CUCMおよびAD FS 2.0によるシングルサインオンの設定

内容

はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)およびActive Directoryフェデレーションサービスでシングルサインオン(SSO)を設定する方法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。

- Cisco Unified Communications Manager（CUCM）
- Active Directoryフェデレーションサービス(AD FS)に関する基礎知識

ラボ環境で SSO を有効にするには、次の構成が必要です:

- AD FSがインストールされているWindows Server。
- LDAP 同期が設定された CUCM
- 標準の CCM スーパー ユーザ ロールが選択されたエンド ユーザ

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いています。

- AD FS 2.0 がインストール済みの Windows Server
- CUCM 10.5.2

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

AD FS 2.0とWindows Server 2008 R2を併用する手順について説明します。これらの手順は、Windows Server 2016上のAD FS 3.0でも機能します。

Windows Server 上での AD FS 2.0 のダウンロードとインストール

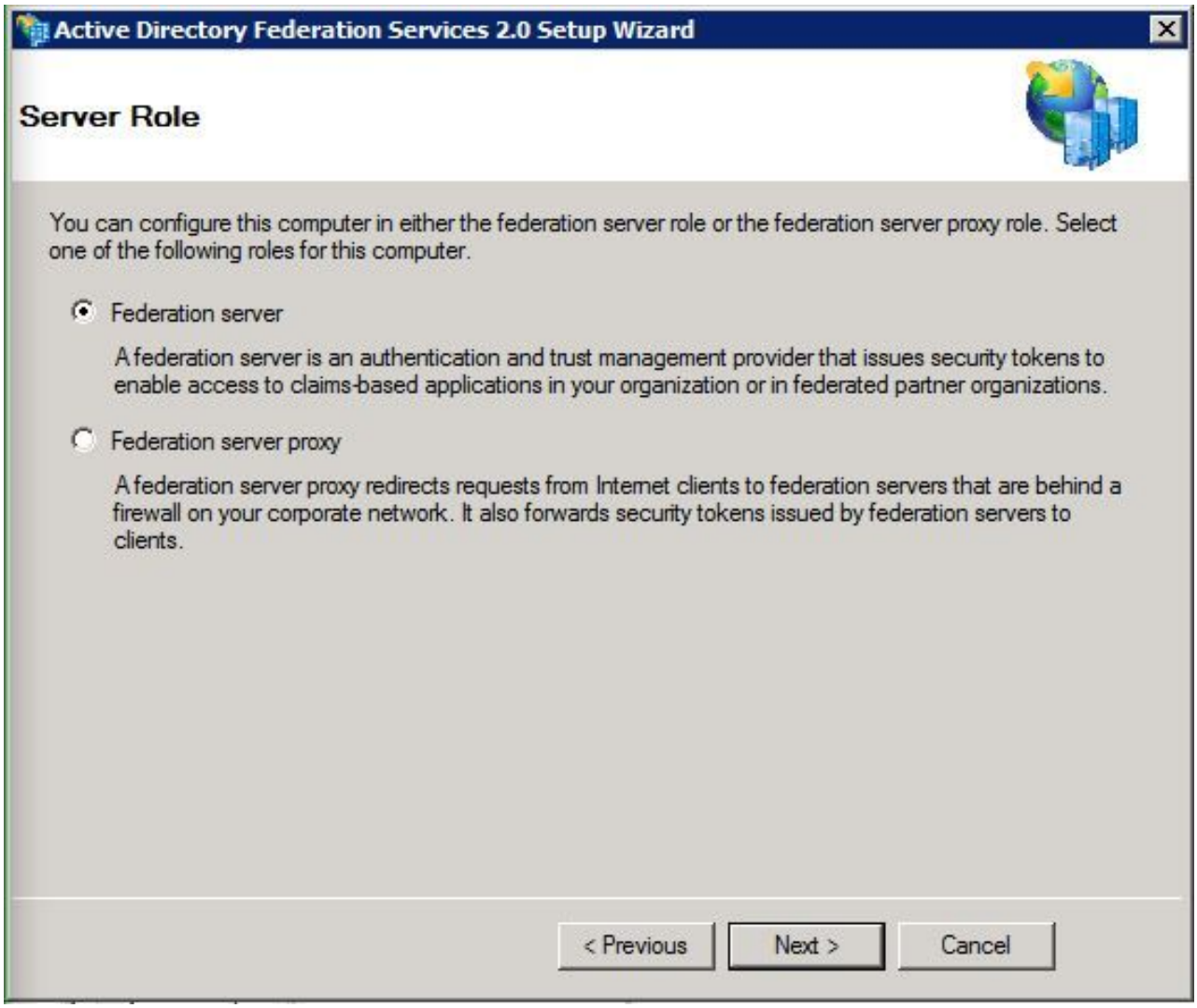
ステップ 1：Download AD FS 2.0に移動します。

ステップ 2：Windows Serverに基づいて適切なダウンロードを選択していることを確認します。

ステップ 3：ダウンロードしたファイルをWindows Serverに移動します。

ステップ 4：インストールを続行します。

ステップ 5：プロンプトが表示されたら、Federation Serverを選択します。



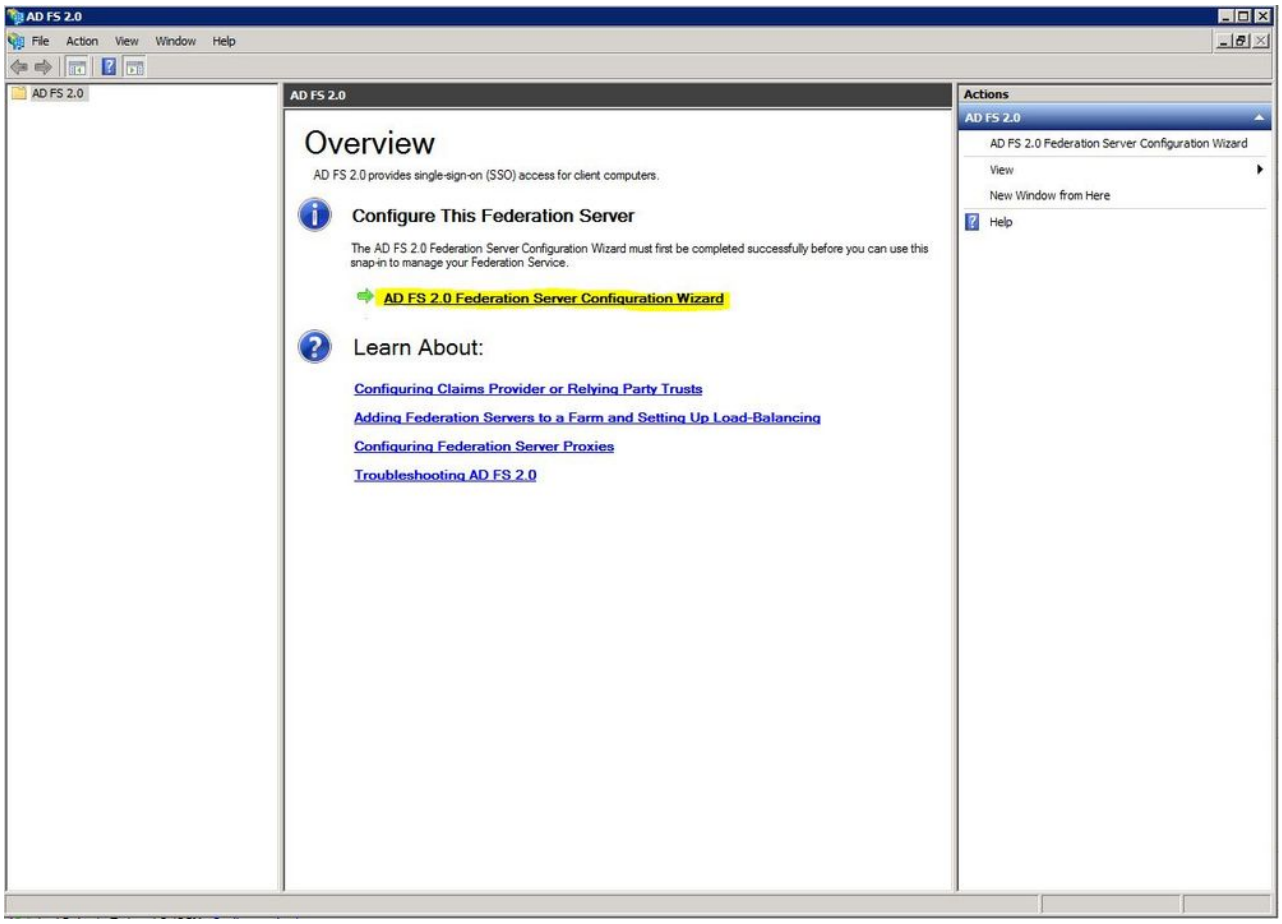
ステップ6：一部の依存関係が自動的にインストールされます。インストールが完了したら、Finishをクリックします。

