anwendung dieses gültige Token für die Anmeldung.

Teil B. Zertifikate für IDP und IDS



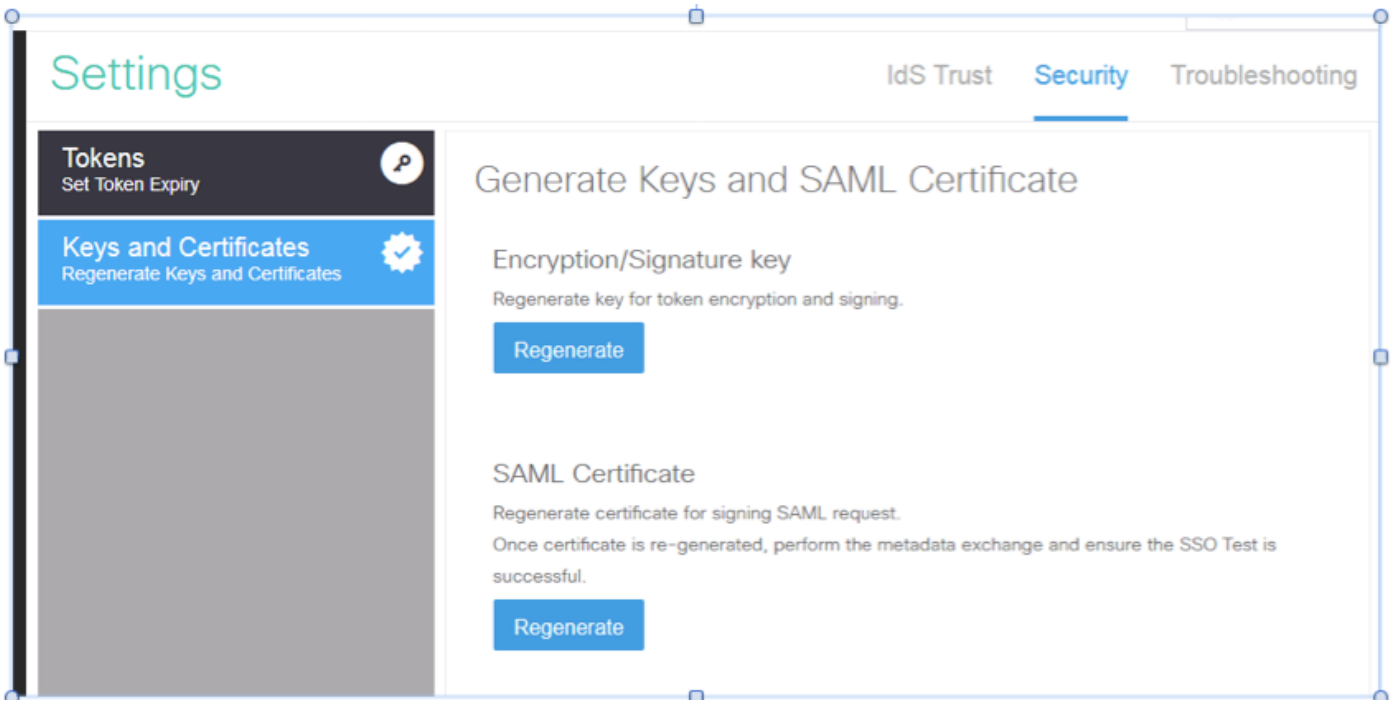
IDP-Zertifikate

- SSL-Zertifikat (SSO)
- Token-Signaturzertifikat
- Token - Entschlüsseln

1. 

IDS-Zertifikate

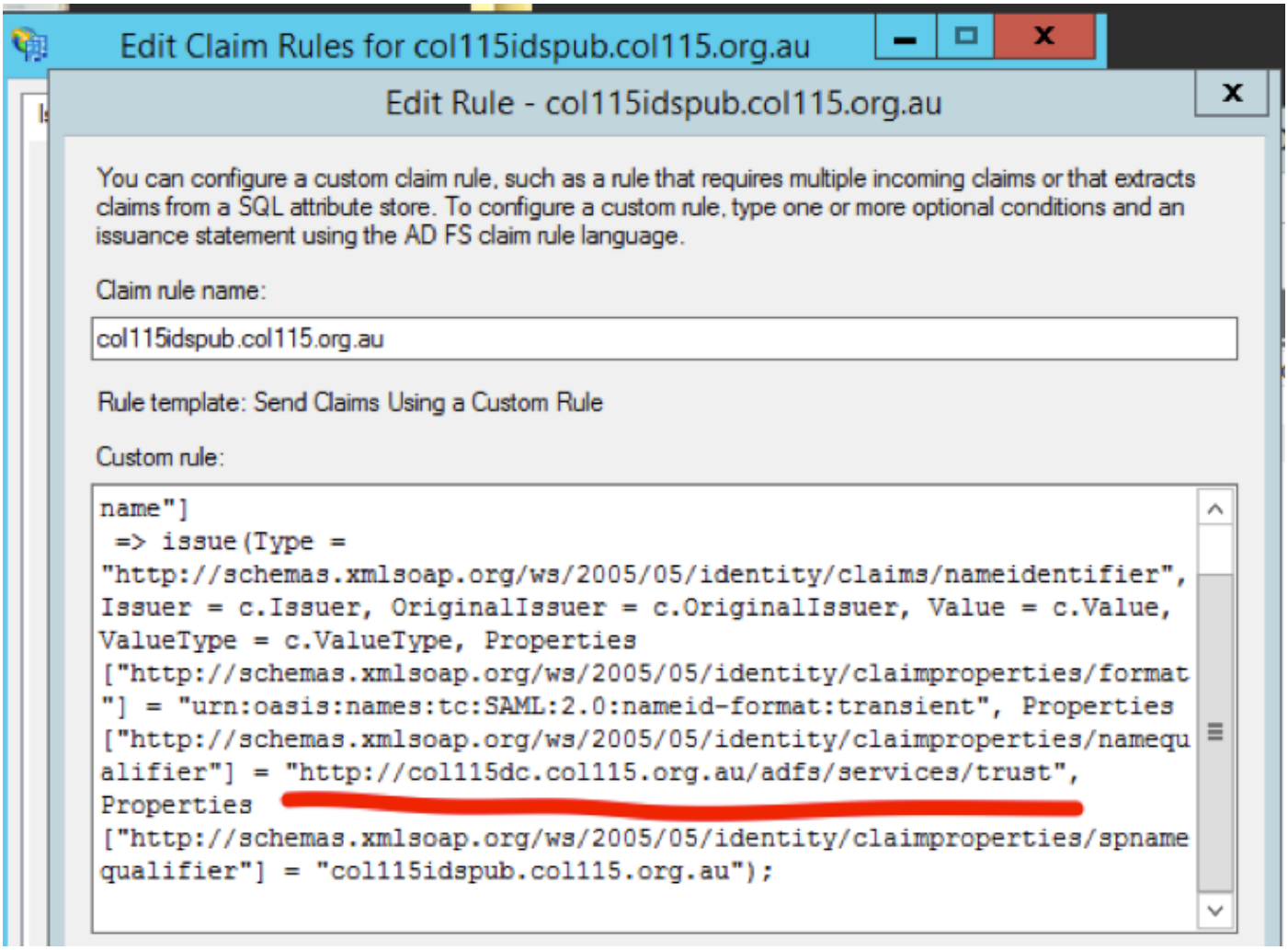
- SAML-Zertifikat
- Signaturschlüssel
- Verschlüsselungsschlüssel



