Настройка двухфакторной аутентификации в Citrix XenDesktop 7.x

Общая информация

Citrix XenDesktop — это решение для виртуализации рабочего стола и приложений Windows.

Двухфакторная аутентификация с помощью устройства Рутокен позволяет лучше защитить доступ к виртуальным рабочим стола.

Для настройки двухфакторной аутентификации необходимо:

1) Создать виртуальную машину.

2) Настроить аутентификацию по смарт-картам.

3) Настроить сквозную аутентификацию по смарт-карте.

Создание виртуальной машины

Подготовка эталонной виртуальной машины

В нашем тестовом окружение эталонная машина — это виртуальная машина с ОС Windows 7 (32bit).

На нее необходимо установить:

- Virtual Delivery Agent (его дистрибутив расположен на диске с ПО XenDesktop 7.0);
- Панель управления Рутокен.

Создание каталога для виртуальной машины

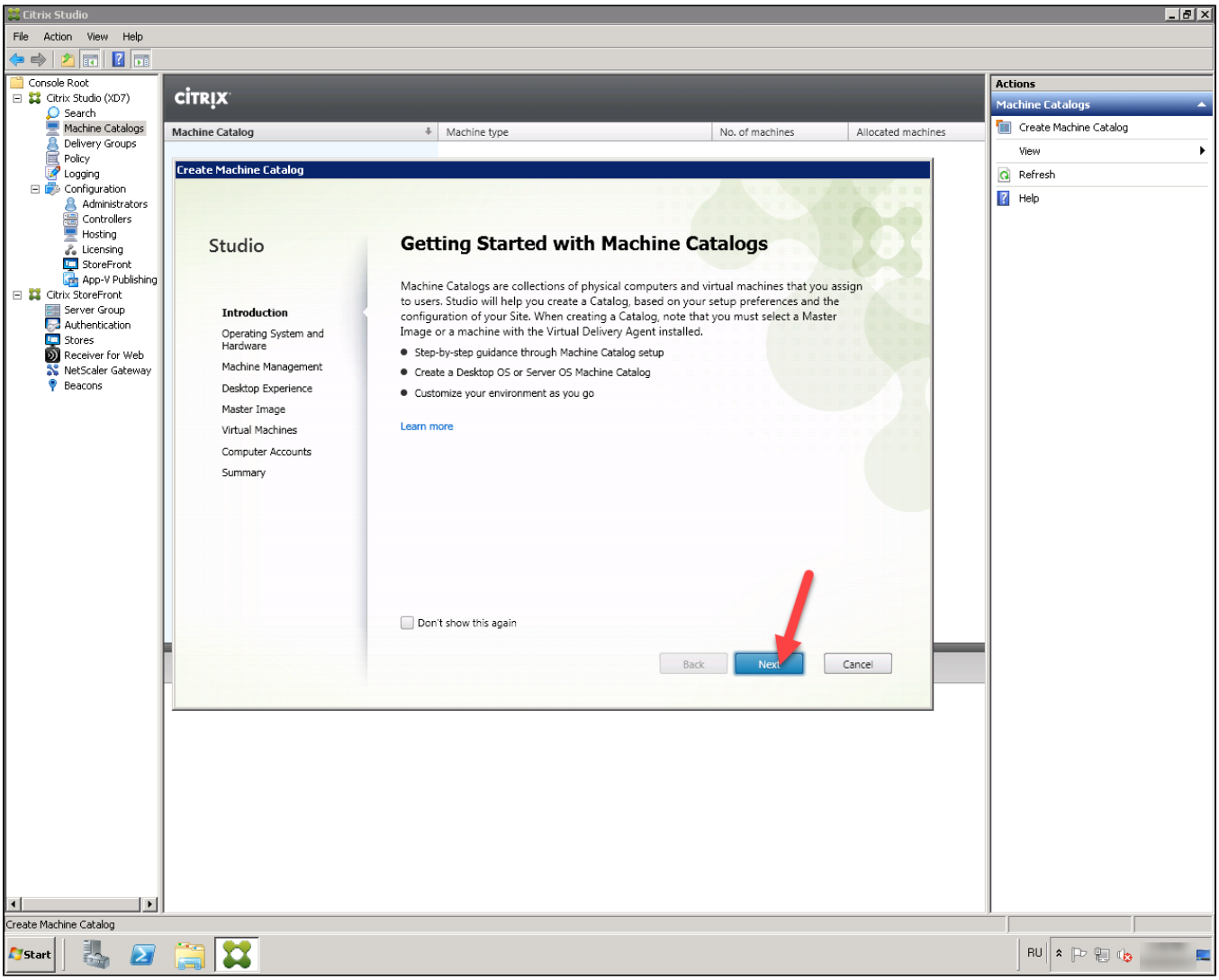
Чтобы создать каталог для виртуальной машины:

1) На сервере запустите **Citrix**. Для этого выберите пункт: Start → All Programs → Citrix.

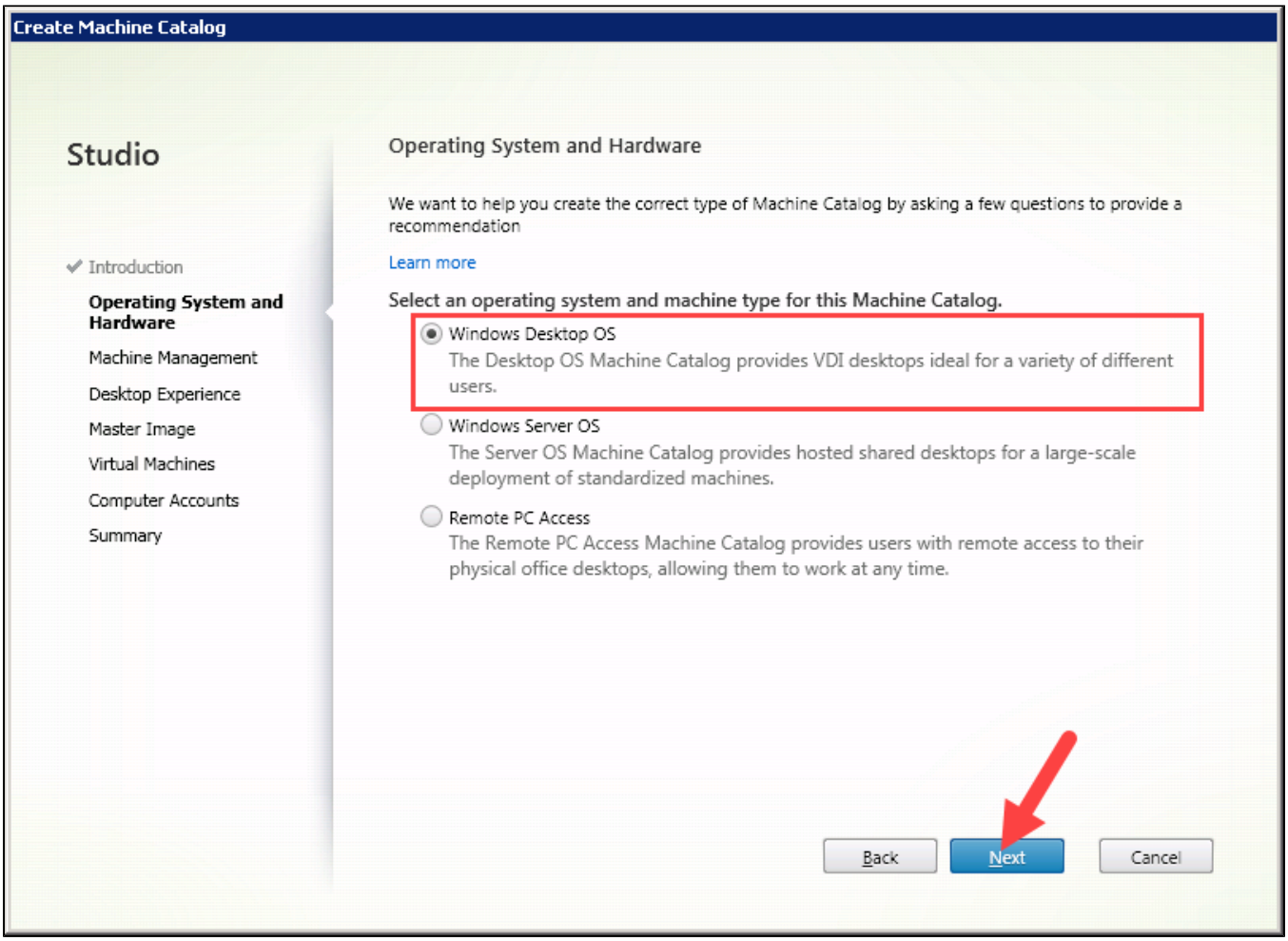
2) Подключитесь к контроллеру **Citrix Delivery Controller**.

3) Перейдите в **Machine Catalogs** и запустите **Create Machine Catalog**.

4) Нажмите **Next**.

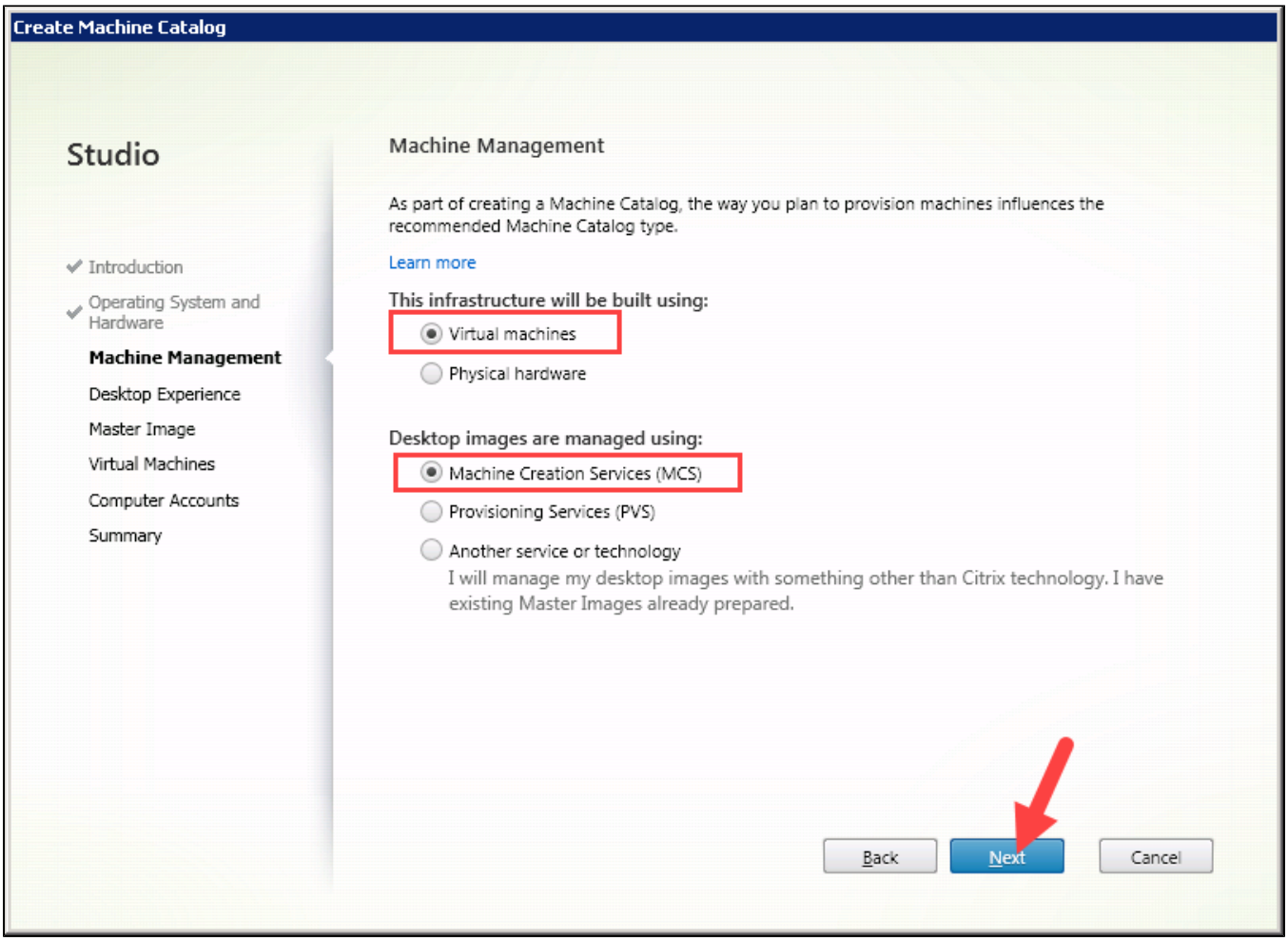


5) Установите переключатель в положение **Windows Desktop OS** и нажмите **Next**.

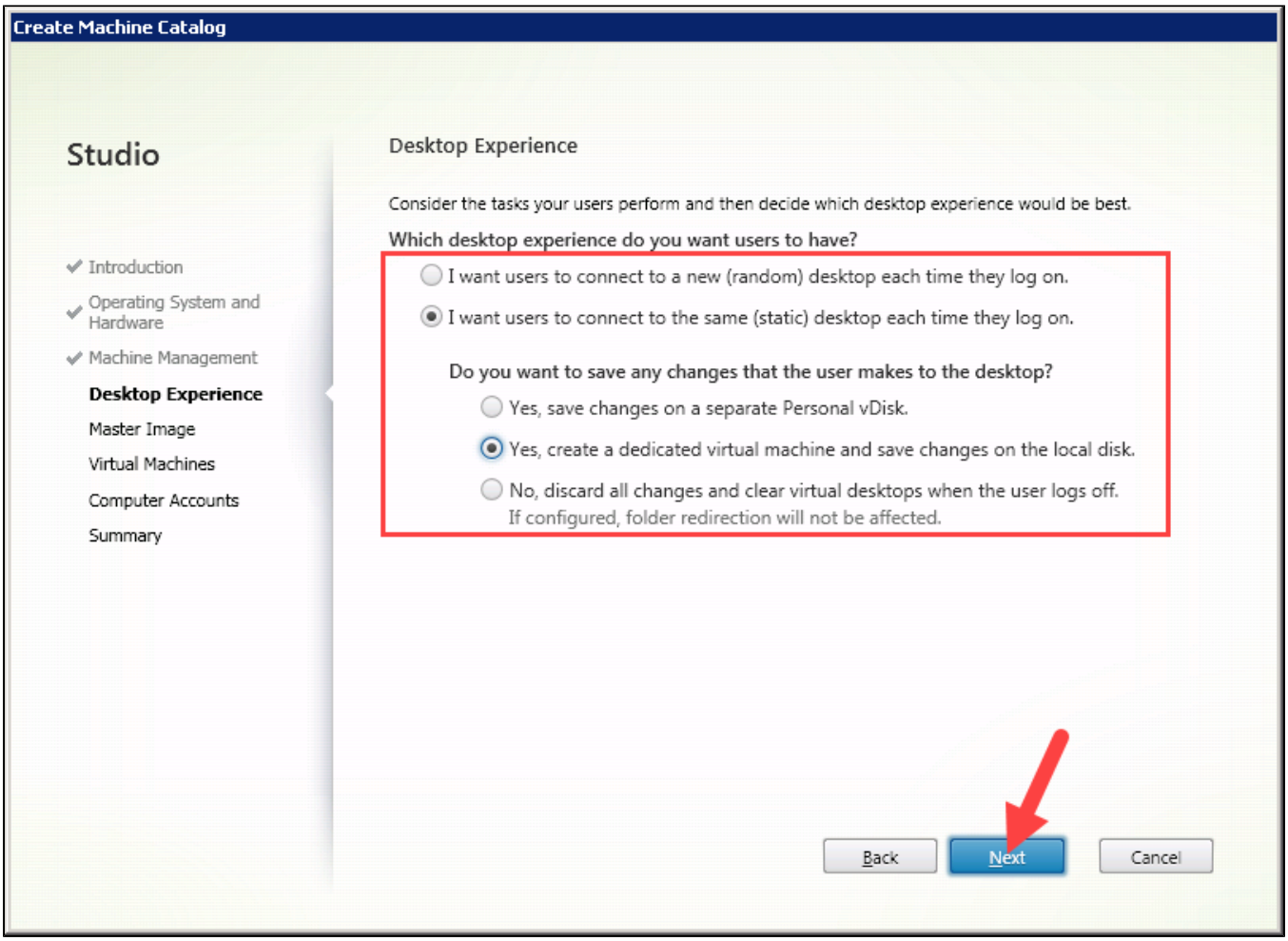


6) Установите переключатели **Virtual Machines** и **Machine Creation Services (MCS)**.

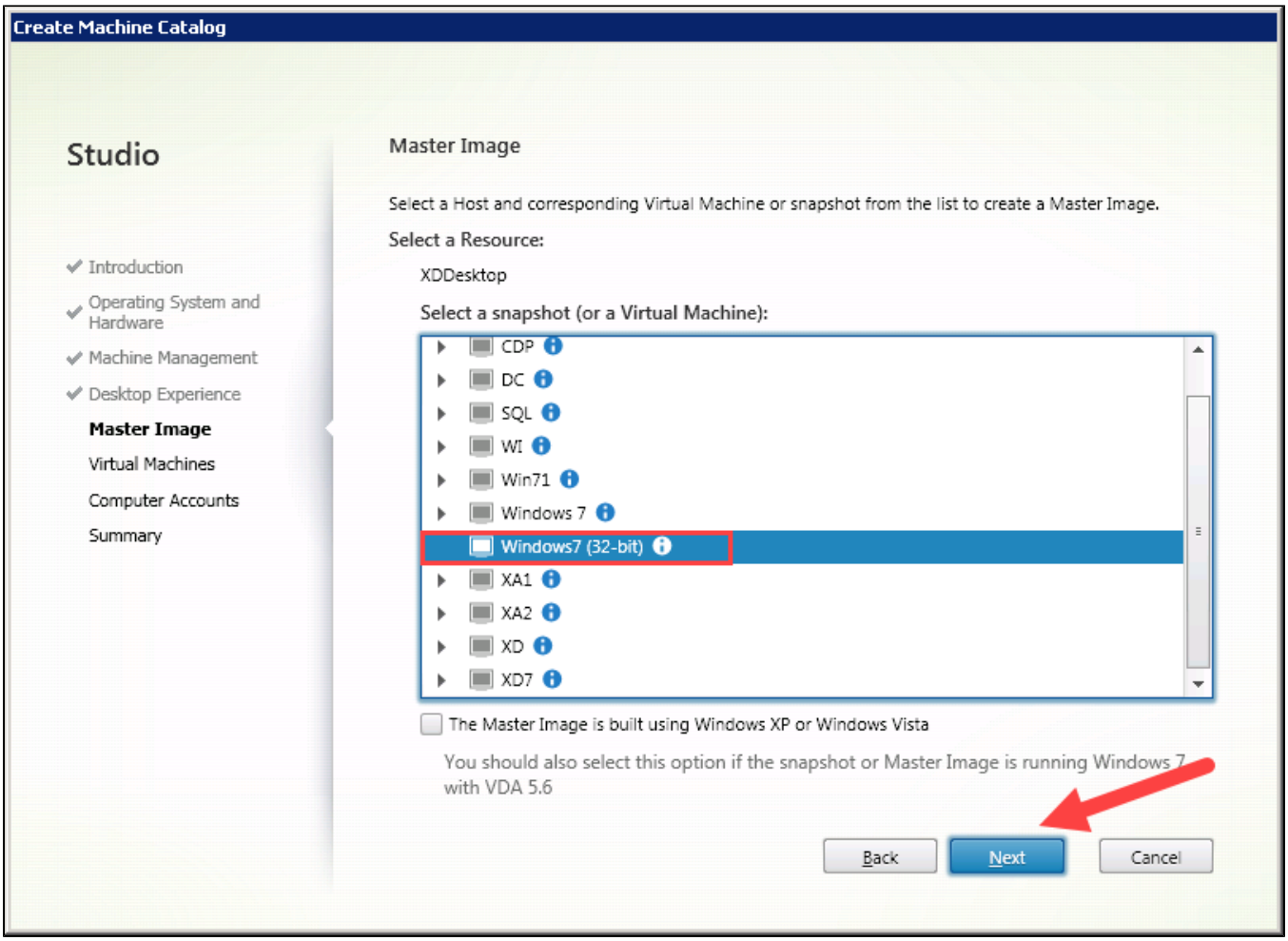
7) Нажмите **Next**.



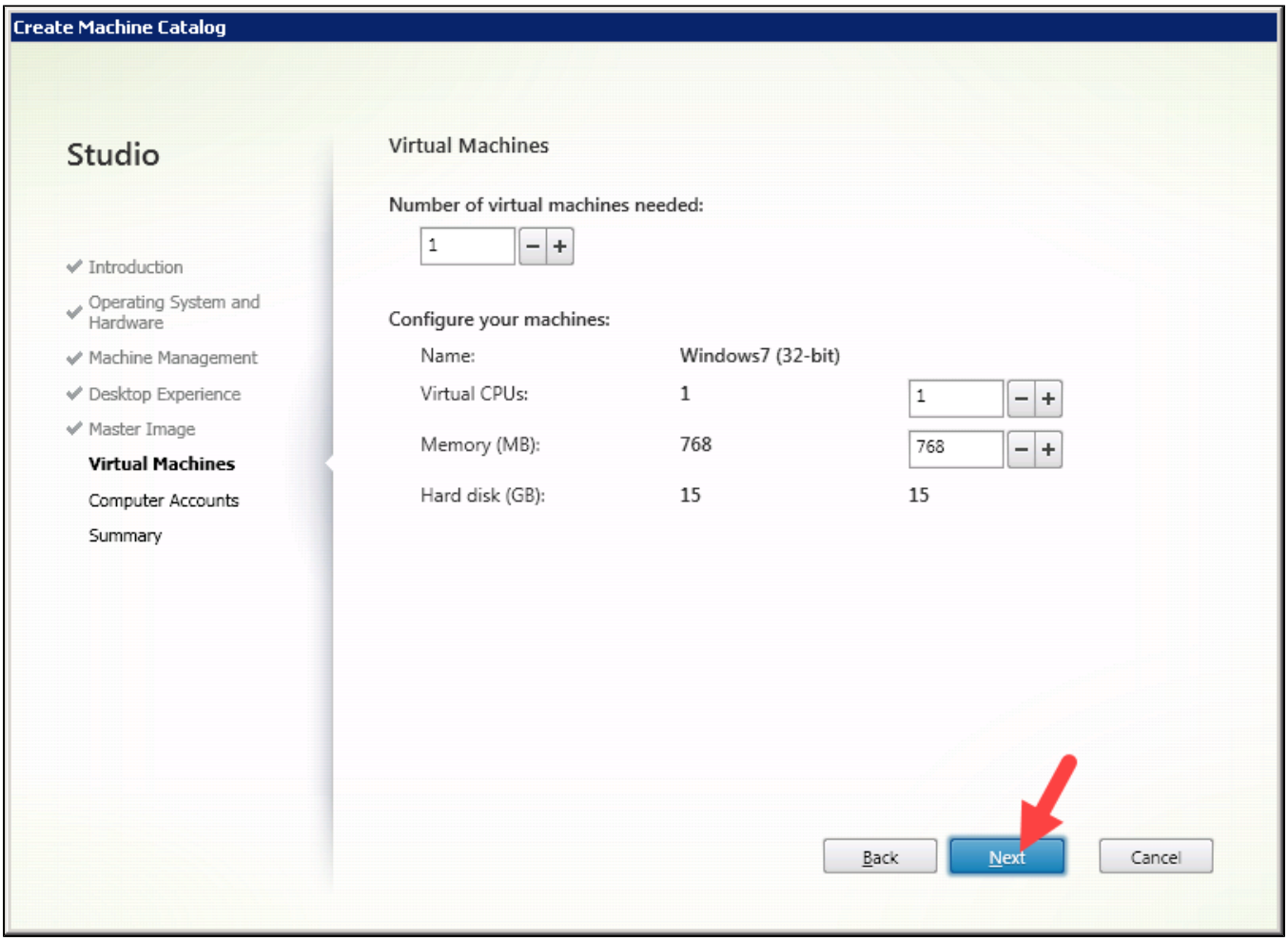
8) В окне **Desktop Experience** выберите необходимые параметры и нажмите **Next**.



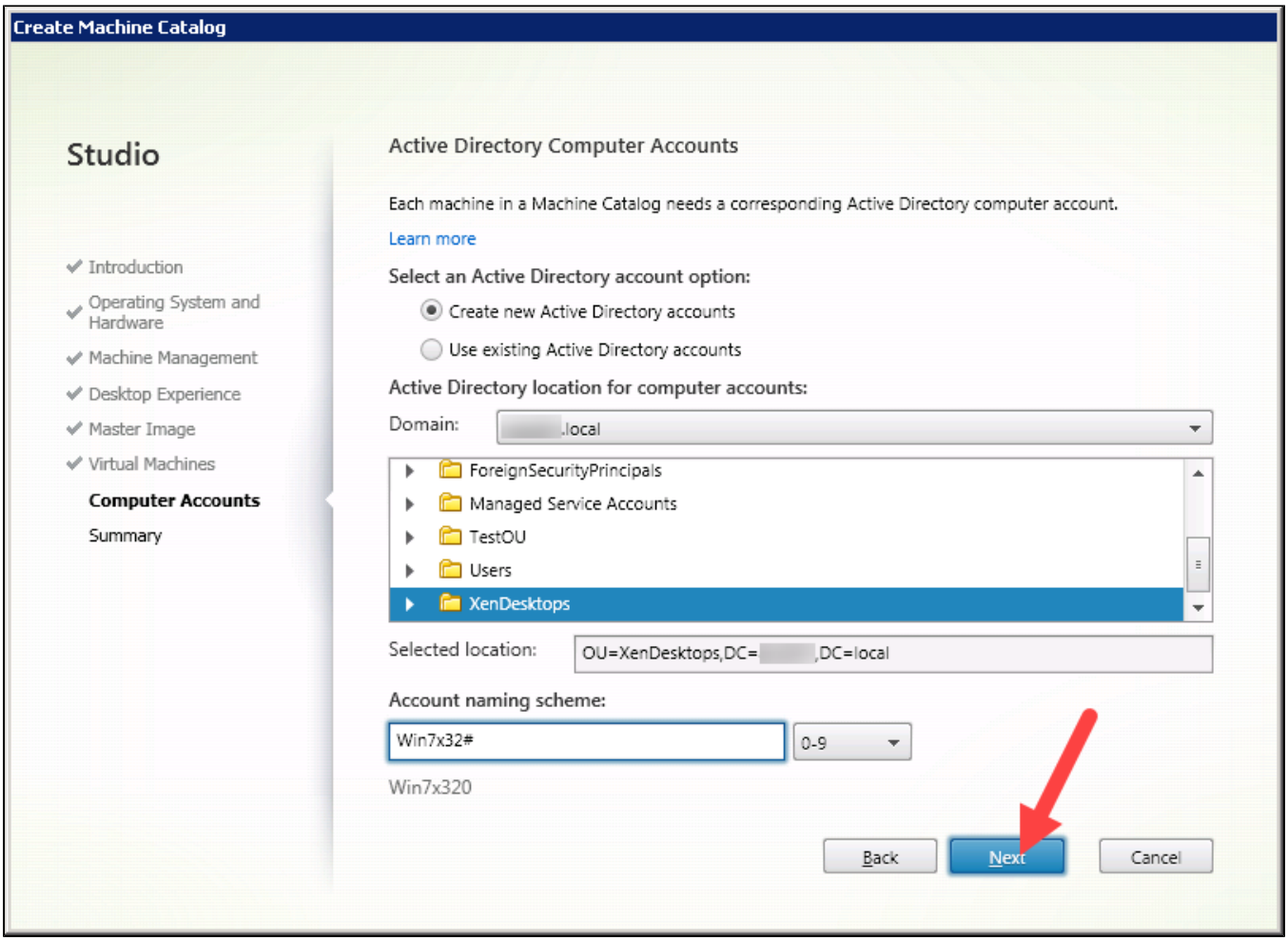
9) Щелкните по названию эталонной виртуальной машины и нажмите **Next**.



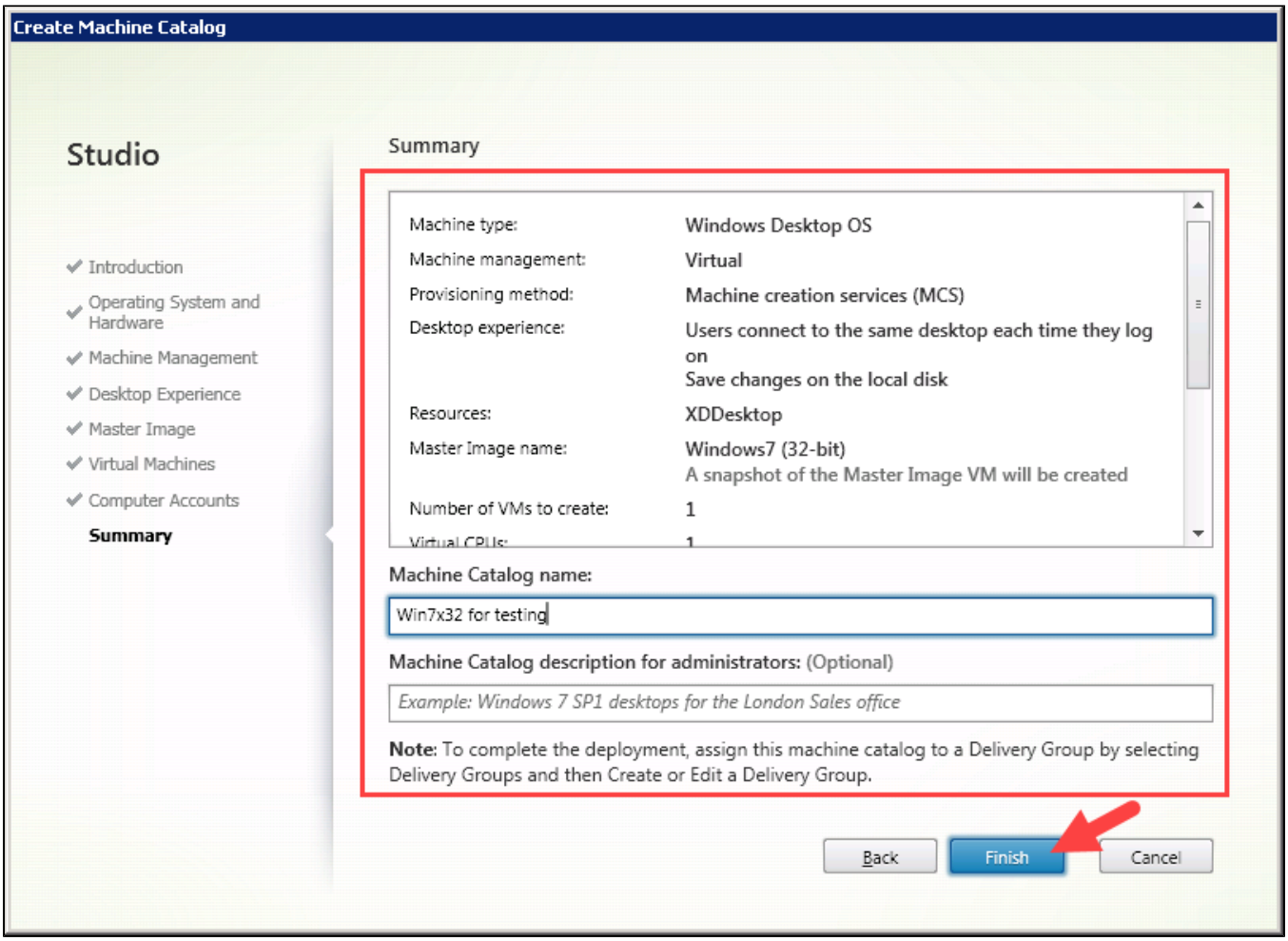
10) Задайте необходимое количество виртуальных машин и нажмите **Next**.



11) Выберите необходимые настройки и нажмите **Next**.



12) Проверьте параметры виртуальных машин, введите имя каталога, имя виртуальной машины и нажмите **Finish**. В результате каталог виртуальных машин будет создан.

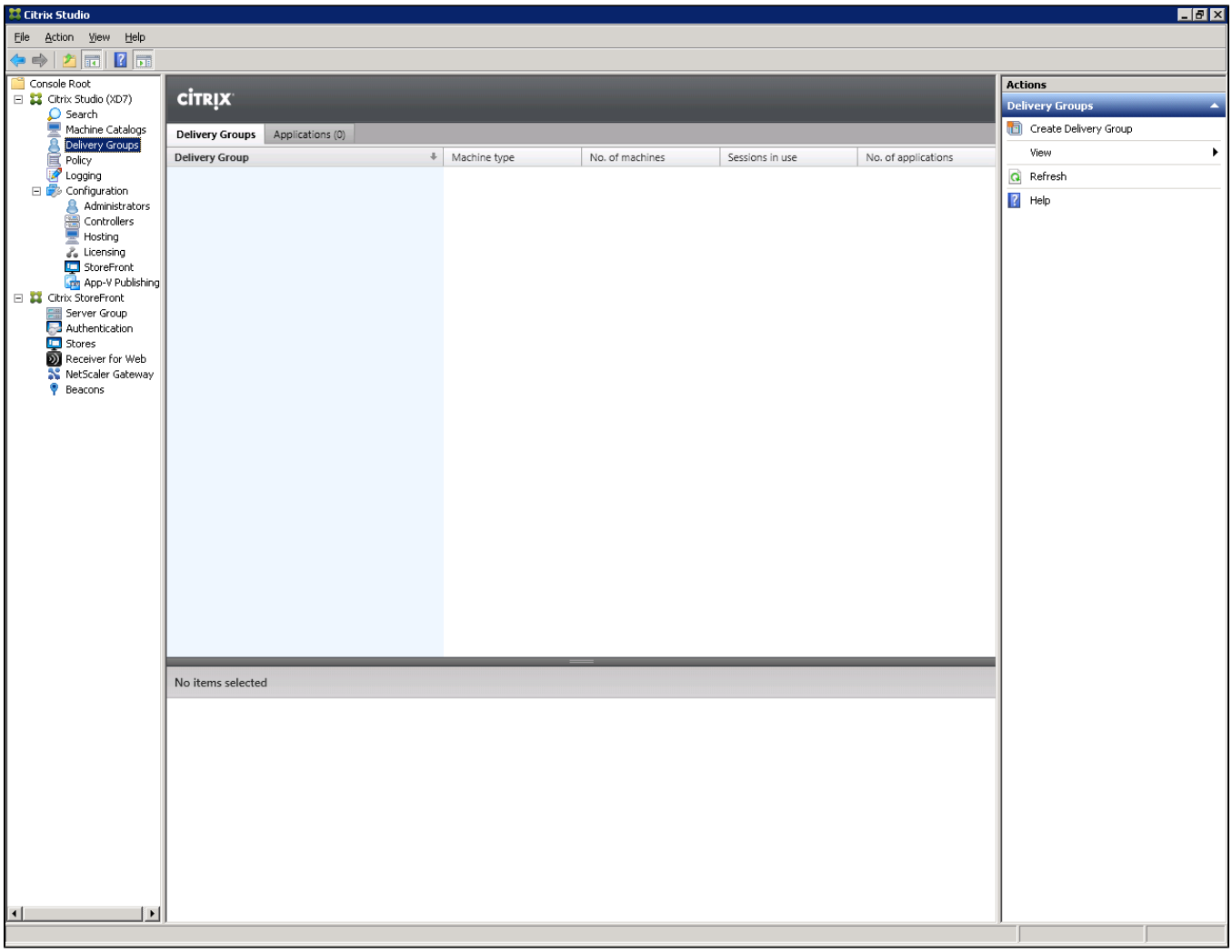


Создание группы пользователей виртуальных машин — Delivery Group

Чтобы создать группу пользователей:

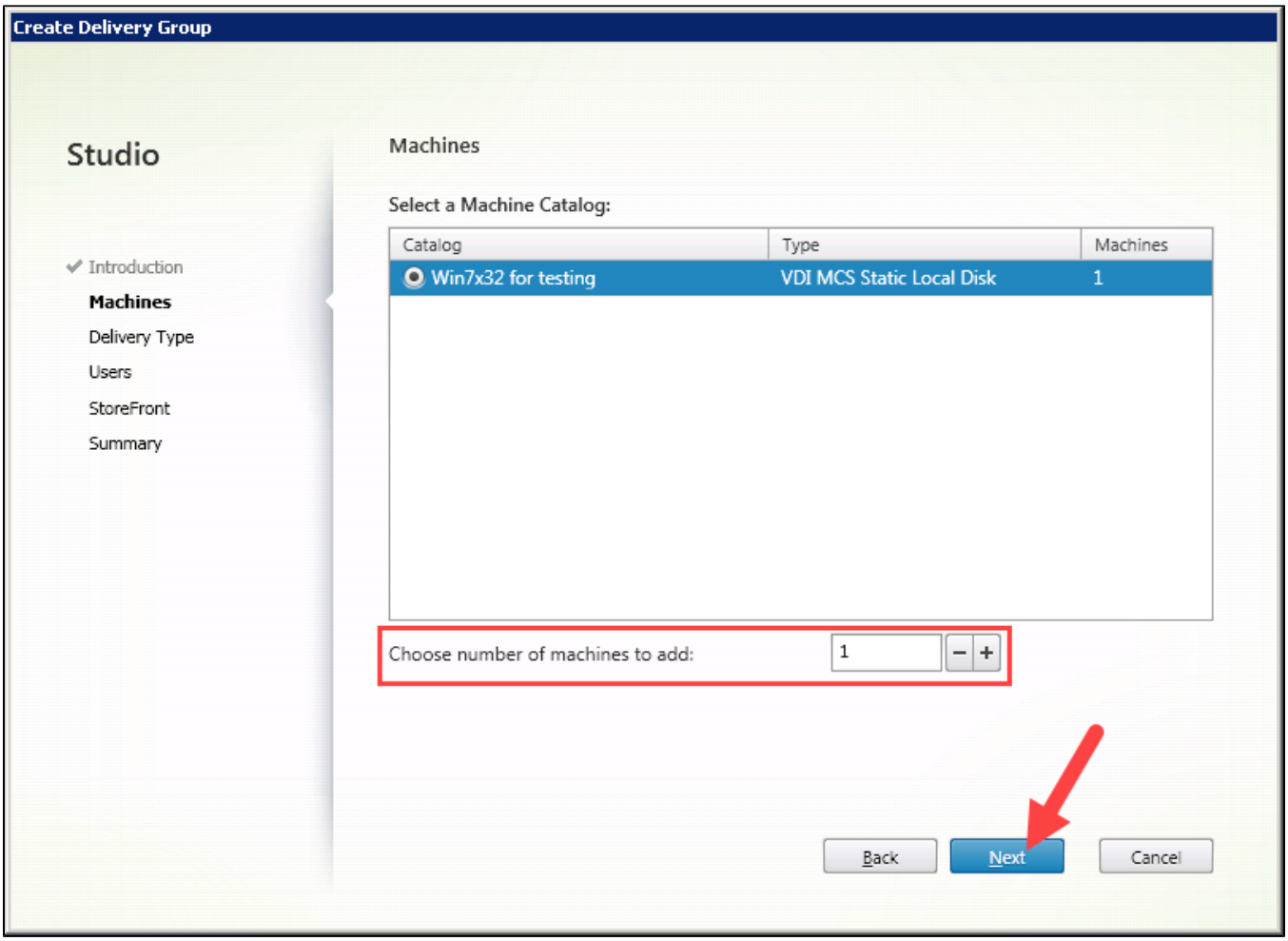
1) На сервере запустите **Citrix**. Для этого выберите пункт: Start → All Programs → Citrix.

2) Перейдите в меню: Delivery Group → Create Delivery Group.

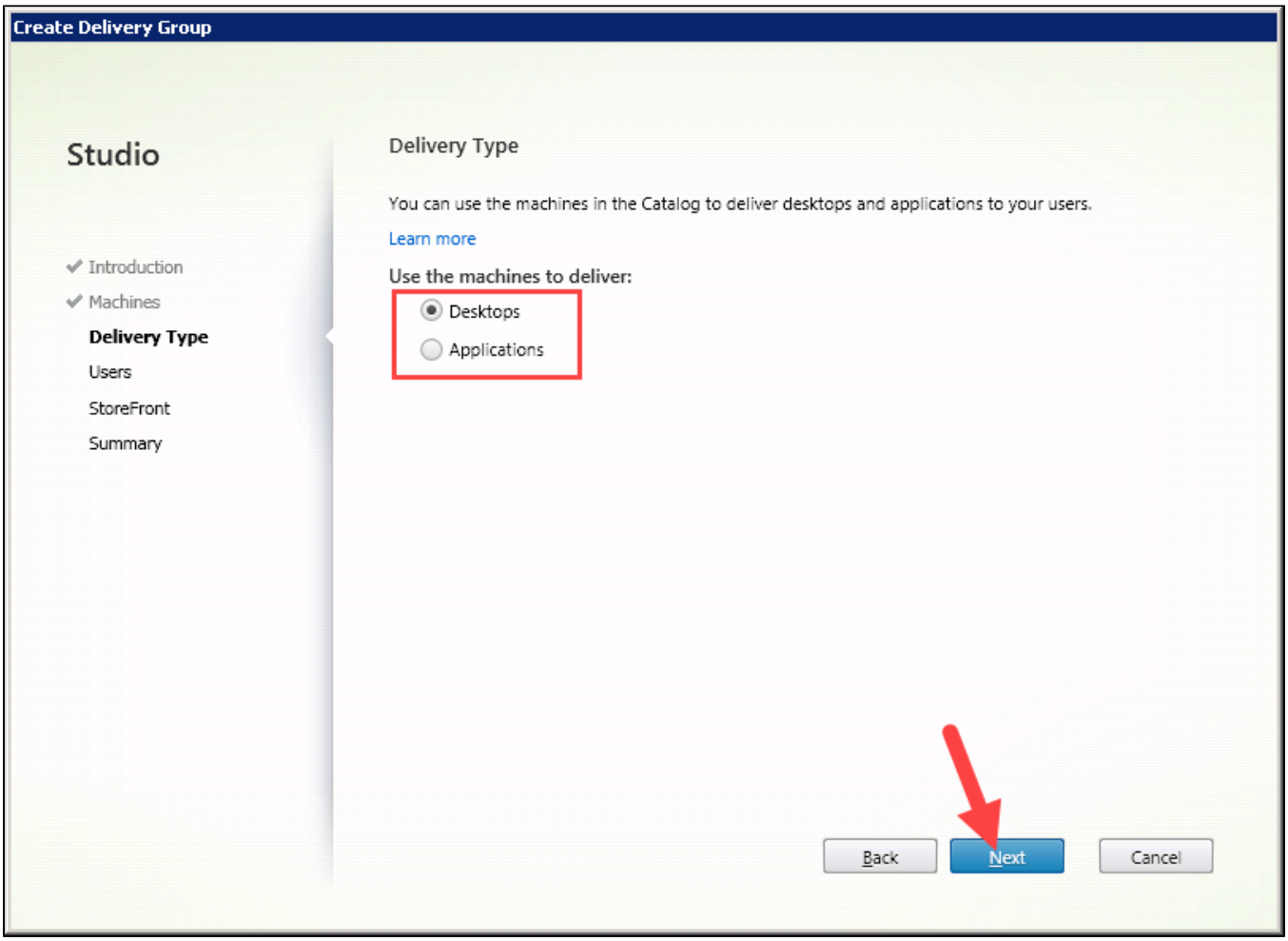


3) Выберите каталог виртуальных машин и укажите сколько виртуальных машин будет доступно этой группе пользователей.

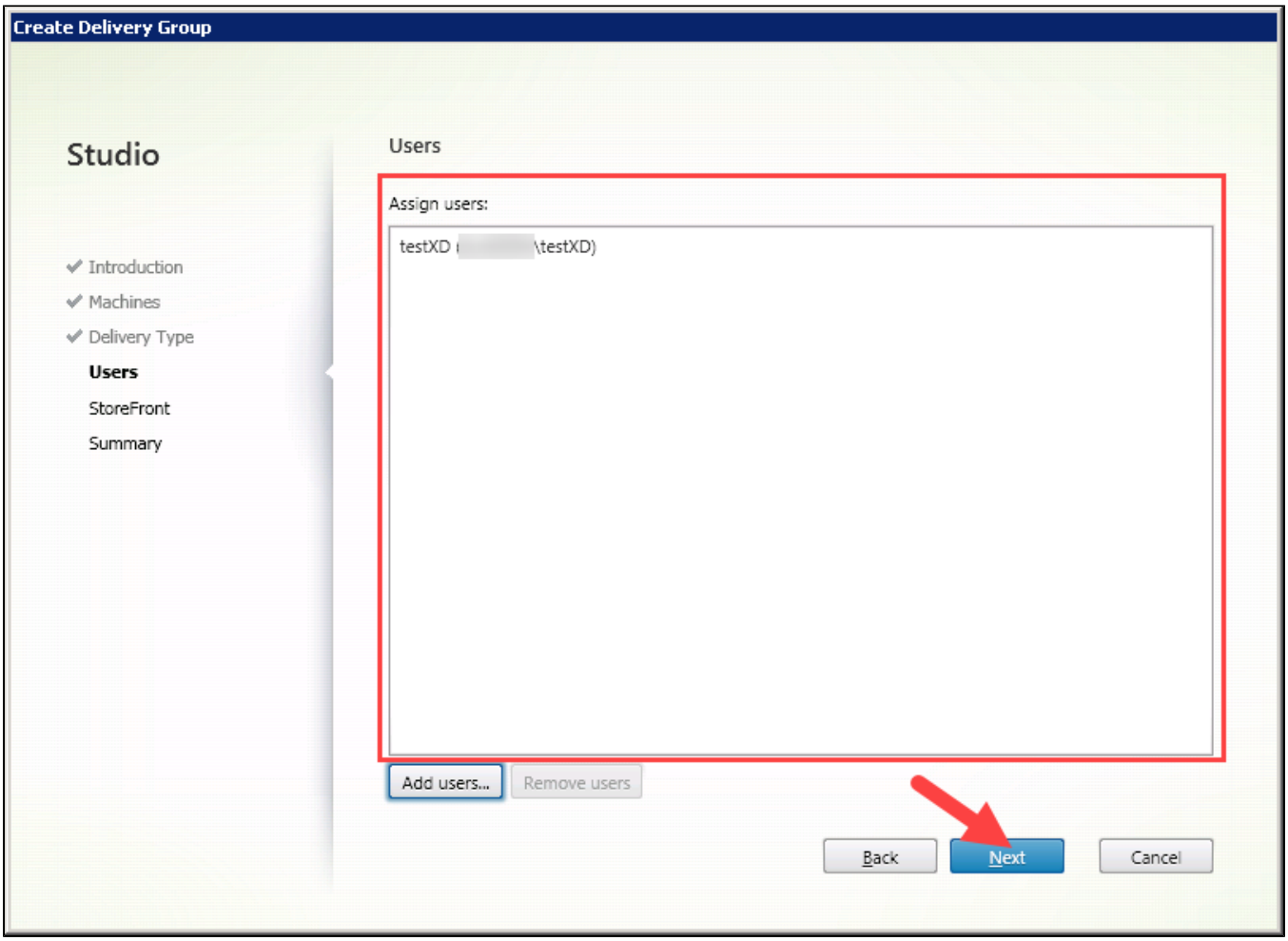
4) Нажмите **Next**.



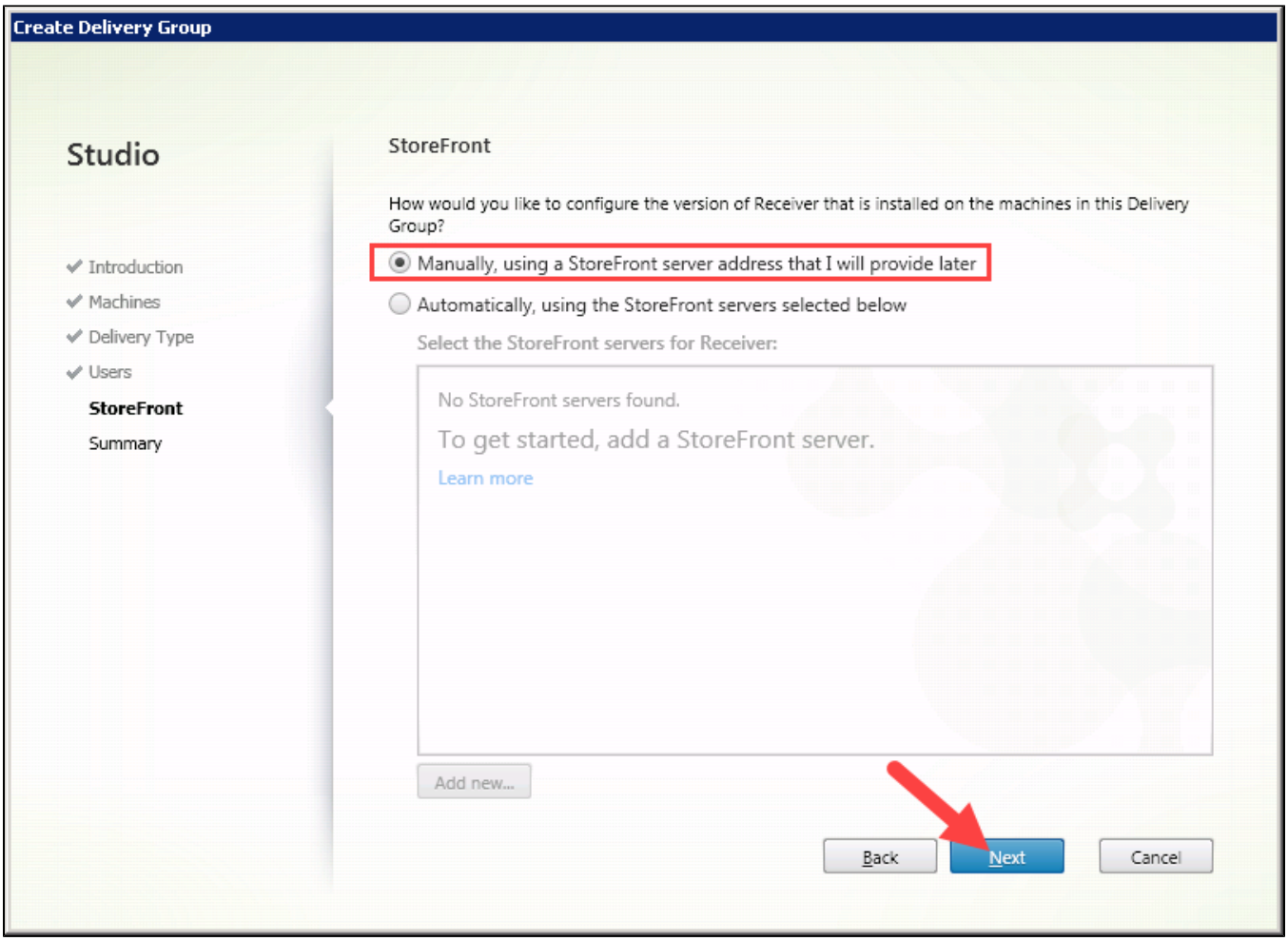
5) Выберите тип ресурсов и нажмите **Next**.



6) Выберите пользователей, с которыми будут связаны виртуальные машины, и нажмите **Next**.

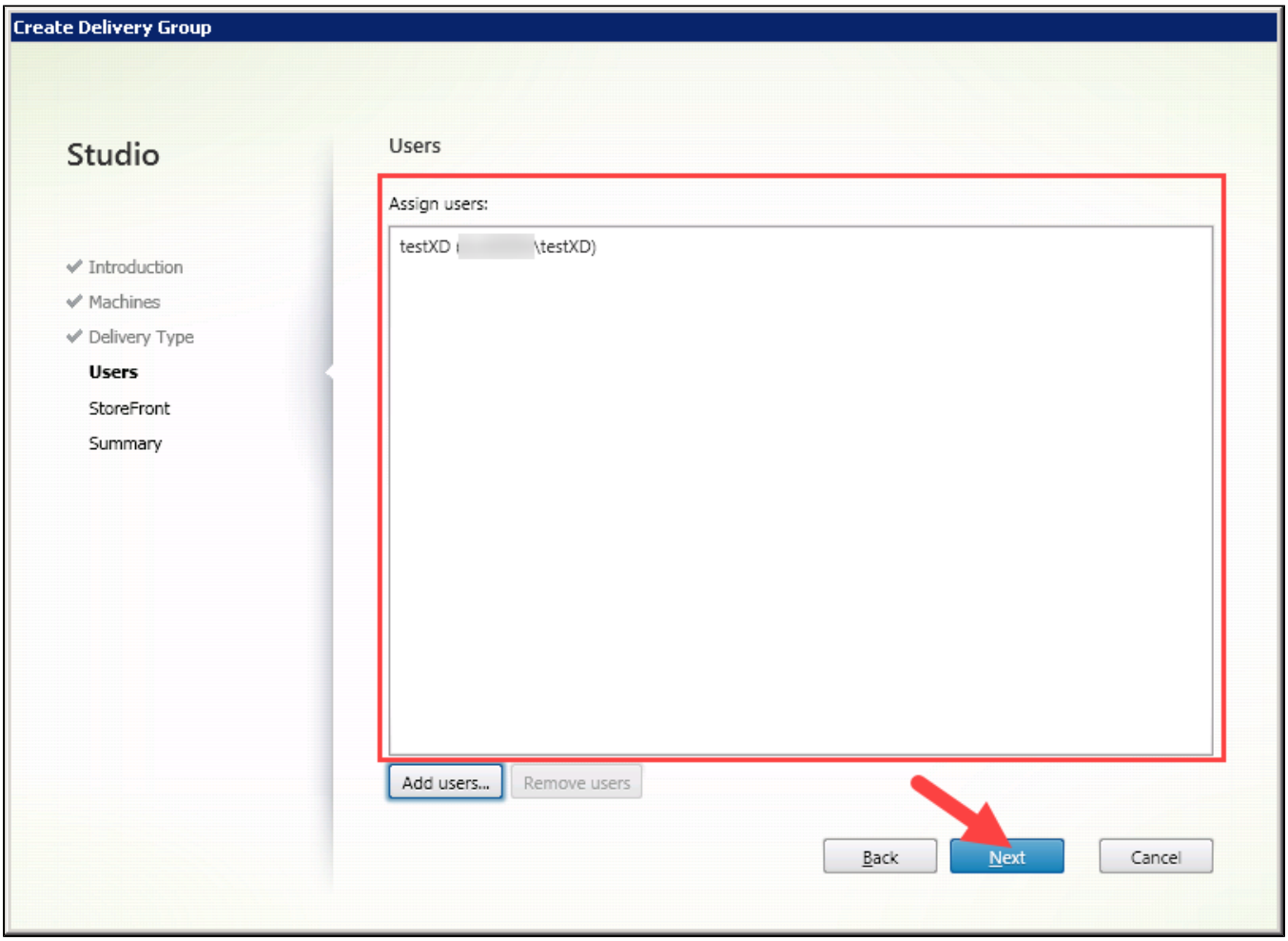


7) На следующем шаге установите переключатель **Manually, using a StoreFront server address that I will provide later** и нажмите **Next**.

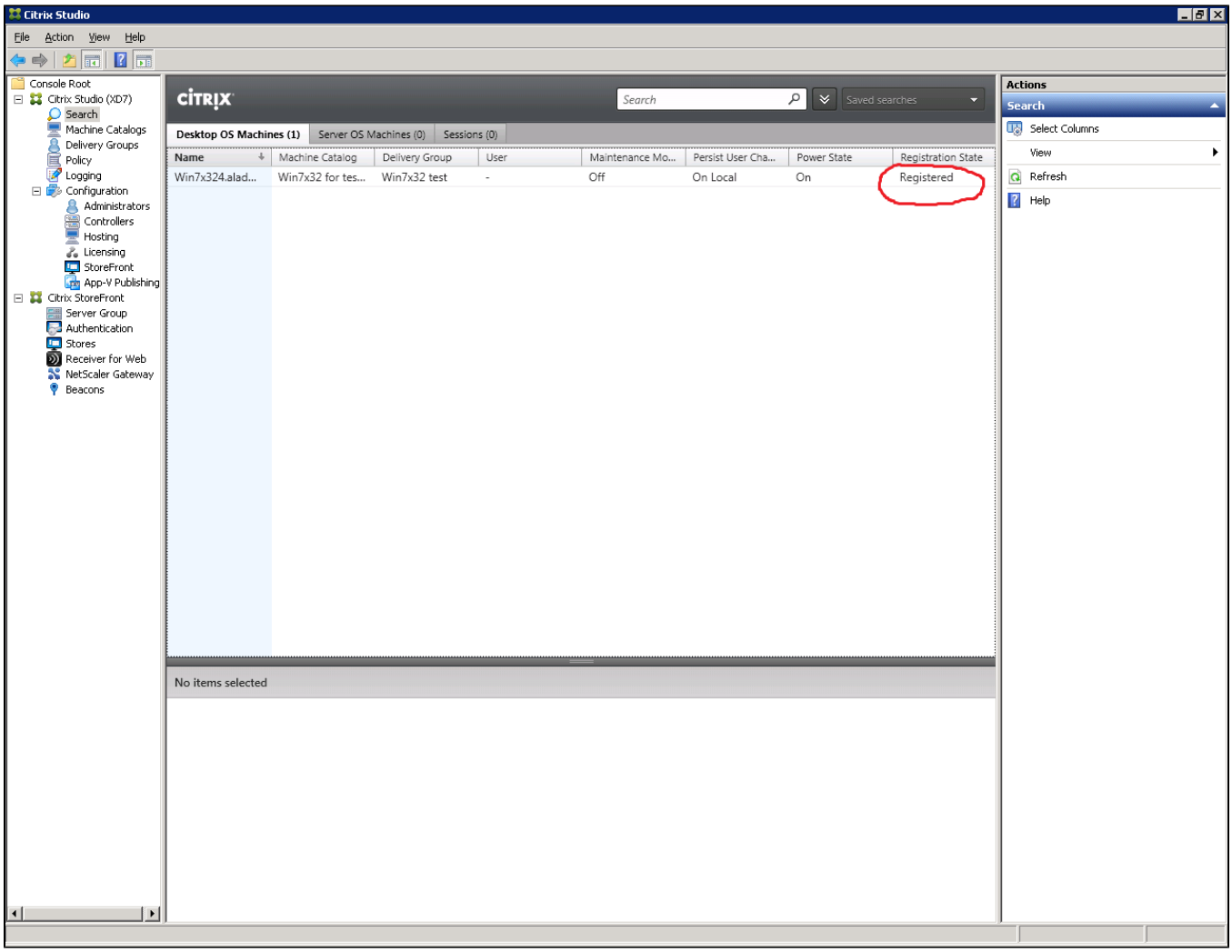


8) Проверьте корректность настроек и введите название группы.

9) Нажмите **Finish**. В результате группа пользователей будет создана.



Убедитесь в том, что все виртуальные машины зарегистрированы (у них должен быть статус Registered).



Проверка доступности виртуальных машин

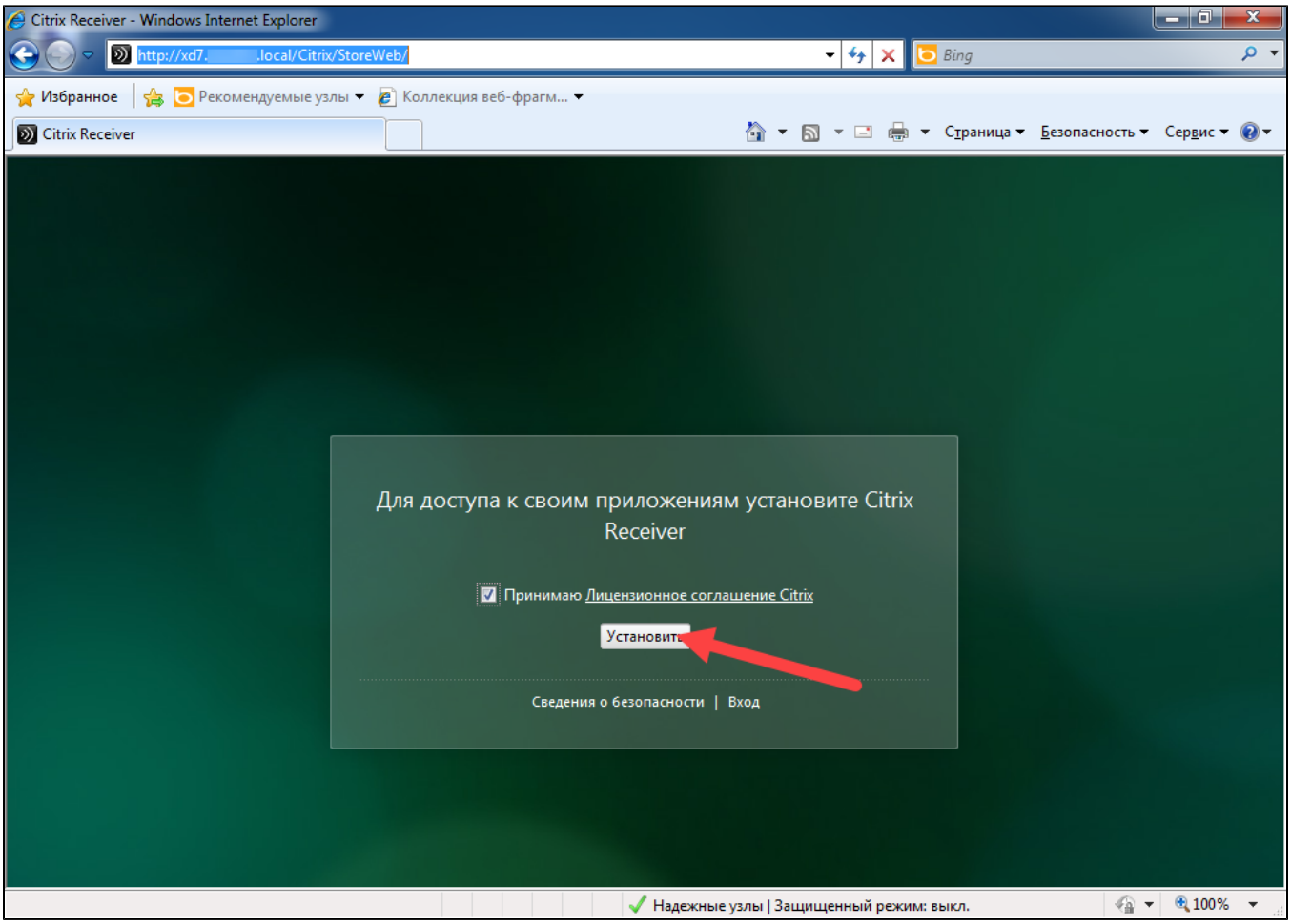
Чтобы проверить доступность виртуальной машины:

1) Перейдите на эталонную виртуальную машину.

2) Откройте браузер и в адресной строке укажите:

http://xd7.aktiv.local/Citrix/StoreWeb/

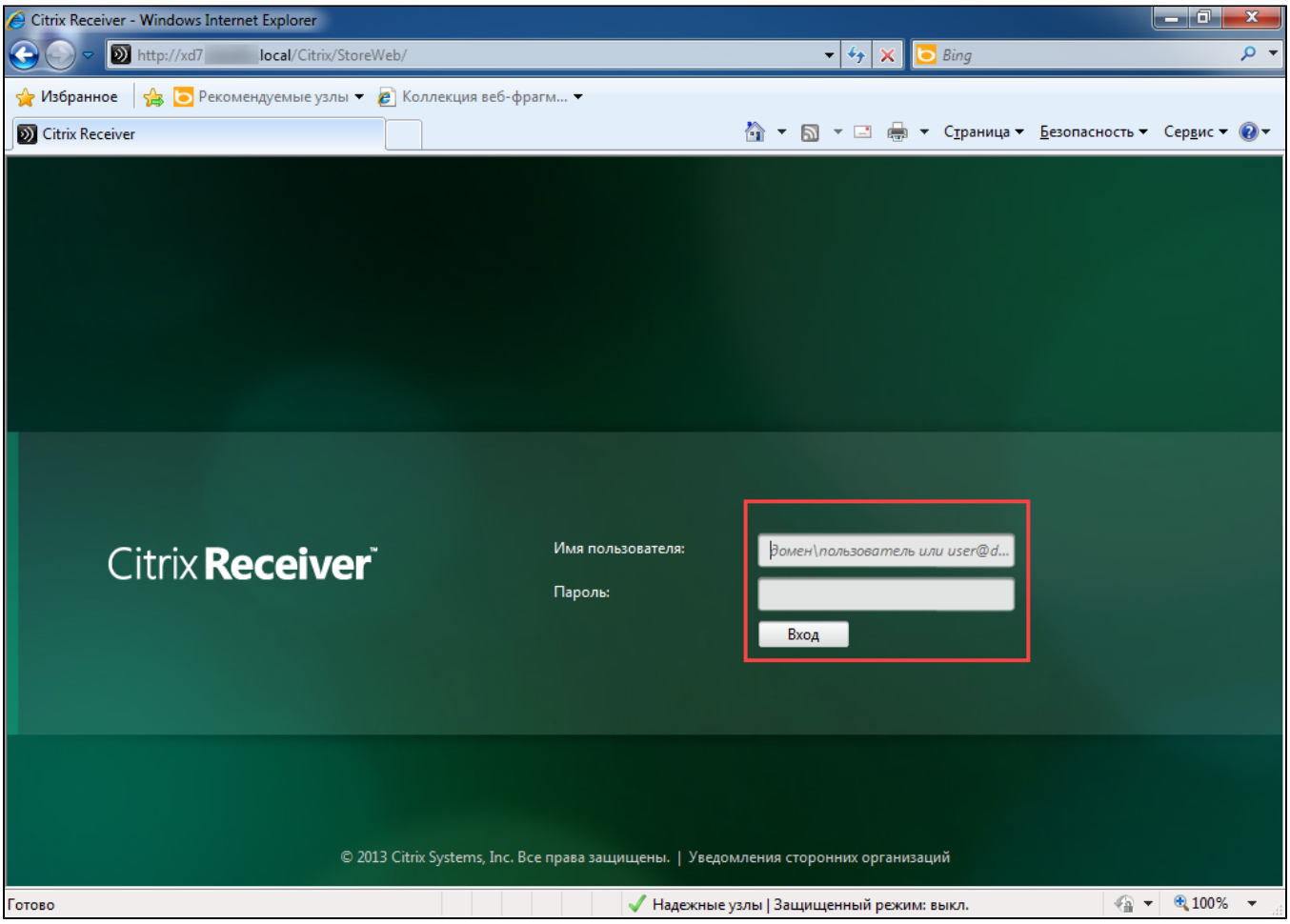
3) Если ПО Citrix Receiver не установлено, то в окне с предложением установки нажмите **Установить**.



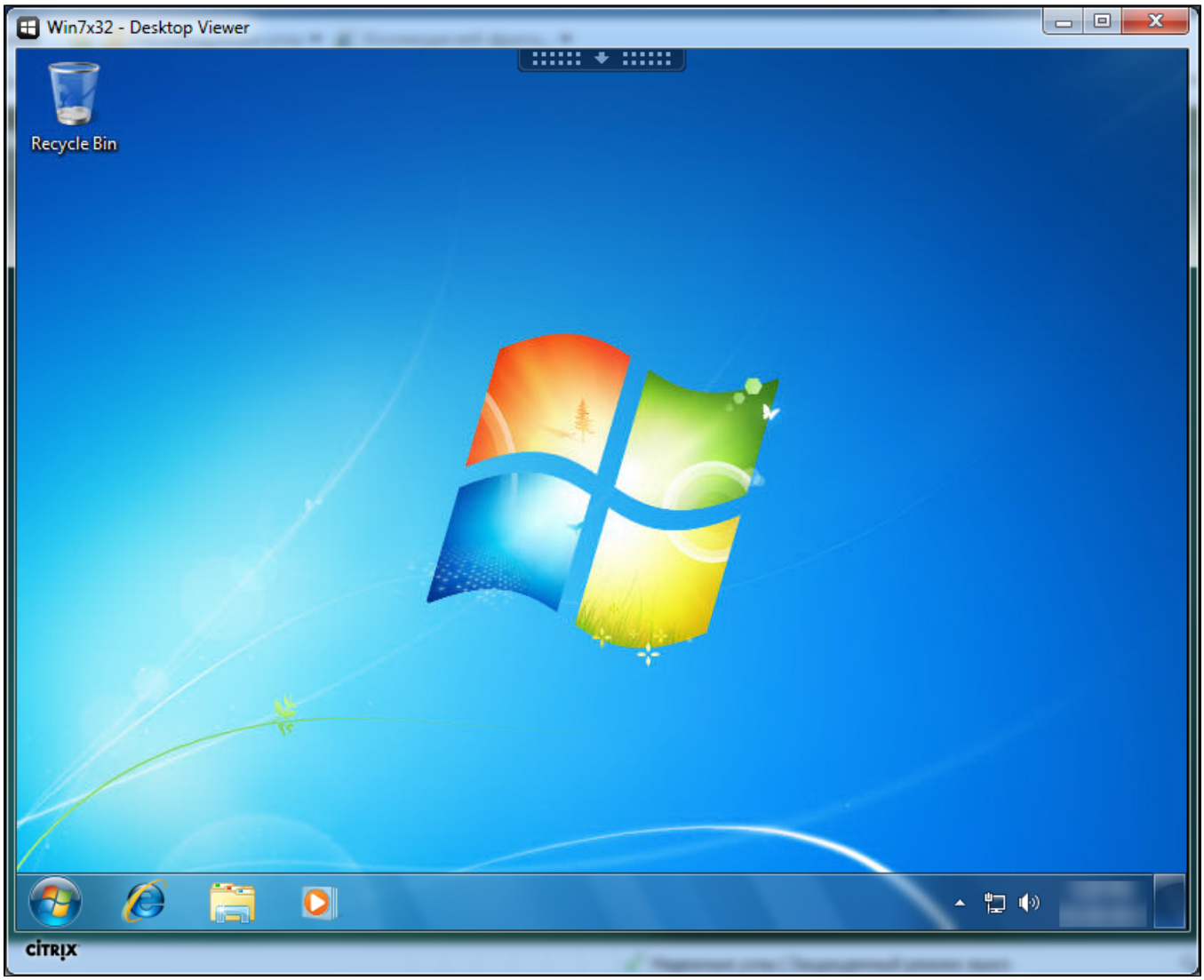
4) Дождитесь окончания процесса установки.

5) Введите логин и пароль учетной записи пользователя. Эта учетная запись должна входить в группу пользователей виртуальных машин.

6) Нажмите **Вход**.



7) Убедитесь в том, что виртуальная машина доступна.

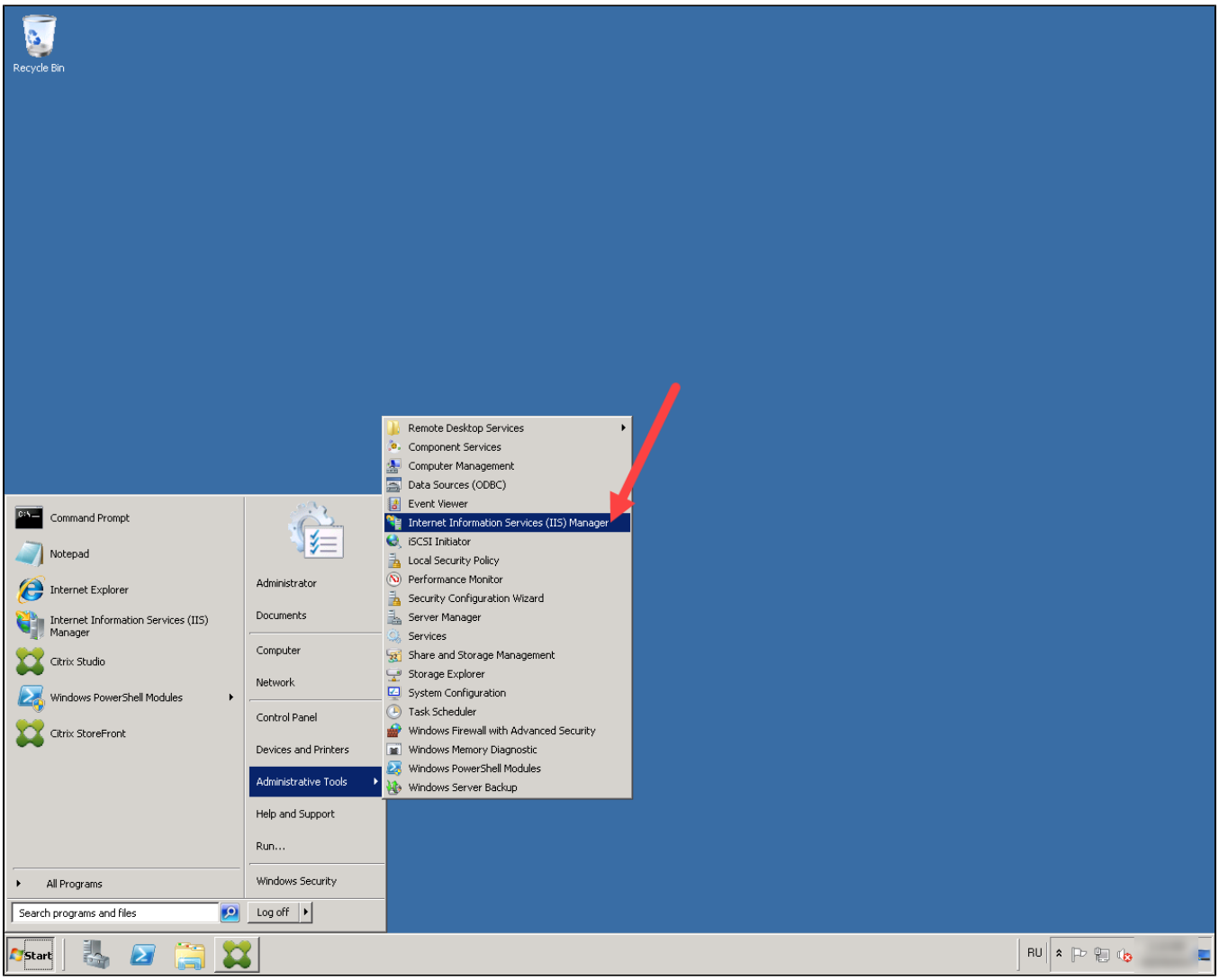


Настройка аутентификации по смарт-картам

Выпуск сертификата для IIS

Чтобы выпустить сертификат для IIS:

1) На сервере запустите оснастку управления сервисом **Internet Information Services (IIS)**.

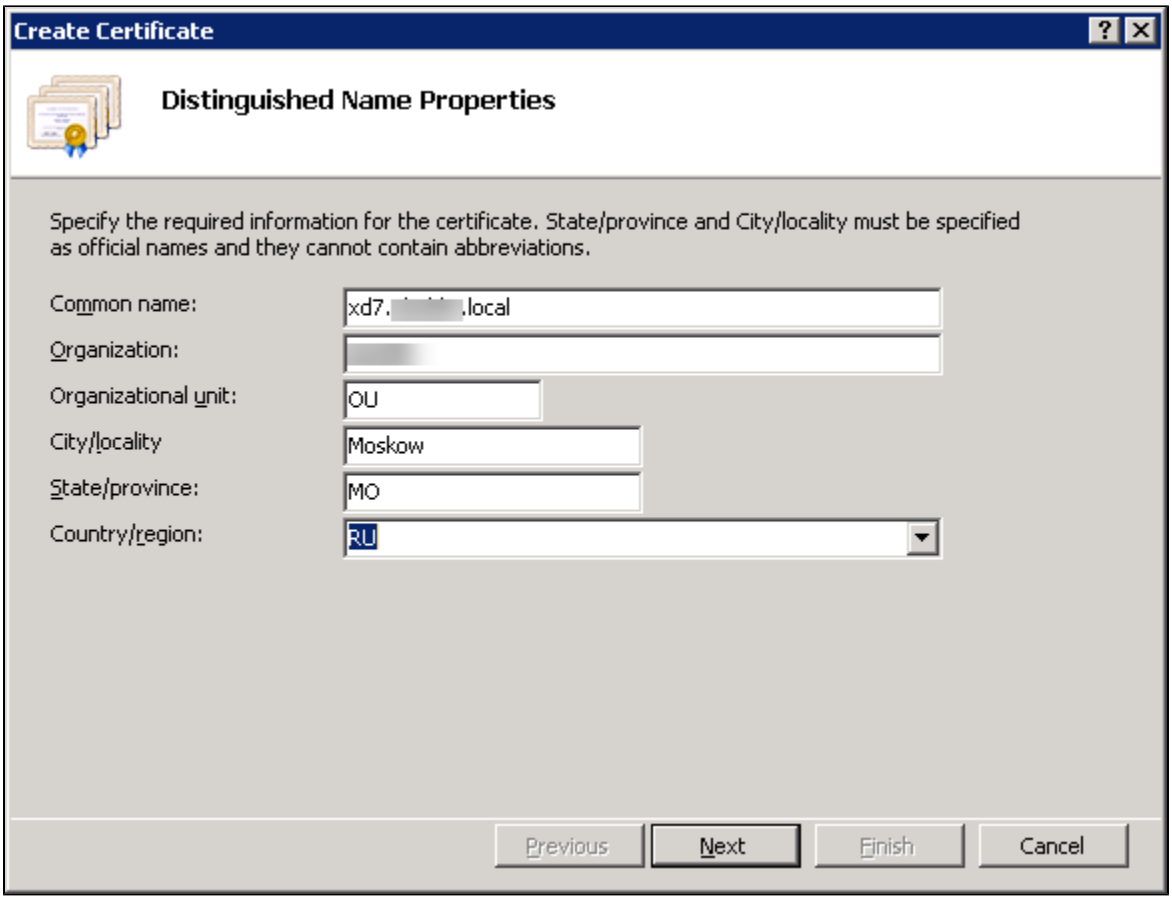


2) Выберите пункт **Server Certificates**.

3) Выберите **Create Domain Certificate**.

4) Введите информацию об организации.

5) В поле **Common name** введите полное доменное имя сервера. В нашем примере это: x7.aktiv.local.

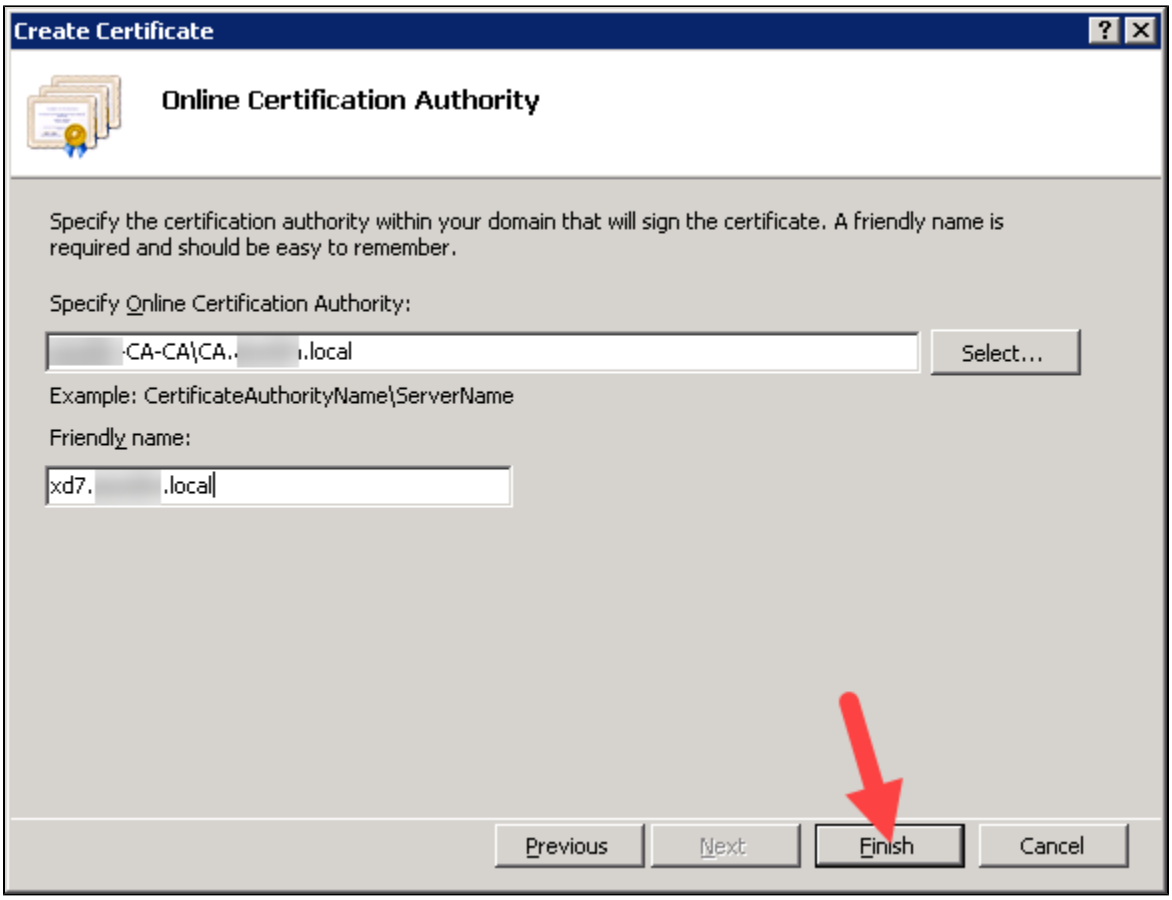


6) Нажмите **Next**.

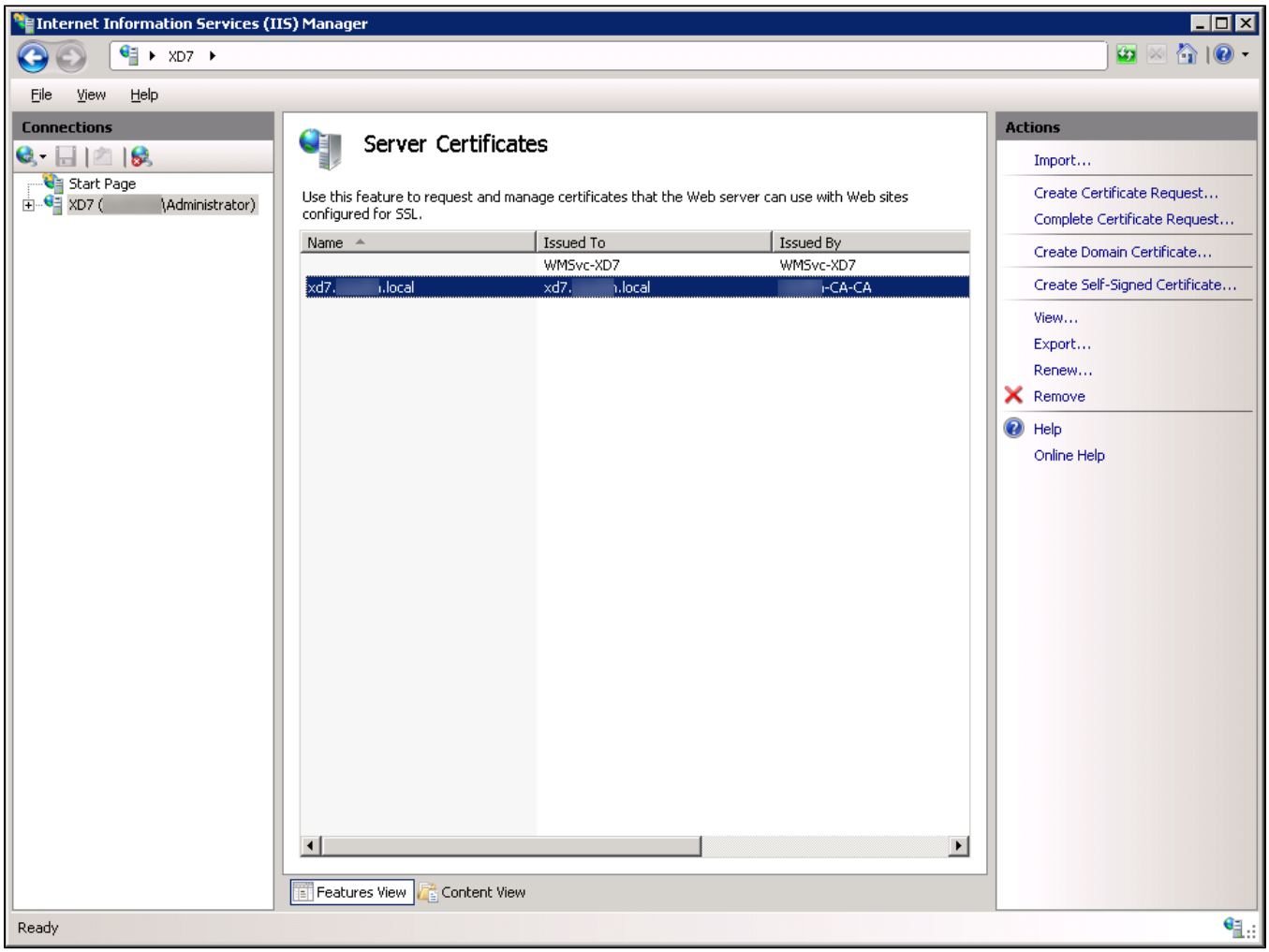
7) Выберите центр сертификации.

8) В поле **Friendly name** введите полное имя сервера. В нашем примере это: x7.aktiv.local.

9) Нажмите **Finish**.



10) Проверьте, что сертификат успешно выпущен.

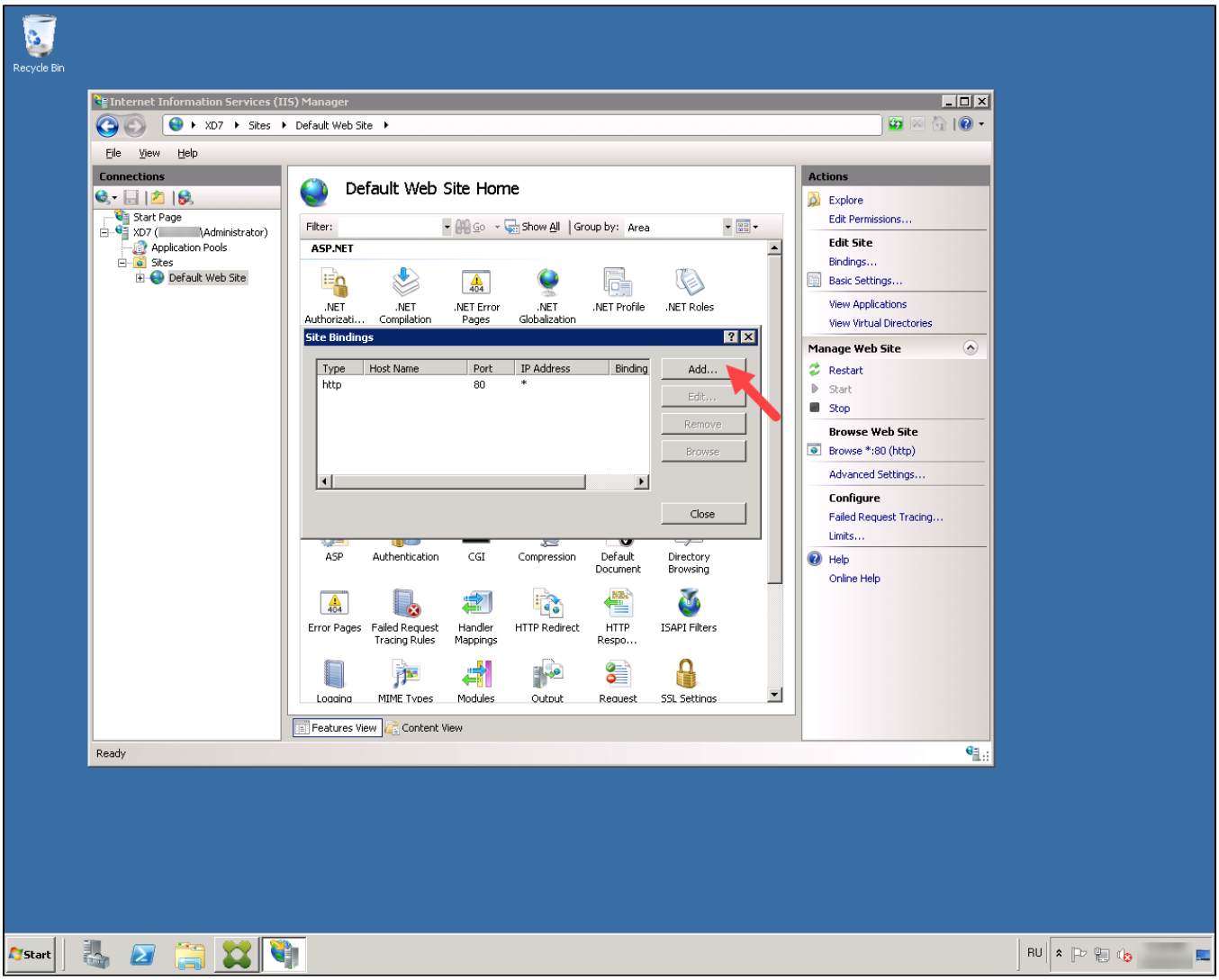


Настройка SSL доступа к IIS

Чтобы настроить SSL доступ:

1) Выберите пункт **Default Web Site** и щелкните **Bindings**.

2) Нажмите **Add**.



3) В раскрывающемся списке **Type** выберите тип соединения https.

4) В раскрывающемся списке **SSL certificate** выберите сертификат.

5) Нажмите **OK**.

6) Убедитесь в том, что данный тип соединения добавлен.

7) Нажмите **Close**.

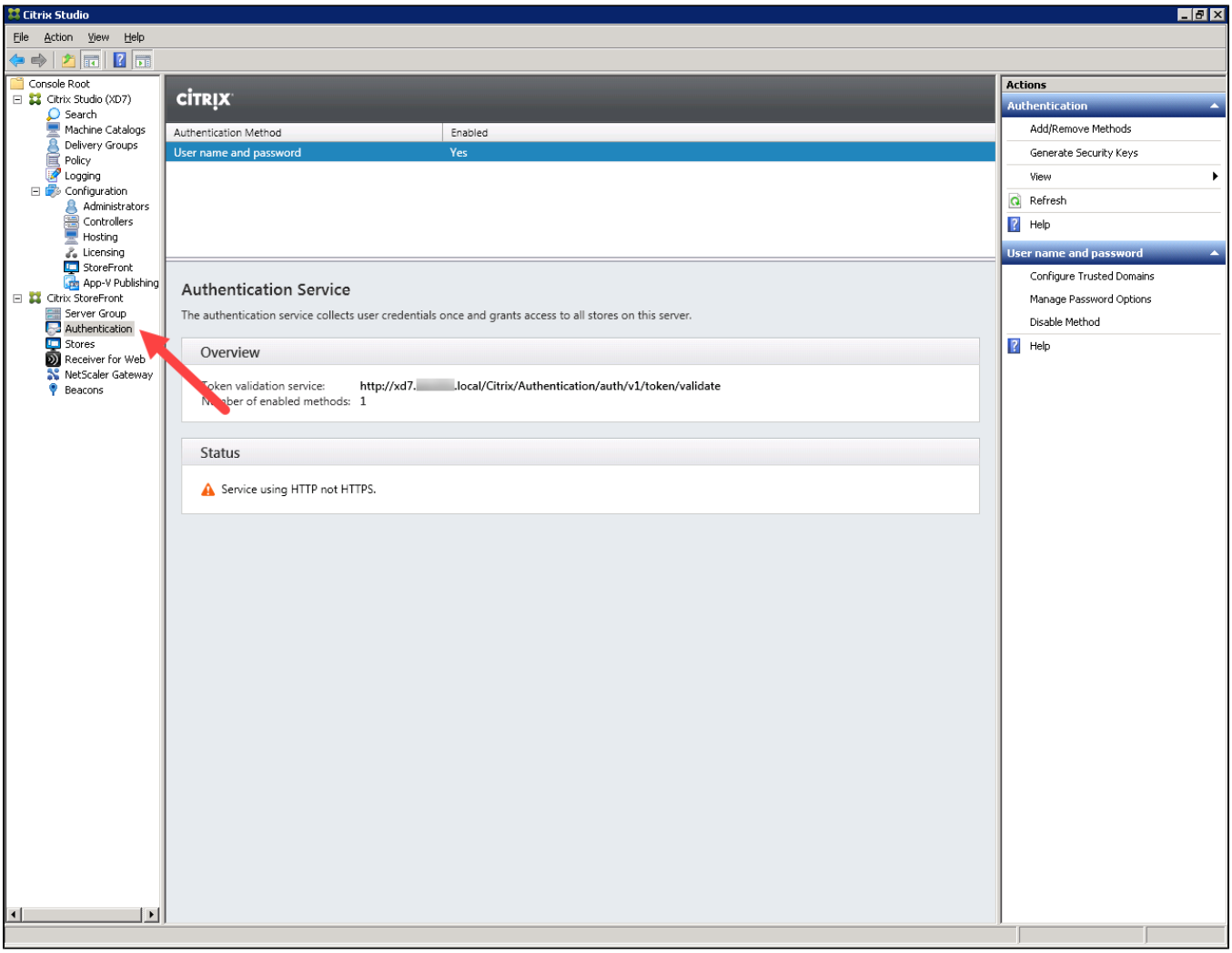
Настройка Citrix StoreFront

При работе с StoreFront в многосерверных установках используйте только один сервер при внесении изменений в настройки. Убедитесь в том, что консоль управления Citrix StoreFront не выполняется на другом сервере или серверах данной серверной группы. После завершения конфигурирования убедитесь в том, что изменения применились на все серверы группы (propagate your configuration changes to the server group).

Чтобы настроить Citrix StoreFront^

1) На сервере запустите **Citrix**.

2) Выберите пункт **Authentication**.

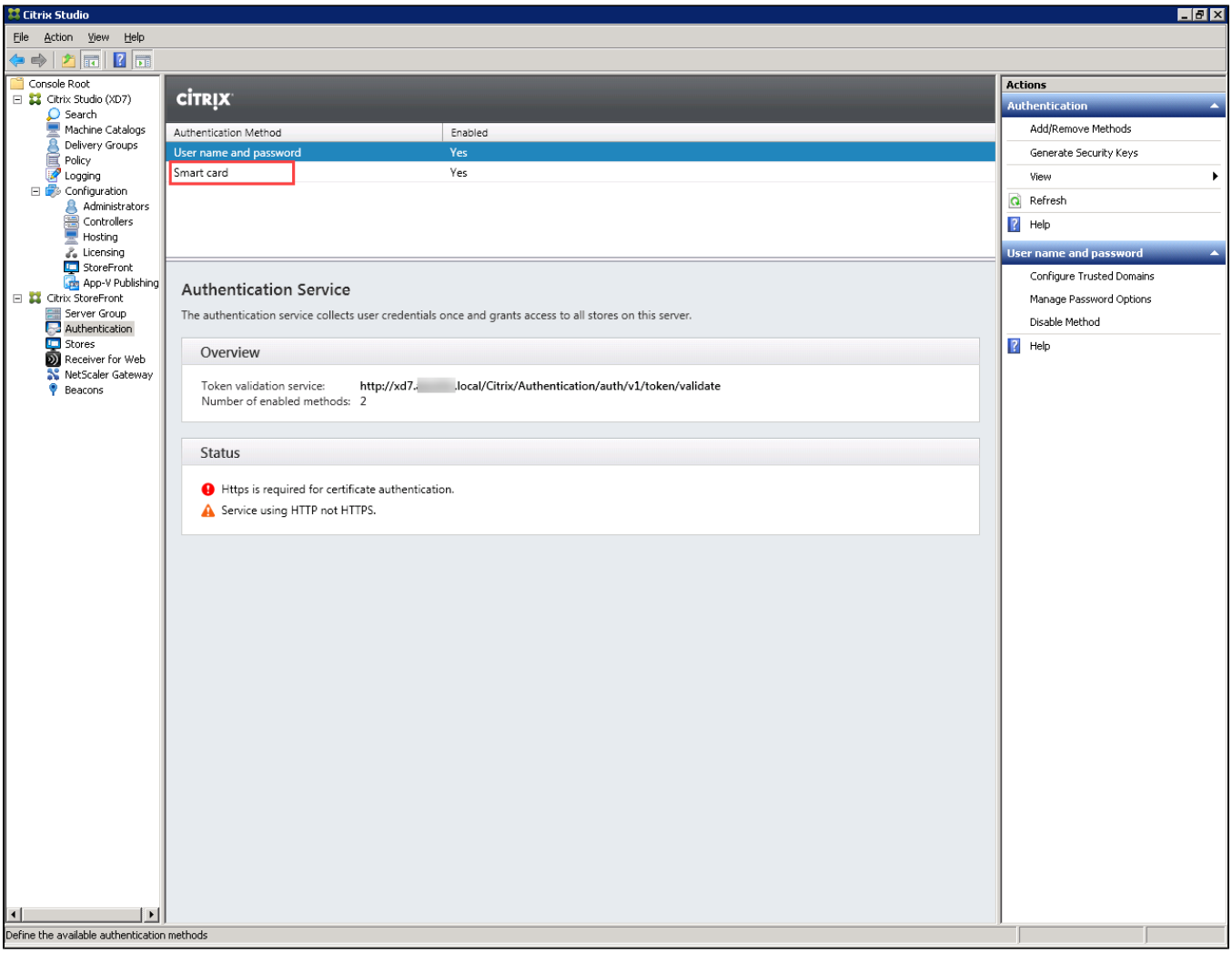


3) Выберите пункт **Add/Remove Authentication Methods**.

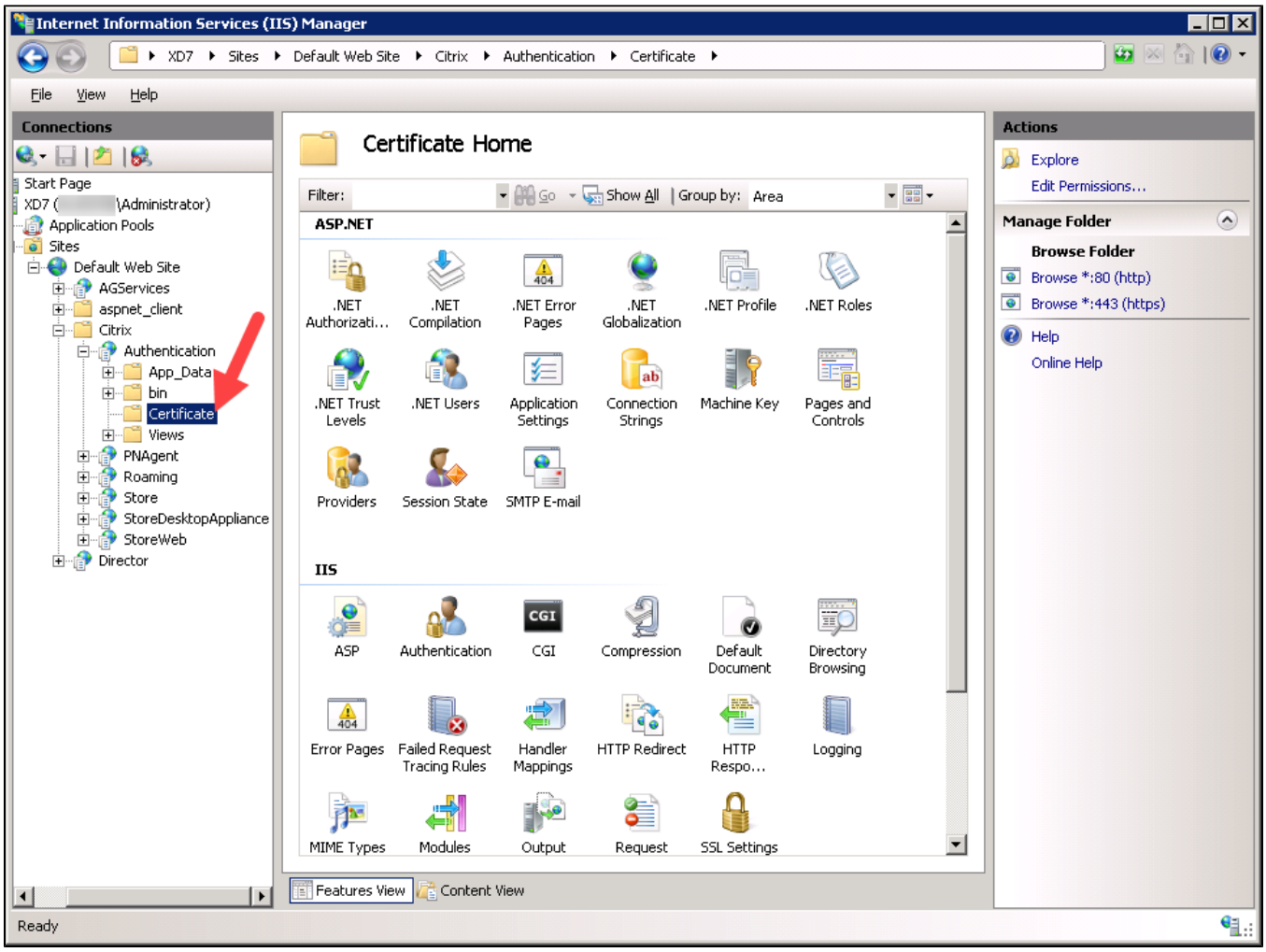
4) В окне **Add/Remove Methods** установите галочку **Smart card**.

5) Нажмите **OK**.

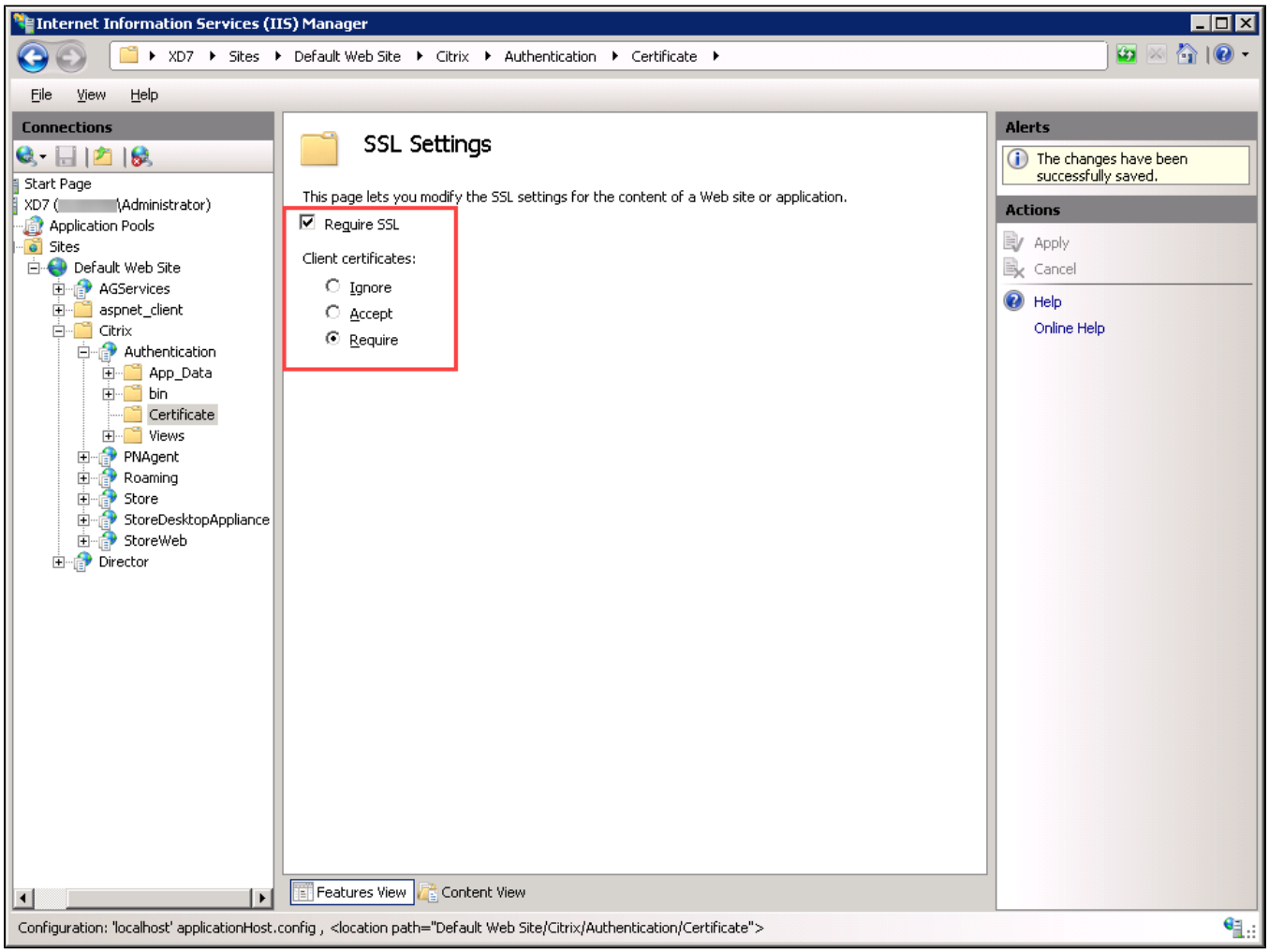
6) Убедитесь в том, что метод добавлен.



7) Выберите пункт: Default Web Site Citrix → Authentication → Certificate.



8) Установите галочку **Require SSL** и переключатель **Require**.



Чтобы проверить корректность настроек SSL-соединение:

1) Подключитесь к компьютеру пользователя.

2) Подключите смарт-карту с сертификатом.

3) Откройте браузер.

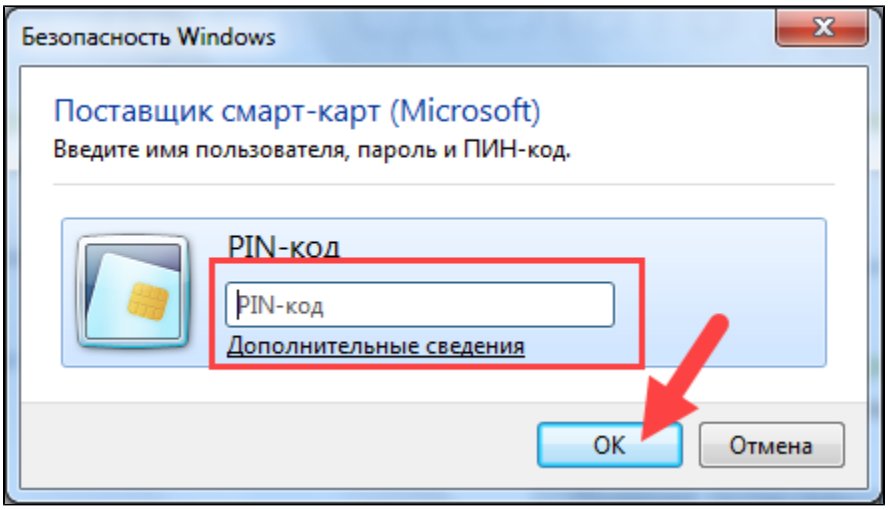
4) В адресной строке введите:

https://xd7.aktiv.local/Citrix/Authentication/Certificate/test.aspx

Вместо xd7.aktiv.local введите полное доменное имя сервера. В браузере отобразится окно для выбора сертификата пользователя.

5) Выберите необходимый сертификат и нажмите **OK**.

6) Введите PIN-код смарт-карты и нажмите **OK**.



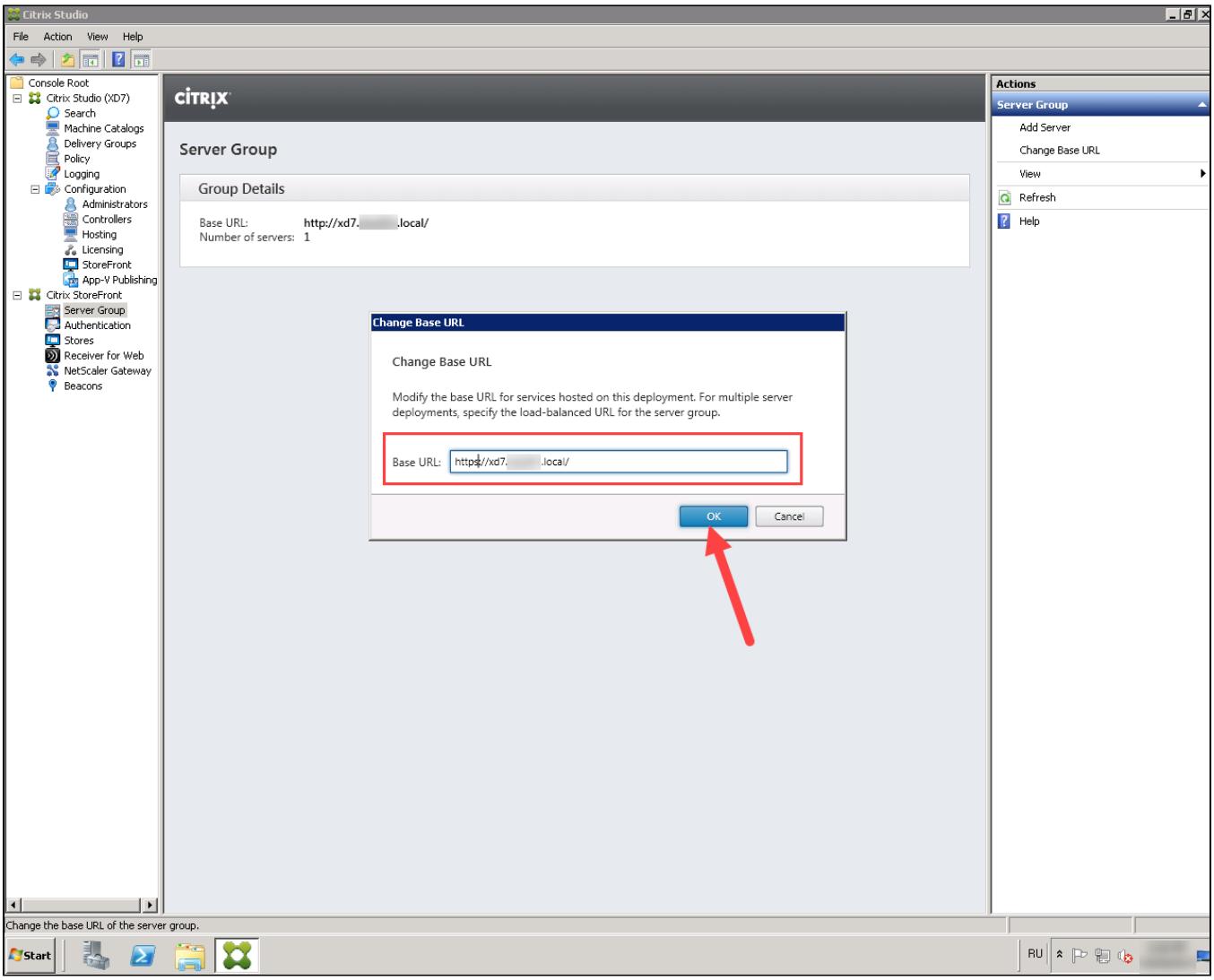
7) Если SSL-соединение настроено корректно, то в браузере отобразится информация о сертификате пользователя.

Чтобы настроить протоколы связи для SSL-соединения:

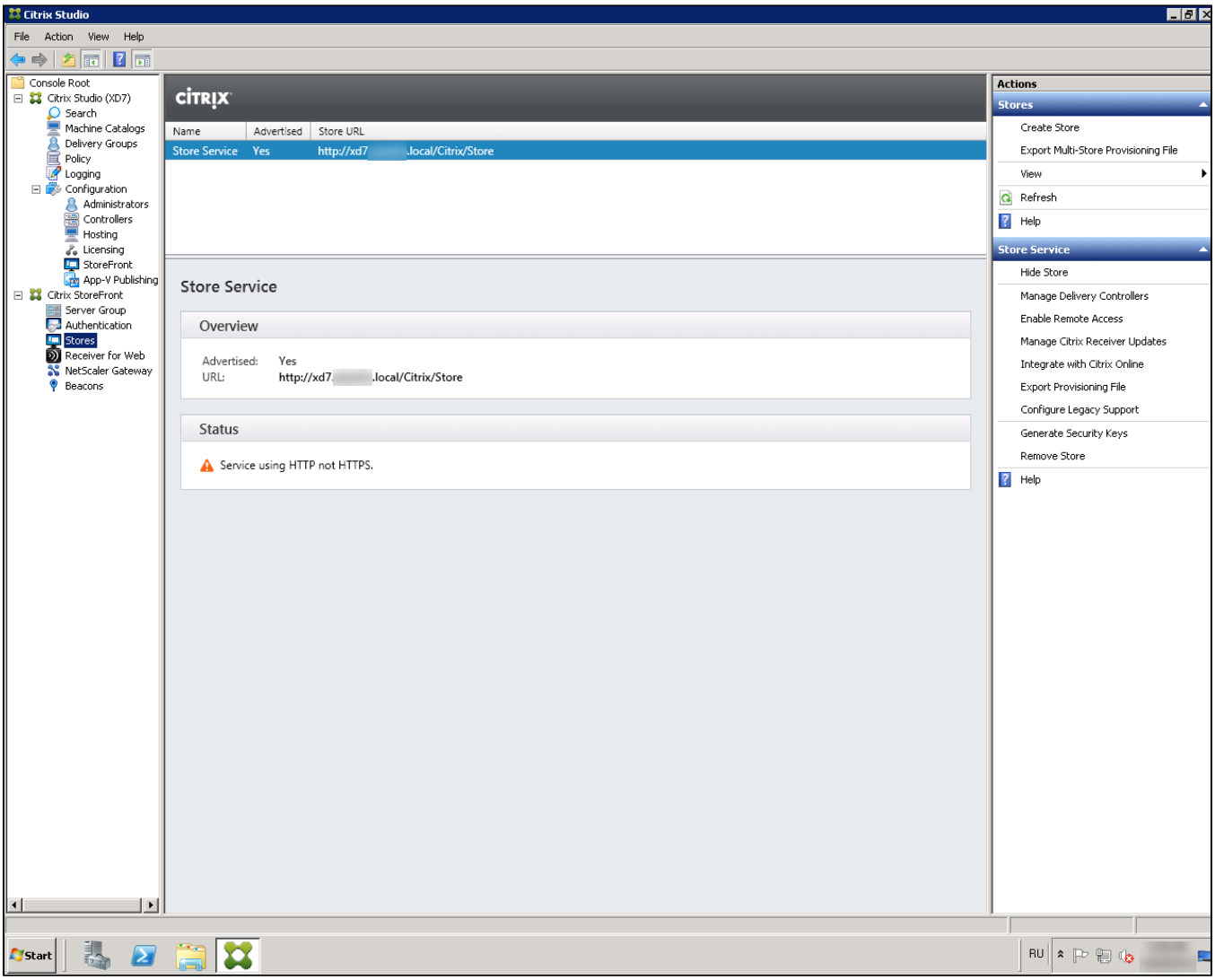
1) На сервере запустите **Citrix** и выберите пункт **Server Group.**

2) Нажмите **Change Base URL** и измените **http** на **https.**

3) Нажмите **OK.**



4) Выберите пункт **Stores.**



5) Щелкните по названию пункта**Manage Delivery Controllers**.

6) В открывшемся окне нажмите **Edit**.

7) В раскрывающемся списке **Transport type** выберите **HTTPS**.

8) Нажмите **OK**.

9) Проверьте, что в поле Status отображается значение **Service using HTTPS**.

10) Перезагрузите сервер.

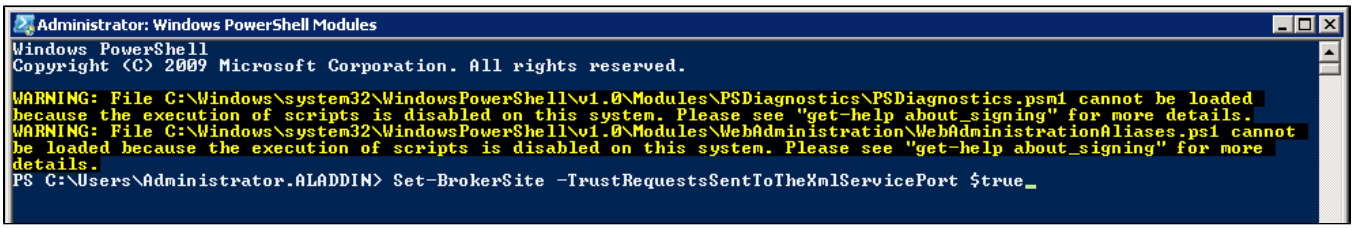
Настройка XML-запросов

Для настройки XML-запросов:

1) На сервере откройте командную строку **Windows PowerShell**.

2) Введите команду:

Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true



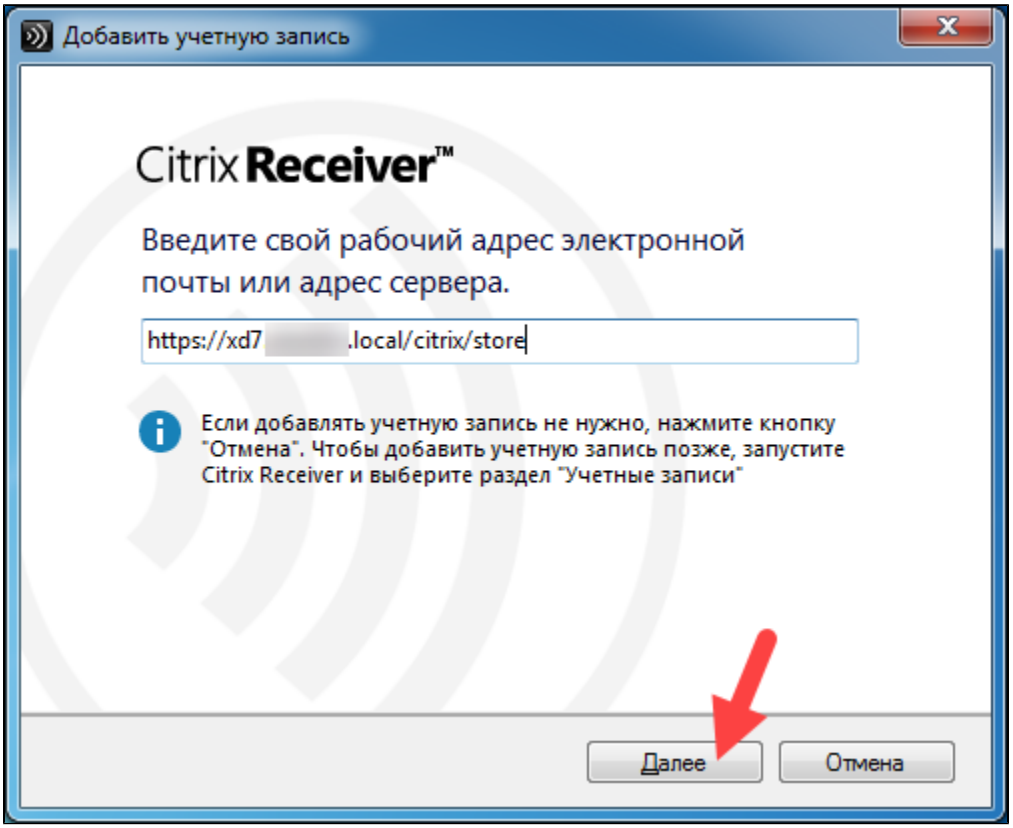
Настройка компьютера пользователя

Чтобы настроить компьютер:

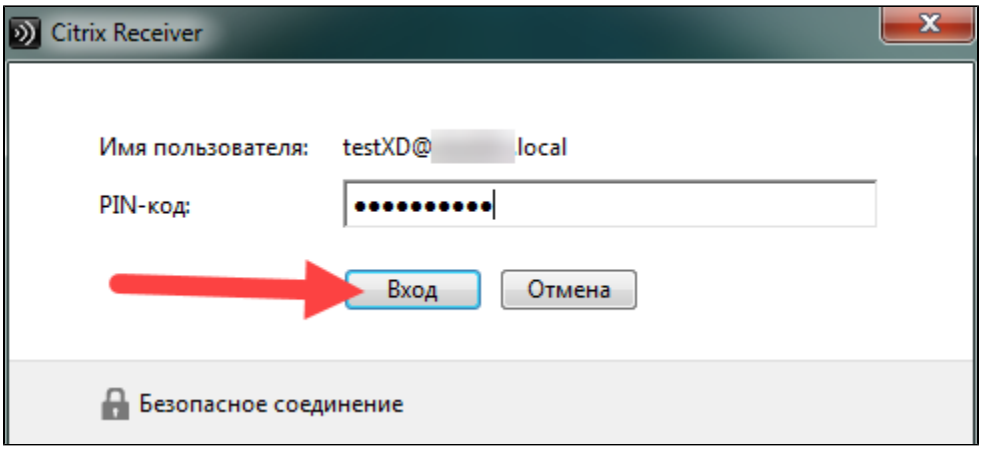
1) Подключитесь к компьютеру пользователя.

2) Откройте **Citrix Receiver**.

3) Введите строку для подключения к серверу и нажмите **Далее**.

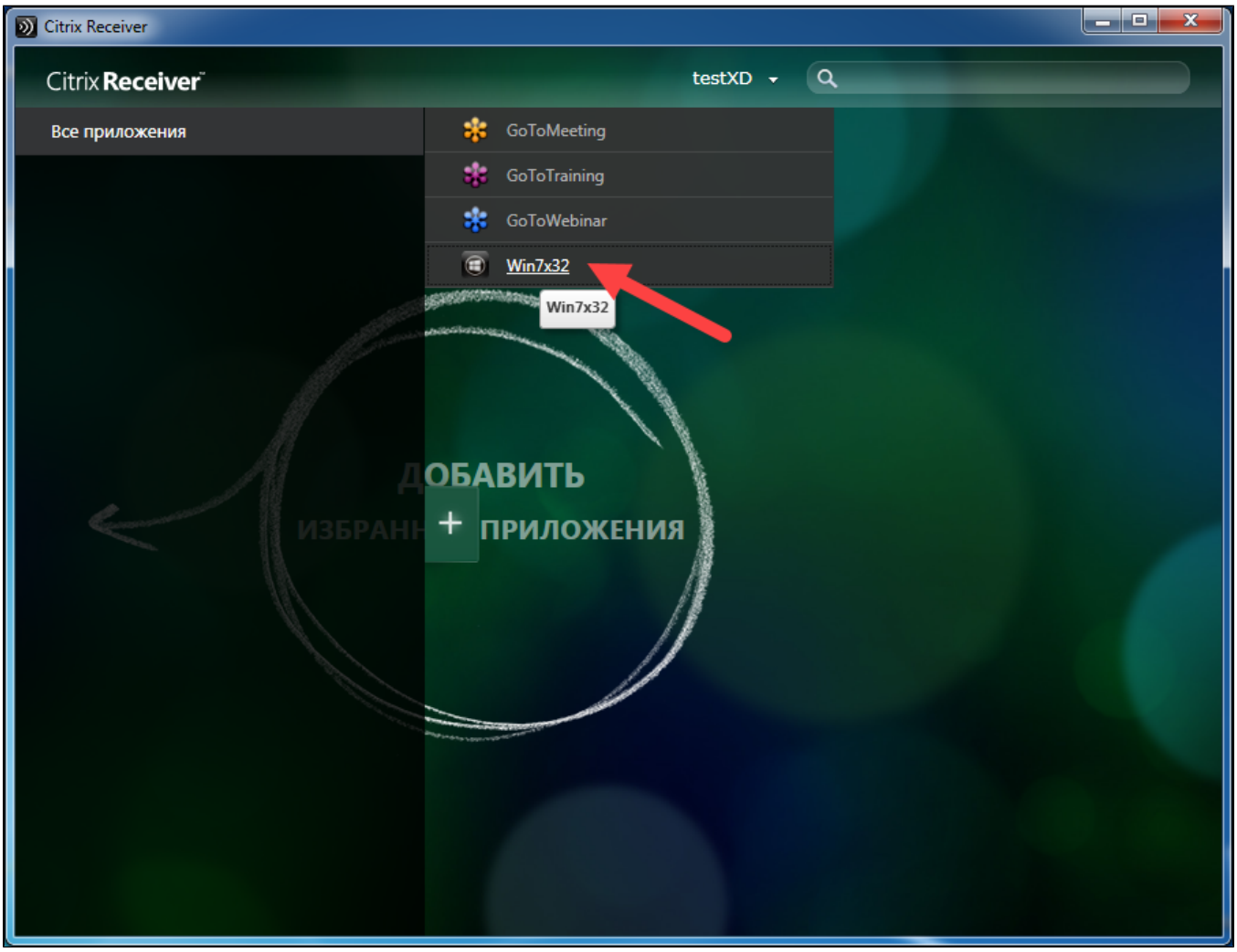


4) Введите PIN-код Рутокена.



5) Подключитесь к серверу приложений. Дождитесь окончания процесса подключения.

6) Перейдите на вкладку **Все приложения** и выберите **Win7x32**.



7) Введите PIN-код Рутокена.

8) Если аутентификация прошла успешно, то все настройки компьютера выполнены корректно.

Настройка сквозной аутентификации по смарт-карте

Порядок настройки Single Sing-On при аутентификации по смарт-карте при использовании XenDesktop 7

Для корректной работы сквозной аутентификации по смарт-картам необходимо, чтобы компьютер пользователя был добавлено в домен или, при использовании нескольких доменов, между доменами были настроены доверительные отношения.

Этапы настройки Single Sign-on (SSO) для аутентификации по смарт-карте:

1) Создание каталога виртуальных машин.

2) Создание группы пользователей виртуальных машин.

3) Установка Citrix Receiver на компьютер пользователя.

4) Настройка политик аутентификации для Citrix XenDesktop.

5) Выпуск сертификата для IIS и настройка SSL доступа к IIS.

6) Настройка XML-запросов к серверу.

7) Настройка Citrix StoreFront для включения SSO при аутентификации по смарт-картам.

8) Настройка компьютера пользователя.

Установка и настройка Citrix Receiver для включения SSO при аутентификации по смарт-картам

Для настройки сквозной аутентификации по смарт-картам на Citrix Receiver необходимо выполнить установку Citrix Receiver с дополнительными параметрами.

Установка Citrix Receiver выполняется из командной строки:

1) На компьютере пользователя запустите утилиту командной строки CMD с правами администратора.

2) В командной строке укажите путь к файлу установщика Citrix Receiver и дополнительно укажите параметры для включения SSO:

/includeSSON AM_SMARTCARDPINENTRY=CSP

Пример: C:\Distr\CitrixReceiver.exe /includeSSON AM_SMARTCARDPINENTRY=CSP

3) Дождитесь окончания процесса установки Citrix Receiver.

4) Перезагрузите компьютер пользователя.

5) После перезагрузки компьютера пользователя проверьте, что в исполняемых процессах (Task Manager/Processes) присутствует процесс ssonsrv.exe.

6) Выполните настройку политик аутентификации для Citrix XenDesktop, которые будут применяться на серверы Citrix и устройствах пользователей.

Подробную информацию для настройки аутентификации по смарт-картам можно найти на странице: http://support.citrix.com/proddocs/topic/receiver-windows-40/receiver-windows-smart-card-cfg.html.

Настройка политик аутентификации для ПО Citrix XenDesktop

Настройку политик рекомендуется выполнять через групповые политики службы каталога Active Directory. Также настройку можно осуществить из оснастки управления локальными политиками.

Для настройки групповых политик:

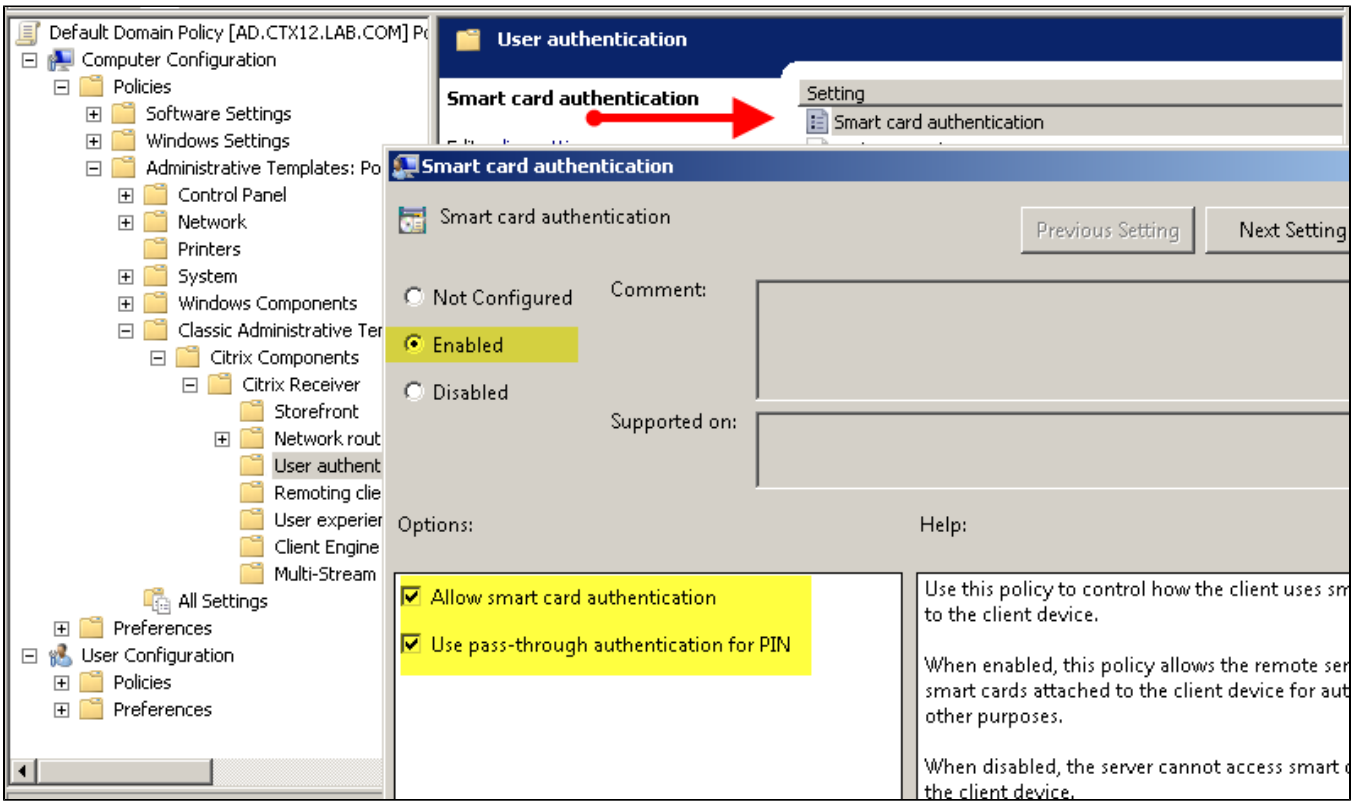
1) В шаблоны групповых политик службы каталога Active Directory импортируйте шаблон политик Citrix ADM Template (**Add Template** в оснастке управления групповыми политиками). Шаблон политик расположен:

C:\Program Files (x86)\Citrix\ICA Client\Configuration\icaclient.adm

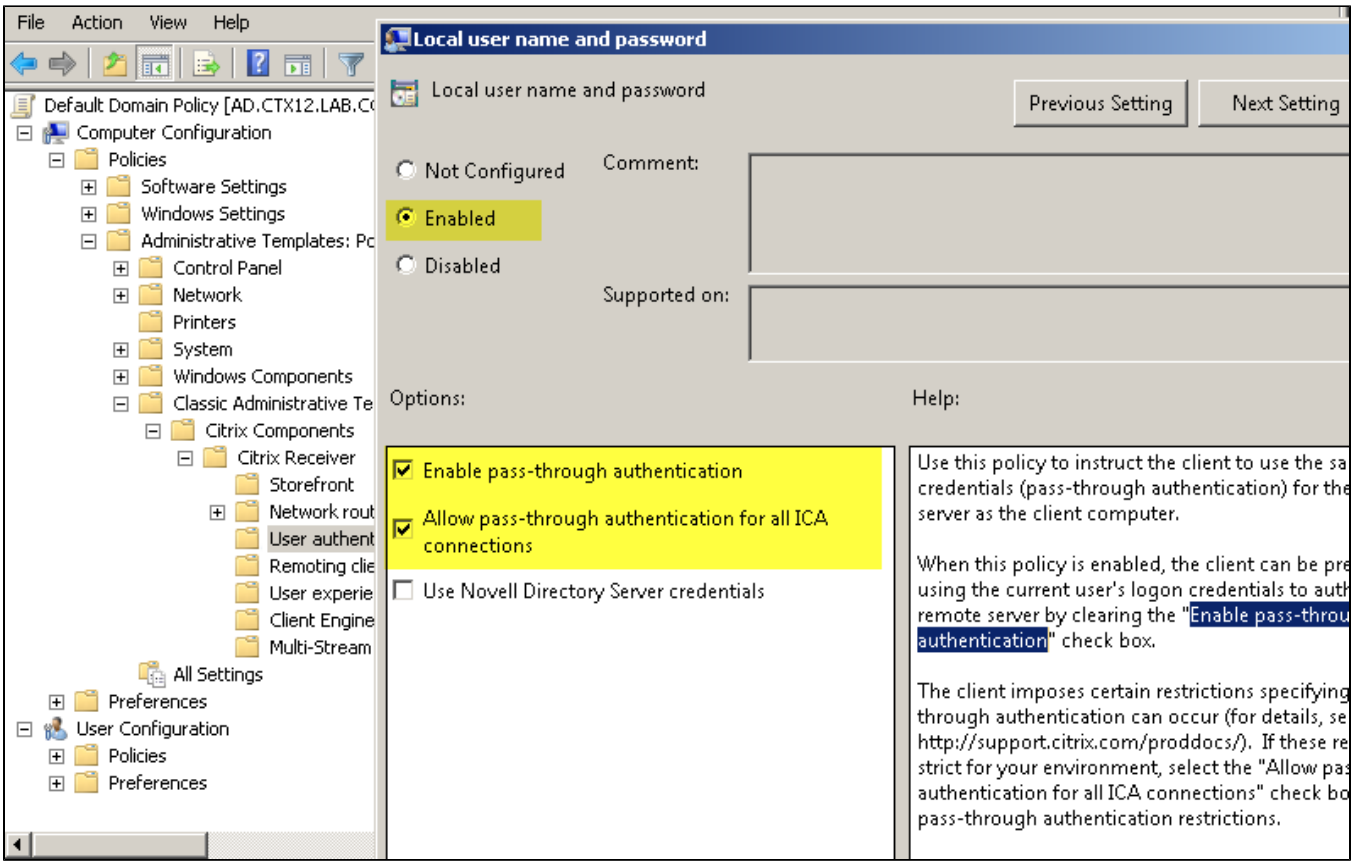
2) Создайте политику (или отредактируйте имеющуюся) и включите сквозную аутентификацию по смарт-картам.

3) Откройте раздел Computer Configuration → Policies → Administrative templates → Classic → Citrix Components → Citrix receiver → User Authentica-tion.

4) Выберите настройку **Smart Card Authentication** и установите галочки **Allow smart card authentication** и **Use pass-through authentication for PIN**.



5) Выберите настройку **Local User Name and Password** и установите галочки **Enable pass-through authentication** и **Allow pass-through authentication for all ICA connections**.



Подробная информация доступна на странице: http://support.citrix.com/proddocs/topic/ica-settings/ica-settings-wrapper.html

Настройка ПО Citrix StoreFront 2.1 для включения сквозной аутентификации по смарт-картам

При работе с Citrix StoreFront в многосерверных установках используйте только один сервер при внесении изменений в настройки.

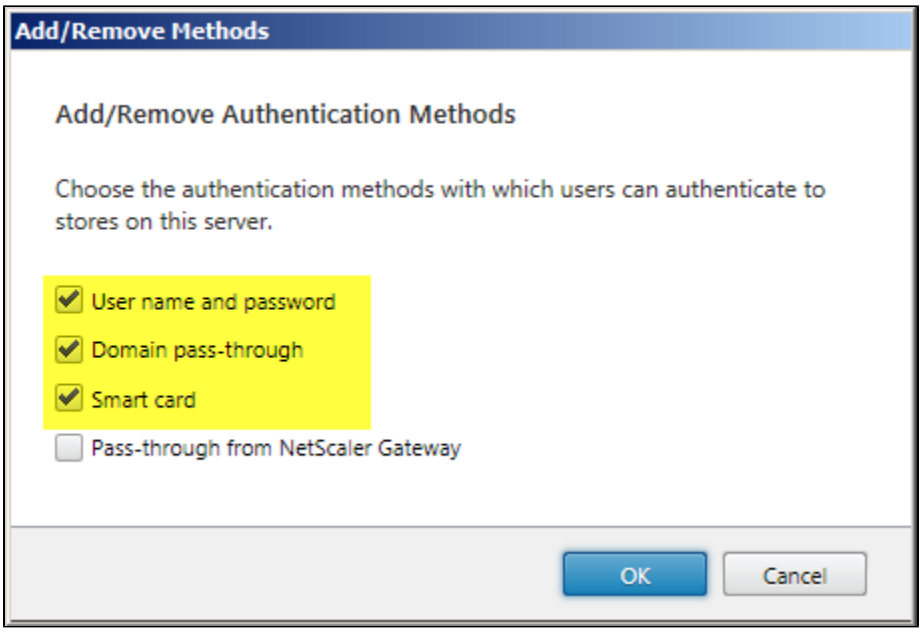
Убедитесь в том, что консоль управления Citrix StoreFront не выполняется на другом сервере данной серверной группы.

После завершения конфигурирования убедитесь в том, что изменения применились для всех серверов группы (propagate your configuration changes to the server group).

Для настройки Citrix StoreFront для работы SSO при аутентификации по смарт-картам:

1) Выполните первоначальную настройку Citrix StoreFront.

2) В разделе **Add/Remove Authentication Methods** установите переключатель **Domain pass-through**.



3) Для включения сквозной аутентификации с использованием смарт-карт необходимо внести дополнительные изменения в конфигурацию. Для этого отредактируйте **default.ica** для каждого Citrix Store, где требуется сквозная аутентификация по смарт-картам.

4) Используя текстовый редактор, откройте файл **default.ica**, который находится в папке:
C:\inetpub\wwwroot\Citrix\storename\App_Data

5) Если в инфраструктуре не используется аутентификация через NetScaler Gateway, то добавьте следующий параметры:
[Application]: DisableCtrlAltDel=Off.
Данная настройка будет применяться для всех пользователей.

6) Для включения сквозной аутентификации по смарт-картам с использованием NetScaler Gateway добавьте следующий параметр:
[Application]: UseLocalUserAndPassword=On

Подробная информация доступна на странице: http://support.citrix.com/proddocs/topic/dws-storefront-21/dws-configure-conf-smartcard.html.

7) Выполните настройку пользователя, согласно разделу.

8) Проверьте, что вход на виртуальную машину пользователя выполняется успешно.

9) Проверьте, что после входа на компьютер пользователя (по смарт-карте или по паролю) больше не появляется окно запроса учётных данных или PIN-кода при доступе к StoreFront и виртуальной машине пользователя.