ISE SCEP 統合用の HTTPS サポートの設定

目次

概要

このドキュメントでは、Identity Services Engine（ISE）に Secure Certificate Enrollment Protocol（SCEP）を統合するために Hypertext Transfer Protocol Secure（HTTPS）サポートを設定するのに必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Microsoft Internet Information Services（IIS）Web サーバに関する基本的な知識
- ISE での SCEP および証明書の設定経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ISE リリース 1.1.x
- Windows Server 2008 R2 Enterprise（KB2483564 および KB2633200 のホットフィックスをインストール済み）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

Microsoft 証明書サービスに関する情報は、Cisco Bring Your Own Device（BYOD）専用の指針として記載しているものです。 Microsoft 認証局、ネットワーク デバイス登録サービス（NDES）、および SCEP に関するサーバ設定については、正式な正しい情報源として、Microsoft の TechNet を参照してください。

背景説明

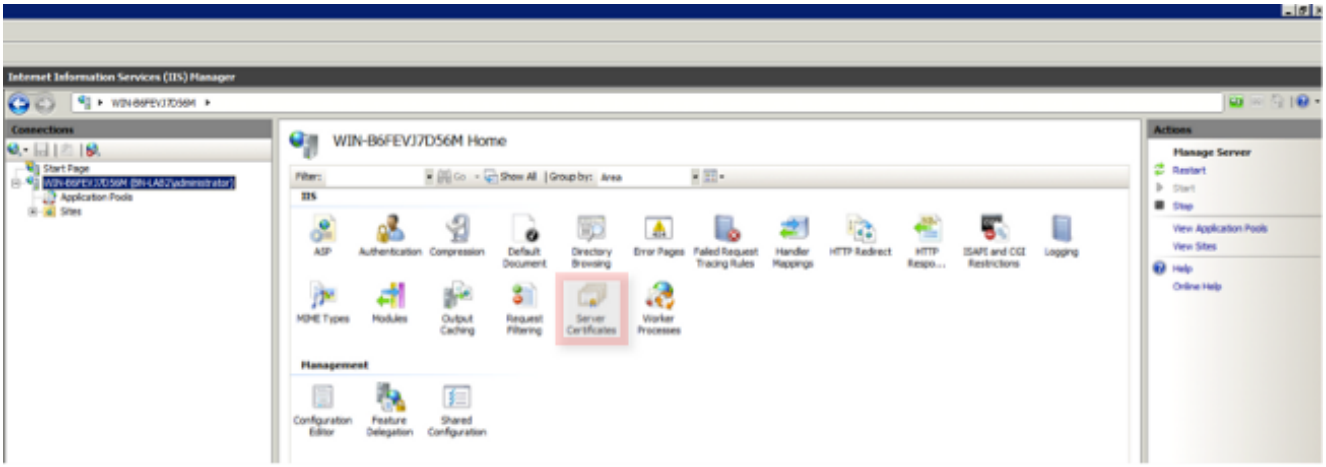
BYOD を導入する上でコア コンポーネントの 1 つとなるのは、NDES ロールがインストールされた Microsoft 2008 R2 Enterprise サーバです。 このサーバは、Active Directory（AD）フォレストのメンバーです。 NDES の初期インストール時に、Microsoft の IIS Web サーバが自動的にインストールされ、SCEP の HTTP 終端をサポートするように設定されます。 BYOD 導入に際して、顧客が ISE と NDES 間の通信に対するセキュリティを強化するために、HTTPS を使用することを要望する場合があります。 以下の手順で、SCEP Web サイトのセキュア ソケット レイヤ（SSL）証明書を要求してインストールするために必要なステップを詳しく説明します。