Teil C. IDP-Zertifizierung im Detail und Konfiguration

SSL-Zertifikat (SSO)

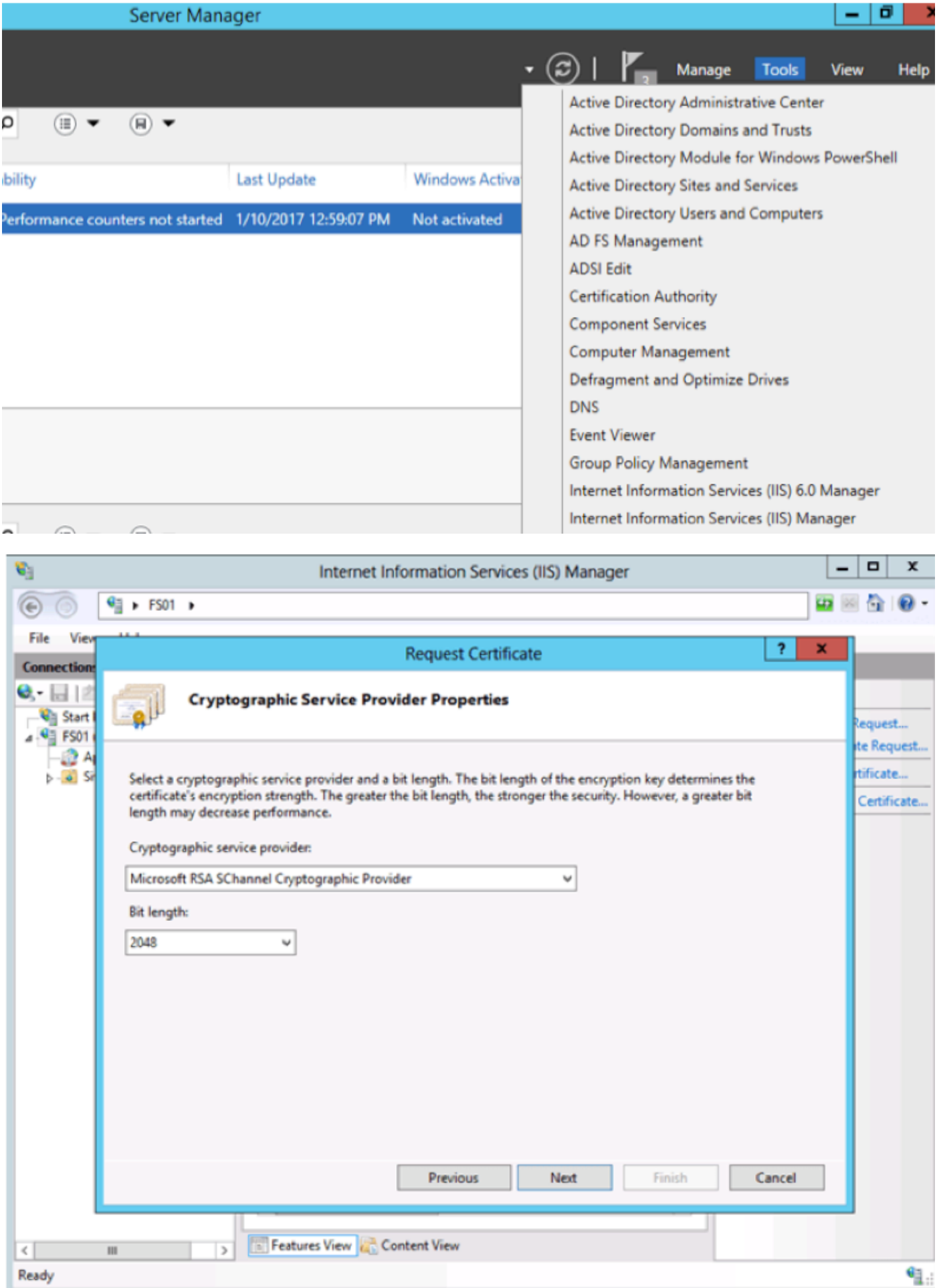
- Dieses Zertifikat wird zwischen IDP und Client verwendet. Kunde muss SSO-Zertifikat vertrauen
- Das SSL-Zertifikat wird zur Verschlüsselung der Sitzung zwischen dem Client und dem IDP-Server bereitgestellt. Dieses Zertifikat ist nicht für ADFS spezifisch, sondern für IIS.
- Der Betreff des SSL-Zertifikats muss mit dem in der ADFS-Konfiguration verwendeten Namen übereinstimmen.



Schritte zum Konfigurieren des SSL-Zertifikats für SSO (lokales Labor mit signierter interner Zertifizierungsstelle)

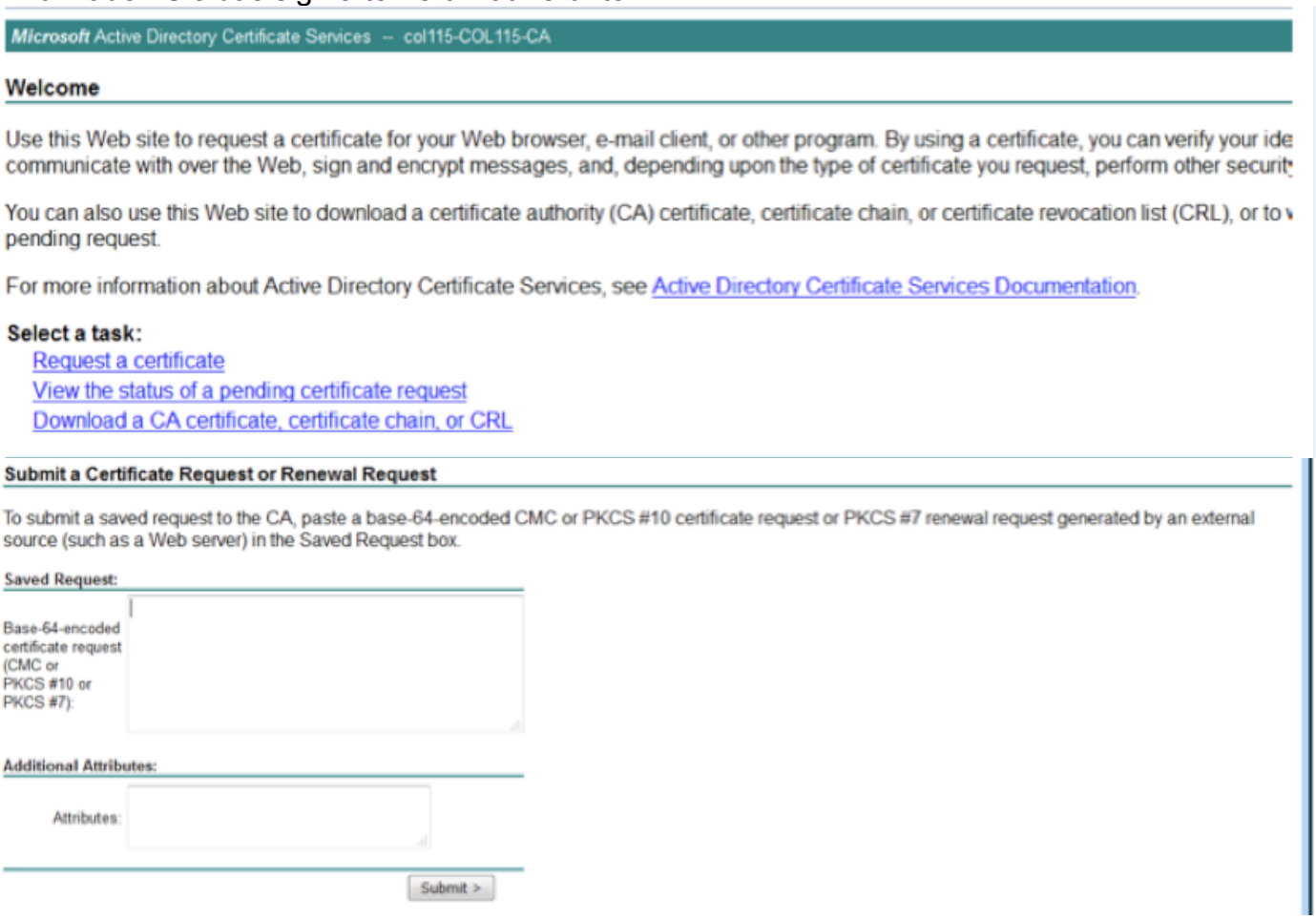
Schritt 1: **Erstellen Sie ein** SSL-Zertifikat mit Zertifikatsanforderung (Certificate Signing Request, CSR), und signieren Sie das Zertifikat von einer internen Zertifizierungsstelle für ADFS.

