

UCCE\PCCE - Verfahren zum Abrufen und Hochladen des Zertifikats der selbstsignierten Windows-Server- oder Zertifizierungsstelle (Certificate Authority, CA) für 2008-Server

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Schritt 1: Erstellen von CSR über den IIS-Manager \(Internetinformationsdienste\)](#)

[Schritt 2: Laden Sie das CA Signed Certificate in den IIS-Manager \(Internetinformationsdienste\) hoch.](#)

[Schritt 3: Binden des signierten CA-Zertifikats an die Standardwebsite](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie das Zertifizierungszertifikat der Zertifizierungsstelle (Certificate Authority, CA) auf Unified Contact Center Enterprise (UCCE)-Windows 2008 R2-Servern konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit dem Prozess für signierte und selbstsignierte Zertifikate vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Windows 2008 R2
- UCCE 10.5(1)

Konfigurieren

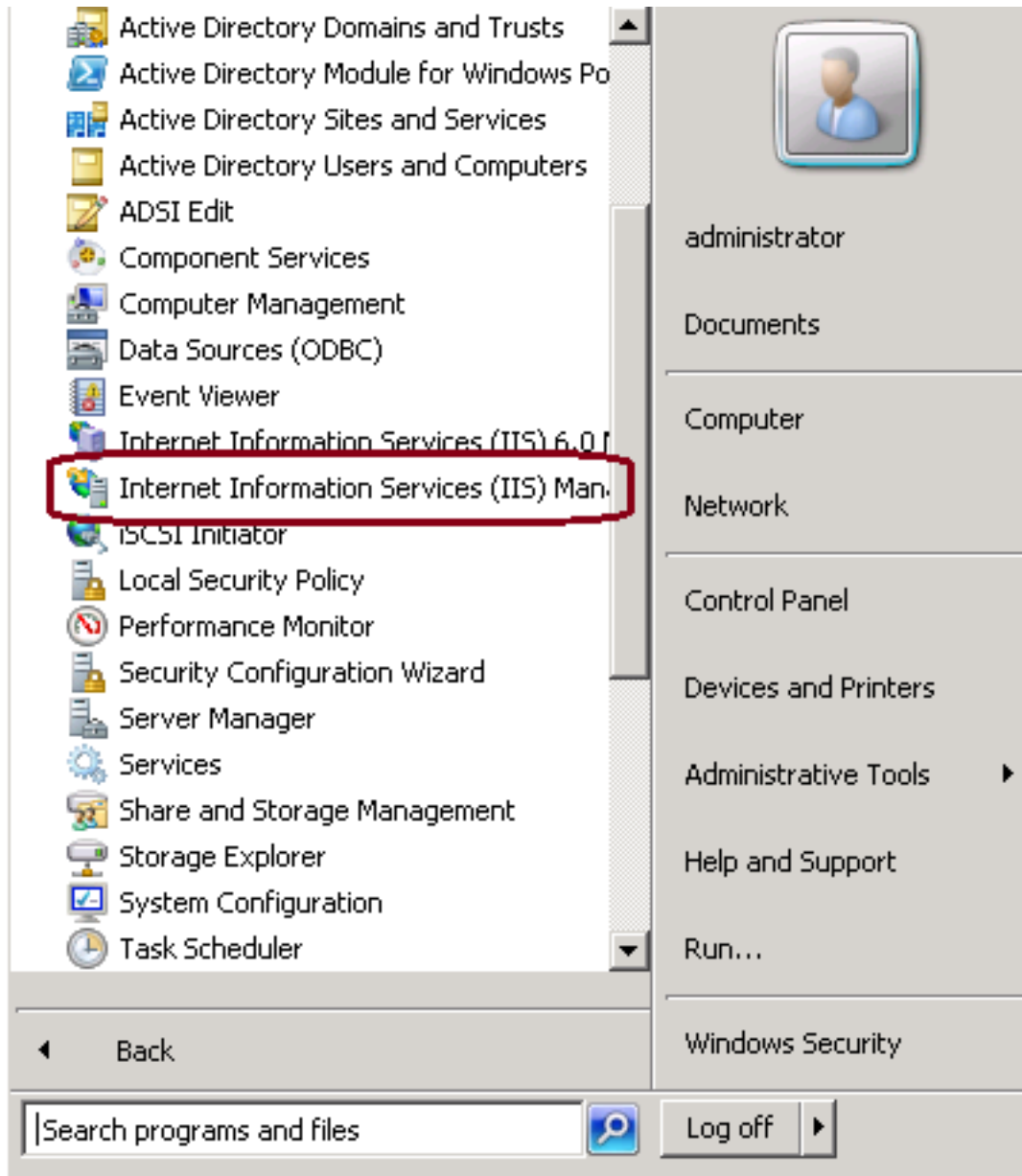
Das Einrichten eines Zertifikats für die HTTPS-Kommunikation auf dem Windows-Server ist ein

dreistufiger Prozess.

