



JaCarta PKI и VMware Horizon View 7

Руководство по настройке

Листов: 15

Автор: Александр Гриценко

Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации в административном интерфейсе VMware Horizon 7 и входа на VDI-машину пользователя 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.". Владелец товарного знака 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 Horizon View 7	4
Настройка VMware Horizon View 7	5
Предварительные требования	5
Настройка сертификатов	5
Экспорт корневого сертификата	5
Создание файла-контейнера ключей JKS	7
Настройка входа по сертификату	8
Настройка проброса смарт-карты пользователя	9
Проверка входа	10
Вход в консоль администрирования	10
Вход на VDI-машину	11
Контакты, техническая поддержка	13
Регистрация изменений	14

О платформе VMware Horizon View 7

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.

Настройка VMware Horizon View 7

Предварительные требования

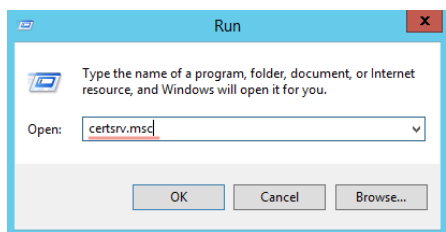
Подразумевается использование ОС семейства MS Windows, совместимых с программным обеспечением **VMware Horizon View**, а также с ПК "**Единый Клиент JaCarta**". Имеется работающая инфраструктура открытых ключей (PKI).

VMware Horizon View должен быть установлен и настроен в соответствии с требуемой конфигурацией.

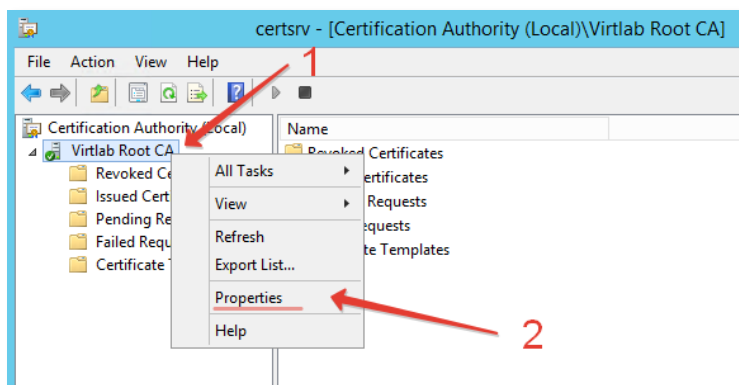
Настройка сертификатов

Экспорт корневого сертификата

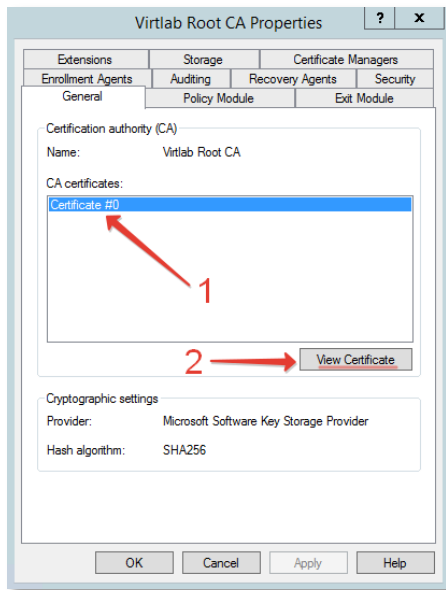
1. Откройте оснастку **Certification Authority** на корневом ЦС, выполнив команду **certsrv.msc**.



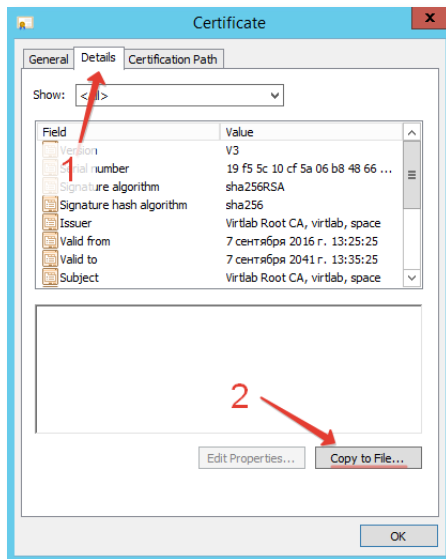
2. Откройте окно **Certification Authority -> CA Name -> Properties**.



