

Eenmalige aanmelding configureren met CUCM en AD FS 2.0

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Download en installeer AD FS 2.0 op uw Windows-server](#)
- [AD FS 2.0 configureren op uw Windows-server](#)
- [Importeer de Idp Metadata naar CUCM / Download de CUCM Metadata](#)
- [CUCM Metadata importeren naar AD FS 2.0-server en claimregels maken](#)
- [SSO-activering op CUCM voltooien en de SSO-test uitvoeren](#)
- [Problemen oplossen](#)
- [Debuggen van SSO-logbestanden instellen](#)
- [Zoek de federatie service naam](#)
- [Servicenaam voor Dotless Certificaat en Federatie](#)
- [De tijd is niet synchroon tussen de CUCM- en IDP-servers](#)
- [Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Single Sign-On (SSO) kunt configureren op Cisco Unified Communications Manager en Active Directory Federation Service.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM)
- Basiskennis van Active Directory Federation Service (AD FS)

Om SSO in uw laboratoriummilieu toe te laten, hebt u deze configuratie nodig:

- Windows Server met AD FS geïnstalleerd.
- CUCM met LDAP-sync geconfigureerd.
- Een eindgebruiker met de Standaard CCM Super Gebruikers rol geselecteerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows-server met AD FS 2.0
- CUCM 10.5.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle

apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De procedure voor AD FS 2.0 met Windows Server 2008 R2 is beschikbaar. Deze stappen werken ook voor AD FS 3.0 op Windows Server 2016.

Download en installeer AD FS 2.0 op uw Windows-server

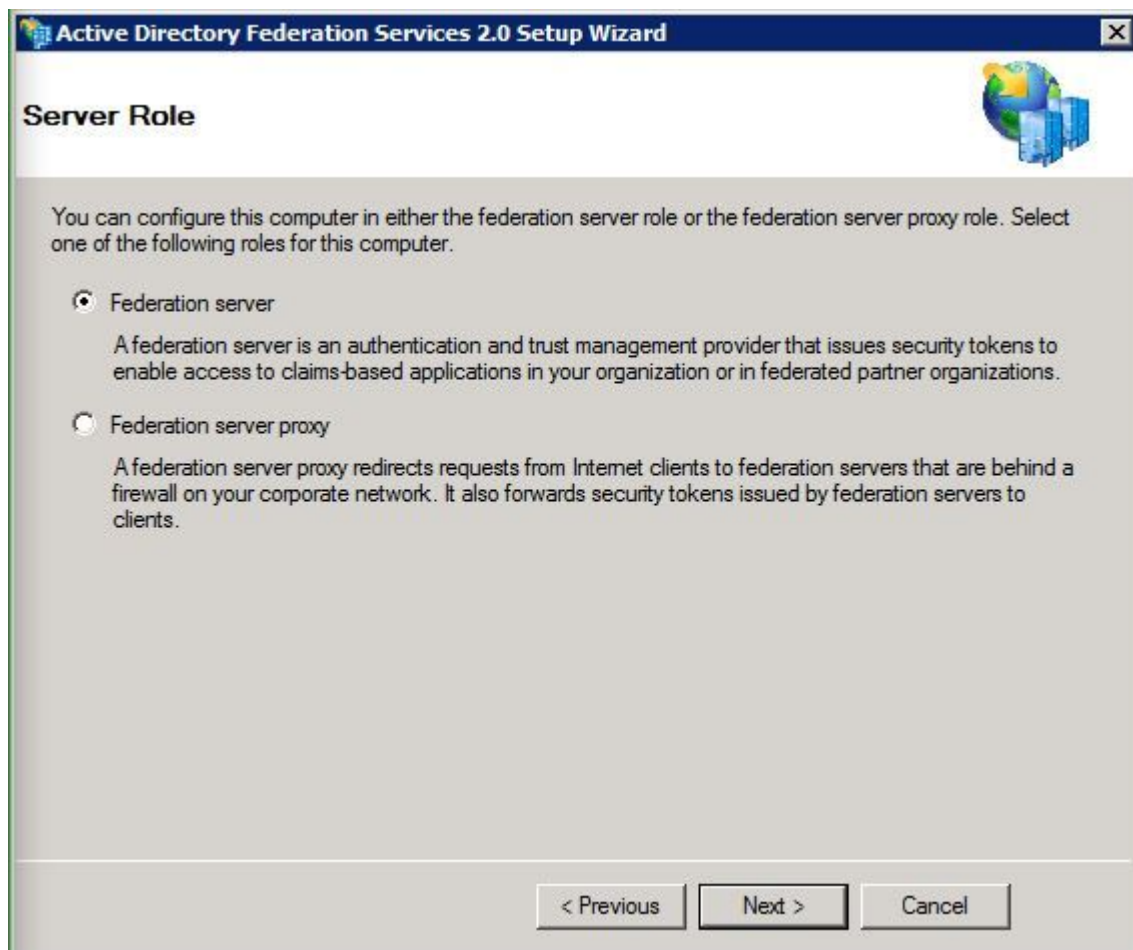
Stap 1. Navigeer naar [Download AD FS 2.0](#).

Stap 2. Zorg ervoor dat u de juiste download selecteert op basis van uw Windows-server.

Stap 3. **Verplaats** het gedownloade bestand naar uw Windows-server.

Stap 4. Ga verder met de installatie:

Stap 5. Kies **Federatie Server** wanneer hierom wordt gevraagd:



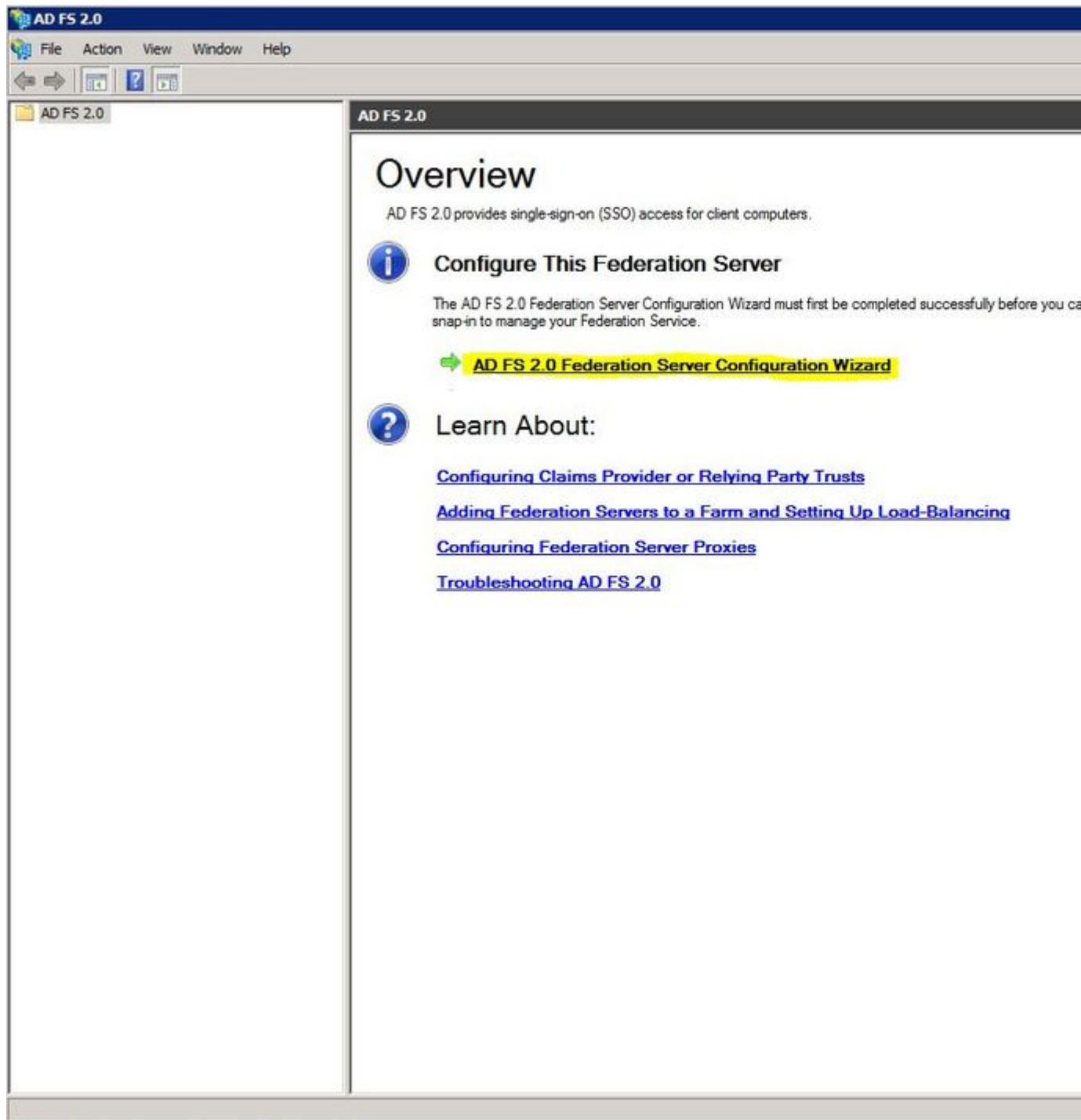
Stap 6. Sommige afhankelijkheden worden automatisch geïnstalleerd - klik op **Voltoeien** als dat is gedaan.

Nu AD FS 2.0 op uw server is geïnstalleerd, moet u enige configuratie toevoegen.

AD FS 2.0 configureren op uw Windows-server

Stap 1. Als het venster AD FS 2.0 na de installatie niet automatisch is geopend, kunt u op **Start** klikken en zoeken naar AD FS 2.0-beheer om het handmatig te openen.

Stap 2. Kies **de configuratiewizard voor AD FS 2.0 Federation Server**.



Stap 3. Klik vervolgens op **Create a new Federation Service**.

Welcome

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results

Welcome to the AD FS 2.0 Federation Server Configuration Wizard

This wizard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service.

Create a new Federation Service

Select this option to set up either a stand-alone federation server or the first server in a federation server farm.

Add a federation server to an existing Federation Service

Select this option to join this computer to an existing federation server farm.

< Previous

Next >

Cancel

Help

Stap 4. Voor de meeste omgevingen is een **zelfstandige federatieserver** voldoende.

Select Stand-Alone or Farm Deployment

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Existing Database
- Summary
- Results

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

 New federation server farm

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

 Stand-alone federation server

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

i You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

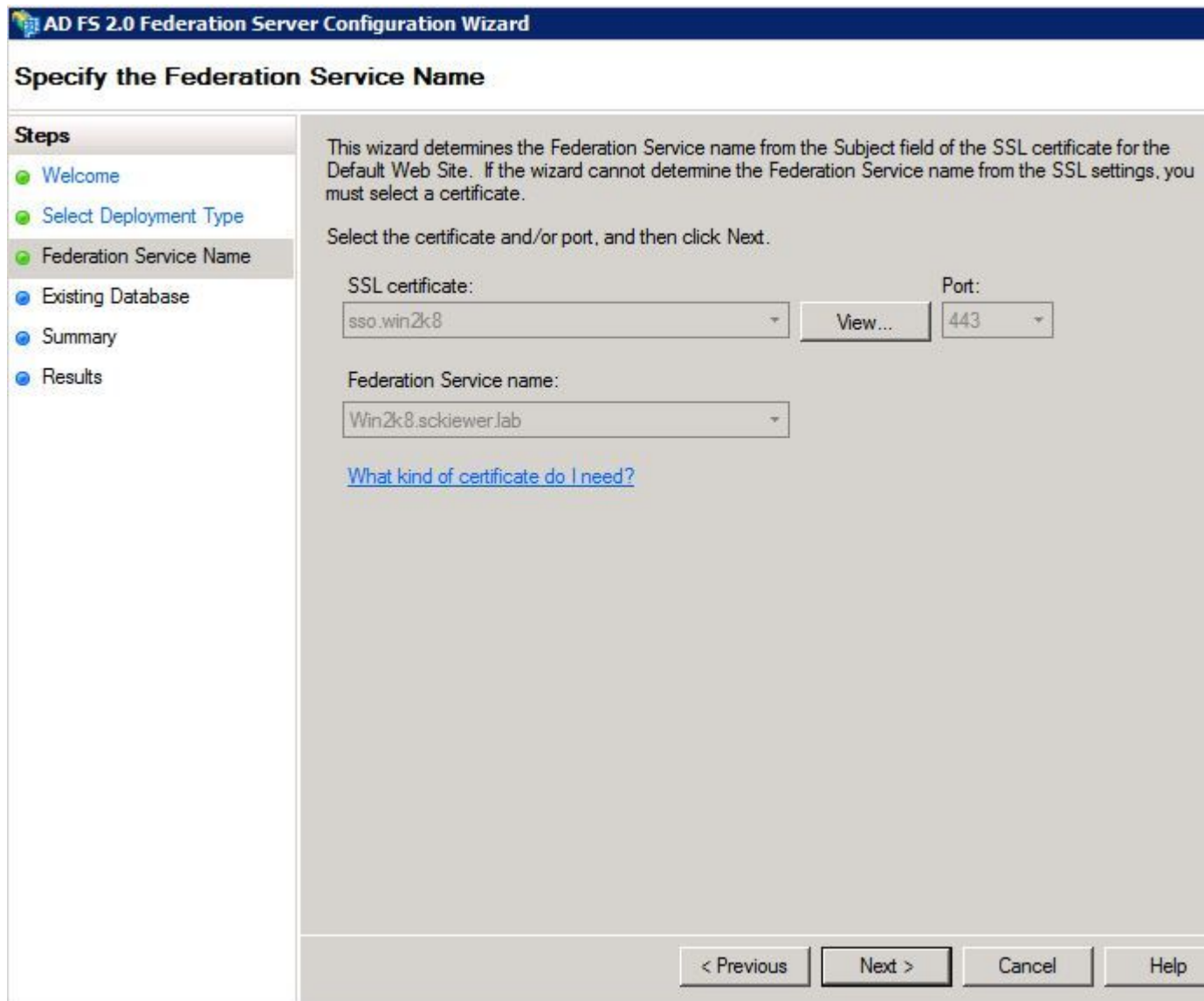
< Previous

Next >

Cancel

Help

Stap 5. Vervolgens wordt u gevraagd een certificaat te kiezen. Dit veld wordt automatisch ingevuld zolang de server een certificaat heeft.



Stap 6. Als u al een AD FS-database op de server hebt, moet u deze verwijderen om door te gaan.

Stap 7. Tot slot bent u op een overzichtsscherm waar u op **Volgende** kunt klikken.

Importeer de Idp Metadata naar CUCM / Download de CUCM Metadata

Stap 1. Update de URL met uw Windows-server hostname/FQDN en download de metadata van uw AD FS-server - <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

Stap 2. Ga naar **Cisco Unified CM Management > System > SAML Single Sign-On**.

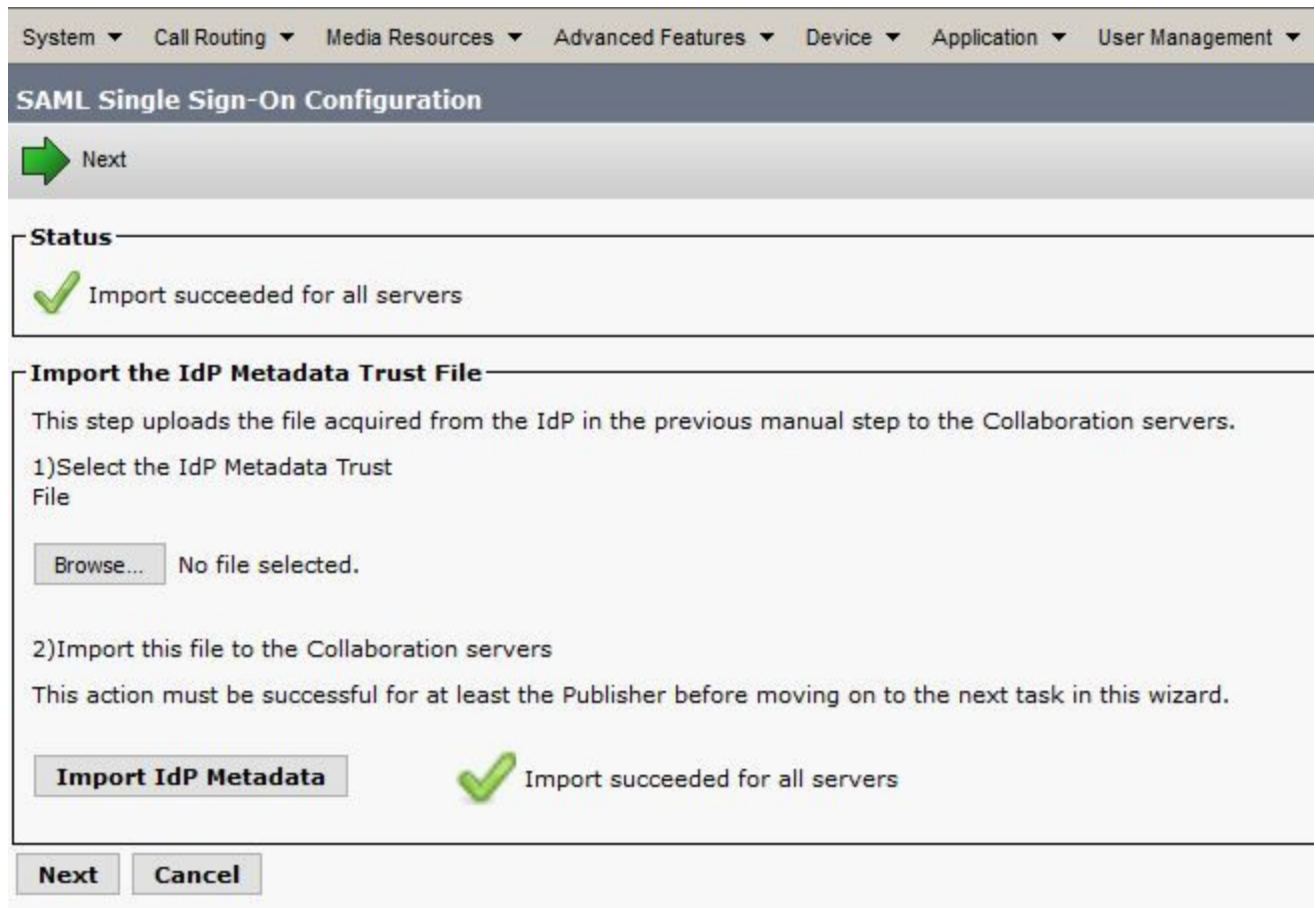
Stap 3. Klik op **SAML SSO inschakelen**.

Stap 4. Als u een waarschuwing over Web Server Connections ontvangt, klikt u op **Doorgaan**.

Stap 5. Vervolgens instrueert CUCM u om het metagegevensbestand te downloaden van uw IDP. In dit scenario is uw AD FS-server de IDP en u hebt de metagegevens in Stap 1 gedownload, dus klik op **Volgende**.

Stap 6. Klik op **Bladeren** > selecteer de optie **.xml in stap 1** > Klik op **IdentityP-metagegevens importeren**.

Stap 7. Een bericht geeft aan dat het importeren is geslaagd:



Stap 8. Klik op Next (Volgende).

Stap 9. Nu u de IdP-metagegevens hebt geïmporteerd in CUCM, moet u de metagegevens van CUCM importeren in uw IdP.

Stap 10. Klik op **Download Trust Metadata File**.

Stap 11. Klik op Next (Volgende).

Stap 12. Verplaats het .zip bestand naar uw Windows Server en haal de inhoud uit een map.

CUCM Metadata importeren naar AD FS 2.0-server en claimregels maken

Stap 1. Klik op **Start** en zoek naar **AD FS 2.0-beheer**.

Stap 2. Klik op **Vereist: voeg een vertrouwde vertrouwende partij toe**.

Opmerking: als u deze optie niet ziet, moet u het venster sluiten en het weer openen.

Stap 3. Zodra u de **Wizard Add Relying Party Trust** hebt geopend, klikt u op **Start**.

Stap 4. Hier moet u de XML-bestanden importeren die u in stap 12 hebt geëxtraheerd. Selecteer **Gegevens over de vertrouwende partij importeren uit een bestand** en blader naar de mappenbestanden en kies de XML voor uw uitgever.

Opmerking: gebruik de vorige stappen voor elke Unified Collaboration-server waarop u SSO wilt gebruiken.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options: 1. 'Import data about the relying party published online or on a local network' (unselected), with a text box for 'Federation metadata address (host name or URL)' and an example 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file' (selected), with a text box for 'Federation metadata file location' containing 'C:\Users\Administrator\Desktop\SPMetadata_1cucm1052.sckiewer.lab.xml' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (unselected). At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

Stap 5. Klik op Next (Volgende).

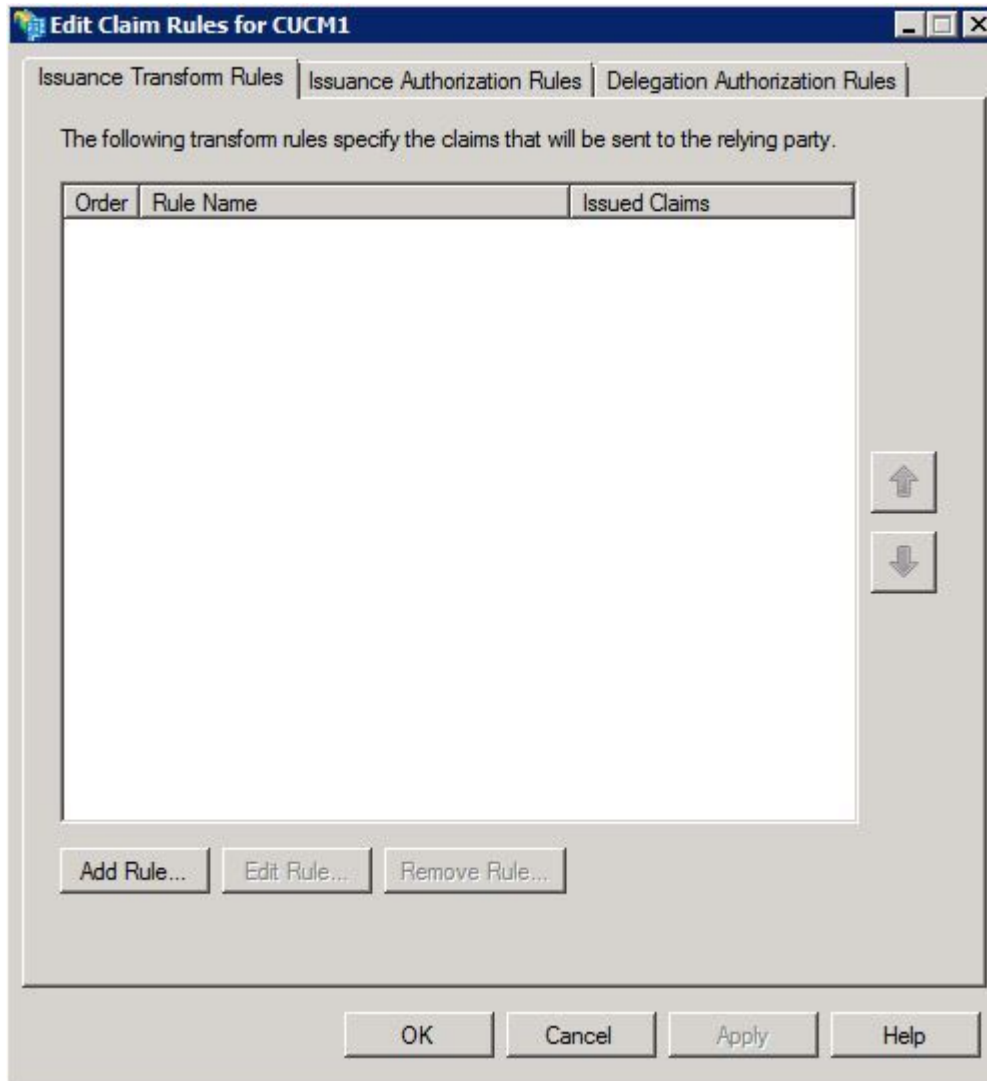
Stap 6. Bewerk de **weergavenaam** en klik op **Volgende**.

Stap 7. Kies **Toestaan voor alle gebruikers om toegang te krijgen tot deze vertrouwende partij** en klik op **Volgende**.

Stap 8. Klik nogmaals **op Volgende**.

Stap 9. Zorg er in dit scherm voor dat u **het dialoogvenster Claimregels bewerken voor dit vertrouwen van de vertrouwende partij** hebt geopend wanneer de wizard wordt ingeschakeld en klik vervolgens op **Sluiten**.

Stap 10. Het venster Claimregels bewerken wordt geopend:



Stap 11. Klik in dit venster op **Regel toevoegen**.

Stap 12. Kies **LDAP-kenmerken als vorderingen verzenden** voor **sjabloon** van **claimregels** en klik op **Volgende**.

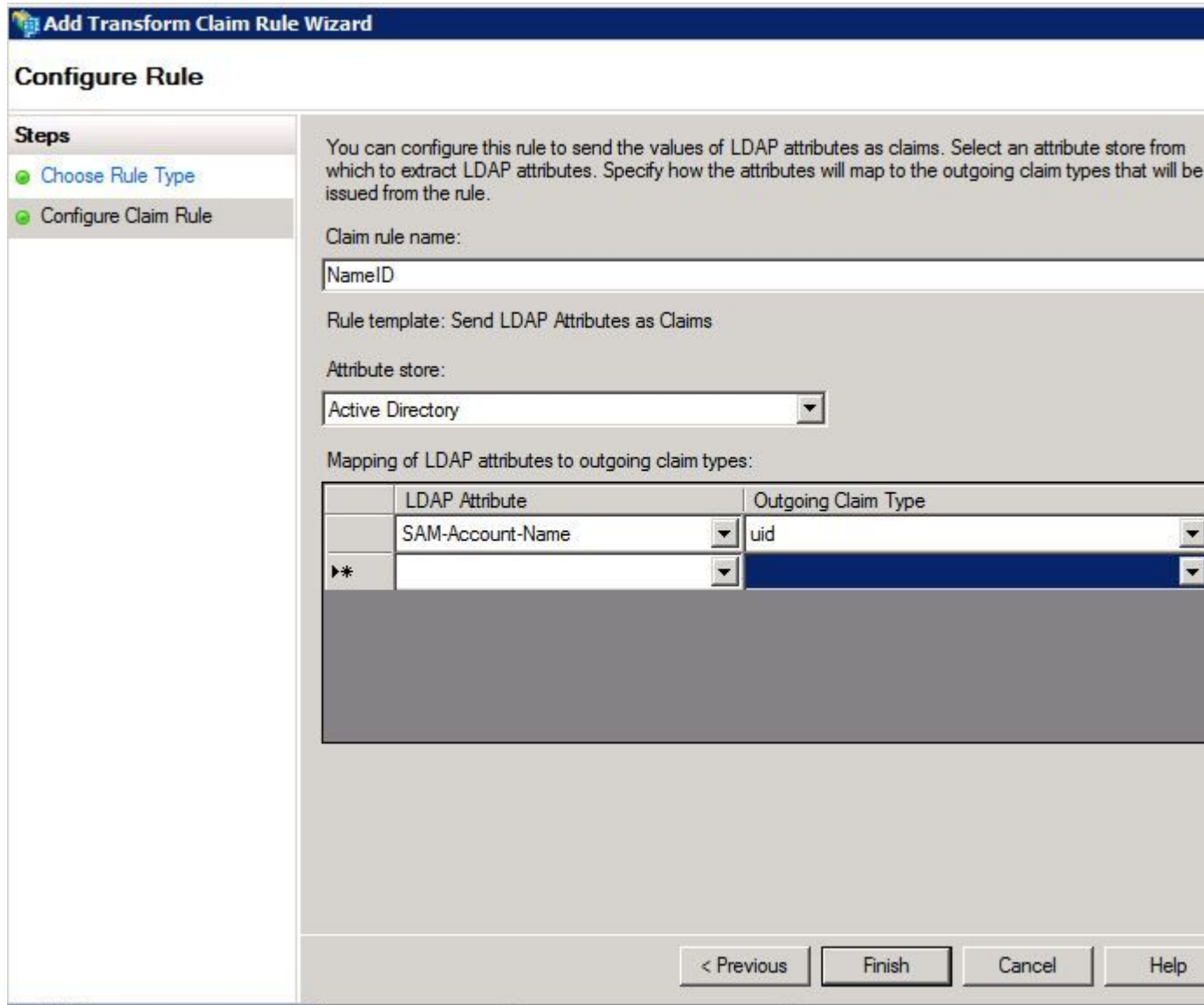
Stap 13. Voer op de volgende pagina **NameID in** voor de **naam** van de **claimregel**.

Stap 14. Kies **Active Directory** voor het **opslaan** van **kenmerken**.

Stap 15. Kies **SAM-Account-Naam** voor het **LDAP-kenmerk**.

Stap 16. Voer **voicemail** in voor **type uitgaande claim**.

Opmerking: uid is geen optie in de vervolgkeuzelijst. Het moet handmatig worden ingevoerd.



Stap 17. Klik op Finish (Voltooien).

Stap 18. De eerste regel is nu klaar. Klik nogmaals op **Regel toevoegen**.

Stap 19. Kies **Aangepaste regel voor het verzenden van claims**.

Stap 20. Voer een **naam voor een claimregel** in.

Stap 21. Plakt de tekst in het veld **Aangepaste regel**:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/vensterboeknaam"]
=> probleem (type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/naamaanduiding", Emittent
= c.Emittent, OriginalEmittent = c.OriginalEmittent, Waarde = c.Value, ValueType = c.ValueType,
Eigenschappen["http://schemas.xmlsoap.org/ws/2005/05/identity/claims/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-
format:transient",Eigenschappen["http://schemas.xmlsoap.org/ws/2005/05/identity/claims/namequal"] =
"http://ADFS\_FEDERATION\_SERVICE\_NAME/com/adfs/service/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spnamequalifier"] =
"CUCM_entity_ID");
```

Stap 22. Zorg ervoor dat u AD_FS_SERVICE_NAME en CUCM_entity_ID in de juiste waarden wijzigt.

Opmerking: als u niet zeker bent van de AD FS-servicenaam, kunt u de stappen volgen om deze te vinden. De CUCM Entity ID kan worden gehaald uit de eerste regel in het CUCM metadata bestand. Er is een entityID op de eerste regel van het bestand dat er zo uitziet, entityID=1cucm1052.sckiewer.lab,. U moet de onderstreepte waarde invoeren in de juiste sectie van de claimregel.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name: CUCM SSO Custom Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> 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://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "1cucm1052.sckiewer.lab");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

Stap 23. Klik op Finish (Voltooien).

Stap 24. Klik op OK.


Opmerking: er zijn claimregels nodig voor elke Unified Collaboration-server waarop u SSO wilt gebruiken.

SSO-activering op CUCM voltooien en de SSO-test uitvoeren


Stap 1. Nu de AD FS server volledig is geconfigureerd, kunt u teruggaan naar CUCM.

Stap 2. Je bent weggegaan op de laatste configuratiepagina:

SAML Single Sign-On Configuration

 Back

Status


 The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test

1) Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrative access.

Valid administrator Usernames

sckiewer

2) Launch SSO test page

Stap 3. Selecteer uw Eindgebruiker die de rol **Standaard CCM Super Gebruikers** heeft geselecteerd en klik op **Uitvoeren SSO Test...**

Stap 4. Zorg ervoor dat uw browser pop-ups toestaat, en voer uw referenties in de prompt in.

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

Stap 5. Klik op **Sluiten** in het pop-upvenster en vervolgens op **Voltooien**.

Stap 6. Na een korte herstart van de webtoepassingen wordt SSO ingeschakeld.

Problemen oplossen

Debuggen van SSO-logbestanden instellen

Om de te zuiveren logboeken SSO te plaatsen, moet u dit bevel in CLI van CUCM in werking stellen:
vastgestelde samltrace niveau debug

De SSO-logbestanden kunnen worden gedownload van RTMT. De naam van de logset is **Cisco SSO**.

Zoek de federatie service naam

Om de naam van de federation service te vinden, klikt u op **Start** en zoeken naar **AD FS 2.0 Management**.

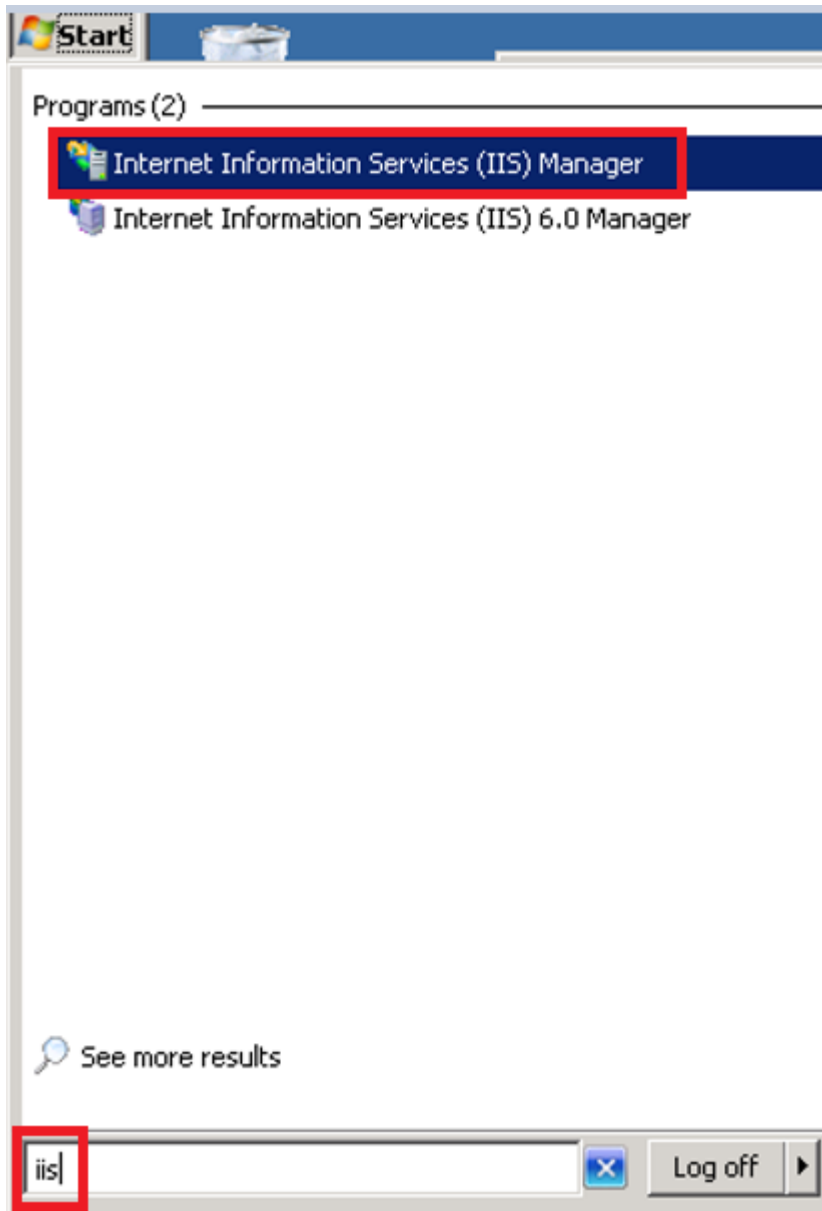
- Klik op **Federatie-eigenschappen bewerken...**
- Terwijl u op het tabblad Algemeen bent, zoekt u naar de **naam van de Federale Dienst**

Servicenaam voor Dotless Certificaat en Federatie

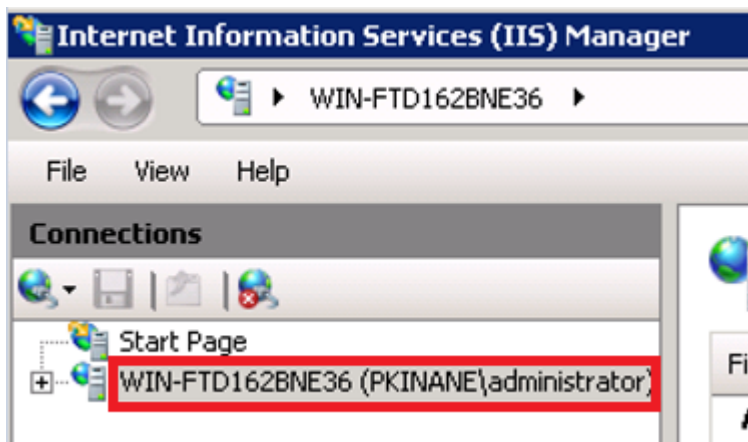
Als u deze foutmelding ontvangt in de configuratiewizard AD FS, moet u een nieuw certificaat maken.

Het geselecteerde certificaat kan niet worden gebruikt om de naam van de Federale Dienst te bepalen omdat het geselecteerde certificaat een dotless (kort genoemd) Onderwerpnaam heeft. Selecteer een ander certificaat zonder een dotless (short-name) Onderwerpnaam, en probeer het nogmaals.

Stap 1. Klik op Start en zoek naar iis en open vervolgens Internet Information Services (IIS) Manager

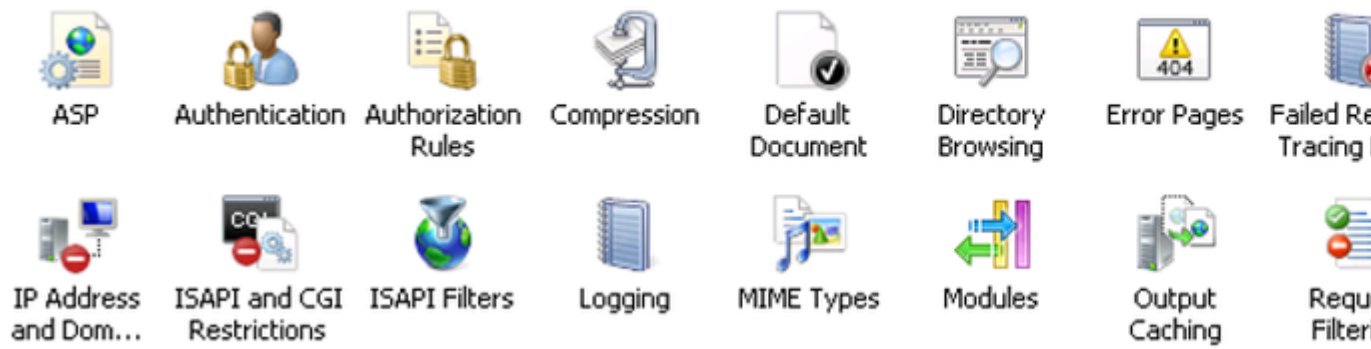


Stap 2. Klik op de naam van de server.

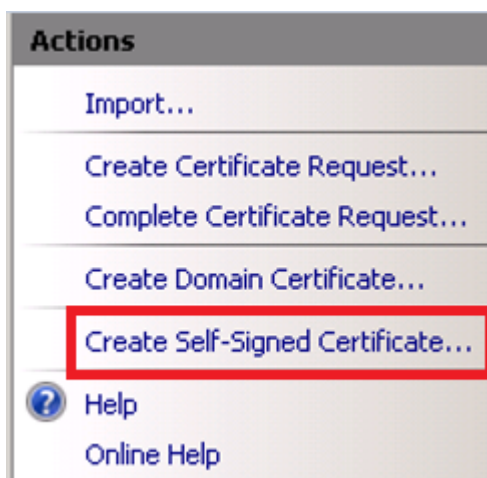


Stap 3. Klik op Servercertificaten.

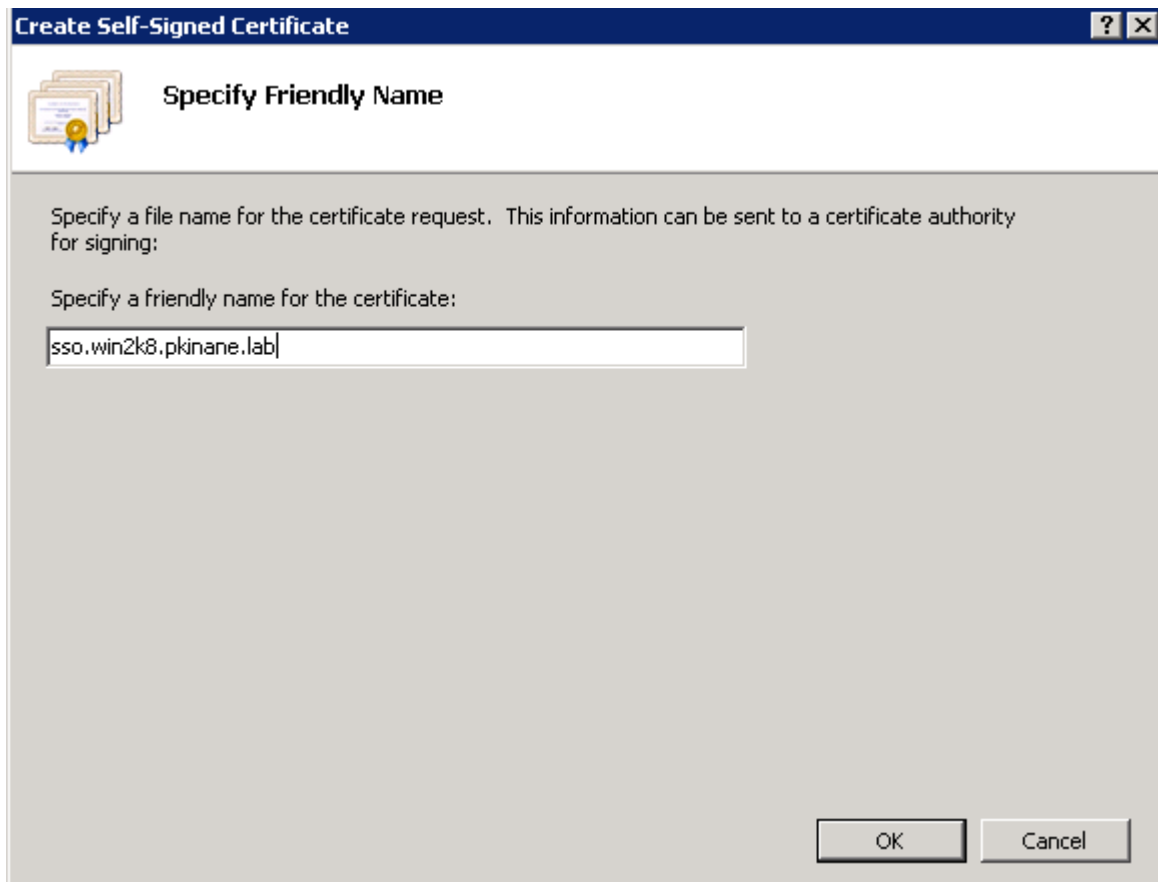
IIS



Stap 4. Klik op Zelfondertekend certificaat maken.



Stap 5. Voer de gewenste naam in voor het alias van uw certificaat.



De tijd is niet synchroon tussen de CUCM- en IDP-servers

Als u deze fout ontvangt wanneer u de SSO-test uitvoert vanuit CUCM, moet u de Windows-server configureren om dezelfde NTP-server(s) te gebruiken als de CUCM.

Ongeldige SAML-respons. Dit kan worden veroorzaakt wanneer de tijd niet synchroon is tussen de Cisco Unified Communications Manager en de IDP-servers. Controleer de NTP-configuratie op beide servers. Start "Utils ntp status" vanuit de CLI om deze status te controleren op Cisco Unified Communications Manager.

Zodra de Windows Server de juiste NTP-servers heeft opgegeven, moet u nog een SSO-test uitvoeren en zien of het probleem blijft bestaan. In sommige gevallen is het noodzakelijk de geldigheidsperiode van de bewering te verdraaien. Meer details over dat proces [hier](#).

Gerelateerde informatie

- [Technische ondersteuning en documentatie](#) â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.