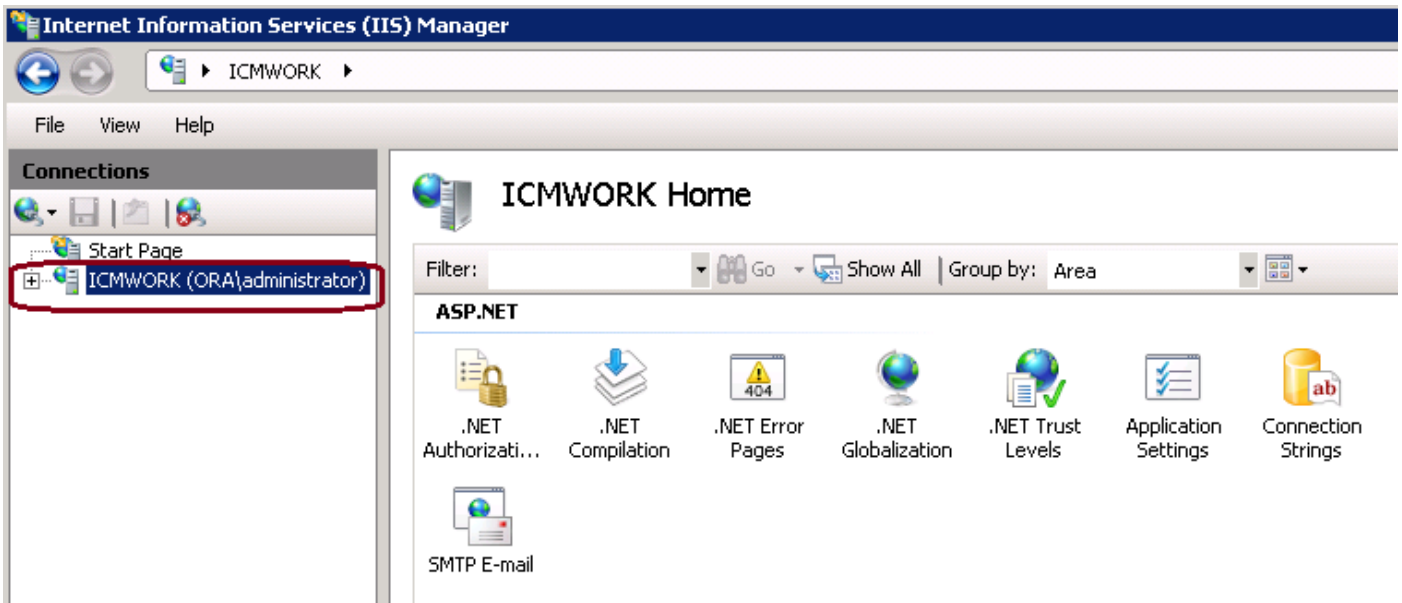
- Erstellen einer CSR-Anfrage (Certificate Signing Request) vom IIS-Manager (Internetinformationsdienste)
- Laden Sie das CA Signed Certificate in den IIS-Manager (Internetinformationsdienste) hoch.
- Binden des signierten CA-Zertifikats an die Standardwebsite

Schritt 1: Erstellen von CSR über den IIS-Manager (Internetinformationsdienste)

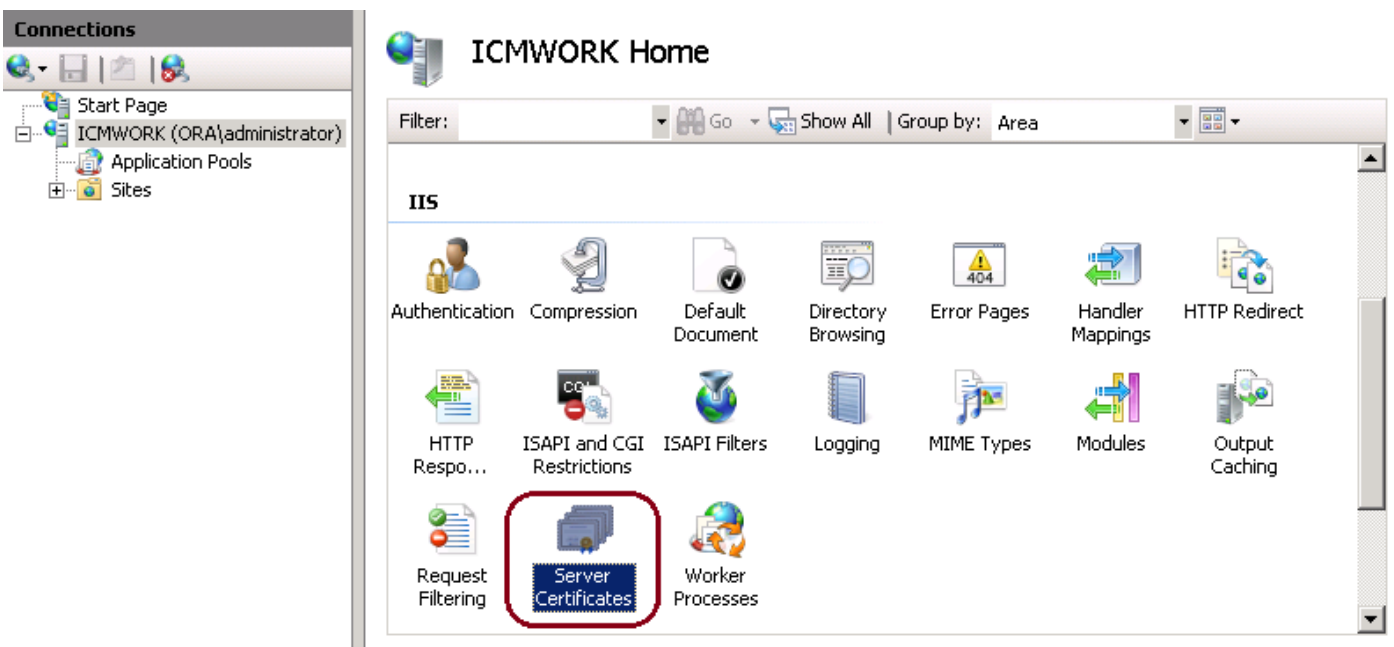
1. Melden Sie sich bei Windows an, und klicken Sie auf **Start > Ausführen > Alle Programme > Verwaltung > Internetinformationsdienste (IIS)-Manager**, wie in diesem Bild gezeigt. Wählen Sie IIS-Version 6 nicht aus, sofern vorhanden.



