

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

## Руководство по настройке

Листов: 22 Автор: Dmitry Shuralev

#### Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации в VDI-сессию, 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".

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.

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.

### Оглавление

О платформе VMware View			
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		

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 хостятся 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.

A 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.

A 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.

Консоль инаблонов сертификатов	
Constructions     Constru	008 R2
Шаблонов сертификатов: 36	10:08 02.05.2012

🔍 🤌		DC VMWare Architectire 192.168.1.100	
Компьютер VMware-vie	<ul> <li>Консоль шаблонов сертификатов</li> <li>Файл Действие Вид Справка</li> <li>Файл Действие Вид Справка</li> </ul>	Сеойства: view2 ? Х	×
Kopsies Witware VSphere Client	Шаблоны сертификатов (DC.VMV 0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Цель: Подлись и шифрование Цалить отозвание или посрочение с сертификатель не аконструктивые разлизи Адмикровать закрытый ключ субъекта Минимальный размер ключа: 2043 У	
WWWare	tel fel fel fel fel fel fel fel fel fel f	<ul> <li>✓ Разрешить экспортировать закрытый ключ</li> <li>При подаче заявки для субъекта и использования закрытого ключа его сертимата следует:</li> <li>✓ Подавать заявку для субъекта, не требув веода данък.</li> <li>✓ Запрашивать пользователя но время регистрация</li> <li>✓ Запрашивать пользования и пребовать ответа при использования закрытого ключа</li> <li>Для выбора поставщиков служб шифросания</li> <li>Поставщиков</li></ul>	
admin.inac	1월 월 월 월 월 19 19 19	ОК Отмена Пряменять Справка Подчиненный центр сертификацам Windows 2000 5.1 Пользователь Windows 2000 3.1	
ru_endeed.co	2000 2000 2000 2000 2000 2000 2000 200	Пользватель Exchange         Windows 2000         7.1           Пользватель Compart-Agroft Windows 2000         11.1           Почтовая реликация каталога         Windows 2000         11.1           Проверенный сеанс         Windows 2000         3.1           Проверенный сеанс         Windows Server 2003 Ent         110.0         Проверс подличности Котролера док           Проверся подличности Котролера док         Windows Server 2003 Ent         110.0         Провер           Проверска подличности Котролера док         Windows Server 2003 Ent         110.0         Проверс	
	и раблонов сертификатов: 36	Только подпись Exchange Windows 2000 6.1	er2008 R2
🖉 Пуск	2 📜 🚺 😜	EN	* P 🙀 🕼 10:00 02.05.2012

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.

Компьютер V	DC VMWare Architectire 192.168.1.100	
Корзина		
2	сегtsrv - [Центр сертификации (Локальный))/VHWare-DC-CA/Шаблоны сертификатов]	
VMware vSphere Client	🙀 Центр сертификации (Локальный) Иня Назначение	
VMWare	Image: WWWare-CC-CA         Image: WWWWare-CC-CA         Image: WWWWare-CC-CA         Image: WWWWARE-CC-CA         Image: WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW	
	Создать Выдаваеный шаблон сертификата овление файлов	
	Вид нинфрование EFS Шифрующая файловая система (EFS)	
	Обновить веп Проверка подлинности клиента, трове	
	Экспортировать список тер Проверка подличности клиента, Прове	
	Справка ватель Шифрующая файловая оистема (EFS), 3	
	од подчименный центр сертификации «Ссе» Дадиинистратор Подписывание списка доверия (Microsof	
	Бключение дополнительных шаблонов сертификатов на этом центре сертификации	
		· · · · · · · · · · · · · · · · · · ·
		Windows Server <sup>2008 R2</sup>
Пуск	🤱 🜌 🚞 🇊	EN 🕈 🕞 📆 🕼 10:23 02.05.2012

