

Handleiding ADFS 4.0 installatie Windows Server 2016

In deze handleiding lees je hoe je jouw instelling of organisatie kunt aansluiten op SURFconext als **Identity Provider**, kortweg **IdP**, met behulp van ADFS. In ADFS-terminologie wordt dit ook een **Claims Provider** genoemd.

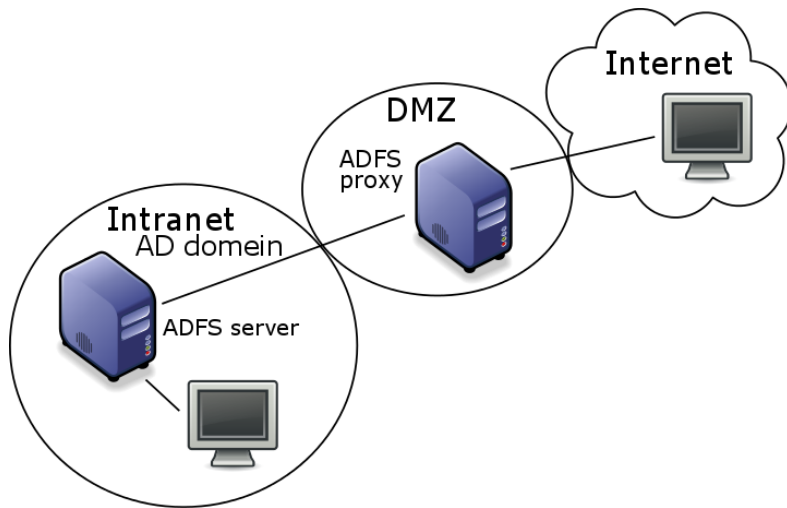
Deze procedure voor het aansluiten als Identity Provider op SURFconext bestaat uit de volgende onderdelen:

- Een ADFS serversysteem inrichten; waaronder Windows Server 2016 configureren en ADFS installeren.
- De ADFS server configureren voor aansluiting als Identity Provider (IdP) voor SURFconext. En attributen configureren en vrijgeven aan SURFconext.
- Een ADFS proxy inrichten indien toegang van buiten het lokale netwerk gewenst is.

Deze handleiding is gebaseerd op de release van ADFS 4 zoals voor Windows Server 2016.

Waarom een server en 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 opstelling. De proxy mag geen lid zijn van het domein en wordt bij voorkeur in de [DMZ](#) 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 4.0 Server inrichten

Dit document beschrijft de installatie van een ADFS server op Windows Server 2016. 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 2016.
- Voeg de ADFS software als feature toe.
- Configureer de basisinstellingen van ADFS.

Windows Server 2016 installeren en configureren

Om een ADFS 4.0 Server te kunnen inrichten, moet je eerst Windows Server 2016 installeren en configureren. Deze ADFS 4.0 Server dient lid te zijn van een domein. In deze handleiding installeren we de **ADDS** en **ADFS** rol op dezelfde server. Deze rollen zijn als volgt te omschrijven:

- **ADDS** - Active Directory Domain Services (AD DS) is een serverrol in Active Directory die beheerders in staat stelt om informatie over bronnen uit een netwerk, maar ook over applicatiegegevens, te beheren en op te slaan in een gedistribueerde database. AD DS kan beheerders ook helpen om de elementen van een netwerk (computers en eindgebruikers) te beheren en te ordenen in een aangepaste hiërarchie.
- **ADFS** - Active Directory Federation Services (ADFS) is een op Windows Server-besturingssystemen draaiend component die gebruikt wordt om gebruikers met een **Single Sign-On** toegang te geven tot systemen en toepassingen die zich over de grenzen van de organisatie heen bevinden. Het maakt gebruik van een op claims gebaseerd autorisatiemodel voor toegangscontrole om de beveiliging van applicaties te handhaven en om een gefedereerde identiteit te implementeren.

Je gaat de onderstaande stappen doorlopen om aan te sluiten op SURFconext:

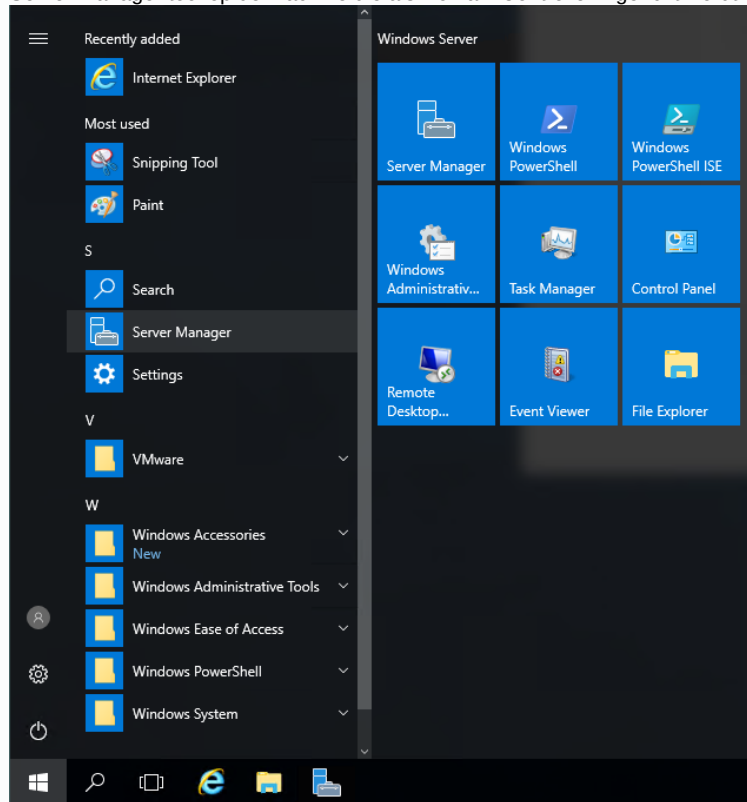
- Installeer Windows Server 2016 op de server.
- Stel de tijd op de server correct in en zorg ervoor dat je deze synchroniseert met een time server (NTP).
- Neem de server op in het domein van de Active Directory waaruit de accounts voor de SURFconext federatie komen.
- Installeer een geldig certificaat 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.

AD DS Server Rol installeren

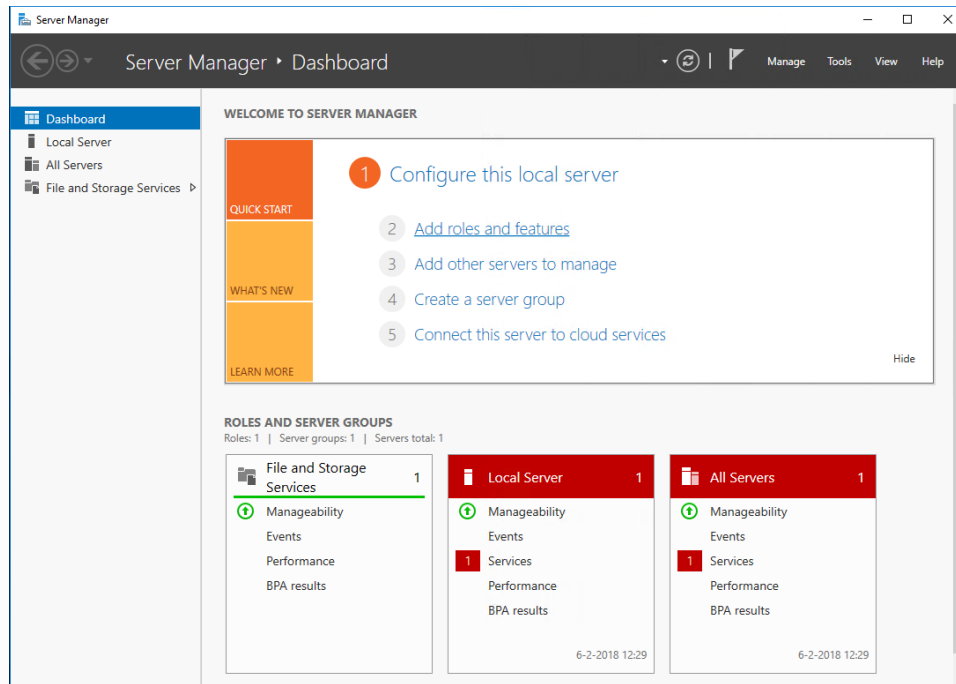
Hieronder wordt ingegaan op het installeren van de **AD DS Server Role** op **Windows Server 2016**. Klik op hieronder op 'Click here to expand' om het stappenplan te zien.

Stappenplan AD DS Server Rol installeren

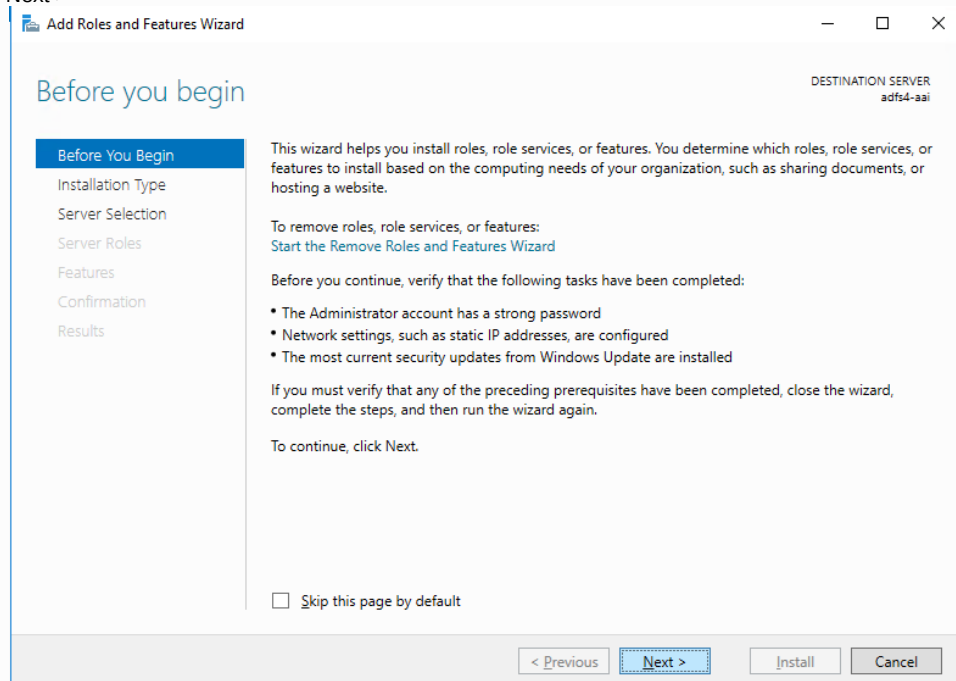
1. Start de Server Manager tool op de machine die als Domain Controller ingericht wordt.



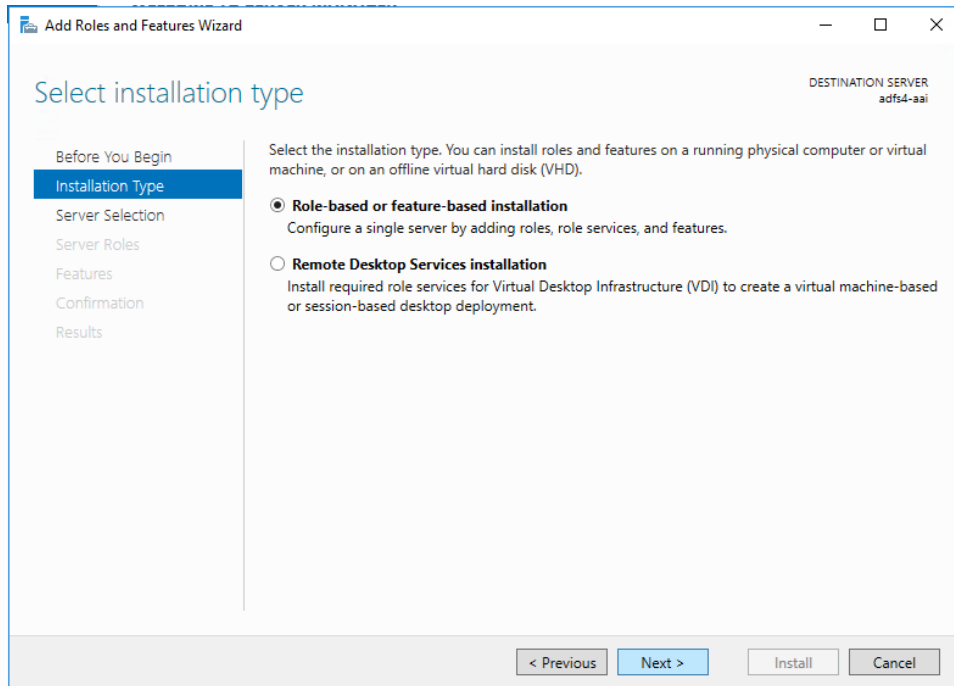
- a. Klik op "Add Roles and Features".



a.
3. Klik op "Next >"

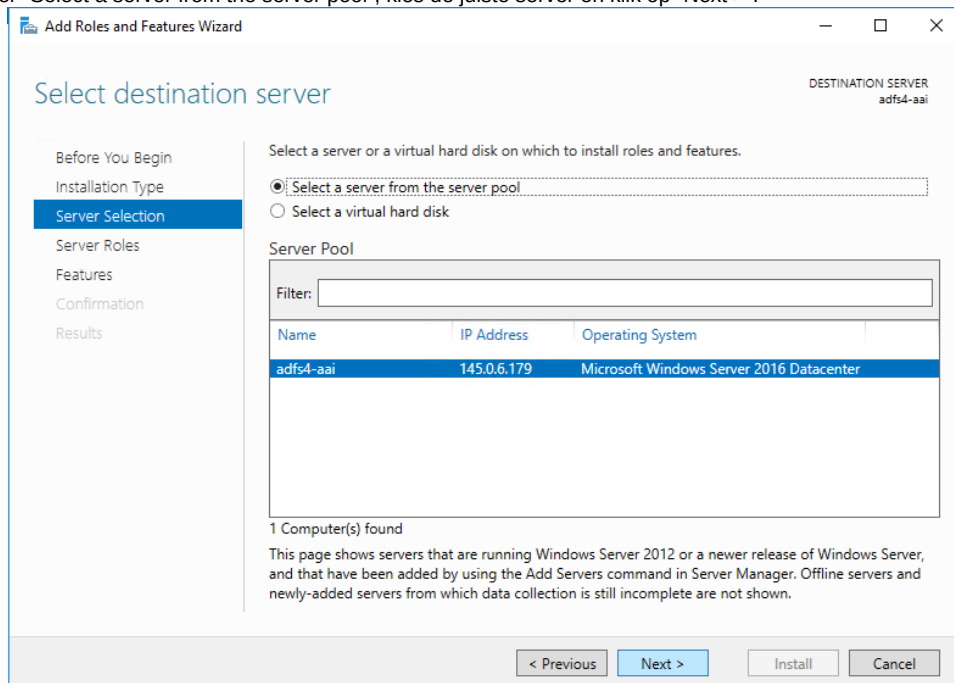


a.
4. Klik op "Role-based or feature-based installation" en klik op "Next >":



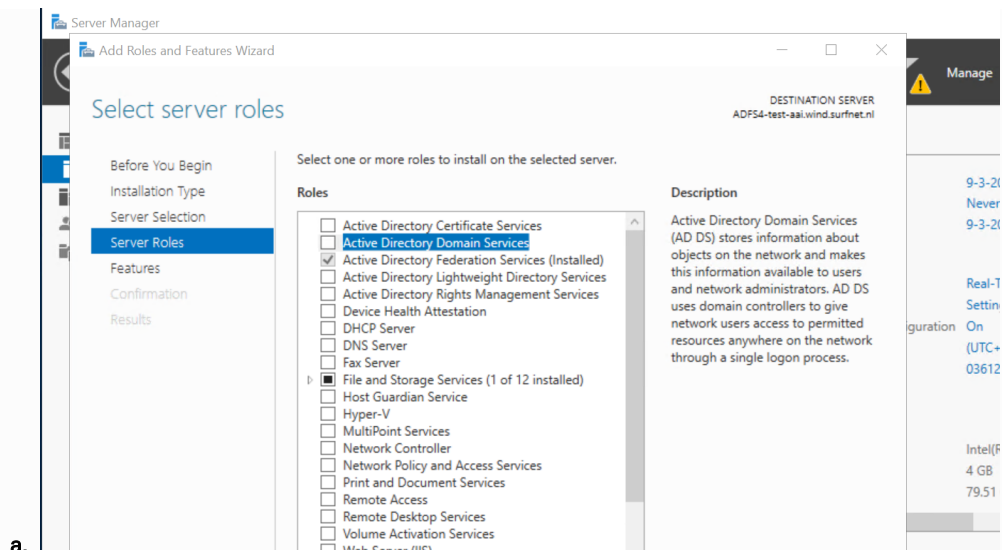
a.

5. Selecteer "Select a server from the server pool", kies de juiste server en klik op "Next >":



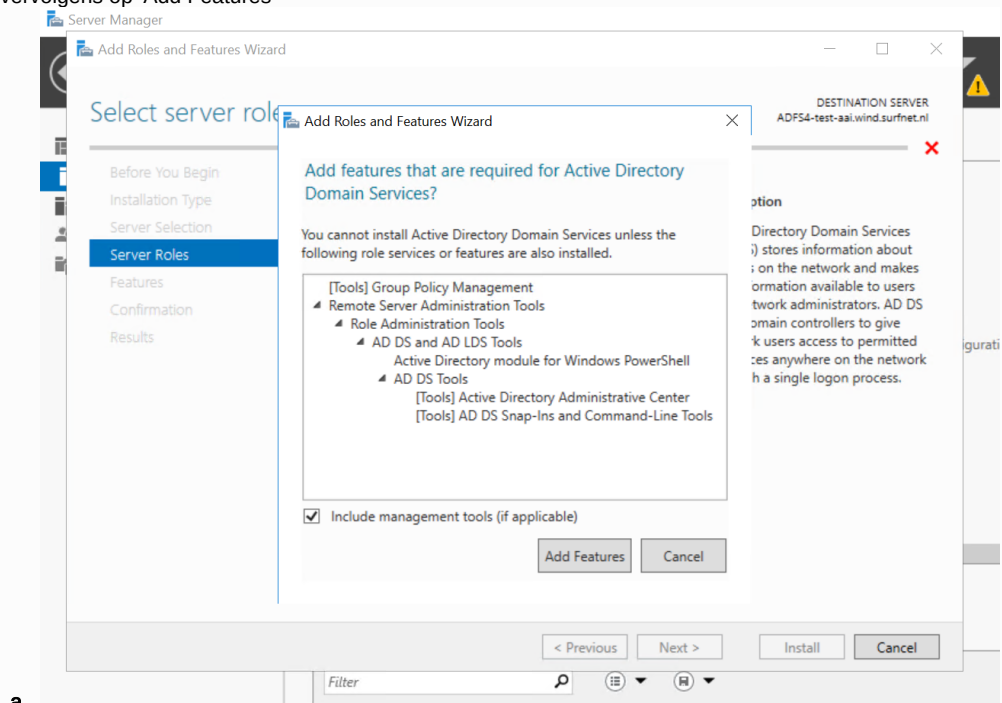
a.