1. Öffnen Sie Server Manager.
2. Klicken Sie auf Extras.
3. Klicken Sie auf Internetinformationsdienste-Manager (IIS).
4. Wählen Sie den lokalen Server aus.
5. Wählen Sie Serverzertifikate aus.
6. Klicken Sie auf Funktion öffnen (Aktionsbereich).
7. Klicken Sie auf Zertifikatsanforderung **erstellen**.
8. Lassen Sie den Kryptografiedienstanbieter standardmäßig unverändert.
9. Ändern Sie die **Bit-Länge in 2048**.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie einen Speicherort für die angeforderte Datei aus.
12. Klicken Sie auf **Fertig stellen**.



Schritt 2: CA signiert die aus Schritt 1 generierte CSR-Anfrage.

1. **Öffnen Sie** den CA-Server, um diesen CSR **http:<CA-Server-IP-Adresse>/certsrv/**zu verwenden.
2. Klicken Sie auf Zertifikat anfordern.
3. Klicken Sie auf Erweiterte Zertifikatsanforderung.
4. **Kopieren Sie** den CSR in eine Base-64-codierte Zertifikatsanforderung.
5. **Senden**.
6. Laden Sie das signierte Zertifikat herunter.



Schritt 3: Installieren Sie das signierte Zertifikat zurück zum ADFS-Server, und weisen Sie die ADFS-Funktion zu.

1. Installieren Sie das signierte Zertifikat zurück zum ADFS-Server. Dazu **öffnen Sie den Server Manager > Extras > Internetinformationsdienste (IIS)-Manager >** .

Lokaler Server > Serverzertifikat > Funktion öffnen (Aktionsbereich).

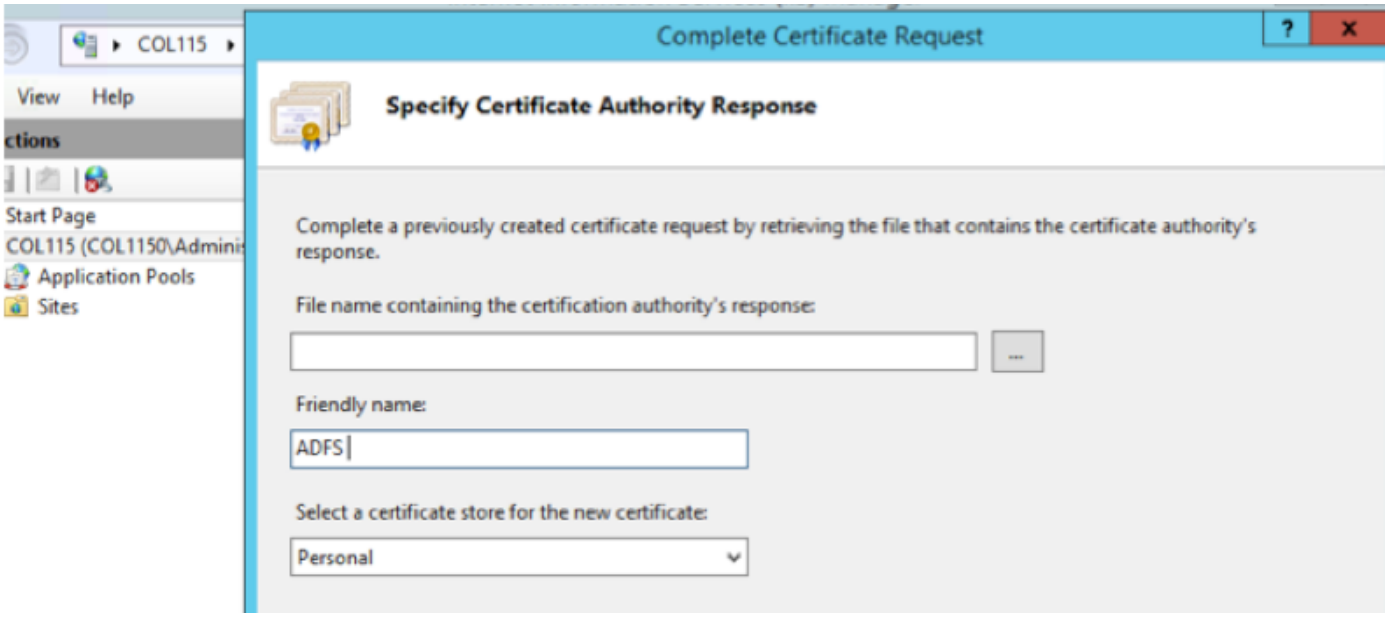
2. Klicken Sie auf Abschlusszertifikatanforderung.

3. Wählen Sie den Pfad zur vollständigen CSR-Datei aus, die Sie vom Zertifikatanbieter des Fremdherstellers abgeschlossen und heruntergeladen haben.

4. **Geben Sie** den freundlichen Namen für das Zertifikat ein.