これで AD FS 2.0 がサーバにインストールされました。一部の設定を追加する必要があります。

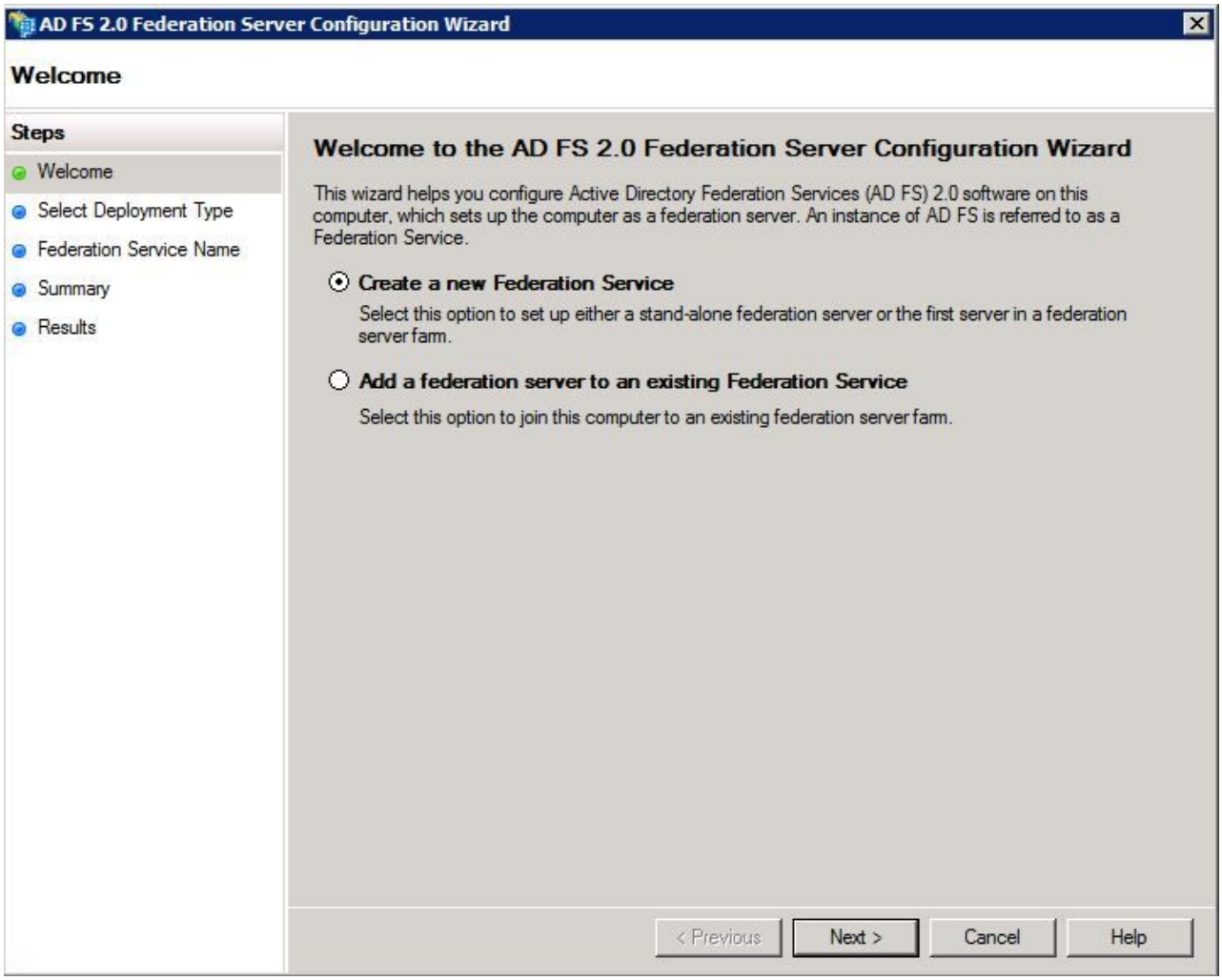
Windows Server 上での AD FS 2.0 の設定

ステップ 1：インストール後にAD FS 2.0ウィンドウが自動的に開かなかった場合は、Startをクリックしてad FS 2.0 Managementを検索し、手動で開くことができます。

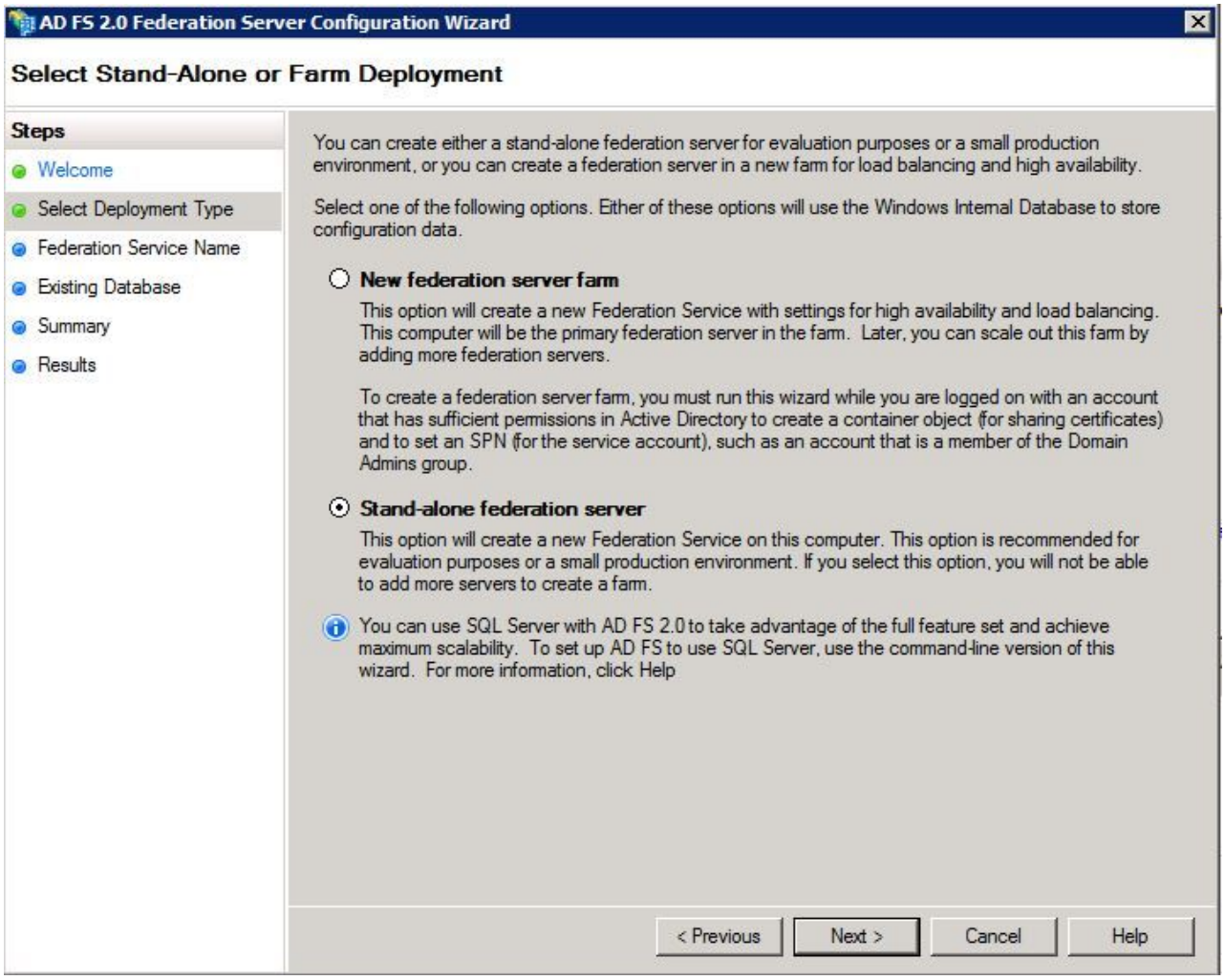
ステップ 2：AD FS 2.0フェデレーションサーバー構成ウィザードを選択します。



