

UCCE\PCCE - Procedura per ottenere e caricare il certificato CA (Certification Authority) o autofirmato di Windows Server sui server 2008

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1. Genera CSR da Gestione Internet Information Services \(IIS\)](#)

[Passaggio 2. Carica il certificato firmato dalla CA in Gestione Internet Information Services \(IIS\)](#)

[Passaggio 3. Associare il certificato CA firmato al sito Web predefinito](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Discussioni correlate nella Cisco Support Community](#)

Introduzione

In questo documento viene descritto come configurare un certificato autofirmato o un certificato dell'Autorità di certificazione (CA) sui server Windows 2008 R2 dell'organizzazione Unified Contact Center (UCCE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del processo dei certificati firmati e autofirmati.

Componenti usati

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

- Windows 2008 R2
- UCCE 10.5(1)

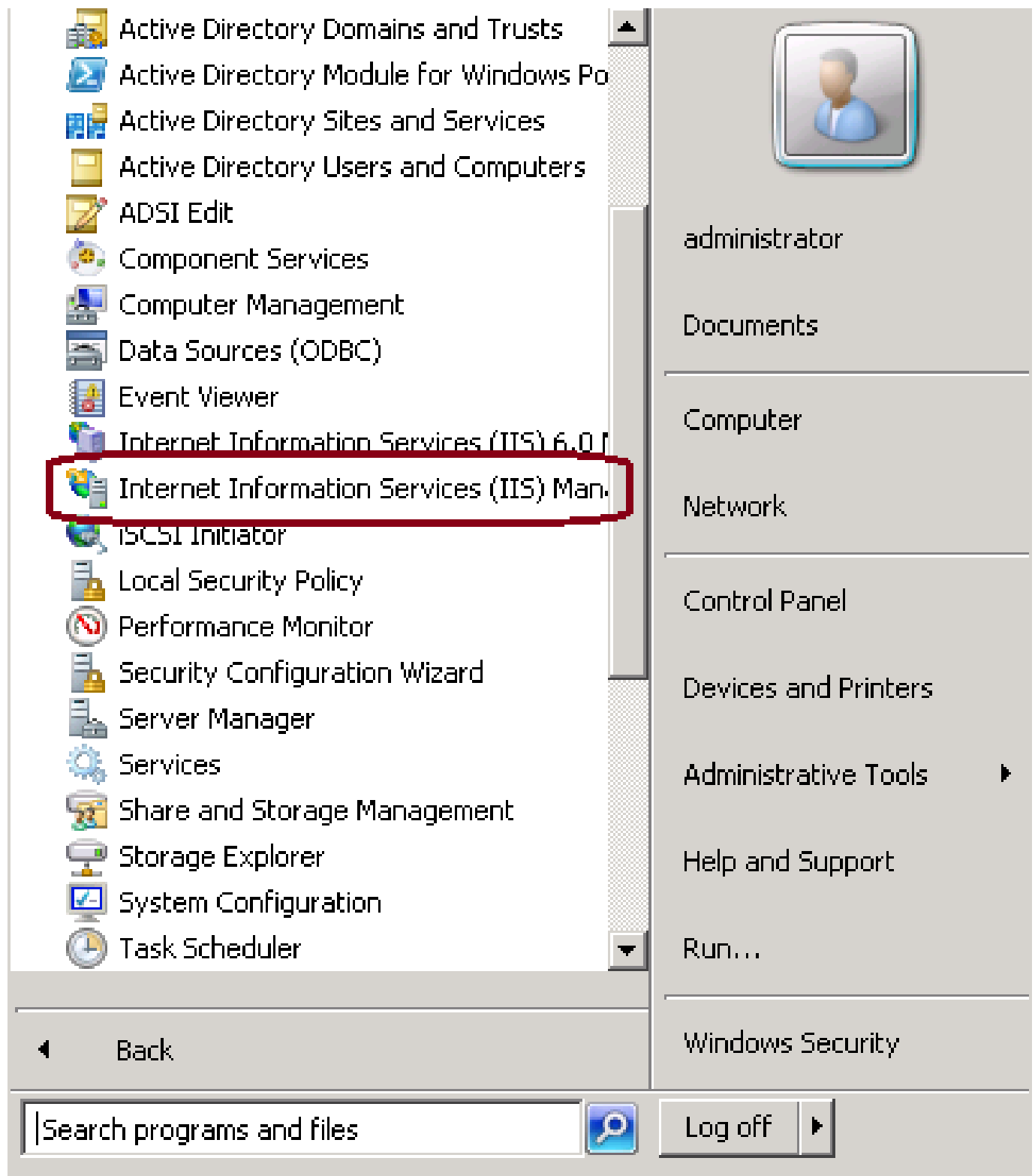
Configurazione

L'impostazione del certificato per la comunicazione HTTPS su Windows Server è un processo in tre passaggi