設定

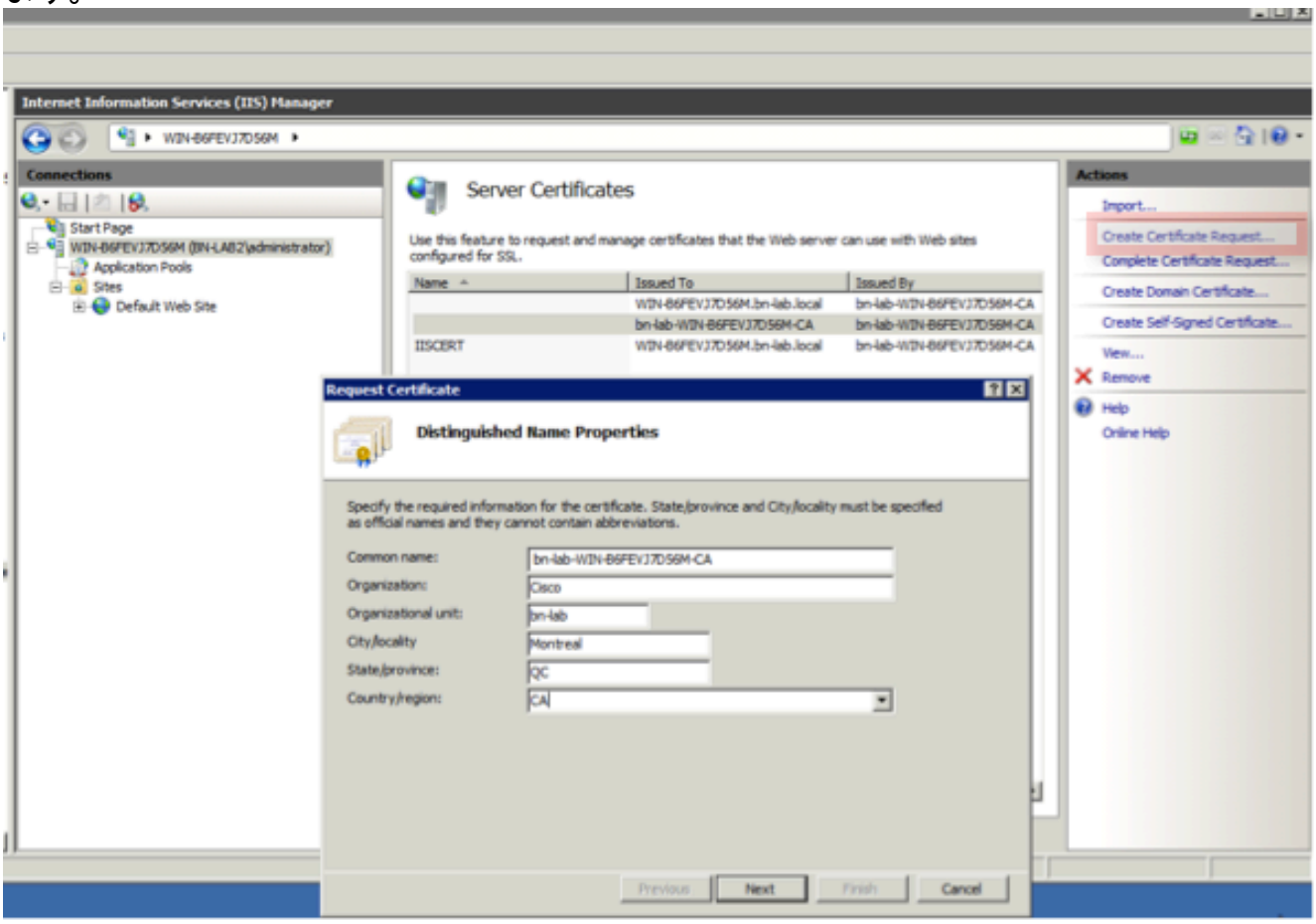
NDES サーバ証明書の設定

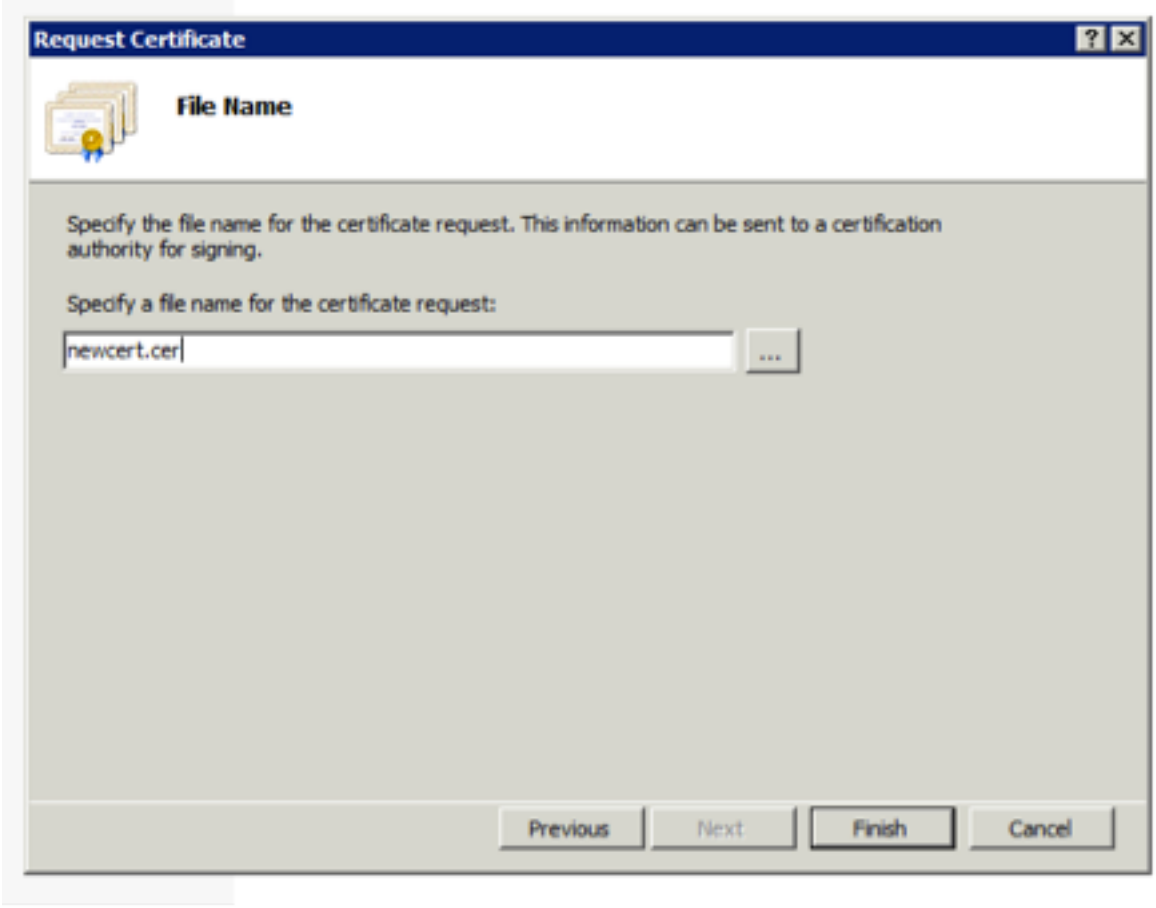
> **注:** IIS の新しい証明書を設定する必要があります（IIS が Verisign などのサードパーティ PKI と統合されている場合、または認証局（CA）と NDES サーバのロールが別のサーバに分かれている場合にのみ必要です）。 インストール時に、NDES のロールが現在の Microsoft CA サーバに設定されている場合、IIS は CA のセットアップ中に作成されたサーバ ID 証明書を使用します。 このようなスタンドアロン設定の場合は、このドキュメントの「**NDES サーバ IIS バインディングの設定**」セクションに直接進んでください。

