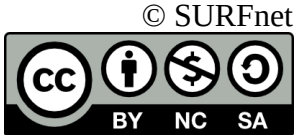
Handleiding ADFS installatie Windows Server 2012 en Server 2012R2



versie: 2.2.0

Inhoudsopgave

Inleiding

In deze handleiding lees je hoe je jouw organisatie kunt aansluiten op SURFconext als Identity Provider met behulp van ADFS (in ADFS-terminologie Claims Provider genoemd).

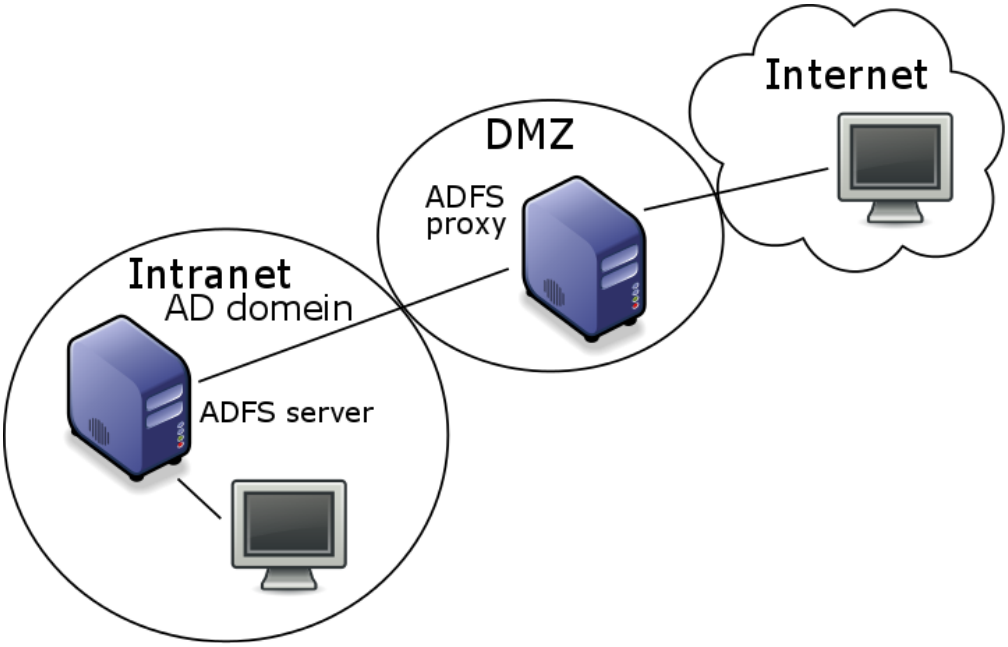
De procedure voor het aansluiten als Identity Provider bestaat uit de volgende onderdelen:

- Een ADFS serversysteem inrichten; waaronder Windows Server 2012(R2) configureren en ADFS installeren. Let op dat de installatie onder Windows Server 2012R2 anders verloopt dan onder Windows Server 2012.
- De ADFS server configureren voor aansluiting als Identity Provider (IdP) voor SURFconext.
- Een ADFS proxy inrichten indien toegang van buiten het lokale netwerk gewenst is. Hier verschilt Windows Server 2012R2 erg veel van Windows Server 2012!
- Attributen vrijgeven aan SURFconext

Deze handleiding is gebaseerd op de release van ADFS 6.2.0.0 zoals meegeleverd in Windows Server 2012 en Server 2012R2.

Waarom een server én een proxy inrichten?

Om de ADFS-server minder kwetsbaar te maken voor aanvallen van buitenaf, moet je naast een ADFS server ook een ADFS-proxy inrichten buiten het Windows-domein. De ADFS-server moet namelijk bij voorkeur niet bereikbaar zijn van buitenaf. Je doet dit door een ADFS-proxy in te richten en deze ‘voor’ de ADFS-server te plaatsen. Dit houdt in dat je twee verschillende Windows Server machines moet configureren in deze setup. De proxy mag geen lid zijn van het domein en wordt bij voorkeur in de DMZ (zie verklarende woordenlijst achterin dit document) geplaatst.



De proxy zorgt ervoor dat gebruikers die niet zijn ingelogd op het (windows-)domain, via een webpagina (username/ password formulier) kunnen inloggen. Dit formulier kan aan de look-and-feel van jouw organisatie worden aangepast.

ADFS 2.0-Server inrichten

Inleiding

Dit document beschrijft de installatie van een ADFS server op Windows Server 2012 en Windows Server 2012R2. Deze installaties hebben voldoende gemeen om beide in dit document te bespreken maar wijken op een aantal punten af, zodat dan verwezen wordt naar de R2 specifieke schermen. Met name het installeren van de ADFS proxy in Windows Server 2012R2 is volledig anders dan in Windows Server 2012.

Voordat je de specifieke instellingen voor SURFconext kunt invoeren, moet je een basisinstallatie op de ADFS server uitvoeren. Hiervoor moet je onderstaande stappen doorlopen:

- Installeer en configureer Windows Server 2012(R2).
- Voeg de ADFS software als feature toe.
- Configureer de basisinstellingen van ADFS.

Windows Server 2012 installeren en configureren

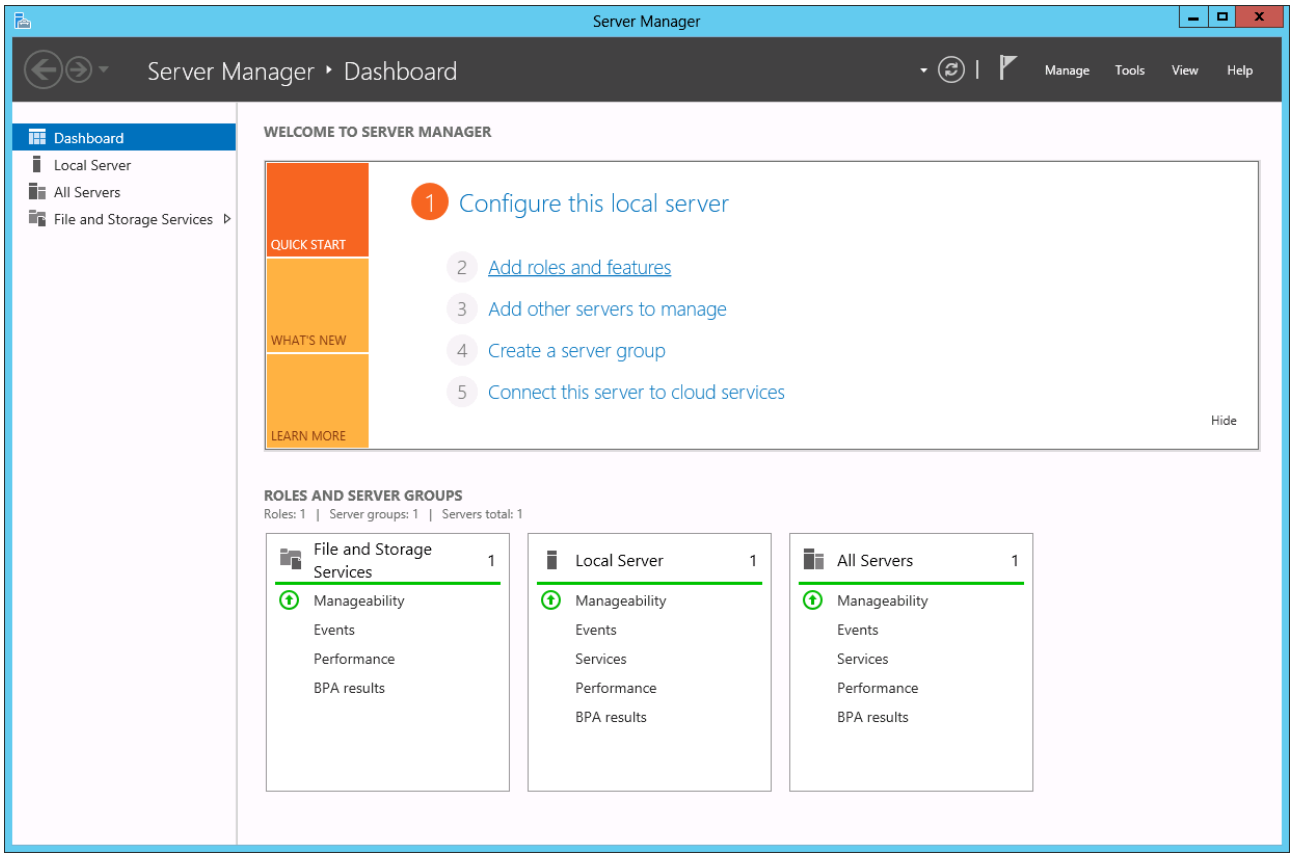
Om een ADFS 2.0-server te kunnen inrichten, moet je eerst Windows Server 2012 installeren en configureren. Hiervoor moet je onderstaande stappen doorlopen:

- Installeer de juiste versie van het besturingssysteem op de server: Windows Server 2012 of Windows Server 2012R2 (standaard of enterprise).
- Stel de tijd op de server correct in en zorg ervoor dat je deze synchroniseert met een time server (NTP).
- Neem de server op in het domein van de Active Directory waaruit de accounts voor de SURFconext federatie komen.
- Installeer een geldig certificaat voor de voorgenomen login URL in de Personal Certificate store van de Local Computer ten behoeve van veilige gegevensuitwisseling met de IdP (SSL) . Zie appendix A: Certificaat installeren.

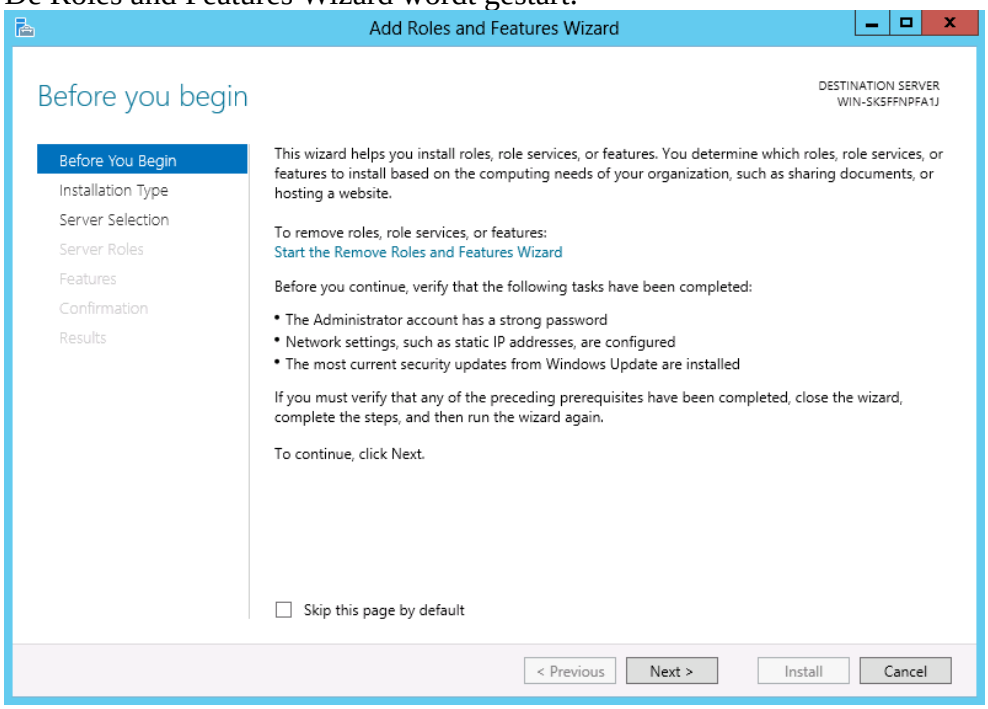
ADFS Server Software installeren

Onderstaand gedeelte van deze handleiding is te gebruiken voor het installeren van de ADFS Server Role op zowel Windows Server 2012 en Windows Server 2012R2.

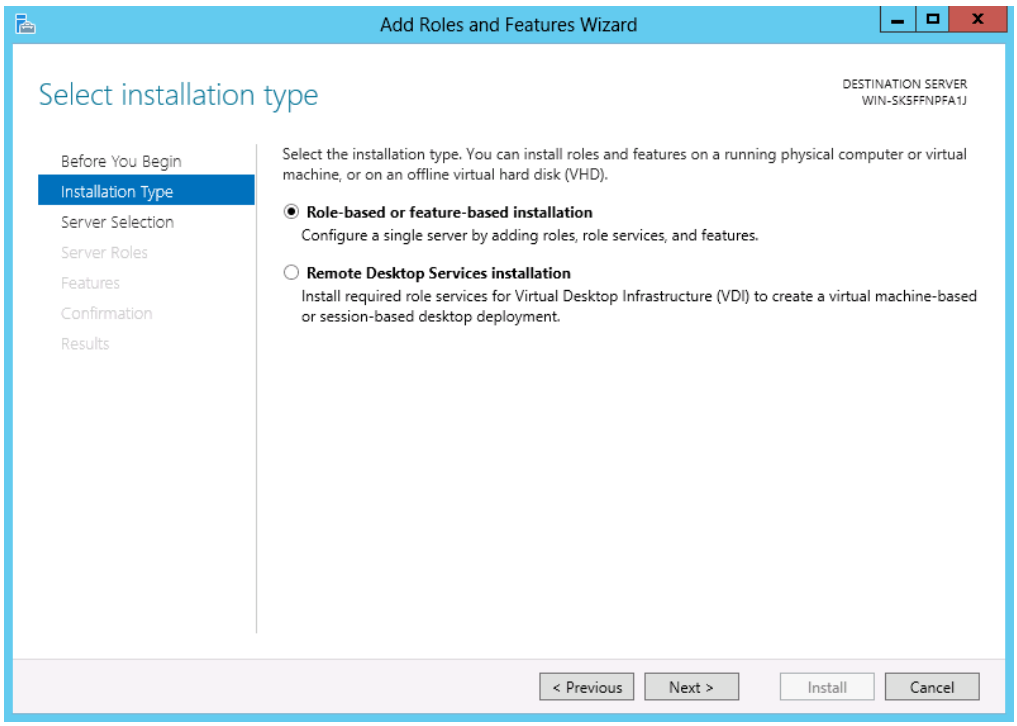
Start de Server Manager tool op de machine die als ADFS Server ingericht wordt en klik op “Add Roles and Features”.



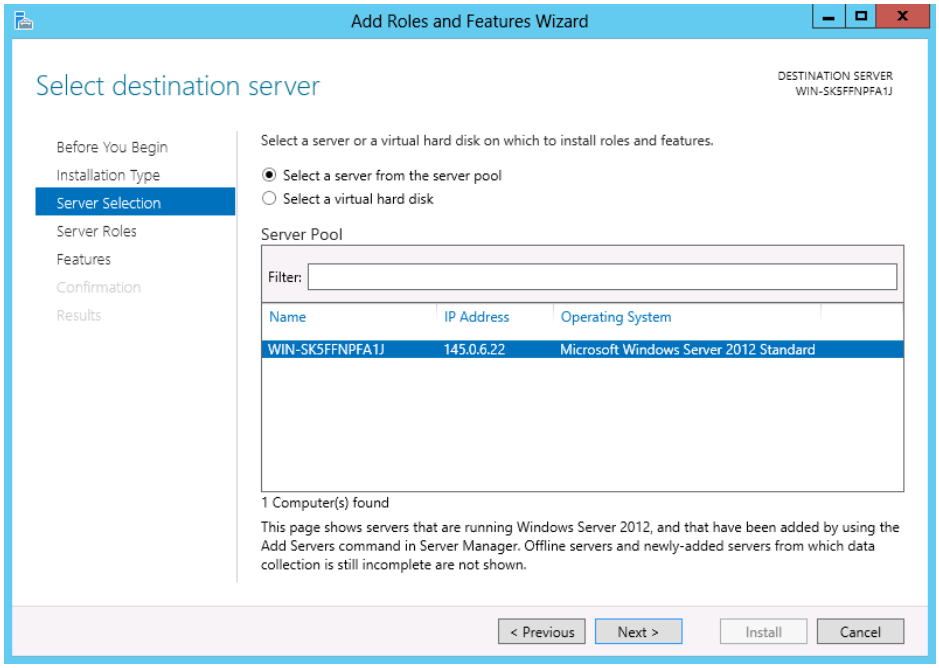
De Roles and Features Wizard wordt gestart:



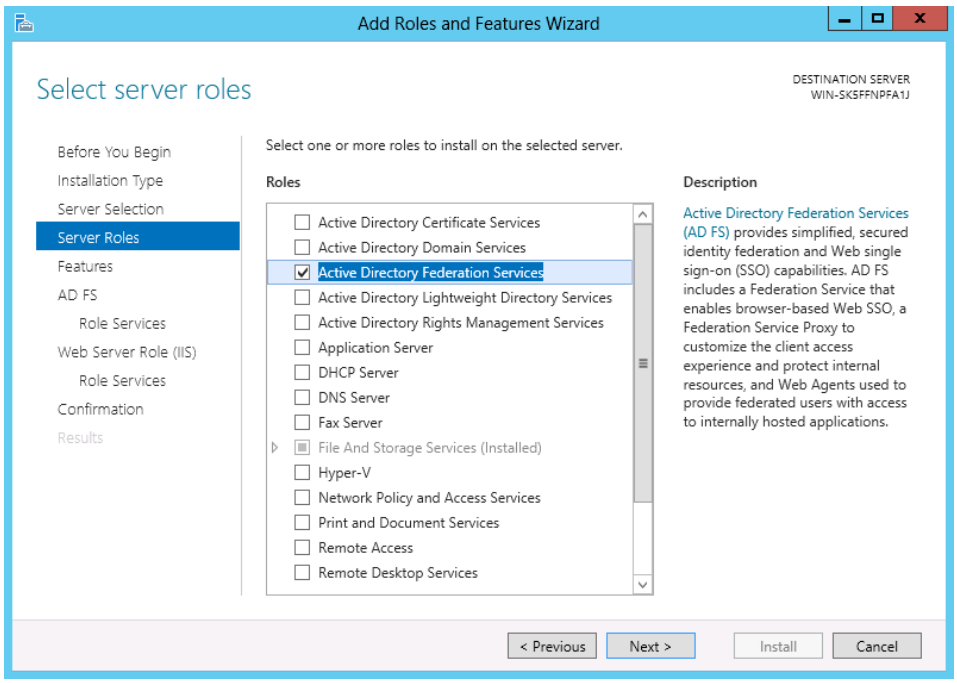
Klik op “Next”



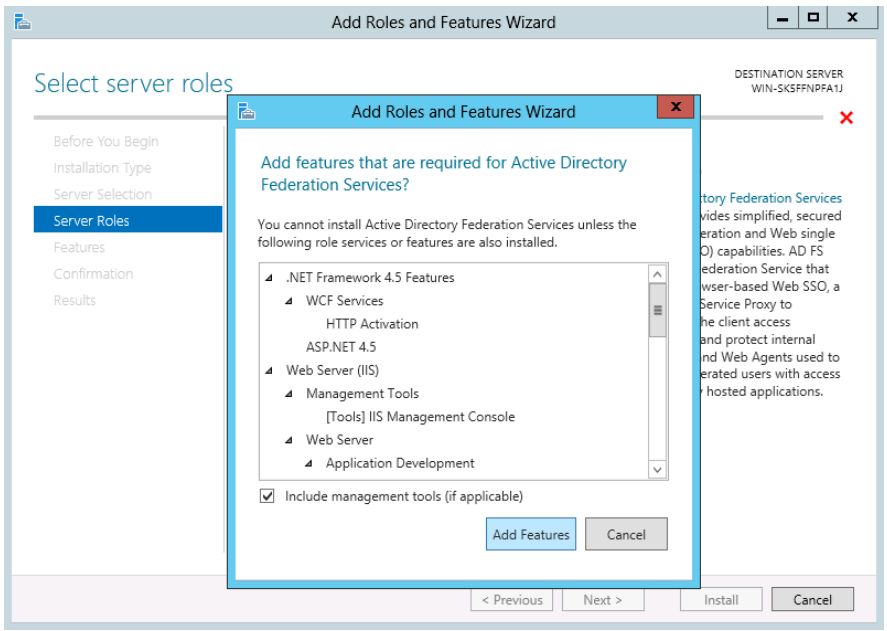
Selecteer “Role-based or feature-based installation” en klik op “Next”



Selecteer de juiste server en klik op “Next”

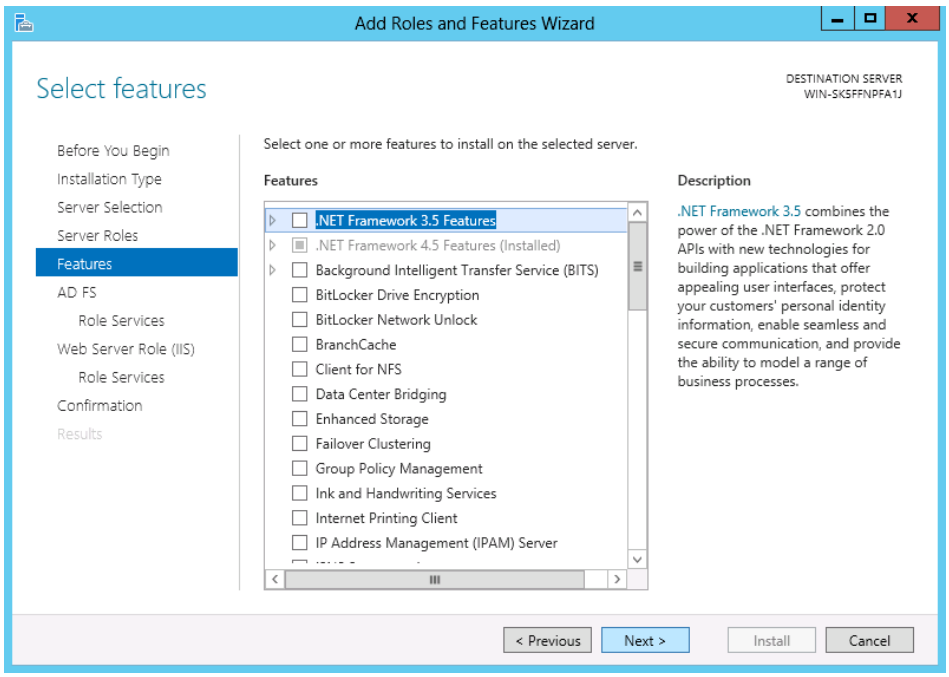


Selecteer “Active Directory Federation Services” en klik op “Next”

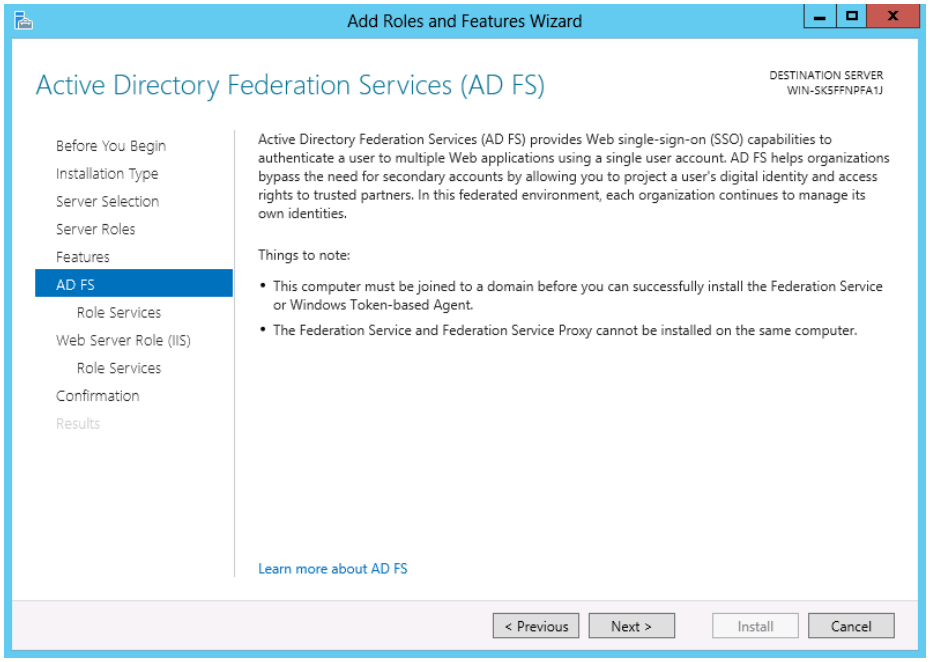


Er verschijnt een waarschuwing dat er meerdere afhankelijkheden zijn en dat deze ook geïnstalleerd zullen worden. Let op dat IIS onder Windows Server 2012R2 geen afhankelijkheid is van ADFS en ook niet geinstalleerd mag worden!

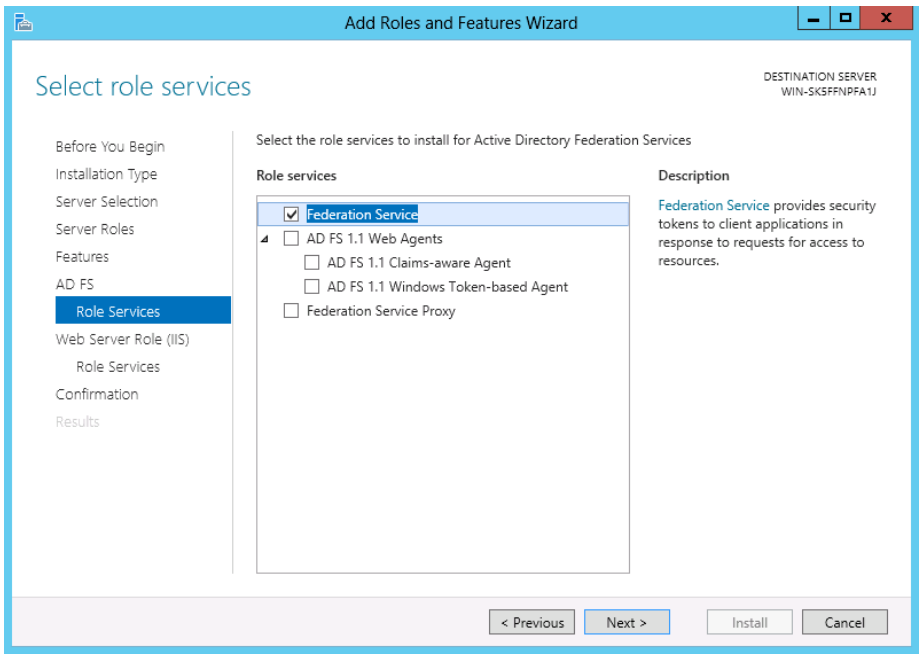
Klik op “Add Features” of “Next” om verder te gaan



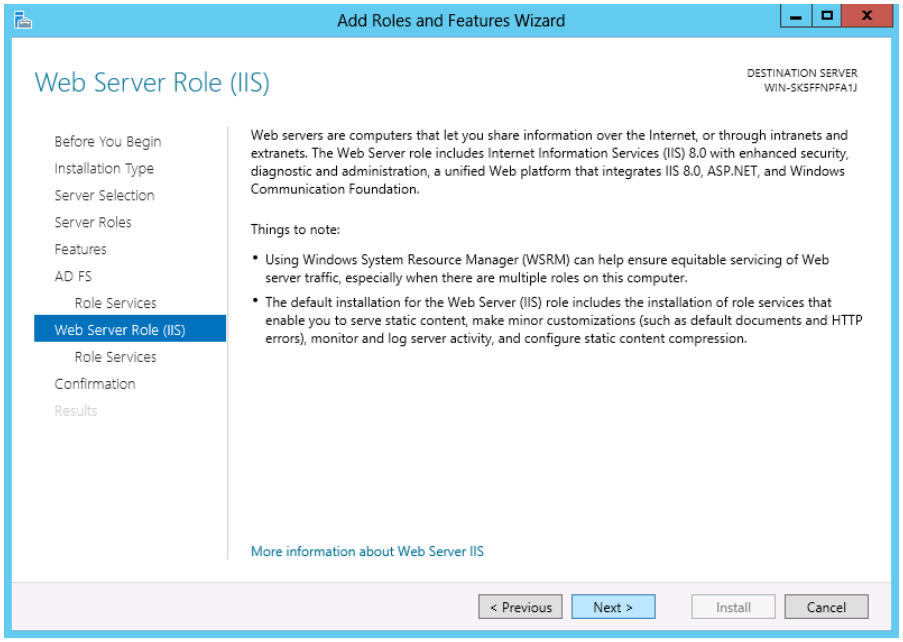
Klik op “Next”



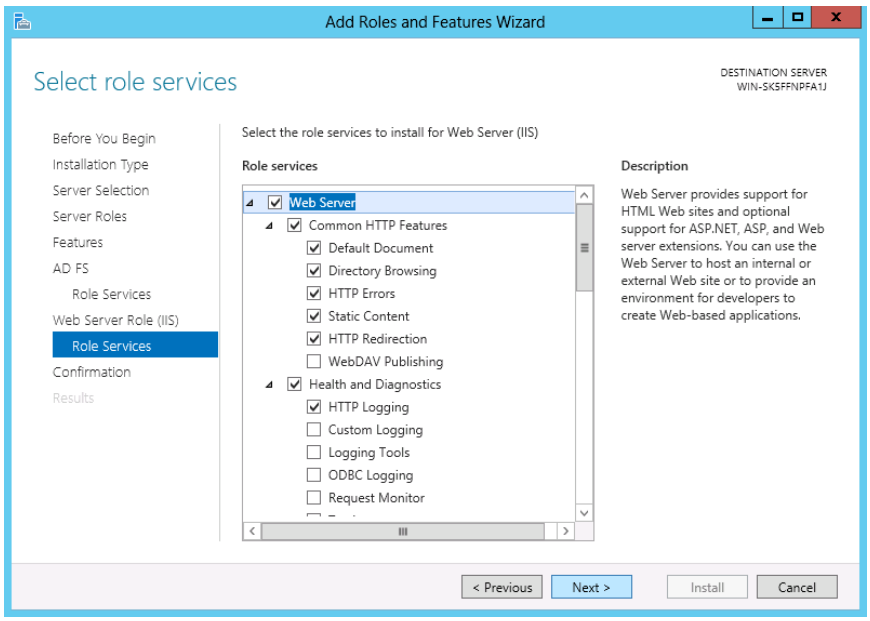
Klik op “Next”



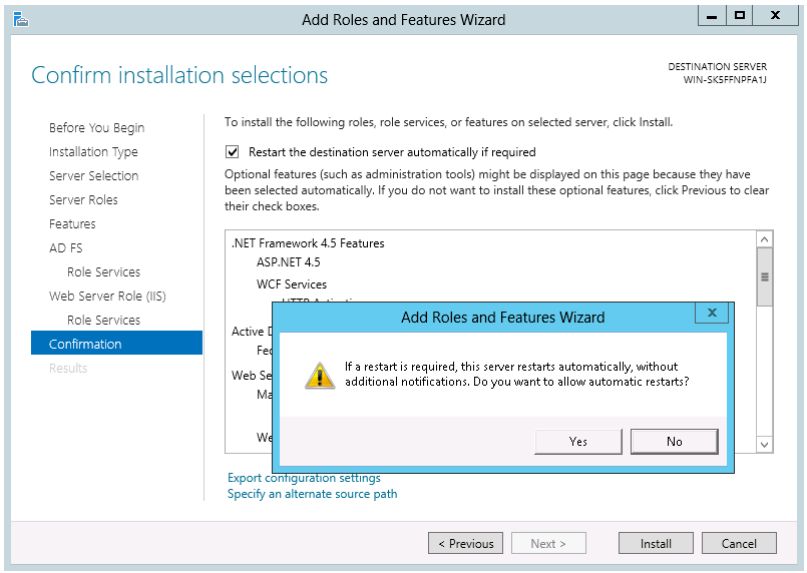
Selecteer “Federation Service” en klik op “Next”.



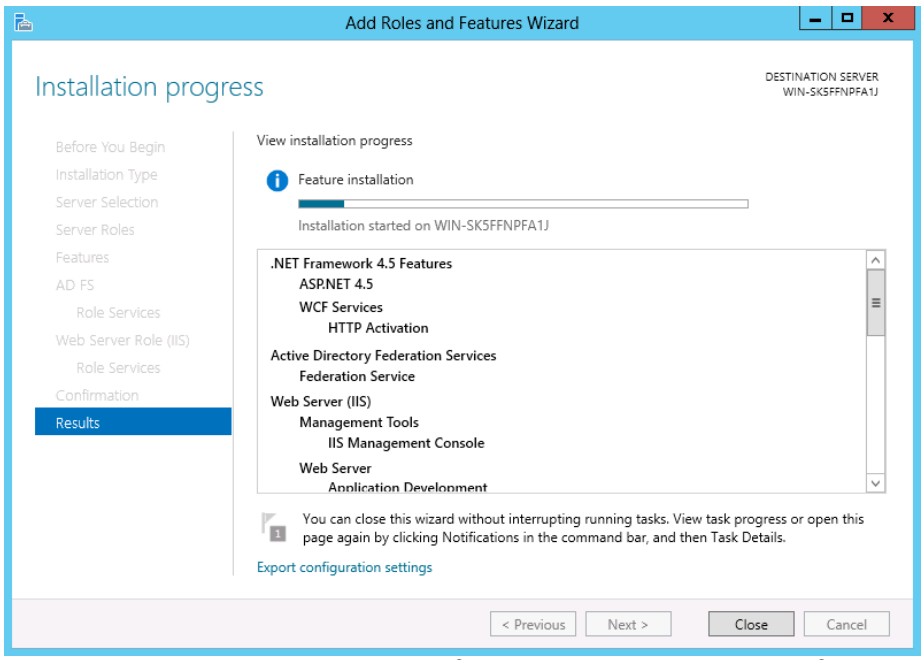
Klik op “Next” (Let op dat Windows Server 2012R2 geen IIS afhankelijkheid heeft en de volgende schermen daardoor niet getoond worden).



