



JaCarta PKI и VMware View 5.x, сертифицированный по ФСТЭК России

Руководство по настройке

Листов: 22

Автор: Dmitry Shuralev

Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации в **VDI-сессии**, а также в административный интерфейс **VMware View 5.x (сертифицированный по требованиям ФСТЭК России)** с использованием электронных ключей **JaCarta PKI** и вспомогательного программного обеспечения "Единый Клиент JaCarta".

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация Apple Inc. Владельцем товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владельцем товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Оглавление

О платформе VMware View	4
Описание демо-стенда	4
Ход настройки	4
Замена сертификата View Connection Server	5
Подготовка шаблона сертификата	5
Выдача сертификата для View Connection Server	7
Замена сертификата, используемого View Connection Server для SSL-соединения	10
Добавление ключей и корневого сертификата в Truststore сервера	13
Настройка View Connection Server	15
Настройка проброса смарт-карты пользователя	18
Проверка работоспособности	19
Контакты, техническая поддержка	20
Регистрация изменений	21


О платформе VMware View

VMware View — продукт для виртуализации персональных компьютеров от VMware, Inc. Первые версии (2.0.0 и 2.1.0) продавались под именем VMware VDI, однако, начиная с версии 3.0.0, имя было изменено на VMware View. Начиная с версии 5.2, стал частью VMware Horizon Suite и получил название VMware Horizon View. Версия 5.1 имеет сертификацию, согласно требованиям **ФСТЭК России**.

Описание демо-стенда


Серверная часть

- VMware Hypervisor (ESXi) – физический сервер с установленным гипервизором – VMware ESXi, на котором hostятся виртуальные машины.
 - Microsoft Windows Server 2012 R2 — сервер с ролью контроллера домена (Domain Controller) и центра сертификации (Certification Authority)
 - Microsoft Windows Server 2012 R2 — сервер с установленным vCenter Server для управления всей виртуальной инфраструктурой
 - Microsoft Windows Server 2012 R2 — View Connection Server – сервер управления инфраструктурой виртуальных рабочих столов. Управляет подключениями к виртуальным рабочим столам, созданием и мониторингом пулов десктопов.

 На каждом сервере должен быть установлен набор драйверов и утилит управления электронными ключами JaCarta PKI: JC-Client 6.32 и выше или "Единый Клиент JaCarta" 2.10 и выше.

Клиентская часть

- Microsoft Windows 7x64 — ПК пользователя, с которого будет осуществляться аутентификация в VMware View.

 На каждом клиентском устройстве должен быть установлен набор драйверов и утилит управления электронными ключами JaCarta PKI: JC-Client 6.32 и выше или "Единый Клиент JaCarta" 2.10 и выше.

Ход настройки

Настоящая инструкция описывает добавление дополнительного способа аутентификации в уже настроенную на парольную аутентификацию VDI-инфраструктуру VMware View по цифровым сертификатам, находящимся на смарт-картах или USB-токенах JaCarta. Это в свою очередь предполагает, что инфраструктура VMware View, а также vCenter уже развёрнуты, также настроен домен контроллер (Active Directory) и центр сертификации (Certification Authority), а у пользователей имеются электронные ключи JaCarta с выпущенными на них цифровыми сертификатами.

Для того чтобы реализовать аутентификацию по смарт-картам или USB-токенам в VMware View, необходимо выполнить следующие действия:

- заменить сертификат, который используется для SSL-соединения между клиентом и View Connection Server;
- добавить корневой сертификат вашего центра сертификации в файл Truststore сервера;
- произвести настройку View Connection Server.

Замена сертификата View Connection Server

Замена сертификата View Connection Server включает ряд действий.

1. Подготовка шаблона сертификата для View Connection Server.
2. Выдача сертификата для View Connection Server.
3. Замена сертификата, используемого View Connection Server для SSL-соединения.

