



JaCarta и Remote Desktop Services

Настройка аутентификации в службу терминалов с использованием JaCarta PKI

Листов: 37

Автор: Dmitry Shuralev

Аннотация

В настоящем документе рассматривается настройка аутентификации по электронным ключам **JaCartaPKI** в сессию **RemoteDesktopServices**. Настоящая инструкция предполагает наличие развёрнутой инфраструктуры PKI на базе центра сертификации Microsoft и не содержит информации по её настройке.

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


Описание демо-стенда	4
Ход настройки	4
Настройка Сервера терминалов	5
Настройка политик безопасности домена (AD)	9
Отключение парольной аутентификации	14
Настройка клиента	16
Проверка работоспособности	17
Windows 7 (Пользователь 1)	17
Настройка подключения	17
Создание ярлыка для быстрого подключения	22
Windows 10 (Пользователь 2)	25
Настройка подключения	26
Создание ярлыка для быстрого подключения	32
Контакты, техническая поддержка	35
Регистрация изменений	36

Описание демо-стенда

Серверная часть

- MicrosoftWindowsServer 2012 R2 —серверсрольюконтроллерадомена (DomainController) ицентрасертификации (CertificationAuthority).
- Microsoft Windows Server 2012 R2 —серверсрольюслужбтерминалов(Remote Desktop Services).


