Unified Contact Center Enterprise（UCCE）シングル サインオン（SSO）の証明書と構成

目次

概要

このドキュメントでは、UCCE SSO に必要な証明書の設定について説明します。 この機能の設定では、HTTPS 用の複数の証明書、デジタル署名、暗号化の設定を行います。

要件

次の項目に関する知識が推奨されます。

- UCCE リリース 11.5
- Microsoft Active Directory（AD ）：Windows サーバにインストールされている AD
- Active Directory フェデレーション サービス（ADFS）バージョン 2.0/3.0

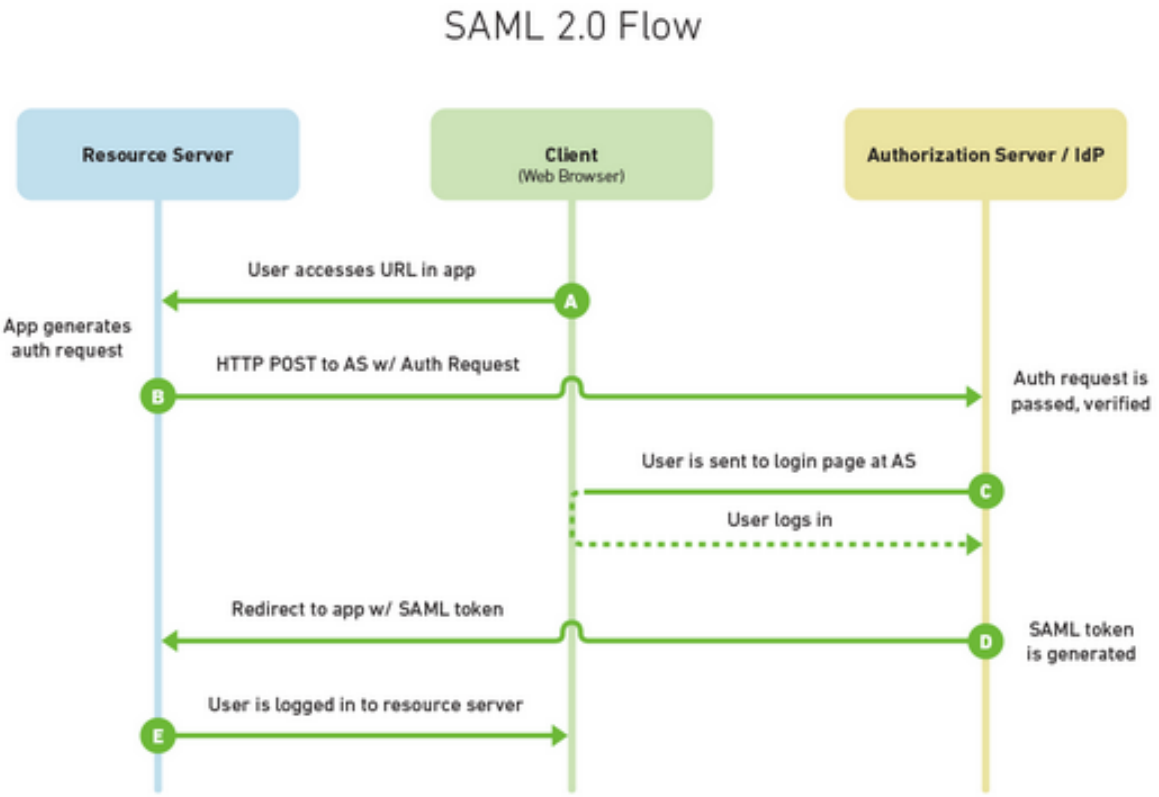
使用するコンポーネント

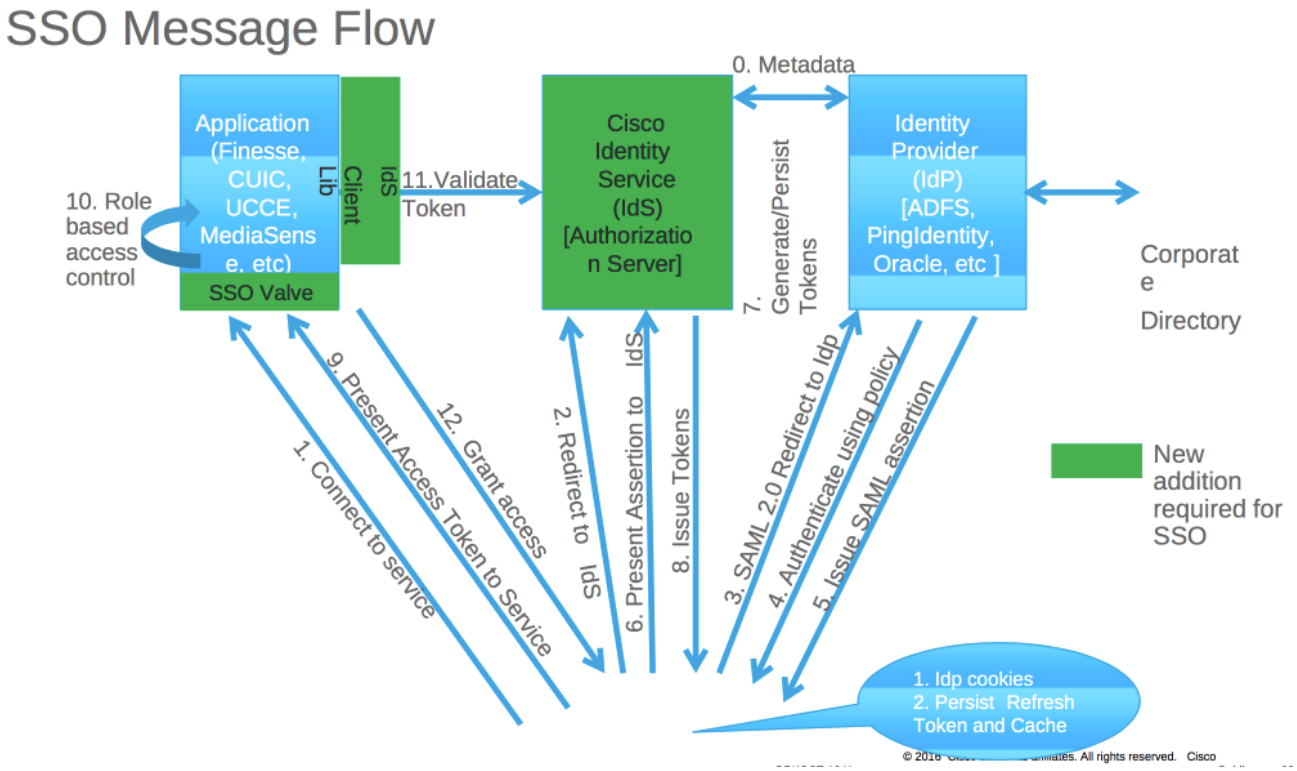
UCCE 11.5

Windows 2012 R2

パート A：SSO メッセージ フロー

The most common SAML flow is shown below:



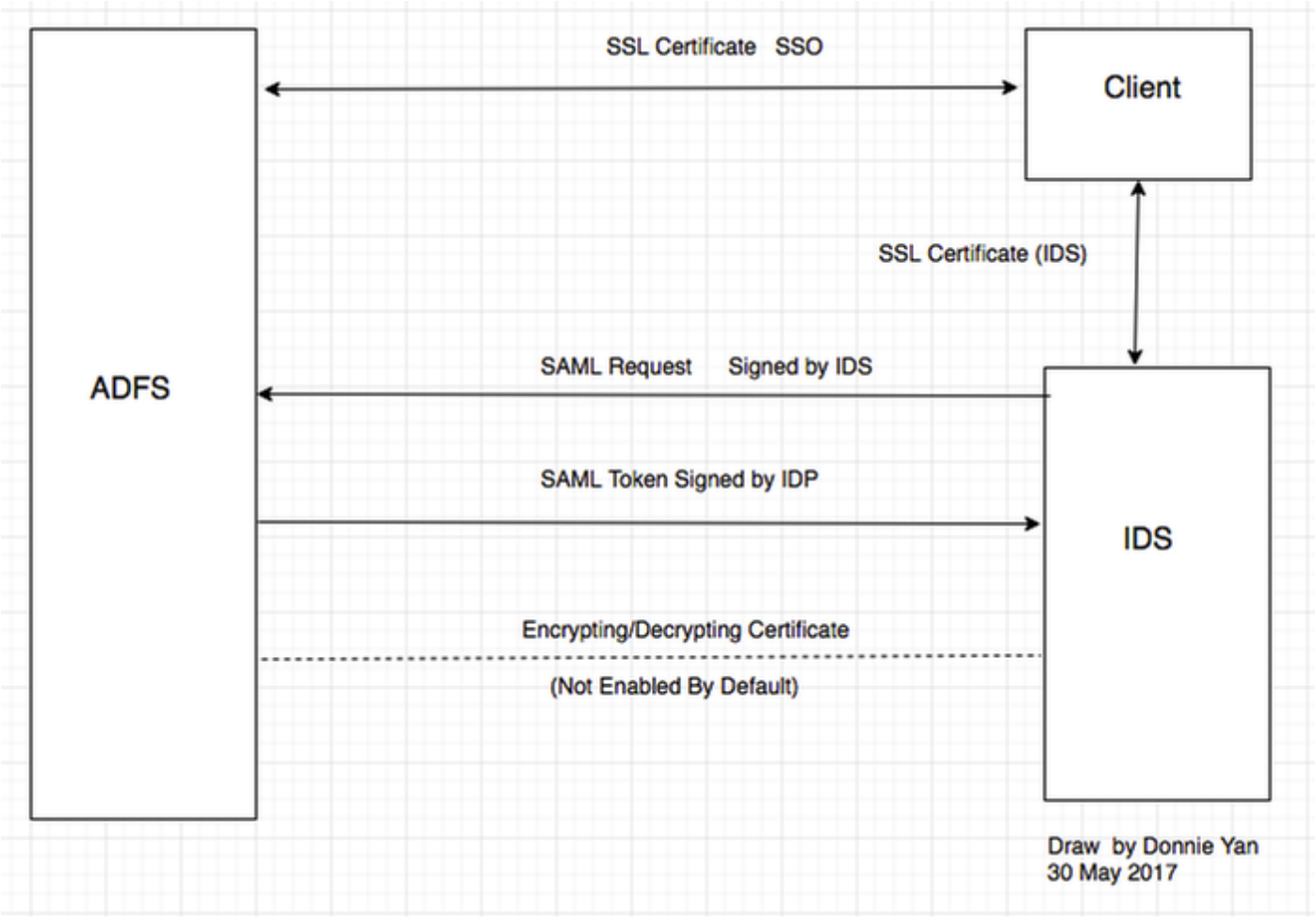


SSO を有効にした状態でエージェントが Finesse デスクトップにログインすると、次のことが起こります。

- アイデンティティ サービス（IDS）と通信するため、Finesse サーバがエージェント ブラウザをリダイレクトする。
- IDS がエージェント ブラウザを SAML 要求付きでアイデンティティ プロバイダー（IDP）にリダイレクトする。

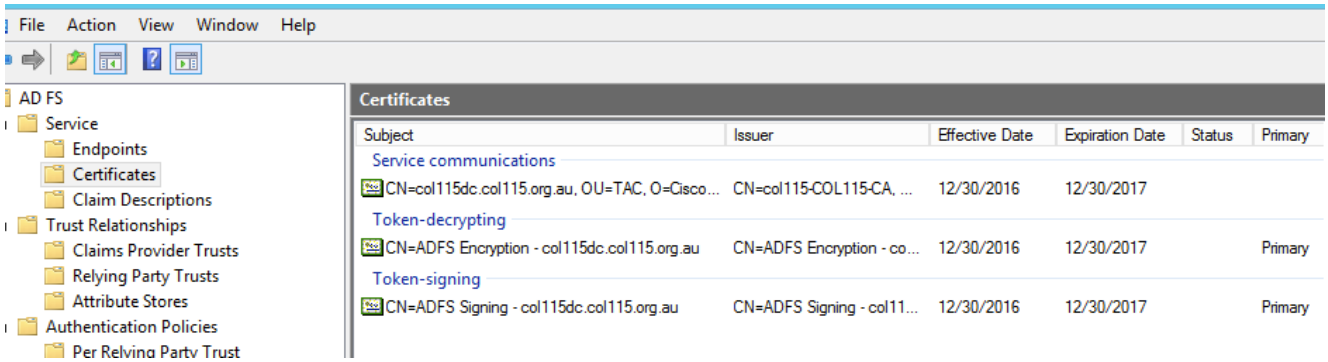
- IDP は SAML トークンを生成し、IDS サーバに渡す。
- トークンが生成されると、エージェントがアプリケーションを参照するたびにこの有効なトークンを使用してログインします。

パート B：IDP および IDS で使用する証明書



IDP 証明書

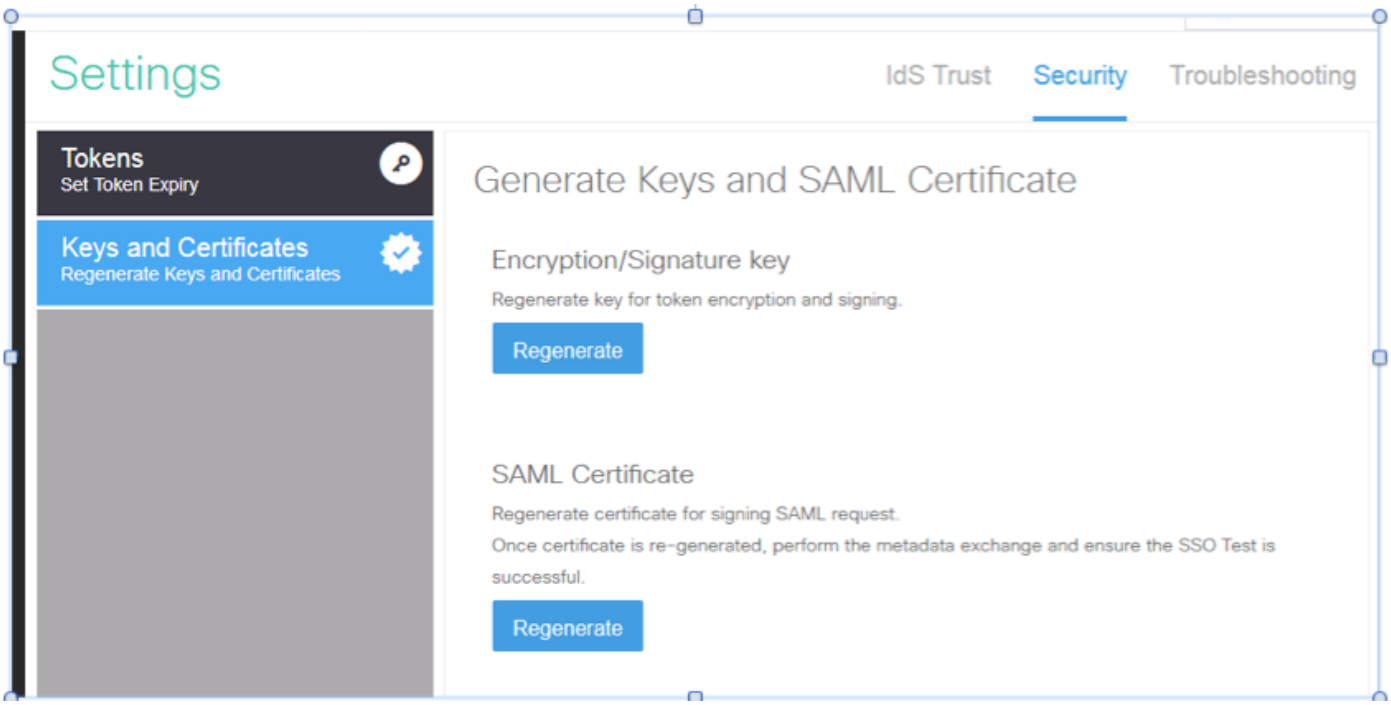
- SSL 証明書（SSO）
- トークン署名証明書
- トークン：復号

1. 

