

UCCE \ PCCE - Procedimento para obter e transferir arquivos pela rede o - do auto de Windows Server assinado ou os server do certificado do Certificate Authority (CA) 2008

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Etapa 1. Gerencia o CSR do gerente do Internet Information Services \(IIS\)](#)

[Etapa 2. Transfira arquivos pela rede o certificado assinado de CA ao gerente do Internet Information Services \(IIS\)](#)

[Etapa 3. Ligue o certificado de CA assinado à website padrão](#)

[Verificar](#)

[Troubleshooting](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este original descreve como configurar certificado Auto-assinada ou do Certificate Authority (CA) na empresa unificada do centro de contato (UCCE) Windows 2008 server R2.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do processo assinada e do certificado auto-assinado.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software:

- Windows 2008 R2
- UCCE 10.5(1)

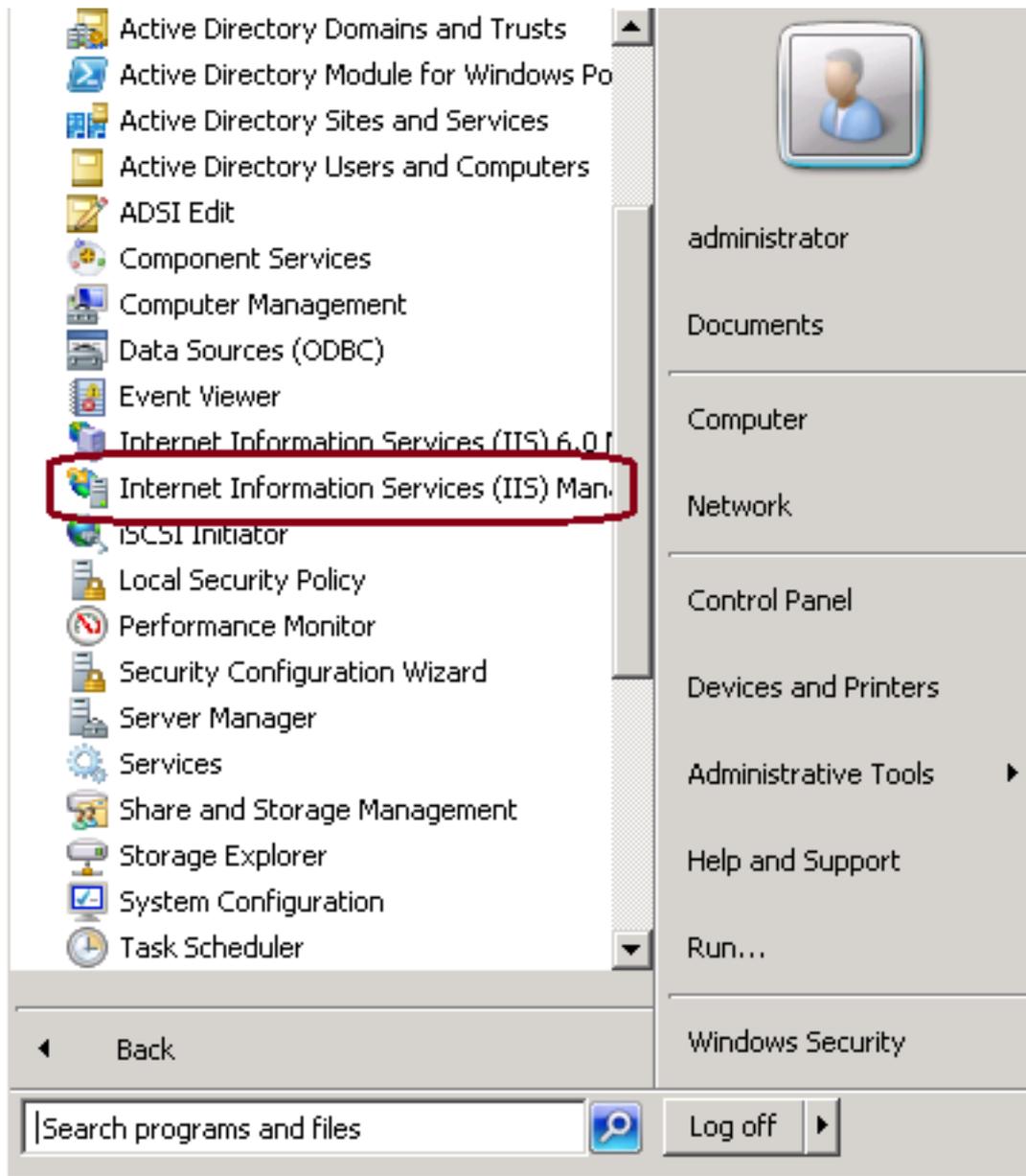
Configurar

Estabelecer o certificado para uma comunicação HTTPS no Windows Server é um processo de etapa de três