1. コンソールまたは RDP を使用して NDES サーバに接続します。
2. [スタート（Start）] -> [管理ツール（Administrative Tools）] -> [インターネットインフォメーションサービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] をクリックします。
3. IIS サーバ名を強調表示してから、[サーバー証明書（Server Certificates）] アイコンをクリックします。

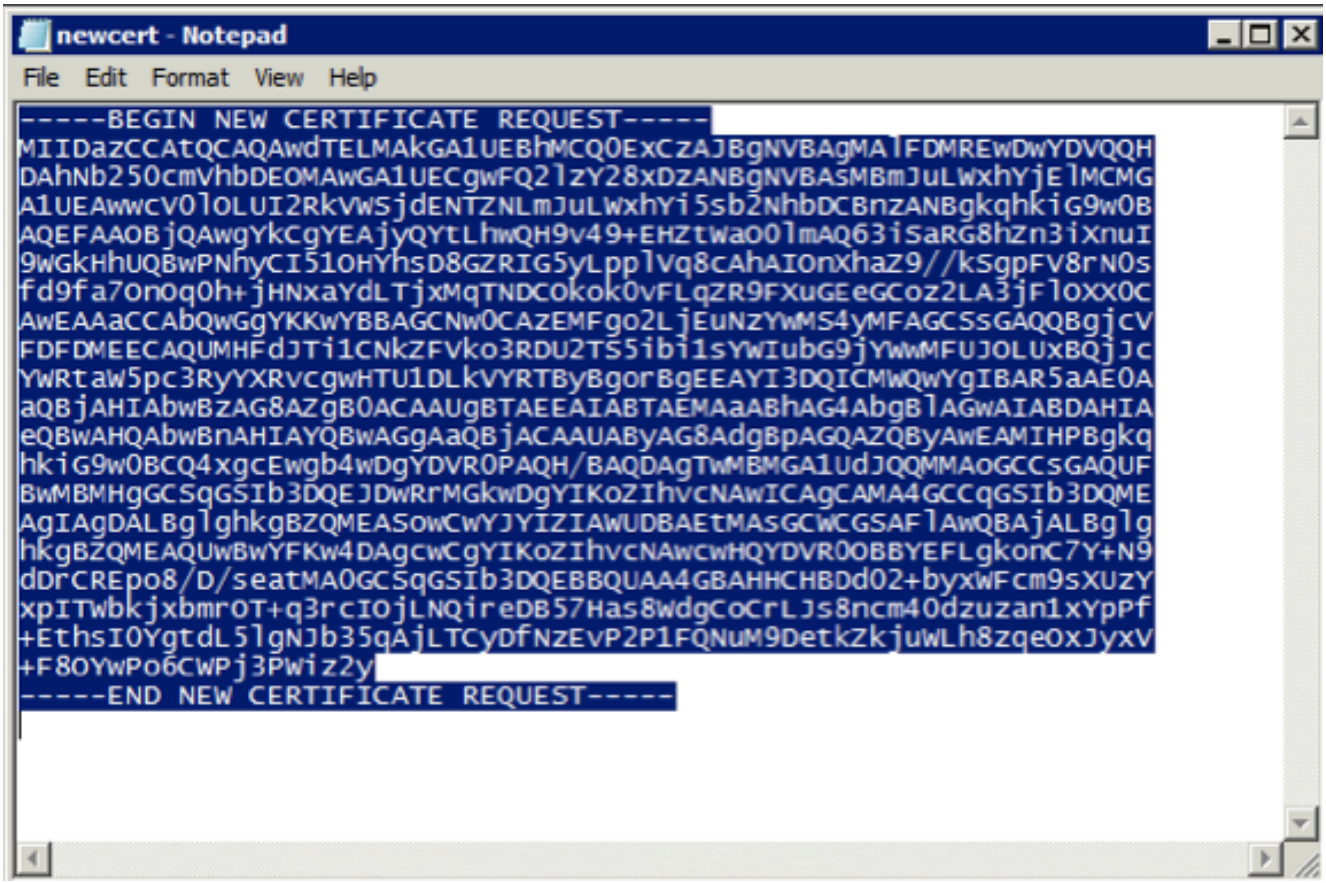


4. [証明書要求の作成（Create Certificate Request）] をクリックし、フィールドに値を入力します。

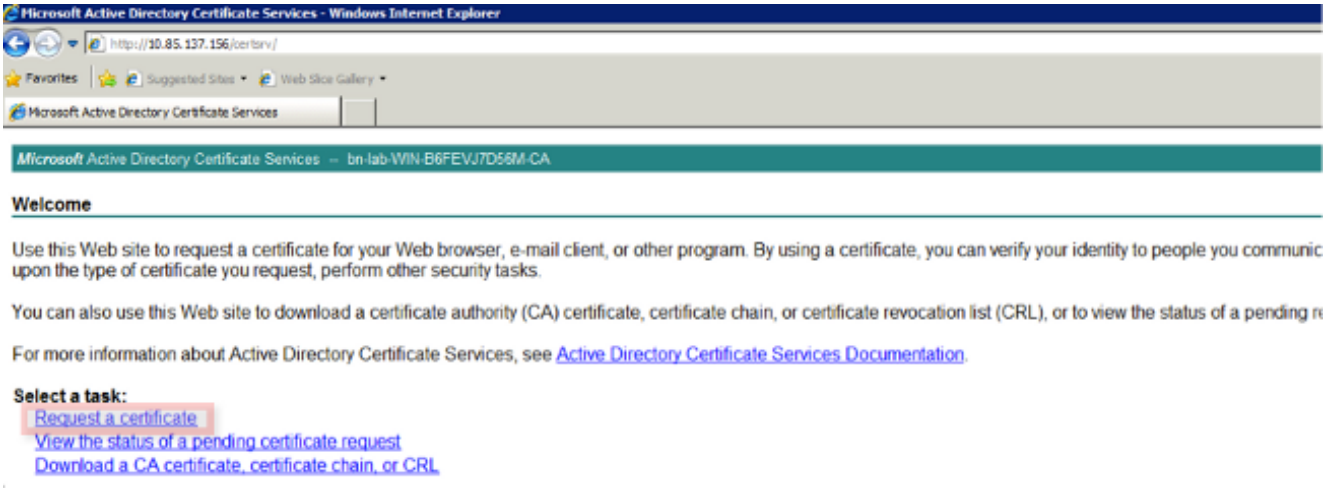




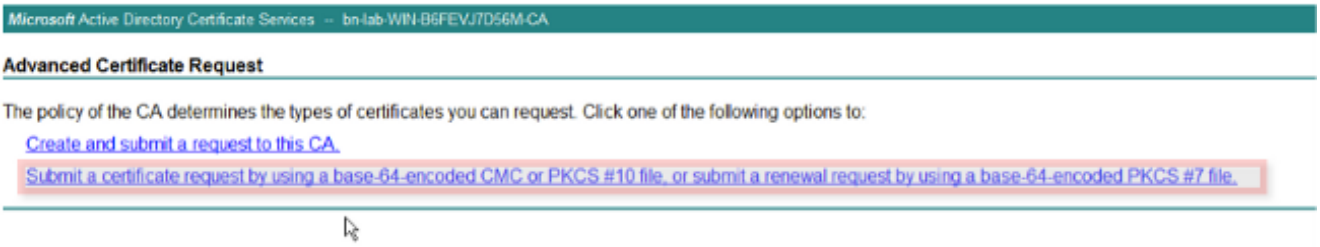
5. 前のステップで作成した .cer ファイルをテキスト エディタで開き、ファイルの内容をクリップボードにコピーします。



