UCCE\PCCE - procedure voor het verkrijgen en uploaden van Windows-serverzelf-ondertekend of CA-certificaat (certificaatautoriteit) op 2008-servers

Inhoud

Inleiding

Dit document beschrijft hoe u zelfgetekende of een certificaat van de Autoriteit (CA) kunt configureren op Unified Contact Center Enterprise (UCCE) Windows 2008 R2-servers.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van het proces van het ondertekende en zelfondertekende certificaat.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Windows 2008 R2
- UCS E10.5(1)

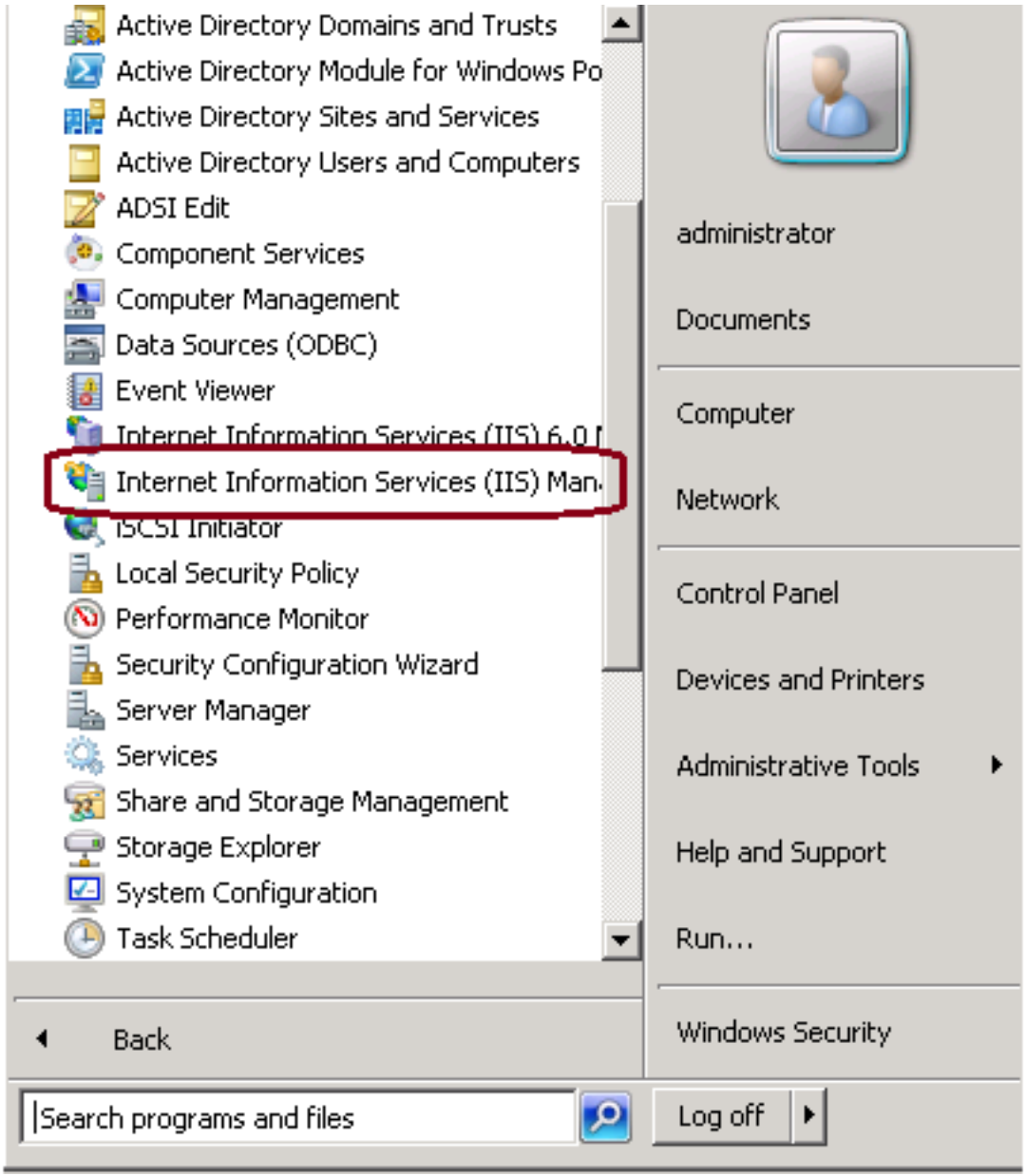
Configureren

Het instellen van een certificaat voor HTTPS-communicatie op Windows-server is een proces dat drie stappen omvat

