ESMART®

ESMART Token – Citrix XenDesktop

Содержание

1. Общая информация

В руководстве кратко описана настройка Citrix XenDesktop для двухфакторной аутентификации при помощи смарт-карт и USB-ключей ESMART Token и ESMART Token ГОСТ. Процедура аналогична для всех поддерживаемых гипервизоров: VMWare ESX, Hyper-V, XenServer.

Необходимо разрешить передачу данных на портах TCP 80 и 443, а также на портах, которые используют компонент Citrix Licensing Service.

1.1 Тестовая среда

В руководстве описана тестовая среда со следующим программным обеспечением:

Windows Server 2012 – Инфраструктурный сервер Citrix

citrix.esmart.local

- *Director*
- *Delivery Controller*
- *Studio*
- *StoreFront*
- *Licensing Service*
- *SQL Server*

Windows server 2012 – Сервер Active Directory

dc.esmart.local

Также должна быть установлена служба сертификации (Microsoft рекомендует устанавливать)

Windows 7 x64 – Эталонная машина

template.esmart.local

- *Virtual Delivery Agent*
- *Citrix Receiver*
- *ESMART PKI Client*

Windows 7 – Клиент

client.esmart.local

- *Citrix Receiver*
- *ESMART PKI Client*

Установка ESMART PKI Client описана в руководствах на сайте www.esmart.ru.

Установка ПО Citrix Desktop не описана в данном руководстве. Для установки системы следуйте руководствам и рекомендациям с сайта производителя http://docs.citrix.com, в том числе документации на русском языке к версии 7,5: https://docs.citrix.com/ru-ru/xenapp-and-xendesktop/7-5.html Если на серверах установлена операционная система Windows Server 2008 рекомендуется применить патч https://support.microsoft.com/en-us/kb/949538

2. Подготовка инфраструктуры PKI

2.1 Подготовка контроллера домена и центра выдачи сертфиикатов

Инфраструктура для авторизации по смарт-картам в Microsoft Windows предполагает наличие в организации минимум одного контроллера домена и минимум одного центра выдачи сертификатов. Для авторизации в Windows по смарт-картам на доменных устройствах и для авторизации на виртуальных или физических ПК в инфраструктуре Citrix может использоваться одна и та же смарт-карта.

Развертывание домена и установка центра выдачи сертификатов в данном руководстве не описана. Используйте руководства по развертыванию центра сертификации с сайта www.esmart.ru/downloads или руководства от Microsoft.

2.2 Необходимые компоненты

Для авторизации по смарт-картам в инфраструктуре Citrix должны быть выполнены следующие условия:

- *Наличие одного или нескольких контроллеров домена;*
- *Наличие одного или нескольких центров сертификации;*
- *Настроенный шаблон **SmartCard User** (Пользователь со смарт-картой) или **SmartCard Logon** (Вход со смарт-картой);*
- *Смарт-карта или USB-ключ ESMART Token с записанным сертификатом доменного пользователя.*

*Записать сертификат пользователя на смарт-карту можно как с помощью оснастки certmgr.msc, так и с помощью приложения ESMART PKI Client (см. **ESMART PKI Client — Руководство администратора**).*

3. Настройка XML-запросов

На серверах, на которых установлены компоненты ПО Citrix XenDesktop (кроме эталонных серверных ОС) необходимо разрешить выполнение XML-запросов. Для этого в консоль Windows Powershell нужно ввести следующие команды:

```
Set -BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Для проверки вводится команда:

```
Get –BrokerSite
```

Ожидаемый вывод:

```
TrustRequestsSentToTheXmlServicePort : true
```

4. Настройка защищенного соединения

4.1 Настройка IIS для серверов StoreFront

Для серверов, на который установлен компонент Citrix StoreFront необходимо настроить защищенное соединение по протоколу HTTPS. Для защищенного соединения используется серверная роль Internet Information Services (Microsoft IIS).

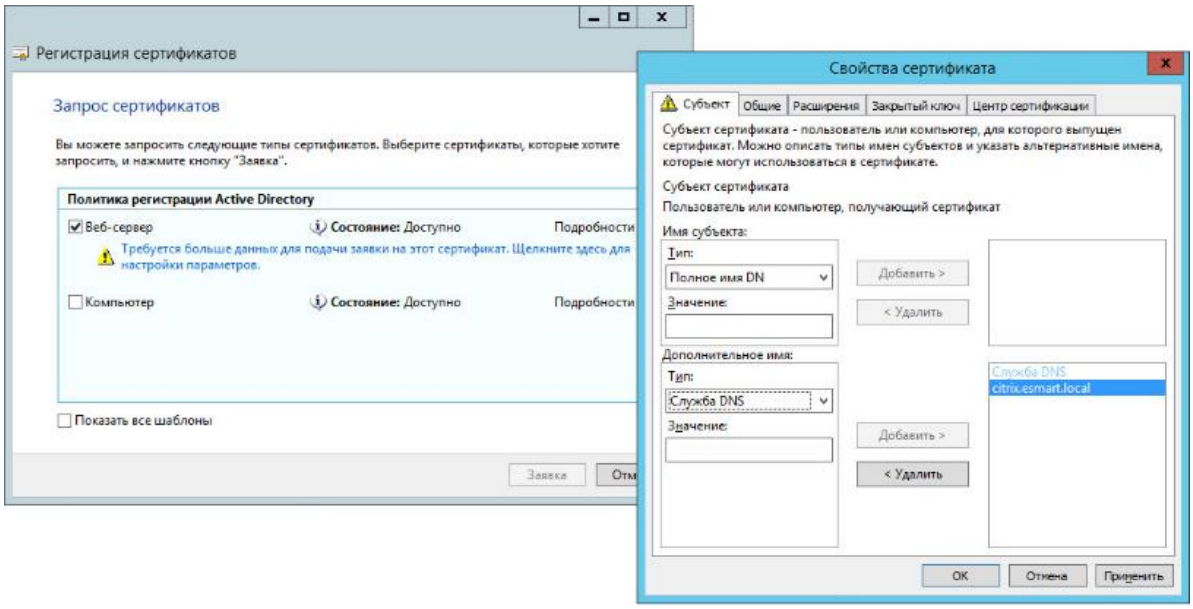
4.2 Получение сертификата web-сервера

Сертификат веб-сервера можно получить методом, описанным ниже, или с помощью раздела панели управления IIS – Управление сертификатами.

Чтобы получить сертификат сервера, откройте консоль MMCи добавьте оснастку Сертификаты › Для учетной записи компьютера › Локальный компьютер или Другой компьютер.

