Konfigurieren der einmaligen Anmeldung mit CUCM und AD FS 2.0

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Single Sign-On (SSO) auf Cisco Unified Communications Manager und dem Active Directory Federation Service beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM)
- Grundlegende Kenntnisse des Active Directory-Verbunddiensts (AD FS)

Um SSO in Ihrer Laborumgebung zu aktivieren, benötigen Sie folgende Konfiguration:

- Windows Server mit installiertem AD FS.
- CUCM mit konfigurierter LDAP-Synchronisierung.
- Ein Endbenutzer, für den die Standard-CCM-Superuser-Rolle ausgewählt wurde.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows Server mit AD FS 2.0
- CUCM 10.5.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Verfahren für AD FS 2.0 mit Windows Server 2008 R2 wird bereitgestellt. Diese Schritte funktionieren auch für AD FS 3.0 unter Windows Server 2016.

Laden Sie AD FS 2.0 auf Ihren Windows Server herunter und installieren Sie es.

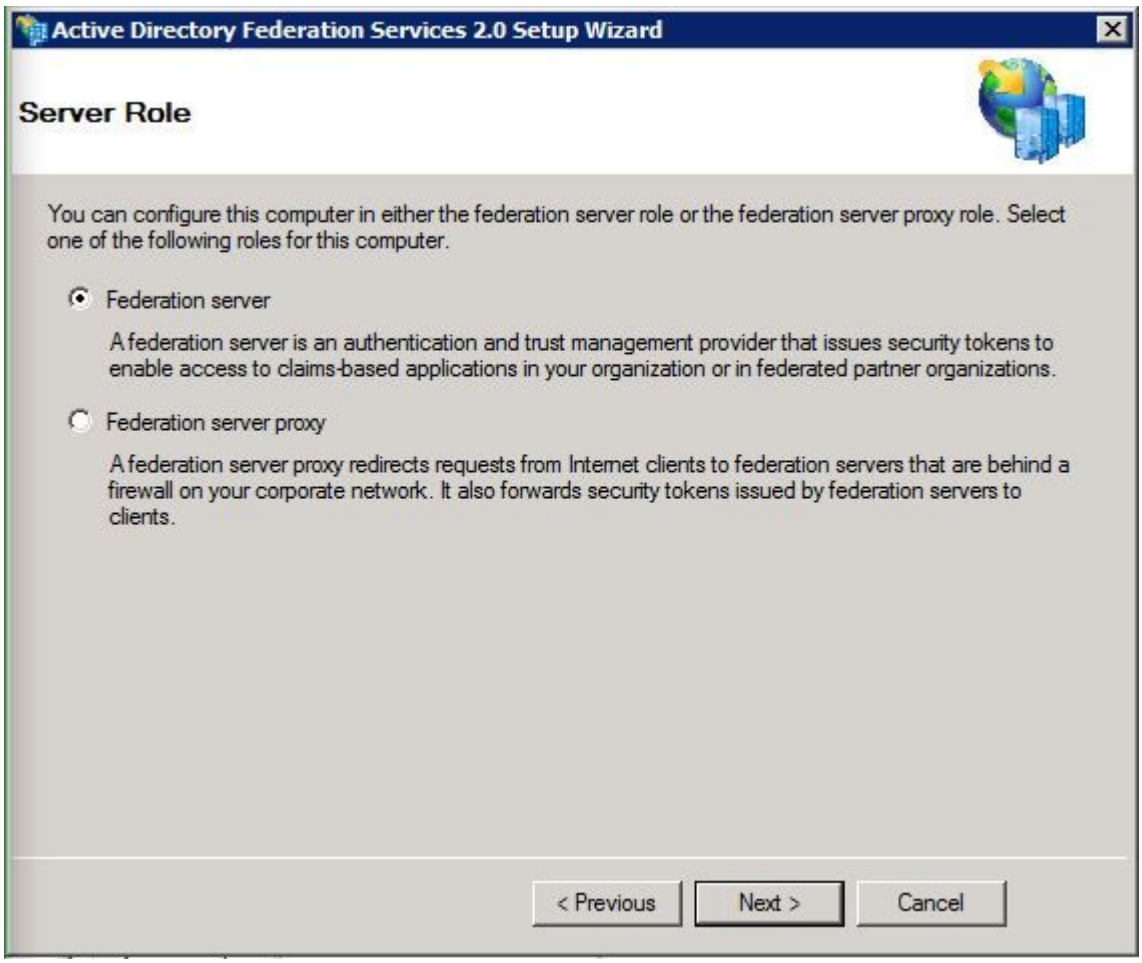
Schritt 1: Navigieren Sie zu AD FS 2.0 herunterladen.

Schritt 2: Stellen Sie sicher, dass Sie den entsprechenden Download auf Basis Ihres Windows-Servers auswählen.

Schritt 3: **Verschieben Sie** die heruntergeladene Datei auf Ihren Windows Server.

Schritt 4: Fahren Sie mit der Installation fort:

Schritt 5: Wenn Sie dazu aufgefordert werden, wählen Sie **Verbundserver aus**:



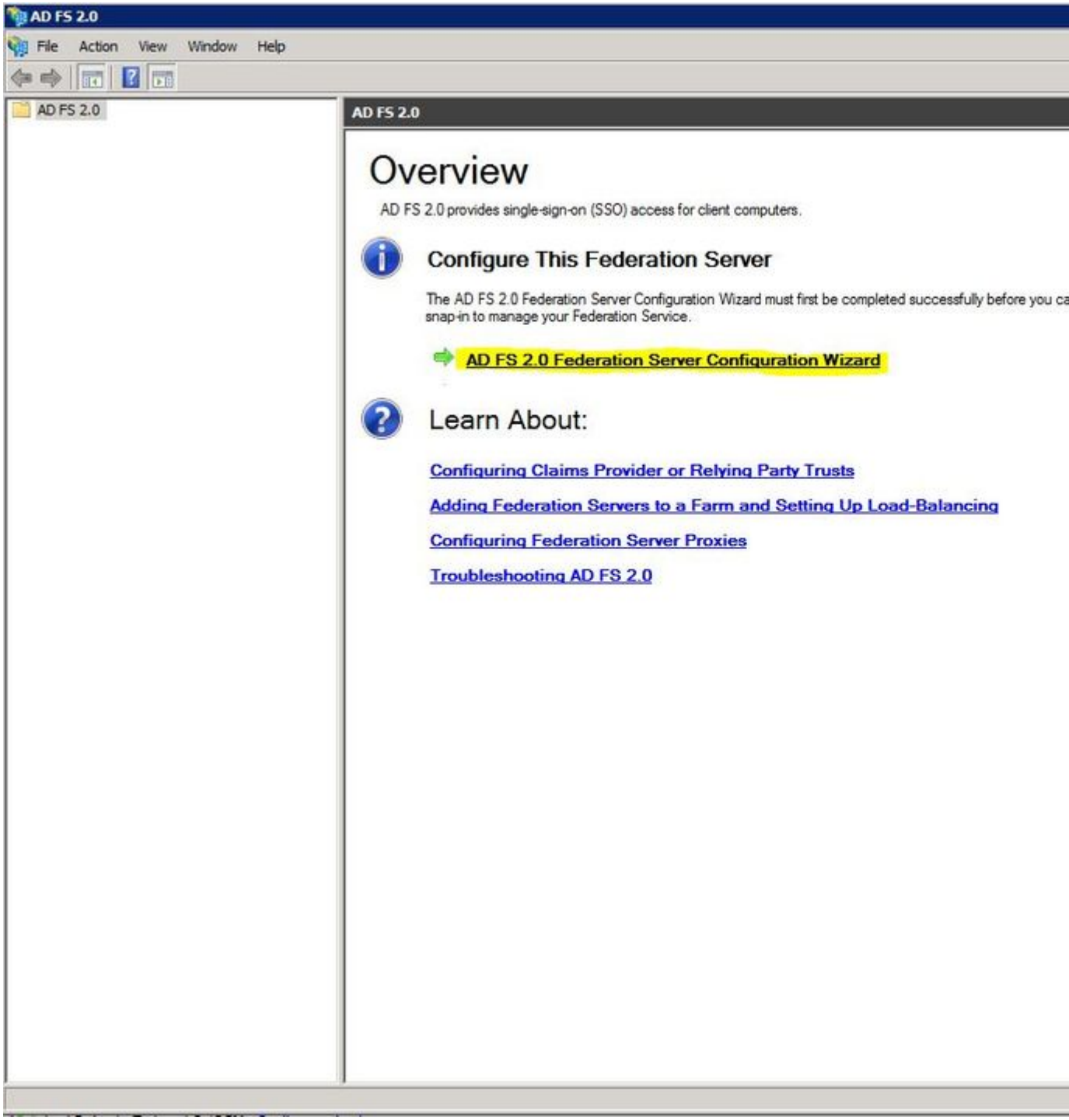
Schritt 6: Einige Abhängigkeiten werden automatisch installiert. Klicken Sie anschließend auf **Fertig stellen**.

