Konfigurieren von SAML SSO auf Cisco Unified Communications Manager mit ADFS 3.0

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Konfiguration der einmaligen Anmeldung mit dem Active Directory Federation Service (ADFS 3.0) unter Verwendung von Windows 2012 R2 auf Cisco Unified Communication Manager (CUCM), Cisco Unity Connection (CUC) und Expressway-Produkten. Schritte zur Konfiguration von Kerberos sind ebenfalls in diesem Dokument enthalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit Single Sign-On (SSO)- und Windows-Produkten vertraut sind.

Verwendete Komponenten

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

- CUCM 11,5
- CUC 11,5
- Expressway 12
- Windows 2012 R2 Server mit folgenden Rollen:
  - Active Directory-Zertifikatsdienste
  - Active Directory-Verbandsdienste

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 potenziellen Auswirkungen eines Befehls verstehen.

Konfigurationsvorprüfung

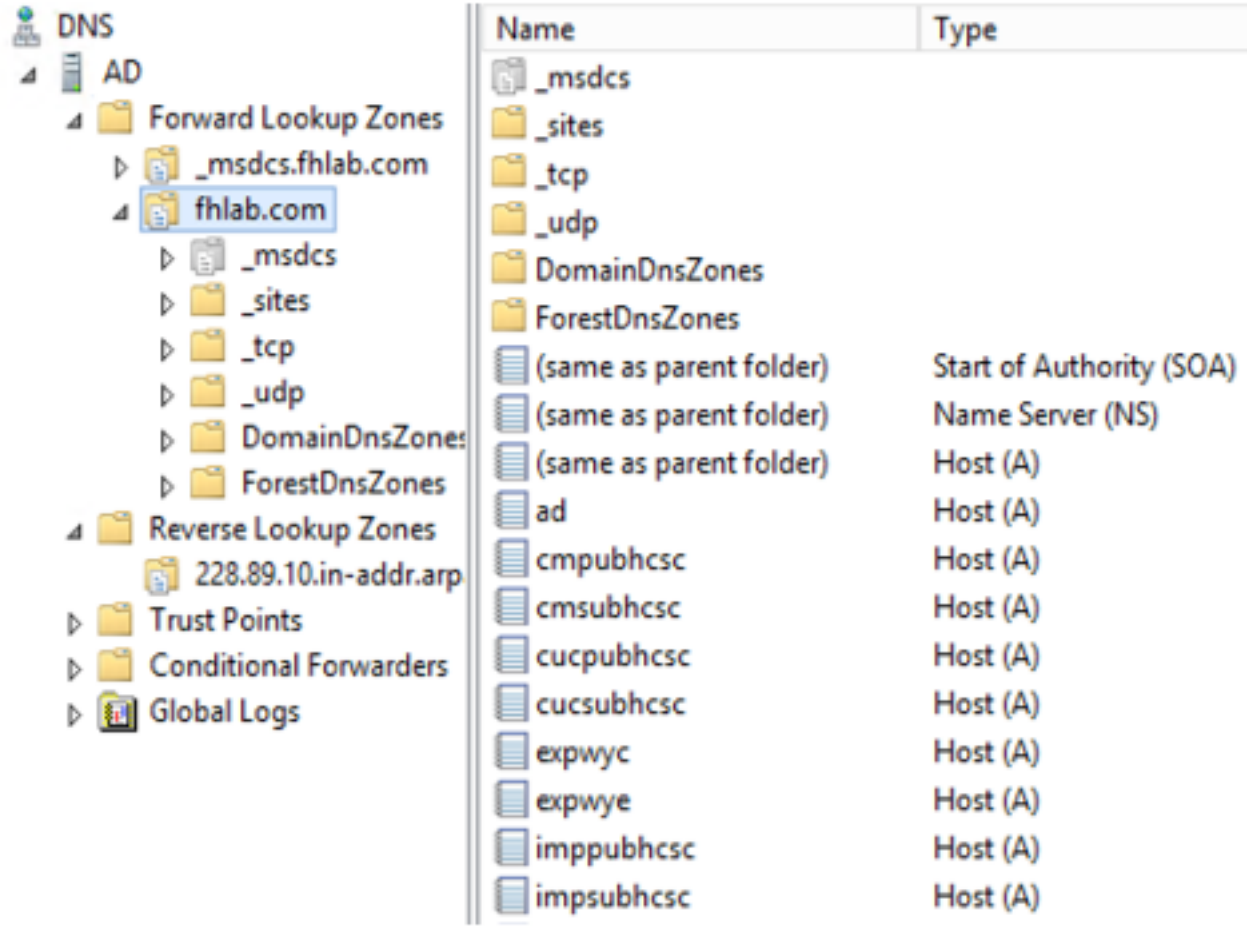
Vor der Installation von ADFS3 müssen diese Serverrollen bereits in der Umgebung vorhanden sein:

·Domänencontroller und DNS

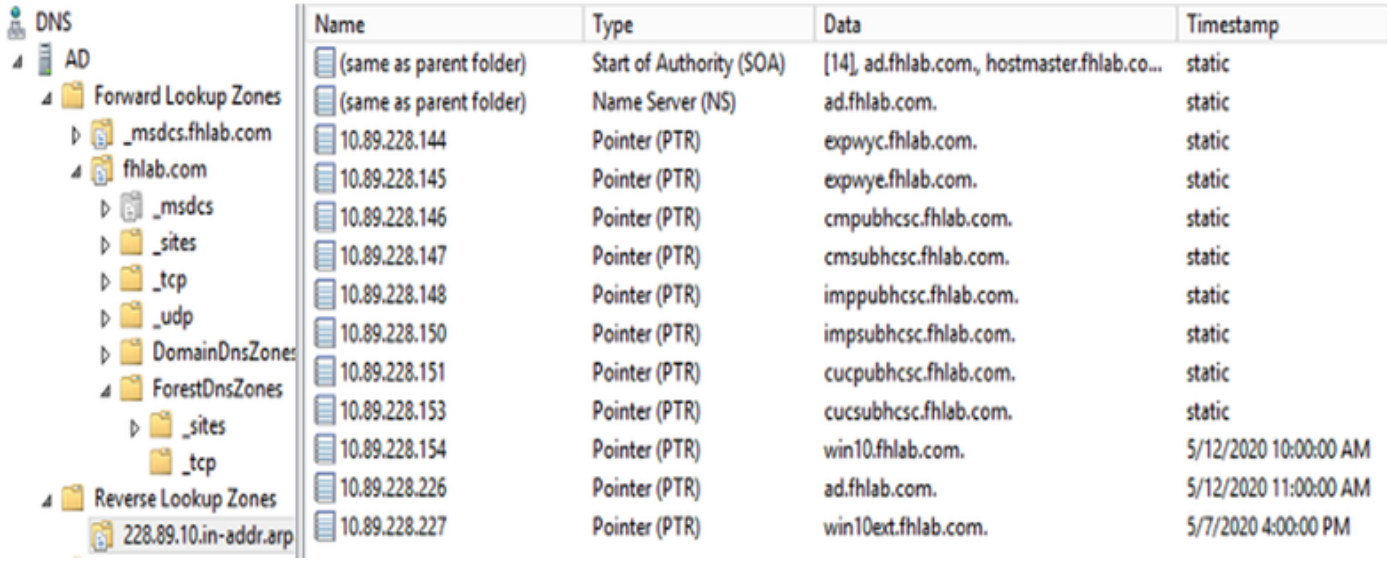
·Alle Server müssen als A-Datensätze zusammen mit ihrem Zeigerdatensatz (ein DNS-Datensatz, der eine IP-Adresse in eine Domäne oder einen Hostnamen auflöst) hinzugefügt werden.

A Datensätze

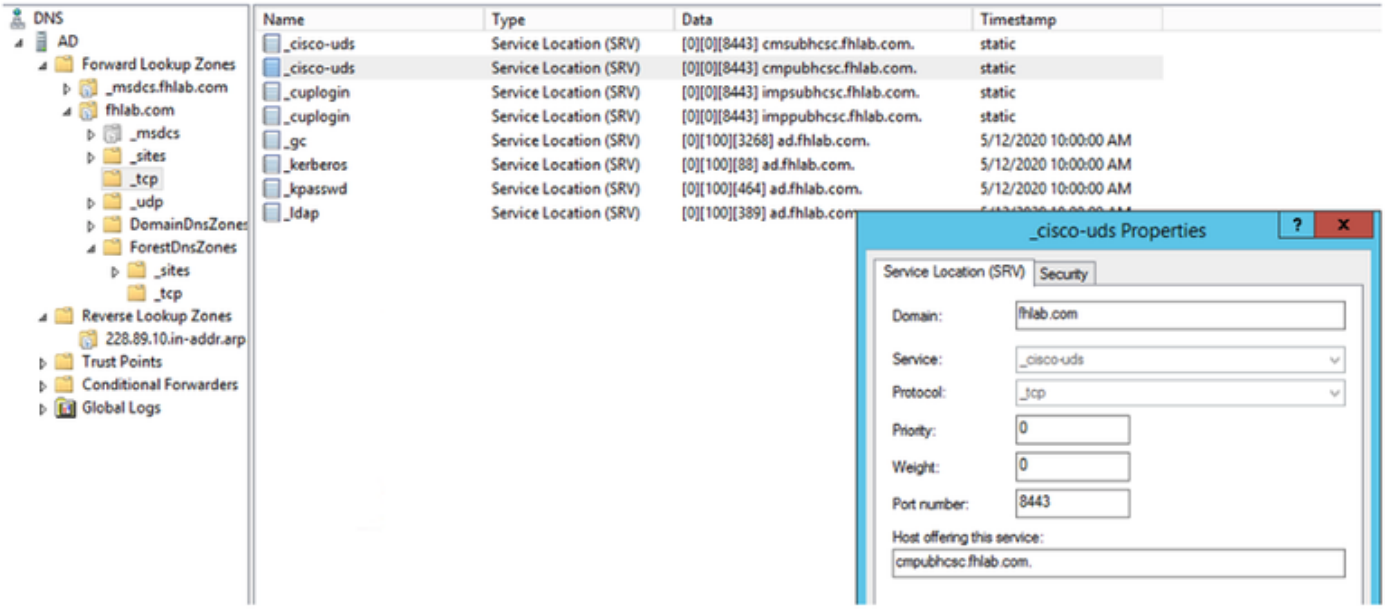
In fhlab.com. hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc und imsubhcsc wurden hinzugefügt.



PTR-Datensätze (Zeiger)

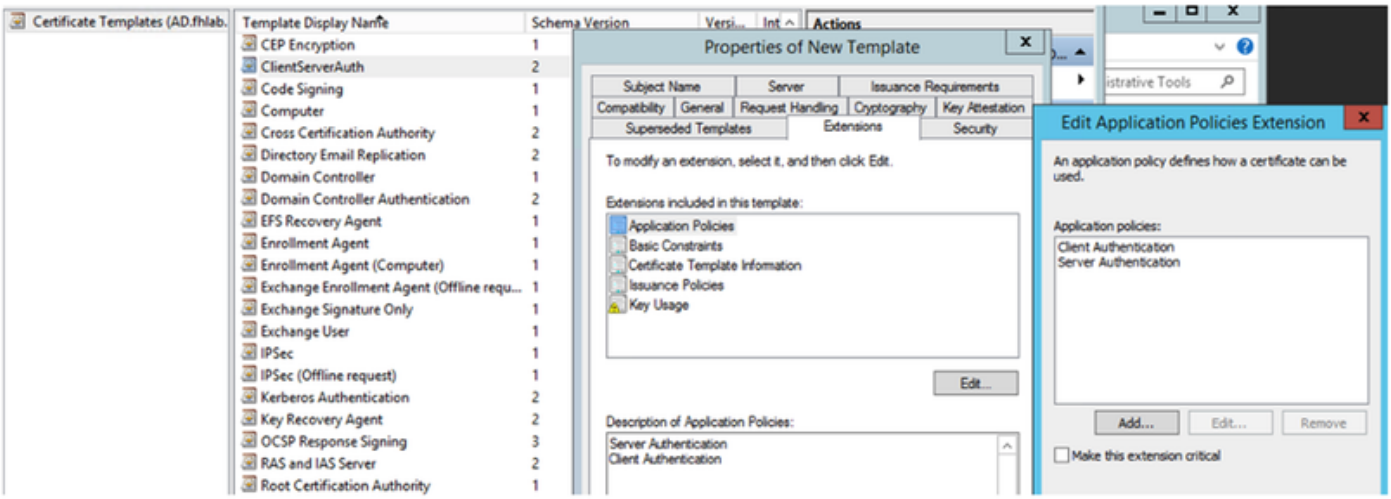


Für Jabber Discovery Services müssen SRV-Datensätze vorhanden sein.

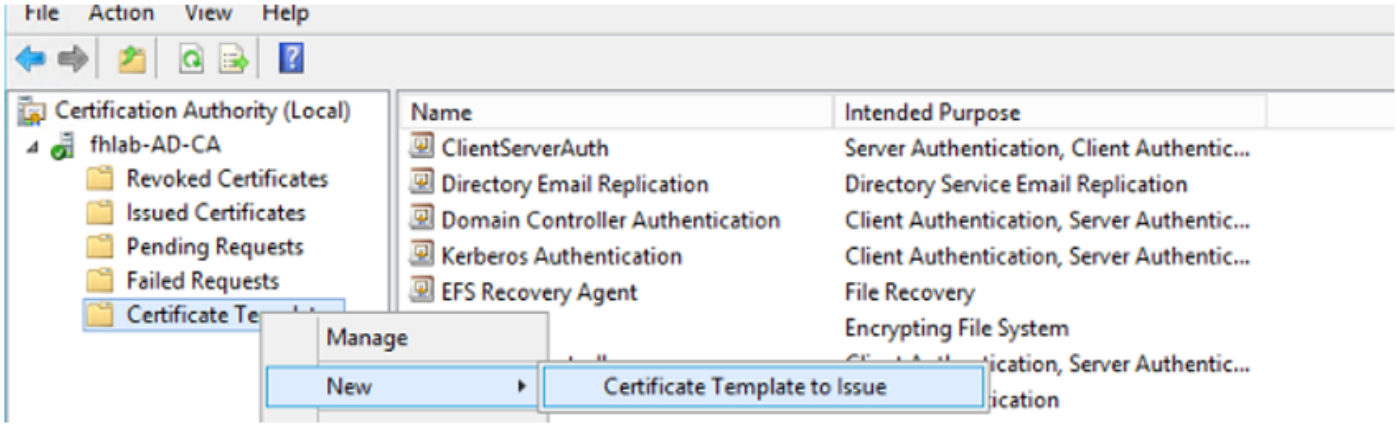


- Stammzertifizierungsstelle (vorausgesetzt, die Zertifikate werden von Enterprise CA signiert)

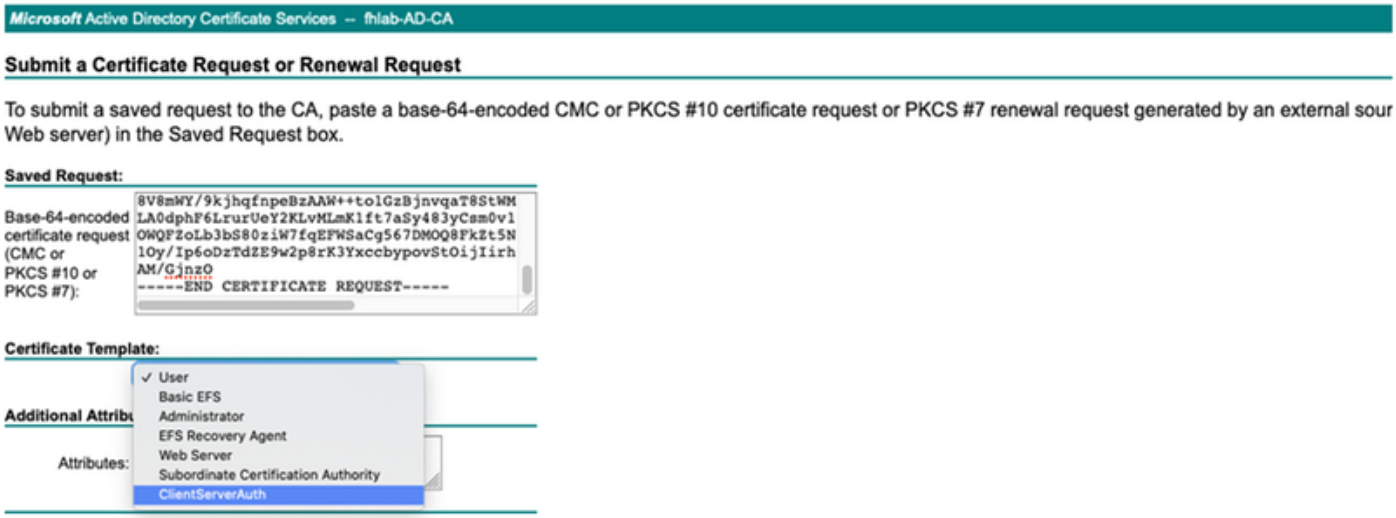
Eine Zertifikatsvorlage muss auf der Grundlage der Vorlage für das Webserverzertifikat erstellt werden. Erstere wird dupliziert, umbenannt und auf der Registerkarte Erweiterungen werden Anwendungsrichtlinien geändert, um eine Richtlinie für die Clientauthentifizierung hinzuzufügen. Diese Vorlage wird benötigt, um alle internen Zertifikate (CUCM, CUC, IMP und Expressway Core) in einer LAB-Umgebung zu signieren. Die interne Zertifizierungsstelle kann auch die Expressway E Certificate Signing Requests (CSR) unterzeichnen.



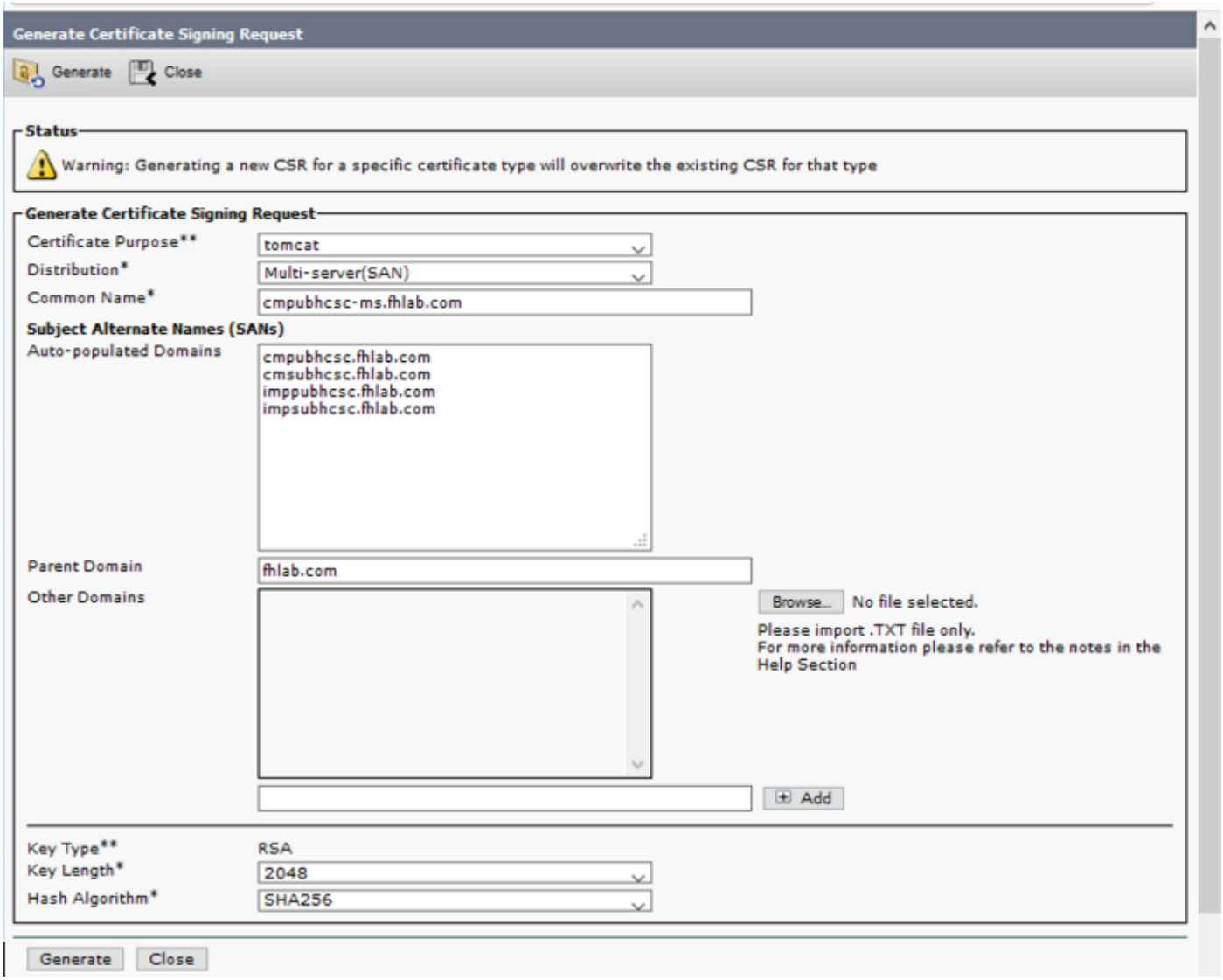
Die erstellte Vorlage muss ausgegeben werden, um CSR signieren zu können.



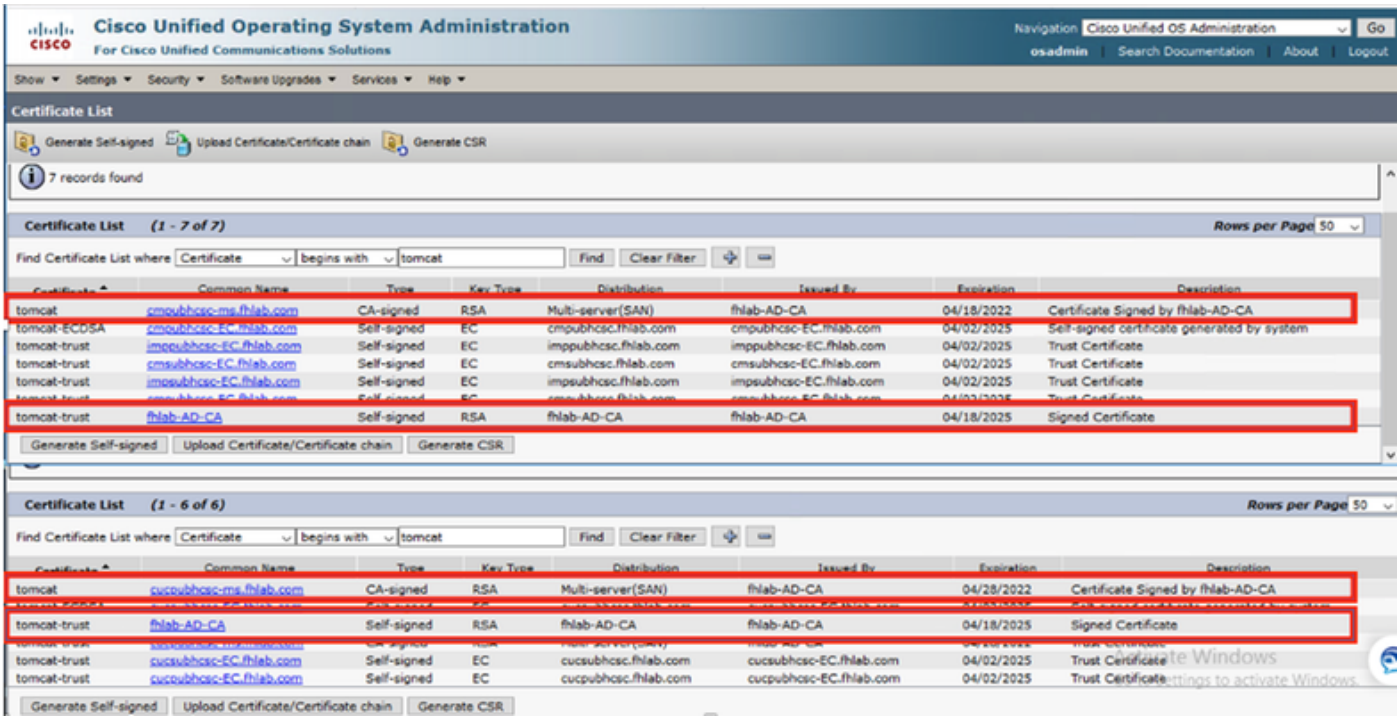
Wählen Sie im Zertifizierungsstellenzertifikat-Web die Vorlage aus, die zuvor erstellt wurde.



CUCM, IMP und CUC Multi-Server CSR müssen von der CA generiert und signiert werden. Der Zweck des Zertifikats muss "tomcat" sein.



Das CA-Stammzertifikat muss an Tomcat Trust und das signierte Zertifikat an Tomcat hochgeladen werden.



- IIS

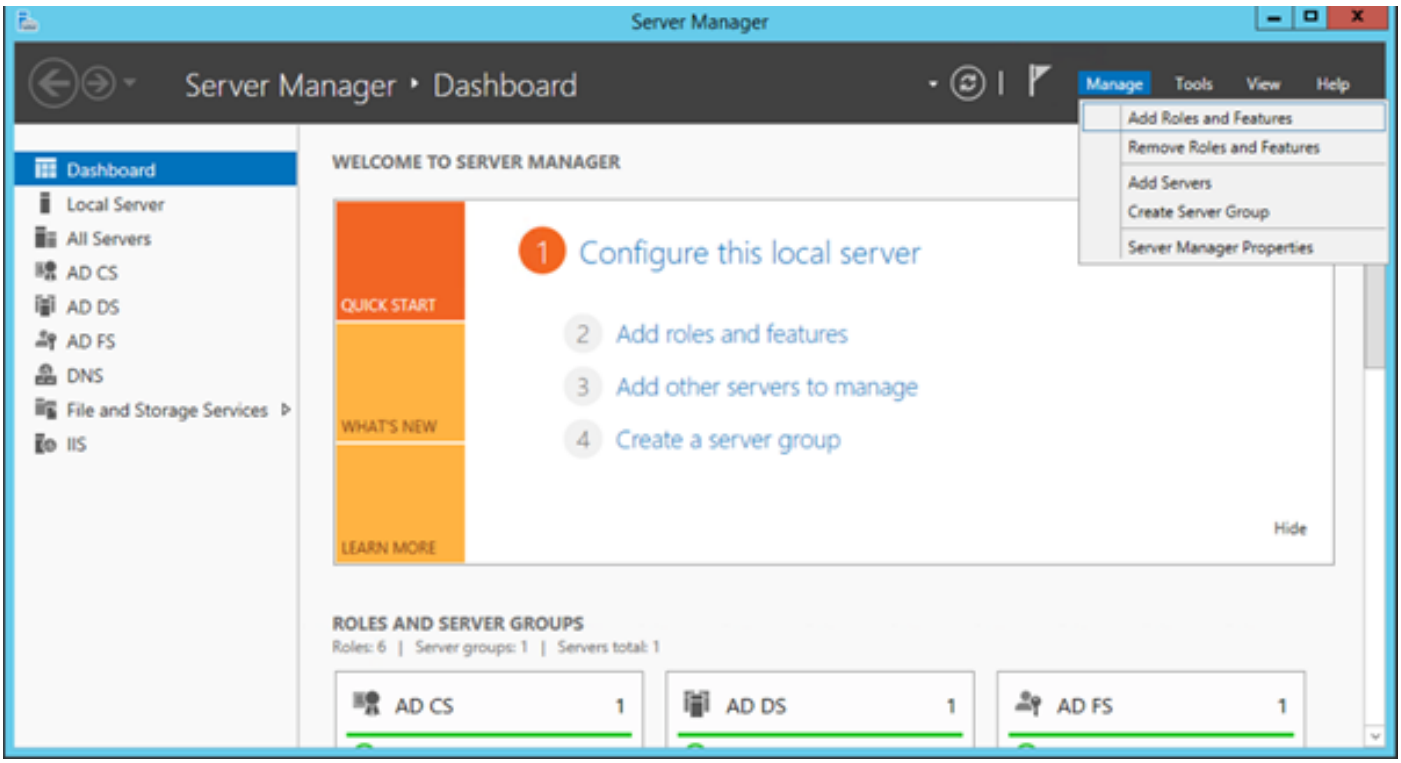
Andernfalls wird in diesem Abschnitt die Installation dieser Rollen beschrieben. Andernfalls

überspringen Sie diesen Abschnitt und fahren Sie direkt zum Download von ADFS3 von Microsoft.

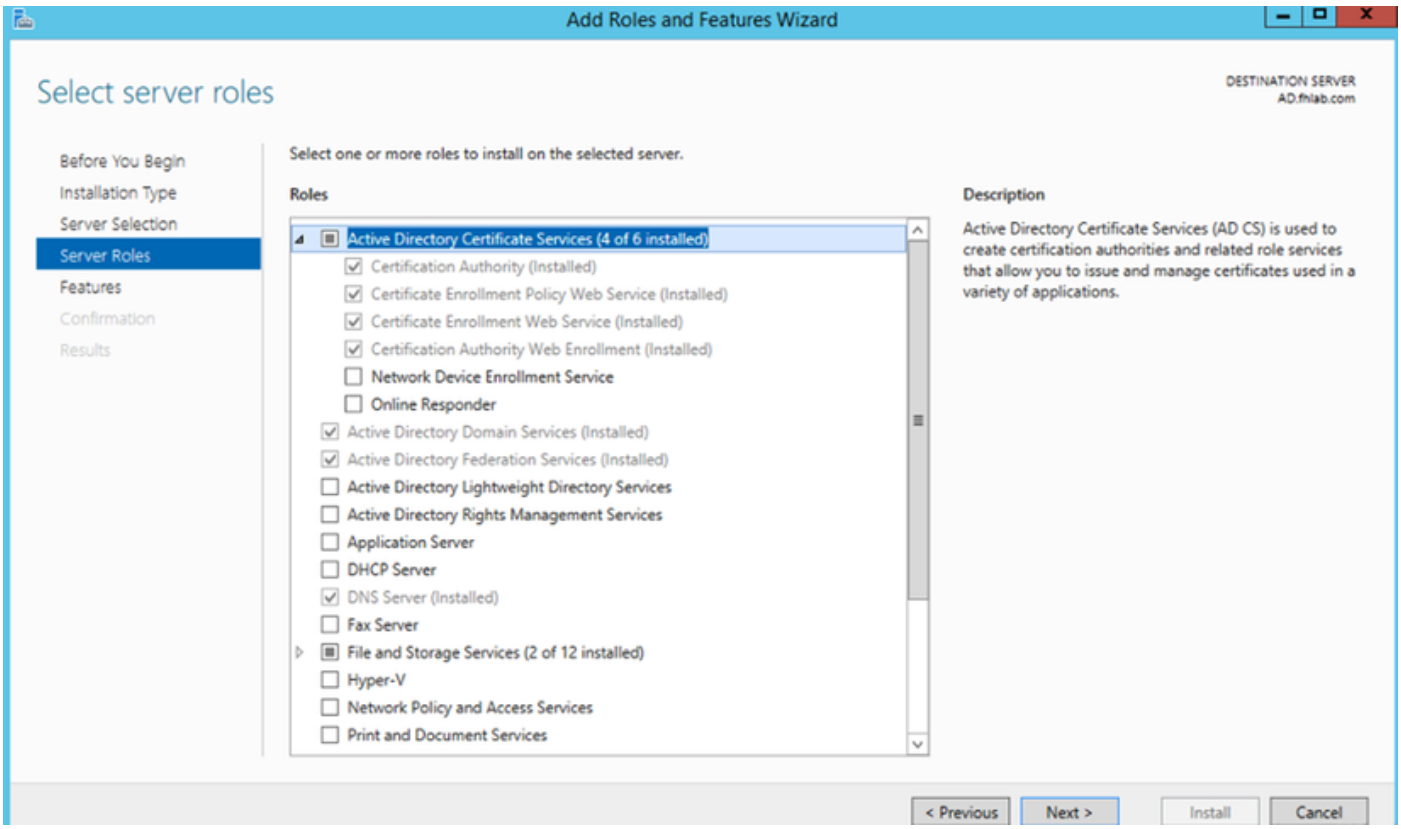
Nach der Installation von Windows 2012 R2 mit DNS können Sie den Server auf einen Domänencontroller verweisen.

Die nächste Aufgabe besteht in der Installation von Microsoft Certificate Services.