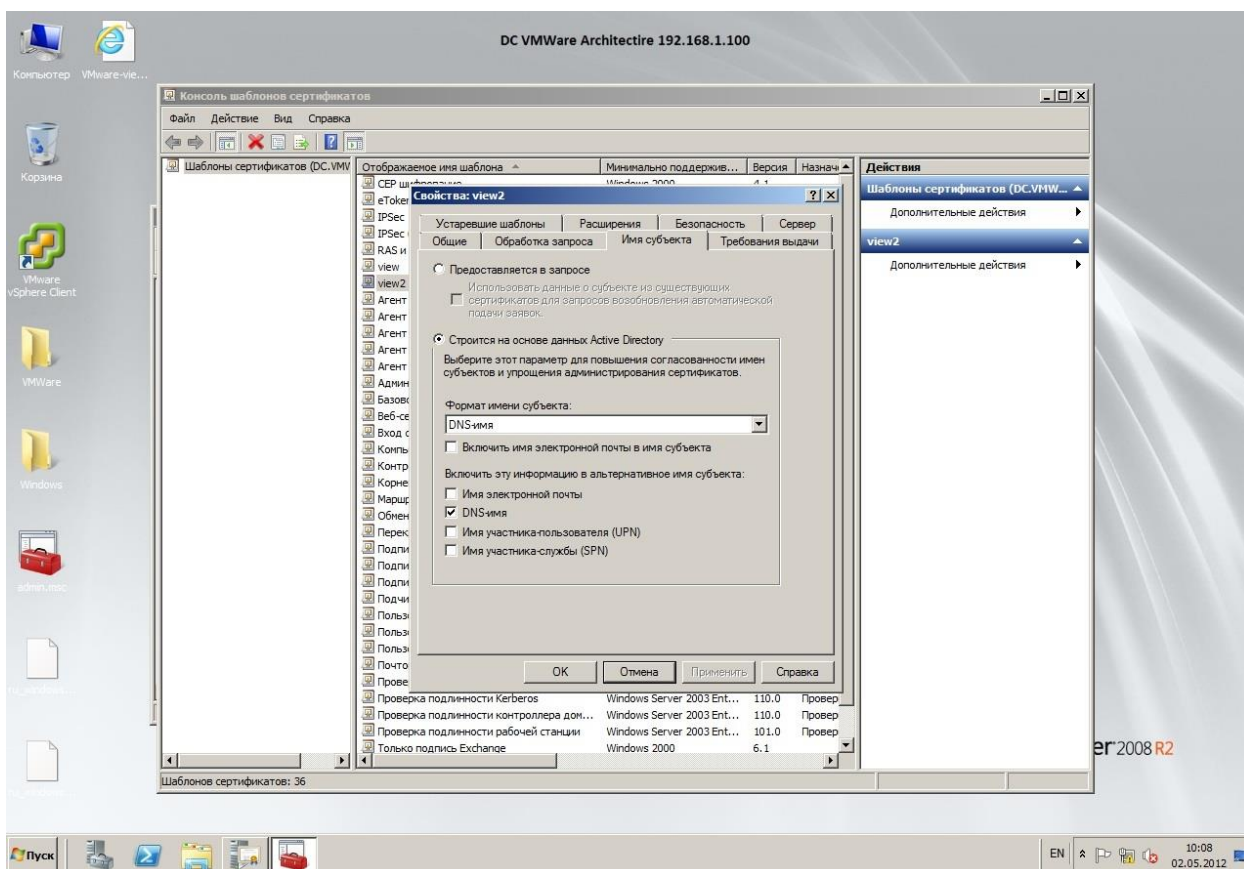
Подготовка шаблона сертификата

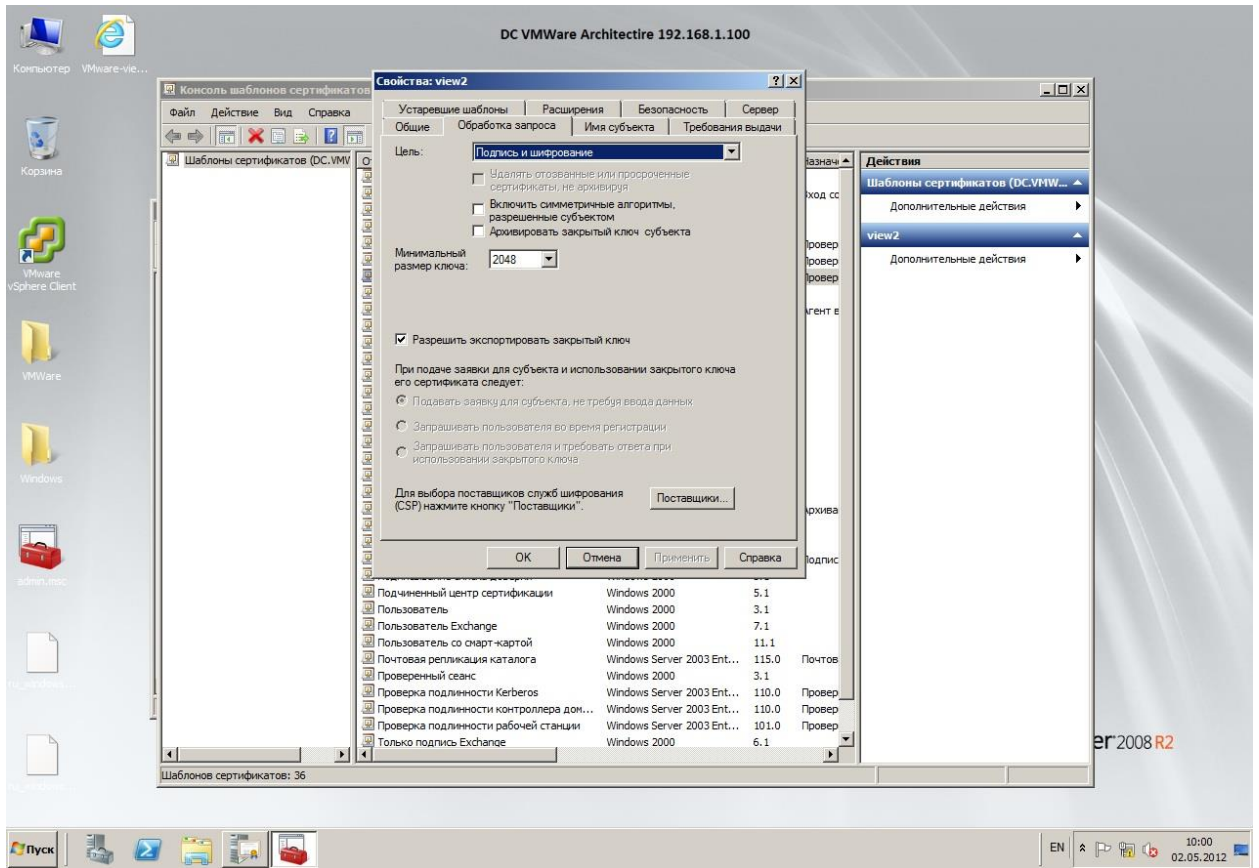
Запустите оснастку Центр сертификации **Пуск -> Администрирование -> Центр сертификации**.

В открывшемся окне выберите ЦС, далее щёлкните правой кнопкой на вкладке Шаблоны сертификатов, выберите пункт Управление. Щёлкните правой кнопкой на шаблоне **Компьютер -> Скопировать шаблон**.

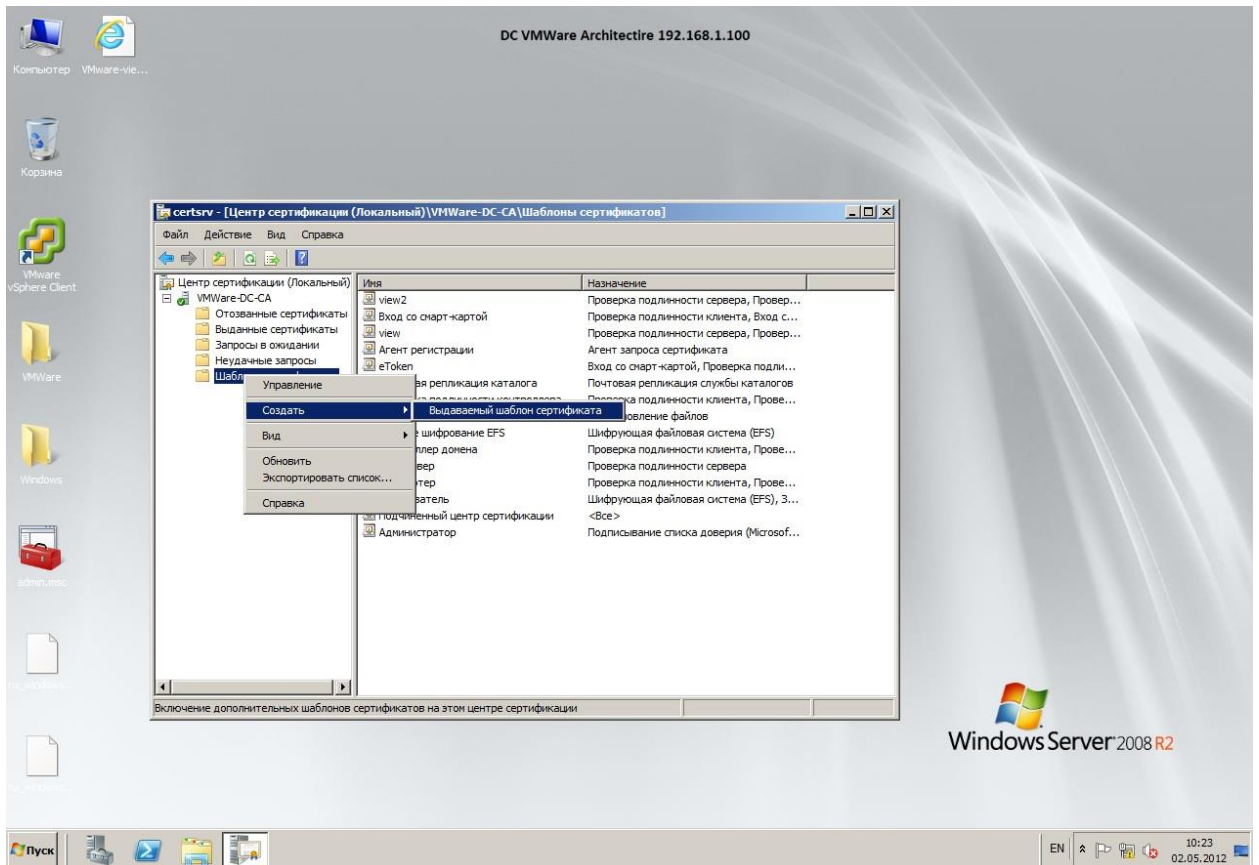
В копии шаблона установите галочку на **Разрешать экспортировать закрытый ключ** и выберите в качестве формата имени субъекта DNS-имя.

Сохраните шаблон.