6. Selecteer **Active Directory Domain Services**



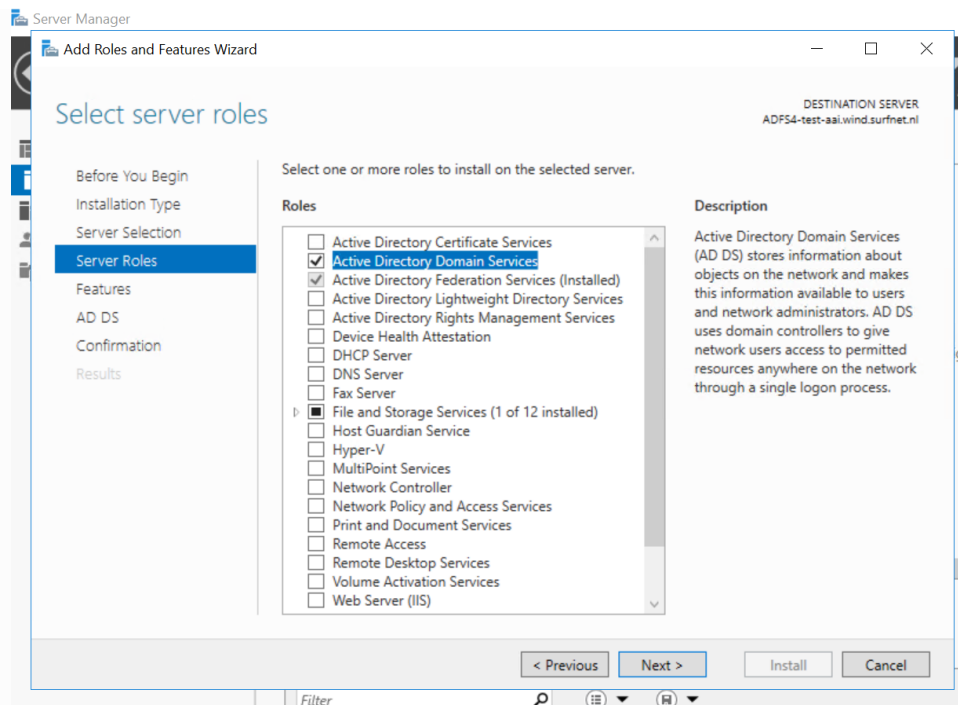
a.

7. Klik vervolgens op 'Add Features'



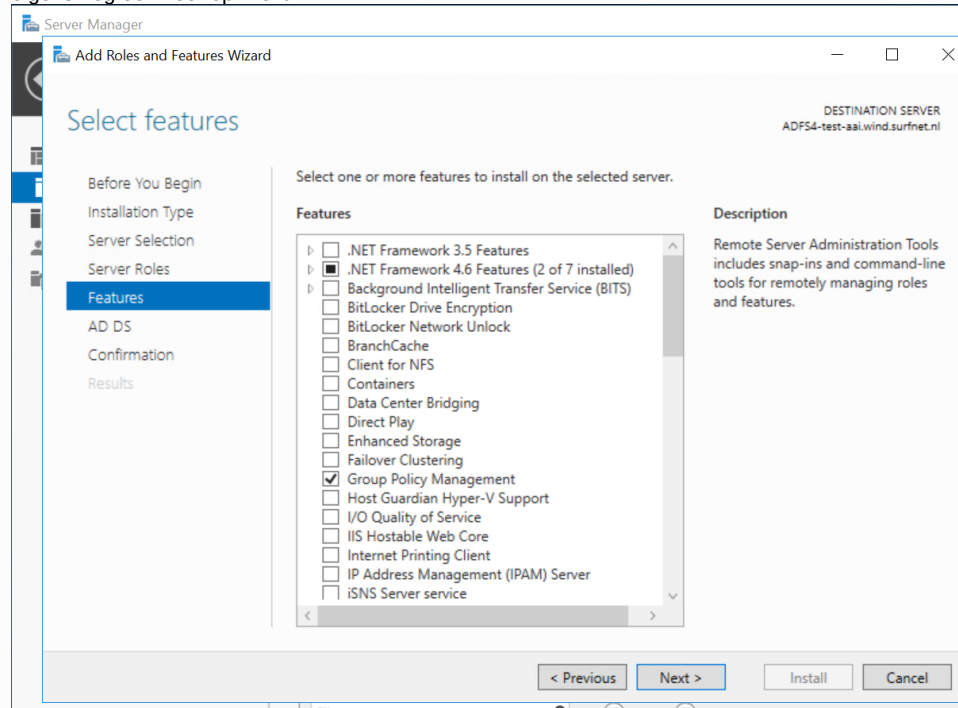
a.

8. Klik op 'Next'



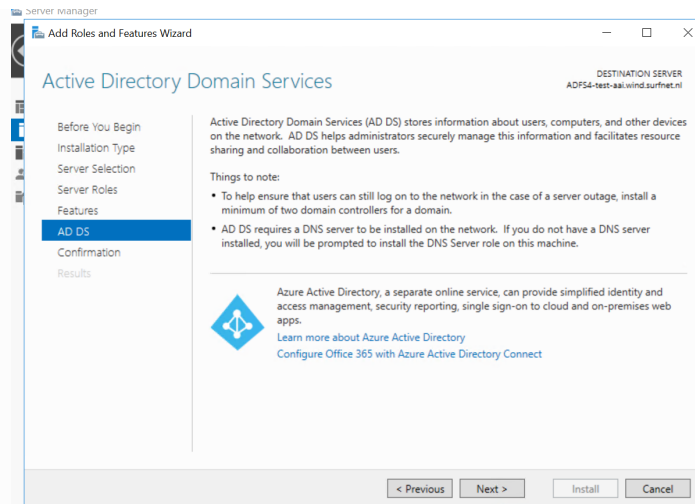
a.

9. Klik vervolgens nog een keer op 'Next'



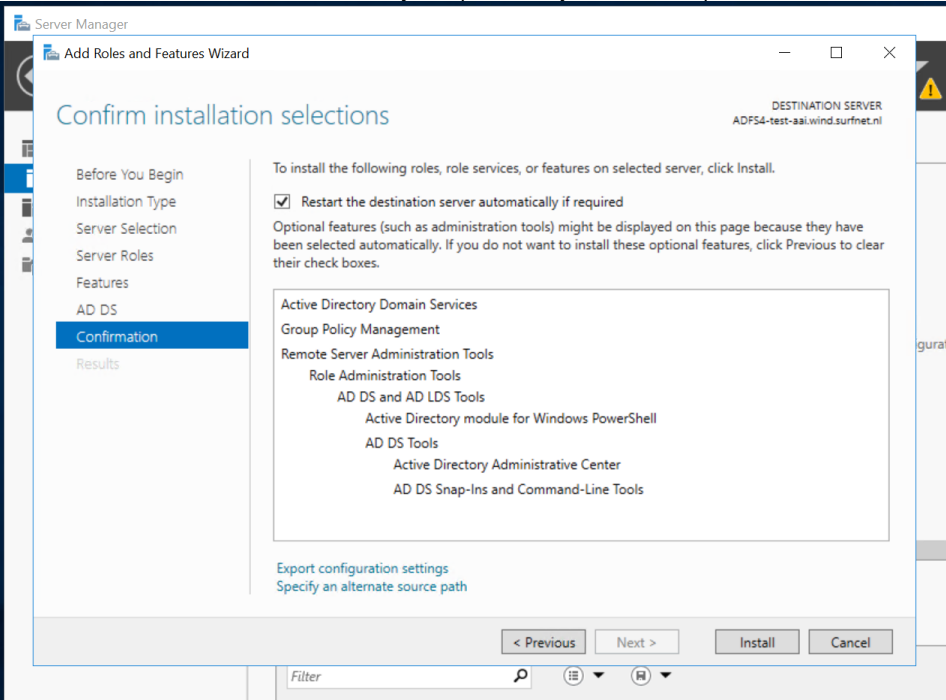
a.

10. Klik nog een keer op 'Next'



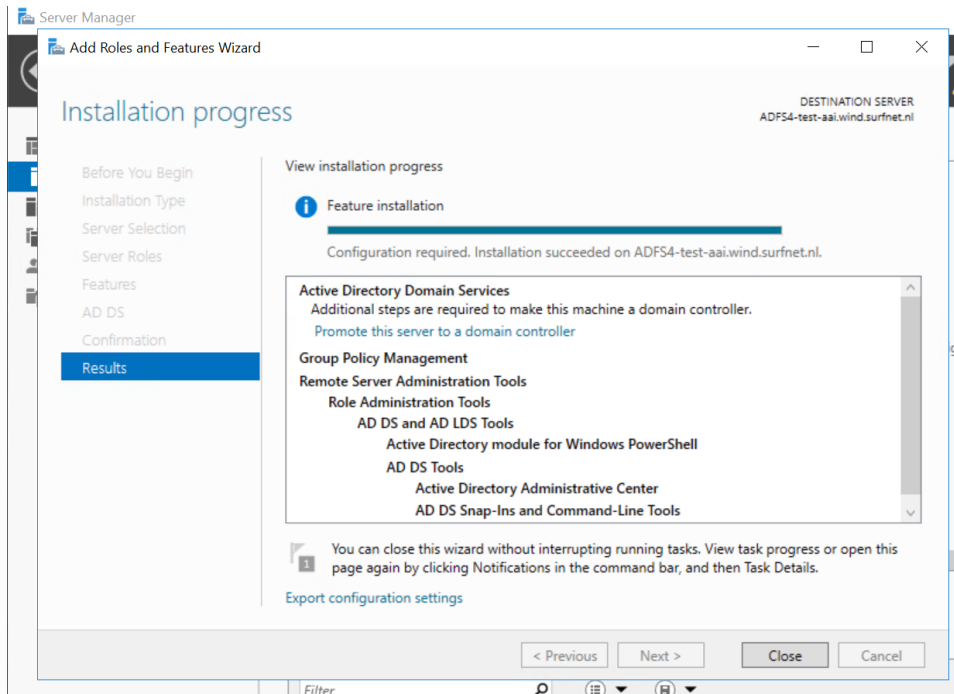
a.

11. Vink het 'Restart the destination server automatically if required' vinkje aan en klik op 'Install'.

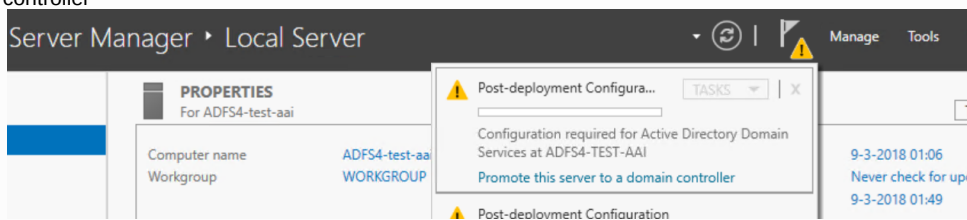


a.

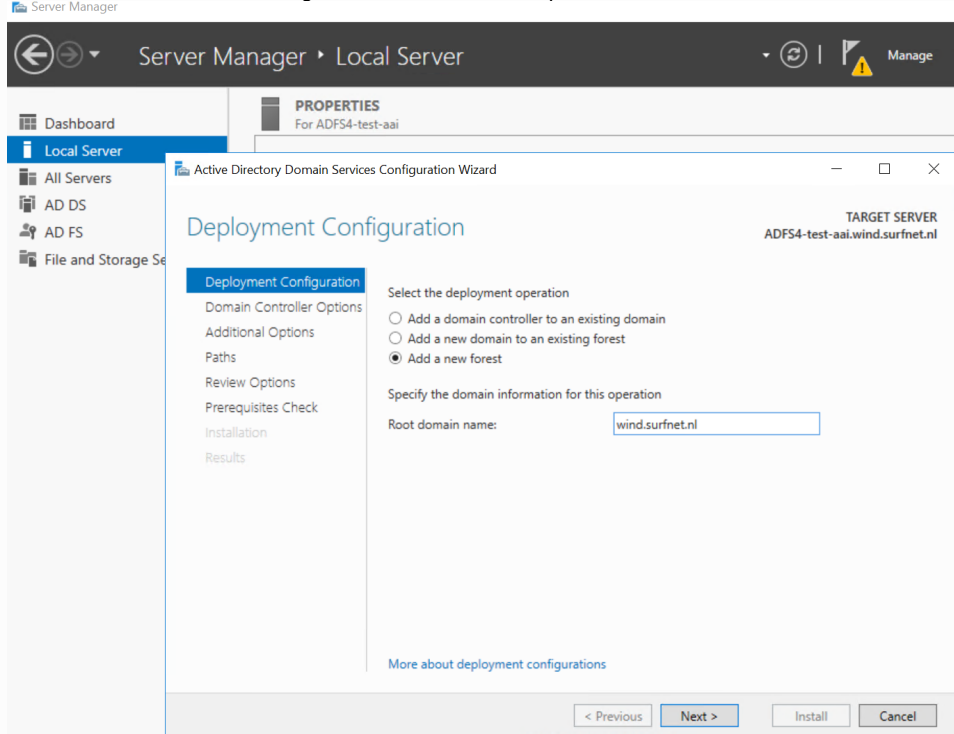
12. Klik op 'Close' wanneer de installatie succesvol is verlopen



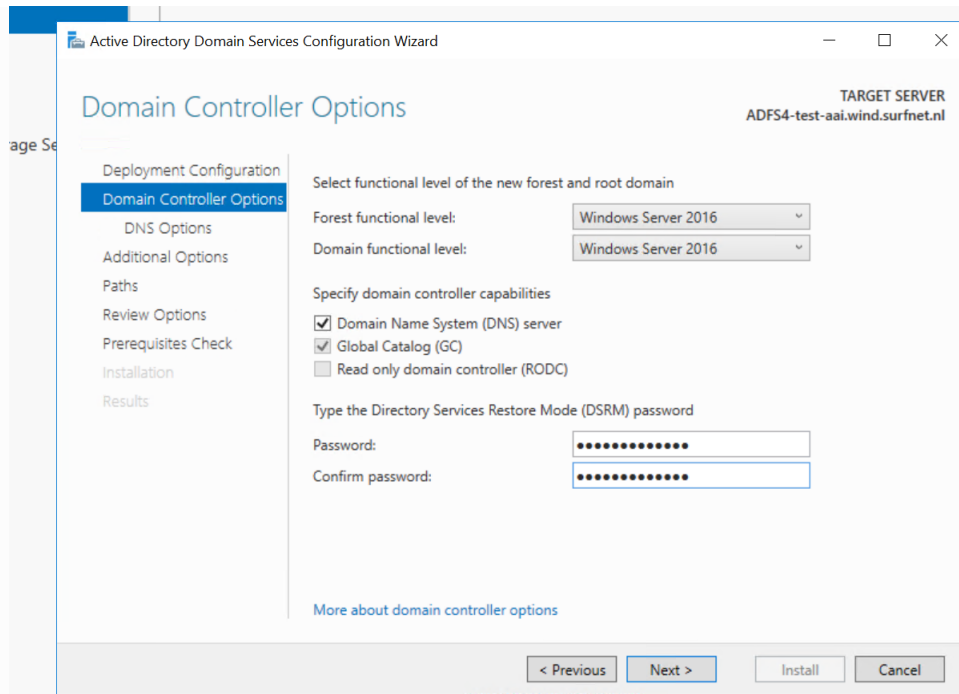
- a.
13. Klik in de Servermanager op het vlaggetje voor meldingen en kies voor de Post-deployment actie 'Promote this server to a domain controller'



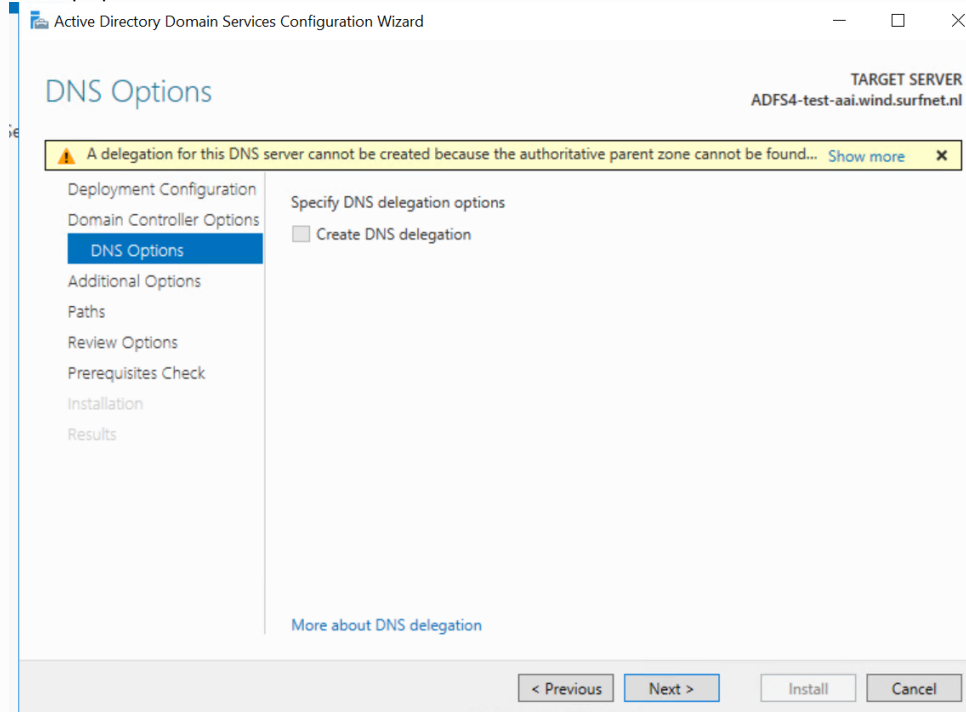
- a.
14. In deze stap kan je kiezen of de machine wordt toegevoegd aan een bestaand domein of niet. Wij kiezen er in deze stap voor om een nieuwe forest aan te maken en geven de naam hiervoor op.