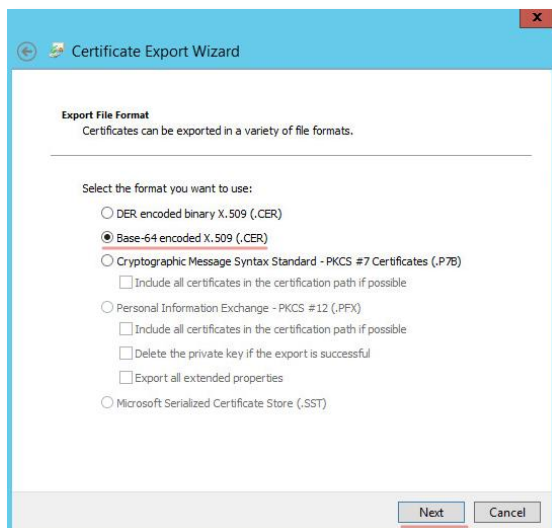
3. На вкладке **General** выберите корневой сертификат и нажмите кнопку **View Certificate**.



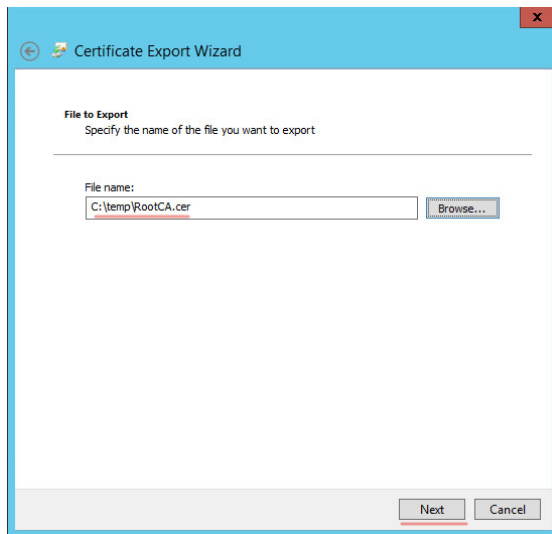
4. Перейдите на вкладку **Details** и нажмите кнопку **Copy to File**.



5. На странице выбора формата файла выберите **Base-64 encoded X.509 (.CER)**.



- Укажите путь экспорта файла, например, **C:\temp\RootCA.cer**.



Создание файла-контейнера ключей JKS

- На сервере **VMware Horizon View** откройте командную строку и перейдите в каталог с утилитой **keytool.exe** (*C:\Program Files\VMware\VMware View\Server\jre\bin*).

```
C:\Users\dcadmin>cd "C:\Program Files\VMware\VMware View\Server\jre\bin"
C:\Program Files\VMware\VMware View\Server\jre\bin>
```

- Импортируйте корневой сертификат в файл-хранилище с помощью команды **keytool -import -alias alias -file root_certificate -keystore truststorefile.key**, где *alias* – псевдоним (любое значение), *root_certificate* – полный путь к файлу сертификата, *truststorefile.key* – имя файл-хранилища. В процессе импорта необходимо будет ввести парольную фразу для защиты хранилища и подтвердить доверие сертификату.

```
C:\Program Files\VMware\VMware View\Server\jre\bin>keytool.exe -import -alias VirlabRootCA -file c:\temp\RootCA.cer -keystore truststorefile.key
Enter keystore password:
Owner: CN=Virtlab Root CA, DC=virtlab, DC=space
Issuer: CN=Virtlab Root CA, DC=virtlab, DC=space
Serial number: 19F52C6746CB40884863745684ab8
Valid from: Wed Sep 07 13:25:25 MSK 2016 until: Sat Sep 07 13:35:25 MSK 2041
Certificate fingerprints:
 MD5: BB:AD:5E:55:5D:BB:41:85:9F:1E:04:70:72:68:C8:0D
 SHA1: 5C:94:9A:DE:74:52:D8:23:79:D0:2E:BF:D9:D6:DD:80:2E:0F:78:14
 SHA256: 2F:ED:C7:46:CB:D0:89:45:65:18:25:CG:19:32:E4:EE:91:4E:EB:F6:DF:DF:54:EC:B2:A5:19:5E:73:90:C1:F6
 Signature algorithm name: SHA256withRSA
 Version: 3

Extensions:
 #1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
    0000: 02 01 00 ...
 #2: ObjectId: 2.5.29.19 Criticality=true
    BasicConstraints:1
       C: true
       PathLen: 2147483647
 #3: ObjectId: 2.5.29.15 Criticality=false
    KeyUsage: 1
       DigitalSignature
       KeyCertSign
       CrlSign
 #4: ObjectId: 2.5.29.14 Criticality=false
    SubjectKeyIdentifier: 1
    KeyIdentifier: 1
    0000: 10 6E 6C 05 C1 C6 EB 95 10 F0 2E 28 84 2B 2D 73 .nl.....<.+>
    0010: E7 8F 23 FB ..#
}

Trust this certificate? [no]: yes
Certificate was added to keystore
C:\Program Files\VMware\VMware View\Server\jre\bin>
```