IDS 証明書

- SAML 証明書
- 署名キー

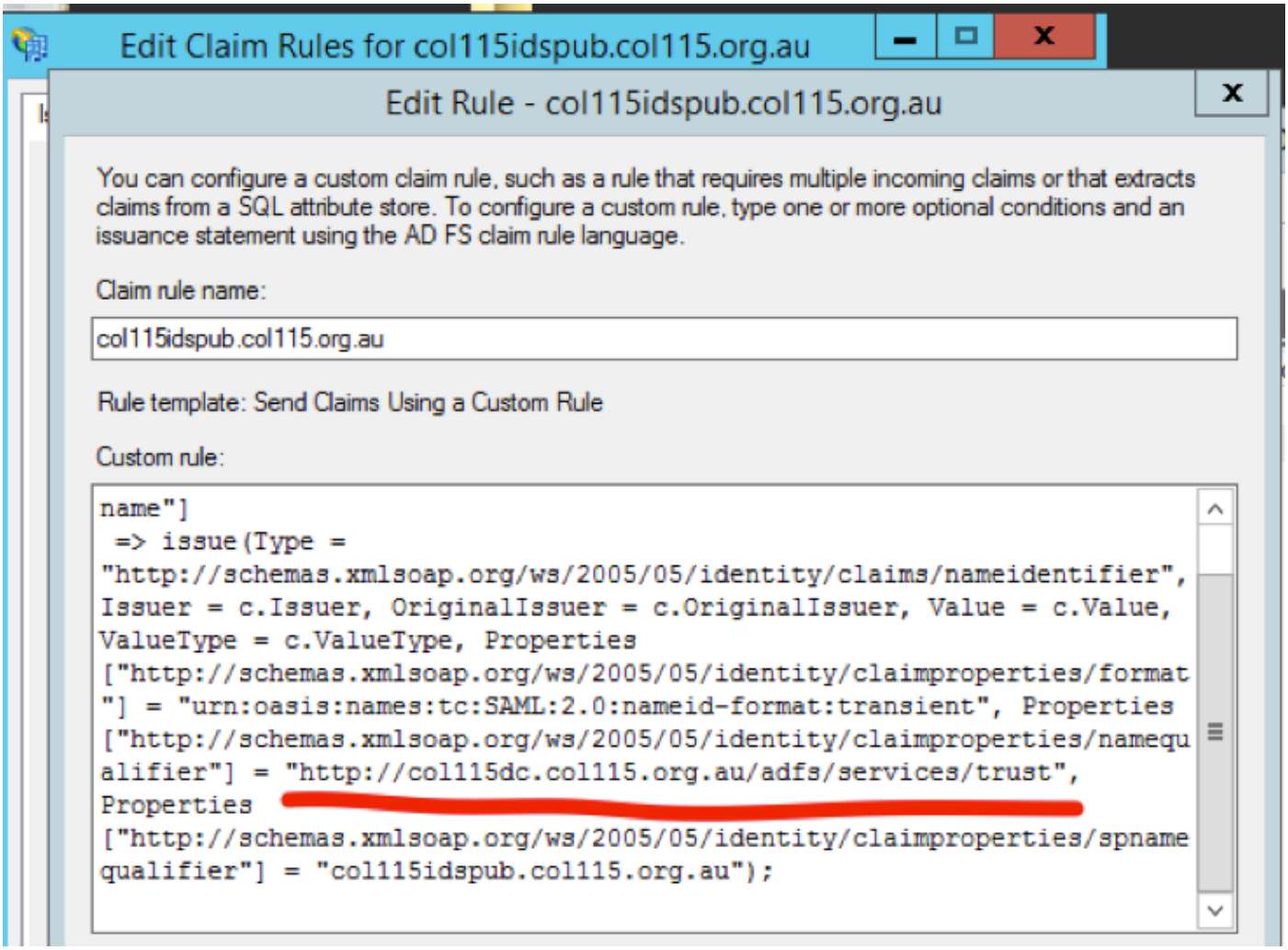
- 暗号キー



パート C：IDP 証明書の詳細と設定

SSL 証明書（SSO）

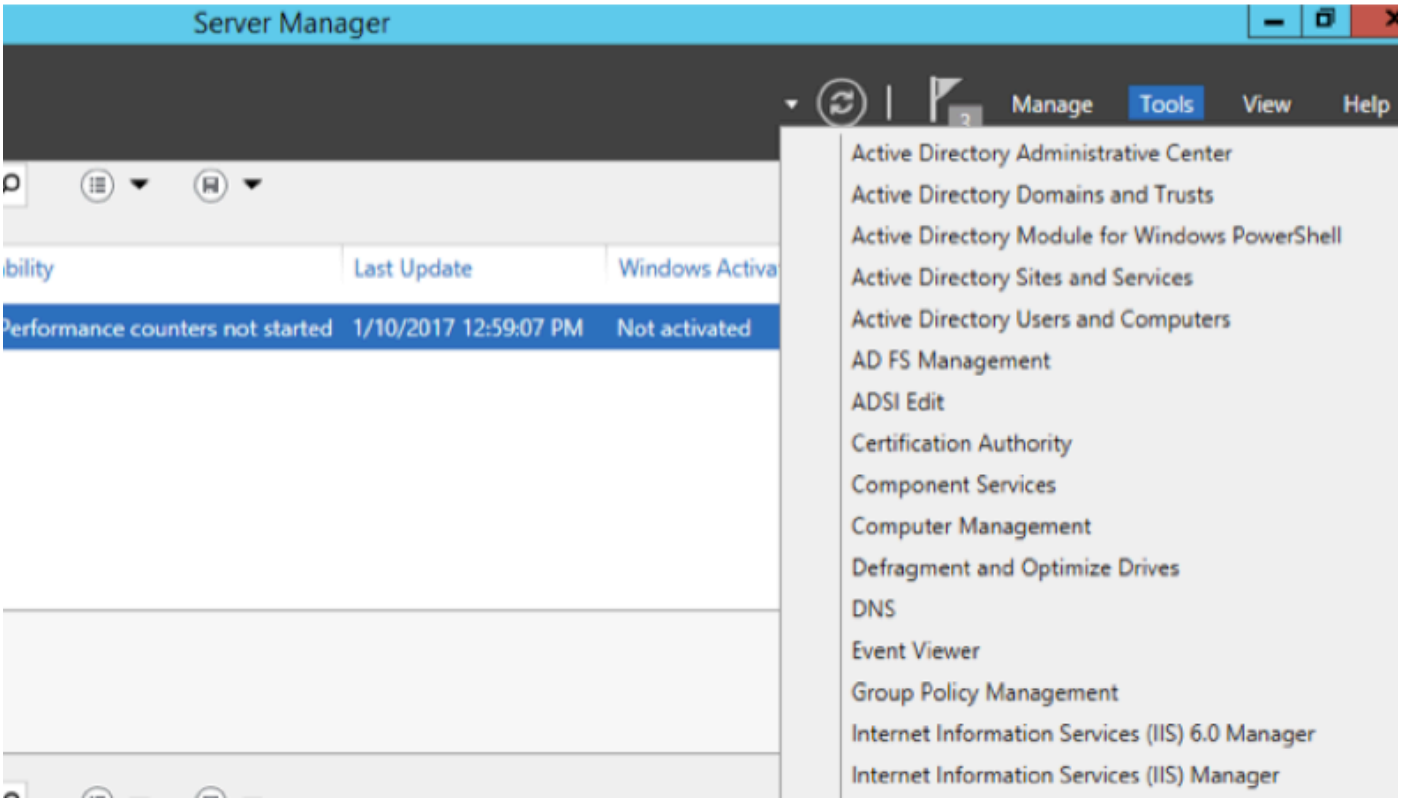
- この証明書は IDP とクライアント間で使用されます。 クライアント側で SSO 証明書を信頼する必要があります。
- SSL 証明書はクライアントと IDP サーバ間のセッションを暗号化するために使用します。 この証明書は ADFS ではなく、IIS 固有の証明書です。
- SSL 証明書の名前が ADFS 設定で使用した名前と一致している必要があります。

