

Konfigurieren des HTTPS-Zugriffs für das UCCE Diagnostic Framework Portico Tool mit Zertifizierungsstelle (Certificate Authority, CA)-signiertem Zertifikat

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Signierte Anfrage für Zertifikat generieren](#)

[Signieren des Zertifikats auf der Zertifizierungsstelle](#)

[Installieren des Zertifikats](#)

[Zertifikat kopieren](#)

[Importieren des Zertifikats in den lokalen Computerspeicher](#)

[Binden des IIS-Zertifikats](#)

[Überprüfen](#)

[Zurück-Plan](#)

[Fehlerbehebung](#)

[Verwandte Artikel](#)

Einführung

Dieses Dokument beschreibt den Konfigurationsprozess zur Installation eines von einer CA signierten Zertifikats für das Unified Contact Center Enterprise (UCCE) Diagnostic Framework Portico-Tool.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Active Directory
- Domain Name System (DNS)-Server
- CA-Infrastruktur bereitgestellt und funktioniert für alle Server und Clients
- Diagnostic Framework-Portal

Der Zugriff auf das Diagnostic Framework Portico-Tool durch die Eingabe der IP-Adresse im Browser, ohne dass eine Zertifikatswarnung angezeigt wird, ist nicht Bestandteil dieses Artikels.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

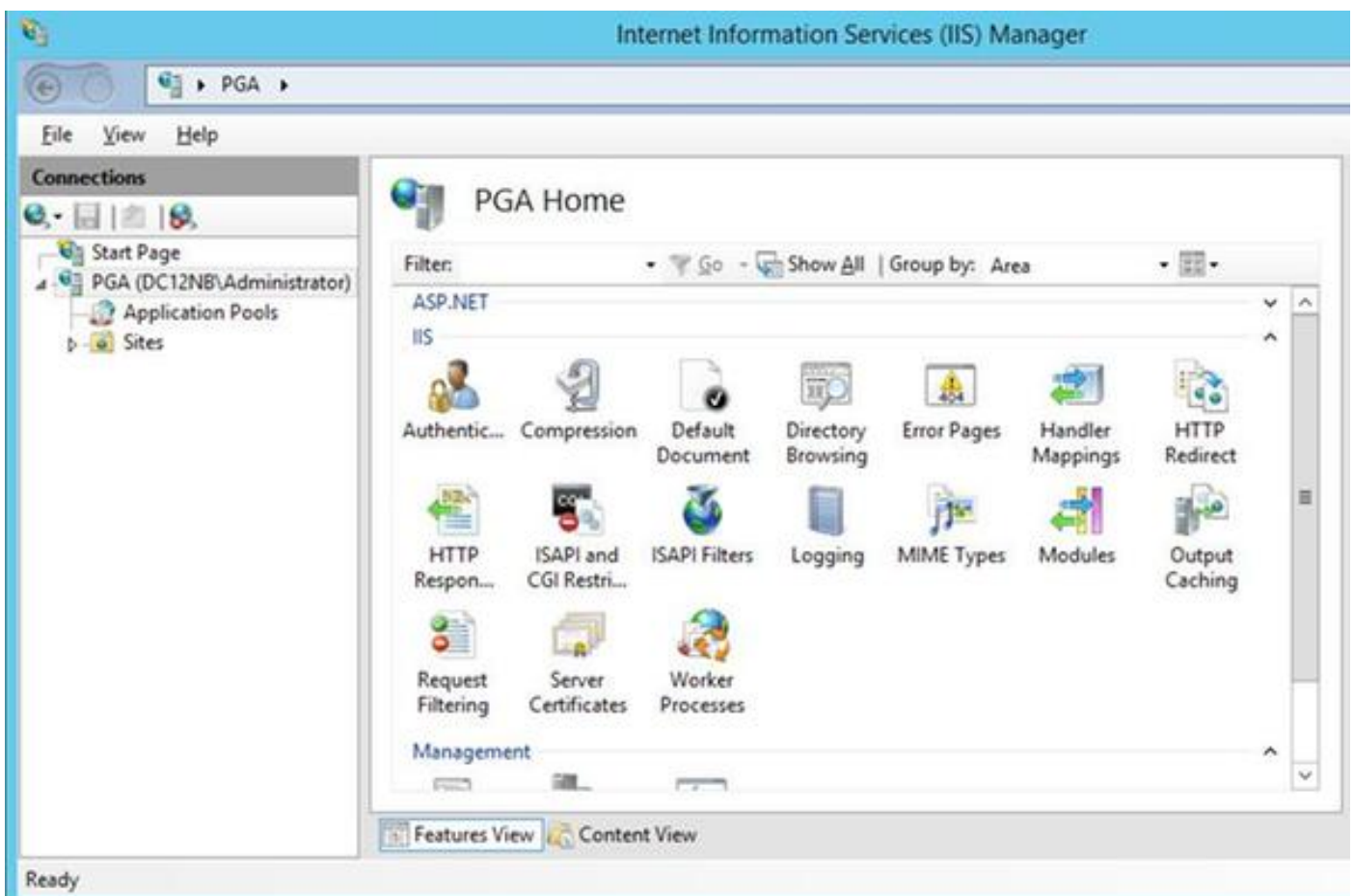
- Cisco UCCE 11.0.1
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2 Certificate Authority
- Microsoft Windows 7 SP1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