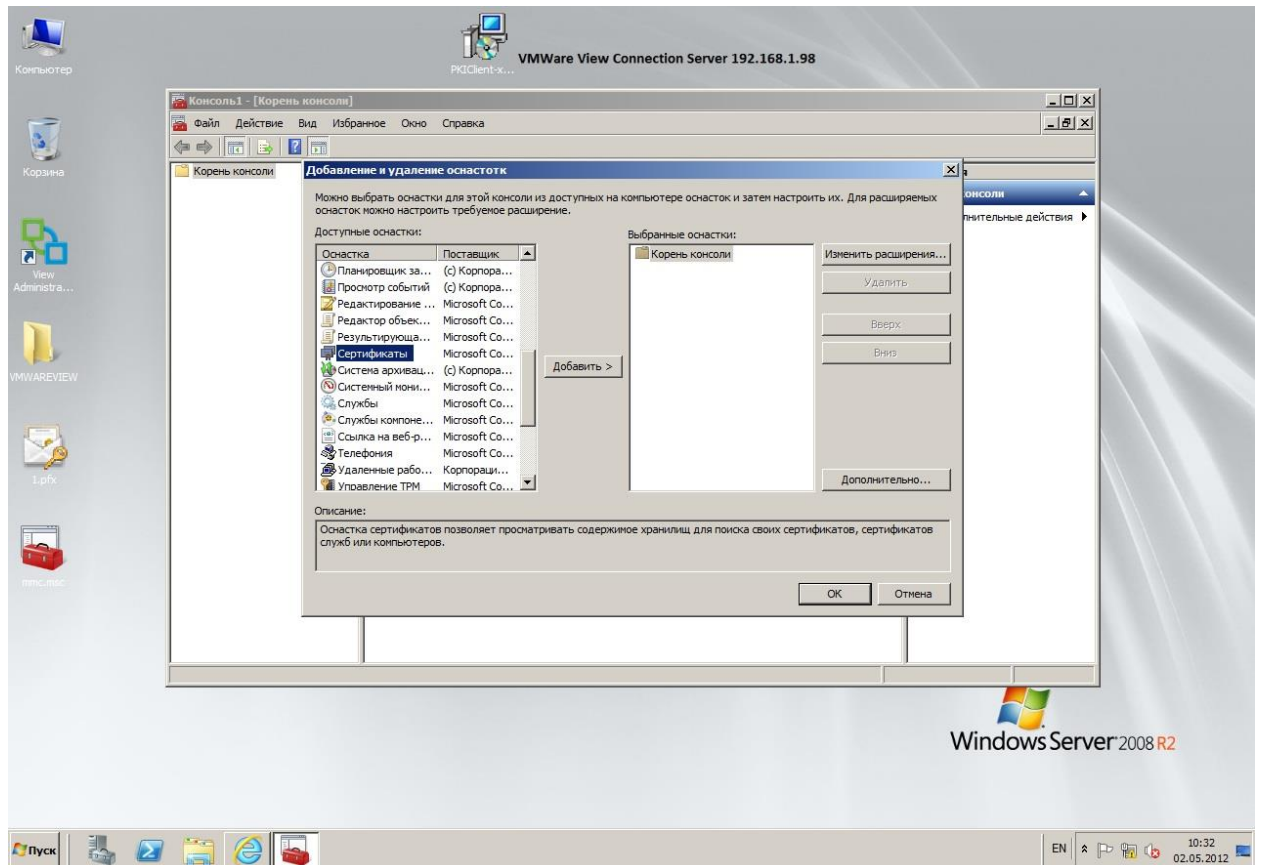


Закройте окно управления шаблонами сертификатов. Щёлкните правой кнопкой на вкладке **Шаблоны сертификатов** -> **Создать** -> **Выдаваемый шаблон сертификата**, в открывшемся меню выберите необходимый шаблон и нажмите **Ок**. Этим действием шаблон будет разрешён к выдаче. На этом подготовка шаблона сертификата закончена.