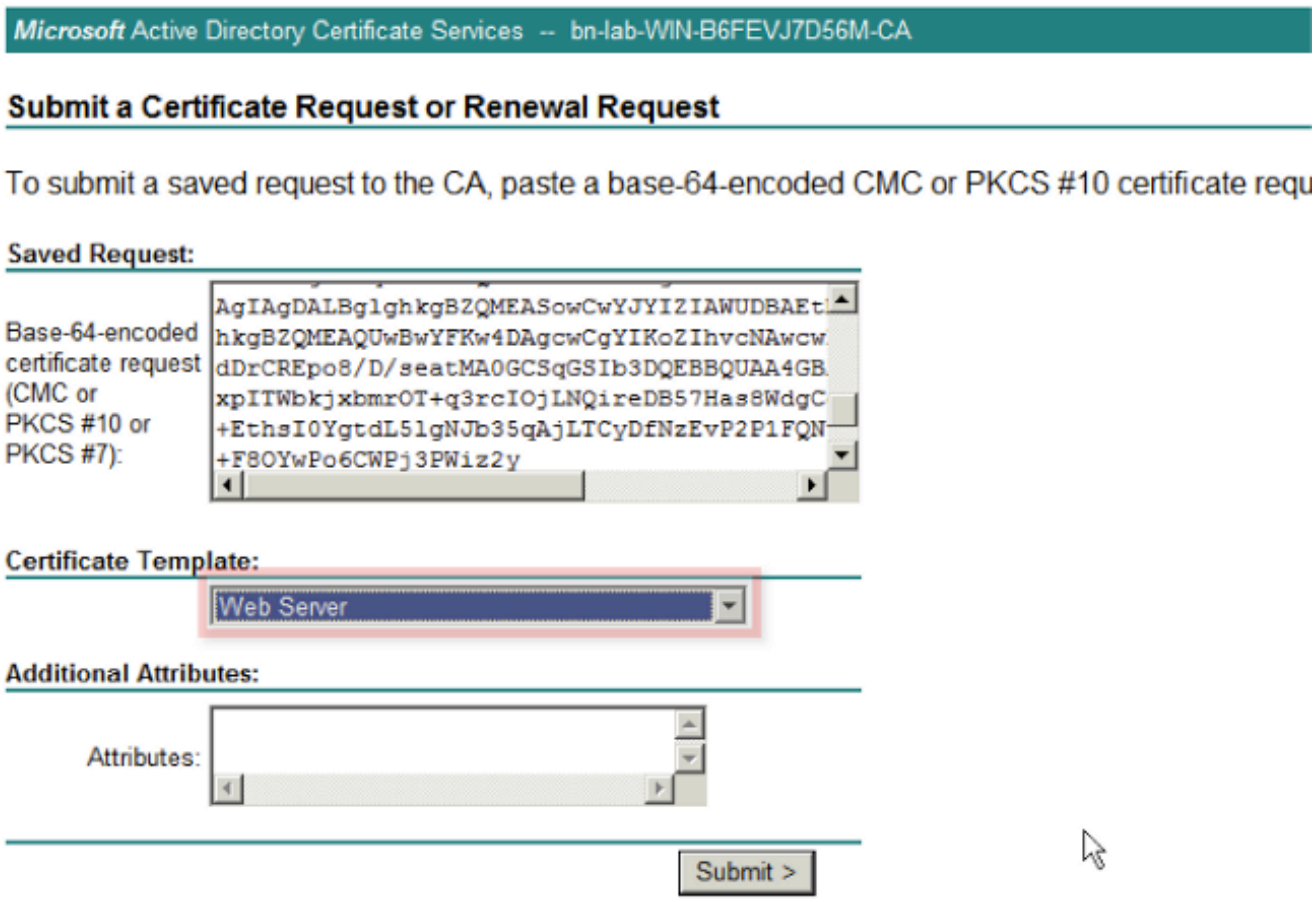
6. Microsoft CA Web Enrollment Web サイトにアクセスし、[証明書の要求（Request a Certificate）] をクリックします。URL の例： http://yourCAIP/certsrv