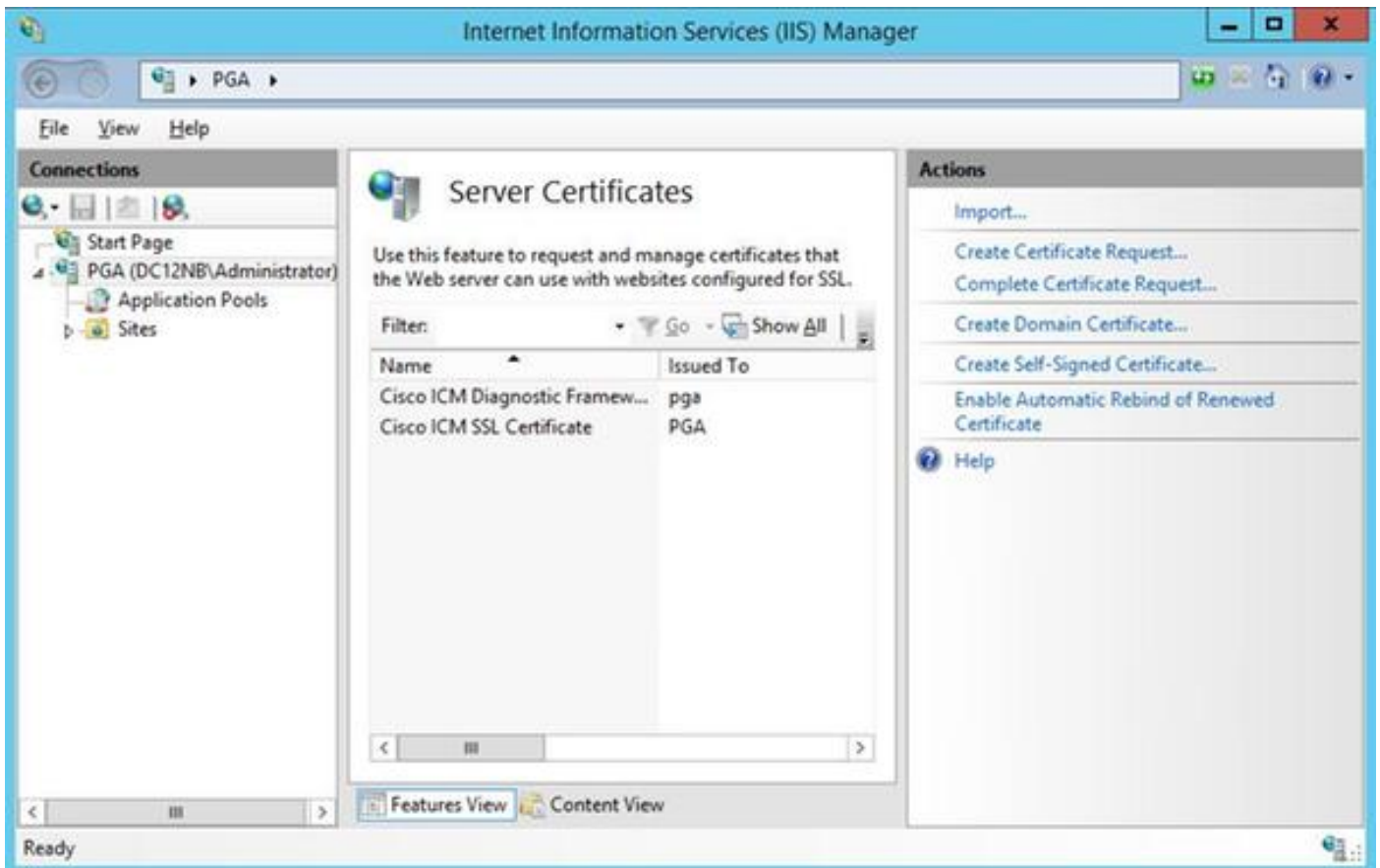
Konfigurieren

Signierte Anfrage für Zertifikat generieren

Öffnen Sie den IIS-Manager (Internetinformationsdienste), wählen Sie im Beispiel die Site, das Peripheral Gateway A (PGA) und die **Serverzertifikate aus**.



Wählen Sie im Aktionsbereich **Zertifikatsanforderung erstellen** aus.



Geben Sie die Felder **Common Name (CN)**, **Organization (O)**, **Organization Unit (OU)**, **Locality (L)**, **State (ST)**, **Country (C)** ein. Der Common Name muss mit dem Hostnamen und dem Domännennamen Ihres vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) übereinstimmen.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