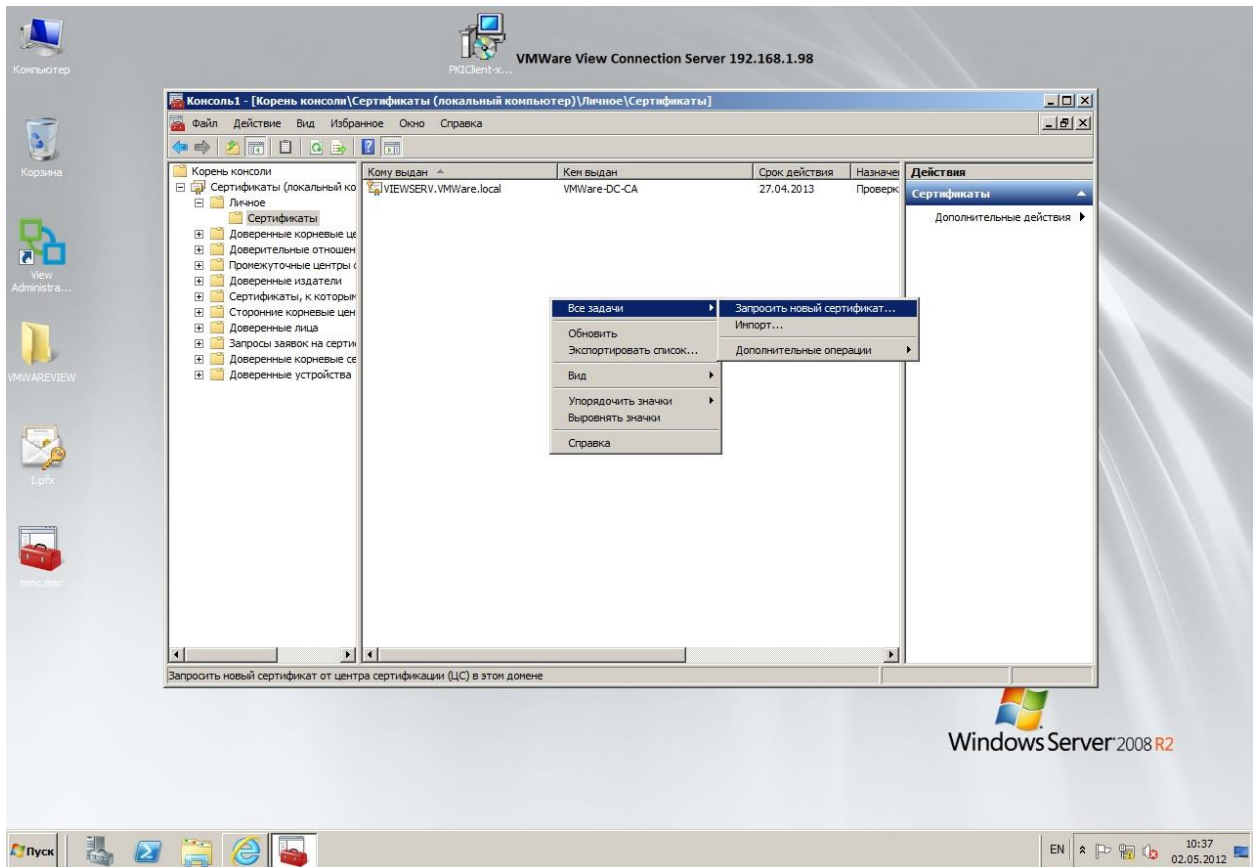


Выдача сертификата для View Connection Server

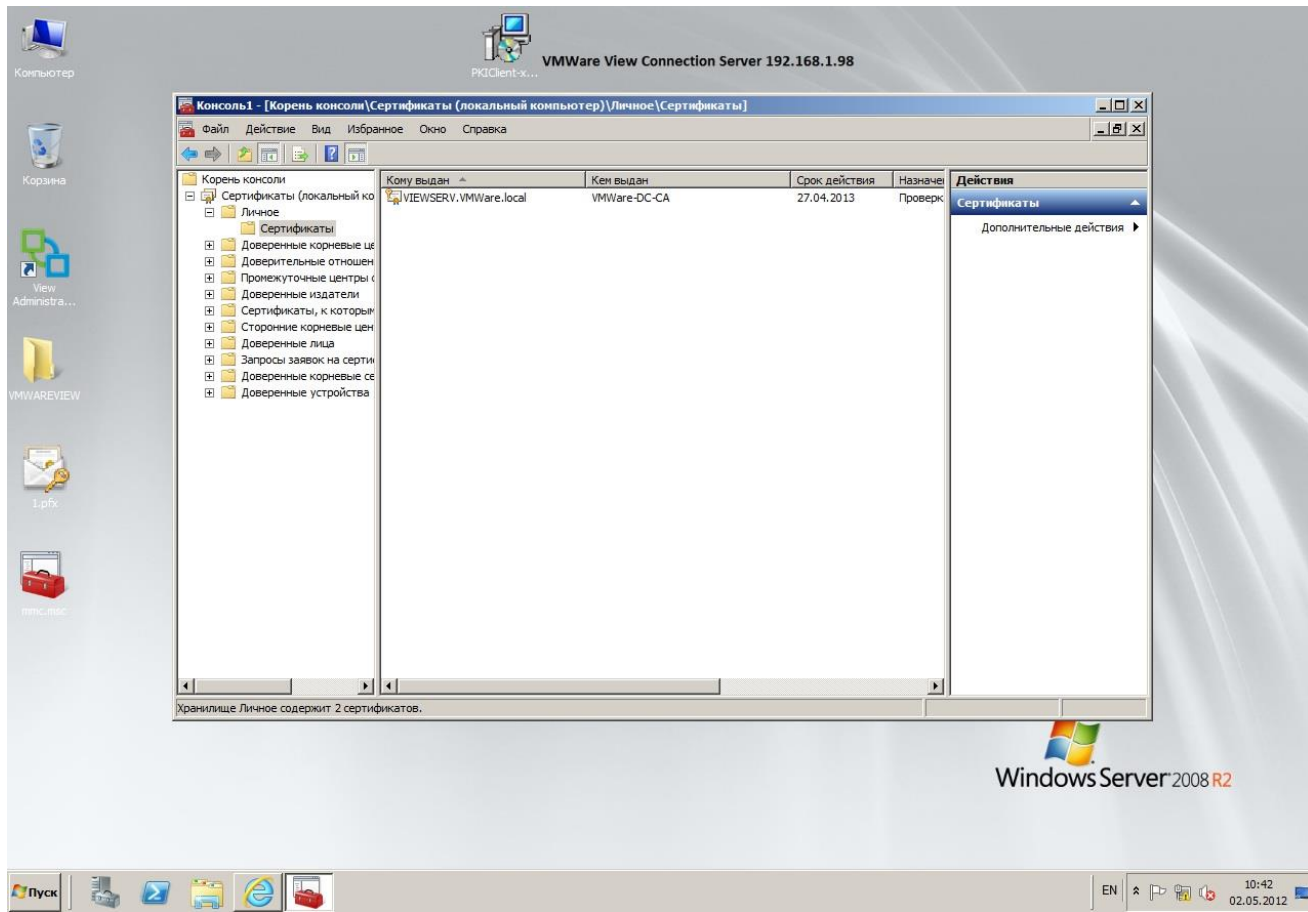
Запустите консоль mmc, нажмите **Файл -> Добавить или удалить оснастку**, дважды щёлкните на **Сертификаты**, в появившемся окне выберите пункт **Учётной записи компьютера -> Далее -> Готово -> ОК**.



В открывшемся окне выберите вкладку **Сертификаты** -> **Личное** -> **Сертификаты**, далее щёлкните правой кнопкой пункт **Все задачи**, нажмите **Запросить новый сертификат** -> **Далее** -> **Далее** -> **Выберите свой шаблон** -> **Заявка**.

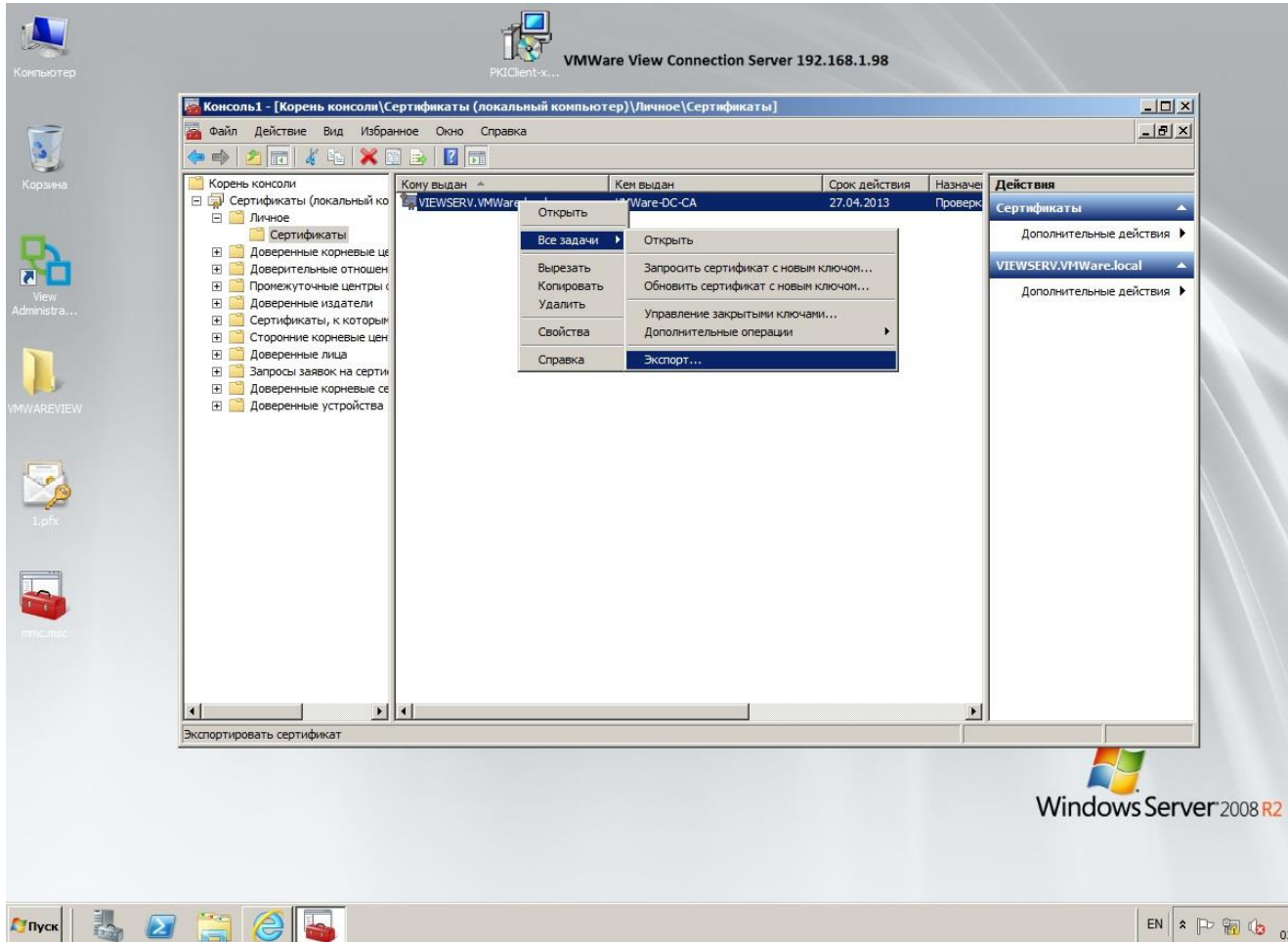


Убедитесь в том, что в консоли появился выданный сертификат.