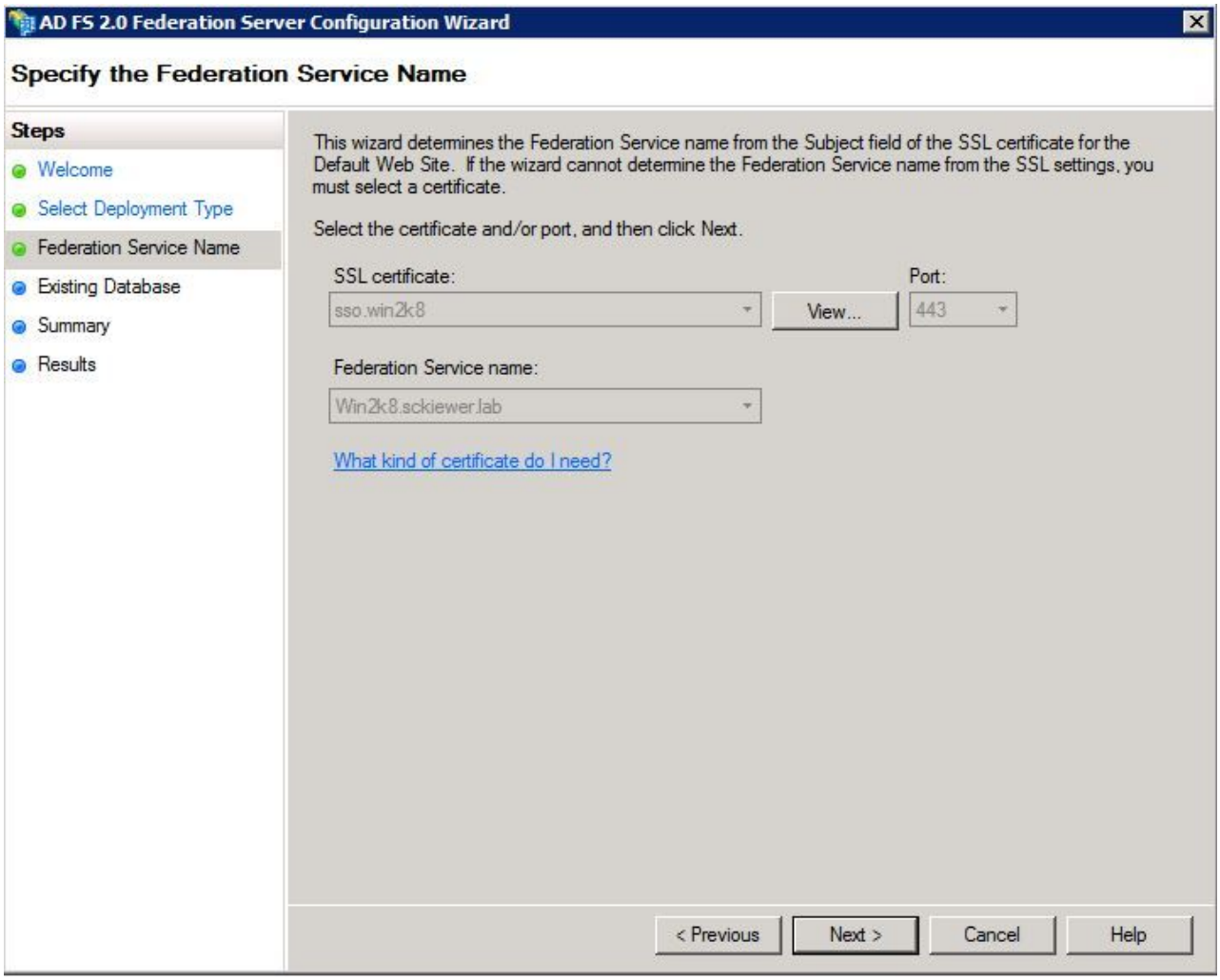
ステップ3：次に、Create a New Federation Serviceをクリックします。



ステップ 4：ほとんどの環境では、スタンドアロンフェデレーションサーバで十分です。



ステップ 5：次に、証明書を選択するように求められます。サーバに証明書がある限り、このフィールドは自動的に入力されます。



手順 6：サーバー上にAD FSデータベースが既に存在する場合、続行するにはデータベースを削除する必要があります。

手順 7：最後に、Nextをクリックできる概要画面が表示されます。

CUCM への Idp メタデータのインポート/CUCM メタデータのダウンロード

ステップ 1：Windowsサーバのホスト名/FQDNでURLを更新し、AD FSサーバからメタデータをダウンロードします。 https://hostname/federationmetadata/2007-06/federationmetadata.xml

ステップ 2：Cisco Unified CM Administration > System > SAML Single Sign-Onの順に移動します。

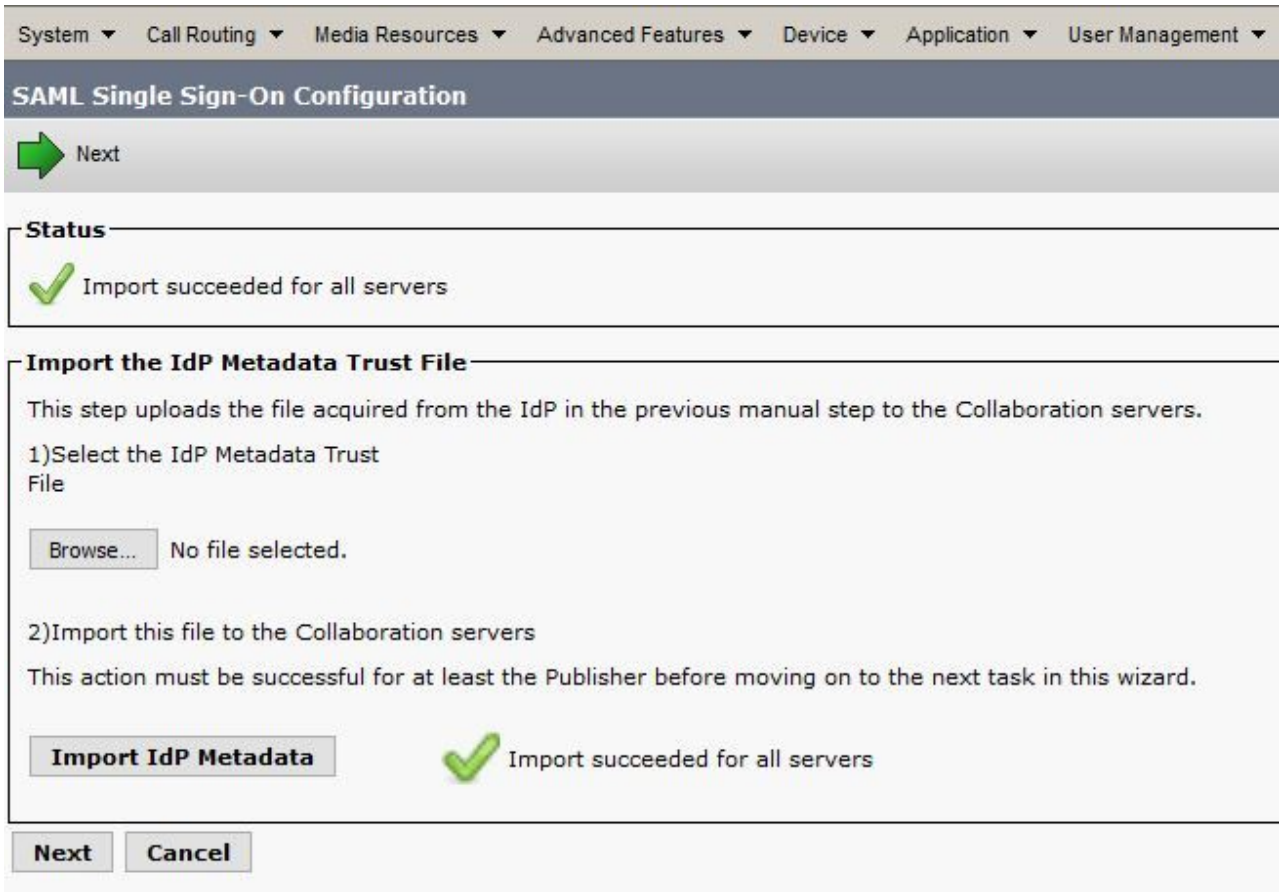
ステップ 3：Enable SAML SSOをクリックします。

ステップ 4：Webサーバの接続に関するアラートを受け取った場合は、Continueをクリックします。

ステップ 5：次に、IdP からメタデータ ファイルをダウンロードするように CUCM から要求されます。 このシナリオでは、AD FSサーバがIdPであり、手順1でメタデータをダウンロードしたので、Nextをクリックします。