5. Wählen Sie als Zertifikatsspeicher Personal aus.

6. Klicken Sie auf **OK**.



7. In dieser Phase wurden alle Zertifikate hinzugefügt. Nun ist die Zuweisung von SSL-Zertifikaten erforderlich.

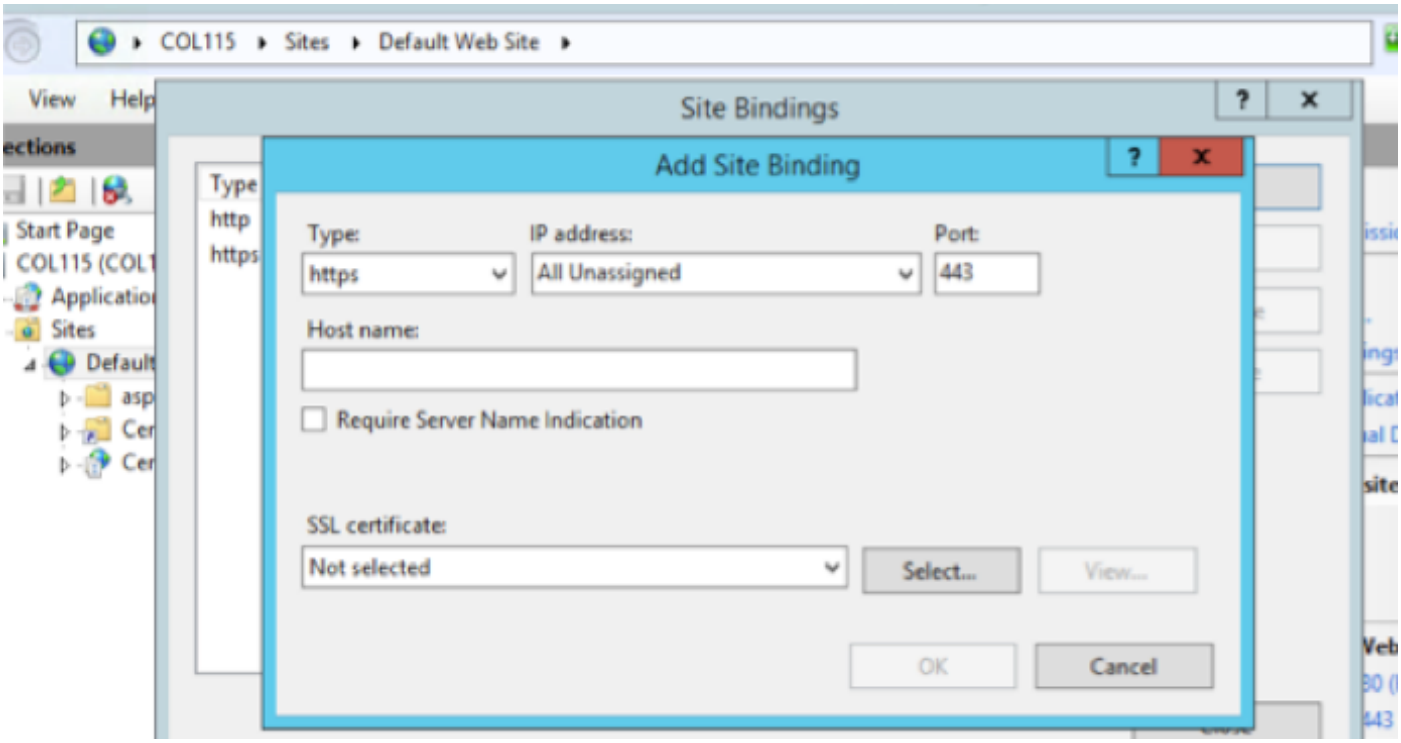
8. **Erweitern Sie** den **lokalen Server > Sites erweitern > Standardwebsite auswählen > Auf Bindungen** (Aktionsbereich) klicken.

9. Klicken Sie auf **Hinzufügen**.

10. **Ändern Sie** den Typ in HTTPS.

11. Wählen Sie Ihr Zertifikat aus dem Dropdown-Menü aus.

12. Klicken Sie auf **OK**.



Nun wurde das SSL-Zertifikat für den ADFS-Server zugewiesen.

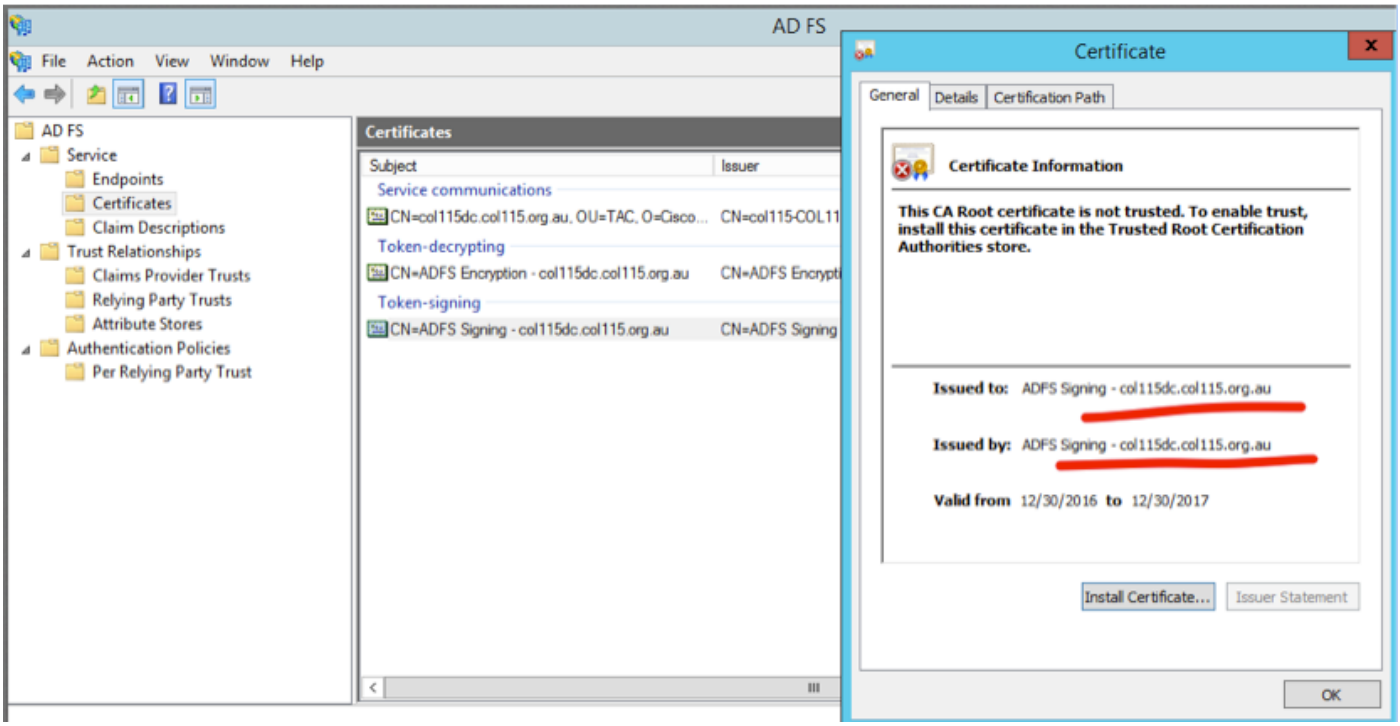
Hinweis: Bei der Installation der ADFS-Funktion muss ein vorheriges SSL-Zertifikat verwendet werden.

Token-Signaturzertifikat

ADFS generiert selbstsigniertes Zertifikat für Token-Signaturzertifikate. Standardmäßig ist sie für ein Jahr gültig.

Das von IDP generierte SAML-Token wird von einem privaten ADFS-Schlüssel (Token Signing Certificate Private Part) signiert. Anschließend überprüft IDS mithilfe des öffentlichen ADFS-Schlüssels. Dieses garantierte signierte Token wird nicht modifiziert.

Das Token Signing Certificate wird immer dann verwendet, wenn ein Benutzer Zugriff auf eine Anwendung von Drittanbietern (Cisco IDS) erhalten muss.

