# Настройка ограниченного делегирования Kerberos для прокси-страниц веб-регистрации

Статья • 21.02.2024

В этой статье приводятся пошаговые инструкции по реализации службы для пользователя в прокси-сервер (S4U2Proxy) или ограниченного делегирования Kerberos в пользовательской учетной записи службы для прокси-страниц веб-регистрации.

*Исходный номер базы знаний:* 4494313

## Сводка

В этой статье приведены пошаговые инструкции по реализации службы для пользователя на прокси-сервер (S4U2Proxy) или ограниченного делегирования только Kerberos для страниц прокси-сервера веб-регистрации. В этой статье описаны следующие сценарии конфигурации:

- Настройка делегирования для пользовательской учетной записи службы
- Настройка делегирования учетной записи NetworkService

> **Примечание**
>
> Рабочие процессы, описанные в этой статье, относятся к определенной среде. Одни и те же рабочие процессы могут не работать в другой ситуации. Однако принципы остаются неизменными. На следующем рисунке представлена эта среда.


## Сценарий 1. Настройка ограниченного делегирования для пользовательской

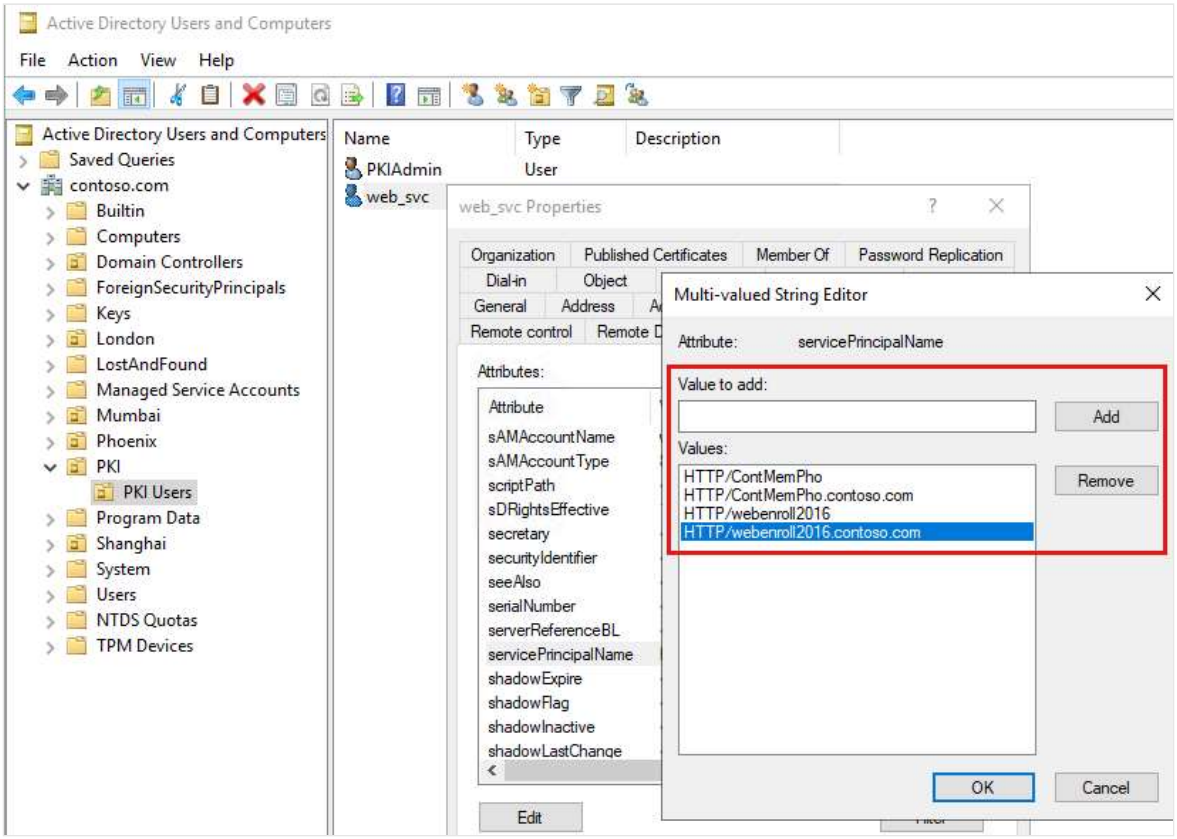
# учетной записи службы

В этом разделе описано, как реализовать ограниченное делегирование службы для пользователей на прокси-сервер (S4U2Proxy) или ограниченное делегирование kerberos при использовании пользовательской учетной записи службы для прокси-страниц веб-регистрации.

## 1. Добавление имени субъекта-службы в учетную запись службы

Свяжите учетную запись службы с именем субъекта-службы (SPN). Для этого выполните следующие действия:

1. В **разделе Пользователи и компьютеры Active Directory** подключитесь к домену, а затем выберите **PKI**>**PKI Пользователи**.
2. Щелкните правой кнопкой мыши учетную запись службы (например, web_svc) и выберите **пункт Свойства**.
3. Выберите**ServicePrincipalNameредактора**> атрибутов.
4. Введите новую строку имени субъекта-службы, выберите **Добавить** (как показано на следующем рисунке) и нажмите **кнопку OK**.