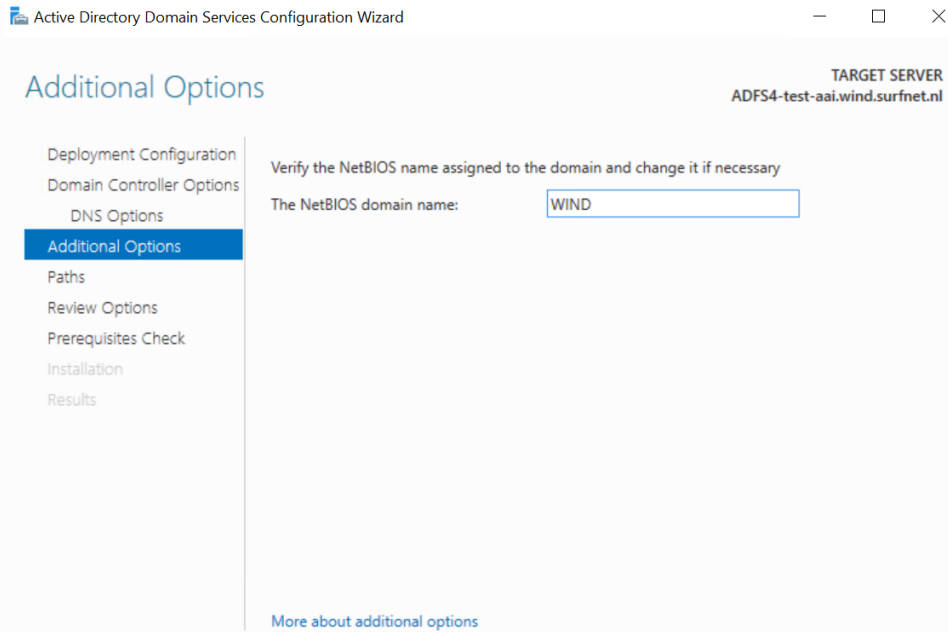
- a.
15. Verander niets aan de settings, geeft een nieuw wachtwoord op en klik op 'Next'



- a.
16. Klik in deze stap op 'Next'

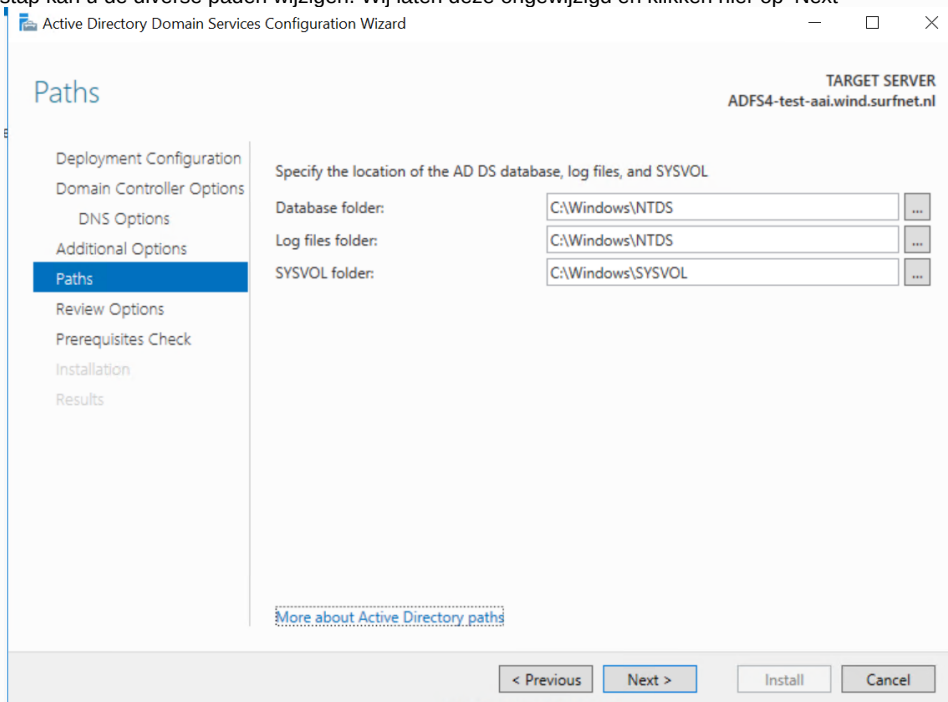


- a.
17. Controleer of de NETBIOS naam voor het domein klopt of pas hem aan naar de juiste en klik op 'Next'



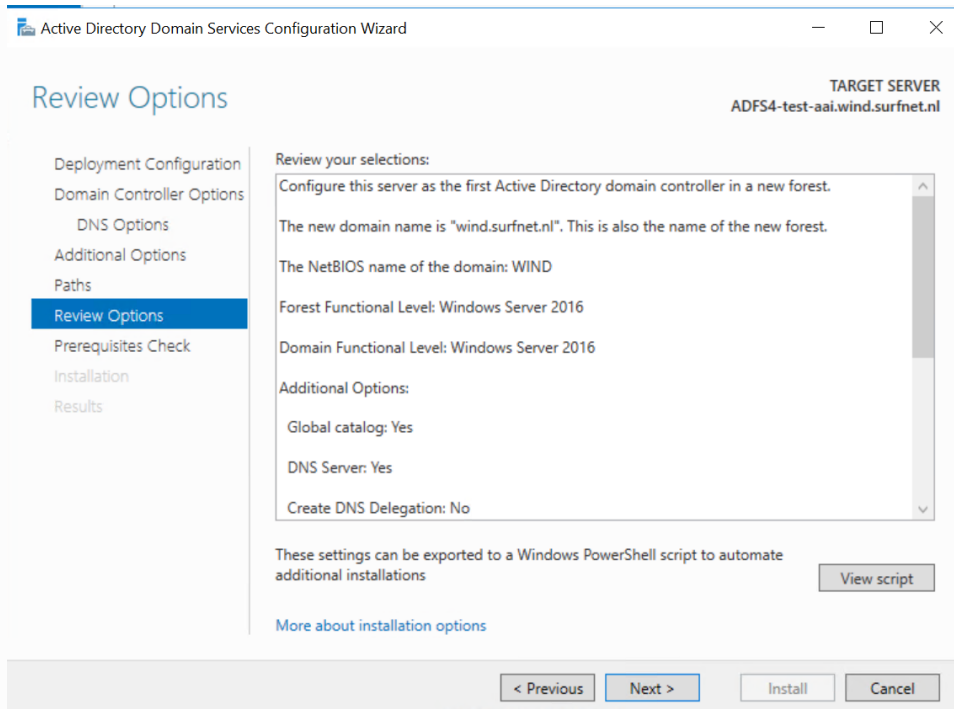
a.

18. In deze stap kan u de diverse paden wijzigen. Wij laten deze ongewijzigd en klikken hier op 'Next'

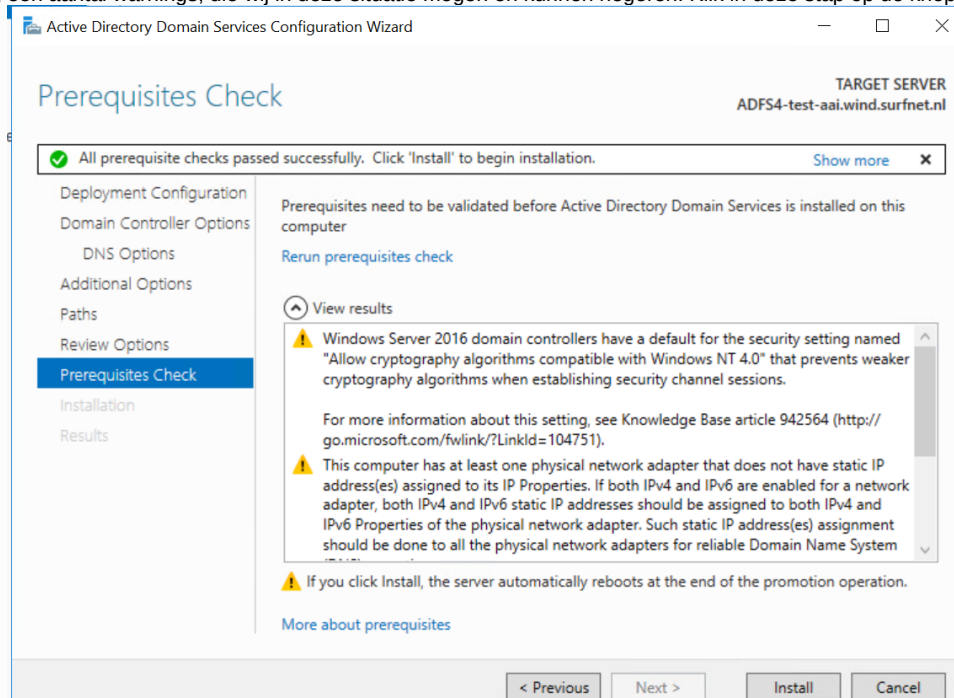


a.

19. Er wordt een overzicht van de instellingen gegenereerd. Klik in deze stap op 'Next'



- a. 20. Wij krijgen een aantal warnings, die wij in deze situatie mogen en kunnen negeren. Klik in deze stap op de knop 'Install'



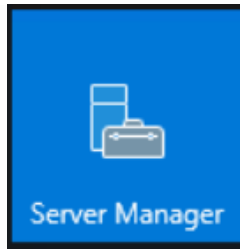
- a. 21. De server zal een keer opnieuw opstarten en vanaf nu is uw server een Domain Controller en onderdeel van een domein.

ADFS Server Software installeren

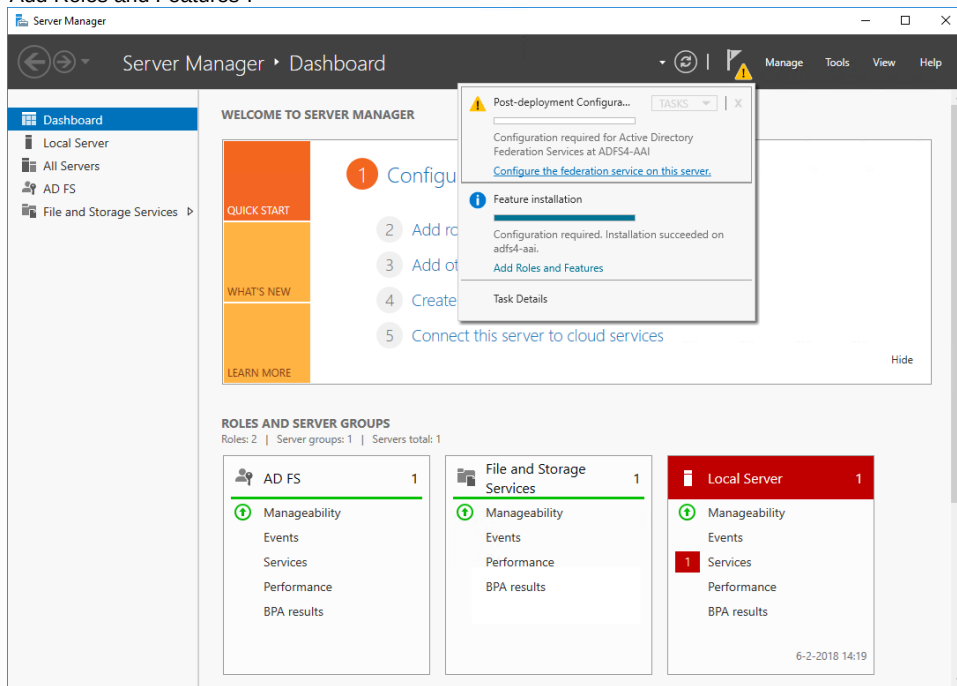
Onderstaand gedeelte van deze handleiding is te gebruiken voor het installeren van de **ADFS Server Role** op **Windows Server 2016**.

Stappenplan AD FS Server Software Installeren

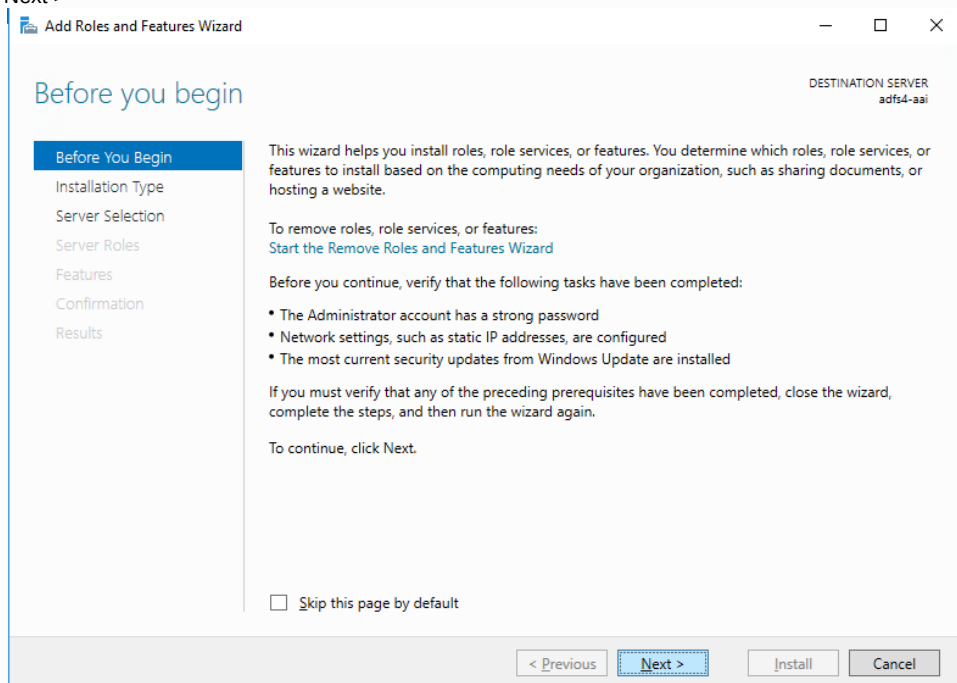
1. Start de Server Manager tool op de machine die als ADFS Server ingericht wordt.



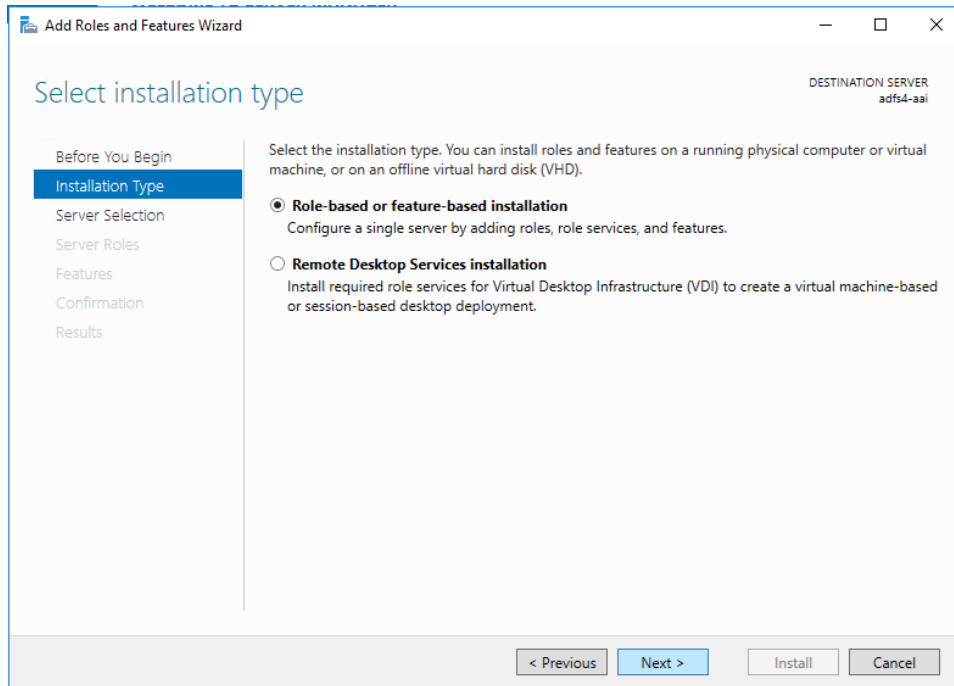
- a.
- Klik op "Add Roles and Features".