2. Wählen Sie im Fensterbereich Verbindungen links den Servernamen aus, wie in diesem Bild gezeigt.



3. Wählen Sie im mittleren Fensterbereich IIS > **Serverzertifikate** aus. Doppelklicken Sie auf Serverzertifikate, um das Zertifikatsfenster zu erstellen, wie in diesem Bild gezeigt.




4. Klicken Sie im rechten Teilfenster auf **Aktionen > Zertifikatsanforderung erstellen**, wie in diesem Bild gezeigt.



5. Geben Sie zum Ausfüllen des Zertifikatsantrags den Gemeinsamen Namen, die Organisation, die Organisationseinheit, Stadt/Ort, Bundesland/Region und das Land/die Region ein, wie in diesem Bild gezeigt.

Request Certificate ? X

 **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:

Organization:

Organizational unit:

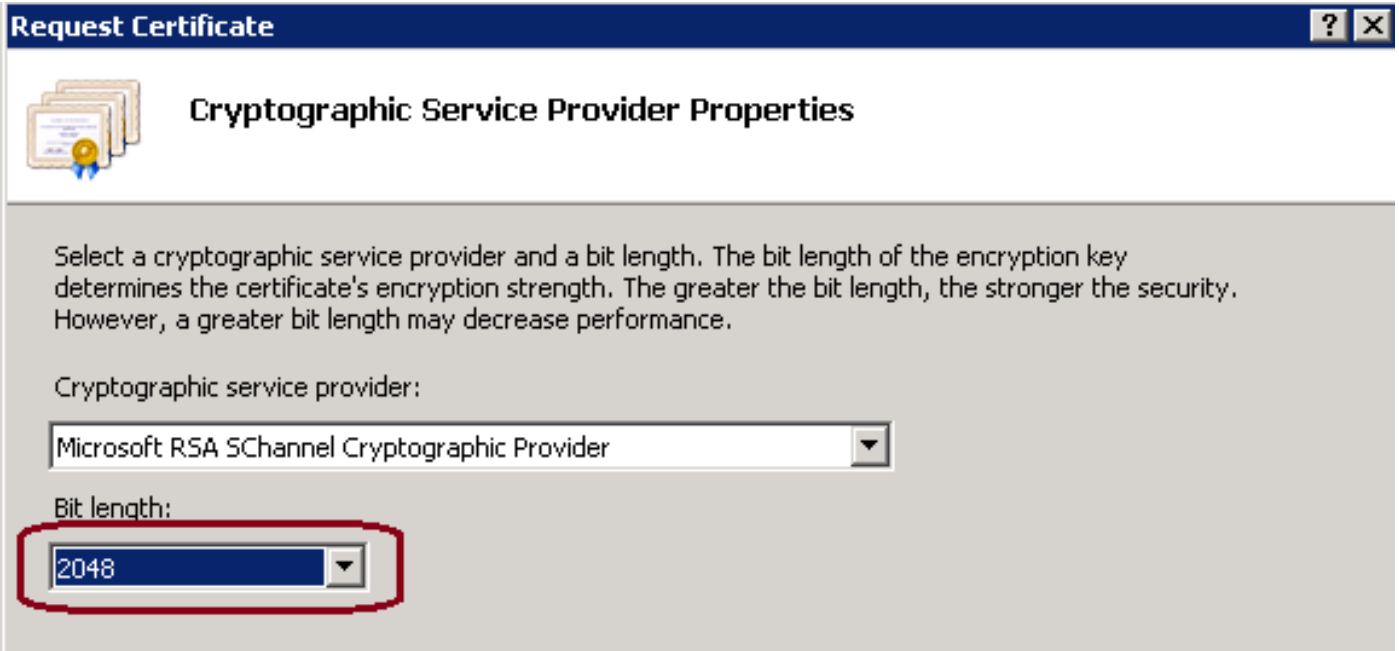
City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

6. Klicken Sie auf Next (Weiter), um die Länge des kryptografischen und Sicherheitsbits zu ändern. Es wird empfohlen, mindestens 2048 zu verwenden, um die Sicherheit zu verbessern, wie in diesem Bild gezeigt.