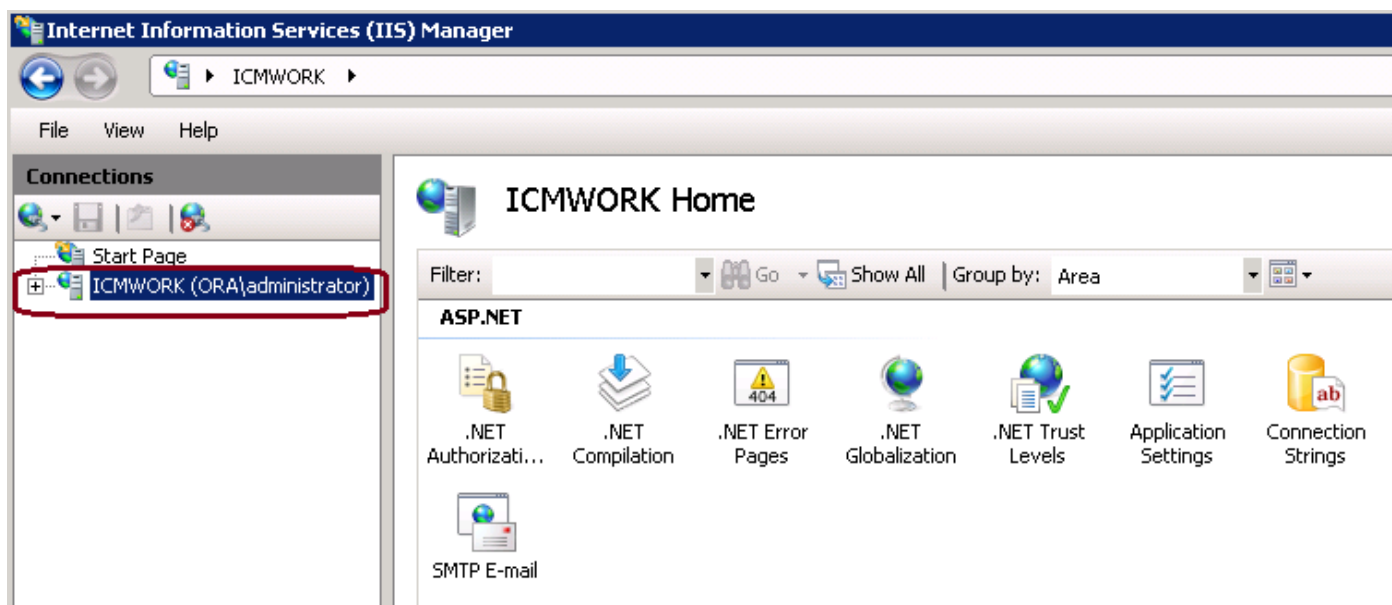
- Genera richiesta di firma del certificato (CSR) da Gestione Internet Information Services (IIS)
- Carica il certificato firmato dalla CA in Gestione Internet Information Services (IIS)
- Associare il certificato CA firmato al sito Web predefinito

Passaggio 1. Genera CSR da Gestione Internet Information Services (IIS)

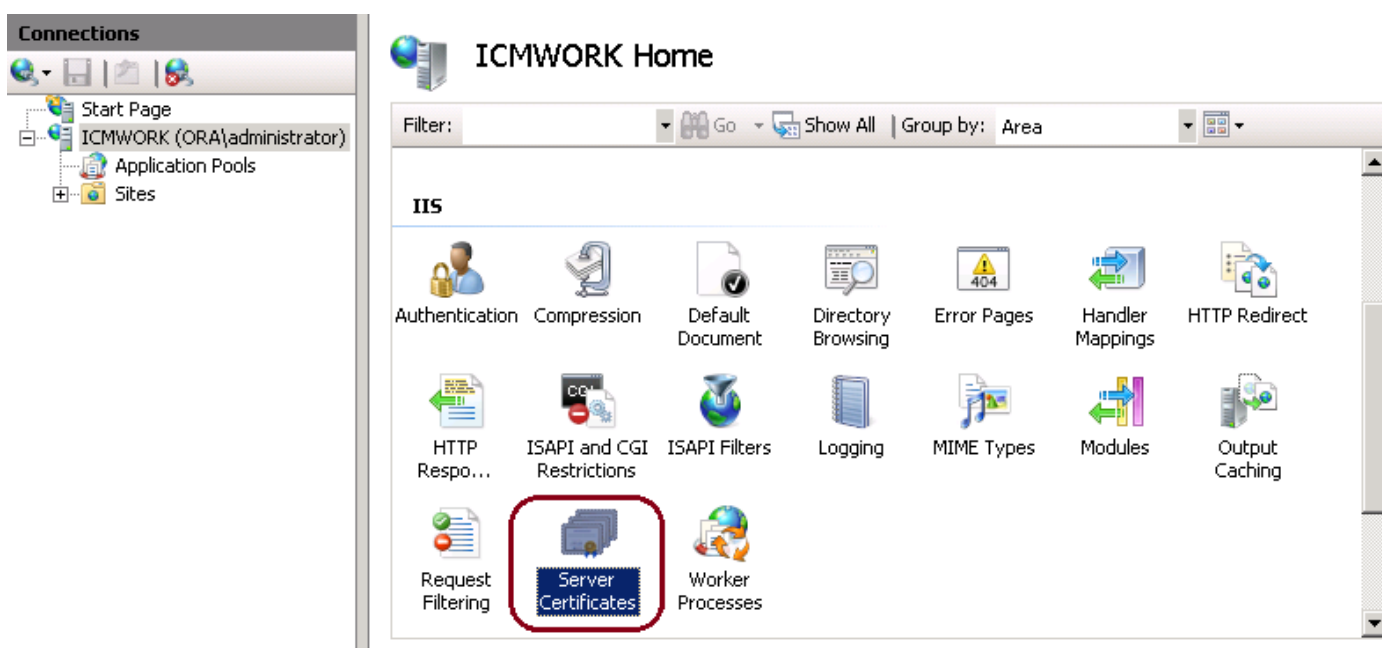
1. Accedere a Windows, fare clic su Start > Esegui > Tutti i programmi > Strumenti di amministrazione > Gestione Internet Information Services (IIS), come mostrato nell'immagine. Non selezionare IIS versione 6 se esistente.