Nachdem Sie AD FS 2.0 auf Ihrem Server installiert haben, müssen Sie eine Konfiguration hinzufügen.

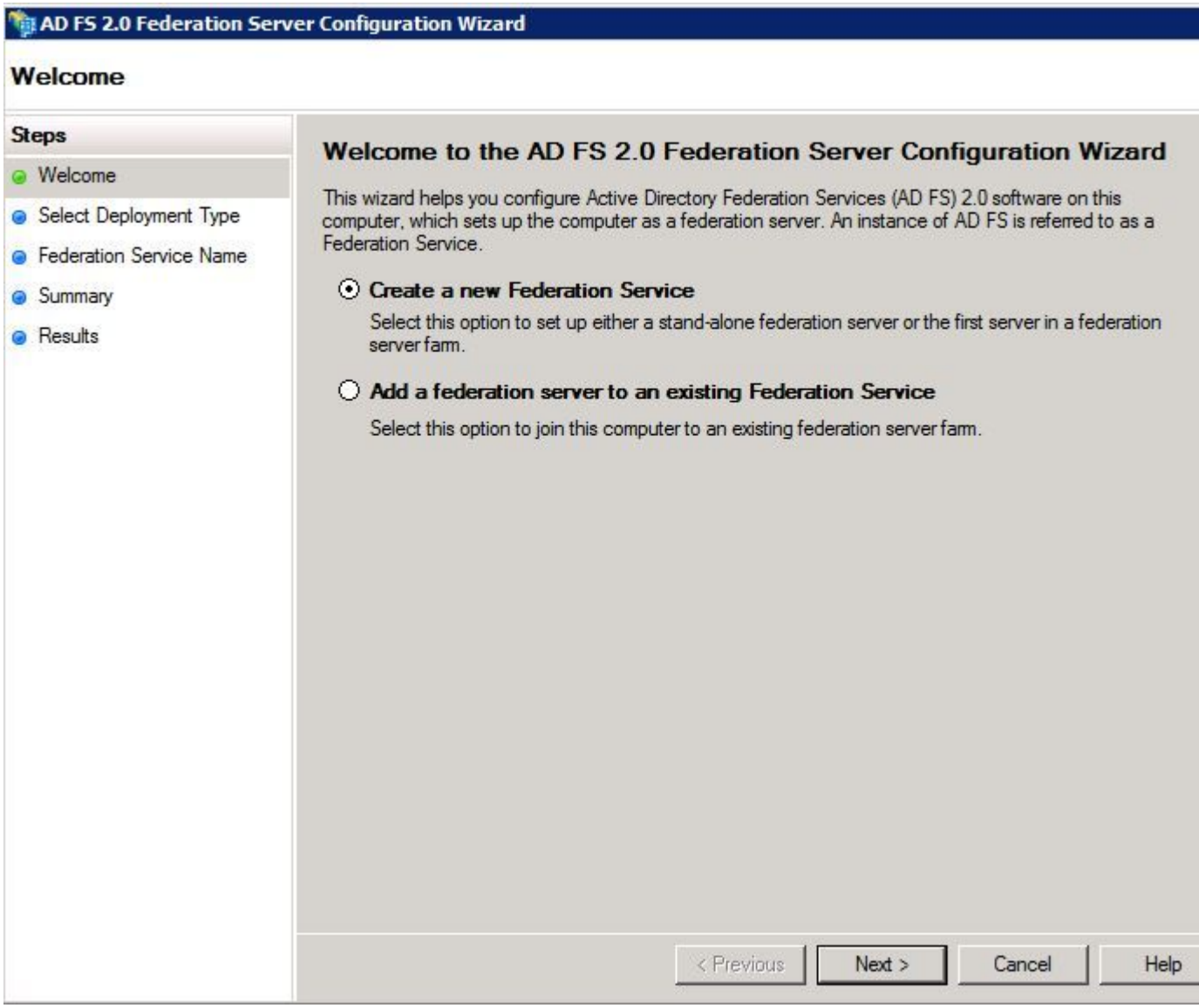
Konfigurieren von AD FS 2.0 auf dem Windows-Server

Schritt 1: Wenn das Fenster AD FS 2.0 nach der Installation nicht automatisch geöffnet wurde, können Sie auf **Start** klicken und nach AD FS 2.0 Management suchen, um es manuell zu öffnen.

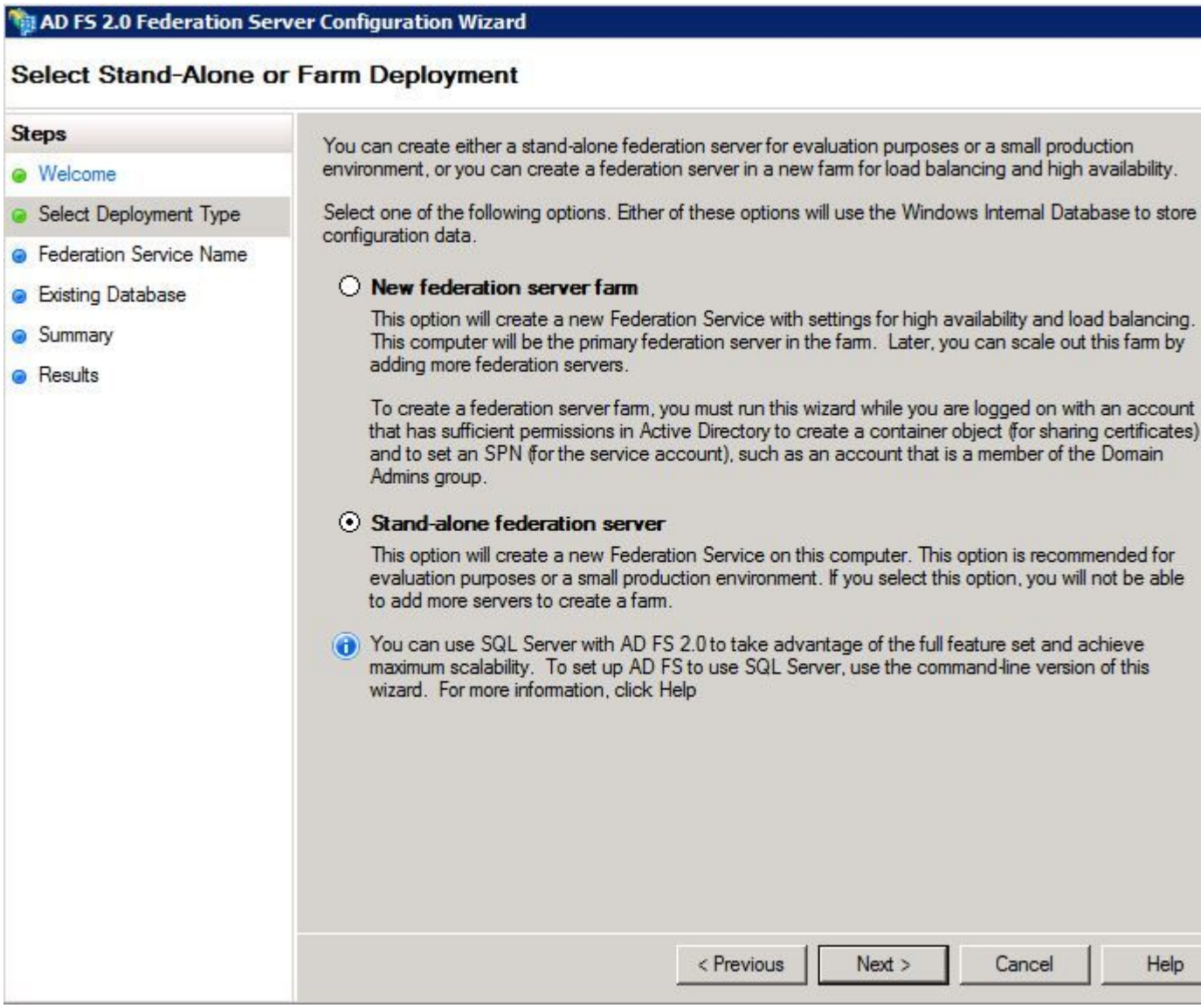
Schritt 2: Wählen Sie **AD FS 2.0 Federation Server Configuration Wizard**.



