Configurare l'accesso HTTPS per lo strumento Portico UCCE Diagnostic Framework con il certificato firmato dall'Autorità di certificazione (CA)

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione relativo all'installazione del certificato firmato dall'autorità di certificazione per lo strumento Portico della diagnostica UCCE (Unified Contact Center Enterprise).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Active Directory
- Server DNS (Domain Name System)
- Infrastruttura CA installata e funzionante per tutti i server e i client
- Diagnostic Framework Portico

L'accesso allo strumento Portico di Diagnostic Framework digitando l'indirizzo IP nel browser senza ricevere un avviso di certificato non rientra nell'ambito di questo articolo.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

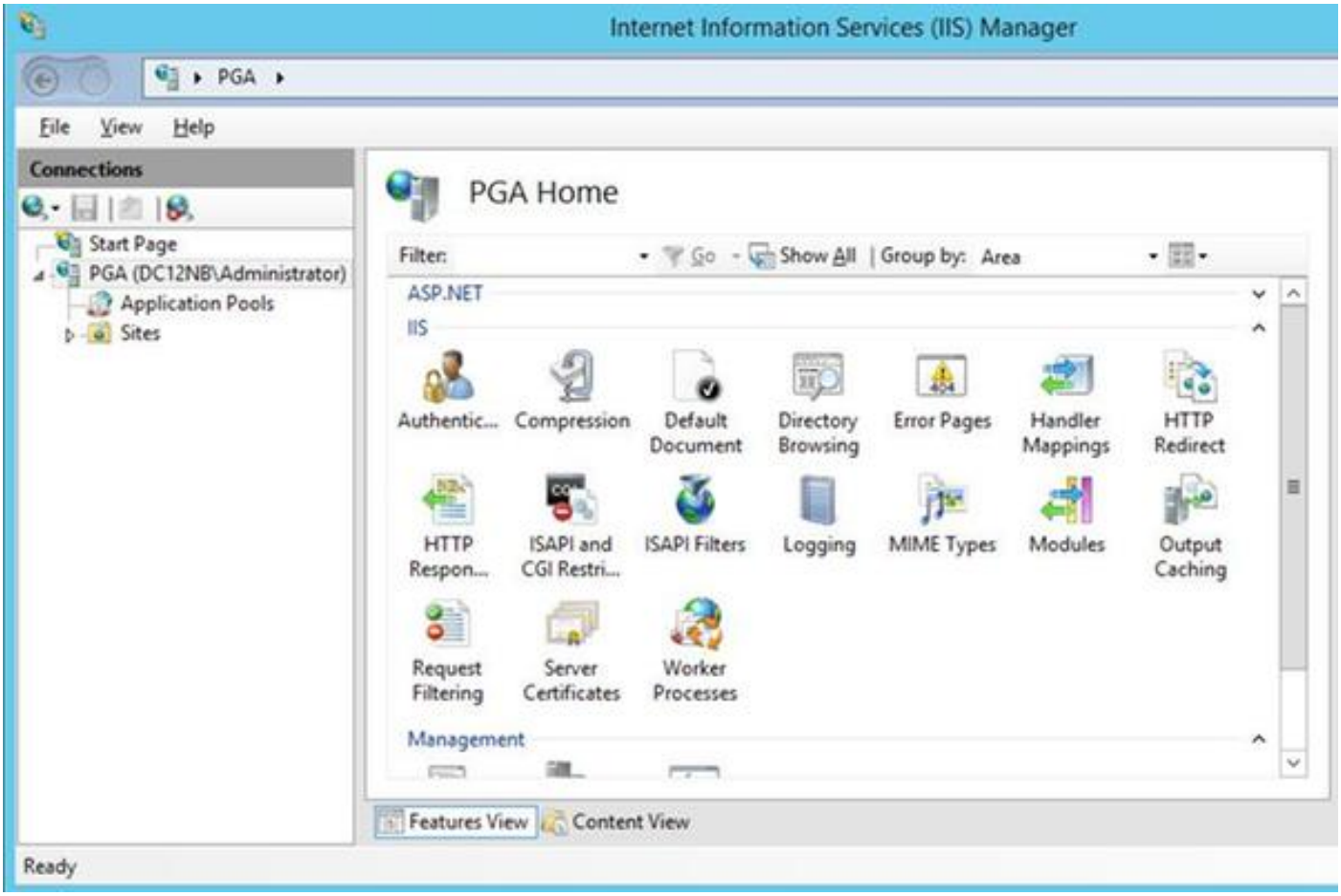
- Cisco UCCE 11.0.1
- Microsoft Windows Server 2012 R2
- Autorità di certificazione di Microsoft Windows Server 2012 R2
- Sistema operativo Microsoft Windows 7 SP1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