2. Nel riquadro a sinistra della finestra Connessioni, selezionare il nome del server, come mostrato in questa immagine.



3. Nel riquadro centrale della finestra, selezionare IIS > Certificati server. Fare doppio clic su Certificati server per generare la finestra del certificato, come illustrato in questa immagine.



4. Nel riquadro di destra, fare clic su Azioni > Crea richiesta certificato, come mostrato in questa immagine.

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

Create Self-Signed Certificate...




Help

Online Help

5. Per completare la richiesta di certificato, inserire il nome comune, l'organizzazione, l'unità organizzativa, la città/località, lo stato/provincia e il paese/area geografica, come illustrato nella seguente immagine.

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. Fare clic su Avanti per modificare la lunghezza in bit della crittografia e della protezione. Per una maggiore sicurezza, si consiglia di utilizzare almeno 2048, come mostrato nell'immagine.

Request Certificate ? X

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

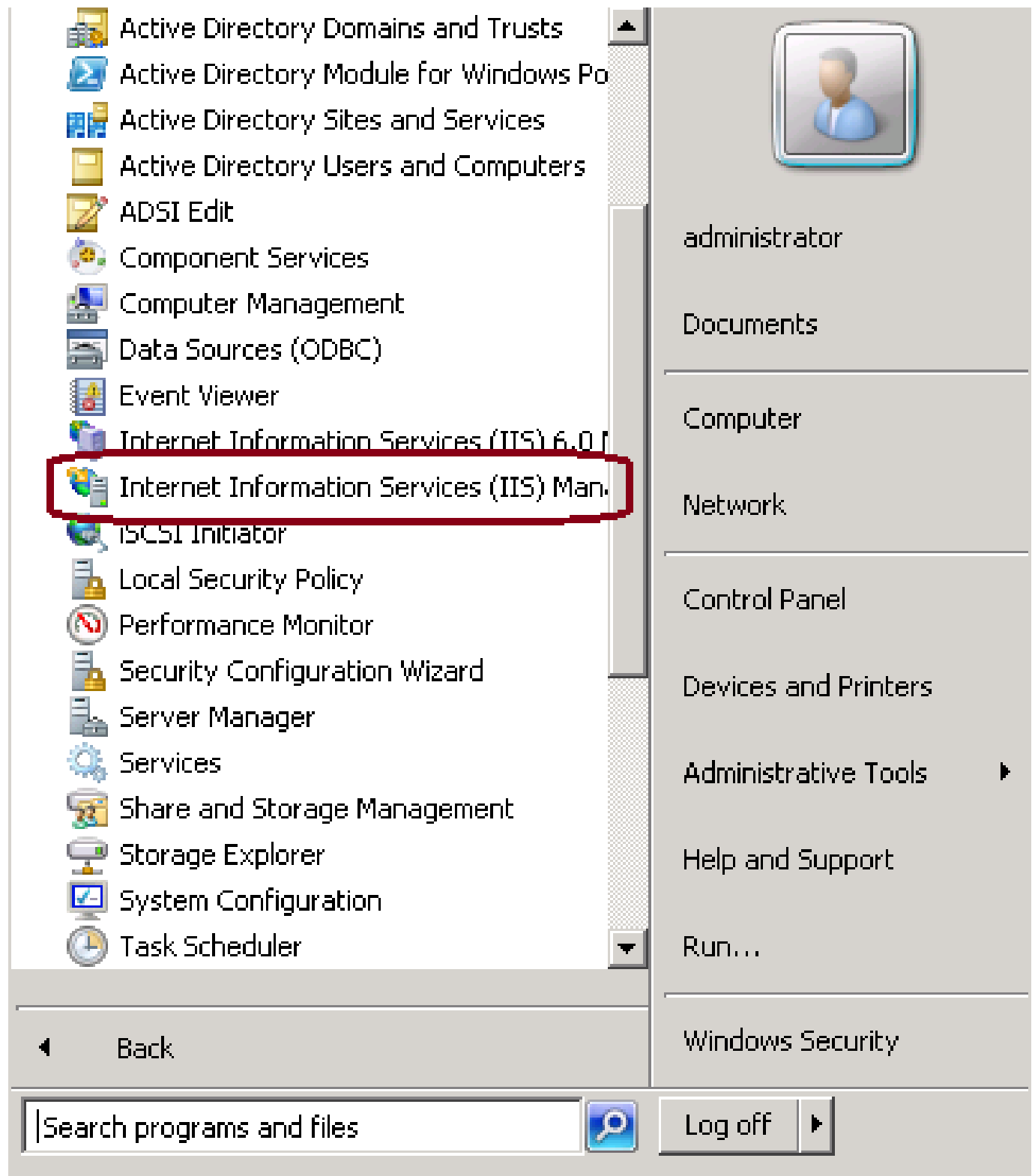
7. Salvare la richiesta di certificato nella posizione desiderata, che verrà salvata in formato .TXT,

come mostrato nell'immagine.