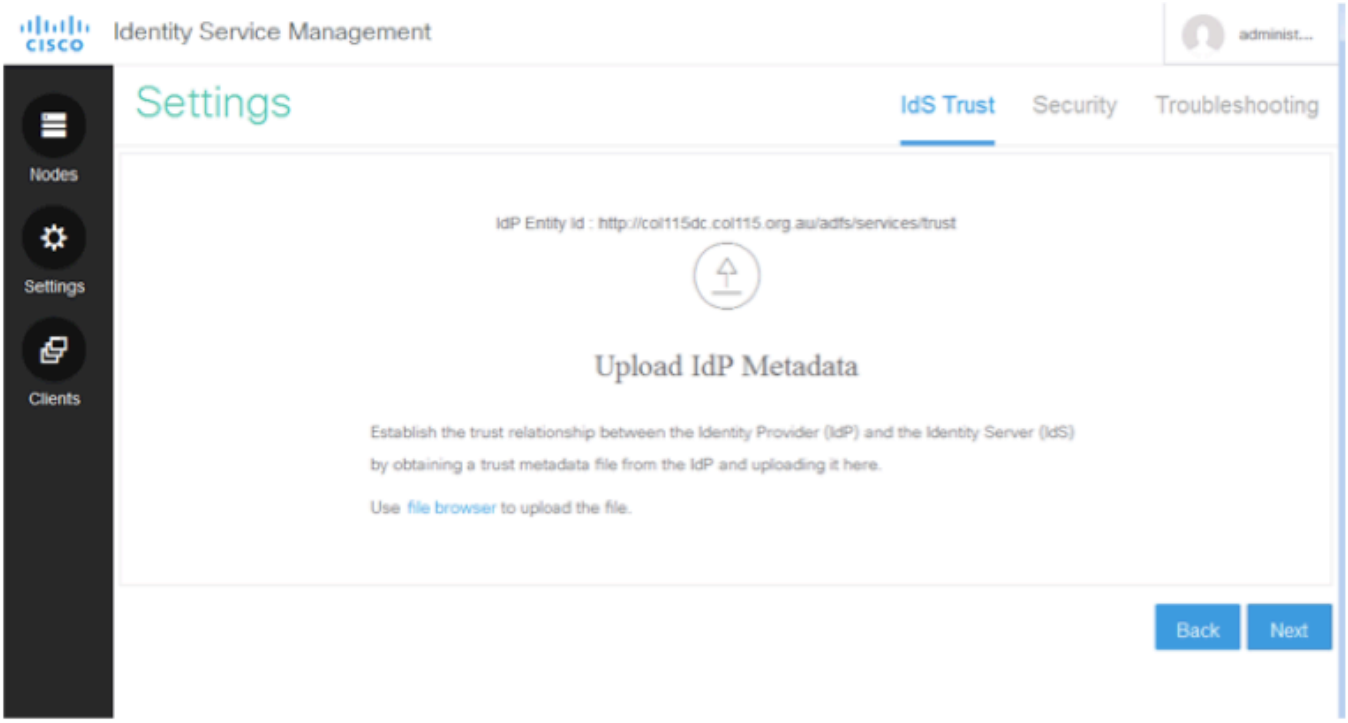


Wie erhält der Cisco IDS-Server den öffentlichen Schlüssel des Token Singing-Zertifikats?

Dies geschieht durch das Hochladen von ADFS-Metadaten auf den IDS-Server und anschließendes Übergeben des öffentlichen ADFS-Schlüssels an den IDS-Server. Auf diese Weise erhält IDS den öffentlichen Schlüssel des ADFS-Servers.

Sie müssen IDP-Metadaten von ADFS **herunterladen**. Informationen zum Herunterladen von IDP-Metadaten finden Sie unter **https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

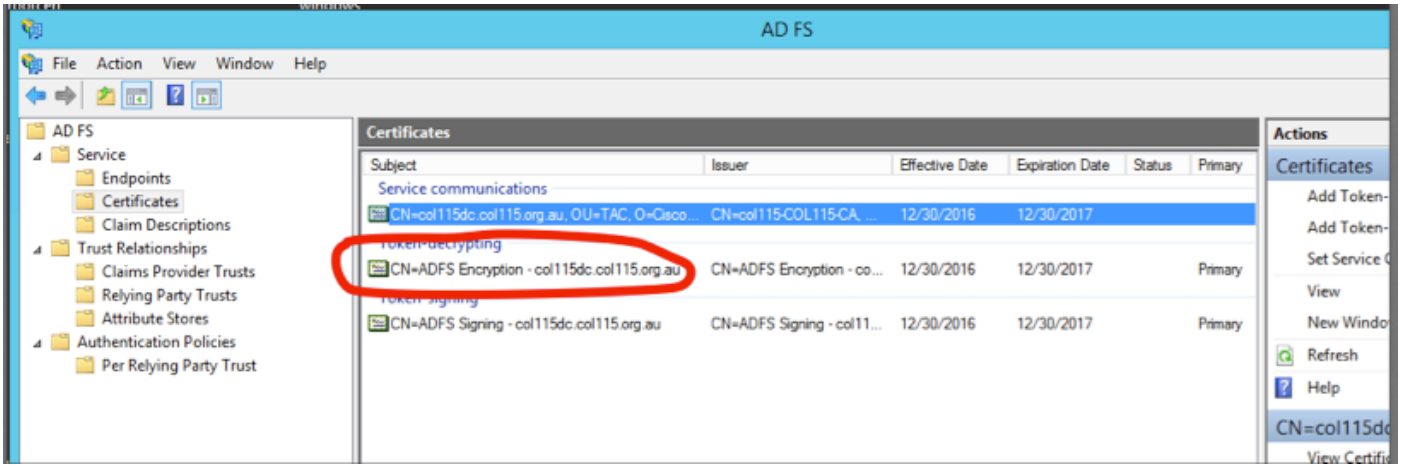
Von ADFS-
Metadaten



ADFS-Metadaten auf IDS hochladen

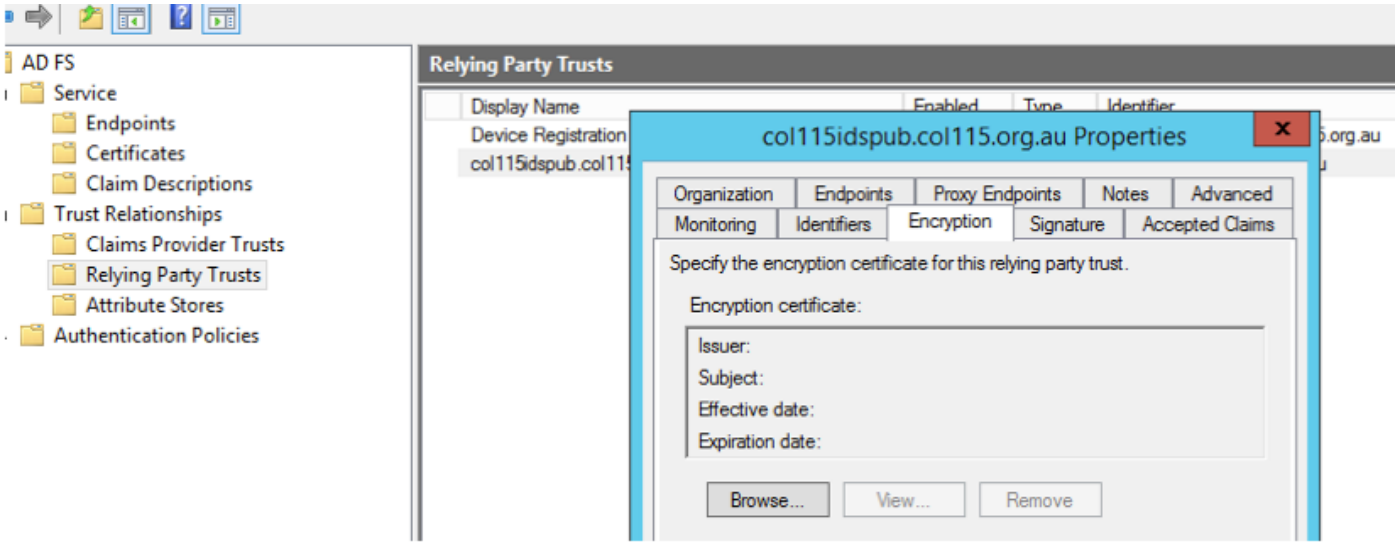
Token-Entschlüsselung

Dieses Zertifikat wird automatisch vom ADFS-Server (selbstsigniert) generiert. Wenn das Token verschlüsselt werden muss, verwendet ADFS den öffentlichen IDS-Schlüssel, um ihn zu entschlüsseln. Wenn Sie jedoch ADFS-Token-Verschlüsselung sehen, bedeutet dies NICHT, dass das Token verschlüsselt ist.