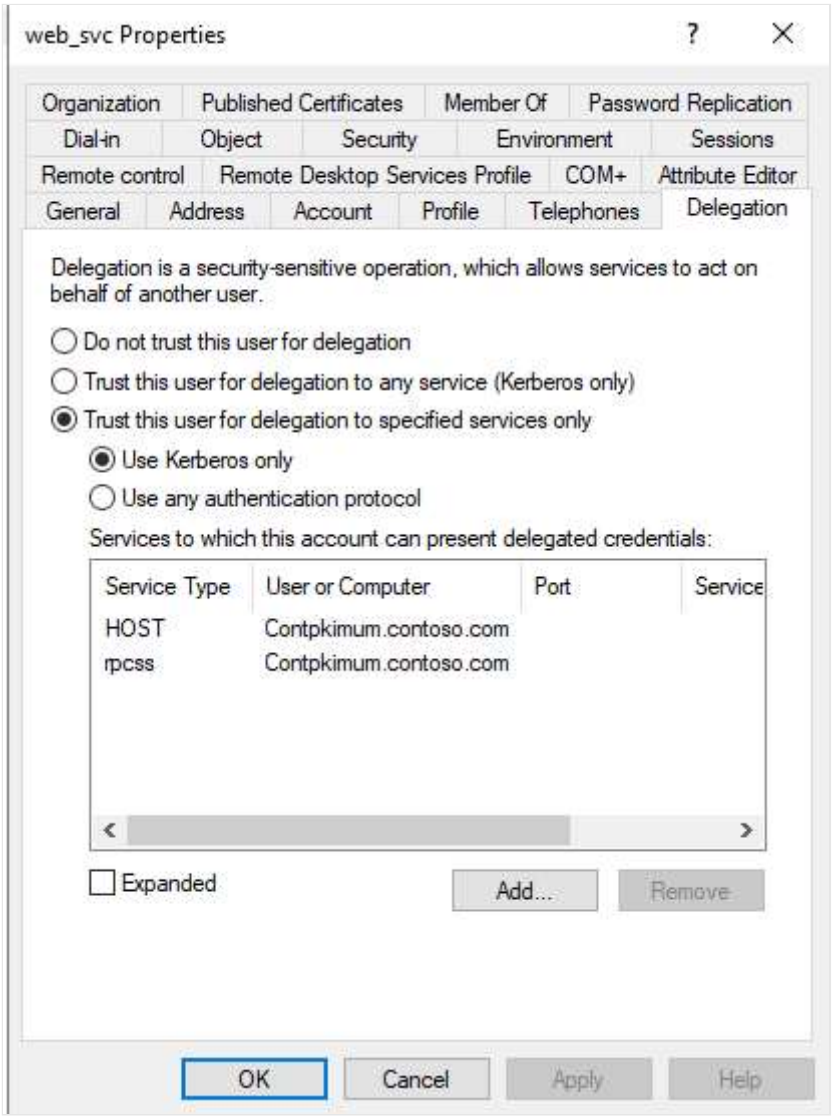
Вы также можете использовать Windows PowerShell для настройки имени субъекта-службы. Для этого откройте окно PowerShell с повышенными привилегиями и выполните команду `setspn -s SPN Accountname`. Например, выполните следующую команду:

Консоль

```
setspn -s HTTP/webenroll2016.contoso.com web_svc
```

## 2. Настройка делегирования

1. Настройте ограниченное делегирование S4U2proxy (только Kerberos) в учетной записи службы. Для этого в диалоговом окне **Свойства** учетной записи службы (как описано в предыдущей процедуре) выберите **Делегирование>доверять этому пользователю только для делегирования указанным службам**. Убедитесь, что выбран параметр **Использовать только Kerberos** .

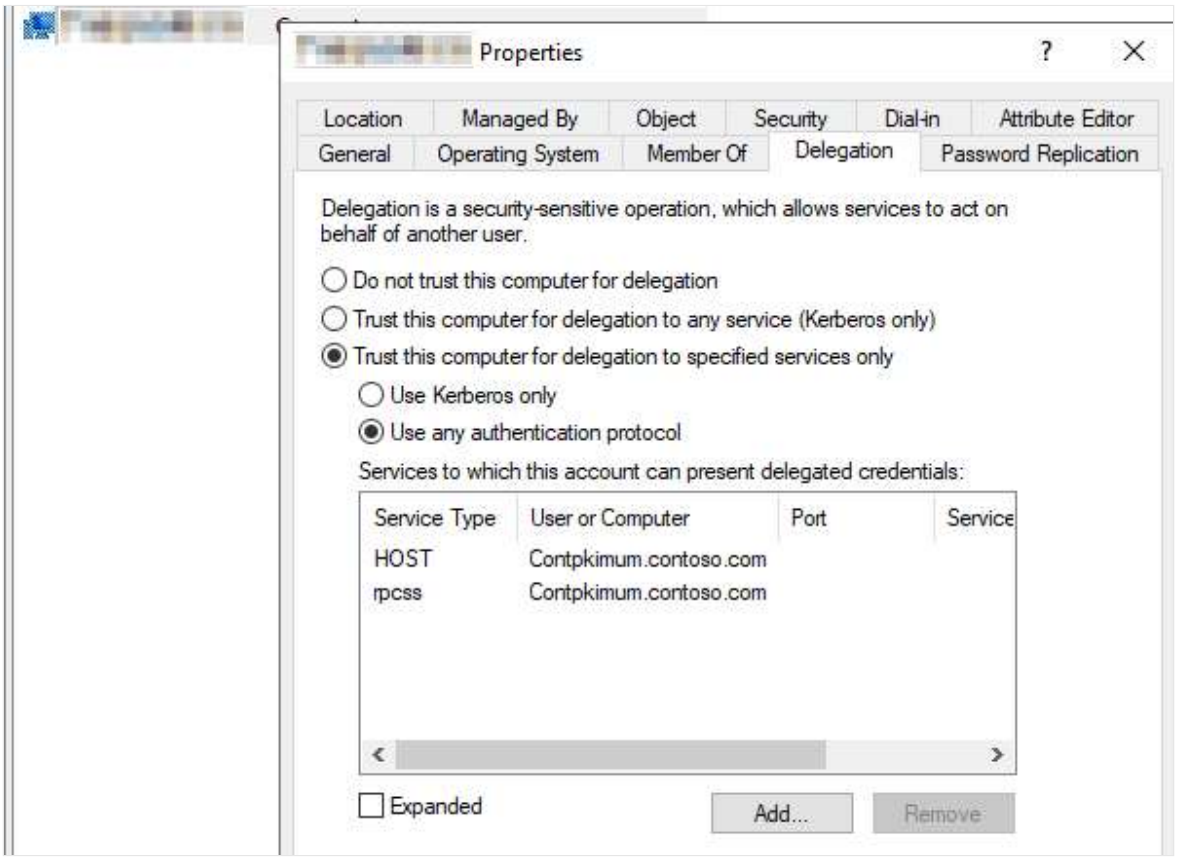


2. Закройте диалоговое окно.

3. В дереве консоли выберите **Компьютеры**, а затем выберите учетную запись компьютера внешнего сервера веб-регистрации.

> ⓘ **Примечание**
>
> Эта учетная запись также называется "учетной записью компьютера".