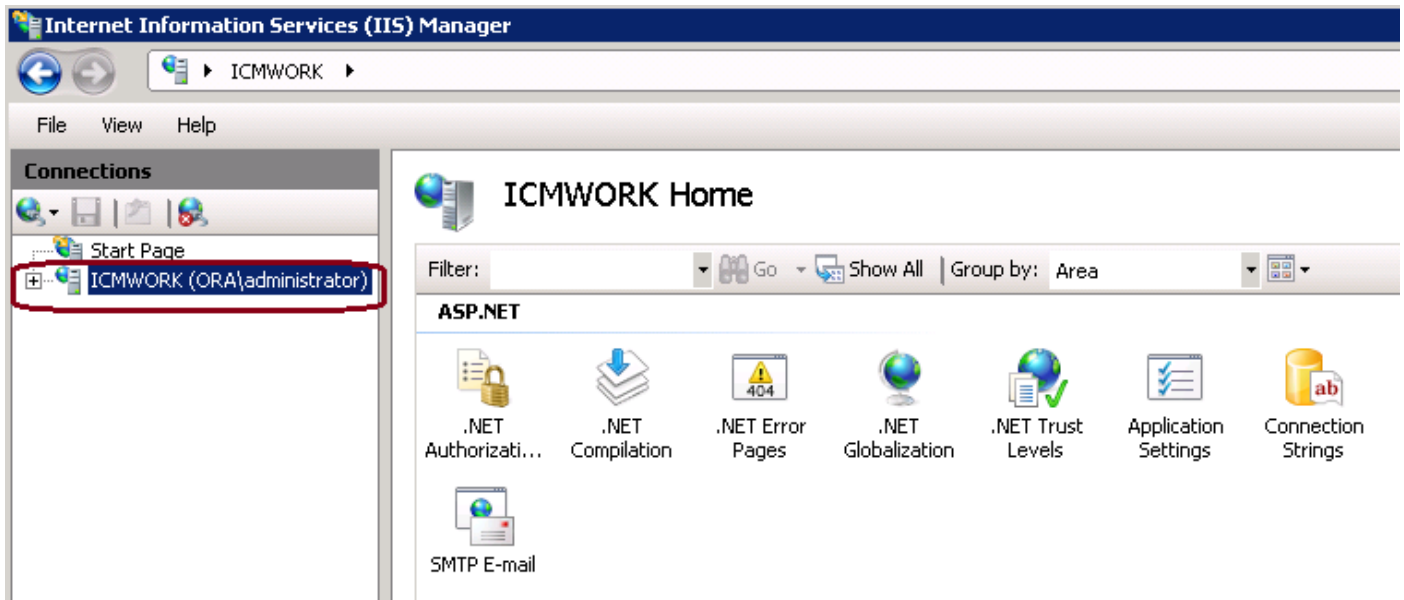
8. Fornire che il file sia firmato dal team che gestisce la richiesta del servizio CA interna o esterna, come mostrato nell'immagine.

Passaggio 2. Carica il certificato firmato dalla CA in Gestione Internet Information Services (IIS)

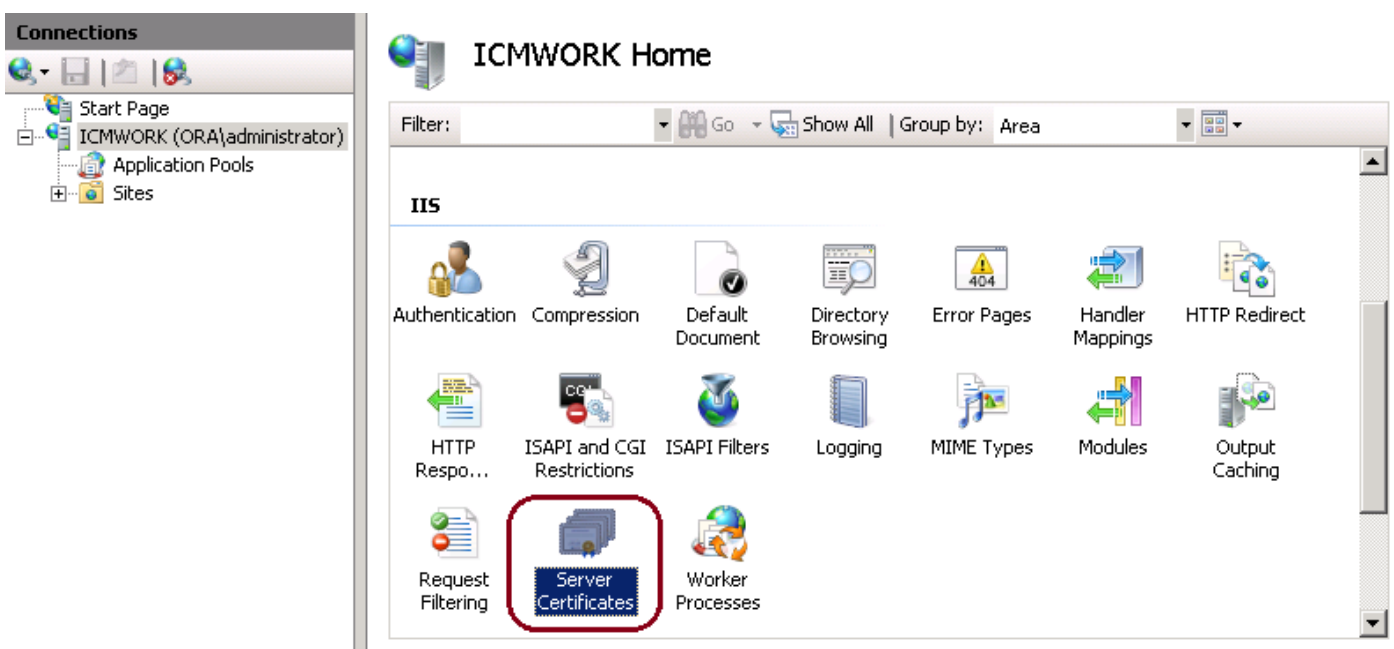
1. Accedere a Windows, fare clic su Start > Esegui > Tutti i programmi > Strumenti di amministrazione > Gestione Internet Information Services (IIS), come illustrato in questa immagine. Non selezionare IIS versione 6 se esistente.