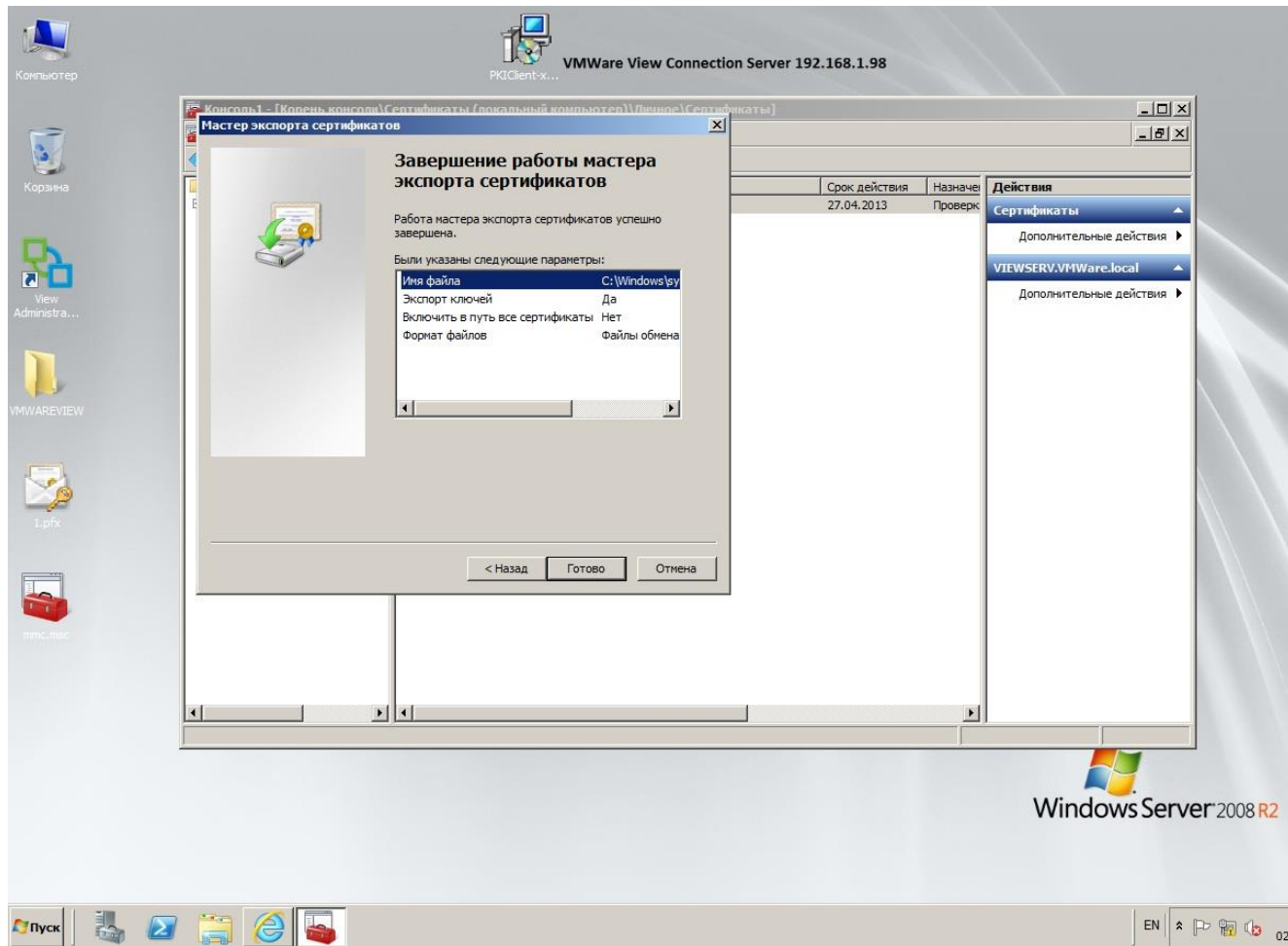


Замена сертификата, используемого View Connection Server для SSL-соединения

Прежде чем производить замену сертификата, его необходимо экспортировать в формате **.pfx**, для этого щёлкните правой кнопкой на выданном сертификате, далее **Все задачи -> Экспорт**.



В открывшемся мастере экспорта сертификатов нажмите **Далее**, на следующей вкладке выберите **Да, экспортировать закрытый ключ** -> **Далее** -> **Далее**, задайте пароль для экспортируемого сертификата -> укажите директорию для создания файла сертификата и его имя -> **Далее** -> **Готово**.



В результате получится файл в формате **.pfx**, содержащий сертификат для замены. После того, как файл сертификата подготовлен, необходимо поместить его в директорию:

C:\Program Files\VMware\VMware View\Server\sslgateway\conf

В этой же директории создайте файл **locked.properties** и в нём укажите следующее:

keyfile=<имя файла>.pfx

keypass=<пароль, указанный при экспорте>

Далее перезапустите службу View Connection Server. Для того чтобы убедиться в том, что служба запущена, и используется именно ваш сертификат, можно посмотреть лог в папке

C:\ProgramData\VMware\VDM\logs\

```

log-2012-04-26.txt — Блокнот
Файл Правка Формат Вид Справка
NFO <Thread-1> [Ice] The Secure Gateway Server will be accessed using URL https://viewServ.VMware.local:443
NFO <Thread-1> [Ice] The PCoIP Secure Gateway will be accessed through 192.168.1.98:4172?4172
NFO <Thread-1> [ab] Setting data frame policy to NEGOTIATE
NFO <Thread-1> [ab] Setting chunk window to 4
NFO <Thread-1> [bn] Setting tailorsBuffers to true, monitorFlow to false, hysteresis to true
ARN <Thread-1> [ah] Failed to determine message security mode, setting to OFF. Invalid value: null
NFO <ws_tomcat-service_init> [AdminUIListener] Initialized standalone WinAuth successfully, my SID is S-1-5-18
NFO <2984> [ws_java_bridgeDLL] JavaBridge installed service AdminBackendService
NFO <ws_tomcat-service_init> [TrackerManager] joining tracker cluster...
NFO <ws_tomcat-service_init> [TrackerManager] joined as first node in the cluster. Ready.
NFO <ws_tomcat-service_init> [BrokerLifecycle] Node has joined cluster
NFO <DesktopControlSessions> [DesktopTracker] Session reader loop configuration: SESSION_POLL=30000ms, SESSION_LIST.
NFO <DesktopControlLdap> [DesktopTracker] LDAP notification configuration: MaxLDAPNotificationsOutstanding=10000, LI
NFO <ws_tomcat-service_init> [EventForwarderHandler] Starting forwarder for ViewDatabaseEventForwarder
NFO <ws_tomcat-service_init> [MaxSessionTaskFactory] MaxSessionTaskFactory was created for the first time on this cl
ARN <EventForwarderHandler-1335416906076> [DatabaseForwarder] No Events Databases specified in ADAM, will not store
NFO <2684> [ws_java_bridgeDLL] JavaBridge installed service JAdmin
NFO <2780> [ws_java_bridgeDLL] JavaBridge installed service PowershellService
NFO <ws_tomcat-service_init> [UserContext] Allow Kerberos logins = true
NFO <Thread-1> [m] The Secure Gateway Server is using SSL certificate store 1.pfx with password of 4 characters
NFO <ws_tomcat-service_init> [CertificateAuthFilter] Smart Card Authentication mode: REQUIRED
NFO <Thread-1> [m] The Secure Gateway Server is listening on https://*:443
NFO <FrontRedirect> [d] AJP services are now ready.
NFO <FrontRedirect> [Processor] Logging HTTP processor installed
NFO <Front> [d] AJP services are now ready.
NFO <Front> [d] Smart Card/Certificate Authentication will not be used as usecertAuth is false
NFO <Poolwatcher> [ApplicationProvisioningManager] Initializing Application Provisioning Manager for node:viewServ
NFO <AppProvisioningManager> [ApplicationProvisioningManager] Application Provisioning Manager started
NFO <Poolwatcher> [VirtualCenterDriver] Setting VC Poll Delay to 60000 ms
NFO <Poolwatcher> [VirtualCenterDriver] Setting VC Resubmit Delay to 20000 ms
NFO <Poolwatcher> [VirtualCenterDriver] Setting Missing VM Scan Delay to 600000 ms
NFO <DesktopControlSessions> [DesktopTracker] Using new agent messaging mode.
ARN <Tracker:PulseTimer> [TrackerManager] (viewServ) Pulse 29: delay 4841 DELAYED
RROR <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to virtualCen
ARN <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with VC <ht
RROR <VCC-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to VirtualCen
RROR <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to virtualCen
ARN <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with VC <ht
RROR <VCC-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to VirtualCen
RROR <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to virtualCen
ARN <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with VC <ht
RROR <VCC-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to VirtualCen
NFO <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [VirtualCenterDriver] validating vms
NFO <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [VirtualCenterDriver] Finished validating vms
NFO <MissingVMScanner-6a63102e-6efa-441d-b177-3f1dc351881a> [VirtualCenterDriver] Scanner started
ARN <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Failed to refresh datastore with
ARN <VirtualCenterDriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Failed to refresh datastore with
  
```

Теперь SSL-соединение строится с использованием этого сертификата.