手順 6：Browse > Select the .xml from Step 1 > Import IdP Metadataの順にクリックします。

手順 7：インポートが成功したことを示すメッセージが表示されます。



ステップ 8：[Next] をクリックします。

ステップ 9：CUCMにIdPメタデータをインポートしたので、CUCMのメタデータをIdPにインポートする必要があります。

ステップ 10：Download Trust Metadata Fileをクリックします。

ステップ 11[Next] をクリックします。

ステップ 12.zipファイルをWindows Serverに移動し、内容をフォルダに解凍します。

AD FS 2.0 サーバへの CUCM メタデータのインポートと要求ルールの作成

ステップ 1：Startをクリックして、AD FS 2.0 Managementを検索します。

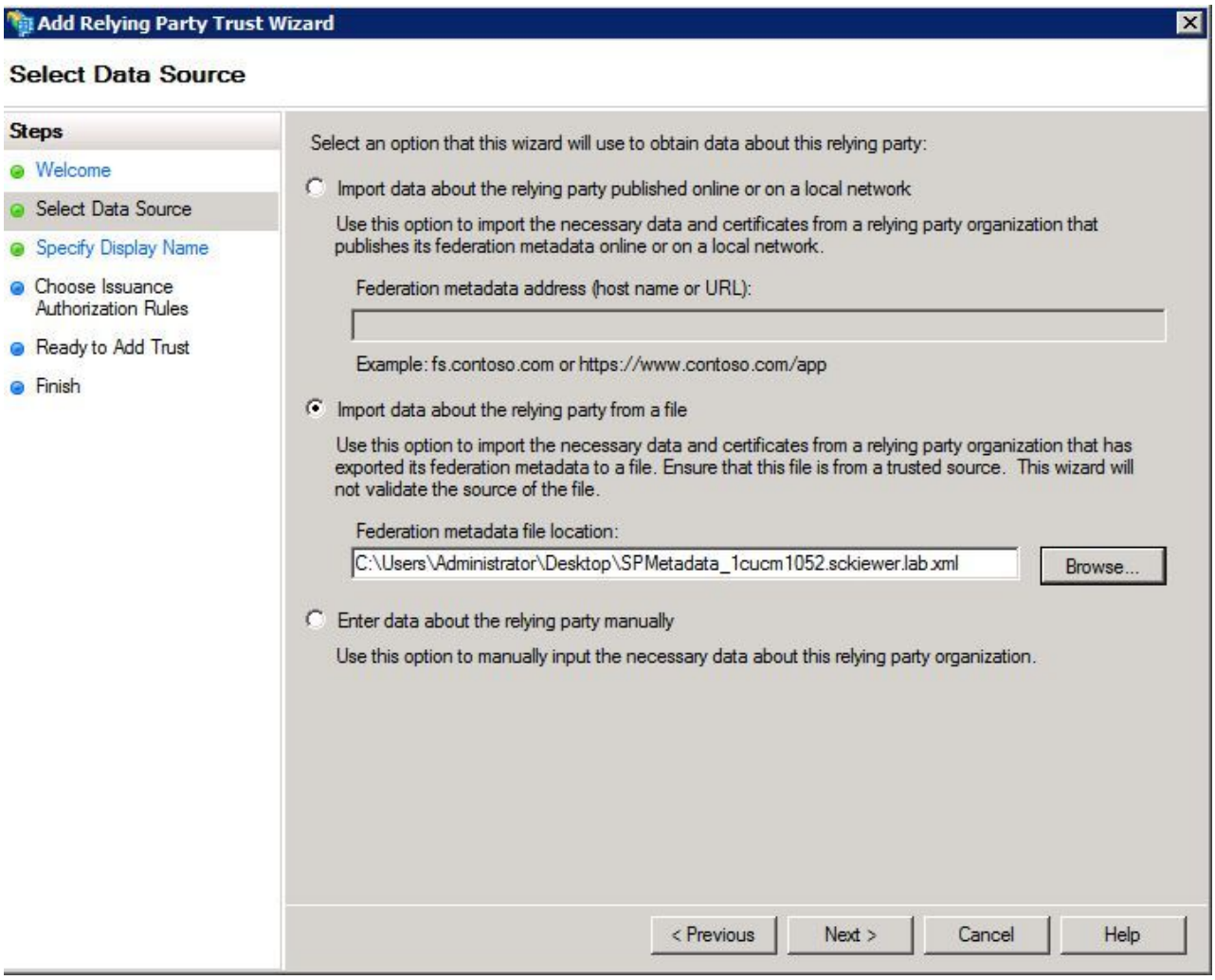
ステップ 2：Required: Add a trusted relying partyをクリックします。

注：このオプションが表示されない場合は、ウィンドウを閉じて再度開く必要があります。

ステップ 3：[Add Relying Party Trust Wizard] ウィザードが開いたら、[Start] をクリックします。

ステップ 4：ここで、ステップ12で抽出したXMLファイルをインポートする必要があります。Import data about the relying party from a fileを選択し、フォルダファイルを参照してパブリッシャ用のXMLを選択します。

注:SSOを使用するすべてのUnified Collaboration Serverに対して、前の手順を使用します。



ステップ 5：[Next] をクリックします。

手順 6：Display Nameを編集して、Nextをクリックします。

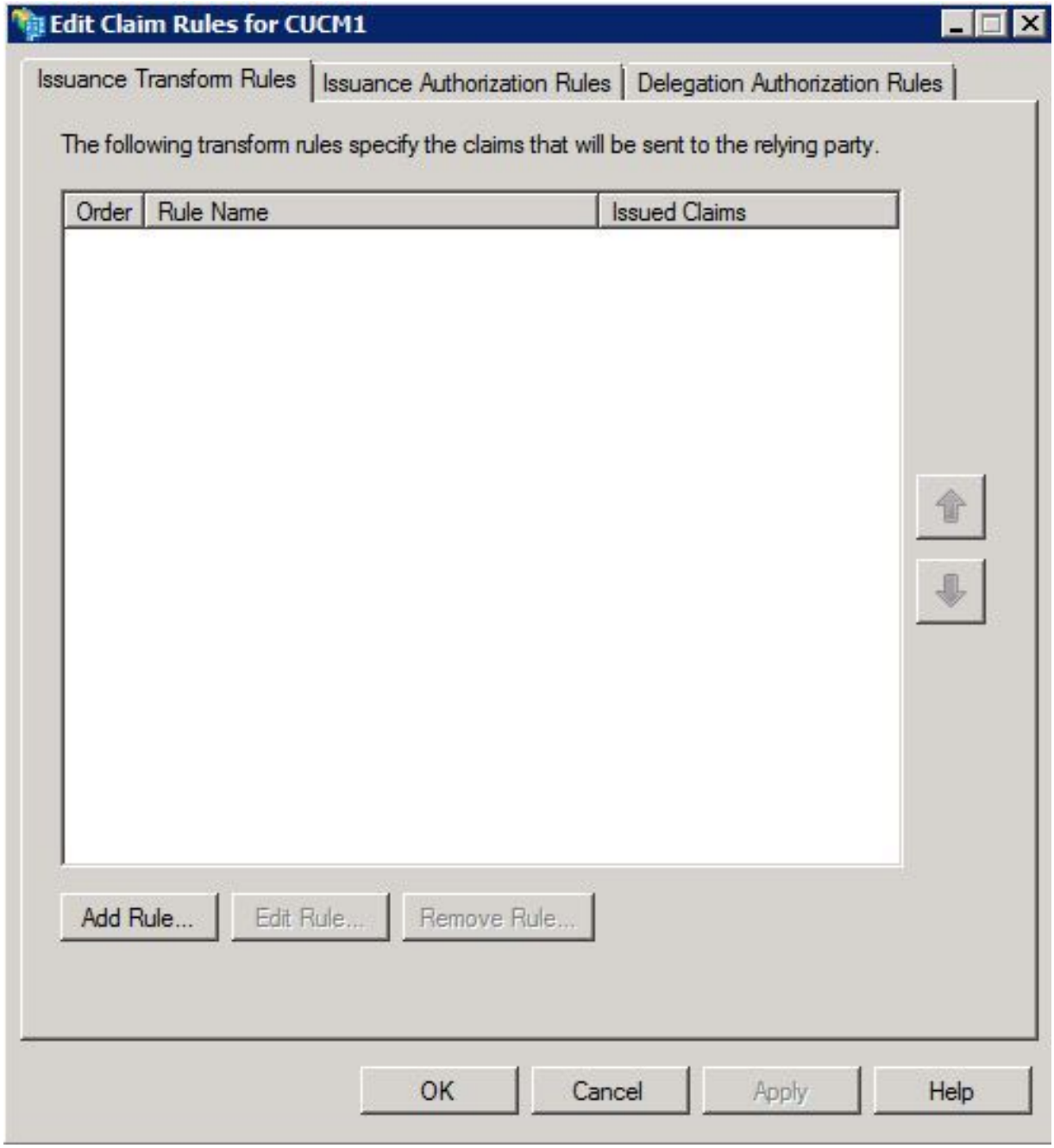
手順 7：[Permit all users to access this relying party] を選択し、[Next] をクリックします。