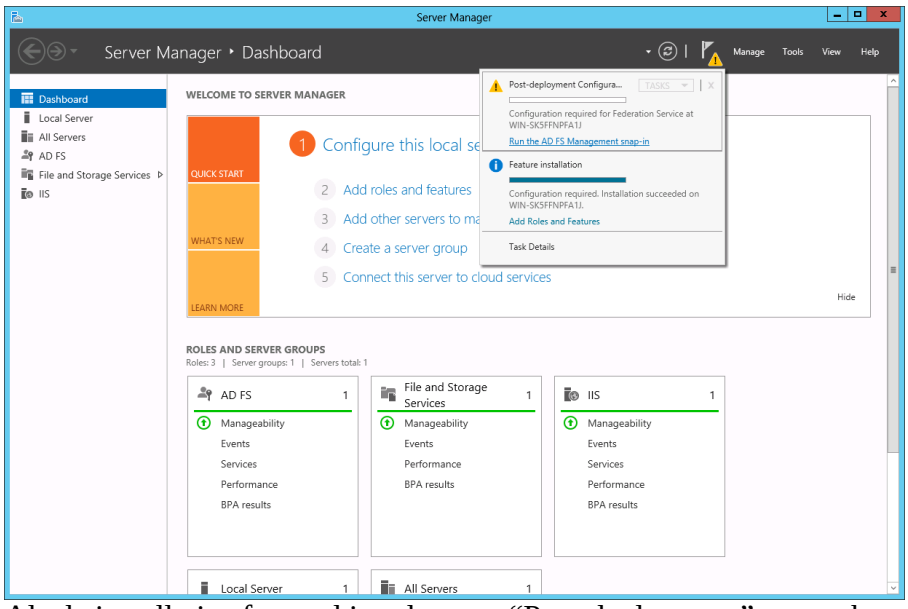
Klik op “Next”.



Kies wat voor deze server toepasselijk is. Klik op “Install”



Wacht eventueel tot de installatie afgerond is. De wizard mag afgesloten worden, de installatie zal op de achtergrond doorgaan.



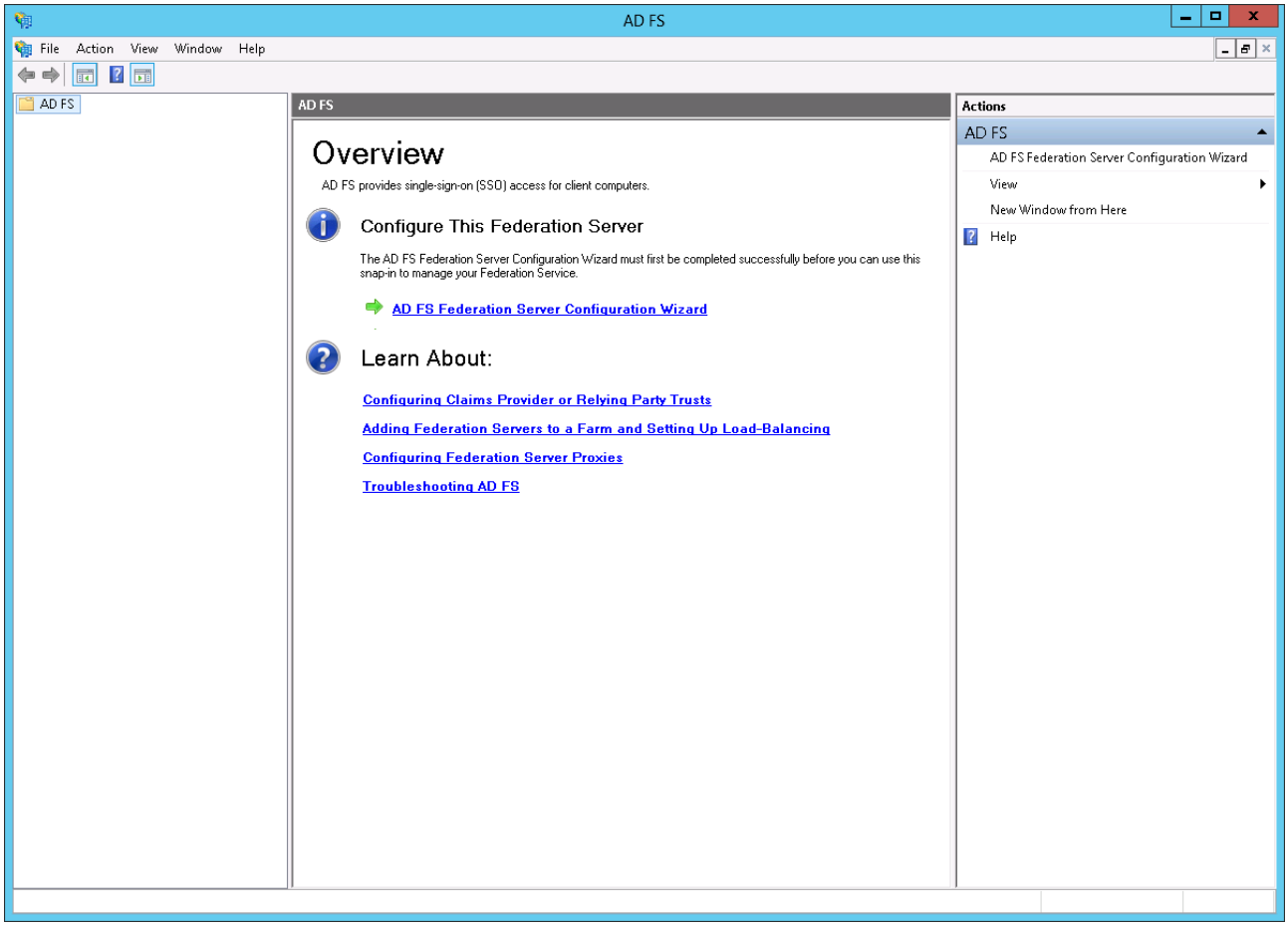
Als de installatie afgerond is zal er een “Post-deployment” waarschuwing “Configuration required for Federation Service at ...” verschijnen in het Server Manager Dashboard. Klik op “Run the AD FS Management snap-in” om de installatie van ADFS te voltooien.

Vanaf hier verschillen de interfaces van Windows Server 2012 en Windows Server 2012 R2. Hieronder volgt de configuratie voor Windows Server 2012.

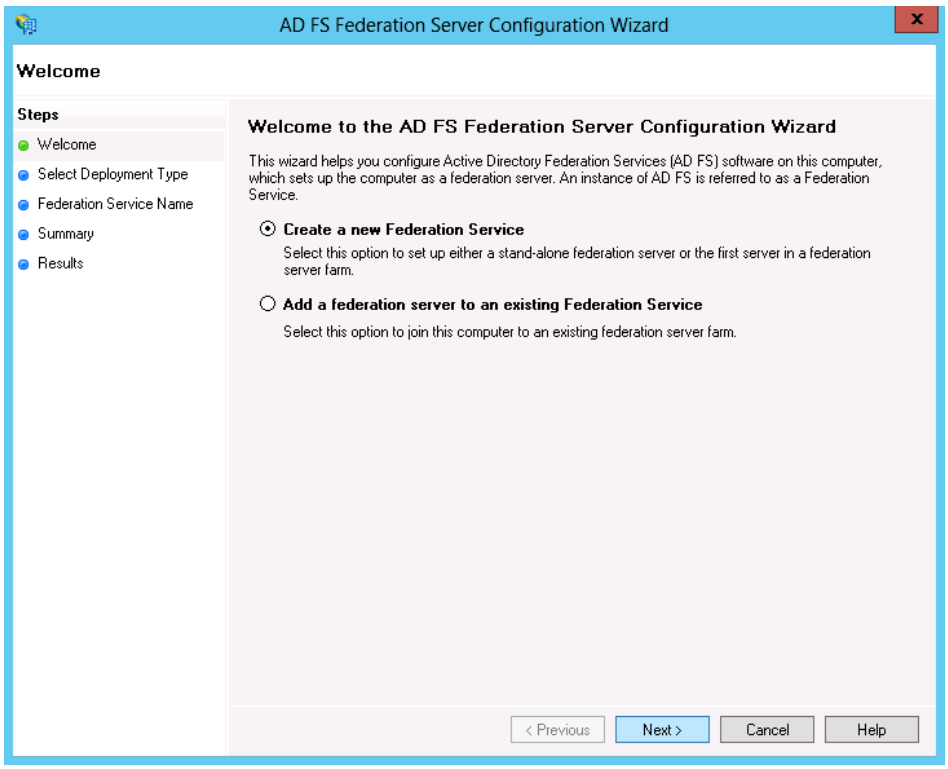
Zie voor de verdere installatie Windows Server 2012R2 “ADFS Configuration Wizard 2012R2” in het volgende hoofdstuk.

ADFS Configuration Wizard 2012

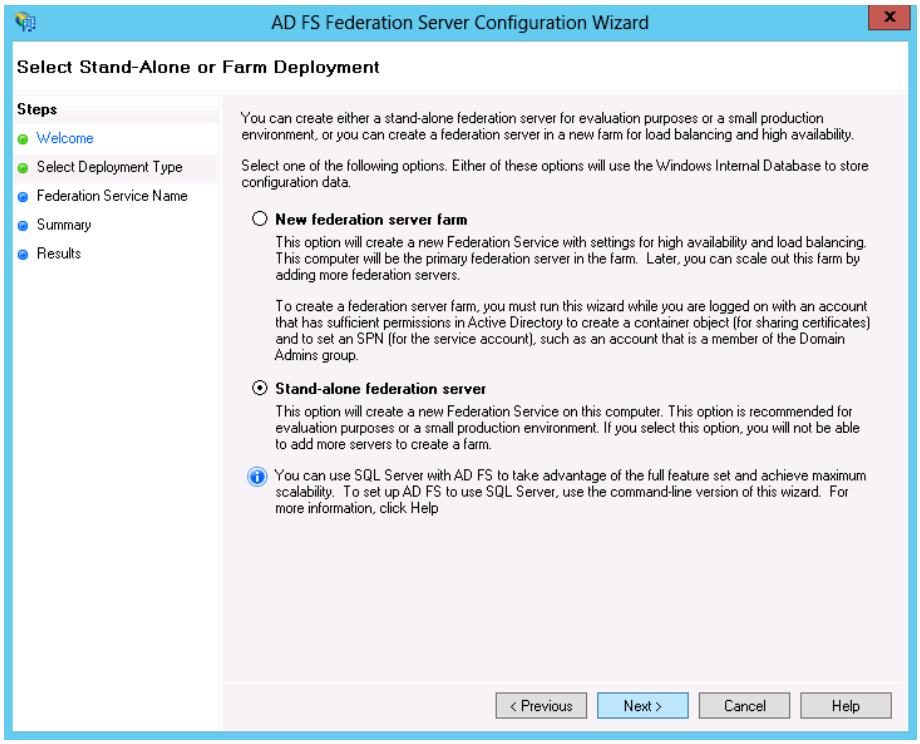
Wanneer op de “Post-deployment” link in het Server Manager Dashboard geklikt wordt zal de ADFS Manager Snap-in gestart worden. Hierin is een link “AD FS Federation Server Configuration Wizard” opgenomen:



Klik op deze link.

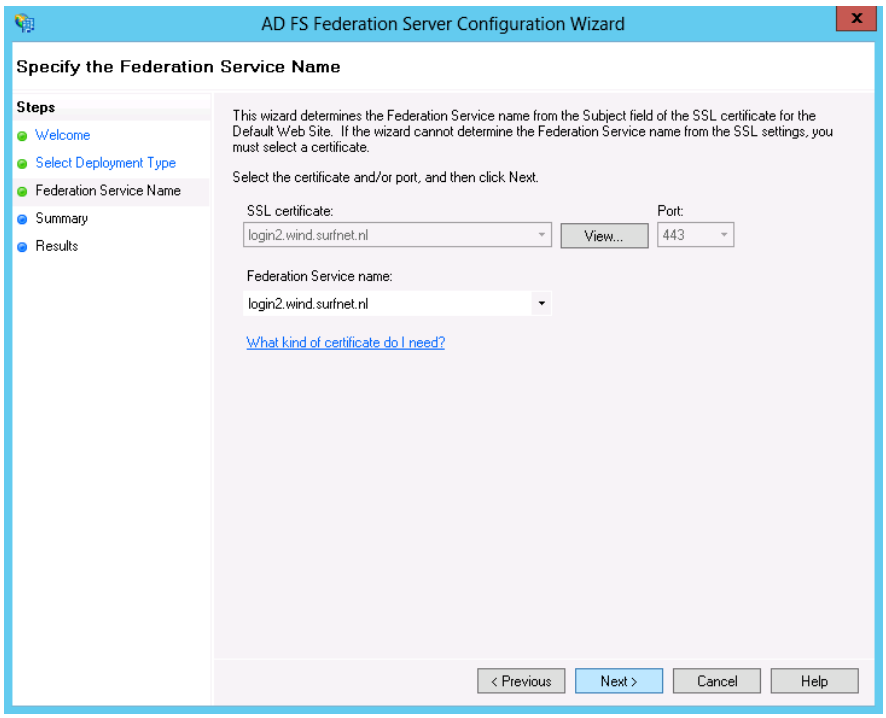


Selecteer “Create a new Federationn Service” en klik op “Next”.

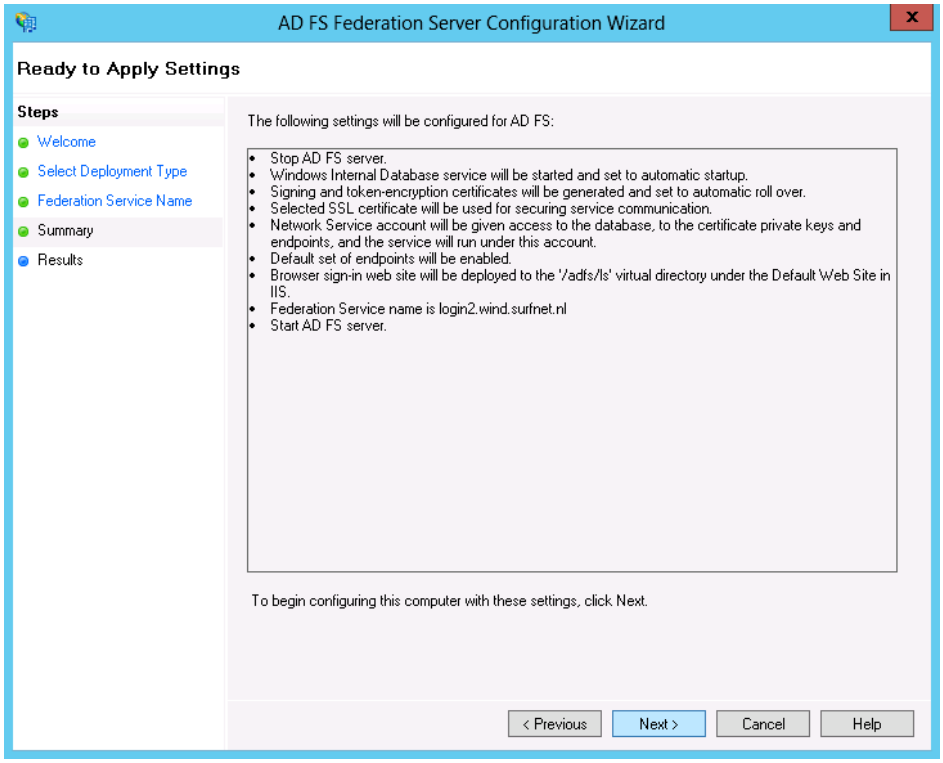


Kies voor een eenvoudige installatie “Stand-alone federation server” en klik op “Next”.

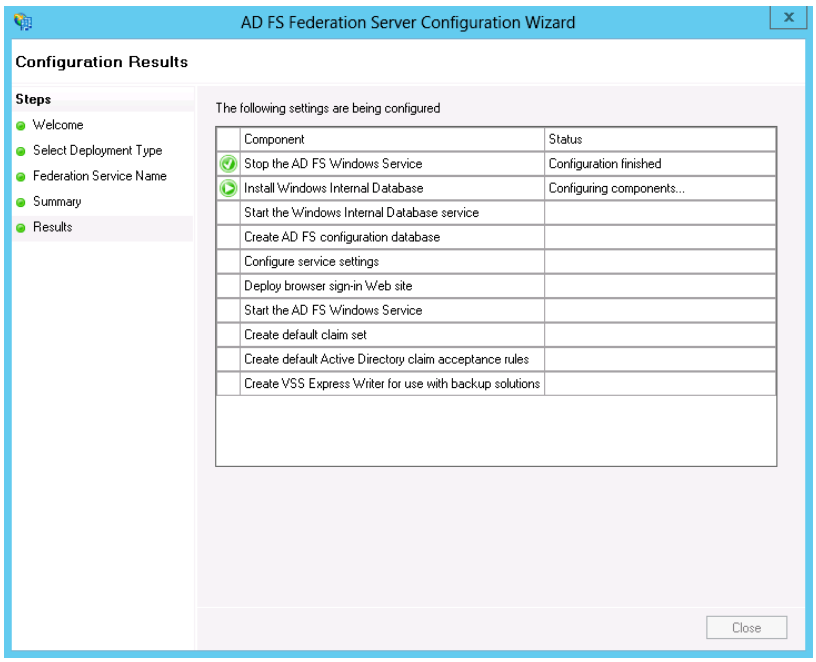
Let op dat deze optie bedoeld is voor evaluatie en kleine productie omgevingen. Een Stand-alone federation server is niet meer om te zetten naar een farm. Een single-server farm kan daarentegen later uitgebreid worden naar meerdere (load balanced) servers maar vereist bij initiële installatie iets meer configuratie die hier niet behandeld zal worden. Over het algemeen is de belasting op een ADFS server niet erg hoog en volstaat deze Stand-alone installatie.



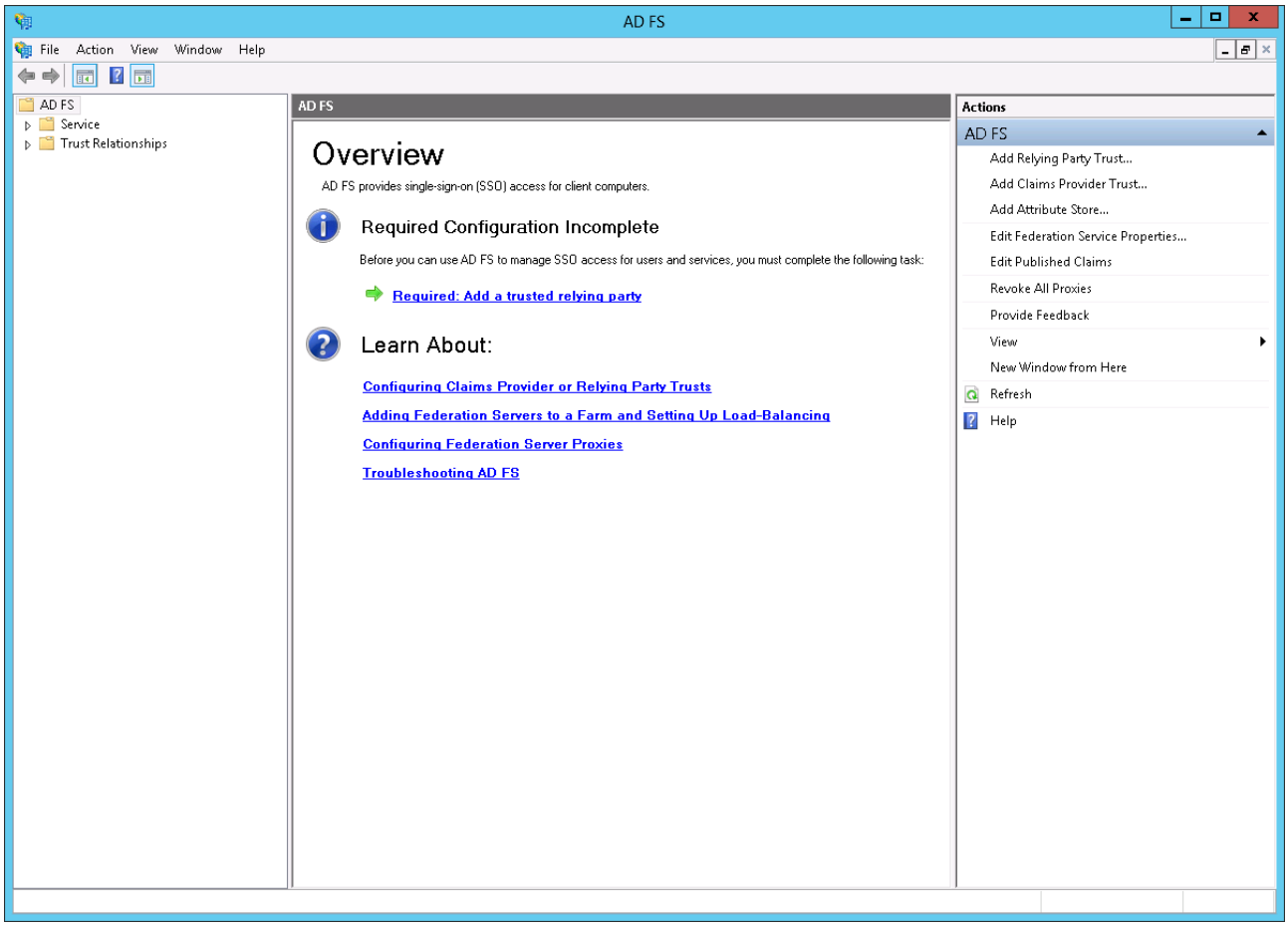
Selecteer het eerder geïnstalleerde SSL certificaat dat gebruikt gaat worden (Appendix A) voor het ontsluiten van de ADFS dienst en klik op “Next”.



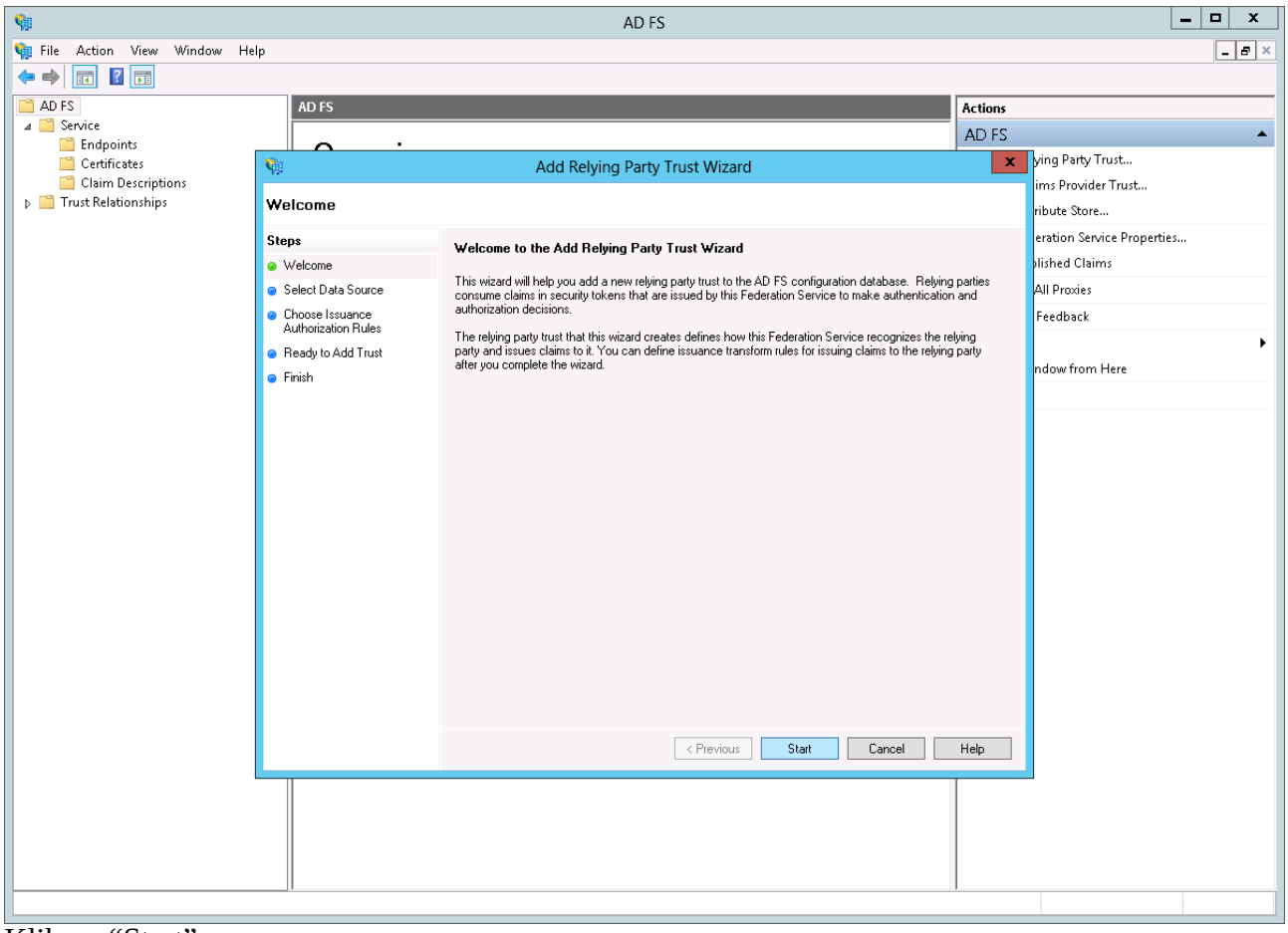
Klik op “Next”.



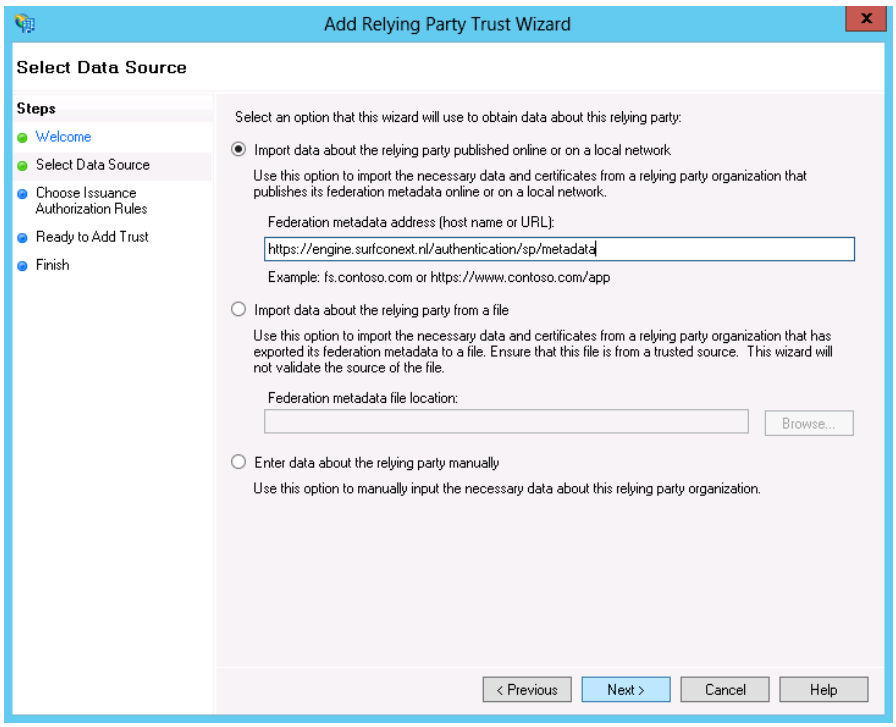
Wacht tot de Wizard klaar is met installatie en klik dan op “Close”.



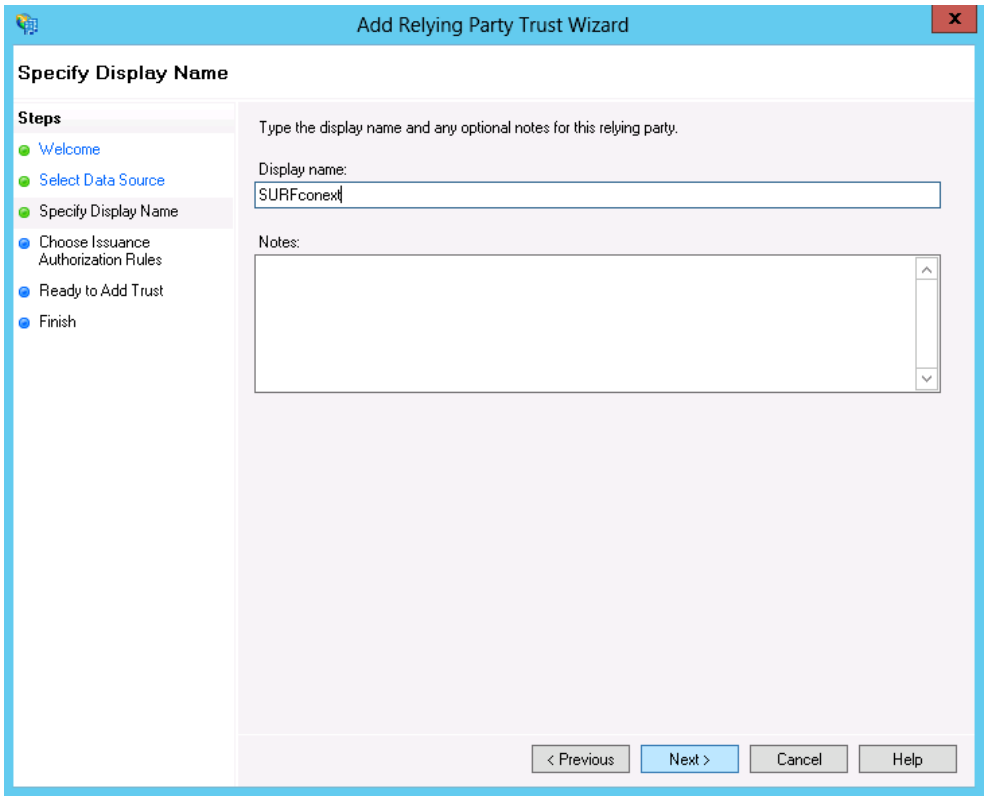
Zodra de Wizard afgesloten is, kan een “Trusted Relying party” (SURFConext) toegevoegd worden. Klik hiervoor op de link “Required: Add a trusted relying party”.



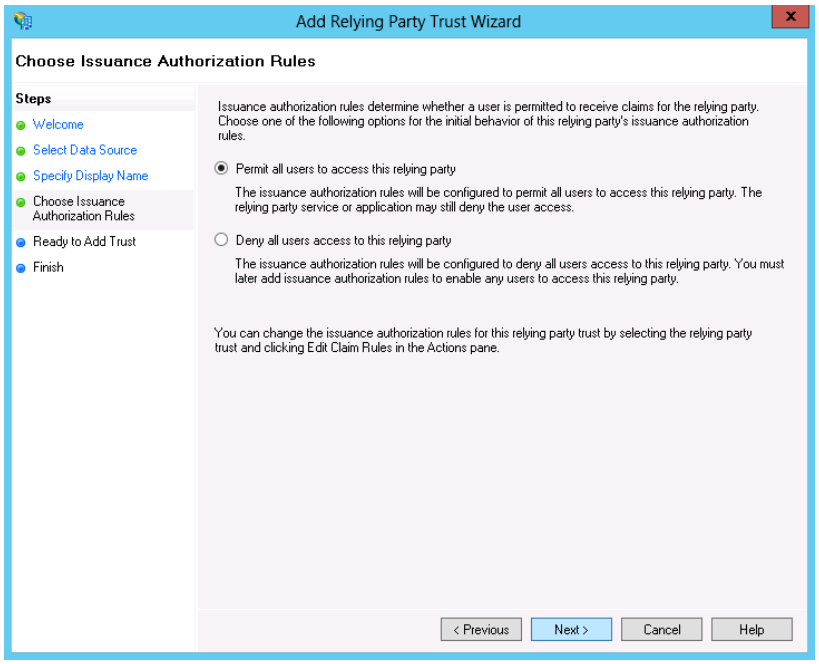
Klik op “Start”.



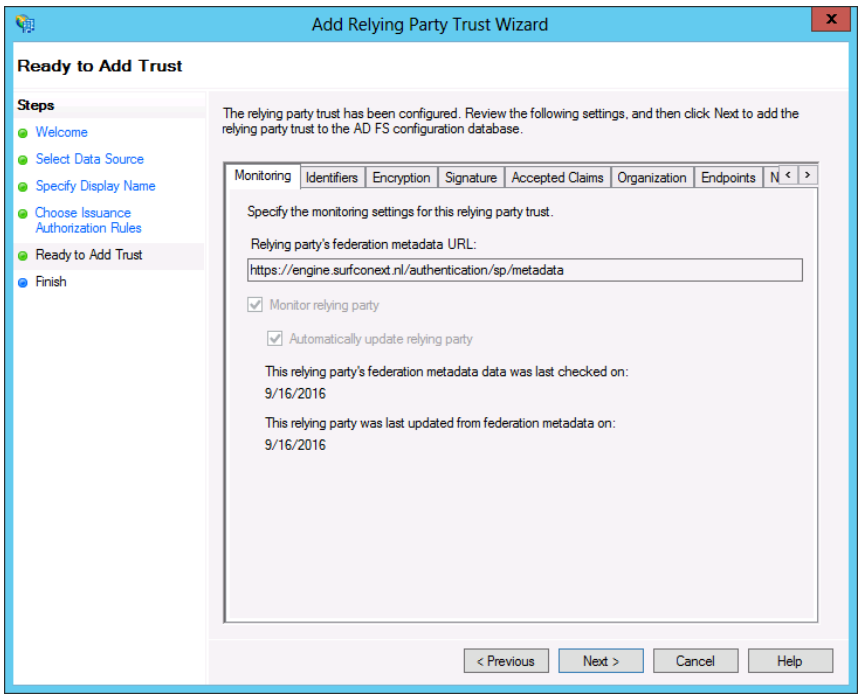
Selecteer “Import data about the relying party published online or on a local network” als de server toegang tot het internet heeft en geef als Federation metadata address “https://engine.surfconext.nl/authentication/sp/metadata” op. Als de server geen toegang tot het internet heeft kan deze metadata ook op een andere computer opgehaald worden en hier middels “Import data about the relying part from a file” optie geïmporteerd worden.



