HTTPS Access voor UCCE Diagnostic Framework Protocol met certificaatautoriteit (CA) - ondertekend certificaat configureren

Inhoud

Inleiding

Dit document beschrijft het configuratieproces voor het installeren van CA-ondertekend certificaat voor Unified Contact Center Enterprise (UCCE) Diagnostic Framework Protocol.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Actieve map
- Domain Name System (DNS)-server
- Uitgebreide CA-infrastructuur voor alle servers en klanten
- Diagnostisch framework Portico

Het gebruik van het diagnostische Kader van het Portico-instrument door het IP-adres in de browser te typen zonder een certificaatwaarschuwing te ontvangen, valt buiten het toepassingsgebied van dit artikel.

Gebruikte componenten

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

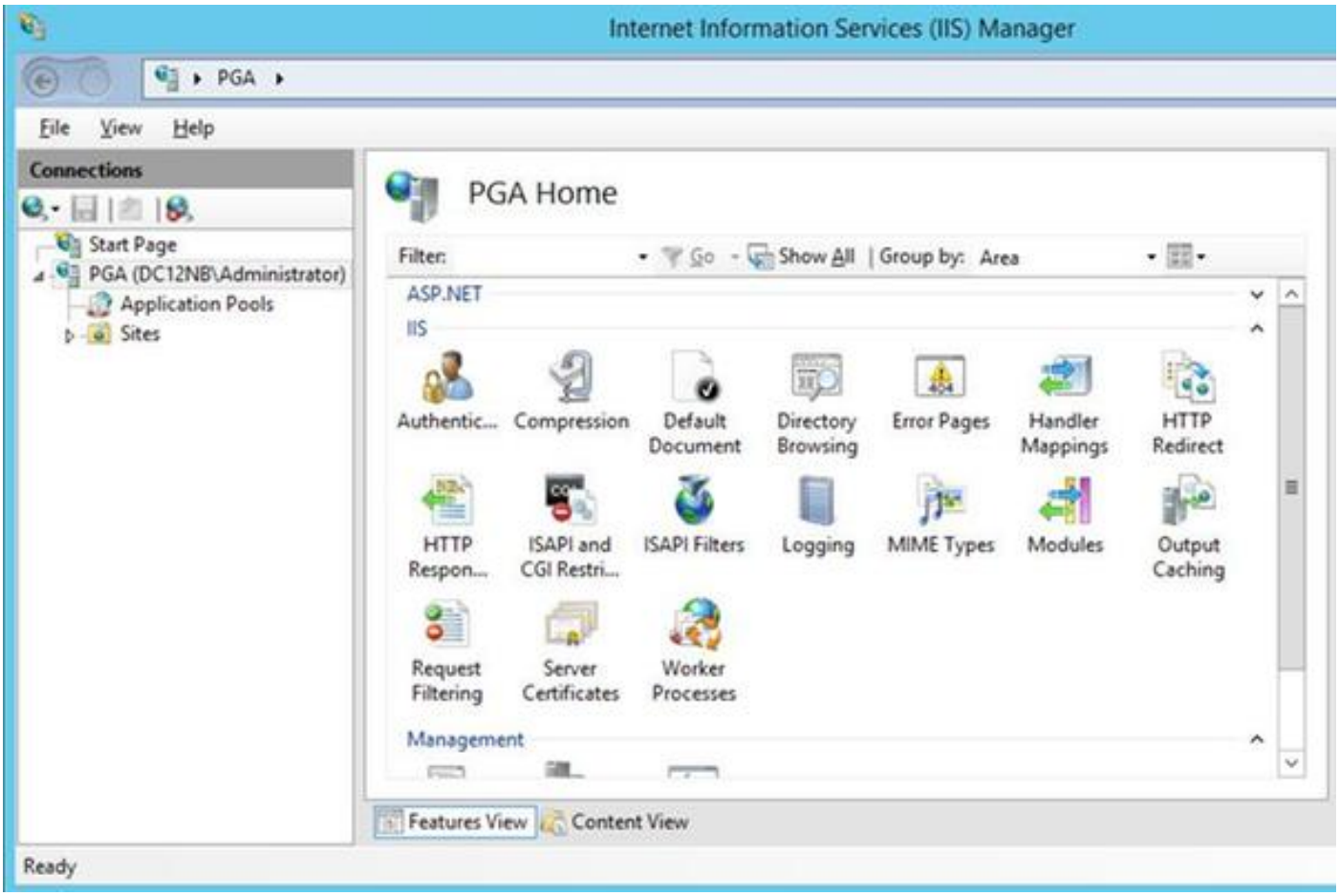
- Cisco UCS E11.0.1
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2-certificeringsinstantie
- Microsoft Windows 7 SP1-OS

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

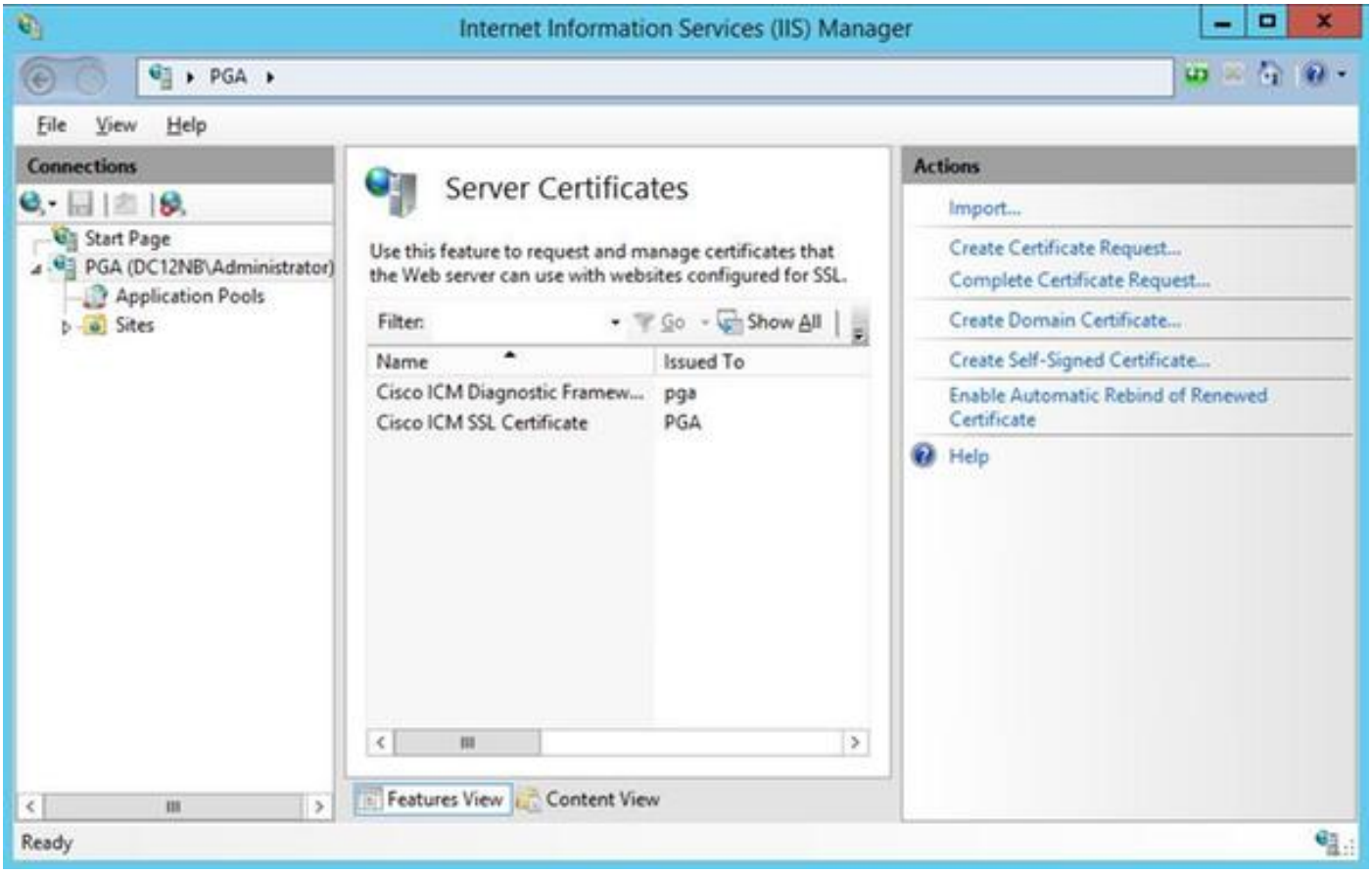
Configureren

certificaataanvraag genereren

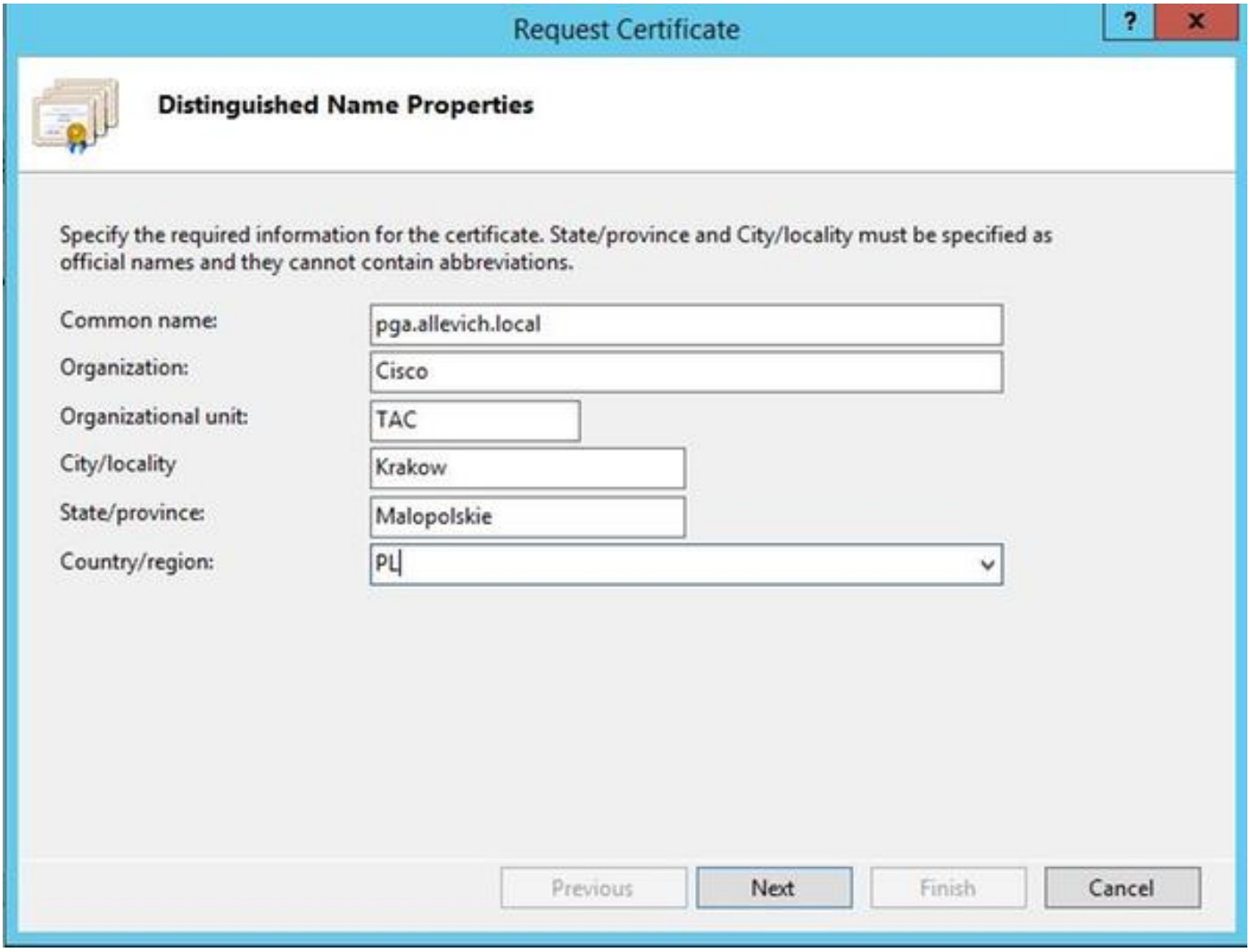
Open Internet Information Services (IS) Manager, selecteer uw site, Perifere Gateway A (PGA) in het voorbeeld en **Server Certificates**.



Selecteer **certificaataanvraag maken** in het deelvenster Handelingen.



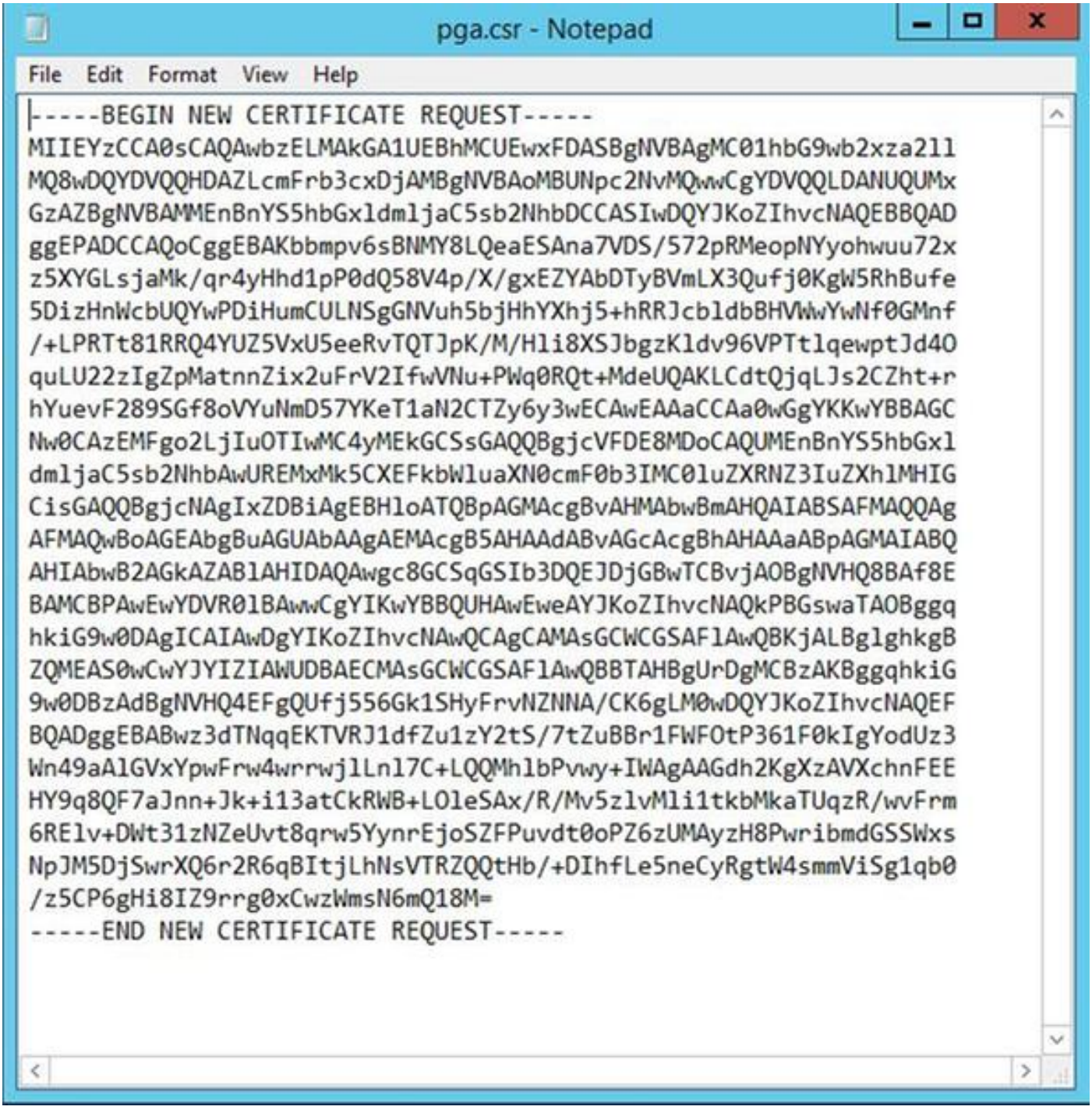
Vul de **gewone benaming** (CN), **Organisatie** (O), **Organisatie-eenheid** (OU), **Locality** (L), **Land (ST) en Land (C) velden in.** De gezamenlijke naam moet dezelfde zijn als uw FQDN-hostname (Full Qualified Domain Name) + domeinnaam.



Laat standaardinstellingen voor cryptografische serviceproviders en specificeer de lengte van het bit: 2048.

Selecteer pad waar u het wilt opslaan. Bijvoorbeeld op het bureaublad met de naam pga.csr.

Open nieuw aangemaakt verzoek in de notitieblok.



Kopieer het certificaat naar de buffer met CTRL+C.

Onderteken het certificaat op de certificaatinstantie

> Opmerking: Als u externe certificeringsinstanties gebruikt (zoals GoDaddy) moet u contact met hen opnemen nadat u een CSR-bestand hebt gegenereerd.

Meld u aan bij de inlogpagina van uw CA-servercertificaat.
https://<CA-serveradres>/certsrv

Selecteer **certificaataanvraag**, **geavanceerde certificaataanvraag** en plak de inhoud van de certificaataanvraag (CSR) op de buffer. Selecteer vervolgens **certificaatsjabloon als webserver**.

Downloadbasis 64 gecodeerd certificaat.

Open het certificaat en kopieer de inhoud van het afdrukveld voor een later gebruik. Verwijder ruimtes uit de thumbnail.

Installeer het certificaat

Kopieert het certificaat.

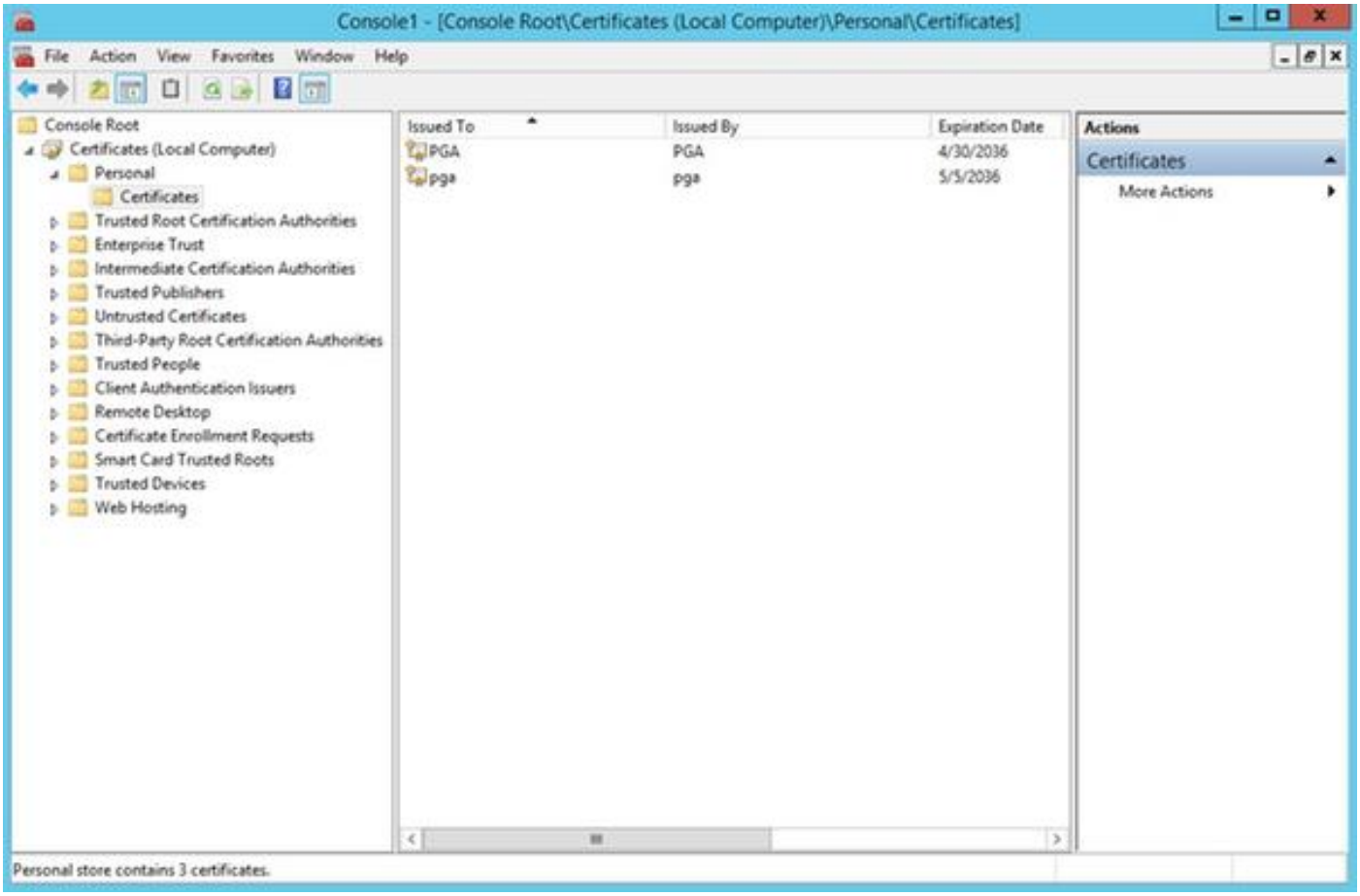
Kopieer het nieuw gegenereerde certificaatbestand naar UCCE VM waar het Portico-gereedschap zich bevindt.

Het certificaat importeren in de lokale computerwinkel

Op dezelfde UCCE-server start u Microsoft Management Console (MMC)-console door startmenu, **type run** en **mmc** te selecteren.

Klik op **Toevoegen/verwijderen** en klik in het dialoogvenster op **Toevoegen**.
Selecteer vervolgens **het** menu **Certificaten** en voeg toe.
Klik in het dialoogvenster Certificaten op **Computer-account > Local Computer > Finish**.

Blader naar de map persoonlijke certificaten.



Selecteer in het werkvenster **Meer acties >Alle taken > Importeren**.

Klik op **Volgende**, **Bladeren** en selecteer het certificaat dat eerder is gegenereerd en in het volgende menu zorg ervoor dat de certificaatopslag op persoonlijk bestand is ingesteld. Controleer op het laatste scherm of **certificaatopslag** en **certificaatbestand zijn** geselecteerd en klik op **Voltooien**.

Bind-IS

Open CMD-toepassing.

Navigeer naar de startmap diagnostisch portico.

```
cd c:\icm\serviceability\diagnostics\bin
```

Verwijder de huidige certificaatbinding voor Portico.

```
DiagFwCertMgr /task:UnbindCert
```

Bind CA ondertekend certificaat.

> **Tip**: Gebruik enige teksteditor (notepad+) om spaties in de hash te verwijderen.

Gebruik de voordien opgeslagen hash met spaties verwijderd.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

Als het certificaat is gebonden, ziet u de soortgelijke regel in de uitvoer.
"De certificatenbinding is GELDIG"
Zorg ervoor dat de certificaatbinding met dit commando succesvol was.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Ook in de uitvoer moet een soortgelijk bericht worden weergegeven.
"De certificatenbinding is GELDIG"

> Opmerking: DiagFwCertMgr zal standaard poort 7890 gebruiken.

Start de diagnostische kaderservice.

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

> **Tip**: De servicelijst en met name de naam van de Portico-service kunnen worden gecontroleerd via een opdracht in de taaklijst van het CMD-gereedschap.

```
tasklist /v
```

Verifiëren

Open: Diagnostic Framework-pagina waarin FQDN wordt gebruikt, en deze mag geen waarschuwingsbericht op het certificaat oproepen.

Voorplan

Voor het geval u de toegang tot het gereedschap Portico hebt verloren, kunt u een zichzelf ondertekend certificaat regenereren en een uitzondering toevoegen.
U kunt deze opdracht gebruiken.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Problemen oplossen

Gebruik geen IP-adres als u inlogt bij het diagnostische framework-protocol. U ontvangt nog steeds een certificaatwaarschuwing, omdat FQDN overeenkomt met de waarde die in het veld certificaat CN gespecificeerd is.

Controleer dat alle servers gesynchroniseerd zijn met de NTP-bron.

```
w32tm /monitor
```

Als u probeert het Onderwerp Alternative Name (SAN) of Elliptic Curve Digital Signature Algorithm (EC DSA) of het 4096 key length-certificaat te gebruiken - isoleer eerst dat dit niet specifiek is voor een van deze functies.

Verwante artikelen

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

CA-ondertekend certificaat via CLI configureren in Cisco Voice Operating System (VOS)