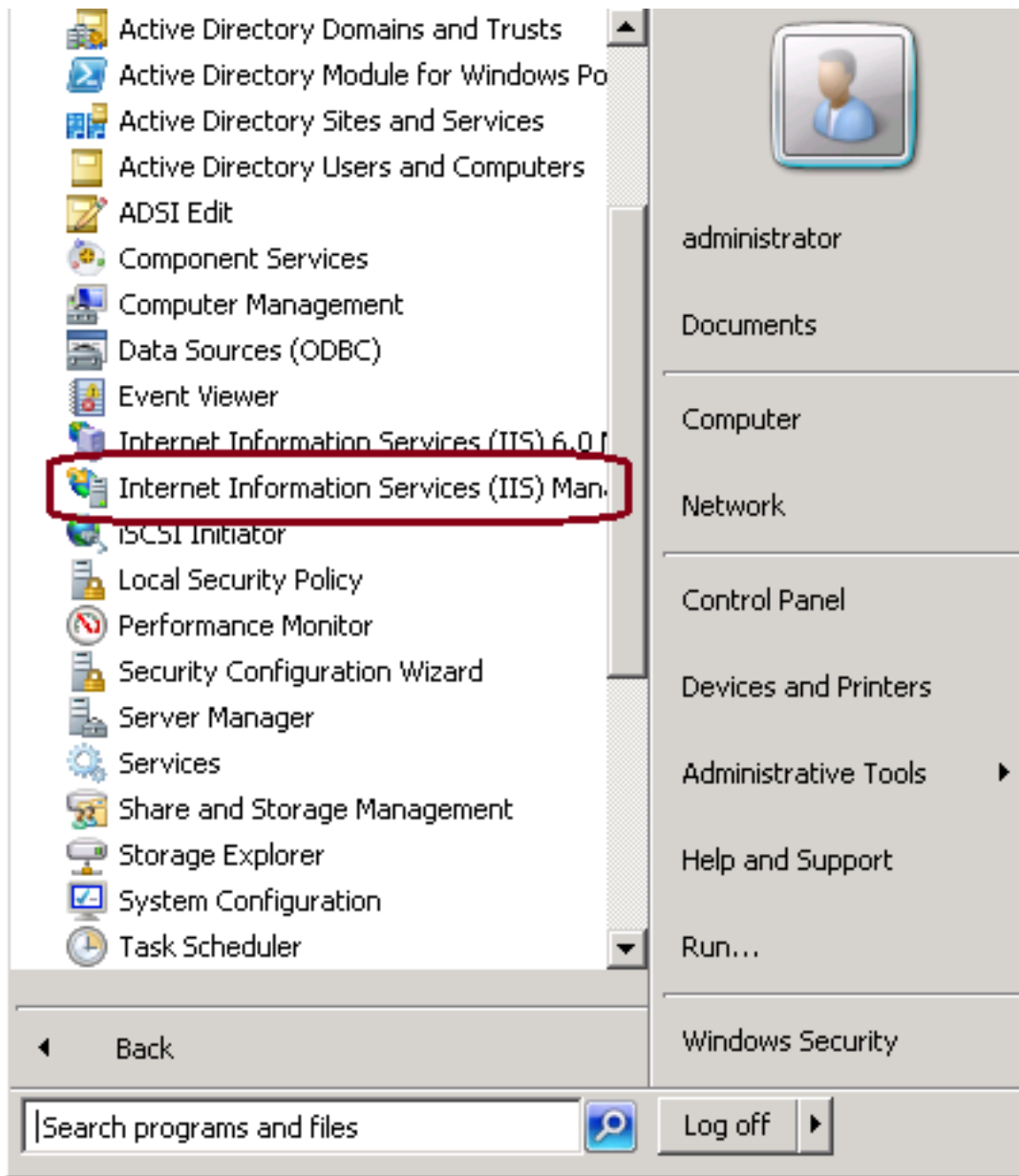


7. Speichern Sie die Zertifikatsanforderung an dem gewünschten Speicherort, der wie in diesem Bild gezeigt als TXT-Format gespeichert wird.

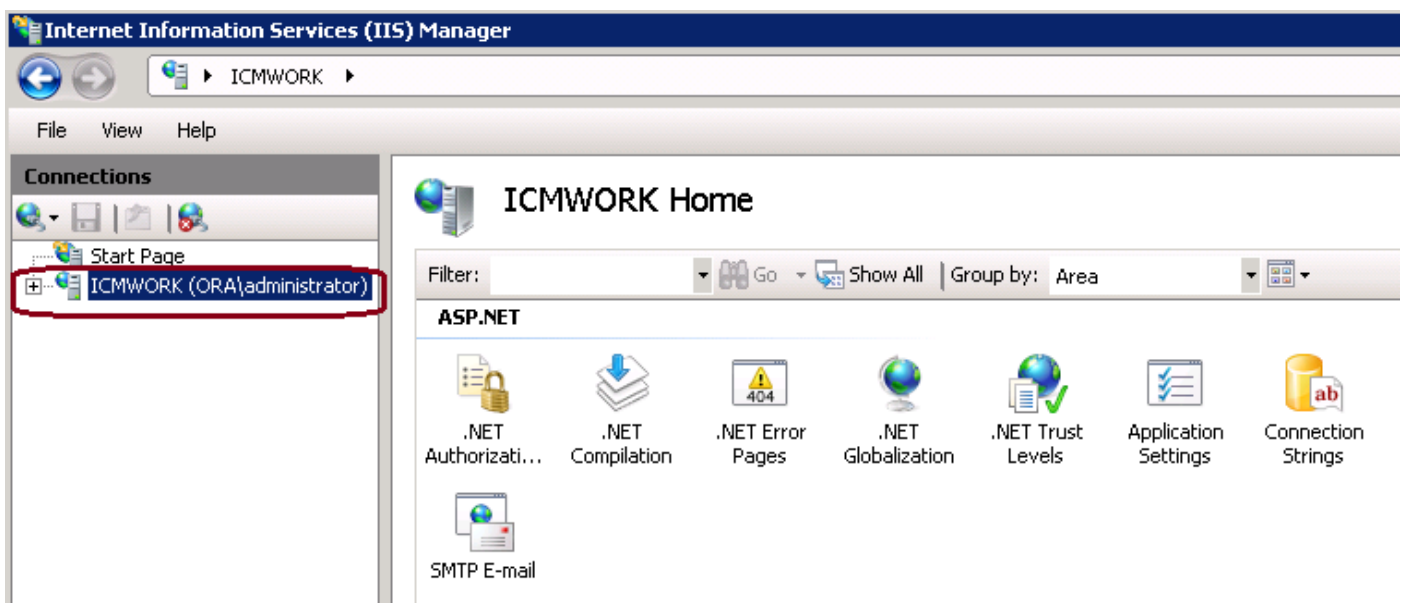
8. Geben Sie diese Datei an, die von dem Team signiert wird, das die interne CA oder die externe CA-Serviceanfrage verwaltet, wie in diesem Bild gezeigt.