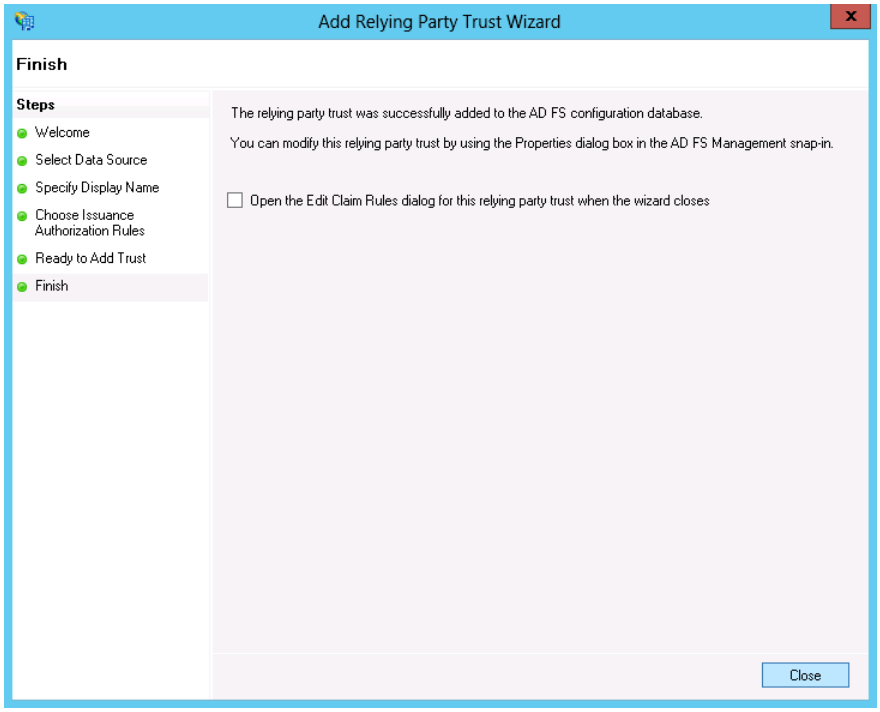
Noem de connectie SURFconext en klik op “Next”. Er is geen expliciete SURFconext acceptie omgeving met eigen metadata. Deze aansluiting zal na technische goedkeuring van SURFnet “productie” status krijgen en hiervoor is geen aanpassing in de metadata nodig.



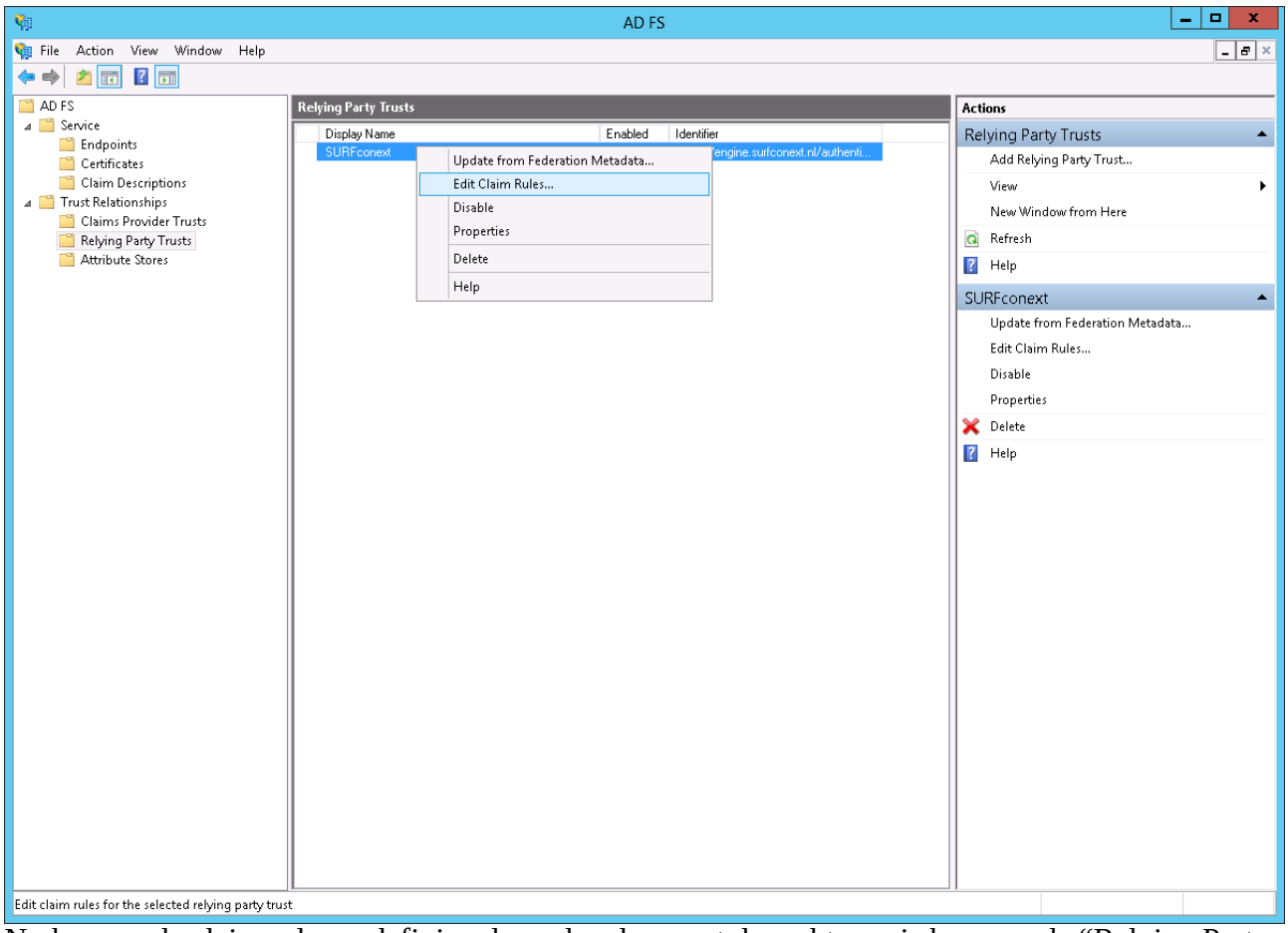
Selecteer hier “Permit all users to acces this relying party” tenzij anders gewenst.



Klik op “Next”.



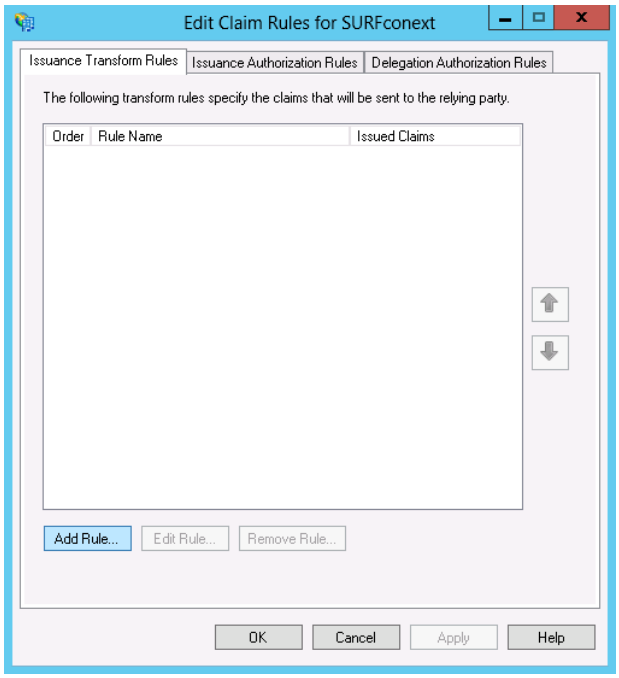
Klik op “Close”. Als het vinkje voor “Open the Edit Claim Rules dialog for this relying party trust when the wizard closes” aangevinkt blijft zal direct de hieronder beschreven “Edit Claim Rules” dialoog geopend worden.



Nu kunnen de claim rules gedefinieerd worden door met de rechtermuis knop op de “Relying Party Trusts” te klikken en “Edit Claim Rules...” te kiezen.

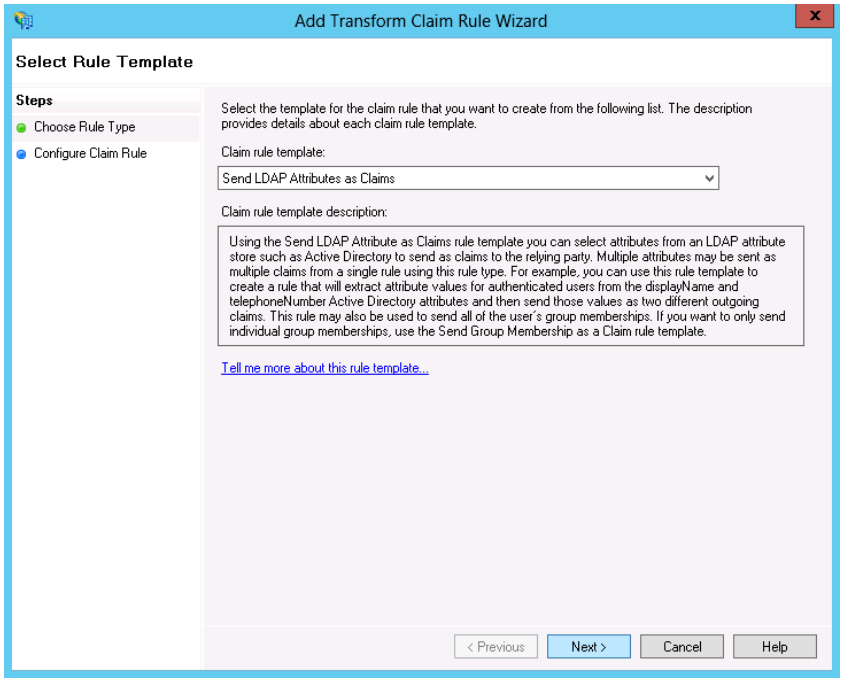
Claim Rules toevoegen

Vanaf hier zijn de Windows Server 2012 en 2012R2 installatie weer identiek.

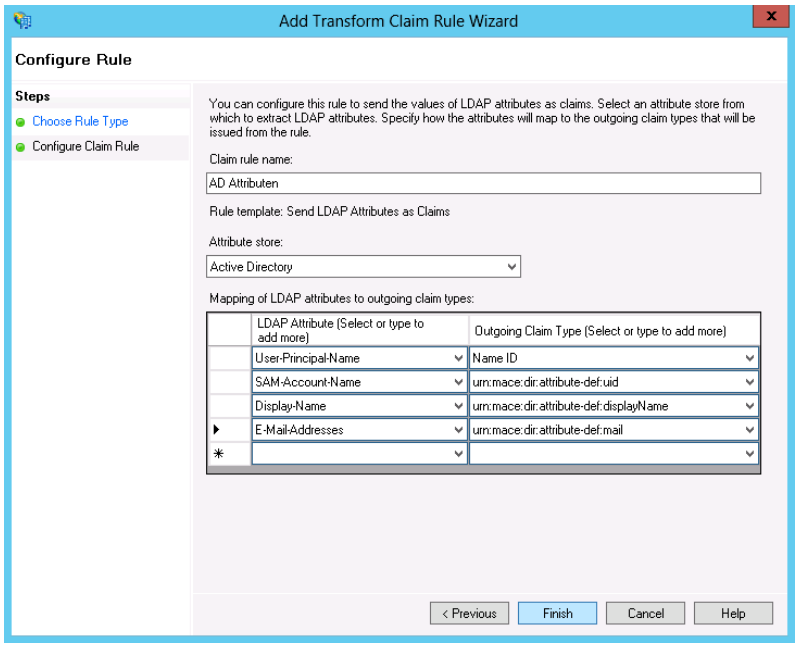


Om informatie over gebruikers aan SURFconext door te geven zullen we Claim rules toe moeten voegen. We beginnen met de eenvoudigste vorm: het transformeren van LDAP (AD) attributen naar SURFconext attributen.

Klik op “Add Rule...”



Selecteer “Send LDAP Attributes as Claims” en klik op “Next”. Hiermee geven we bestaande attributen in AD uit als Federatie attributen naar SURFconext.



Geef de rule een naam “AD Attributen”, kies “Active Directory” als Attribute store” en voeg een voor een de volgende Mappings toe:

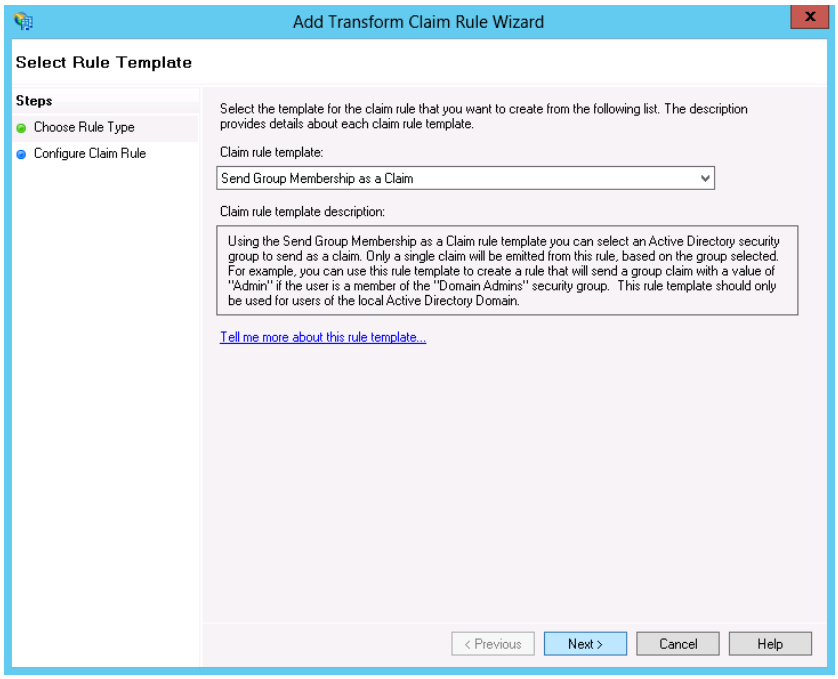
LDAP Attribute	**Outgoing Claim Type**
User-Principal-Name	Name ID
SAM-Account-Name	urn:mace:dir:attribute-def:uid
Display-Name	urn:mace:dir:attribute-def:displayName

E-Mail-Addresses	urn:mace:dir:attribute-def:mail

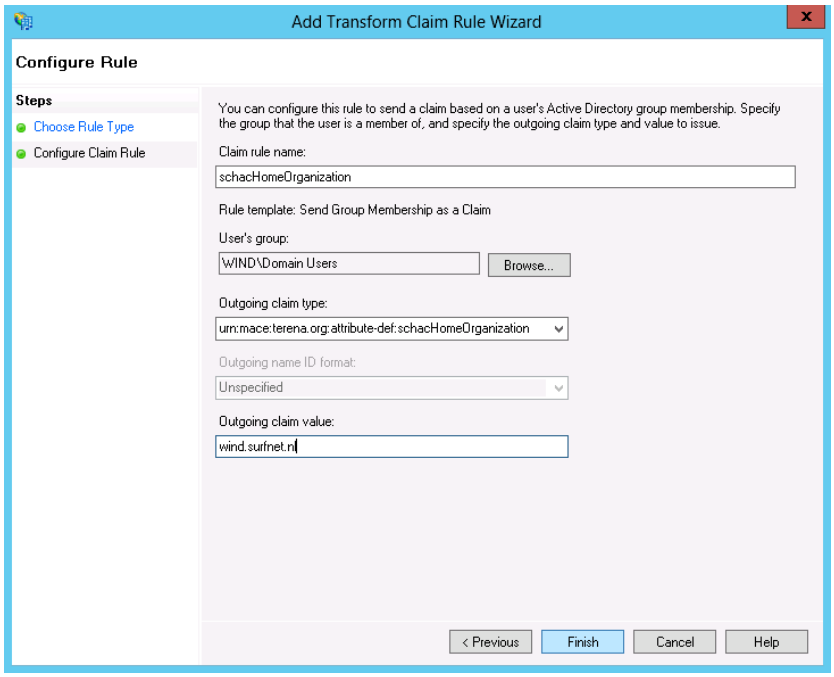
Kies “Finish”.

Vervolgens willen we voor iedereen het schacHomeOrganization met een vaste uitgaande waarde configureren. We doen dit door deze claim afhankelijk te laten zijn van lidmaatschap van de groep “Domain Users” (waar iedereen lid van is, als het goed is).

Selecteer weer “Add Rule...”



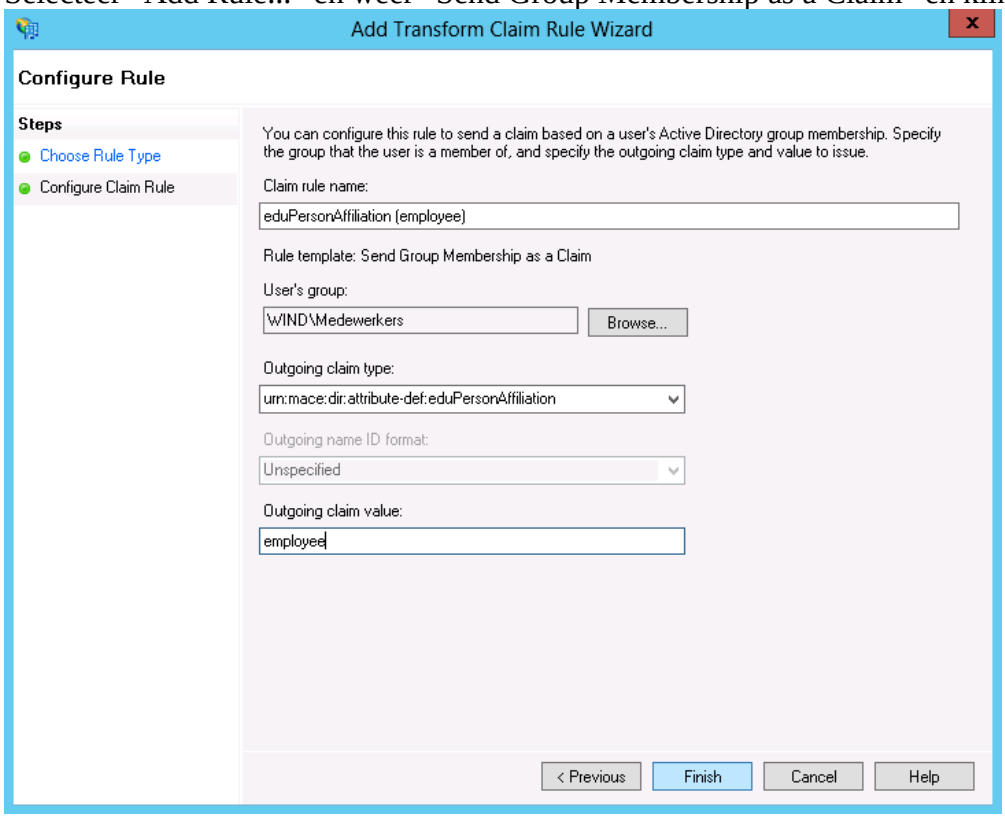
En selecteer “Send Group Membership as a Claim” en klik op “Next”.



Noem de rule “schacHomeOrganization” selecteer User's group “Domain Users”, Outgoing claim type “urn:mace:terena.org:attribute-def:schacHomeOrganization” en Outgoing claim value de DNS domeinnaam van de instelling (bijvoorbeeld 'surfnet.nl'). Klik op “Finish”.

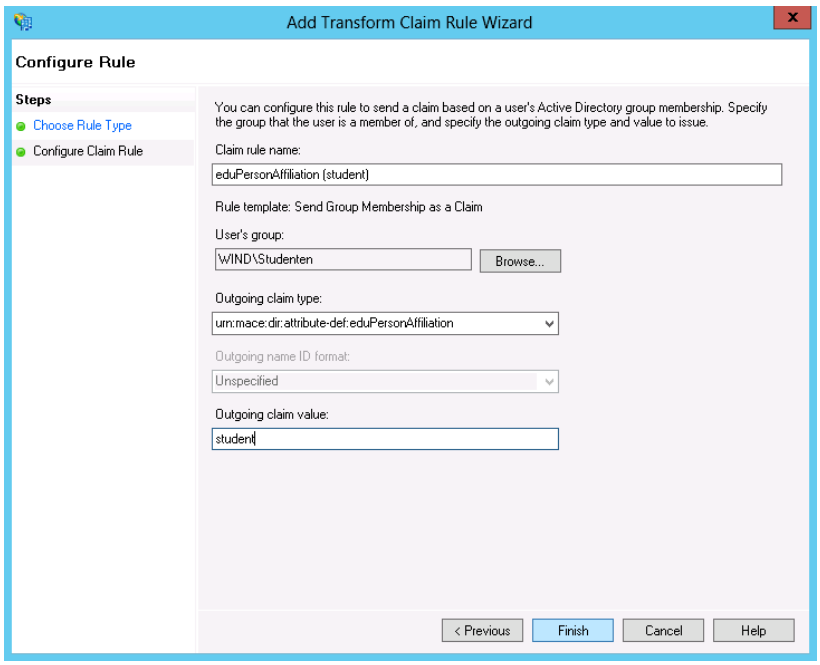
Nu gaan we twee rules toevoegen die beide een andere waarde voor hetzelfde attribuut (eduPersonAffiliation) uitgeven afhankelijk van de groep waarin de gebruiker zit.

Selecteer “Add Rule...” en weer “Send Group Membership as a Claim” en klik op “Next”.



Geef de Claim rule name “eduPersonAffiliation (employee)”, kies als User's group de AD groep voor alle medewerkers en Outgoing claim type “urn:mace:dir:attribute-def:eduPersonAffiliation”. Geef als waarde voor Outgoing claim value “employee”. Klik op “Finish”.

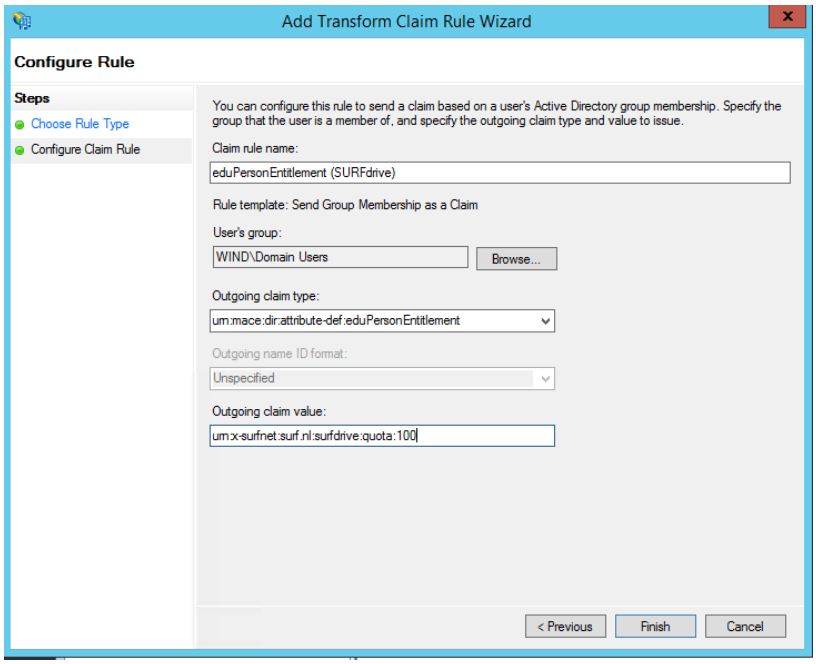
Selecteer nogmaals “Add Rule...” en weer “Send Group Membership as a Claim” en klik op “Next”.



Noem de rule “eduPersonAffiliation (student)”, kies als User's group de AD groep waar alle studenten in zitten en Outgoing claim type “urn:mace:dir:attribute-def:eduPersonAffiliation”. Selecteer als Outgoing claim value de waarde “student”. Klik op “Finish”.

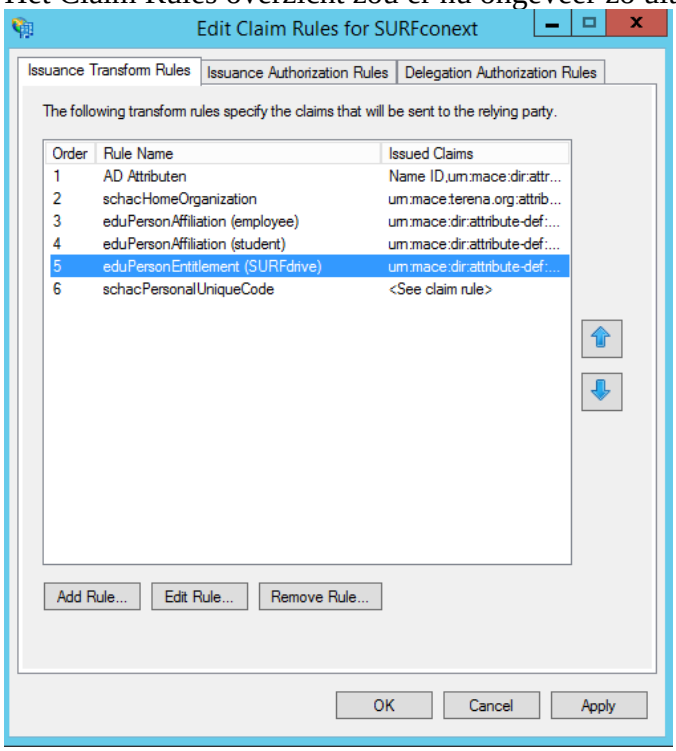
Het eduPersonEntitlement attribuut wordt door SURFConext gebruikt om applicatie specifieke attributen door te geven zoals voor de applicatie SURFdrive. Als het attribuut de waarde “urn:x-surfnet:surf.nl:surfdrive:quota:100” bevat mag de gebruiker hier gebruik van maken. We gaan de uitgifte van dit attribuut en deze waarde koppelen aan lidmaatschap van de AD groep “Users”.

Selecteer nogmaals “Add Rule...” en weer “Send Group Membership as a Claim” en klik op “Next”.



Noem de rule “eduPersonEntitlement (SURFdrive)” en kies de AD groep waar alle gebruikers lid van zijn. Geef Outgoing claim type “urn:mace:dir:attribute-def:eduPersonEntitlement” en de Outgoing claim value de waarde “urn:x-surfnet:surf.nl:surfdrive:quota:100”.

Het Claim Rules overzicht zou er nu ongeveer zo uit moeten zien:



Als alles klopt, klik op “OK”.

Custom claim rules

Het kan voorkomen dat de gewenste waarde van een bepaald attribuut niet beschikbaar is in AD maar wel daaruit afgeleid zou kunnen worden. Een voorbeeld is schacPersonalUniqueCode. De vereiste syntax van dit attribuut is

urn:schac:personalUniqueCode:nl:local:<schacHomeOrganisation>:<id_type>:<id_token>

Let op dat de waarde een URN is en daarom moet voeldoen aan de eisen die aan een URN gesteld worden. Een belangrijke eis is dat een URN geen spaties mag bevatten.

Bijvoorbeeld:

urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:90210

Hiervan is het employeeid “90210” waarschijnlijk wel beschikbaar als medewerkernummer en kan het attribuut dus samengesteld worden uit de tekst

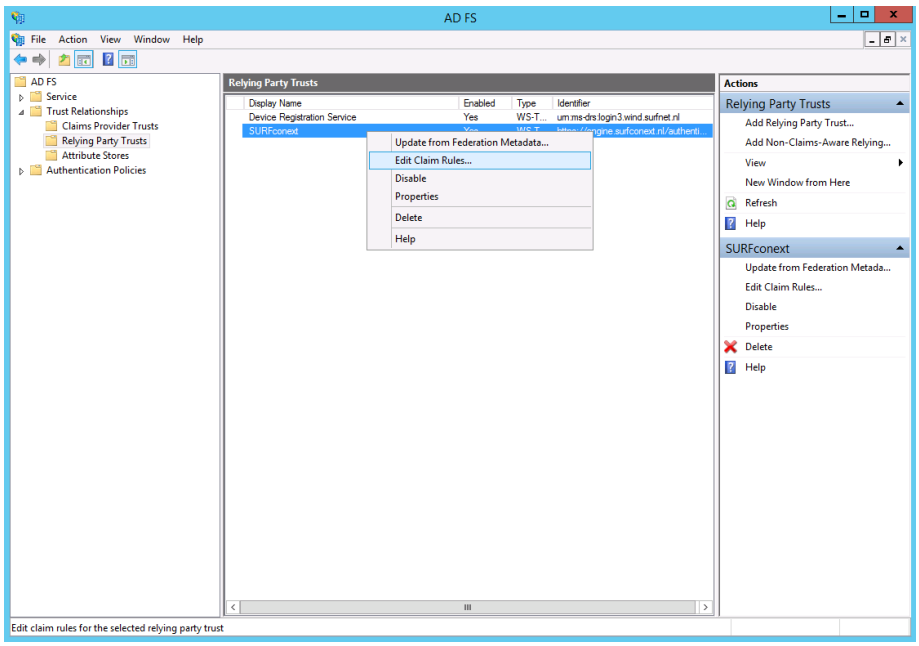
“urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:”

en bijvoorbeeld

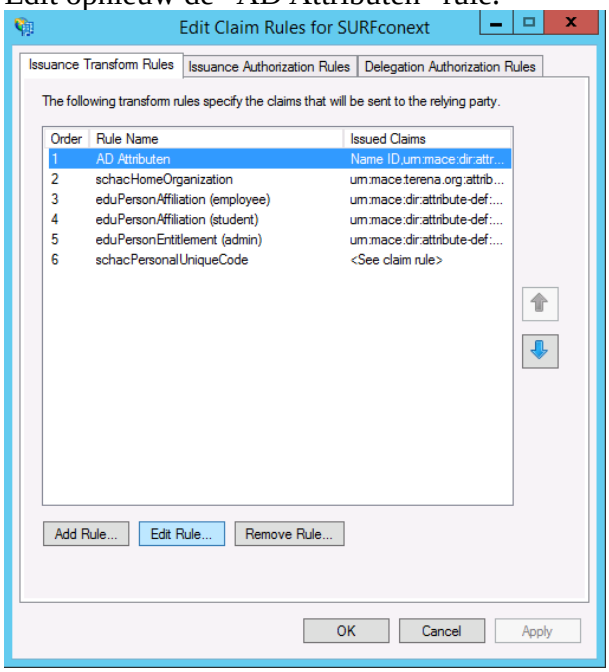
(de waarde van) het AD attribuut Employee-Number

Hiervoor kennen we de waarde van het AD attribuut Employee-Number eerst toe aan “urn:mace:dir:attribute-def:employeeNumber” en stellen daarmee later de personalUniqueCode samen.

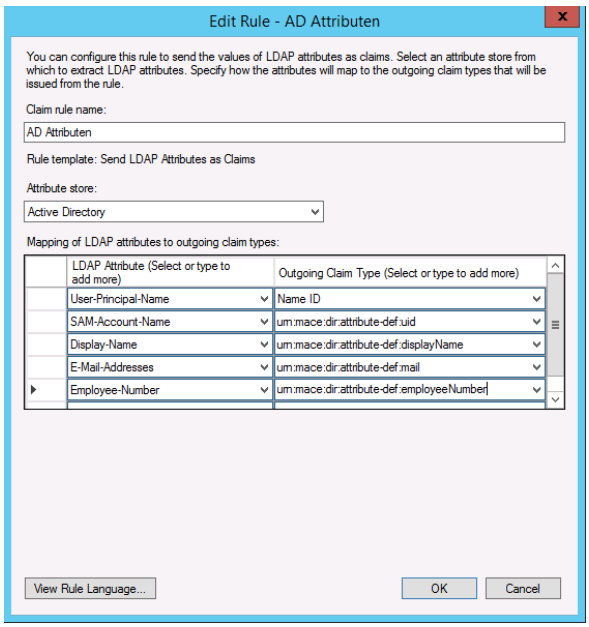
Edit opnieuw de Claim Rules van de Relying Party SURFconext



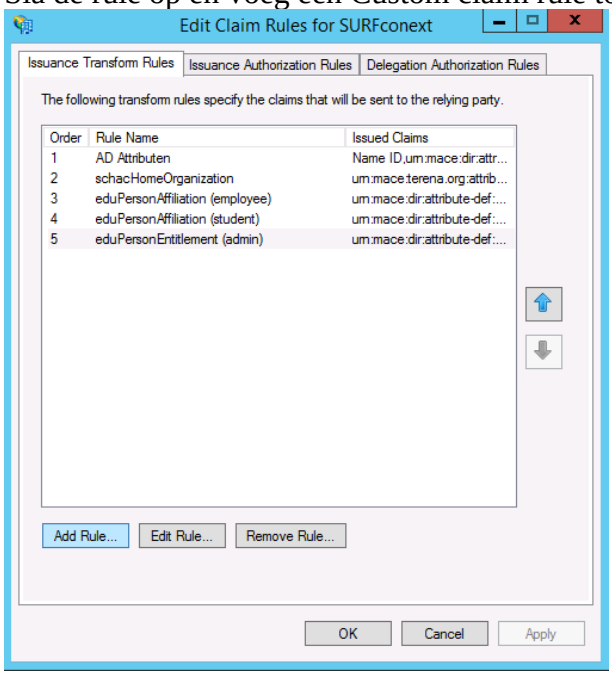
Edit opnieuw de “AD Attributen” rule.



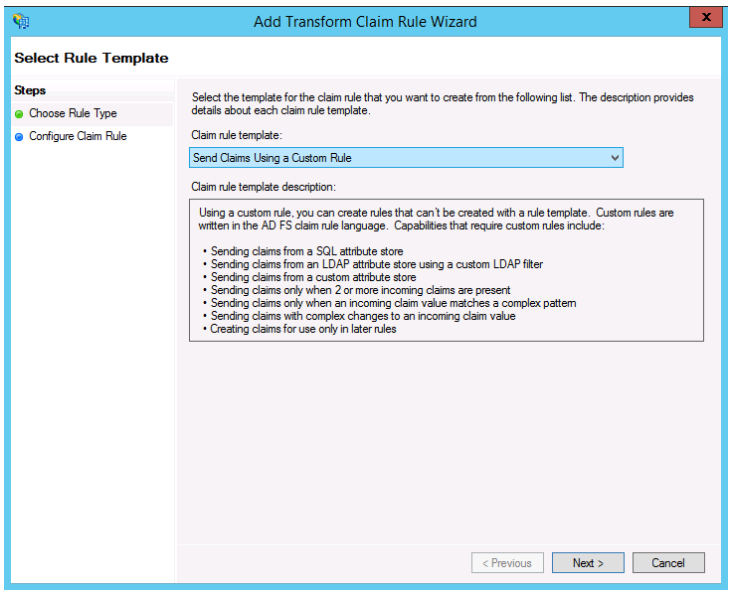
Voeg een regel toe die Employee-Number koppelt aan “urn:mace:dir:attribute-def:employeeNumber”.