Wenn Sie sehen möchten, ob die Tokenverschlüsselung für eine bestimmte Anwendung eines vertrauenden Drittanbieters aktiviert wurde, müssen Sie die Registerkarte Verschlüsselung für eine bestimmte Anwendung eines Drittanbieters überprüfen.

Dieses Bild zeigt, dass die Tokenverschlüsselung NICHT aktiviert wurde.



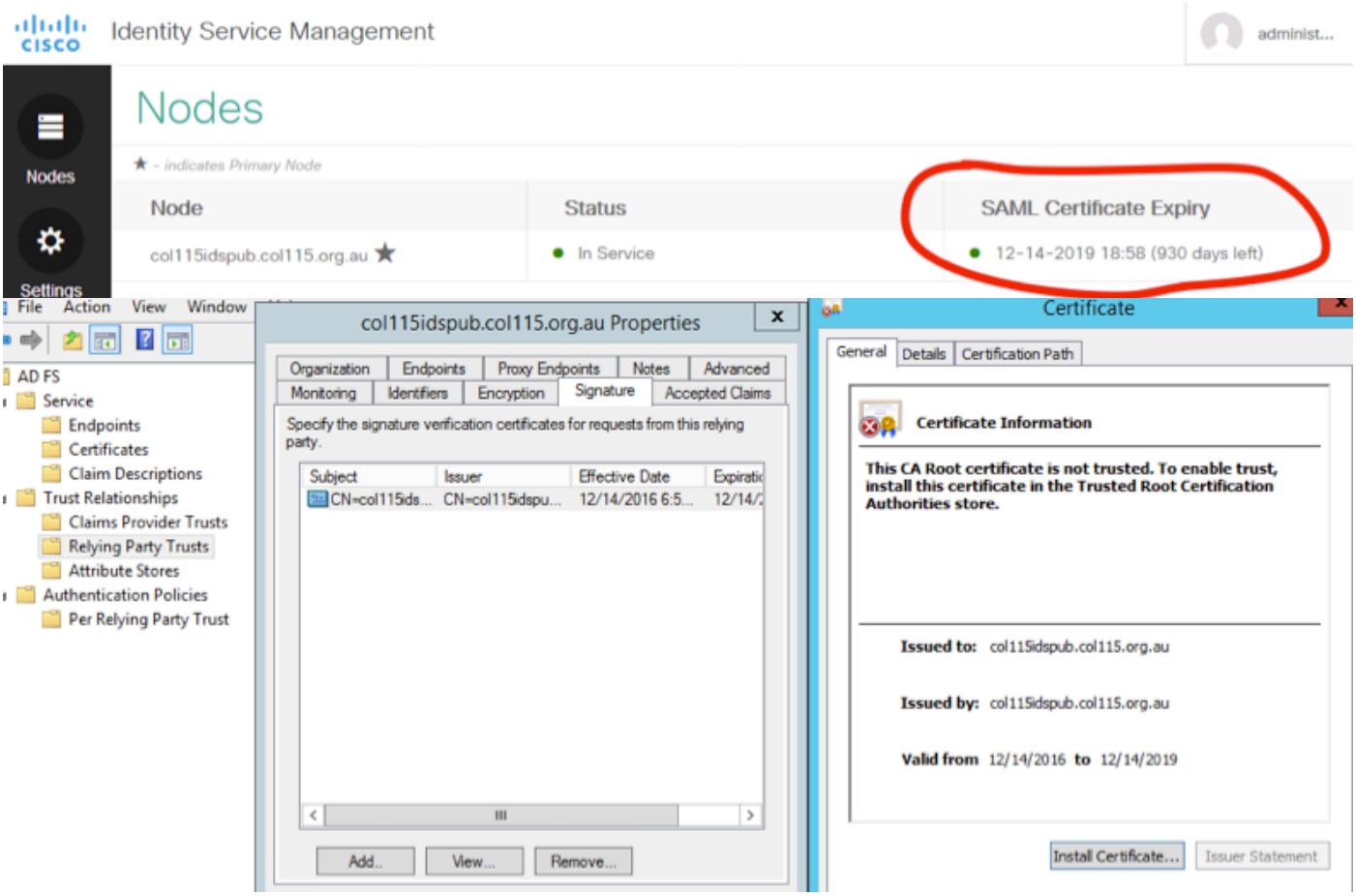
Verschlüsselung NICHT aktiviert

Teil D. Cisco IDS Side Certificate

- SAML-Zertifikat
- Verschlüsselungsschlüssel
- Signaturschlüssel

SAML-Zertifikat

Dieses Zertifikat wird vom IDS-Server (selbstsigniert) generiert. Standardmäßig ist sie für 3 Jahre gültig.