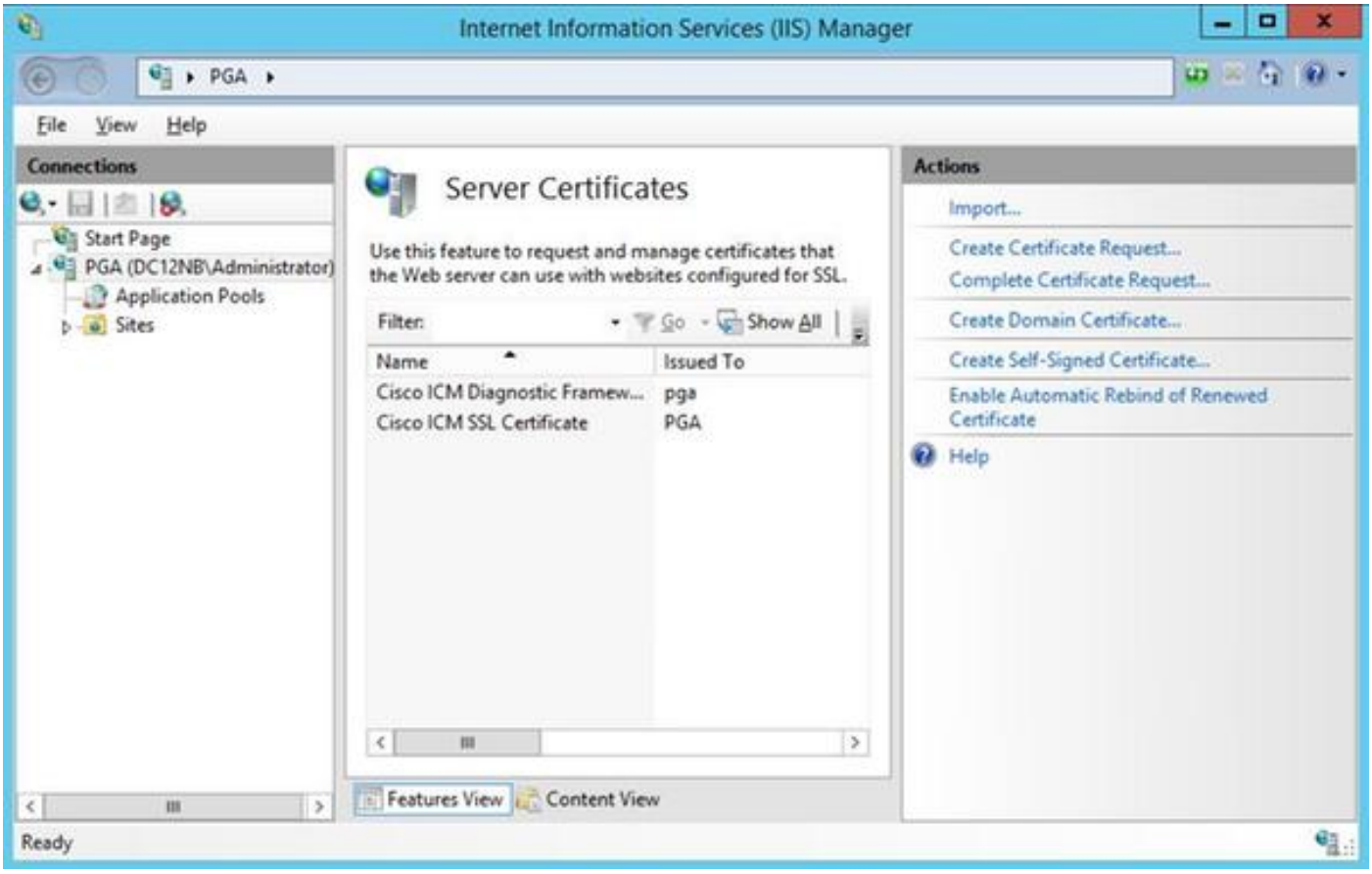
Configurazione

Genera richiesta firmata certificato

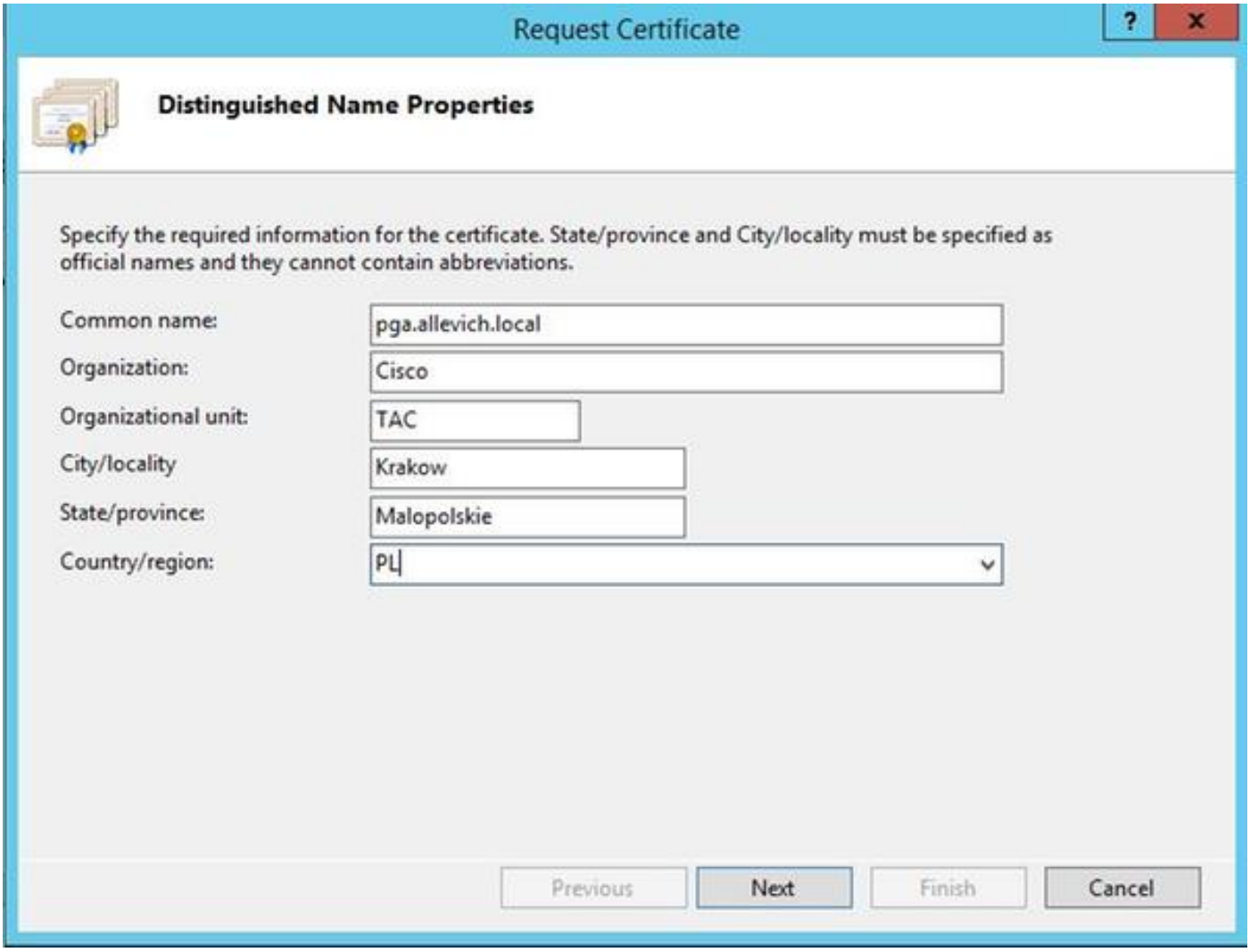
Aprire Gestione Internet Information Services (IIS), selezionare il sito, PGA (Peripheral Gateway A) nell'esempio e **Certificati server**.



Selezionare **Crea richiesta certificato** nel pannello azioni.



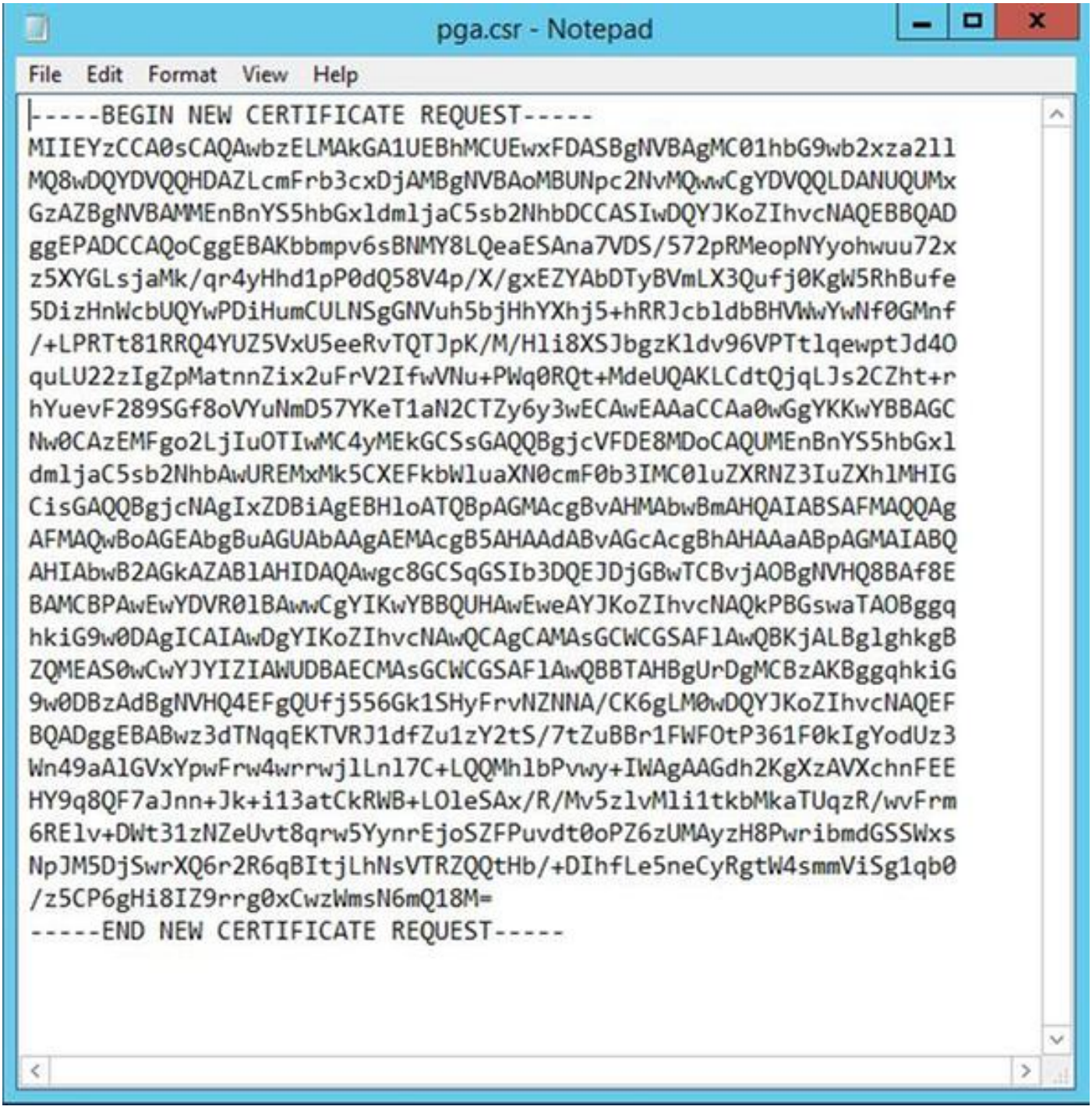
Inserire i campi Nome comune (CN), Organizzazione (O), Unità organizzativa (OU), **Località** (L), **Stato** (ST), **Paese** (C). Il nome comune deve corrispondere al nome host + nome di dominio completo (FQDN).



Accettare le impostazioni predefinite per il provider del servizio di crittografia e specificare la lunghezza in bit: 2048.

Selezionare il percorso in cui archiviare. Ad esempio sul desktop con il nome pga.csr.

Aprire la richiesta appena creata nel Blocco note.



Copiare il certificato nel buffer premendo CTRL+C.

Firma il certificato nell'autorità di certificazione

> **Nota:** Se si utilizza un'autorità di certificazione esterna, ad esempio GoDaddy, è necessario contattarli dopo la generazione del file CSR.

Accedere alla pagina di registrazione dei certificati del server CA.
https://<indirizzo-server-CA>/certsrv

Selezionare **Request Certificate** (Richiedi certificato), **Advanced Certificate Request** (Richiesta avanzata certificato) e incollare il contenuto Certificate Signing Request (CSR) nel buffer. Quindi selezionare **Modello di certificato come server Web**.

Scarica certificato codificato Base 64.

Aprire il certificato e copiare il contenuto del campo dell'identificazione personale per un utilizzo successivo. Rimuovere gli spazi dall'identificazione personale.

Installa il certificato

Copia il certificato

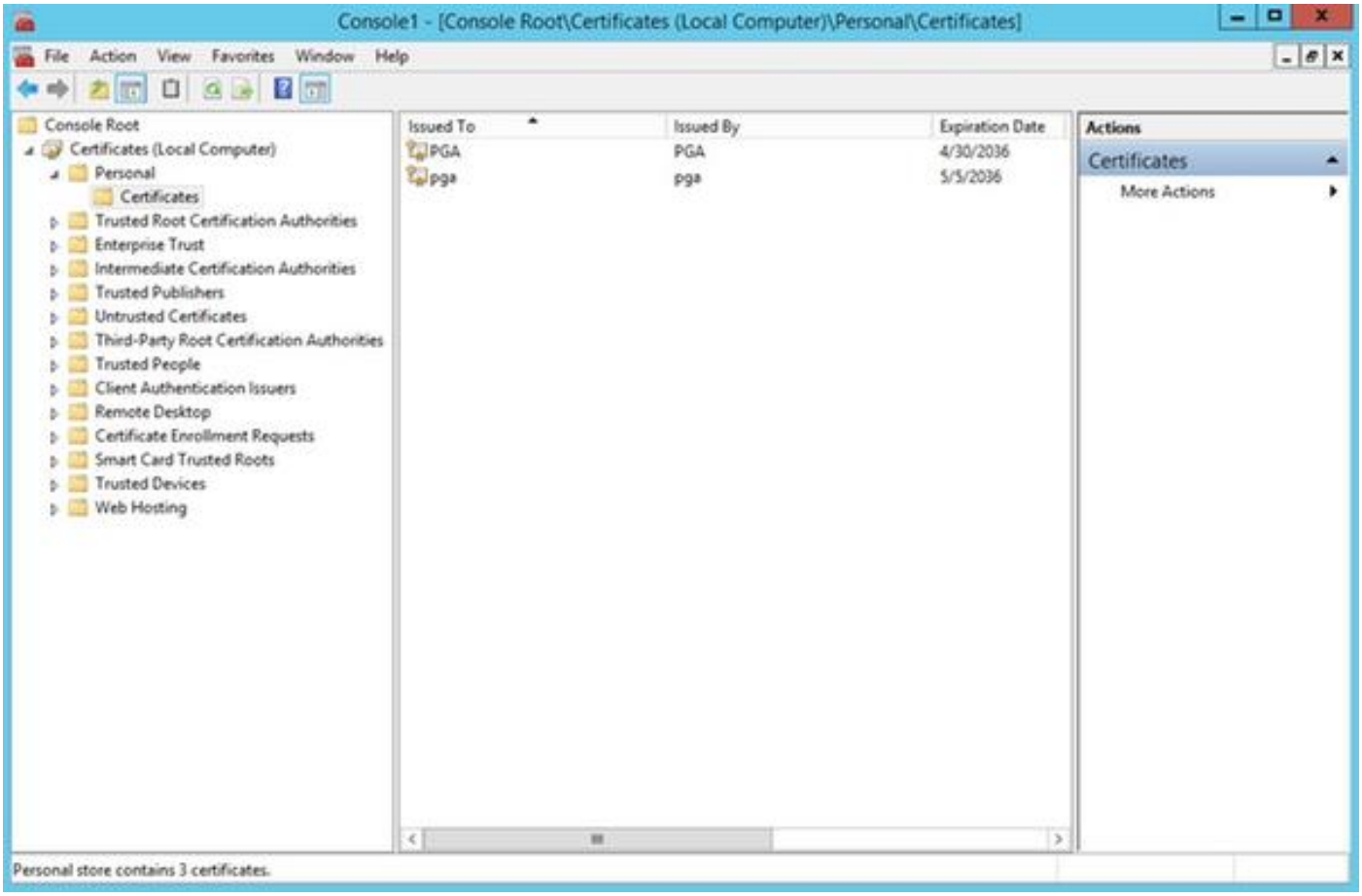
Copiare il file del certificato appena generato nella macchina virtuale UCCE in cui si trova lo strumento Portico.

Importa il certificato nell'archivio del computer locale

Nello stesso server UCCE avviare la console MMC (Microsoft Management Console) selezionando il menu Start, digitare **run** e **mmc**.

Fare clic su **Aggiungi/Rimuovi snap-in** e nella finestra di dialogo fare clic su **Aggiungi**.
Quindi scegliere **Certificati** dal menu e aggiungere.
Nella finestra di dialogo Snap-in certificati fare clic su **Account computer > Computer locale > Fine**.

Passare alla cartella dei certificati personali.



Nel riquadro delle azioni selezionare **Altre azioni > Tutte le attività > Importa**.

Fare clic su **Avanti**, **Sfoglia** e selezionare il certificato generato in precedenza. Nel menu successivo verificare che l'archivio certificati sia stato impostato su personale. Nell'ultima schermata verificare che l'**archivio certificati** e il **file di certificato siano** selezionati e fare clic su **Fine**.

Associa certificato IIS

Aprire l'applicazione CMD.

Passare alla home directory di Diagnostic Portico.

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

Rimuove il binding del certificato corrente per lo strumento Portico.

```
DiagFwCertMgr /task:UnbindCert
```

Associa certificato firmato CA.

> **Suggerimento**: Utilizzare un editor di testo (blocco note++) per rimuovere gli spazi nell'hash.

Usa l'hash salvato in precedenza con gli spazi rimossi.

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

Se il certificato viene associato correttamente, nell'output verrà visualizzata la riga simile.
"Il binding del certificato è VALIDO"
Verificare che il binding dei certificati sia stato eseguito correttamente utilizzando questo comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Anche in questo caso dovrebbe essere visualizzato un messaggio simile nell'output.
"Il binding del certificato è VALIDO"

> **Nota:** Per impostazione predefinita, DiagFwCertMgr utilizza la porta 7890.

Riavviare il servizio Framework di diagnostica.

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

> **Suggerimento**: L'elenco dei servizi e in particolare il nome del servizio Portico possono essere controllati tramite il comando tasklist nello strumento CMD.

```
tasklist /v
```

Verifica

Aprire la pagina Framework di diagnostica utilizzando FQDN e non visualizzare un messaggio di avviso del certificato.

Piano di backup

Nel caso si perda l'accesso allo strumento Portico è possibile rigenerare il certificato autofirmato e aggiungere un'eccezione.
Per eseguire questa operazione, utilizzare il comando.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Risoluzione dei problemi

Non utilizzare l'indirizzo IP quando si accede allo strumento Portico di Diagnostic Framework. Viene comunque visualizzato un avviso di certificato perché il nome di dominio completo deve corrispondere al valore specificato nel campo CN certificato.

Verificare che tutti i server siano sincronizzati con l'origine NTP.

```
w32tm /monitor
```

Se si tenta di utilizzare il certificato relativo alla lunghezza della chiave SAN (Subject Alternative Name), EC DSA (Elliptic Curve Digital Signature Algorithm) o 4096, è innanzitutto necessario verificare che non sia specifico di una di queste funzionalità.

Articoli correlati

UCCE\PCCE - Procedura per ottenere e caricare il certificato CA (Certification Authority) o autofirmato di Windows Server sui server 2008
Configurazione del certificato firmato dalla CA tramite CLI in Cisco Voice Operating System (VOS)