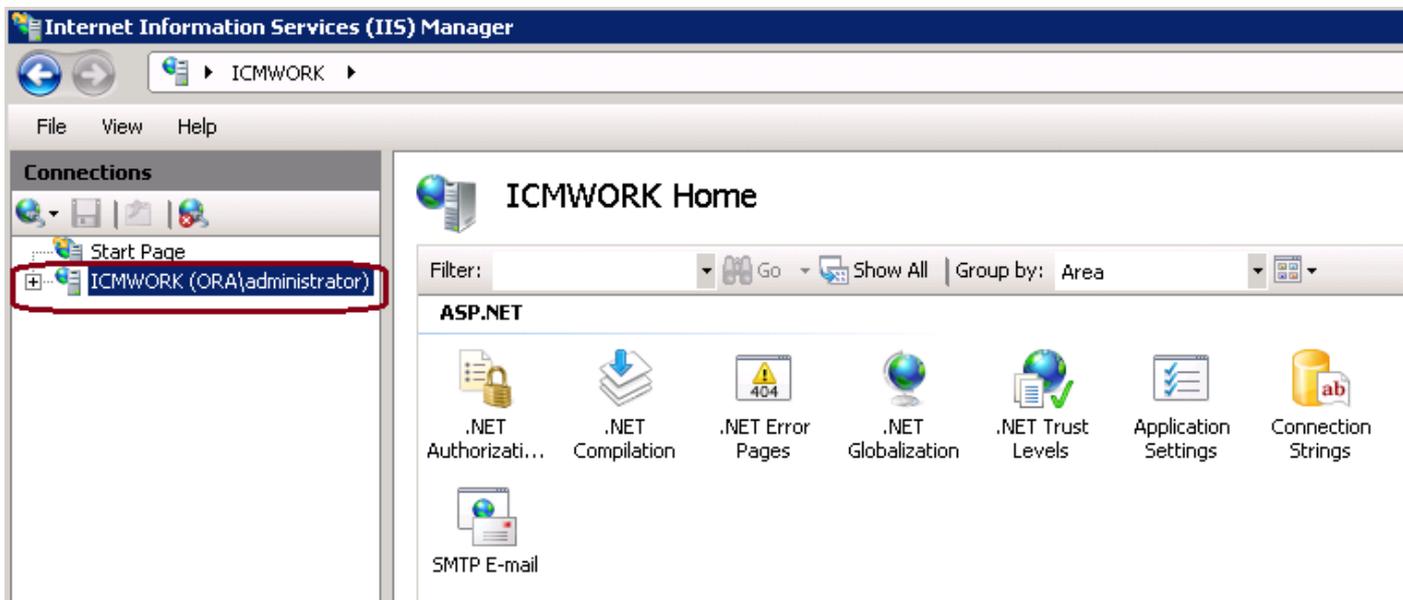
- Gerencia a solicitação de assinatura de certificado (CSR) do gerente do Internet Information Services (IIS)
- Transfira arquivos pela rede o certificado assinado de CA ao gerente do Internet Information Services (IIS)
- Ligue o certificado de CA assinado à website padrão

Etapa 1. Gerencia o CSR do gerente do Internet Information Services (IIS)

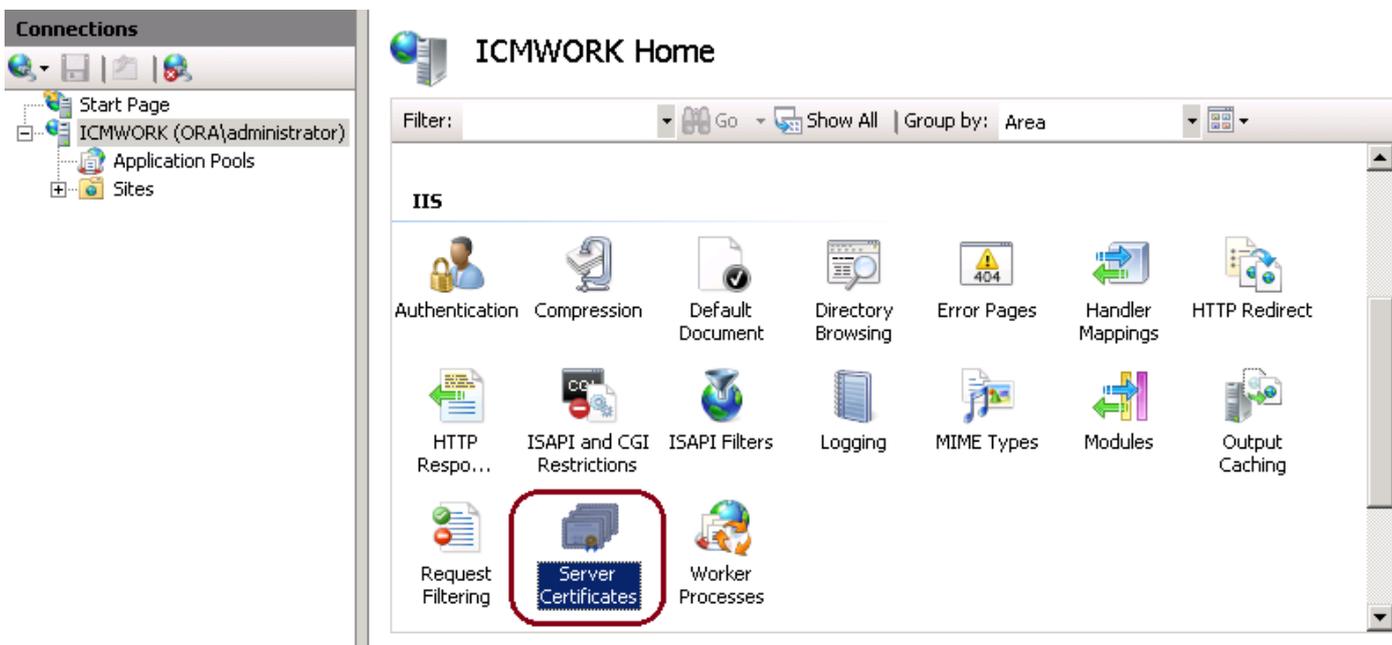
1. Entre a Windows, **Iniciar > Executar do clique > todos os programas > ferramentas administrativas > gerente do Internet Information Services (IIS)**, segundo as indicações desta imagem. Não selecione a versão 6 IIS se existe.