4. Настройте ограниченное делегирование S4U2self (переход к протоколу) в учетной записи компьютера. Для этого щелкните правой кнопкой мыши учетную запись компьютера и выберите **Свойства**>**Делегирование**>**Доверять этому компьютеру только для делегирования указанным службам**. Выберите параметр **Использовать любой протокол проверки подлинности**.

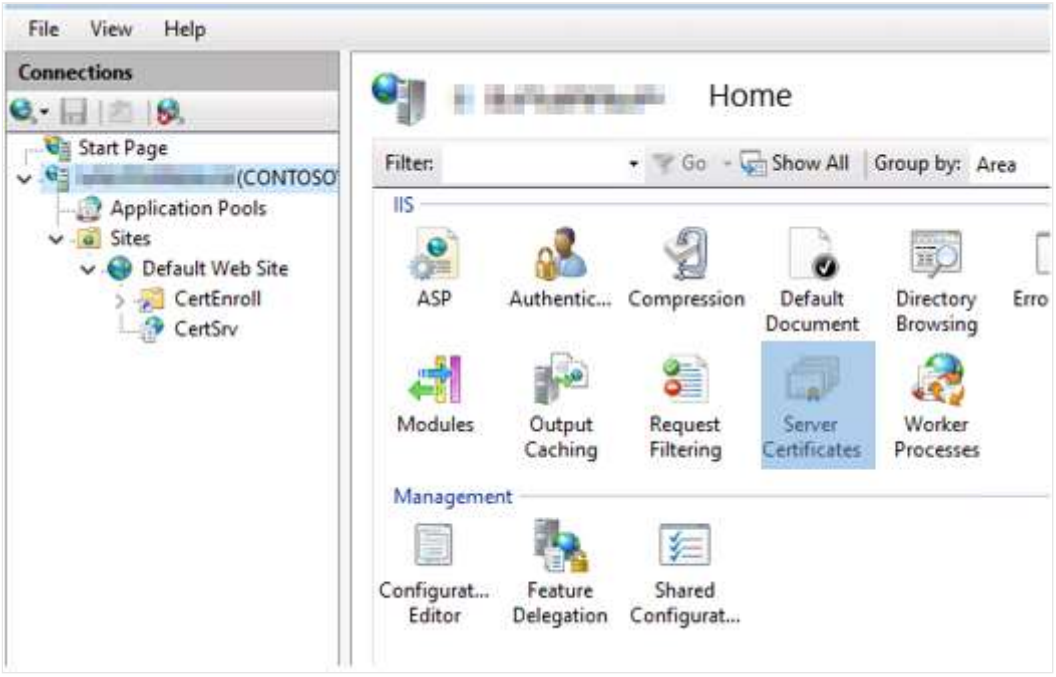



## 3. Создание и привязка SSL-сертификата для регистрации в Интернете

Чтобы включить страницы регистрации в Интернете, создайте сертификат домена для веб-сайта, а затем привяжите его к веб-сайту по умолчанию. Для этого выполните следующие действия:

1. Откройте диспетчер служб IIS.

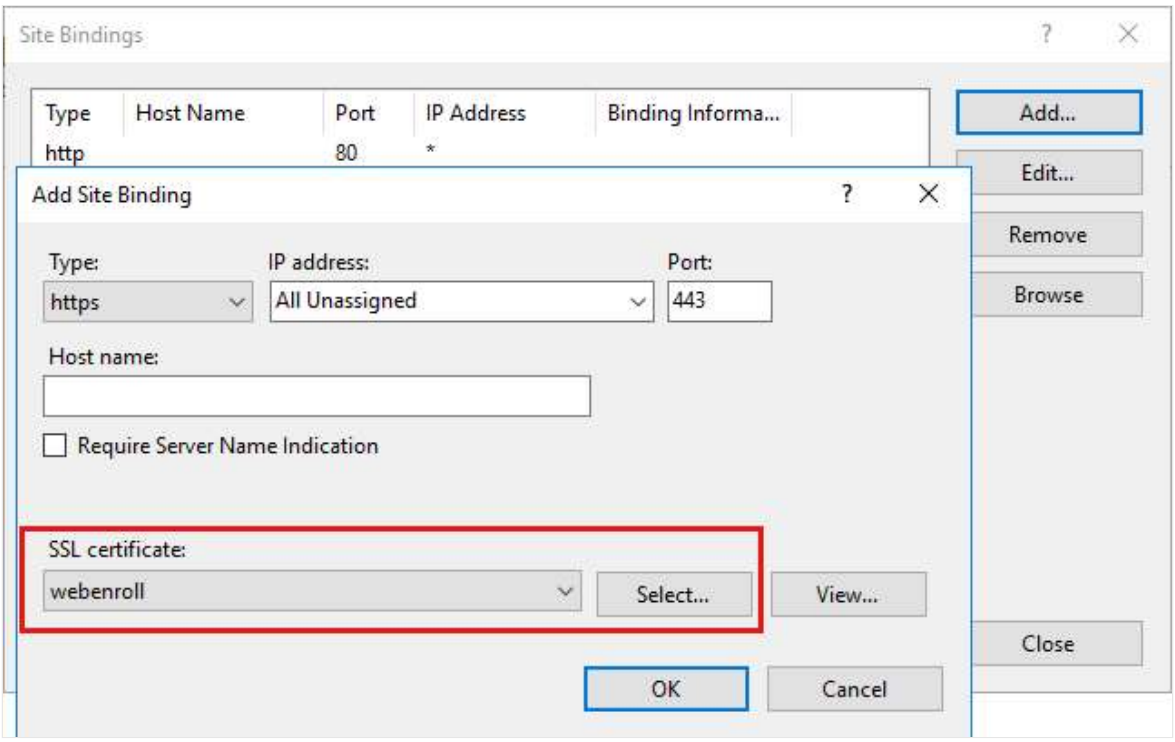
2. В дереве консоли выберите <***HostName***>, а затем **— Сертификаты сервера**.

> **Примечание**
>
> *<Узла>* — это имя интерфейсного веб-сервера.
>
> 
> 

3. В меню **Действия** выберите **Создать сертификат домена**.

4. После создания сертификата выберите **Веб-сайт по умолчанию** в дереве консоли, а затем выберите **Привязки**.