Решение может быть развёрнуто в рамках любой версии современногоMicrosoftWindowsServer (2003, 2008, 2012, 2016), настоящий пример описывает работу с Server 2012 R2. В минимальной конфигурации требуется один сервер, на котором могут быть установлены сразу все роли — контроллер домена (ActiveDirectory), центр сертификации (CertificationAuthority) и сам терминальный сервер (RemoteDesktopServices).

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

Клиентская часть

- MicrosoftWindows 7x64—ПКпользователя№ 1
- MicrosoftWindows10x64 —ПКпользователя № 2

Со стороны клиента используются два ПК для одновременной аутентификации двух пользователей. Клиентской ОС может выступать любой Windows, Linux или специализированная прошивка устройства, способная работать протоколом RDPи смарт-картами.

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

Ход настройки

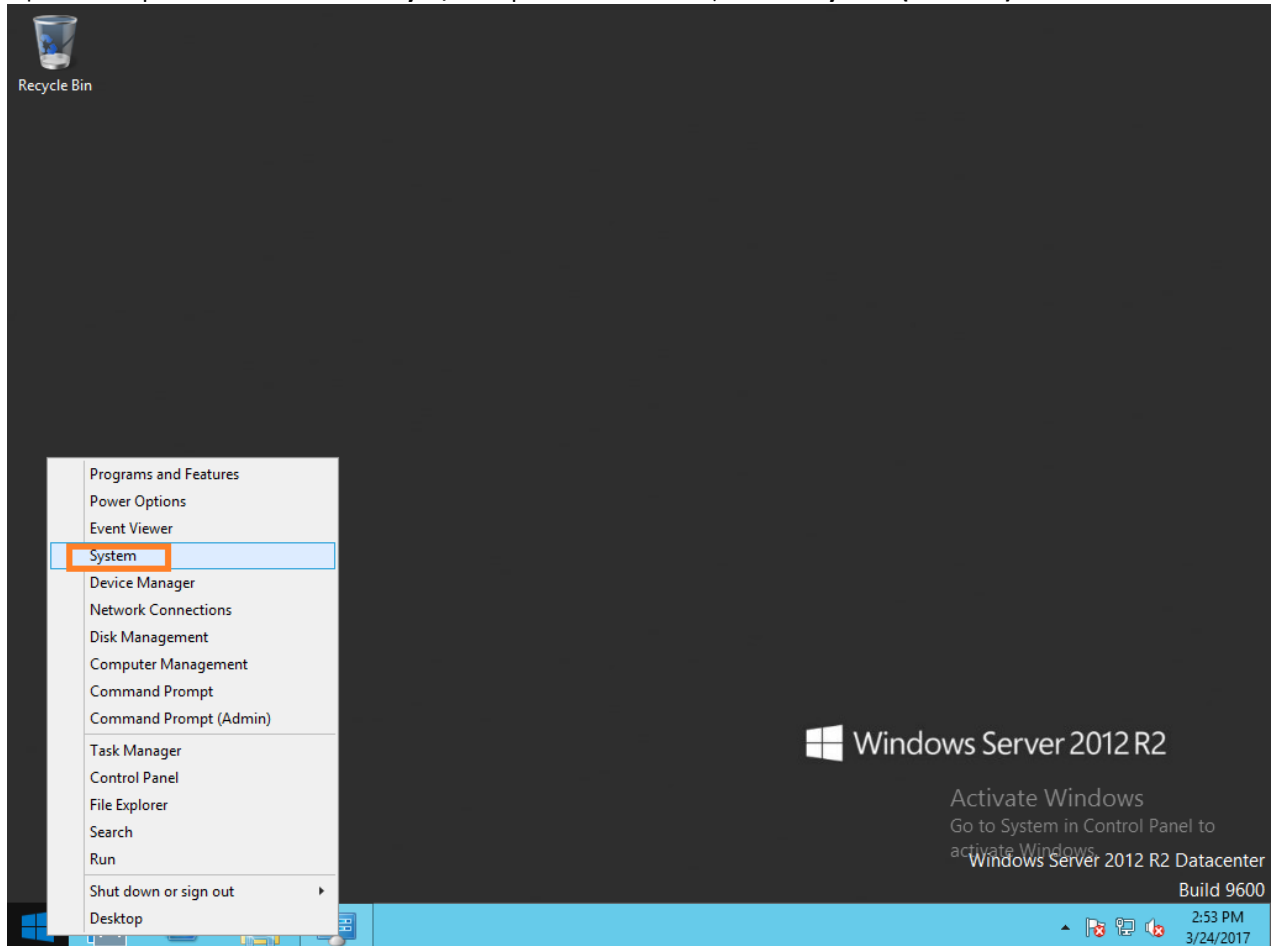
Настоящая инструкция не рассматривает ход настройки контроллера домена, центра сертификации и установки драйверов и утилит управленияэлектронными ключами JaCarta. Для получения справки по этим вопросам следует обратиться к следующим источникам:

- документация по WindowsServer версии, соответствующей установленной, для настройкироли домен контроллера;
- "JaCartадля Windows,руководство по внедрению" для настройки центра сертификации и аутентификации по смарт-картам и USB-токенам;
- "JC-Client,руководство администратора" или "Единый Клиент JaCarta,руководство администратора" для установки и настройки драйверов и утилит управления электронными ключами JaCarta.

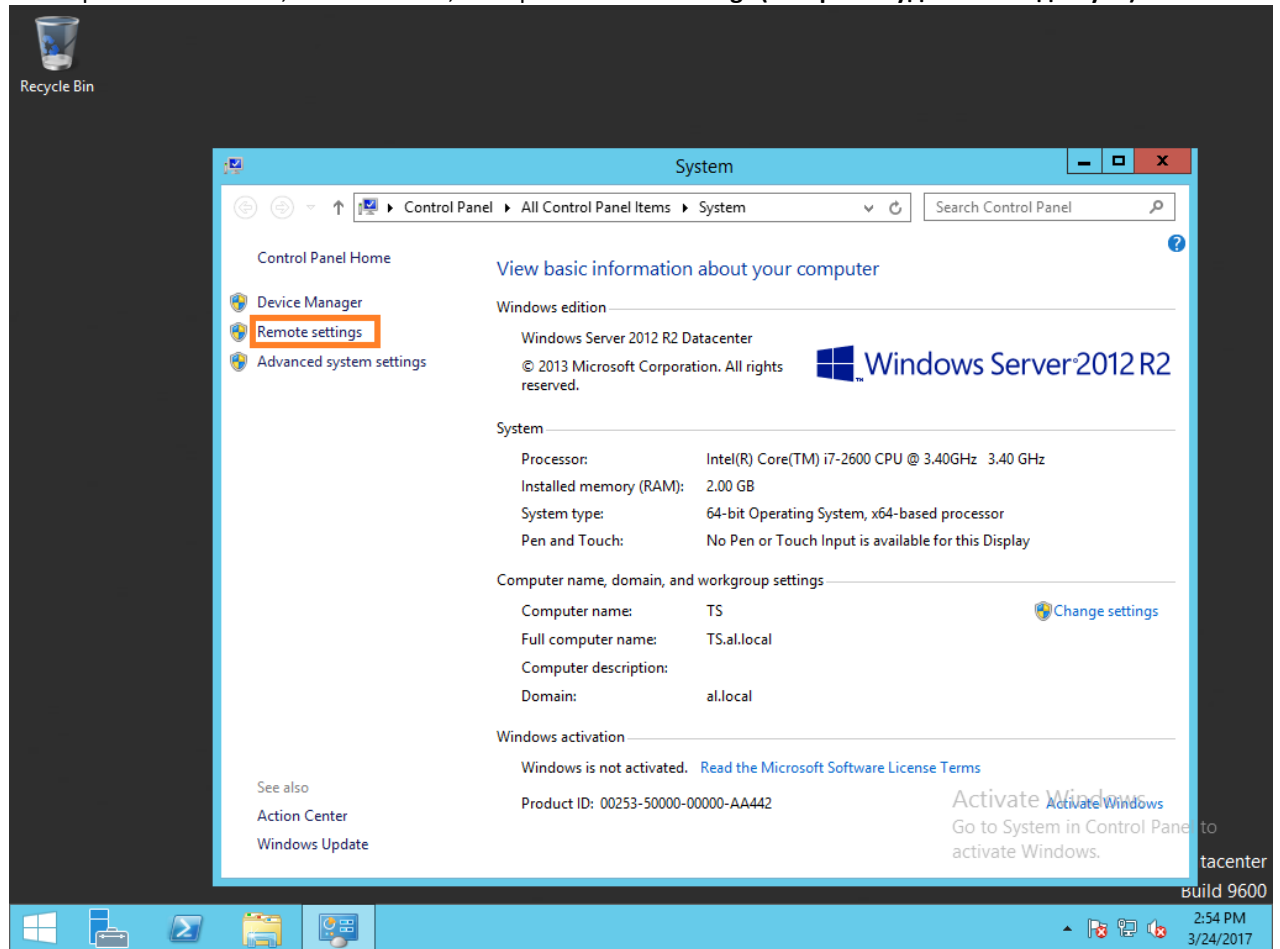
Настройка Сервера терминалов

На сервере с ролью RemoteDesktopServices необходимо выполнить следующие действия.


Щёлкните правой кнопкой меню **Пуск**, в открывшемся окне щёлкните **System (Система)**.