Navigieren Sie zum Server Manager, und fügen Sie eine neue Rolle hinzu:



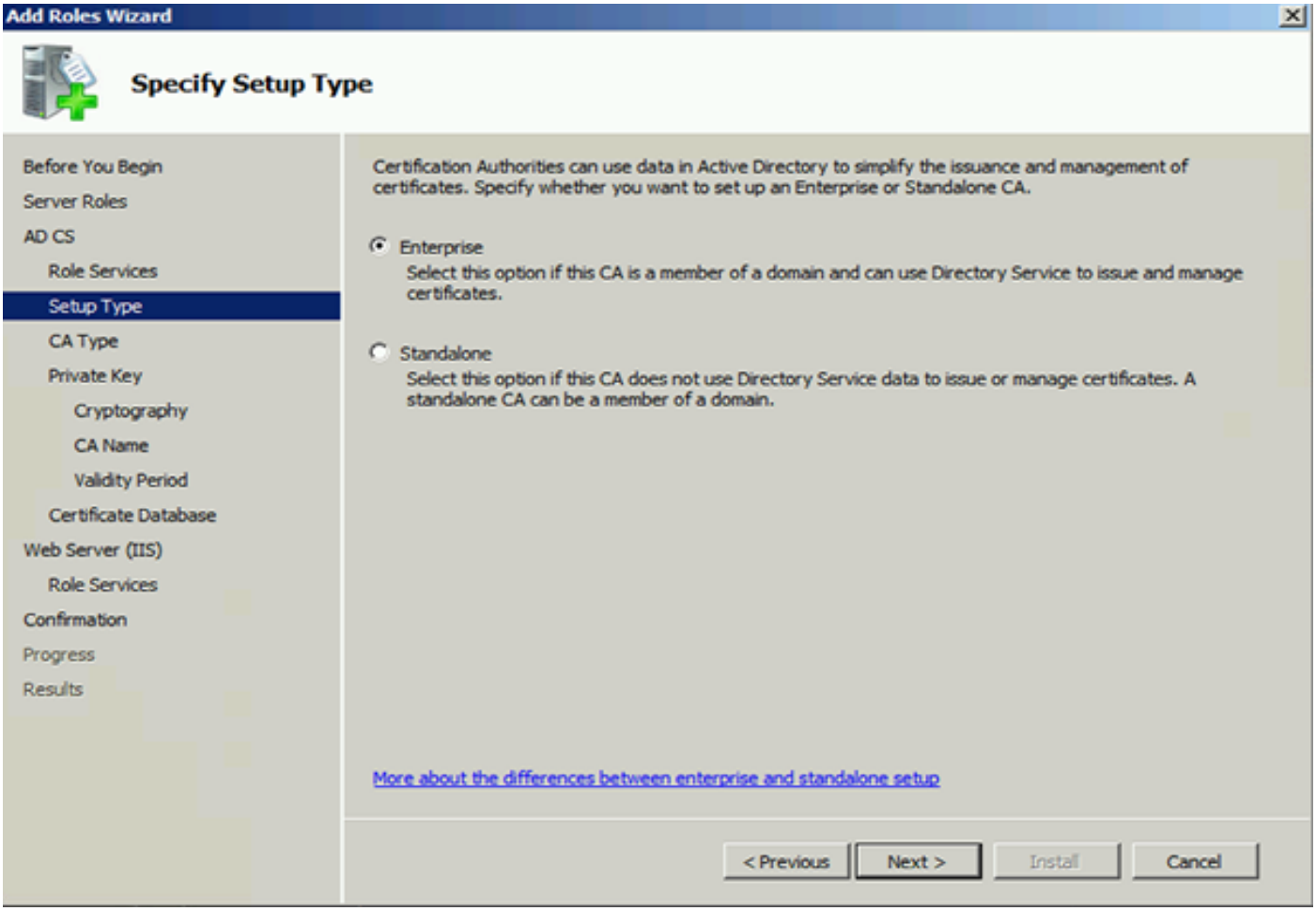
Wählen Sie die Rolle **Active Directory-Zertifikatdienste aus**.



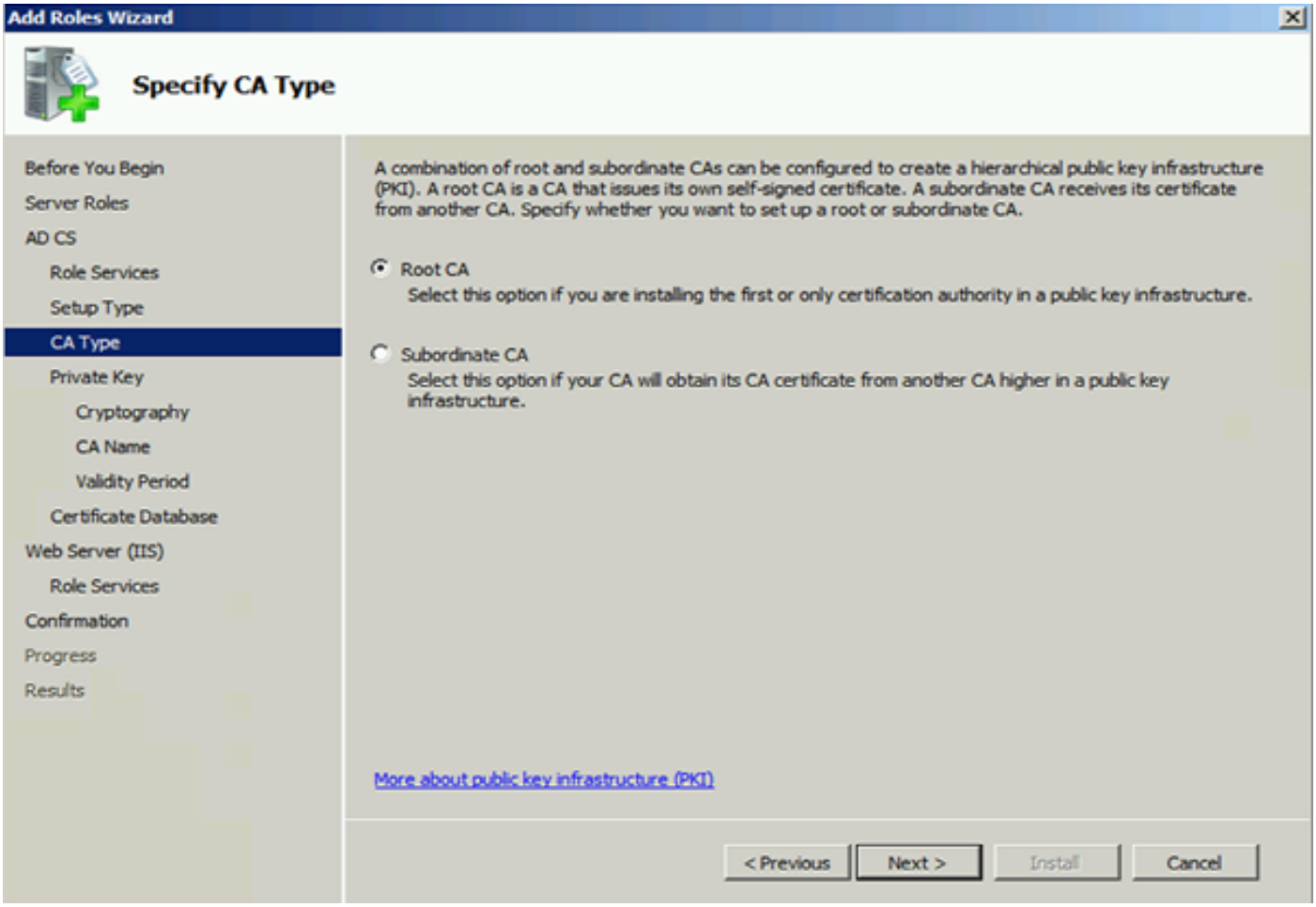
Stellen Sie diese Dienste bereit - Webdienst für die Zertifizierungsstellen-Registrierung für Zertifikatszertifikate. Nachdem diese beiden Rollen installiert wurden, konfigurieren Sie sie, und installieren Sie dann den **Webdienst für die Zertifikatregistrierung** und die **Webregistrierung der Zertifizierungsstelle**. Konfigurieren Sie sie.

Wenn die Zertifizierungsstelle installiert ist, werden auch zusätzliche Rollendienste und Features hinzugefügt, die erforderlich sind, z. B. IIS.

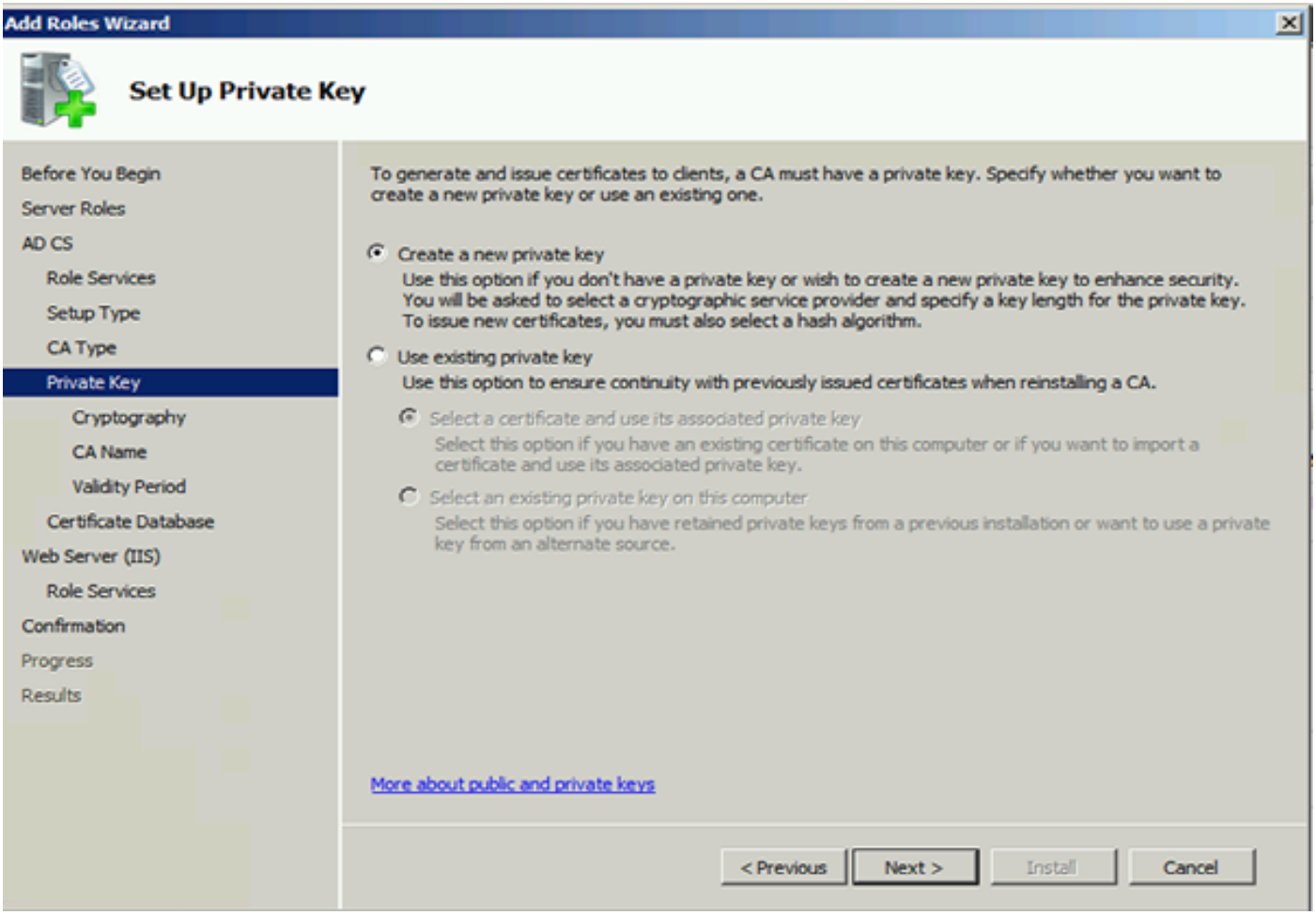
Je nach Bereitstellung können Sie Enterprise oder Standalone auswählen.



Für den CA-Typ können Sie die Root CA oder die untergeordnete CA auswählen. Wenn keine andere CA in der Organisation bereits ausgeführt wird, wählen Sie **Root CA (Stammzertifizierungsstelle)** aus.

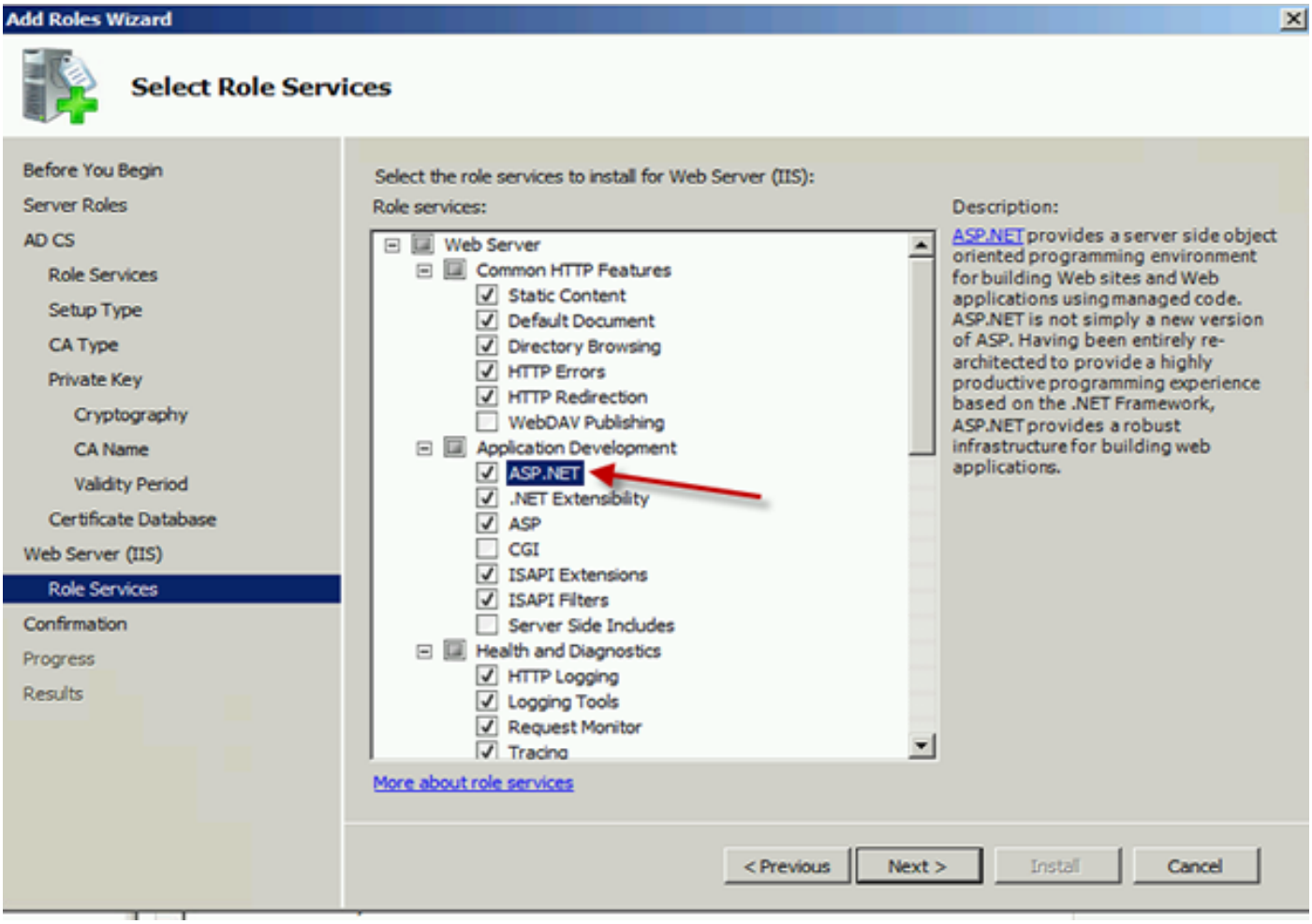


Im nächsten Schritt erstellen Sie einen privaten Schlüssel für Ihre CA.

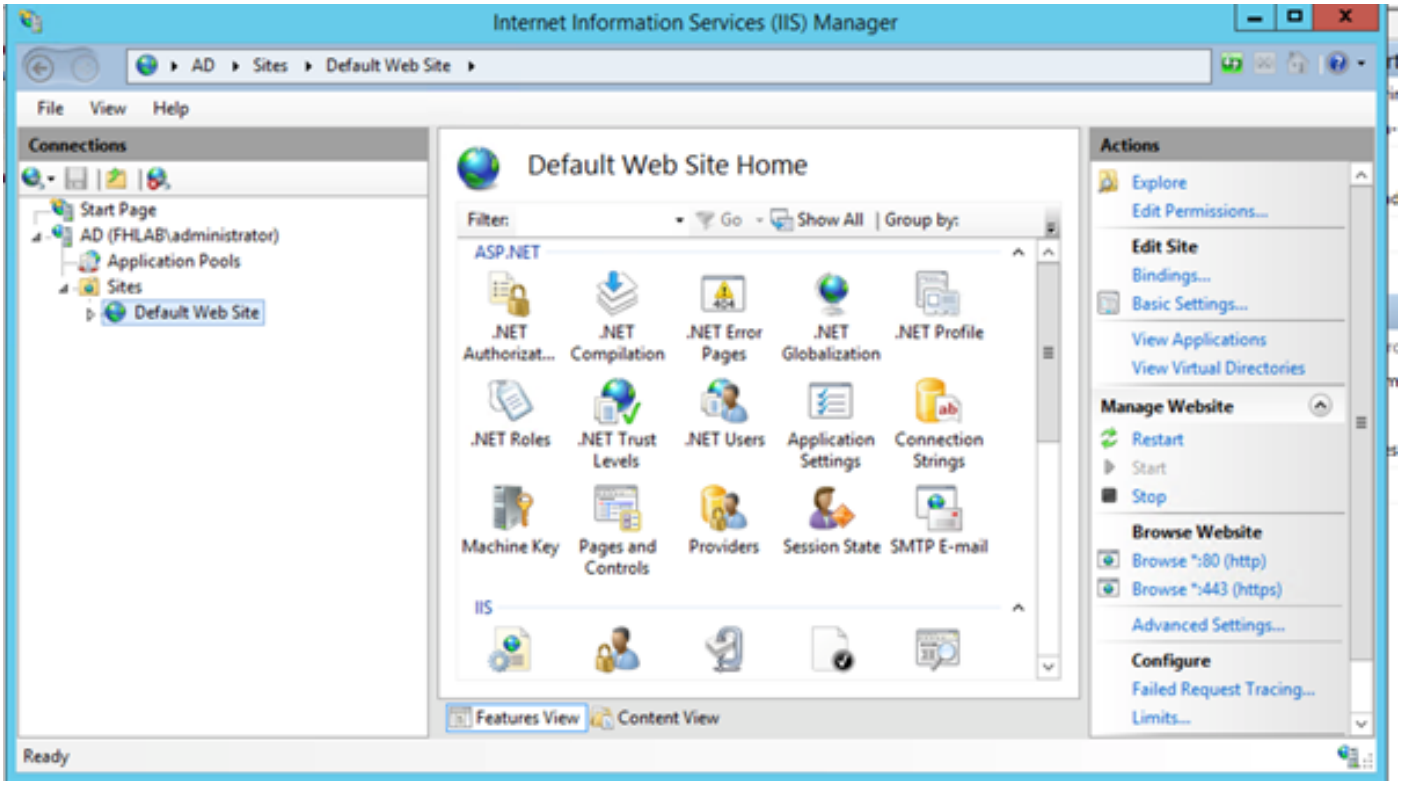


Dieser Schritt ist nur erforderlich, wenn Sie ADFS3 auf einem separaten Windows Server 2012

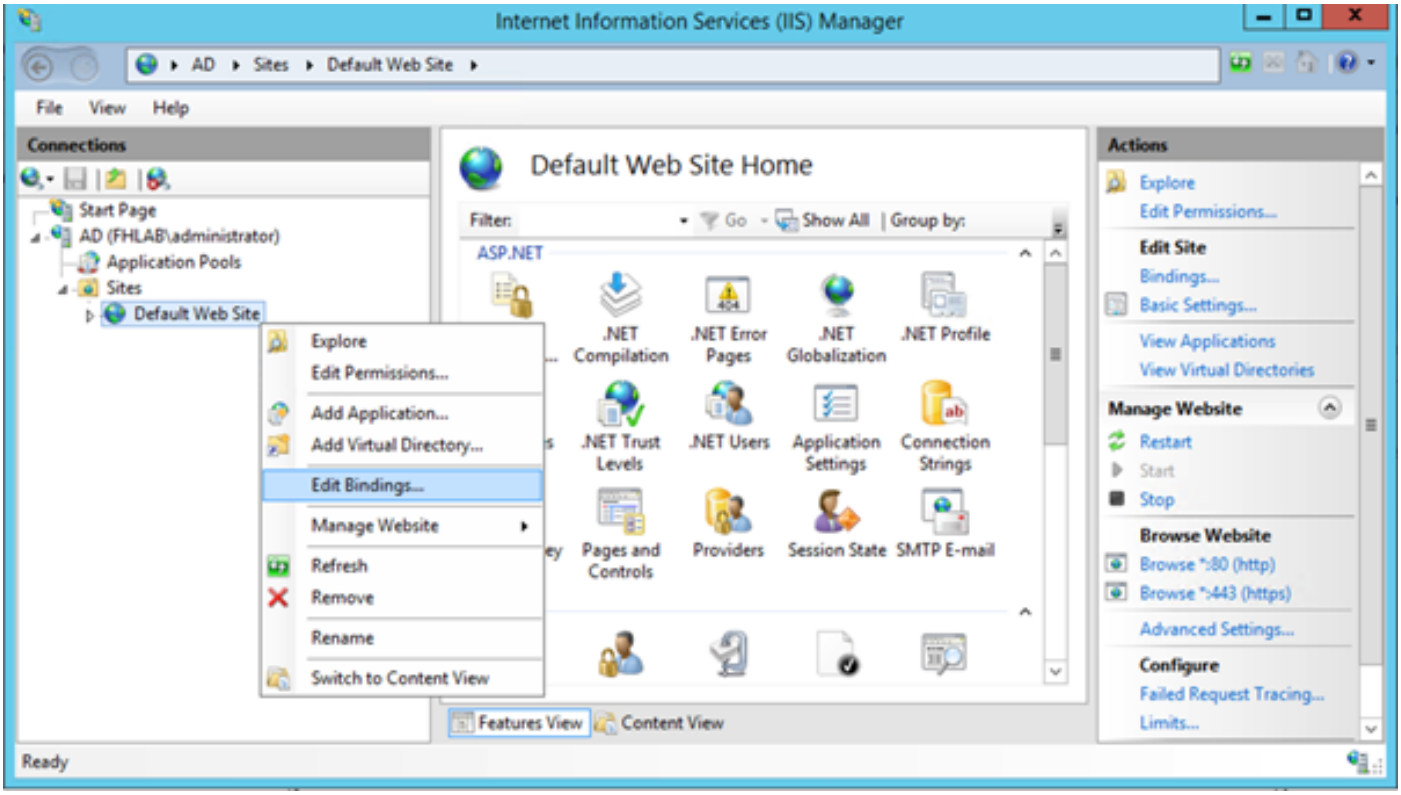
installieren. Nachdem Sie die CA konfiguriert haben, müssen die Rollendienste für IIS konfiguriert werden. Dies ist für die Webregistrierung in der CA erforderlich. Für die meisten ADFS-Bereitstellungen ist eine zusätzliche Rolle in IIS erforderlich, wenn Sie unter Anwendungsentwicklung auf **ASP.NET** klicken.



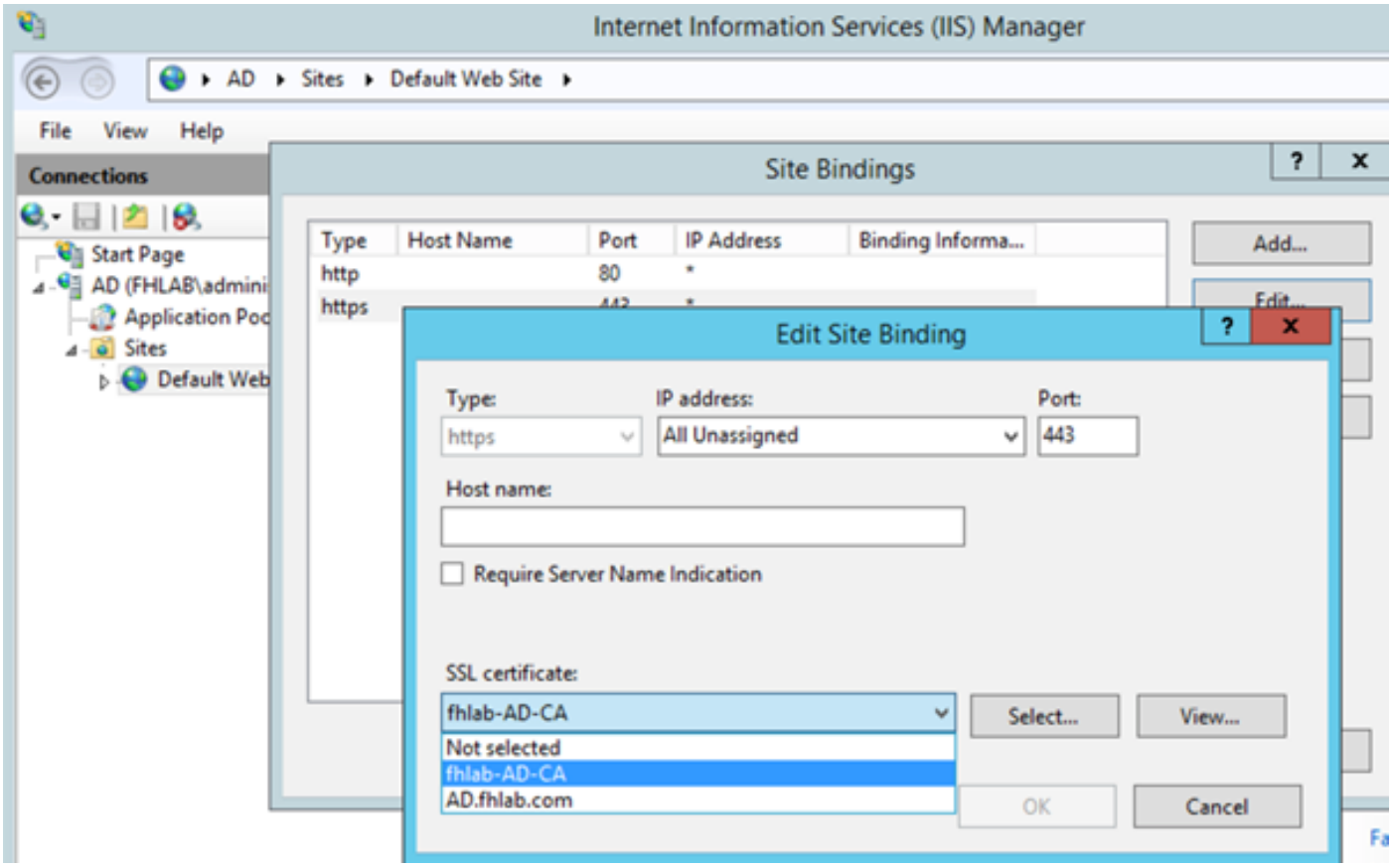
Klicken Sie im Server Manager auf **Webserver > IIS**, und klicken Sie dann mit der rechten Maustaste auf **Standardwebsite**. Die Binding muss geändert werden, um zusätzlich zu HTTP auch HTTPS zuzulassen. Dies geschieht zur Unterstützung von HTTPS.



Wählen Sie **Bindungen bearbeiten aus**.

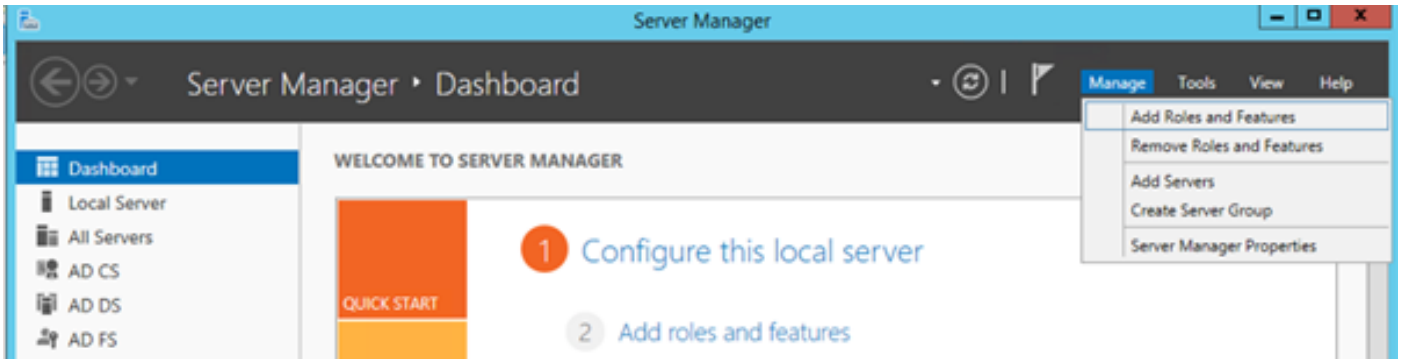


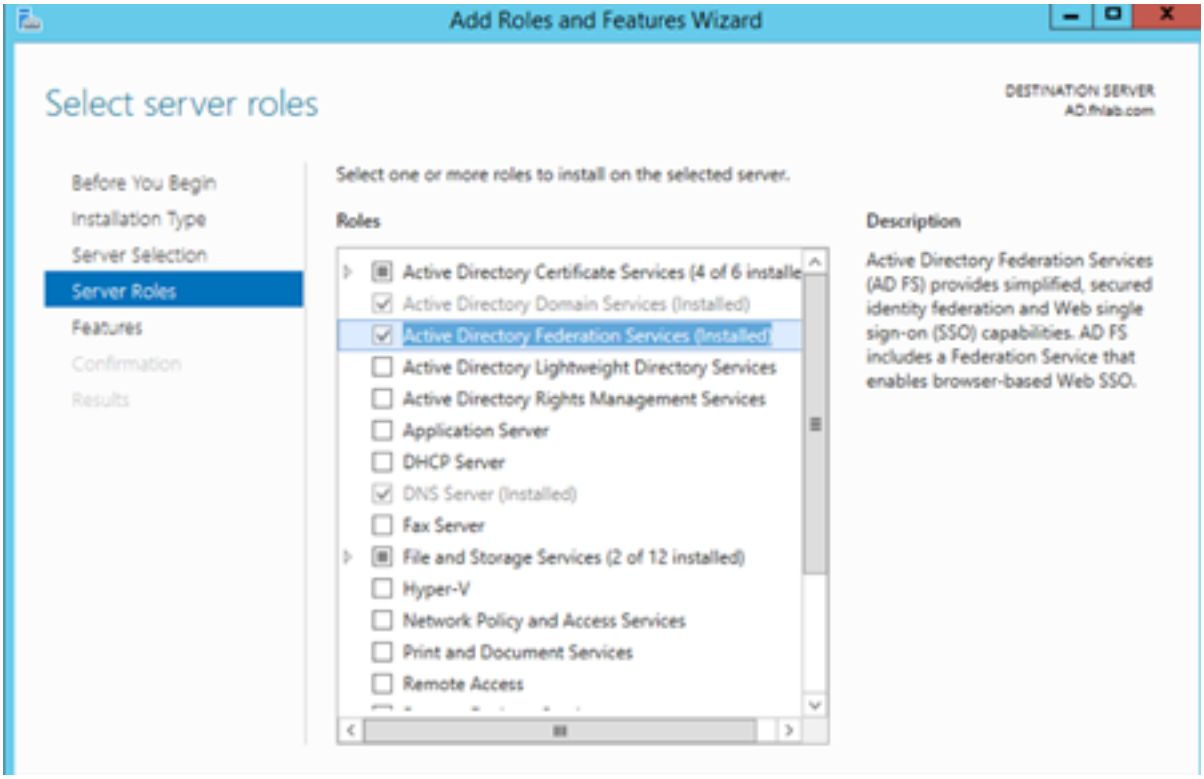
Fügen Sie eine neue Site Binding hinzu, und wählen Sie **HTTPS** als Typ aus. Wählen Sie für das SSL-Zertifikat das Serverzertifikat aus, das den gleichen FQDN wie Ihr AD-Server haben sollte.