Добавление ключей и корневого сертификата в Truststore сервера

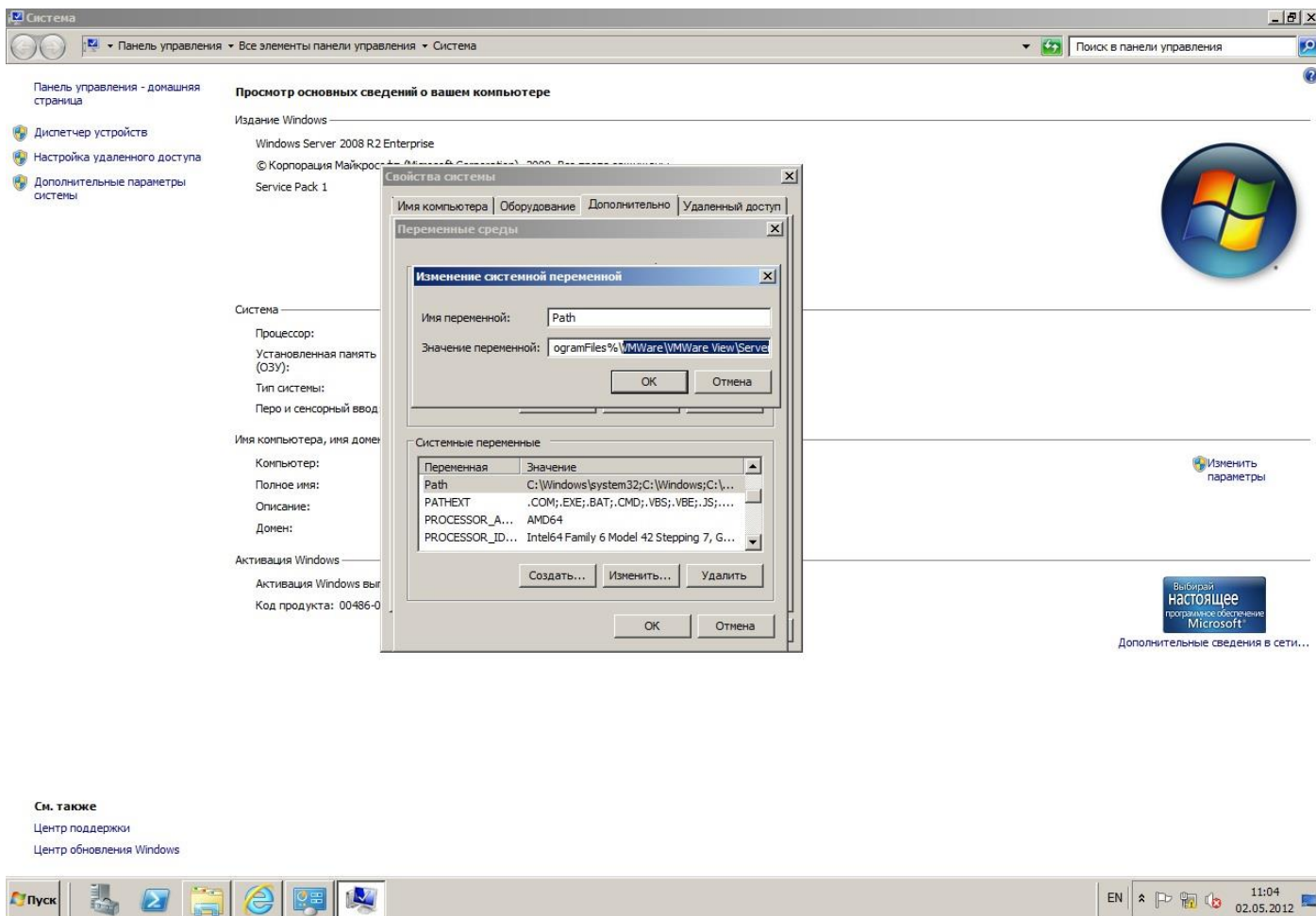
Далее необходимо настроить доверие сервера VMware View, т.е. определить, кому можно доверять при аутентификации по сертификатам, хранимым на смарт-картах или USB-токенах. Для этого нужно:

- создать файл Truststore – хранилище ключей;
- разрешить Smart Card Logon в настройках View Connection Server.

Для того чтобы создать файл Truststore, можно воспользоваться утилитой keytool из Java Runtime Environment (JRE), которая устанавливается с VMware View, но, чтобы было удобно воспользоваться ею из командной строки, нужно добавить путь к файлам Java в переменные окружения сервера.

Откройте **Свойства компьютера** -> **Дополнительные параметры системы** -> **Дополнительно** -> **Переменные среды** -> в системной переменной Path, в конце строки добавьте:


;%ProgramFiles%\VMware\VMware View\Server\jre\bin



По аналогии с экспортом сертификата View Connection Server, описанным выше, произведите экспорт корневого сертификата вашего ЦС. А полученный сертификат в формате **.cer** добавьте в хранилище ключей View Connection Server. Для этого откройте командную строку **Пуск** -> **Выполнить** -> **cmd.exe**. Далее перейдите в каталог **C:\Program Files\VMware\VMware View\Server\sslgateway\conf**

и задайте следующую команду:

```
keytool -import -alias <Псевдоним_по_желанию> -file <Файл_сертификата>  
-keystore <Имя_файла_хранилища>
```

 Пример команды: `keytool -import -alias alias -file CA.cer -keystore truststorefile.key`

В процессе импорта необходимо будет ввести парольную фразу для защиты хранилища и подтвердить доверие сертификату.