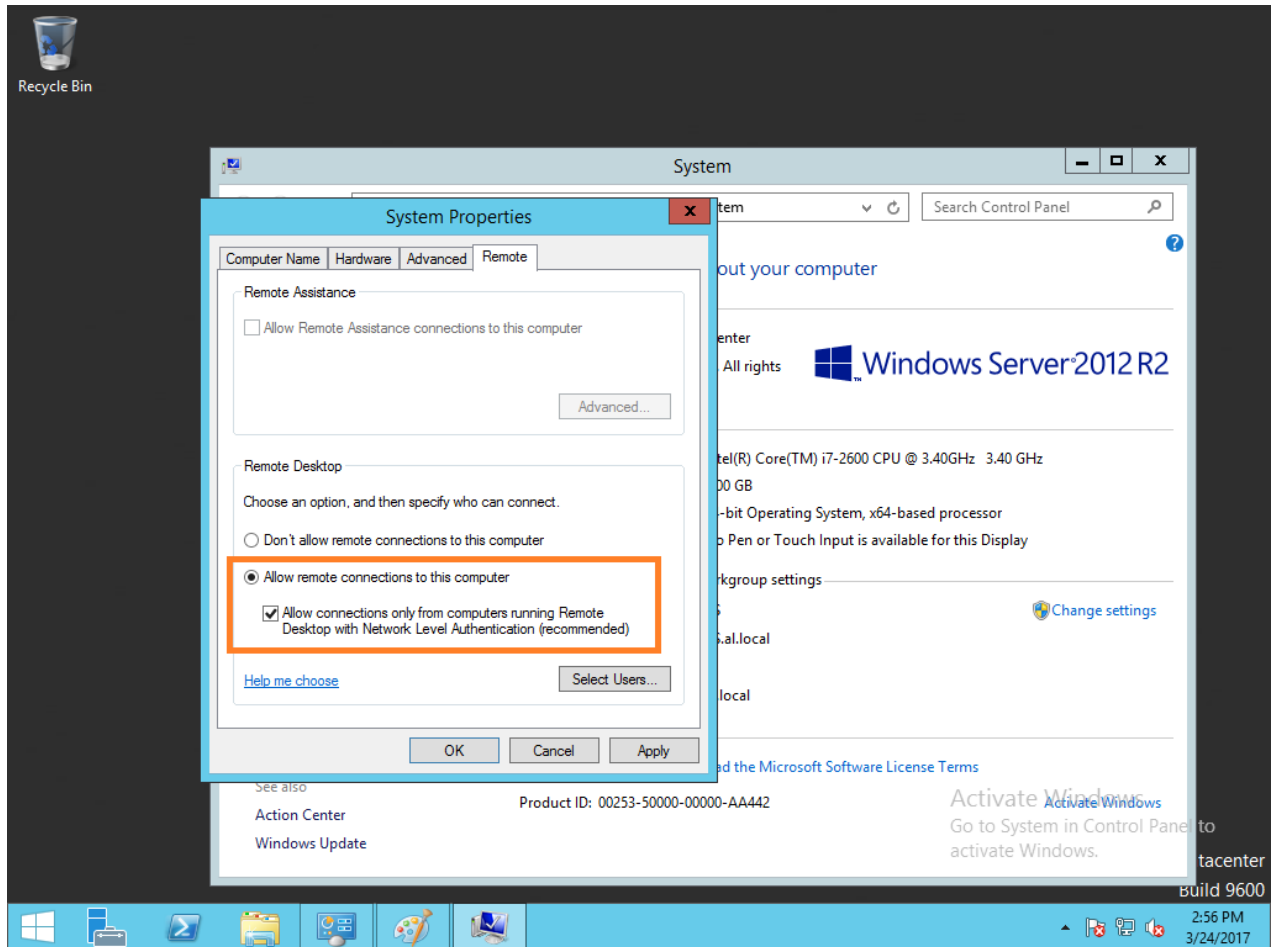


В отобразившемся окне, в левой части, выберите **RemoteSettings (Настройка удалённого доступа)**.



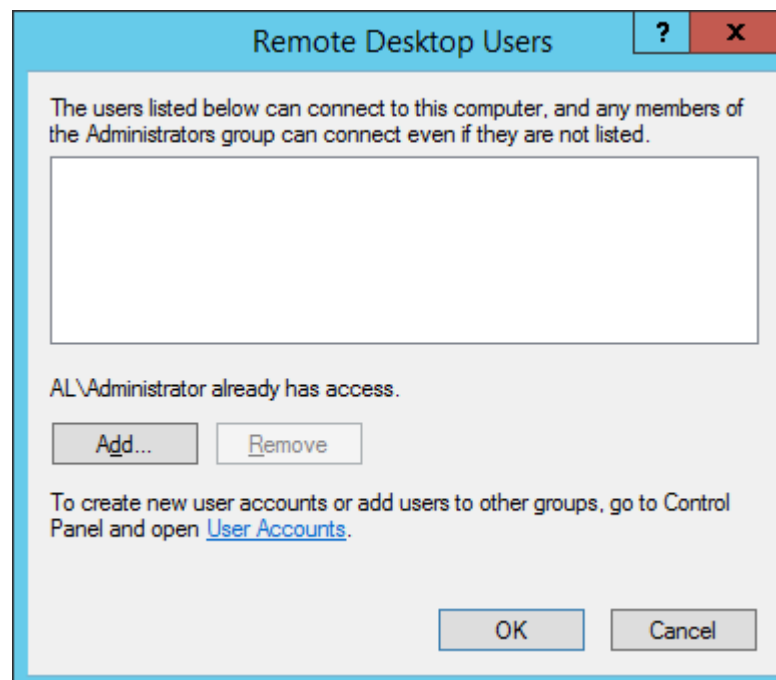
В настройках удалённого доступа разрешите удалённое подключение.

 Опционально можно включить/отключить проверку на уровне сети (NLA). Не все RDP-клиенты имеют поддержку NLA, например, дефолтный RDP-клиент в ОС Windows XP не поддерживает NLA.