Sla de rule op en voeg een Custom claim rule toe door op de “Add Rule...” knop te klikken.



Kies in het volgende venster voor “Send Claims Using a Custom Rule” en klik op “Next”.



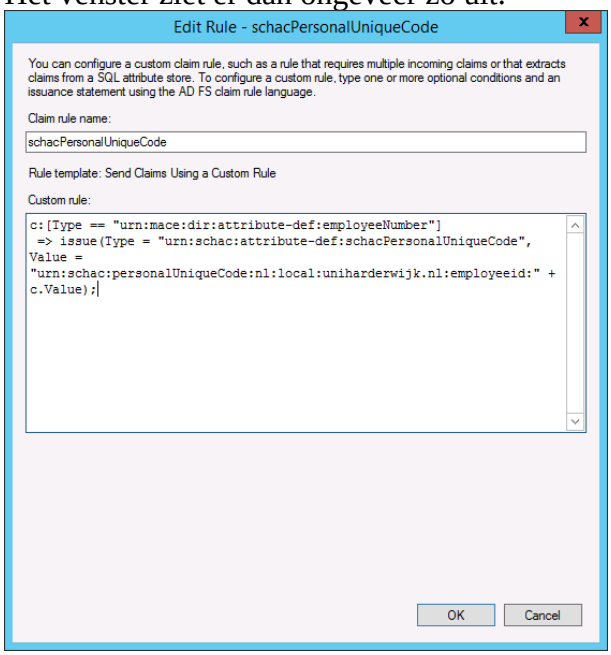
Geef de rule een beschrijvende naam zoals “schacPersonalUniqueCode” en creëer de gewenste attribuutsamenstelling op basis van een tekst en één of meerdere bestaande attributen.

```
c:[Type == "urn:mace:dir:attribute-def:employeeNumber"]
 => issue(Type = "urn:schac:attribute-def:schacPersonalUniqueCode", Value =
"urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:" + c.Value);
```

Bovenstaande code dient als volgt gelezen worden:

Als een attribuut van het type “urn:mace:dir:attribute-def:employeeNumber” bestaat, bewaar dit attribuut *dan* in variabele “c” *en* geef een nieuw attribuut van type “urn:schac:attribute-def:schacPersonalUniqueCode” uit met een samenstelling van de letterlijke tekst “urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:” en de *waarde* van het attribuut in variabele “c”.

Het venster ziet er dan ongeveer zo uit:



Als de Rule compleet is, klik dan op “OK”.
Een meer geavanceerde rule, welke ook de “*schacHomeOrganization*” en de “*affiliation*” meeneemt, ziet er dan als volgt uit:

```
c1:[Type == "urn:mace:dir:attribute-def:employeeNumber"] &&
c2:[Type == "urn:mace:terena.org:attribute-def:schacHomeOrganization"] &&
c3:[Type == "urn:mace:dir:attribute-def:eduPersonAffiliation"]
 => issue(Type = "urn:schac:attribute-def:schacPersonalUniqueCode", Value =
"urn:schac:personalUniqueCode:nl:local:" + c2.Value + ":" + c3.Value + "id:" + c1.Value);
```

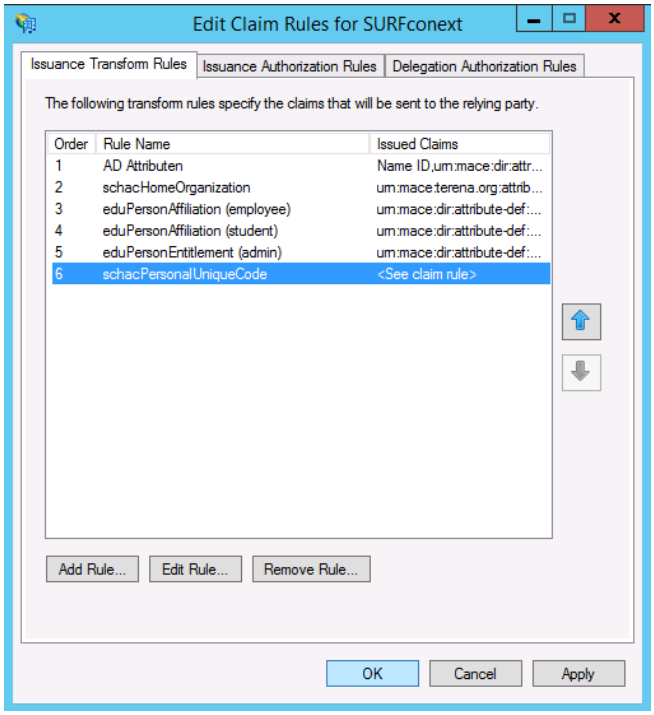
Om eduPersonScopedAffiliation toe te voegen aan de ADFS claims kan de volgende Custom claims rule gebruikt worden, er vanuit gaande dat de claims "urn:mace:dir:attribute-def:eduPersonAffiliation" en "urn:mace:terena.org:attribute-def:schacHomeOrganization" zoals eerder in deze handleiding beschreven, correct gedefinieerd zijn.

Kies weer voor "Edit Claim rules" en "Add Rule". Kies in het volgende scherm voor "Send Claims Using a Custom Rule" en klik op "Next".

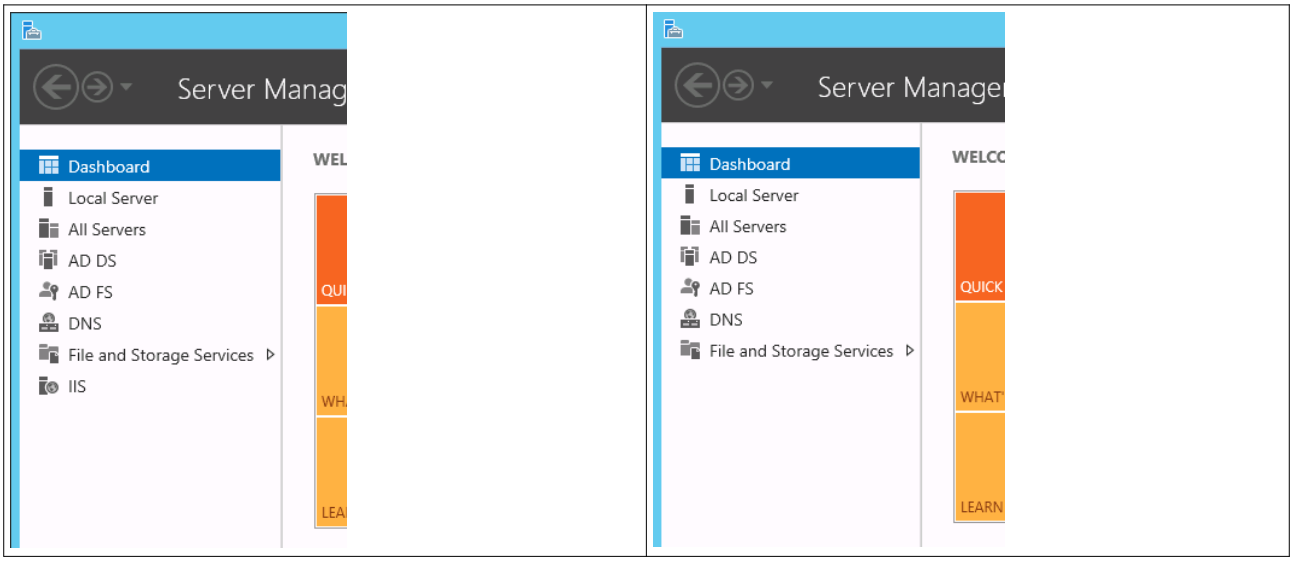
Geef de Rule een beschrijvende naam zoals "Create eduPersonScopedAffiliation" en plak de volgende code in het "Custom Rule" venster:

c1:[Type == "urn:mace:dir:attribute-def:eduPersonAffiliation"] &&
c2:[Type == "urn:mace:terena.org:attribute-def:schacHomeOrganization"]
=> issue(Type = "urn:mace:dir:attribute-def:eduPersonScopedAffiliation", Value = c1.Value + "@" + c2.Value);

Klik "Finish" en klik "Ok" in de "Edit Claims Rules" dialoog. Test hierna de uitgifte van het nieuwe attribuut.

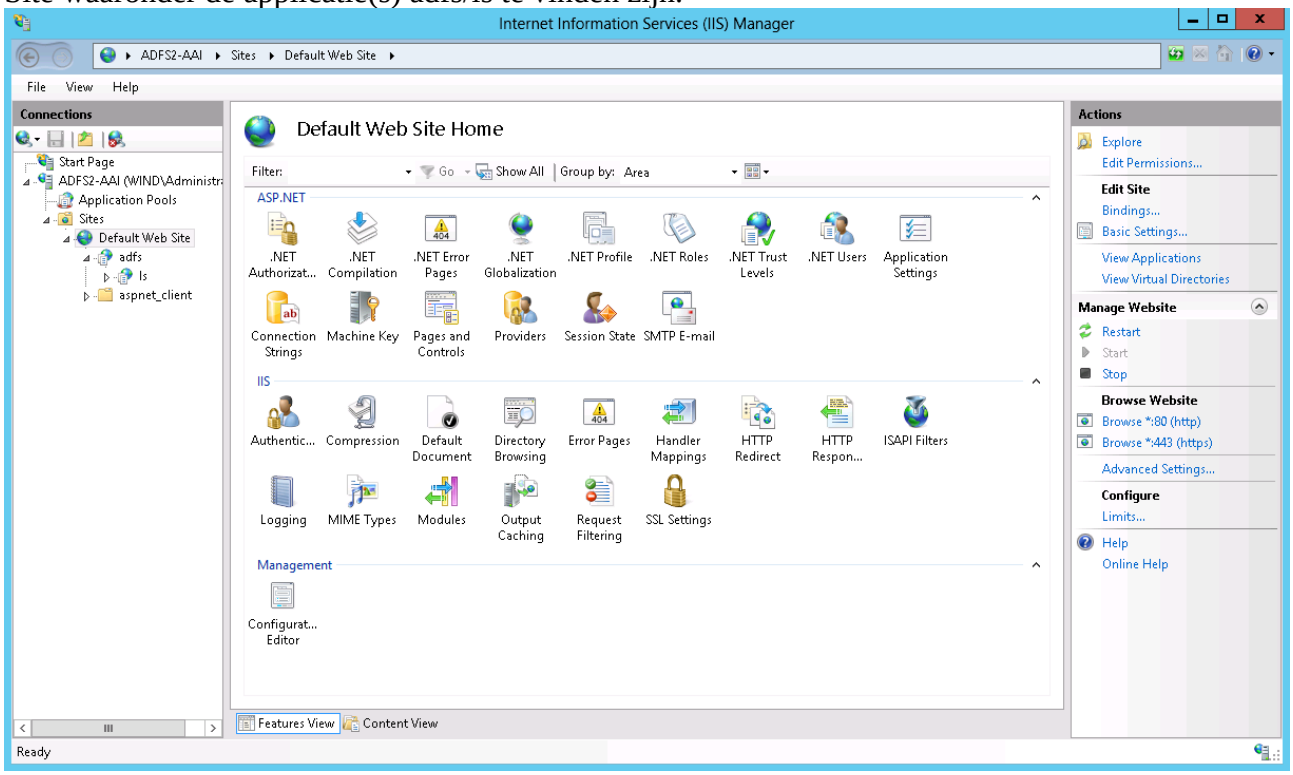


En bewaar, als alles klopt de Claim Rules set door op “OK” te klikken.



Zo horen het Dashboard van een Windows Server 2012 (links) en Windows Server 2012R2 (rechts) er na installatie uit te zien. Let op het verschil dat IIS niet geïnstalleerd is onder 2012R2.

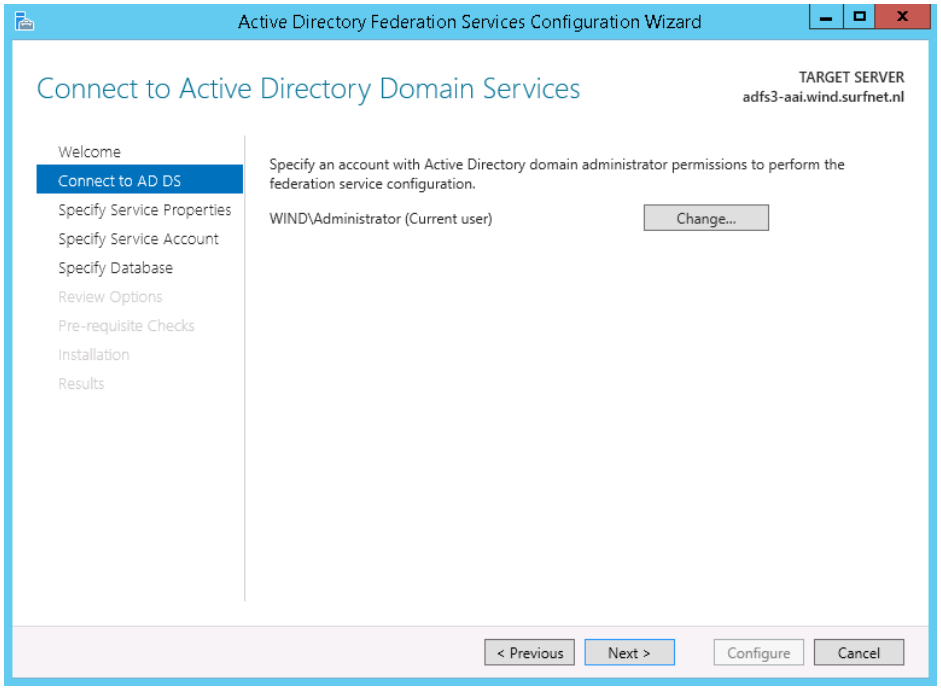
Controleer onder Windows Server 2012 of er een IIS service geïnstalleerd is met een default Web Site waaronder de applicatie(s) adfs/ls te vinden zijn.



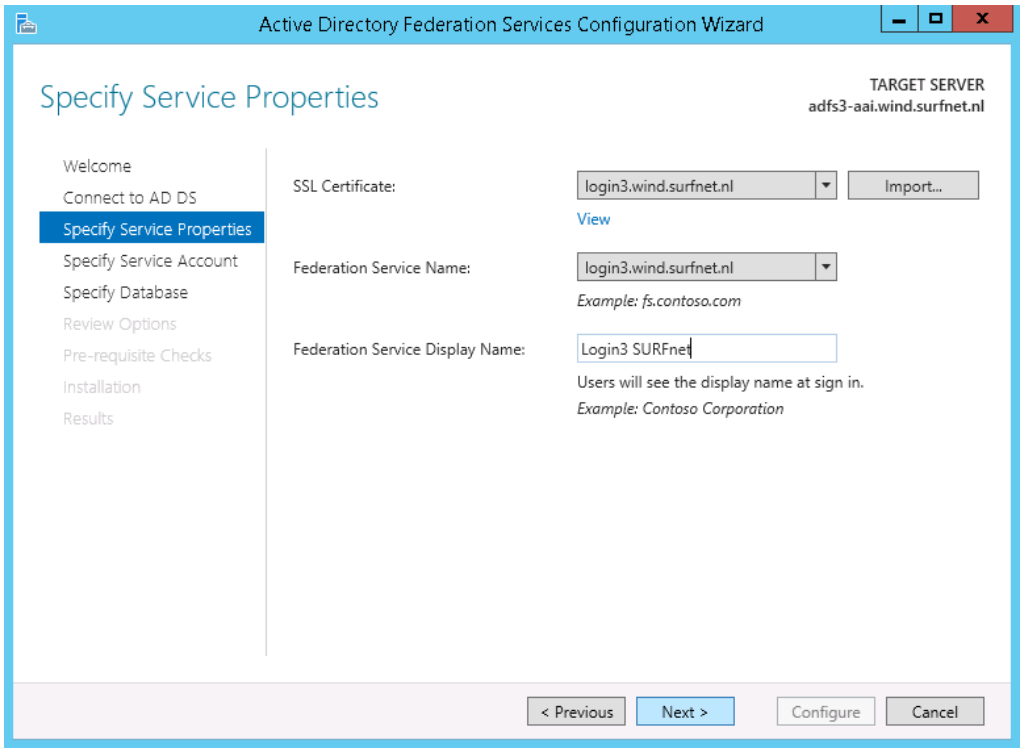
Let op: onder Windows Server 2012R2 ontbreekt deze stap!

ADFS Configuration Wizard 2012R2

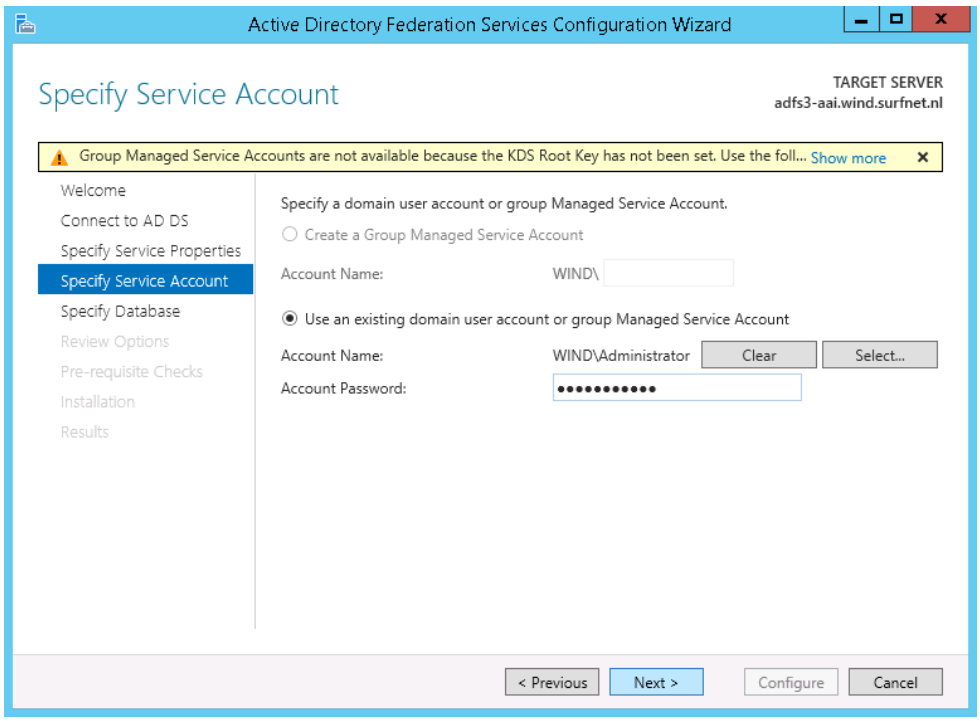
De ADFS installatie Wizard zie er onder Windows Server 2012R2 anders uit. We pakken hier de draad na installatie van de “ADFS Role” zoals hierboven beschreven op.



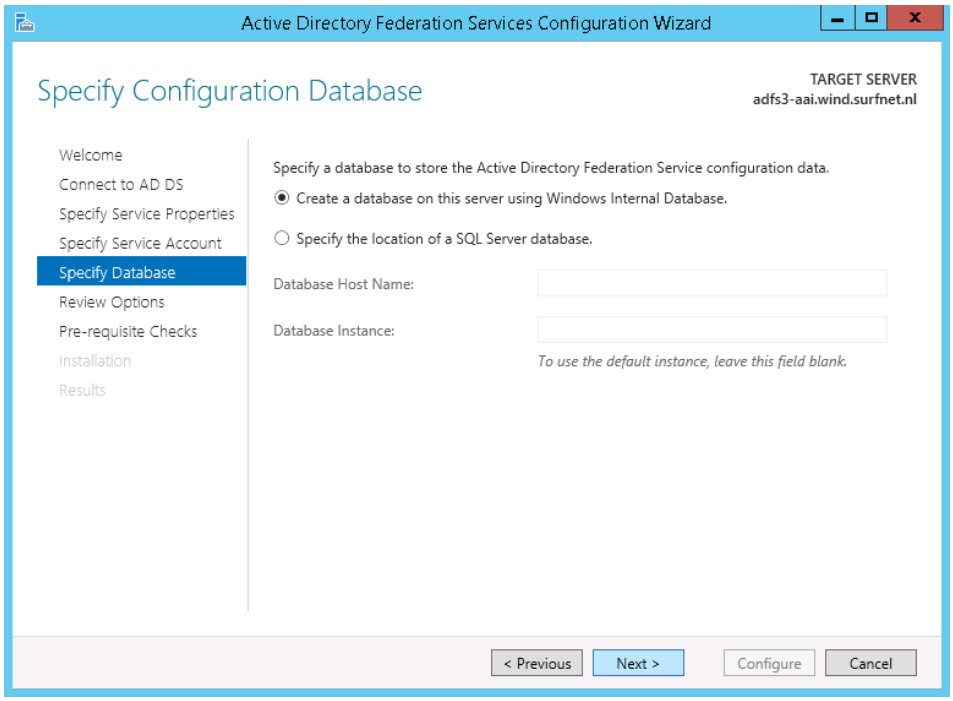
Kies voor een AD Administrator account waarmee de rest van deze Wizard voltooid zal worden en klik op “Next”.



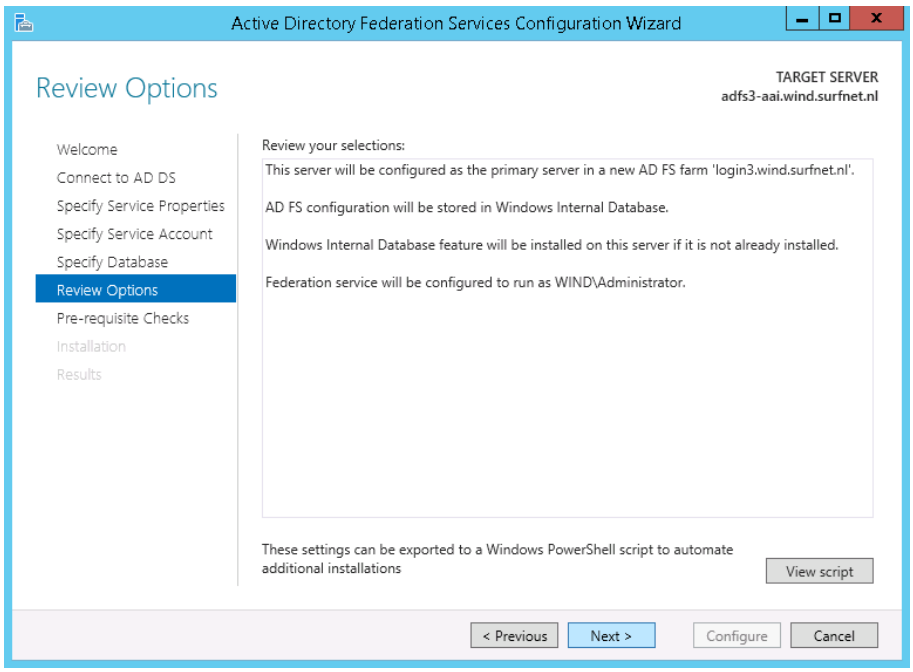
Kies het vooraf geïnstalleerde SSL certificaat waarmee de ADFS dienst ontsloten zal worden en een handige “Display Name” (bijvoorbeeld Login SURFnet). Klik op “Next”.



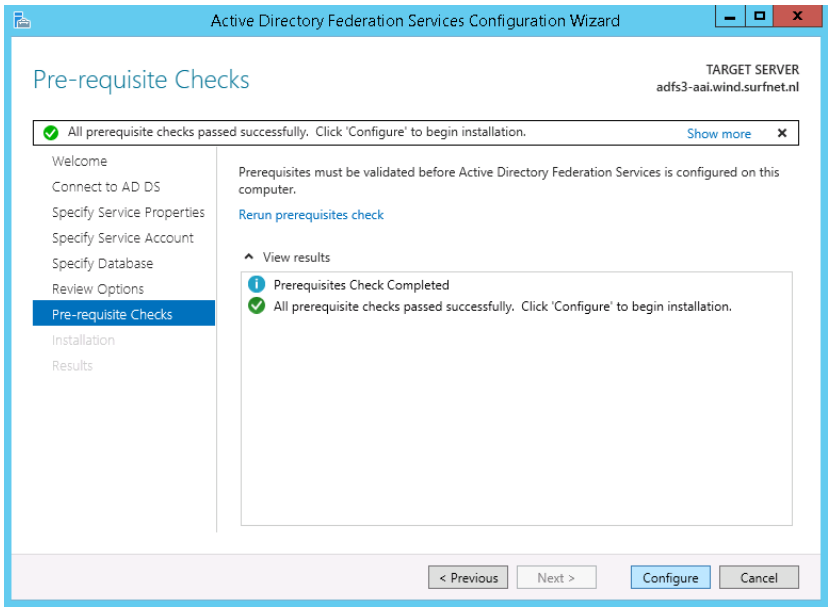
De waarschuwing in de gele balk kan opgelost worden door op “Show more” te klikken en het voorgestelde commando “Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)” in een Powershell uit te voeren. Kies voor een eenvoudige installatie een domain Administrator account voor het installeren van de ADFS service. Er kan ook gekozen worden voor een “Group Managed Account”.



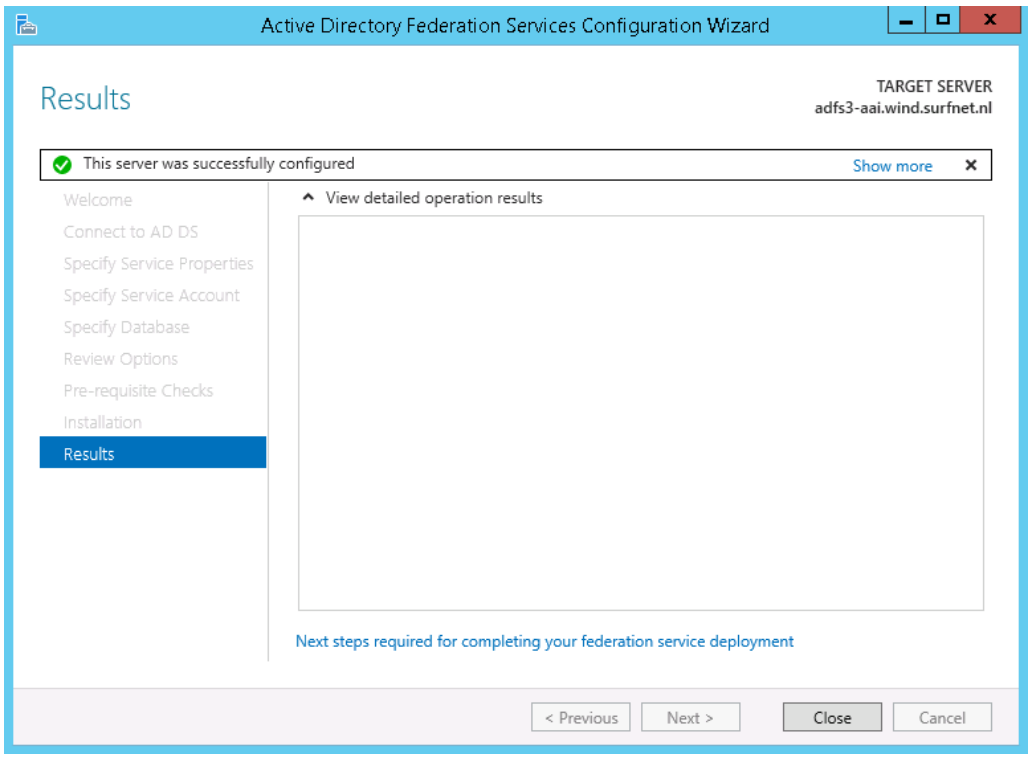
Selecteer “Create a database on this server using Windows Internal Database.” en klik op “Next”.



Klik op “Next”.

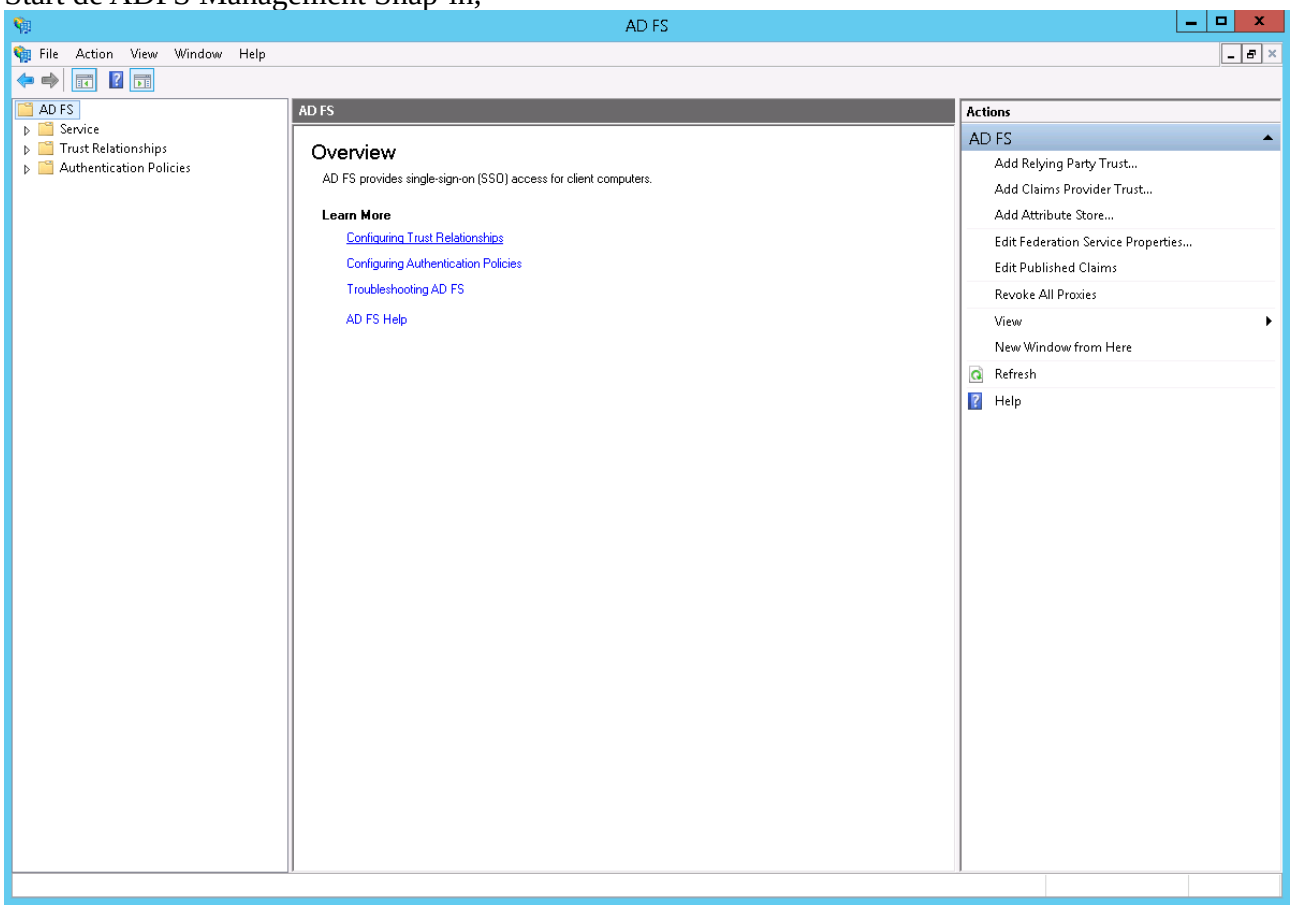


Klik op “Configure”.