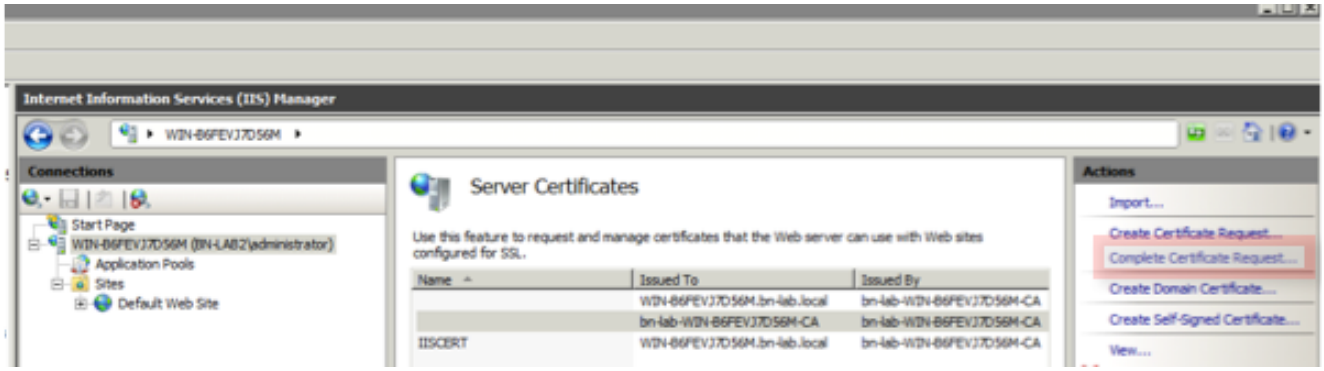
7. [...を使用して証明書の要求を送信する（Click Submit a certificate request by using....）] をクリックします。 クリップボードの証明書の内容を貼り付け、[Webサーバー（Web Server）] テンプレートを選択します。



8. [送信（Submit）] をクリックしてから、証明書ファイルをデスクトップに保存します。

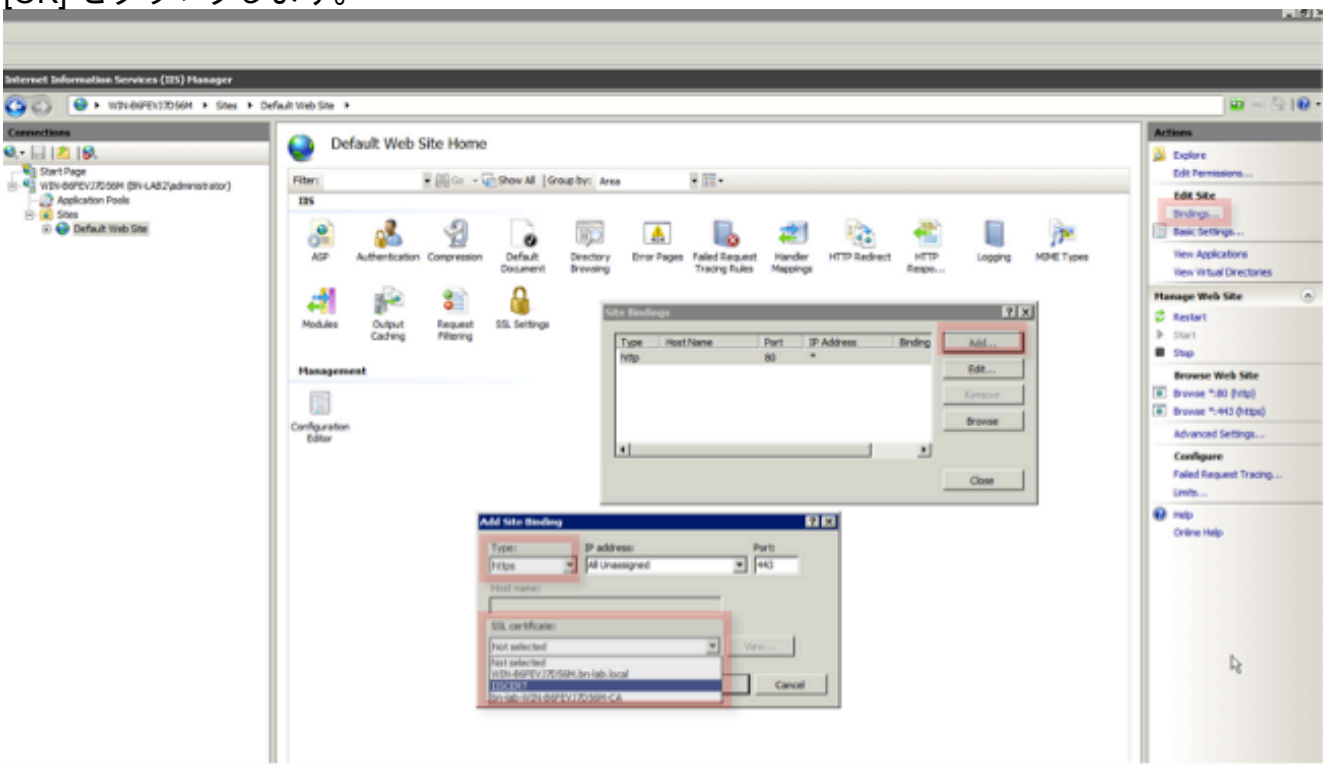


9. NDES サーバに戻り、IS マネージャ ユーティリティを開きます。 サーバ名をクリックし、新しく作成したサーバ証明書をインポートするために [証明書要求の完了（Complete Certificate Request）] をクリックします。