### 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.** 

KOHO	оль1 - [Корень консолк]	
Kop	нь консоли Добавление и удаление оснастотк	×
	Мажно выбрать оснастки для этой консоли из доступных на компьютере оснасток и затем настроить их. Для рас оснасток можно настроить требуемсе расшорение.	ширяемых онсоли
	Доступные оснастки: Выбранные оснастки:	
	Оснастка Поставщик - Какена Корень консоли Изменить ра	аширения
	(д) Гроснотр соовтии (с) корпора 20 Редактирование Microsoft Co	
	Pegaktop объек Microsoft Co     Bet     Bet	epx
	Сертификаты Містозоft Со Вебанить В	нз
w in the second s		
	Службы Microsoft Co	
	Churke Ha Be6-p Microsoft Co	
	😵 Телефония Microsoft Co	
	Дополнит Дополнит Дополнит Дополнит	тельно
	Описание:	
	Оснастка сертификатов позволяет просматривать содержимое хранилищ для поиска своих сертификатов, серти служб или компьютеров.	ификатов
	ок	Отмена
-		
		A
		Windows Server 2008 R

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.

Компьютер	РКСисоль1 - IKолень консолк/Селтификаты (покальный конпылтел)) Лимиос/Се Мастер экспорта сертификатов Завершение работы мастера		LIX Liter
Kopsieva View Administra VMWAREVIEW Lofix	якспорта сертификатов услешно завершена. Выли указаны следующие параметры: Ими файла Экспорт ключей Экспорт кл	Срок действия Назнах 27.04.2013 Провен	е Действия Сертификаты Дополнительные действия ) VIEWSERV.VNWare.local Дополнительные действия )
			Windows Server 2008

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\

ыотер	Ing-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 the for the to true, monitorFlow to false, hysteresis to true</thread-1></thread-1></thread-1></thread-1></thread-1>	
ыютер	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 thunk window to 4 NFO <thread-1> [ab] Setting there to true, monitorFlow to false, hysteresis to true</thread-1></thread-1></thread-1></thread-1></thread-1>	
	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> [bh] Setting there to true, monitorFlow to false, hysteresis to true</thread-1></thread-1></thread-1></thread-1></thread-1>	
Ţ	NFO <thread-1> [bn] Setting tailorBuffers to true, monitorFlow to false, hysteresis to true</thread-1>	and the second se
	ARN <thread-1> [ah] Failed to determine message security mode, setting to OFF. Invalid value: null</thread-1>	
зина	NFO <ws_tomcatservice_init> [AdminuIListener] initialized standalone winAuth successuily, my SID is 5-1-5-18 NFO &lt;2884&gt; [ws_java_bridgeDL] JavaBridge installed service AdminBackendservice NFO <ws_tomcatservice_init> [TrackerManager] Joining tracker cluster</ws_tomcatservice_init></ws_tomcatservice_init>	\$
	NFO <ws_tomcatservice_init> [BrokerLifecyCle] Node has joined cluster NFO   vesktopControlSessions&gt; [DesktopTracker] Session reader loop configuration: SESSION_POLL=30000ms, SESSI NFO   NFO   NFO clustcopControlLdap&gt; [DesktopTracker] LAP notification configuration: MaxLDAPNotificationSoutstanding=1</ws_tomcatservice_init>	CON_LIST
w stra	NFO <ws_tomcatservice_init> [EventForwarderHandler] Starting forwärder for ViewDatabaseEventForwarder NFO <ws_tomcatservice_init> [MaxSessionTaskFactory] MaxSessionTaskFactory was created for the first time on ARN <eventforwarderhandler-1335416906076> [DatabaseForwarder] No Events Databases specified in ADAM, will no NFO &lt;2684&gt; [ws_java_bridgeDL] javaBridge installed service Jadmin NFO &lt;2684&gt; [ws_java_bridgeDL] javaBridge installed service Jadmin</eventforwarderhandler-1335416906076></ws_tomcatservice_init></ws_tomcatservice_init>	this clubt store
	NFO <27.00> [ms_java_0) lugebit; Javab luge instance service where service instance of the service inits [usercontext] Allow Kerberos logins = true NFO <thread-1> [m] The secure Gateway Server is using SSL certificate store 1.pfx with password of 4 charact</thread-1>	ters
1	NFO <ws_tomcatservice_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.</frontredirect></thread-1></ws_tomcatservice_init>	
	INFO <frontredirect> [d] Smart Card/Certificate Authentication will not be used as not configured for SSL NFO <frontredirect> [Processor] Logging HTTP processor installed NFO <front> [d] AJP services are now ready.</front></frontredirect></frontredirect>	
3	NFO <front> [d] Smart Card/Certificate Authentication will not be used as useCertAuth is false NFO <poolwatchers [applicationprovisioningmanager]="" application="" for="" initializing="" manager="" node:vi<br="" provisioning="">NFO <appprovisioningmanager> [ApplicationProvisioningManager] Application Provisioning Manager started NFO <poolwartchers. 60000="" [virtualcenterpriver]="" delay="" ms<="" p="" poll="" setting="" to="" vc=""></poolwartchers.></appprovisioningmanager></poolwatchers></front>	iewServ
<mark>/2</mark> fx	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</tracker:pulsetimer></desktopcontrolsessions></poolwatcher></poolwatcher>	
1	RROR <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to vir ARN <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with RROR <vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to vir RROR <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to vir</virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a>	rtualCen 1 VC <ht rtualCen rtualCen</ht 
	ARM <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with RROR <vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to Vir RROR <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Problem connecting to Vir ARN <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [Audit] unable to establish a connection with RROR <vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [ServiceConnection25] Problem connecting to Vir</vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a>	1 VC <ht 'tualCen' 'tualCen' 1 VC <ht' rtualCen'</ht' </ht 
	NFO <vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993> [VcCache] Initial update completed in 12 863ms 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</missingvmscanner-6a63102e-6efa-441d-b177-3f1dc351881a></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></vcc-6a63102e-6efa-441d-b177-3f1dc351881a-1335416915993>	for VC I
	ARN <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Failed to refresh datastc ARN <virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a> [ServiceConnection] Failed to refresh datastc</virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a></virtualcenterdriver-6a63102e-6efa-441d-b177-3f1dc351881a>	ore with
		•
	Window	Sonvor or