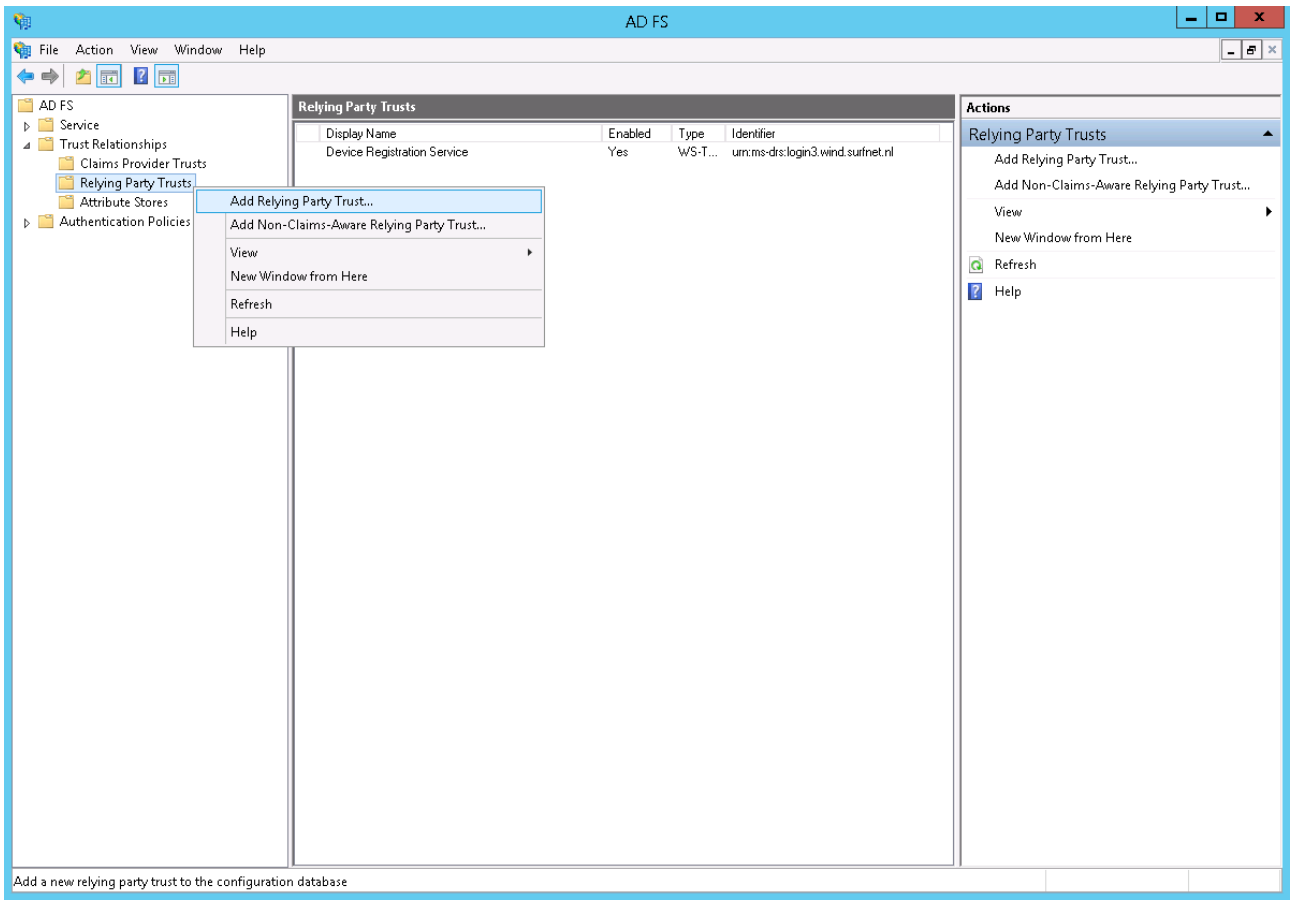


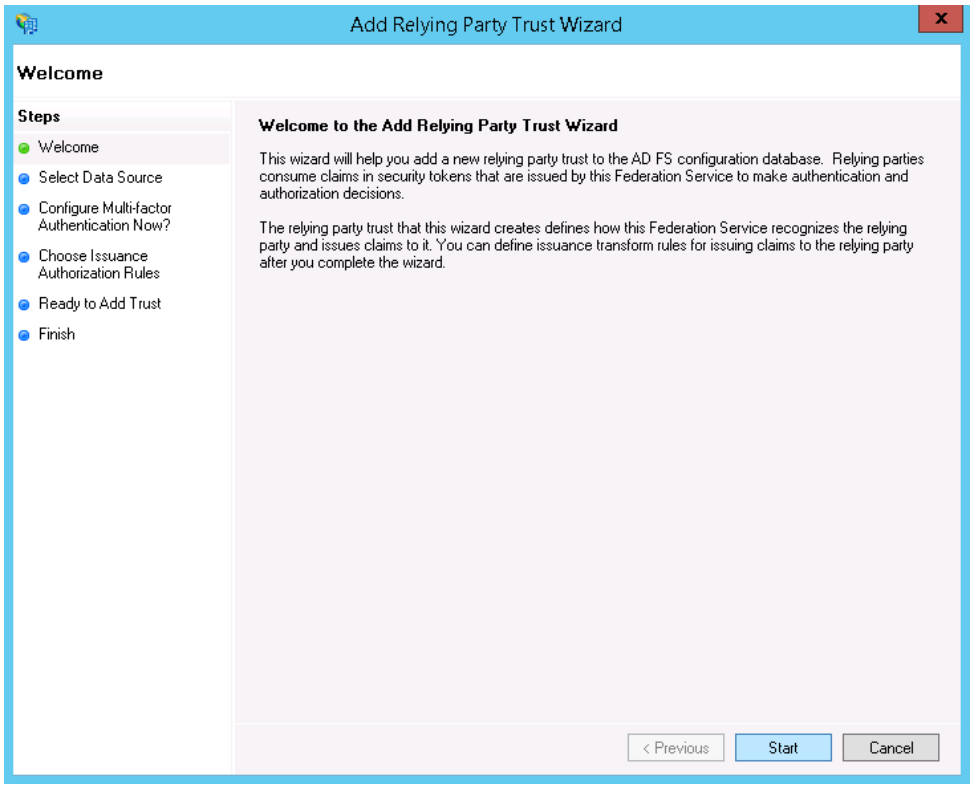
Wacht tot de installatie voltooid is en Klik op “Close”.

Start de ADFS Management Snap-in,

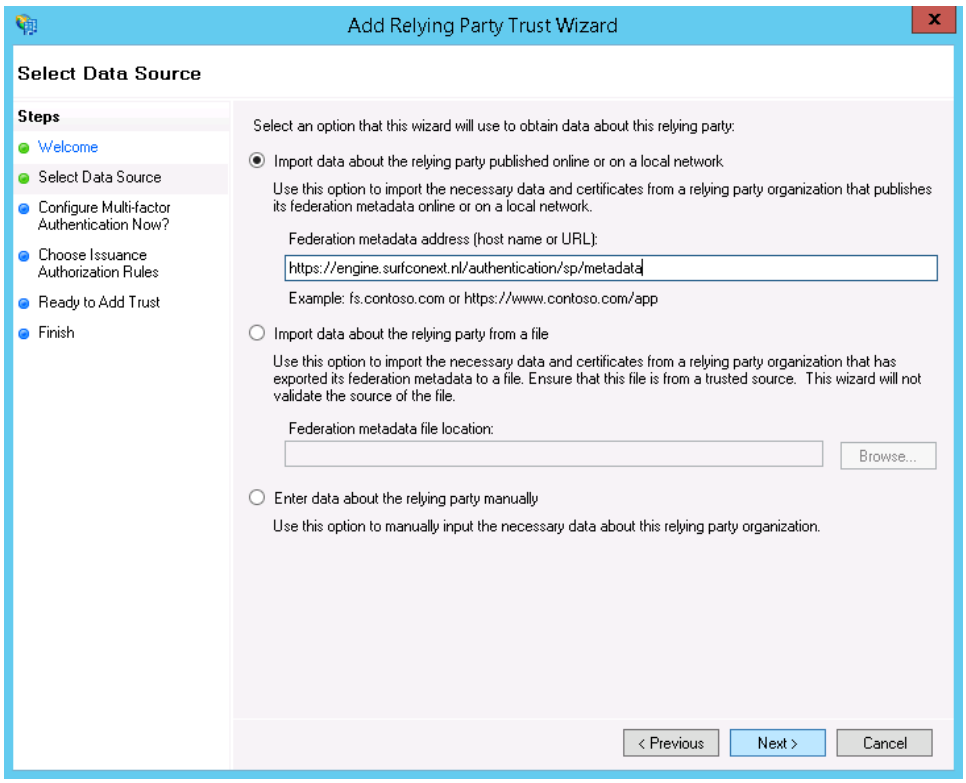


en selecteer “Add Relying Party Trust...” aan de rechter kant onder “Actions” of navigeer aan de linkerkant naar “Relying Party Trusts” en selecteer met de rechtermuis knop “Add Relying Party Trust...” zoals hieronder.

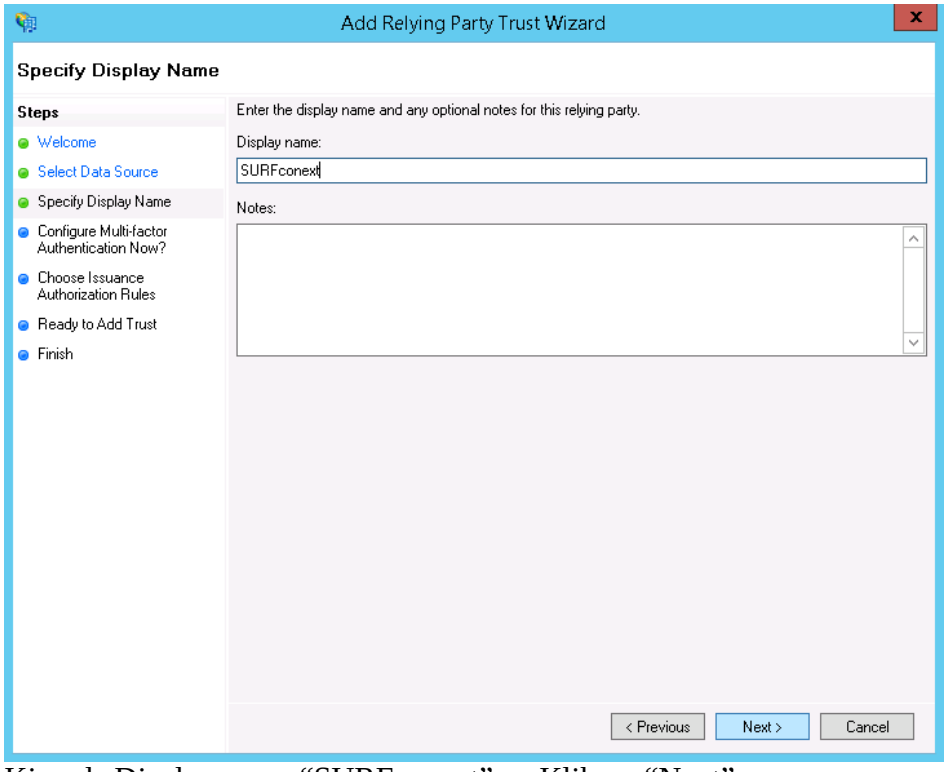




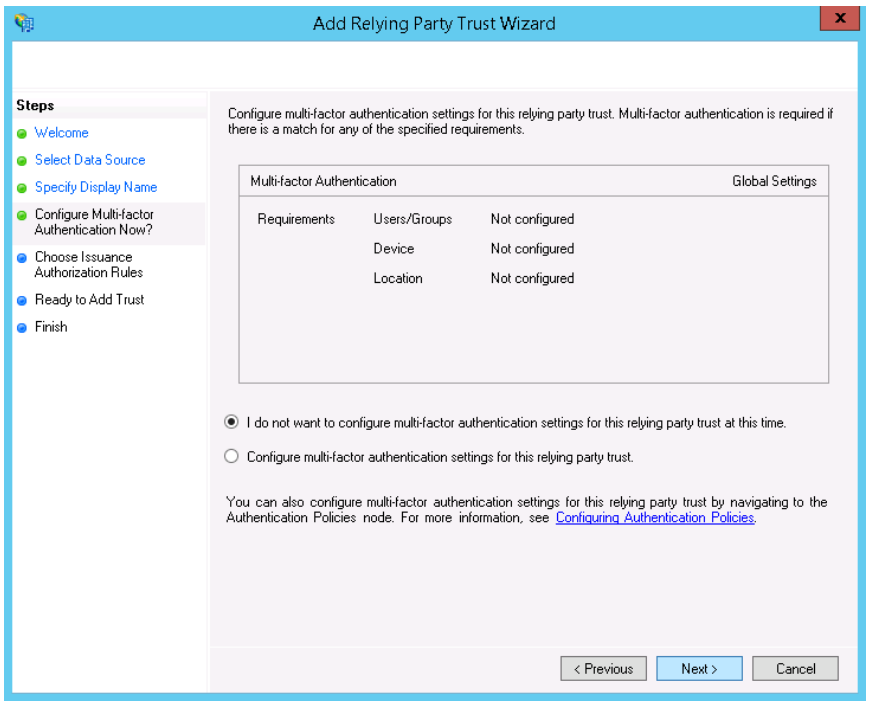
Klik op “Start”



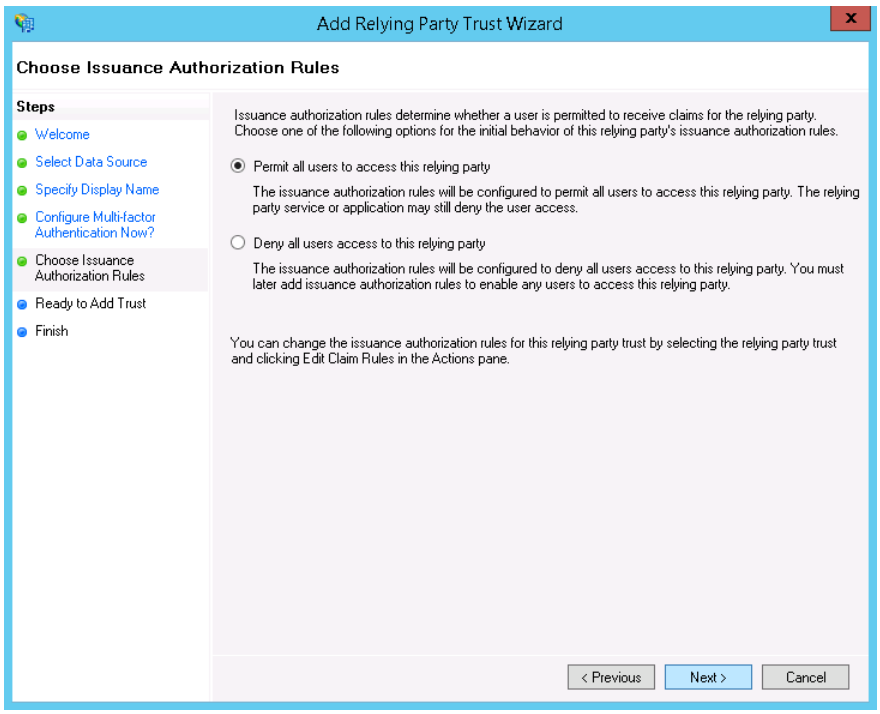
Selecteer “Import data about the relying party published online or on a local network” als de server toegang tot het internet heeft en geef als Federation metadata address “https://engine.surfconext.nl/authentication/sp/metadata” op. Als de server geen toegang tot het internet heeft kan deze metadata ook op een andere computer opgehaald worden en hier middels “Import data about the relying part from a file” optie geïmporteerd worden.



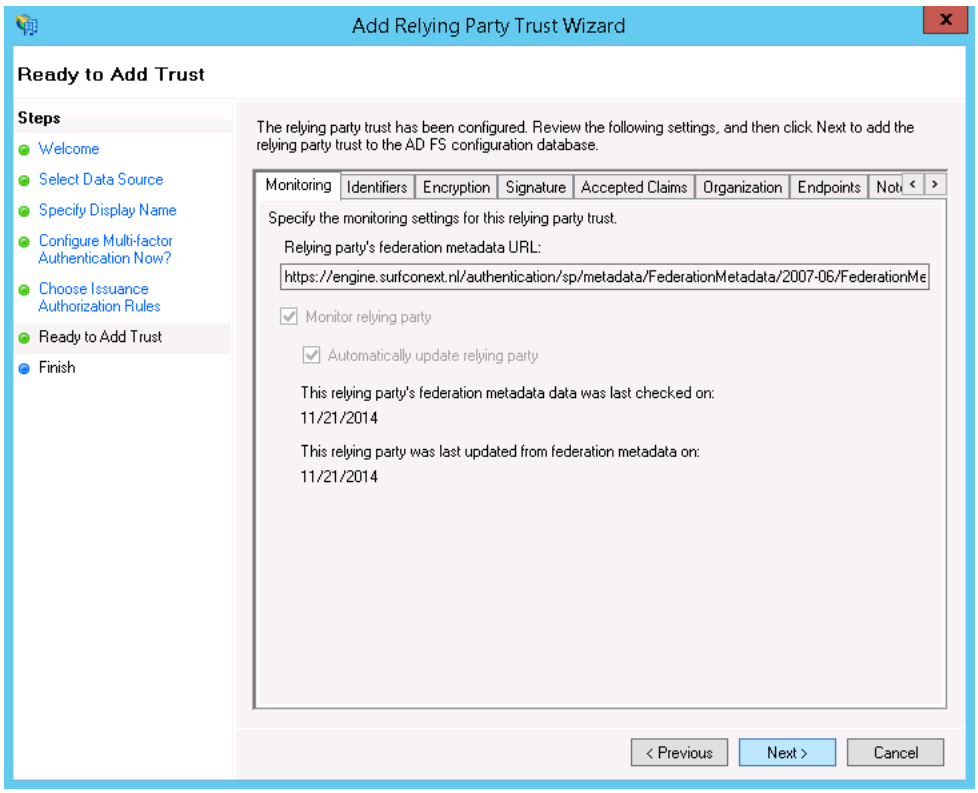
Kies als Display name “SURFconext” en Klik op “Next”.



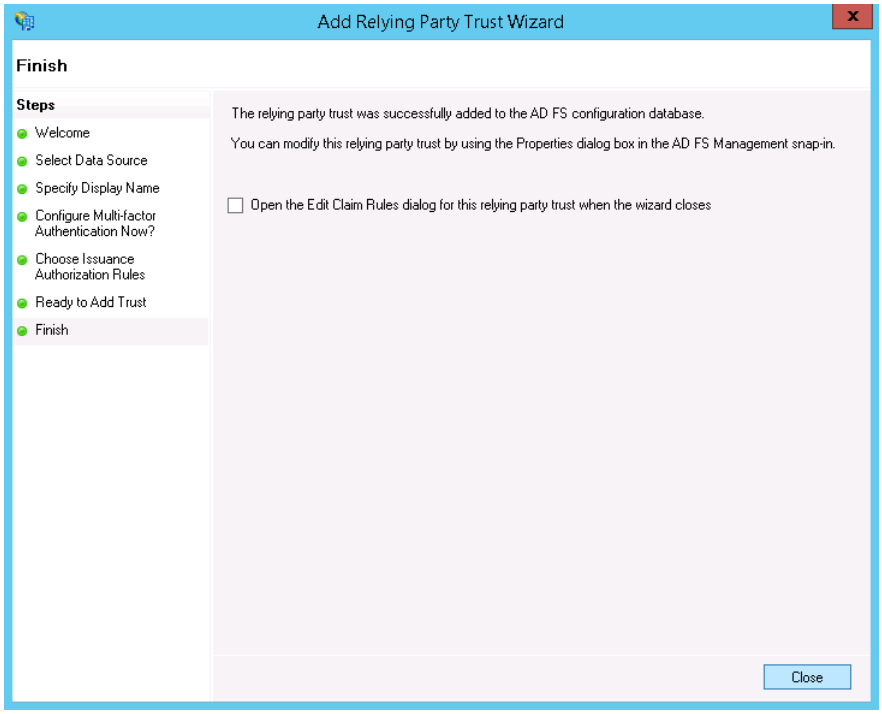
Selecteer voor een eenvoudige installatie zonder “multi-factor authentication” voor “I do no want to configure multi-factor authentication settings for this relying party trust at this time” en Klik op “Next”.



Selecteer “Permit all users to acccess this relying party” indien gewenst en Klik op “Next'.



Klik op “Next”.



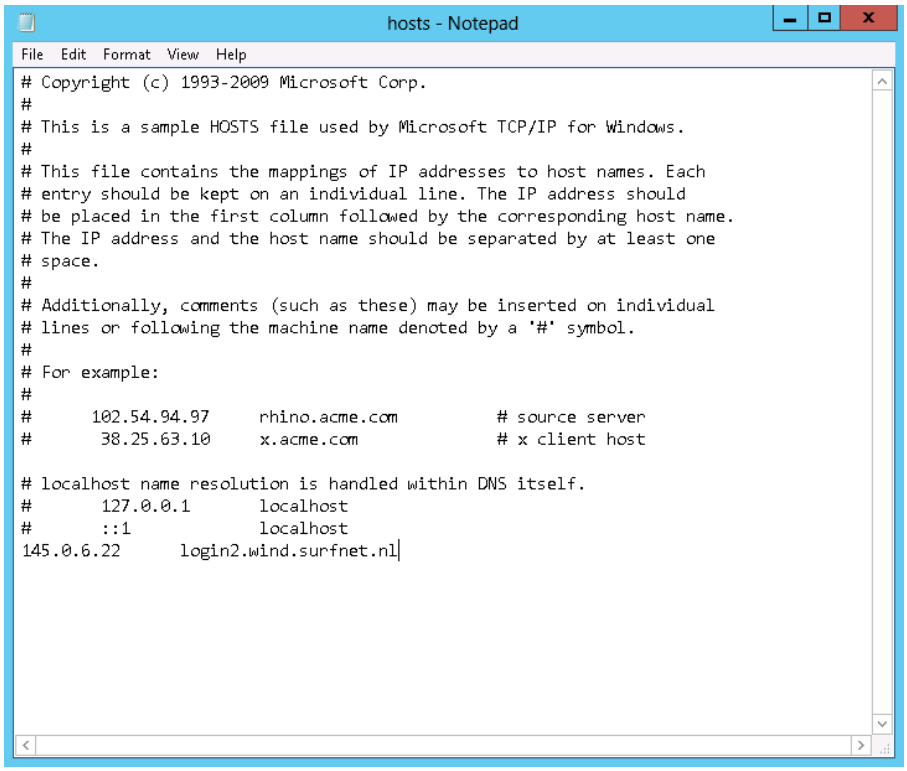
Klik op “Close”. Als het vinkje voor “Open the Edit Claim Rules dialog for this relying party trust when the wizard closes” aangevinkt blijft zal direct de hieronder beschreven “Edit Claim Rules” dialoog geopend worden. Anders kunnen de claim rules gedefinieerd worden door met de rechtermuis knop op de relying party te klikken en “Edit Claim Rules...” te kiezen. Ga daarvoor naar “Claim Rules toevoegen” terug in het Windows Server 2012 hoofdstuk.

ADFS Proxy installeren

Omdat de installatie van de ADFS proxy onder Windows Server 2012 en 2012R2 erg veel verschilt van elkaar, is deze voor beide servers van begin tot eind beschreven. Hieronder volgt de uitleg voor Server 2012, daarna komt Server 2012R2.

Algemeen

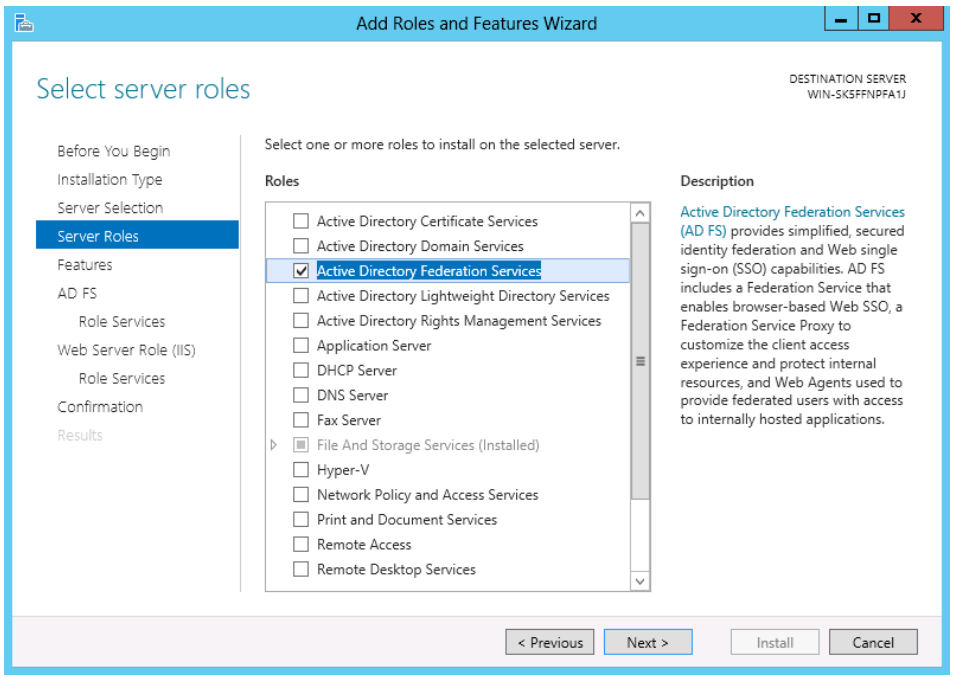
Het is belangrijk dat de ADFS Proxy de ADFS server onder de voor de ADFS service gekozen DNS naam kan bereiken. De Proxy zelf moet echter onder dezelfde naam voor de buitenwereld (het internet) bereikbaar zijn. Hiervoor kan een split-DNS (zie verklarende woordenlijst) configuratie ingericht worden. Als dat niet mogelijk is, moet de Proxy op een andere manier verteld worden wat het IP adres van de ADFS server is. Dat kan met behulp van de hosts file (C:\Windows\System32\Drivers\etc). Voeg hiervoor een regel toe met vooraan het fysieke adres van de ADFS server en daarachter de servicenaam waaronder de ADFS dienst beschikbaar is:



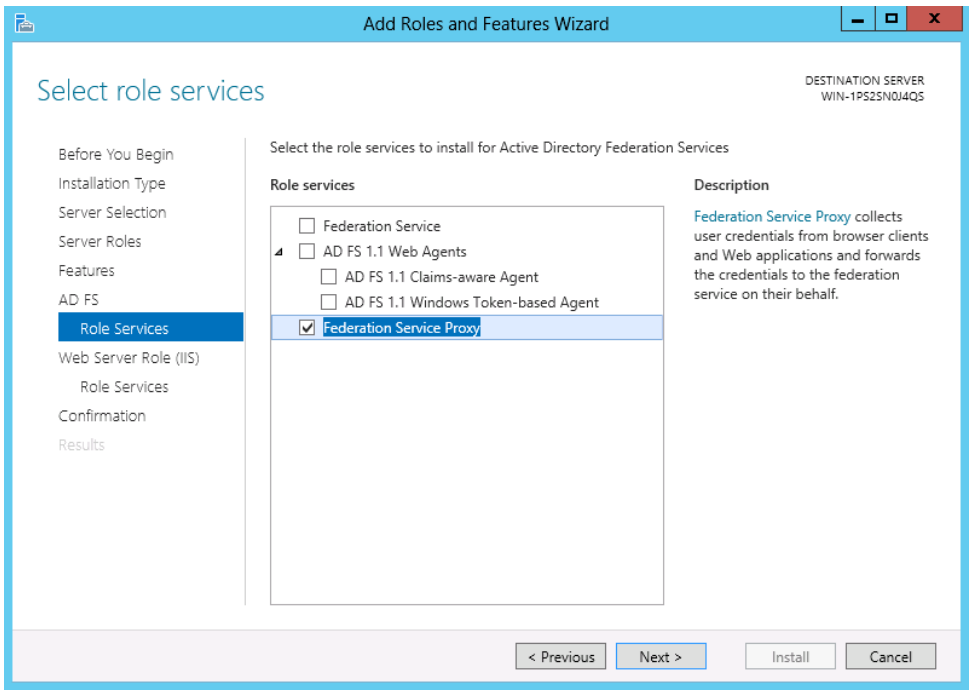
Let op: dit bestand is alleen als Administrator te bewerken. Start hiervoor een Notepad op onder “run as Adminstrator” conditie.

ADFS Proxy installeren onder Windows Server 2012

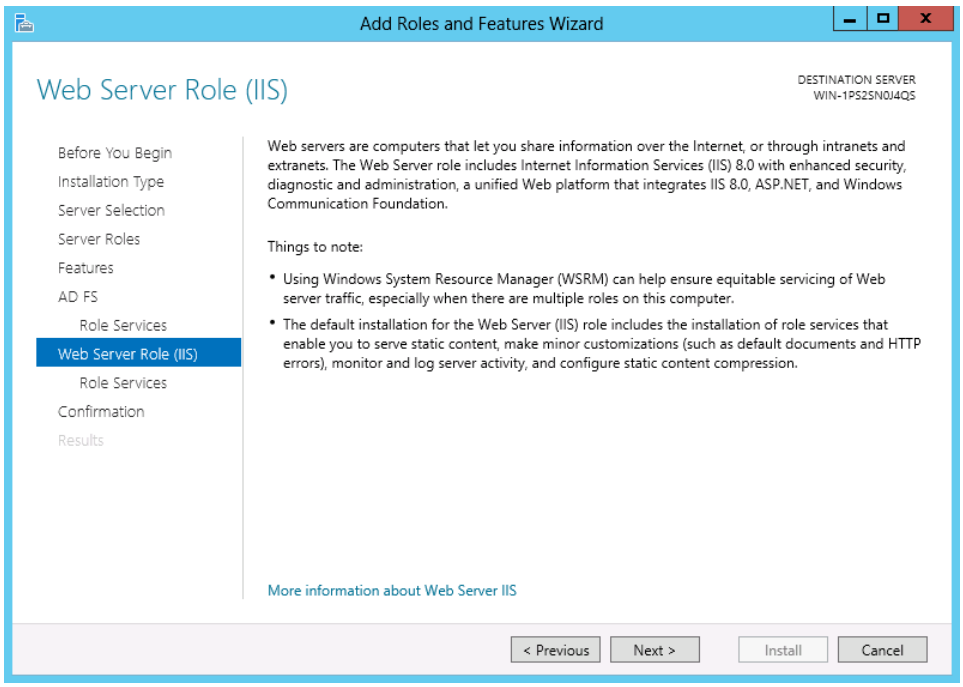
Kies in het Server Manager Dashboard weer voor “Add roles and features” en klik zoals hiervoor beschreven door de eerste schermen en selecteer wederom “Active Directory Federation Services”:



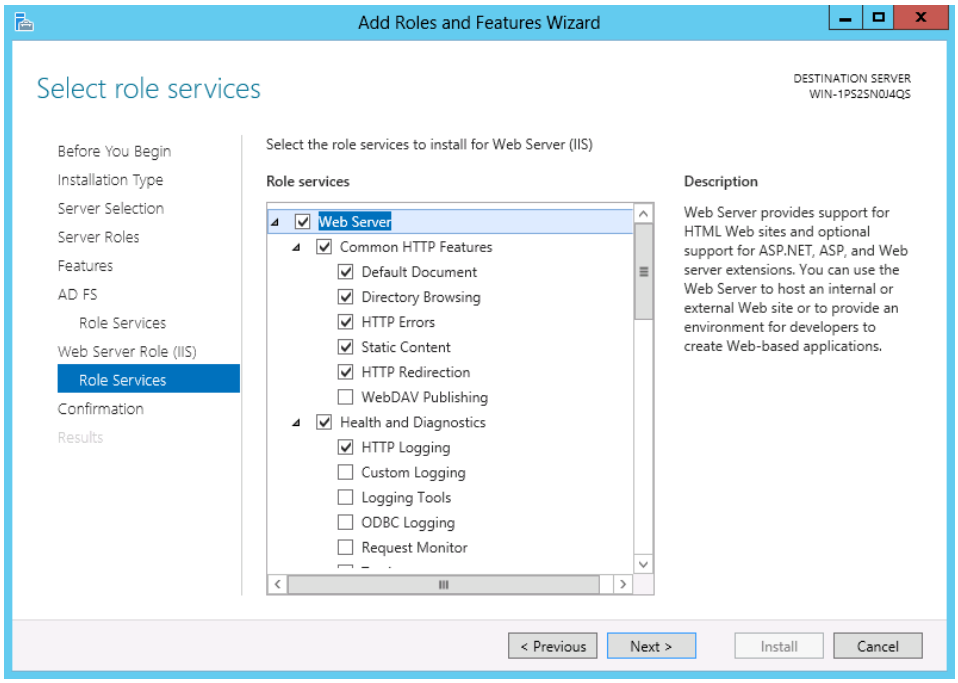
Klik op “Next” tot de AD FS Role services gekozen kunnen worden en selecteer “Federation Service Proxy”:



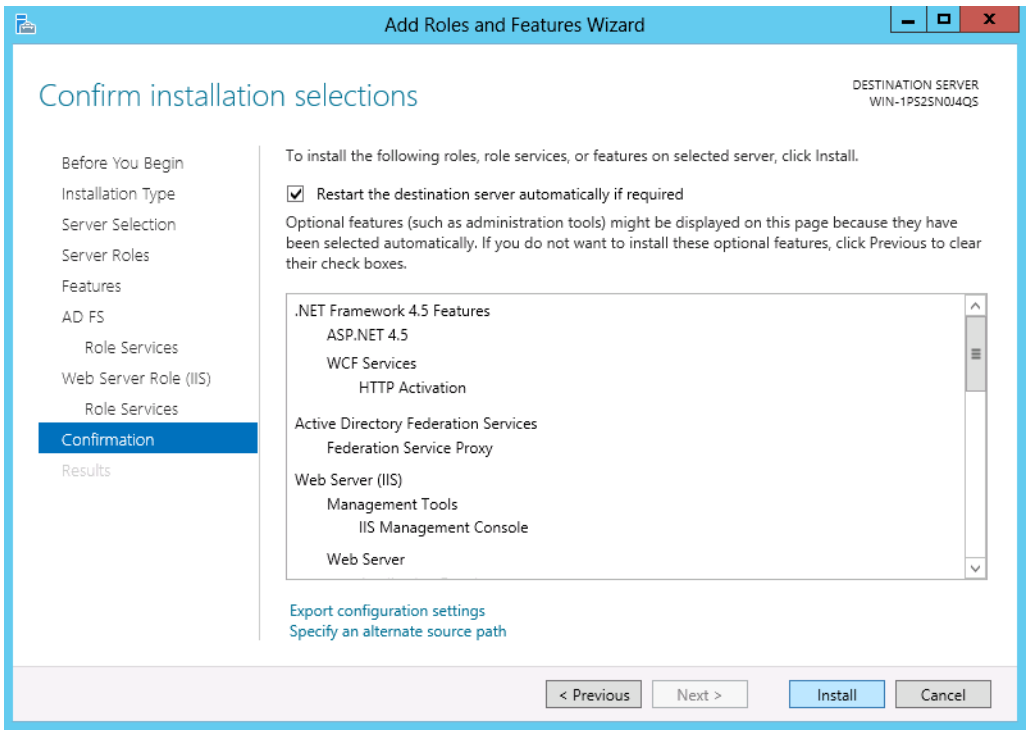
Accepteer de afhankelijkheden door “Add Features” te kiezen en klik op “Next”.



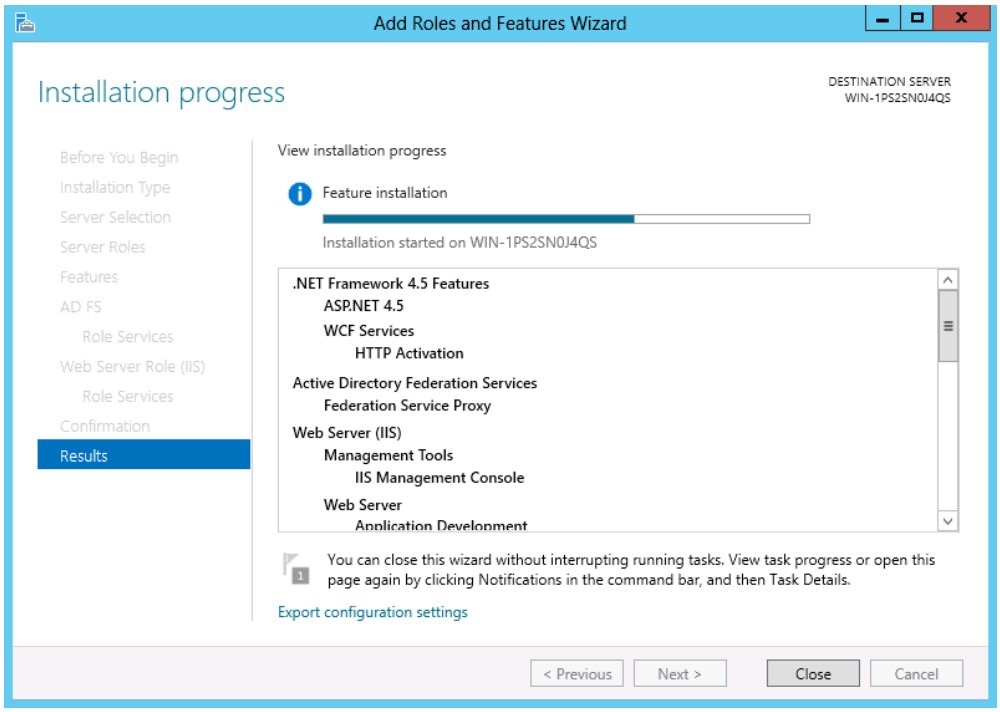
Klik op “Next”.



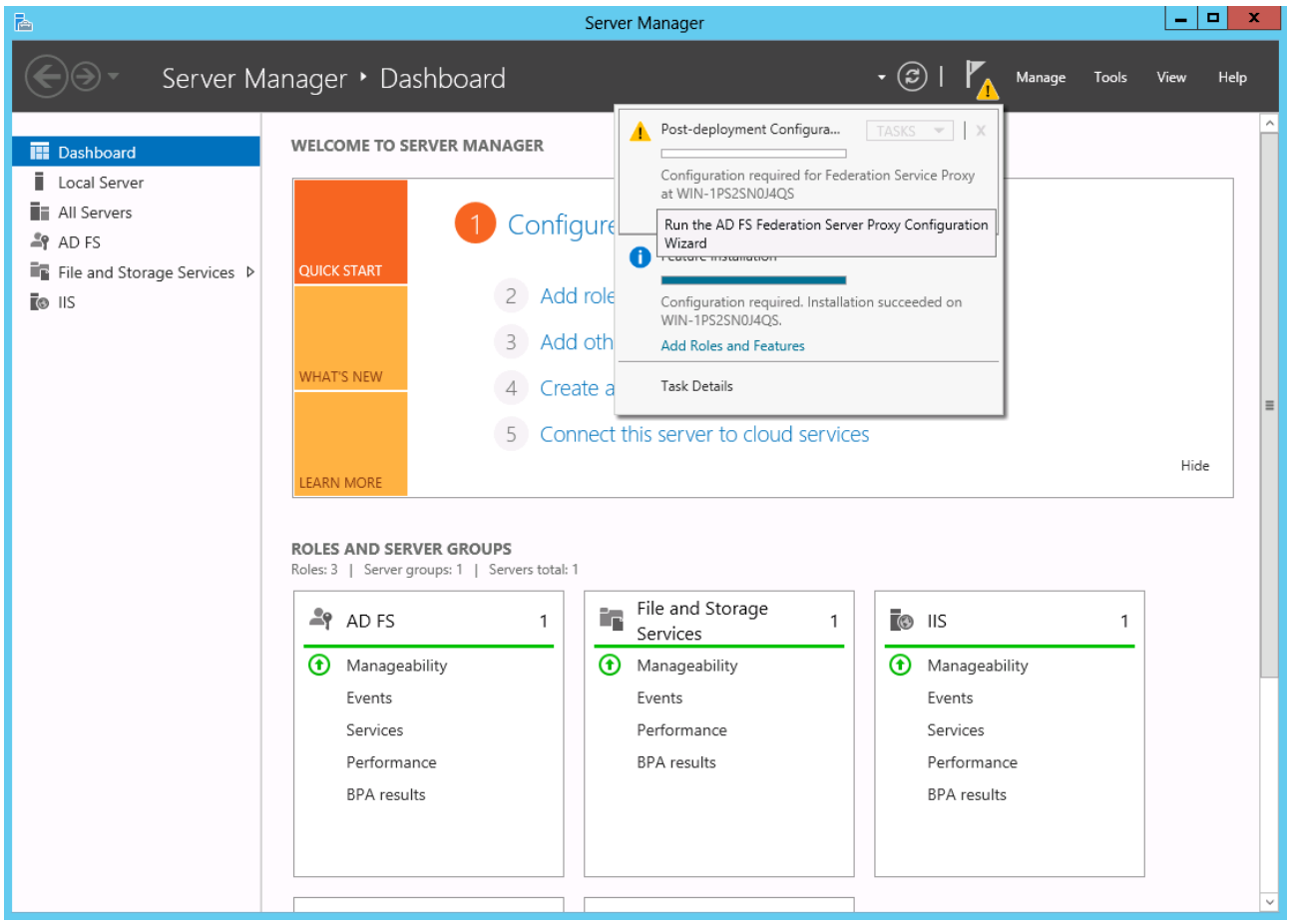
Klik op “Next”.



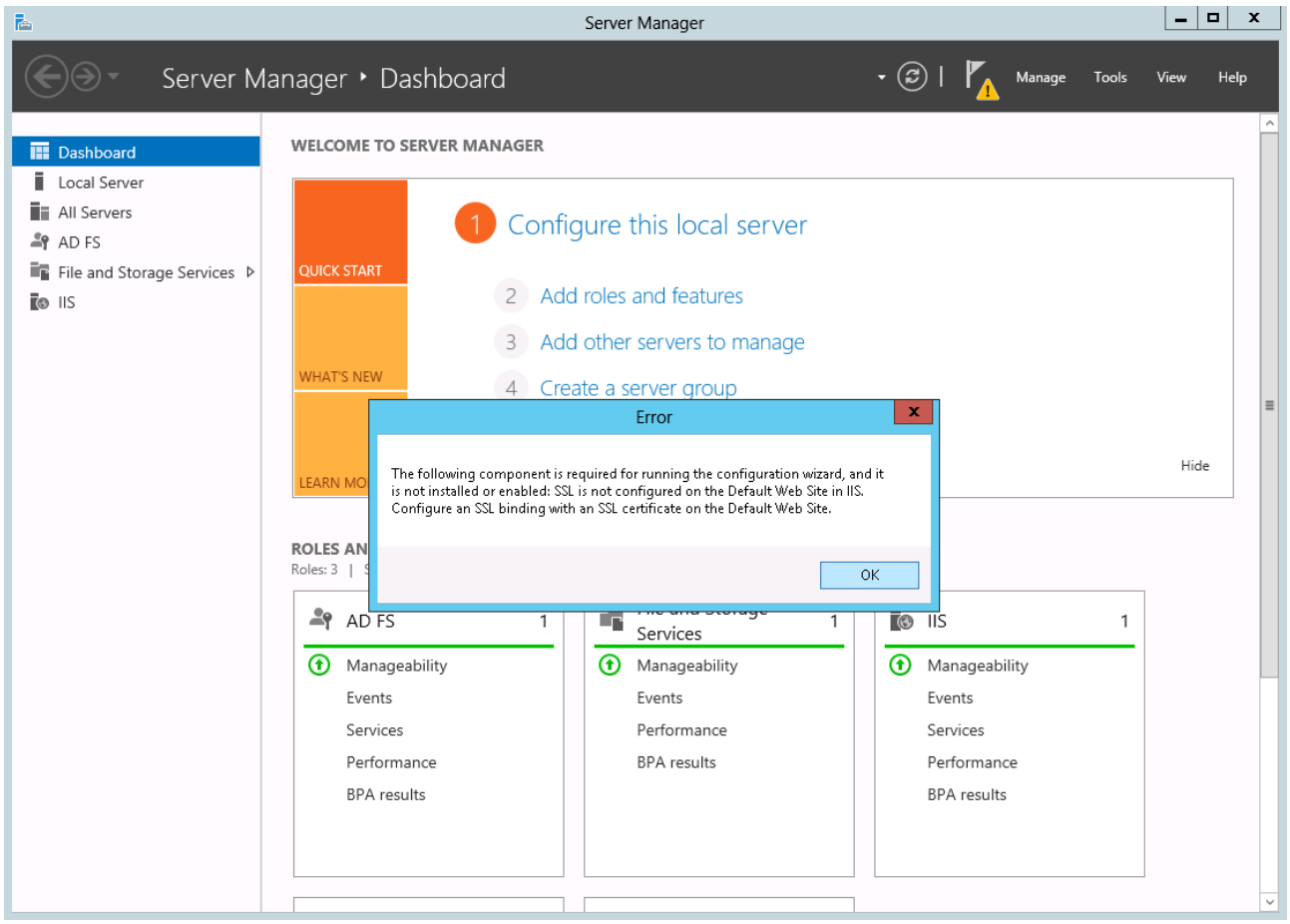
Kies indien gewenst “Restart the destination server automatically if required” en Klik op “Install”.



Wacht eventueel de installatie af en Klik op “Close”.

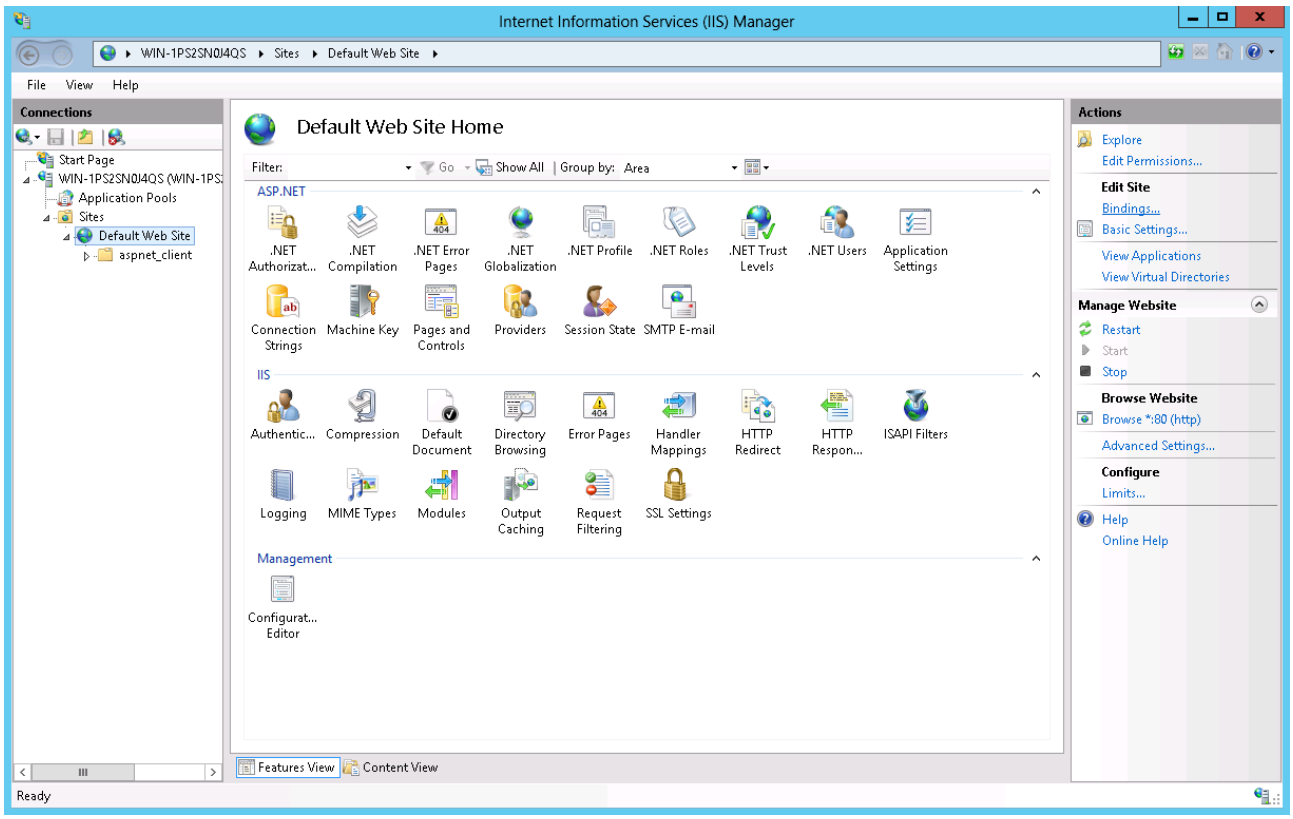


Na installatie verschijnt een Post-deployment alert “Configuration required for the Federation Service Proxy at ...” in het Server Manager Dashboard. Klik op deze link.

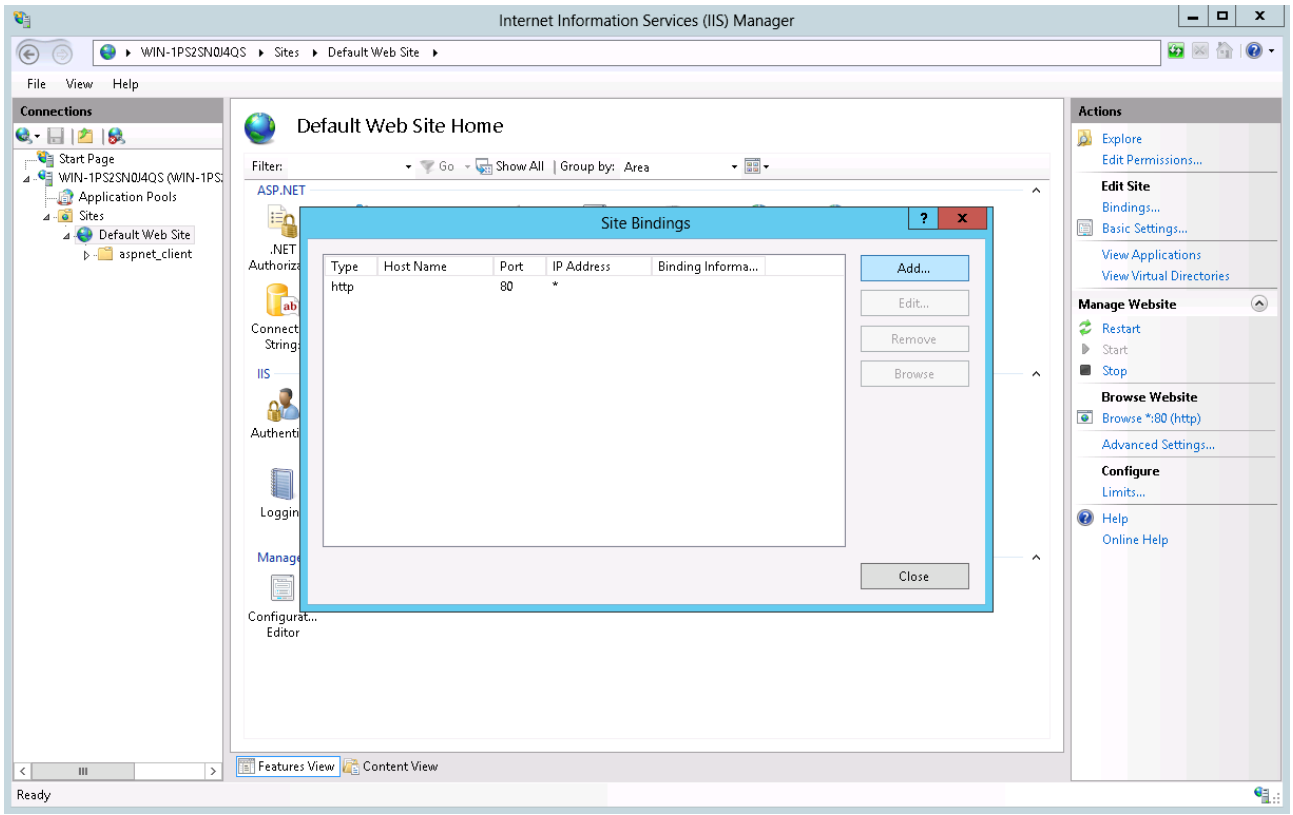


De Proxy configuratie vereist een geldig en werkend SSL certificaat in de zojuist geïnstalleerde IIS omgeving. Installeer hiervoor eerst het SSL certificaat dat ook op de ADFS Server geïnstalleerd is door het daar bijvoorbeeld als .pfx bestand te exporteren. Zie voor de installatie van een SSL certificaat “Appendix A: Certificaat Installeren”.

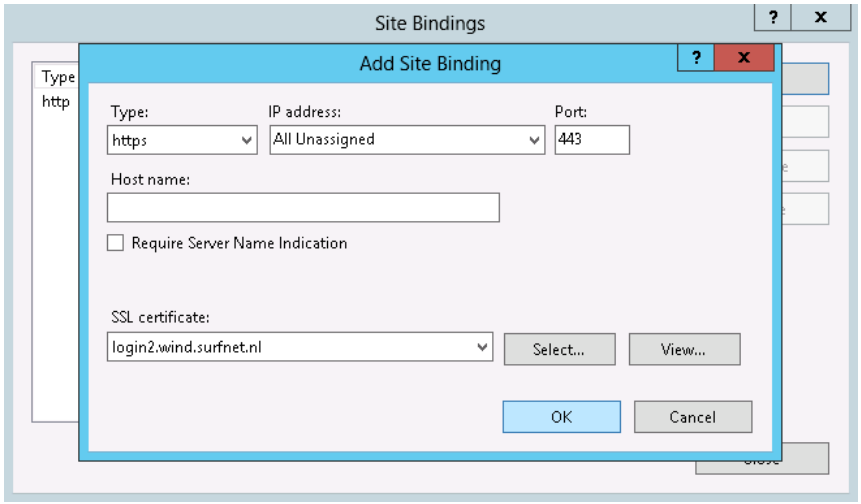
Open vervolgens de IIS manager:



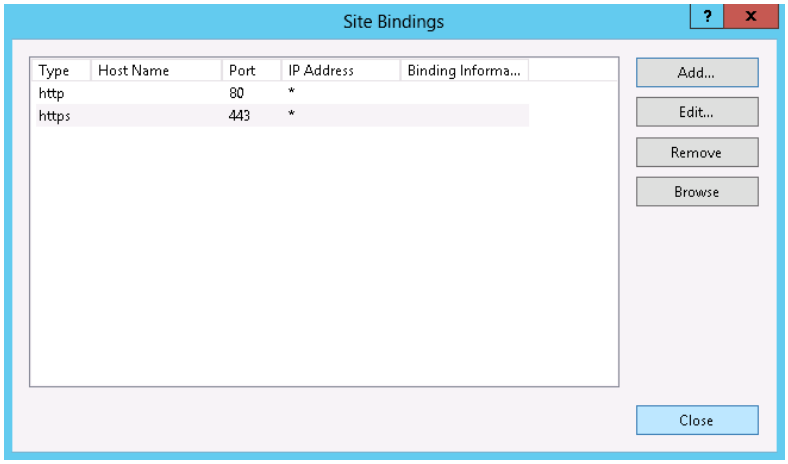
en kies voor de Default Web Site rechts bovenaan “Bindings...” onder “Edit Site”.



Klik op “Add...”

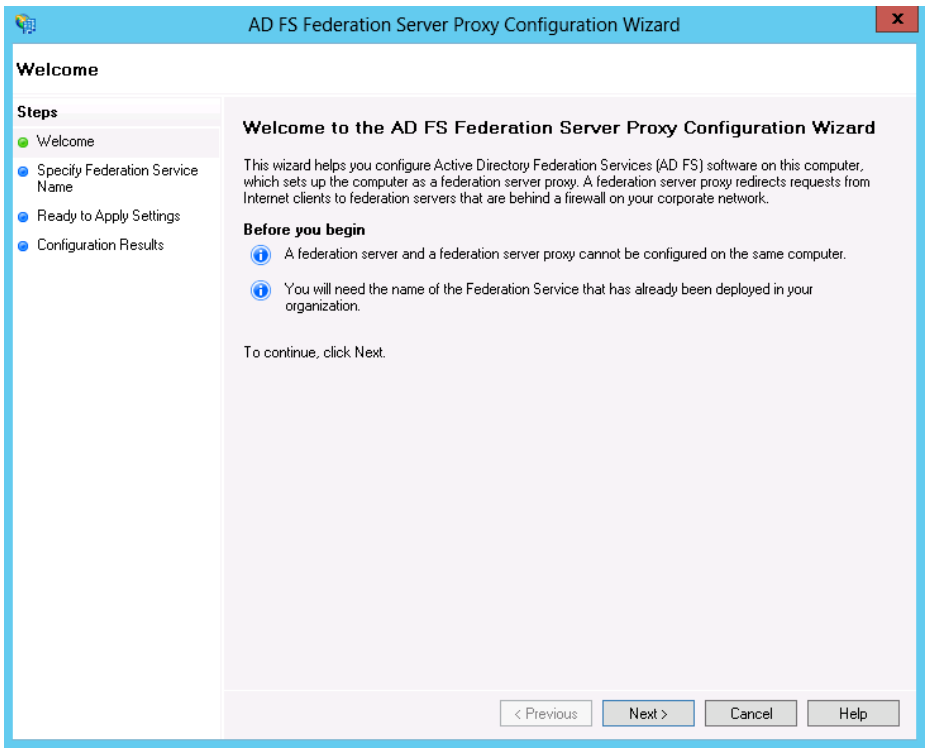


Selecteer Type “https” en selecteer het eerder geïnstalleerde SSL service certificaat en klik op “OK”. De “Site Bindings” configuratie zou er nu als volgt uit moeten zien:

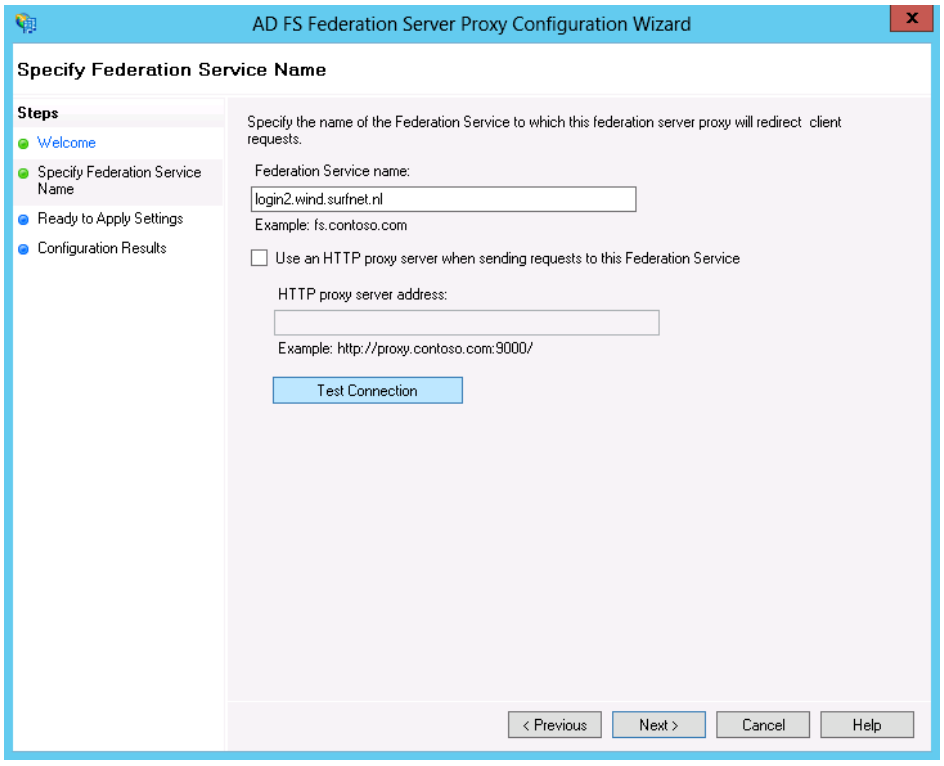


Klik op “Close”.

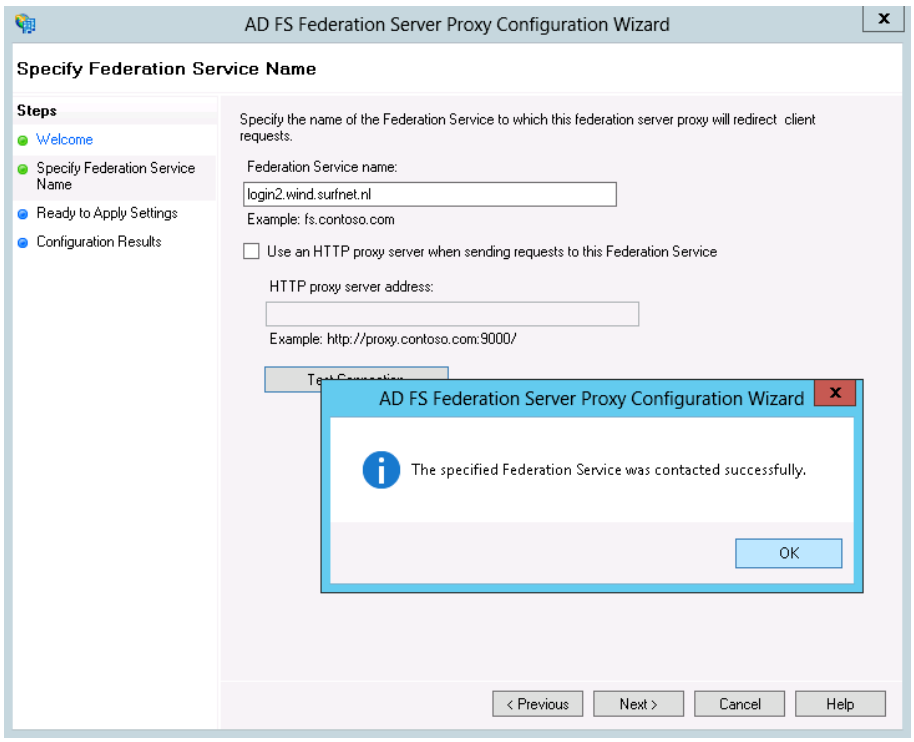
De ADFS Proxy Configuration Wizard kan nu opnieuw gestart worden vanuit het Server Management Dashboard:



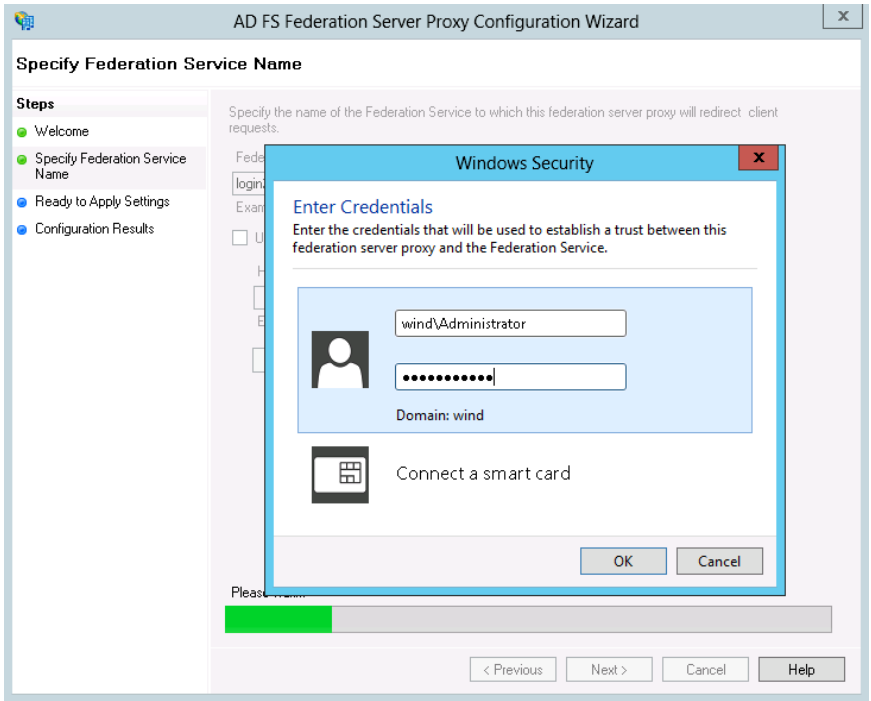
Klik op “Next”.



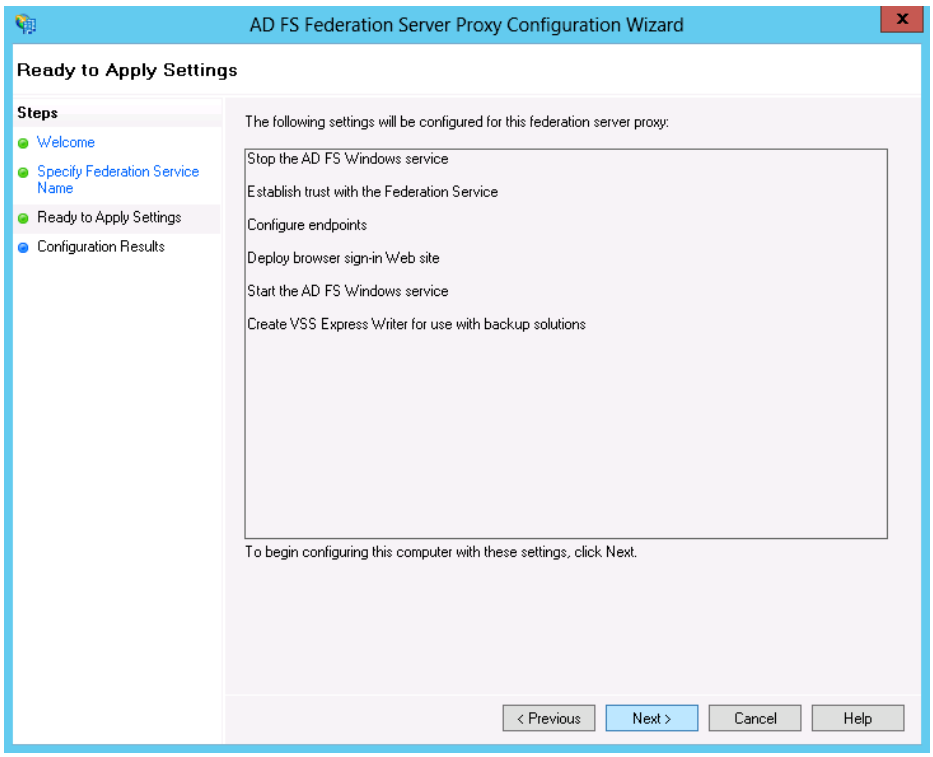
Kies dezelfde DNS naam als de ADFS Server voor “Federation Service Name” en test eventueel de connectie met de ADFS Server door op de knop “Test Connection” te klikken.



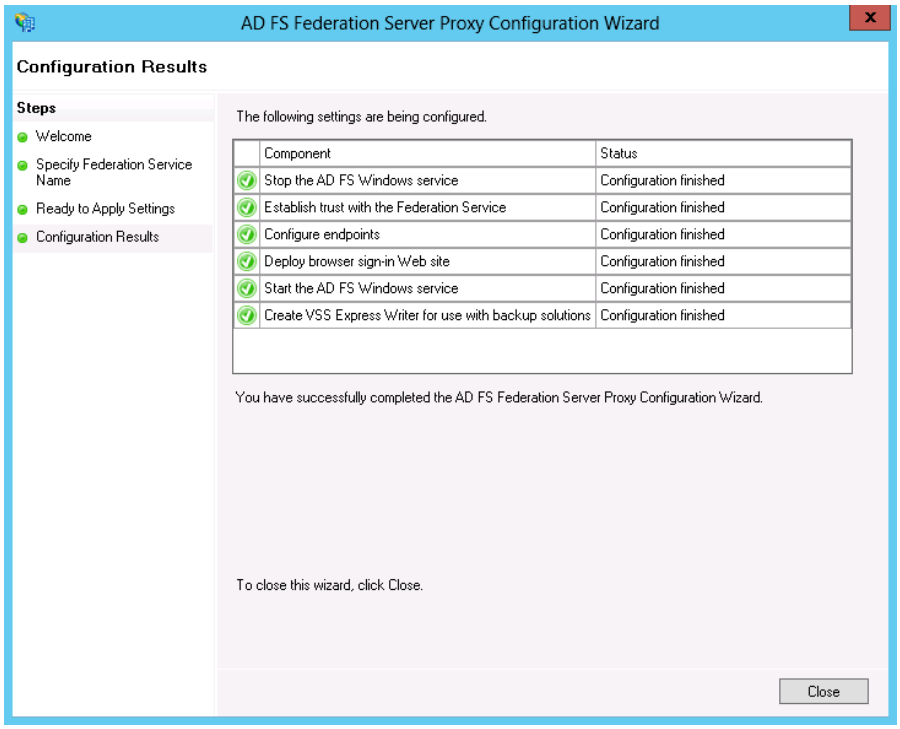
Als deze test slaagt kan “OK” en “Next” gekozen worden.



Voer de gegevens van een domein Administrator in voor het eenmalig opzetten van de trust tussen de Proxy en Server en klik “OK”.