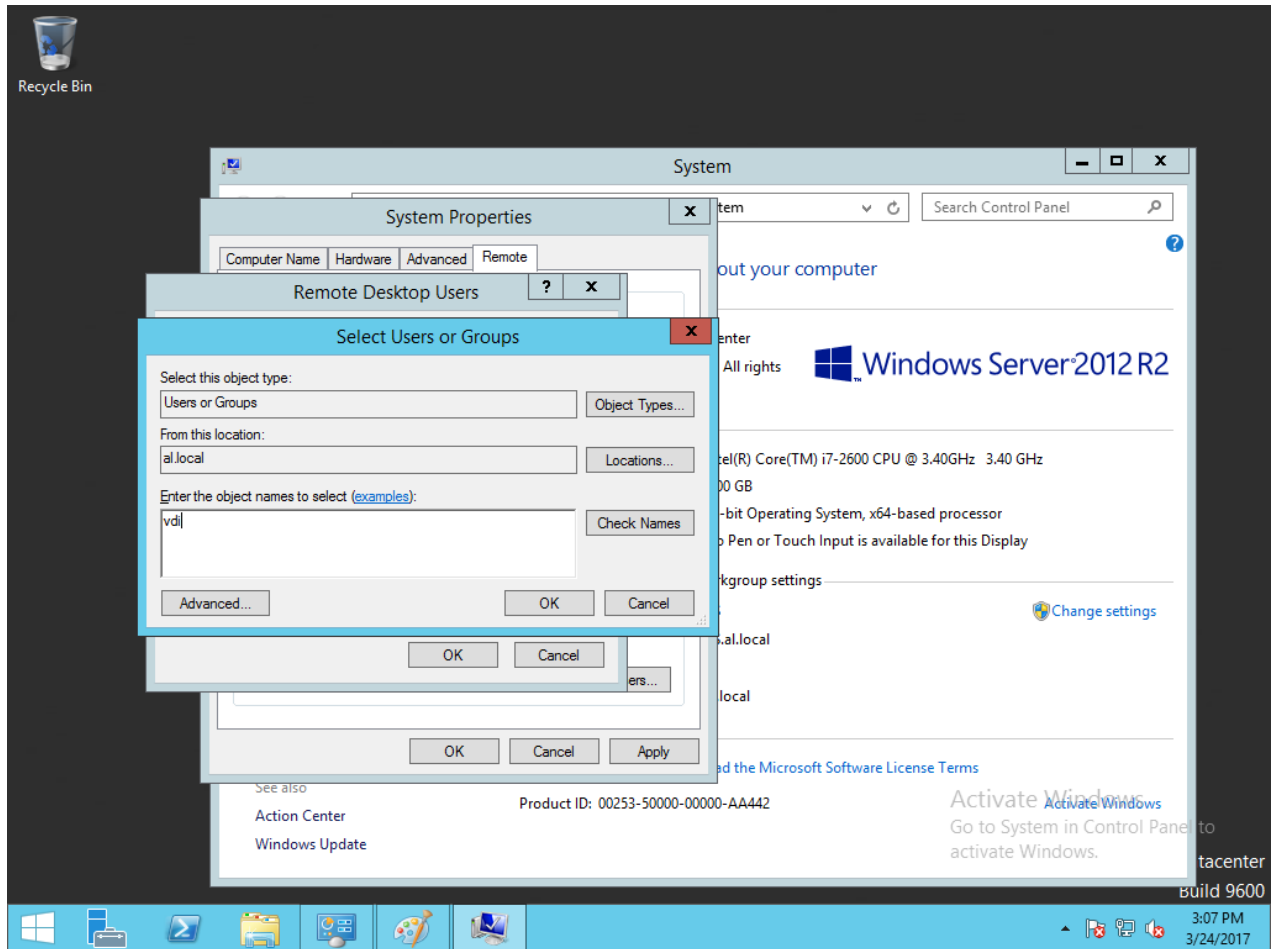
Нажмите **Select User... (Выбрать пользователей...)** и укажите пользователей или целые группы пользователей из AD, которым будет разрешён доступ к службе RemoteDesktopServices.