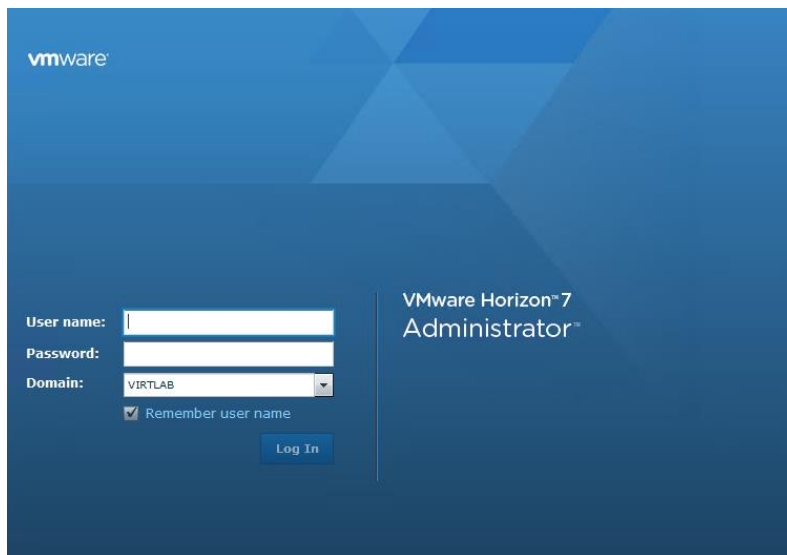
- Файл-хранилище **truststorefile.key** необходимо скопировать в директорию SSL Gateway: *install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key*.
- В директории SSL Gateway (*install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties*) необходимо создать файл с именем **locked.properties** и отредактировать его (например, в блокноте) до следующего содержимого:

```
trustKeyfile= truststorefile.key
trustStoretype=JKS
useCertAuth=true
```

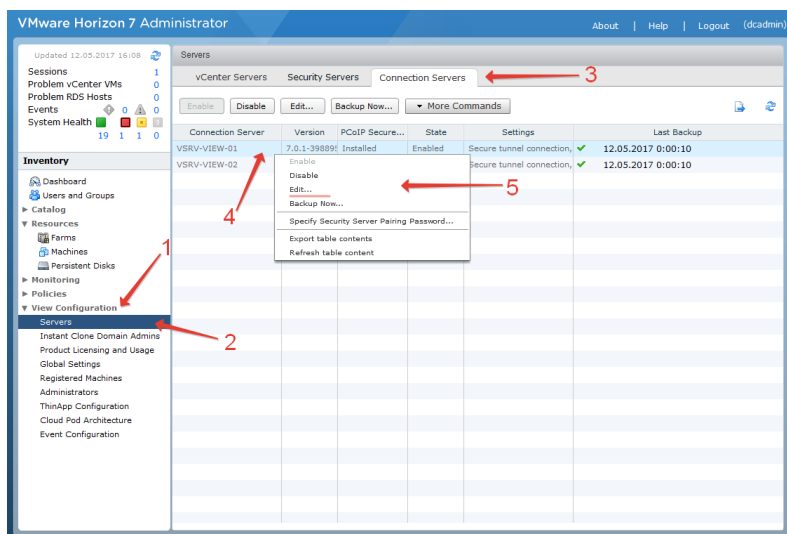
- Сохраните файл и перезагрузите службу **View Connection Server**.