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:

- 8 × И Систе Поиск в панели управ 🖼 🝷 Панель управления 🝷 Все элементы панели управления 🝷 Система ,0 Панель управления - домашняя Просмотр основных сведений о вашем компьютере Издание Windo 🚱 Диспетчер устройств Windows Server 2008 R2 Enterprise 🍘 Настройка удаленного доступа © Корпорация Майкрос 🚱 Дополнительные параметры Service Pack 1 Имя компьютера Оборудование Дополнительно Удаленный доступ X X Система Path Процессор: нной: ogramFiles% 🛛 Установленная память (ОЗУ): Тип системы Перо и сенсорный вво, Имя компьютера, имя до le nener Компьютер: Изменить Переменная Значение параметры Полное имя: C:\Windows\system32;C:\Windows;C:\.. Path PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;... Описание: PROCESSOR A... AMD64 Ломен: PROCESSOR\_ID... Intel64 Family 6 Model 42 Stepping 7, G... -Активация Windows Создать.. Изменить... Удалить Активация Windows вы настоящее Код продукта: 00486-0 ОК Отмена См. также Центр поддержки Центр обновления Windows

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

Миск 🛃 😰 🚞 🈂 💷 🕵

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:

EN \* P 11:04

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

Мпример: 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".

🖉 VMware View Administrator - Windows Inte	ernet Explorer				8 ×
COO V (@ https://localhost/admin/	م	💌 😵 Ошибка серт 🗟 😚 🗙 🥥 VMware View Adminis	strator X	û 🕁	( <u>Ö</u> )
🔺 🕨 🍓 VMware View Admi	nistrator			About   Help   Logout (vmvsadm	iin)
Updated 05/02/2012 12:02 PM Remote Sessions 0 Local Sessions 0 Problem Desktops 0 System Health 0 Desktops 5 Visers and Groups Vinventory Pols Pols Pols Policies View Configuration Servers Product Licensing and Usage Global Settings Registered Desktop Sources Administrators ThinApp Configuration Event Configuration Event Configuration Transfer Server Repository	Global Settings Edit Session timeout: Require SSL for client connections and View Administrator: Reauthenticate secure tunnel connections after network interruption: Message security mode: Disable Single Sign-On for Local Mode operations: Auto Update: Pre-login message: Display warning before forced logoff:	600 minutes Yes No Disabled No Yes			
🔊 Пуск 🛛 🐫 🎑				EN 🕈 🕞 👘 🕼 12:03 02.05.201	2

Зайдите в Web-консоль VMware View.