Теперь добавьте в уже созданный ранее файл `locked.properties` следующие строчки:

```
trustKeyfile=<Имя_файла_хранилища>  
trustStoretype=JKS  
useCertAuth=true
```


 Пример: `trustKeyfile= truststorefile.key`

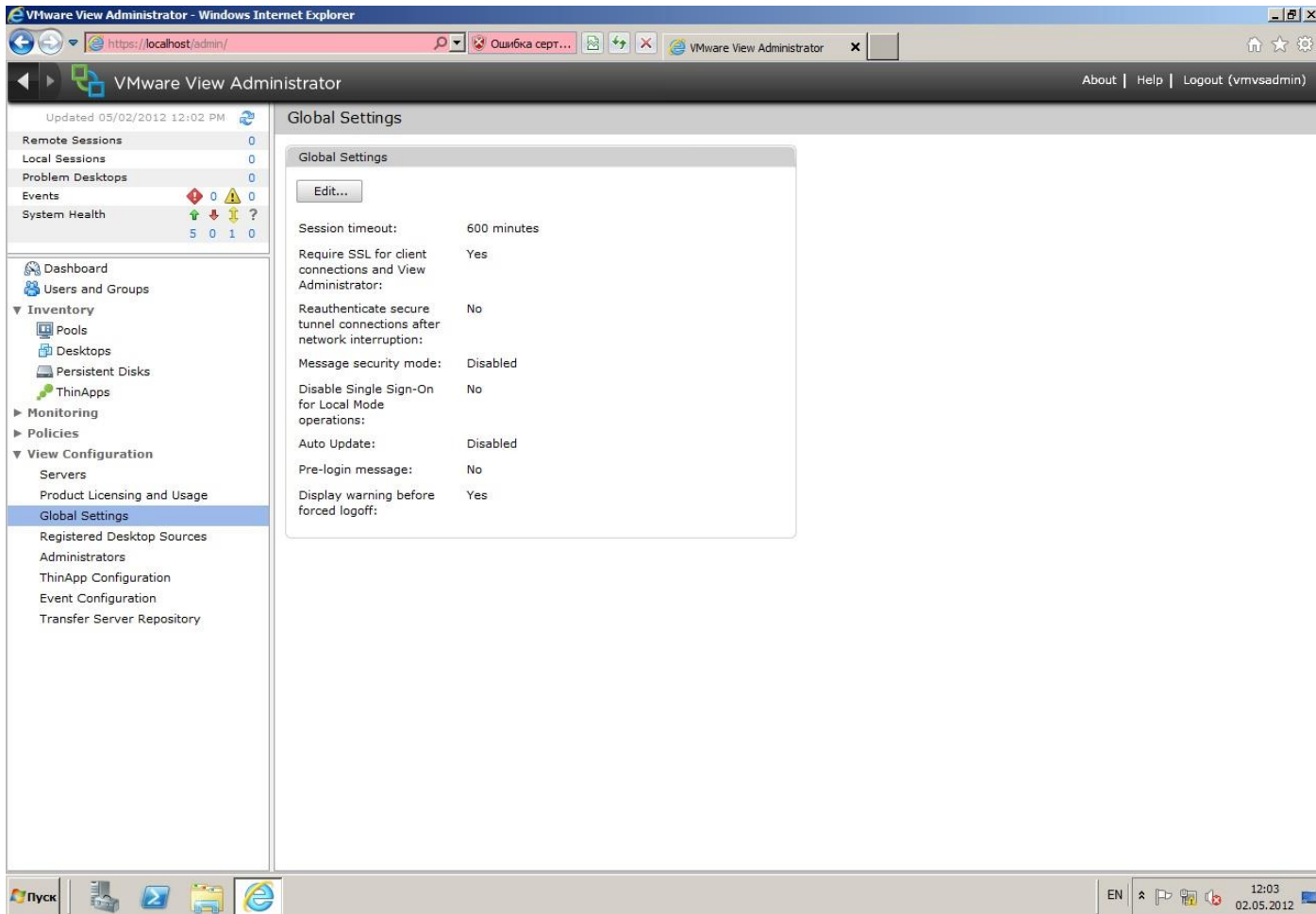
```
trustStoretype=JKS
```

```
useCertAuth=true
```

Настройка View Connection Server

Необходимо включить функции Smart Card Logon в настройках View Connection Server.

 Прежде чем включать аутентификацию по смарт-картам, убедитесь в том, что в глобальных настройках View Connection Server установлен флаг "Require SSL for client connections and View Administrator".



The screenshot shows the VMware View Administrator web interface in Internet Explorer. The browser address bar shows <https://localhost/admin/>. The page title is "VMware View Administrator". The left sidebar contains a navigation menu with the following items: Dashboard, Users and Groups, Inventory (Pools, Desktops, Persistent Disks, ThinApps), Monitoring, Policies, and View Configuration (Servers, Product Licensing and Usage, Global Settings, Registered Desktop Sources, Administrators, ThinApp Configuration, Event Configuration, Transfer Server Repository). The "Global Settings" page is displayed, showing a list of configuration options:

Setting	Value
Session timeout:	600 minutes
Require SSL for client connections and View Administrator:	Yes
Reauthenticate secure tunnel connections after network interruption:	No
Message security mode:	Disabled
Disable Single Sign-On for Local Mode operations:	No
Auto Update:	Disabled
Pre-login message:	No
Display warning before forced logoff:	Yes

The Windows taskbar at the bottom shows the Start button, several application icons, and the system tray with the date "02.05.2012" and time "12:03".

Зайдите в Web-консоль VMware View.

Перейдите во **View Configuration** → **Servers** → **Connections Servers** → **Edit**.

The screenshot displays the VMware View Administrator web interface in Internet Explorer. The browser address bar shows <https://localhost/admin/>. The page title is "VMware View Administrator".

Servers

vCenter Servers

Buttons: Add..., Edit..., Remove

vCenter Server
192.168.1.99(vmwadmin)

Security Servers

Buttons: Edit..., Remove

Security Server	Version	PCoIP	Connection Server

View Connection Servers

Buttons: Enable, Disable, Edit..., Backup Now..., More Commands

View Connection Server	Version	PCoIP	State	Settings	Last Backup
VIEWSERV	5.0.0-48167	Secure Gateway installed	Enabled	Secure tunnel connection, Sm	

Transfer Servers

Transfer Server Repository: Not Configured

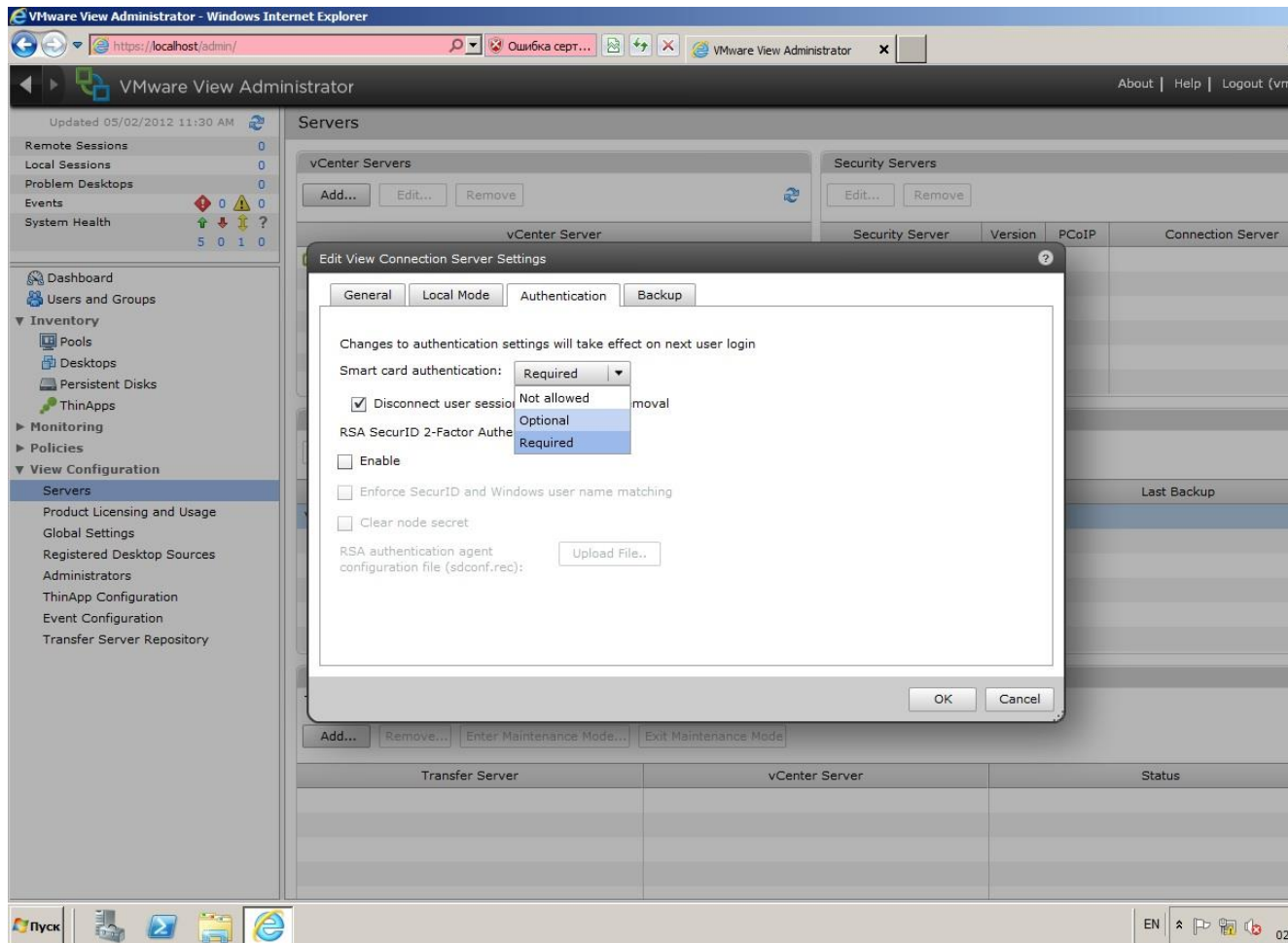
Buttons: Add..., Remove..., Enter Maintenance Mode..., Exit Maintenance Mode