В оснастке Сертификаты перейдите в раздел: Личное › Сертификаты. В верхнем меню выберите Действие › Все задачи › Запросить новый сертификат.

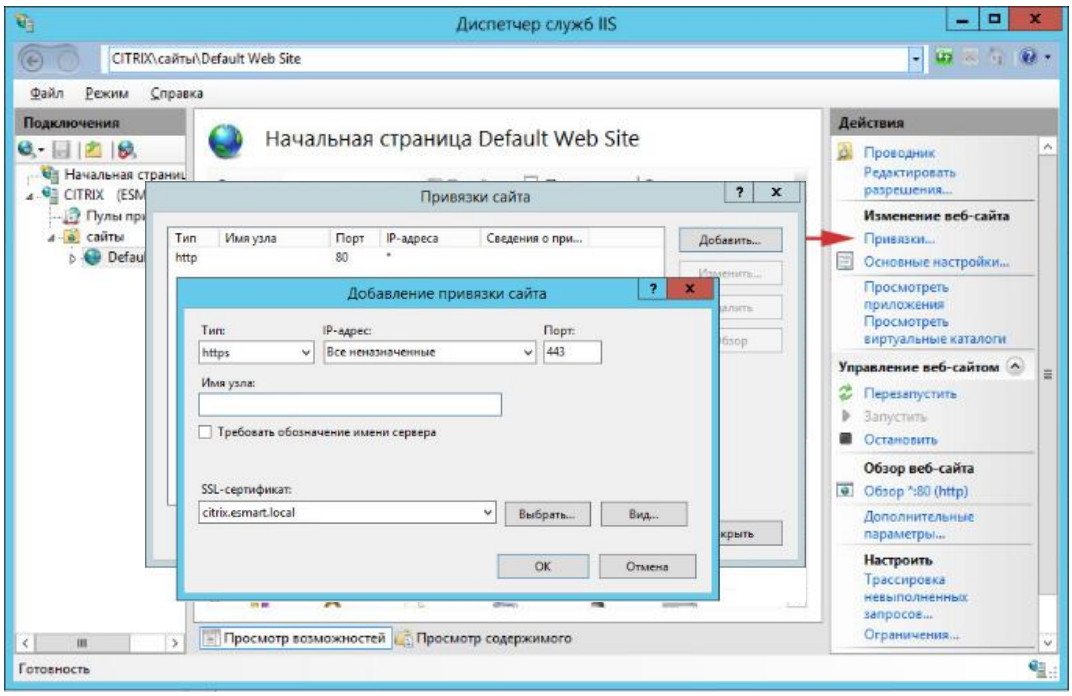
Следуя подсказкам мастера выдачи сертификатов перейдите к окну выбора шаблонов и отметьте шаблон сертификата Веб-сервер. Задайте требуемые параметры сертификата: Служба DNS: DNS-имя сервера StoreFront (в примере citrix.esmart.local).

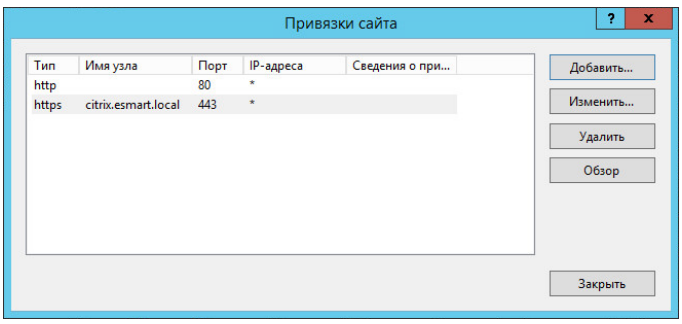


Дождитесь сообщения об успешной выдаче сертификата. Полученный сертификат сервера появится в оснастке Сертификаты консоли MMC.

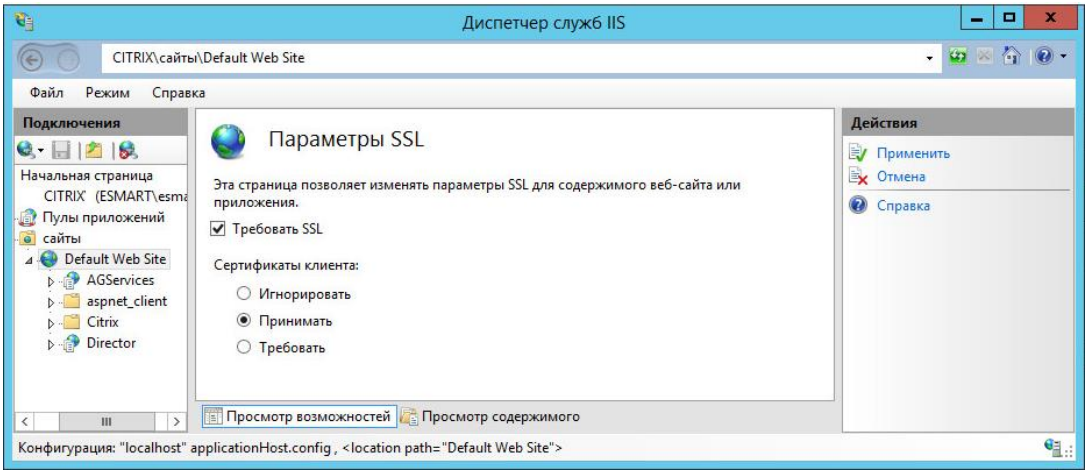
4.3 Привязка сертификата к IIS

Откройте Диспетчер серверов и выберите роль IIS. В настройках Default Web Site выберите Привязки...





После выполнения привязки необходимо отметить опцию Требовать SSL в разделе Параметры SSL.