Перейдите во View Configuration -> Servers -> Connections Servers -> Edit.

🖉 VMware View Administrator - Windows Int	ternet Explorer								
COC  The https://localhost/admin/	_م	🛛 😵 Ошибка серт	🗟 😽 🗙 🎯 VMwar	e View Admin	istrator X				
🔺 🕨 🔁 VMware View Adm	inistrator						,	About   Help   I	Logout (v
Updated 05/02/2012 11:30 AM 💦	Servers								
Remote Sessions 0	vCenter Servers				Security Servers				
Problem Desktops 0	VCENter Servers				Security Servers				
Events 🚯 0 🚹 0	Add Edit R	emove		2	Edit Remove				
System Health 🔒 🕴 🧘 ? 5 0 1 0		vCenter Server			Security Server	Version	PCoIP	Connectio	on Server
A 1997 A 1997	192.168.1.99(vmwadmin)	)			-				
🚱 Dashboard									
👸 Users and Groups									
V Inventory									
Pools									
Desktops									
This Appa									
Manitaring	View Connection Servers								
Policies									
View Configuration		Edit Backup Now	<ul> <li>More Comma</li> </ul>	ands					
Servers	View Connection Server	Version	PCoIP	State	Settings			Last Backup	
Product Licensing and Usage	VIEWSERV	5.0.0-48167 Secur	e Gateway installed	Enable	d Secure tunnel connect	tion Sm		Loot Boonap	
Global Settings	VIEWBERV	51010 40107 50001	e outeway instance	Endbic					
Registered Desktop Sources									
Administrators									
ThinApp Configuration									
Event Configuration									
Transfer Server Repository									
	Transfer Servers								
	Transfer Server Repository:	Not Configured							
	Add Remove	nter Maintenance Mode	Exit Maintenance	Mode					
	Transfer	Server		vCenter	Server			Status	
🔊 Пуск 🛛 遇 🔀 🌈								EN 🖈 🔁	h 🕼 ,

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 ОК.

<b>OVMware View Administrator - Windows Int</b>	ernet Explorer		
COO 🗢 🙋 https://localhost/admin/	🔎 💌 😵 Ошибка серт 🖄 🍕	X 🧭 VMware View Administrator	
🔺 🕨 🏪 VMware View Adm	inistrator		About   Help   Logout (v
Updated 05/02/2012 11:30 AM       ♥         Remote Sessions       0         Local Sessions       0         Problem Desktops       0         Events       ♥         System Health       If It	Servers	Security Servers  Edit Remove Security Server  ackup on next user login  vval  fing  CK Edit Remove Security Server  CK Edit Remove Security Server  Security Server  Security Server  CK Edit Remove Security Server  Edit Remove Security Server  Security Security Server  Security S	Version PCoIP Connection Server
	Transfer Server	vCenter Server	Status
Autor 🕌 🖂 🧮			EN 🕆 🕑 🗑 🕼

Далее необходимо перезапустить службу View Connection Server.

На этом настройка View Connection Server закончена.

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.

🞼 VMware Horizon Agent	×
Custom Setup Select the program features you want installed.	₽
Click on an icon in the list below to change how a feature is installed.	on
This feature will be installed on local hard drive. This feature, and all subfeatures, will be installed on local hard drives.	rive.
<ul> <li>X This feature will not be available.</li> </ul>	
Install to:	hange
Help Space < Back Next >	Cancel

# 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 произойдёт аутентификация и отобразятся доступные для пользователя ресурсы.

Computer	mmc		
<b>M</b>			
Receiver		VMware View Client	
		Enter the host name or IP address of the View Connection Server.	
Remote		Connection Server: viewserv.vmware.local	
Desktop		Port: (Leave blank for default)	
		SSL: Use secure connection (SSL) <u>Configure SSL</u>	
FBWF Disable		Support Information Connecting	
20		Connect Cancel Help Options <<	
		Videore View Client	
FBWF Enable			
		VMware View <sup>®</sup> 5	
		le https://viewserv.vmware.local	
<u>U</u>		Please enter your PIN.	
		PIN:	
		OK Cancel	WVQE
Vilitor			
	a 😁 🔊		<u> </u>
	S 🗐 💟		

## 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 Аpple 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