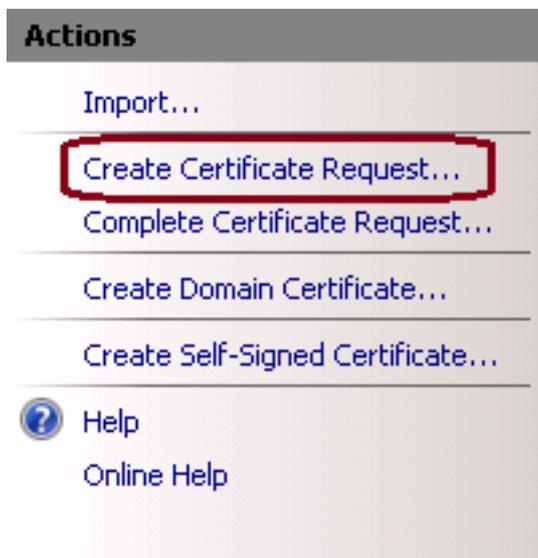
2. Na placa de indicador das conexões ao esquerda, selecione o nome do servidor, segundo as indicações desta imagem.



3. Na placa de janela intermediária, selecione **IIS > certificados de servidor**. Fazer duplo clique em certificados de servidor para gerar o indicador do certificado, segundo as indicações desta imagem.



4. No painel correto, clique sobre **ações > criam o pedido do certificado**, segundo as indicações desta imagem.



5. Para terminar o pedido do certificado, entre na unidade do Common Name, da organização, da organização, na cidade/localidade, no estado/província e no país/região, segundo as indicações desta imagem.

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:

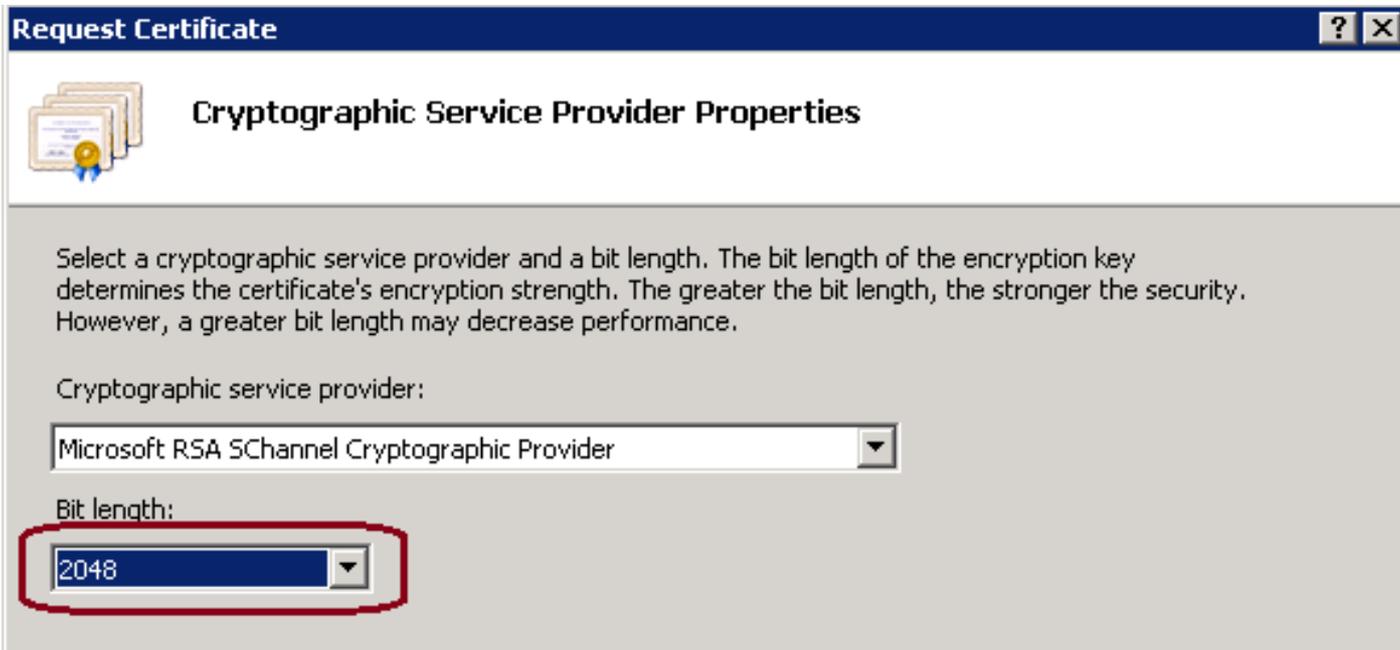
City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

6. O clique ao lado de altera o criptograficamente e comprimento de bit da Segurança, recomenda-se usar pelo menos 2048 para a melhor Segurança, segundo as indicações desta imagem.

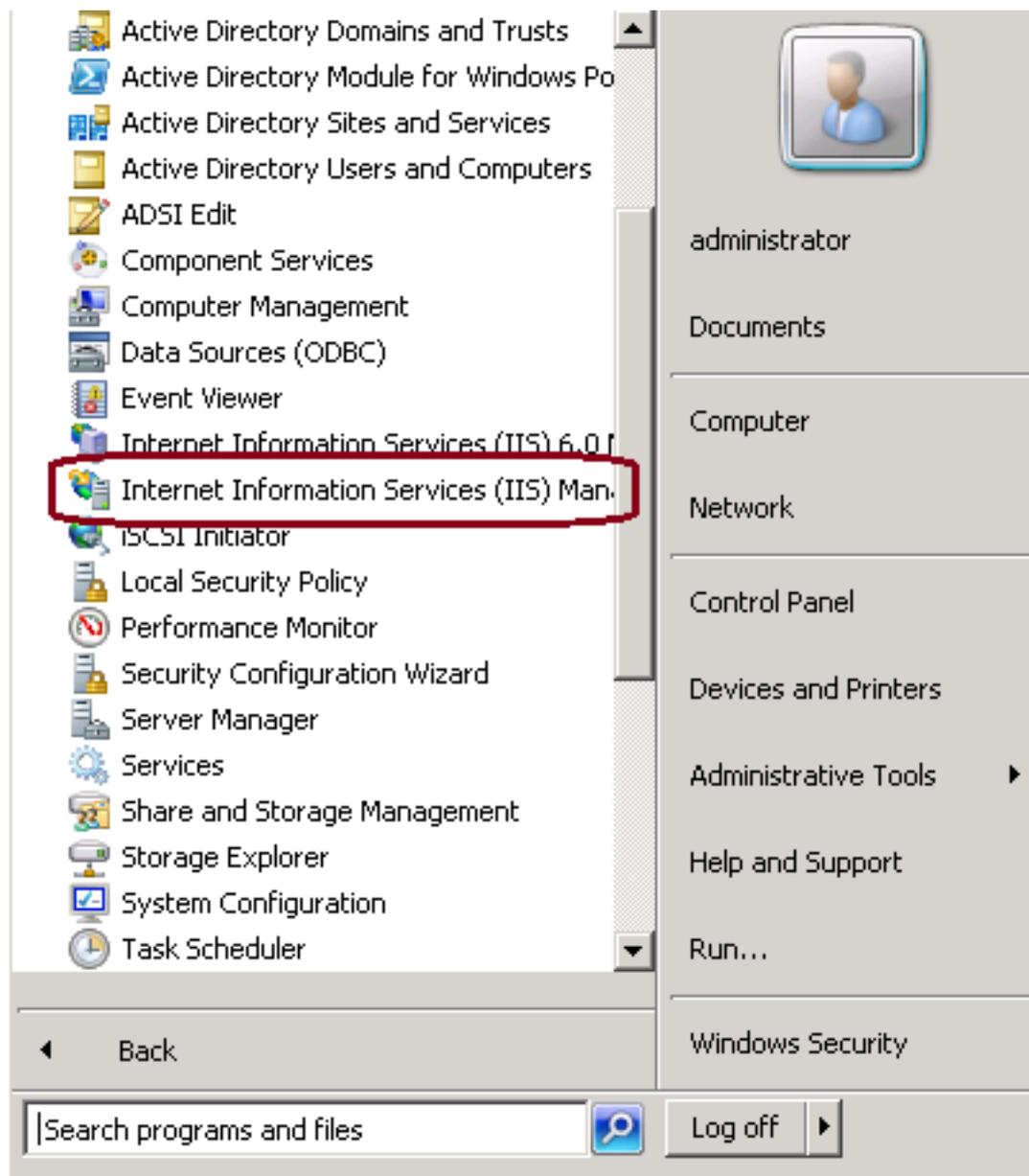


7. Salvar o pedido do certificado no lugar desejado que salvar como um formato do .TXT, segundo as indicações desta imagem.

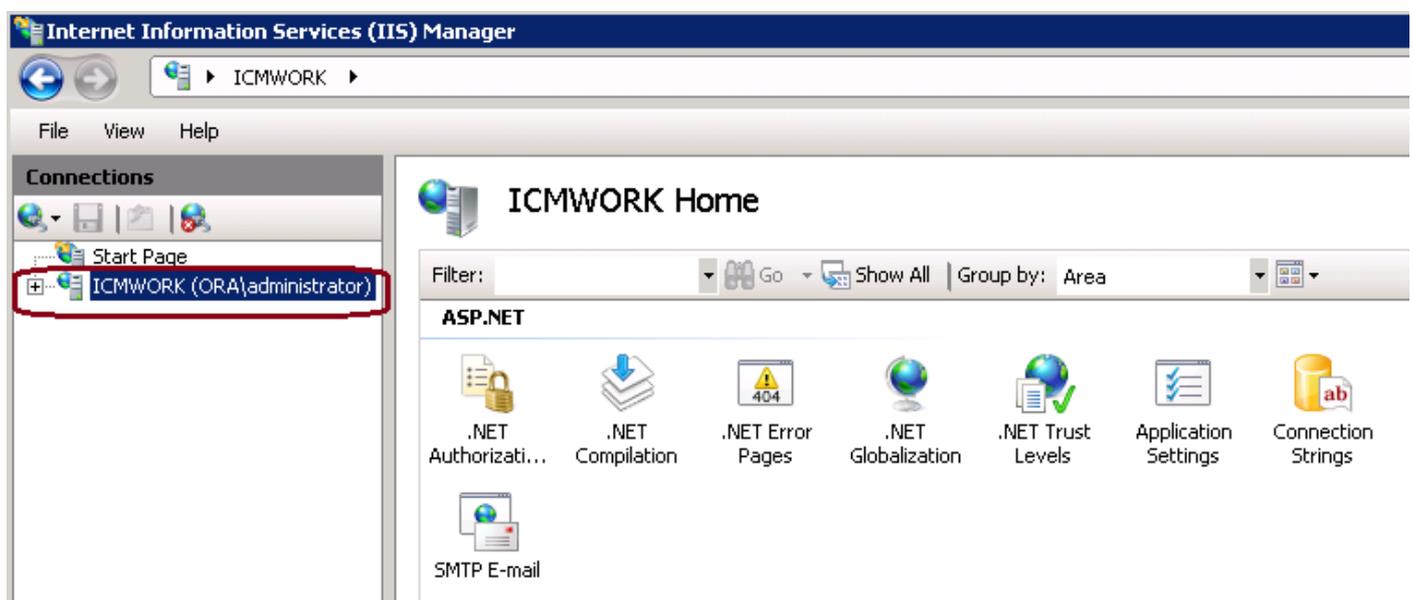
8. Forneça este arquivo a ser assinado pela equipe que controla CA interno ou o pedido externo do serviço de CA, segundo as indicações desta imagem.

Etapa 2. Transfira arquivos pela rede o certificado assinado de CA ao gerente do Internet Information Services (IIS)

1. Entre a Windows, **Iniciar > Executar do clique > todos os programas > ferramentas administrativas > gerente do Internet Information Services (IIS)**, segundo as indicações desta imagem. Não selecione a versão 6 IIS se existe.

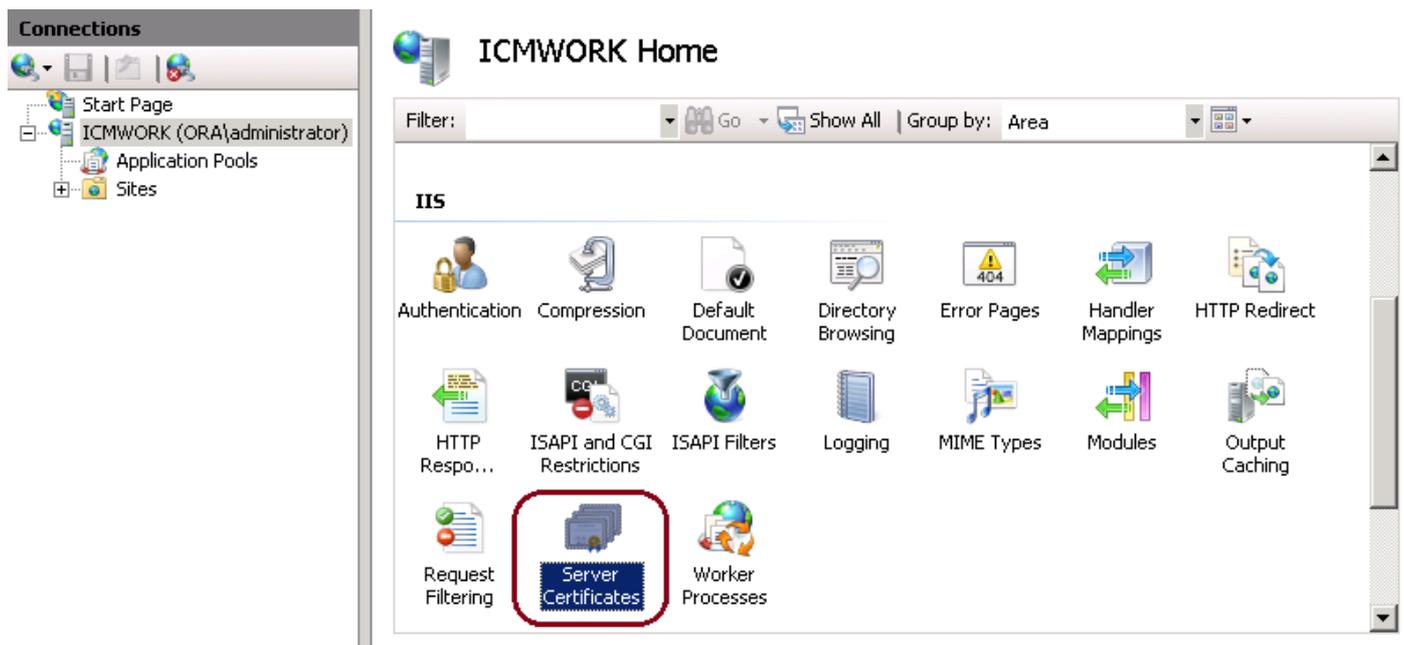


2. Na placa de indicador das conexões ao esquerda, selecione o nome do servidor, segundo as indicações desta imagem.

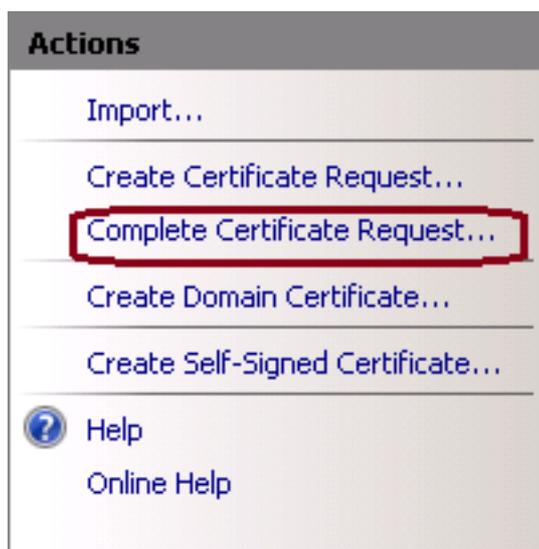


3. Na placa de janela intermediária, selecione **IIS > certificados de servidor**. Fazer duplo clique em

certificados de servidor para gerar o indicador do certificado, segundo as indicações desta imagem.



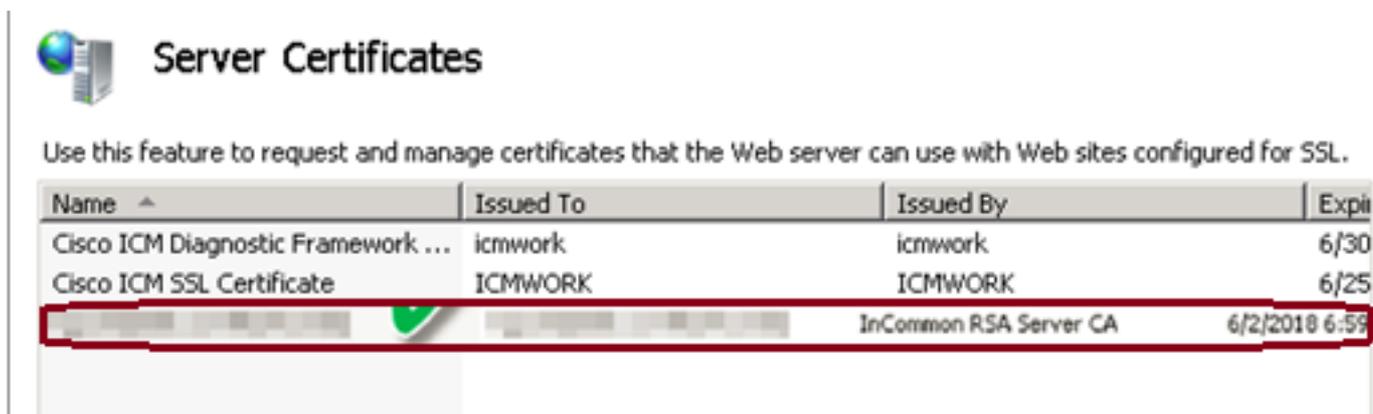
4. No painel correto, clique sobre **ações > pedido do certificado completo**, segundo as indicações desta imagem.



5. Antes desta etapa, assegure-se de que o certificado assinado esteja no formato .CER e esteja transferido arquivos pela rede ao servidor local. Clique... o botão para consultar o arquivo .CER. Dentro do nome amigável, use o FQDN do server, segundo as indicações desta imagem.

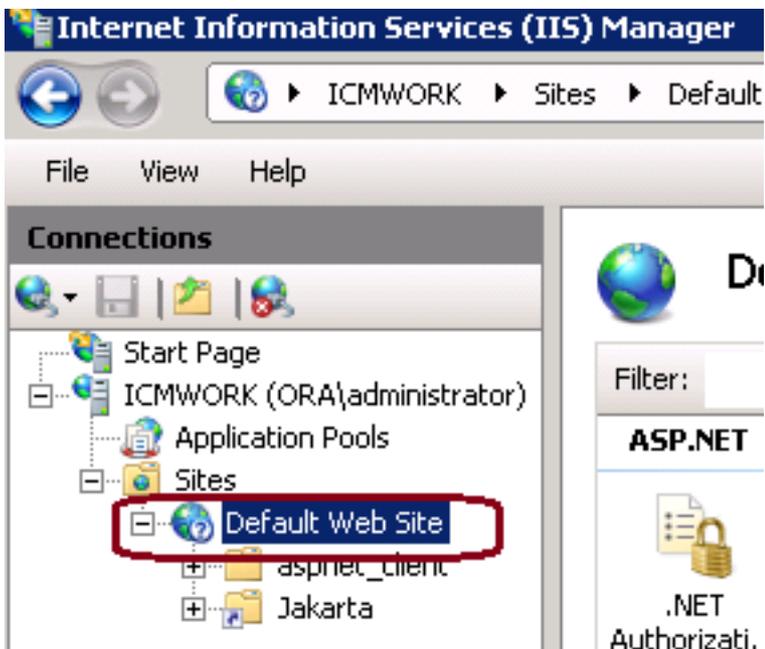


6. Clique a **APROVAÇÃO** para transferir arquivos pela rede o certificado. Quando completo, confirme o certificado aparece agora no indicador dos certificados de servidor, segundo as indicações desta imagem.