ステップ 8：もう一度 [Next] をクリックします。

ステップ 9：この画面で、Open the Edit Claim Rules dialog for this relying party trust when the wizard closesにチェックマークが入っていることを確認してから、Closeをクリックしま

す。

ステップ 10：[クレームルールの編集]ウィンドウが開きます。



ステップ 11このウィンドウで、[Add Rule] をクリックします。

ステップ 12Claim rule templateで、Send LDAP Attributes as Claimsを選択し、Nextをクリックします。

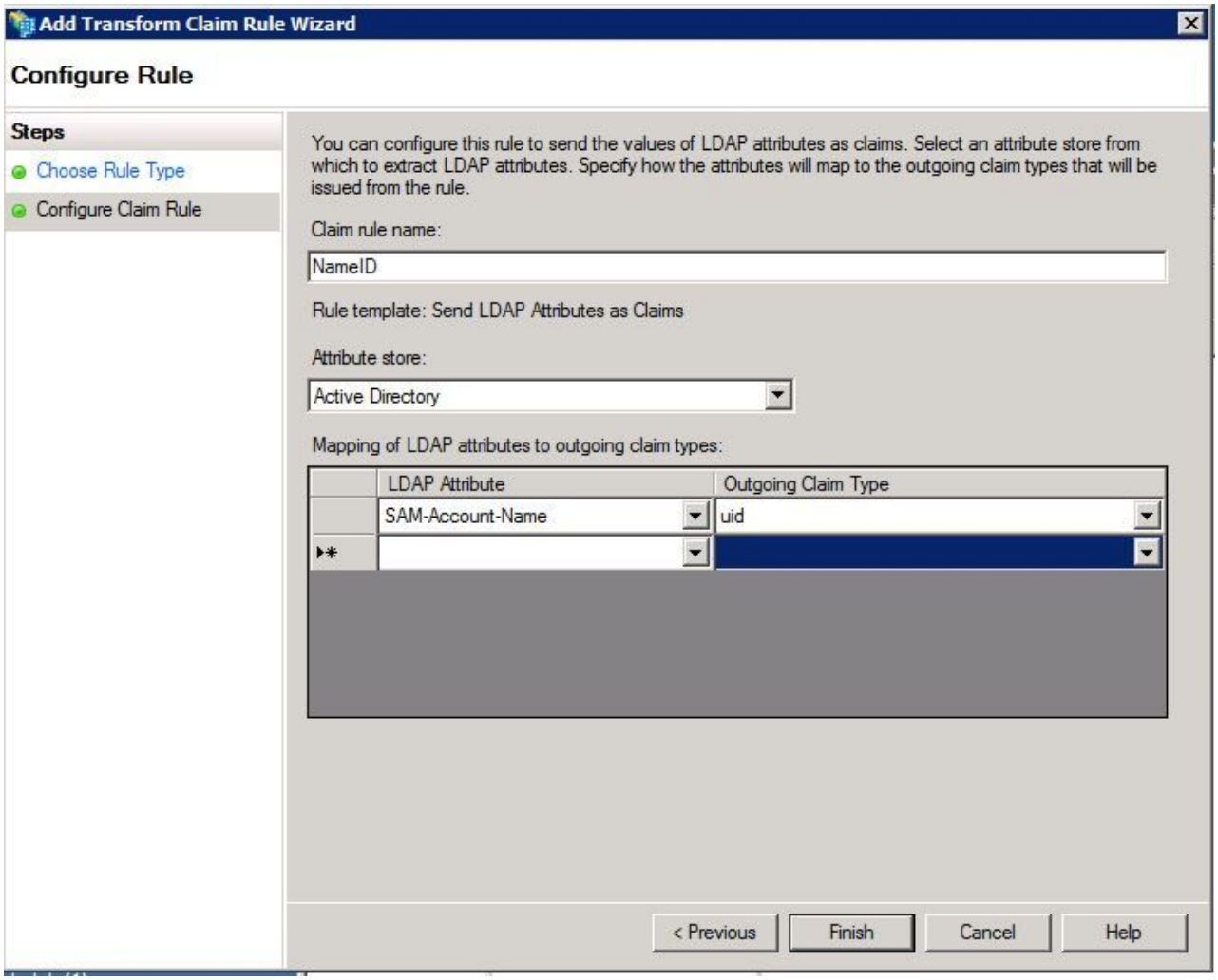
ステップ 13次のページで、クレームルール名としてNameIDを入力します。

ステップ 14：Attribute storeに対してActive Directoryを選択します。

ステップ 15：LDAP Attributeに対してSAM-Account-Nameを選択します。

ステップ 16：[Outgoing Claim Type] にuidを入力します。

注: uidはドロップダウンリストのオプションではないため、手動で入力する必要があります。



ステップ 17：[Finish] をクリックします。

ステップ 18：これで、最初のルールが完了しました。Add Ruleをもう一度クリックします。

ステップ 19：Send Claims Using a Custom Ruleを選択します。

ステップ 20：クレームルール名を入力します。

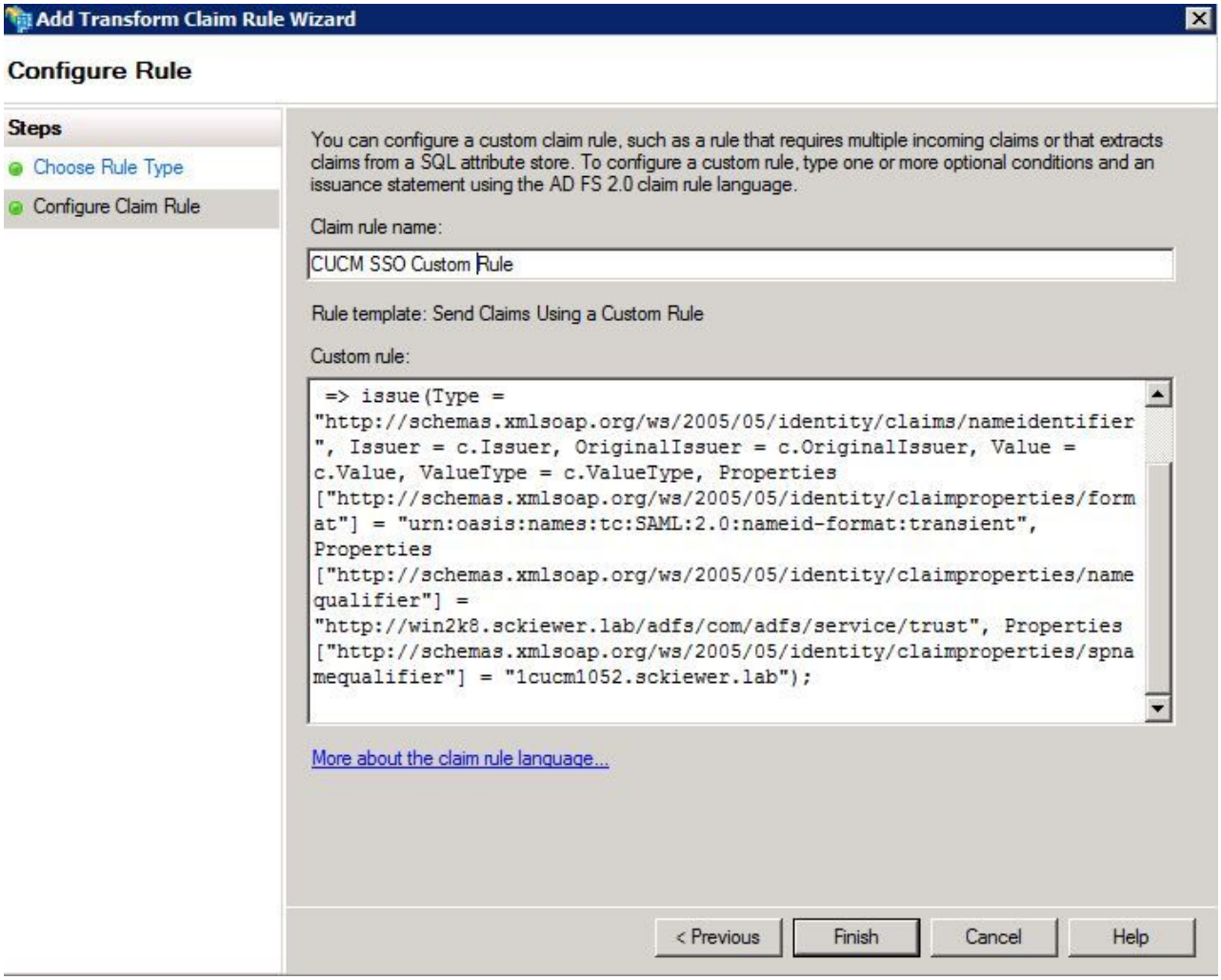
ステップ 21：Custom ruleフィールドに、次のテキストを貼り付けます。

c:[== "http://schemas.microsoft.com/ws/2008/06/identity/と入力します。
claims/windowsaccountname"]
=> issue(タイプ= "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifie
= "http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =

"CUCM_ENTITY_ID");

ステップ 22：AD_FS_SERVICE_NAMEとCUCM_ENTITY_IDを適切な値に変更してください。

注:AD FSサービス名が不明な場合は、手順に従って検索できます。 CUCMエンティティIDは、CUCMメタデータファイルの最初の行から取得できます。 ファイルの最初の行に、次のようなentityIDがあります。entityID=1cucm1052.sckiewer.lab,請求ルールの該当するセクションに下線の値を入力する必要があります。