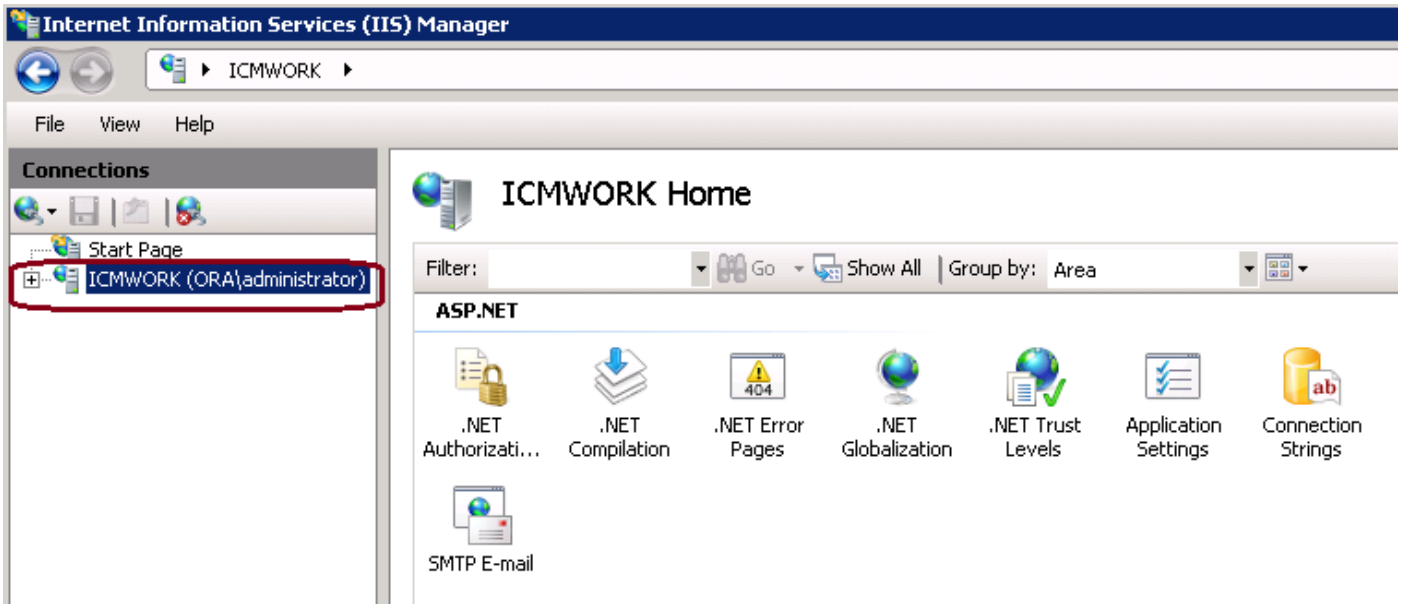
- CSR (certificaataanvraag) genereren via Internet Information Services (IS) Manager
- Upload het CA-ondertekend certificaat naar Internet Information Services (IS) Manager
- Bind het ondertekende CA-certificaat op de Standaardwebsite

Stap 1. Generate CSR van Internet Information Services (IS) Manager

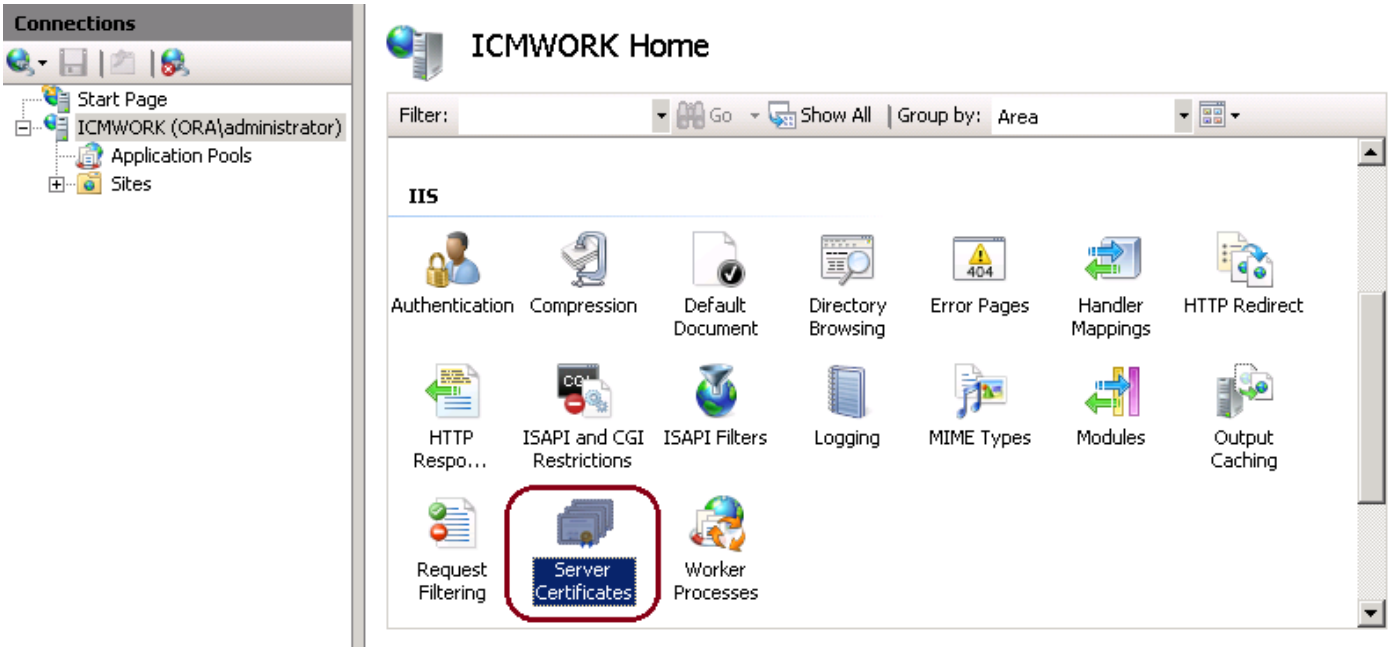
1. Meld u aan bij Windows en klik op **Start > Start > Alle programma's > Administratieve tools > Internet Information Services (IS) Manager**, zoals in deze afbeelding. Selecteer geen IS versie 6 als deze bestaat.