- a.
- Klik op "Next >"

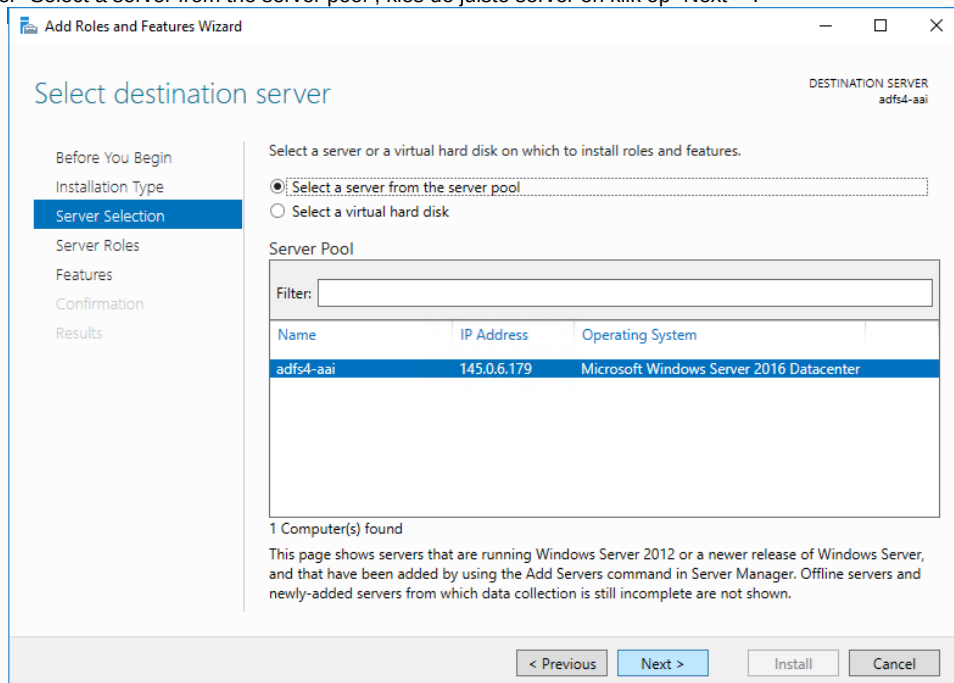


- a.
- Klik op "Role-based or feature-based installation" en klik op "Next >":



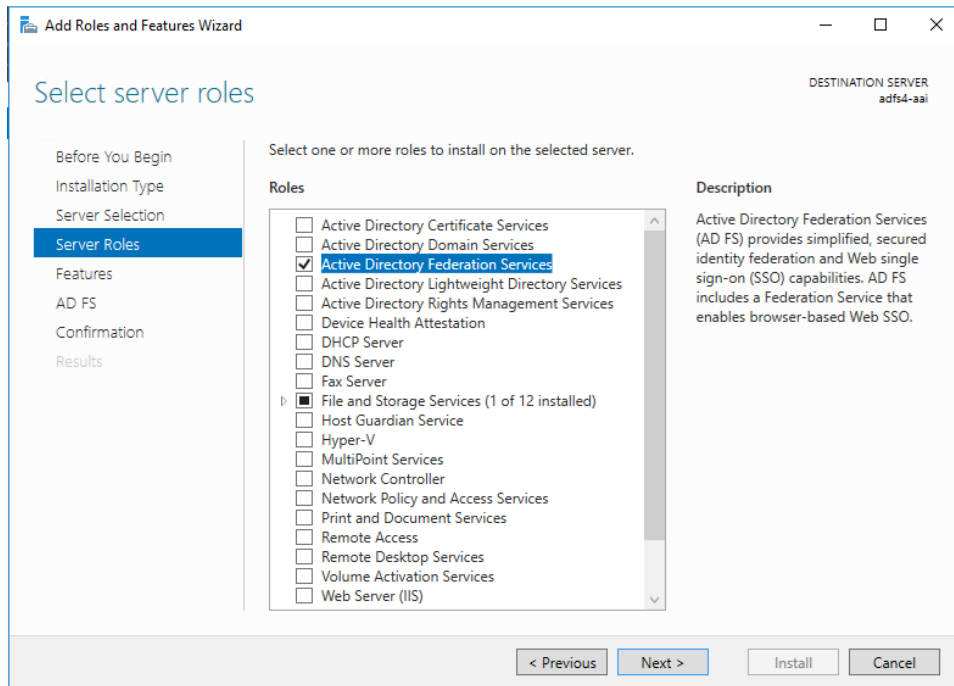
a.

5. Selecteer "Select a server from the server pool", kies de juiste server en klik op "Next >":



a.

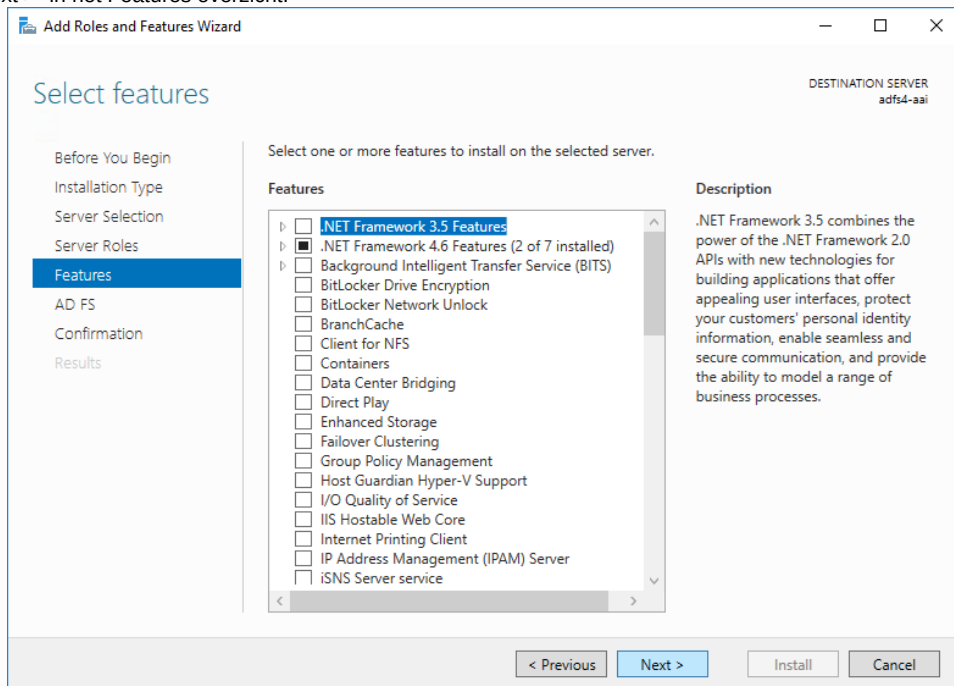
6. Selecteer "Active Directory Federation Services" en klik op "Next >":



a.

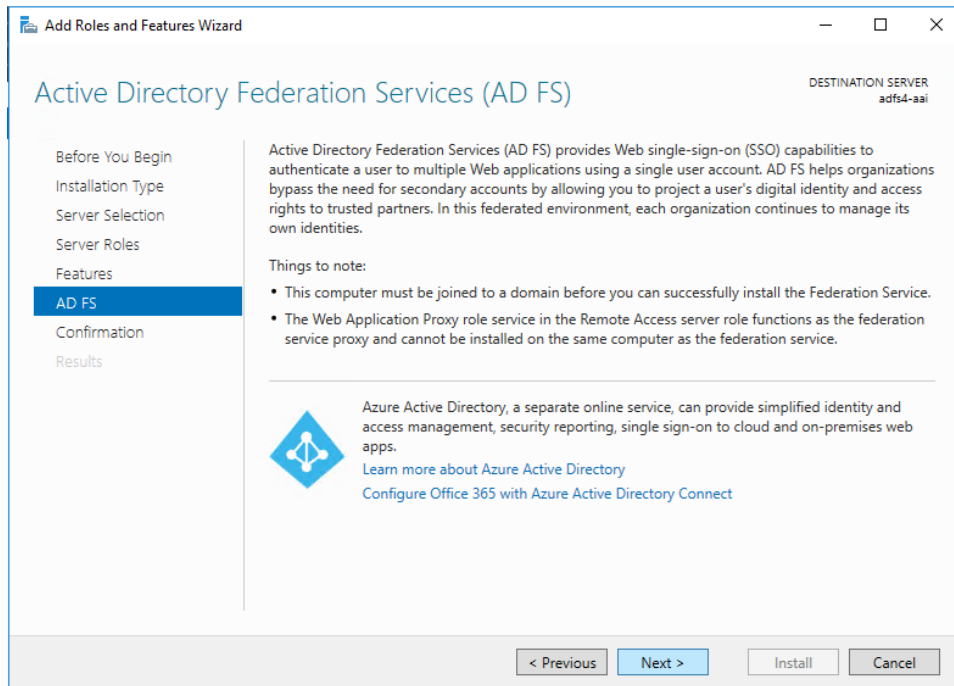
7. Klik "Next >" in het Features overzicht:

Procedure

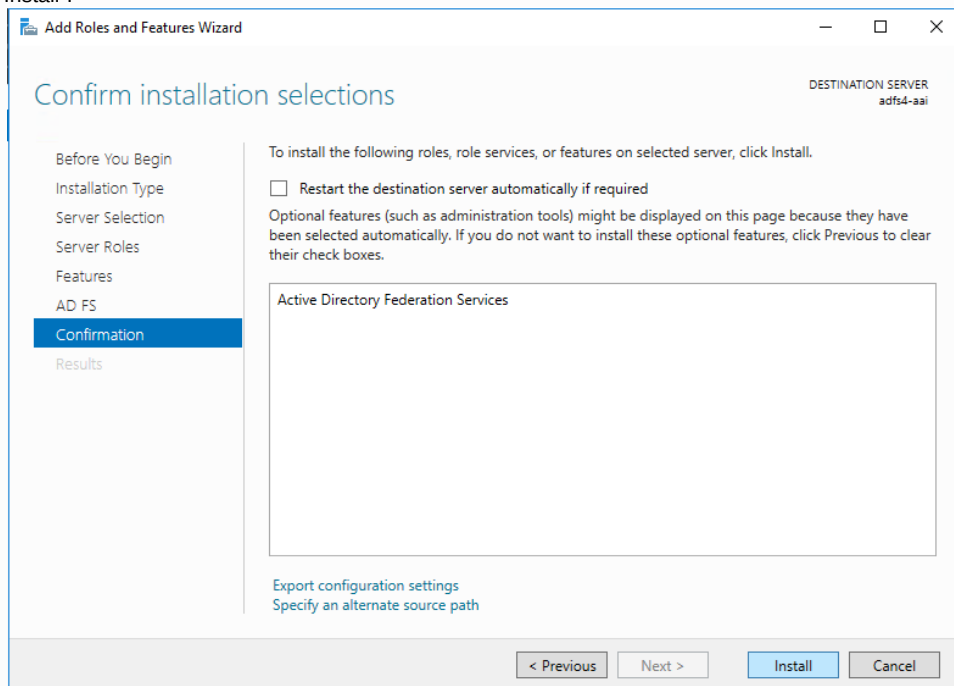


a.

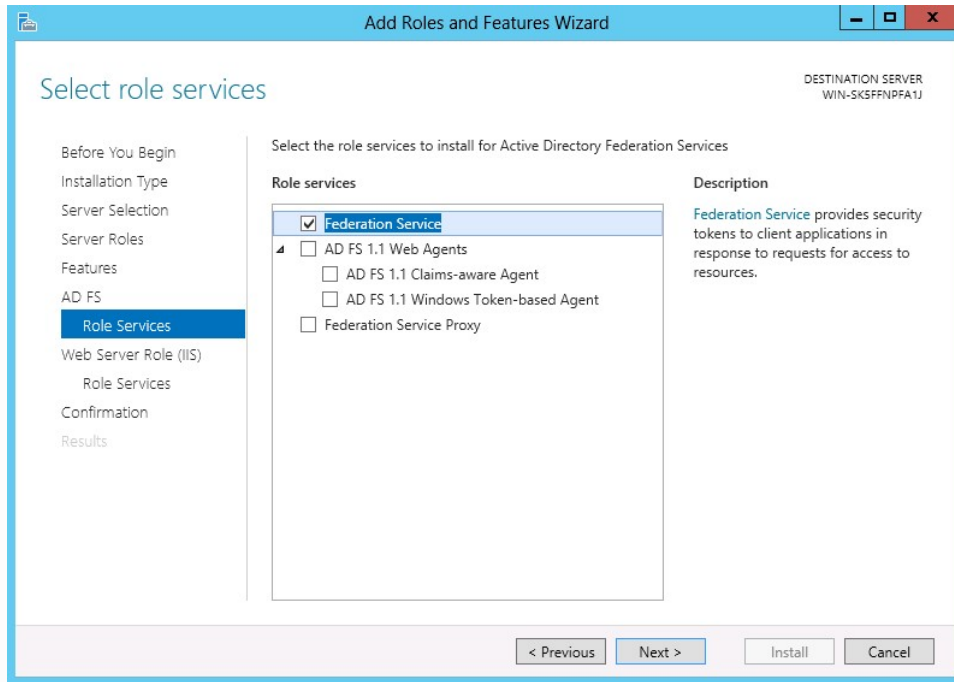
8. Klik op "Next >":



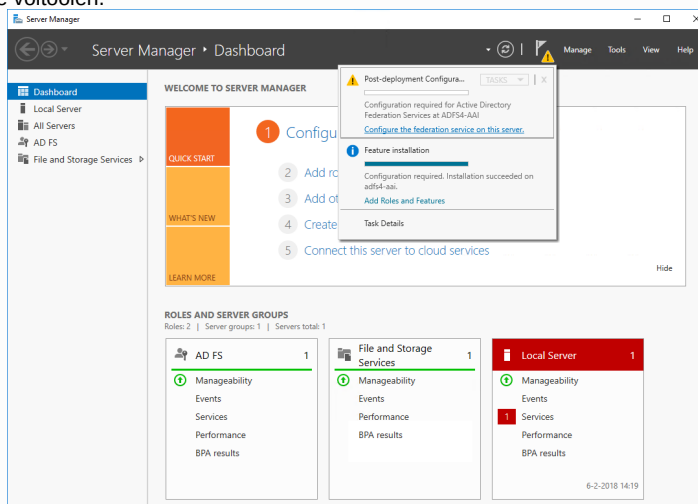
- a.
9. Klik op "Install":



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



- a.
11. 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 "Configure the federation service on this server" om de installatie van ADFS te voltooien.



- a.
12. Klik "Next >" in het eerste scherm:

Active Directory Federation Services Configuration Wizard

Welcome

TARGET SERVER
adfs4-aa1.TESTDOMEIN.nl

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

[AD FS prerequisites](#)

Select an option below:

☒ Create the first federation server in a federation server farm

☐ Add a federation server to a federation server farm

Configuring sign-in to Office 365? Exit this wizard and use [Azure Active Directory Connect](#).

< Previous Next > Configure Cancel

a.

13. Kies het AD Administrator account en klik op "Next >":

Active Directory Federation Services Configuration Wizard

Connect to Active Directory Domain Services

TARGET SERVER
adfs4-aa1.TESTDOMEIN.nl

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

TESTDOMEIN\Administrator (Current user) [Change...](#)

< Previous Next > Configure Cancel

a.

14. Kies het vooraf geïnstalleerde SSL certificaat (Appendix A) waarmee de ADFS dienst ontsloten zal worden en een handige "Displayname" bijvoorbeeld Login Universiteit Harderwijk). Klik op "Next >":

- a.
15. 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. Uit veiligheidsoogpunt en voor de beheersbaarheid kan er voor worden gekozen om een Group Managed Service Account te gebruiken:

- a.
16. Selecteer "Create a database on this server using Windows Internal Database." en klik op "Next >":

Active Directory Federation Services Configuration Wizard

TARGET SERVER
adfs4-aa1.TESTDOMEIN.nl

Specify Configuration Database

Specify a database to store the Active Directory Federation Service configuration data.

☒ Create a database on this server using Windows Internal Database.

☐ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

< Previous Next > Configure Cancel

a.
17. Klik op "Next >":

Active Directory Federation Services Configuration Wizard

TARGET SERVER
adfs4-aa1.TESTDOMEIN.nl

Review Options

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'adfs4-aa1.wind.surfnet.nl'.

AD FS configuration will be stored in Windows Internal Database.

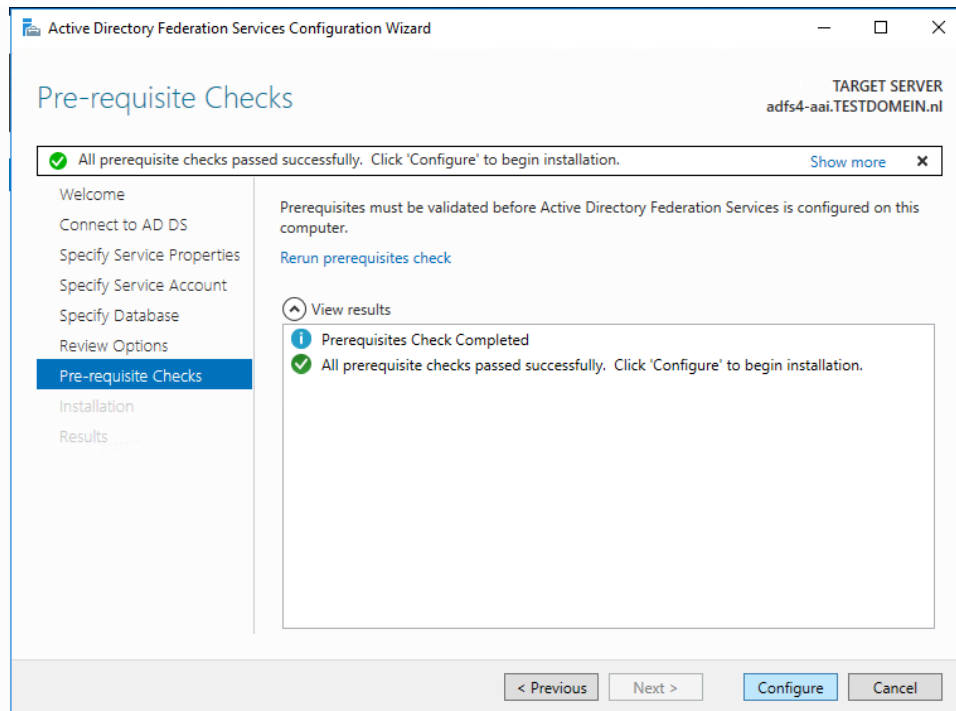
Windows Internal Database feature will be installed on this server if it is not already installed.

Federation service will be configured to run as TESTDOMEIN\Administrator.