ステップ 23：[Finish] をクリックします。

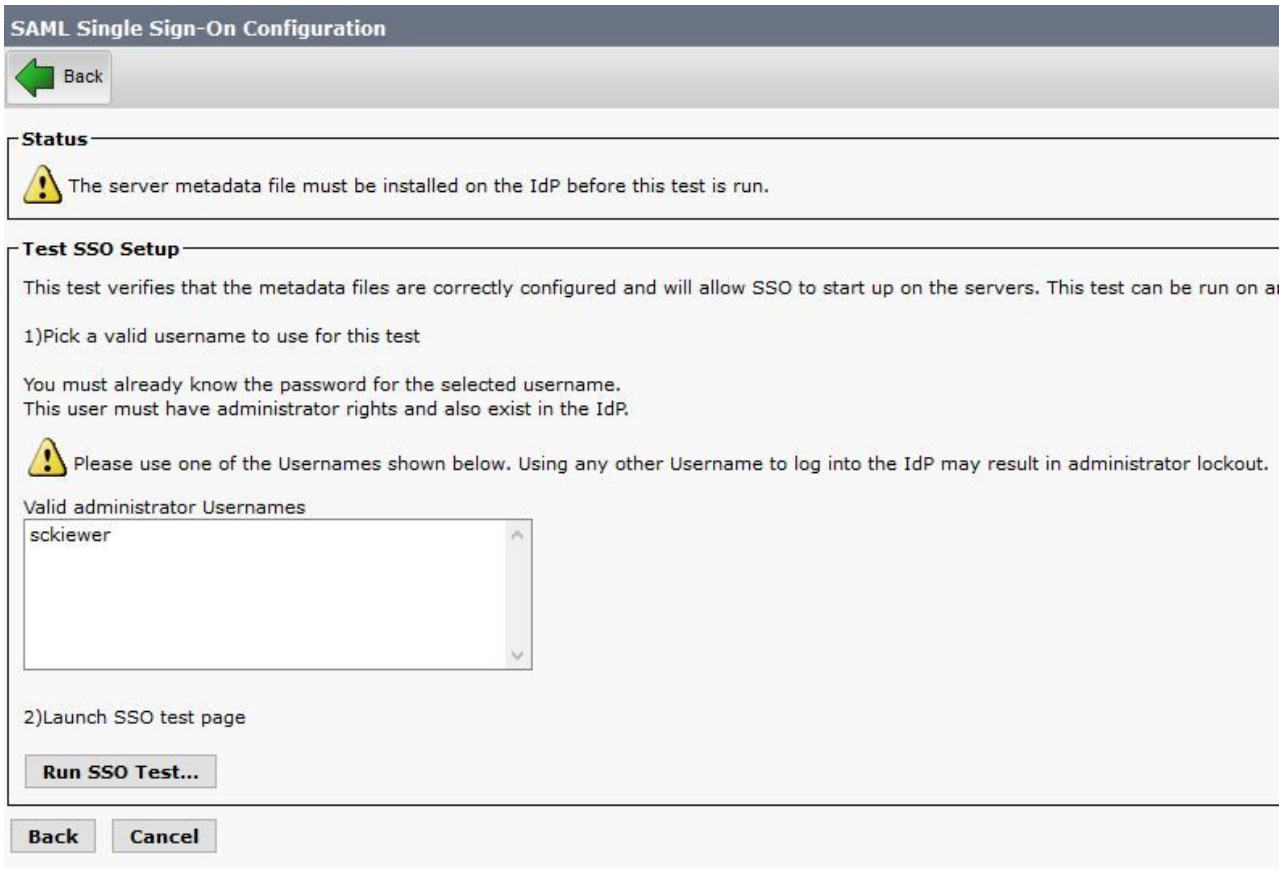
ステップ 24：[OK] をクリックします。

注：要求ルールは、SSOを使用するすべてのUnified Collaboration Serverに必要です。

CUCMでのSSO有効化の完了とSSOテストの実行

ステップ 1：AD FSサーバが完全に設定されたので、CUCMに戻ることができます。

ステップ 2：最後の設定ページで作業を中断しました。



ステップ 3：Standard CCM Super Usersロールが選択されているエンドユーザを選択し、Run SSO Test...をクリックします。

ステップ 4： ブラウザでポップアップが許可されていることを確認し、プロンプトにクレデンシャルを入力します。

ステップ 5：ポップアップウィンドウでCloseをクリックし、次にFinishをクリックします。

手順 6：Webアプリケーションの短時間の再起動後、SSOが有効になります。

トラブルシュート

デバッグする SSO ログの設定

SSOログをデバッグに設定するには、CUCMのCLIでset samltrace level debugコマンドを実行する必要があります。