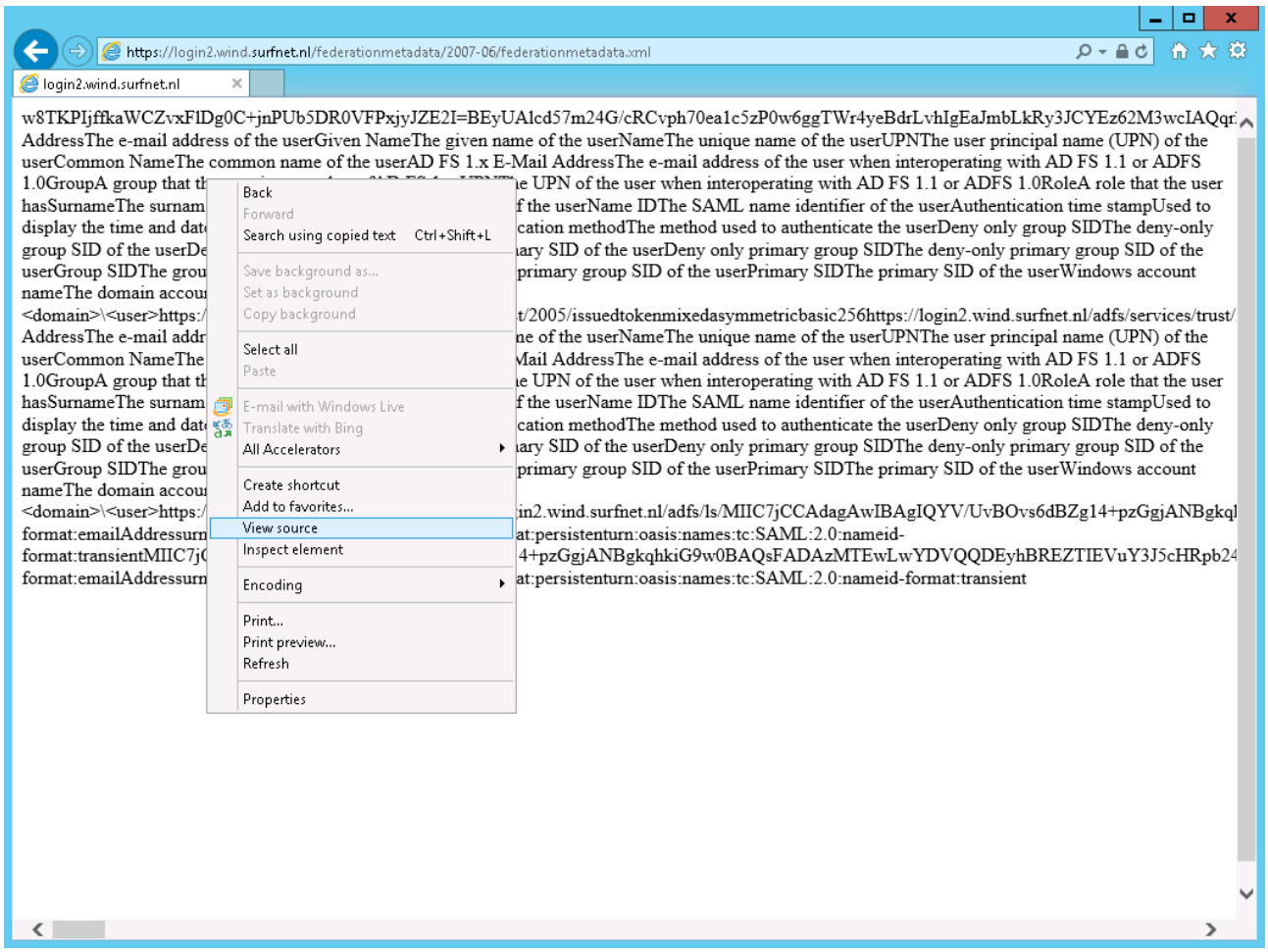
Klik op “Next”.



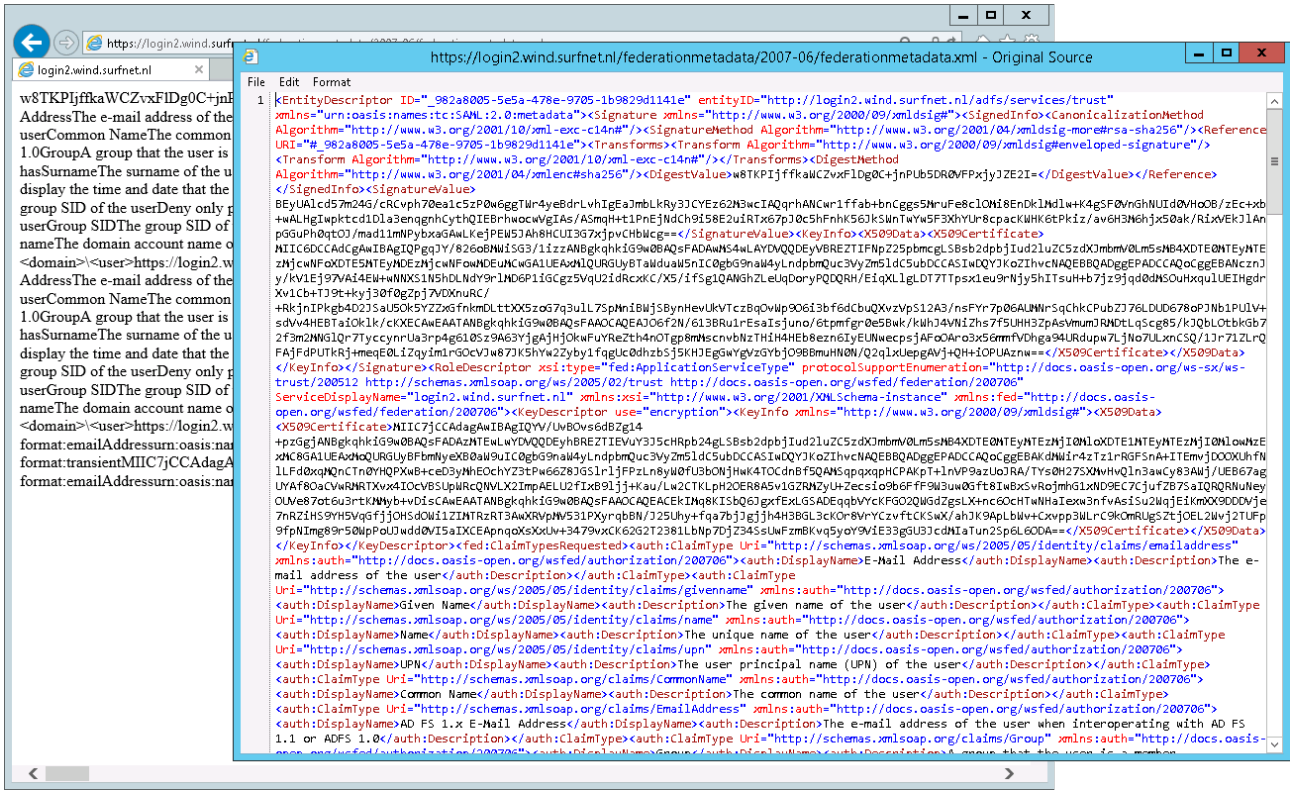
Wacht tot de installatie voltooid is en klik op “Close”.

Surf te controle naar de ADFS service URL (zowel vanuit een plek die op de ADFS Server uitkomt als vanaf een plek die op de Proxy uitkomt) en controleer de inhoud van de volgende URL:

https://<servicenaam>/federationmetadata/2007-06/federationmetadata.xml



Deze URL dient zoals hierboven te zien is een XML document te bevatten. Als de browser geen document laat zien kan met “View Source” het document in een editor getoond worden.



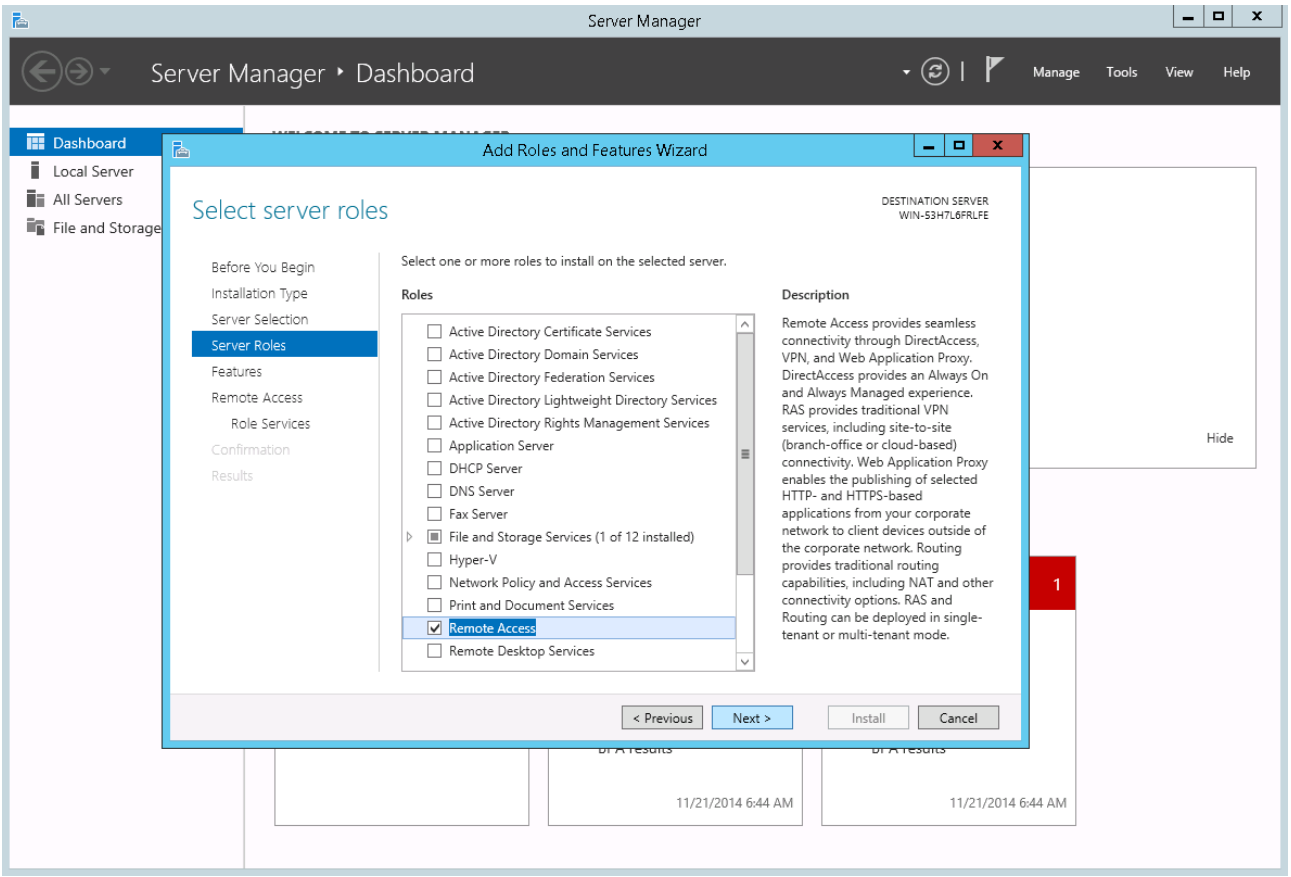
Als deze test slaagt kan de metadata URL aan SURFnet doorgegeven worden zoals beschreven in het hoofdstuk “Metadata doorgeven aan SURFnet”.

Op de ADFS Proxy is deze URL nu nog plaintext (http) beschikbaar. Dit kan geen kwaad, maar kan voor de zekerheid uitgeschakeld worden door de binding van de default site in IIS met poort 80 ongedaan te maken.

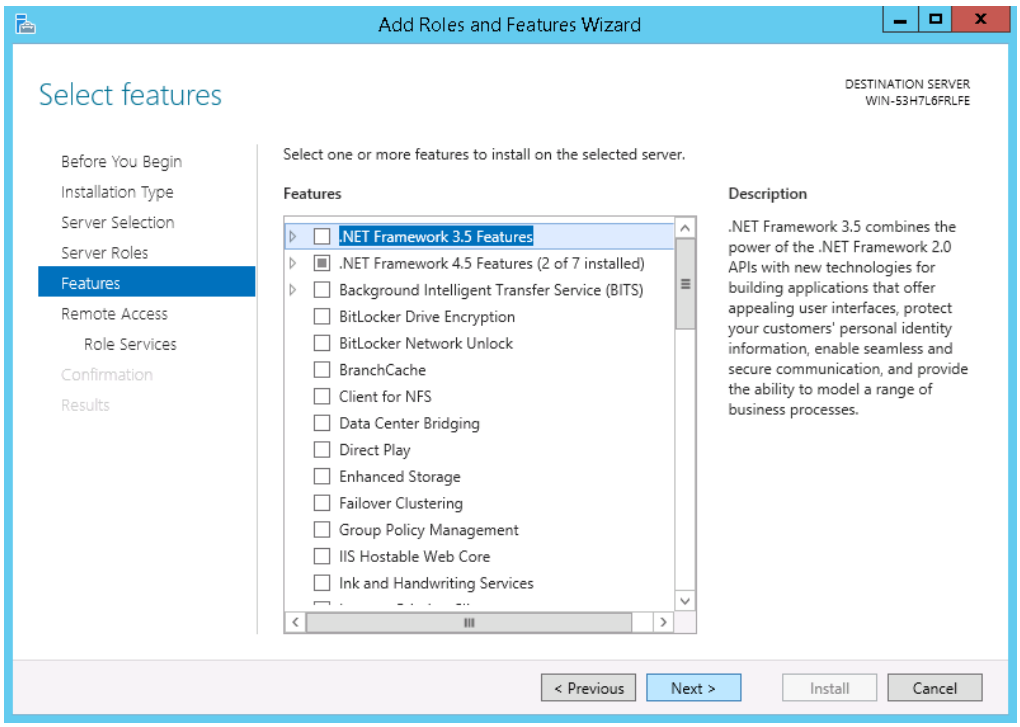
ADFS Proxy installeren onder Windows Server 2012R2

Zorg ervoor dat de Proxy server de ADFS server onder de ADFS service URL kan bereiken zoals beschreven in de inleiding van het ADFS Proxy hoofdstuk. Dit kan met split DNS of een hosts file regel opgelost worden.

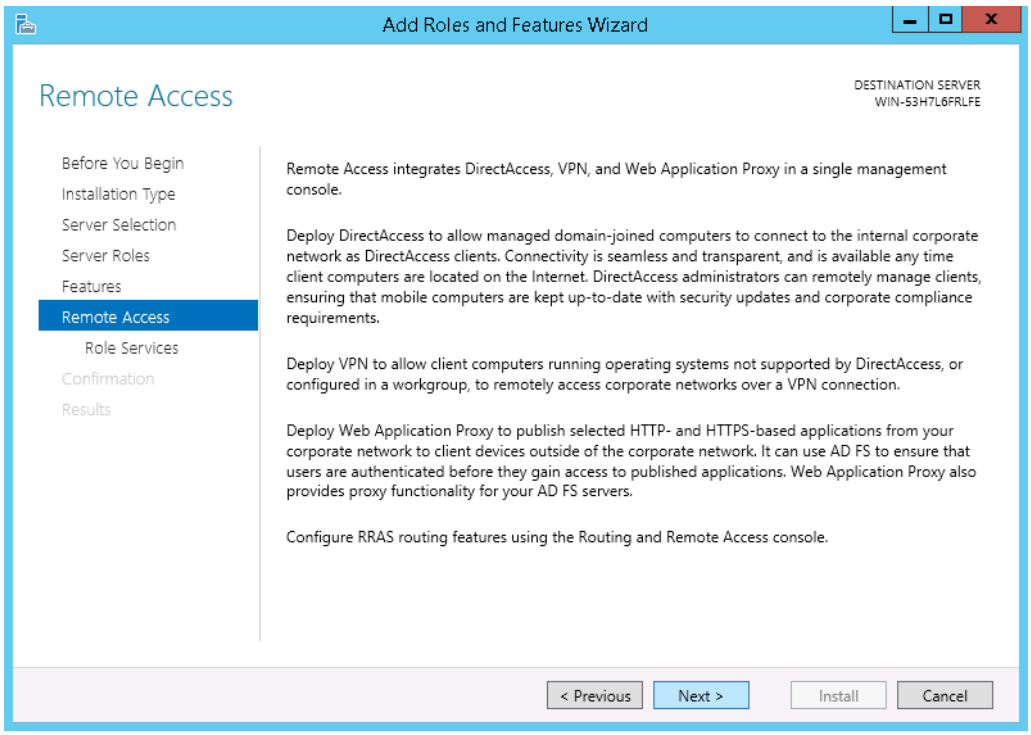
Kies in het Server Management Dashboard voor “Add roles and features” en klik door tot de Server Role “Remote Access” gekozen kan worden:



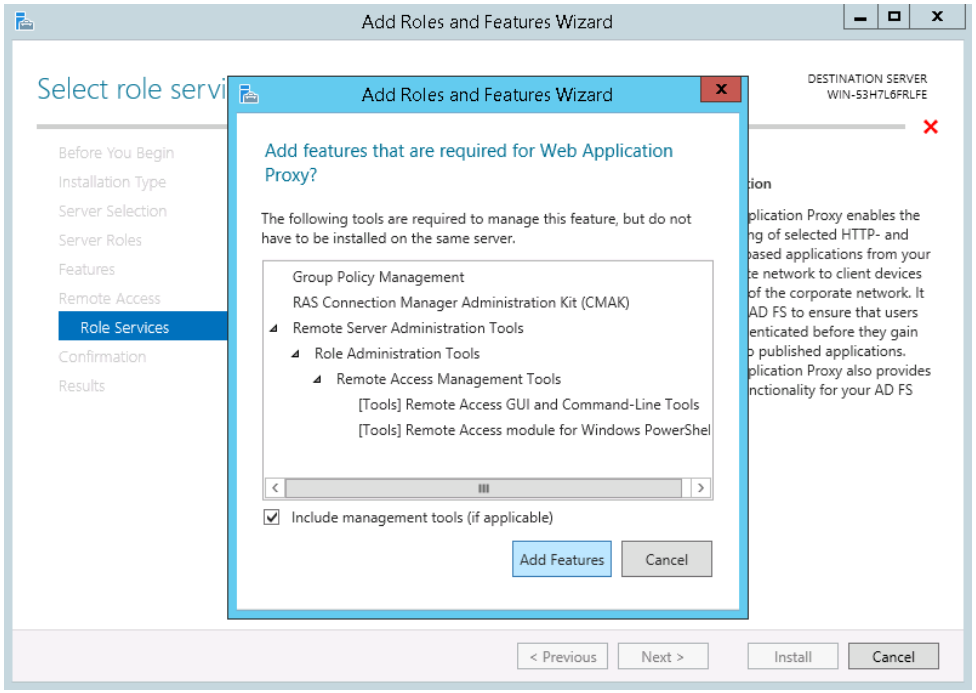
Klik op “Next”.



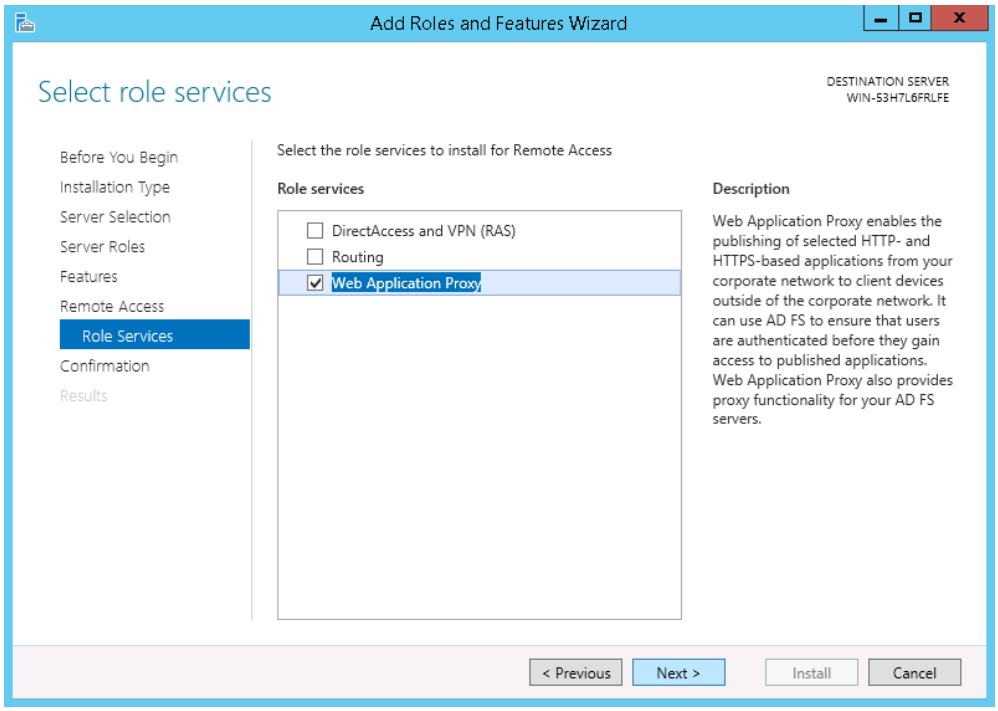
Klik op “Next”.



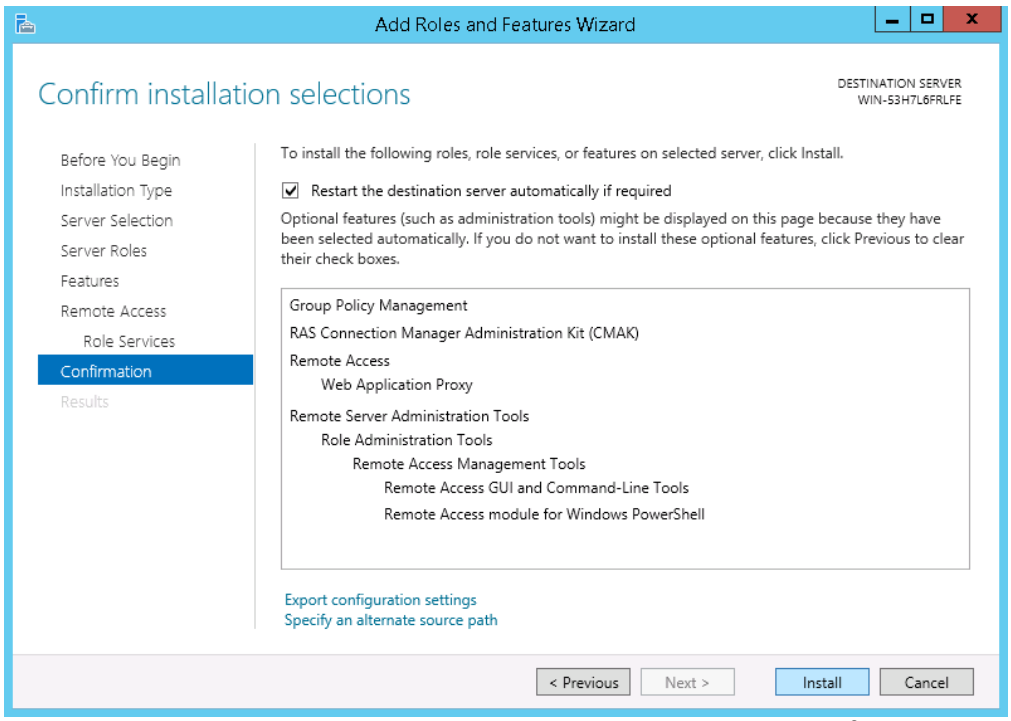
Klik op “Next”.



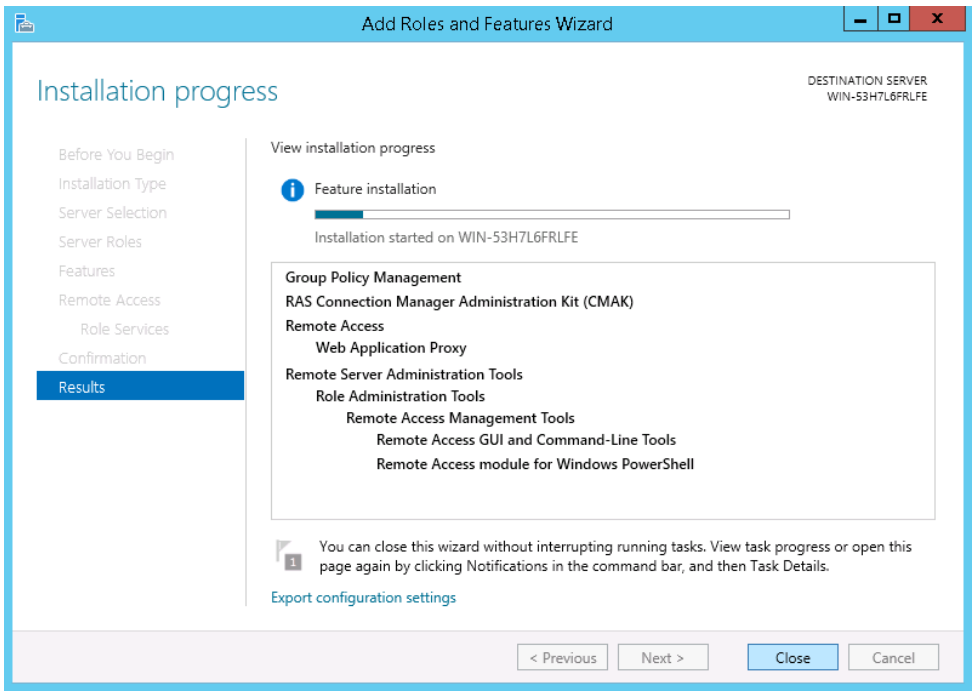
Accepteer de afhankelijkheden door “Add Features” te kiezen en klik op “Next”.



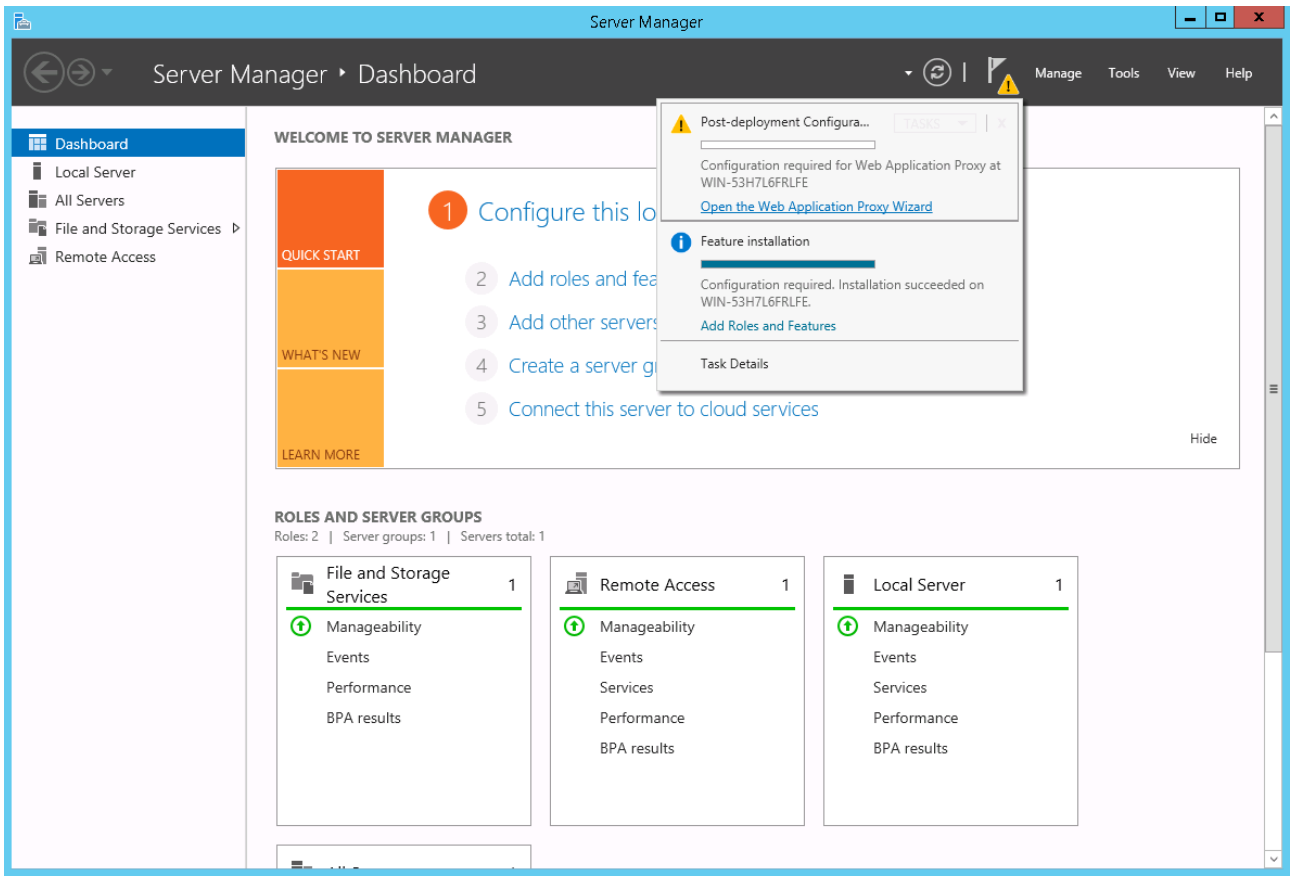
Kies tijdens de Role Services keuze “Web Application Proxy” en klik op “Next”.



Selecteer eventueel “Restart the destination server automatically if required” en klik op “Install”.

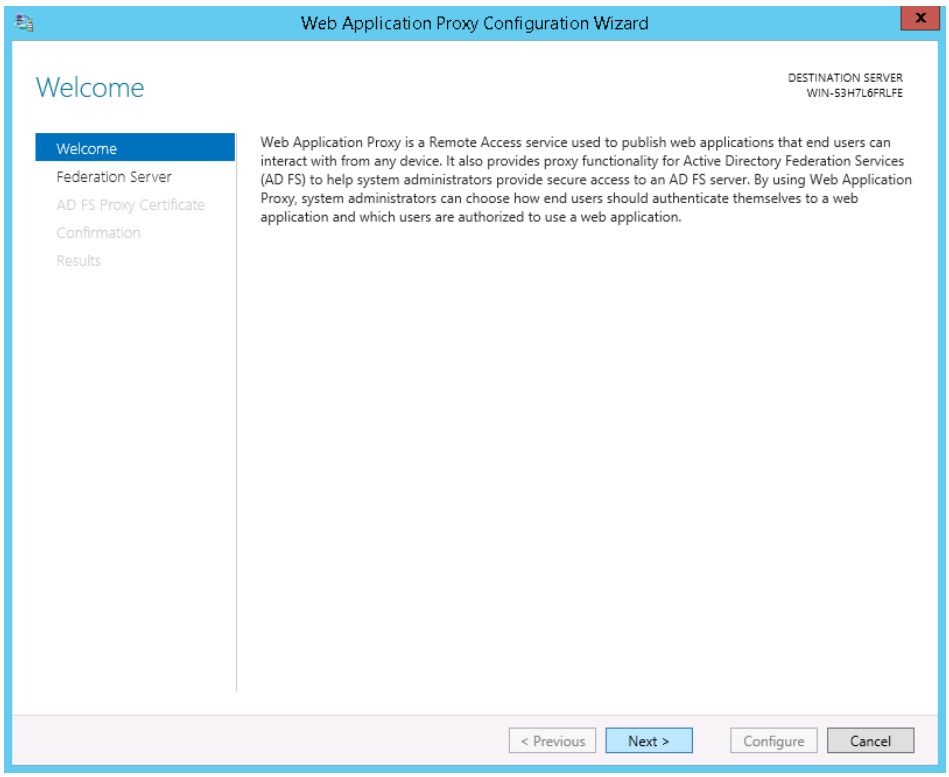


Wacht eventueel de installatie af en klik op “Close”.

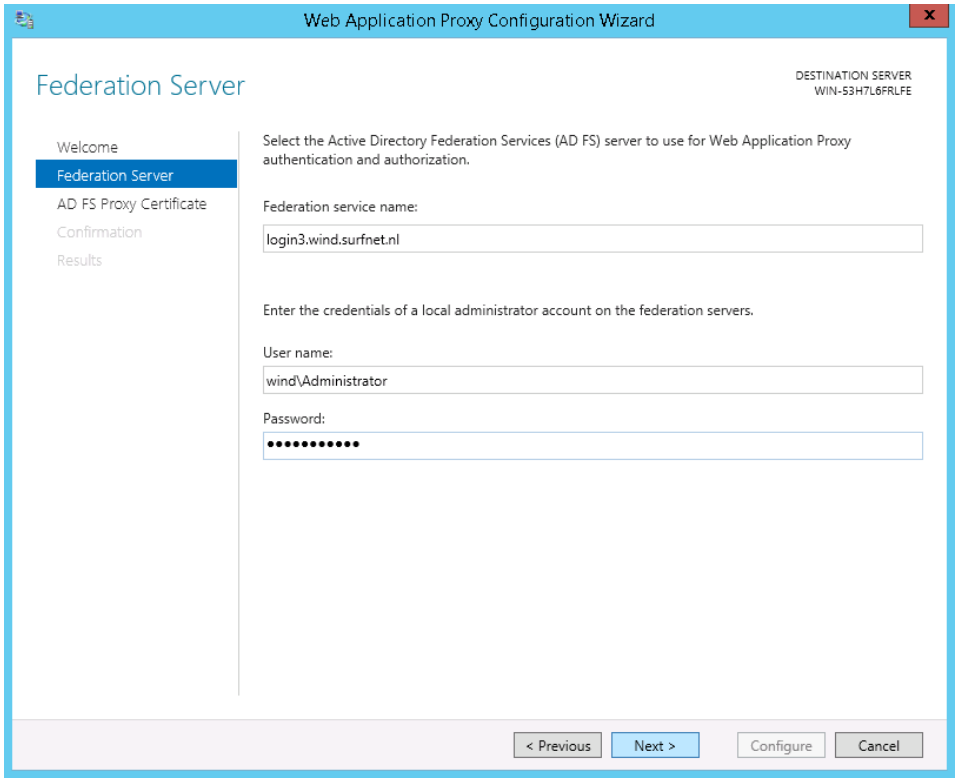


In het Server Manager Dashboard verschijnt weer een “Post-deployment” waarschuwing “Configuration required for Web Application Proxy at ...”. Zorg eerst dat het ADFS Service URL certificaat zoals geïnstalleerd op de ADFS server ook op deze server geïnstalleerd is voordat deze “Post-deployment actie” gekozen wordt. Hoe dit moet staat beschreven in “Appendix A: Certificaat installeren”.

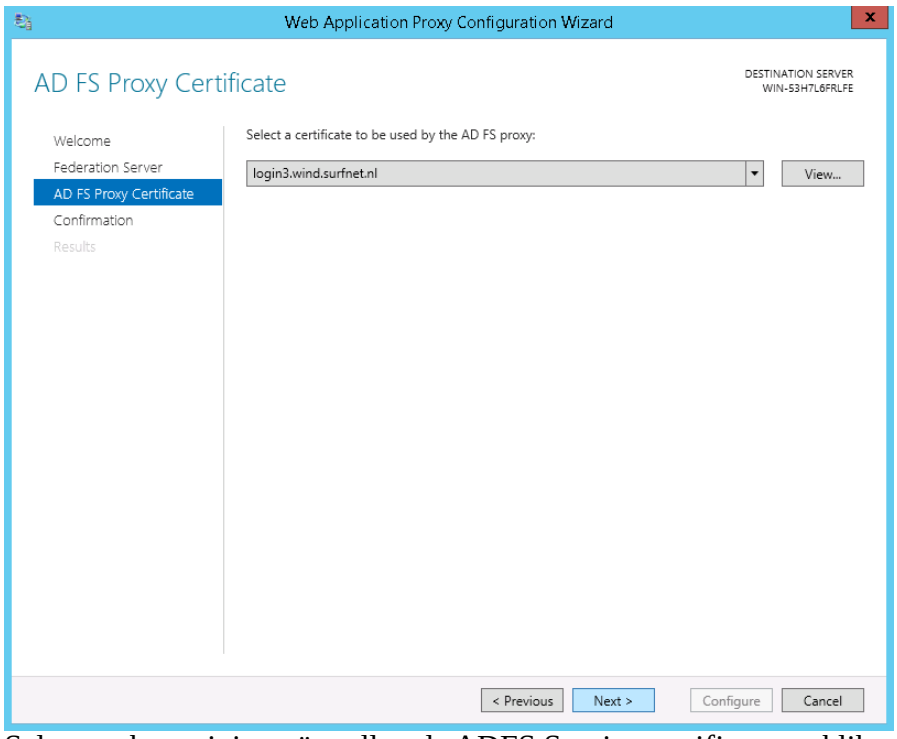
Kies daarna de “Post-deployment” configuratie voor de ADFS Proxy activiteit:



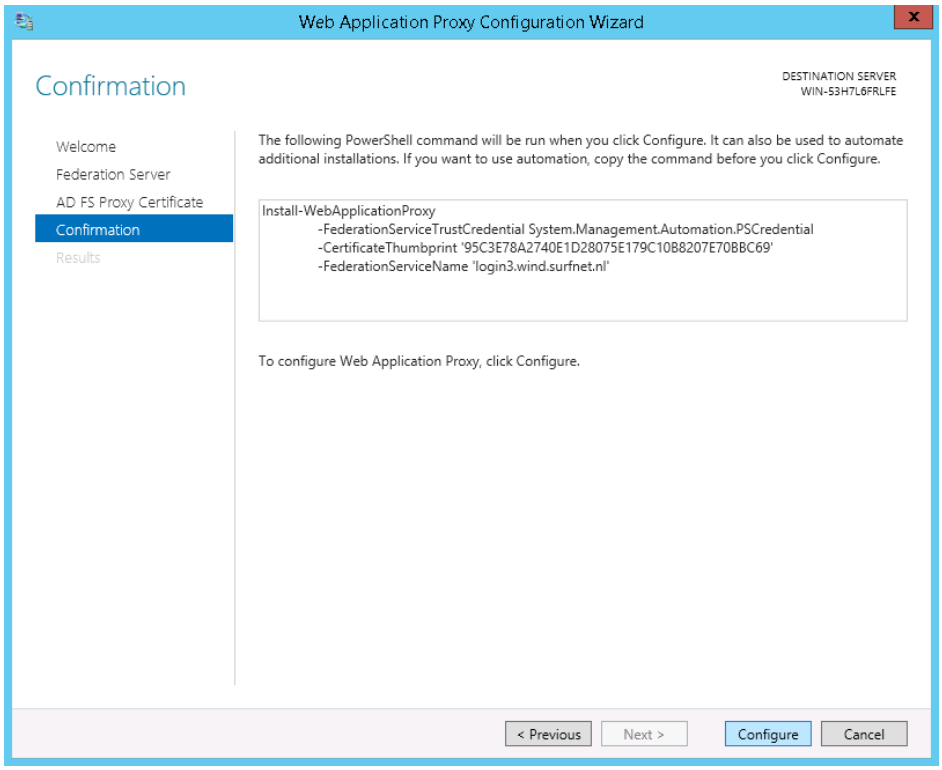
Klik op “Next”.



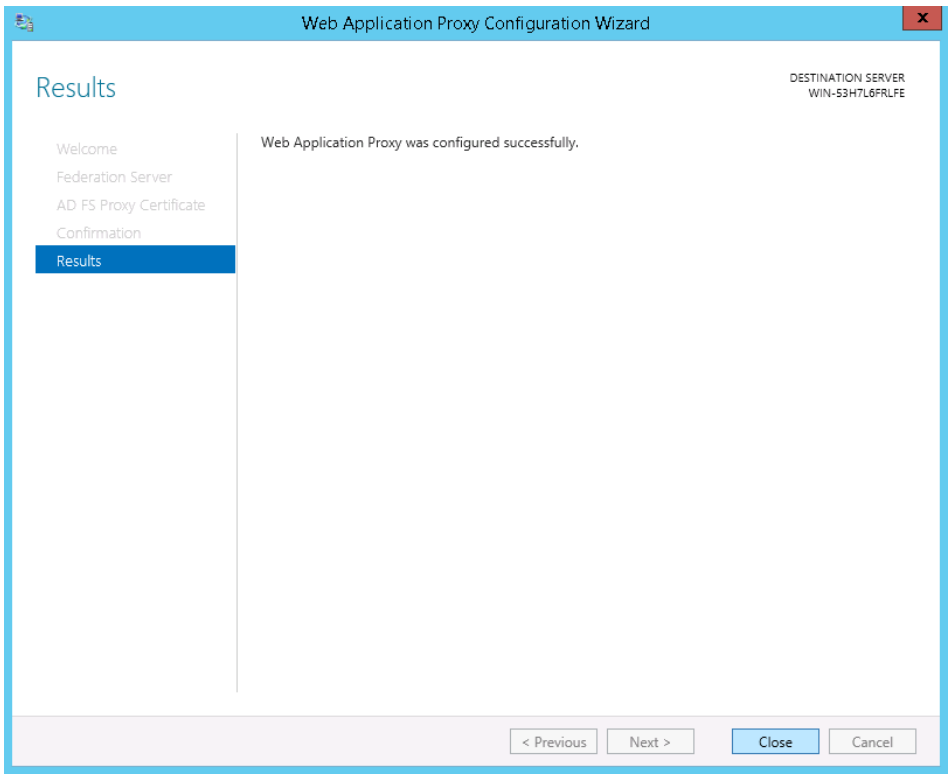
Geef als service naam precies dezelfde service URL als waaronder de ADFS service te bereiken is op en geef de gegevens van de lokale Administrator op. Klik op “Next”.



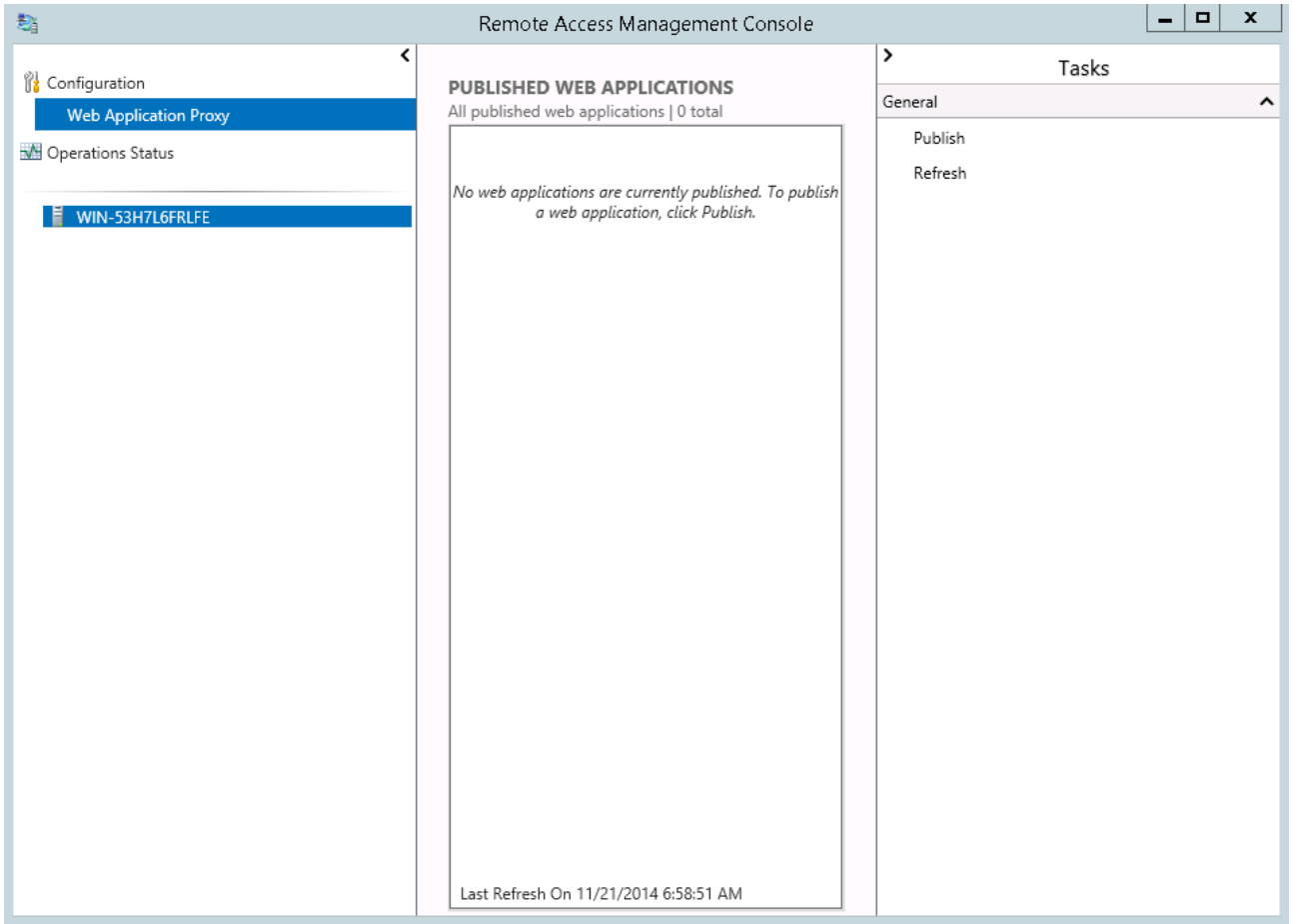
Selecteer het zojuist geïnstalleerde ADFS Service certificaat en klik op “Next”.



Klik op “Configure”.



Wacht het configuratieproces af en klik op “Close”.



Een correct geconfigureerde ADFS proxy ziet er nu in het “Remote Access Management Console” als hierboven uit.

Metadata doorgeven aan SURFnet

Als de ADFS server en ADFS Proxy of Web Application Proxy geïnstalleerd zijn en hun werking gecontroleerd kan de metadata URL doorgeven worden aan SURFnet. Om er voor te zorgen dat de metadata voor de Identity Provider langer houdbaar is verlengen we de duur van het Token Signing certificaat op de ADFS server eerst even door in een Powershell de volgende commando's uit te voeren:

```
Set-ADFSProperties -CertificateDuration 1825
```

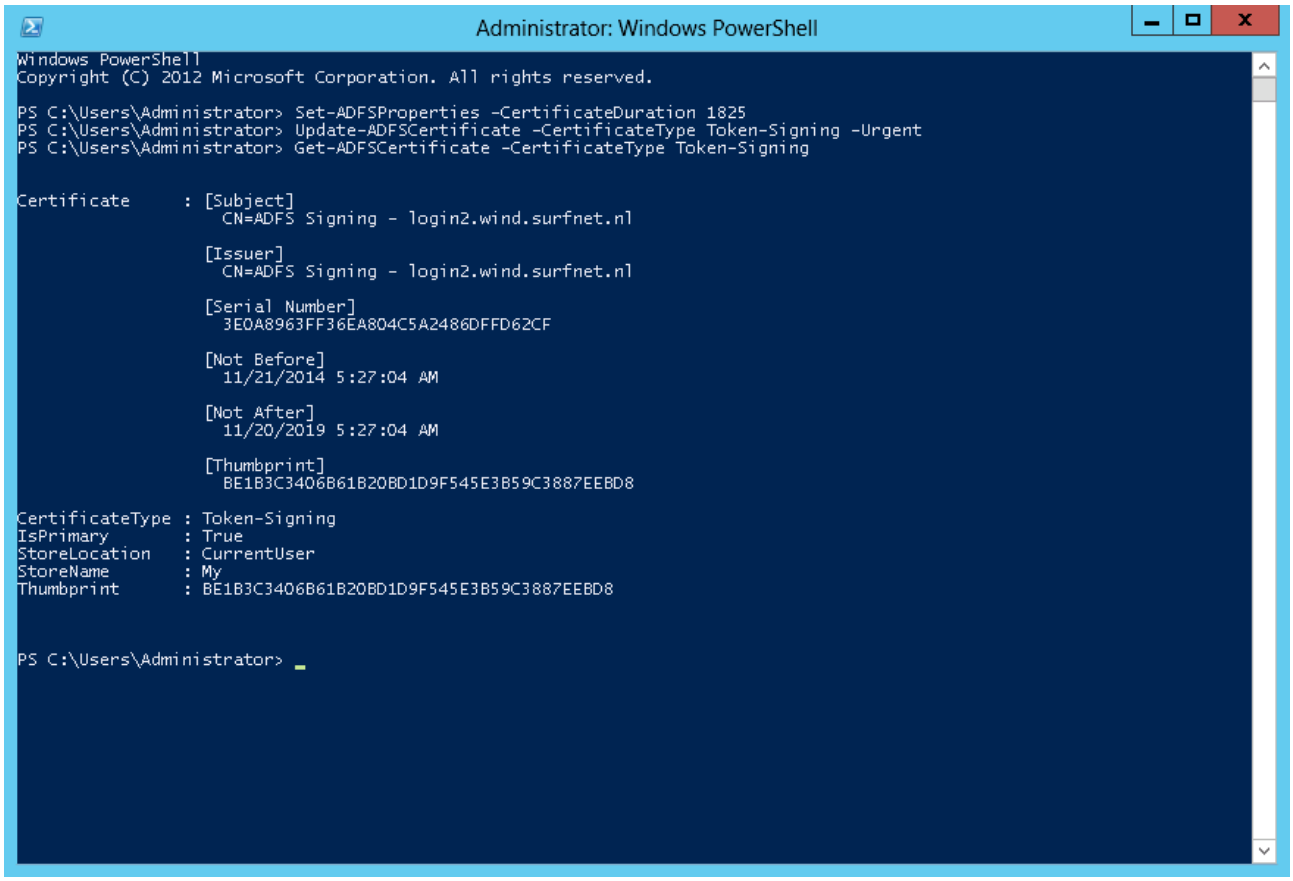
Als er nog geen andere Relying Party Trusts configuraties bestonden voor deze installatie:

```
Update-ADFSCertificate -CertificateType Token-Signing -Urgent
```

(deze worden namelijk onbruikbaar door het uitvoeren van bovenstaande commando)

en ter controle:

```
Get-ADFSCertificate -CertificateType Token-Signing
```



Het Token-Signing certificaat is nu als het goed is vijf jaar geldig.

Aanleveren Metadata

Vervolgens kan een mail naar SURFconext gestuurd worden met daarin de volgende informatie:

- Metadata URL: https://<servicenaam>/federationmetadata/2007-06/federationmetadata.xml

En alle onder deze URL genoemde extra gegevens:
https://wiki.surfnet.nl/display/surfconextdev/Vereiste+metadata

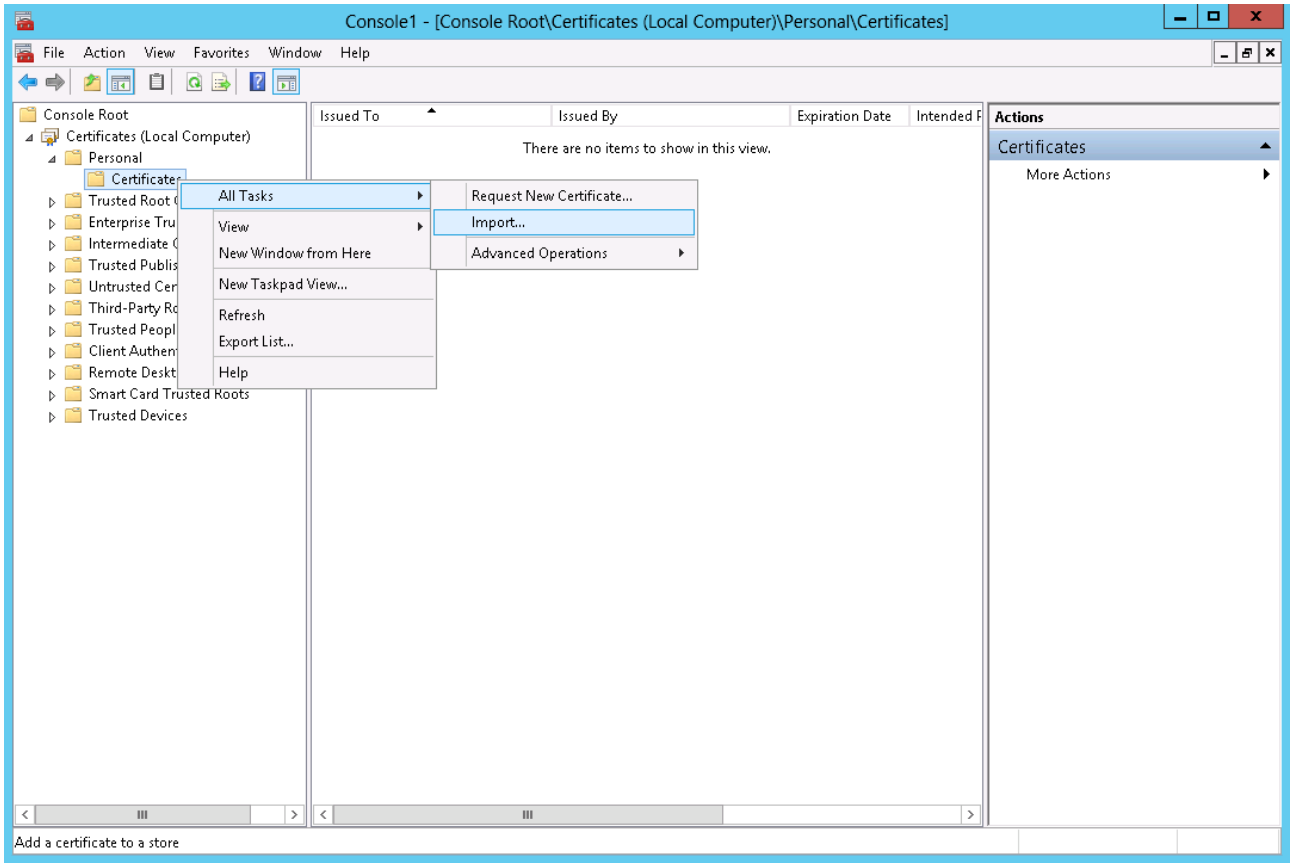
Appendix A Certificaat installeren

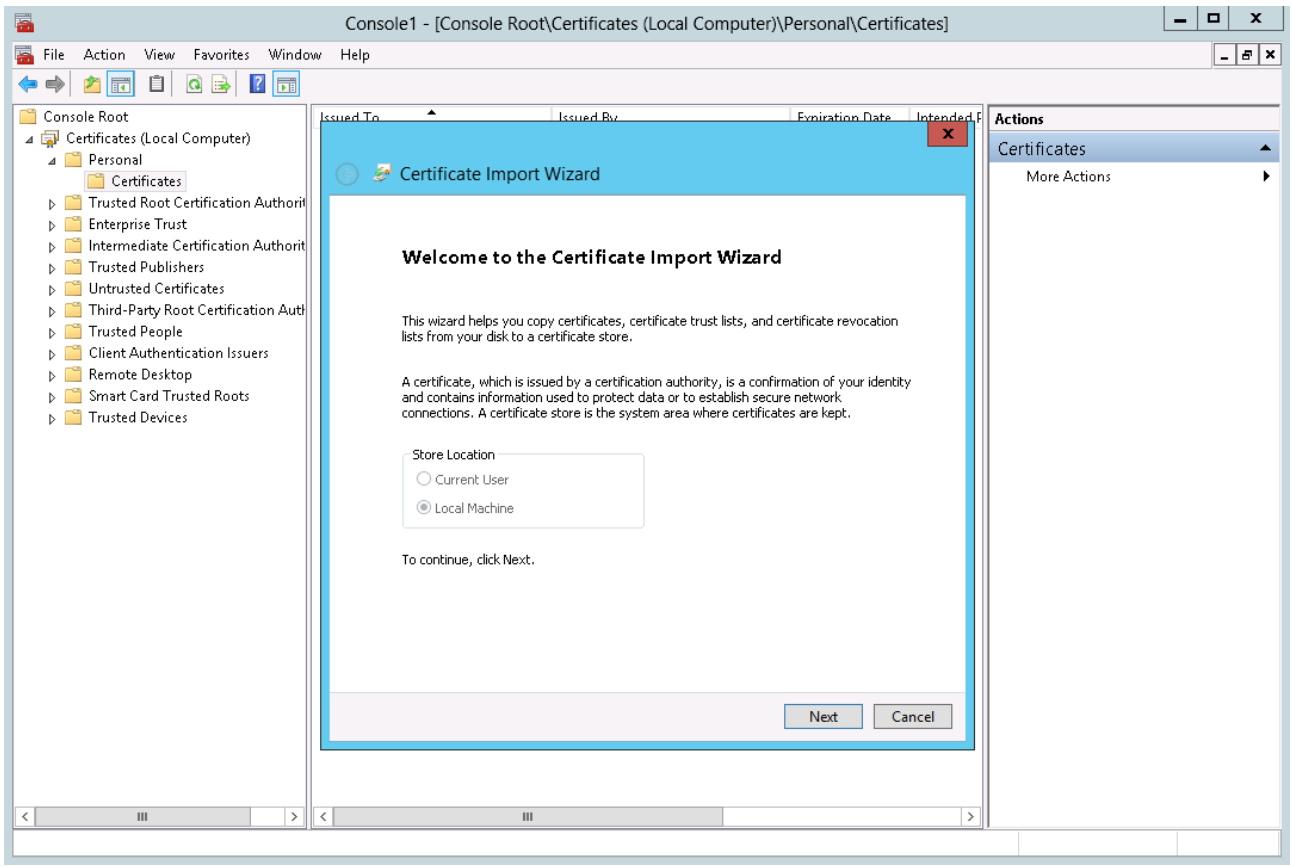
Deze handleiding gaat er vanuit dat het certificaat plus private key beschikbaar is in de vorm van een .pfx bestand. Als het certificaat en de private key alleen los beschikbaar zijn als respectievelijk *cert.pem* en *cert.key* met certificate chain *chain.pem*, is daar met het volgende openssl commando een *cert.pfx* bestand van te maken:

```
#openssl pkcs12 -export -passout pass:123welkom -in cert.pem -certfile chain.pem
-inkey cert.key -out cert.pfx
```

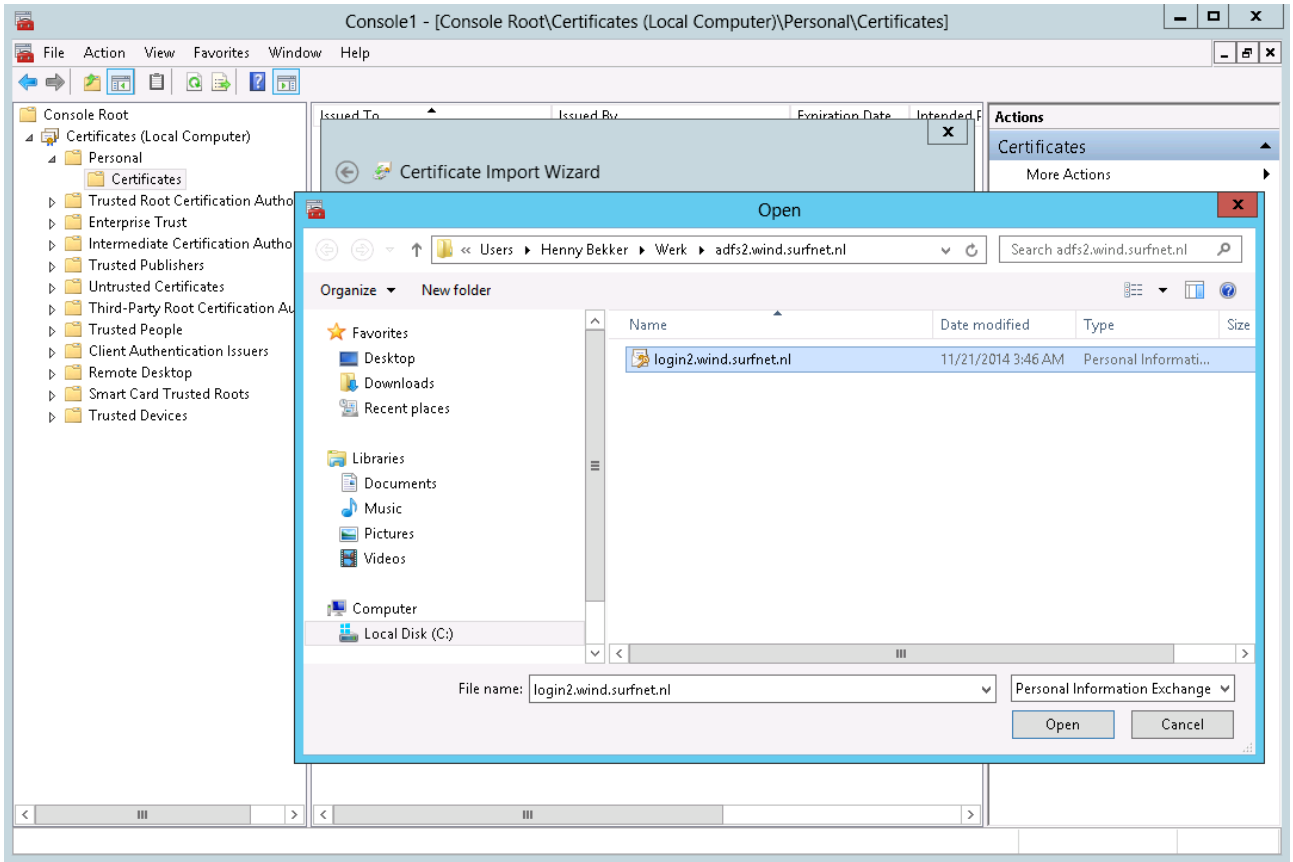
Het cert.pfx bestand heeft nu als voorbeeld wachtwoord *123welkom*.

Open de MMC en voeg de cerrtificate manager Snap-in voor Local Computer toe. Selecteer de Personal Certificate Store en kies Import... zoals hieronder laat zien.

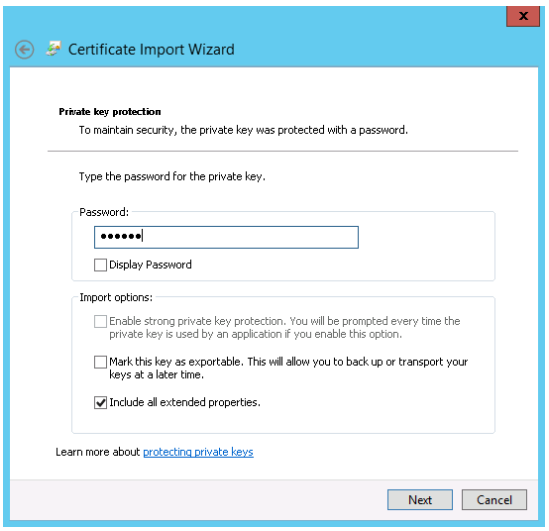




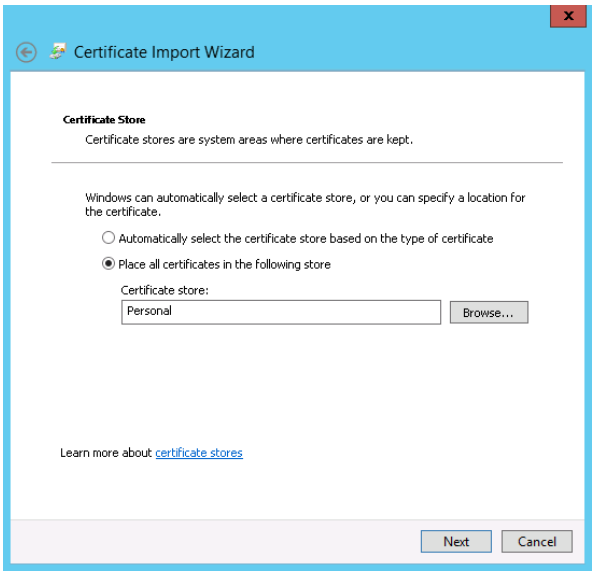
Klik op next.



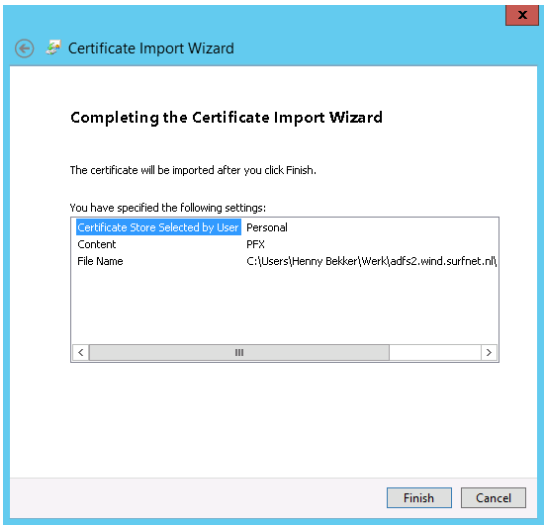
Zoek het bestand waarin het certificaat inclusief private key staat (meestal een pfx bestand) en klik op “Open”.



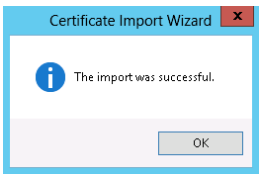
Geef het wachtwoord waarmee de pfx opgeslagen is en klik op “Next”.



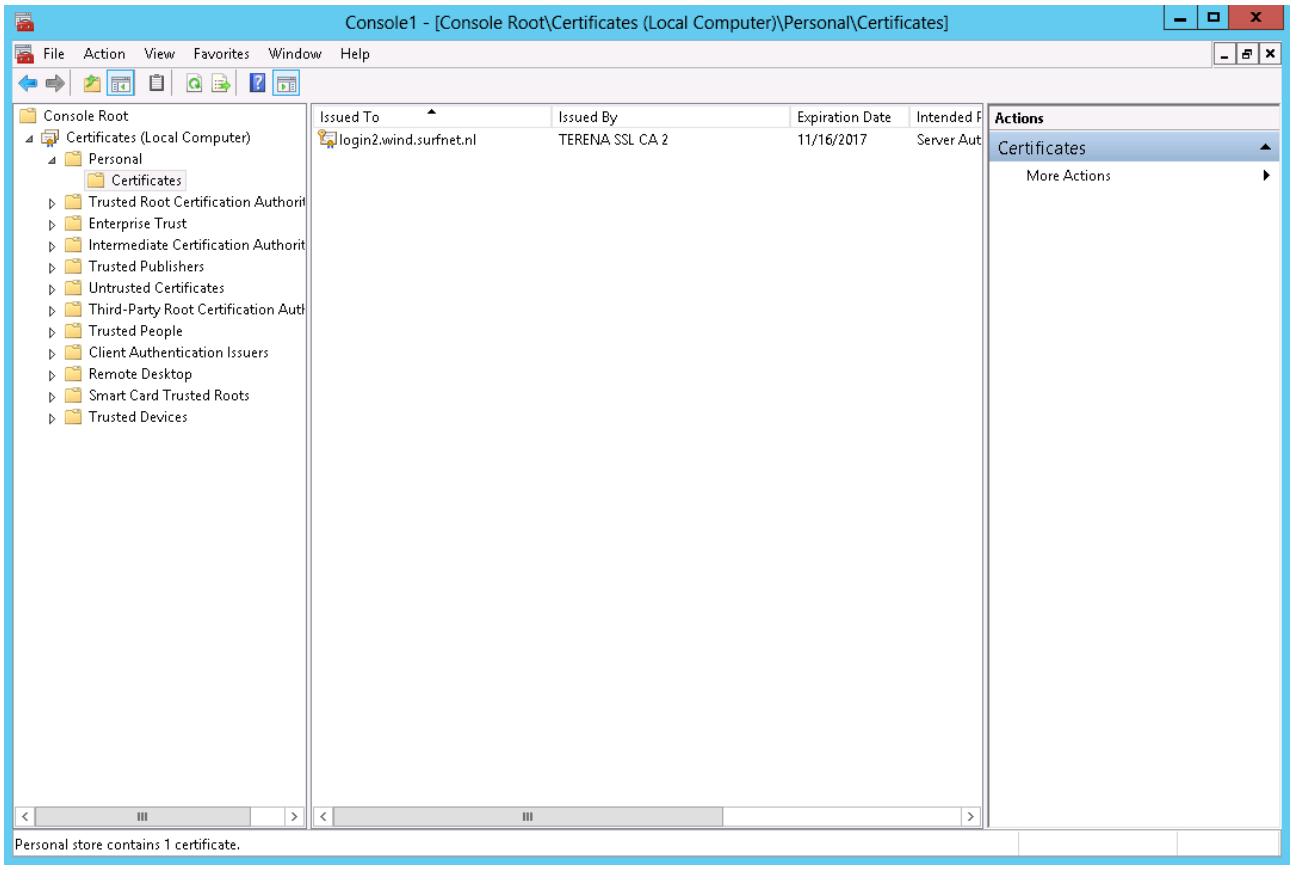
Kies de Personal store en klik op “Next”.



Klik op “Finish”.



Klik op “OK”.



Controleer of het certificaat, inclusief private key, correct geïmporteerd is. Aanwezigheid van de private key is te herkennen aan het sleuteltje linksboven het icoontje van het certificaat.

Verklarende woordenlijst

DMZ

DMZ staat voor Demilitarized Zone en is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. Het externe netwerk is meestal het internet.
Een DMZ is feitelijk een andere naam voor een extranet, een gedeelte van het netwerk dat voor de buitenwereld volledig toegankelijk is.
Op het netwerksegment van de DMZ zijn meestal servers aangesloten die diensten verlenen die vanuit het interne en externe netwerk aangevraagd kunnen worden (bijvoorbeeld een webserver en/ of mailserver). De DMZ dient door een firewall beschermd te worden, maar moet wel zodanig geconfigureerd worden (gaten in de firewall) dat de diensten binnen de DMZ toegankelijk blijven. (Bron: Wikipedia)

Split-DNS

Is de een Domain Name System (DNS) implementatie waarbij verschillende verzamelingen DNS gegevens worden geleverd afhankelijk van de bron van het DNS verzoek. In de praktijk komt het er op neer dat de DNS server voor een computer binnen het intranet een private adres van de server binnen de intranet grenzen geeft en voor gebruikers van buitenaf (het internet) het adres van de server in de DMZ (zie hierboven) of de firewall/router die verbonden is met de server.