2. Selecteer in het venster Connections links de servernaam, zoals in deze afbeelding.

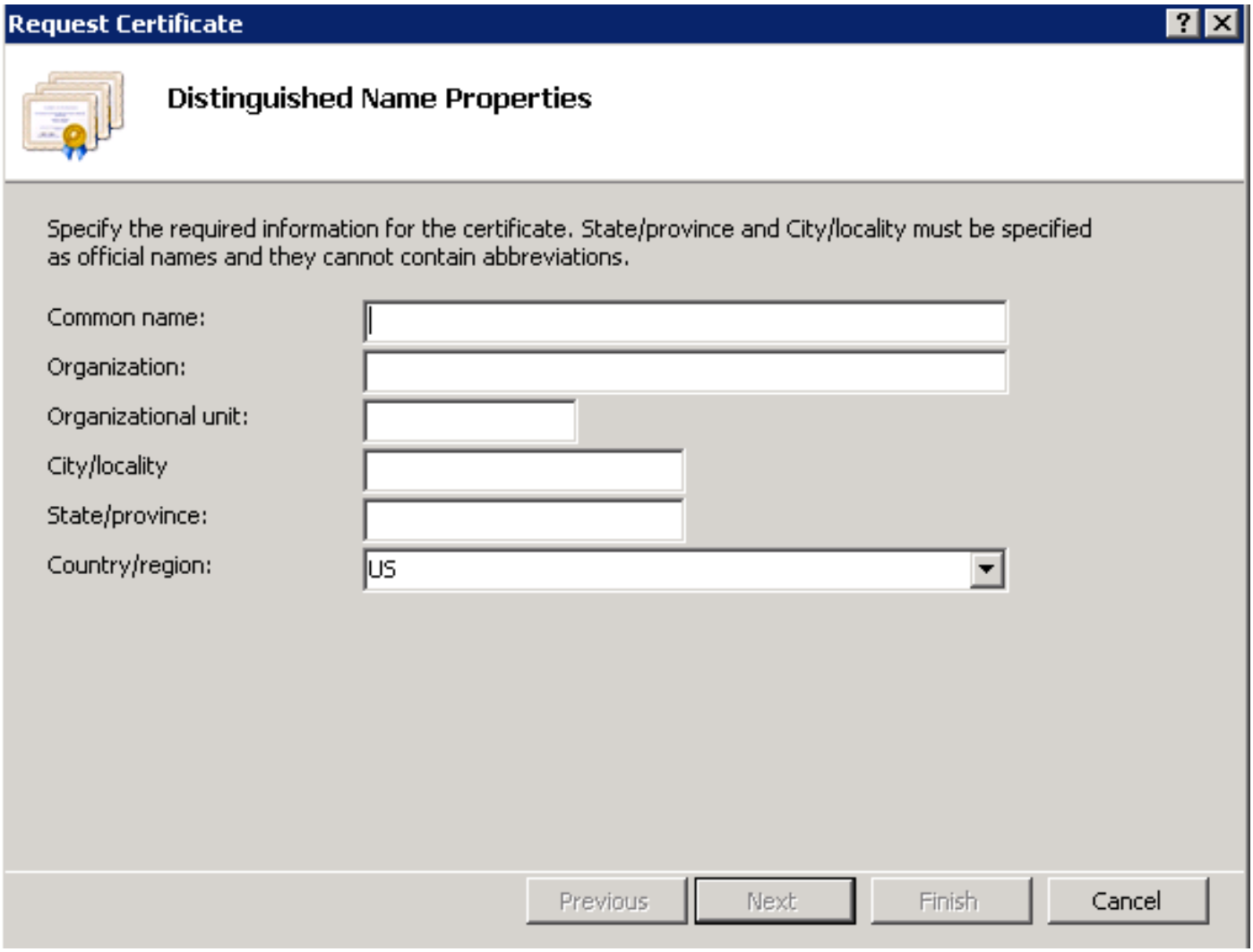


3. Selecteer in het middenvenster de optie **IS > Server Certificates**. Dubbelklik op Server-certificaten om het certificaatvenster te genereren, zoals in deze afbeelding wordt weergegeven.