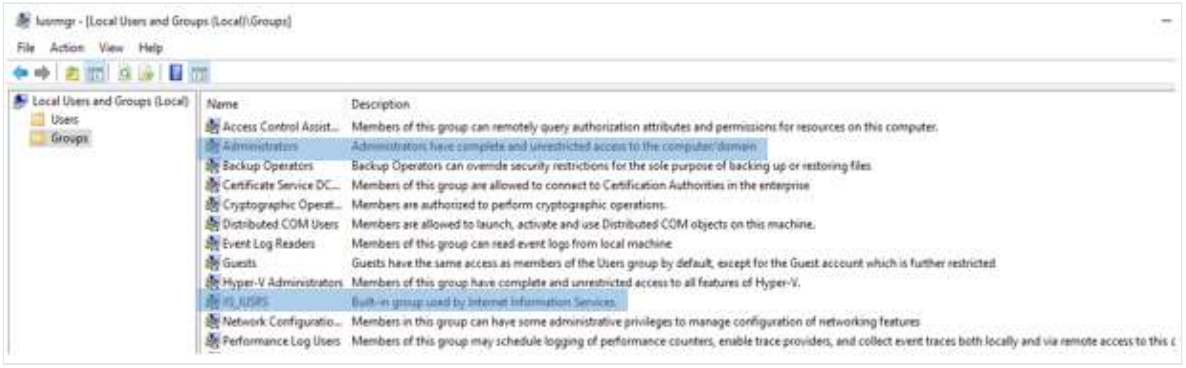
5. Убедитесь, что для **параметра Порт** задано значение **443**. Затем в разделе **SSL-сертификат** выберите сертификат, созданный на шаге 3.



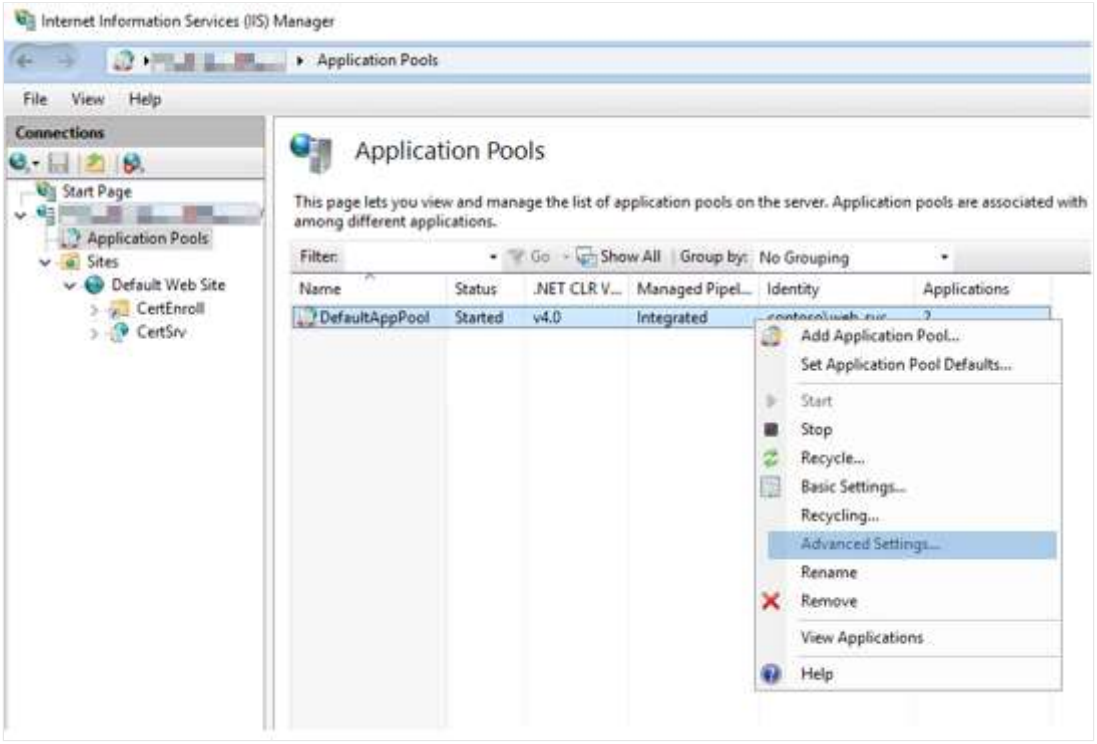

6. Нажмите **кнопку OK** , чтобы привязать сертификат к порту 443.

## 4. Настройка внешнего сервера веб-регистрации для использования учетной записи службы

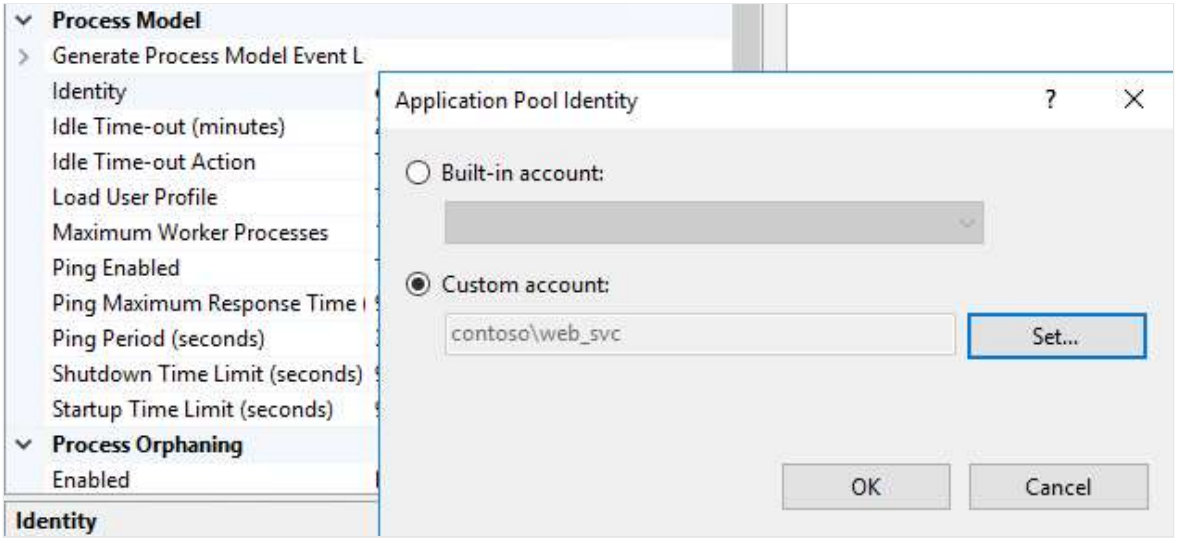
> ⓘ **Важно!**
>
> Убедитесь, что учетная запись службы является частью **локальных администраторов** или **IIS_Users** группы на веб-сервере.




1. Щелкните правой кнопкой мыши **DefaultAppPool** и выберите **Пункт Дополнительные параметры**.

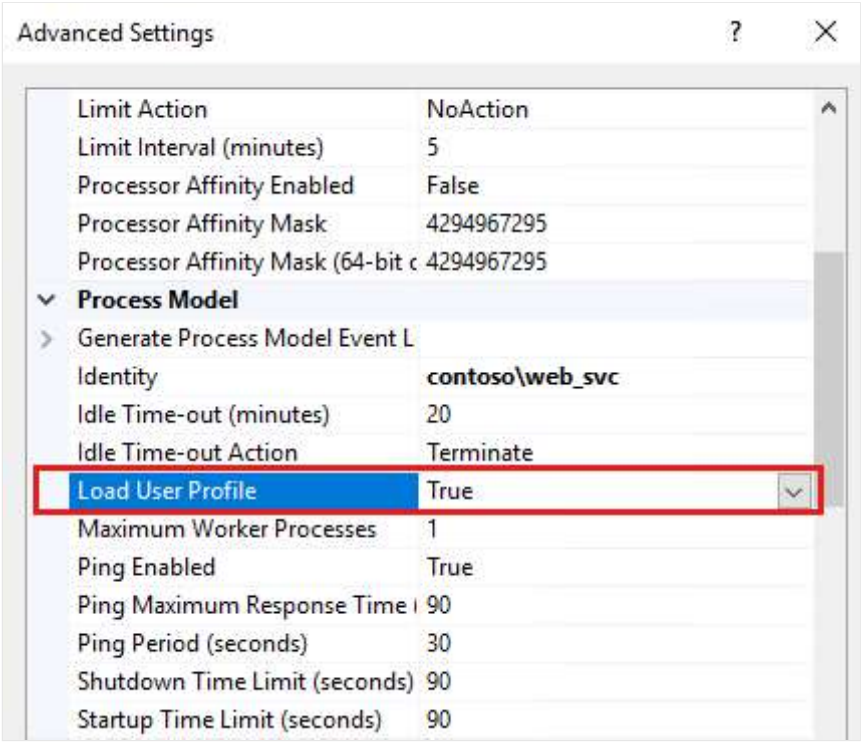



2. Выберите**Обработать удостоверениемодели**>, выберите **Пользовательская учетная запись**, а затем нажмите **кнопку Задать**. Укажите имя и пароль учетной записи службы.




3. Нажмите **кнопку ОК** в диалоговом окне **Настройка учетных данных** и **удостоверения пула приложений** .

4. В **разделе Дополнительные параметры** найдите **Пункт Загрузить профиль пользователя** и убедитесь, что для него задано значение **True**.




5. Перезагрузите компьютер.

# Сценарий 2. Настройка ограниченного делегирования в учетной записи NetworkService

В этом разделе описывается реализация ограниченного делегирования S4U2Proxy или Kerberos при использовании учетной записи NetworkService для страниц прокси-сервера веб-регистрации.

## Необязательный шаг. Настройка имени для подключений

Вы можете назначить имя роли веб-регистрации, которую клиенты могут использовать для подключения. Такая конфигурация означает, что входящие запросы не должны знать имя компьютера внешнего сервера веб-регистрации или другие сведения о маршрутизации, например каноническое dns-имя (CNAME).

Например, предположим, что имя компьютера сервера веб-регистрации — WEBENROLLMAC (в домене Contoso). Вместо этого входящие подключения должны использовать имя ContosoWebEnroll. В этом случае URL-адрес подключения будет следующим:

```
https://contosowebenroll.contoso.com/certsrv
```

Это не будет следующее:

```
https://WEBENROLLMAC.contoso.com/certsrv
```

Чтобы использовать такую конфигурацию, выполните следующие действия.

1. В файле зоны DNS для домена создайте запись псевдонима или запись имени узла, которая сопоставляет новое имя подключения с IP-адресом роли веб-регистрации. Используйте средство проверки связи для проверки конфигурации маршрутизации.

   В примере, который был рассмотрен ранее, `Contoso.com` файл зоны имеет запись псевдонима, которая сопоставляет ContosoWebEnroll с IP-адресом роли веб-регистрации.

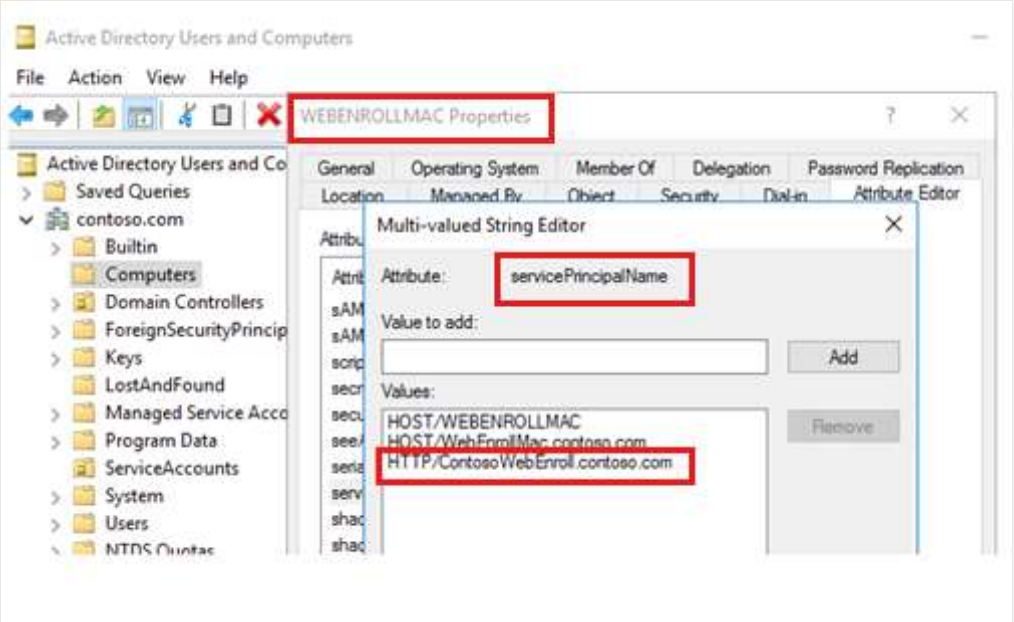
2. Настройте новое имя в качестве имени субъекта-службы для внешнего сервера веб-регистрации. Для этого выполните следующие действия:
   a. В разделе Пользователи и компьютеры Active Directory подключитесь к домену, а затем выберите **Компьютеры**.
   b. Щелкните правой кнопкой мыши учетную запись компьютера внешнего сервера веб-регистрации и выберите **Пункт Свойства**.