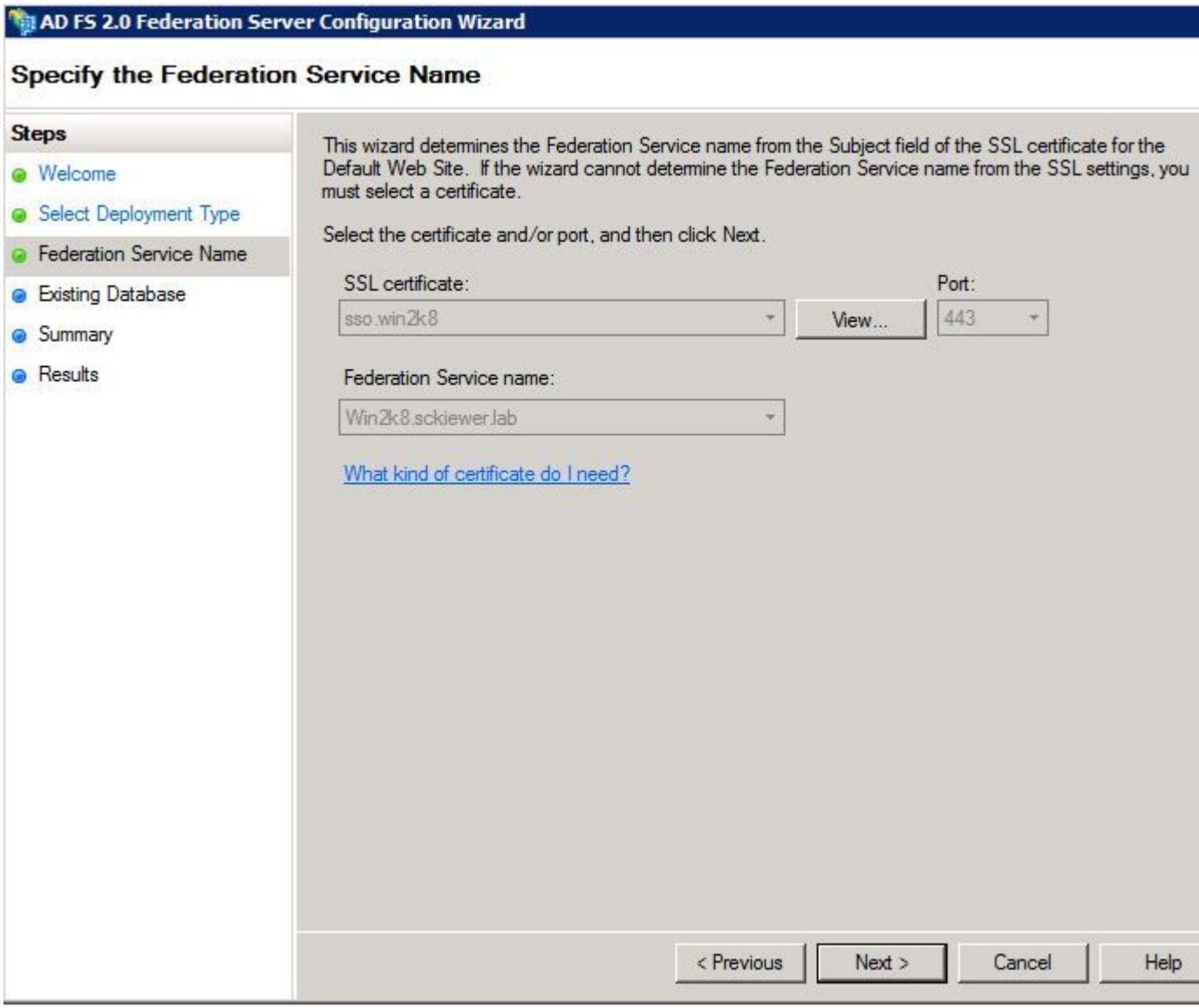
Schritt 3: Klicken Sie anschließend auf **Neuen Verbunddienst erstellen**.



Schritt 4: In den meisten Umgebungen ist **ein Standalone-Verbundserver** ausreichend.



Schritt 5: Als Nächstes werden Sie aufgefordert, ein Zertifikat auszuwählen. Dieses Feld wird automatisch ausgefüllt, solange der Server über ein Zertifikat verfügt.



Schritt 6: Wenn auf dem Server bereits eine AD FS-Datenbank vorhanden ist, müssen Sie diese entfernen, um fortzufahren.

Schritt 7. Schließlich wird ein Übersichtsbildschirm angezeigt, in dem Sie auf **Weiter** klicken können.

Importieren Sie die IP-Metadaten in CUCM/Laden Sie die CUCM-Metadaten herunter.

Schritt 1: Aktualisieren Sie die URL mit Ihrem Windows Server-Hostnamen/FQDN, und laden Sie die Metadaten von Ihrem AD FS-Server herunter: https://hostname/federationmetadata/2007-06/federationmetadata.xml

Schritt 2: Navigieren Sie zu **Cisco Unified CM Administration** > **System** > **SAML Single Sign-On**.

Schritt 3: Klicken Sie auf **SAML SSO aktivieren**.

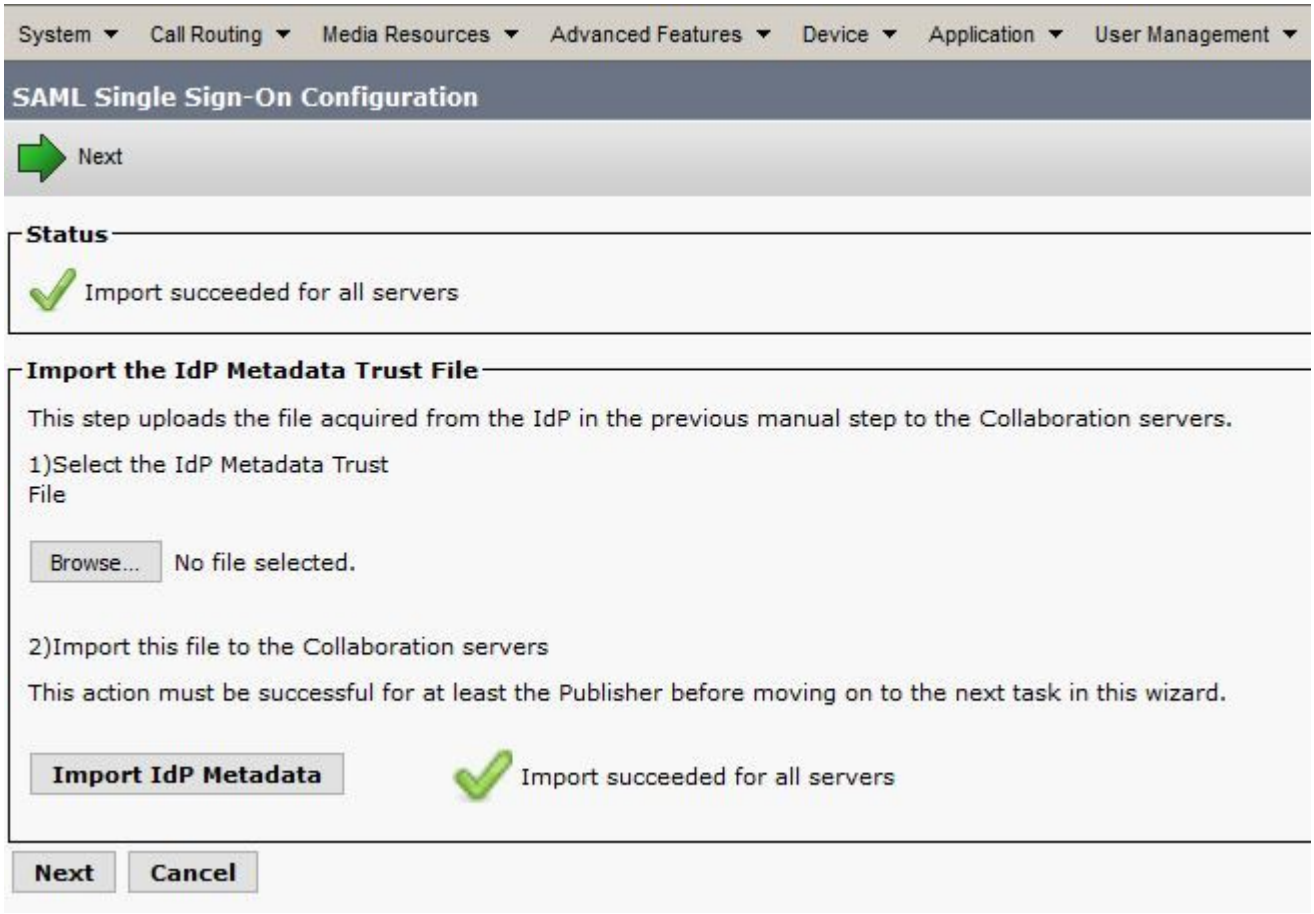
Schritt 4: Wenn Sie eine Warnung über Webserververbindungen erhalten, klicken Sie auf **Weiter**.

Schritt 5: Als Nächstes weist CUCM Sie an, die Metadatendatei von Ihrem IdP herunterzuladen. In

diesem Szenario ist der AD FS-Server IdP, und Sie haben die Metadaten in Schritt 1 heruntergeladen. Klicken Sie daher auf **Weiter**.

Schritt 6: Klicken Sie auf **Durchsuchen** > **Wählen Sie die XML-Datei aus Schritt 1 aus** > klicken Sie auf **IDp-Metadaten importieren**.

Schritt 7. Eine Meldung zeigt an, dass der Import erfolgreich war:



Schritt 8: Klicken Sie auf Next (Weiter).

Schritt 9. Nachdem Sie die IdP-Metadaten in CUCM importiert haben, müssen Sie die CUCM-Metadaten in Ihren IdP importieren.

Schritt 10. Klicken Sie auf **Vertrauenswürdige Metadatendatei herunterladen**.

Schritt 11. Klicken Sie auf Next (Weiter).

Schritt 12: Verschieben Sie die ZIP-Datei auf Ihren Windows Server, und extrahieren Sie den Inhalt in einen Ordner.

Importieren von CUCM-Metadaten in einen AD FS 2.0-Server und Erstellen von Anspruchsregeln

Schritt 1: Klicken Sie auf **Start**, und suchen Sie nach **AD FS 2.0 Management**.

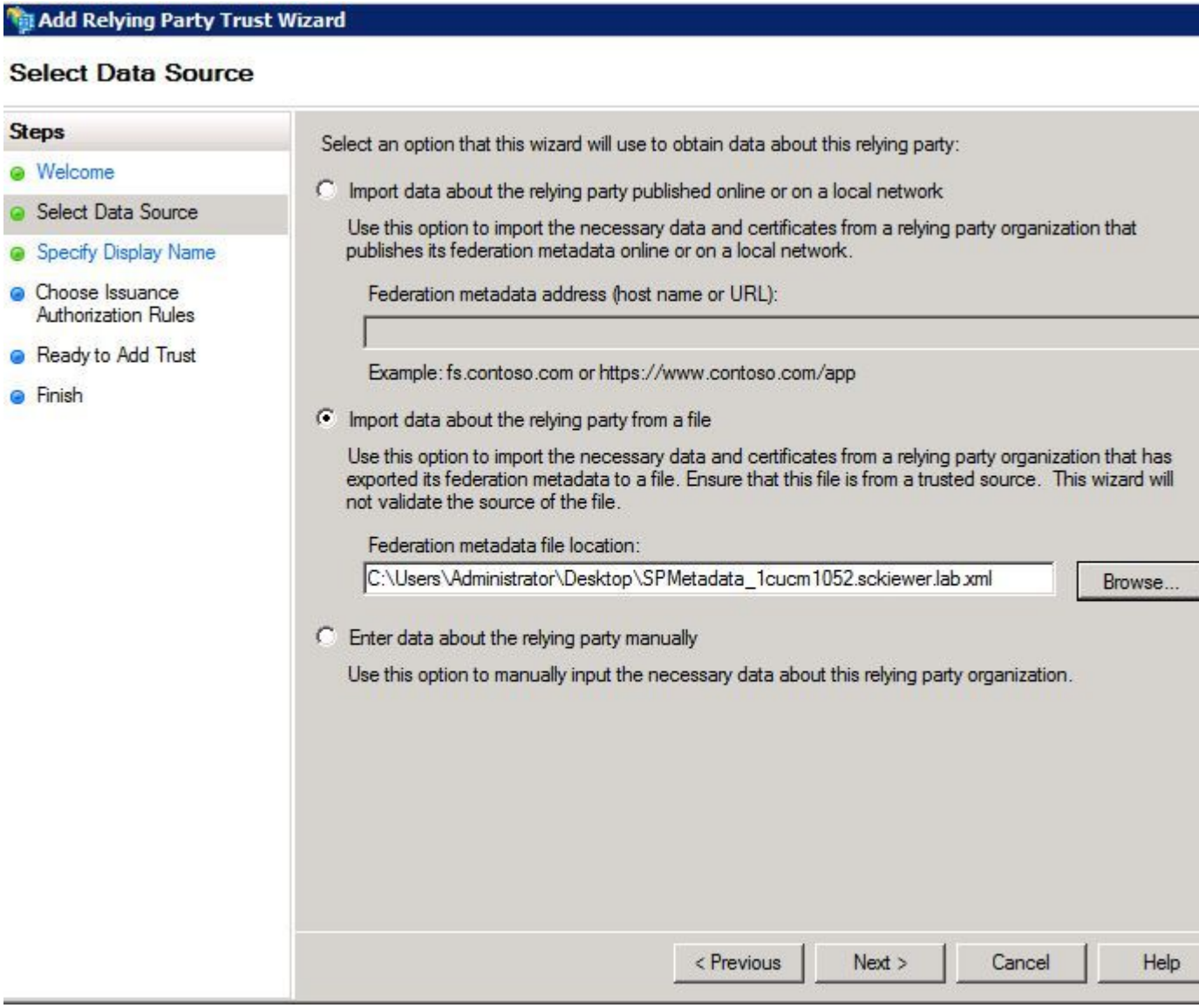
Schritt 2: Klicken Sie auf **Erforderlich: Vertrauenswürdige vertrauende Seite hinzufügen**.

Hinweis: Wenn diese Option nicht angezeigt wird, müssen Sie das Fenster schließen und es wieder öffnen.

Schritt 3: Wenn der **Assistent zum Hinzufügen von Vertrauensstellungen für vertrauende Partei** geöffnet ist, klicken Sie auf **Start**.

Schritt 4: Hier müssen Sie die XML-Dateien importieren, die Sie in Schritt 12 extrahiert haben. Wählen Sie **Daten über die vertrauende Partei aus einer Datei importieren** und navigieren Sie zu den Ordnerdateien, und wählen Sie die XML-Datei für den Herausgeber aus.

Hinweis: Verwenden Sie die vorherigen Schritte für alle Unified Collaboration-Server, auf denen Sie SSO verwenden möchten.



Schritt 5: Klicken Sie auf Next (Weiter).

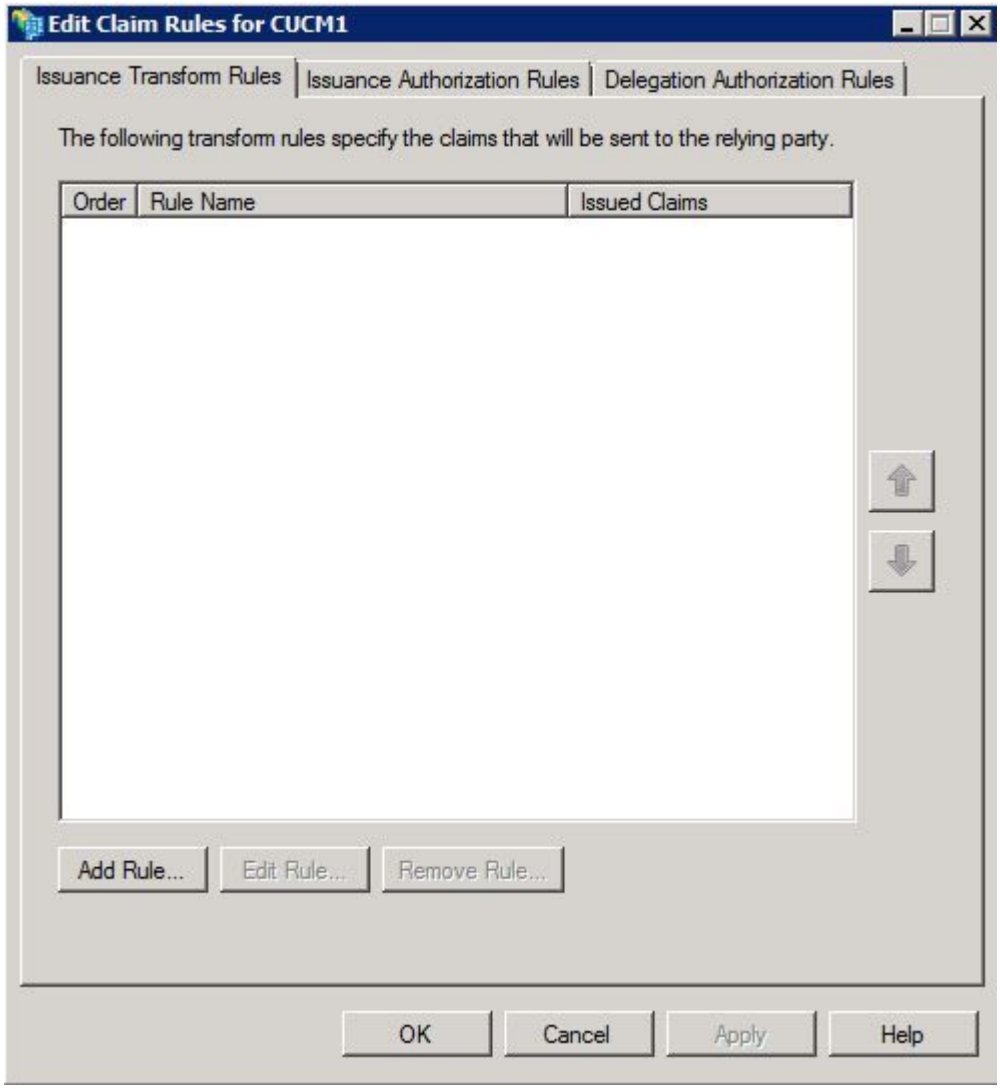
Schritt 6: Bearbeiten Sie den **Anzeigenamen,** und klicken Sie auf **Weiter**.

Schritt 7. Wählen Sie **Alle Benutzer für den Zugriff auf diese vertrauende Seite zulassen aus,** und klicken Sie auf **Weiter**.

Schritt 8: Klicken Sie erneut auf **Weiter**.

Schritt 9. Stellen Sie in diesem Bildschirm sicher, dass Sie **das Dialogfeld Anspruchsregeln bearbeiten für diese Vertrauensstellung der vertrauenden Seite geöffnet** haben, **wenn der Assistent geschlossen** ist, und klicken Sie dann auf **Schließen**.

Schritt 10. Das Fenster Anspruchsregeln bearbeiten wird geöffnet:



Schritt 11. Klicken Sie in diesem Fenster auf **Regel hinzufügen**.

Schritt 12: Wählen Sie als **Anspruchsregelvorlage LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.

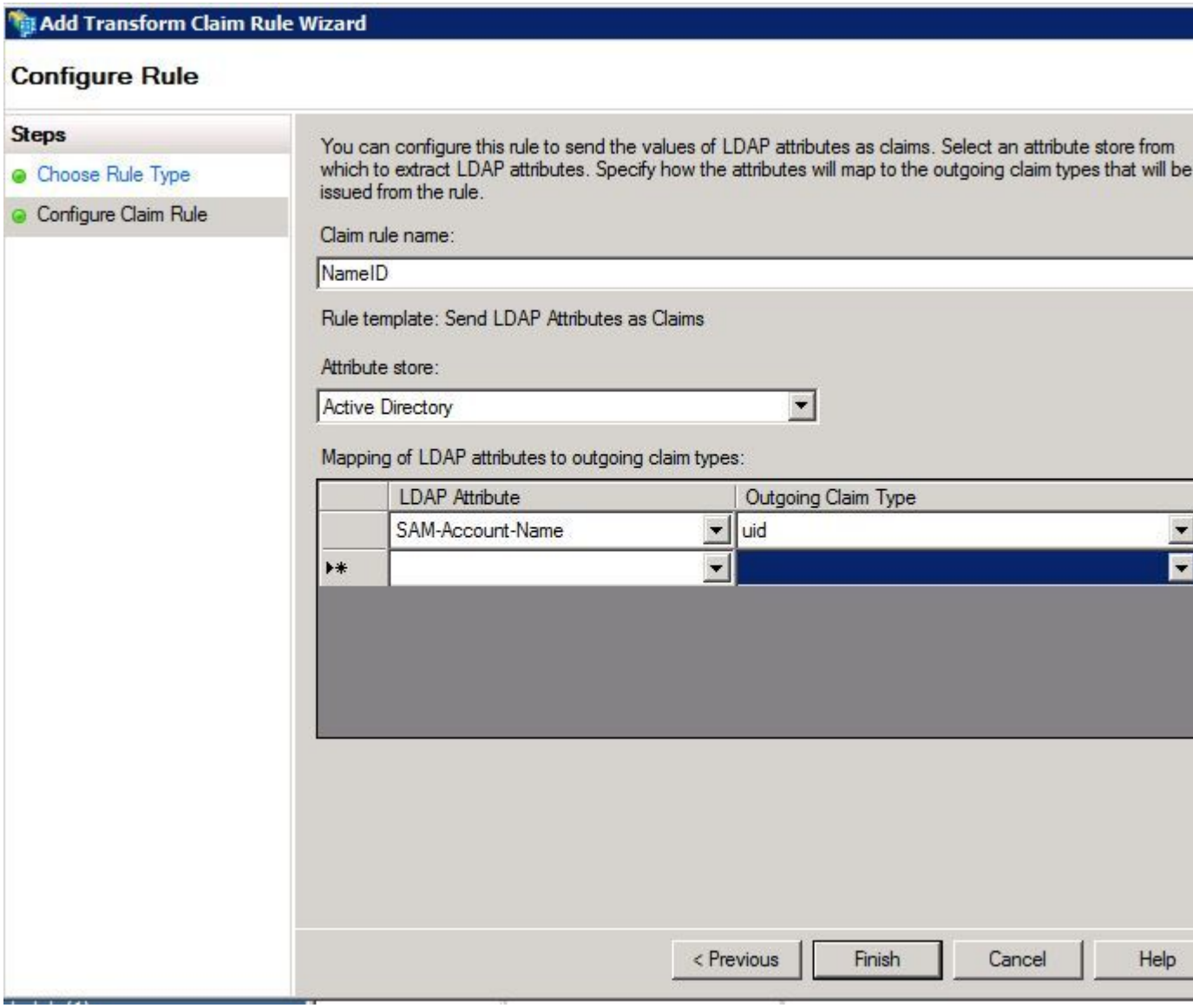
Schritt 13: Geben Sie auf der nächsten Seite **NameID** für den **Namen** der **Anspruchsregel ein**.

Schritt 14: Wählen Sie **Active Directory** für den **Attributspeicher aus**.

Schritt 15: Wählen Sie **SAM-Kontoname** als **LDAP-Attribut**.

Schritt 16: Geben Sie **UID** für den **ausgehenden Forderungstyp ein**.

Hinweis: uid ist keine Option in der Dropdown-Liste - es muss manuell eingegeben werden.



Schritt 17: Klicken Sie auf Beenden.

Schritt 18: Die erste Regel ist nun abgeschlossen. Klicken Sie erneut auf **Regel hinzufügen**.

Schritt 19: Wählen Sie **Anträge mithilfe einer benutzerdefinierten Regel senden aus**.

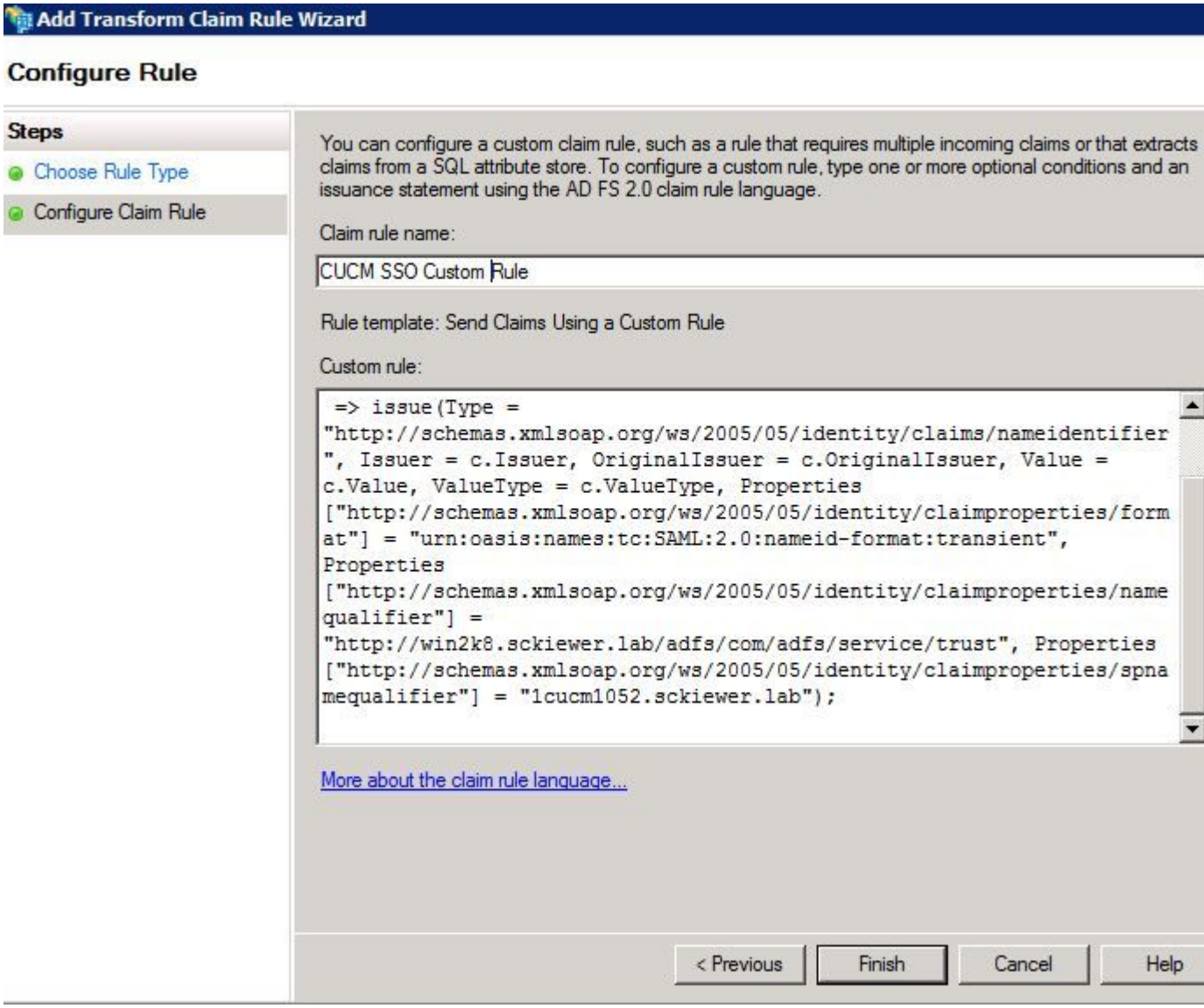
Schritt 20: Geben Sie einen **Namen für die Anspruchsregel ein**.

Schritt 21: Fügen Sie im Feld **Benutzerdefinierte Regel** den folgenden Text ein:

c:[Geben Sie == "http://schemas.microsoft.com/ws/2008/06/identity/Claims/windowsaccountname"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/cltargets/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/namequalifier"] = "http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "CUCM_ENTITY_ID");

Schritt 22: Stellen Sie sicher, dass Sie AD_FS_SERVICE_NAME und CUCM_ENTITY_ID in die entsprechenden Werte ändern.

Hinweis: Wenn Sie sich nicht sicher sind, wie der AD FS-Servicename lautet, können Sie die Schritte für die Suche ausführen. Die CUCM-Element-ID kann aus der ersten Zeile der CUCM-Metadatendatei abgerufen werden. In der ersten Zeile der Datei befindet sich eine entityID=1cucm1052.sckiewer.lab. Sie müssen den unterstrichenen Wert in den entsprechenden Abschnitt der Anspruchsregel eingeben.



Schritt 23: Klicken Sie auf Beenden.

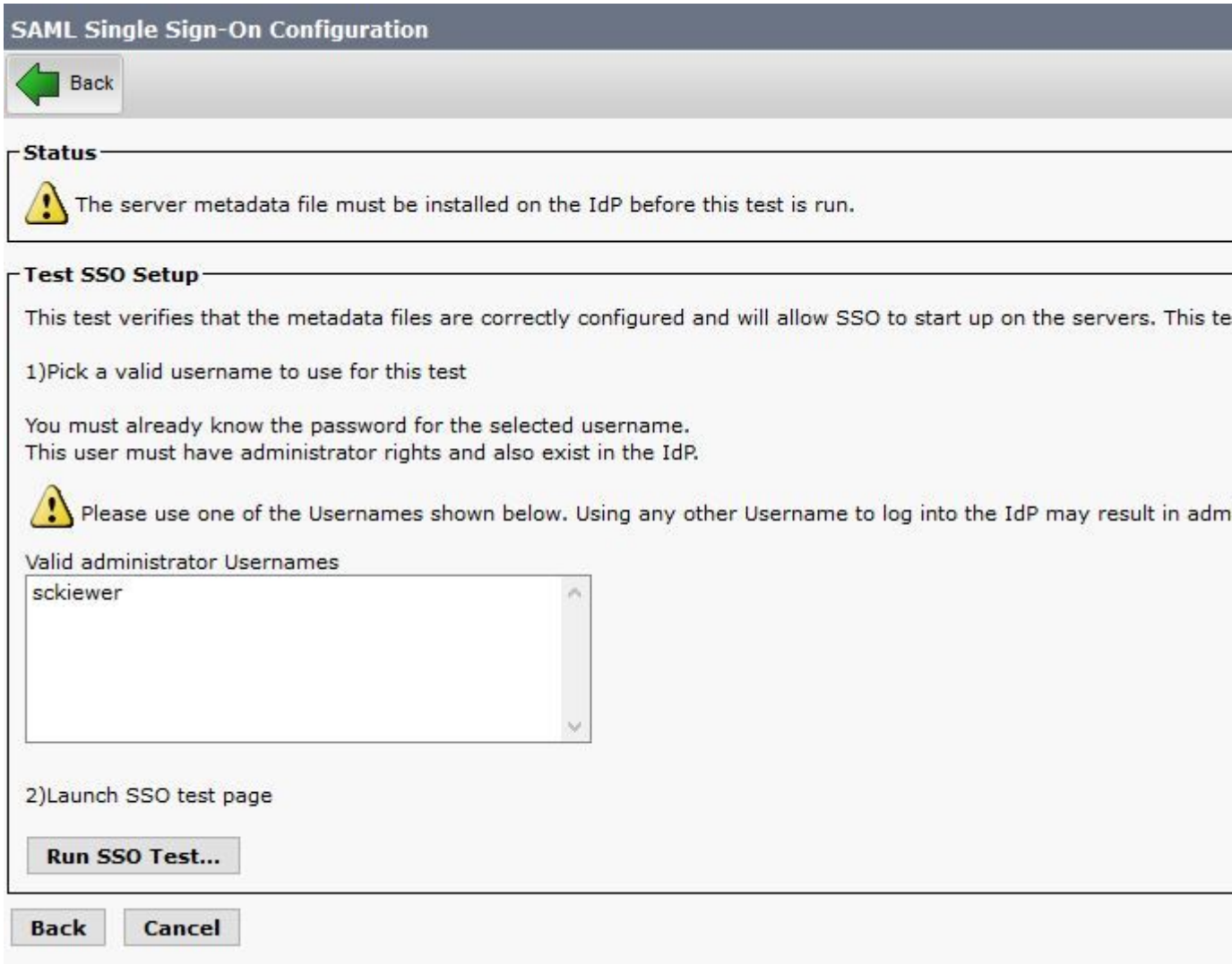
Schritt 24: Klicken Sie auf OK.

Hinweis: Anspruchsregeln sind für alle Unified Collaboration-Server erforderlich, auf denen Sie SSO verwenden möchten.

Beenden der SSO-Aktivierung auf dem CUCM und Durchführen des SSO-Tests

Schritt 1: Nachdem der AD FS-Server vollständig konfiguriert ist, können Sie zum CUCM zurückkehren.

Schritt 2: Sie haben auf der letzten Konfigurationsseite aufgehört:



Schritt 3: Wählen Sie den Endbenutzer aus, für den die **Standard-CCM-**Benutzerrolle "**Super Users**" ausgewählt ist, und klicken Sie auf **Run SSO Test (SSO-Test ausführen).**

Schritt 4: Stellen Sie sicher, dass Ihr Browser Popups zulässt, und geben Sie Ihre Anmeldeinformationen in die Eingabeaufforderung ein.

Schritt 5: Klicken Sie im Popup-Fenster auf **Schließen** und dann auf **Fertig stellen**.

Schritt 6: Nach einem kurzen Neustart der Webanwendungen ist SSO aktiviert.

Fehlerbehebung

SSO-Protokolle auf Debugging festlegen

Um die SSO-Protokolle als debug festzulegen, müssen Sie diesen Befehl in der CLI des CUCM ausführen: **set sam trace level debug**

Die SSO-Protokolle können von RTMT heruntergeladen werden. Der Name des Protokollsatzes lautet **Cisco SSO**.

Verbunddienstnamen suchen

Um den Namen des Verbunddiensts zu finden, klicken Sie auf **Start**, und suchen Sie nach **AD FS 2.0 Management**.

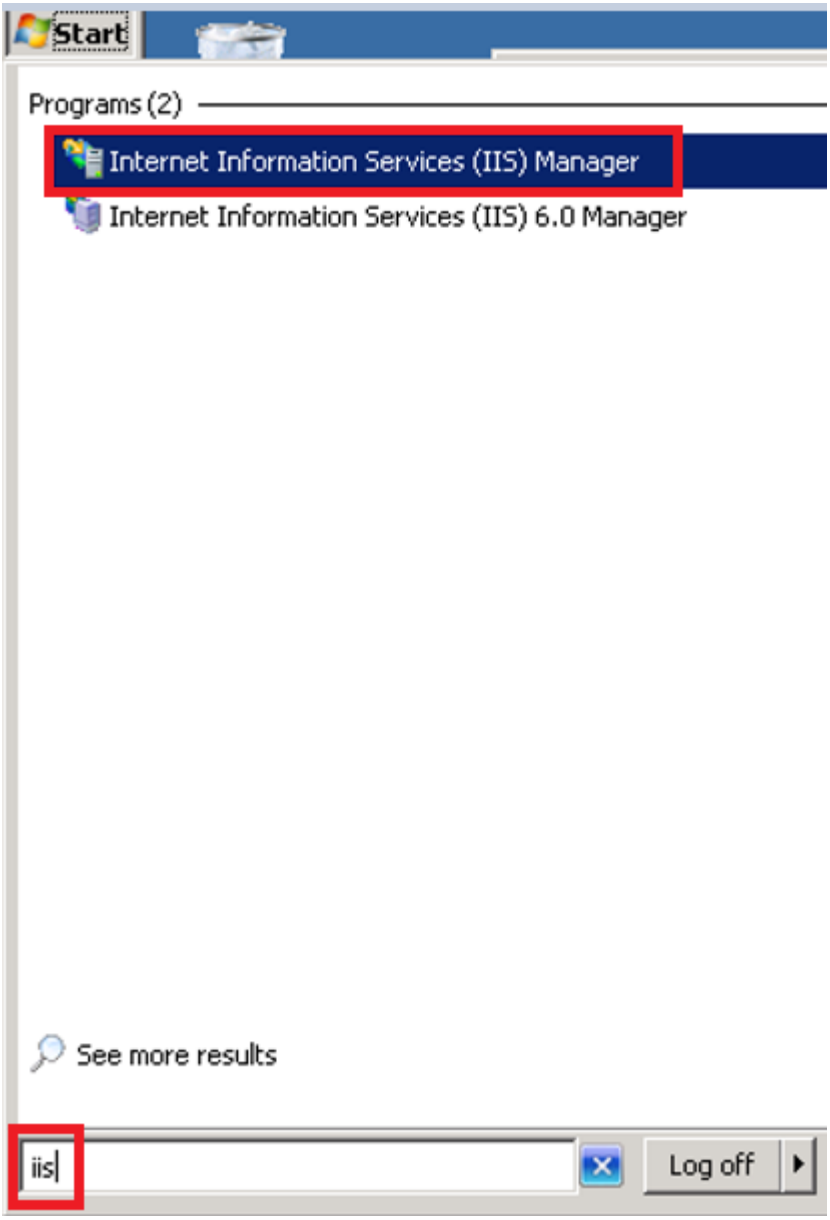
ãƒ» Klicken Sie auf **Verbunddiensteigenschaften** bearbeiten**...**
ãƒ» Suchen Sie auf der Registerkarte "Allgemein" nach dem **Namen des Verbunddiensts.**

Name des Zertifikats und Verbunddiensts ohne Punkte

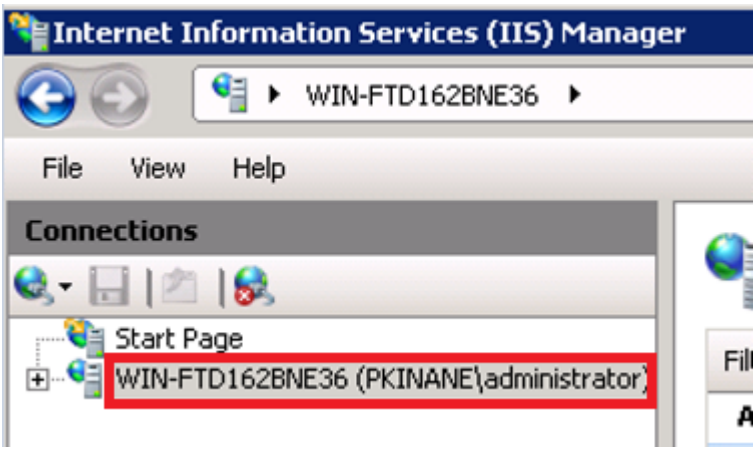
Wenn Sie diese Fehlermeldung im AD FS-Konfigurationsassistenten erhalten, müssen Sie ein neues Zertifikat erstellen.

Das ausgewählte Zertifikat kann nicht zum Ermitteln des Verbunddienstnamens verwendet werden, da das ausgewählte Zertifikat einen dotless (short-names) Subject-Namen hat. Wählen Sie ein anderes Zertifikat ohne einen dotless (short-names) Subject-Namen aus, und versuchen Sie es dann erneut.

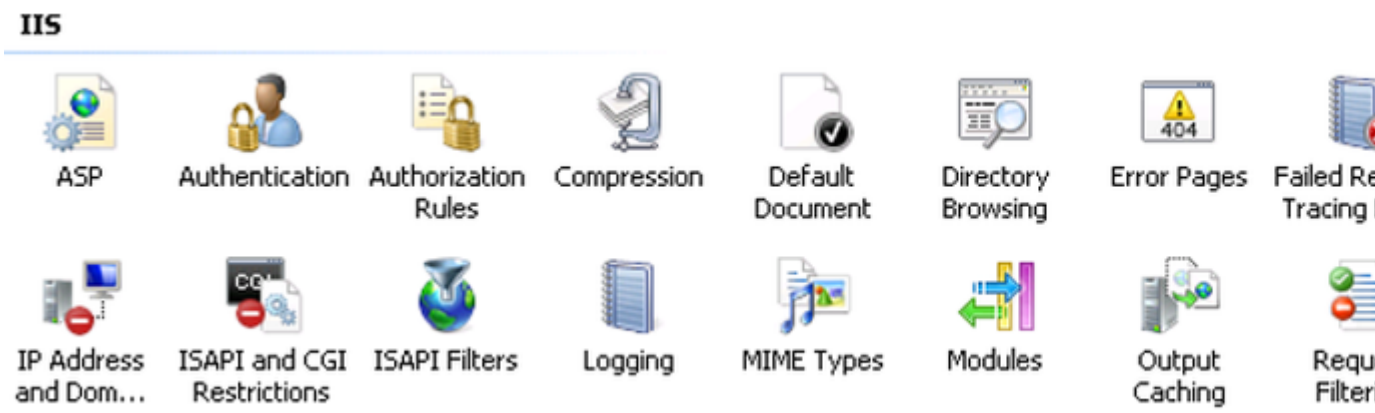
Schritt 1: Klicken Sie auf Start, suchen Sie nach, und öffnen Sie dann den Internetinformationsdienste-Manager (IIS).



Schritt 2: Klicken Sie auf den Namen Ihres Servers.

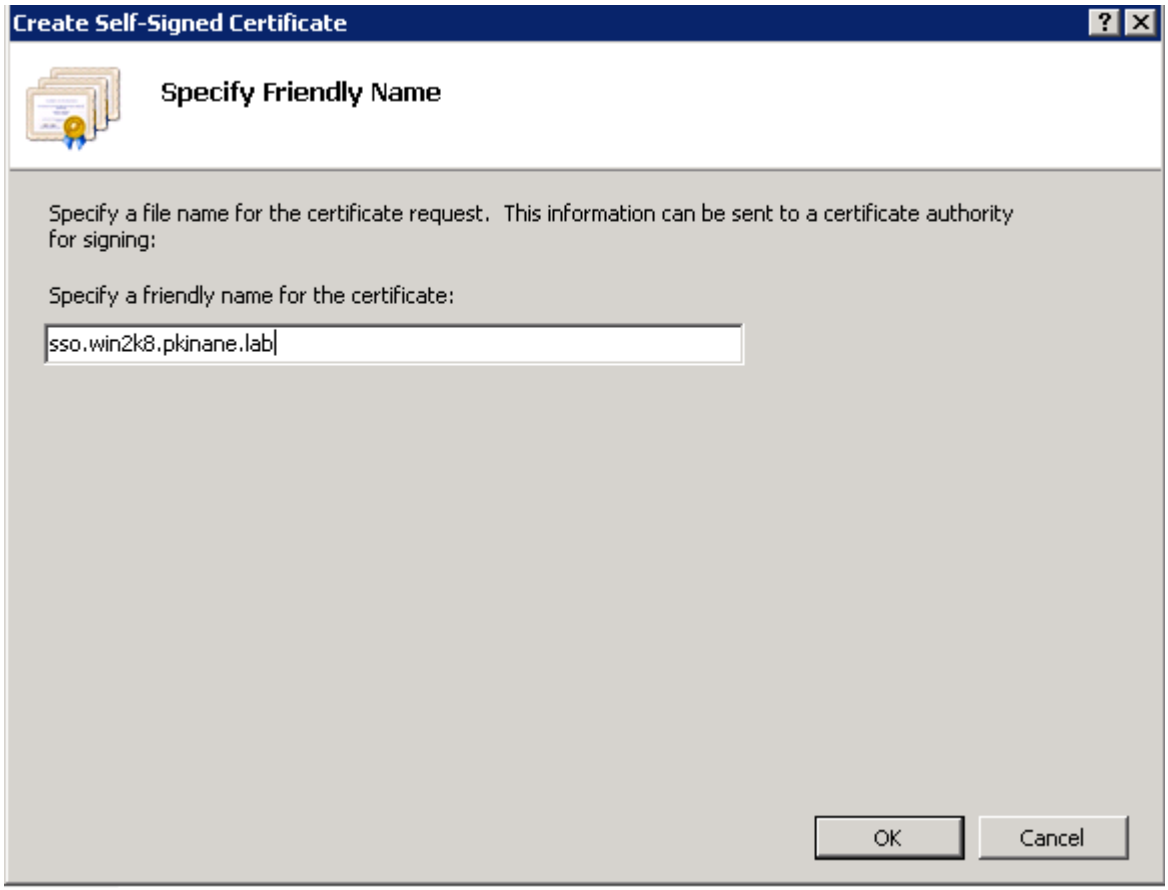


Schritt 3: Klicken Sie auf Serverzertifikate.



Schritt 4: Klicken Sie auf Selbstsigniertes Zertifikat erstellen.

Schritt 5: Geben Sie den gewünschten Namen für den Alias Ihres Zertifikats ein.



Die Zeit ist nicht synchron zwischen dem CUCM- und dem IDP-Server.

Wenn dieser Fehler beim Ausführen des SSO-Tests vom CUCM auftritt, müssen Sie den Windows-Server so konfigurieren, dass er die gleichen NTP-Server wie der CUCM verwendet.

Ungültige SAML-Antwort. Dies kann verursacht werden, wenn die Zeit zwischen dem Cisco Unified Communications Manager und den IDP-Servern nicht mehr synchron ist. Überprüfen Sie die NTP-Konfiguration auf beiden Servern. Führen Sie "utils ntp status" in der CLI aus, um diesen Status in Cisco Unified Communications Manager zu überprüfen.

Wenn auf dem Windows-Server die richtigen NTP-Server angegeben wurden, müssen Sie einen weiteren SSO-Test durchführen und überprüfen, ob das Problem weiterhin besteht. In einigen Fällen ist es notwendig, die Gültigkeitsdauer der Aussage zu verzerren. Nähere Einzelheiten zu diesem Prozess finden Sie hier.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.