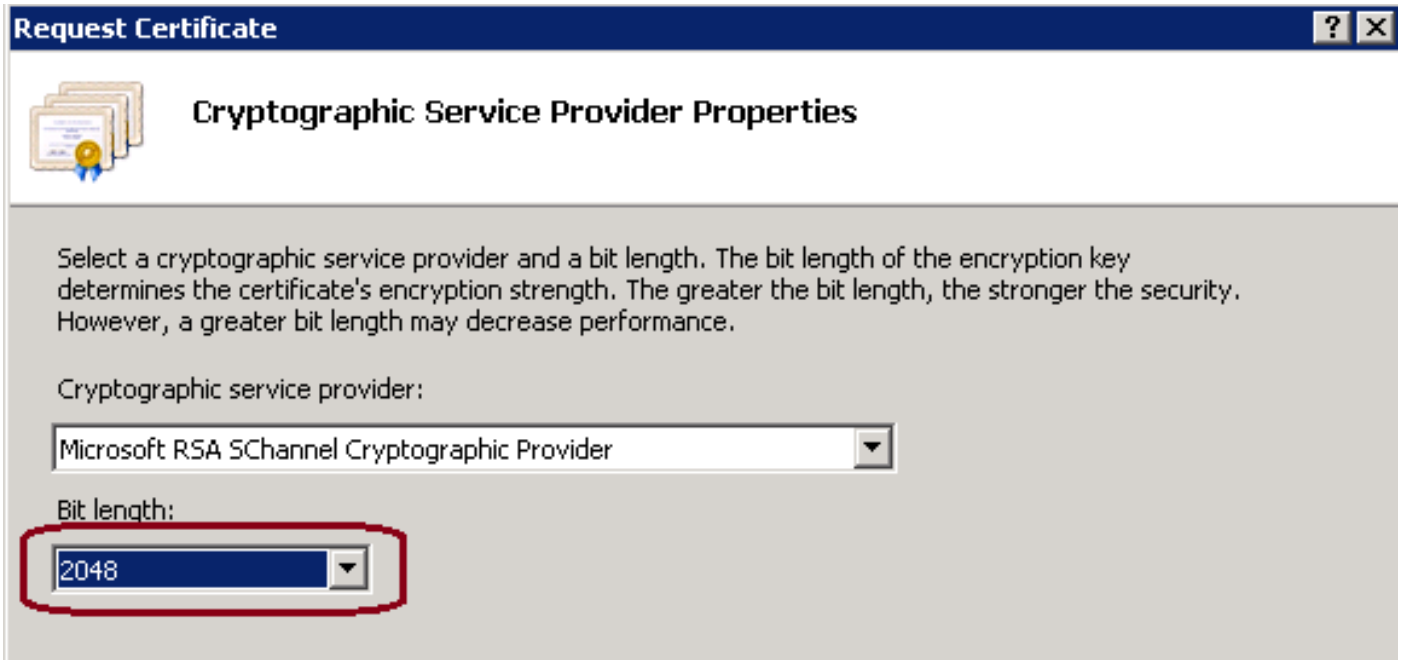


4. Klik in het rechtervenster op **Acties > certificaataanvraag maken** zoals in deze afbeelding.

5. Om het certificaatverzoek in te vullen, vermeld de gemeenschappelijke naam, organisatie, organisatie-eenheid, stad/plaats, staat/provincie en land/regio, zoals in deze afbeelding aangegeven.



6. Klik op Next om de cryptografische en beveiligingsbit length te wijzigen, en wordt aanbevolen om ten minste 2048 te gebruiken voor een betere beveiliging, zoals in deze afbeelding wordt getoond.

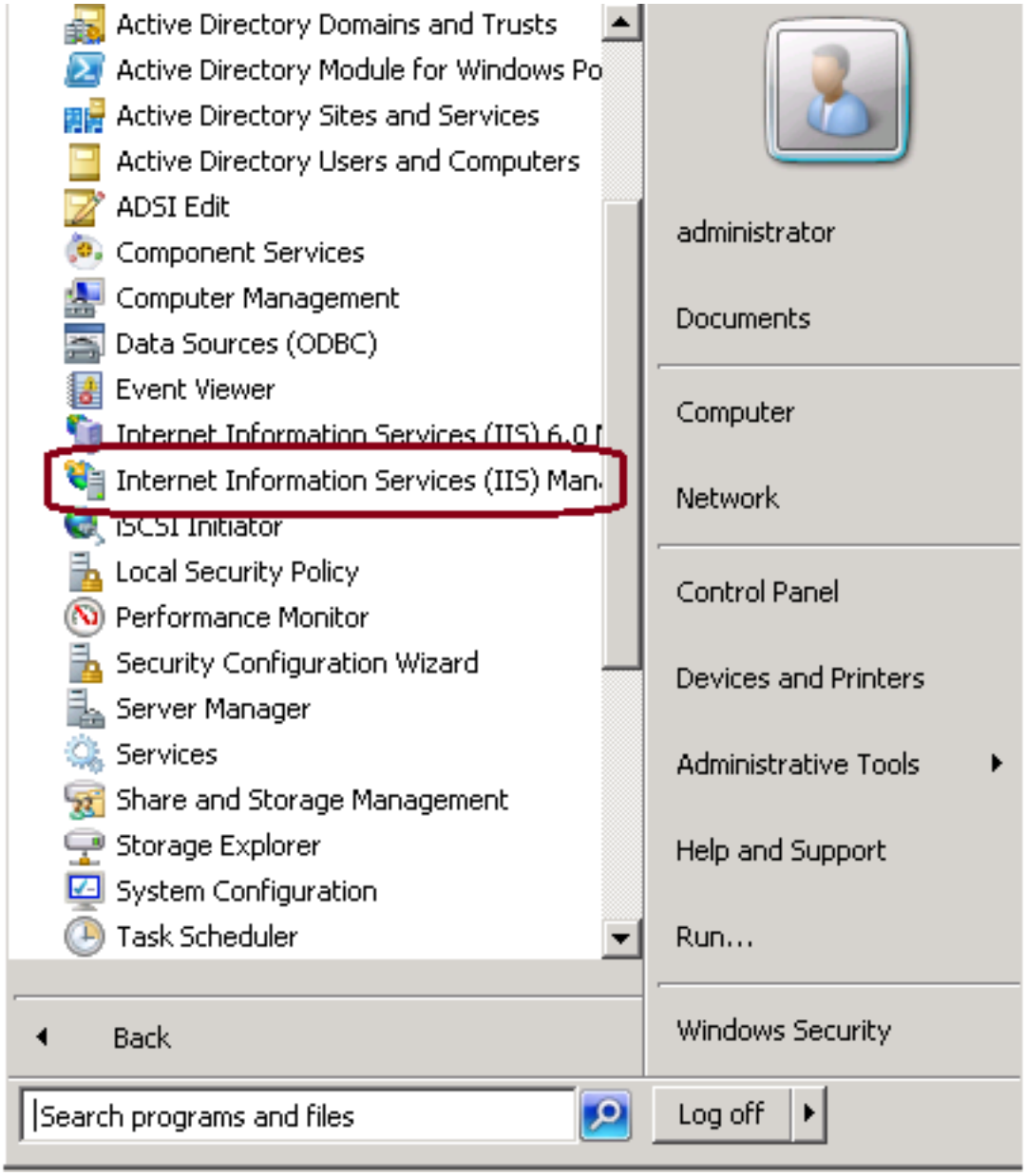


7. Sla de certificaataanvraag op de gewenste locatie op, die als een .TXT-indeling wordt opgeslagen, zoals in deze afbeelding.

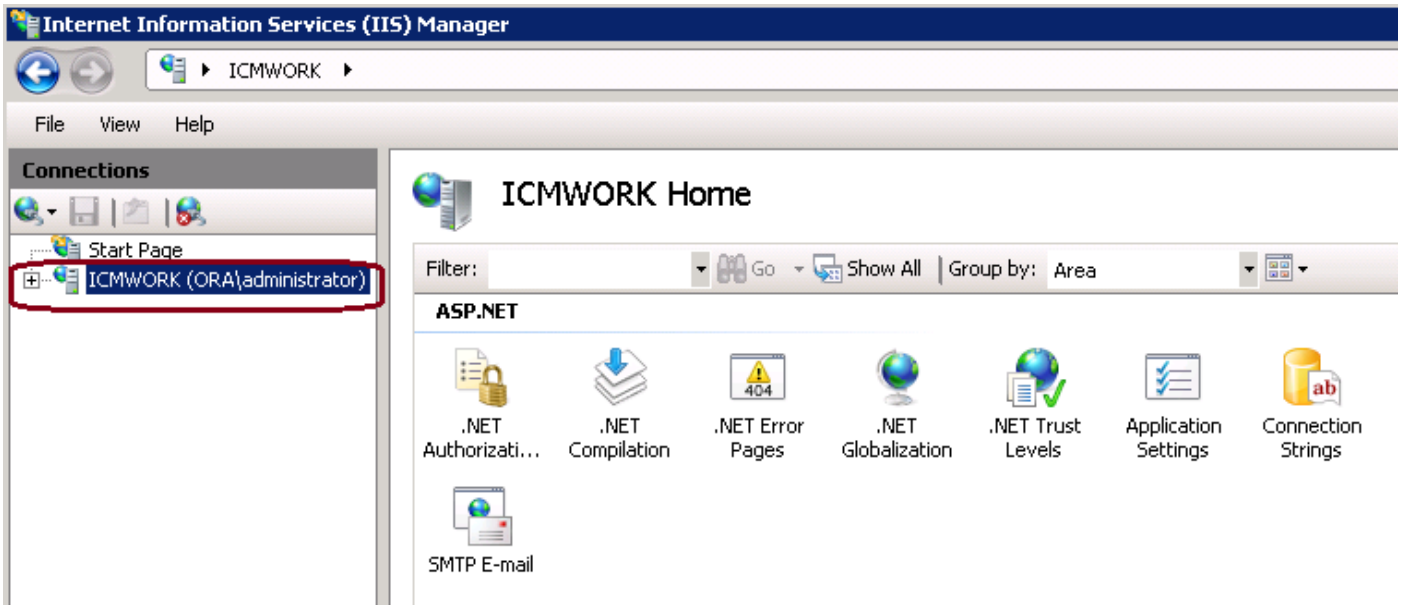
8. Geef dit bestand op dat moet worden getekend door het team dat het interne CA- of externe CA-serviceverzoek beheert, zoals in deze afbeelding.

Stap 2. Upload het CA-ondertekende certificaat naar Internet Information Services (IS) Manager

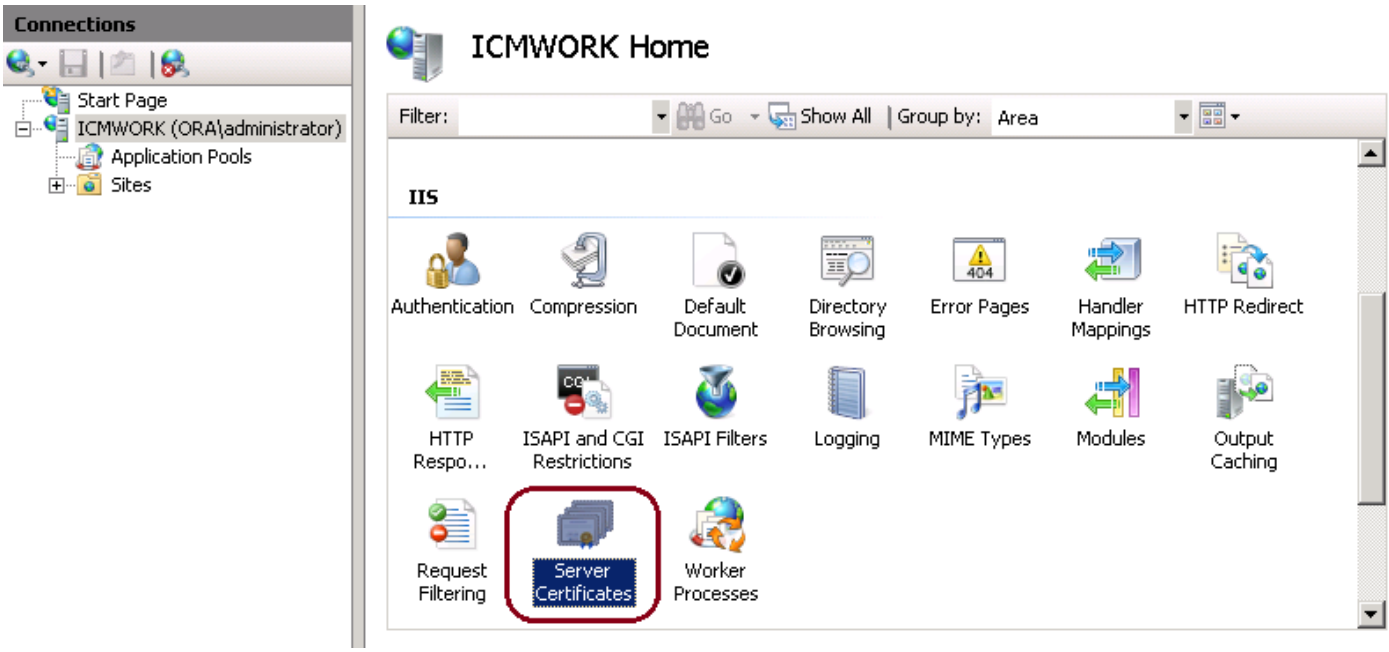
1. Meld u aan bij Windows en klik op **Start > Start > Alle programma's > Administratieve tools > Internet Information Services (IS) Manager,** zoals in deze afbeelding wordt getoond. Selecteer geen IS versie 6 als deze bestaat.