Настройка входа по сертификату

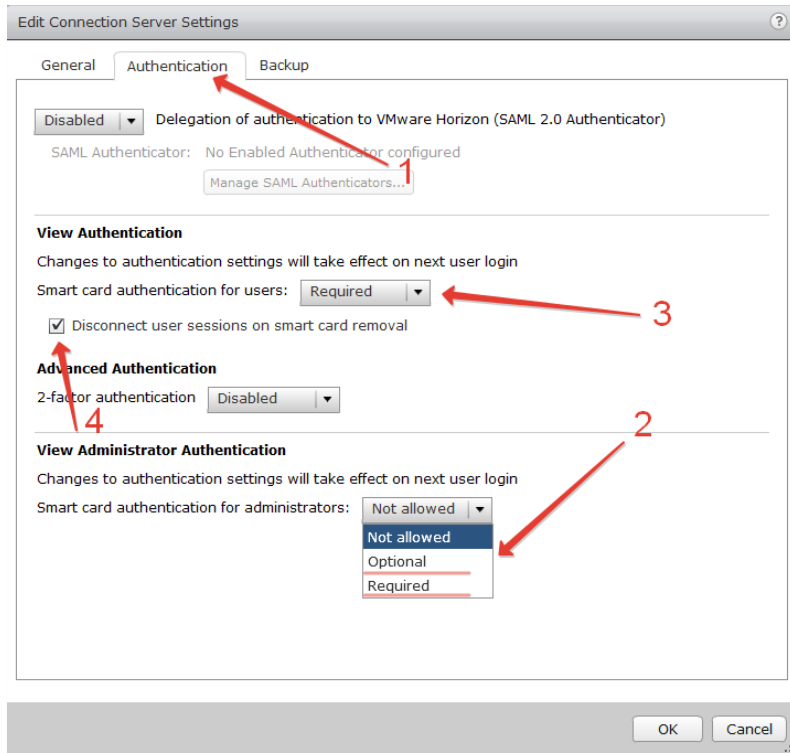
- Зайдите в Web-консоль VMware Horizon View.



- Перейдите в свойства сервера: **Inventory -> View Configuration -> Servers -> Connections Servers -> Edit**.



- Перейдите на вкладку **Authentication** и выберите предпочтительный режим аутентификации. Аутентификация в административную консоль по смарт-карте настраивается из выпадающего списка **Smart card authentication for administrators**:
 - **Not Allowed** – не использовать смарт-карту;
 - **Optional** – смешанная аутентификация (или по паролю или по смарт-карте);
 - **Required** – обязательное использование смарт-карты.
 Аутентификация пользователя в VDI по смарт-карте настраивается из выпадающего списка **Smart card authentication for users**:
 - **Not Allowed** – не использовать смарт-карту;
 - **Optional** – смешанная аутентификация (или по паролю или по смарт-карте);
 - **Required** – обязательное использование смарт-карты.
 Опция **"Disconnect user sessions on smart card removal"** определяет политику при отключении смарт-карты. Установите галочку, если необходимо производить отключение сессии при изъятии смарт-карты.



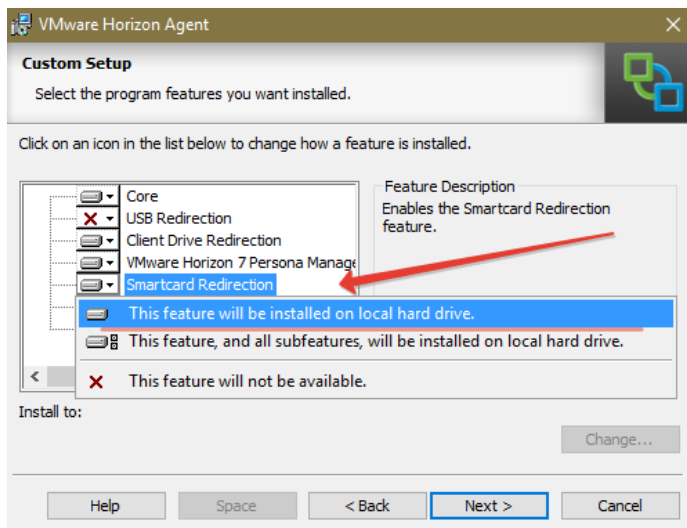
4. Нажмите кнопку **ОК**.