SSO ログは RTMT からダウンロードできます。設定されたログの名前は、Cisco SSO です。

フェデレーションサービス名の検索

フェデレーションサービス名を検索するには、StartをクリックしてAD FS 2.0 Managementを検索します。

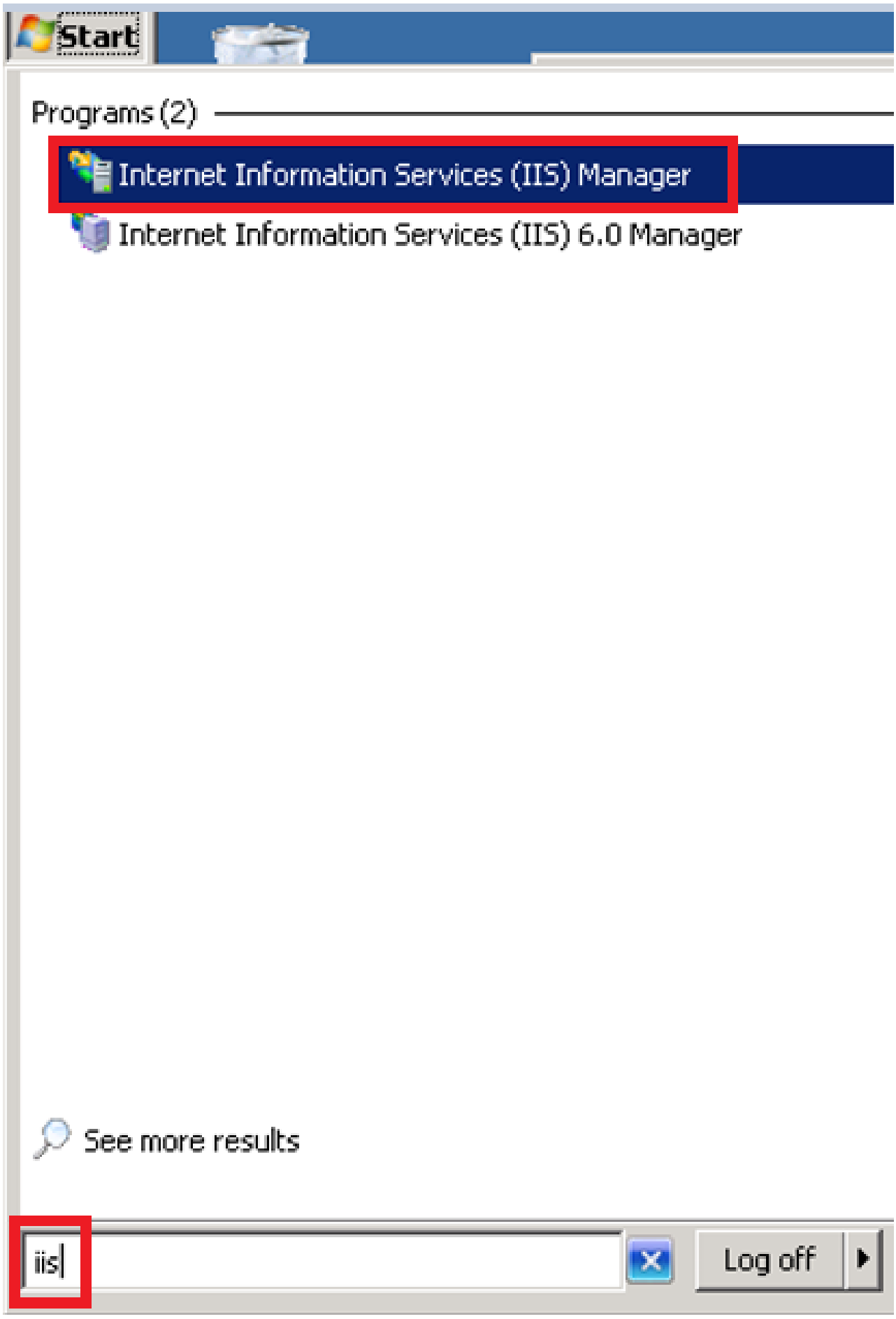
- [フェデレーションサービスのプロパティの編集...]をクリックします。
- [全般]タブで、フェデレーションサービス名を探します

ドットなしの証明書とフェデレーションサービス名

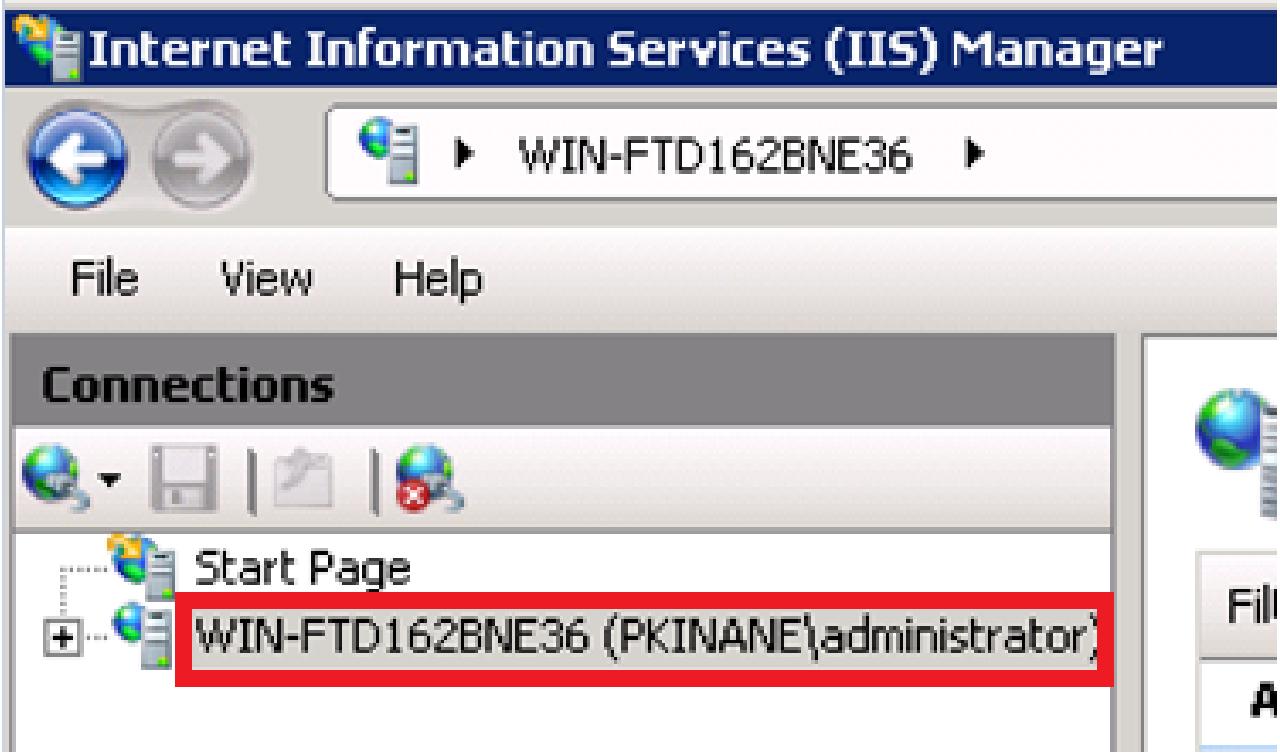
AD FS構成ウィザードでこのエラーメッセージが表示された場合は、新しい証明書を作成する必要があります。

選択された証明書にはドットなしの（短い名前の）サブジェクト名があるため、選択された証明書を使用してフェデレーションサービス名を決定することはできません。ドットなしの（短い名前の）サブジェクト名を持たない別の証明書を選択し、再試行してください。

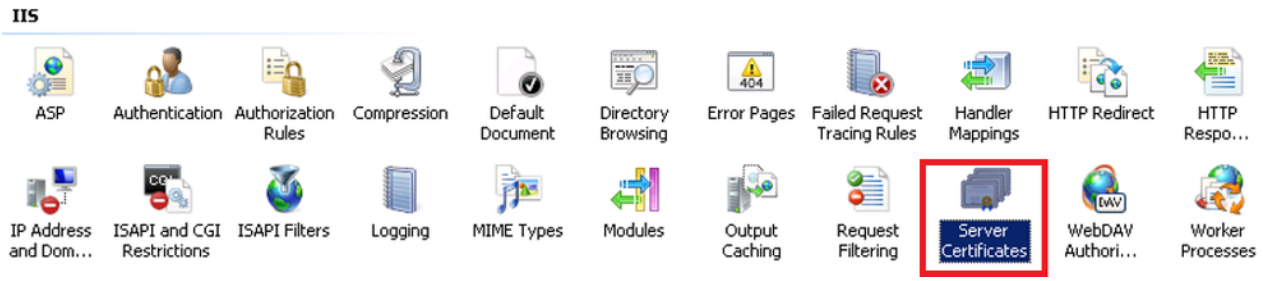
ステップ 1：[スタート]ボタンをクリックしてiisを検索し、[インターネットインフォメーションサービス(IIS)マネージャ]を開きます