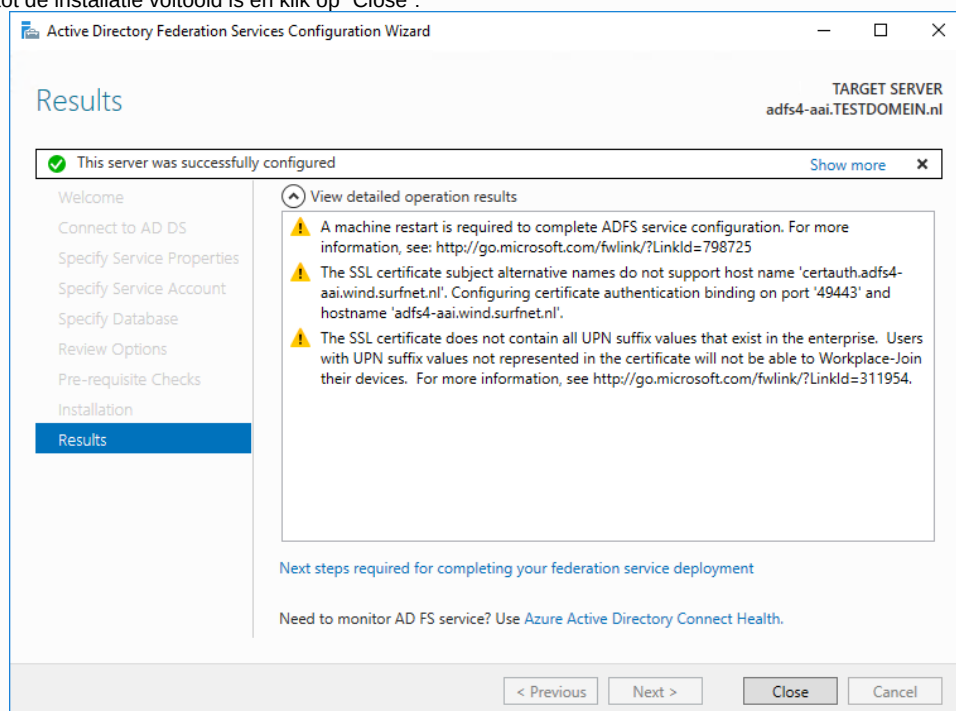
These settings can be exported to a Windows PowerShell script to automate additional installations [View script](#)

< Previous Next > Configure Cancel

a.
18. Klik op "Configure":



- a.
19. Wacht tot de installatie voltooid is en klik op "Close":



- a.
20. Om verder te gaan zijn er claim beschrijvingen nodig. "step 4" op de wiki (<https://wiki.surfnet.nl/display/services/Configure+Office+365+with+AD+FS+and+SURFconext+Step-by-Step>) is hierbij nodig. Open PowerShell en voer de volgende commando's uit:

Claim description PowerShell

```
# Create AD FS Claim Descriptions

# ADD UID CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:uid -ClaimType urn:mace:dir:attribute-def:uid -ShortName uid -IsAccepted $false -IsOffered $false

# ADD MAIL CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:mail -ClaimType urn:mace:dir:attribute-def:mail -ShortName mail -IsAccepted $false -IsOffered $false
```

```
# ADD DISPLAYNAME CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:displayName -ClaimType urn:mace:dir:attribute-def:displayName -ShortName displayName -IsAccepted $false -IsOffered $false

# ADD schacHomeOrganization CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name schacHomeOrganization -ClaimType urn:mace:terena.org:attribute-def:schacHomeOrganization -ShortName schacHomeOrganization -IsAccepted $true -IsOffered $true

# ADD eduPersonAffiliation CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:eduPersonAffiliation -ClaimType urn:mace:dir:attribute-def:eduPersonAffiliation -ShortName eduPersonAffiliation -IsAccepted $true -IsOffered $true

# ADD eduPersonEntitlement CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:eduPersonEntitlement -ClaimType urn:mace:dir:attribute-def:eduPersonEntitlement -ShortName eduPersonEntitlement -IsAccepted $false -IsOffered $false

# ADD employeeNumber CLAIM DESCRIPTION
Add-ADFSClaimDescription -Name urn:mace:dir:attribute-def:employeeNumber -ClaimType urn:mace:dir:attribute-def:employeeNumber -ShortName employeeNumber -IsAccepted $false -IsOffered $false
```

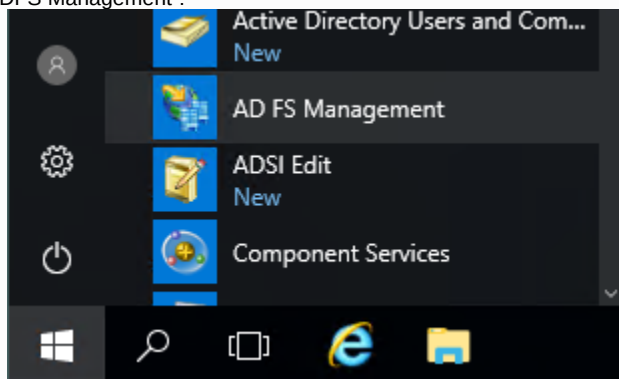
21. Stap 5 in de wiki beschrijft het toevoegen van de "SURFconext Relying Party Trust". Download het configuratiebestand: [Claim Issuance Rules.txt](#) (op <https://edu.nl/grq3c>)
22. De url van de metadata (\$MetadataURL) is afhankelijk op welke omgeving van SURFconext wordt aangesloten (De productie- of testomgeving):
 - a. De "**productie omgeving van SURFconext**" is t.b.v. productie diensten en productie IdP's. De Public SAML metadata (de entity descriptor) van de SURFconext SP Proxy voor deze omgeving staat op <https://metadata.surfconext.nl/sp-metadata.xml>.
 - b. De "**test omgeving van SURFconext**" is voor het aansluiten van nieuwe diensten & IdP's. Deze omgeving heeft eigen SAML endpoint en staat geheel los van de "productie omgeving van SURFconext" omgeving van SURFconext". De metadata voor jouw IdP is hier te vinden: <https://metadata.test.surfconext.nl/sp-metadata.xml>
23. De Public SAML metadata (de entity descriptor) van de SURFconext IdP Proxy voor deze omgeving is te vinden op onze [meta data-pagina](#). Overweeg om te beginnen op onze testomgeving. Raadpleeg [onze wiki wat deze omgevingen](#) voor je kunnen betekenen. Gebruik de **SURFconext SP proxy metadata** van test of productie. Kopieer onderstaande PowerShell commando's en voer deze uit nadat bij \$MetadataURL de juiste url is ingesteld (22.) en \$ClaimIssuanceFile het pad naar het zojuist gedownloade bestand is ingesteld

Claim description PowerShell

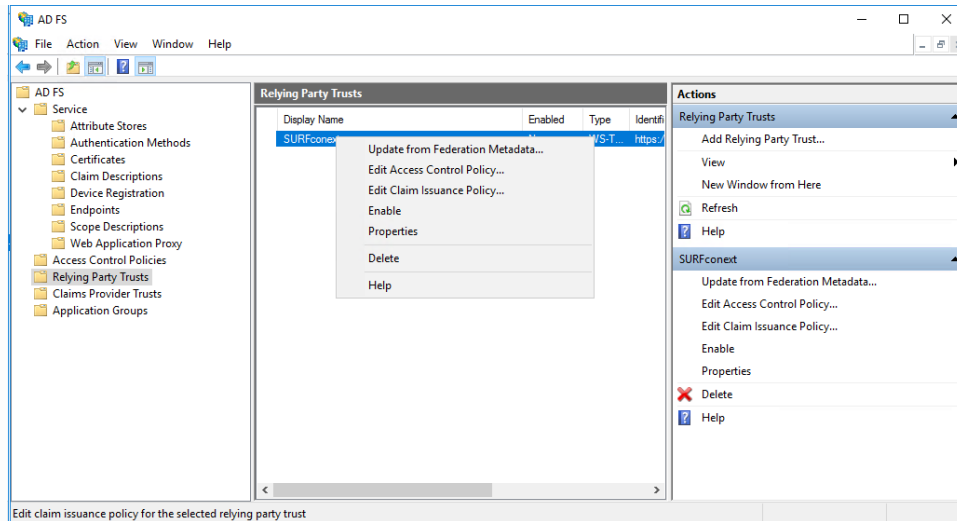
```
# CREATE SURFCONEXT RELYING PARTY TRUST
$RelyingPartyTrustName = "SURFconext"
$MetadataURL = "https://metadata.surfconext.nl/sp-metadata.xml"
$ClaimIssuanceFile = "THE LOCATION OF YOUR CLAIM ISSUANCE RULE FILE"
$ACPNName = "Permit everyone"

Add-ADFSRelyingPartyTrust -Name $RelyingPartyTrustName -MetadataUrl $MetadataURL -
IssuanceTransformRulesFile $ClaimIssuanceFile -AutoUpdateEnabled:$true -
MonitoringEnabled:$true -AccessControlPolicyName $ACPNName
```

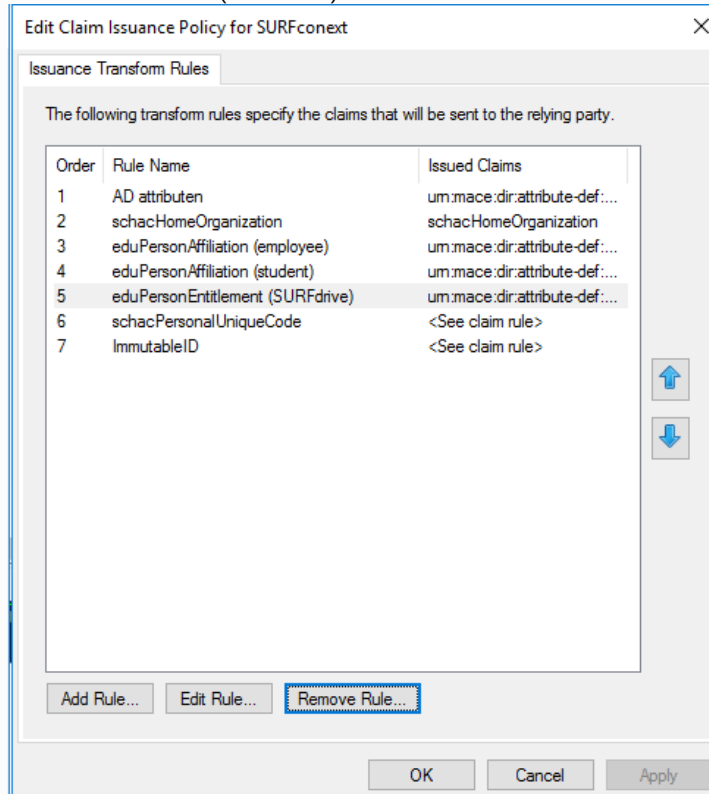
24. Start "ADFS Management":



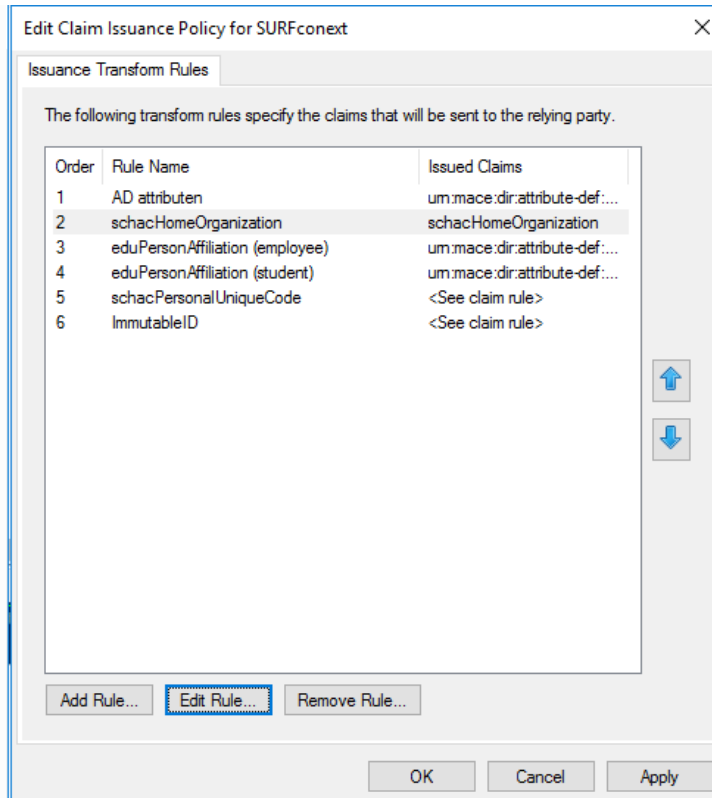
- a.
25. Ga naar "Relying Party Trust" en klik rechts op "SURFconext" > "Edit Claim Issuance Policy...":



- a.
26. Klik op "eduPersonEntitlement (SURFdrive)" en kies "Remove Rule..." > "OK":

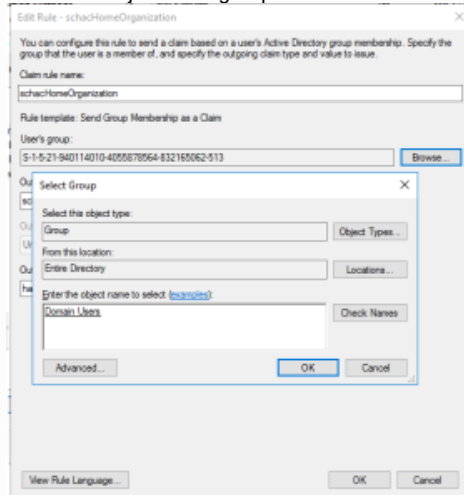


- a.
27. Kies voor "schacHomeOrganization" > "Edit rule...":



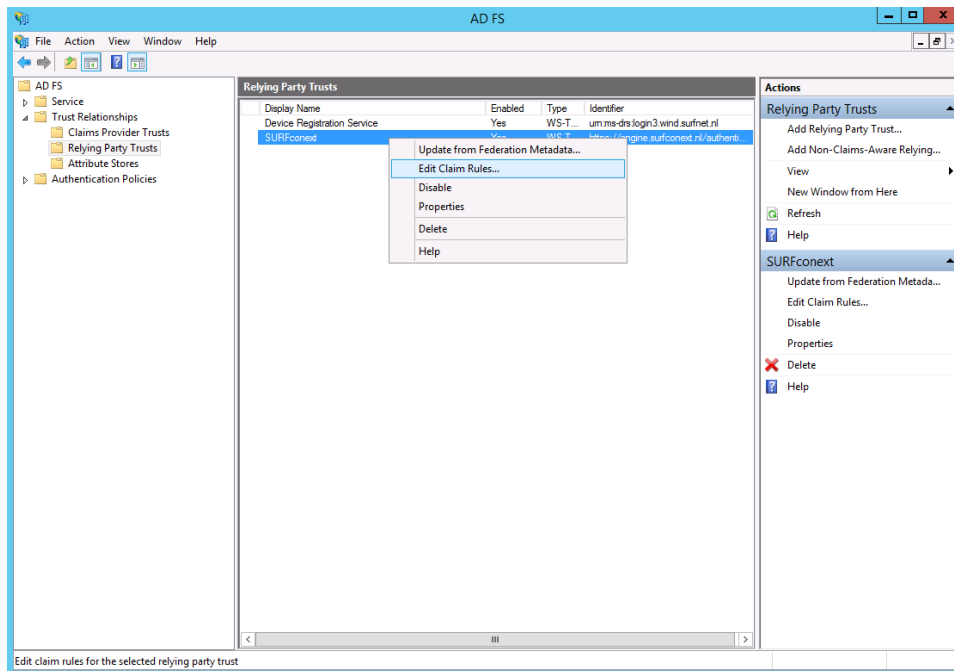
a.

28. Kies voor "Browse" bij "User's group" en vul "Domain Users" in > "OK" en weer "OK":



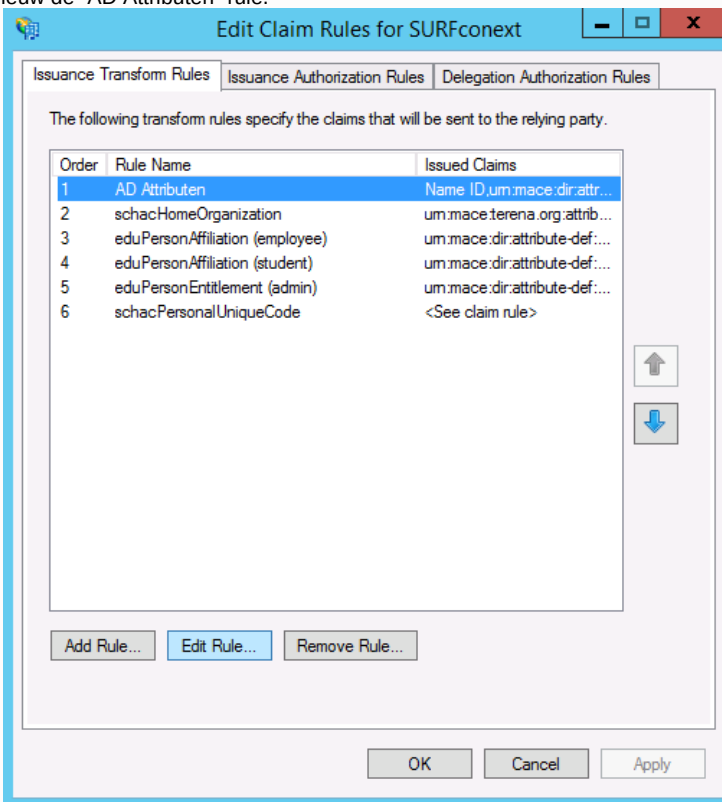
a.

29. Doe hetzelfde voor de eduPersonAffiliation Student en Employee. Vul bij Student de studenten AD groep in. Bij Employee de medewerkers AD groep. Indien deze AD groepen nog niet bestaan maak deze dan aan. En Klik "OK" om dit scherm te sluiten.
30. 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 voldoen 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:unihardervijk.nl:employeeid:90210. Hiervan is het employeeid "90210" waarschijnlijk wel beschikbaar als medewerkersnummer en kan het attribuut dus samengesteld worden uit de tekst "urn:schac:personalUniqueCode:nl:local:unihardervijk.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.
31. Edit opnieuw de Claim Rules van de Relying Party SURFconext



a.

32. Edit opnieuw de “AD Attributen” rule.



a.

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

Edit Rule - AD Attributen

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Name ID
SAM-Account-Name	um:mace:dir:attribute-def:uid
Display-Name	um:mace:dir:attribute-def:displayName
E-Mail-Addresses	um:mace:dir:attribute-def:mail
Employee-Number	um:mace:dir:attribute-def:employeeNumber

- a.
34. Sla de rule op en voeg een Custom claim rule toe door op de "Add Rule..." knop te klikken.

Edit Claim Rules for SURFconext

Issuance Transform Rules | Issuance Authorization Rules | Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	AD Attributen	Name ID, um:mace:dir:attr...
2	schacHomeOrganization	um:mace:terena.org:attrib...
3	eduPersonAffiliation (employee)	um:mace:dir:attribute-def:...
4	eduPersonAffiliation (student)	um:mace:dir:attribute-def:...
5	eduPersonEntitlement (admin)	um:mace:dir:attribute-def:...

- a.
35. Kies in het volgende venster voor "Send Claims Using a Custom Rule" en klik op "Next":
36. Geef de rule een beschrijvende naam zoals "schacPersonalUniqueCode" en creëer de gewenste attribuutsamenstelling op basis van een tekst en één of meerdere bestaande attributen.