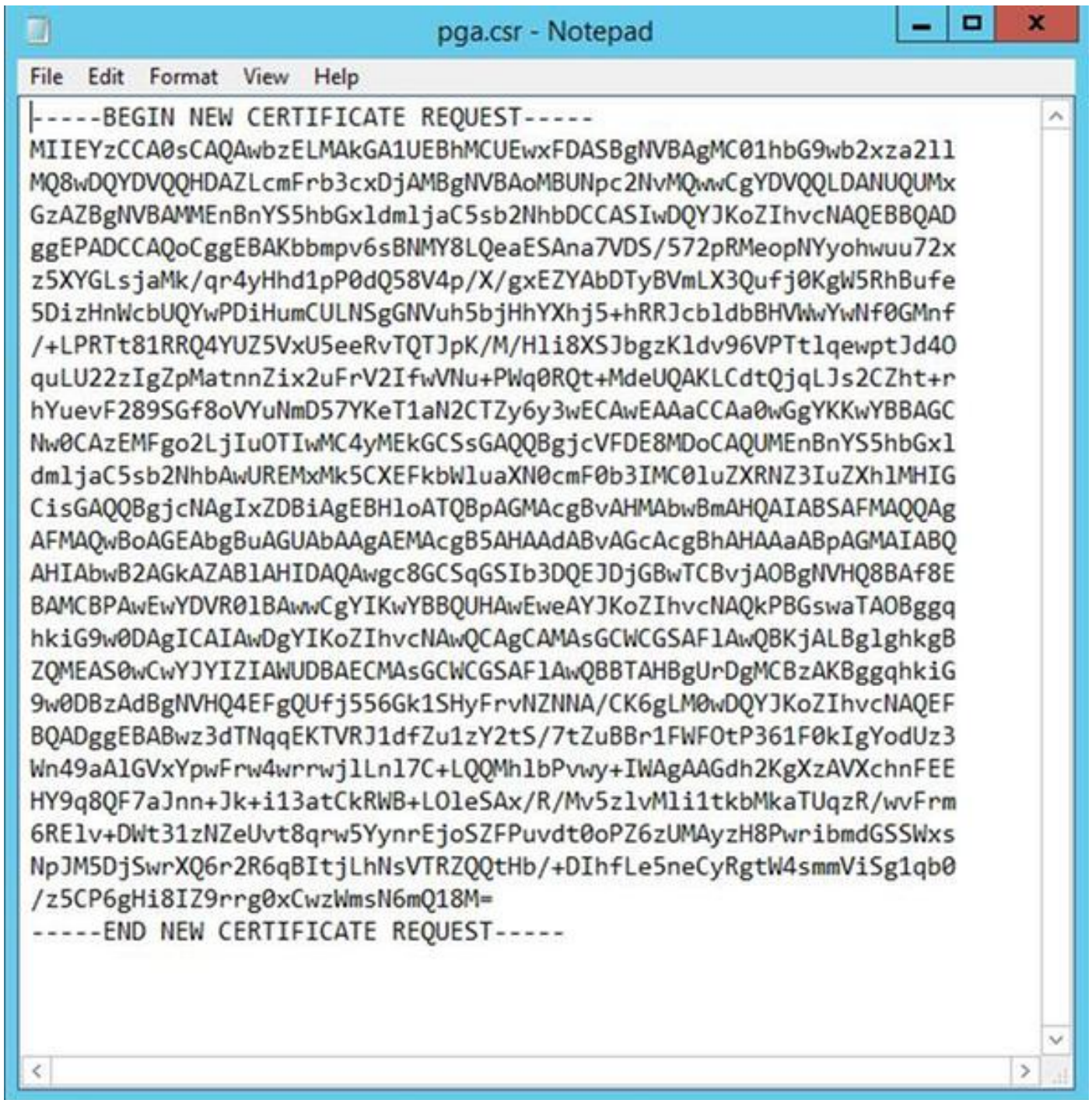
Common name:	<input type="text" value="pga.allevich.local"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="TAC"/>
City/locality:	<input type="text" value="Krakow"/>
State/province:	<input type="text" value="Malopolskie"/>
Country/region:	<input type="text" value="PL"/>

Previous Next Finish Cancel

Lassen Sie die Standardeinstellungen für den Kryptografiedienstanbieter unverändert, und geben Sie die Bitlänge an: 2048.

Wählen Sie den Pfad zum Speichern aus. Beispielsweise auf dem Desktop mit dem Namen pga.csr.