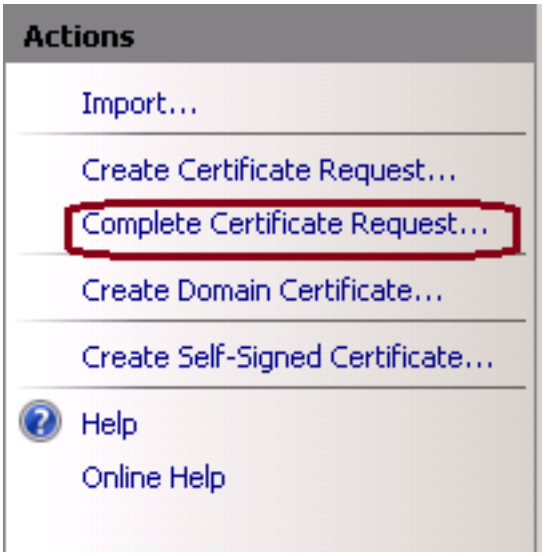
2. Selecteer in het venster Connections links de servernaam, zoals in deze afbeelding.



3. Selecteer in het middenvenster de optie **IS > Server Certificates**. Dubbelklik op Server Certificaten om het certificaatvenster te genereren, zoals in deze afbeelding wordt weergegeven.

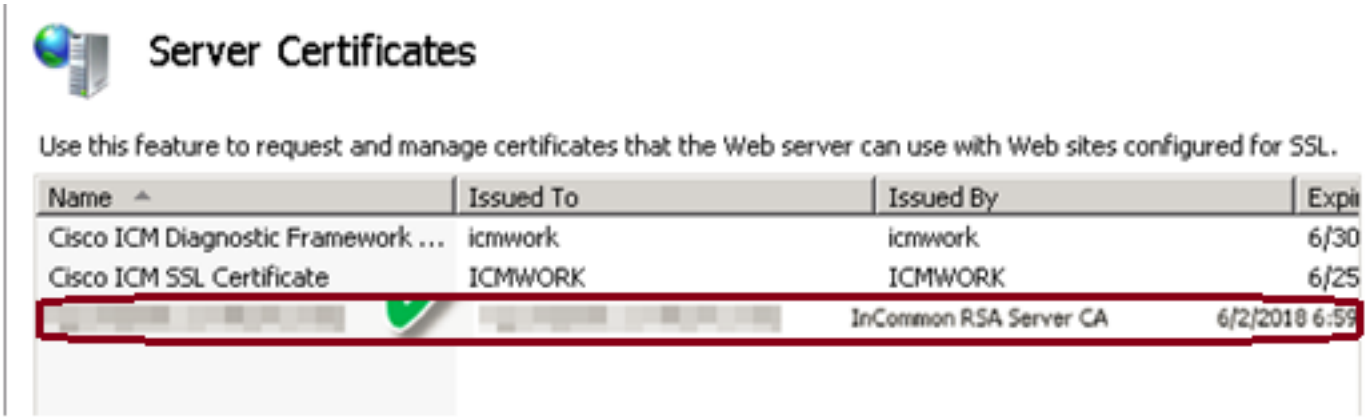


4. Klik in het rechtervenster op **Acties > Complete certificaataanvraag**, zoals in deze afbeelding weergegeven.



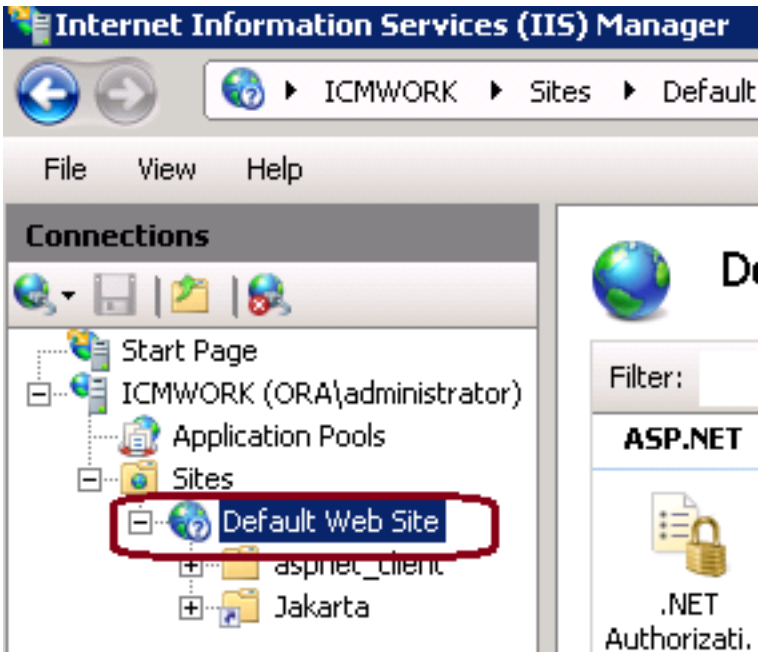
5. Zorg ervoor dat het ondertekende certificaat in .CER-indeling is en aan de lokale server is geüpload. Klik op de knop ... om door het .CER-bestand te bladeren. In de Vriendelijke naam, gebruik FQDN van de server, zoals getoond in deze afbeelding.

6. Klik op OK om het certificaat te uploaden. Na voltooiing, bevestig het certificaat nu in het venster Server Certificates, zoals in deze afbeelding weergegeven.

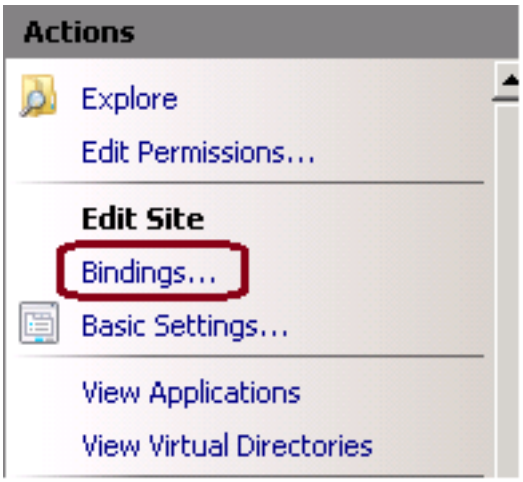


Stap 3. Bind het ondertekende CA-certificaat aan de standaardwebsite

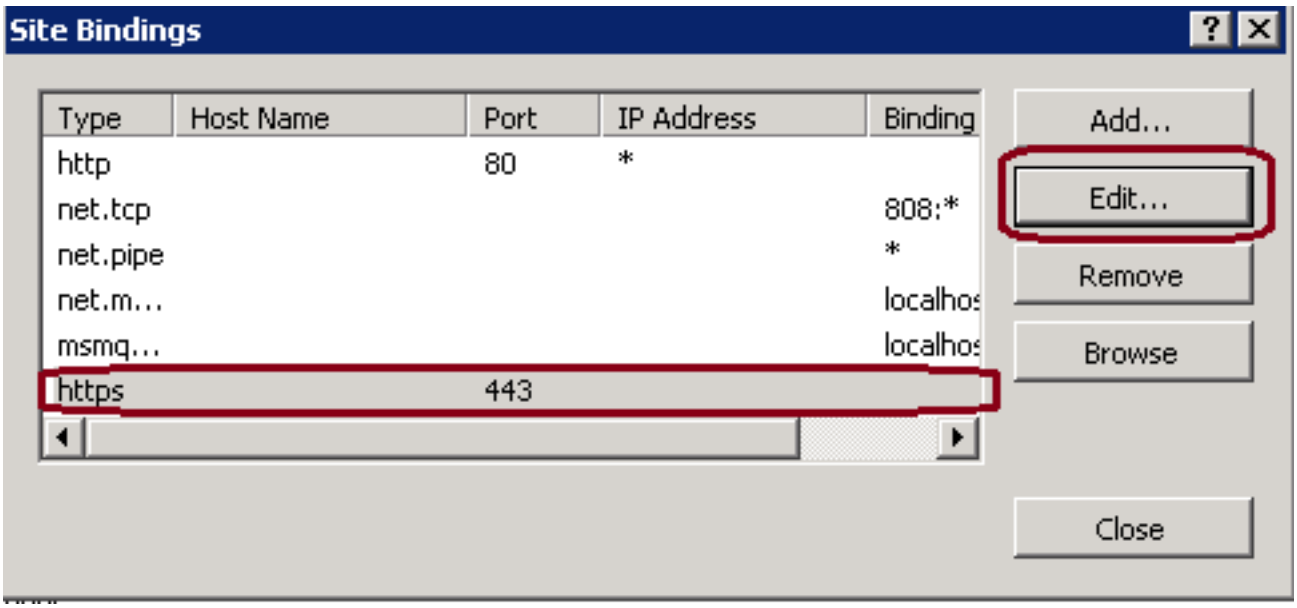
1. In het vliegtuig van het venster Connections Manager, klik met de linkerhand op de **<server_name> Plaatsen > Standaardwebsite**, zoals in deze afbeelding wordt getoond.



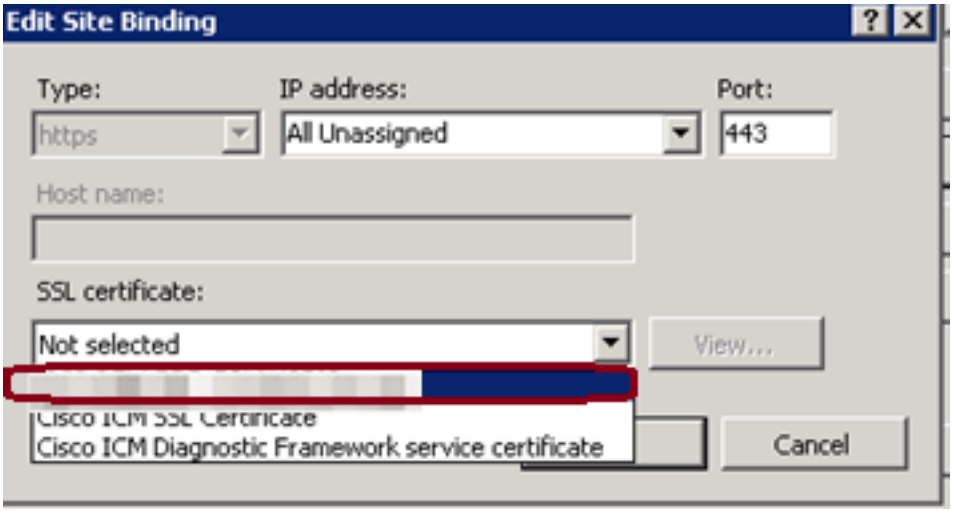
2. Klik in het deelvenster Handelingen aan de rechterkant op Bindingen, zoals in deze afbeelding.