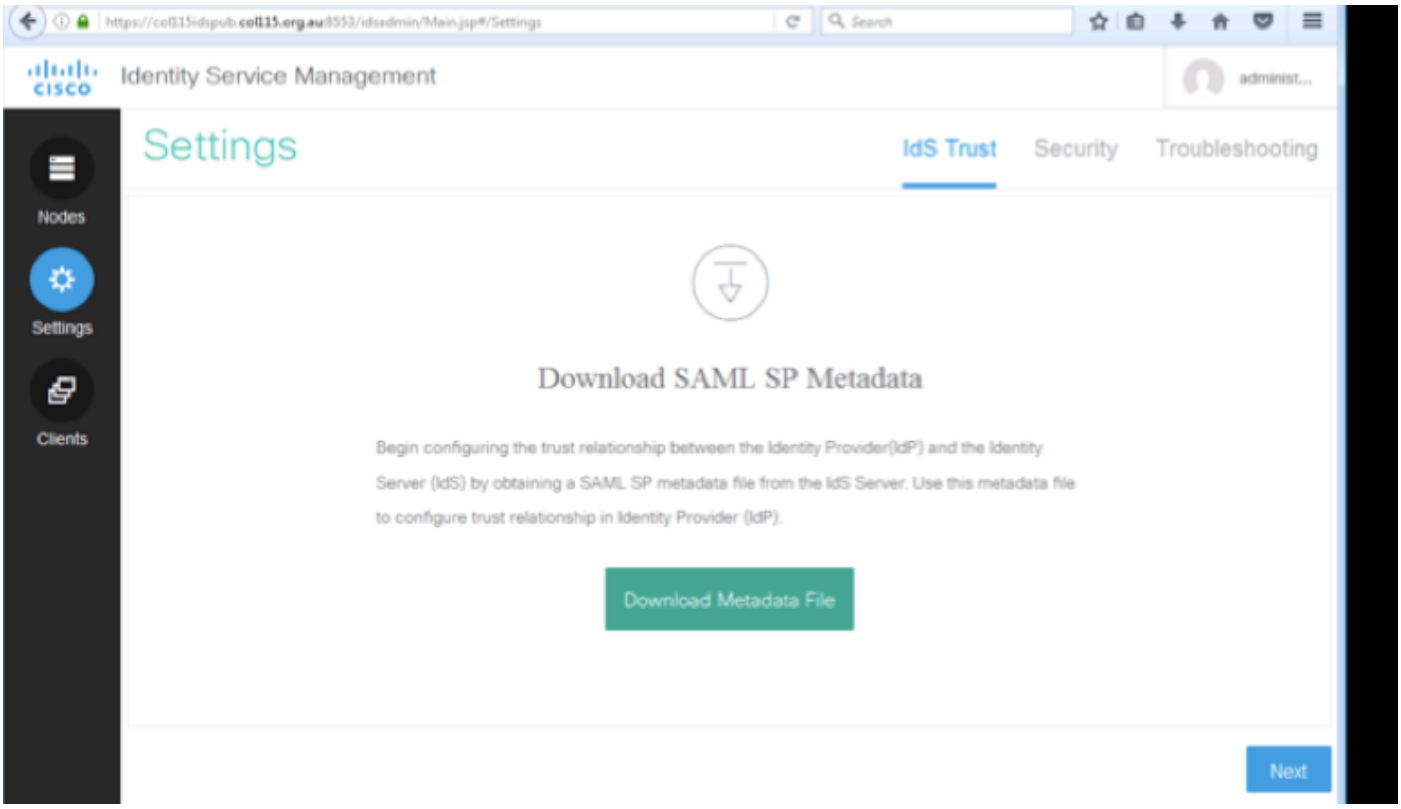


Dieses Zertifikat wird zum Signieren der SAML-Anforderung und zum Senden an IDP (ADFS) verwendet. Dieser öffentliche Schlüssel befindet sich in den IDS-Metadaten und muss in den ADFS-Server importiert werden.

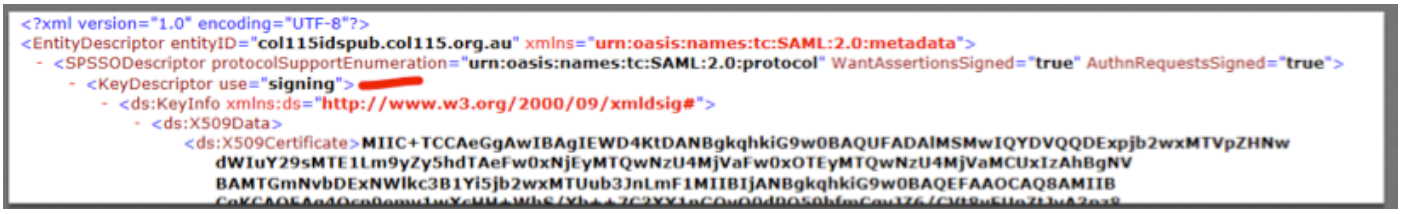
1. SAML SP-Metadaten vom IDS-Server **herunterladen**

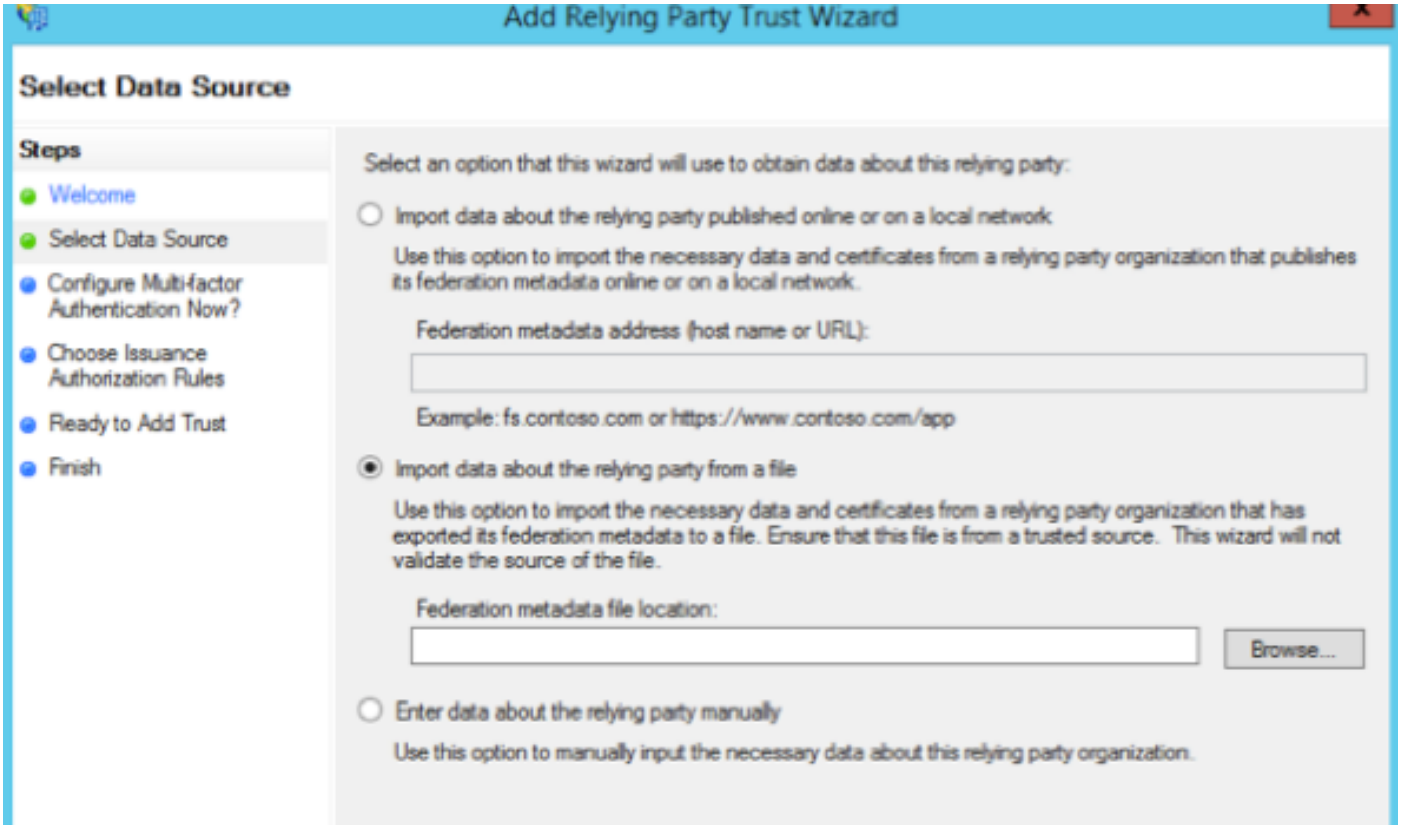
2. Rufen Sie **https://<ids server FQDN>:8553/idsadmin/**auf.