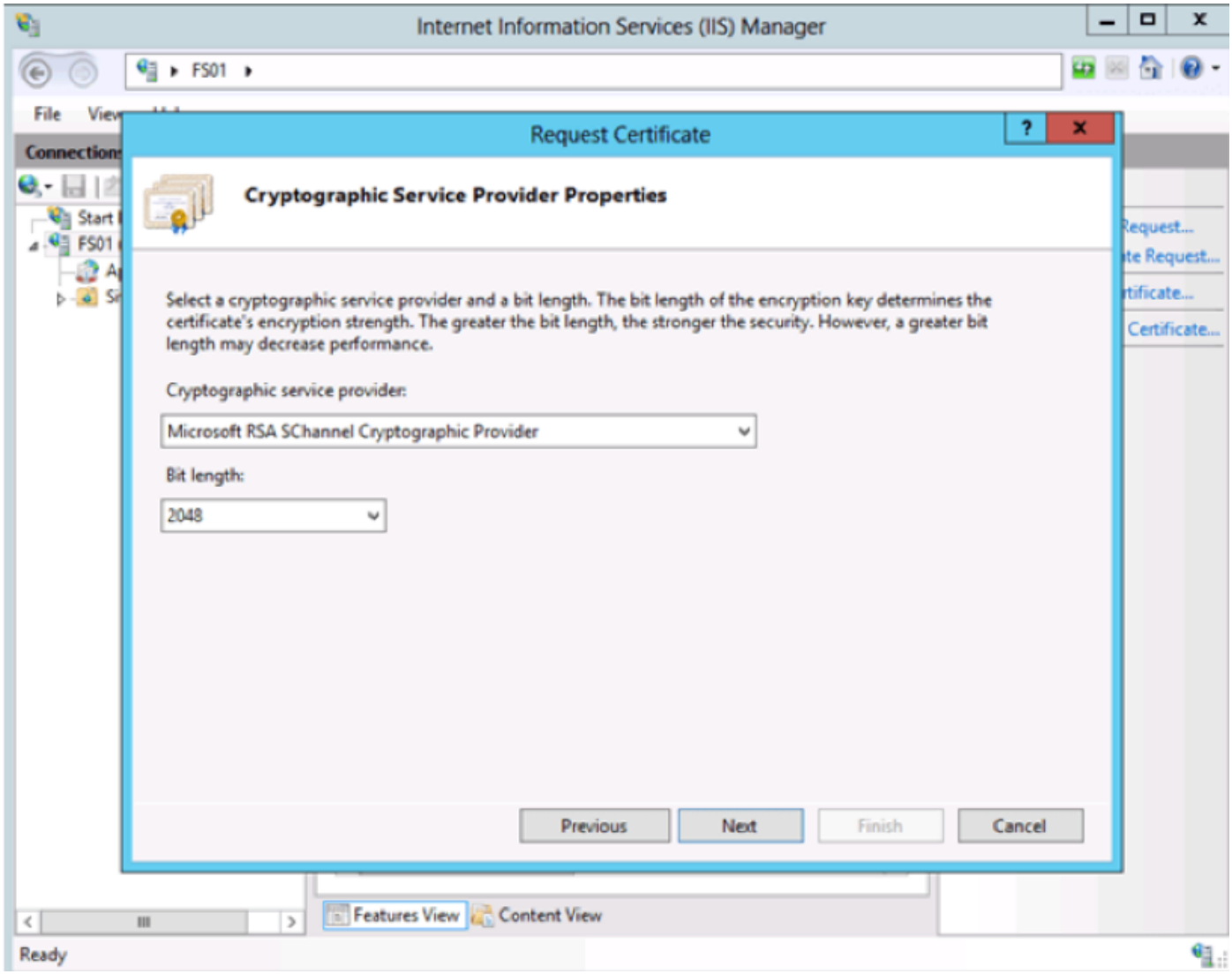


SSO のための SSL 証明書設定手順（内部 CA 署名済みのローカル ラボ）

ステップ 1：ADFS 用に証明書署名要求（CSR）を含む SSL 証明書を作成し、内部 CA で署名する。

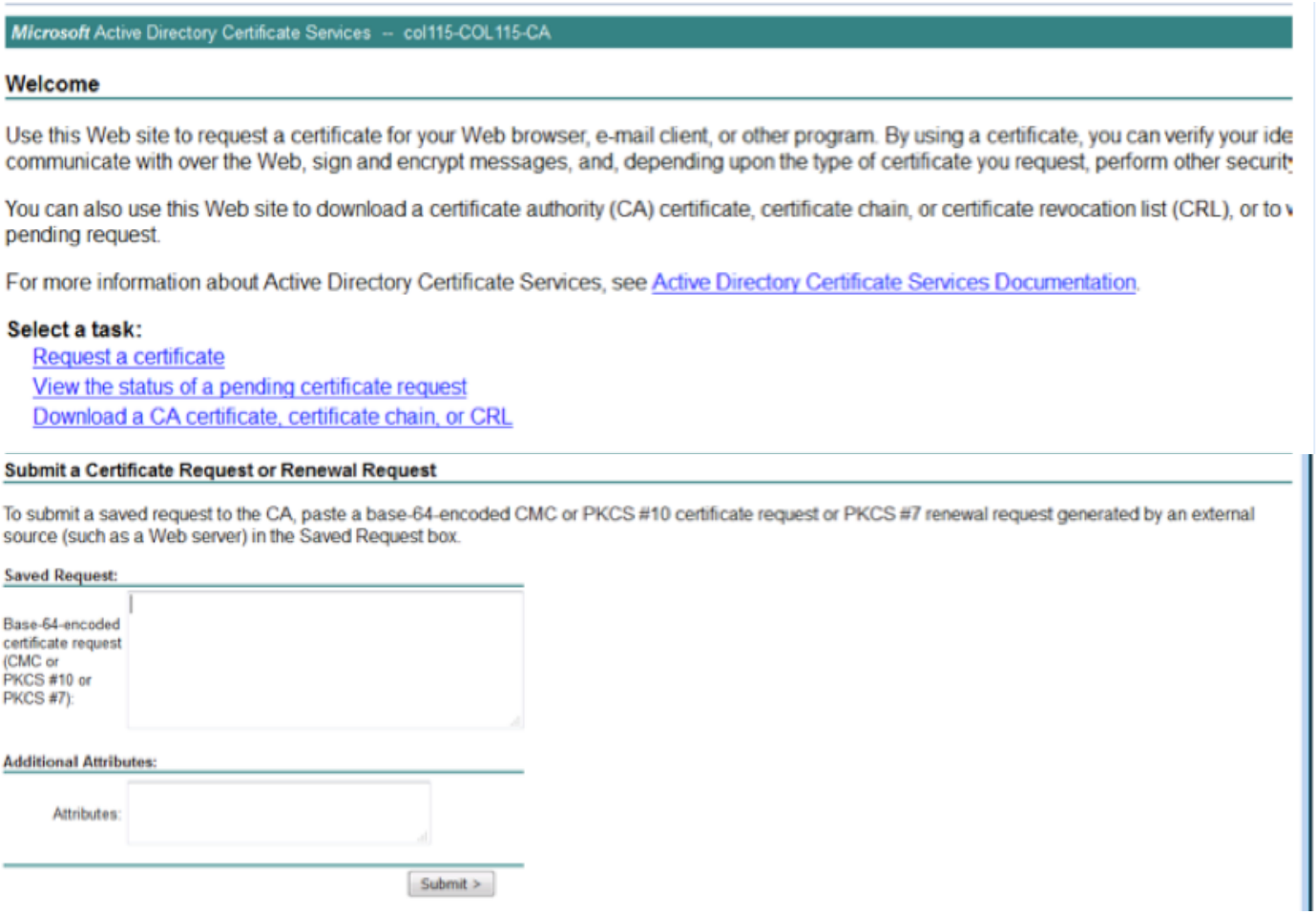
1. [Server Manager] を開きます。
2. [Tools] をクリックします。
3. [Internet Information Services (IIS) Manager] をクリックします。
4. ローカル サーバを選択します。
5. [Server Certificates] を選択します。
6. [Open Feature] をクリックしてアクション パネルを開きます。
7. [create certificate request] をクリックします。
8. [Cryptographic service provider] はデフォルトのままにしてください。
9. [Bit Length] を 2048 に変更します。
10. [Next] をクリックします。
11. 要求したファイルを保存する場所を選択します。
12. **[Finish] をクリックします。**





ステップ 2：ステップ 1 で生成した CSR に CA の署名を入れる。

1. [Open] で、作成した CSR に署名する CA サーバを開きます。**http: <CA Server ip address>/certsrv/**
2. [Request a certificate] をクリックします。
3. [Advanced certificate request] をクリックします。
4. CSR をコピーして [Based-64 encoded certificate request] に入れます。
5. [Submit] をクリックします。
6. 署名済みの証明書をダウンロードします。



ステップ 3：署名付き証明書を ADFS サーバに戻してインストールし、ADFS 機能を割り当てる。

1. 署名付き証明書を ADFS サーバに戻してインストールします。 インストールするには、[Server manager] > [Tools] > [Click Internet Information Services(IIS) Manager] >

[Local Server] > [Server Certificate] > [Open Feature] でアクション パネルを開きます。

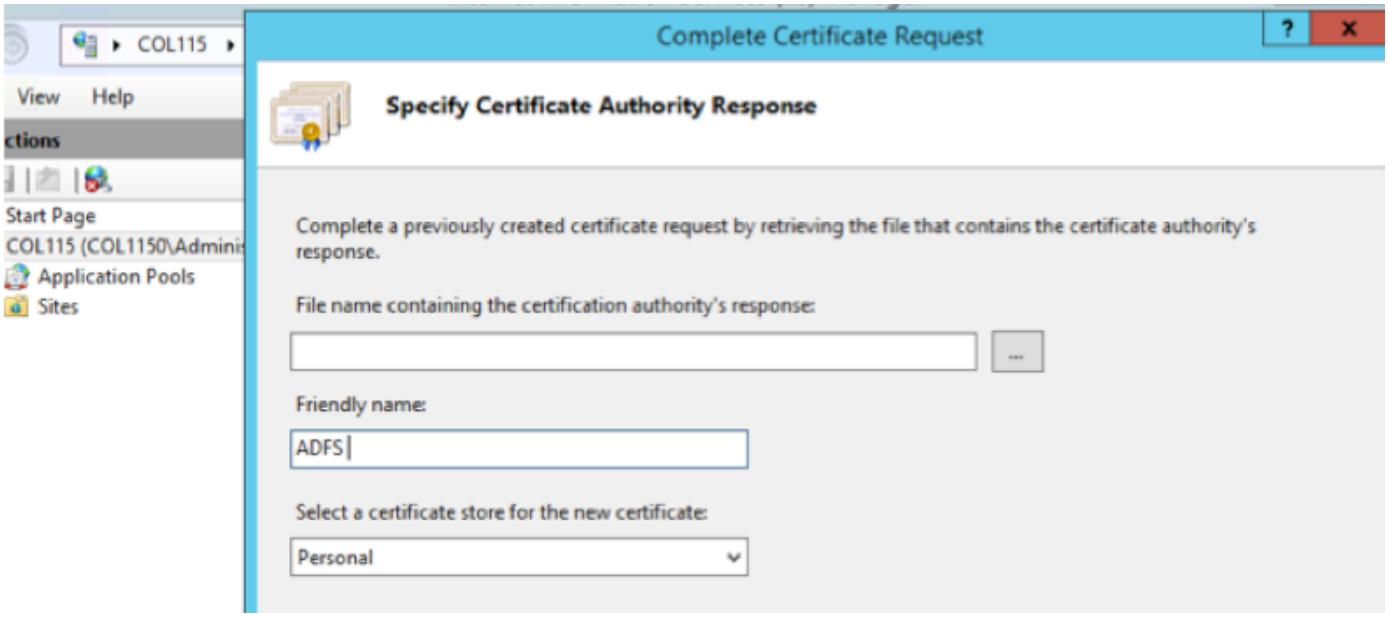
2. [Complete Certificate Request] をクリックします。

3. 署名が完了し、サード パーティ証明書プロバイダーからダウンロードした CSR ファイルのパスを選択します。

4. 証明書のフレンドリ名を入力します。

5. 証明書ストアには [Personal] を選択します。

6. [OK] をクリックします。



7. ここまでで、すべての証明書が追加されました。 次に、SSL 証明書を割り当てる必要があります。

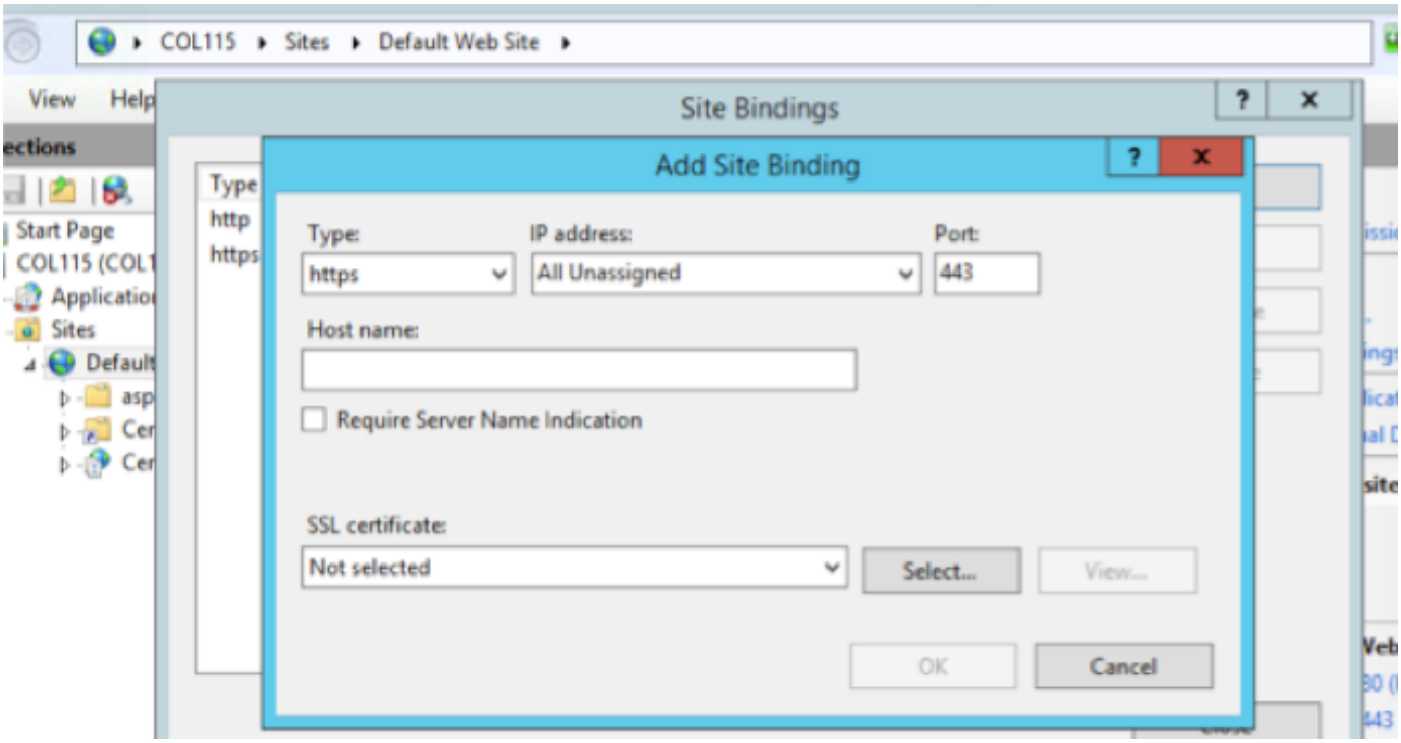
8. [Expand local server] > [Expand Sites] > [Select Default Web Site] > [Click Bindings] でアクション ペインを開きます。

9. [Add] をクリックします。

10. [type] を HTTPS に変更します。

11. ドロップダウン メニューから証明書を選択します。

12. [OK] をクリックします。



これで ADFS サーバの SSL 証明書の割り当ては完了です。

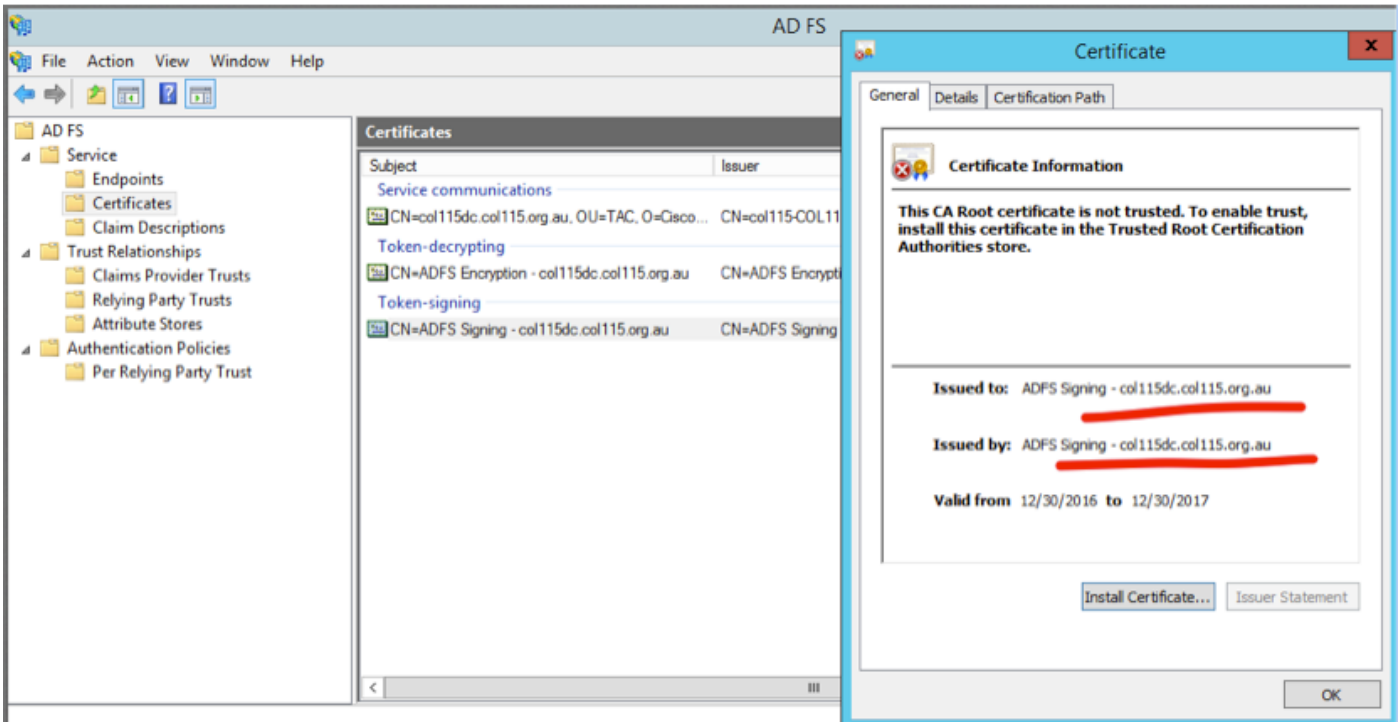
注: ADFS 機能のインストール中は、以前の SSL 証明書を使用する必要があります。

トークン署名証明書

ADFS ではトークン署名証明書用に自己署名証明書を生成します。 有効期間はデフォルトで 1 年間です。

IDP が生成した SAML トークンは ADFS 秘密キー（トークン署名証明書の非公開部分）で署名されます。 一方 IDS は ADFS 公開キーを使って検証します。 このことにより、署名済みトークンに変更が加えられないことを保証します。

ユーザが証明書利用者アプリケーション（Cisco IDS）にアクセスするたびにトークン署名証明署を使用します。

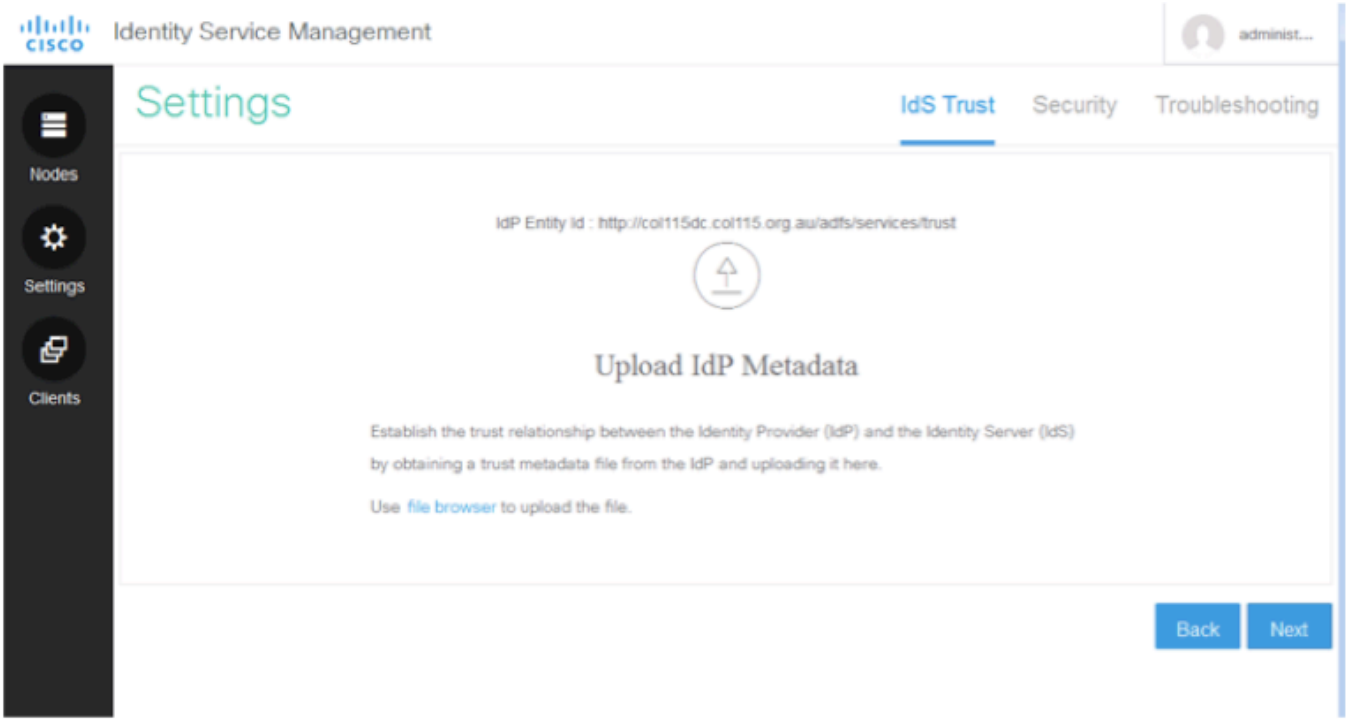


Cisco IDS サーバでのトークン署名証明書の公開キー取得方法

IDS サーバに ADFS メタデータをアップロードし、IDS サーバに ADFS の公開キーを渡す方法を使います。 この方法で IDS は ADFS サーバの公開キーを取得します。

ADFS から IDP メタデータをダウンロードする必要があります。 IDP メタデータのダウンロードについては、**https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml** を参照してください。

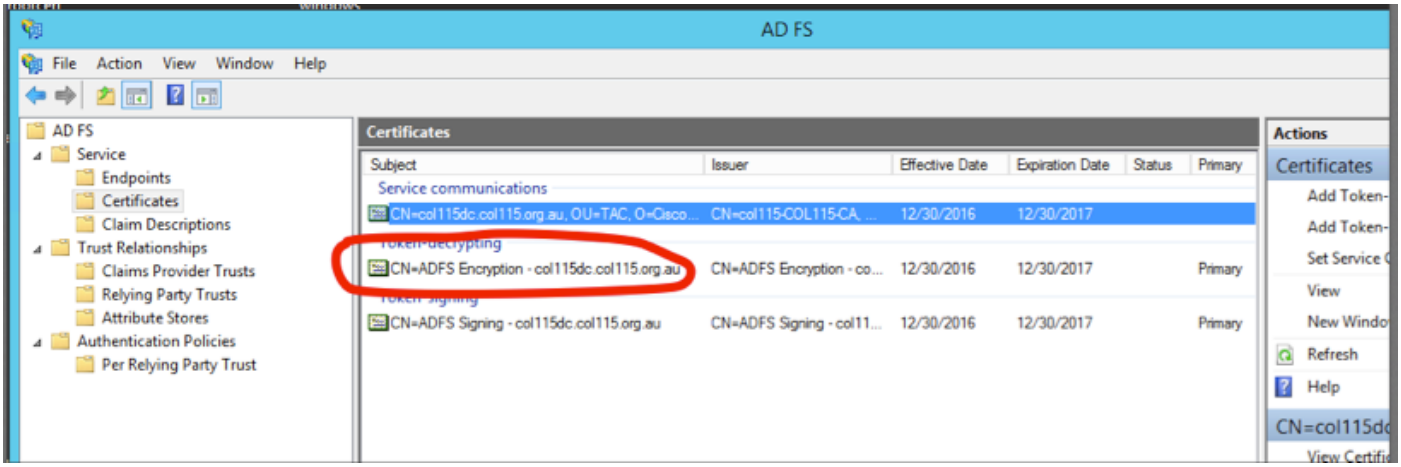
ADFS からメタデータは



IDS に ADFS メタデータをアップロードします

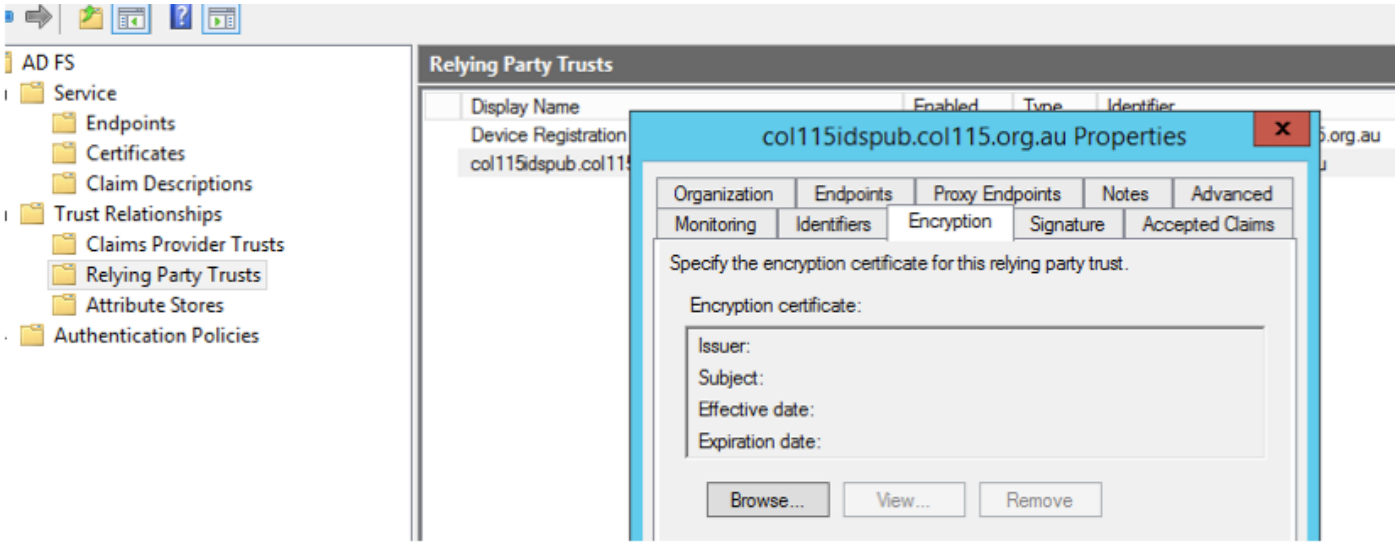
トークン復号

この証明書は ADFS サーバが自動的に生成します（自己署名付き）。 トークンの暗号化が必要な場合、ADFS は IDS 公開キーを使って復号します。 ただし、[ADFS token-dcrypting] の表示は、トークンが暗号化されていることを意味しているわけではありません。



ある特定の証明書利用者アプリケーションでトークンの暗号化が有効になっているかどうかを確認するには、そのアプリケーションの暗号化タブの確認が必要です。

この画面では、トークン暗号化は無効になっています。



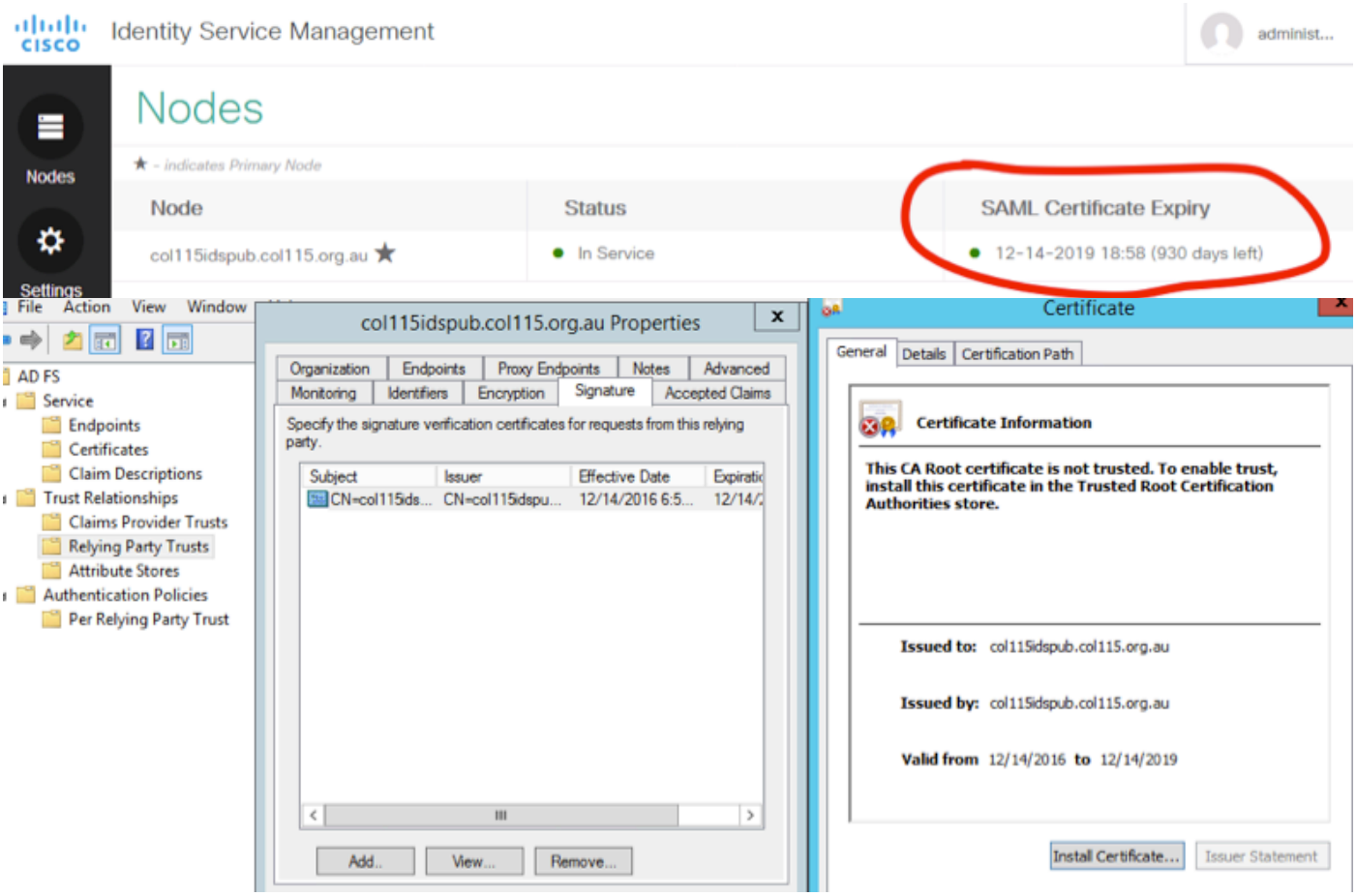
暗号化が有効でない状態

パート D：Cisco IDS 側の証明書

- SAML 証明書
- 暗号キー
- 署名キー

SAML 証明書

この証明書は IDS サーバが生成します（自己署名付き）。 有効期間はデフォルトで 3 年間です。

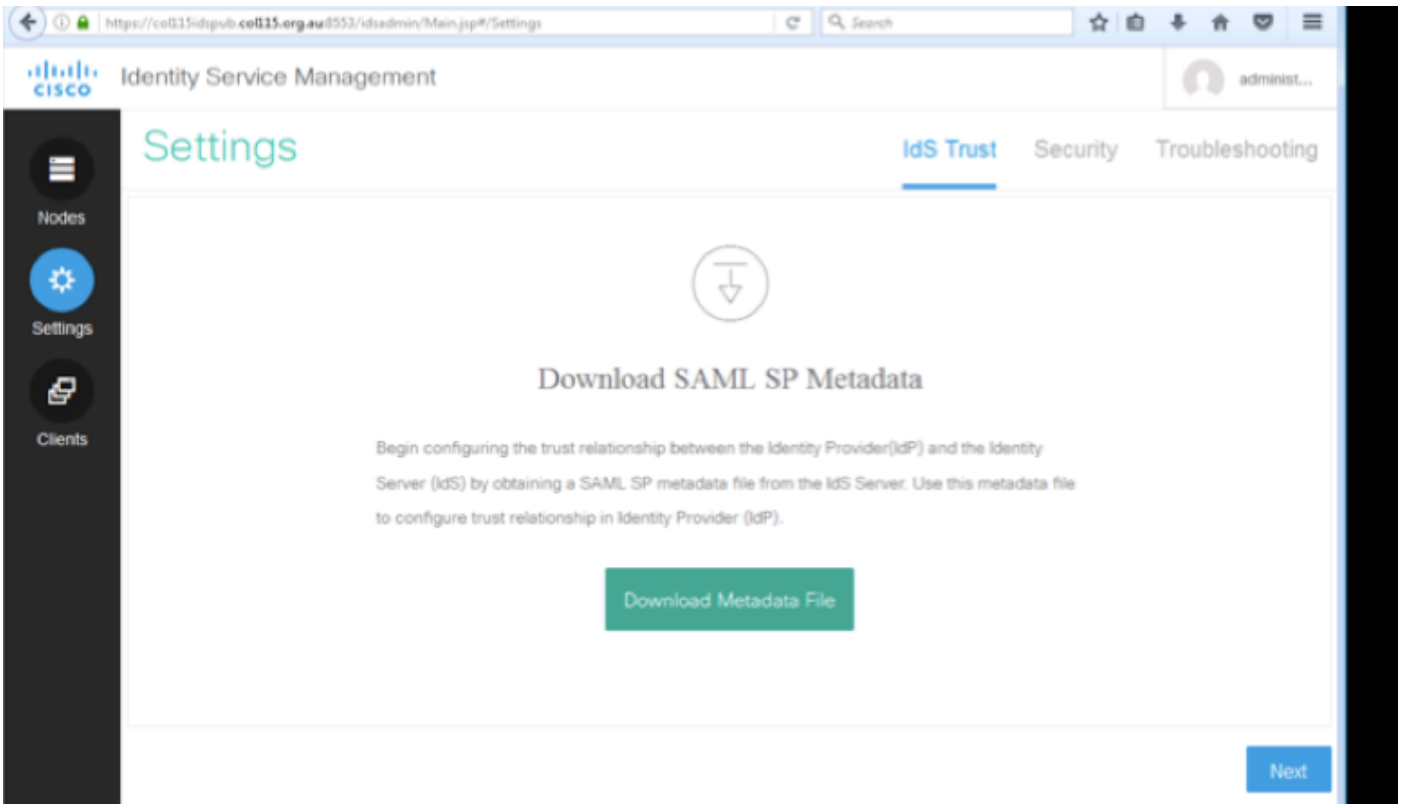


この証明書は SAML 要求の署名、IDP（ADFS）への送信に使用されます。 この公開キーは IDS メタデータ内にあり、ADFS サーバにインポートする必要があります。

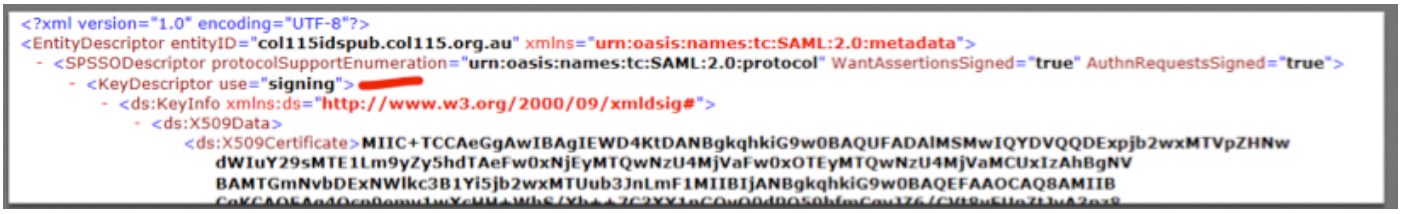
1. IDS サーバから SAML SP メタデータをダウンロードします。

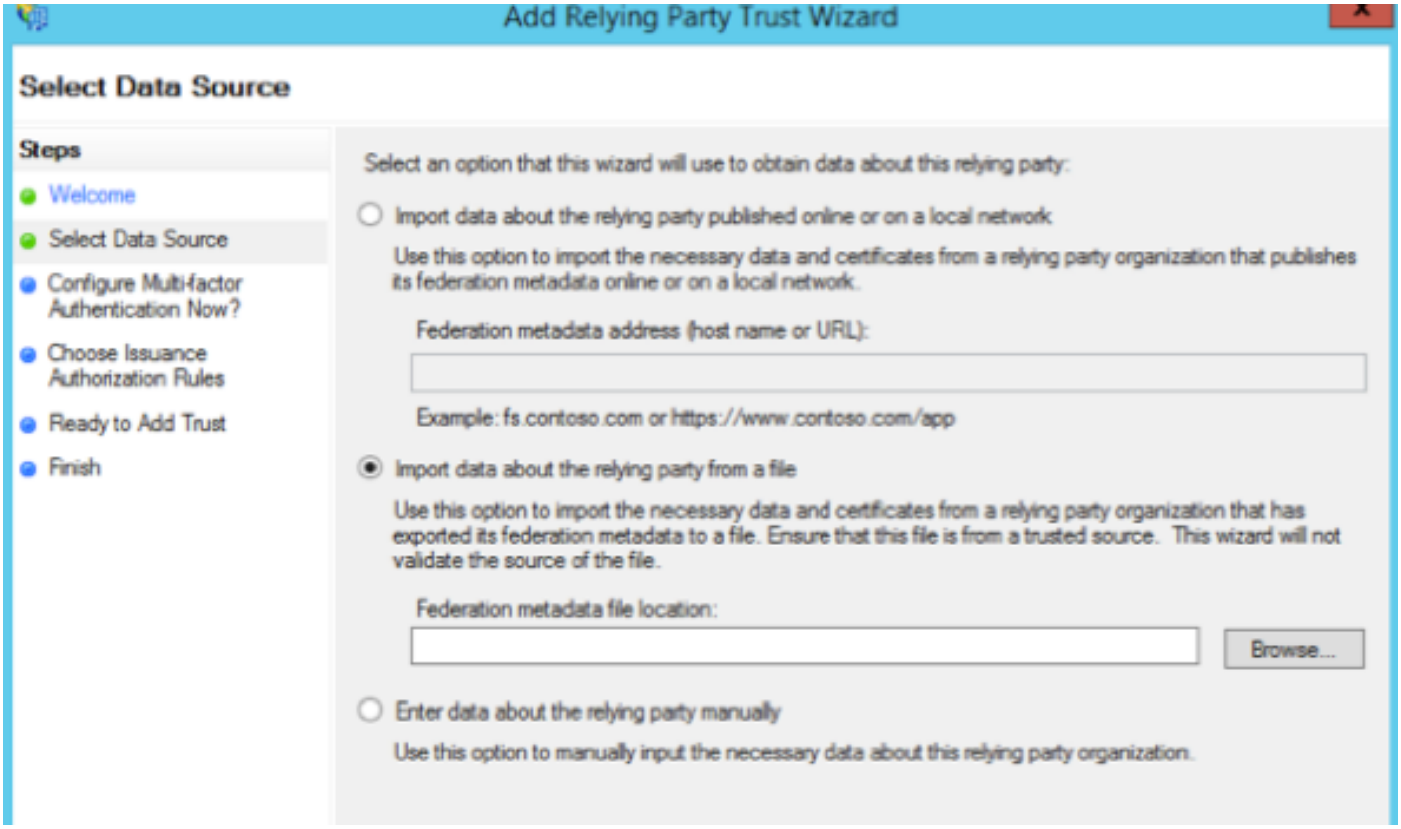
2. **https://<ids server FQDN>:8553/idsadmin/** にアクセスします。

3. 設定を選択し、SAML SP メタデータをダウンロードして保存します。

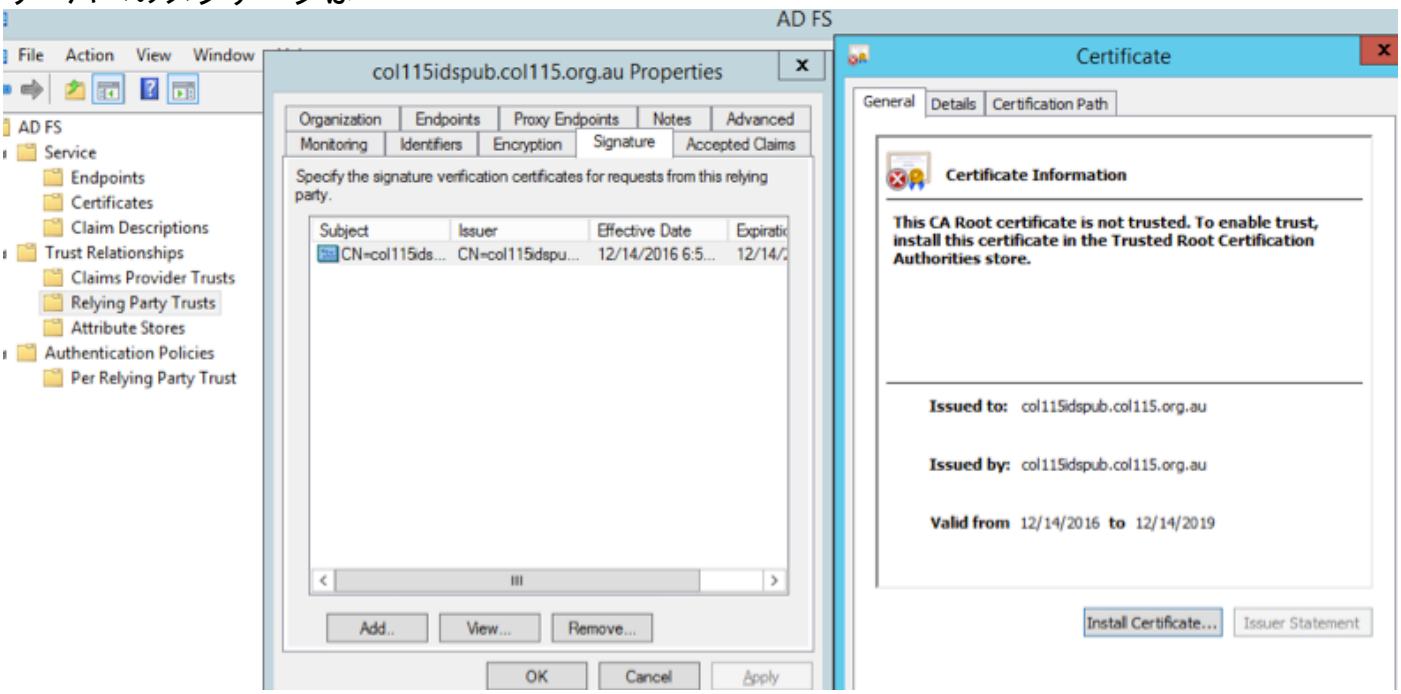


IDS サーバインポートからの
ADFS





サーバへのメタデータは

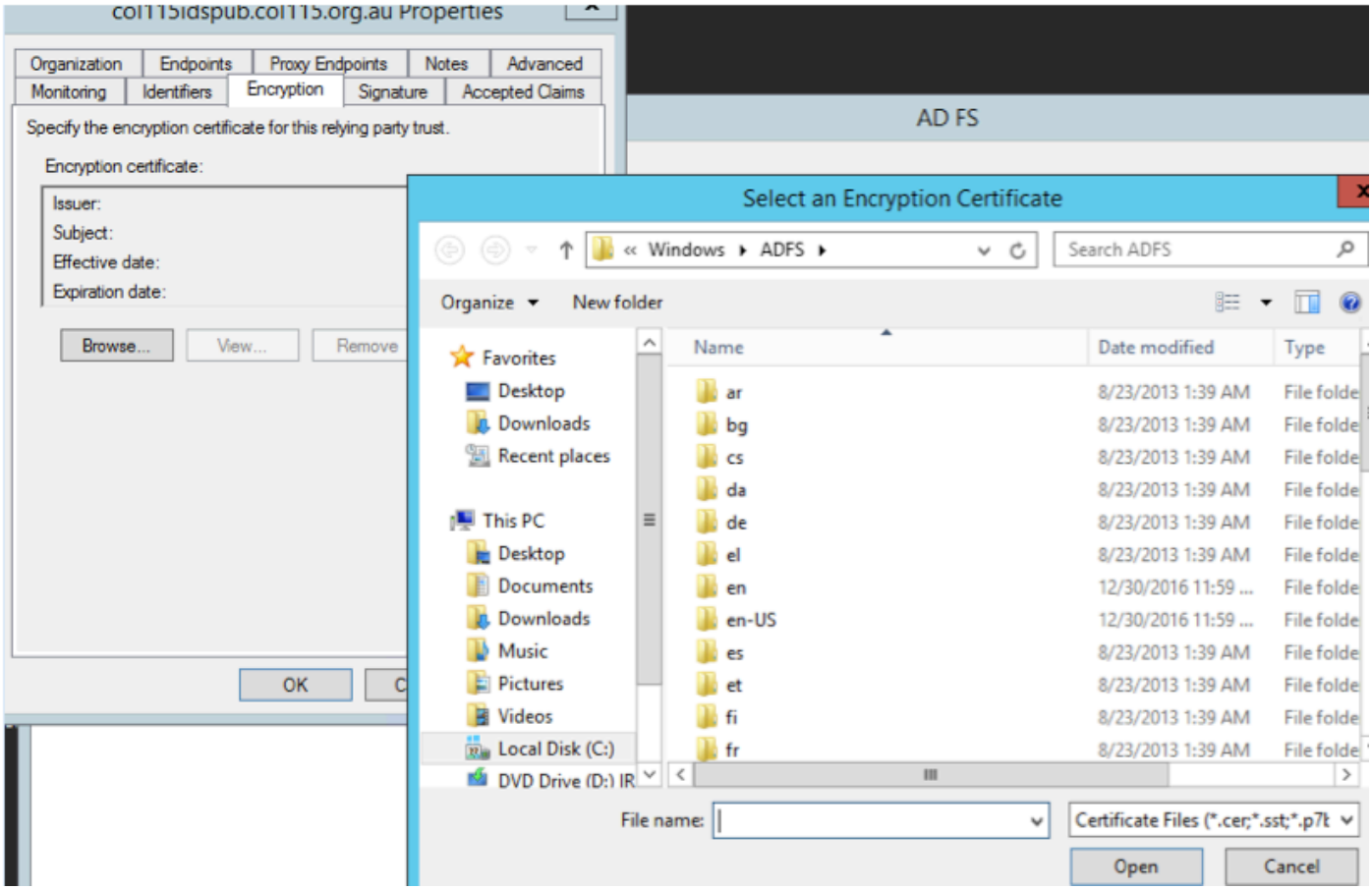


ADFS 側から確認します

IDS は SAML 要求の署名に使用した SAML 証明書を再生成すると、メタデータ交換を行います。

暗号キーと署名キー

暗号化はデフォルトでは無効になっています。 暗号化を有効にした場合、ADFS にアップロードする必要があります。



参考資料：

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