Öffnen Sie die neu erstellte Anfrage im Notizblock.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYzCCA0sCAQAwbzELMAKGA1UEBhMCUEwxFDASBgNVBAGMC01hbG9wb2xza211
MQ8wDQYDVQQHDAZLcmFr3cxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUx
GzAZBgNVBAMMEBnYS5hbGxldm1jaC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKbbmpv6sBNMY8LQeaESAna7VDS/572pRMeopNYyohuu72x
z5XYGLsjaMk/qr4yHhd1pP0dQ58V4p/X/gxEZYAbDTyBVmLX3Qufj0KgW5RhBufe
5DizHnWcbUQYwPDiHumCULNSgGNVuh5bjHhYXhj5+hRRJcb1dbBHVVwYwNf0GMnf
/+LPRTt81RRQ4YUZ5VxU5eeRvTQTJpK/M/H1i8XSJbgzK1dv96VPTt1qewptJd40
quLU22zIgZpMatnnZix2uFrV2IfwVNu+Pwq0RQt+MdeUQAKLCdtQjqLJs2CZht+r
hYuevF289SGf8oVYuNmD57YKeT1aN2CTZy6y3wECAwEAaCCAA0wGgYKKwYBBAGC
Nw0CAzEMFgo2LjIu0TIwMC4yMEkGCSsGAQQBgjcVFDE8MD0CAQUMENBnYS5hbGx1
dmljaC5sb2NhbAwUREMxMk5CXEFkbWluaXN0cmF0b3IMC0luZXRNZ3IuZXh1MHIG
CisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcGvAHMAbwBmAHQAIABSAFMAQQAg
AFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQ
AHIAbwB2AGkAZABIAHIDAQAawgc8GCSqGSIb3DQEJDDjGBwTCBvjA0BgNVHQ8BAf8E
BAMCBPAwEwYDVR01BAwwCgYIKwYBBQUHAWeweAYJKoZIhvcNAQkPBGswaTA0Bggq
hkiG9w0DAGICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAF1AwQBKjALBglghkgB
ZQMEAS0wCwYJYIZIAWUDBAECMA5GCWCGSAF1AwQBBTAHBgUrDgMCBzAKBggqhkiG
9w0DBzAdBgNVHQ4EFgQUFj556Gk1SHyFrvNZNNA/CK6gLM0wDQYJKoZIhvcNAQEF
BQADggEBABwz3dTnqqEKTVRJ1dfZu1zY2tS/7tZuBBn1FWF0tP361F0kIgYodUz3
Wn49aA1GVxYpwFrw4wrrwj1Ln17C+LQQMh1bPvwy+IWAgaAGdh2KgXzAVXchnFEE
HY9q8QF7aJnn+Jk+i13atCkRWB+L01eSAx/R/Mv5z1vM1i1tkbMkaTUqzR/wvFrm
6RElv+Dwt31zNZeUvt8qrw5YynrEjoSZFPuvdt0oPZ6zUMAYzH8PwribmdGSSWxs
NpJM5DjSwrXQ6r2R6qBItjLhNsVTRZQQtHb/+DIhfLe5neCyRgtW4smmViSg1qb0
/z5CP6gHi8IZ9rrg0xCwzWmsN6mQ18M=
-----END NEW CERTIFICATE REQUEST-----
```

Kopieren Sie das Zertifikat mit STRG+C in den Puffer.

Signieren des Zertifikats auf der Zertifizierungsstelle

Hinweis: Wenn Sie eine externe Zertifizierungsstelle (wie GoDaddy) verwenden, müssen Sie diese kontaktieren, nachdem Sie eine CSR-Datei erstellt haben.

Melden Sie sich bei der Anmeldeseite für das CA-Serverzertifikat an.

<https://<CA-Server-Adresse>/certsrv>

Wählen Sie **Zertifikat anfordern**, **Erweiterte Zertifikatsanforderung** aus, und fügen Sie den CSR-Inhalt (Certificate Signing Request) in den Puffer ein. Wählen Sie dann **Zertifikatsvorlage als Webserver** aus.

Base 64-verschlüsseltes Zertifikat herunterladen

Öffnen Sie das Zertifikat, und kopieren Sie den Inhalt des Thumbprint-Felds zur späteren Verwendung. Entfernen Sie Leerzeichen vom Daumenabdruck.

Installieren des Zertifikats

Zertifikat kopieren

Kopieren Sie die neu generierte Zertifikatsdatei in UCCE VM, wo sich das Portico-Tool befindet.

Importieren des Zertifikats in den lokalen Computerspeicher

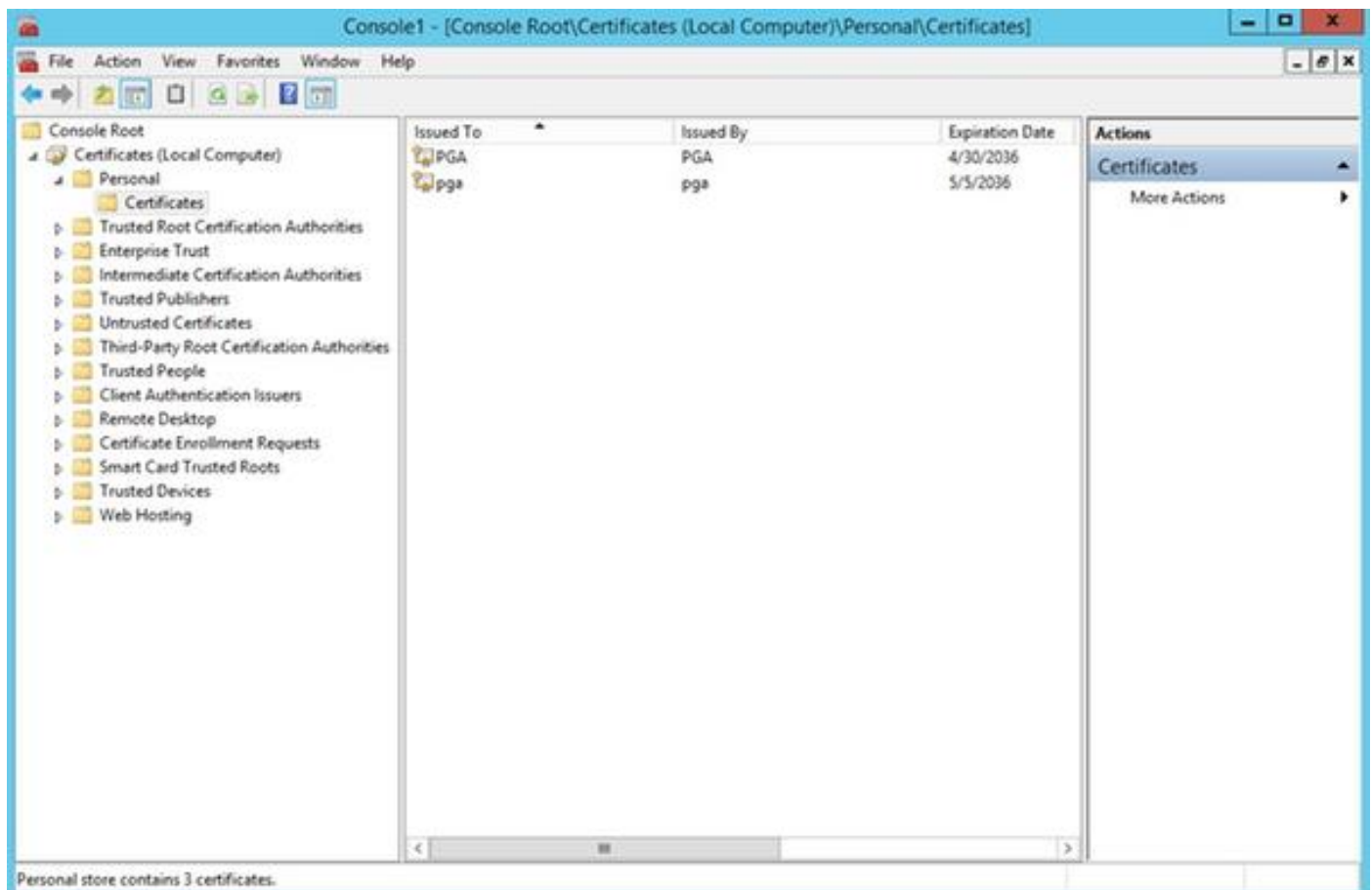
Starten Sie auf demselben UCCE-Server die Microsoft Management Console (MMC)-Konsole, indem Sie das Startmenü auswählen, **run** und **mmc** eingeben.

Klicken Sie auf **Snap-In hinzufügen/entfernen**, und klicken Sie im Dialogfeld auf **Hinzufügen**.

Wählen Sie dann das Menü **Zertifikate** aus, und fügen Sie es hinzu.

Klicken Sie im Dialogfeld Certificates Snap-In (Zertifikate) auf **Computerkonto > Lokaler Computer > Fertig stellen**.

Navigieren Sie zum Ordner für persönliche Zertifikate.



Wählen Sie im Aktionsbereich **Weitere Aktionen > Alle Aufgaben > Importieren aus**.

Klicken Sie auf **Weiter**, **Durchsuchen**, und wählen Sie das zuvor erstellte Zertifikat aus. Stellen Sie im nächsten Menü sicher, dass der Zertifikatsspeicher auf Personal eingestellt wurde. Überprüfen Sie im letzten Bildschirm den **Zertifikatsspeicher** und die **Zertifikatsdatei**, die ausgewählt sind, und klicken Sie auf **Fertig stellen**.

Binden des IIS-Zertifikats

Öffnen Sie die CMD-Anwendung.

Navigieren Sie zum Hauptordner Diagnostic Portico.

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

Entfernen Sie die aktuelle Zertifikatbindung für das Portico-Tool.

```
DiagFwCertMgr /task:UnbindCert
```

Zertifizierungsstelle signiertes Bind-Zertifikat.

Tipp: Verwenden Sie einen Texteditor (notepad++), um Leerzeichen im Hash zu entfernen.

Verwenden Sie den zuvor gespeicherten Hash mit entfernten Leerzeichen.

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

Wenn das Zertifikat erfolgreich gebunden wurde, sollte die entsprechende Zeile in der Ausgabe angezeigt werden.

"Die Zertifikatbindung ist GÜLTIG."

Stellen Sie sicher, dass die Zertifikatsbindung mit diesem Befehl erfolgreich war.

```
DiagFwCertMgr /task:ValidateCertBinding
```

In der Ausgabe sollte eine ähnliche Meldung angezeigt werden.

"Die Zertifikatbindung ist GÜLTIG."

Hinweis: DiagFwCertMgr verwendet standardmäßig Port 7890.

Starten Sie den Diagnostic Framework-Dienst neu.

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

Tipp: Die Dienstliste und insbesondere der Name des Portico-Service können über den Befehl tasklist im CMD-Tool überprüft werden.

`tasklist /v`

Überprüfen

Öffnen Sie die Diagnostic Framework-Seite mit FQDN, und es sollte keine Zertifikatswarnmeldung angezeigt werden.

Zurück-Plan

Falls Sie den Zugriff auf das Portico-Tool verloren haben, können Sie ein selbstsigniertes Zertifikat neu erstellen und eine Ausnahme hinzufügen.
Dieser Befehl kann verwendet werden.

`DiagFwCertMgr /task:CreateAndBindCert`

Fehlerbehebung

Verwenden Sie keine IP-Adresse, wenn Sie sich beim Diagnostic Framework Portico-Tool anmelden. Sie erhalten immer noch eine Zertifikatswarnung, da FQDN mit dem im Zertifikats-CN-Feld angegebenen Wert übereinstimmen muss.

Überprüfen Sie, ob alle Server mit der NTP-Quelle synchronisiert sind.

`w32tm /monitor`

Wenn Sie ein Zertifikat mit dem Schlüssellänge "Subject Alternative Name (SAN)" oder "Elliptic Curve Digital Signature Algorithm (EC DSA)" oder ein Zertifikat mit der Schlüssellänge 4096 verwenden möchten, müssen Sie zunächst isolieren, dass es nicht nur für eine dieser Funktionen gilt.

Verwandte Artikel

[UCCE\PCCE - Verfahren zum Abrufen und Hochladen des Zertifikats der selbstsignierten Windows-Server- oder Zertifizierungsstelle \(Certificate Authority, CA\) für 2008-Server Konfigurieren des signierten Zertifikats der CA über die CLI im Cisco Voice Operating System \(VOS\)](#)