Transfer Server	vCenter Server	Status

VMware View позволяет применять три варианта использования смарт-карт.

1. **Not allowed** – не используется (вход только по паролю пользователя).
2. **Optional** – по выбору (по паролю или смарт-карте).
3. **Required** – требуется смарт-карта или USB-токен (вход только по смарт-карте).

Выберите нужный и нажмите **OK**.



Далее необходимо перезапустить службу View Connection Server.

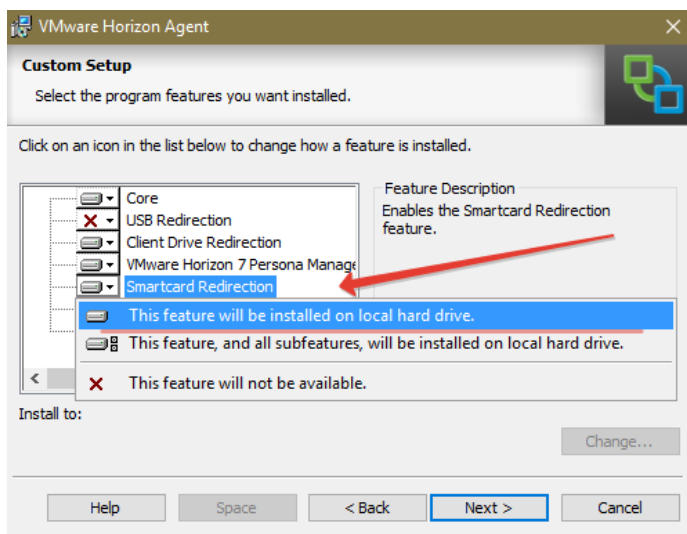
На этом настройка View Connection Server закончена.

Настройка проброса смарт-карты пользователя

Проброс смарт-карты пользователя позволяет производить прозрачную аутентификацию в виртуальную машину с вводом PIN-кода один раз.

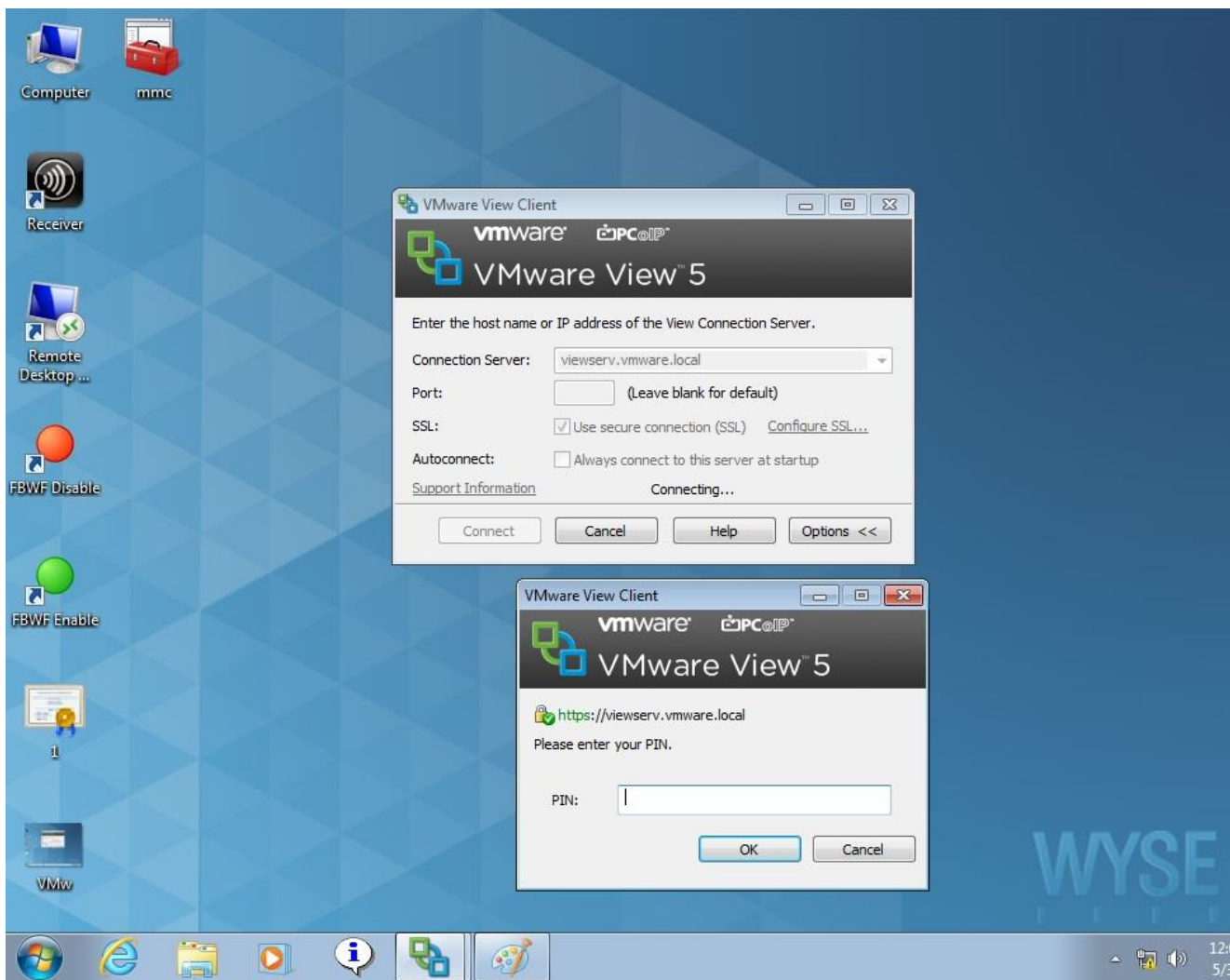
При использовании тонких клиентов Teradici настройка, как правило, не требуется.

При использовании программных клиентов Windows, MacOS, Linux необходимо выполнить установку VMware View Agent с активацией опции Smartcard Redirection.



Проверка работоспособности

Для корректной работы на стороне клиента необходимо добавить сертификат вашего ЦС в список доверенных, а также производить подключение к View Connection Server по имени сервера, указанному в выданном ему сертификате. После ввода PIN-кода произойдет аутентификация и отобразятся доступные для пользователя ресурсы.



Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru