Настройка аутентификации в Citrix XenDesktop 7.x с использованием смарт-карт JaCarta PKI

Краткое руководство

Аннотация

Настоящий документ представляет собой сведения о настройке двухфакторной аутентификации с использованием смарт-карт JaCarta PKI в виртуальной среде Citrix XenDesktop версии 7.x.

За технической поддержкой обращайтесь на веб-сайт ЗАО «Аладдин Р. Д.» по адресу http://www.aladdin-rd.ru/support/index.php.

Версия	1.4
Листов	45

Телефон +7 (495) 223-00-01 • Факс +7 (495) 646-64-40 • aladdin@aladdin-rd.ru • www.aladdin-rd.ru

Содержание

Краткое описание инфраструктуры демо-стенда

- Microsoft Windows Server 2008 R2 – сервер с ролью контроллер домена (DC.aladdin.local).
- Microsoft Windows Server 2008 R2 – сервер с ролью центр сертификации Microsoft Certification Authority (MS CA) (CA.aladdin.local):
  - JC Client 6.24.16.
- Microsoft Windows Server 2008 R2 – компоненты программного обеспечения (ПО) XenDesktop (Citrix Director, Citrix License Server, Citrix Studio, Citrix StoreFront, Citrix Delivery Controller) (XD7.aladdin.local). Данные компоненты могут быть установлены на разных серверах.
  - ПО Citrix XenDesktop 7.0.
- Microsoft Windows 7 64-bit – тестовый ПК пользователя (Test2.aladdin.local):
  - Citrix Receiver 4.0.0.45893;
  - JC Client 6.24.16.
- Microsoft Windows 7 32-bit – тестовая эталонная машина – «золотой» образ, с которого будут развернуты виртуальные машины для пользователей (win7x32.aladdin.local):
  - Citrix Receiver 4.0.0.45893;
  - JC Client 6.24.16;
  - Virtual Delivery Agent.

1. Создание виртуальных машин

1.1. Создание каталога виртуальных машин

Перед созданием каталога для виртуальных машин необходимо подготовить эталонную машину. В данном тестовом окружение – это виртуальная машина с операционной системой (ОС) Windows 7 (32-bit).

Для подготовки эталонной машины на неё необходимо установить ПО Virtual Delivery Agent (дистрибутив, которого расположен на диске с ПО XenDesktop 7.0), JC Client 6.24.16[1], а также другое ПО, которое необходимы для работы пользователей данной группы. После установки виртуальную машину необходимо выключить.

Создание каталога для виртуальных машин

На сервере, где установлен компонент **Citrix Studio**[2], запустите **Citrix Studio** (Start -> All Programs -> Citrix), подключитесь к Citrix Delivery Controller и перейдите в **Machine Catalogs,** запустите мастер создания каталога **Create Machine Catalog** (рис. 1).

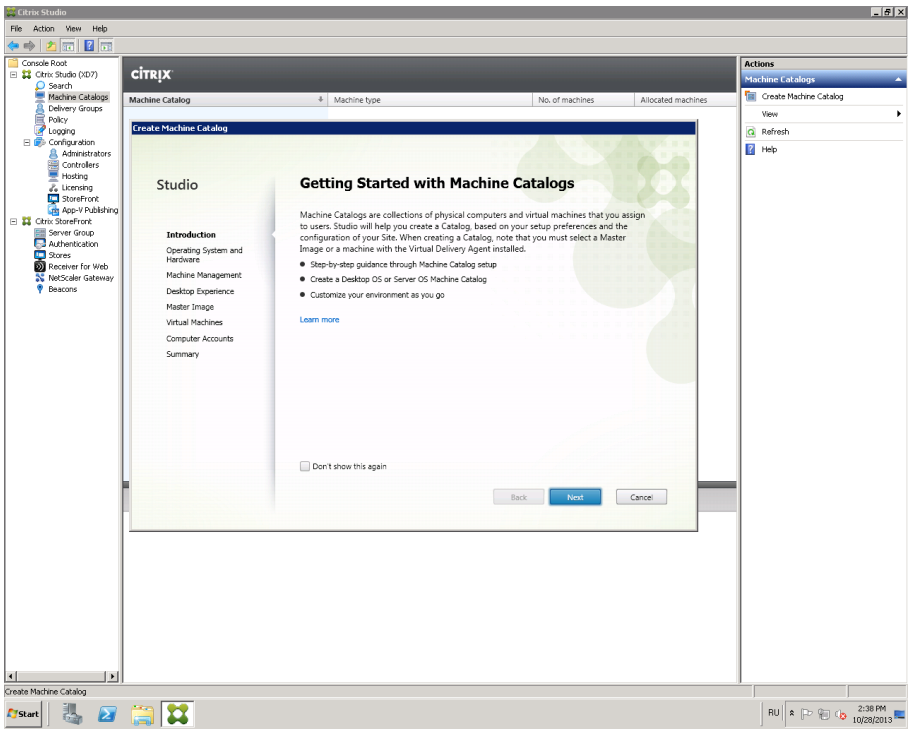

Рис. 1 — Окно «Create Machine Catalog»

Нажмите **Next.**

[1] Установка и настройка ПО JC Client 6.24.16 описана в документе «JC-Client — Руководство администратора».
[2] Установка и настройка ПО Citrix XenDesktop 7.x описана на сайте
http://support.citrix.com/proddocs/topic/xendesktop-71/cds-install-config-intro.html

Выберите пункт **Windows Desktop OS или другой пункт в зависимости от настроек вашей среды** (рис. 2).

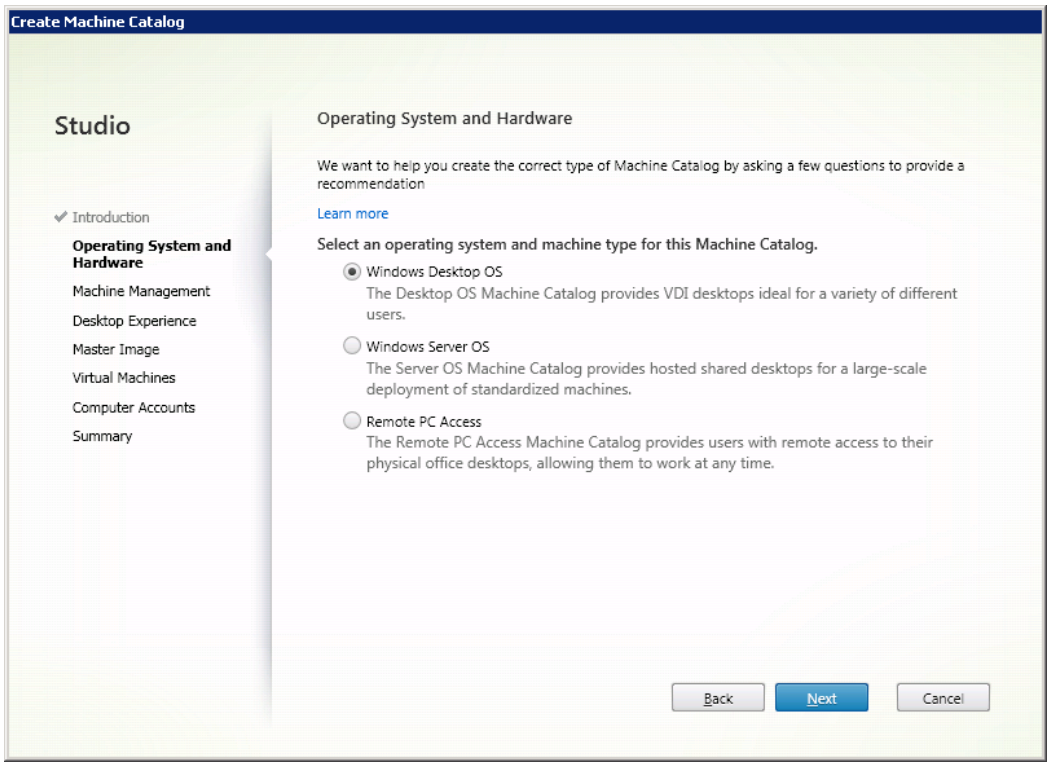

Рис. 2 — Окно выбора операционной системы для каталога

Нажмите **Next.**

Выберите пункт **Virtual machines** и **Machine Creation Services (MCS)** (рис. 3).

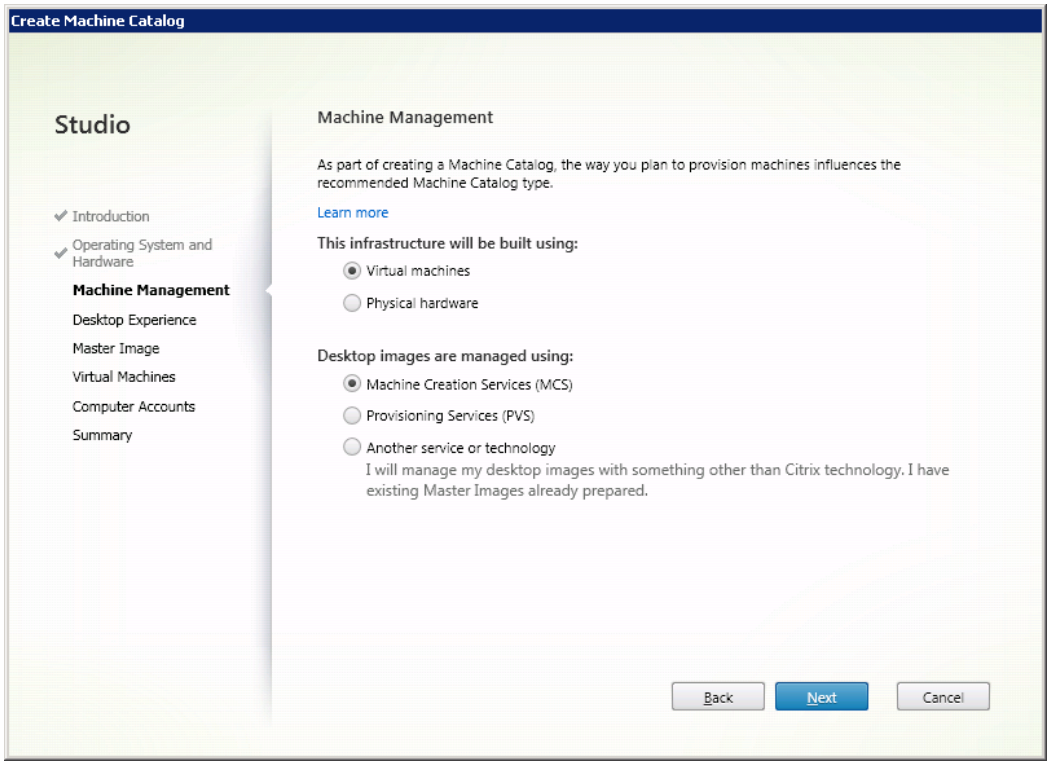

Рис. 3 — Окно выбора способа доставки виртуальной машины

Нажмите **Next.**

В окне **Desktop Experience** настройте параметры рабочих столов для пользователей и способ хранения пользовательских данных, так как показано ниже (рис. 4). Могут быть выбраны другие параметры в зависимости от настроек вашей среды и требуемых задач.

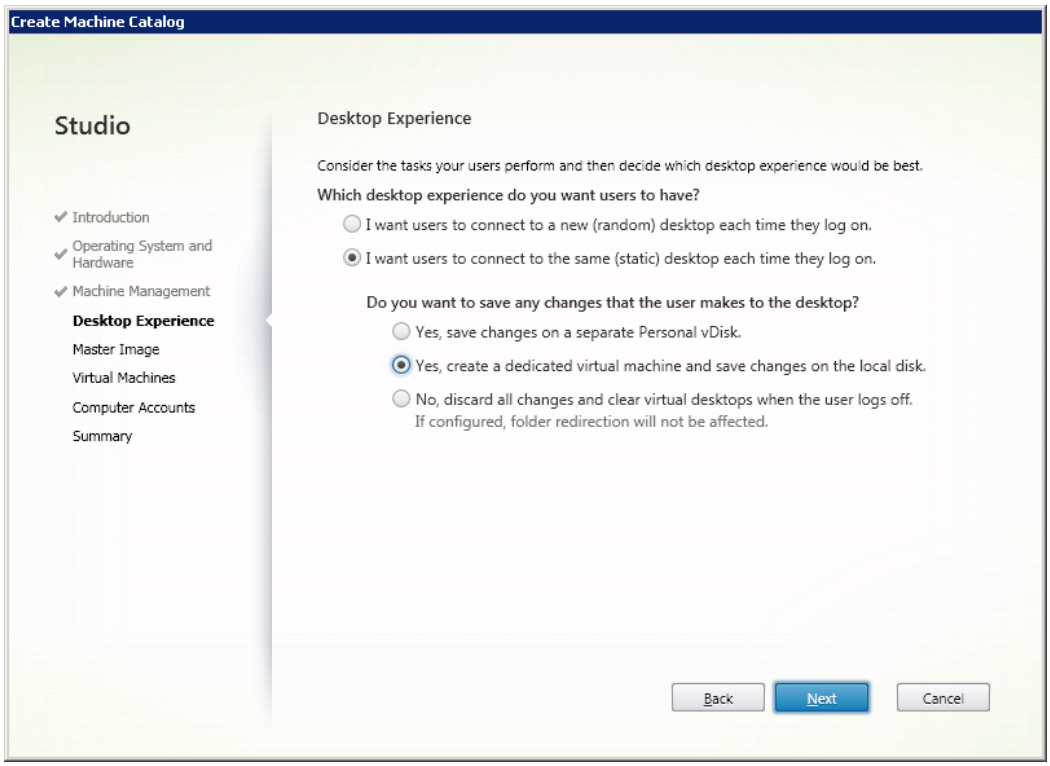

Рис. 4 — Окно настроек параметров виртуальной машины

Нажмите **Next.**

Из списка доступных виртуальных машин выберите ранее созданную эталонную машину (рис. 5).

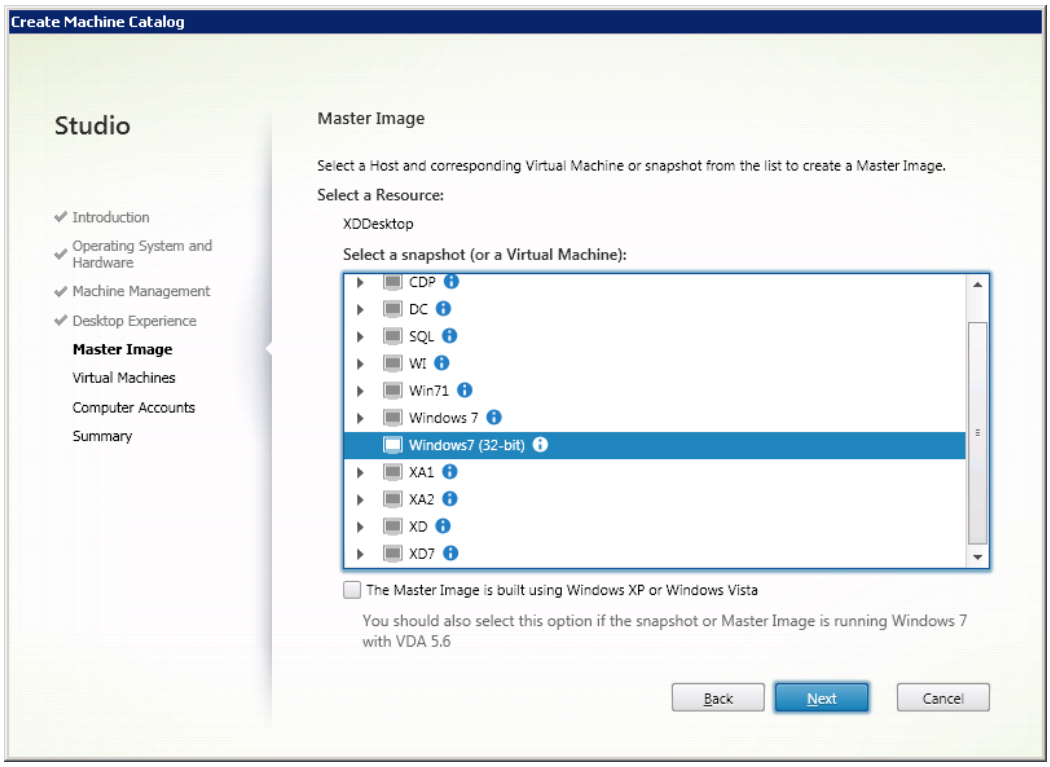

Рис. 5 — Окно выбора эталонной машины

Нажмите **Next.**

Задайте количество виртуальных машин в каталоге и задайте их технические характеристики (рис. 6).

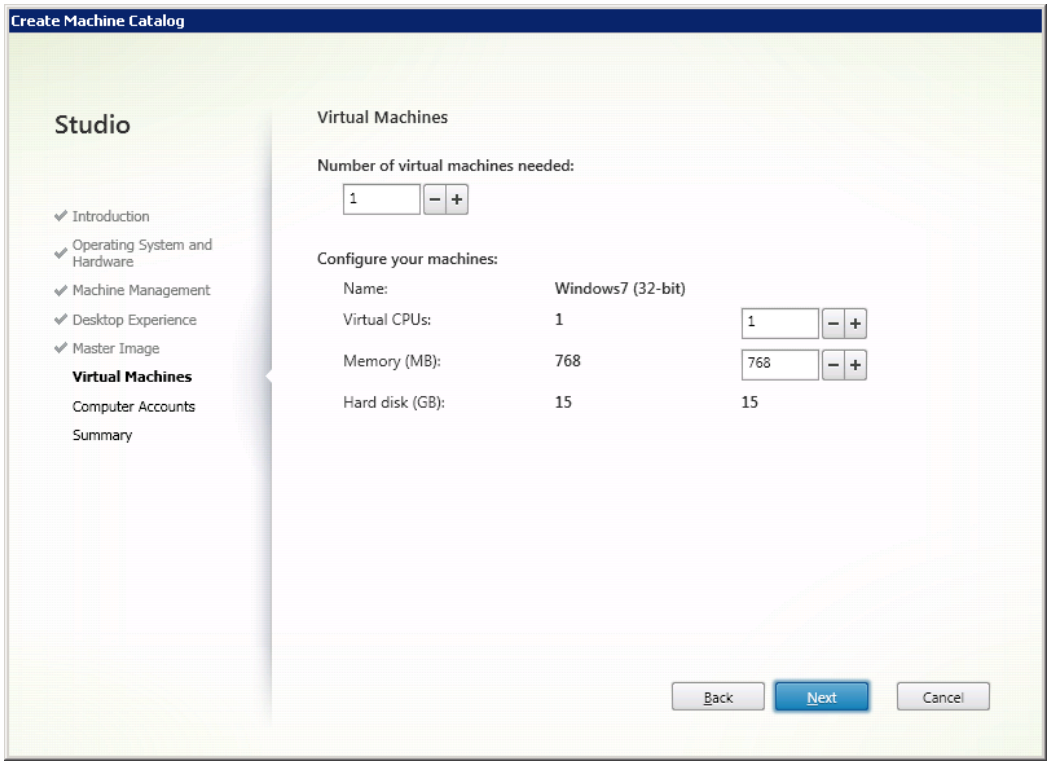

Рис. 6 — Выбор параметров виртуальных машин пользователей

Нажмите **Next.**

Настрайте схему для автоматического добавления учетных записей созданных машин в службу каталогов **Active Directory (AD)** (рис. 7).

Для простоты администрирования можно предварительно создать организационный модуль (OU) в службе каталогов **AD,** куда будут добавлены учетные записи создаваемых виртуальных машин.

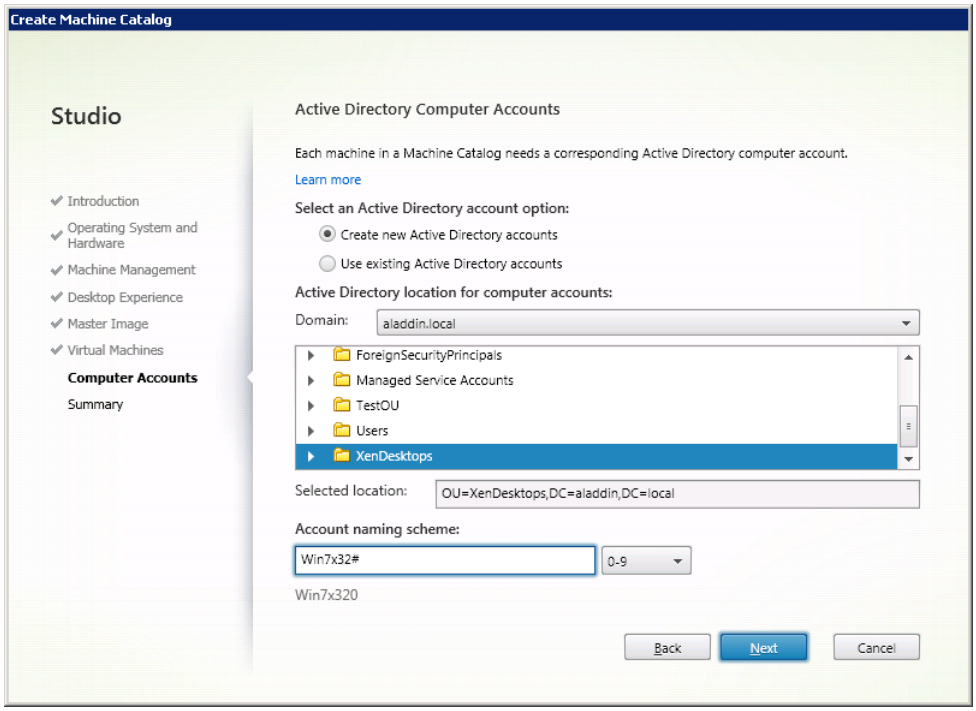

Рис. 7 — Окно «Active Directory Computer Account»

Нажмите **Next.**

Проверьте параметры создаваемых виртуальных машин и определите имя для каталога, а также имя виртуальной машины для отображения у пользователей (рис. 8).

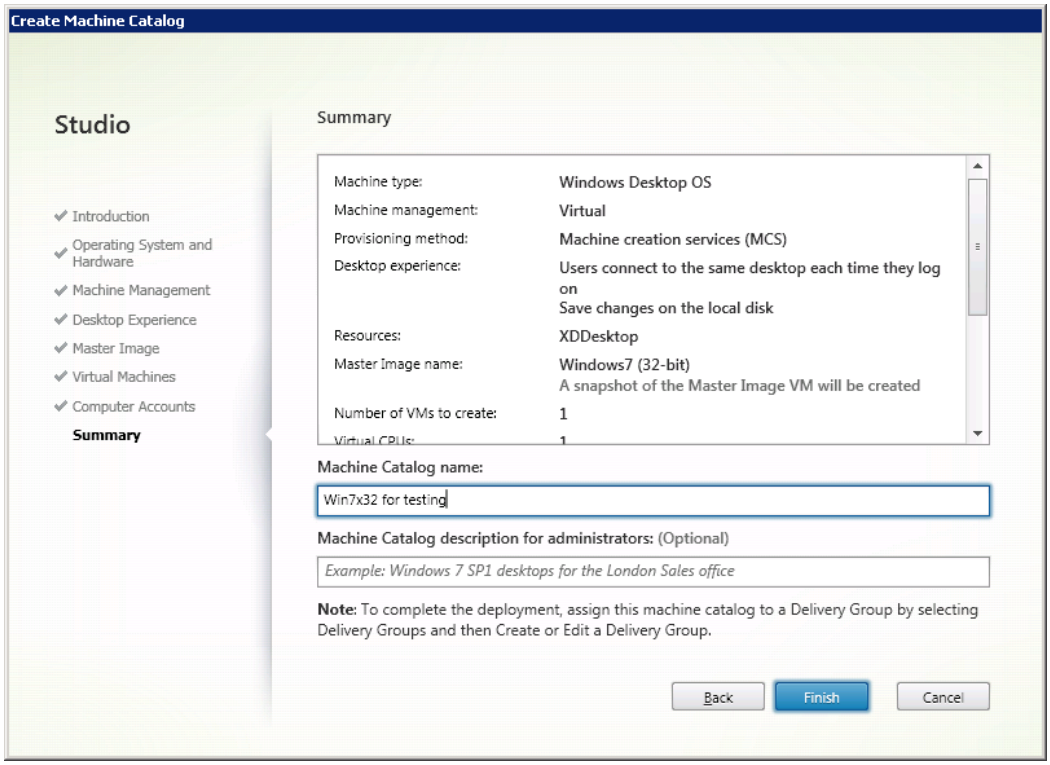

Рис. 8 — Окно «Summary»

Нажмите **Finish.**

Каталог виртуальных машин создан (рис. 9).

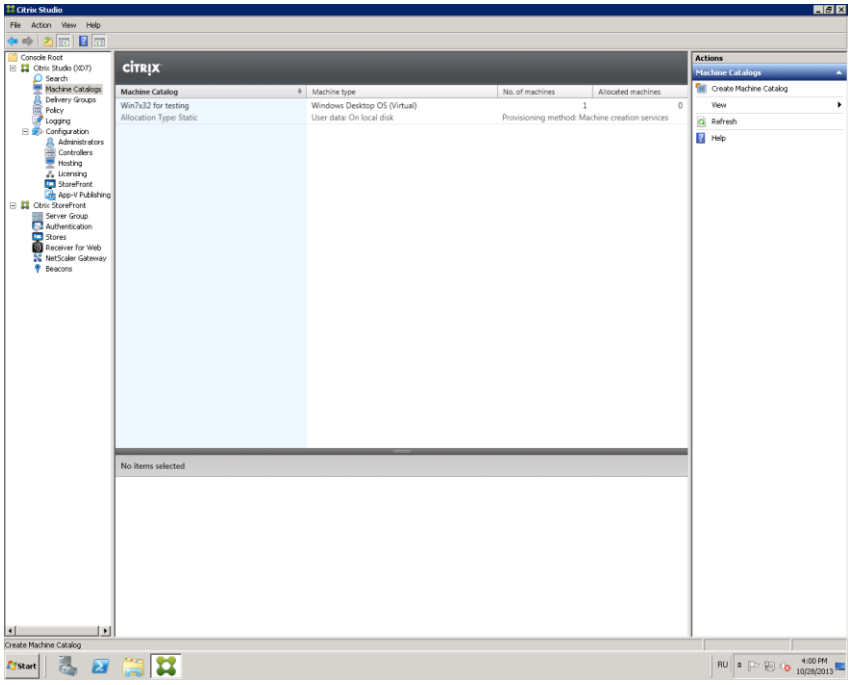

Рис. 9 — Созданный каталог виртуальных машин

1.2. Создание группы пользователей виртуальных машин - Delivery Group

Для связи созданных виртуальных машин с пользователями, необходимо настроить группу пользователей виртуальных машин (**Delivery Group).**

Откройте консоль управления **Citrix Studio** и перейдите во вкладку **Delivery Group** -> **Create Delivery Group** (рис. 10).

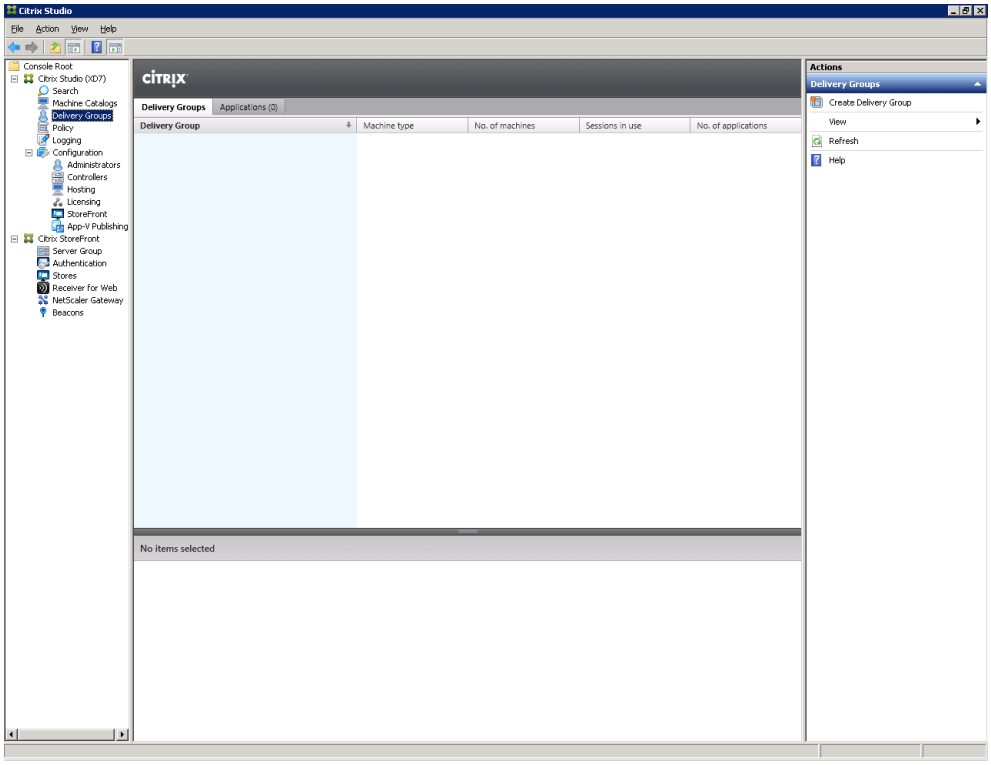

Рис. 10 — Окно «Delivery Group»

Выберите ранее созданный каталог виртуальных машин и укажите сколько виртуальных машин будет доступно для пользователей этой группы (рис. 11).

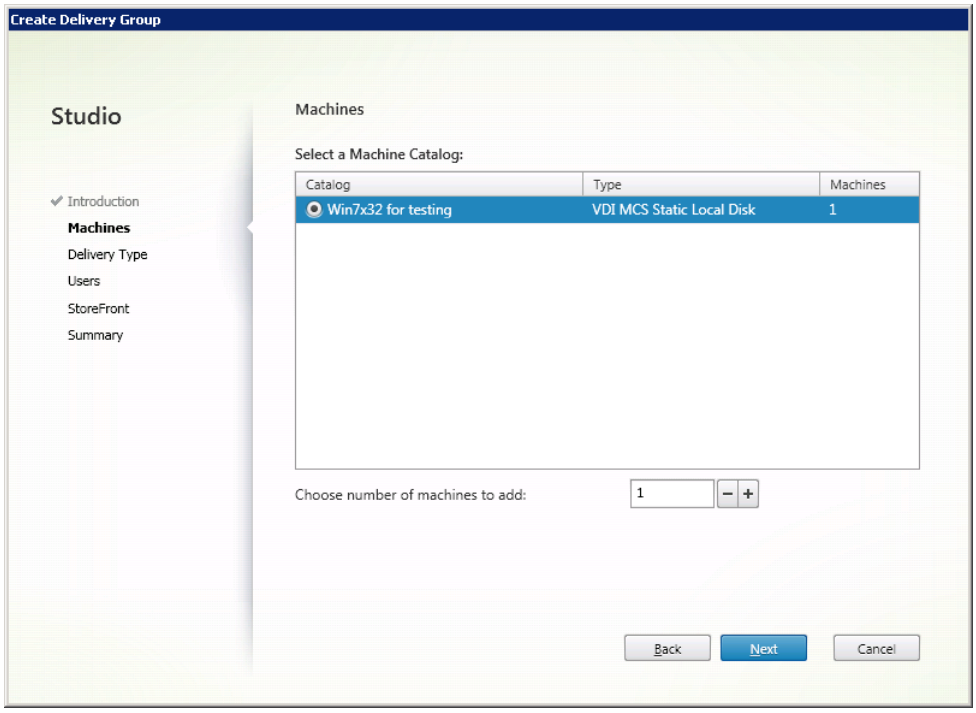

Рис. 11 — Окно «Machines»

Нажмите **Next.**

Выберите тип доставляемых ресурсов: приложения или виртуальные машины (рис. 12).

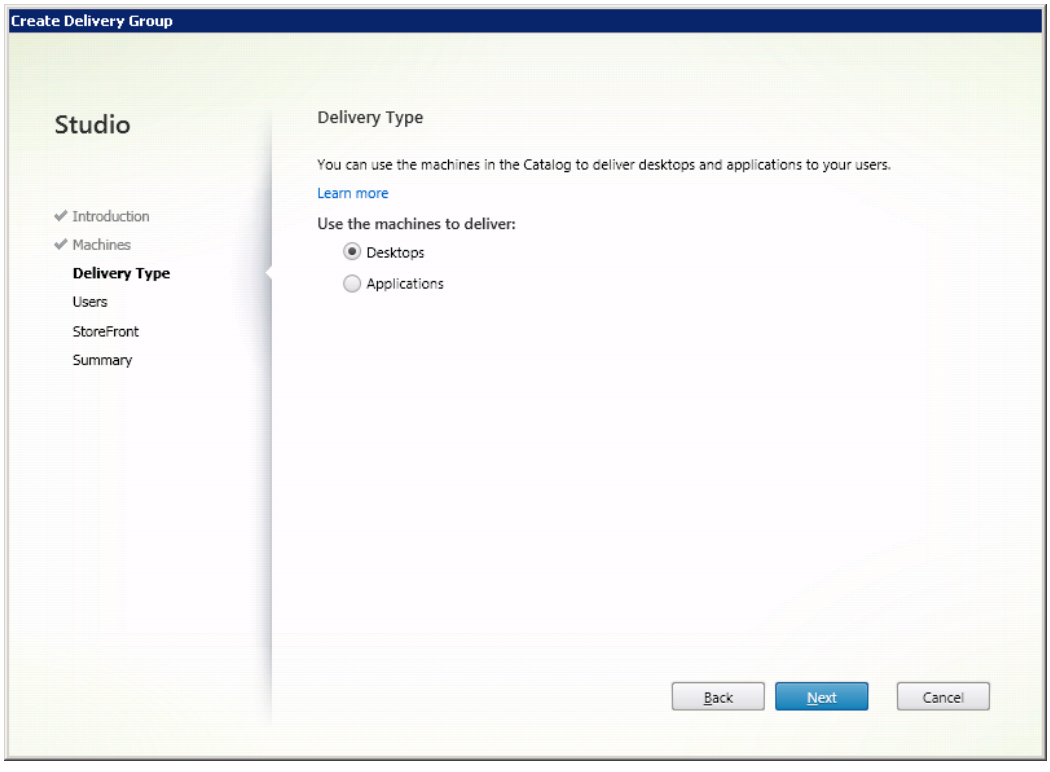

Рис. 12 — Выбор «Delivery Type»

Нажмите **Next.**

Назначьте пользователей, с которыми будут связаны виртуальные машины (рис. 13).