Schritt 2: Laden Sie das CA Signed Certificate in den IIS-Manager (Internetinformationsdienste) hoch.

1. Melden Sie sich bei Windows an, und klicken Sie auf **Start > Ausführen > Alle Programme > Verwaltung > Internetinformationsdienste (IIS)-Manager**, wie in diesem Bild gezeigt. Wählen Sie IIS-Version 6 nicht aus, sofern vorhanden.

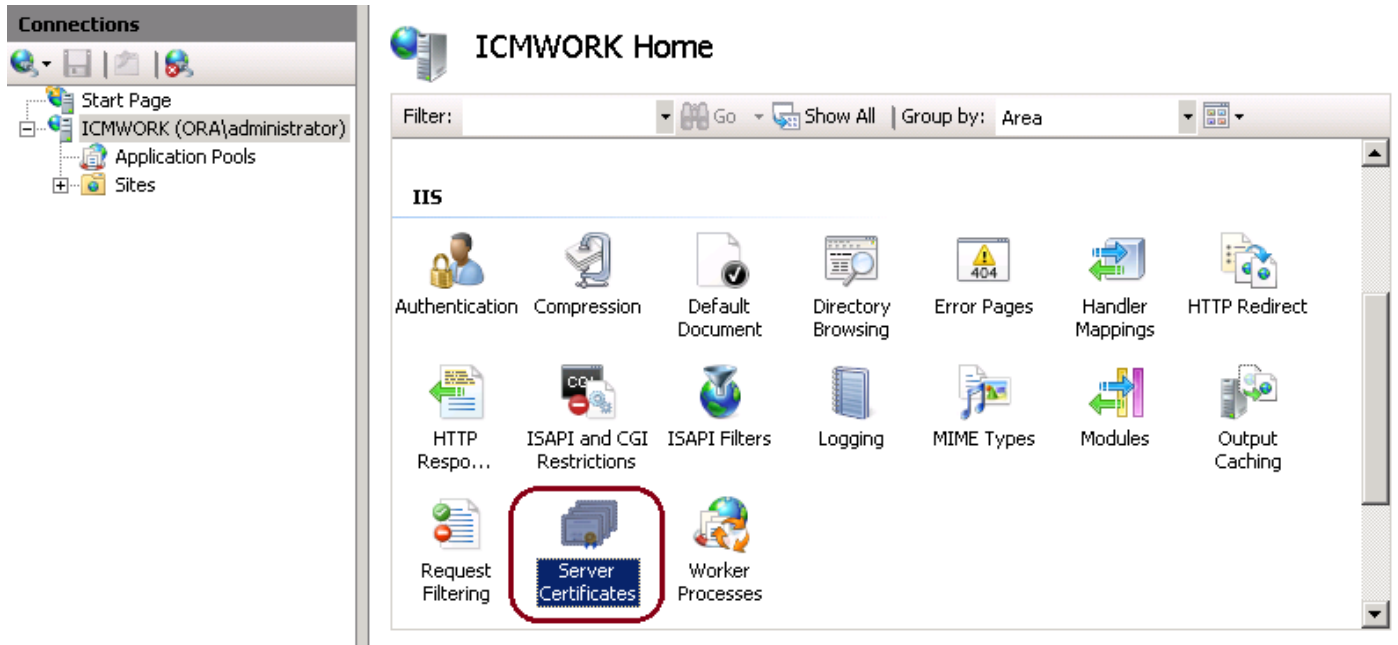


2. Wählen Sie im Fensterbereich Verbindungen links den Servernamen aus, wie in diesem Bild gezeigt.

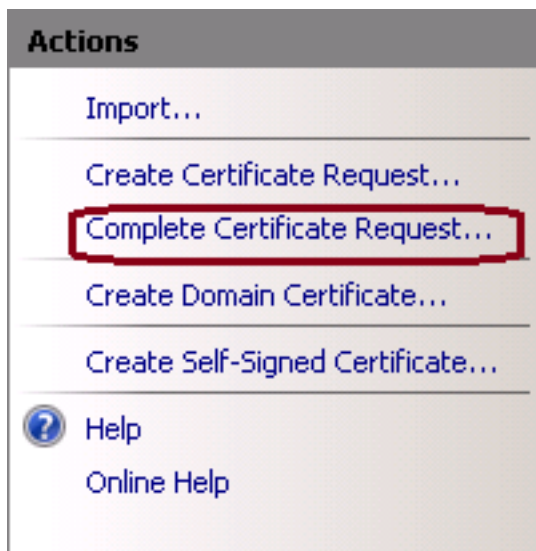


3. Wählen Sie im mittleren Fensterbereich IIS > **Serverzertifikate** aus. Doppelklicken Sie auf