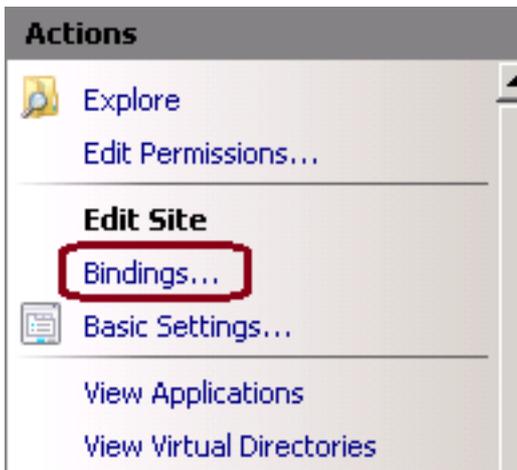


Etapa 3. Ligue o certificado de CA assinado à website padrão

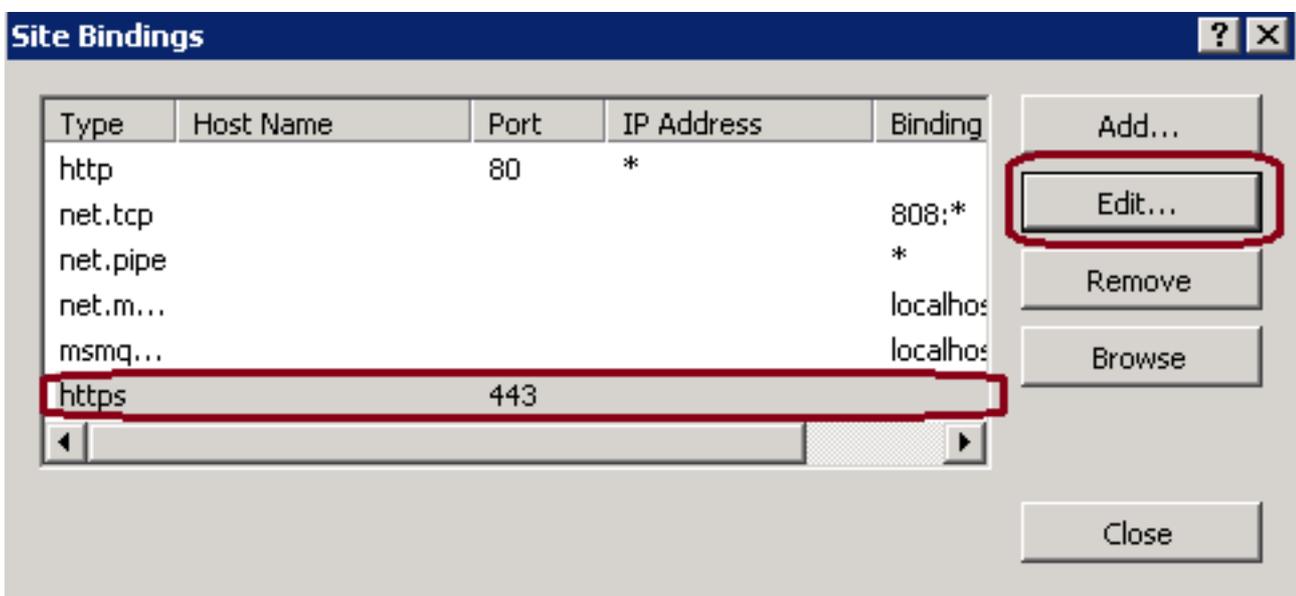
1. No gerenciador de IIS sob o plano do indicador das conexões, a mão esquerda, clica sobre o **<server_name>** > os locais > a **website padrão**, segundo as indicações desta imagem.



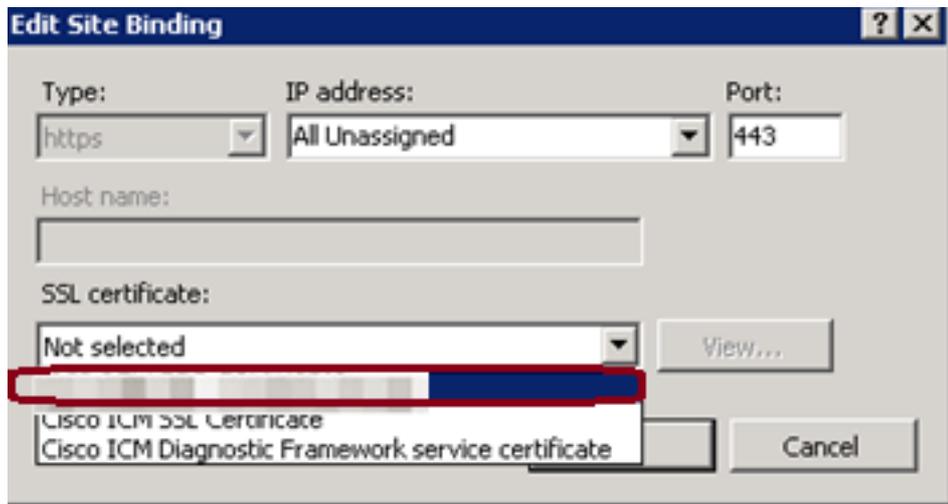
2. Sob a placa de indicador das ações no lado direito, clique sobre emperramentos, segundo as indicações desta imagem.



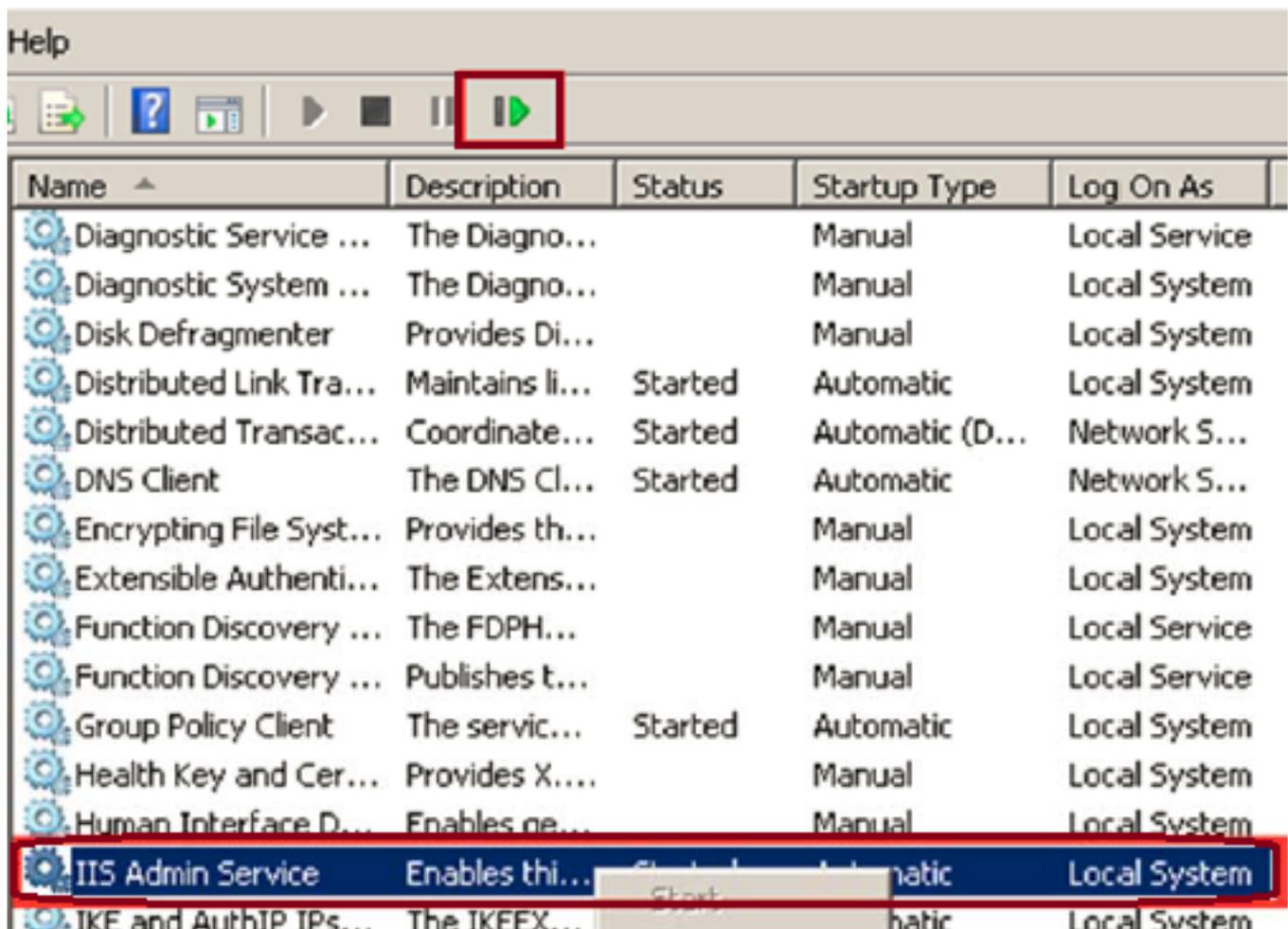
3. No indicador dos emperramentos do local, clique sobre https para destacar mais opções. Clique sobre Edit para continuar, segundo as indicações desta imagem.



4. Sob o parâmetro do certificado SSL, clique sobre a seta para baixo para selecionar o certificado assinado transferido arquivos pela rede previamente. Veja o certificado assinado para verificar o caminho de certificação e avalie fósforos o servidor local. Quando APROVAÇÃO terminada da imprensa, então perto da saída fora do indicador dos emperramentos do local, segundo as indicações desta imagem.



5. Reinicie o serviço IIS Admin sob os serviços MMC pressão-no clique no **Iniciar > Executar > no services.msc.** , segundo as indicações desta imagem.



6. Se bem sucedido, o navegador da Web do cliente não deve alertar nenhum aviso do erro do certificado ao entrar no FQDN URL para o site.

Note: Se o serviço IIS Admin falta reinicie o Serviço de Publicação na Web.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.