      > ⓘ **Примечание**
      >
      > Эта учетная запись также называется "учетной записью компьютера".

   c. Выберите**ServicePrincipalNameредактора**> атрибутов.
   d. Введите **HTTP/<*ConnectionName*>.<*DomainName*.com**> нажмите **кнопку Добавить**, а затем нажмите **кнопку ОК**.

      > ⓘ **Примечание**
      >
      > В этой строке <*ConnectionName*> — это новое имя, которое вы определили, а <*DomainName*> — это имя домена. В примере строка

имеет значение **HTTP/ContosoWebEnroll.contoso.com**.




## 1. Настройка делегирования

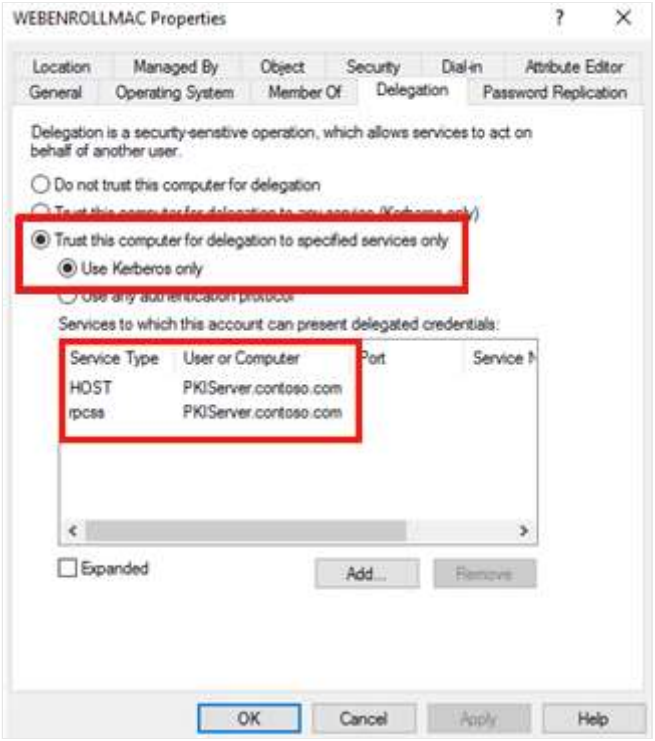
1. Если вы еще не подключились к домену, выполните это в **разделе Пользователи и компьютеры Active Directory**, а затем выберите **Компьютеры**.

2. Щелкните правой кнопкой мыши учетную запись компьютера внешнего сервера веб-регистрации и выберите **Пункт Свойства**.

   > ⓘ **Примечание**
   >
   > Эта учетная запись также называется "учетной записью компьютера".

3. Выберите **Делегирование**, а затем выберите **Доверять этому компьютеру только для делегирования указанным службам**.

   > ⓘ **Примечание**
   >
   > Если вы можете гарантировать, что клиенты всегда будут использовать проверку подлинности Kerberos при подключении к этому серверу, выберите **Использовать только Kerberos**. Если некоторые клиенты будут использовать другие методы проверки подлинности, такие как NTLM или проверка подлинности на основе форм, выберите **Использовать любой протокол проверки подлинности**.



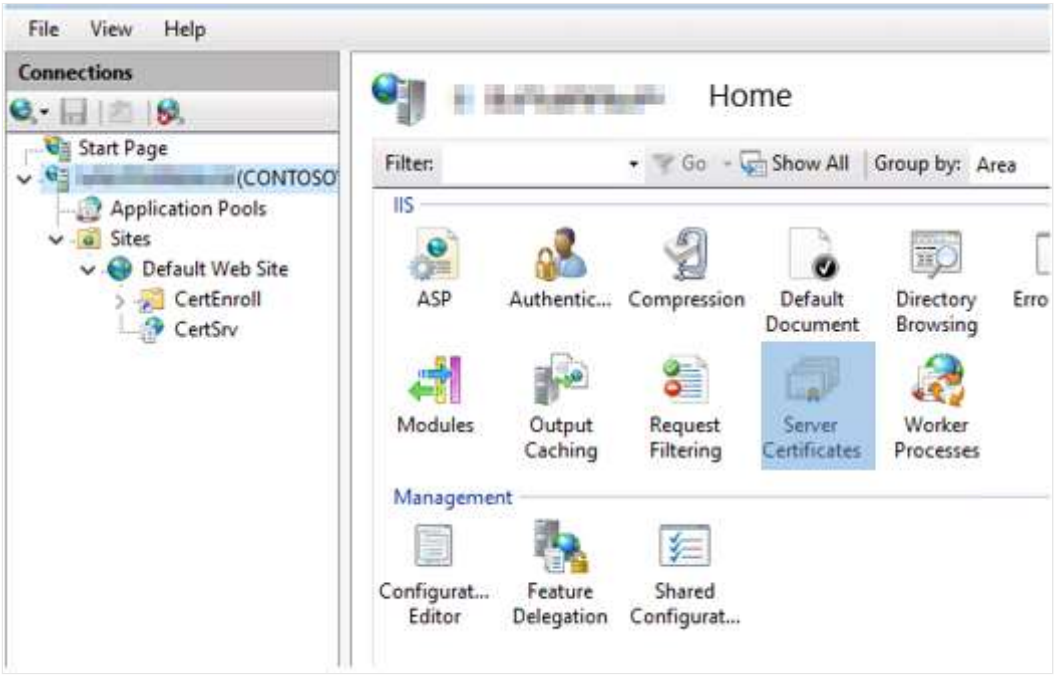

## 2. Создание и привязка SSL-сертификата для регистрации через Интернет

Чтобы включить страницы регистрации в Интернете, создайте сертификат домена для веб-сайта, а затем привяжите его к первому сайту по умолчанию. Для этого выполните следующие действия:

1. Откройте диспетчер IIS.
2. В дереве консоли выберите <***HostName***>, а затем в области действий выберите **Сертификаты сервера** .