3. Wählen Sie Einstellungen aus, laden Sie SAML SP-Metadaten herunter, und **speichern Sie** sie.

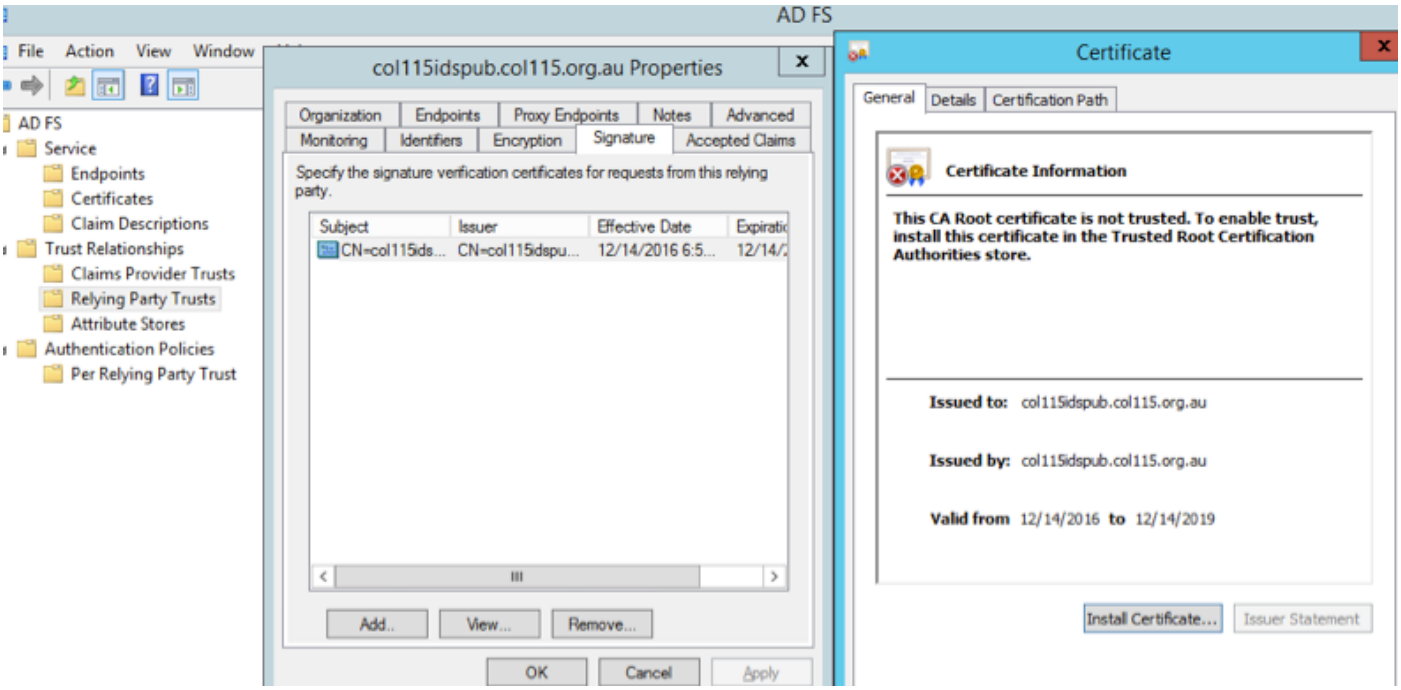


Metadaten vom IDS-Server





Import auf ADFS-Server

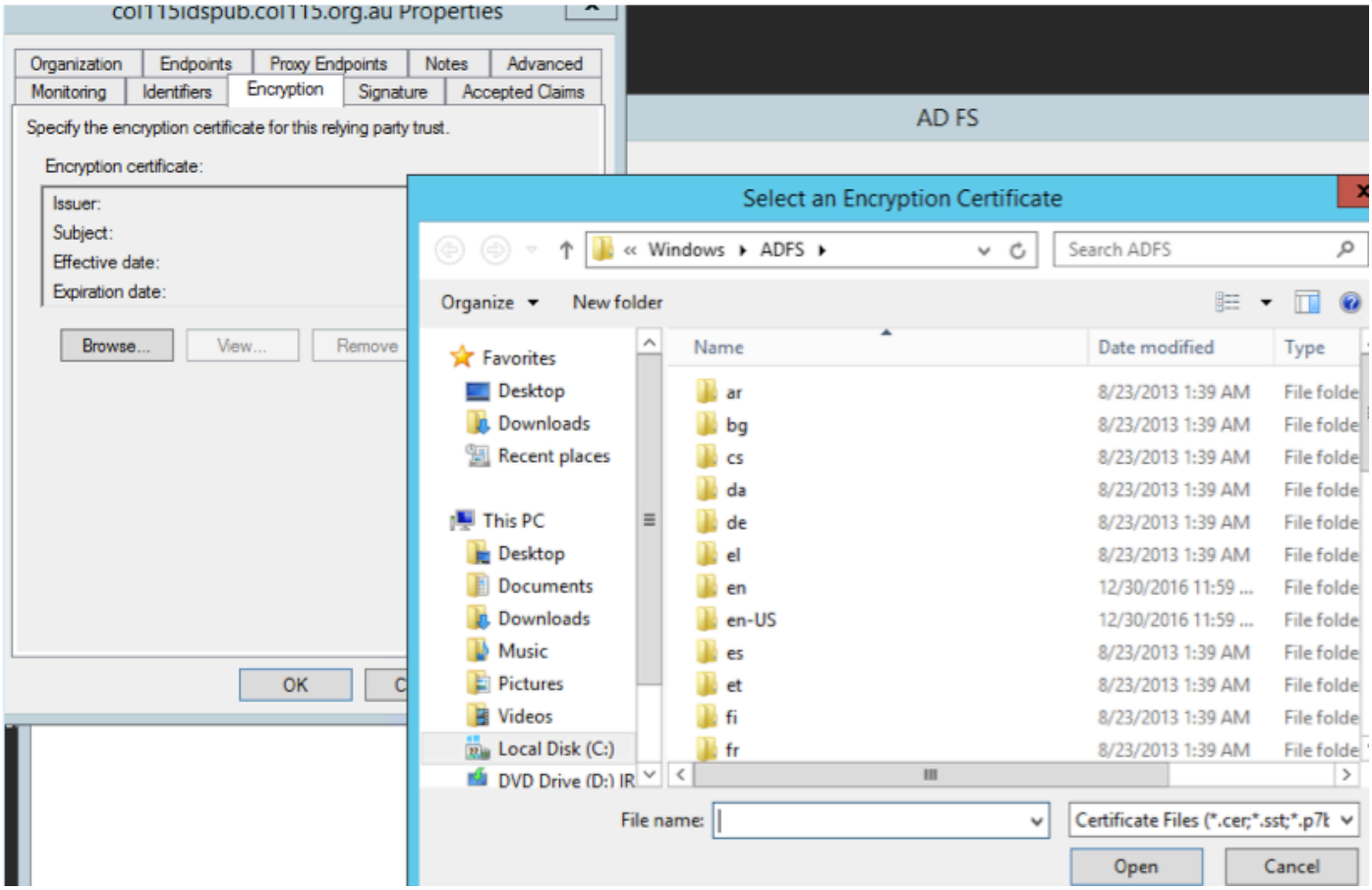


Überprüfen von ADFS-Seite

Wenn IDS das SAML-Zertifikat neu generiert, das zum Signieren der SAML-Anforderung verwendet wird, führt es einen Metadatenaustausch durch.

Verschlüsselungs-/Signaturschlüssel

Die Verschlüsselung ist standardmäßig nicht aktiviert. Wenn die Verschlüsselung aktiviert ist, muss sie in ADFS hochgeladen werden.



Referenz:

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