UCCE\PCCE - Процедура, чтобы получить и загрузить Windows Server Сам? Подписанный или Сертификат Центра сертификации (CA) на 2008 серверах

Содержание

Введение

Этот документ описывает, как настроить Самоподписанный или Сертификат Центра сертификации (CA) на серверах Windows 2008 R2 Унифицированного предприятия Contact Center (UCCE).

Предварительные условия

Требования

Cisco рекомендует ознакомиться с процессом Со знаком и процессом Подписанного сертификата.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Windows 2008 R2
- UCCE 10.5 (1)

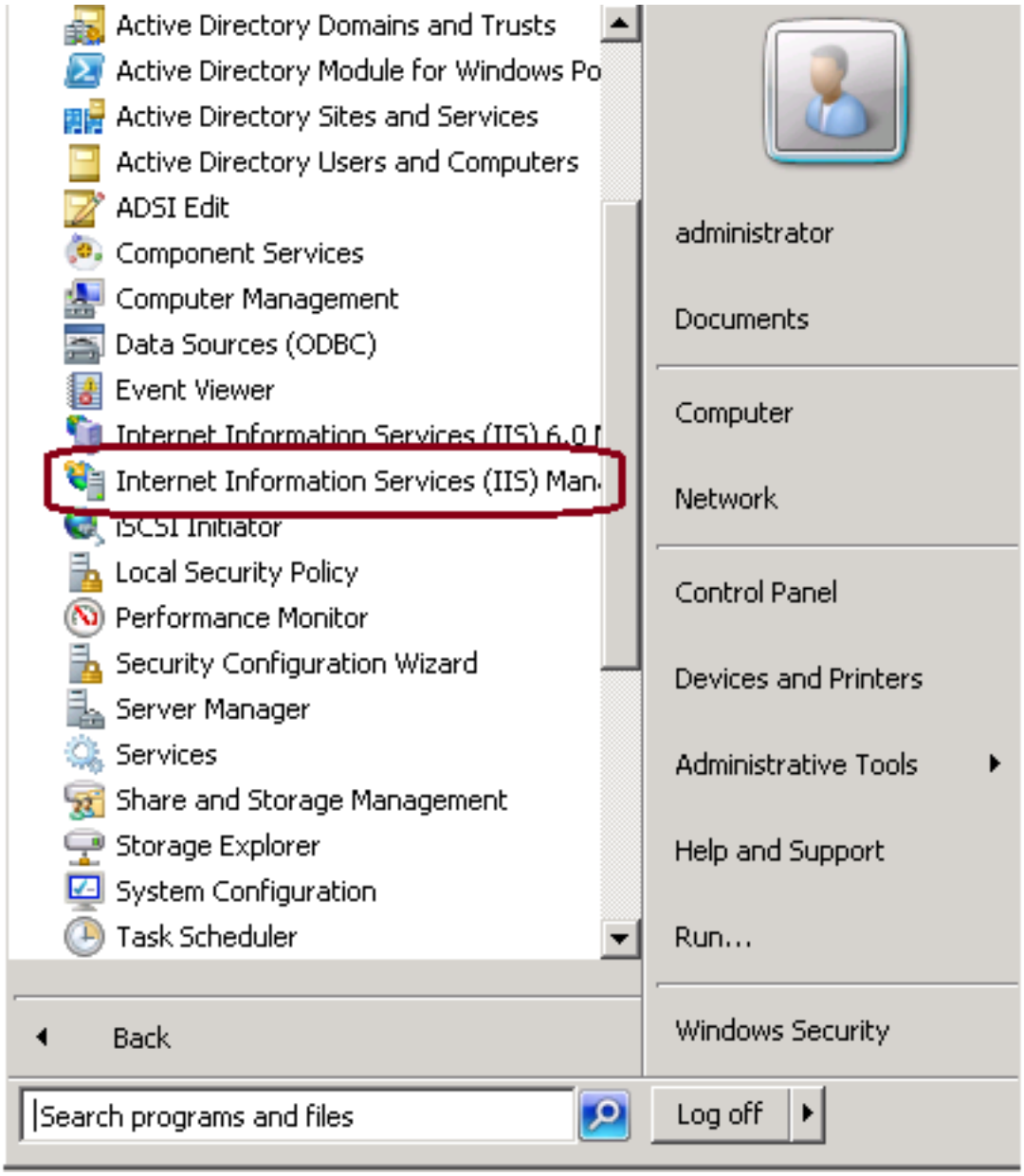
Настройка

Устанавливание сертификата для Связи HTTPS на Windows Server является тремя процессами шага

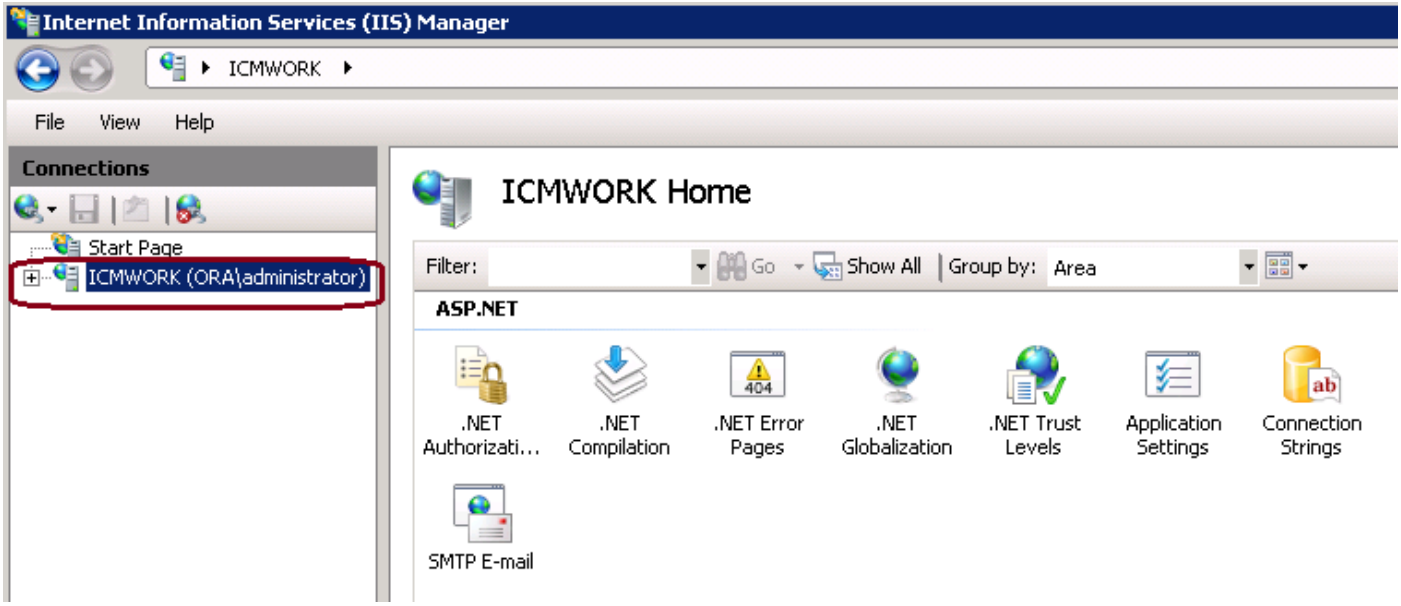
- Генерируйте запрос подписи сертификата (CSR) от менеджера информационных сервисов интернета (IIS)
- Загрузите подписанный сертификат CA менеджеру информационных сервисов интернета (IIS)
- Свяжите сертификат CA со знаком с веб-сайтом по умолчанию

Шаг 1. Генерируйте CSR от менеджера информационных сервисов интернета (IIS)

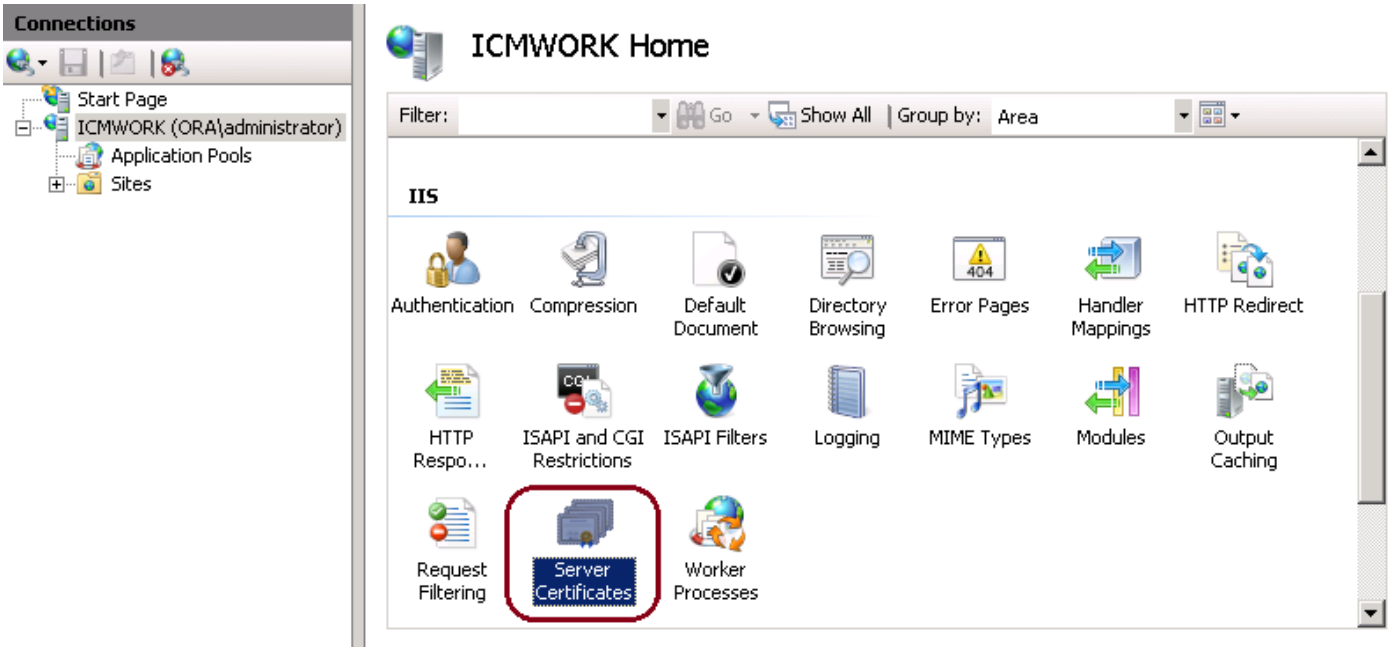
1. Войдите в систему Windows, нажмите **Start> Run> All Programs> Administrative Tools> Internet Information Services (IIS) Manager**, как показано в этом образе. Не выбирайте версию 6 IIS, если она существует.



2. В оконном стекле Соединений налево, выберите имя сервера, как показано в этом образе.

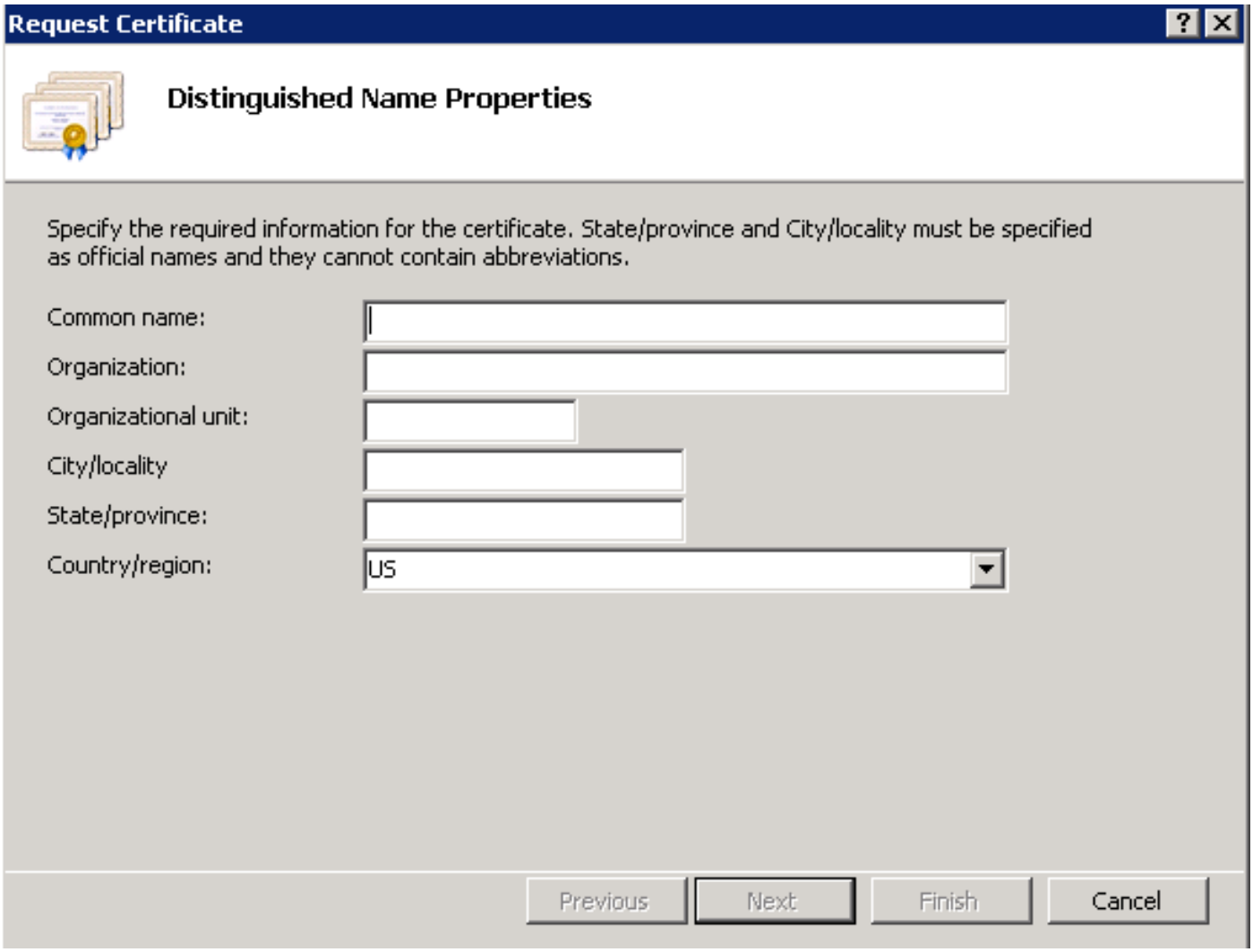


3. В области среднего окна выберите **IIS> Server Certificates**. Двойной щелчок на Серверных сертификатах для генерации окна сертификата, как показано в этом образе.

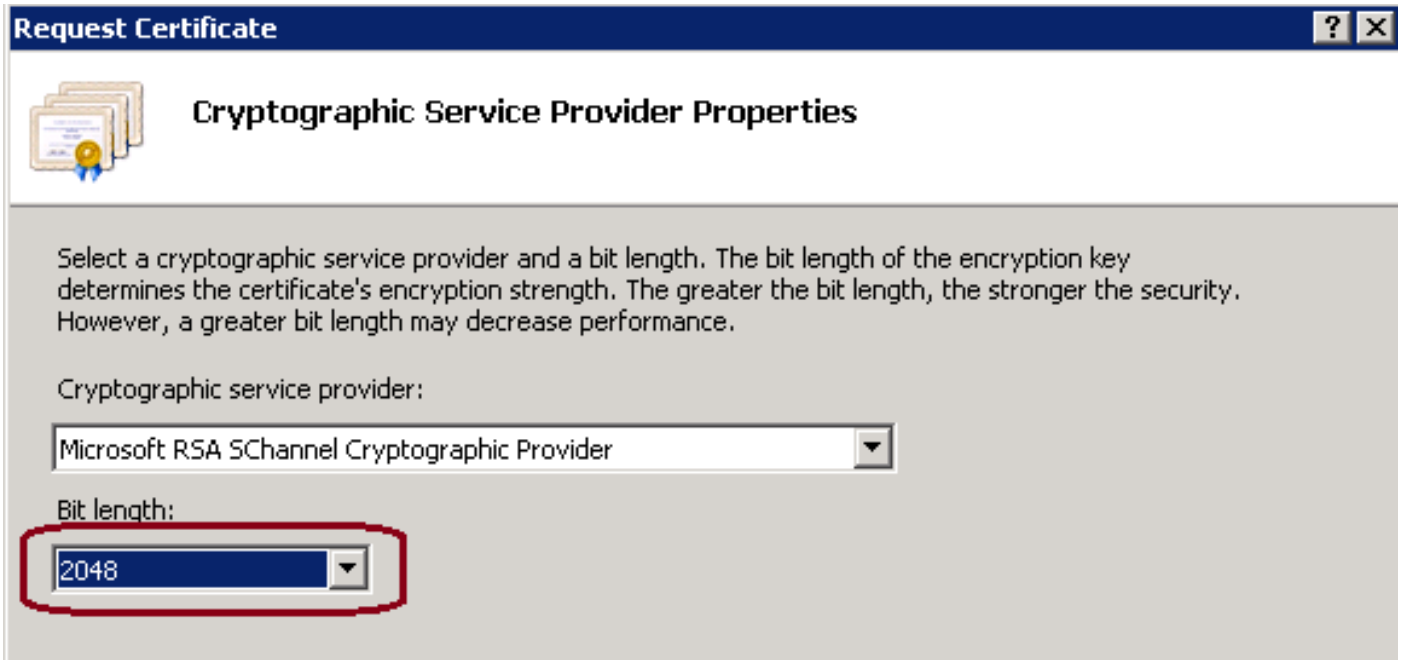


4. На правой панели щелкните **по Actions> Create Certificate Request**, как показано в этом образе.

5. Для завершения запроса сертификата войдите в Общем имени, Организации, Организационном модуле, Городе/местности, Состоянии/области и Стране/области, как показано в этом образе.



6. Нажмите Next для изменения длины криптографического и бита защиты, рекомендуется использовать, по крайней мере, 2048 для лучшей безопасности, как показано в этом образе.

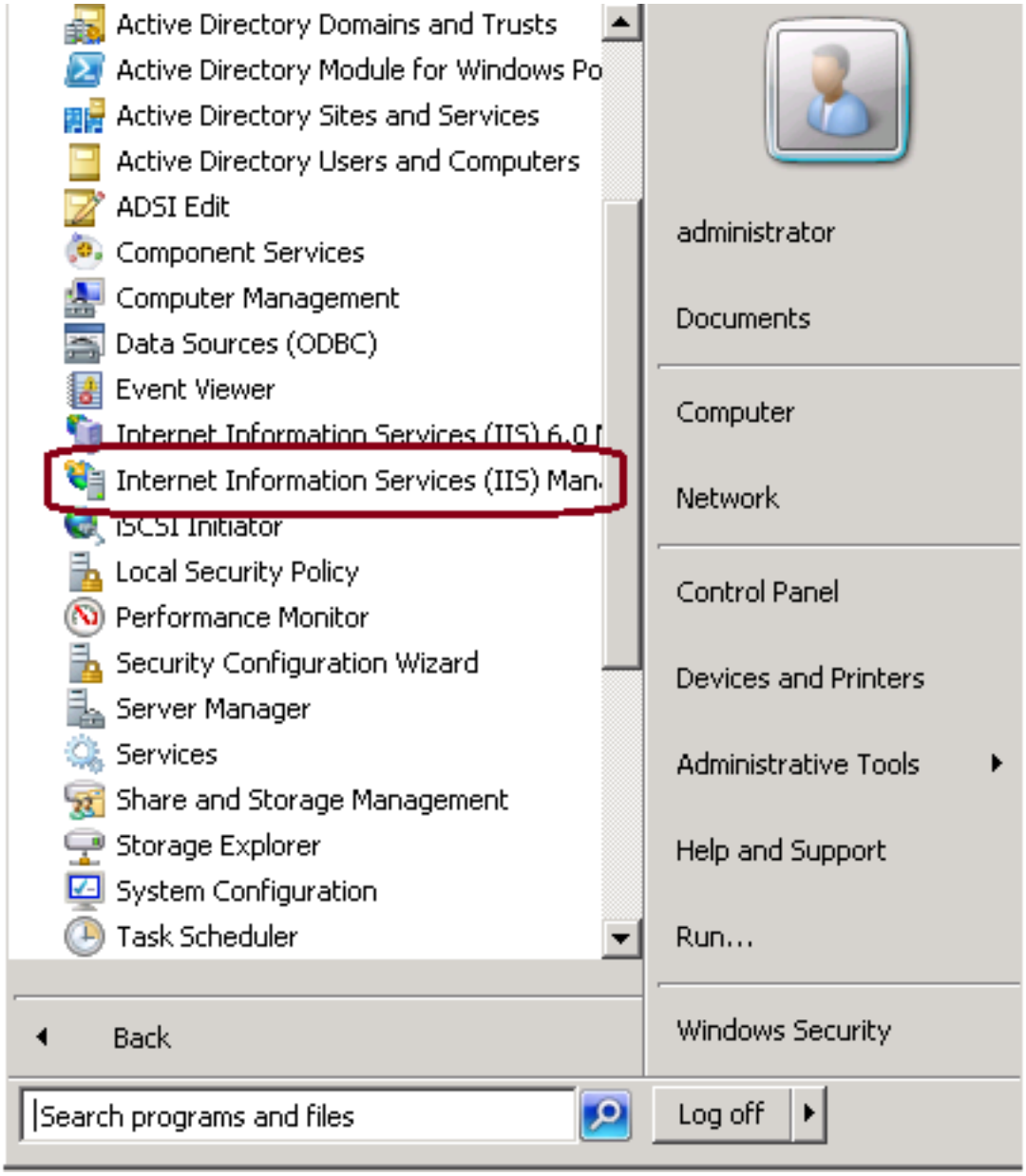


7. Сохраните запрос сертификата в желаемом местоположении, которое будет сохранено как формат.TXT, как показано в этом образе.

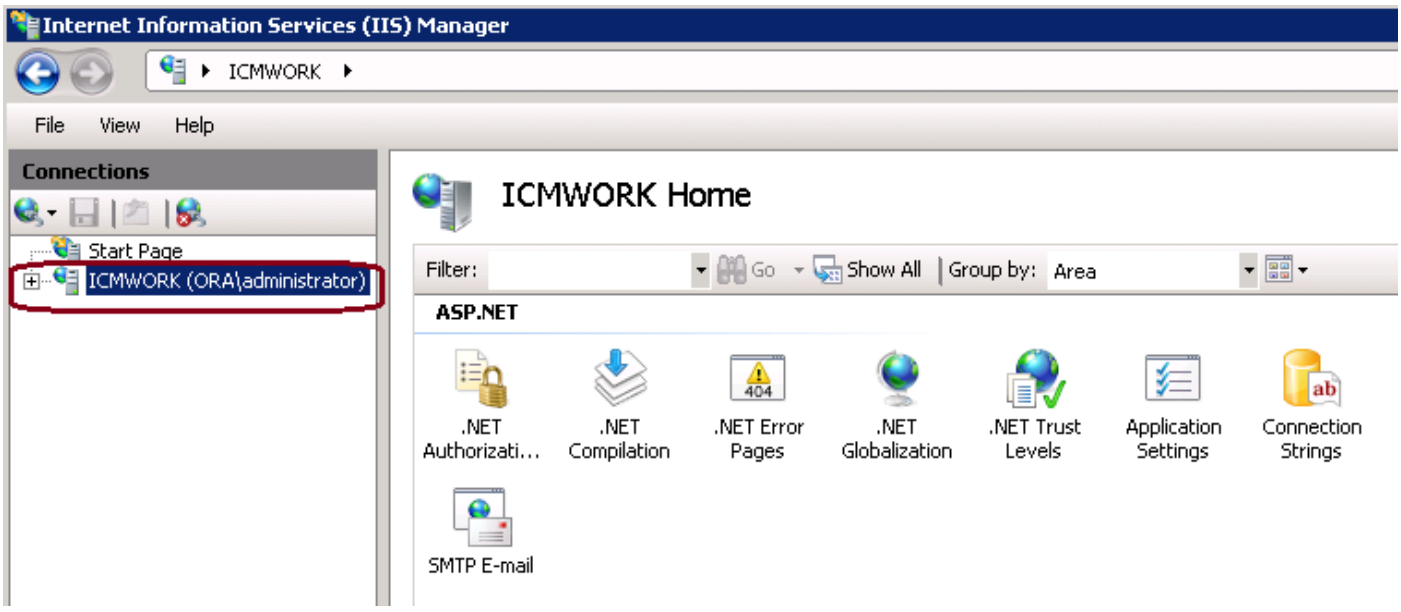
8. Предоставьте этот файл, который будет подписан командой, которая управляет внутренним CA или внешним запросом на обслуживание CA, как показано в этом образе.

Шаг 2. Загрузите подписанный сертификат CA менеджеру информационных сервисов интернета (IIS)

1. Войдите в систему Windows, нажмите **Start> Run> All Programs> Administrative Tools> Internet Information Services (IIS) Manager,** как показано в этом образе. Не выбирайте версию 6 IIS, если она существует.

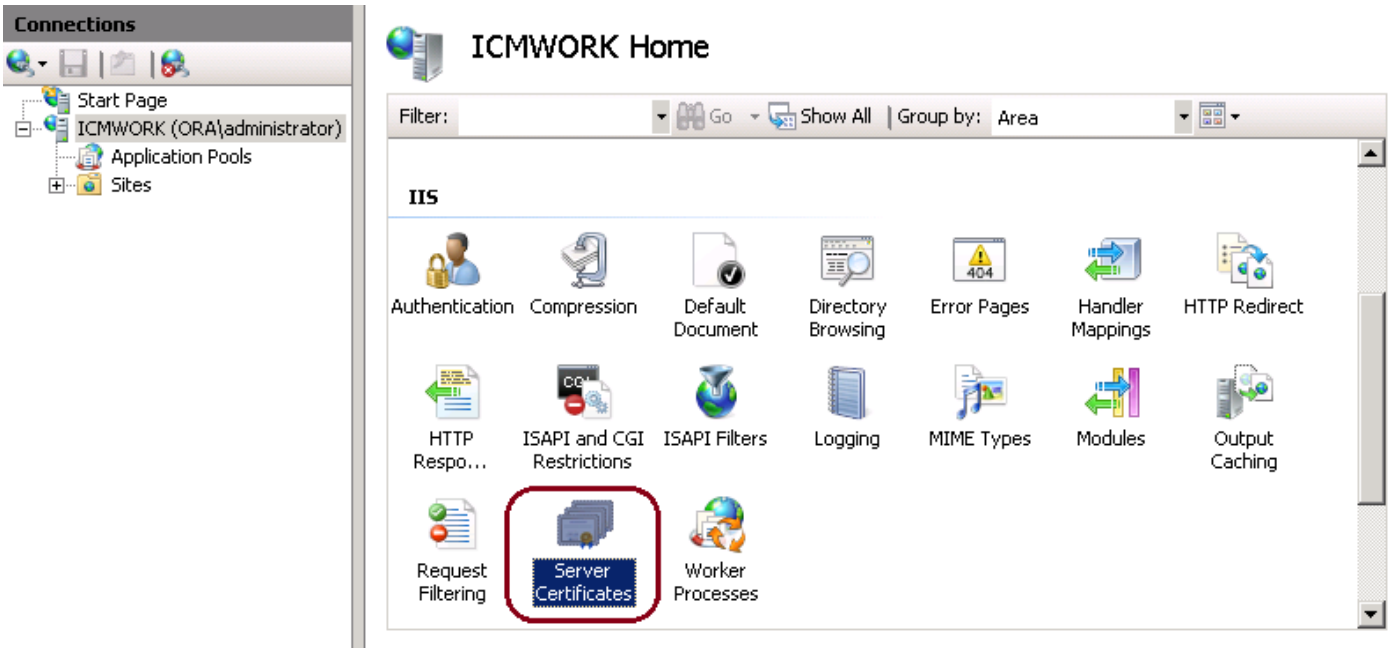


2. В оконном стекле Соединений налево, выберите имя сервера, как показано в этом образе.

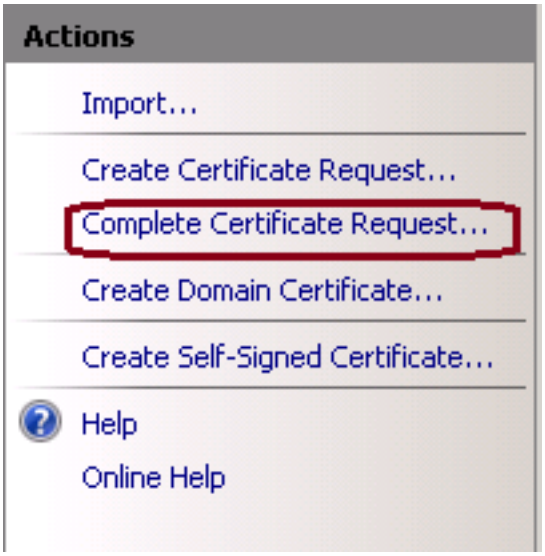


3. В области среднего окна выберите **IIS> Server Certificates**. Двойной щелчок на Серверных

сертификатах для генерации окна сертификата, как показано в этом образе.

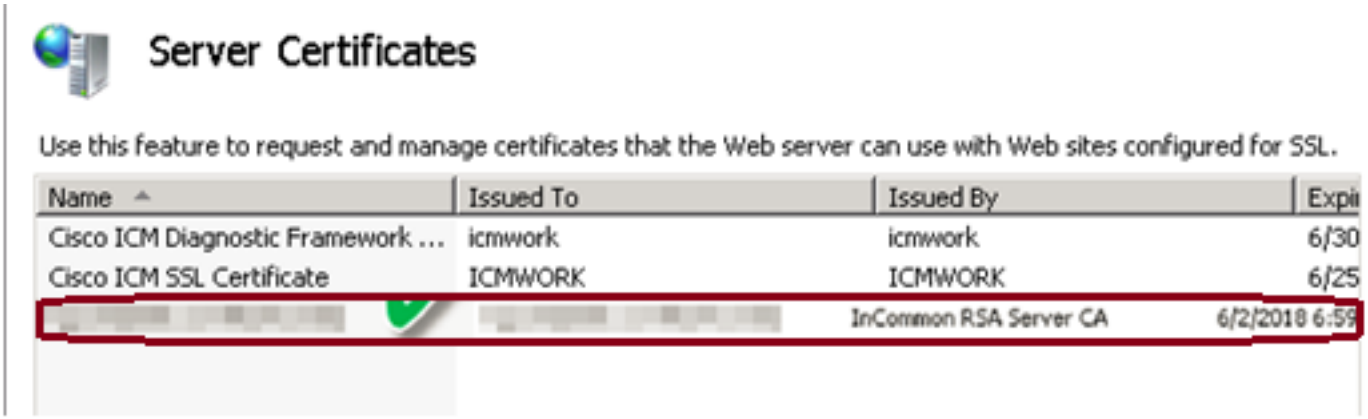


4. На правой панели щелкните **по Actions> Complete Certificate Request**, как показано в этом образе.



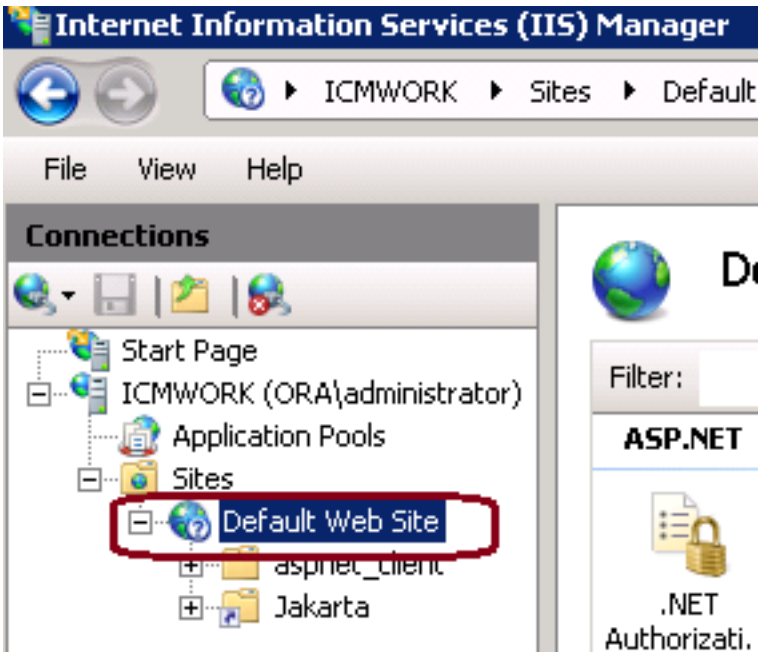
5. До этого шага гарантируйте, что подписанный сертификат находится в формате.CER и был загружен к локальному серверу. Нажмите … кнопку для просмотра.CER файла.
В Дружественном названии используйте FQDN сервера, как показано в этом образе.

6. Нажмите OK для загрузки сертификата. Когда завершенный, подтвердите, что сертификат теперь появляется в окне Server Certificates, как показано в этом образе.



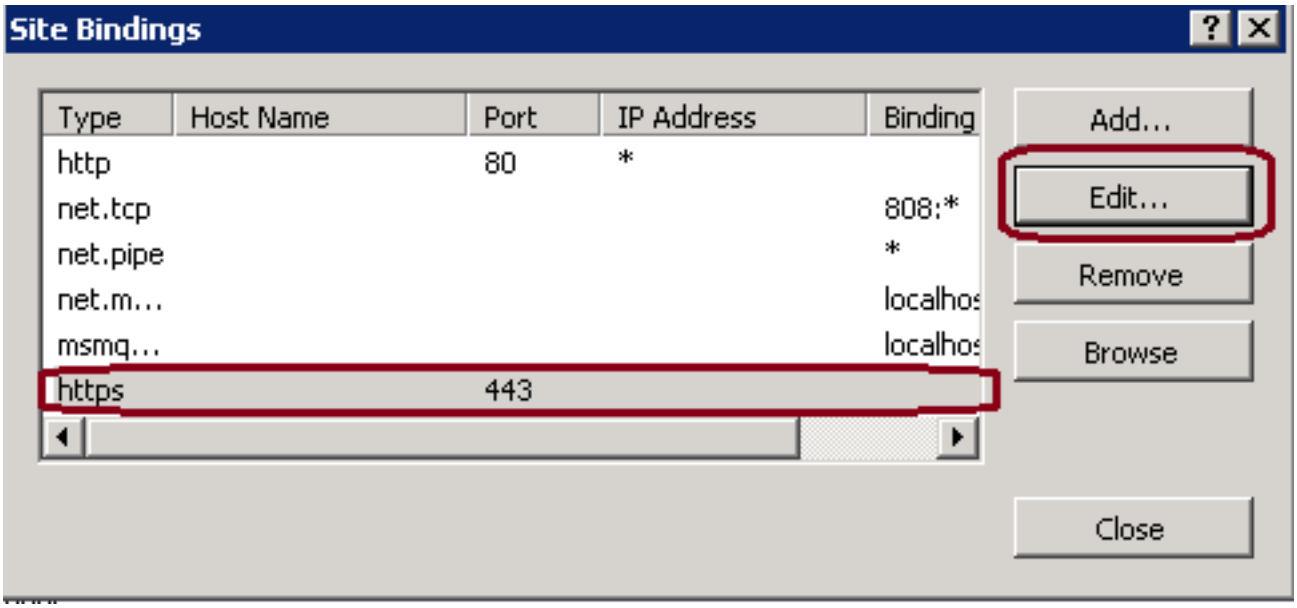
Шаг 3. Свяжите сертификат CA со знаком с веб-сайтом по умолчанию

1. В Диспетчере IIS Под плоскостью окна Connections, левой рукой, щелкают **<server_name>> Узлы> Веб-сайт по умолчанию**, как показано в этом образе.

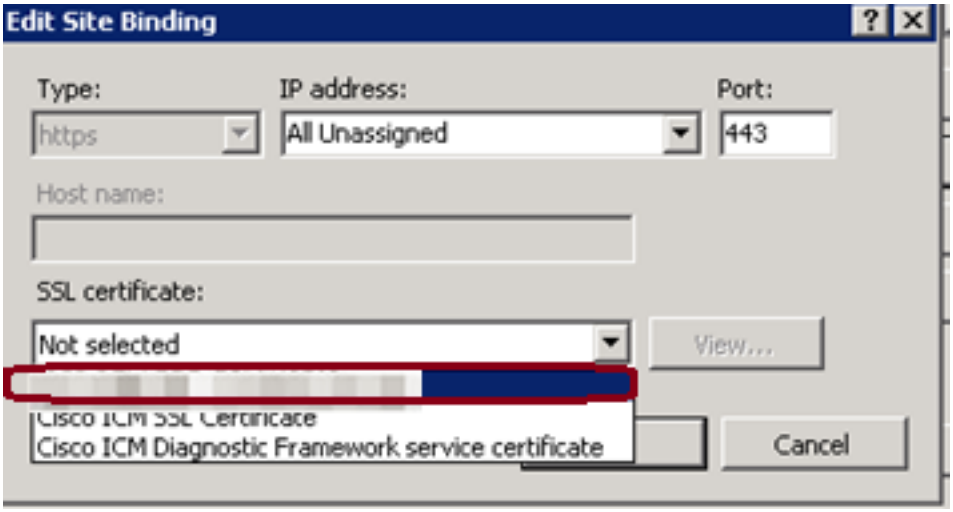


2. Под оконным стеклом Действий на правой стороне щелкните по Bindings, как показано в этом образе.

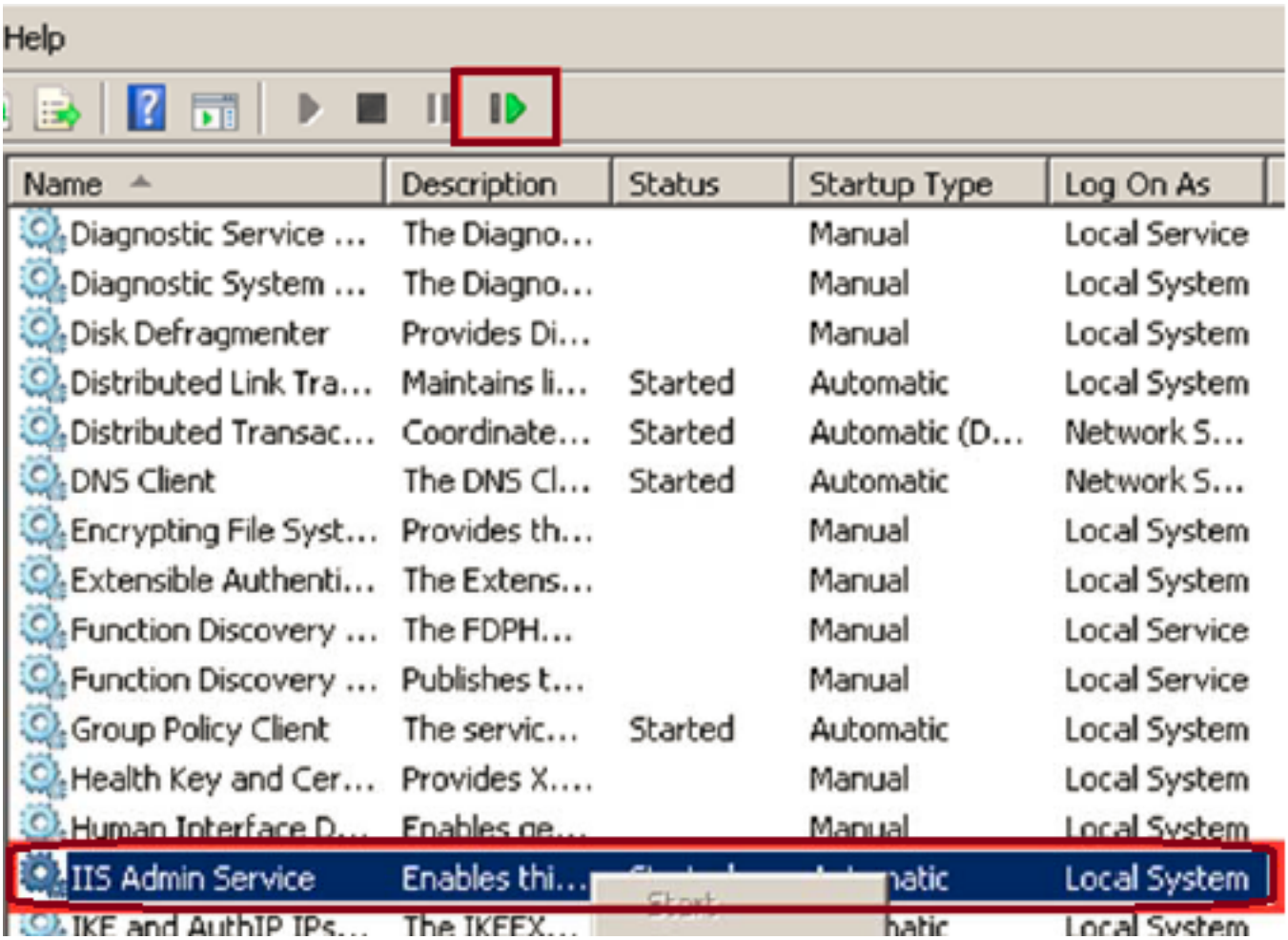
3. В окне связываний узла щелкните по https для выделения большего количества опций. Щелкните по Edit для продолжения, как показано в этом образе.



4. Под параметром сертификата SSL щелкните по стрелке вниз для выбора Signed Certificate, загруженного ранее. Просмотрите Подписанный сертификат, чтобы проверить, что Путь сертификации и значения совпадают с локальным сервером. Когда завершено нажмите OK, затем Близко к выходу из окна Site Bindings, как показано в этом образе.



5. Перезапустите Сервис Admin IIS под моментальным снимком MMC Сервисов - в путем **нажимания кнопку Старт> Выполнение> services.msc.**, как показано в этом образе.



6. Если успешный, клиентский web-браузер не должен вызывать ошибку сертификата, предупреждающую при вводе в URL FQDN для веб-сайта.

> **Примечание:** Если Сервис Admin IIS отсутствует, перезапускают Сервис веб-публикации.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.