> ⓘ **Примечание**

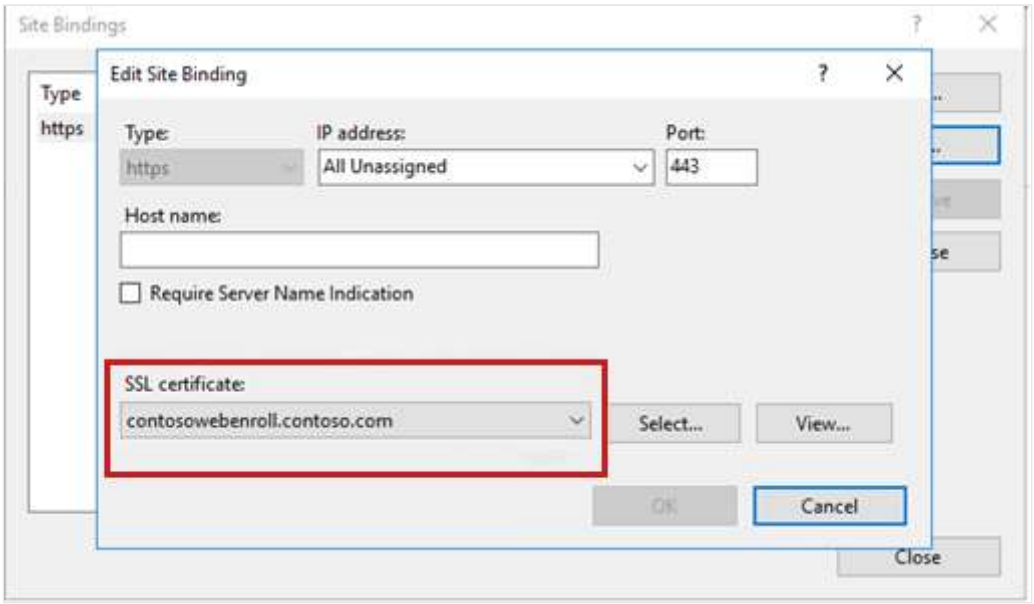
*<Узла>* — это имя интерфейсного веб-сервера.




3. В меню **Действия** выберите **Создать сертификат домена**.

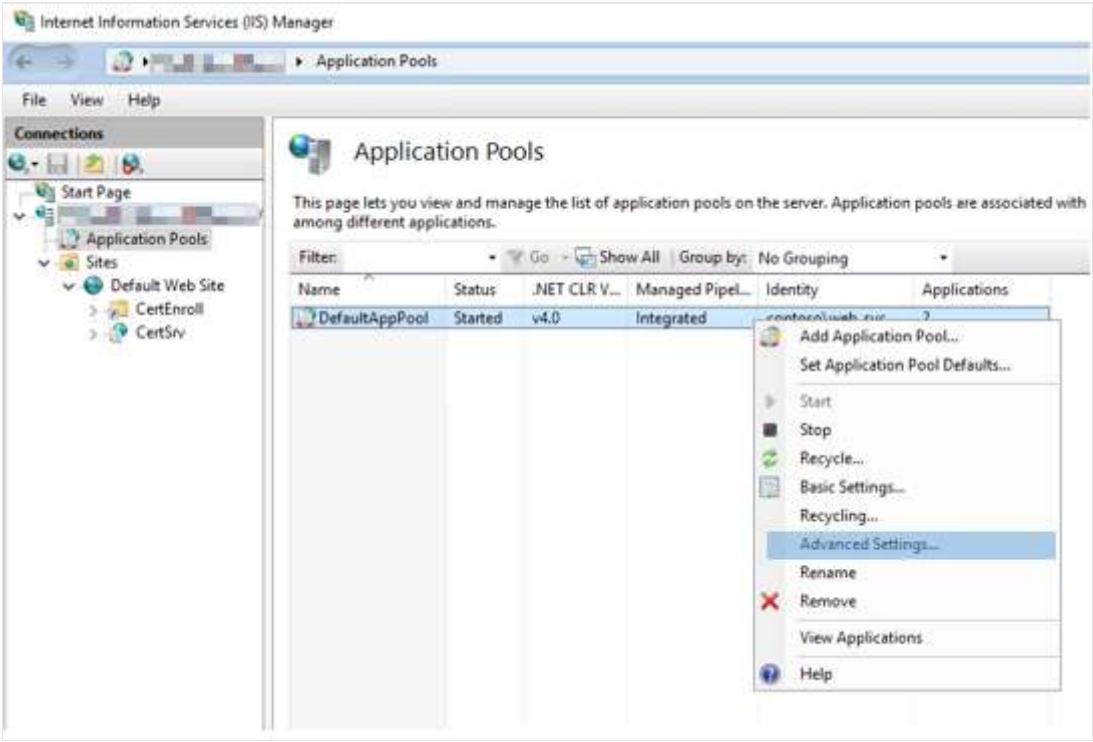
4. После создания сертификата выберите **Веб-сайт по умолчанию**, а затем — **Привязки**.

5. Убедитесь, что для **параметра Порт** задано значение **443**. Затем в разделе **SSL-сертификат** выберите сертификат, созданный на шаге 3. Нажмите **кнопку ОК** , чтобы привязать сертификат к порту 443.