5. Настройка методов авторизации

5.1 Предварительные этапы

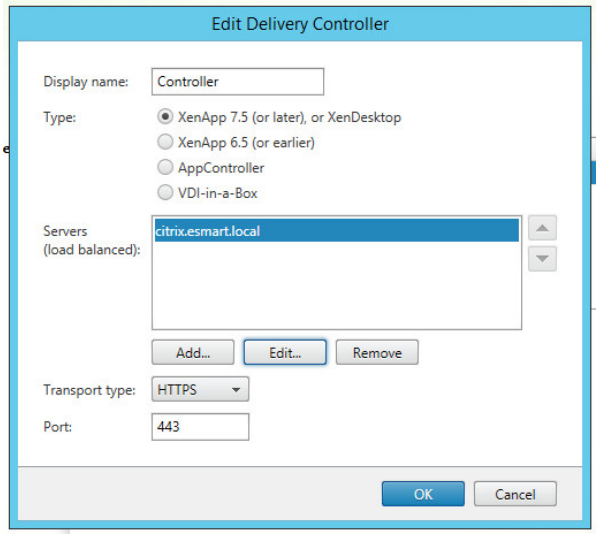
Предварительно требуется создать и настроить в Citrix Studio:

- *Machine Catalog (в примере MC1);*
- *Delivery Group (в примере DG1).*

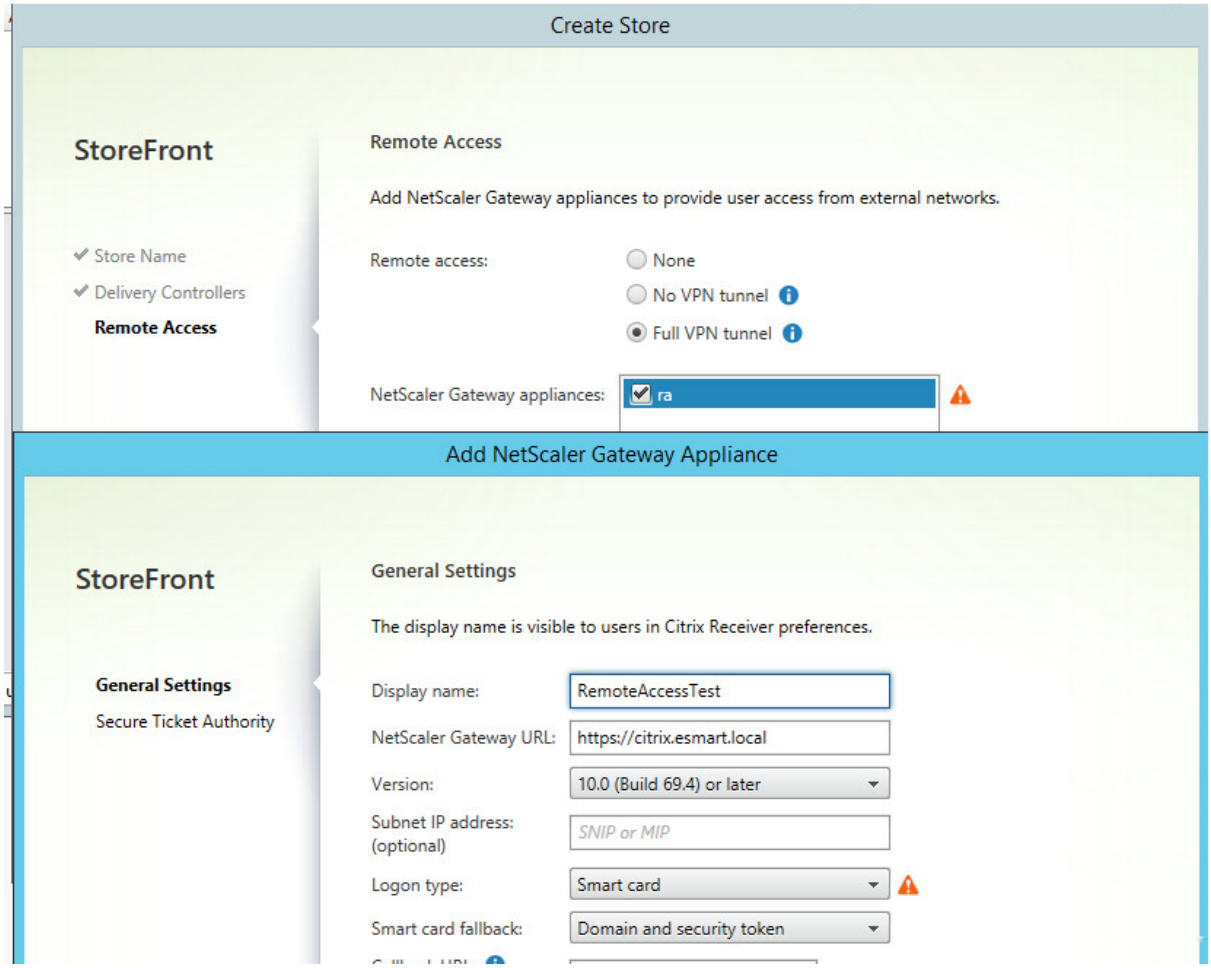
Для Delivery Group должен быть назначен по крайней мере один StoreFront сервер и создан тип Store.

5.2 Создание объекта Citrix Store

В оснастке Citrix StoreFront перейдите на вкладку Stores. Начните создание нового объекта Store. Задайте его имя и перейдите к добавлению Delivery Controller. В типе транспорта укажите HTTPS и номер порта 443. Добавьте в список серверы, на которые установлен компонент Delivery Controller.

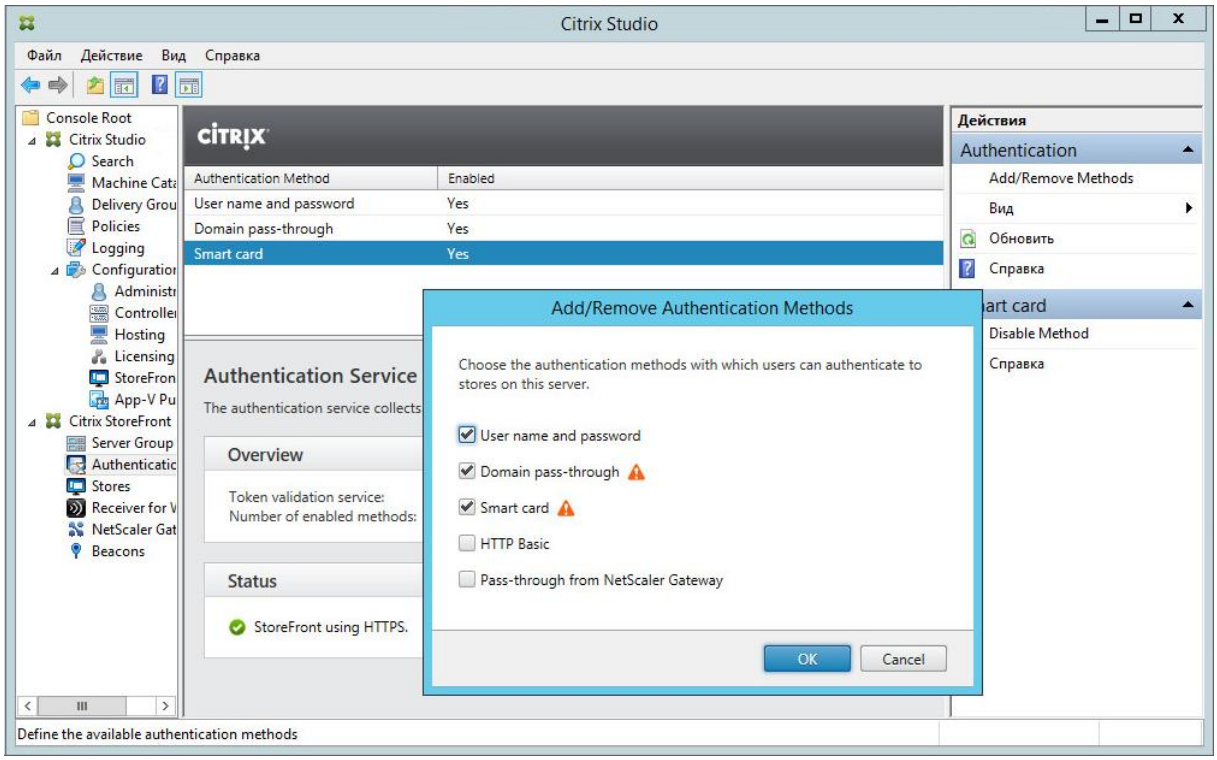