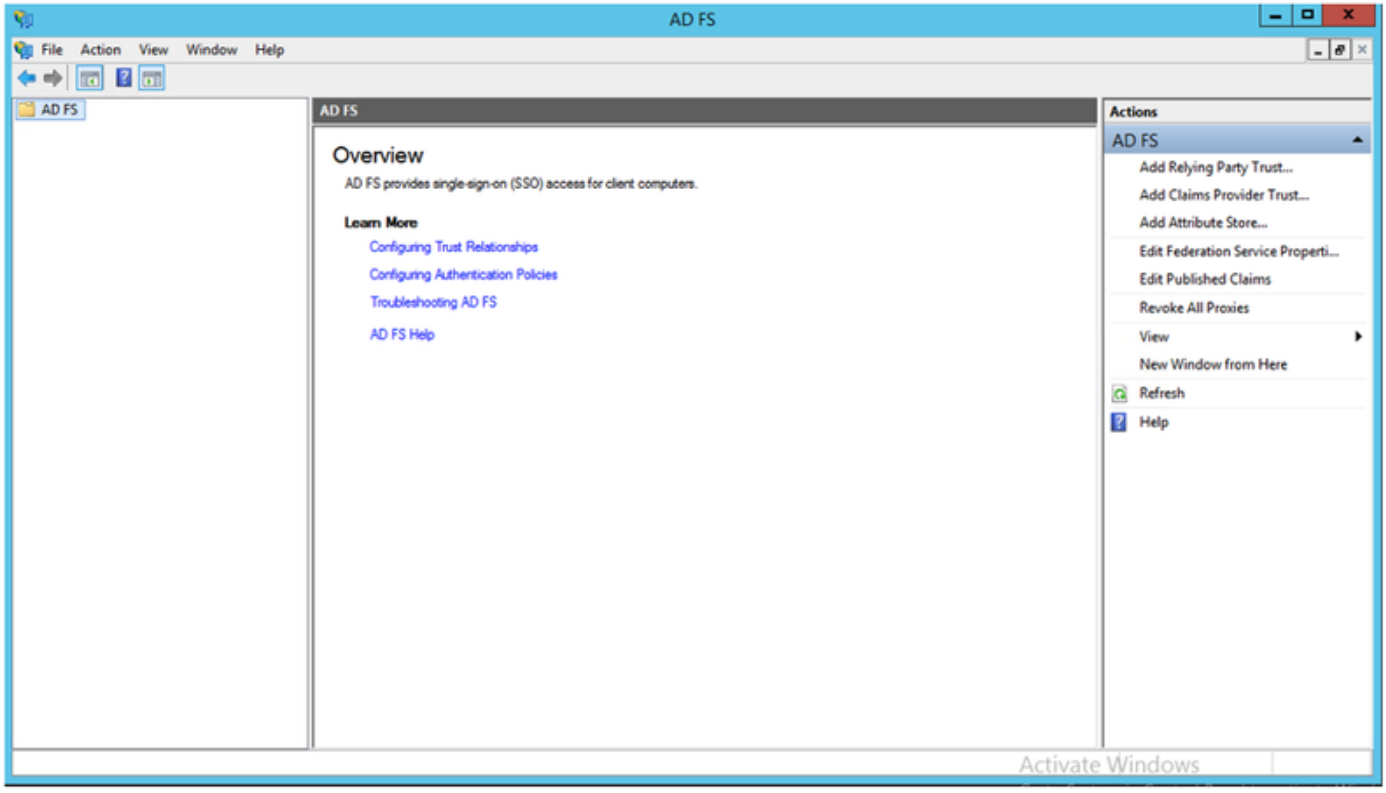
Alle erforderlichen Rollen sind in der Umgebung installiert, sodass Sie jetzt mit der Installation von ADFS3 Active Directory Federation Services (auf Windows Server 2012) fortfahren können.

Navigieren Sie für die Serverrolle zu **Server Manager > Verwalten > Serverrollen und -funktionen hinzufügen**, und wählen Sie **Active Directory Federation Services aus**, wenn Sie den IDP im Kundennetzwerk im privaten LAN installieren.





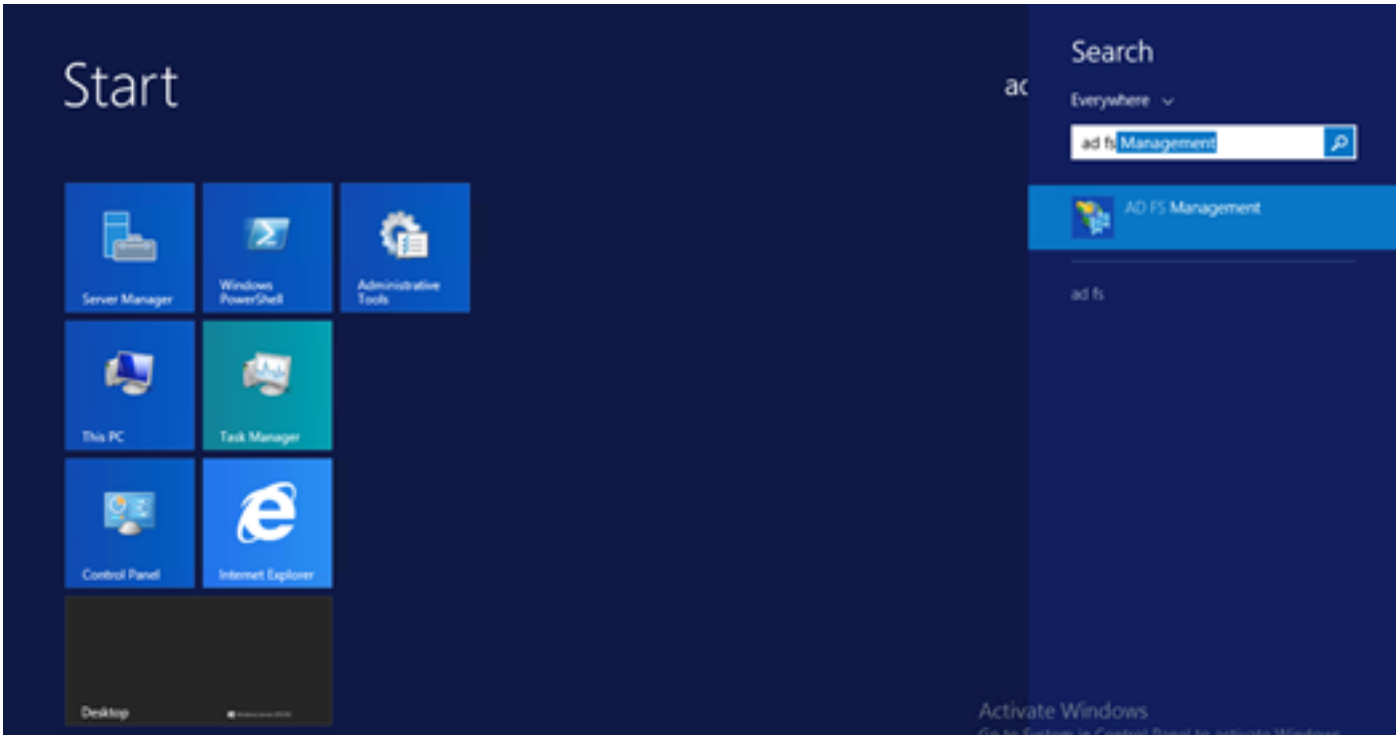
Sobald die Installation abgeschlossen ist, können Sie sie über die Taskleiste oder das Startmenü öffnen.



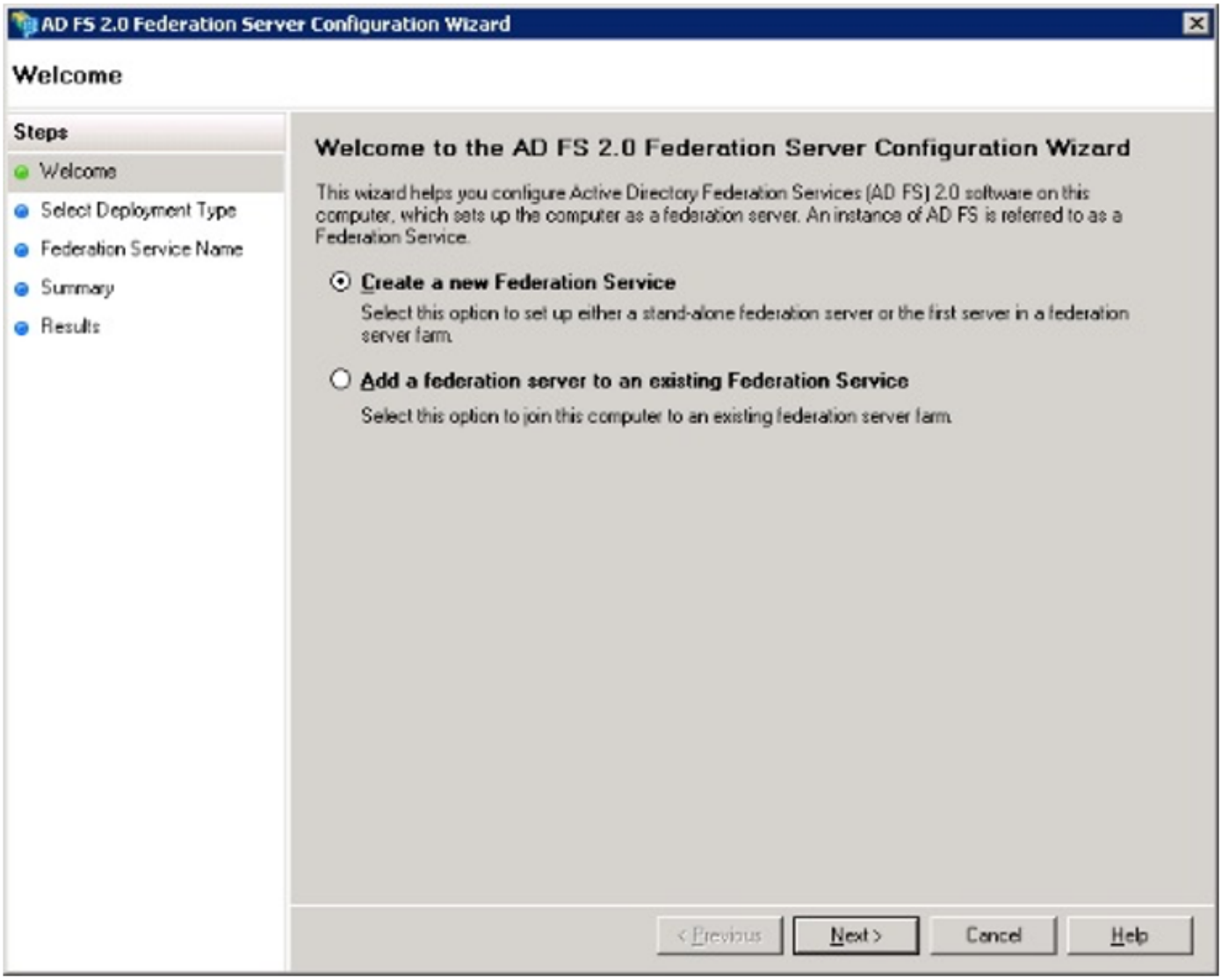
Erstkonfiguration von ADFS3

In diesem Abschnitt wird die Installation eines neuen, eigenständigen Föderationsservers beschrieben. Dieser kann jedoch auch verwendet werden, um ihn auf einem Domänencontroller zu installieren.

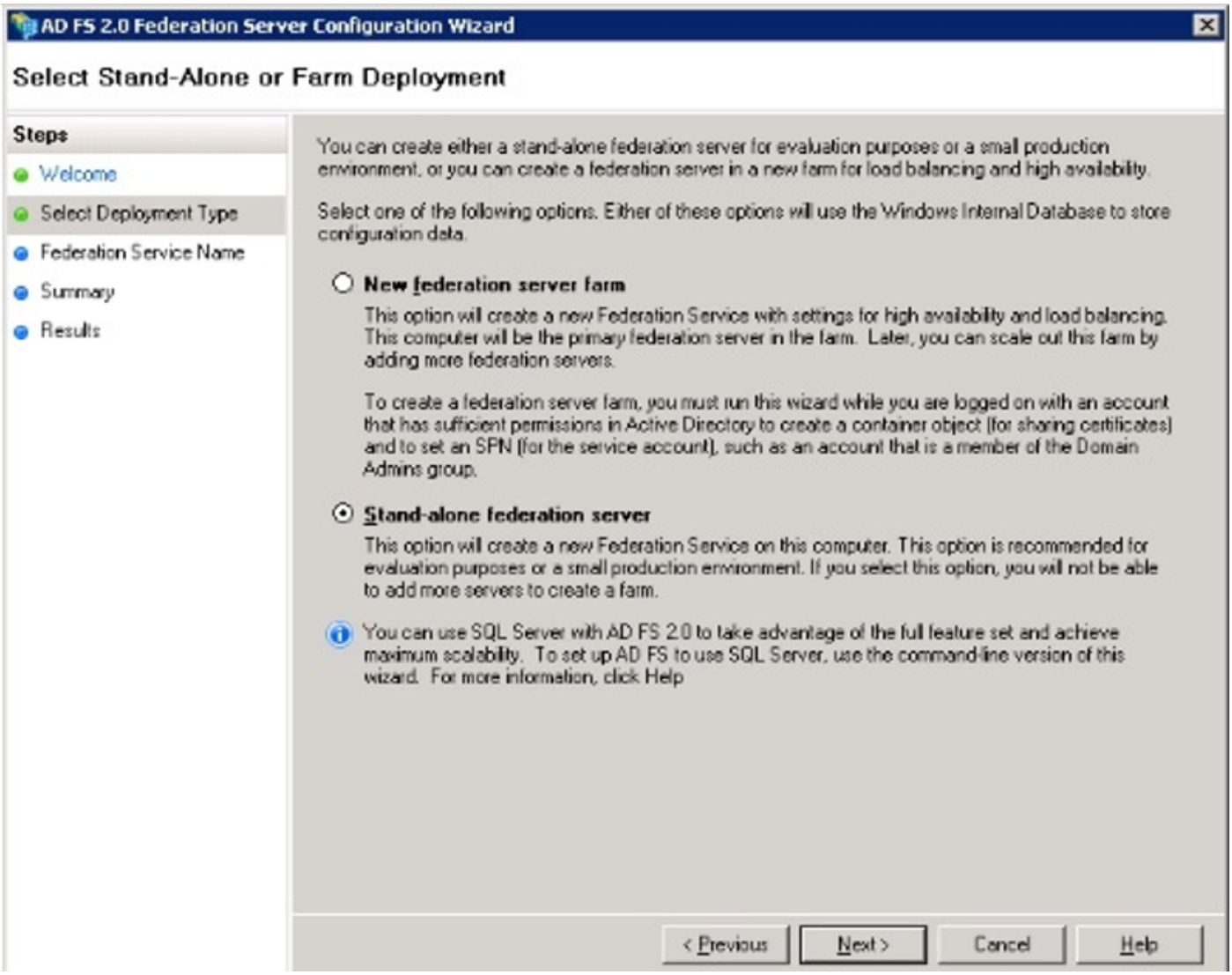
Wählen Sie **Windows** aus, und geben Sie **AD FS Management** ein, um die ADFS Management Console wie im Bild gezeigt zu starten.



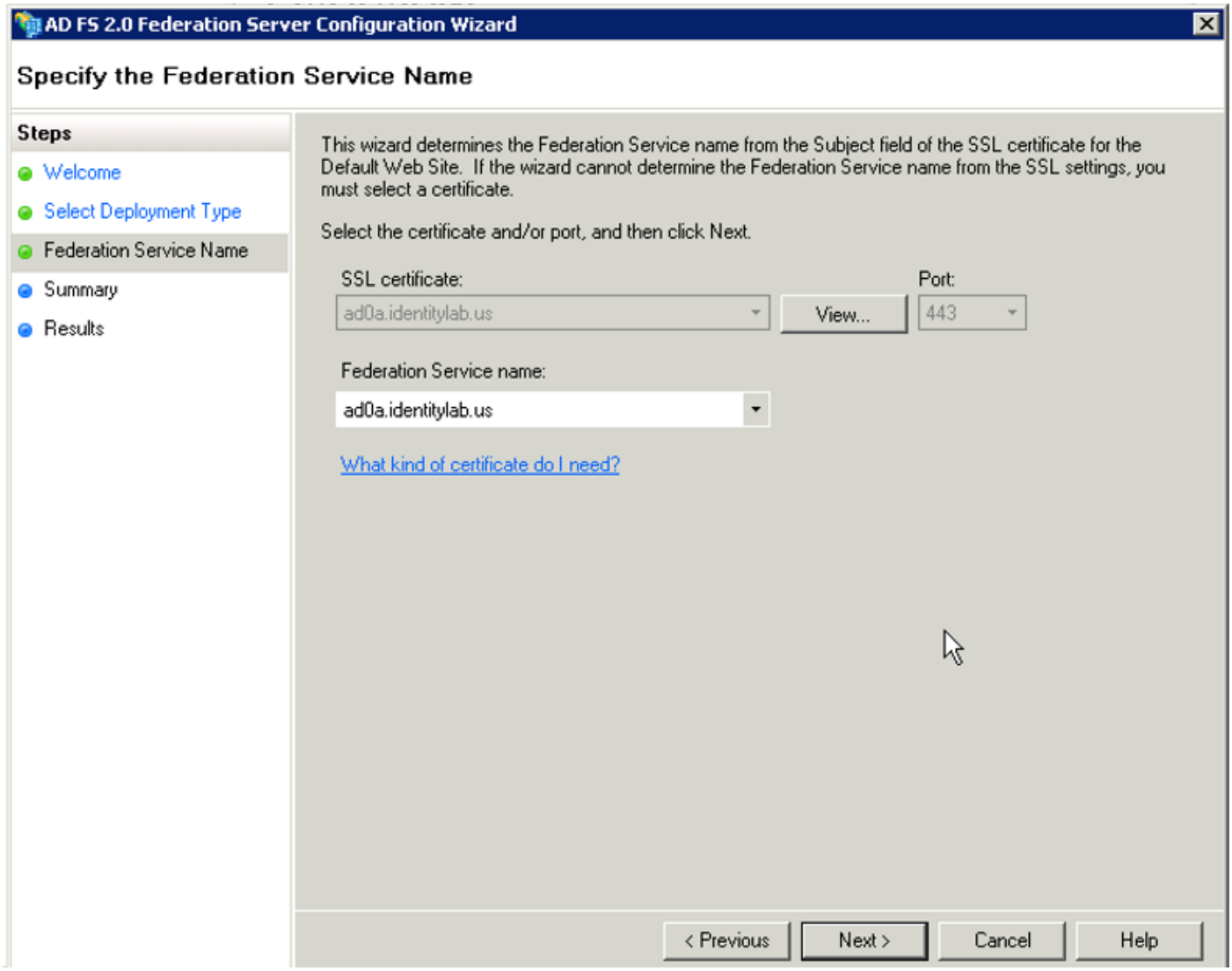
Wählen Sie die Option **AD FS 3.0 Federation Server Configuration Wizard** (Assistent zum Konfigurieren von AD FS-Servern) aus, um die ADFS-Serverkonfiguration zu starten. Diese Screenshots stellen die gleichen Schritte in AD FS 3 dar.



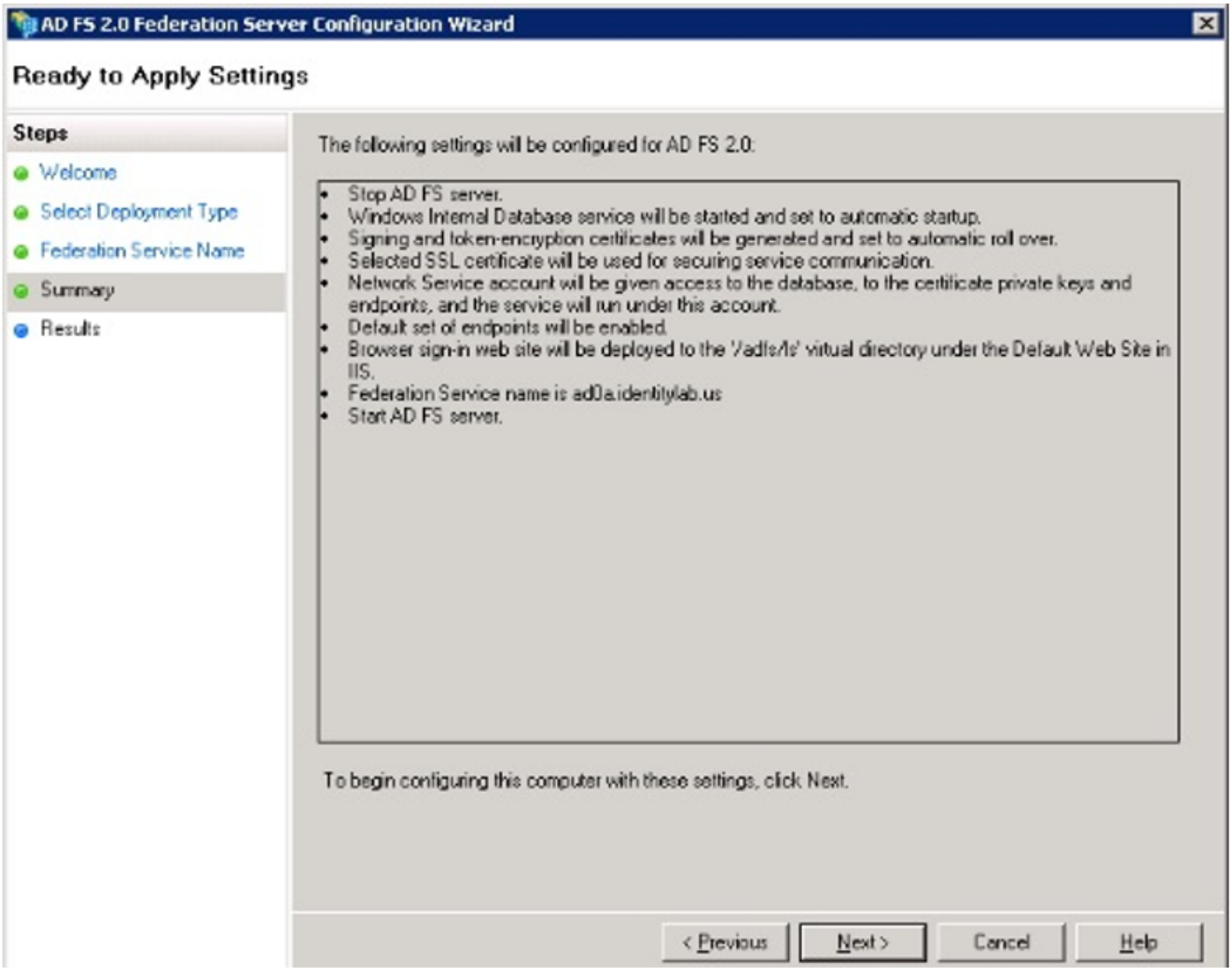
Wählen Sie Neuen **Föderationsdienst** erstellen aus, und klicken Sie auf **Weiter**.



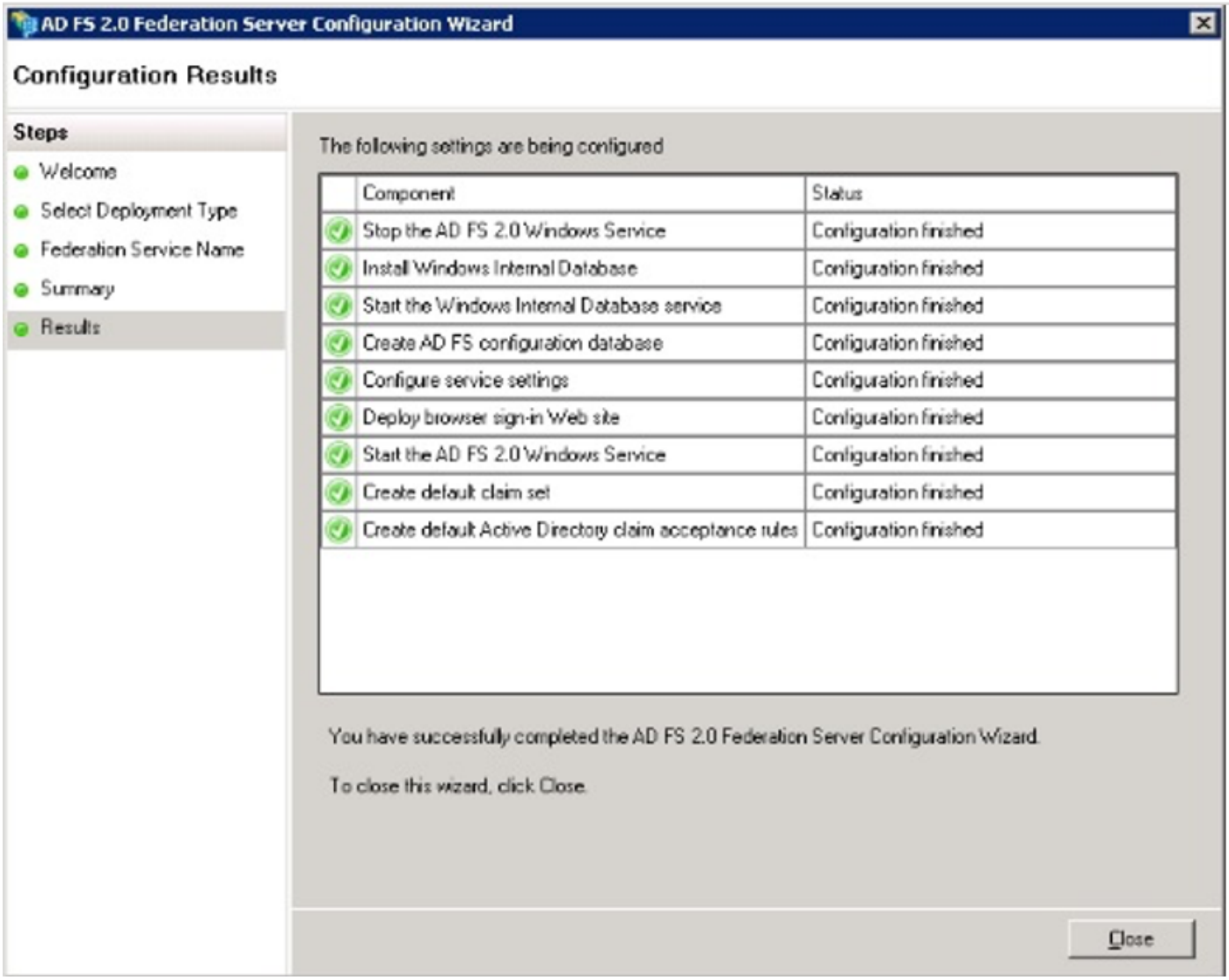
Wählen Sie Standalone Federation Server (eigenständiger Föderationsserver) aus, und klicken Sie auf **Next (Weiter)**, wie im Bild gezeigt.



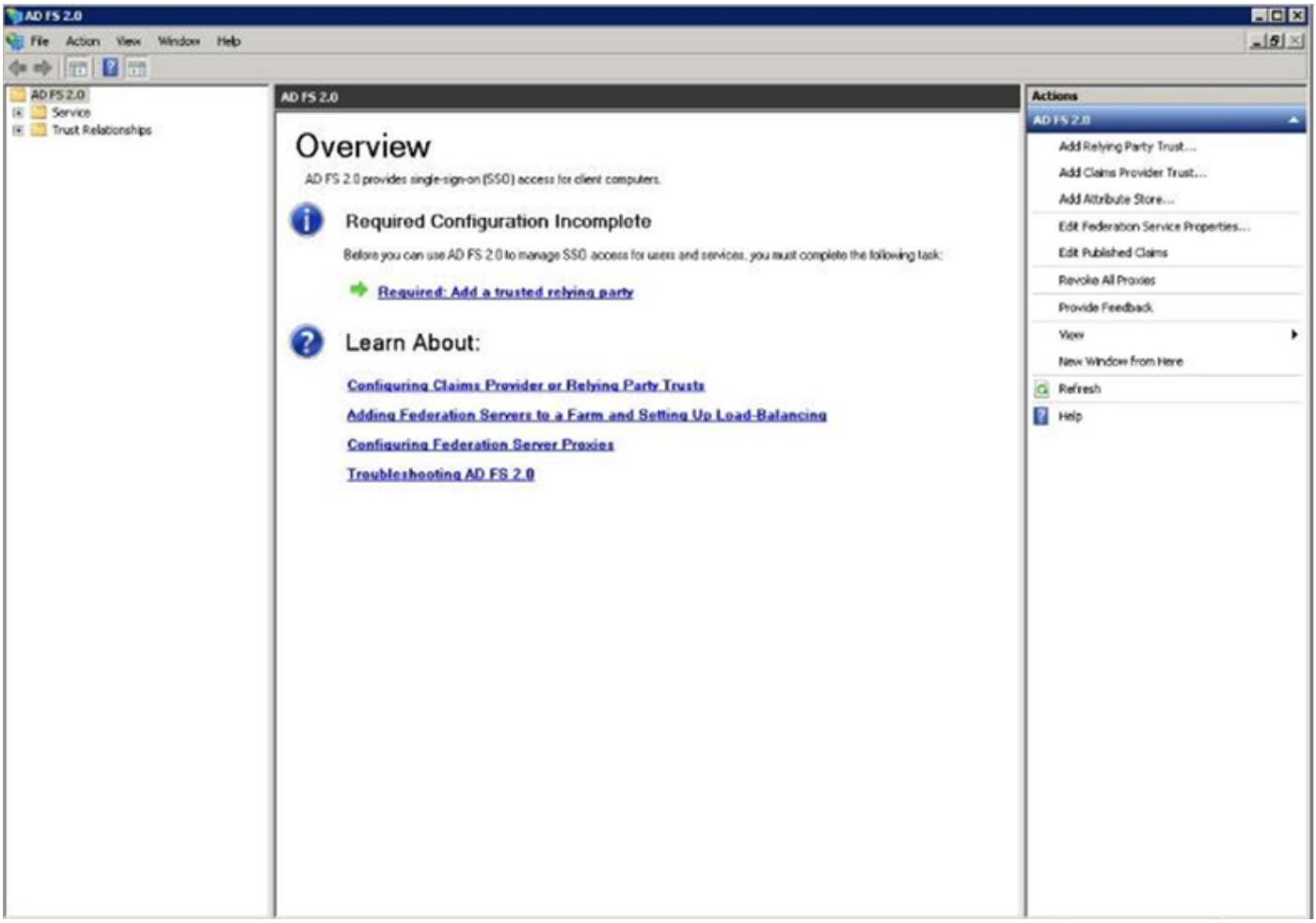
Wählen Sie unter SSL-Zertifikat das selbst signierte Zertifikat aus der Liste aus. Der Name des Föderationsdiensts wird automatisch eingetragen. Klicken Sie auf **Weiter**.



Überprüfen Sie die Einstellungen, und klicken Sie auf **Weiter**, um die Einstellungen zu übernehmen.



Bestätigen Sie, dass alle Komponenten erfolgreich abgeschlossen wurden, und klicken Sie auf **Schließen**, um den Assistenten zu beenden und zur Hauptverwaltungskonsole zurückzukehren. Dies kann einige Minuten dauern.

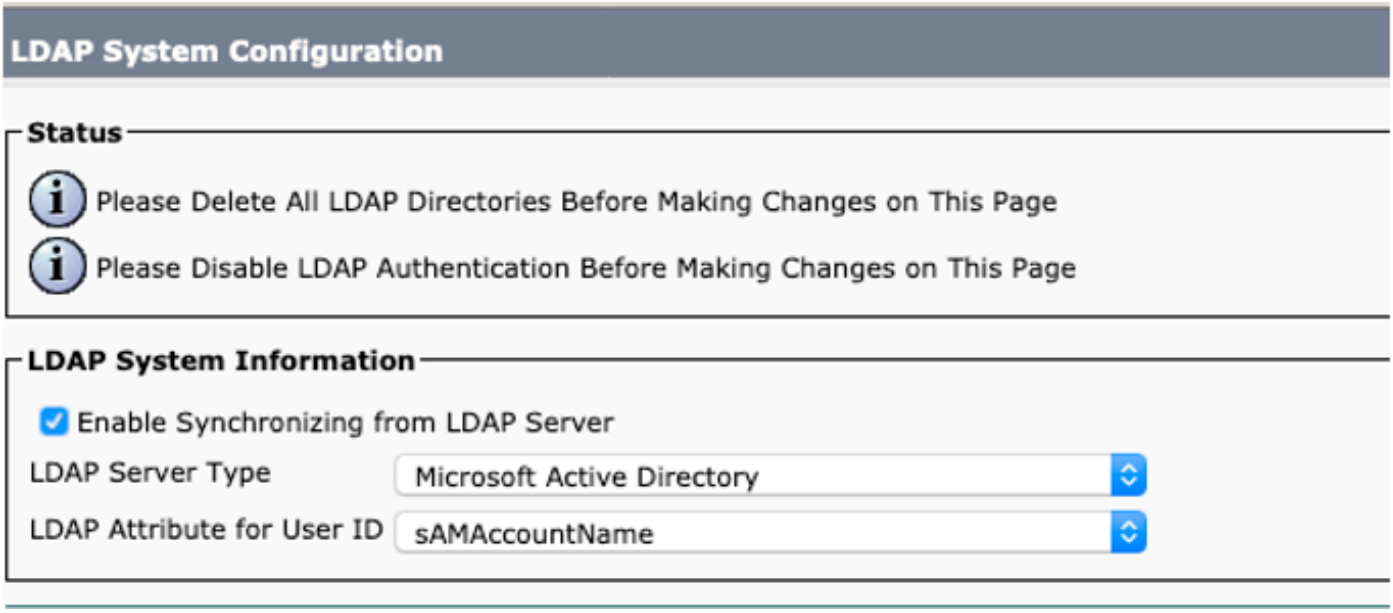


ADFS ist nun effektiv aktiviert und als Identitätsanbieter (Identity Provider, IDP) konfiguriert. Als Nächstes müssen Sie CUCM als zuverlässigen Partner hinzufügen. Bevor Sie dies tun können, müssen Sie zunächst eine Konfiguration in der CUCM-Verwaltung vornehmen.