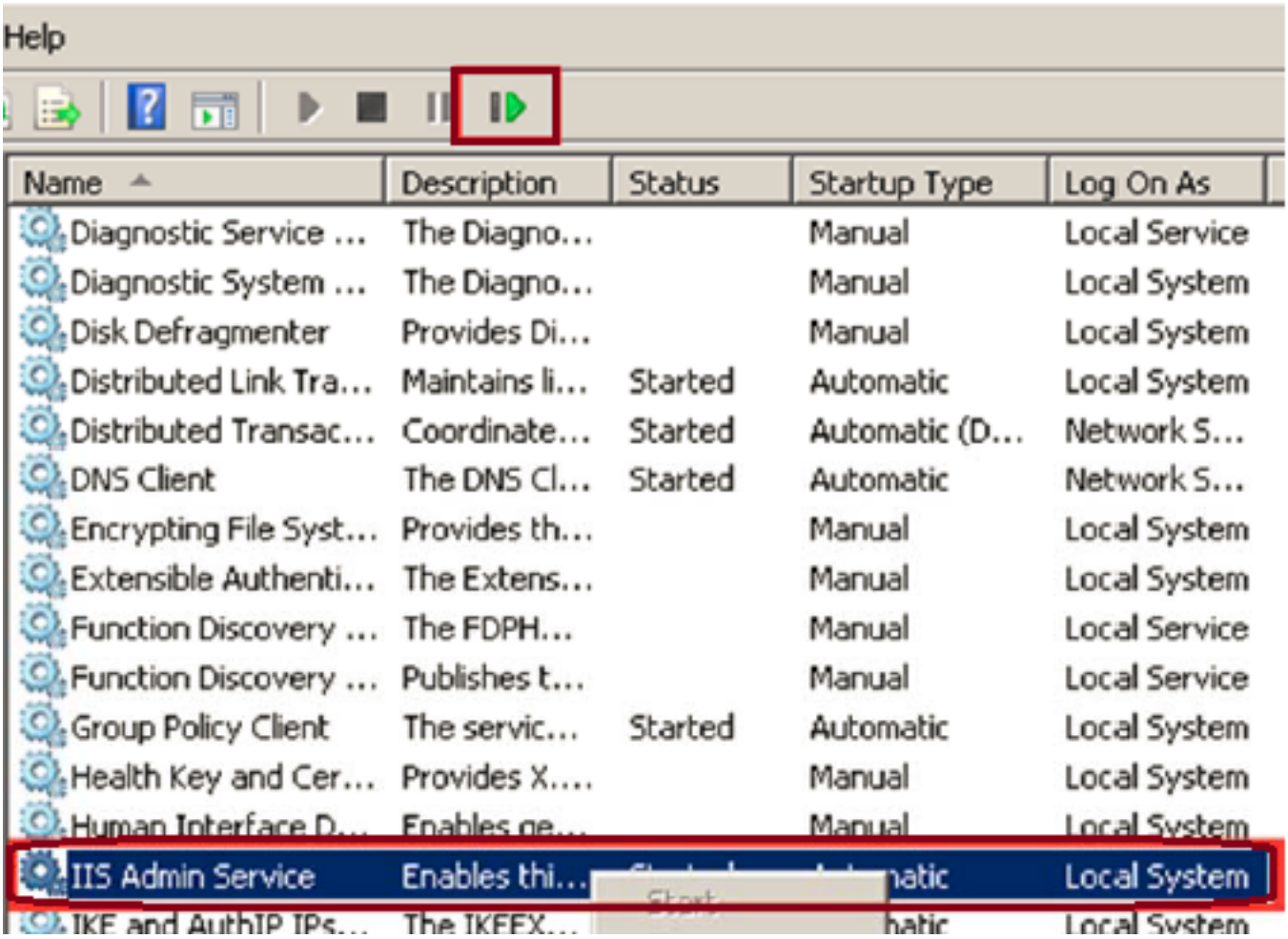
3. Klik in het venster Site bindings op https om meer opties te markeren. Klik op Bewerken om verder te gaan, zoals in deze afbeelding.



4. Klik onder de SSL certificaatparameter op het pijltje onder in om het eerder geüpload Gesigneerde certificaat te selecteren. Bekijk het ondertekende certificaat om het certificeringspad en de waarden die overeenkomen met de lokale server te controleren. Na voltooiing druk op OK, dan sluit u af om uit het venster Site Bindings, zoals in deze afbeelding weergegeven.



5. Start de IIS Admin Service opnieuw onder de CZS MCS-module door op **Start > Run > Services.msc.** te klikken, zoals in deze afbeelding wordt getoond.



6. Indien geslaagd, zou de client web browser geen certificaatfout moeten veroorzaken wanneer zij de FQDN URL voor de website invoert.

> Opmerking: Als de IIS Admin Service niet is voltooid, levert u de World Wide Web Publishing Service op.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Over deze vertaling

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