При необходимости добавьте шлюз NetScaler Gateway для удаленного доступа (с использованием VPN-соединения или без). В настройках NetScaler Gateway можно указать первичную авторизацию по смарт-картам и вторичную авторизацию, например, по логину и паролю (как показано на рисунке).



5.3 Настройка StoreFront

Для аутентификации по смарт-картам необходимо включить данный метод в оснастке управления компонентом StoreFront. Отметьте опцию Smart Card и Domain pass-through. Остальные настройки устанавливаются в соответствии с корпоративными требованиями.



При настройке инфраструктуры, содержащей несколько серверных групп StoreFront, необходимо следовать рекомендациям Citrix (http://support.citrix.com/proddocs/topic/dws-storefront-21/dws-configure-server-group.html)

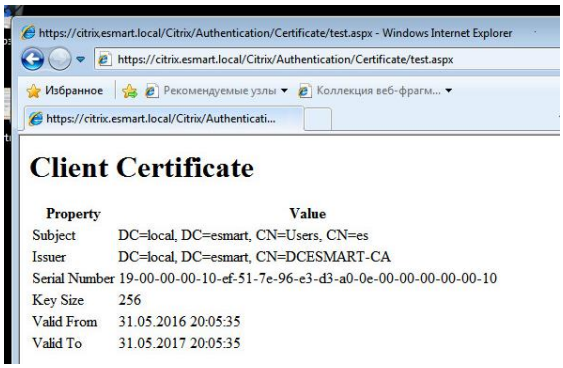
5.4 Проверка аутентификации по сертификатам

Подключите к клиентскому компьютеру считыватель со смарт-картой или USB-токен ESMART Token, на который записан доменный сертификат пользователя для авторизации в Windows. Для проверки настройки безопасного соединения по смарт-картам, перейдите в браузере Internet Explorer на следующий адрес:

*https://**storefront-name**/Citrix/Authentication/Certificate/test.aspx, например:*

https://citrix.esmart.local/Citrix/Authentication/Certificate/test.aspx

При переходе по данной ссылке будет запрошен сертификат пользователя. Выберите сертификат, записанный на смарт-карту и введите ПИН-смарт-карты. Если авторизация прошла успешно, на странице будут показаны параметры сертификата пользователя на смарт-карте.