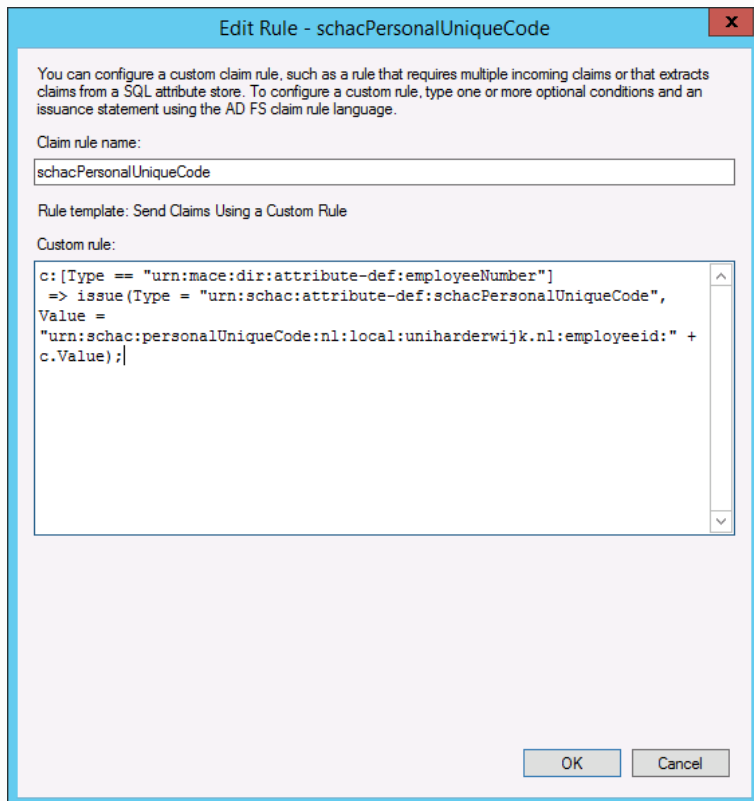
```
c:[Type == "urn:mace:dir:attribute-def:employeeNumber"]

=> 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:



37. Als de Rule compleet is, klik dan op "OK".

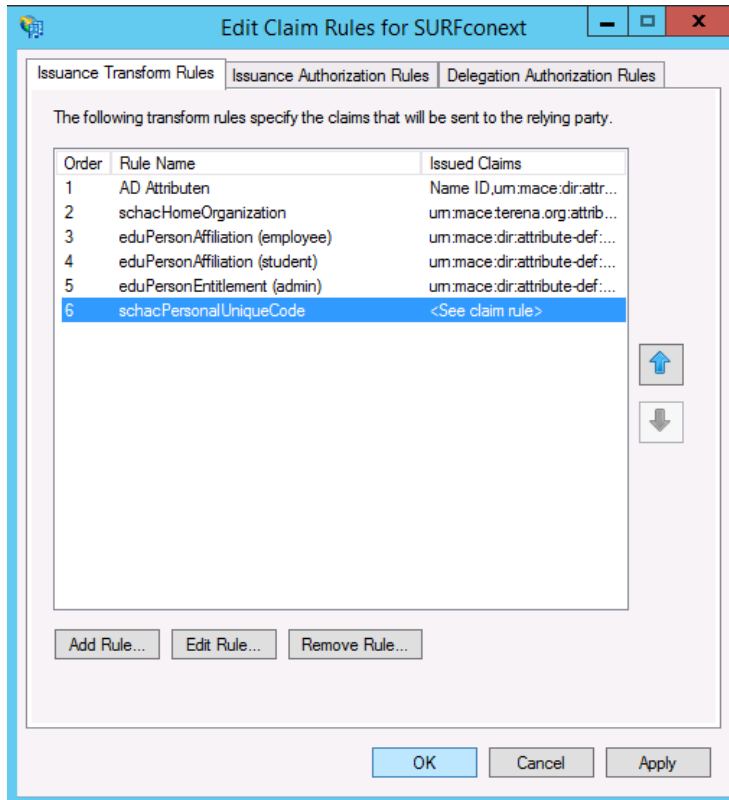
38. Een meer geavanceerde rule, welke ook de "schacHomeOrganization" en de "affiliation" meeneemt, ziet er dan als volgt uit:

```
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);
```

39. **eduPersonScopedAffiliation.** 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.



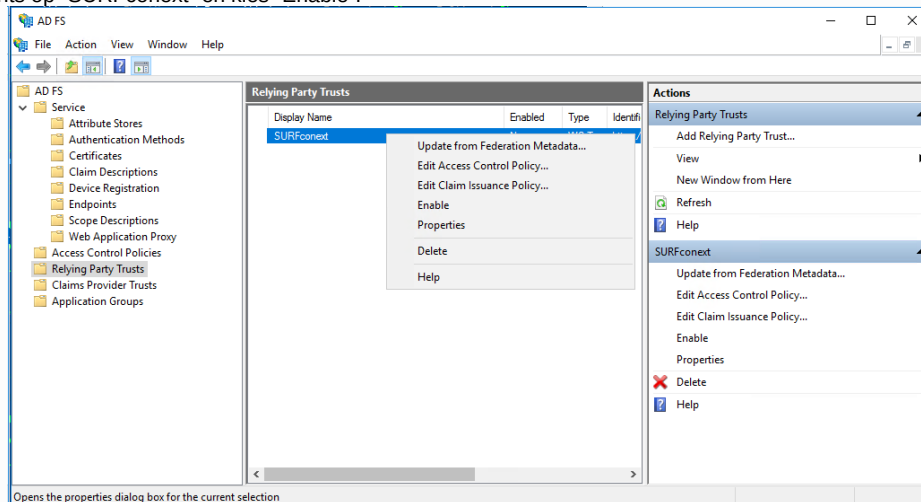
a.

40. Toevoegen claim op basis van groepslidmaatschap, bv eduPersonEntitlement:

```
c:[Type == http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid, Value == "<Type hier het SID van de juiste AD groep>" Issuer == "AD AUTHORITY"]
=> issue(Type = "urn:mace:dir:attribute-def:eduPersonEntitlement", Value = "urn:mace:surfnet.nl:surfconext.nl:surfnet.nl:eduvpn:admin", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, ValueType = c.ValueType);
```

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

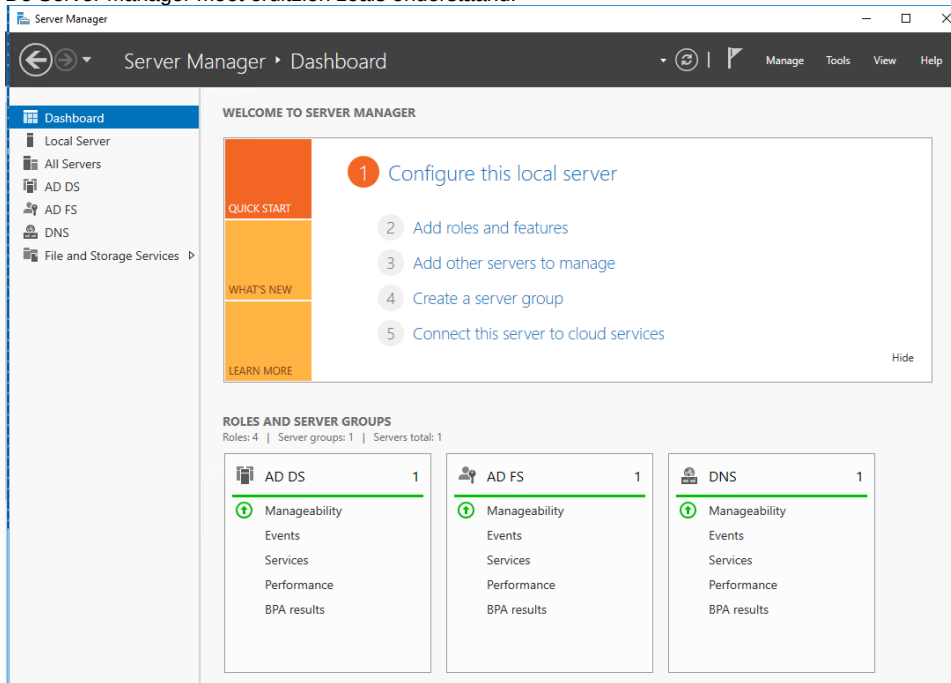
42. Klik rechts op "SURFconext" en kies "Enable":



a.

Opens the properties dialog box for the current selection

43. De Server Manager moet eruitzien zoals onderstaand:



ADFS Proxy installeren

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](#) configuratie ingericht worden. Dit is 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 of de firewall/router die verbonden is met de server. Als dat niet mogelijk is, moet de Proxy op een andere manier verteld worden wat het IP adres van de ADFS server is. Dit 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:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#127.0.0.1               localhost
#::1                     localhost
```

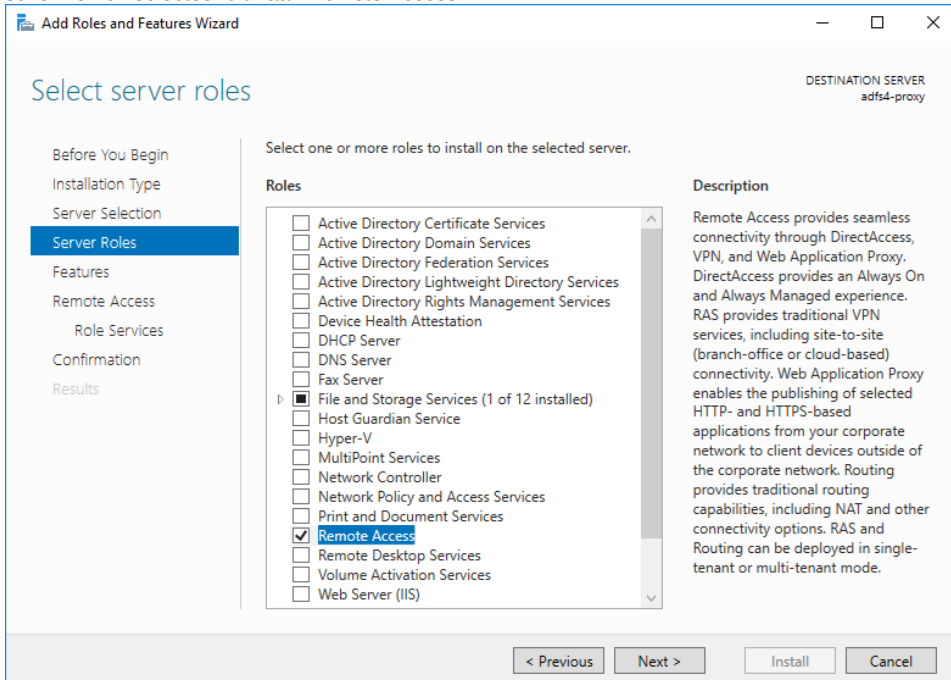
Let op: dit bestand is alleen als Administrator te bewerken. Start hiervoor een Notepad op onder "run as Administrator" conditie.

ADFS Proxy installeren

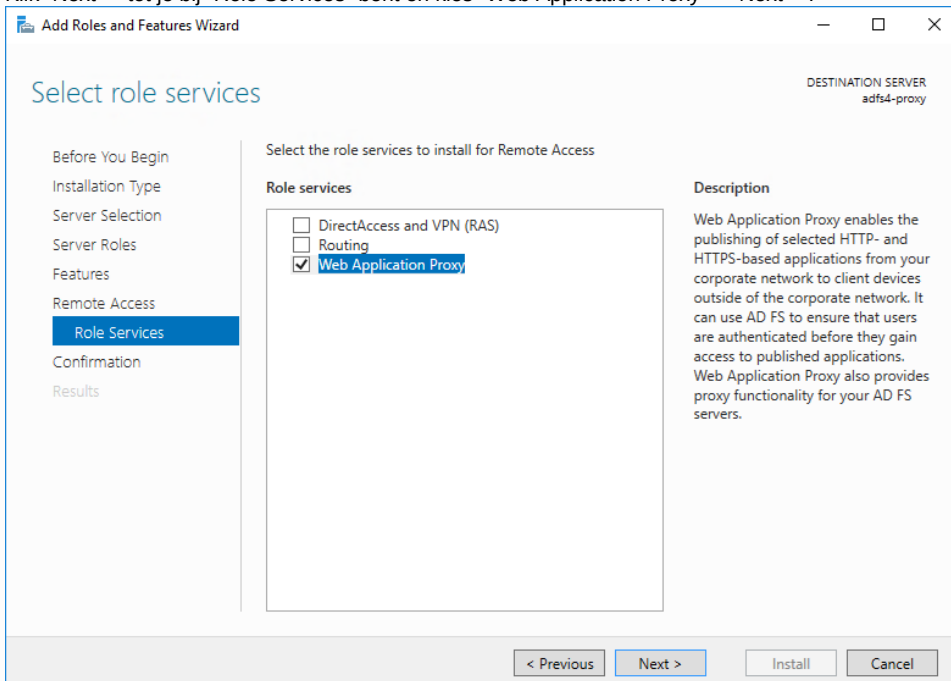
We gaan nu de ADFS Proxy installeren. Volg de stappen zoals hieronder aangegeven.

Stappenplan AD FS Proxy Installeren

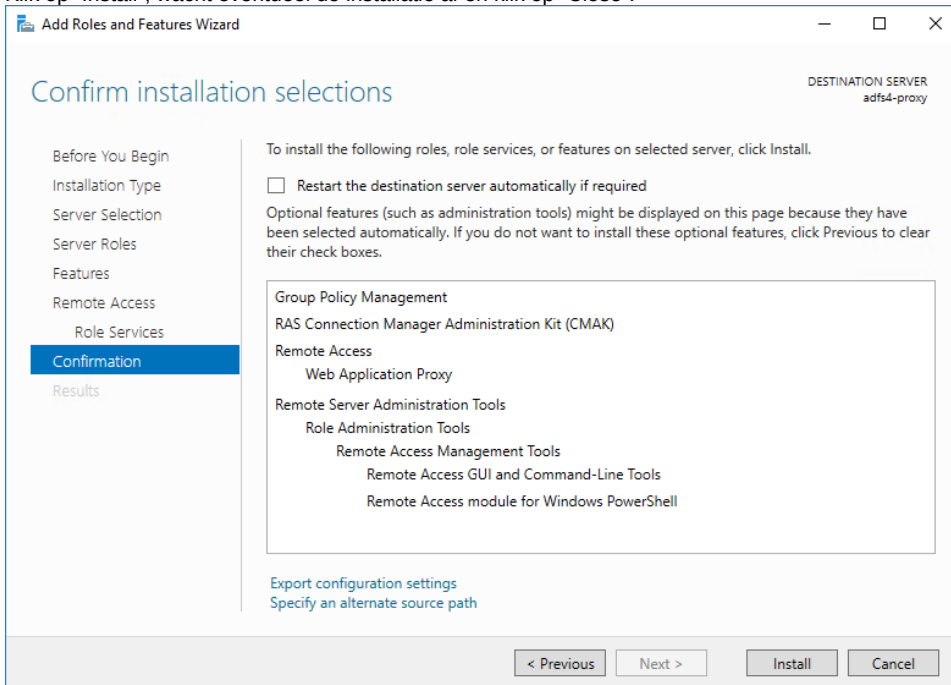
1. Kies in het Server Manager Dashboard weer voor "Add roles and features" en klik zoals hiervoor beschreven door de eerste schermen en selecteer ditmaal "Remote Access":



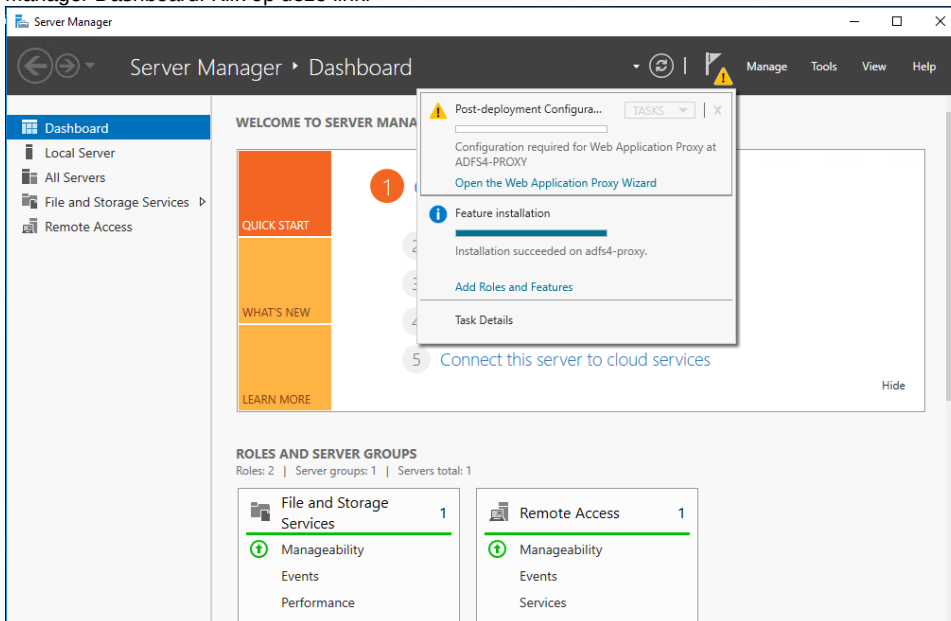
2. Klik "Next >" tot je bij "Role Services" bent en kies "Web Application Proxy" > "Next >":



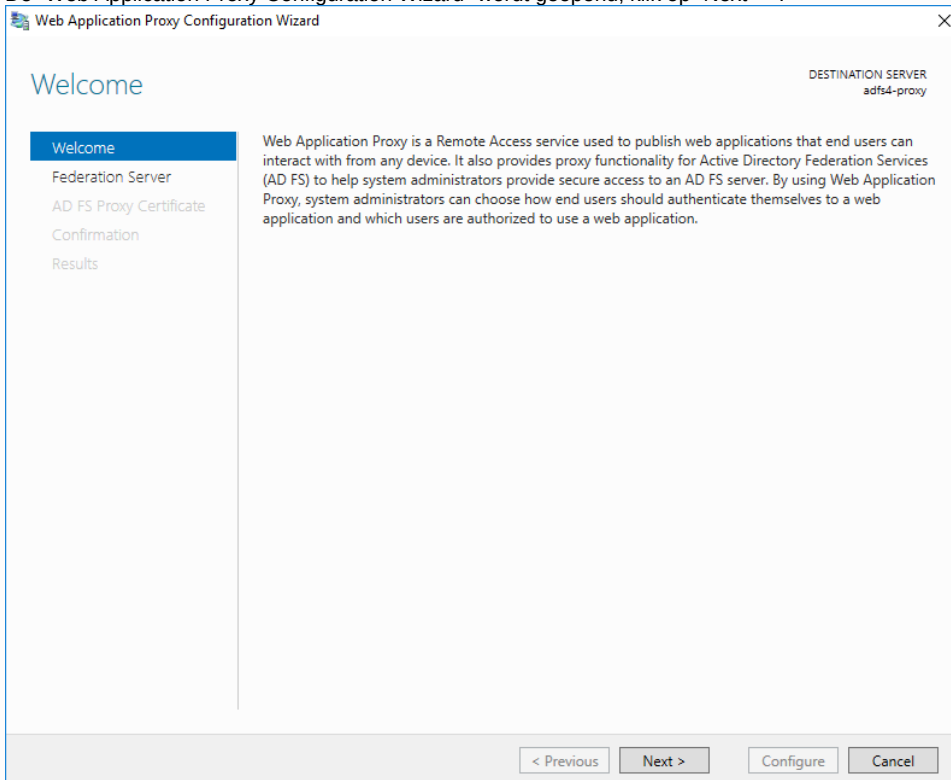
3. Klik op "Install", wacht eventueel de installatie af en klik op "Close":



4. De Proxy configuratie vereist een geldig en werkend SSL certificaat. 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".
5. Na installatie verschijnt een Post-deployment alert "Configuration required for the Federation Service Proxy at ..." in het Server Manager Dashboard. Klik op deze link:

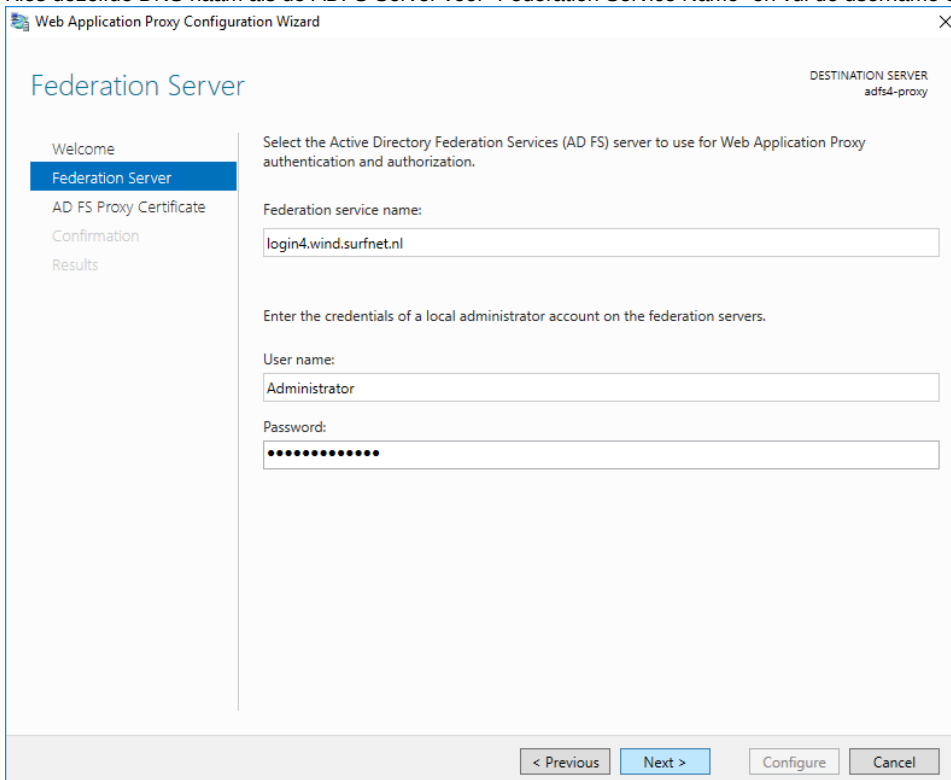


6. De "Web Application Proxy Configuration Wizard" wordt geopend, klik op "Next >":



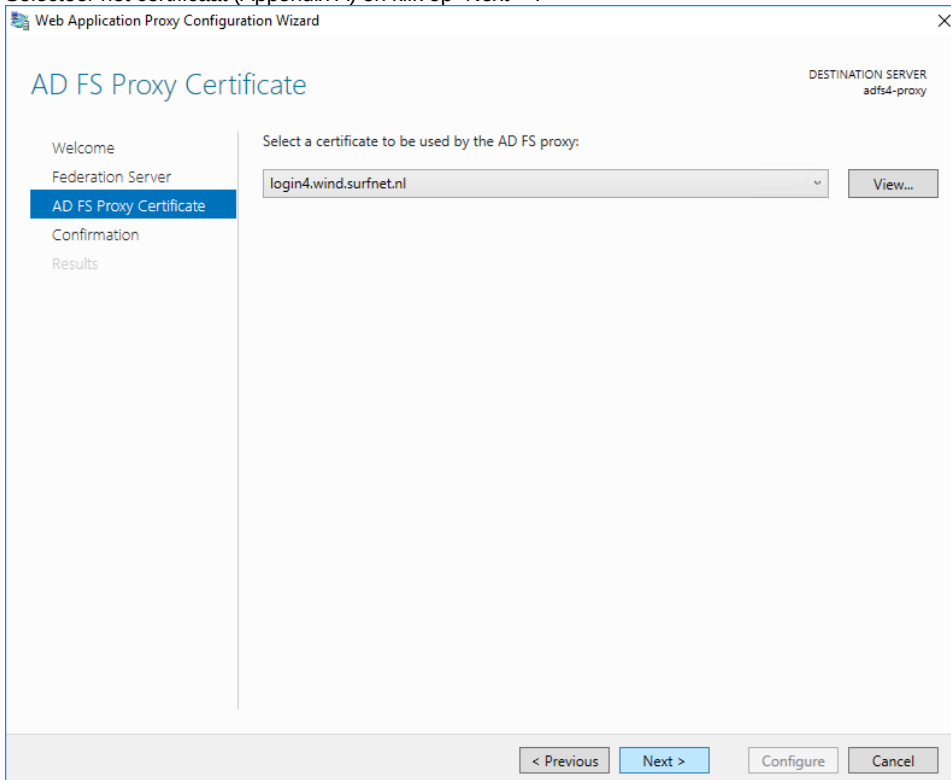
The screenshot shows the 'Welcome' screen of the 'Web Application Proxy Configuration Wizard'. The title bar reads 'Web Application Proxy Configuration Wizard'. On the left, a navigation pane lists 'Welcome' (selected), 'Federation Server', 'AD FS Proxy Certificate', 'Confirmation', and 'Results'. The main area has a heading 'Welcome' and a paragraph explaining that Web Application Proxy is a Remote Access service used to publish web applications. In the top right corner, it says 'DESTINATION SERVER adfs4-proxy'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

7. Kies dezelfde DNS naam als de ADFS Server voor "Federation Service Name" en vul de username en password in:

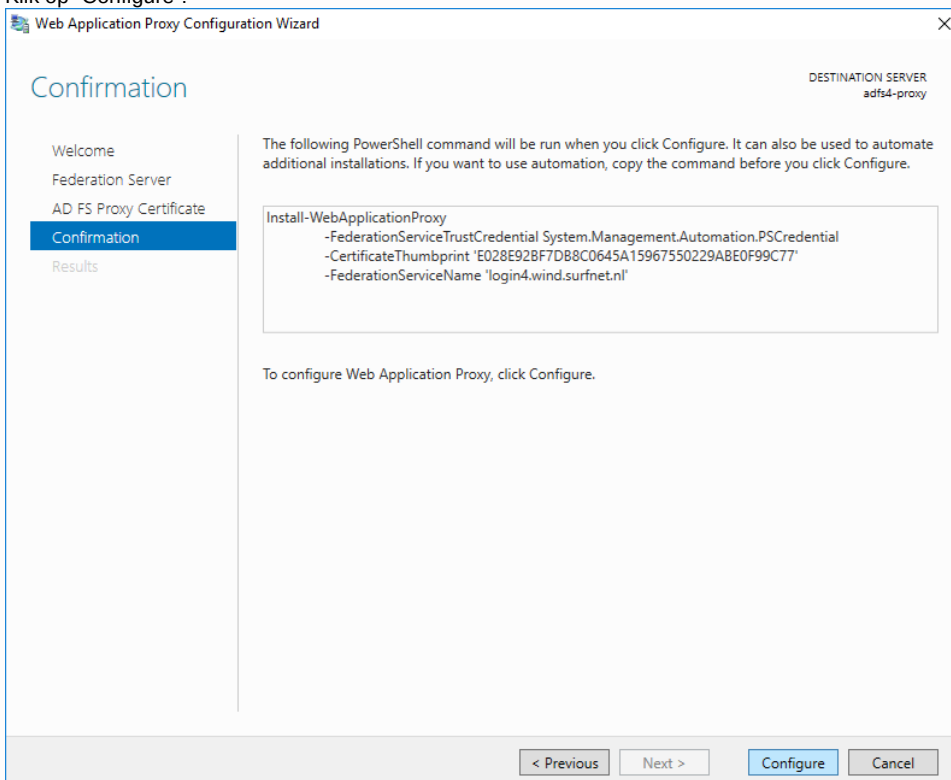


The screenshot shows the 'Federation Server' screen of the 'Web Application Proxy Configuration Wizard'. The title bar reads 'Web Application Proxy Configuration Wizard'. The navigation pane on the left now has 'Federation Server' selected. The main area has a heading 'Federation Server' and a paragraph: 'Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.' Below this, there is a text box for 'Federation service name:' containing 'login4.wind.surfnet.nl'. Further down, it says 'Enter the credentials of a local administrator account on the federation servers.' followed by text boxes for 'User name:' (containing 'Administrator') and 'Password:' (containing masked characters). The bottom buttons are '< Previous', 'Next >', 'Configure', and 'Cancel'.

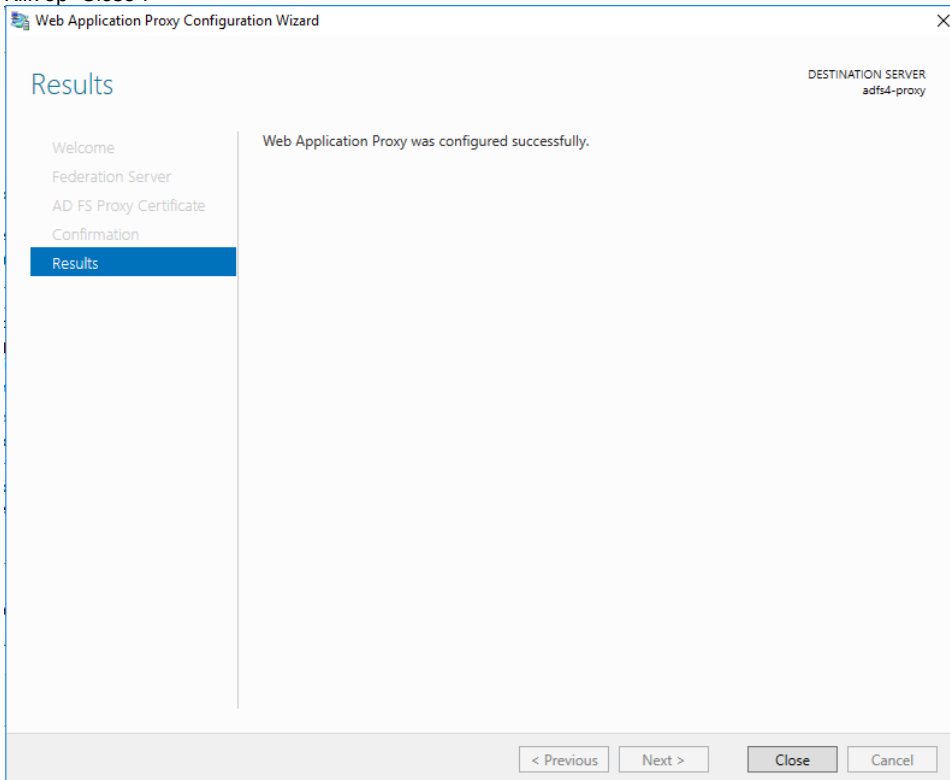
8. Selecteer het certificaat (Appendix A) en klik op "Next >":



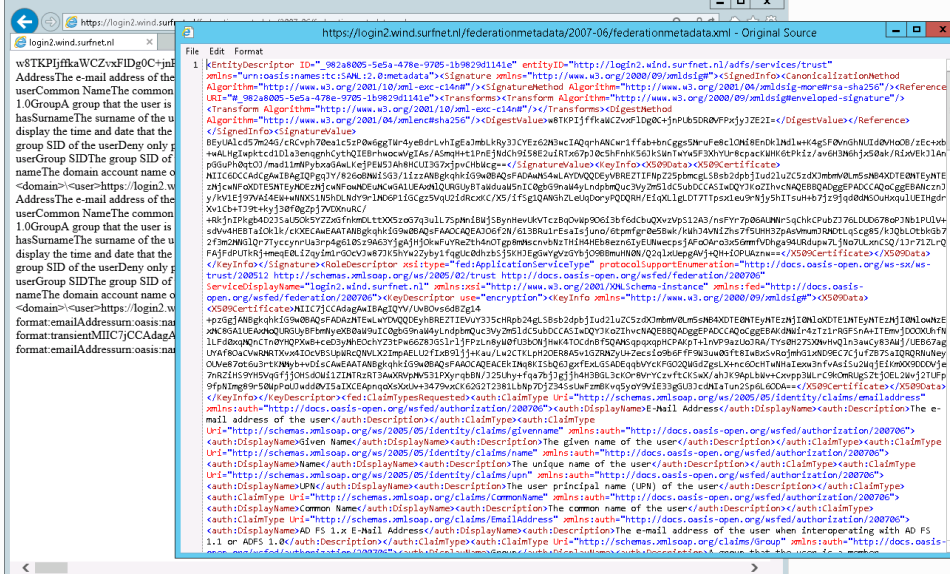
9. Klik op "Configure":



10. Klik op "Close":



11. Surf ter 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 hieronder 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



12. Als deze test slaagt kan de metadata URL aan SURFconext doorgegeven worden zoals beschreven in het hoofdstuk "Metadata doorgeven aan SURFconext".

⚠ 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.

Metadata doorgeven aan SURFconext

Als de ADFS server en ADFS Proxy of Web Application Proxy geïnstalleerd zijn en hun werking gecontroleerd kan de metadata URL doorgeven worden aan SURFconext. 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
```

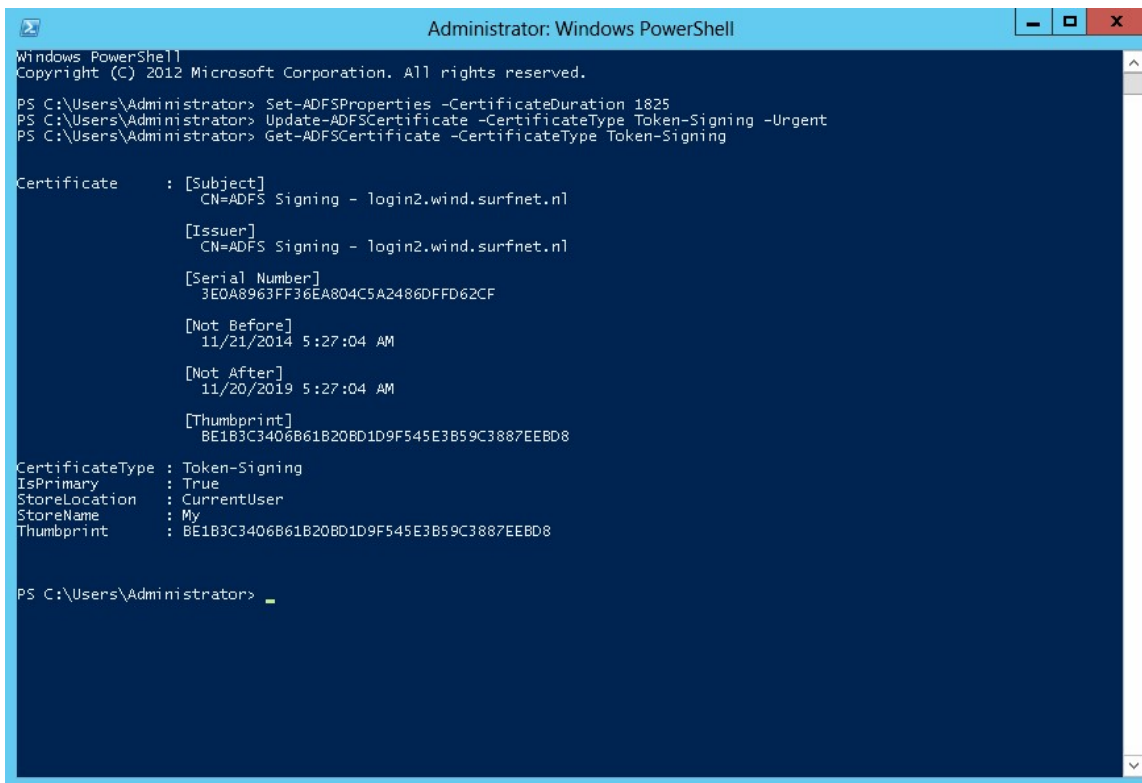
Als er nog geen andere Relying Party Trusts configuraties bestonden voor deze installatie:

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

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

En ter controle:

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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Set-ADFSProperties -CertificateDuration 1825
PS C:\Users\Administrator> Update-ADFSCertificate -CertificateType Token-Signing -Urgent
PS C:\Users\Administrator> Get-ADFSCertificate -CertificateType Token-Signing

Certificate       : [Subject]
                   CN=ADFS Signing - login2.wind.surfnet.nl
                   [Issuer]
                   CN=ADFS Signing - login2.wind.surfnet.nl
                   [Serial Number]
                   3E0A8963FF36EA804C5A2486DFFD62CF
                   [Not Before]
                   11/21/2014 5:27:04 AM
                   [Not After]
                   11/20/2019 5:27:04 AM
                   [Thumbprint]
                   BE1B3C3406B61B20BD1D9F545E3B59C3887EEBD8

CertificateType   : Token-Signing
IsPrimary         : True
StoreLocation     : CurrentUser
StoreName         : My
Thumbprint        : BE1B3C3406B61B20BD1D9F545E3B59C3887EEBD8

PS C:\Users\Administrator> _
```

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

Aanleveren Metadata

Vervolgens kan een mail naar SURFconext gestuurd worden (support@surfconext.nl) 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>. Het advies is om Appendix B door te nemen over openstaande poorten op de server.

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:

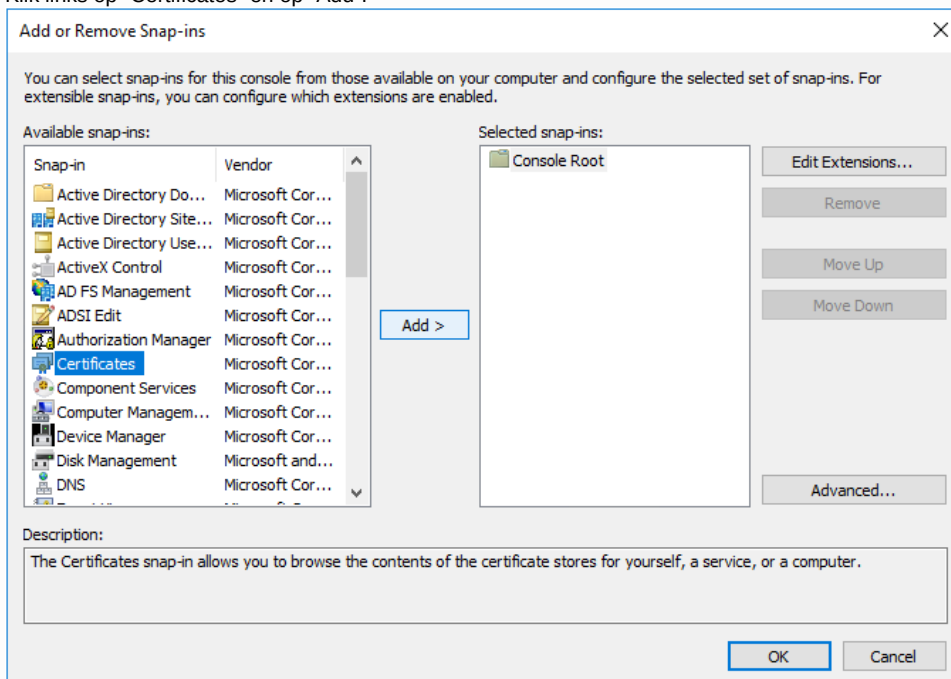
```
#openssl pkcs12 -export -passout pass:123welkom -in cert.pem -certfile chain.pem -inkey cert.key -out cert.pfx
```

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

Volg het stappenplan zoals hieronder aangegeven.

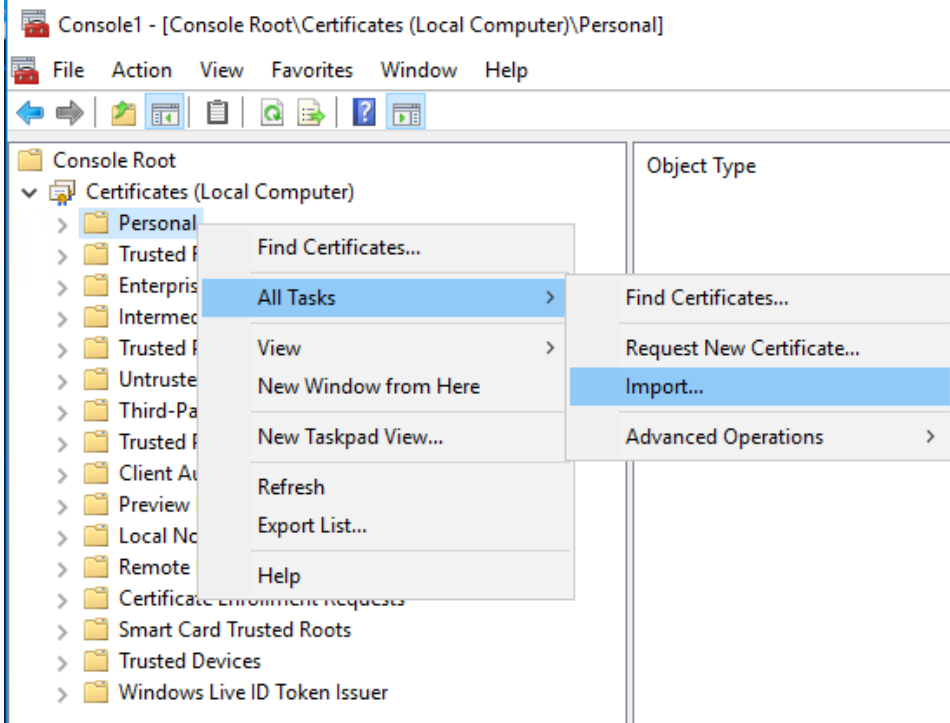
Stappenplan Certificaat Installeren

1. Open MMC in het start menu.
2. Ga naar "File" -> "Add/Remove Snap-in".
3. Klik links op "Certificates" en op "Add".

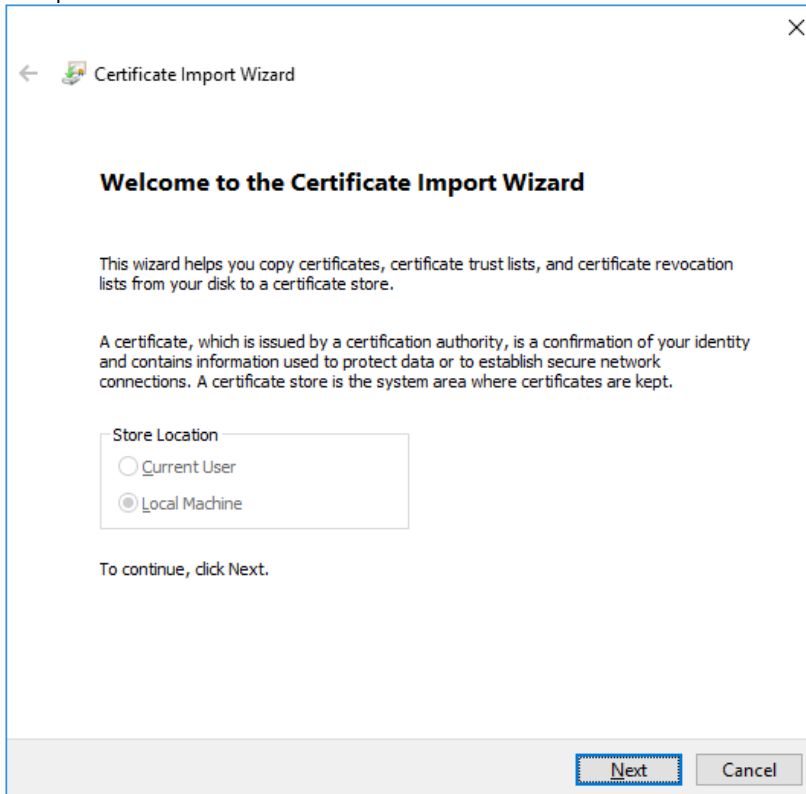


4. Kies voor "Computer account" en klik op "Next".
5. Klik op "Finish".
6. En klik op "OK".

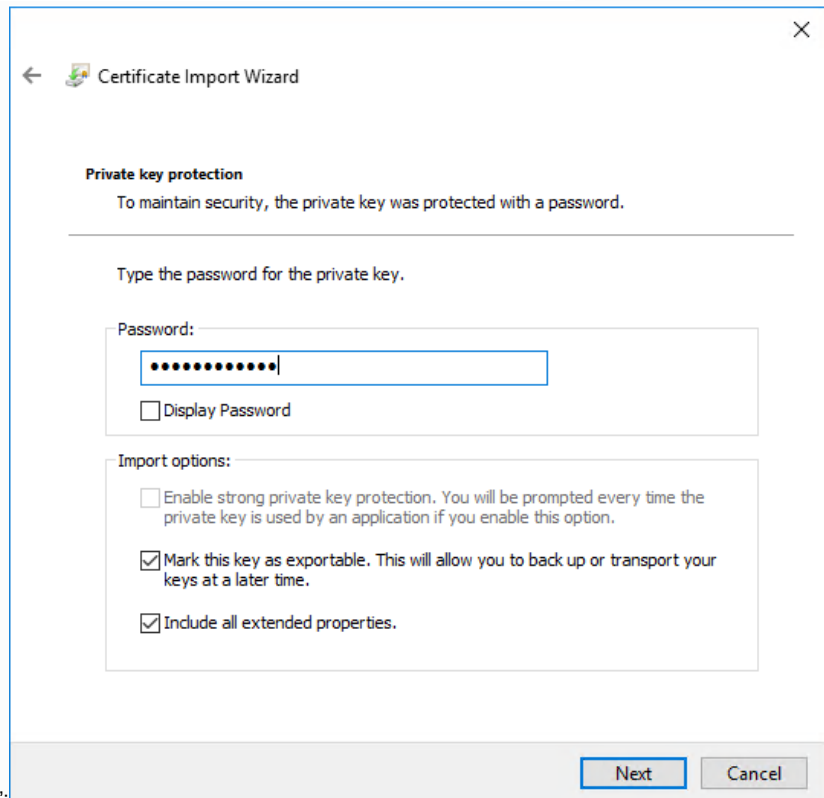
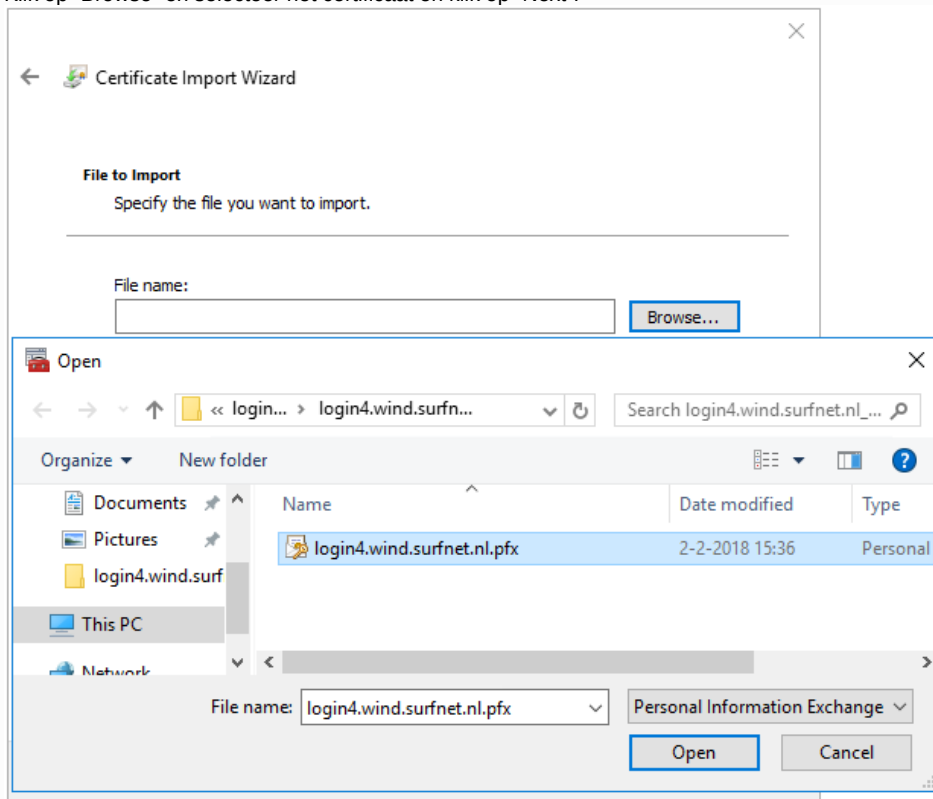
7. Klik rechts op "Personal" -> "All Tasks" -> "Import...":



8. Klik op "Next":

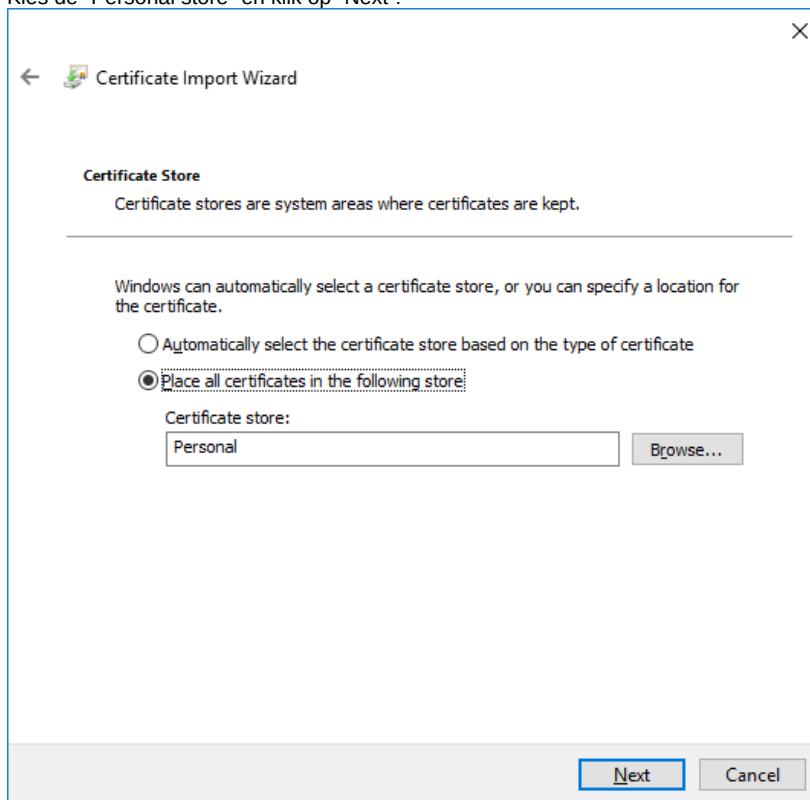


9. Klik op "Browse" en selecteer het certificaat en klik op "Next":

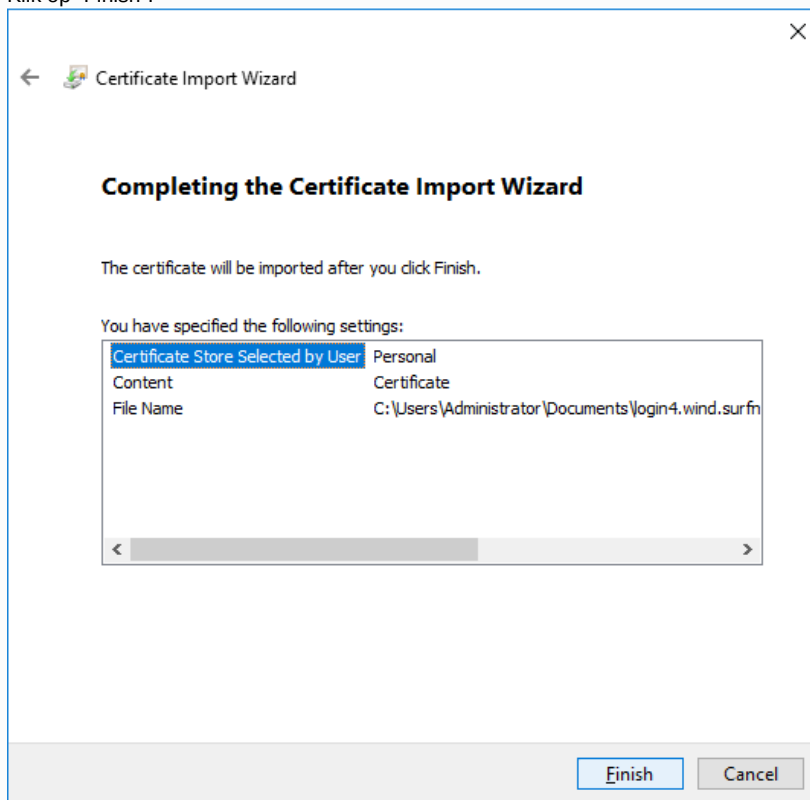


10. Vul het wachtwoord in en klik op "Next":

11. Kies de "Personal store" en klik op "Next":



12. Klik op "Finish":



13. Klik op "OK" als aangegeven wordt dat de import succesvol is.
14. 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.

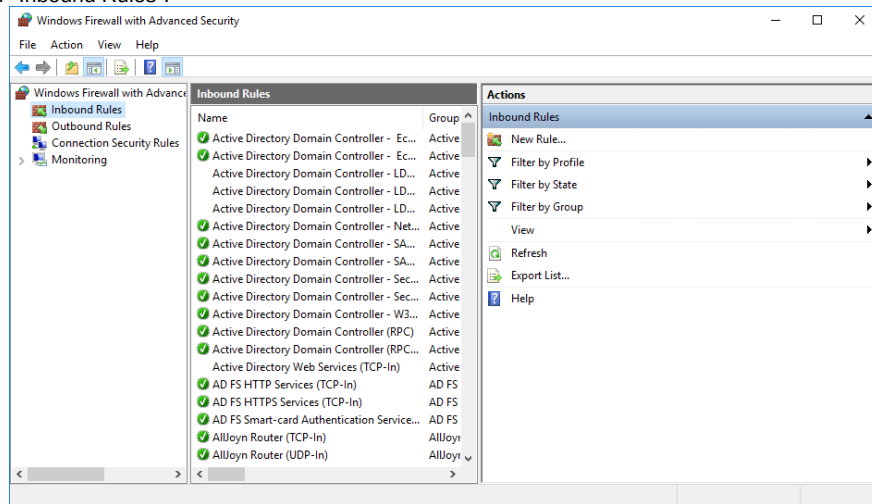
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
login4.wind.surfnet.nl	TERENA SSL CA 3	17-11-2020	Server Authenticati...	<None>		

Appendix B Poorten dichtzetten

Om verkeerd gebruik van je proxy te voorkomen kun je Outbound en Inbound regels definiëren. Doorloop onderstaande stappen en maak aanpassingen waar nodig om poorten dicht te zetten of regels te definiëren.

Firewall en poortconfiguraties

1. Ga naar de ADFS server
2. Open "Windows Firewall".
3. Ga naar "Inbound Rules":



- a. Disable de volgende regels:
 - a. Active Directory Domain Controller - LDAP (TCP-In)
 - b. Active Directory Domain Controller - LDAP (UDP-In)
 - c. Active Directory Domain Controller - LDAP for Global Catalog (UDP-In)
 - d. Active Directory Web Services (TCP-In)
 - e. DNS (TCP, Incoming)
 - f. DNS (UDP, Incoming)
5. Ga naar Outbound rules en disable de volgende regels:
 - a. Xbox Game UI
 6. Ga nu naar de ADFS Proxy en open daar ook Windows Firewall
 7. Ga naar Outbound rules en disable de volgende regels:
 - a. Xbox Game UI