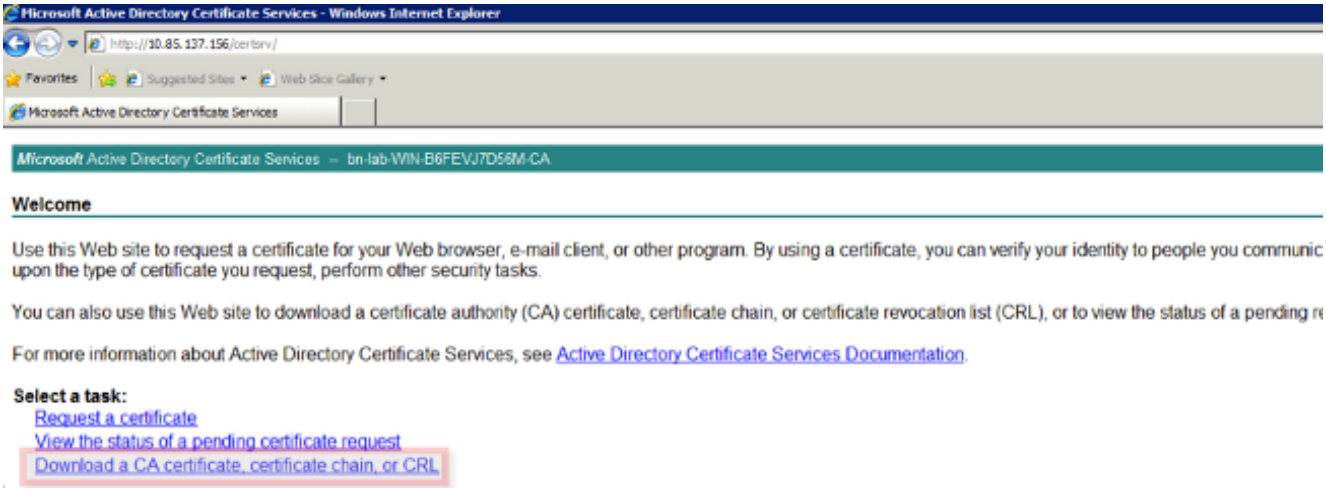
NDES サーバ IIS バインディングの設定

1. **サーバ名**を展開し、[サイト（Sites）] を展開して [既定のWebサイト（Default Web Site）] をクリックします。
2. 右上隅の [バインド（Bindings）] をクリックします。
3. [追加（Add）] をクリックし、[タイプ（Type）] を HTTPS に変更して、ドロップダウン リストから証明書を選択します。
4. [OK] をクリックします。

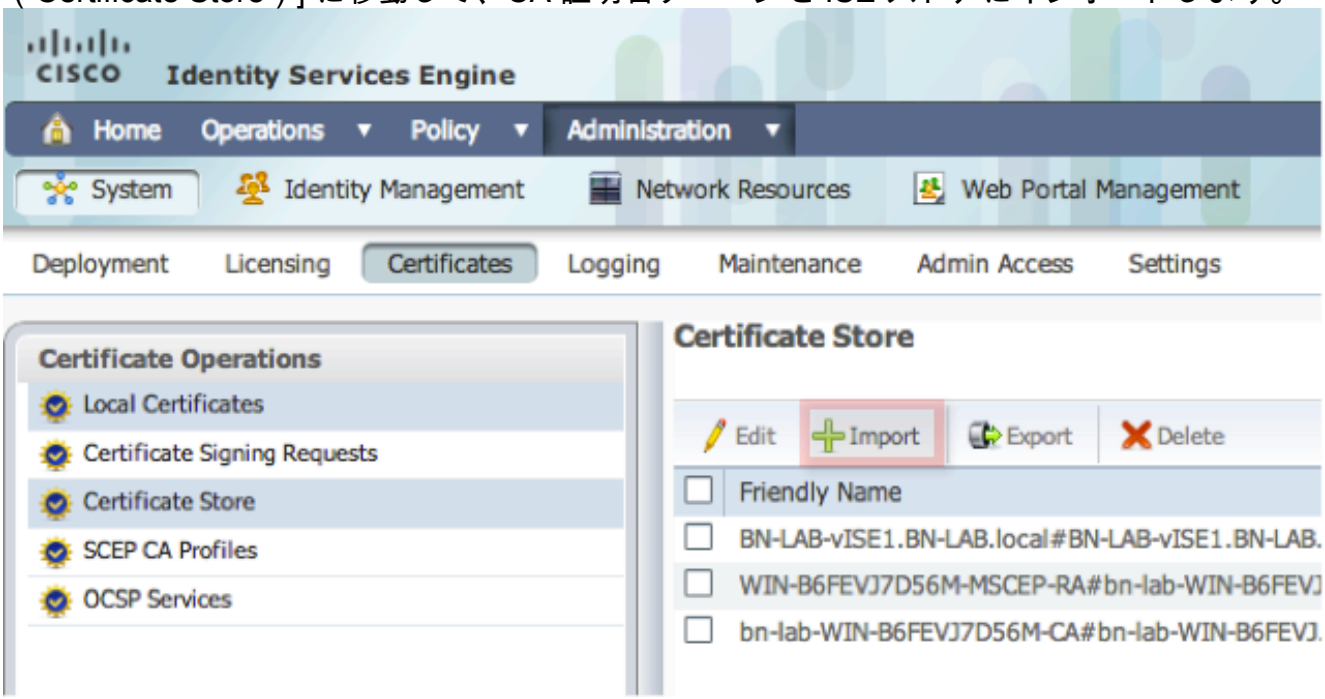


ISE サーバの設定

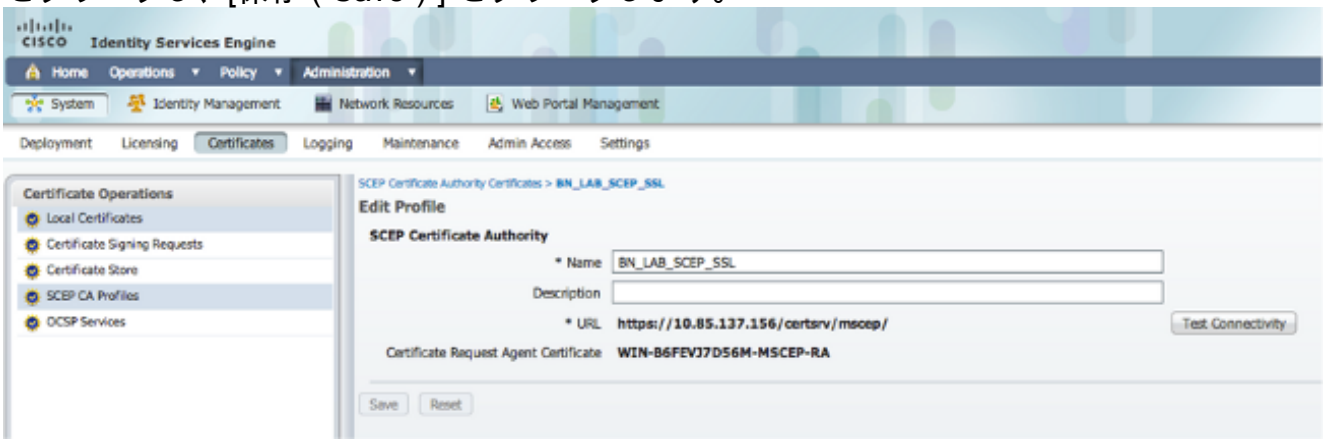
1. CA サーバの Web Enrollment インターフェイスに接続し、CA 証明書チェーンをダウンロードします。



2. ISE GUI で [管理（Administration）] -> [証明書（Certificates）] -> [証明書ストア（Certificate Store）] に移動して、CA 証明書チェーンを ISE ストアにインポートします。



3. [管理（Administration）] -> [証明書（Certificates）] -> [SCEP CAプロファイル（SCEP CA Profiles）] に移動し、HTTPS の URL を設定します。 [接続のテスト（Test Connectivity）] をクリックし、[保存（Save）] をクリックします。



確認

ここでは、設定が正常に動作していることを確認します。

- [管理（Administration）] -> [証明書（Certificates）] -> [証明書ストア（Certificate Store）] に移動し、CA 証明書チェーンと NDES サーバ登録認証局（RA ）証明書が存在することを確認します。
- Wireshark または TCP ダンプを使用して、ISE 管理ノードと NDES サーバとの間の初期 SSL 交換をモニタします。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- デバッグ地点および取得地点と、エンドポイントである ISE、NDES、および CA 間のパスを識別するのに役立つように、BYOD ネットワーク トポロジを論理的な中継点に分割します。
- TCP 443 が、ISE と NDES サーバの間の双方向で許可されていることを確認します。
- CA および NDES サーバ アプリケーション ログに登録エラーがないか監視し、Google または TechNet を使用してこれらのエラーを調査します。
- ISE PSN で TCP ダンプ ユーティリティを使用し、NDES サーバとの間でやりとりするトラフィックを監視します。 これは [Operations] > [Diagnostic Tools] > [General Tools] にあります。
- ISE PSN とやりとりする SCEP トラフィックを取得するために、NDES サーバに Wireshark をインストールするか、中継スイッチ上で SPAN を使用します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

関連情報

- **BYOD のための SCEP サポートの設定**
- **テクニカルサポートとドキュメント - Cisco Systems**