2. Nel riquadro a sinistra della finestra Connessioni, selezionare il nome del server, come mostrato in questa immagine.



3. Nel riquadro centrale della finestra, selezionare IIS > Certificati server. Fare doppio clic su Certificati server per generare la finestra del certificato, come mostrato nell'immagine.



4. Nel riquadro di destra, fare clic su Azioni > Completa richiesta certificato, come mostrato in questa immagine.

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

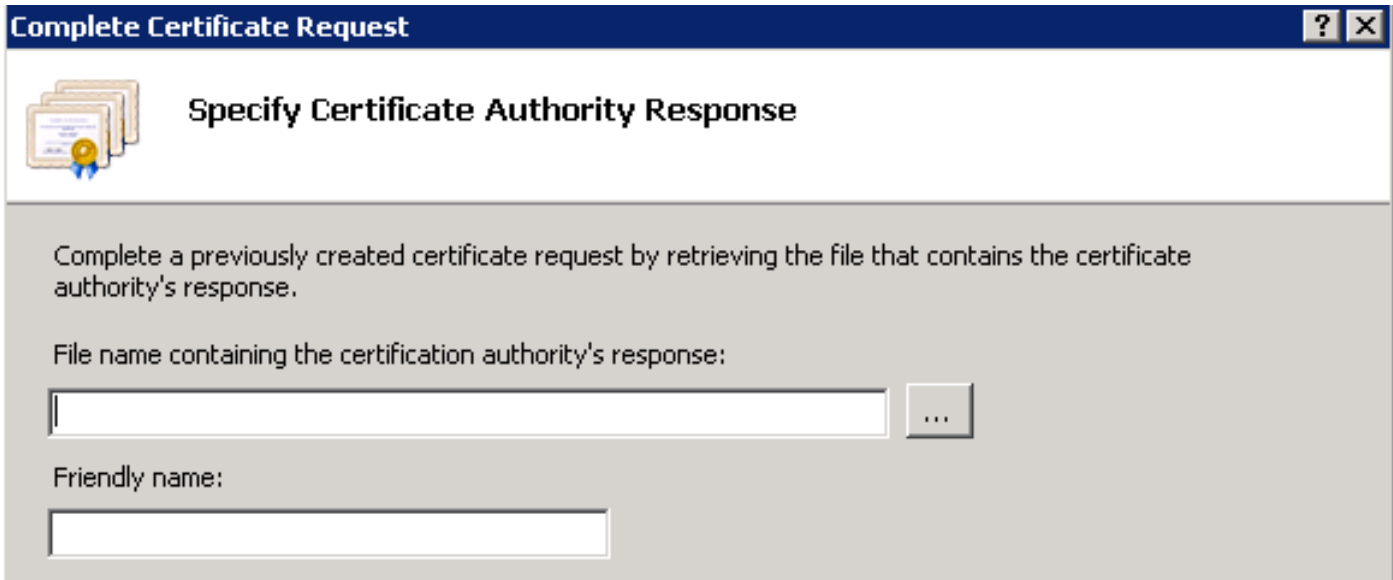
Create Self-Signed Certificate...



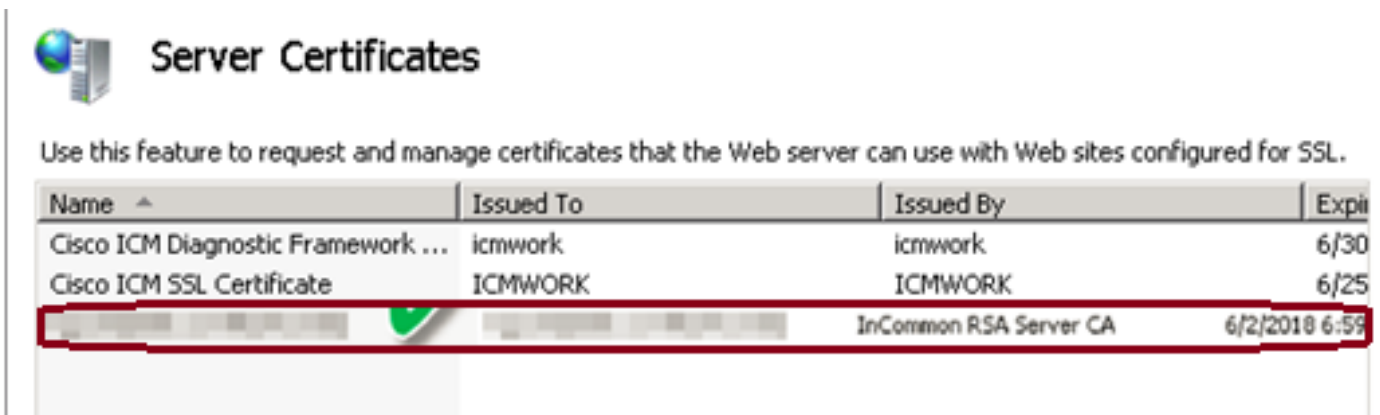
Help

Online Help

5. Prima di questa fase, verificare che il certificato firmato sia in formato CER e sia stato caricato nel server locale. Fare clic sul pulsante ... per sfogliare il file con estensione CER. All'interno del nome descrittivo, utilizzare il nome di dominio completo del server, come illustrato in questa immagine.

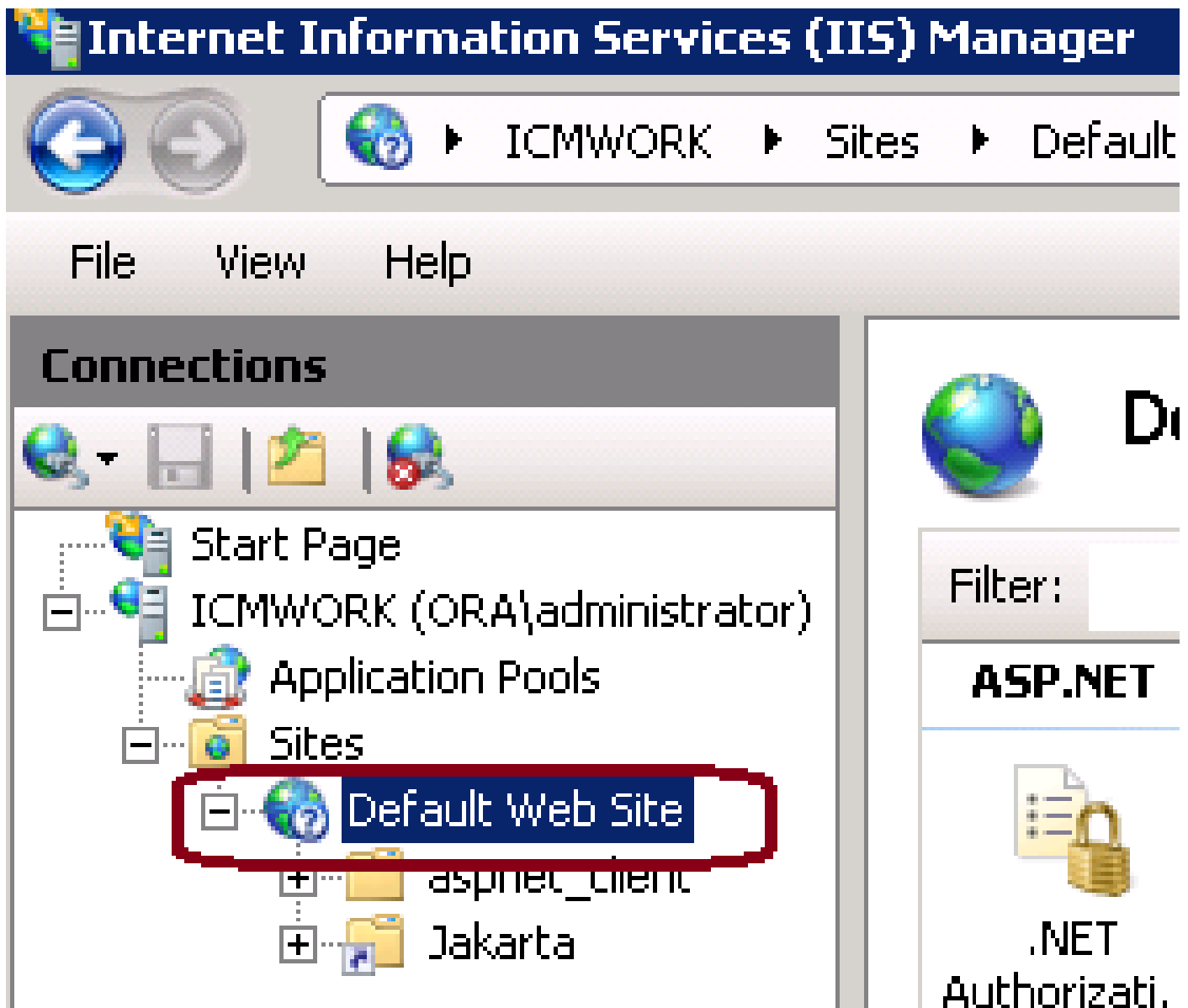


6. Scegliere OK per caricare il certificato. Al termine, verificare che il certificato sia visualizzato nella finestra Certificati server, come illustrato nell'immagine.



Passaggio 3. Associare il certificato CA firmato al sito Web predefinito

1. In Gestione IIS Sotto il piano della finestra Connessioni, fare clic con il pulsante sinistro del mouse su <nome_server> > Siti > Sito Web predefinito, come mostrato in questa immagine.



2. Sotto il riquadro a destra della finestra Azioni, fare clic su Associazioni, come mostrato in questa immagine.

Actions



Explore

Edit Permissions...

Edit Site

Bindings...

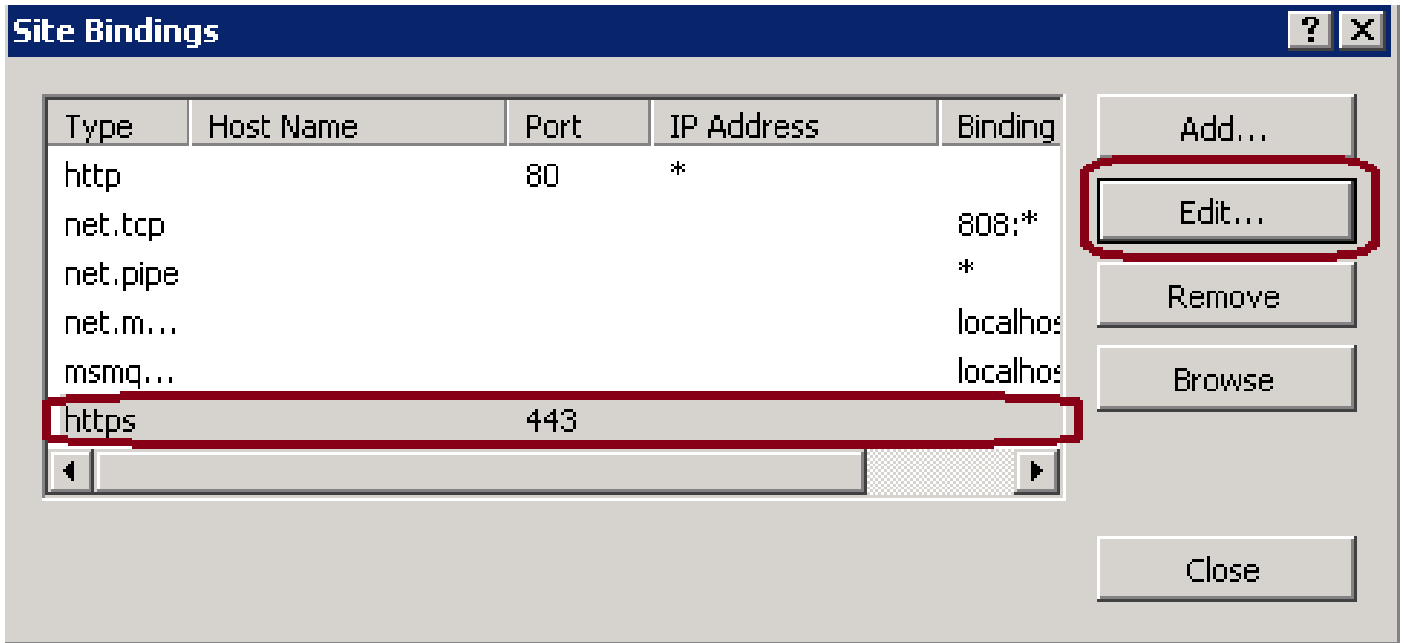


Basic Settings...

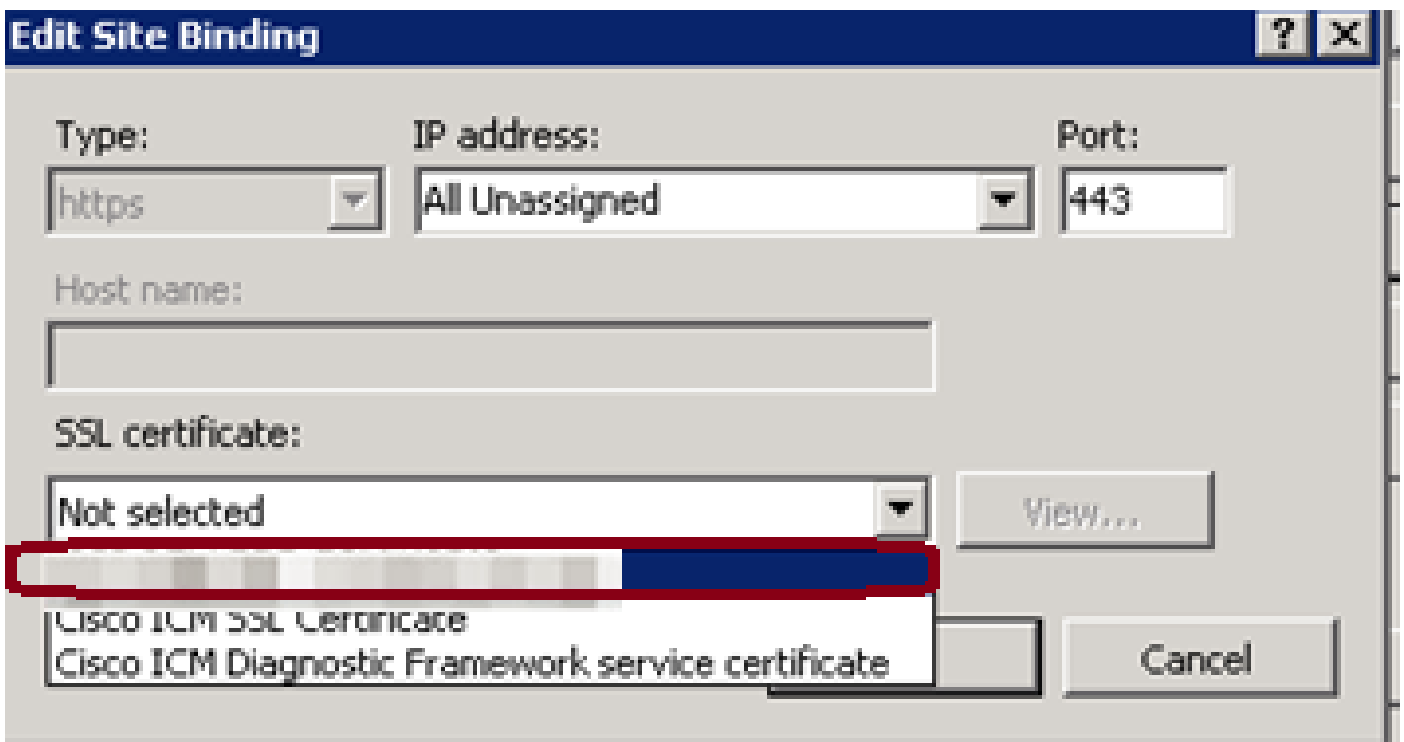
View Applications

View Virtual Directories

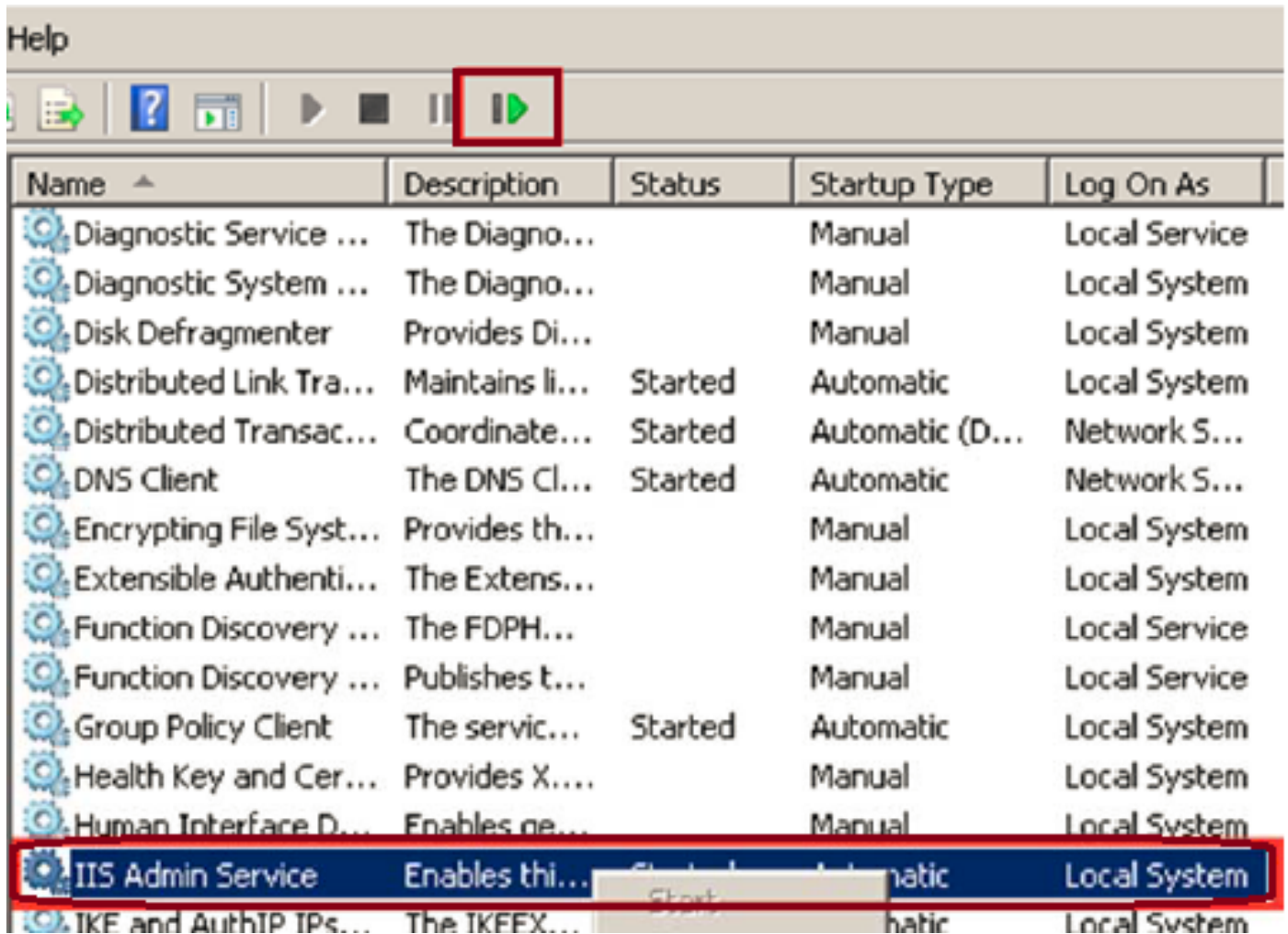
3. Nella finestra binding sito, fare clic su https per evidenziare altre opzioni. Fare clic su Modifica per continuare, come mostrato nell'immagine.



4. In corrispondenza del parametro del certificato SSL, fare clic sulla freccia in giù per selezionare il certificato firmato caricato in precedenza. Visualizzare il certificato firmato per verificare che il percorso della certificazione e i valori corrispondano al server locale. Al termine, fare clic su OK, quindi su Chiudi per uscire dalla finestra Associazioni sito, come mostrato nell'immagine.



5. Riavviare il servizio Amministrazione di IIS nello snap-in MMC Servizi facendo clic su Start > Eseguì > services.msc., come mostrato nell'immagine.



6. Se l'operazione ha esito positivo, il browser Web del client non deve visualizzare alcun avviso di errore del certificato quando si immette l'URL FQDN per il sito Web.

Nota: se il servizio di amministrazione di IIS non è presente, riavviare il servizio Pubblicazione sul Web.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).