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.

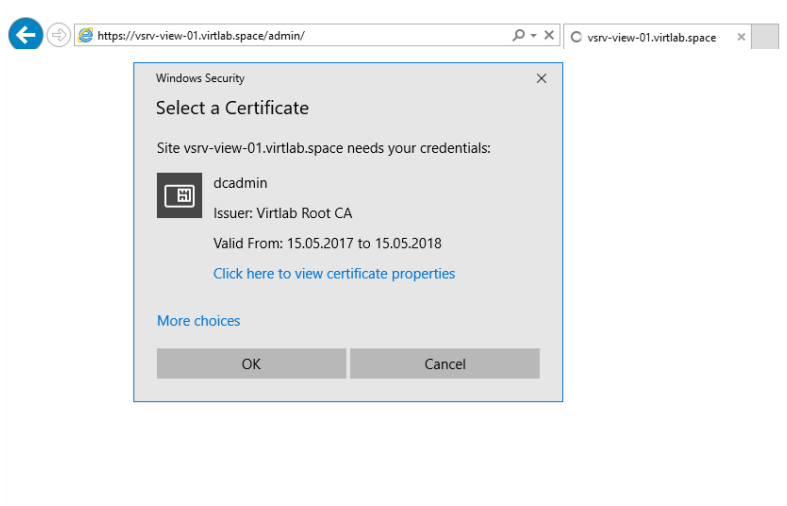
При использовании программных клиентов Windows, macOS, Linux необходимо выполнить установку VMware View Agent с активацией опции Smartcard Redirection.



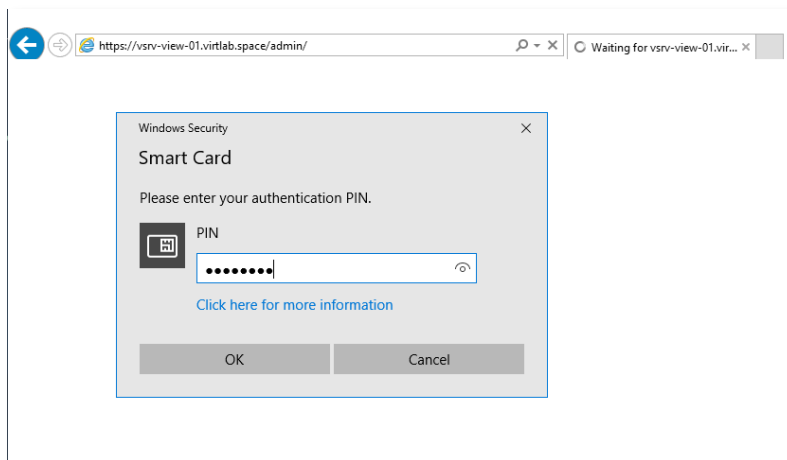
Проверка входа

Вход в консоль администрирования

1. Вставьте смарт-карту и перейдите в консоль администрирования.
2. В появившемся окне формы входа выберите сертификат администратора и нажмите кнопку **OK**.