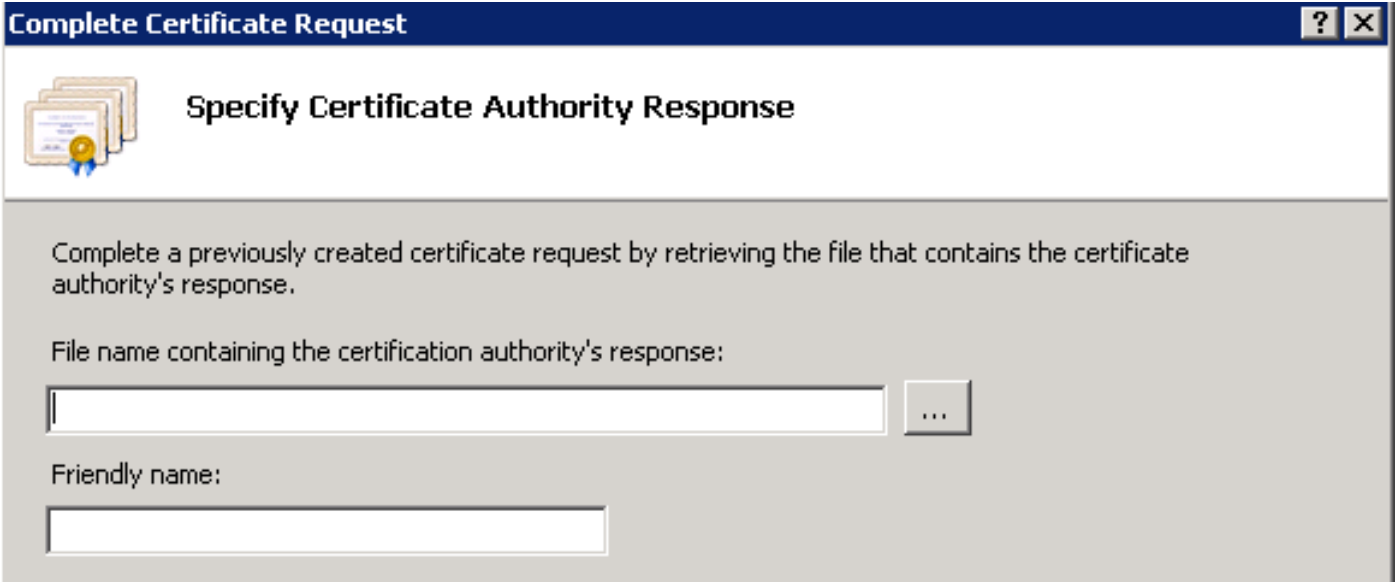
Serverzertifikate, um das Zertifikatsfenster zu erstellen, wie in diesem Bild gezeigt.



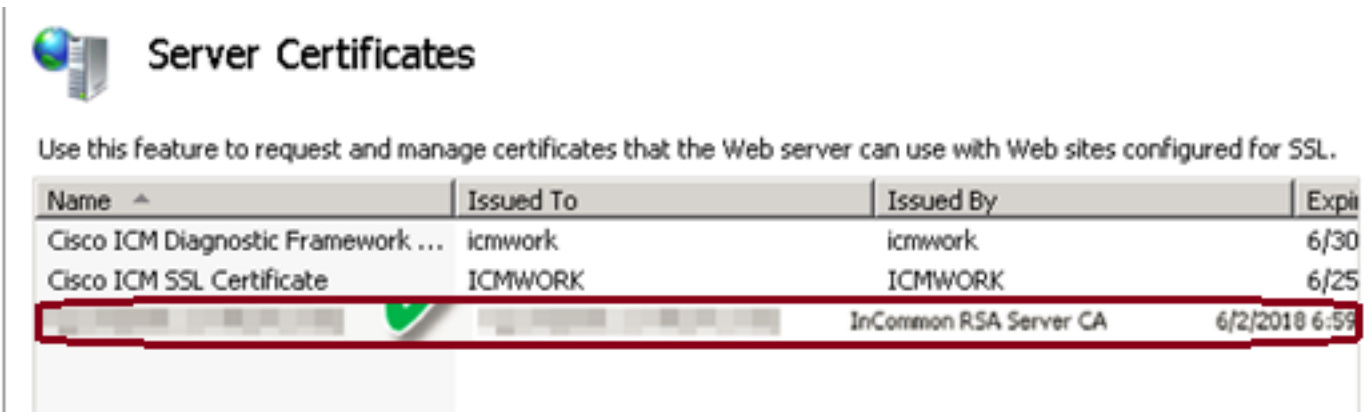
4. Klicken Sie im rechten Teilfenster auf **Aktionen > Zertifikatsanforderung abschließen**, wie in diesem Bild gezeigt.



5. Stellen Sie vor diesem Schritt sicher, dass das signierte Zertifikat im CER-Format vorliegt und auf den lokalen Server hochgeladen wurde. Klicken Sie auf die Schaltfläche ..., um die CER-Datei zu durchsuchen. Verwenden Sie im Namen Friendly den FQDN des Servers, wie in diesem Bild gezeigt.

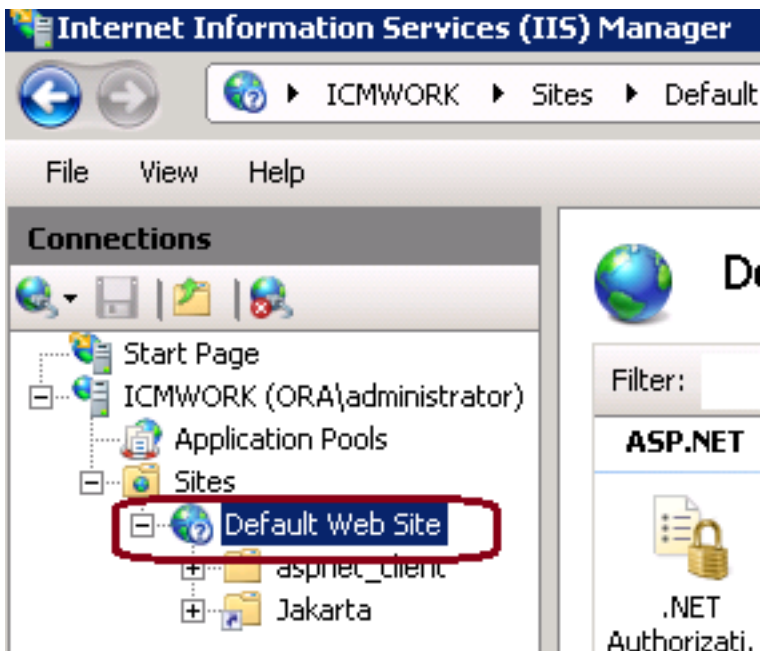


6. Klicken Sie auf OK, um das Zertifikat hochzuladen. Bestätigen Sie nach Abschluss dieses Vorgangs, dass das Zertifikat jetzt im Fenster Serverzertifikate angezeigt wird, wie in diesem Bild gezeigt.



Schritt 3: Binden des signierten CA-Zertifikats an die Standardwebsite

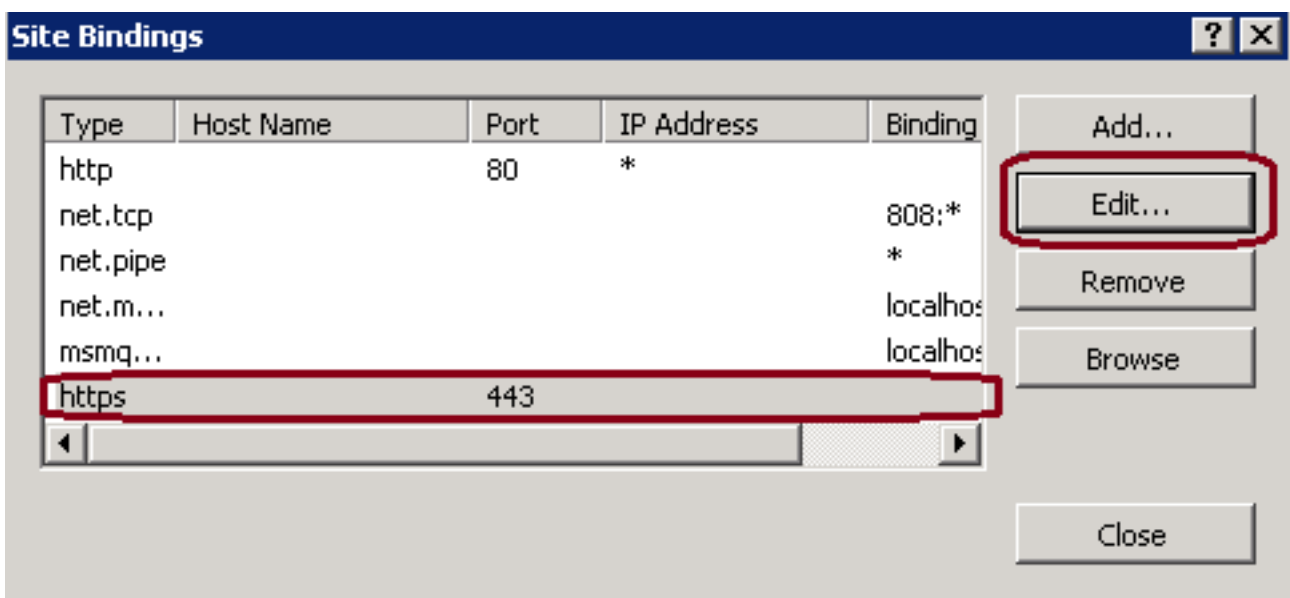
1. Klicken Sie im IIS-Manager auf der linken Seite unter dem Fenster Verbindungen auf **<server_name> > Sites > Default Web Site**, wie in diesem Bild gezeigt.



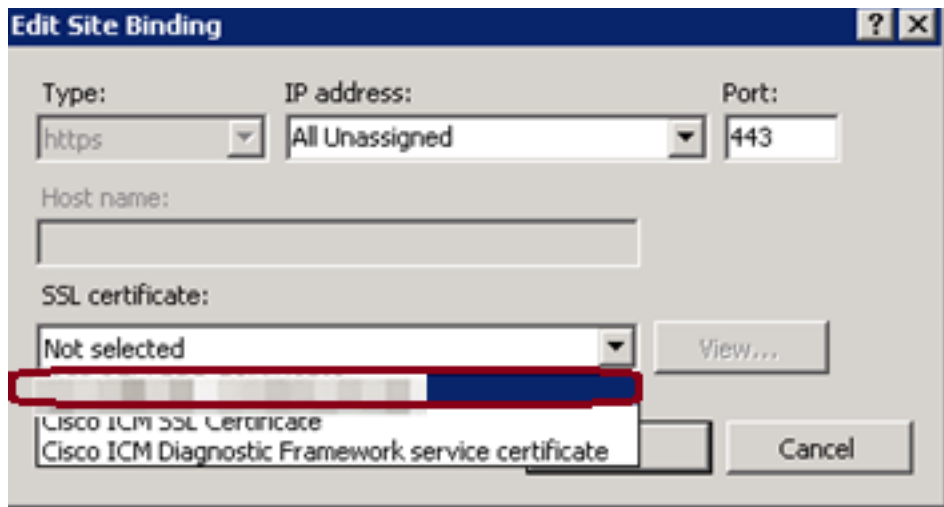
2. Klicken Sie im Fenster Aktionen auf der rechten Seite auf Bindungen, wie in diesem Bild gezeigt.