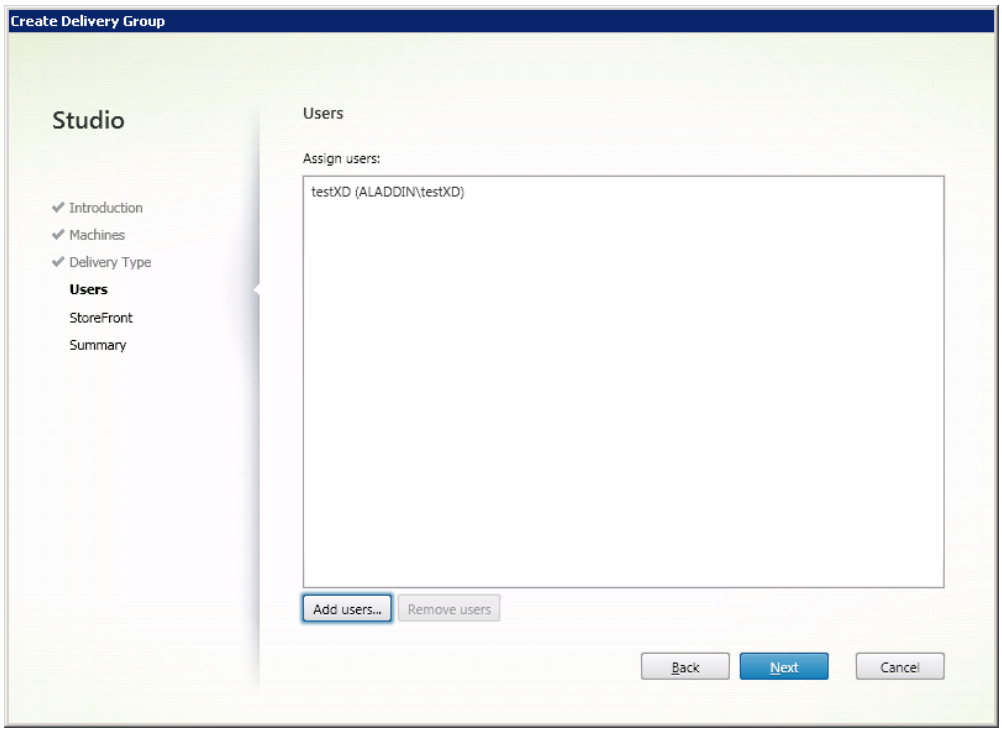

Рис. 13 — Окно выбора пользователей

Нажмите **Next.**

ПО **Citrix Receiver** настраивается позднее (см. раздел 2.5).

В следующем окне выберите пункт **Manually, using a StoreFront server address that I will provide later** (рис. 14).

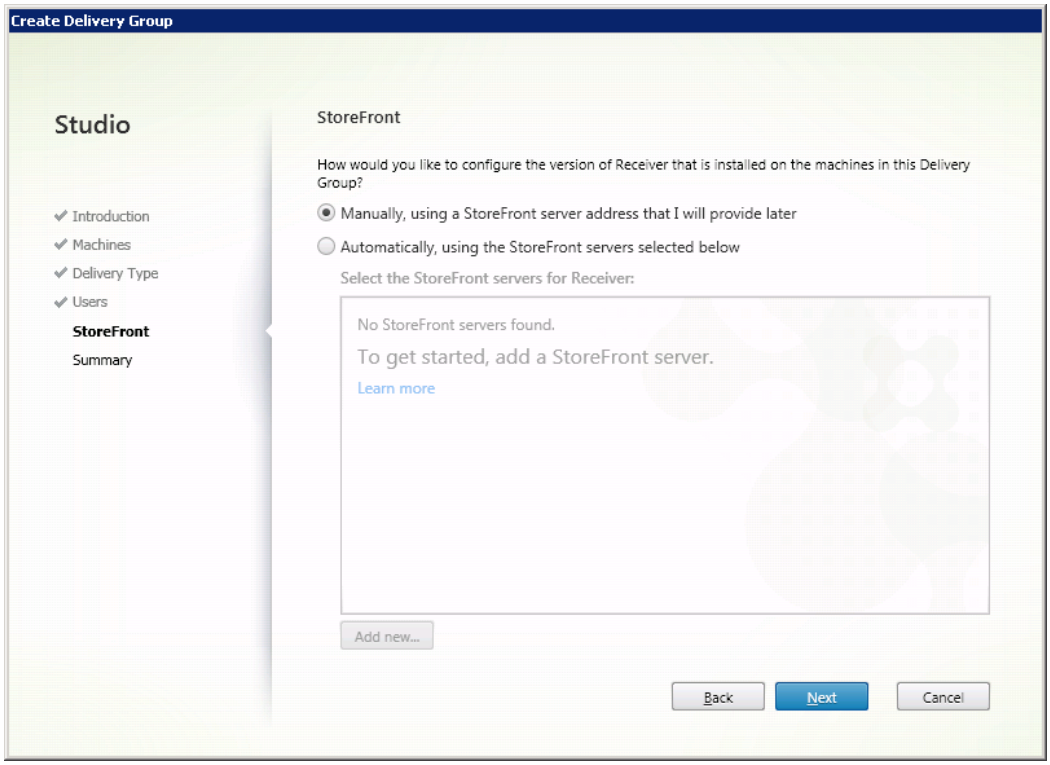

Рис. 14 — Окно настройки «Citrix StoreFront»

Нажмите **Next.**

Проверьте итоговые настройки и определите название группы (рис. 15).

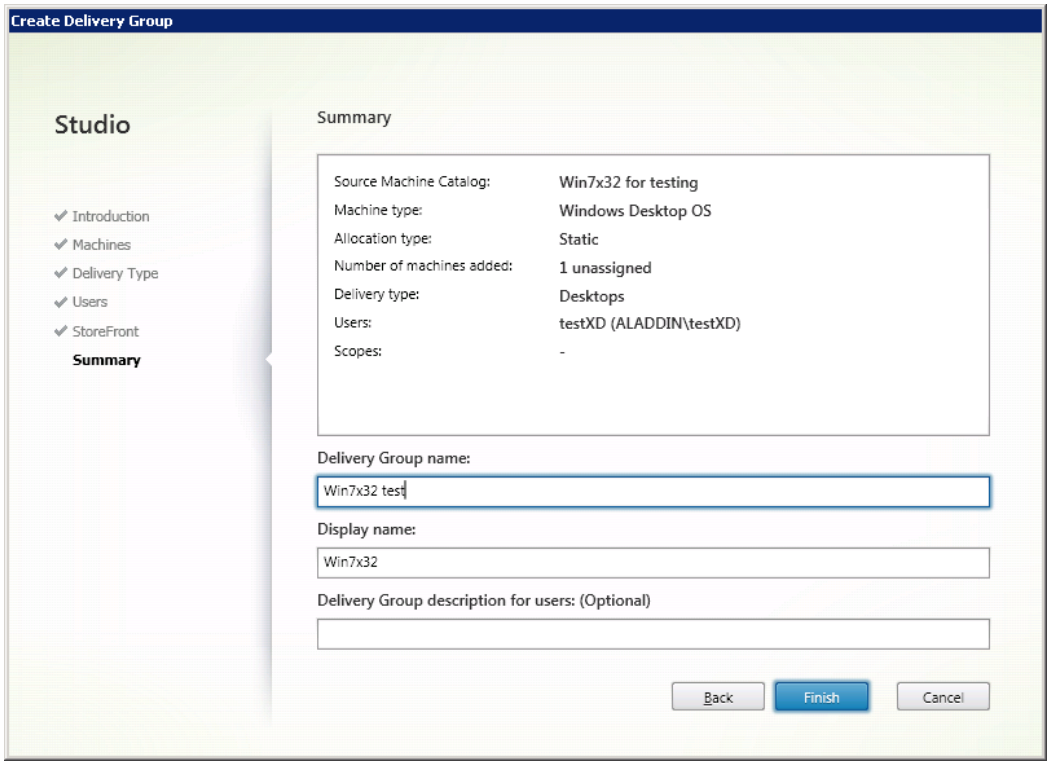

Рис. 15 — Окно «Summary»

Нажмите **Finish.**

Группа пользователей виртуальных машин создана (рис. 16).

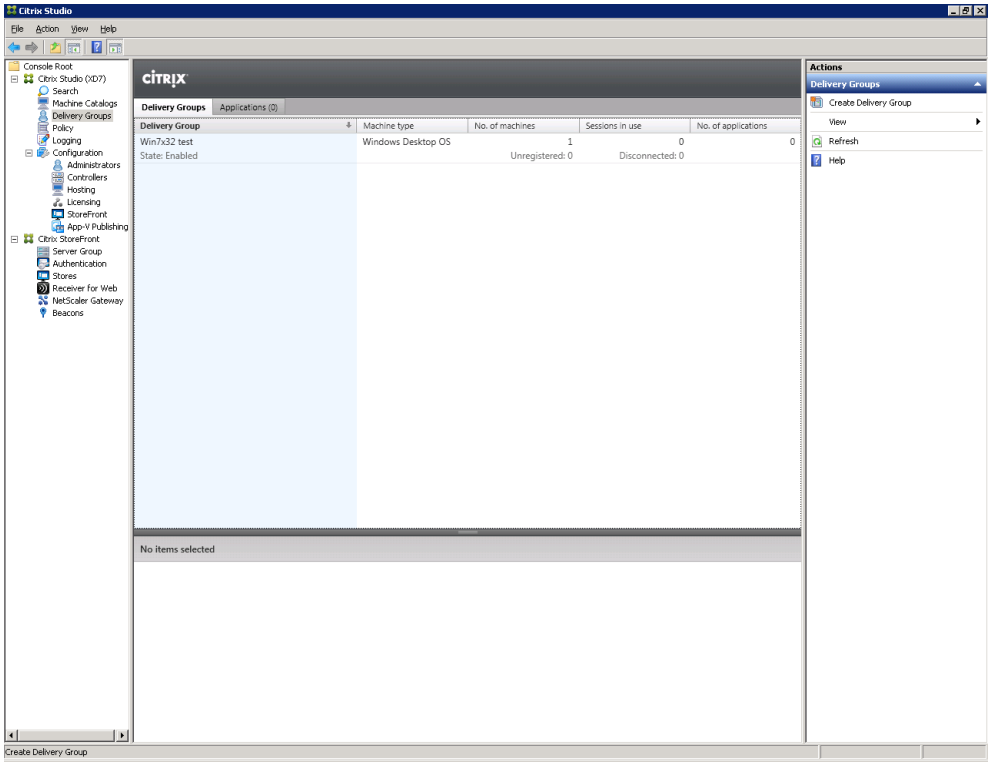

Рис. 16 — Созданная «Delivery Group»

Внимание: Убедитесь, что все виртуальные машины в пуле зарегистрированы (имеют статус Registered (рис. 17)).

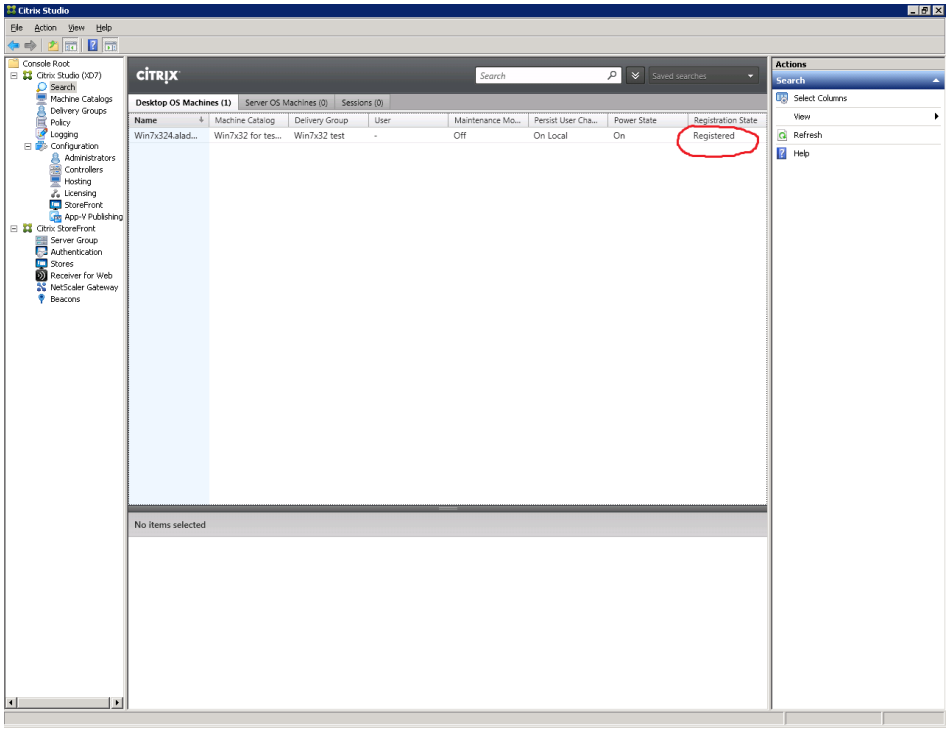

Рис. 17 — Окно статуса виртуальных машин

1.3. Проверка доступности виртуальных машин

Перейдите на рабочую станцию (ПК) пользователя. Это Windows 7 x64 с предустановленным JC Client 6.24.16.

Откройте браузер и в адресной строке укажите путь к веб-интерфейсу ПО Citrix **XenDesktop:** **http://xd7.aladdin.local/Citrix/StoreWeb/** (рис. 18).

Если ПО **Citrix Receiver** не установлено, отобразится окно установки ПО Citrix Receiver (рис. 19).

Нажмите **Установить.**

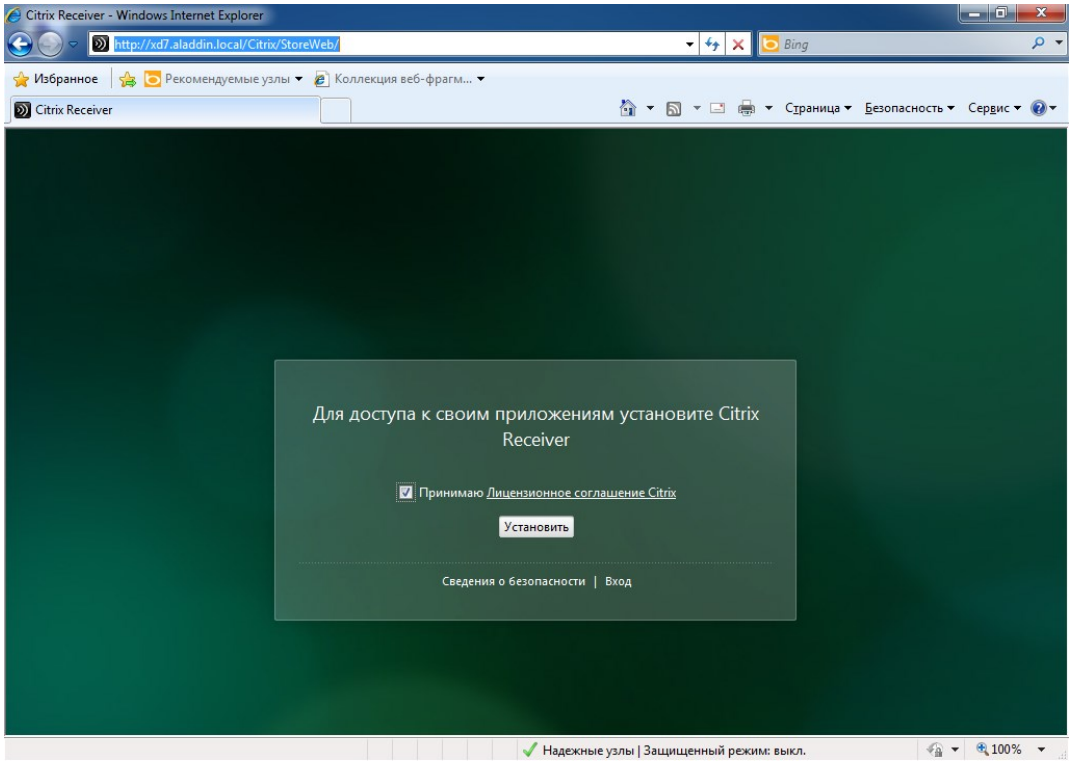

Рис. 18 — Web-интерфейс ПО XenDesktop

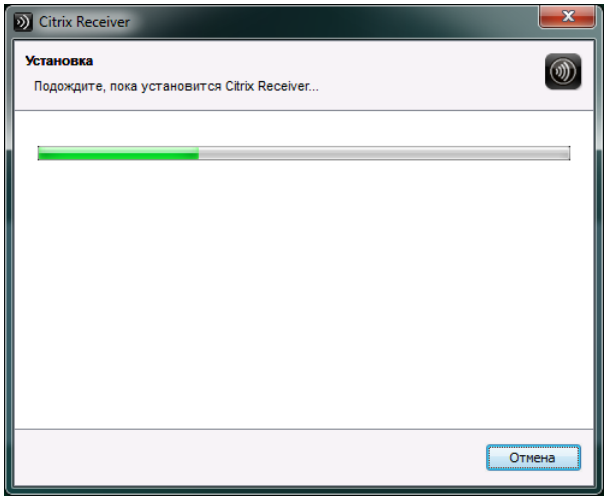

Рис. 19 — Установка ПО Citrix Receiver

Введите **Логин** и **Пароль** учетной записи пользователя в службе каталогов AD. Данная учетная запись должна входит в группу пользователей виртуальных машин, которая была создана в разделе 1.2 (рис. 20).

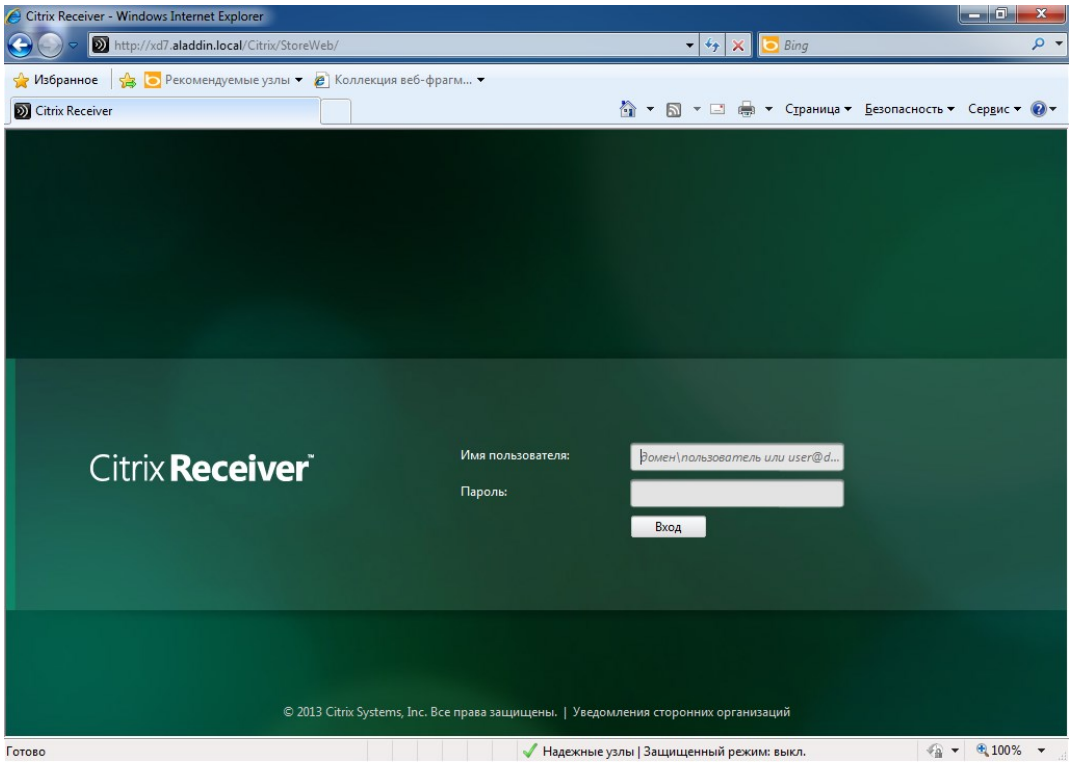

Рис. 20 — Окно аутентификации пользователя на Web-интерфейсе ПО XenDesktop

Убедитесь, что виртуальная машина доступна. После чего, завершите сеанс пользователя (рис. 21) (Пуск -> Выйти из системы).

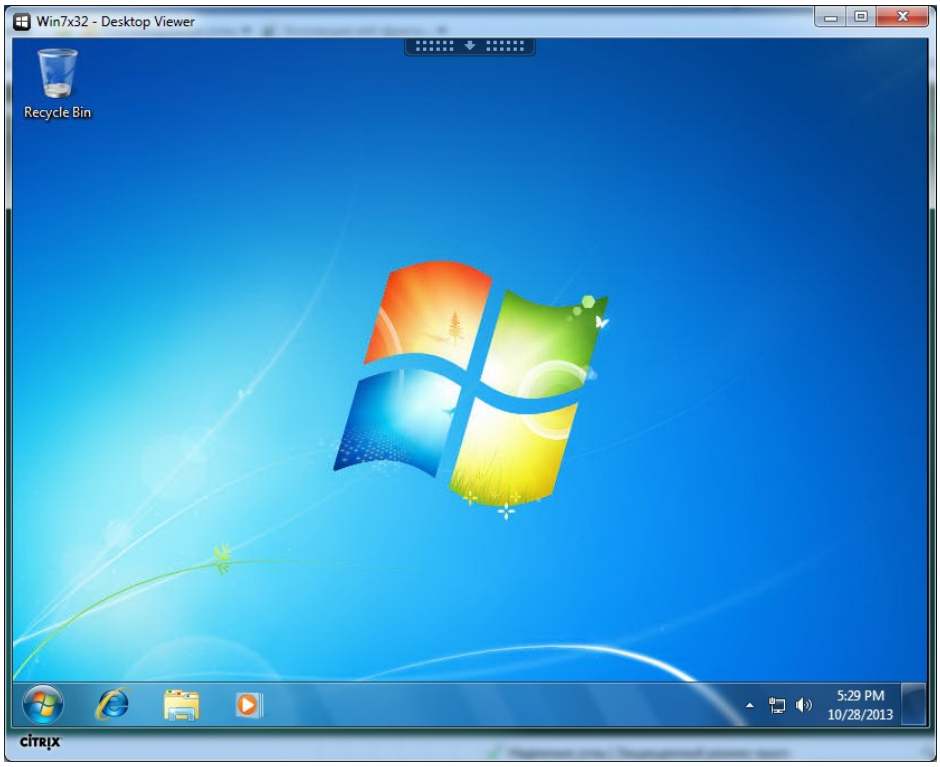

Рис. 21 — Виртуальная машина пользователя

2. Настройка аутентификации по смарт-картам

2.1. Выпуск сертификата для IIS

На сервере, где установлено ПО XenDesktop 7, запустите оснастку управления сервисом Internet Information Services (IIS) (рис. 22).

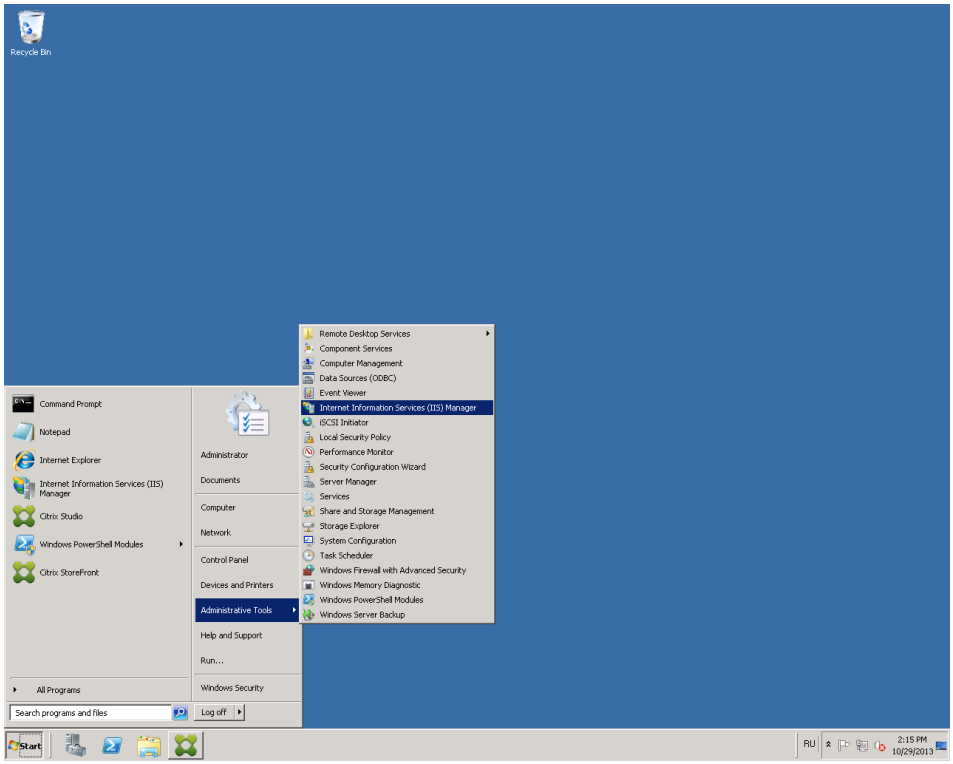

Рис. 22 — Путь к оснастке управления сервисом IIS

Откройте вкладку **Server Certificates** (рис. 23).

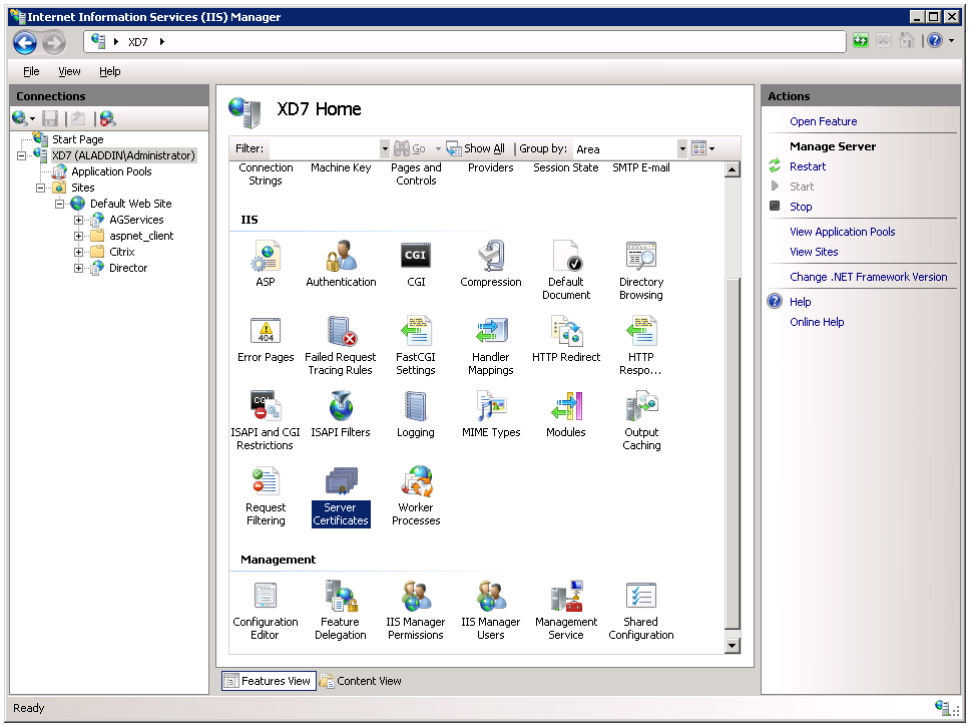

Рис. 23 — Оснастка управления сервисом IIS

Выберите **Create Domain Certificate** (рис. 24).

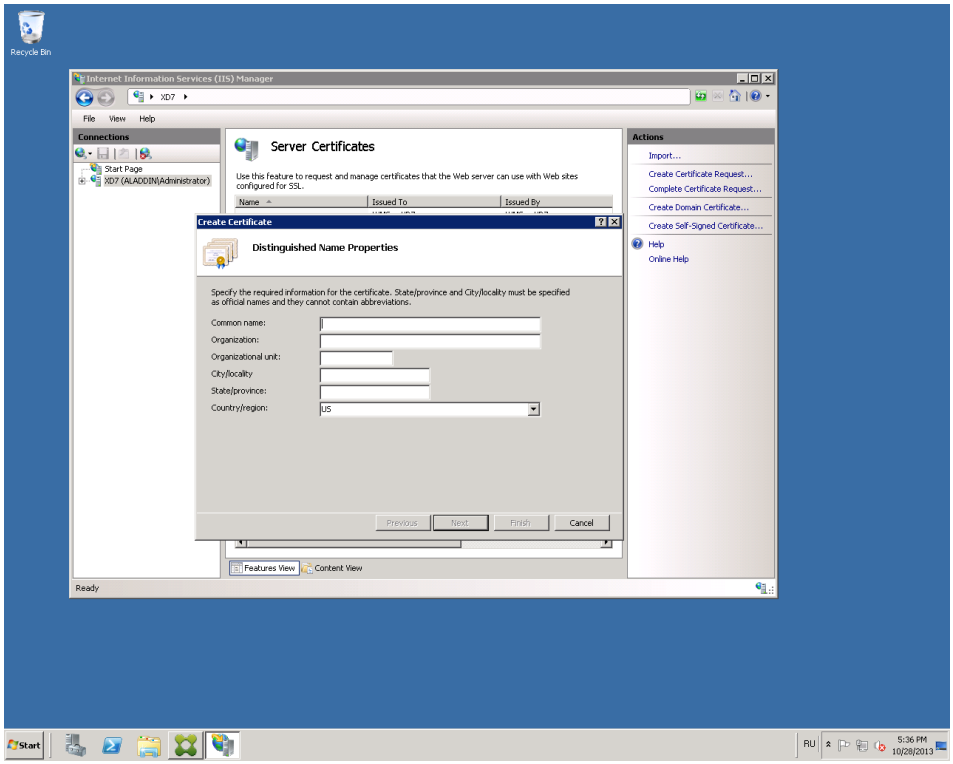

Рис. 24 — Вкладка «Create Certificate»

Заполните информацию об организации для выпускаемого сертификата (рис. 25).

В поле **Common name** укажите полное доменное имя сервера с установленным ПО XenDesktop. В настоящем примере: xd7.aladdin.local.

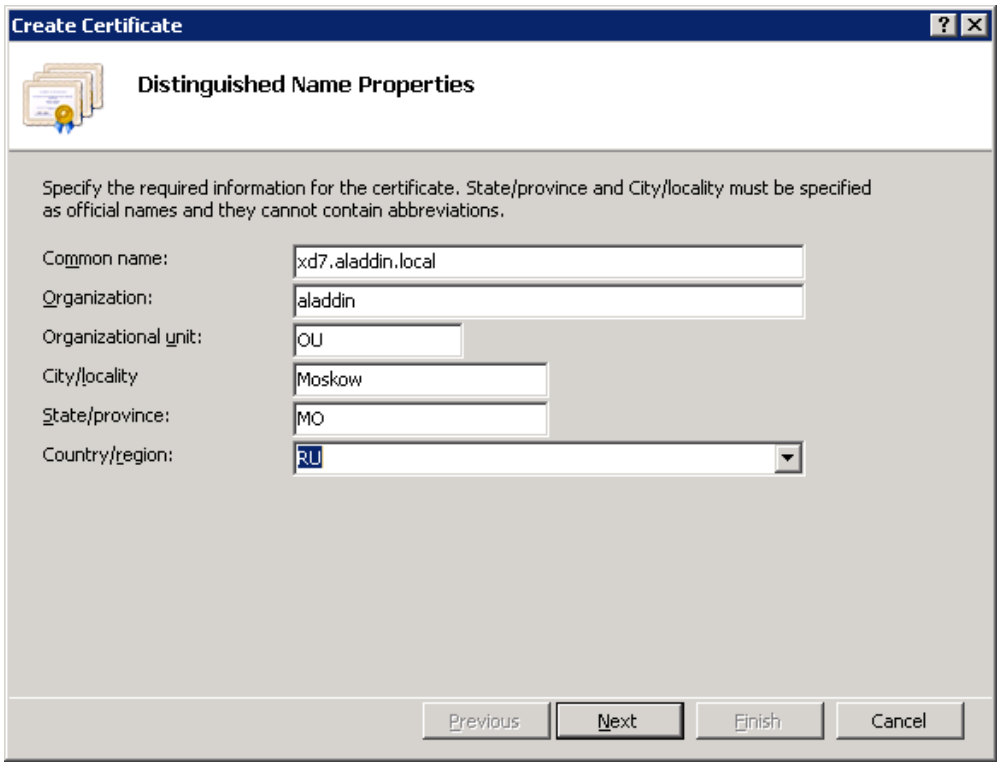

Рис. 25 — Данные об организации в выпускаемом сертификате

Выберите центр сертификации организации и в поле **Friendly name** укажите полное доменное имя сервера с установленным ПО **XenDesktop.** В настоящем примере: **xd7.aladdin.local** (рис. 26).

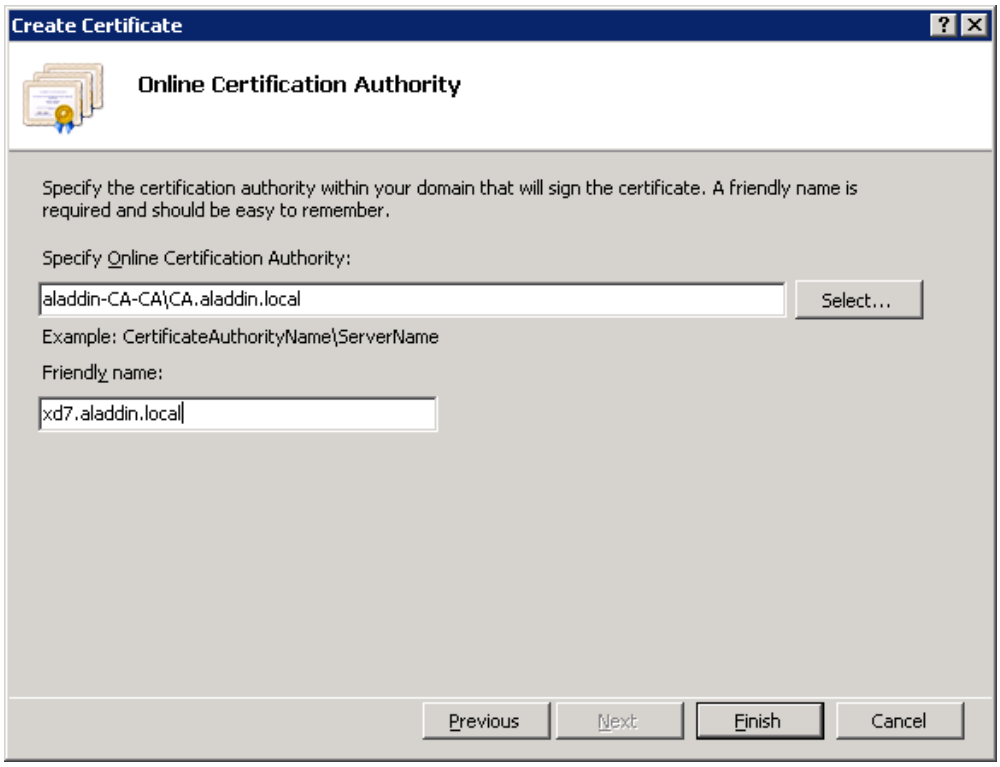

Рис. 26 — Выпуск сертификата для сервиса IIS

Нажмите **Finish.**

Убедитесь, что сертификат выпущен успешно (рис. 27).

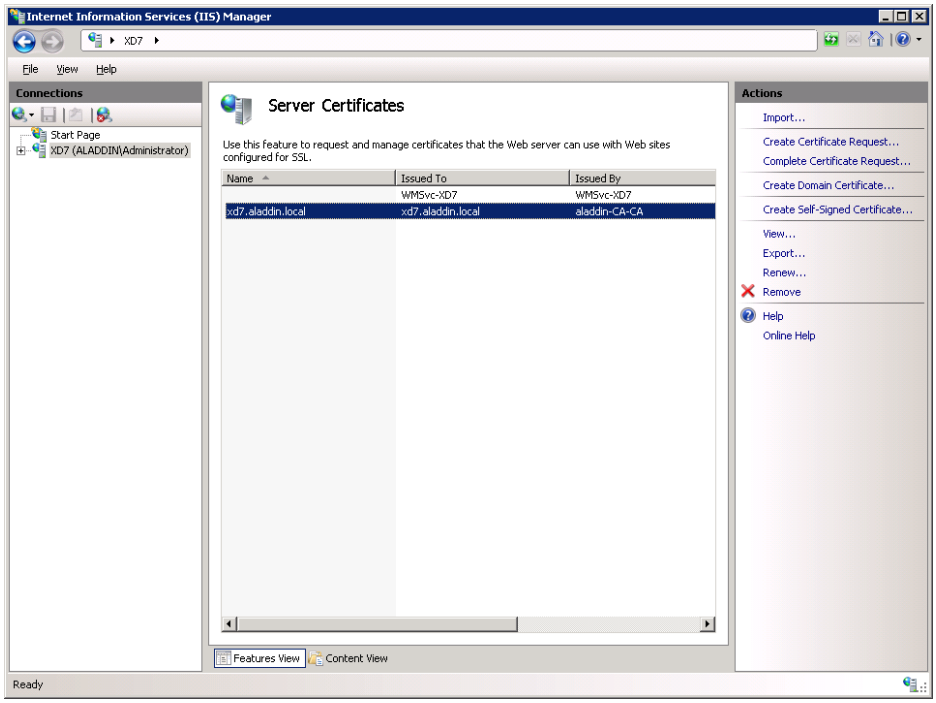

Рис. 27 — Результат выпуска сертификата

2.2. Настройка SSL доступа к IIS

Перейдите на вкладку **Default Web Site** и нажмите **Bindings…**

В открывшемся окне нажмите **Add** (рис. 28).

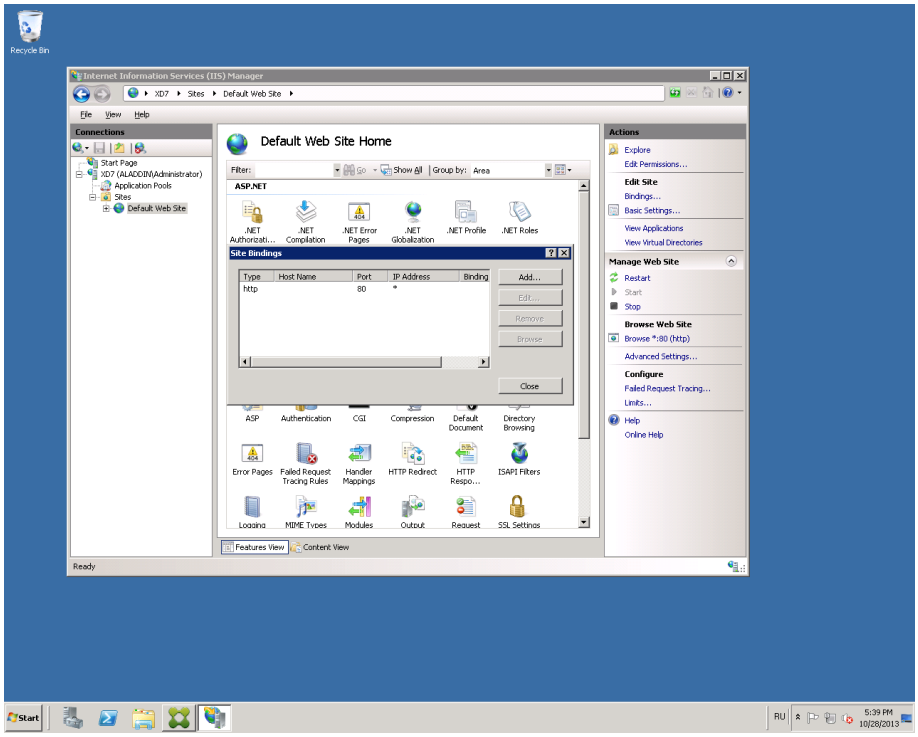

Рис. 28 — Окно настройки «Site Bindings»

Выберите тип соединения **https,** а в списке SSL certificate, выберите ранее выпущенный сертификат для IIS (рис. 29).

В настоящем примере имя сертификата: xd7.aladdin.local.

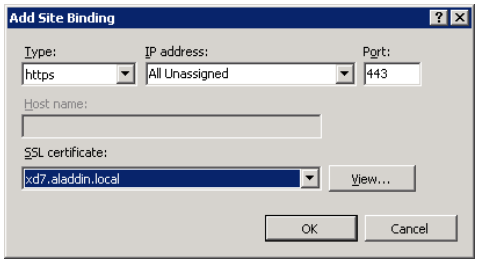

Рис. 29 — Окно «Add Site Binding»

Нажмите **OK.**

Убедитесь, что данный тип соединения добавлен в список (рис. 30).

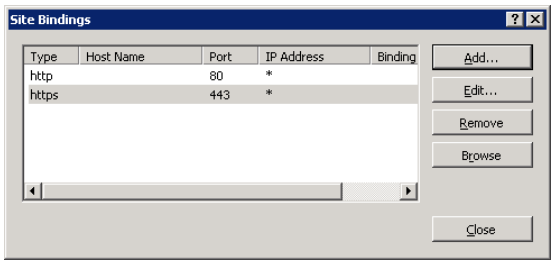

Рис. 30 — Результат настройки типа соединения

Закройте окно «Site Bindings».

2.3. Настройка Citrix StoreFront

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

Запустите Citrix Studio. Во вкладке Citrix StoreFront откройте вкладку Authentication (рис. 31).

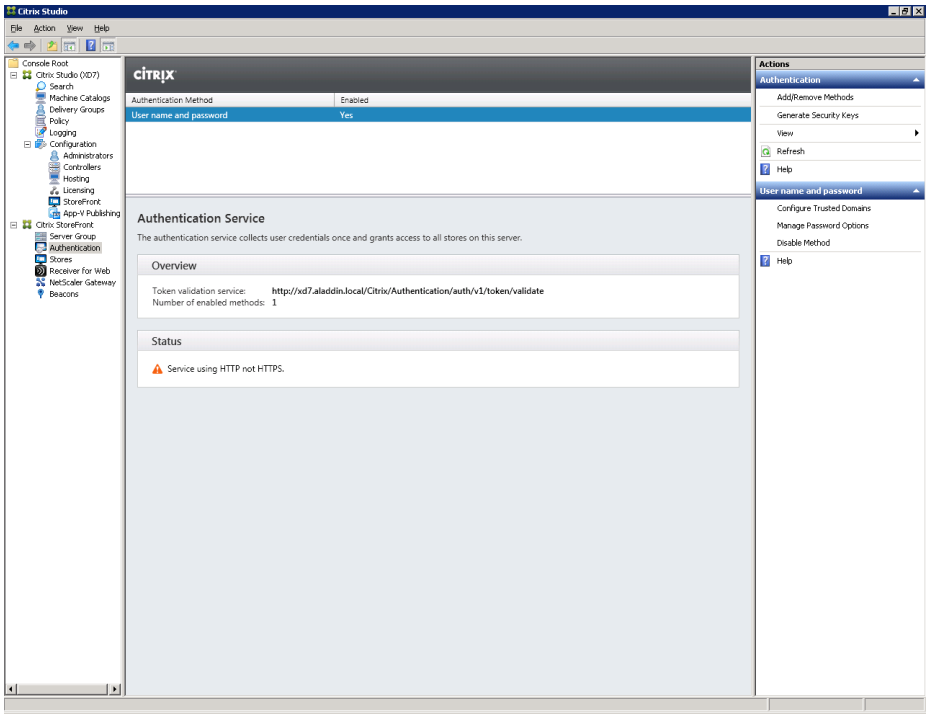

Рис. 31 — Вкладка «StoreFront Authentication»

Выберите пункт Add/Remove Authentication Methods.

Откроется окно **Add/Remove Methods** (рис. 32).

Выберите метод аутентификации Smart card.

Рис. 32 — Окно «Add/Remove Authentication Methods»

Нажмите **OK.**

Убедитесь, что на вкладке **Authentication** добавился метод аутентификации **Smart card** (рис. 33).

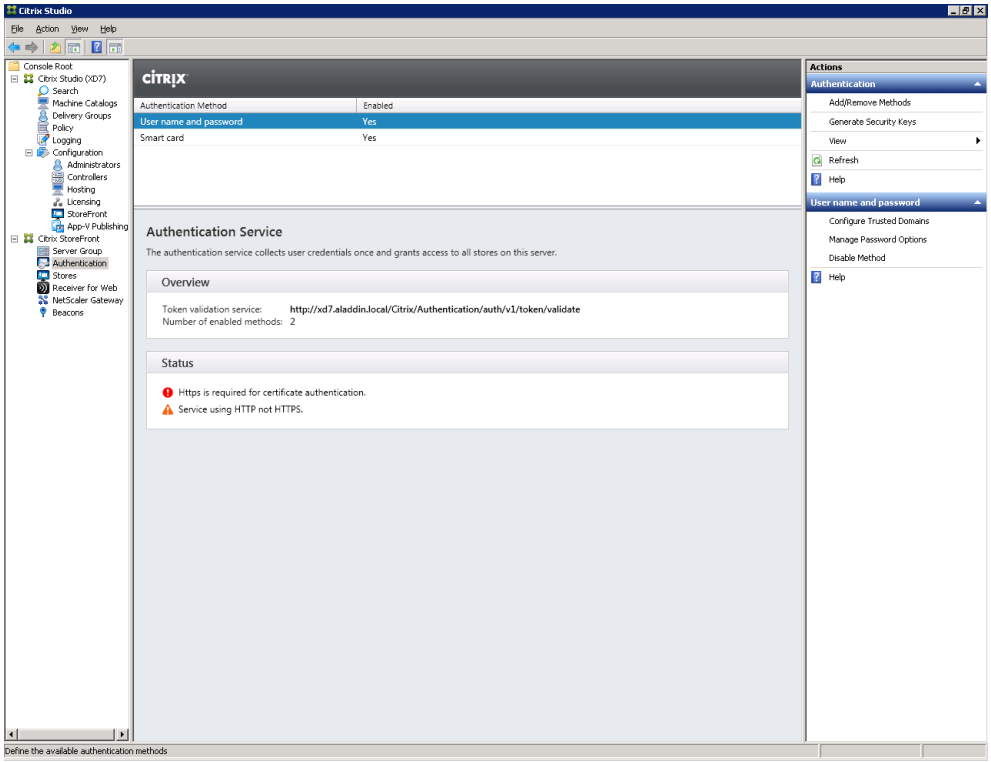

Рис. 33 — Результат изменения методов аутентификации

Откройте **Default Web Site** -> **Citrix** -> **Authentication** -> **Certificate** (рис. 34).

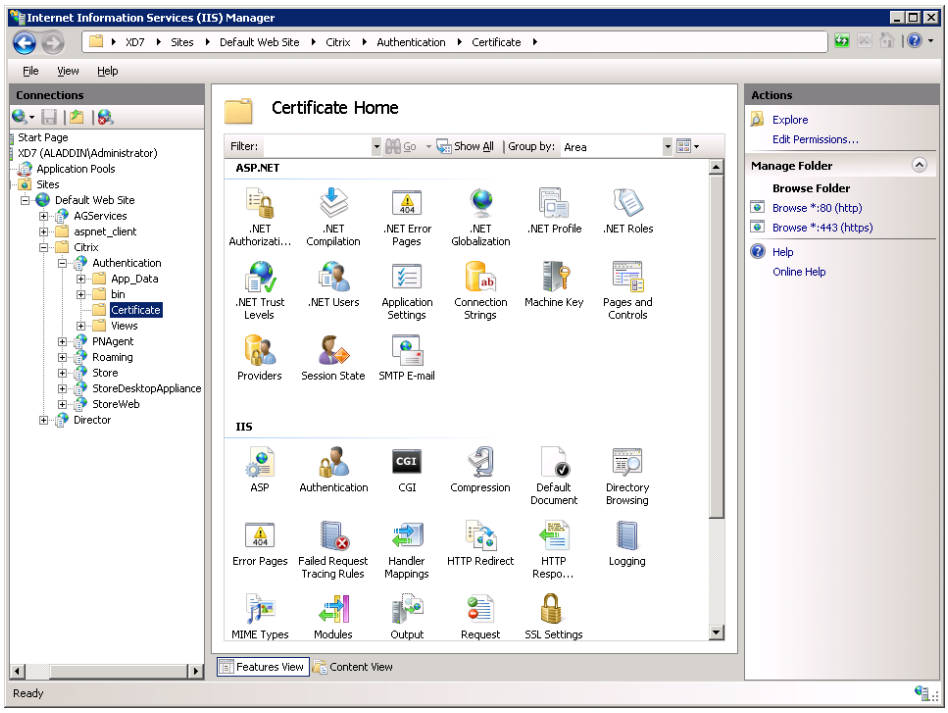

Рис. 34 — Вкладка Certificate Home

Выберите пункт SSL Settings -> Require SSL. Отметьте параметр Require (рис. 35).

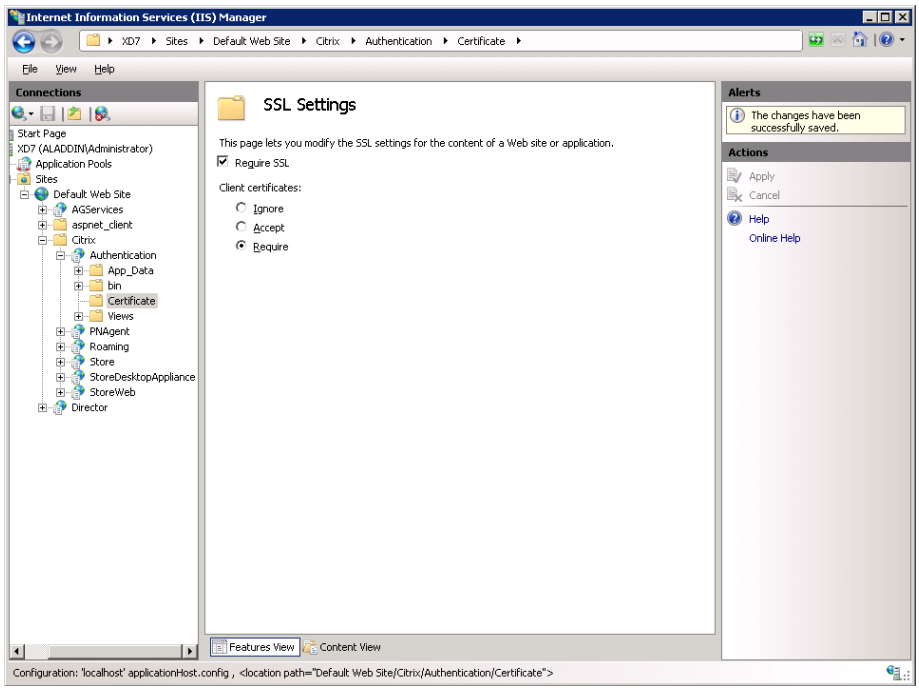

Рис. 35 — Настройки SSL Settings

Для проверки правильности SSL-настроек, необходимо выполнить следующую последовательность действий:

- Подключитесь к ПК пользователя;

- Подключите смарт-карту с сертификатом пользователя к ПК пользователя;
- Откройте браузер;
- В адресной строке укажите путь к странице с тестовым приложением. В настоящем примере — https://xd7.aladdin.local/Citrix/Authentication/Certificate/test.aspx.

⚠ Вместо xd7.aladdin.local необходимо указать полное доменное имя сервера с ПО Citrix XenDesktop.

Отобразится следующее окно, в котором необходимо выбрать сертификат пользователя (рис. 36).

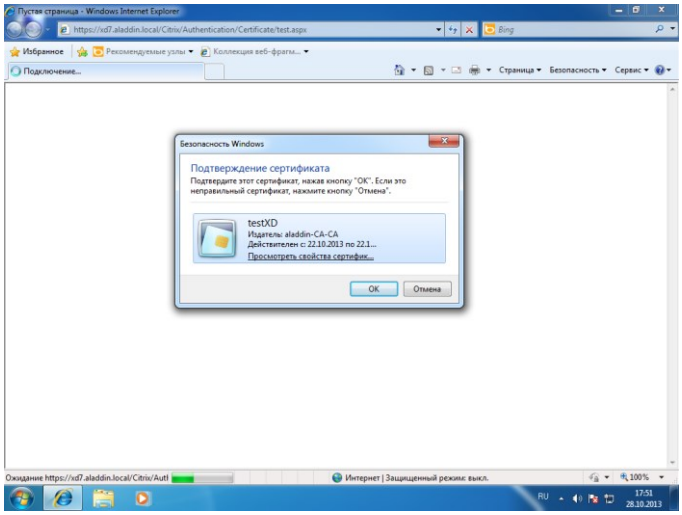

Рис. 36 — Окно запроса сертификата пользователя

Выберите сертификат пользователя и нажмите **OK.**

Отобразится следующее окно (рис. 37).

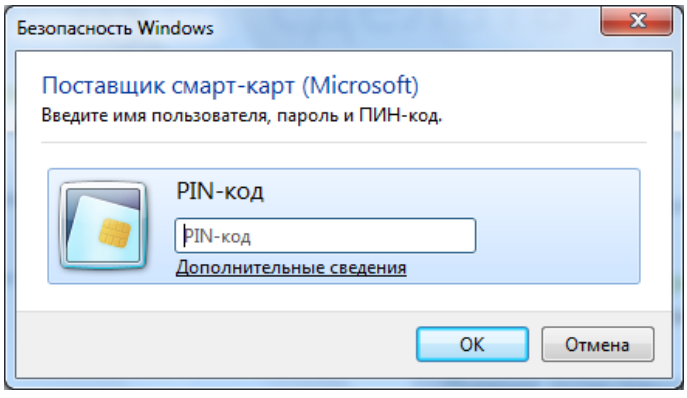

Рис. 37 — Окно запроса PIN-кода для смарт-карты пользователя

Введите PIN-код смарт-карты пользователя и нажмите **OK.**

Если SSL соединение установлено успешно, то вы увидите на открывшейся странице информацию о сертификате пользователя (рис. 38).

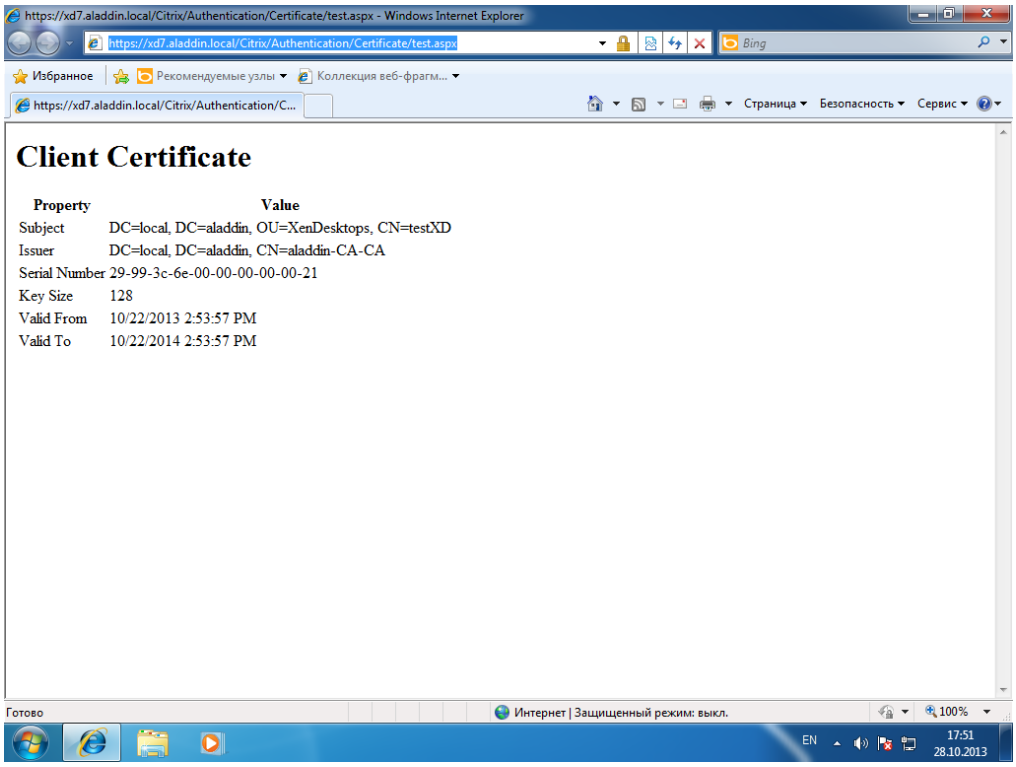

Рис. 38 — Окно проверки сертификата пользователя

Подключитесь к серверу с установленным ПО Citrix **XenDesktop** и выполните настройку протоколов связи для **SSL**.

Запустите **консоль управления Citrix Studio.** Для этого откройте ПО **Citrix StoreFront** и выберите вкладку **Server Group.** Выберите пункт **Change Base URL** и измените значение **http** на **https** (рис. 39).

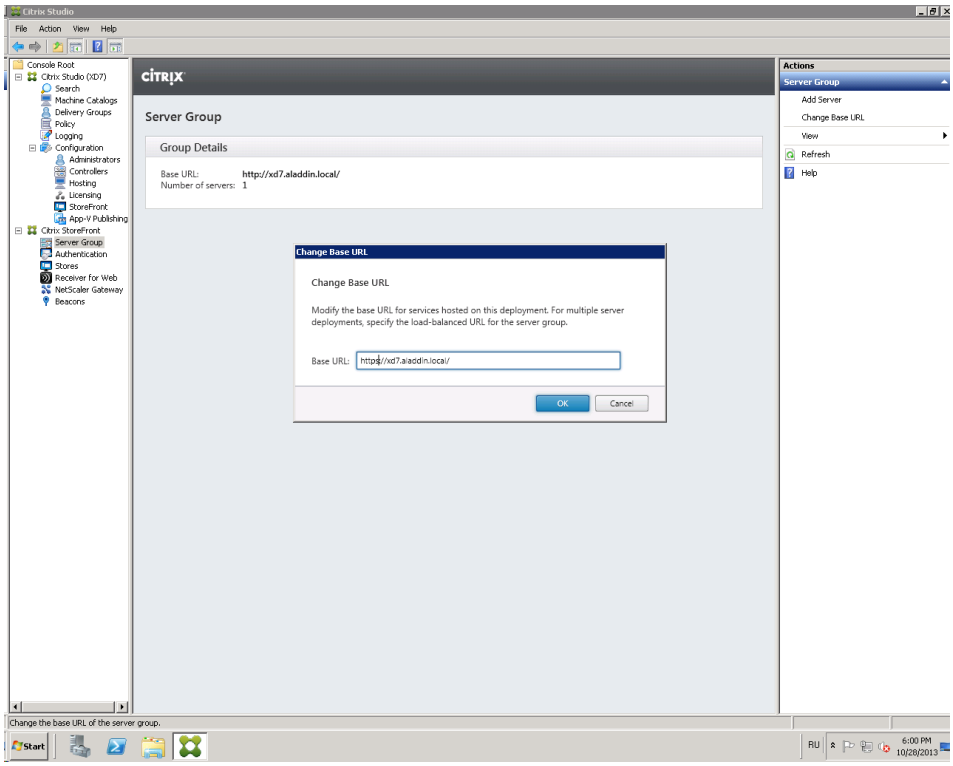

Рис. 39 — Окно «Change Base URL»

Нажмите OK.

Перейдите на вкладку Stores (рис. 40).

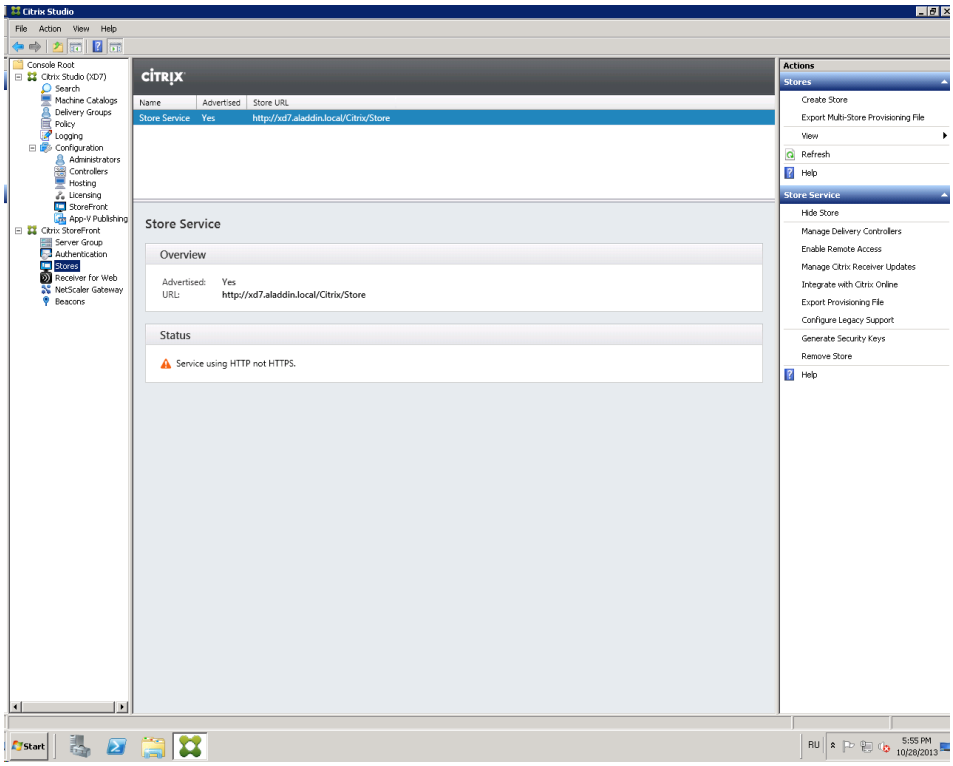

Рис. 40 — Вкладка «Stores»

Выберите пункт **Manage Delivery Controllers**.

В открывшемся окне нажмите **Edit** (рис. 41).

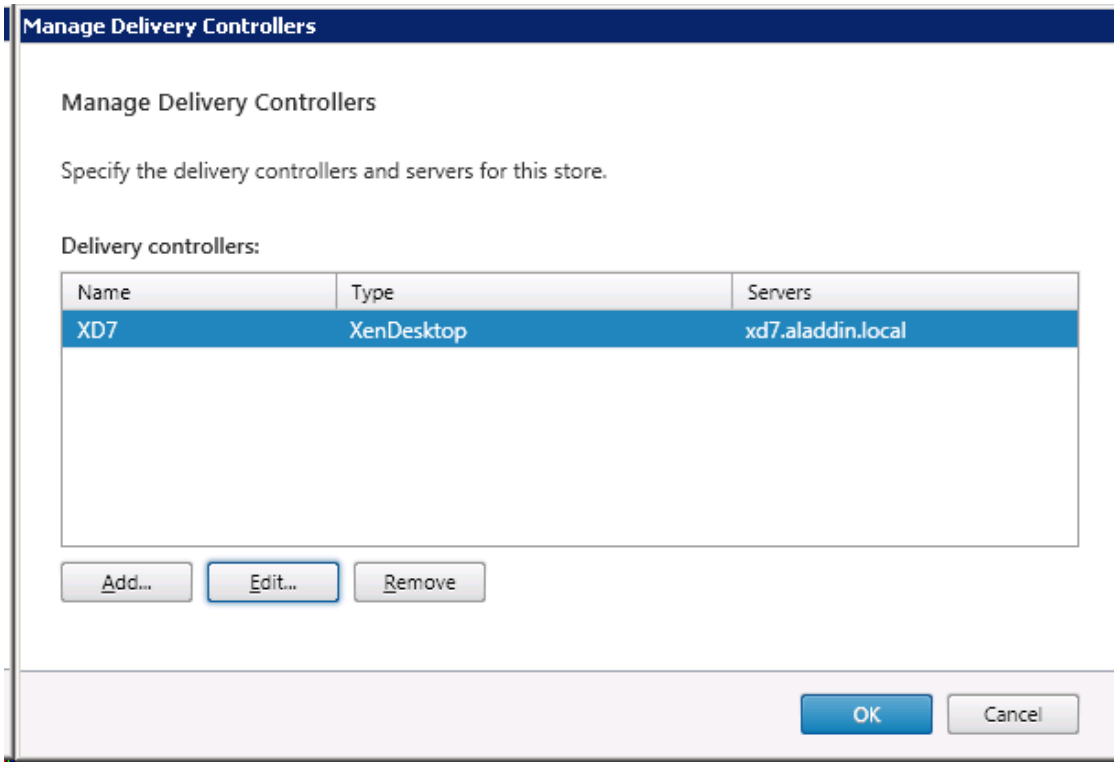

Рис. 41 — Окно «Manage Delivery Controllers»

В поле **Transport type** замените HTTP на HTTPS (рис. 42; рис. 43).

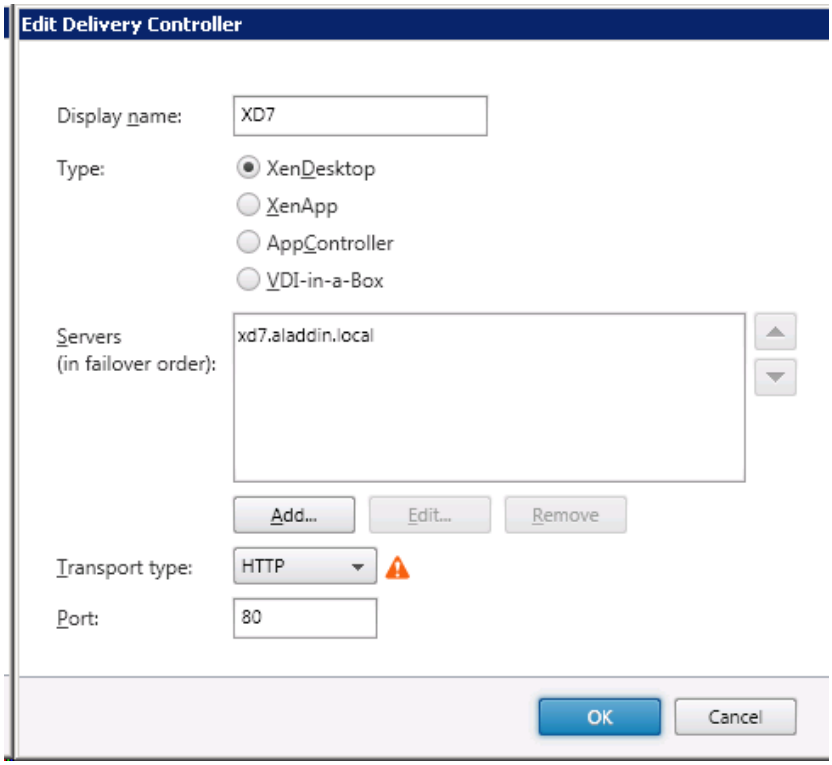

Рис. 42 — Окно «Edit Delivery Controller» с значением HTTP

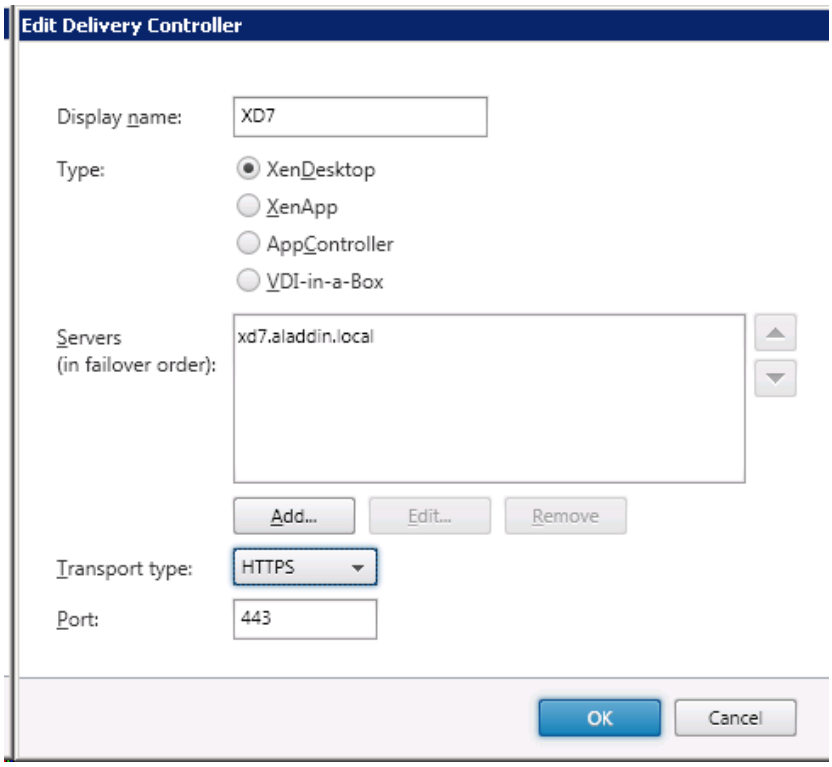

Рис. 43 — Окно «Edit Delivery Controller» с значением HTTPS

Нажмите **OK.**

Убедитесь, что в поле **Status** появилось значение **Service using HTTPS** (рис. 44).

Внимание: После применение настроек необходимо выполнить перезагрузку сервера с ПО Citrix XenDesktop

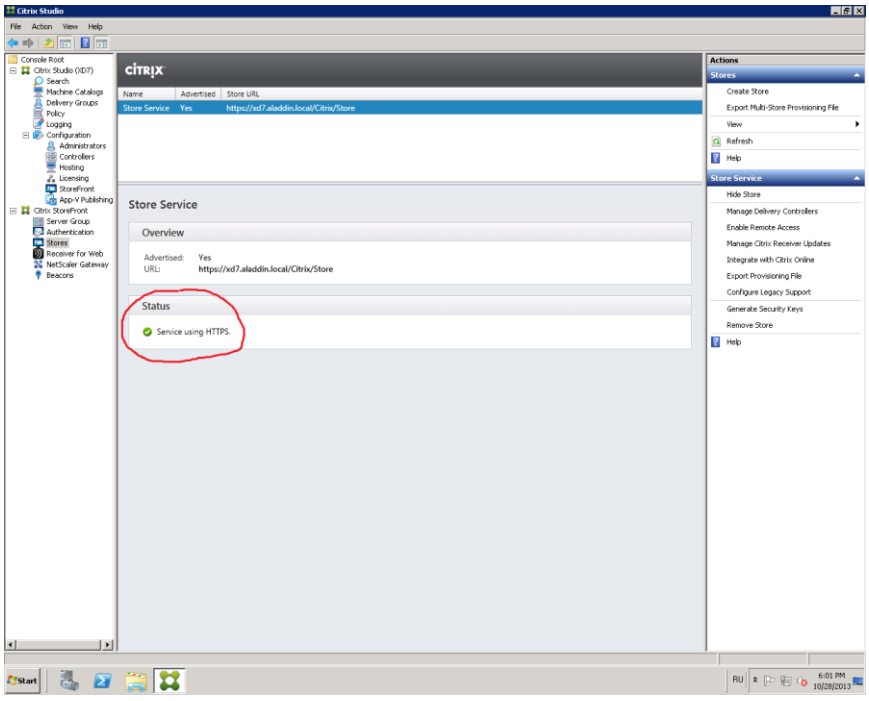

Рис. 44 — Значение поля Status

2.4. Настройка XML-запросов

Необходимо разрешить XML-запросы к серверу с установленным ПО Citrix XenDesktop. Для этого выполните следующие действия.

На сервере с установленным ПО Citrix XenDesktop откройте командную строку **Windows PowerShell** (рис. 45).

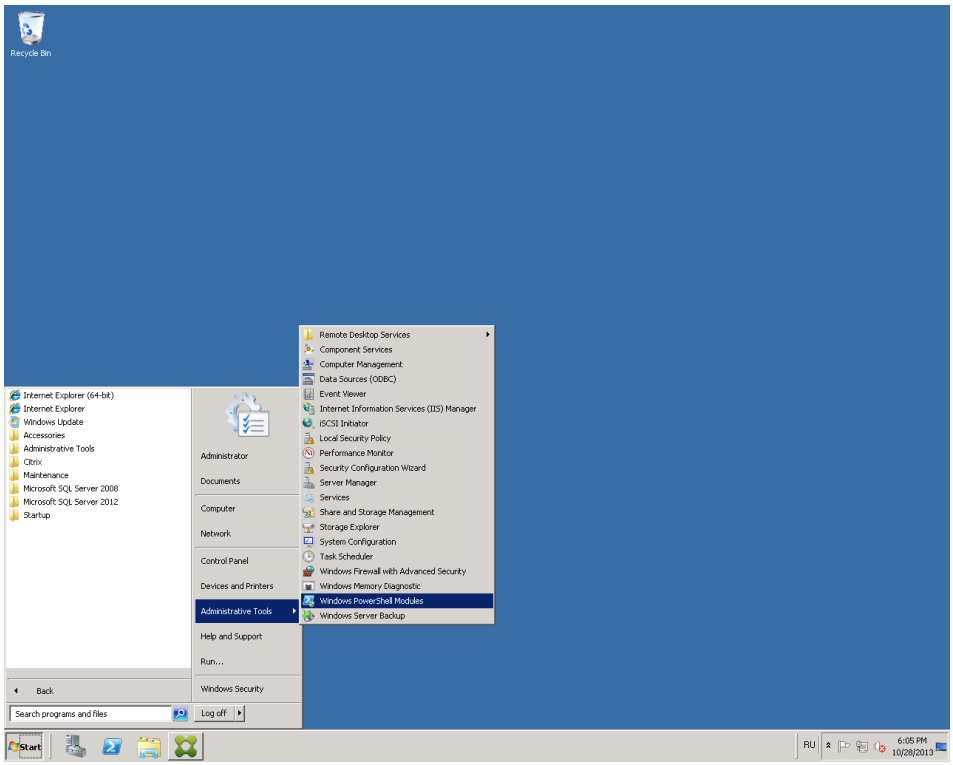

Рис. 45 — Путь к командной строке «Windows PowerShell»

В открывшейся командной строке выполните команду:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true (рис. 46)
```

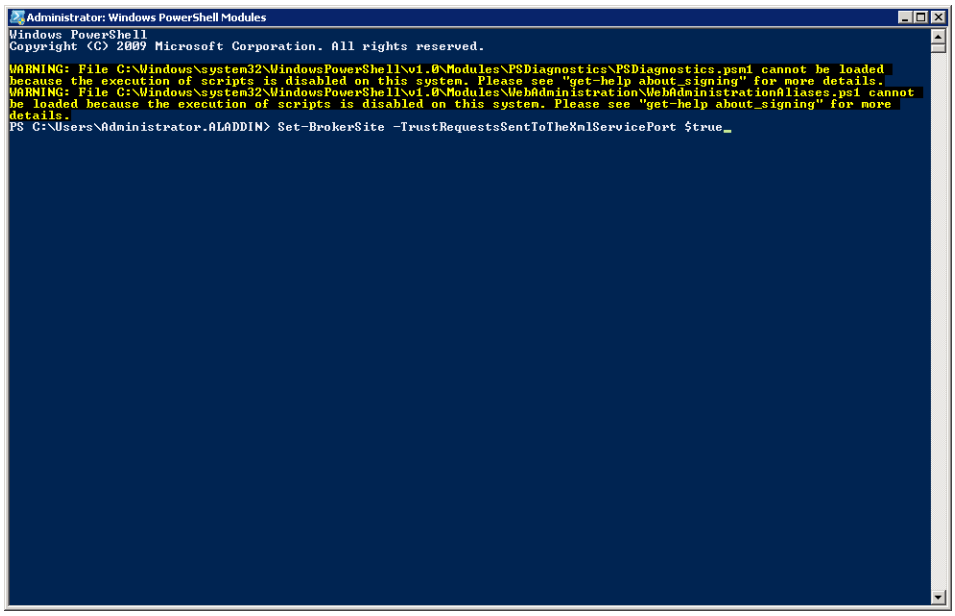

Рис. 46 — Команда строка «Windows PowerShell»

2.5. Настройка ПК пользователя

Поключитесь к ПК пользователя. Откройте ПО Citrix Receiver и добавьте строку подключения к серверу, с опубликованными рабочими столами и/или приложениями (рис. 47).

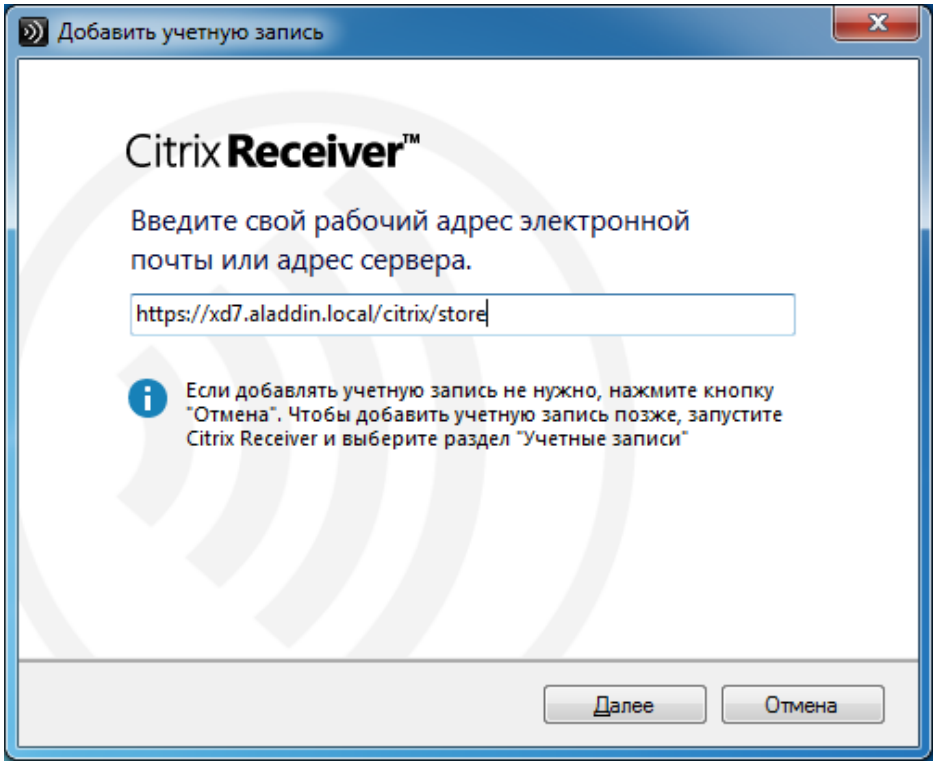

Рис. 47 — Добавление адерса сервера в ПО Citrix Receiver

Для обеспечения корректной работы, необходимо чтобы **адрес сервера с ПО Citrix StoreFront** был добавлен **в доверенные(Trusted**) или **локальные(Local Intranet)** сайты в используемом браузере. В настройках уровня безопасности для каждого из вариантов необходимо убедится, что включена настройка **Automatic logon with the current user name and password.** Рекомендуется использовать браузер – Internet Explorer 9.0 и выше.

Если адрес сервера указан верно, а смарт-карта с сертификатом подключена к USB-порту ПК пользователя, откроется окно с запросом PIN-кода пользователя (рис. 48).

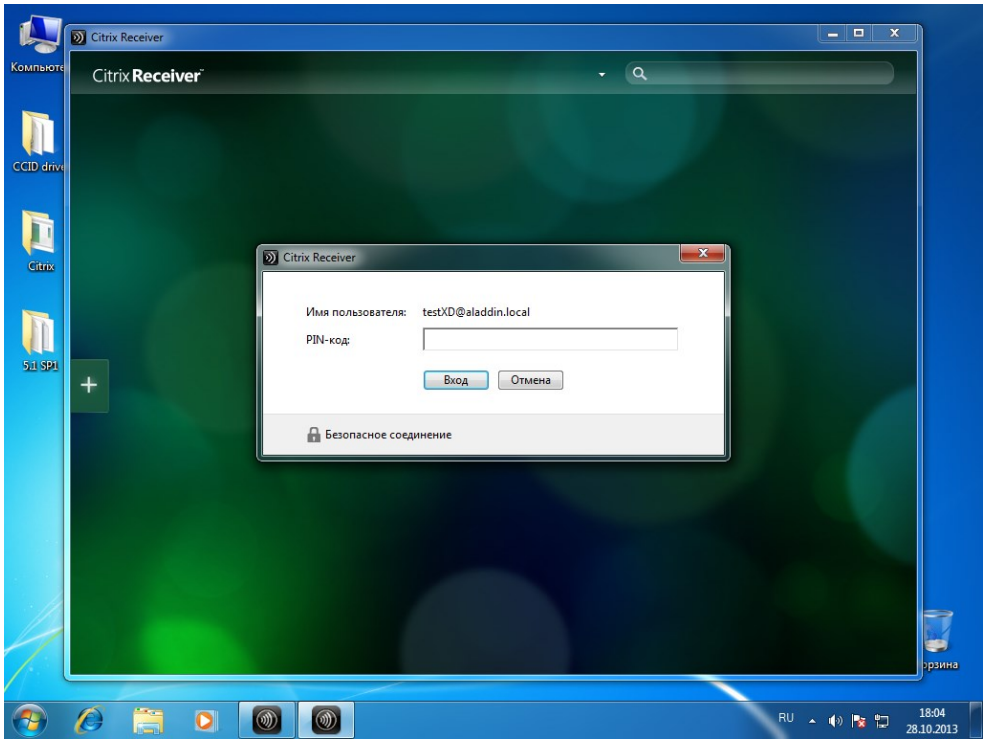

Рис. 48 — ПО Citrix Receiver: запрос PIN-кода для смарт-карты пользователя

Введите PIN-код пользователя (рис. 49).

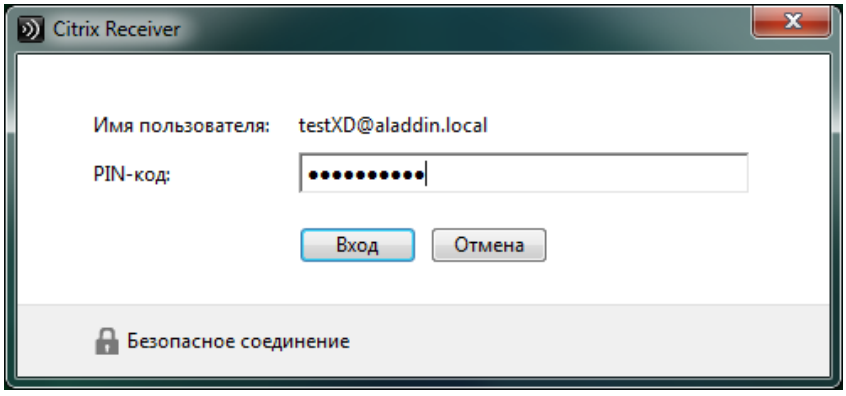

Рис. 49 — Ввод PIN-кода пользователя

Подключение к серверу приложений (рис. 50).

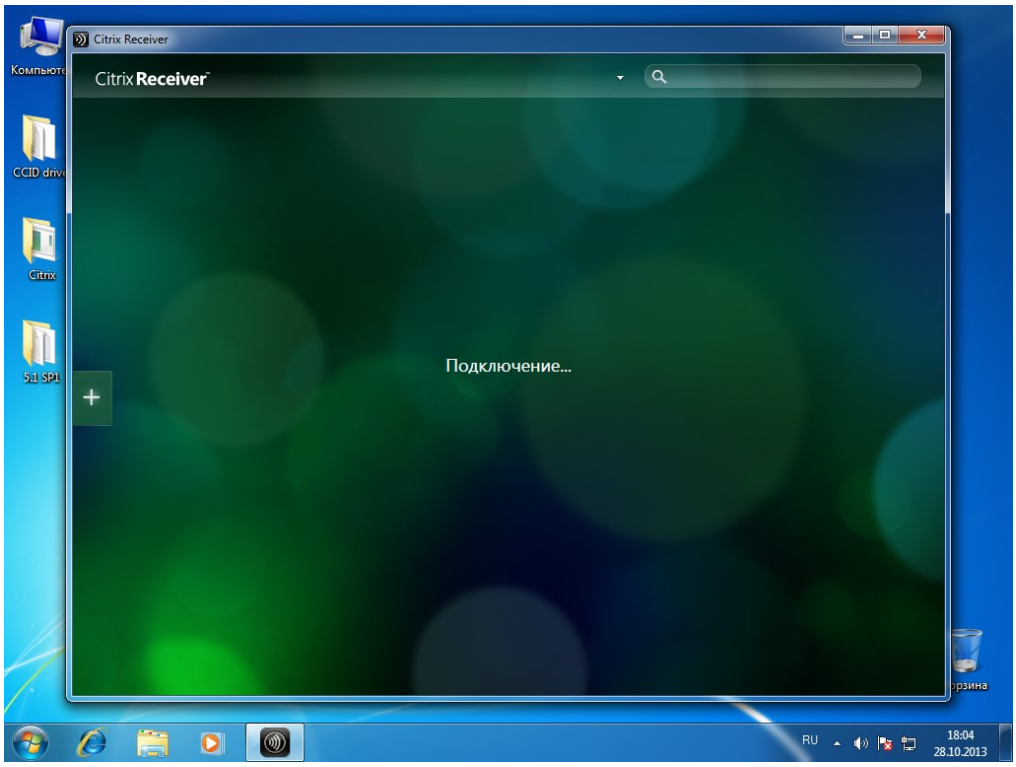

Рис. 50 — Подключение к серверу приложений

После подключения откройте вкладку **Все приложения.** Отобразятся доступные приложения и рабочие столы.

В настоящем примере выберите **Win7x32** (рис. 51).

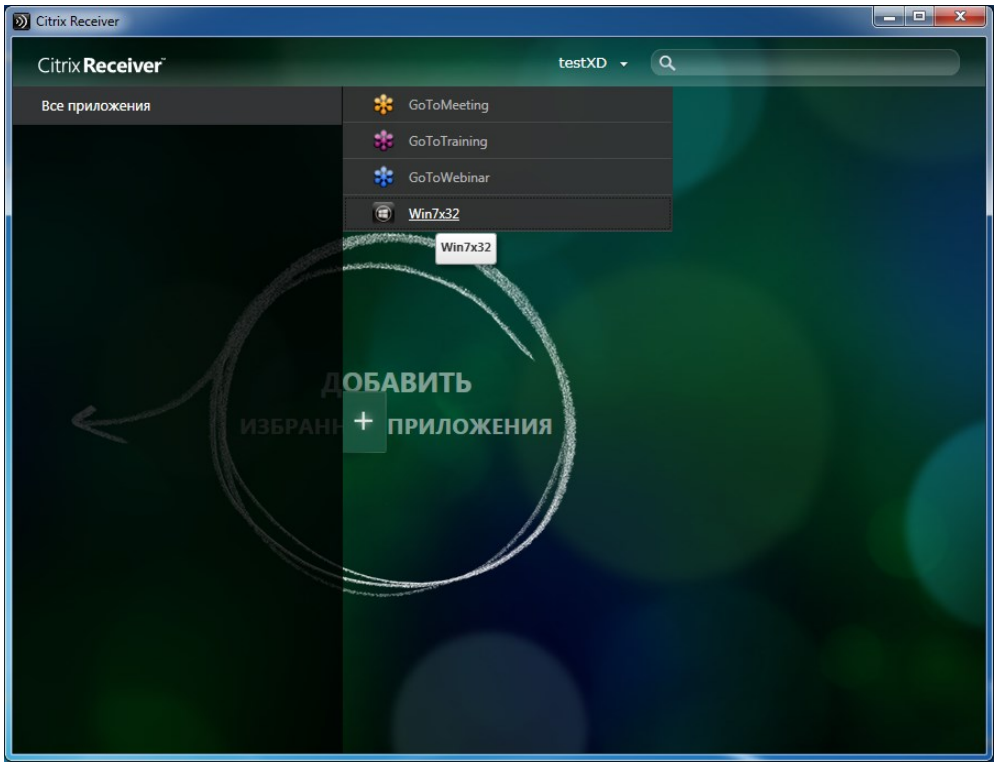

Рис. 51 — Список доступных приложений

Для входа в ОС Windows на виртуальной машине необходимо ввести PIN-код на ключевой носитель пользователя (рис. 52).

Рис. 52 — Аутентификация по смарт-карте на удаленном рабочем столе

Аутентификация прошла успешно (рис. 53).

Рис. 53 — Успешная аутентификация по смарт-карте в удаленном рабочем столе

3. Настройка сквозной аутентификации по смарт-карте

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

⚠ Внимание: Для корректной работы сквозной аутентификации по смарт-картам необходимо, чтобы конечное устройство пользователя (ПК пользователя) было добавлено в домен, в котором находятся инфраструктурные серверы с установленным ПО Citrix XenDesktop 7 (Delivery Controller, StoreFront и тд.) или, при использовании нескольких доменов, между доменами были настроены доверительные отношения.

Настройка Single Sign-on (SSO) для аутентификации по смарт-карте при использовании ПО XenDesktop7 состоит из следующих этапов:

1. Создание каталога виртуальных машин (стр. 4).
2. Создание группы пользователей виртуальных машин (стр. 10).
3. Установка ПО Citrix Receiver 4.0 и выше на ПК пользователя (стр. 39).
4. Настройка политик аутентификации ПО Citrix XenDesktop (стр. 40).
5. Выпуск сертификата для IIS и настройка SSL доступа к IIS (стр. 19 и 23).
6. Настройка XML-запросов к серверу, с установленным ПО XenDesktop 7 (стр. 32).
7. Настройка ПО Citrix StoreFront 2.1 для включения SSO при аутентификации по смарт-картам (стр. 42).
8. Настройка ПКпользователя (стр. 34).

3.2. Установка и настройка ПО Citrix Receiver 4.0 для включения SSO при аутентификации по смарт-картам.

Для настройки сквозной аутентификации по смарт-картам на Citrix Receiver 4.0 необходимо выполнить установку Citrix Receiver 4.0 с дополнительными параметрами. Установка Citrix Receiver 4.0 выполняется из командной строки:

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

2. В командной строке указать путь к файлу установщика Citrix Receiver 4.0 и дополнительно указать параметры для включения SSO:

```
/includeSSON AM_SMARTCARDPINENTRY=CSP.
```

Пример:

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

3. Дождитесь окончания установки ПО Citrix Receiver 4.0 и перезагрузите ПК пользователя.

4. После перезагрузки ПК пользователя проверьте, что в исполняемых процессах (Task Manager/Processes) присутсвует процесс **ssonsrv.exe.**

5. Выполните настройку политик аутентификации для ПО Citrix XenDesktop, которые будут применяться на серверы Citrix и устройства пользователей, как описано в разделе 3.3.

⚠ Подробную информацию для настройки аутентификации по смарт-картам можно найти на сайте электронной документации: http://support.citrix.com/proddocs/topic/receiver-windows-40/receiver-windows-smart-card-cfg.html. Для настройки параметров сквозной аутентификации необходимо обратить внимание на следующие разделы: **To enable single sign-on for smart card authentication**, **To use CSP PIN prompts**.

3.3. 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 политики необходимо выполнить следующую последовательность действий:

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

⚠ Шаблон политик можно найти в папке установки клиента ПО Citrix Receiver: **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 Authentication.

4. Выберите настройку Smart Card Authentication и включите параметры «Allow smart card authentication» и «Use pass-through authentication for PIN». Выберите настройку Local User Name and Password и включите параметры «Enable pass-through authentication» и «Allow pass-through authentication for all ICA connections» (рис. 54; рис. 55).

Подробной информация доступна на сайте — http://support.citrix.com/proddocs/topic/ica-settings/ica-settings-wrapper.html

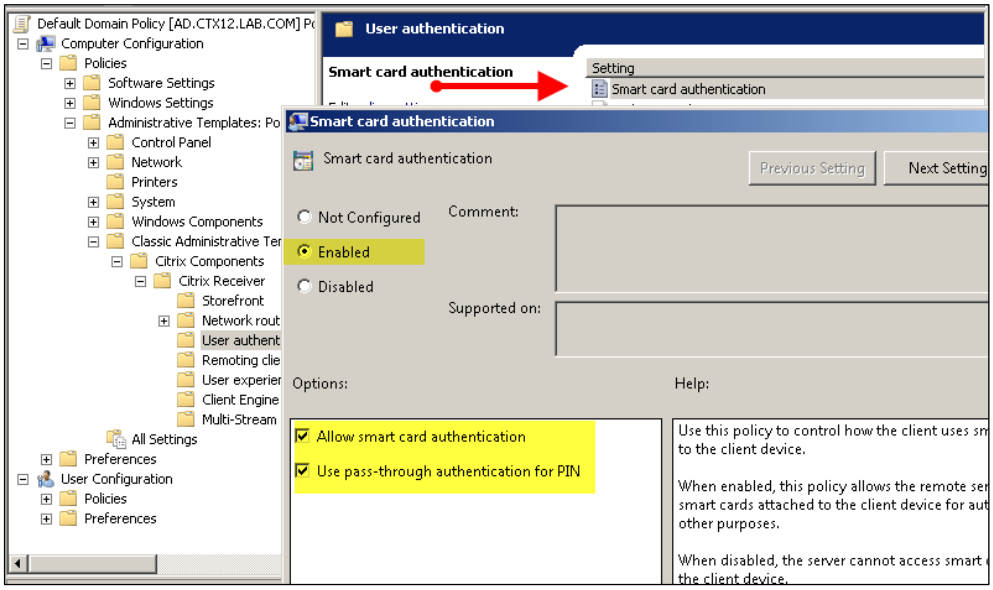

Рис. 54 — Настройка групповых политик AD для SSO

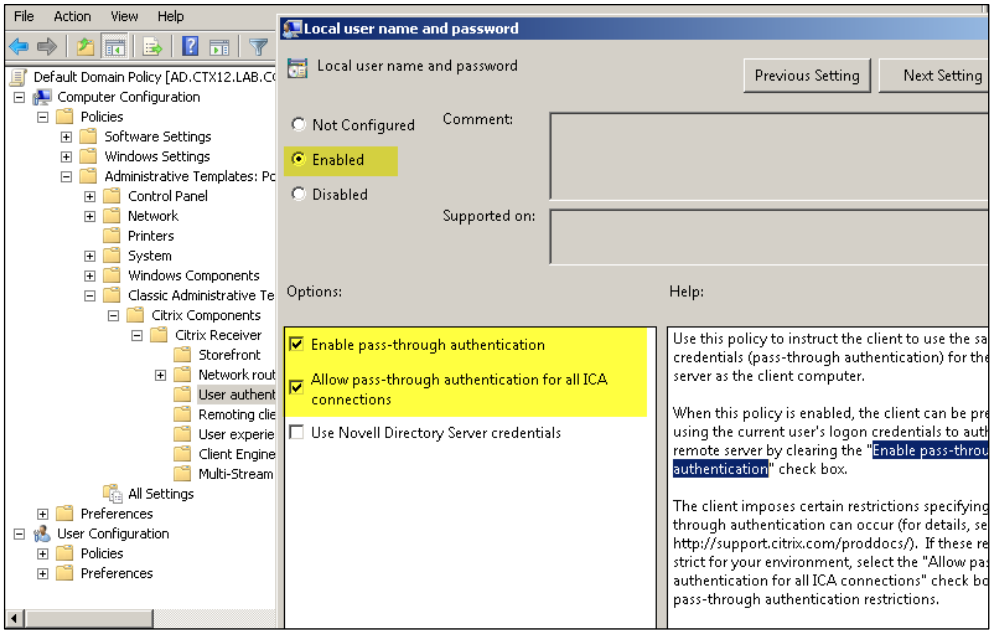

Рис. 55 — Настройка групповых политик службы каталога AD для SSO

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

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

Для настройки ПО Citrix StoreFront для работы SSO при аутентификации по смарт-картам необходимо выполнить следующие действия на сервере с установленным ПО Citrix StoreFront:

1. Выполните первоначальную настройку ПО Citrix StoreFront 2.1 согласно разделу — Настройка Citrix StoreFront (стр. 24).

2. В разделе Add/Remove Authentication Methods добавьте метод аутентификации Domain pass-through (рис. 56).

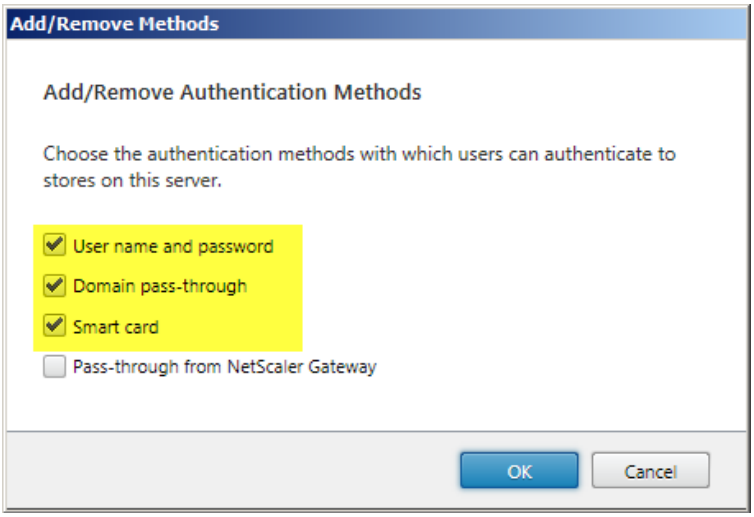

Рис. 56 — Настройка метода аутентификации

3. Для включения сквозной аутентификации с использованием смарт-карт необходимо внести дополнительные изменения в конфигурацию. Для этого отредактируйте **default.ica**, для каждого ПО 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 сайте: http://support.citrix.com/proddocs/topic/dws-storefront-21/dws-configure-conf-smartcard.html.

7. Выполните настройку пользователя согласно разделу — Настройка ПК пользователя (см. раздел 2.5). Проверить, что вход на виртуальную машину пользователя выполняется успешно. Проверить, что после входа на ПК пользователя (по смарт-карте или по паролю) больше не появляется окно запроса учетных данных или PIN-кода при доступе к StoreFront или/и к виртуальной машине пользователя.

Список сокращений

ОС — операционная система;

ПО — программное обеспечение;

ПК — персональный компьютер;

AD — active directory;

CA — certification authority;

CMD — command line interpreter;

DC — domain controller;

JC — JaCarta;

MS CA — microsoft certification authority;

HTTP — hyper text transfer protocol;

HTTPS — hyper text transfer protocol secure;

IIS — internet information services;

OU — organizational unit;

PIN — personal identification number;

PKI — public key infrastructure;

SSL — secure sockets layer;

SSO — single sign-on;

XML — eXtensible markup language.

Лист регистрации изменений

Табл. 1 — Регистрация изменений

Версия документа	Изменения
1.0	Исходная версия документа.
1.1	Внесены изменения по аутентификации по смарт-картам.
1.2	Внесены дополнения для сквозной аутентификации по смарт-картам.
1.3	Внесены изменения и корректировки по сквозной аутентификации по смарт-картам.
1.4	Форматирование документа в новом корпаративном шаблоне, вычитка, редактирование.

Телефон: +7 (495) 223-00-01
Факс: +7 (495) 646-64-40
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12
Лицензия ФСБ России № 12632 Н от 20.12.12
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer
Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011