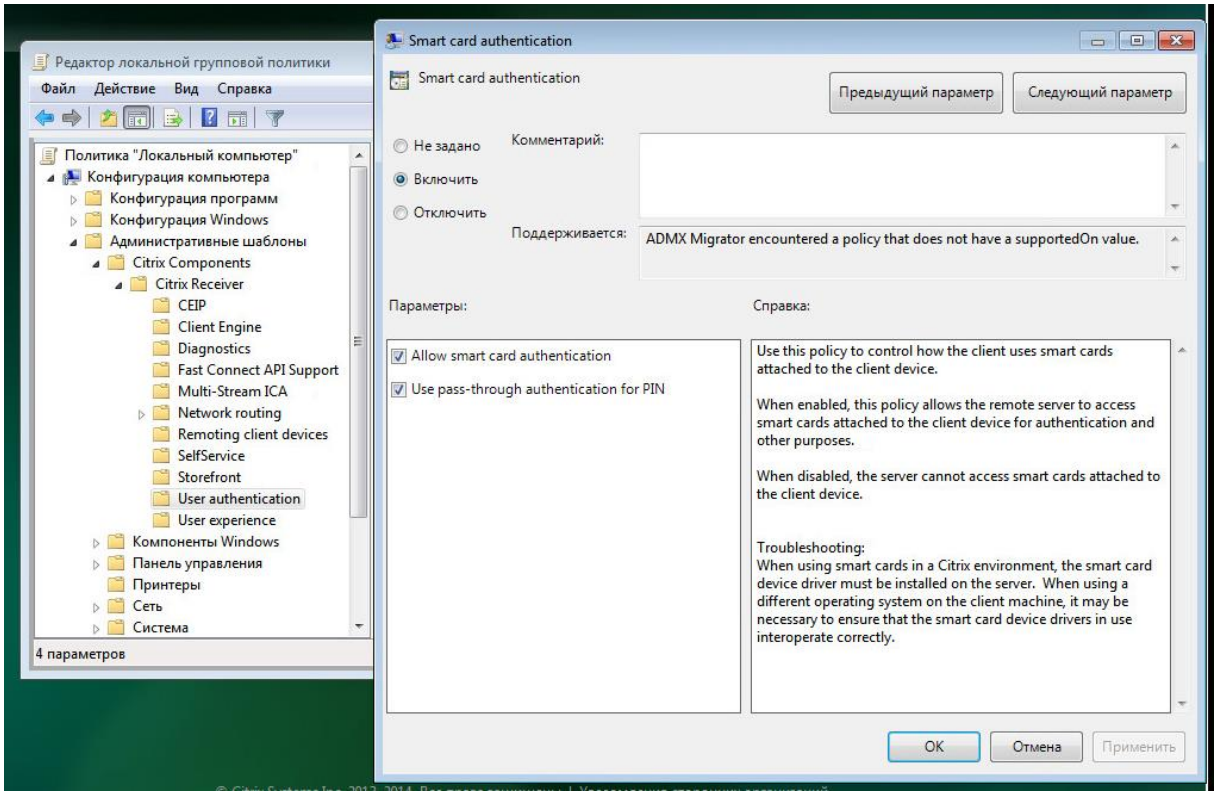


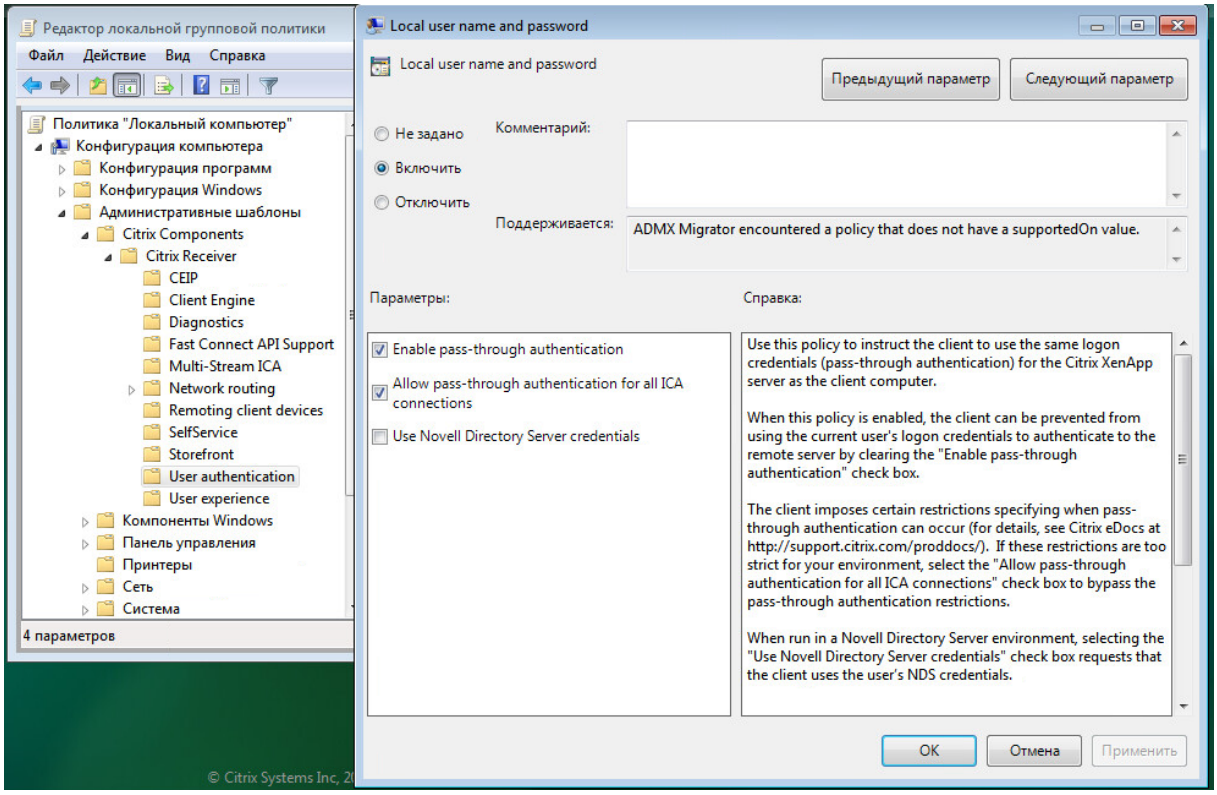
6. Групповые политики

На клиентские машины требуется распространить групповые политики Citrix. Файл шаблона находится в директории

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

Рекомендуется распространение через доменные групповые политики, но допускается и изменение локальных групповых политик.





7. Подготовка клиентских машин

7.1 Проверка авторизации через Web-интерфейс

Проверьте возможность авторизации по картам через Web-интерфейс (в браузере должно быть разрешено выполнение JavaScript):

*https:// **StoreFrontServer**/Citrix/**Storename**Web*

в примере

https://citrix.esmart.local/Citrix /ESMARTauthStoreWeb

Добавьте серверы StoreFront в настройках браузера Internet Explorer в категорию Local Zone или Trusted Zone.

7.2 Получение профиля для Citrix Receiver и авторизация

Установите Citrix Receiver на клиентский ПК. Рекомендуется установка с опцией /includeSSON AM_SMARTCARDPINENTRY=CSP

D:\Installers\CitrixReceiver.exe /includeSSON AM_SMARTCARDPINENTRY=CSP

Профиль для настройки Citrix Receiver можно получить через web-интерфейс, описанный выше. В правом верхнем углу web-страницы нажмите на имя пользователя и выберите опцию Активировать. Полученный файл будет автоматически ассоциирован с приложением Citrix Receiver. При открытии Citrix Receiver проверьте и подтвердите доверие к серверу Citrix. Запустите или перезапустите приложение Citrix Receiver. Авторизуйтесь с помощью смарт-карты на доступном рабочем столе.