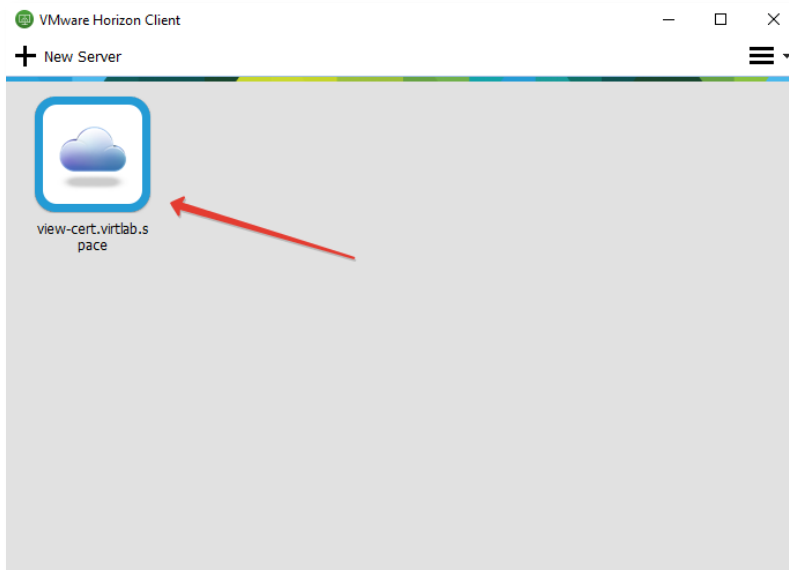


3. Отобразится запрос на ввод PIN-кода. После успешной проверки PIN будет произведена аутентификация в Web-интерфейс.

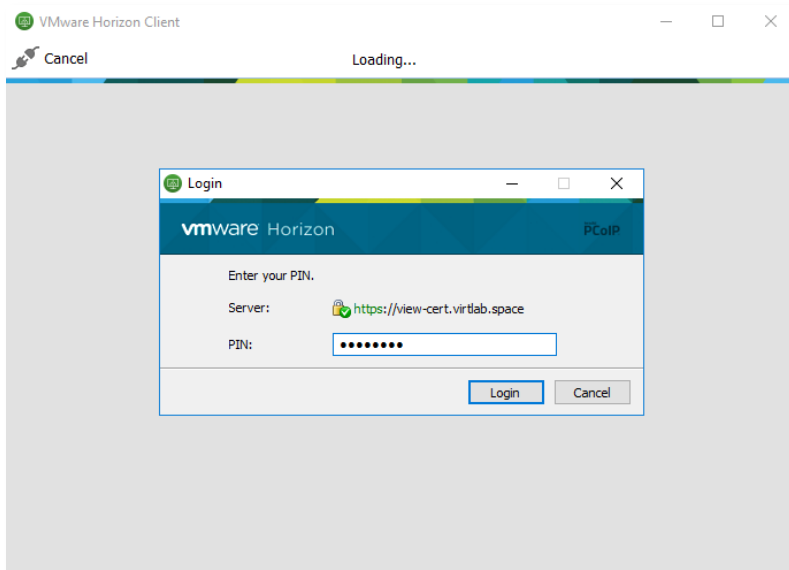


Вход на VDI-машину

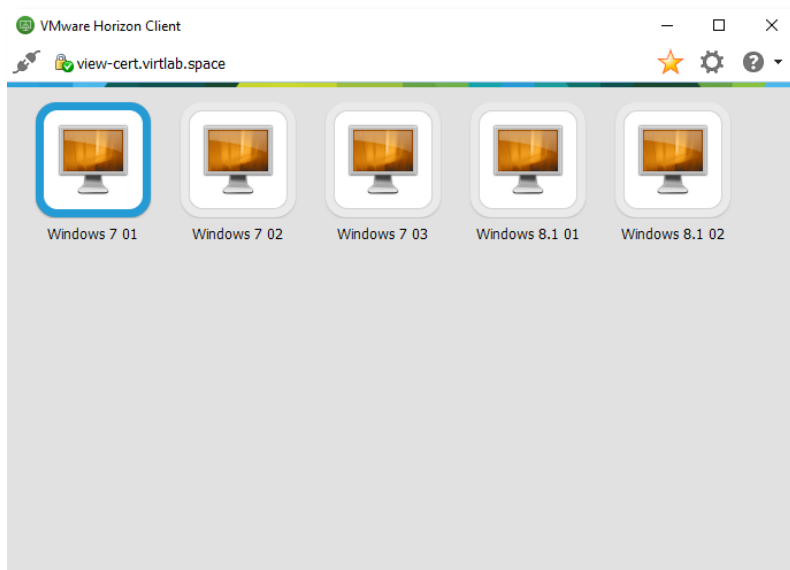
1. Запустите VMware Horizon Client и выберите подключение.



2. Отобразится запрос на ввод PIN-кода.



3. После успешной аутентификации отображаются доступные 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