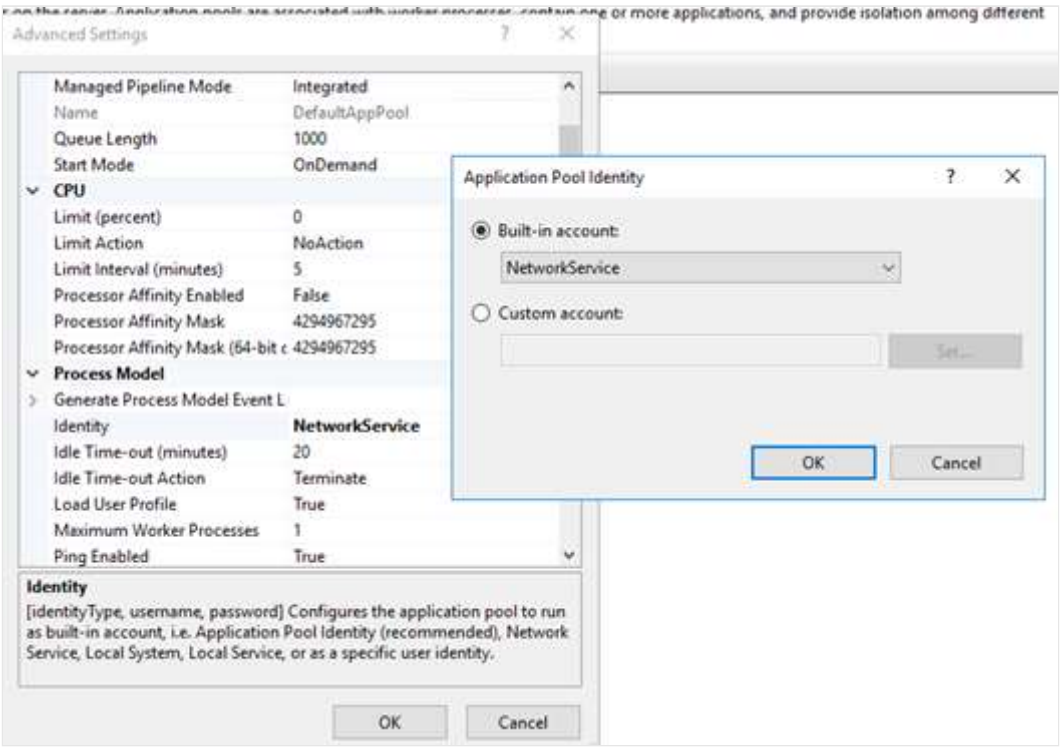



## 3. Настройка внешнего сервера веб-регистрации для использования учетной записи NetworkService

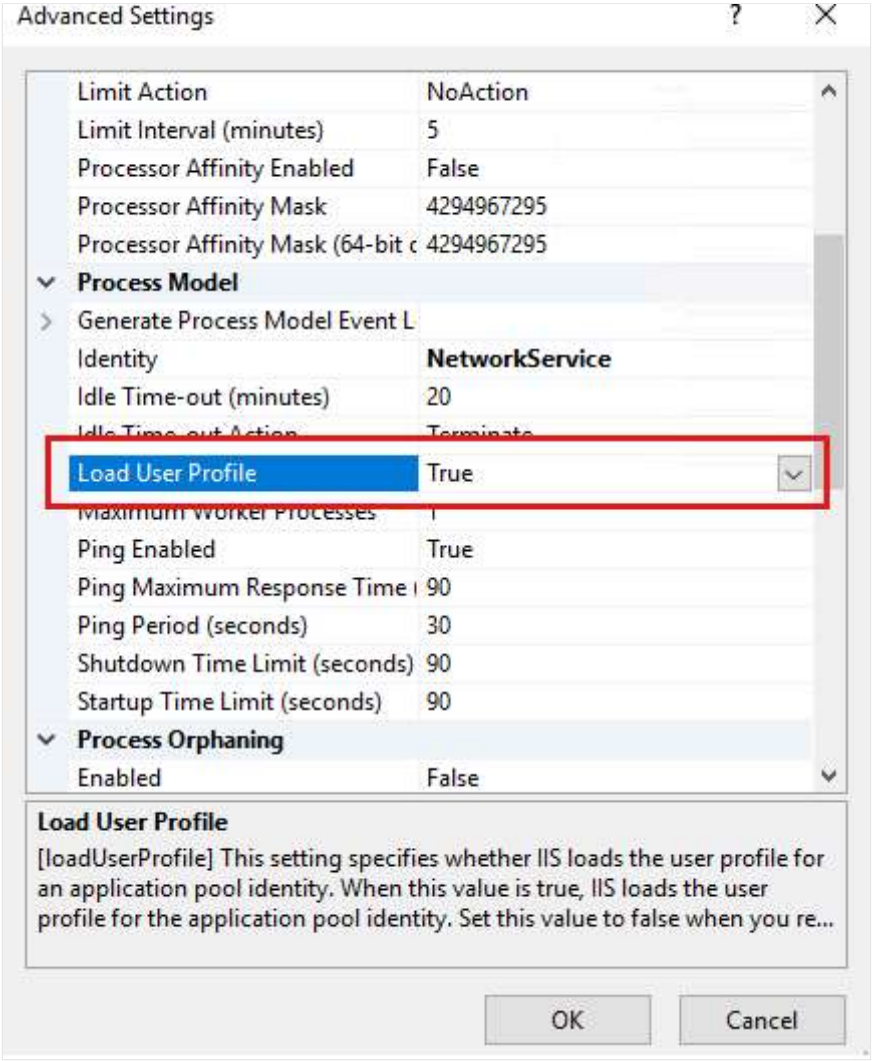
1. Щелкните правой кнопкой мыши **DefaultAppPool** и выберите **Пункт Дополнительные параметры**.




2. Выберите **Идентификатор модели**> обработки**.** Убедитесь, что выбрана **встроенная учетная запись** , а затем выберите **NetworkService**. Затем нажмите **OK**.




3. В **разделе Дополнительные свойства** найдите **Пункт Загрузить профиль пользователя**, а затем убедитесь, что для него задано значение **True**.




4. Перезапустите службу IIS.

## Статьи по теме

Дополнительные сведения об этих процессах см. в разделе Проверка подлинности пользователей веб-приложений.

Дополнительные сведения о расширениях протоколов S4U2self и S4U2proxy см. в следующих статьях:

- [MS-SFU]: Расширения протокола Kerberos: служба для пользователя и протокола ограниченного делегирования
- 4.1 Пример одной области S4U2self
- 4.3. Пример S4U2proxy

---

## Обратная связь

**Были ли сведения на этой странице полезными?** Да Нет

Отзыв о продукте