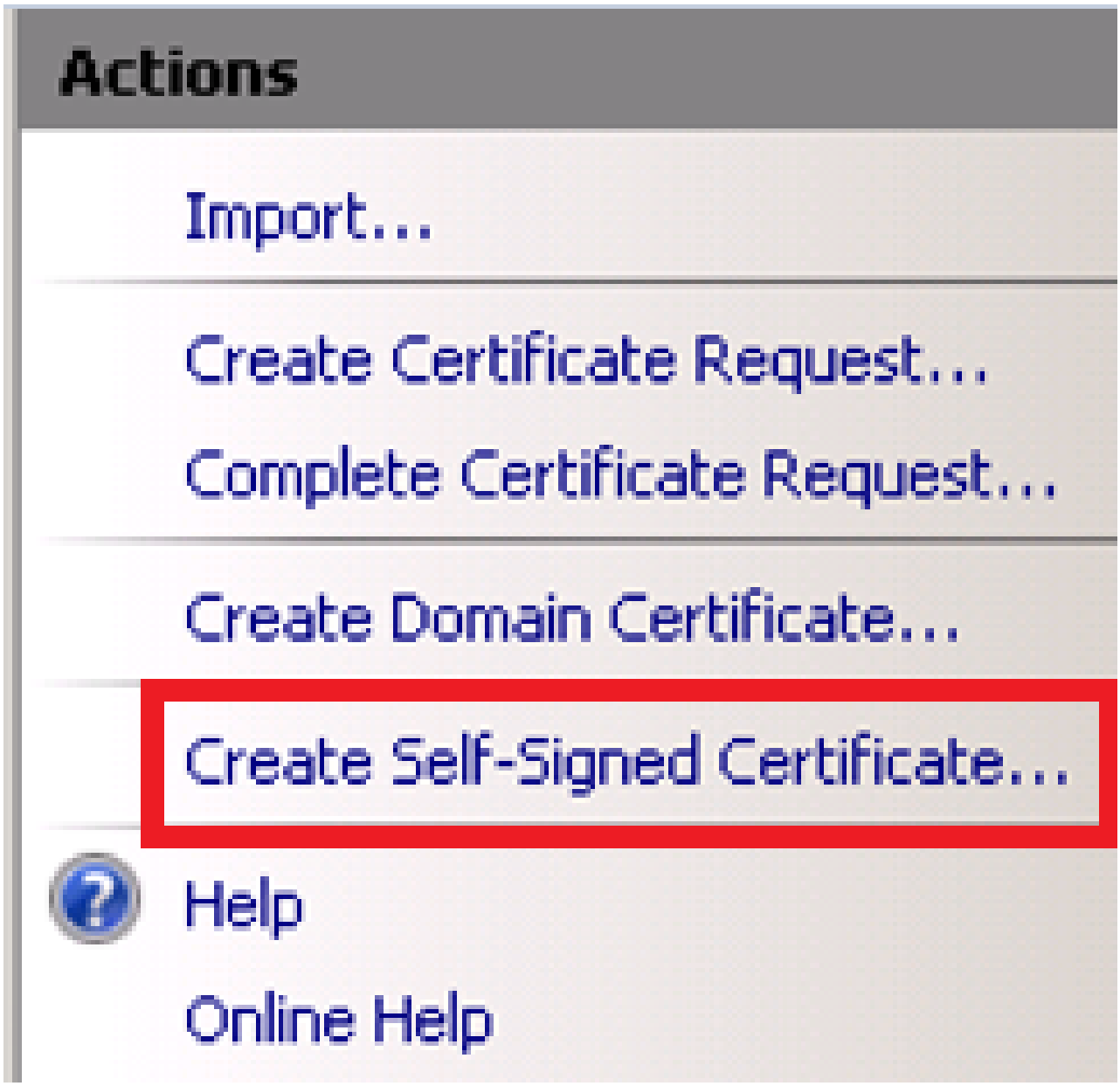
ステップ 2：サーバ名をクリックします。



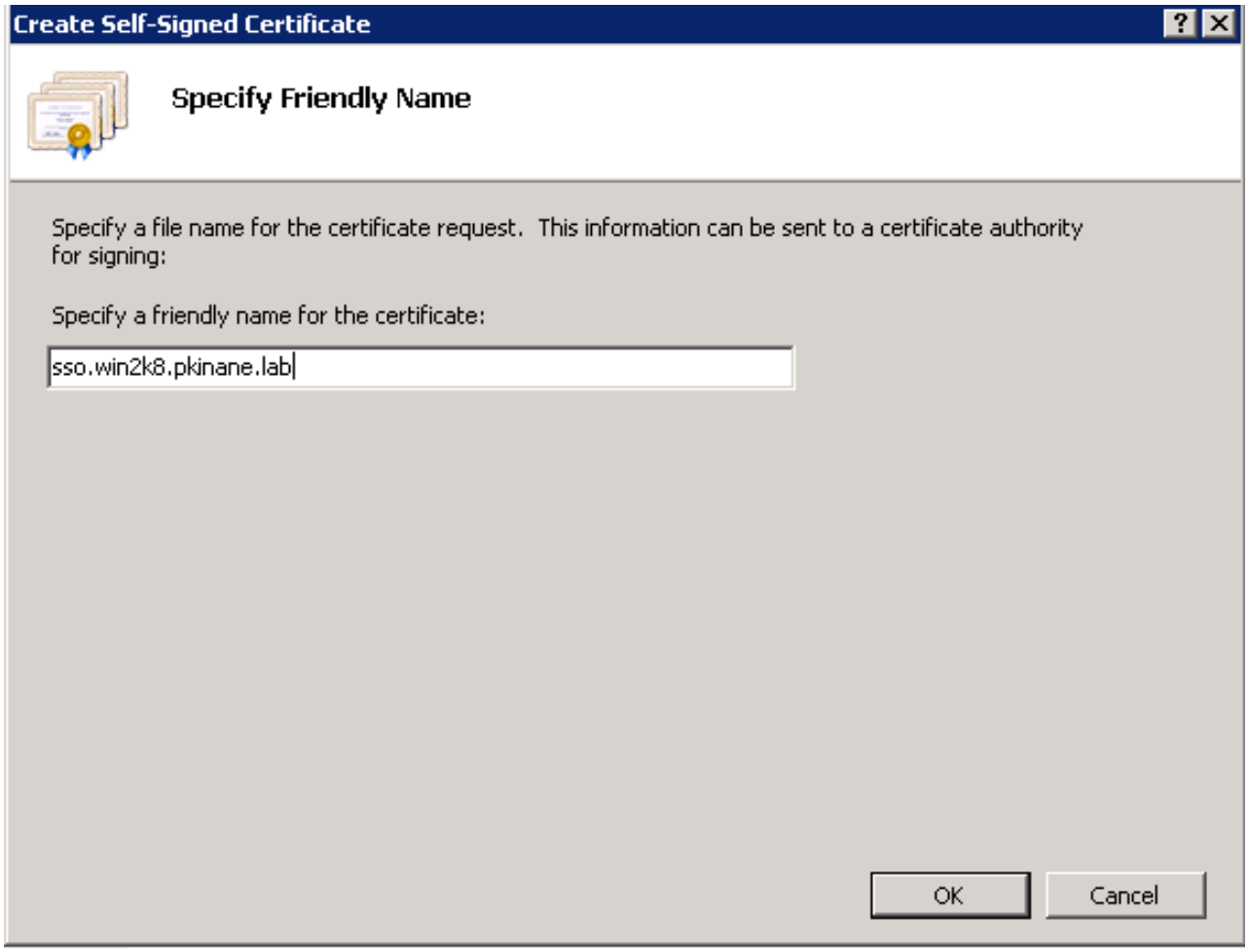
ステップ 3：Server Certificatesをクリックします。



ステップ 4：Create Self-Signed Certificateをクリックします。



ステップ 5：証明書のエイリアスとして名前を入力します.



CUCM サーバと IDP サーバ間で時刻が同期しない

CUCMからSSOテストを実行するときにこのエラーが表示された場合は、CUCMと同じNTPサーバを使用するようにWindowsサーバを設定する必要があります。

無効なSAML応答です。これは、Cisco Unified Communications ManagerサーバとIDPサーバ間で時刻が同期していないときに発生する可能性があります。Please verify the NTP configuration on both servers.CLIから「utils ntp status」を実行し、Cisco Unified Communications Manager上でこのステータスを確認します。

Windows Serverで正しいNTPサーバを指定したら、別のSSOテストを実行して、問題が解決するかどうかを確認する必要があります。 場合によっては、アサーションの有効期間をスキューする必要があります。 そのプロセスの詳細については、ここを参照してください。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。