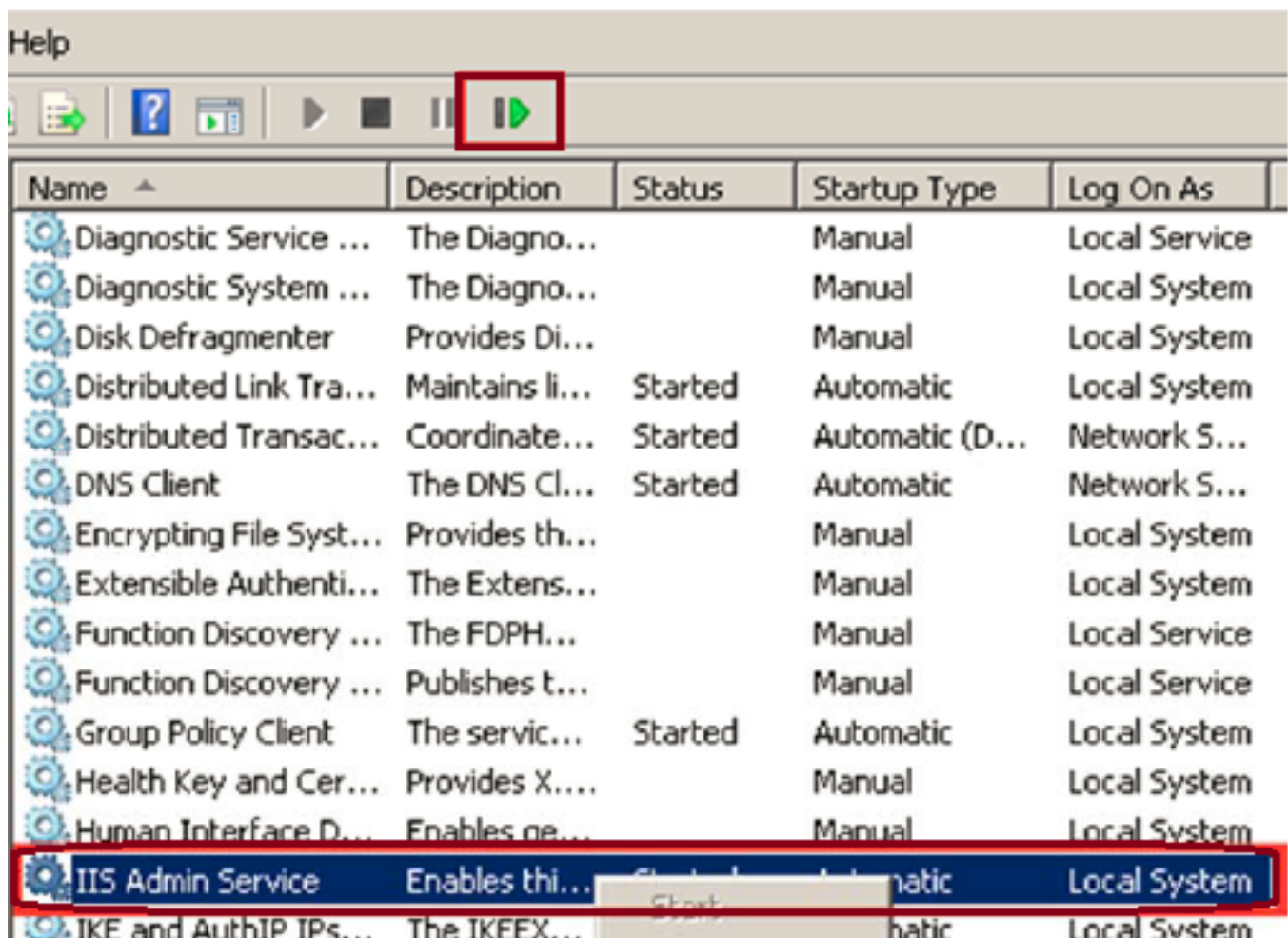
3. Klicken Sie im Fenster für Sitebindungen auf https, um weitere Optionen zu markieren. Klicken Sie auf Bearbeiten, um fortzufahren, wie in diesem Bild gezeigt.



4. Klicken Sie unter dem SSL-Zertifikatparameter auf den Abwärtspfeil, um das zuvor hochgeladene signierte Zertifikat auszuwählen. Zeigen Sie das signierte Zertifikat an, um den Zertifizierungspfad zu überprüfen, und die Werte stimmen mit dem lokalen Server überein. Wenn Sie fertig sind, drücken Sie OK, und schließen Sie das Fenster Site Bindings, wie in diesem Bild gezeigt.



5. Starten Sie den IIS-Admin-Dienst unter dem MMC-Snap-In Dienste neu, indem Sie auf **Start > Ausführen > services.msc** klicken, wie in diesem Bild gezeigt.



6. Bei erfolgreicher Eingabe der FQDN-URL für die Website sollte der Client-Webbrowser keine Warnung wegen eines Zertifikatsfehlers auslösen.

Hinweis: Wenn der IIS-Admin-Dienst fehlt, starten Sie den World Wide Web Publishing-Dienst neu.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.