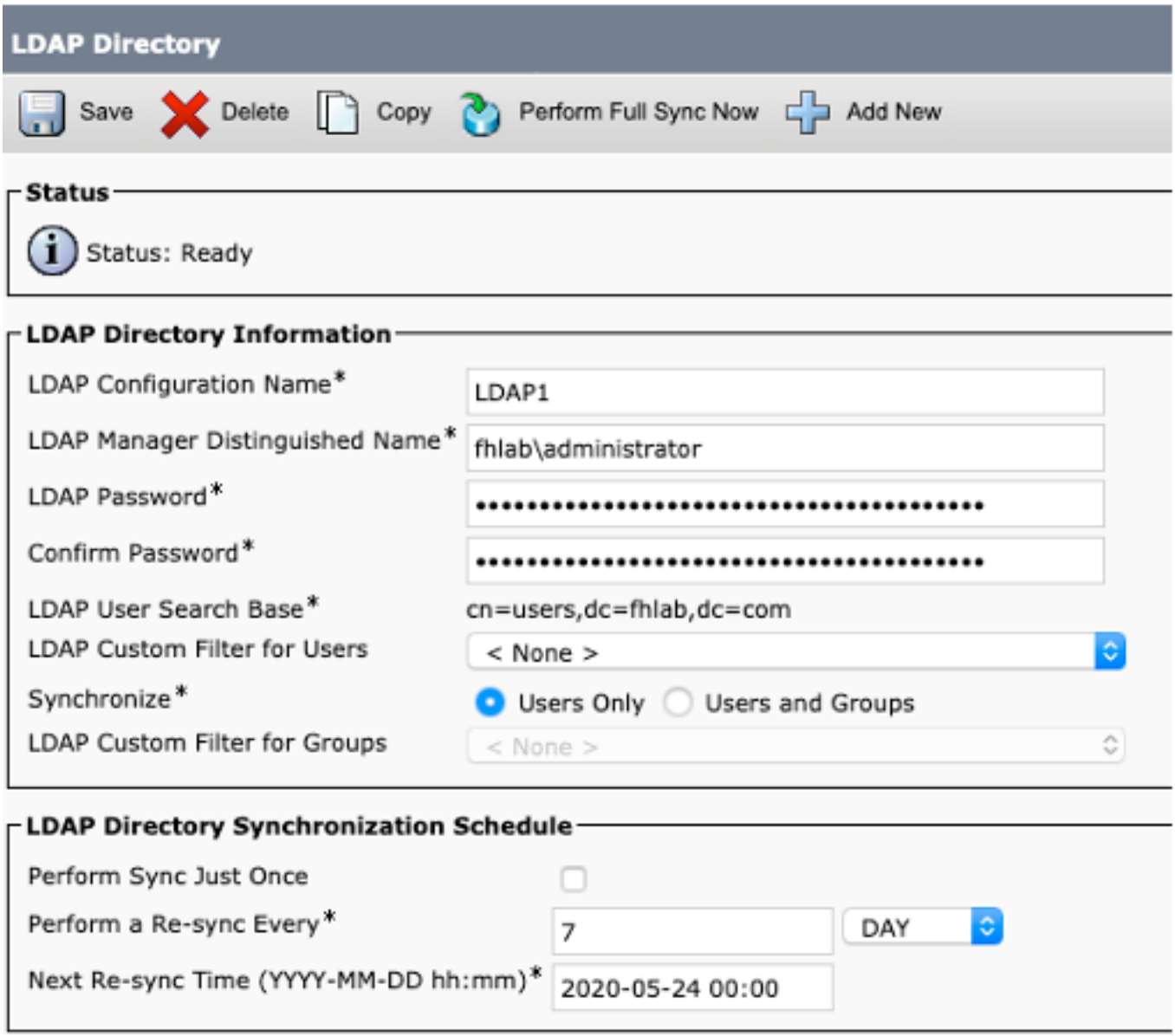
Konfigurieren von SSO auf CUCM mit ADFS

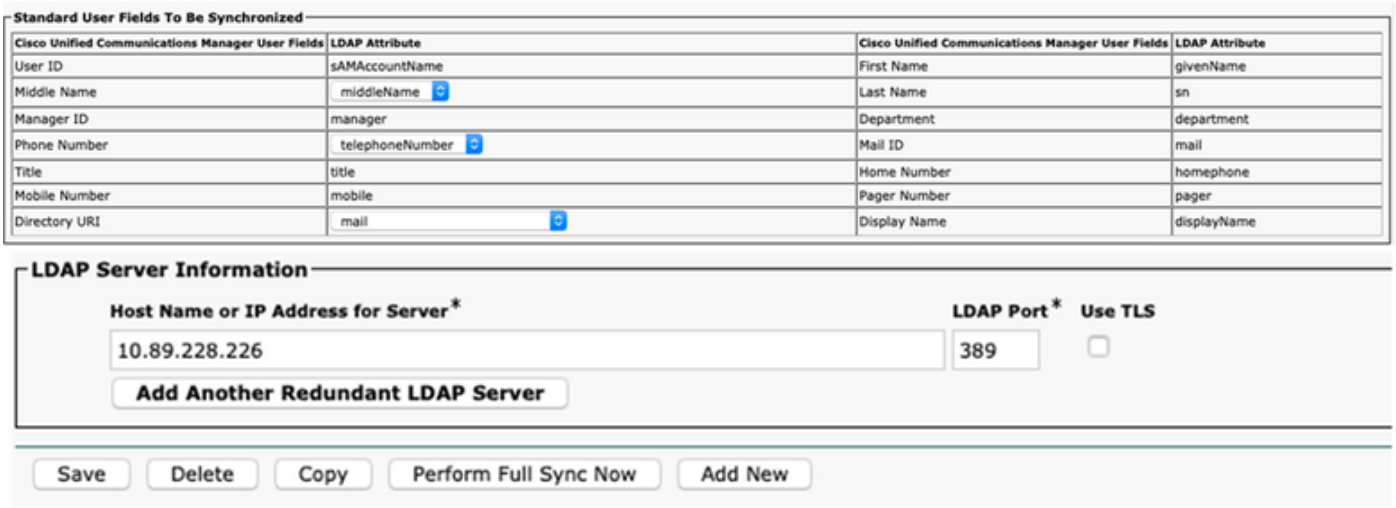
LDAP-Konfiguration

Der Cluster muss LDAP-integriert in Active Directory sein, und die LDAP-Authentifizierung muss konfiguriert werden, bevor es weitergeht. Navigieren Sie zur **Registerkarte System > LDAP System** wie im Bild gezeigt.

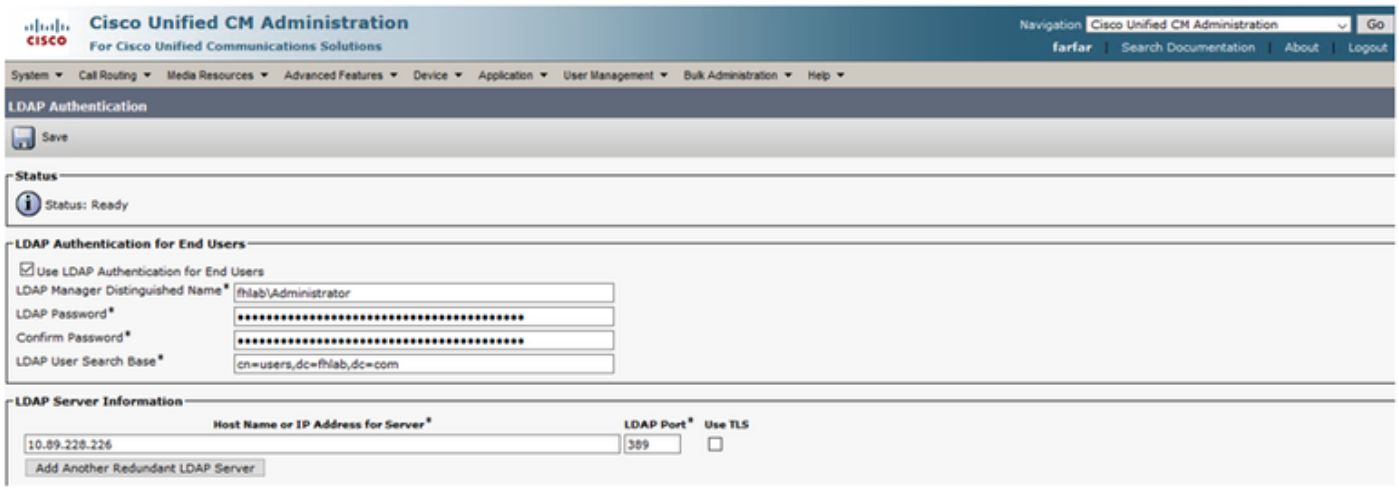


Navigieren Sie anschließend zur **Registerkarte System > LDAP Directory (System > LDAP-Verzeichnis)**.

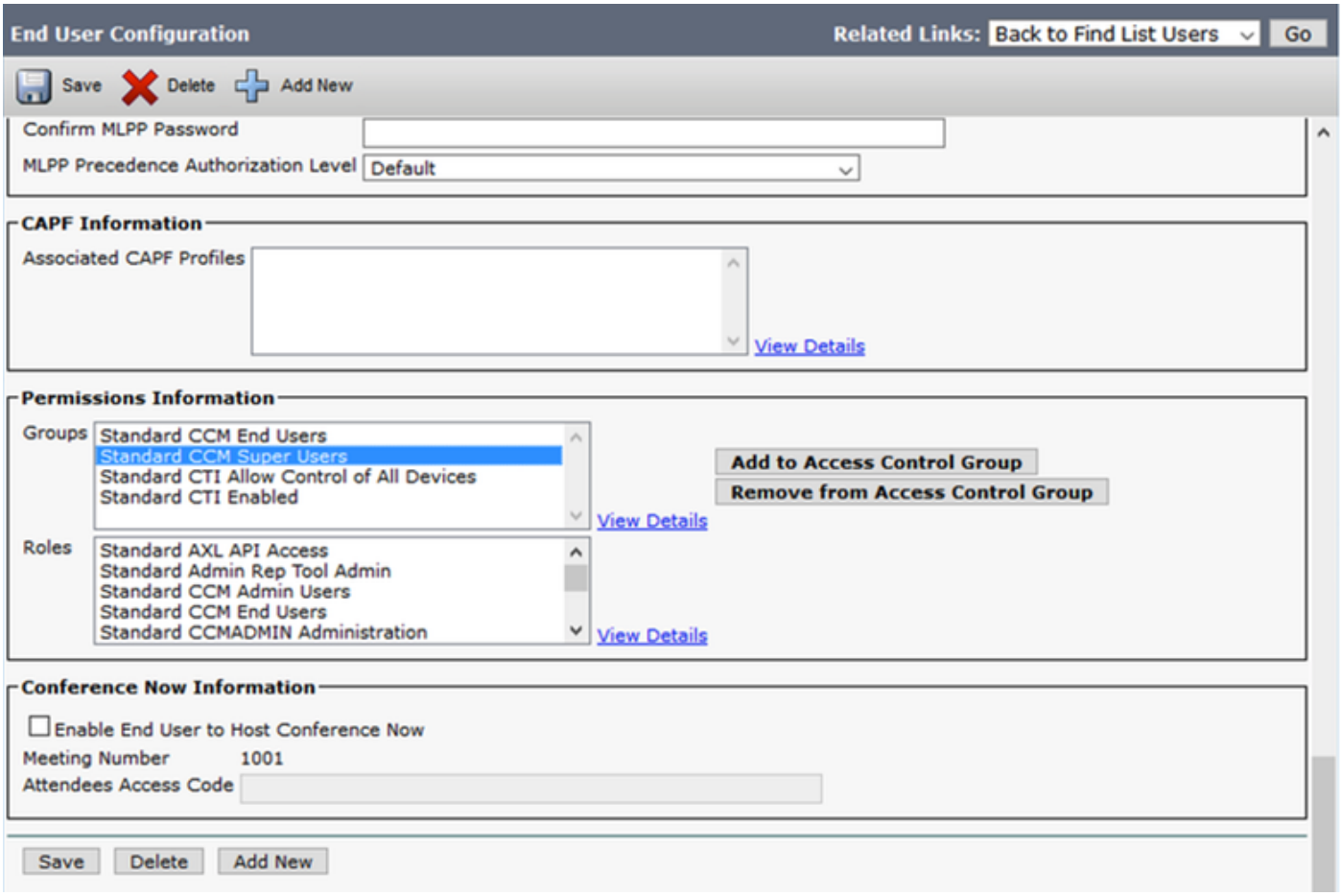




Nachdem die Active Directory-Benutzer mit dem CUCM synchronisiert wurden, muss die LDAP-Authentifizierung konfiguriert werden.



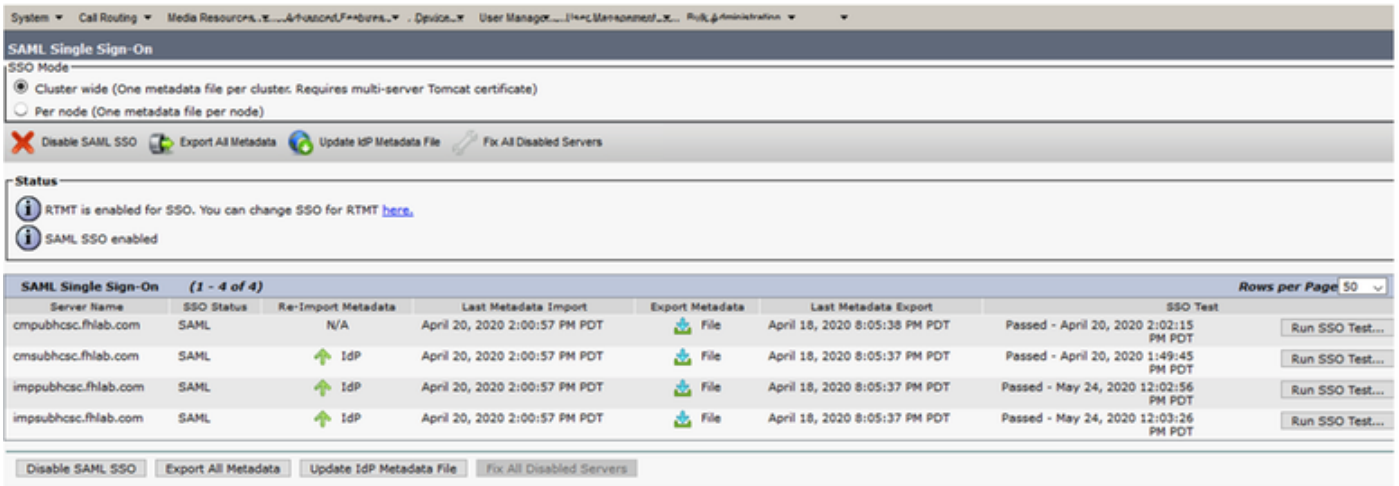
Endbenutzer in CUCM müssen bestimmte Zugriffskontrollgruppen seinem Endbenutzerprofil zugewiesen haben. Die ACG sind Standard-CCM-Super-Benutzer. Der Benutzer wird zum Testen von SSO verwendet, wenn die Umgebung bereit ist.



CUCM-Metadaten

In diesem Abschnitt wird der Prozess für den CUCM Publisher angezeigt.

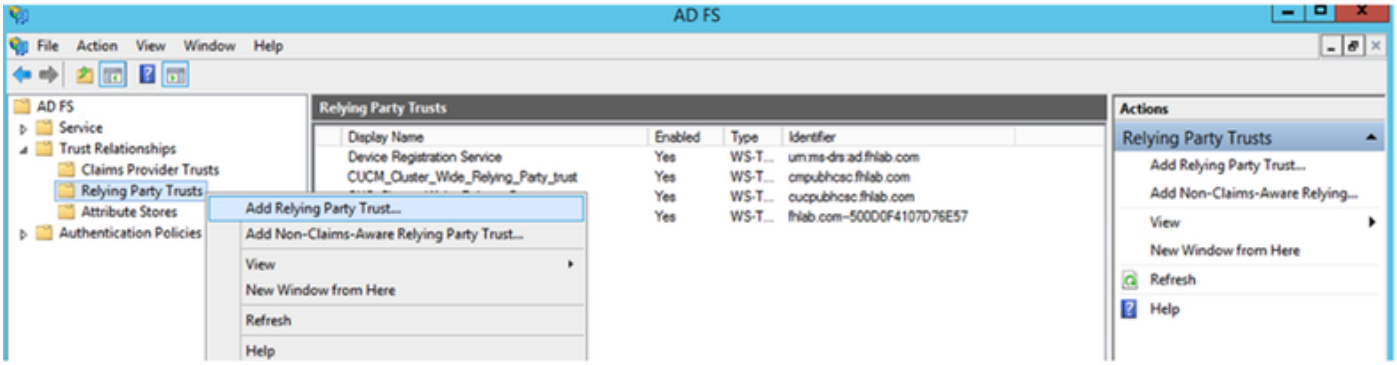
Die erste Aufgabe besteht darin, die CUCM-Metadaten abzurufen, für die Sie zur URL navigieren müssen. **https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadaten/sp** oder kann von der **Registerkarte System (System) > SAML Single Sign-on** heruntergeladen werden. Dies kann pro Knoten oder Cluster-weit erfolgen. Diese Option ist clusterweit vorzuziehen.



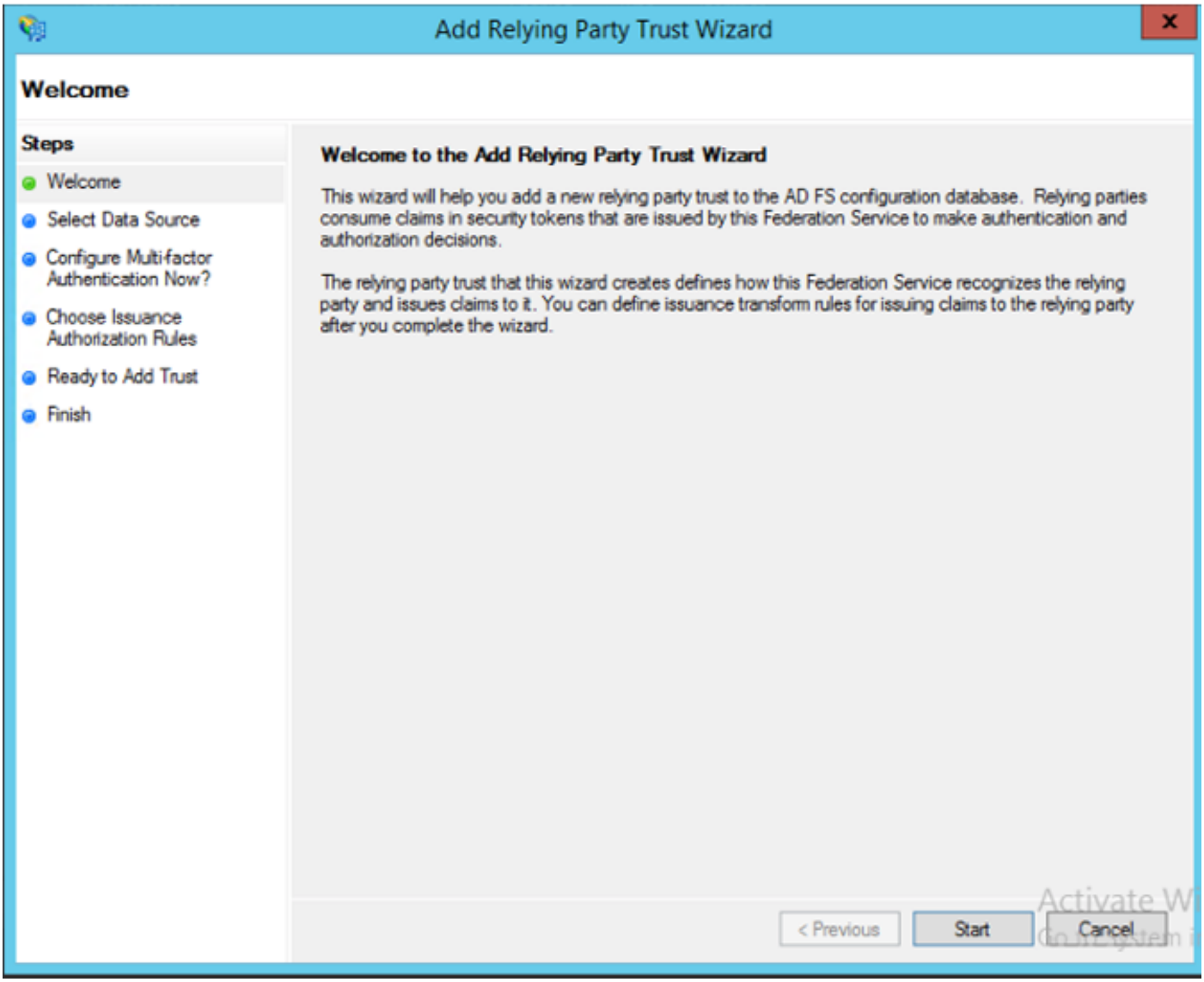
Speichern Sie die Daten lokal mit einem aussagekräftigen Namen wie sp_cucm0a.xml, danach benötigen Sie sie.

Konfigurieren der ADFS-Relationship-Partei

Kehren Sie zur Verwaltungskonsole AD FS 3.0 zurück.

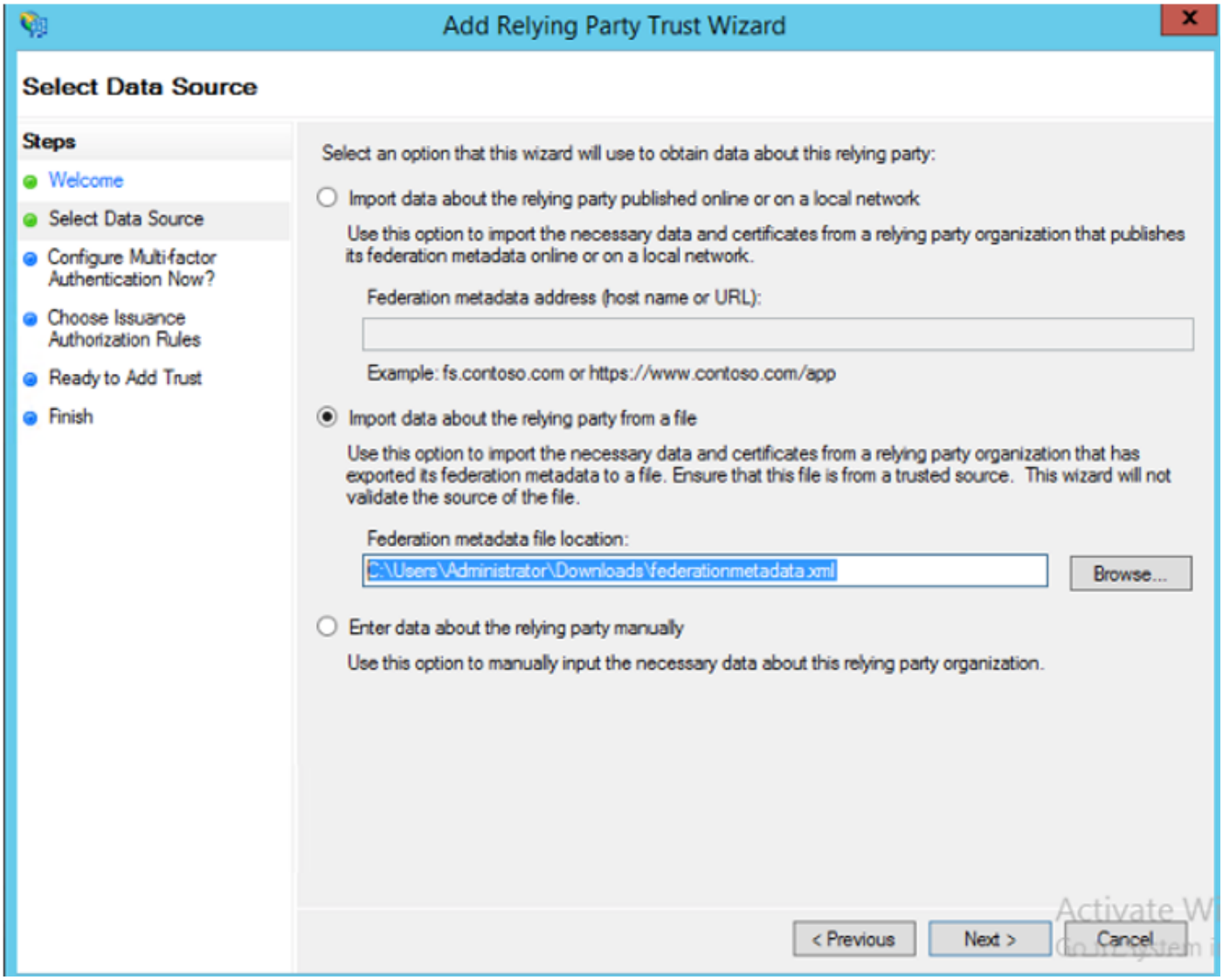


Klicken Sie auf **Assistent zum Hinzufügen von Vertrauenswürdigkeit**.

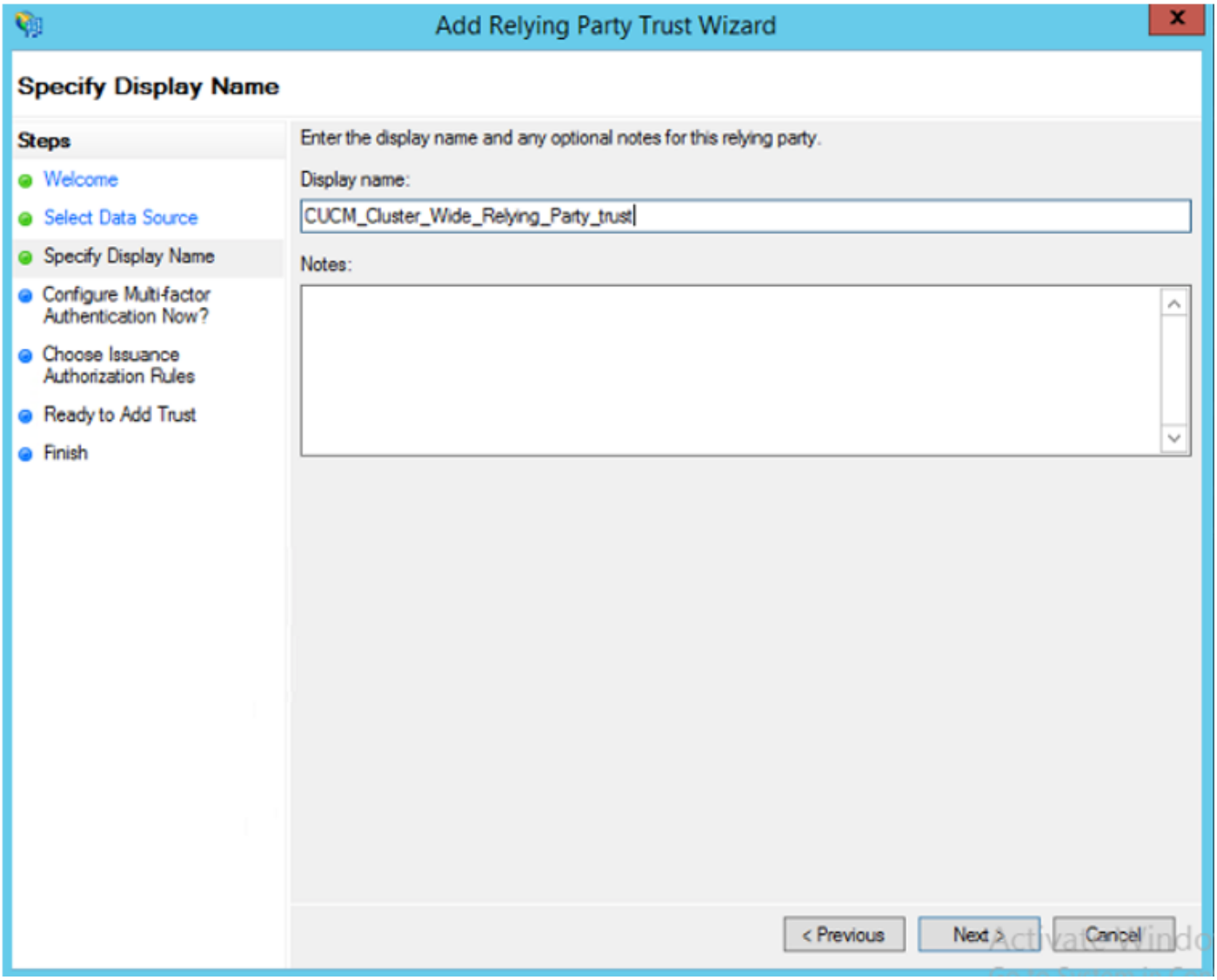


Klicken Sie auf **Start**, um fortzufahren.

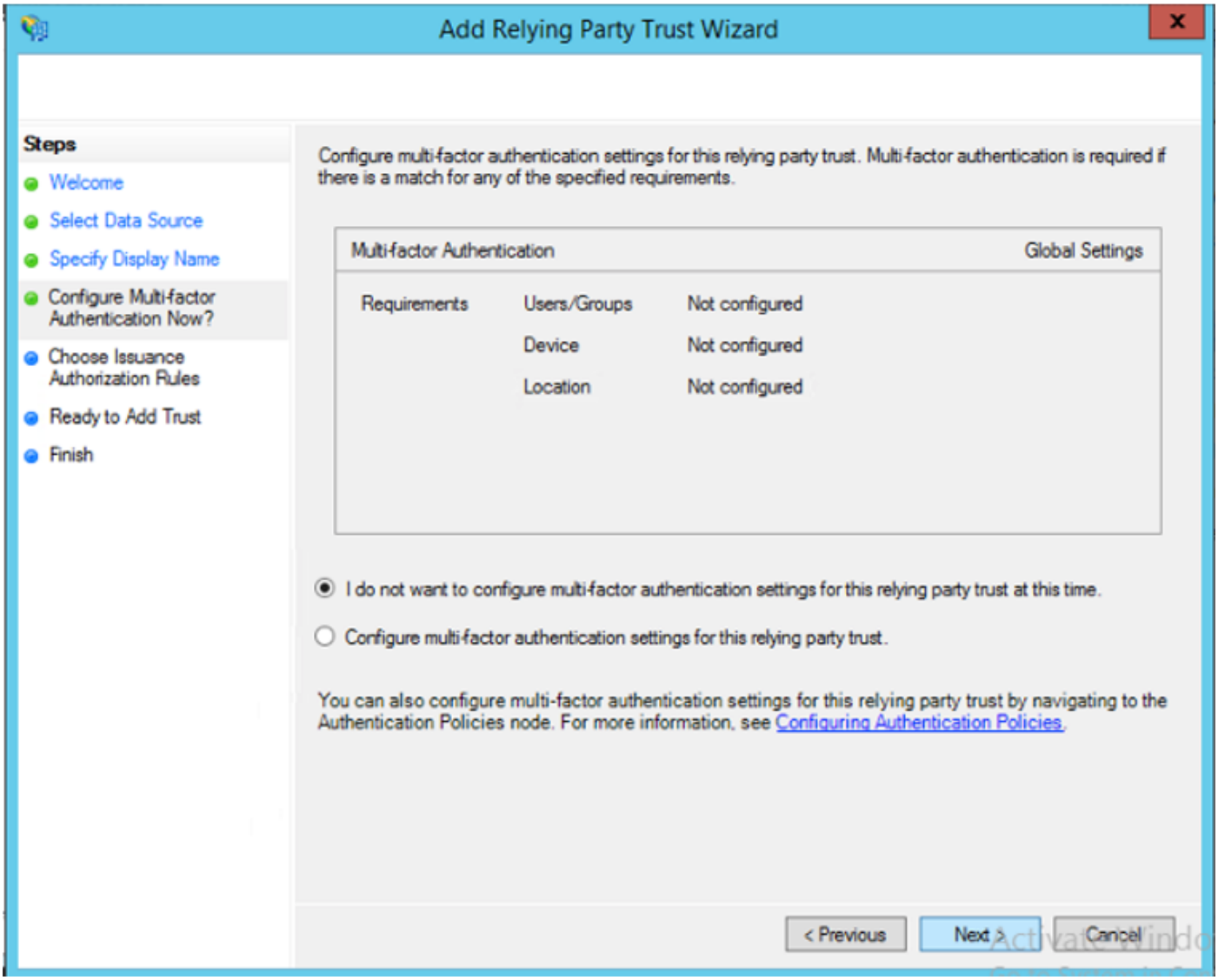
Wählen Sie die zuvor gespeicherte XML-Datei **Federationmedatada.xml** aus, und klicken Sie auf **Weiter**.



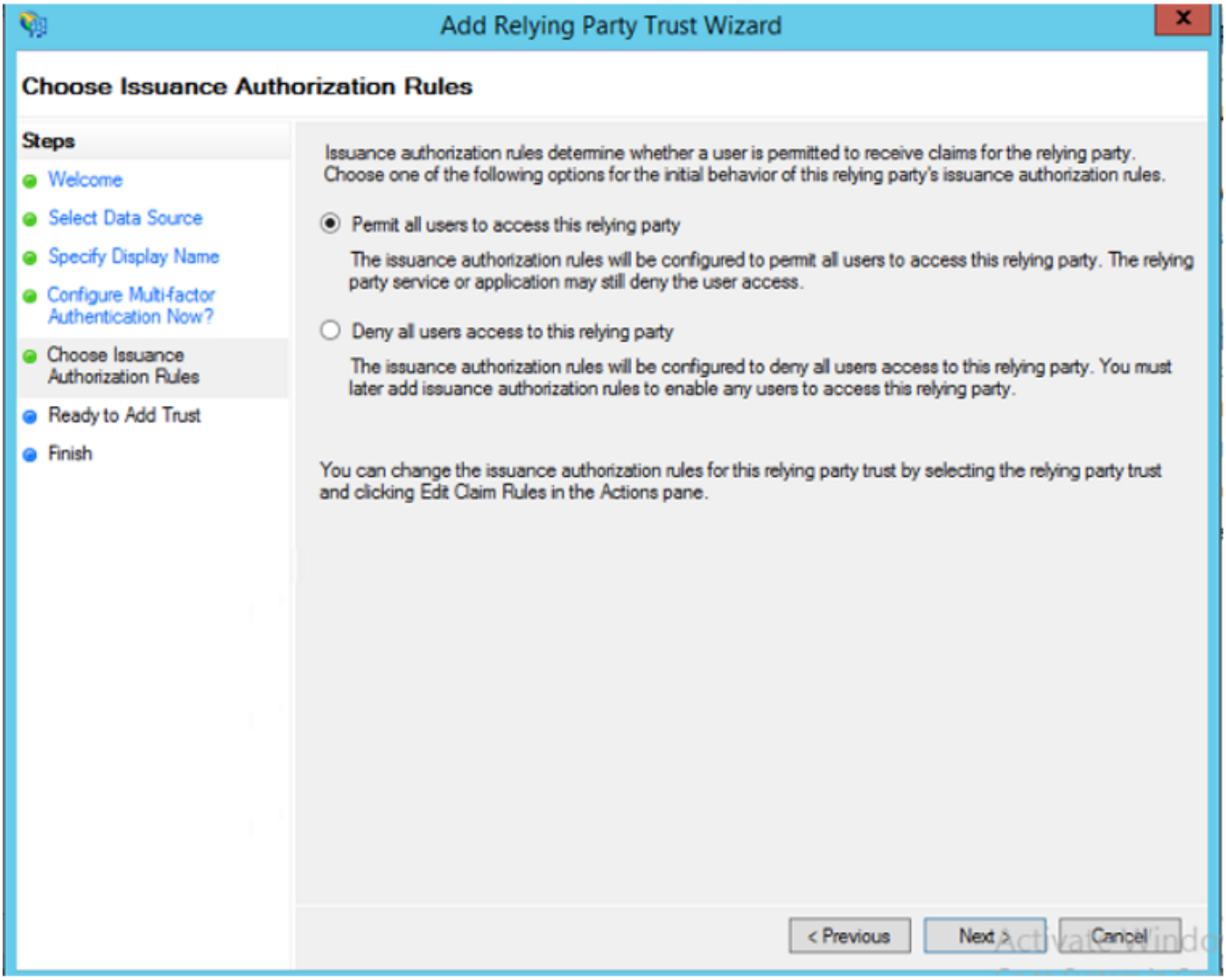
Verwenden Sie **CUCM_Cluster_Wide_Relying_Party_trust** als Anzeigenamen, und klicken Sie auf **Weiter**.



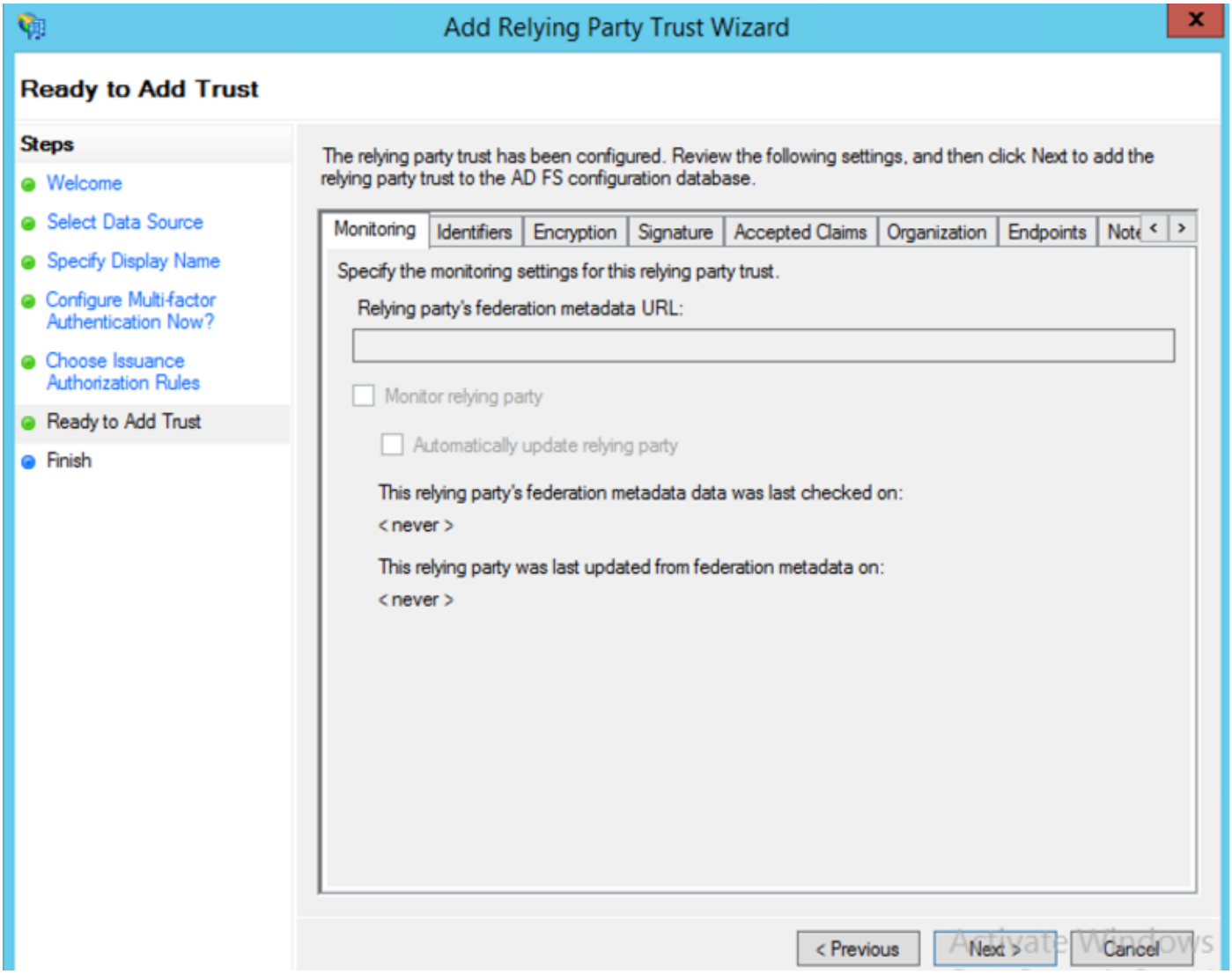
Wählen Sie die erste Option aus, und klicken Sie auf **Weiter**.



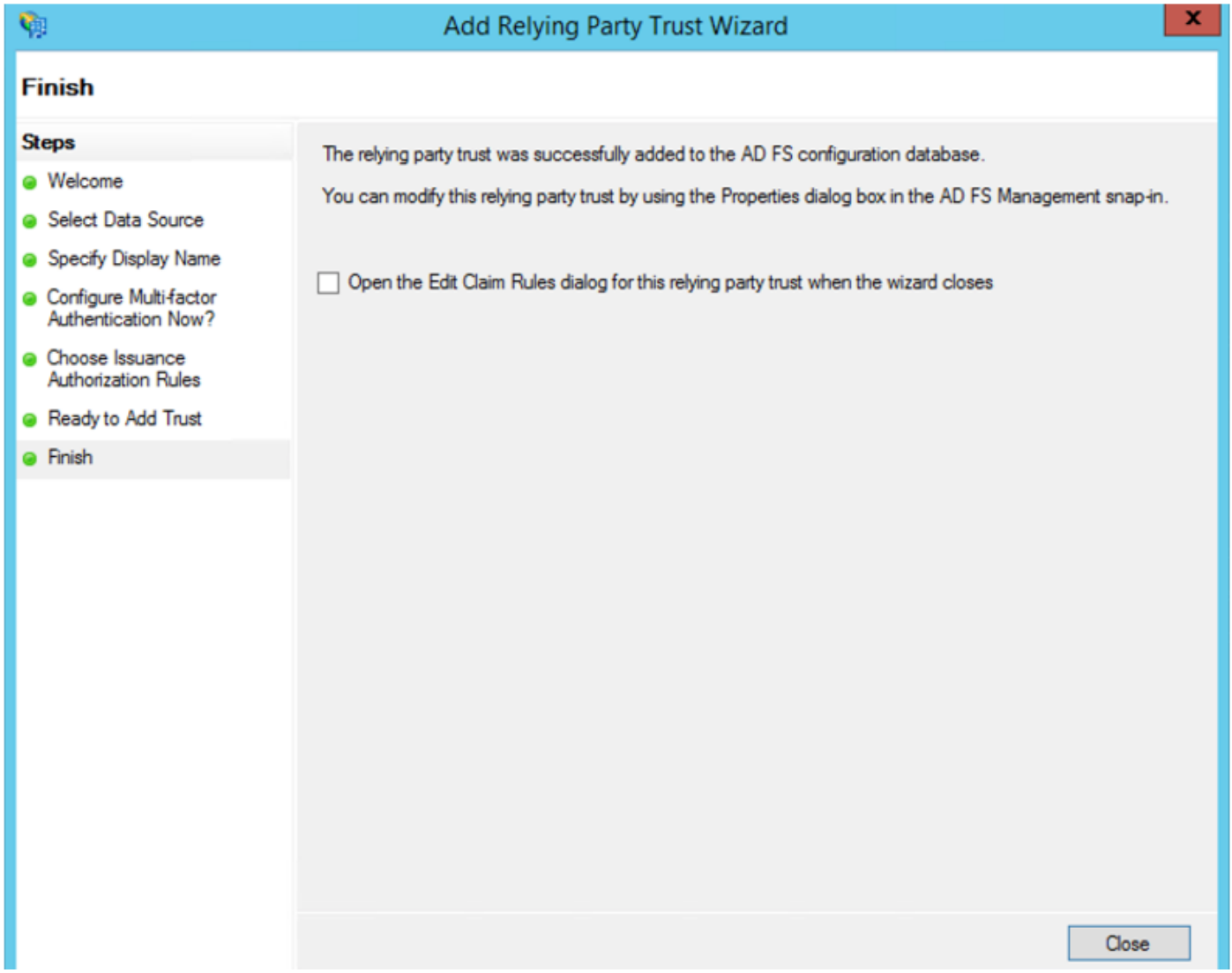
Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei aus**, und klicken Sie auf **Weiter,** wie im Bild gezeigt.



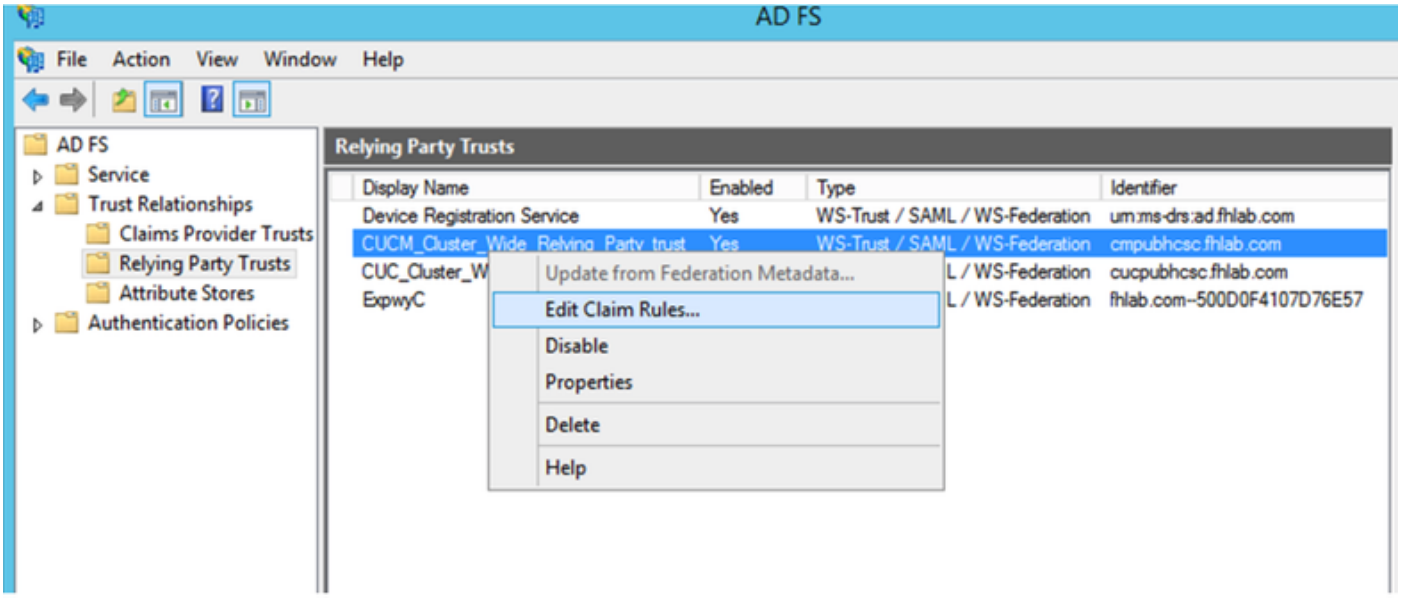
Überprüfen Sie die Konfiguration, und klicken Sie auf **Weiter**, wie im Bild gezeigt.



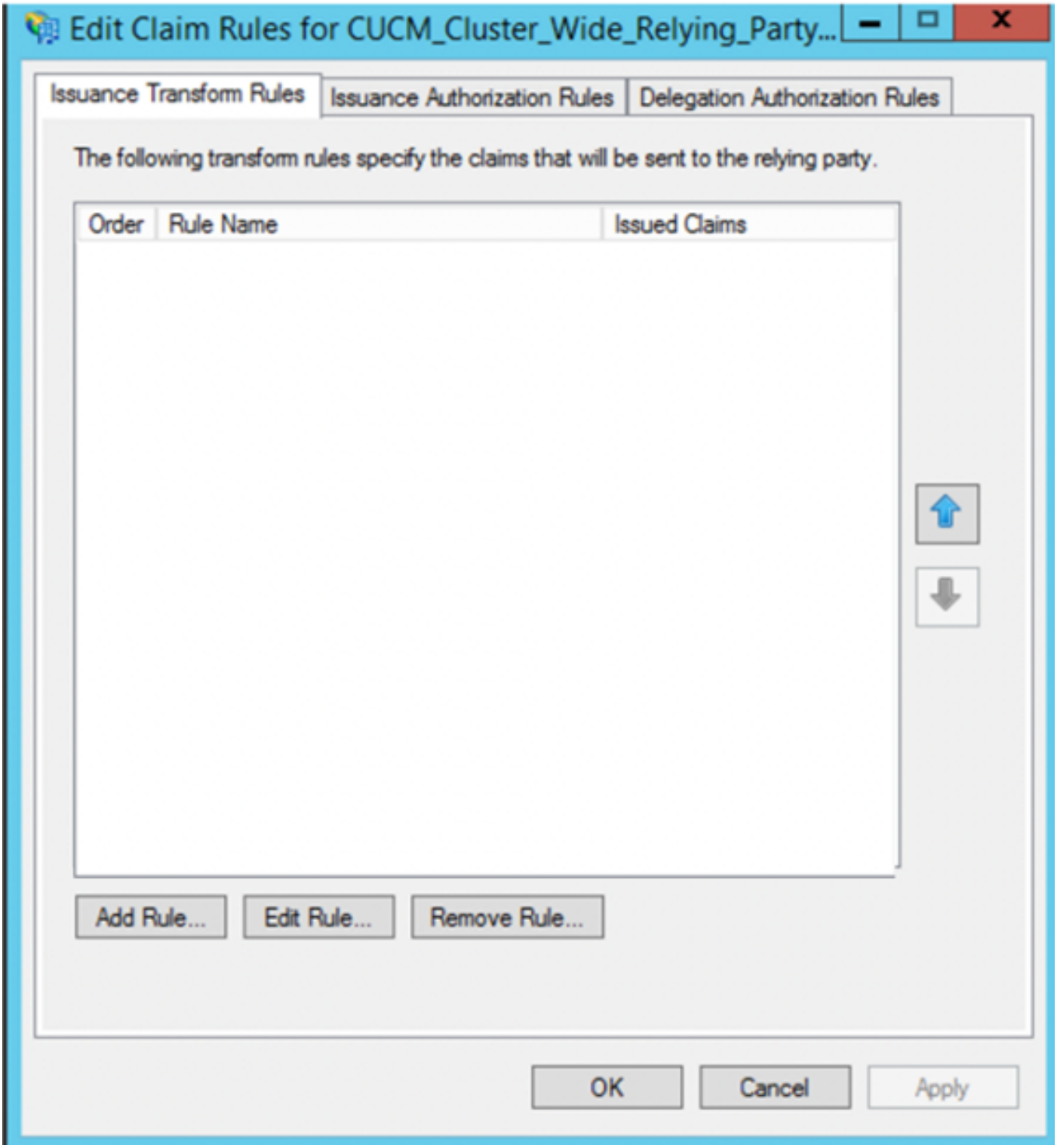
Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Schließen**.



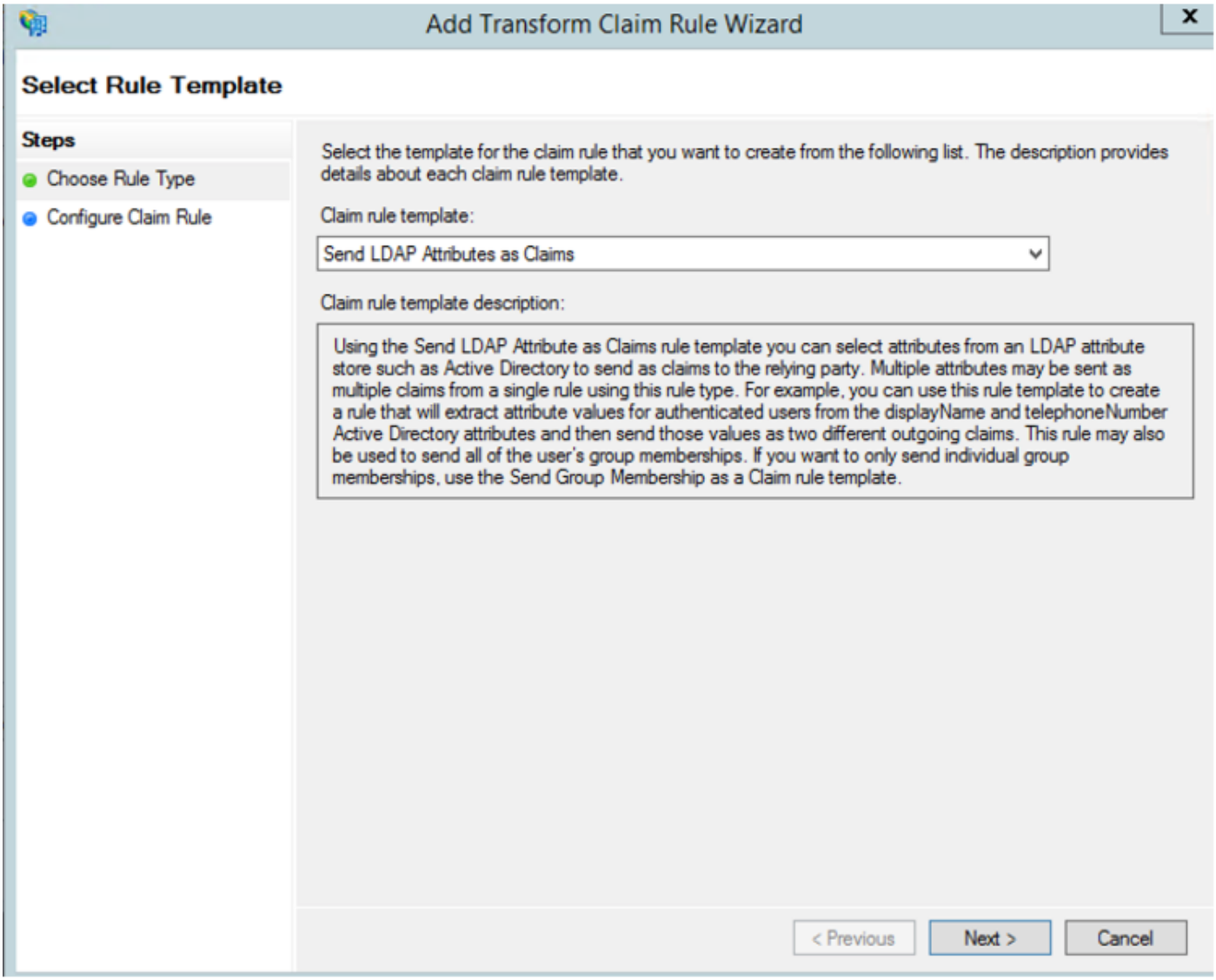
Wählen Sie mit der zweiten Maustaste die **Relying Party Trust** aus, die Sie gerade erstellt haben, und **bearbeiten Sie** die Konfiguration der Anspruchsregeln, wie im Bild gezeigt.



Klicken Sie auf **Regel hinzufügen** wie im Bild gezeigt.



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



Konfigurieren Sie diese Parameter:

Name der Anspruchsregel: NameID

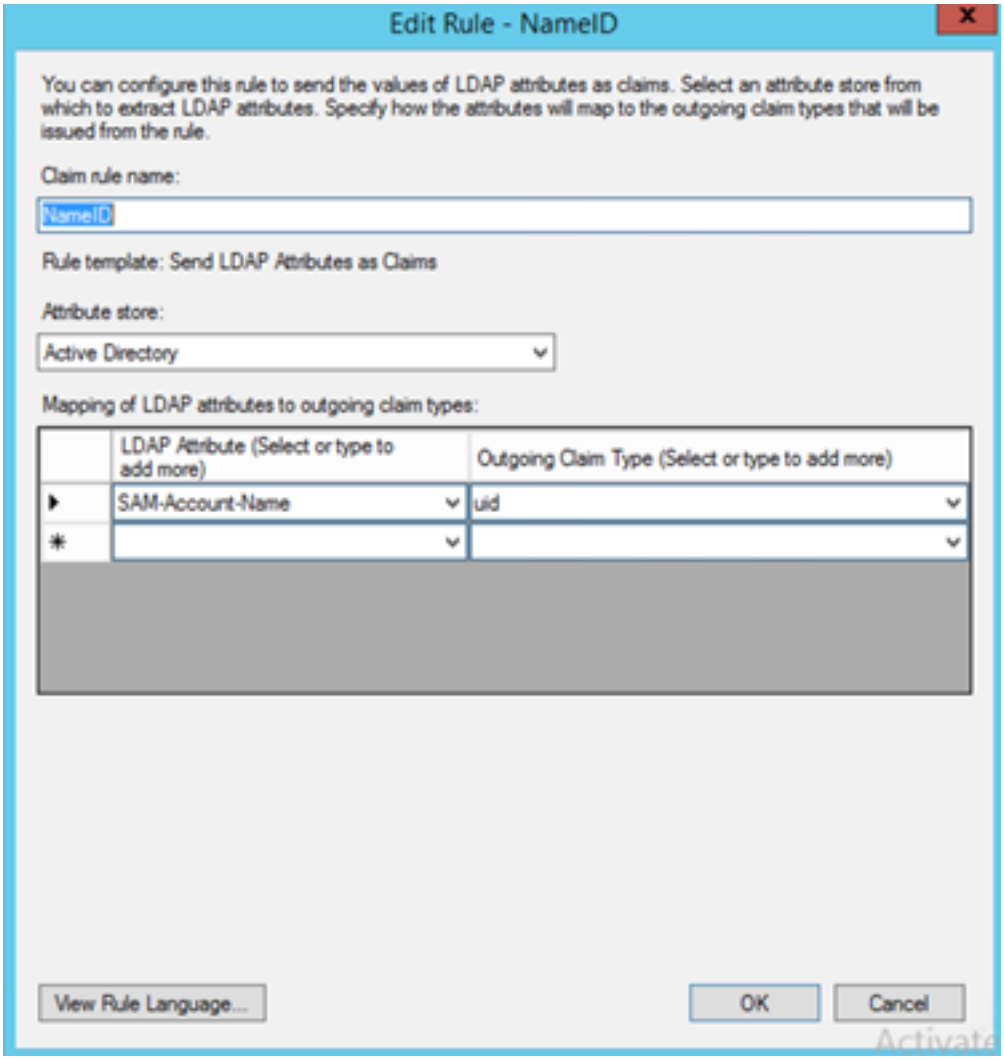
Attributspeicher: Active Directory (doppelklicken Sie auf den Pfeil des Dropdown-Menüs)

LDAP-Attribut: SAM-Kontoname

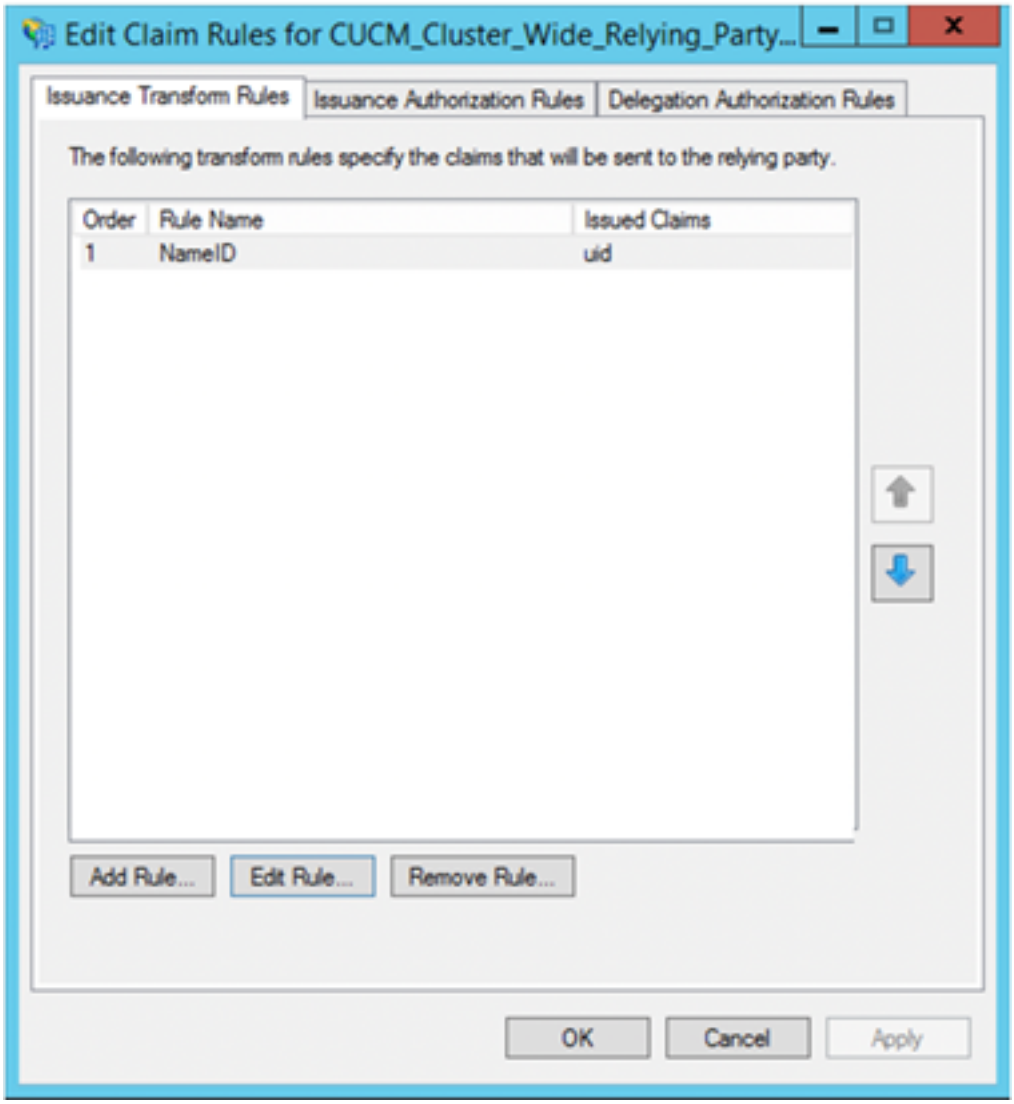
Ausgehender Anspruchstyp: uid

Klicken Sie auf **FERTIG/OK**, um fortzufahren.

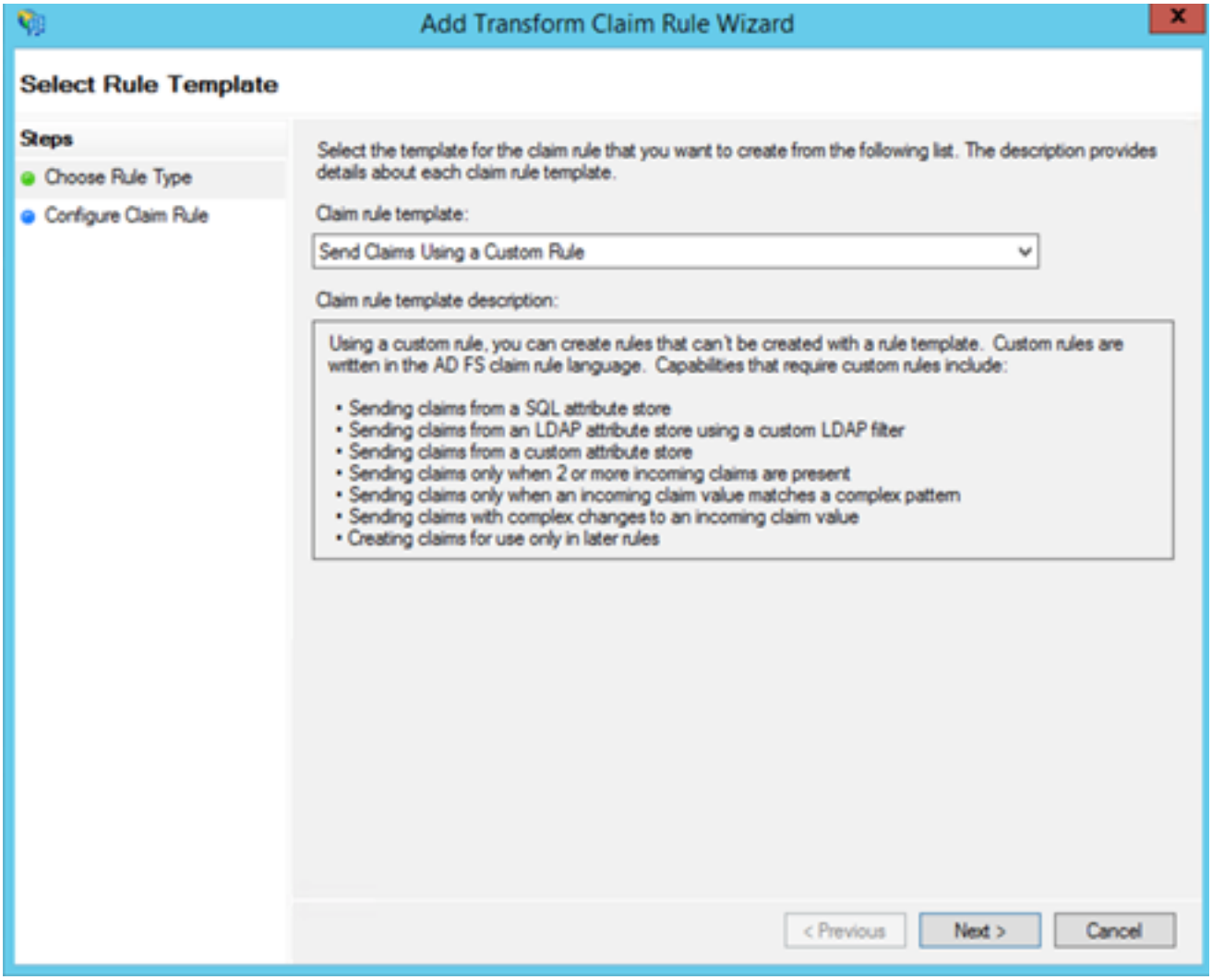
Bitte beachten Sie, dass uid nicht im Kleinbuchstaben angezeigt wird und nicht bereits im Dropdown-Menü vorhanden ist. Geben Sie es ein.



Klicken Sie erneut auf **Regel hinzufügen**, um eine andere Regel hinzuzufügen.



Wählen Sie **Anträge mit einer benutzerdefinierten Regel senden aus,** und klicken Sie auf **Weiter**.

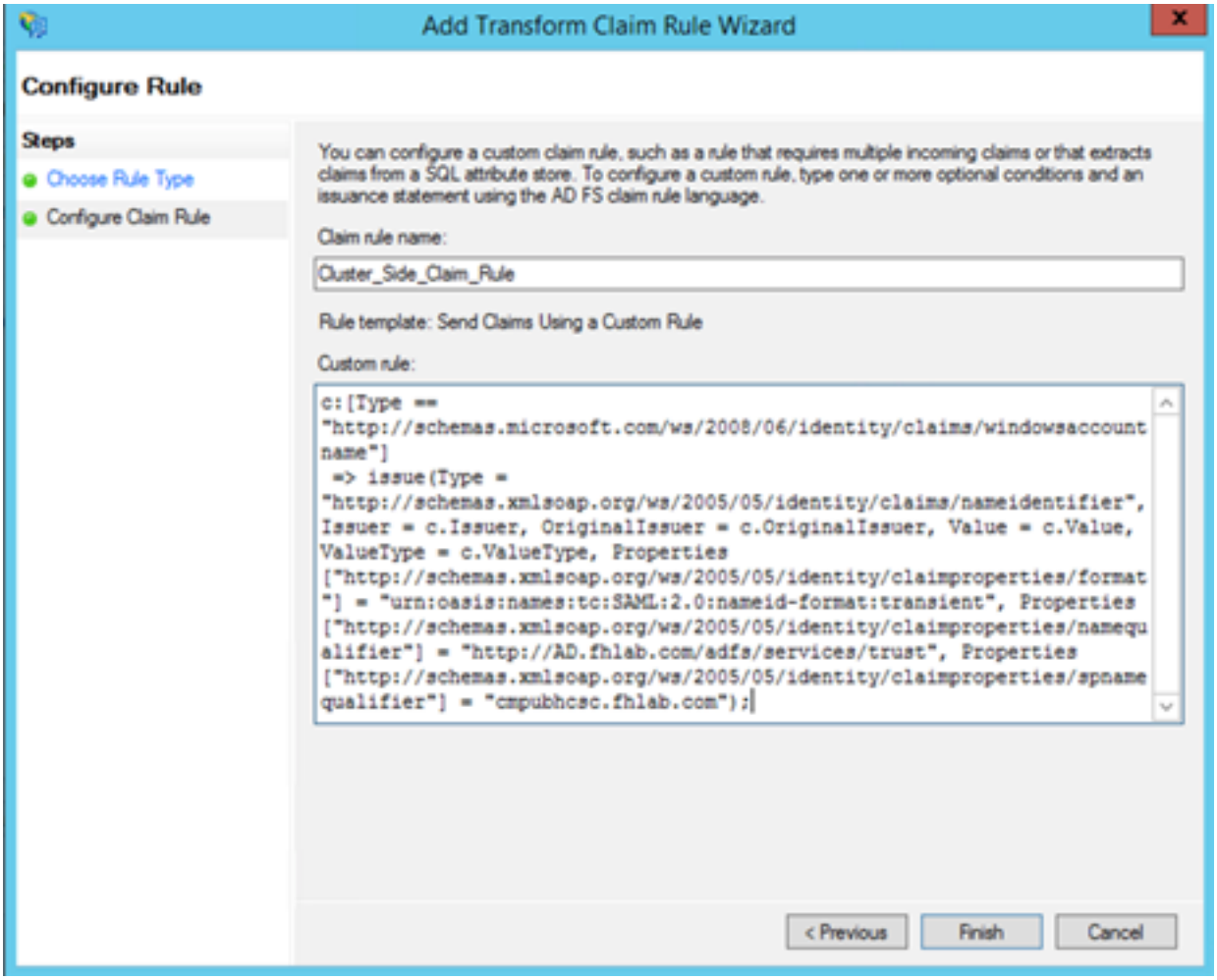


Erstellen Sie eine benutzerdefinierte Regel mit dem Namen Cluster_Side_Claim_Rule.

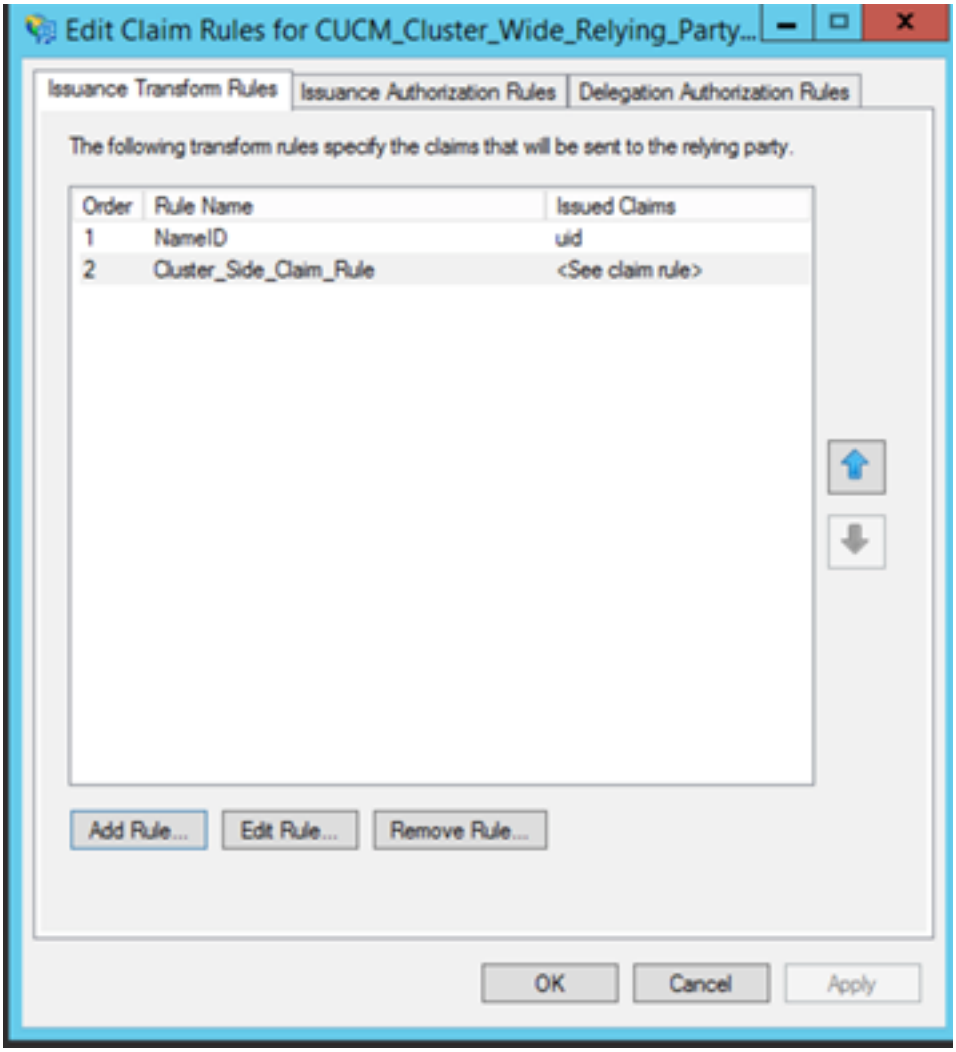
Kopieren Sie diesen Text und fügen Sie ihn hier direkt in das Regelfenster ein. In manchen Fällen werden Kostenvoranschläge geändert, wenn sie in einem Texteditor bearbeitet werden. Dies führt dazu, dass die Regel beim Testen der SSO-Funktion fehlschlägt:

```
c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "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/namequalifier"]
= "http://<ADFS FQDN>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<CUCM Pub FQDN>");

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "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/namequalifier"] =
"http://AD.fhlab.com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"cmpubhcsc.fhlab.com");
```

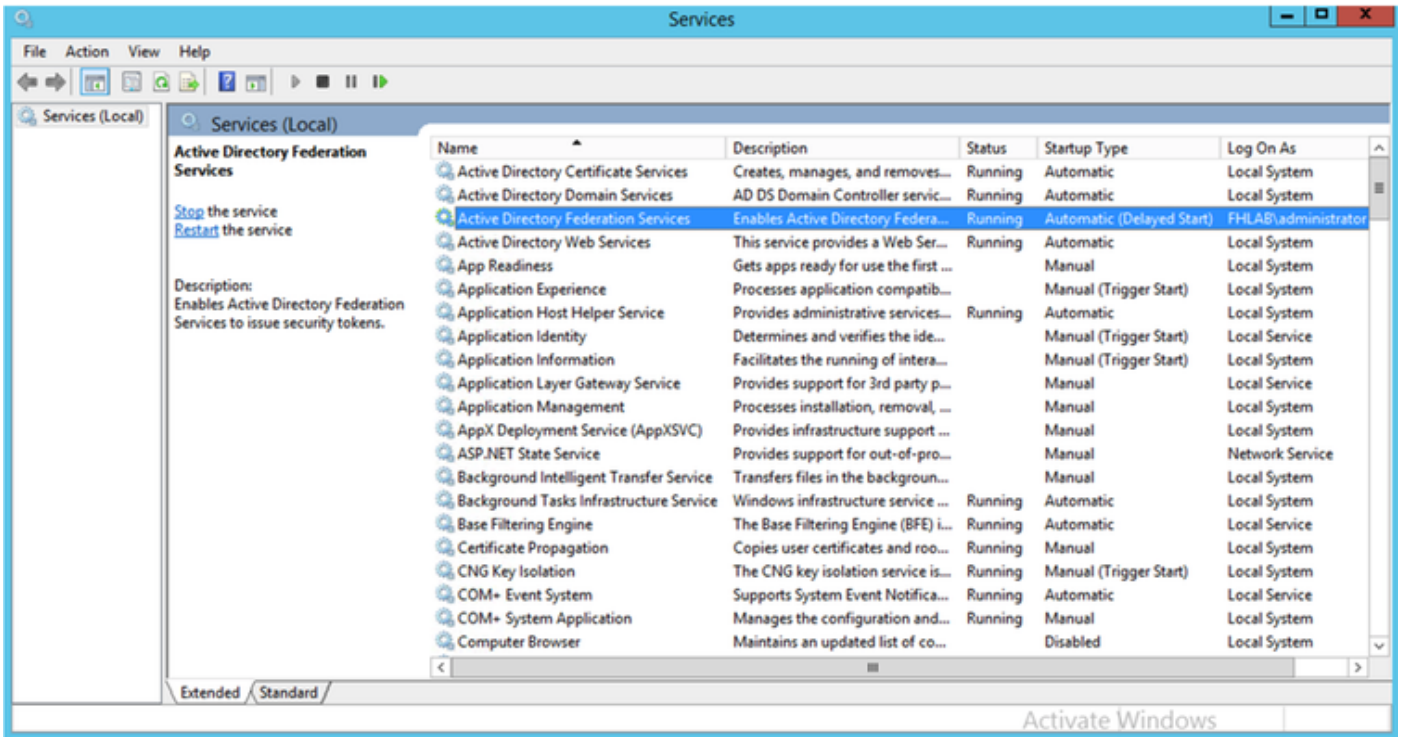
Klicken Sie auf **Fertig stellen**, um fortzufahren.



Sie sollten jetzt zwei Regeln für ADFS definieren. Klicken Sie auf **Übernehmen** und **OK**, um das Regelfenster zu schließen.



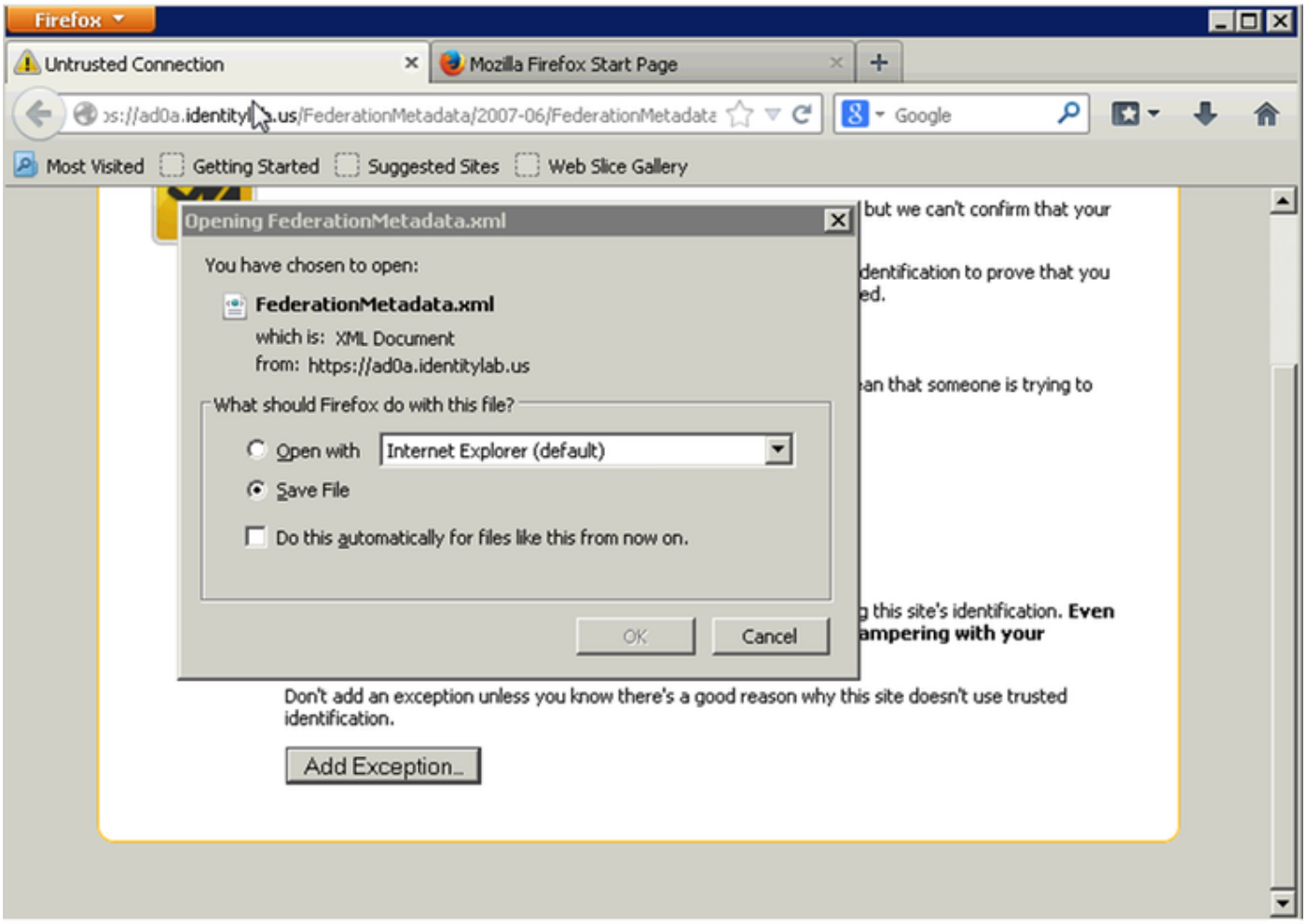
CUCM wird nun erfolgreich als vertrauenswürdiger vertrauender Partei zu ADFS hinzugefügt.



Bevor Sie fortfahren, starten Sie bitte den ADFS-Dienst neu. Navigieren Sie zu **Startmenü > Verwaltung > Dienste**.

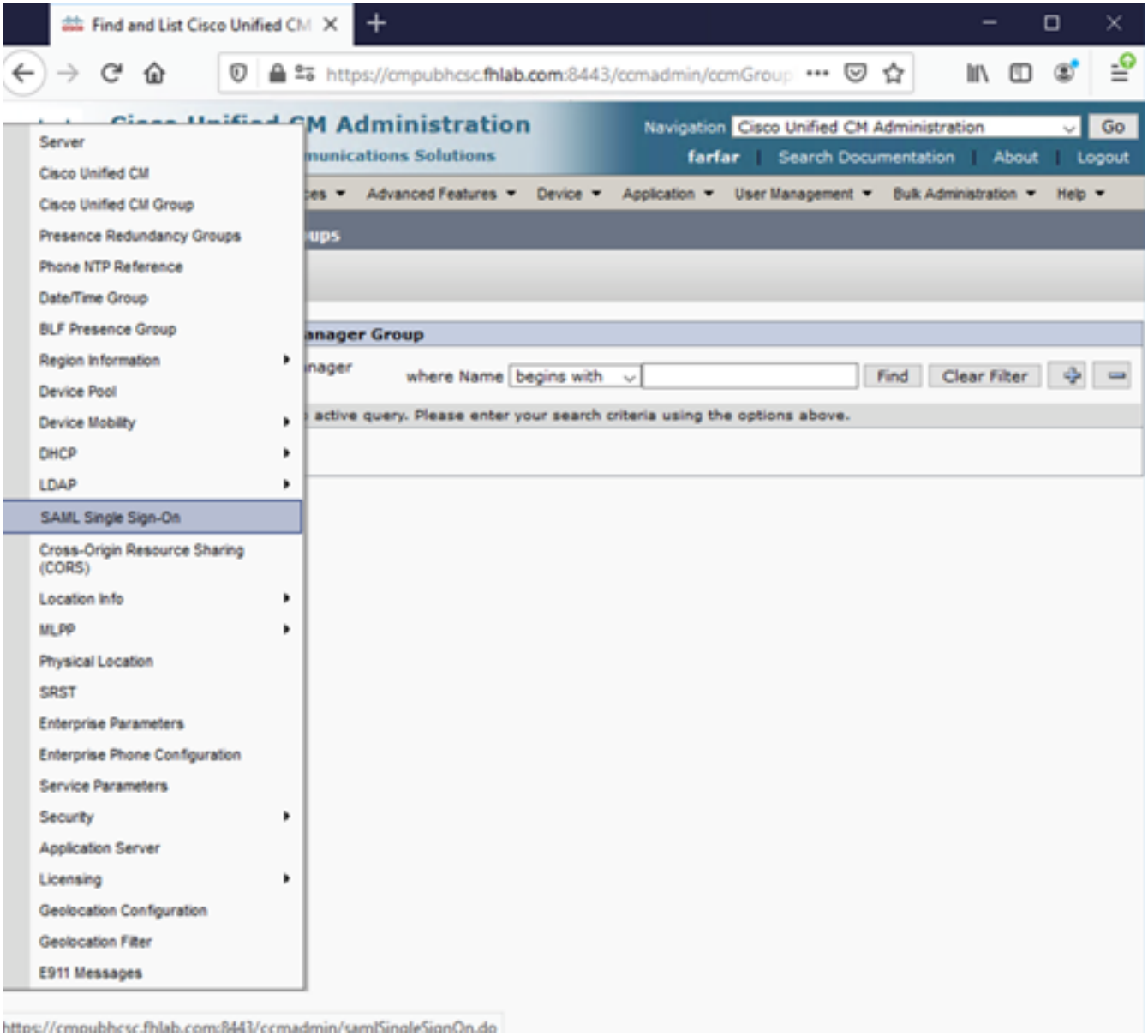
IDP-Metadaten

Sie müssen dem CUCM Informationen zu unserem IDP geben. Diese Informationen werden mithilfe von XML-Metadaten ausgetauscht. Stellen Sie sicher, dass dieser Schritt auf dem Server ausgeführt wird, auf dem ADFS installiert ist.

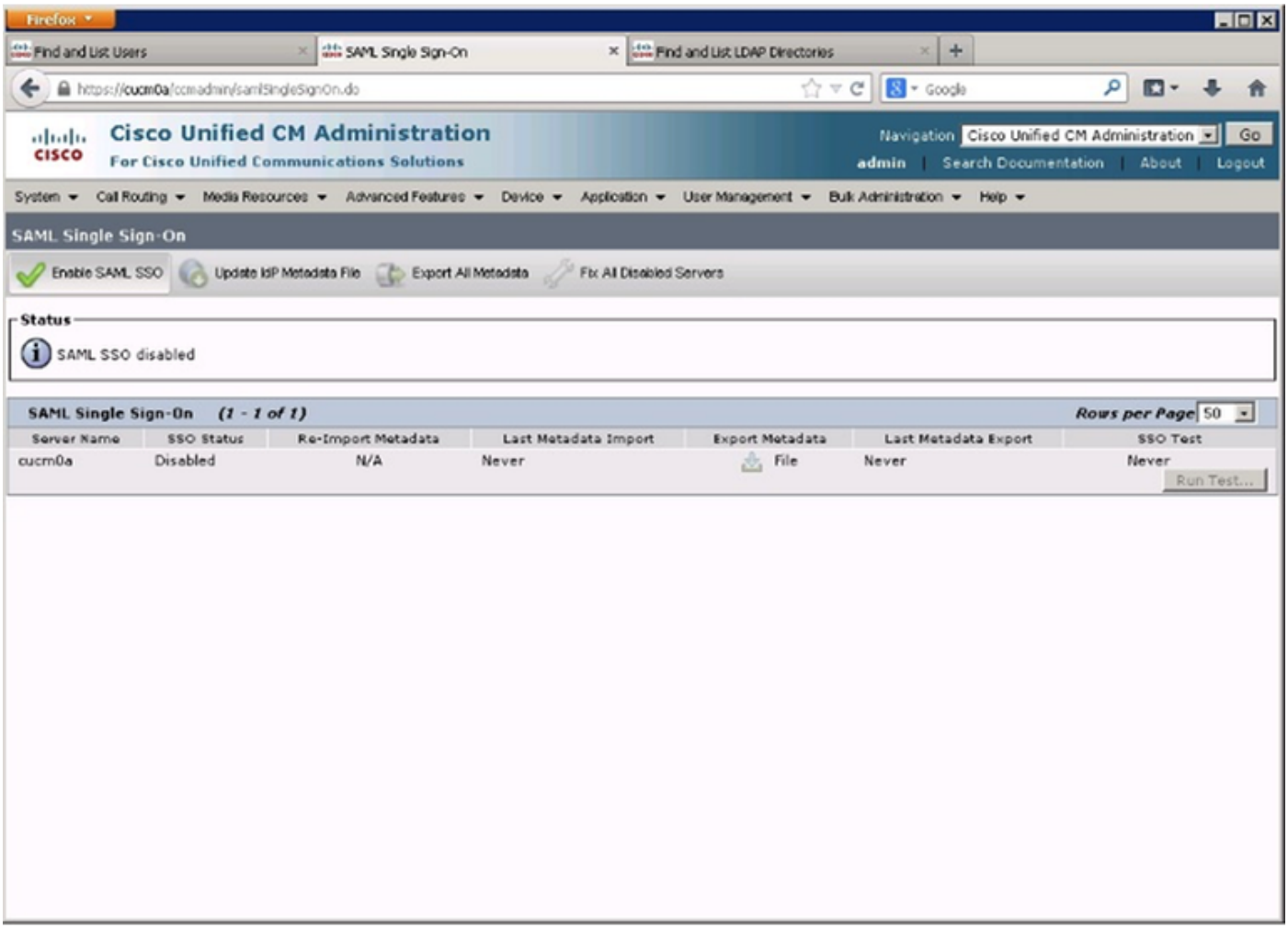


Zuerst müssen Sie eine Verbindung mit dem ADFS (IdP) über einen Firefox-Browser herstellen, um die XML-Metadaten herunterzuladen. Öffnen Sie einen Browser unter https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml, und speichern Sie die Metadaten in einem lokalen Ordner.

Navigieren Sie jetzt zu CUCM-Konfiguration, und wählen Sie **Menü > SAML Single Sign On (Menü für die einmalige Anmeldung) aus**.



Kehren Sie zurück zu CUCM Administration, und wählen Sie **SYSTEM > SAML Single Sign-On aus**.

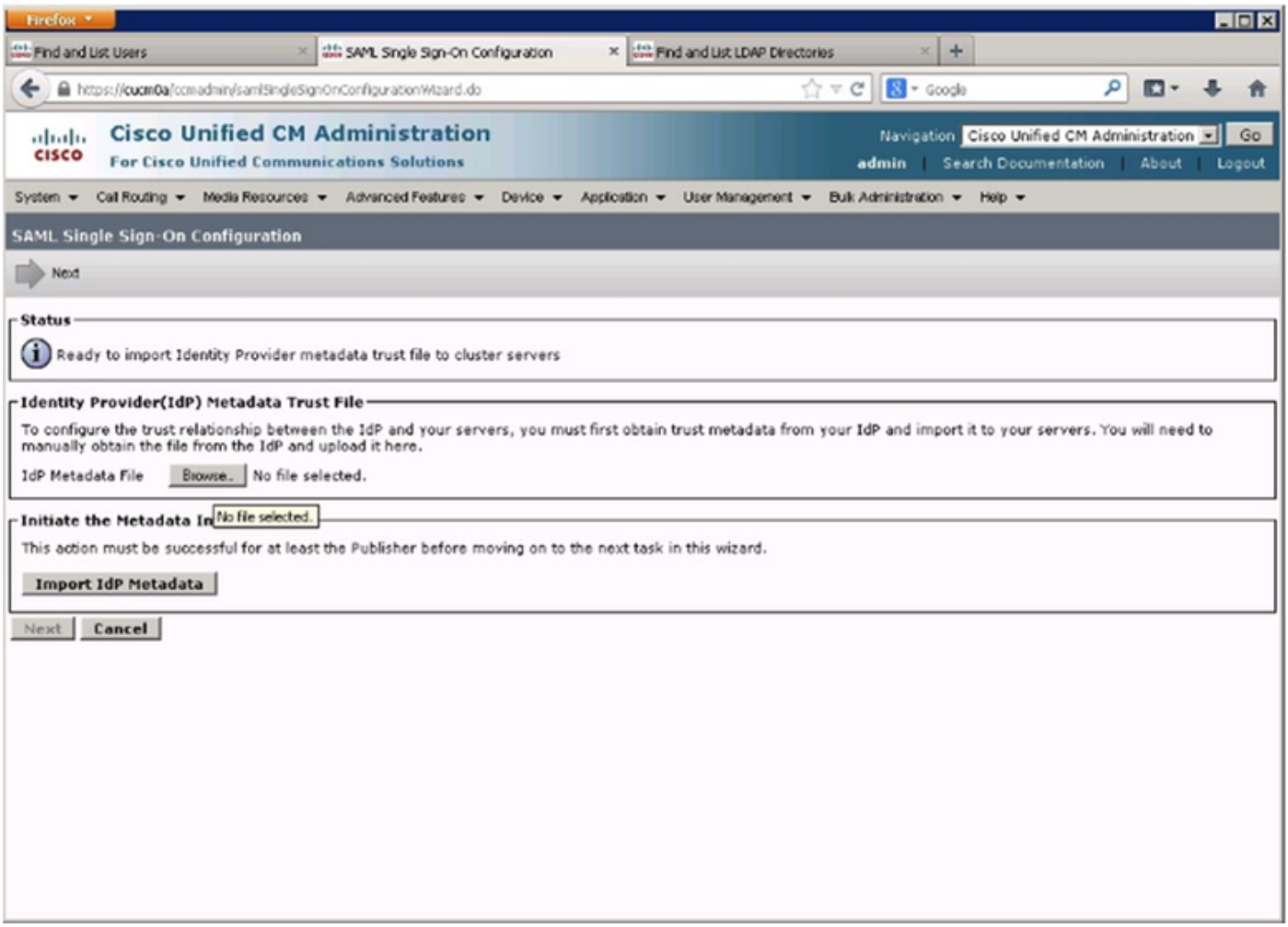


Wählen Sie **SAML-SSO aktivieren aus**.

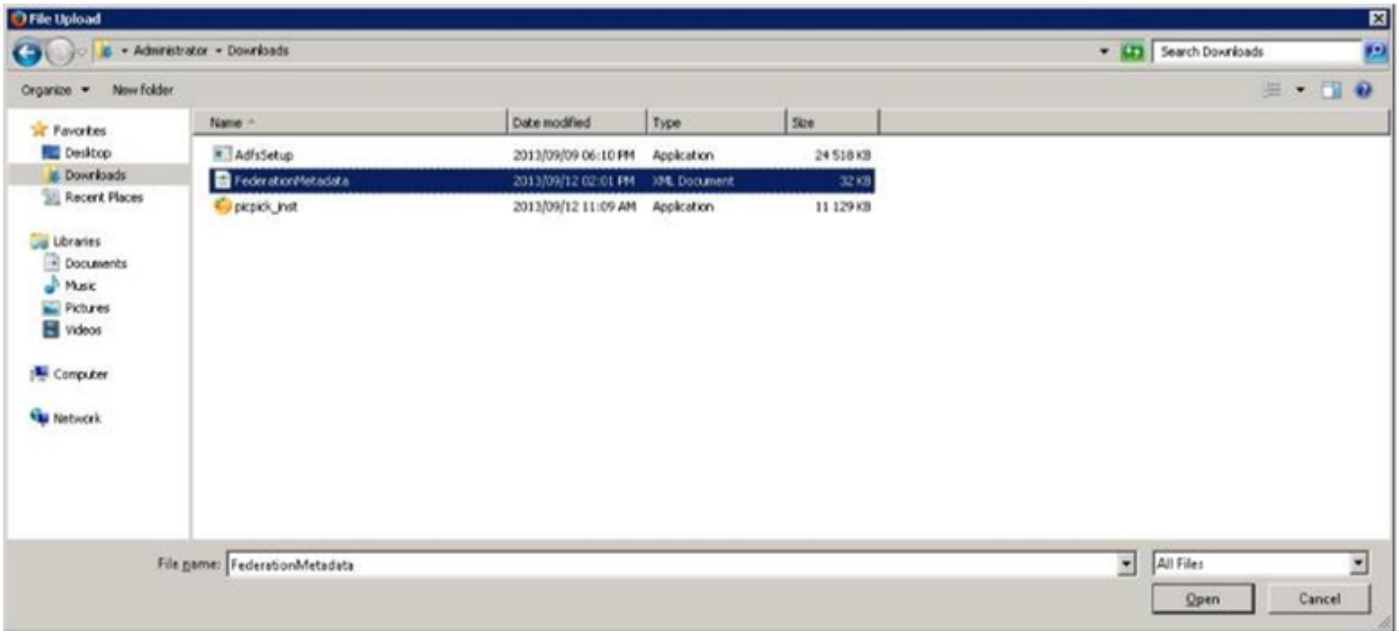
Klicken Sie auf **Weiter**, um die Warnung zu bestätigen.

Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen..** um die XML-Datei

FederationMetadata.xml-Metadaten zu importieren, die Sie zuvor wie im Bild gezeigt gespeichert haben.

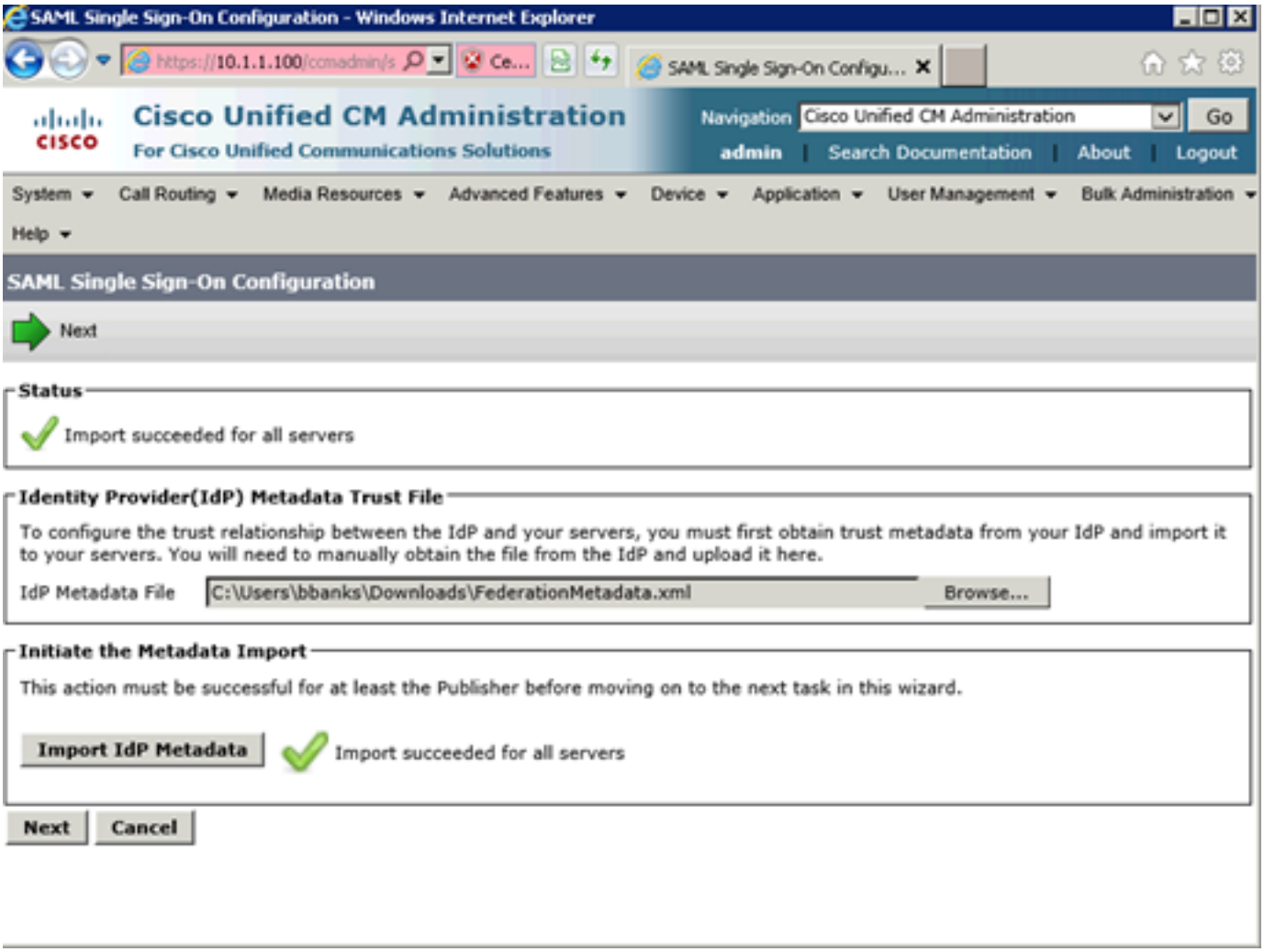


Wählen Sie die XML-Datei aus, und klicken Sie auf **Öffnen**, um sie unter "Favoriten" aus den Downloads in CUCM hochzuladen.

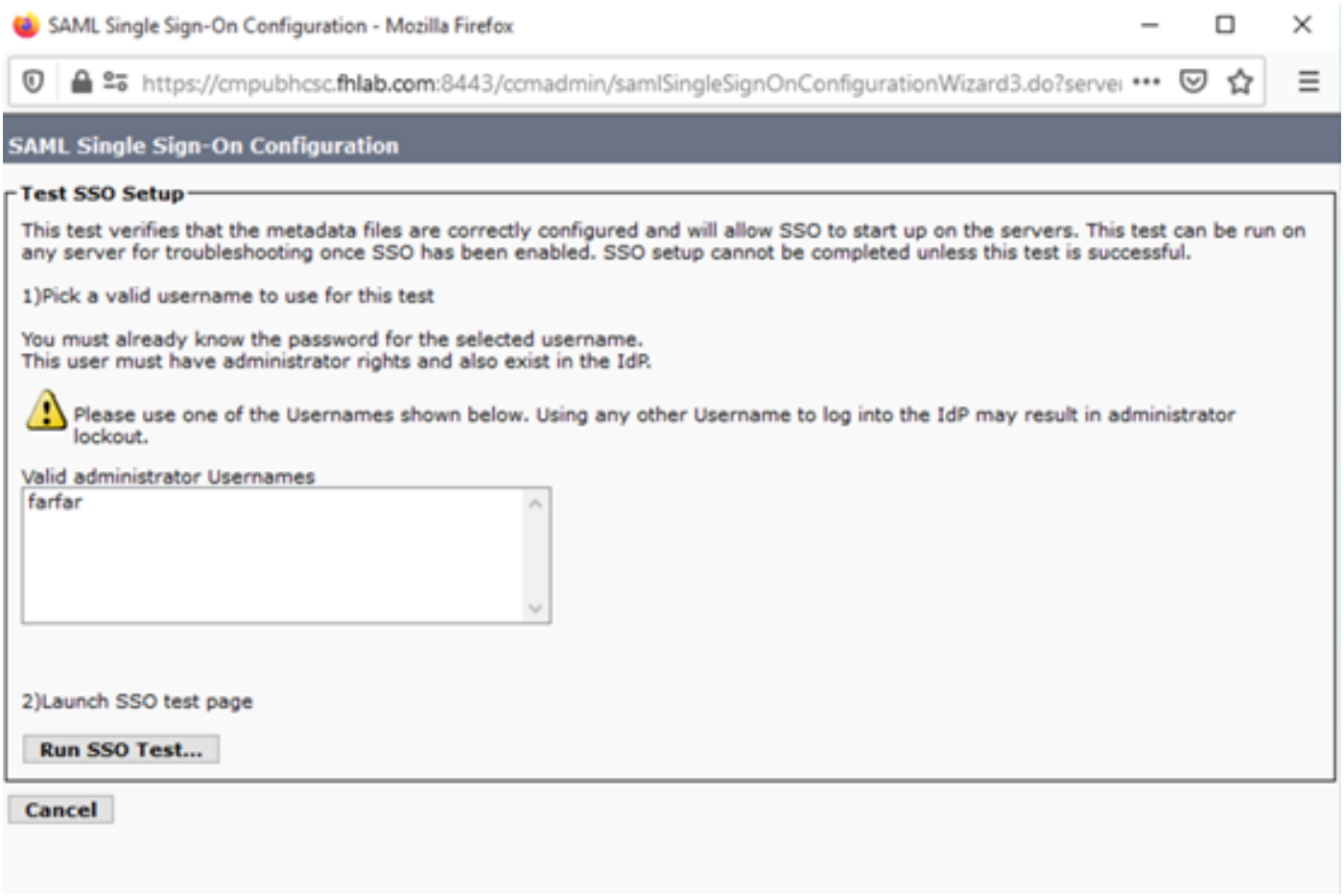


Klicken Sie nach dem Hochladen auf Import IdP Metadata (IDP-Metadaten importieren), um die IDP-Informationen in CUCM zu importieren. Bestätigen Sie, dass der Import erfolgreich war, und

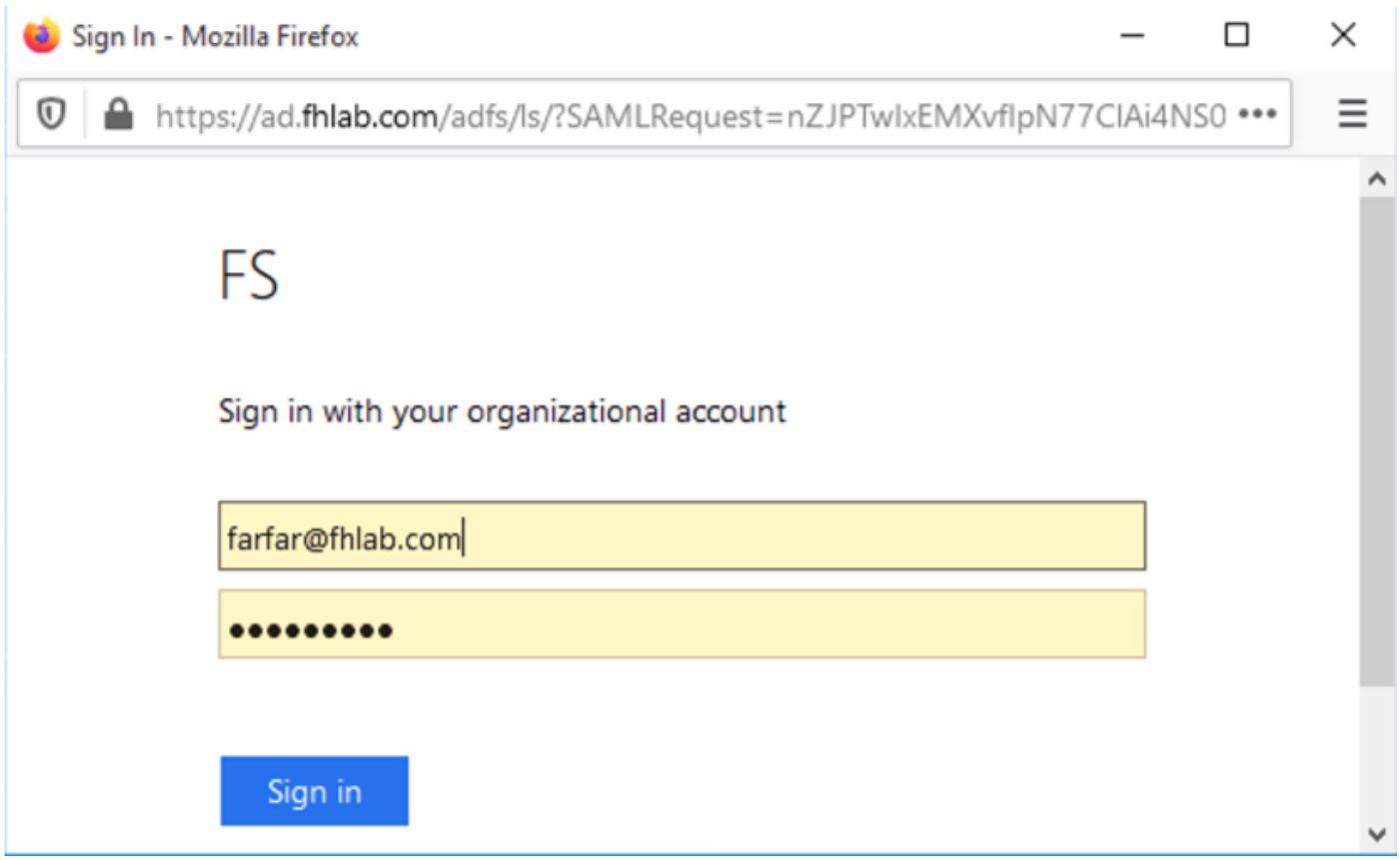
klicken Sie auf Weiter, um fortzufahren.



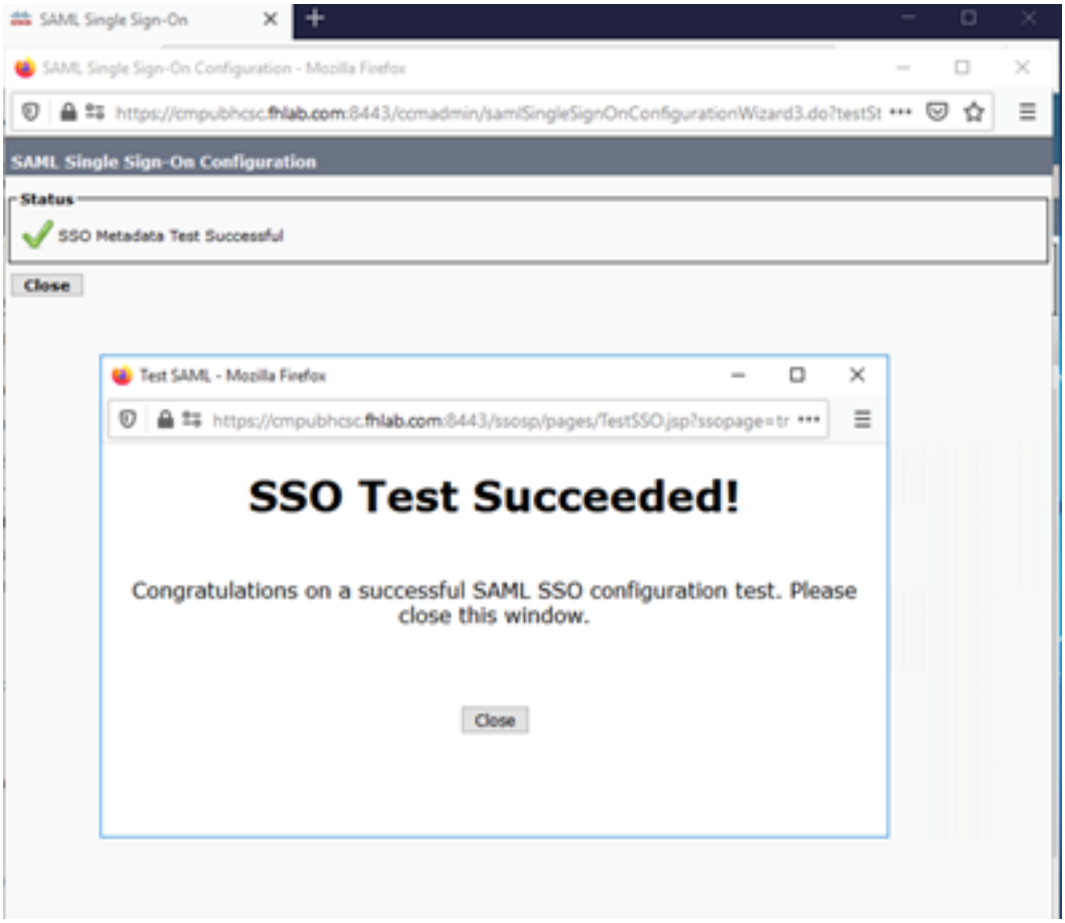
Wählen Sie den Benutzer aus, der dem Standard-CCM-Super-Benutzer angehört, und klicken Sie auf SSO-TEST AUSFÜHREN.



Wenn ein Dialogfeld zur Benutzerauthentifizierung angezeigt wird, melden Sie sich mit dem entsprechenden Benutzernamen und Kennwort an.



Wenn alles korrekt konfiguriert wurde, sollte die Meldung angezeigt werden, dass der SSO-Test erfolgreich durchgeführt wurde.



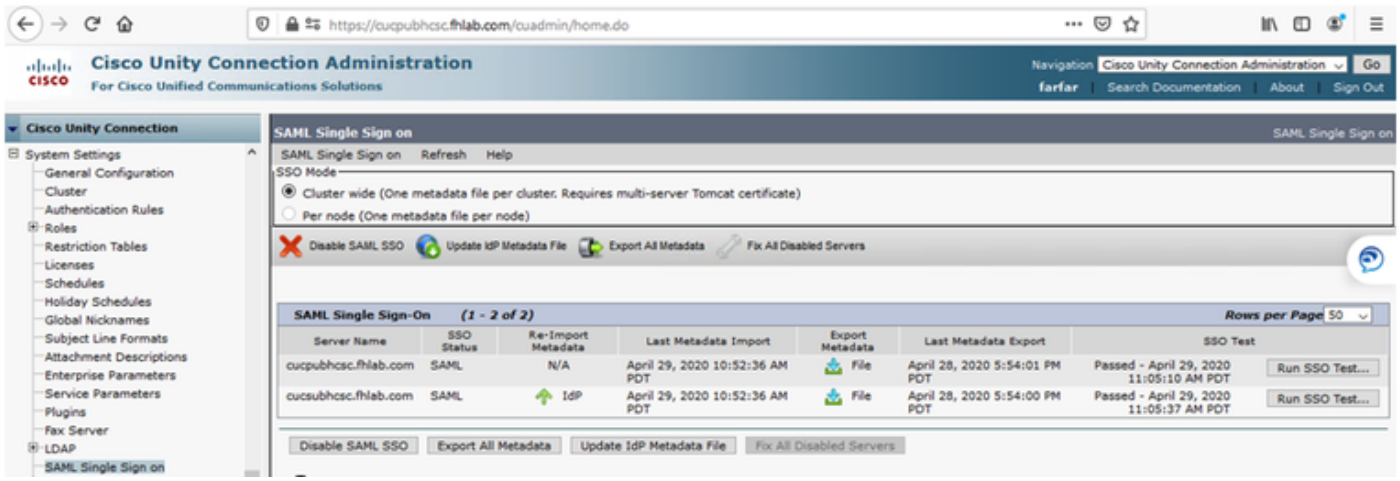
Klicken Sie auf SCHLIESSEN und FERTIG, um fortzufahren.

Die grundlegenden Konfigurationsaufgaben zur Aktivierung von SSO auf CUCM mithilfe von ADFS wurden jetzt erfolgreich abgeschlossen.

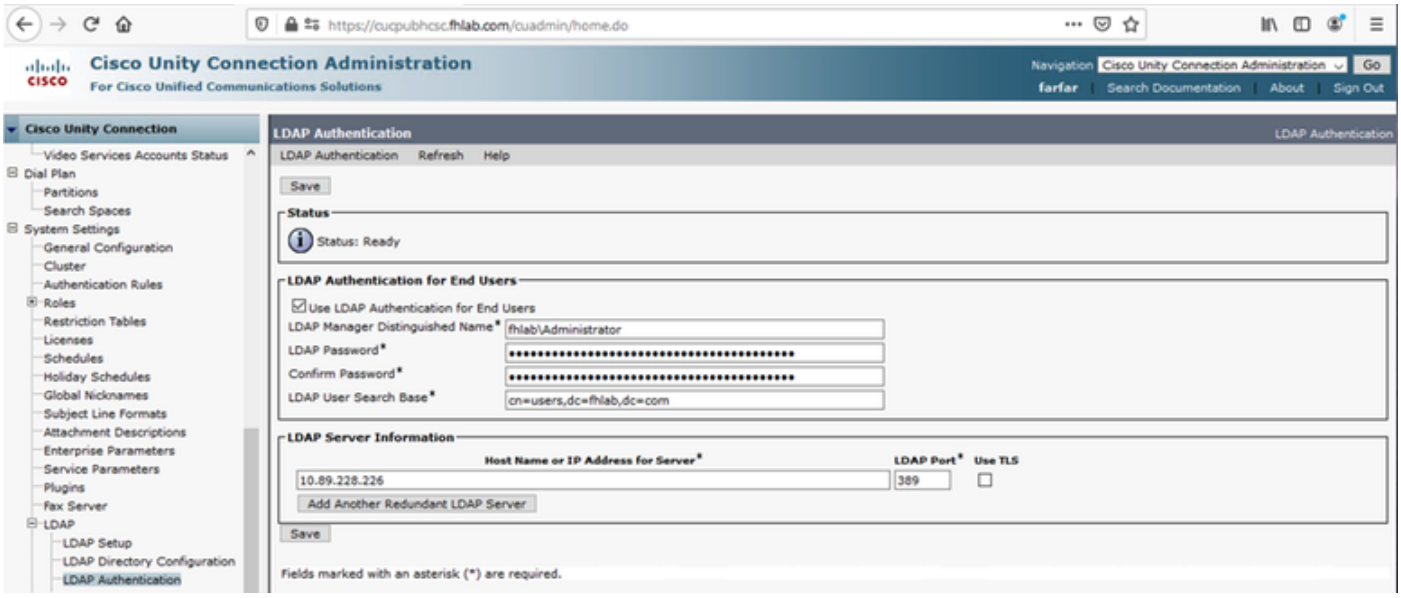
Konfigurieren von SSO auf CUC

Zum Aktivieren von SSO in Unity Connection kann derselbe Prozess ausgeführt werden.

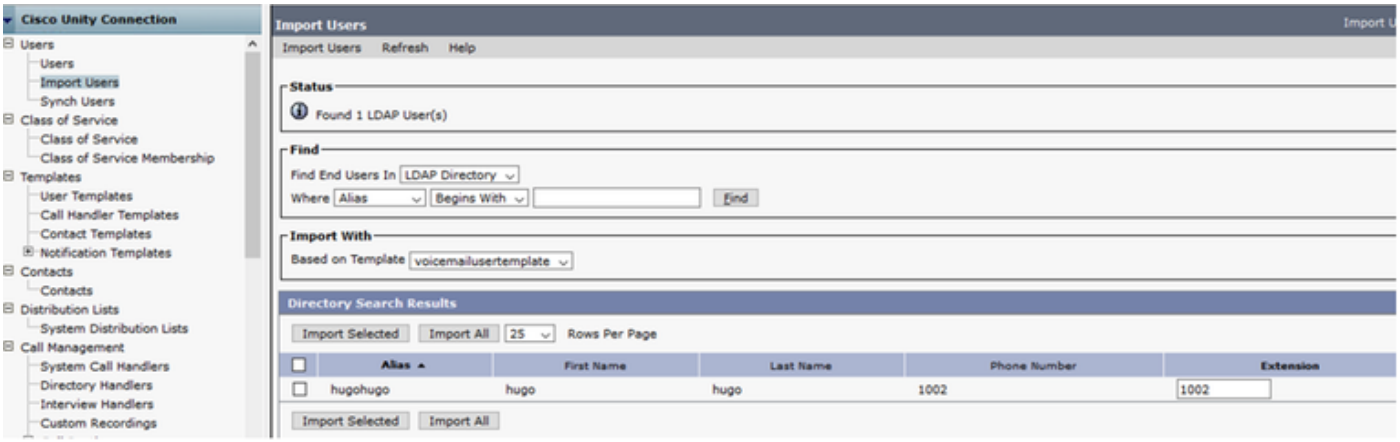
LDAP-Integration mit CUC.



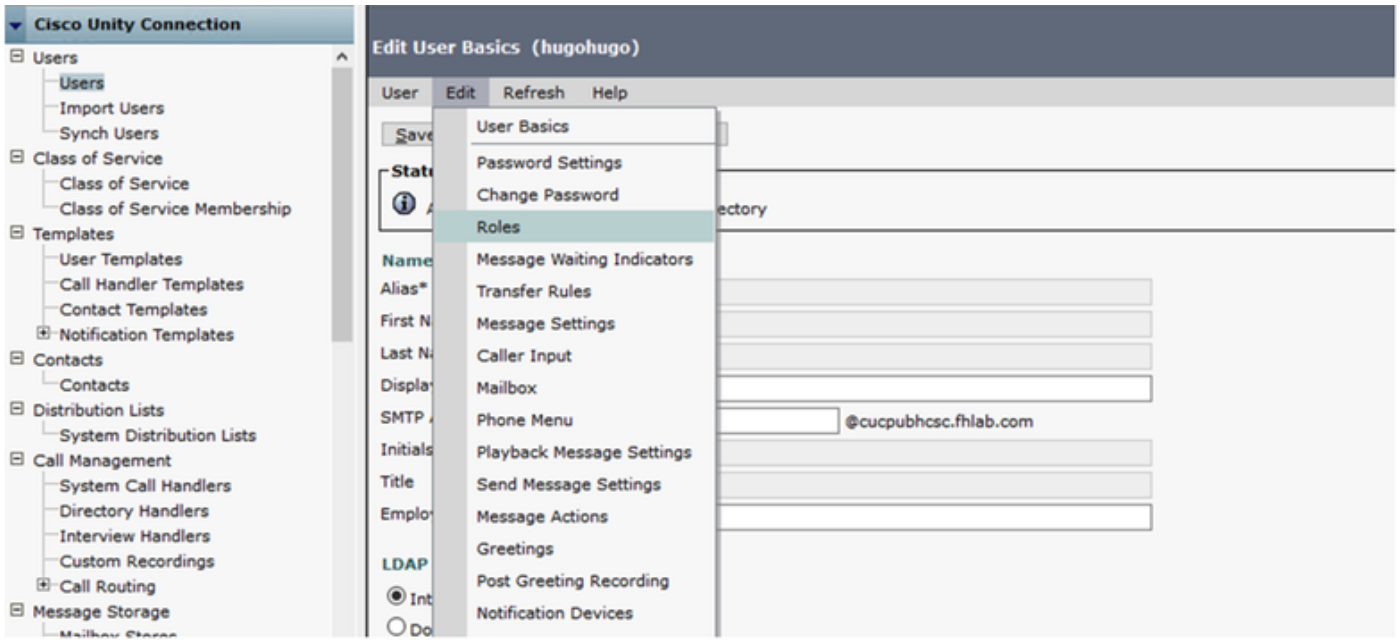
Konfigurieren der LDAP-Authentifizierung



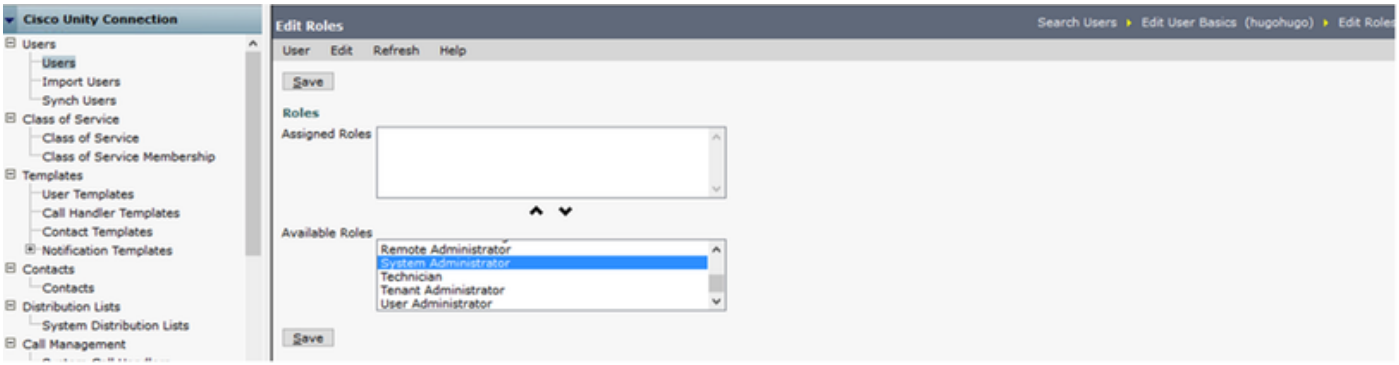
Importieren Sie die Benutzer aus LDAP, denen Voicemail zugewiesen ist, sowie den Benutzer, der für das Testen von SSO verwendet wird.



Navigieren Sie zu **Benutzer > Bearbeiten > Rollen** wie im Bild gezeigt.

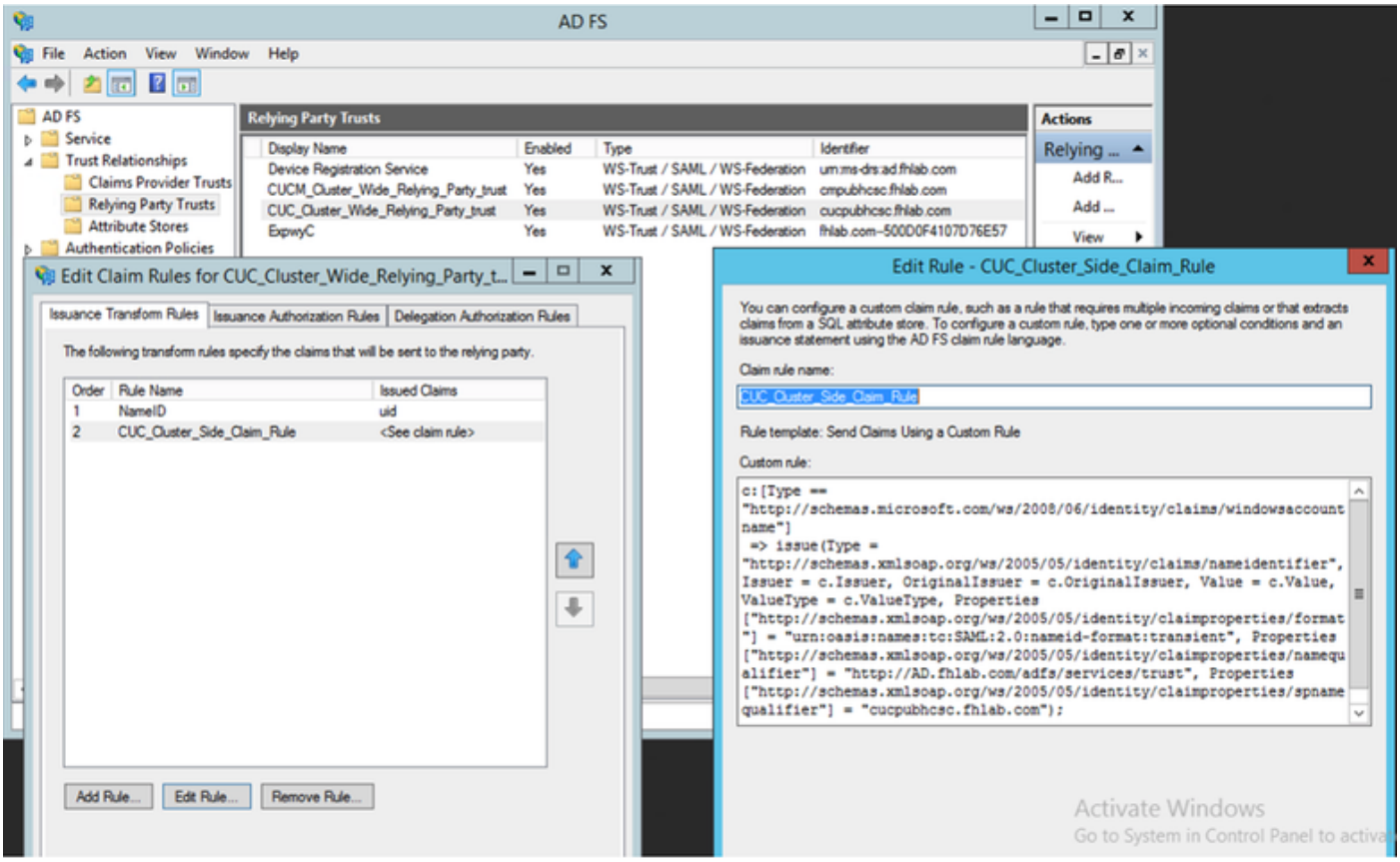


Weisen Sie dem Testbenutzer die Rolle des Systemadministrators zu.

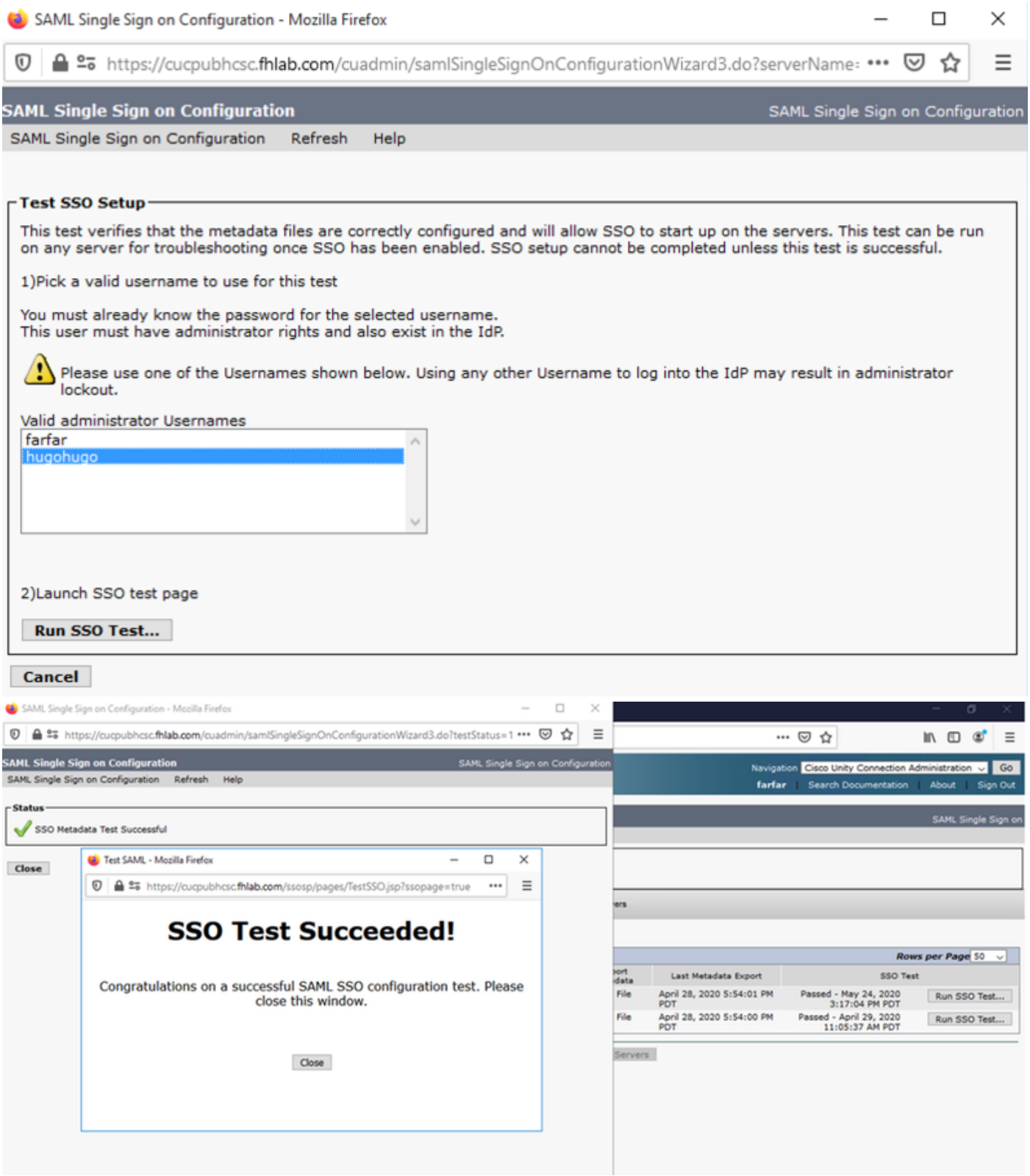


CUC-Metadaten

Sie sollten jetzt CUC-Metadaten heruntergeladen, RelyingPartyTrust für CUC erstellt, CUC-Metadaten hochgeladen und die Regeln erstellt haben, die I AD FS für ADFS 3.0 darstellt.



Gehen Sie zu SAML Single Sign-On und aktivieren Sie SAML SSO.



Konfigurieren von SSO auf Expressway

Metadaten in Expressway C importieren

Öffnen Sie einen Browser unter https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml, und speichern Sie die Metadaten in einem lokalen Ordner.

Upload to **Configuration > Unified Communications > IDP**.

Metadaten aus Expressway C exportieren

Gehen Sie zu configuration -> Unified Communications -> IDP -> SAML-Daten exportieren.

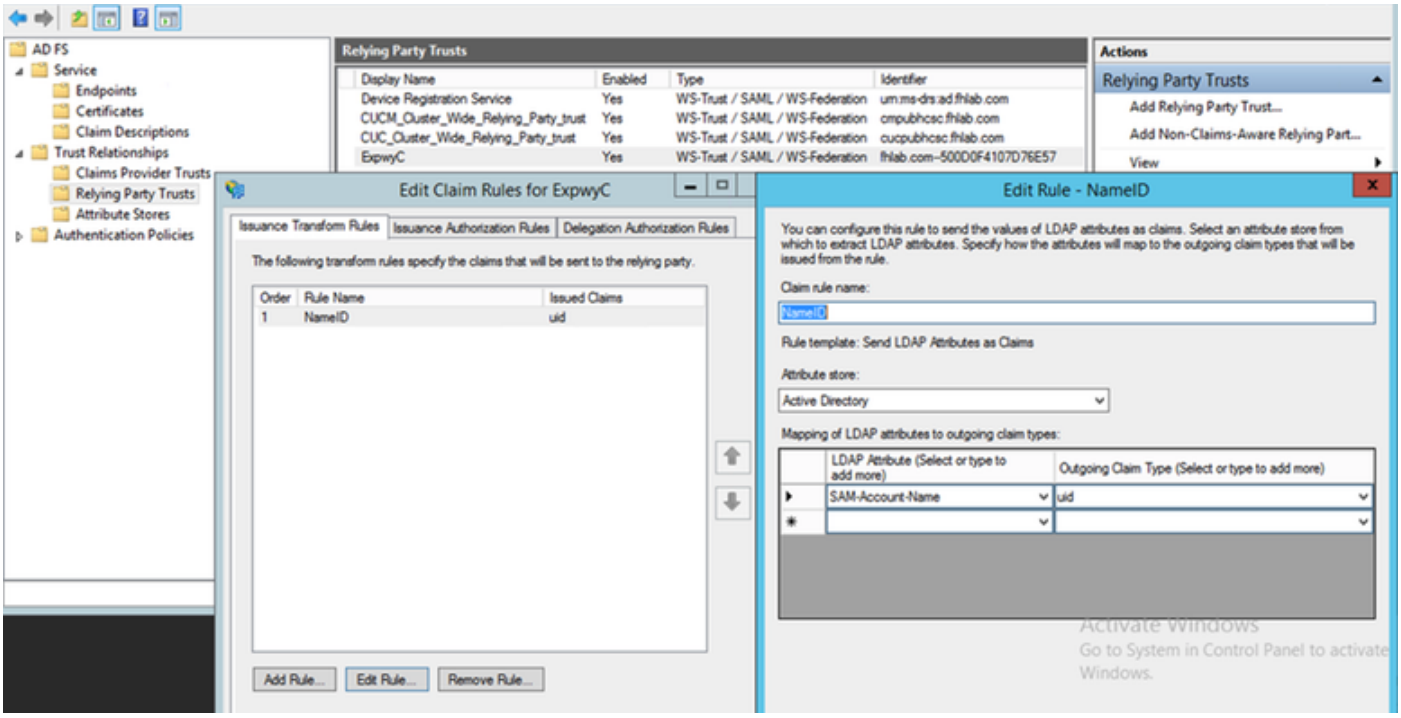
Der Cluster-Modus verwendet ein selbstsigniertes Zertifikat (mit langer Lebensdauer), das in der SAML enthalten ist.

Metadaten und werden zum Signieren von SAML-Anforderungen verwendet

- Klicken Sie im clusterweiten Modus auf Herunterladen der einzelnen clusterweiten Metadatendatei.
- Klicken Sie im Peer-Modus neben dem Peer auf Herunterladen, um die Metadatendatei für einen einzelnen Peer herunterzuladen. Um alle Dateien in eine ZIP-Datei zu exportieren, klicken Sie auf Alle herunterladen.

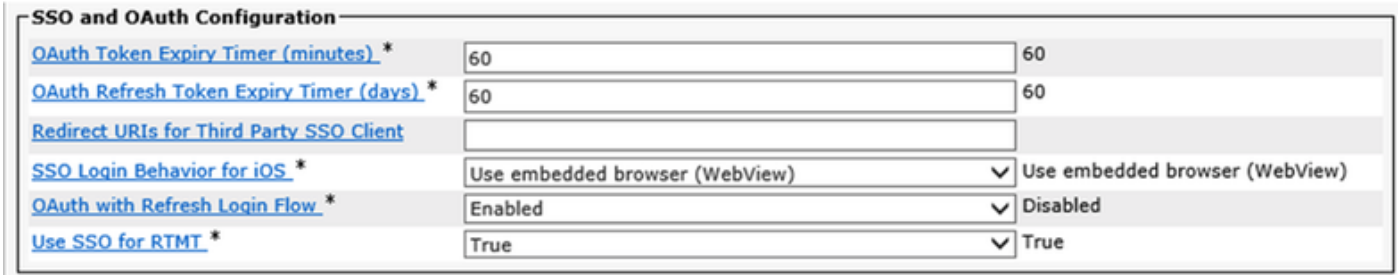
Hinzufügen eines Vertrauens für eine vertrauenswürdige Partei für Cisco Expressway-E

Erstellen Sie zunächst Relying Party Trusts für die Expressway-ES, und fügen Sie dann eine Anspruchsregel hinzu, um Identität als UID-Attribut zu senden.

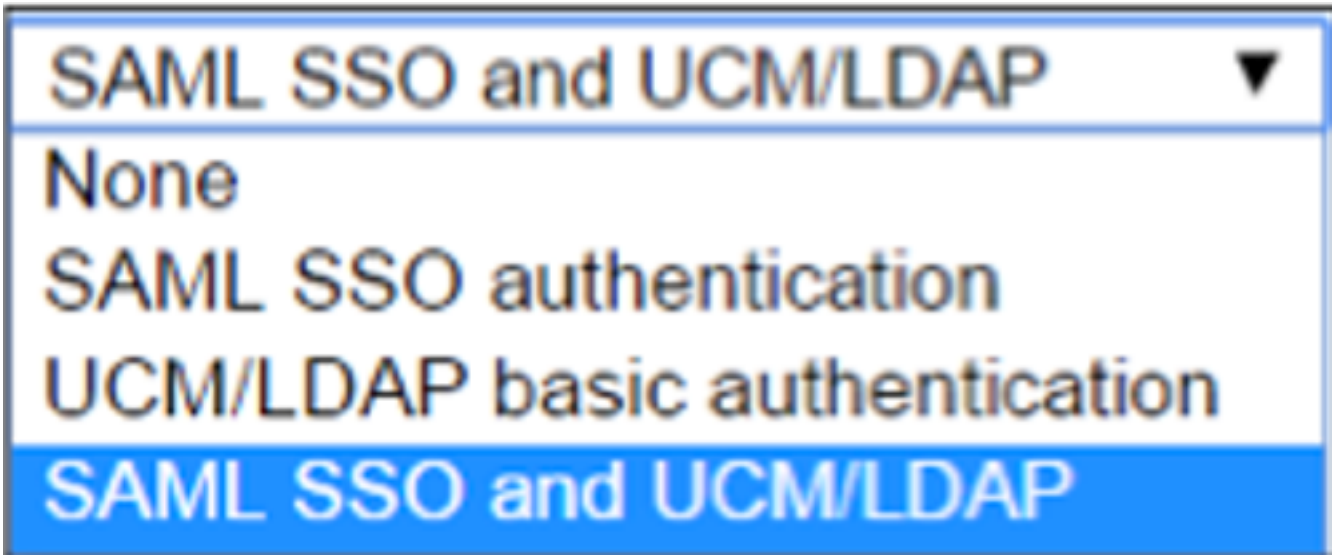


OAuth mit Refresh Login

Überprüfen Sie in Cisco CUCM Enterprise-Parametern, ob der Parameter OAuth with Refresh login flow aktiviert ist. Gehen Sie zu **Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration**.



Authentifizierungspfad



- Wenn der Authentifizierungspfad auf "SAML SSO Authentication" gesetzt ist, können nur Jabber-Clients, die ein SSO-fähiges Unified CM-Cluster verwenden, MRA auf diesem Expressway verwenden. Hierbei handelt es sich um eine Konfiguration, die nur für SSOs gilt.
- Die Expressway-MRA-Unterstützung für alle IP-Telefone, alle TelePresence-Endpunkte und alle Jabber-Clients, die an ein Unified CM-Cluster weitergeleitet werden, das nicht für SSO konfiguriert ist, erfordert den Authentifizierungspfad, um die UCM-/LDAP-Authentifizierung einzuschließen.
- Wenn ein oder mehrere Unified CM-Cluster Jabber SSO unterstützen, wählen Sie "SAML SSO and UCM/LDAP" aus, um sowohl SSO als auch grundlegende Authentifizierung zuzulassen.

SSO-Architektur

SAML ist ein XML-basiertes, auf offenen Standards basierendes Datenformat, mit dem Administratoren nach der Anmeldung bei einer dieser Anwendungen problemlos auf bestimmte Cisco Collaboration-Anwendungen zugreifen können. SAML SSO verwendet das SAML 2.0-Protokoll, um domänenübergreifende und produktübergreifende einmalige Anmeldung für Cisco Collaboration-Lösungen zu ermöglichen.

Anmeldungsablauf am Standort

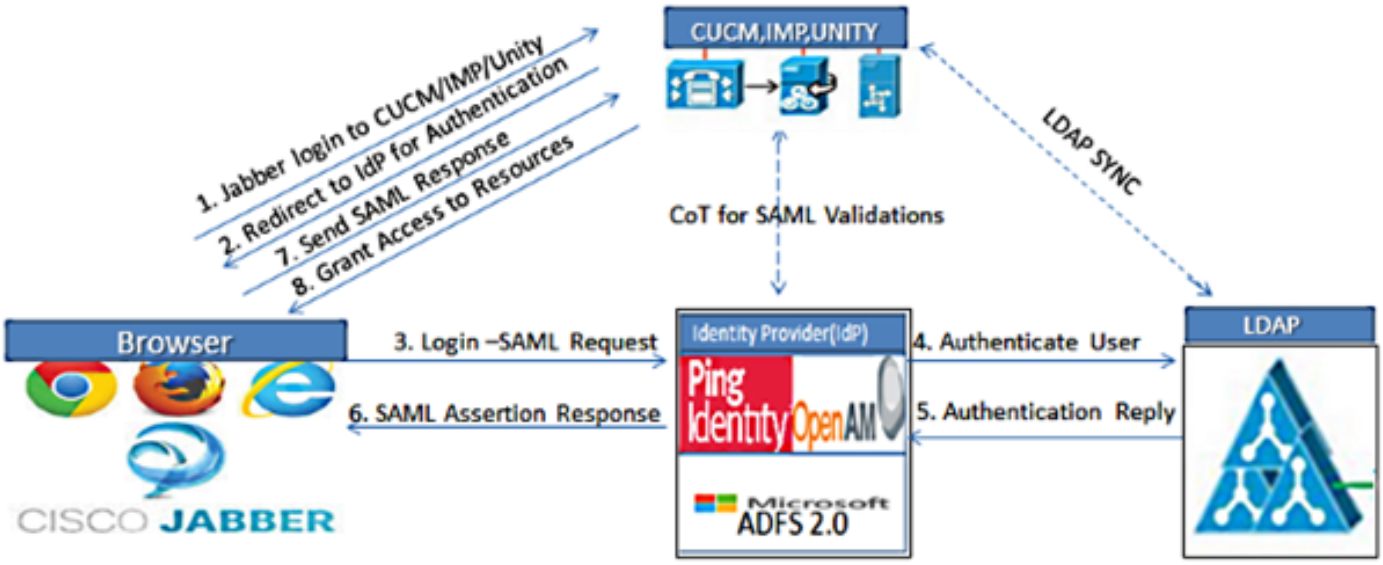
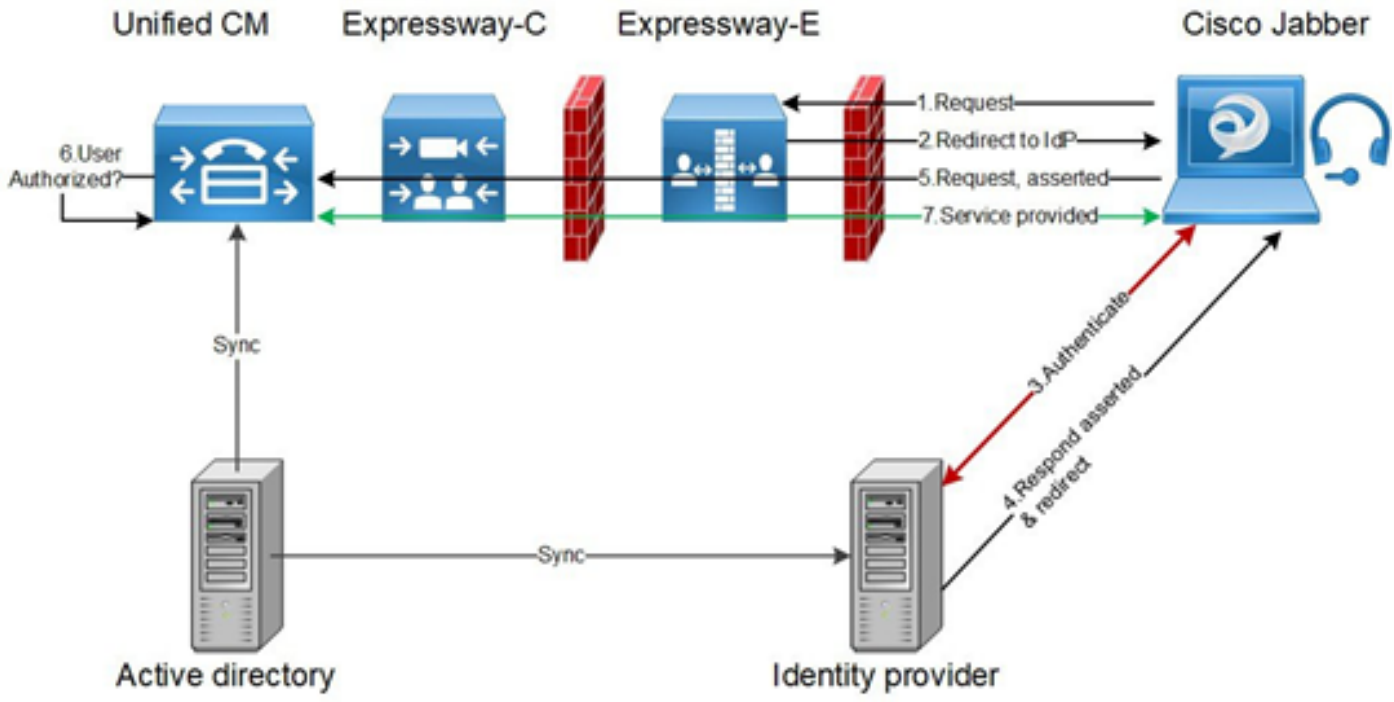


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA-Anmeldeablauf



OAuth

OAuth ist ein Standard, der die Autorisierung unterstützt. Ein Benutzer muss authentifiziert werden, bevor er autorisiert werden kann. Der Autorisierungscode-Grant-Flow stellt eine Methode bereit, mit der ein Client auf Zugriffs- und Aktualisierungs-Token zugreifen kann, um auf eine Ressource zuzugreifen (Unified CM-, IM&P-, Unity- und Expressway-Dienste). Dieser Datenfluss basiert auch auf Umleitung und erfordert daher, dass der Client mit einem vom Benutzer gesteuerten HTTP-User-Agent (Webbrowser) interagieren kann. Der Client stellt eine erste Anforderung an den Autorisierungsserver über HTTPS. Der OAuth-Server leitet den Benutzer an einen Authentifizierungsdienst um. Diese kann auf Unified CM oder einer externen IDP ausgeführt werden, wenn SAML SSO aktiviert ist. Je nach verwendeter Authentifizierungsmethode kann dem

Endbenutzer eine Webseitenansicht zur Selbstauthentifizierung angezeigt werden. (Die Kerberos-Authentifizierung ist ein Beispiel, das keine Webseite anzeigen würde.) Im Gegensatz zum impliziten Grant-Flow führt ein erfolgreicher Grant-Fluss dazu, dass die OAuth-Server dem Webbrowser einen "Autorisierungscode" ausgeben. Hierbei handelt es sich um einen einmaligen, kurzlebigen eindeutigen Code, der dann vom Webbrowser an den Client zurückgegeben wird. Der Client stellt dem Autorisierungsserver diesen "Autorisierungscode" zusammen mit einem vorinstallierten geheimen Schlüssel zur Verfügung und erhält im Austausch ein "Zugriffstoken" und ein "Aktualisierungstoken". Der in diesem Schritt verwendete Clientgeheim ermöglicht es dem Autorisierungsdienst, die Verwendung auf registrierte und authentifizierte Clients zu beschränken. Die Token werden für folgende Zwecke verwendet:

Zugriffs-/Aktualisierungstoken

Zugriffs-Token: Dieses Token wird vom Autorisierungsserver ausgegeben. Der Client stellt das Token einem Ressourcenserver zur Verfügung, wenn er auf geschützte Ressourcen auf diesem Server zugreifen muss. Der Ressourcenserver kann das Token validieren und Verbindungen mithilfe des Tokens vertrauen. (Cisco Access Token haben standardmäßig eine Lebensdauer von 60 Minuten.)

Aktualisierungstoken: Dieses Token wird erneut vom Autorisierungsserver ausgegeben. Der Client stellt dieses Token zusammen mit dem Clientgeheimnis dem Autorisierungsserver zur Verfügung, wenn das Zugriffstoken abgelaufen ist oder abläuft. Wenn das Aktualisierungstoken noch gültig ist, gibt der Autorisierungsserver ein neues Zugriffstoken aus, ohne dass eine weitere Authentifizierung erforderlich ist. (Die Standardeinstellung der Cisco Refresh Tokens beträgt 60 Tage.) Wenn das Aktualisierungstoken abgelaufen ist, muss ein neuer vollständiger OAuth-Autorisierungscode-Fluss initiiert werden, um neue Token zu erhalten.

Der Ablauf der OAuth-Autorisierungscodes für die Gewährung ist besser

Im impliziten Grant-Flow wird das Zugriffstoken über einen HTTP-Benutzer-Agent (Browser) an den Jabber-Client übergeben. Im Berechtigungscode-Grant-Fluss wird das Zugriffstoken direkt zwischen dem Autorisierungsserver und dem Jabber-Client ausgetauscht. Das Token wird mithilfe eines zeitlich begrenzten eindeutigen Autorisierungscodes vom Autorisierungsserver angefordert. Dieser direkte Austausch des Zugriffs-Tokens ist sicherer und reduziert das Risiko.

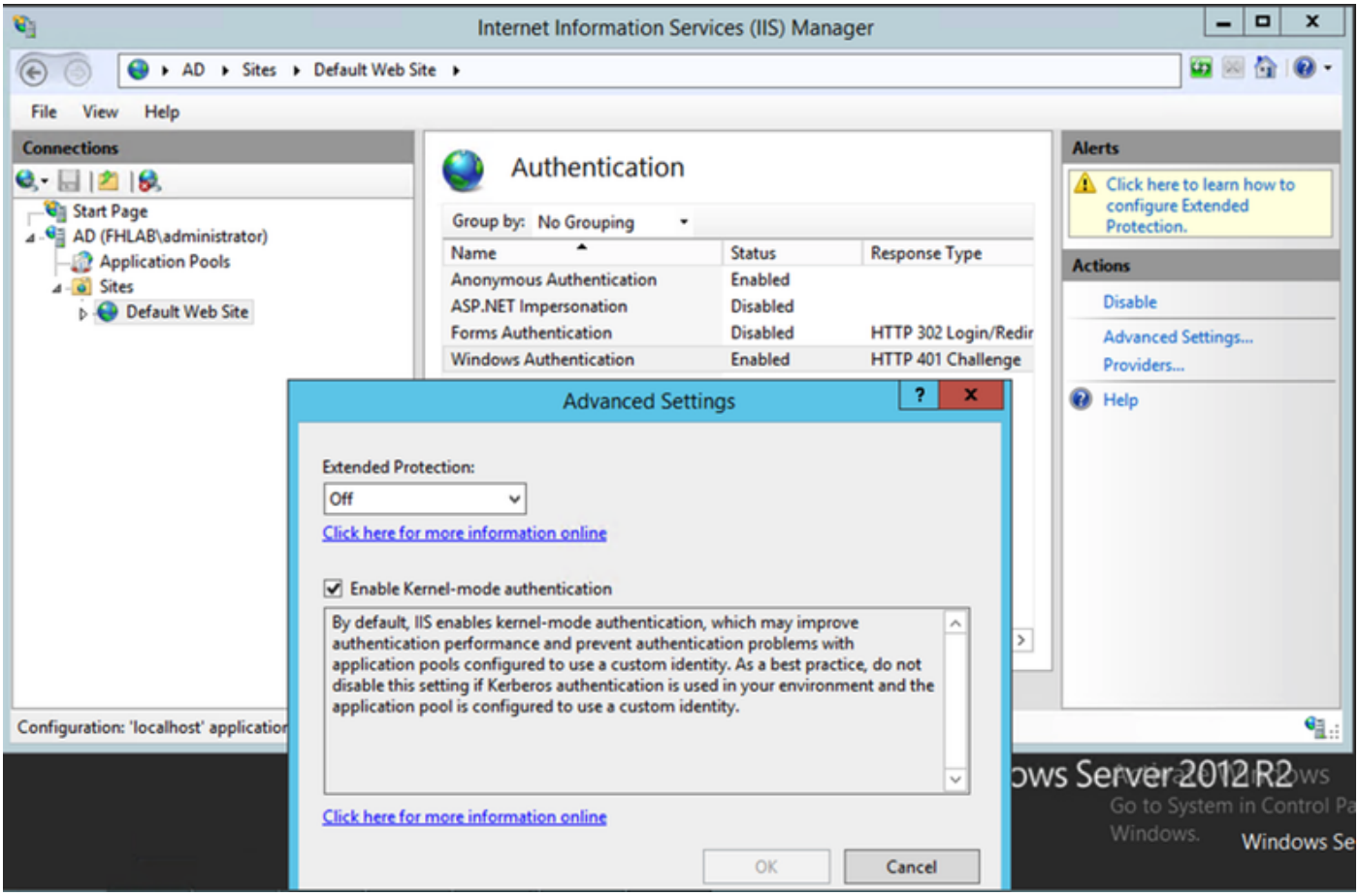
Der OAuth-Autorisierungscode-Grant-Fluss unterstützt die Verwendung von Aktualisierungstoken. Dies verbessert die Benutzerfreundlichkeit, da die Benutzer sich nicht so häufig erneut authentifizieren müssen (standardmäßig 60 Tage).

Konfigurieren von Kerberos

Windows-Authentifizierung auswählen

Internetinformationsdienste-Manager (IIS) > Sites > Default Web Site > Authentication > Windows Authentication > Advance Settings.

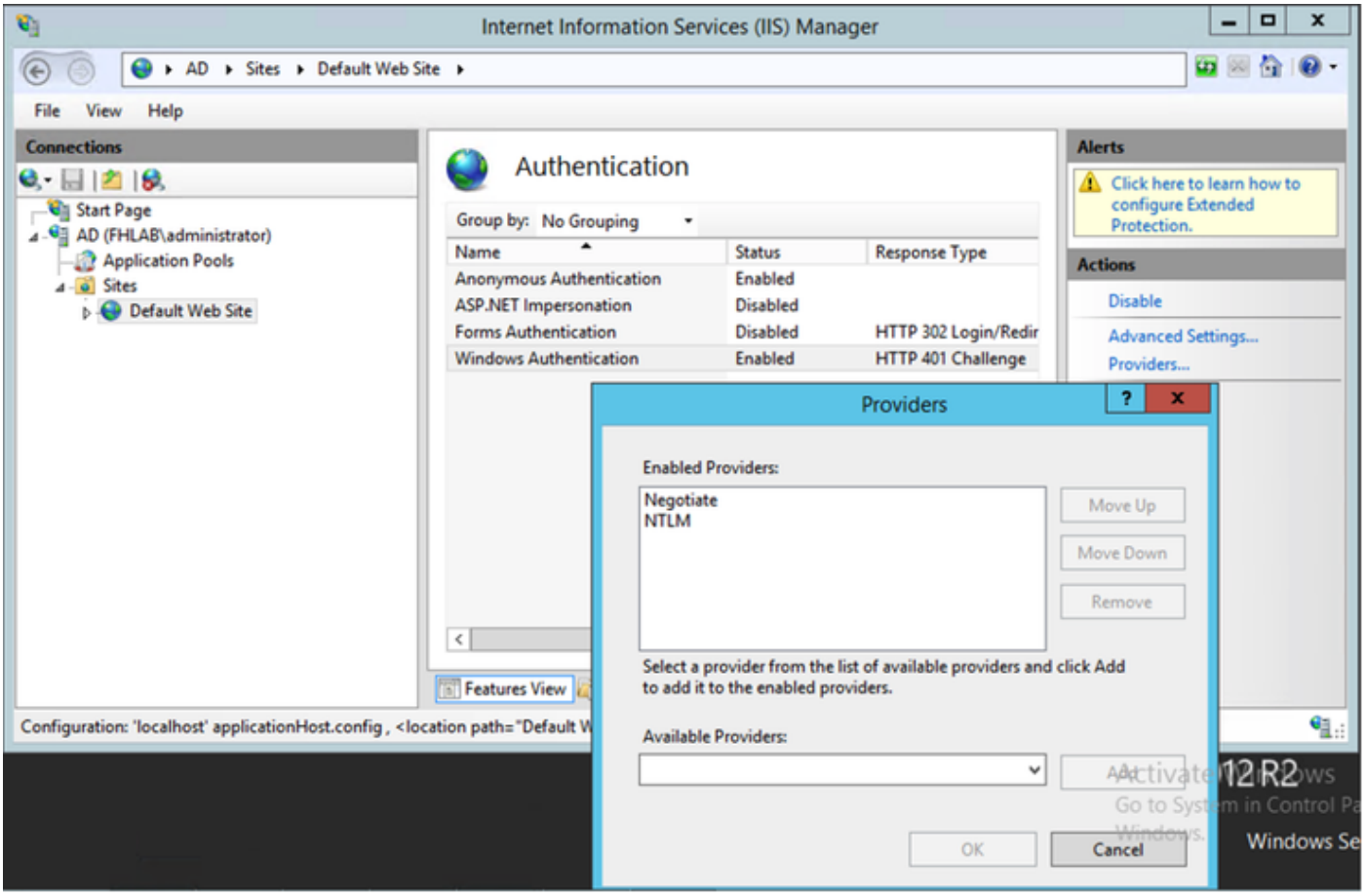
1. Deaktivieren Sie Kernel-Modus-Authentifizierung aktivieren.
2. Stellen Sie sicher, dass der erweiterte Schutz deaktiviert ist.



ADFS unterstützt beide Kerberos NTLM

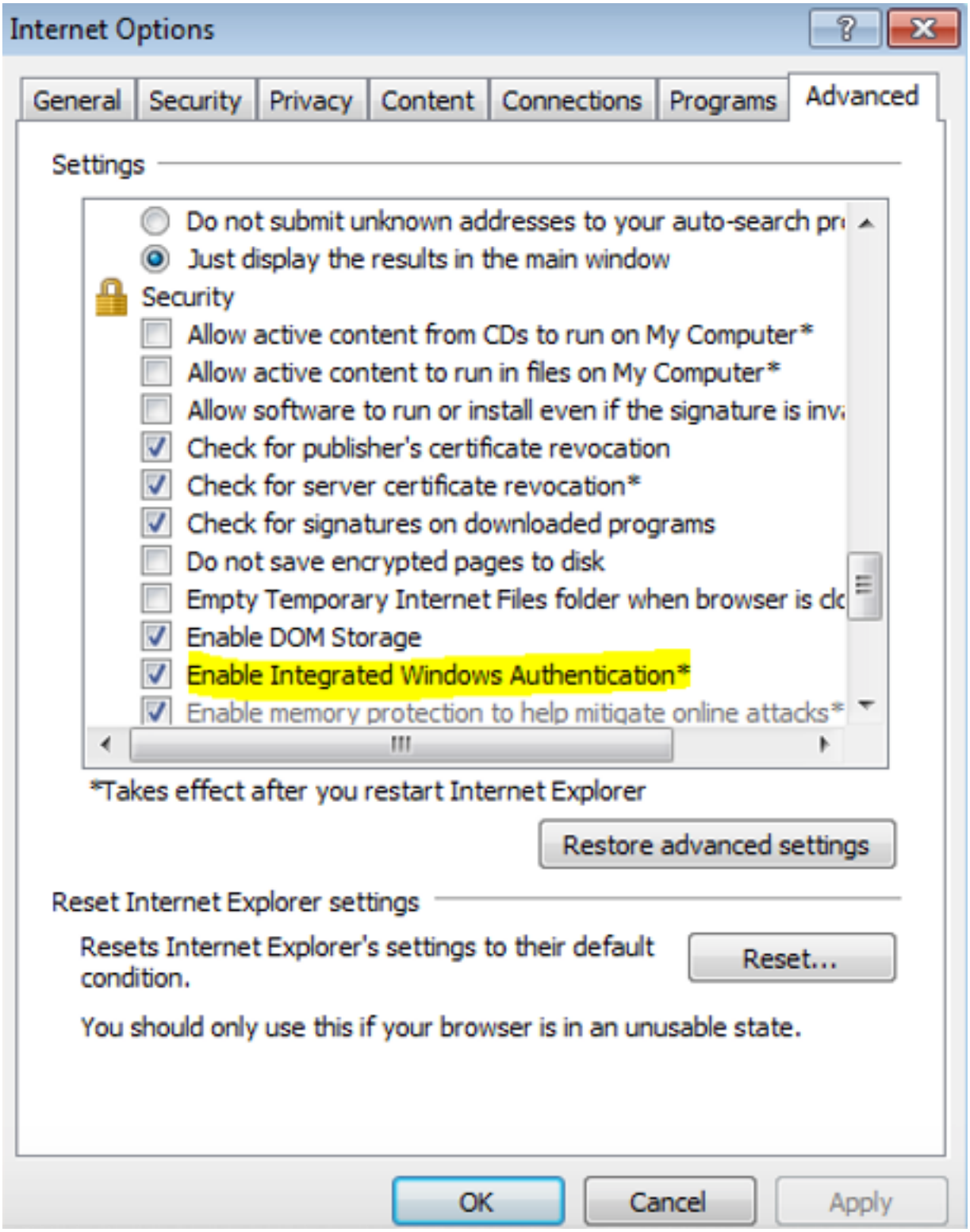
Stellen Sie sicher, dass AD FS Version 3.0 sowohl das Kerberos-Protokoll als auch das NT LAN Manager-Protokoll (NTLM) unterstützt, da alle Nicht-Windows-Clients Kerberos nicht verwenden können und sich auf NTLM verlassen.

Wählen Sie im rechten Teilfenster Anbieter aus, und stellen Sie sicher, dass Negotiate und NTLM unter Enabled Providers (Aktivierte Anbieter) vorhanden sind:



Konfigurieren von Microsoft Internet Explorer

Stellen Sie sicher, dass **Internet Explorer > Erweitert > Integrierte Windows-Authentifizierung aktivieren** aktiviert ist.



ADFS-URL unter Sicherheit > Intranetzonen > Standorte hinzufügen