В открывшемся окне **RemoteDesktopUser (Пользователи удалённого рабочего стола)** нажмите **Add... (Добавить...)**




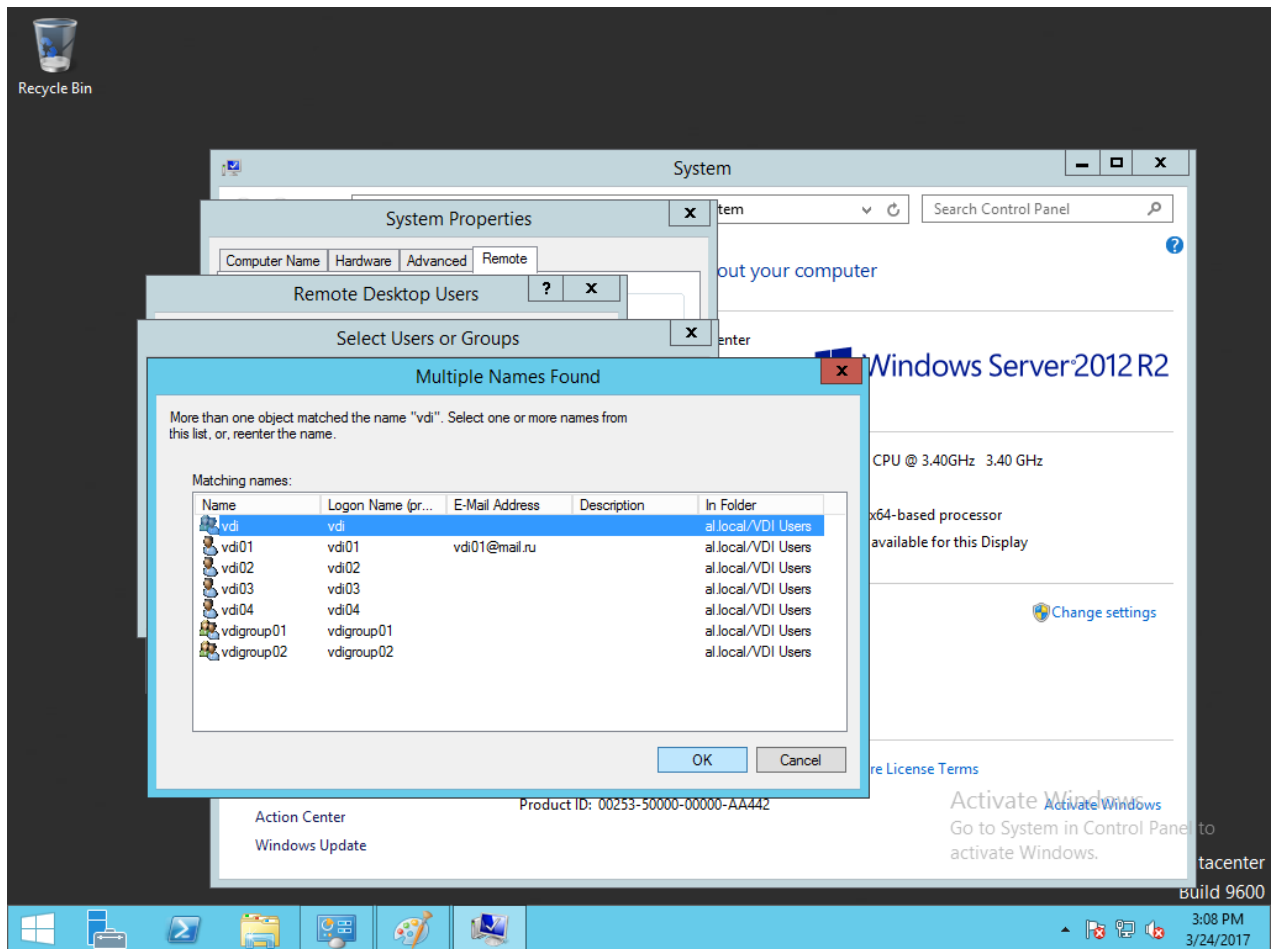
Отобразится меню **SelectUsersorGroups (Выбор: "Пользователи" или "Группы")**. В поле **Fromthislocation (В следующем месте)** должно отображаться имя Вашего домена. Далее введите

имя пользователя или имя группы, можно неполностью и нажмите **CheckNames (Проверить имена)**. Система предложит полный список соответствий имён для введённого значения.



Выберите нужного пользователя или группу, примените изменения, **OK->OK->Apply (Применить)**.

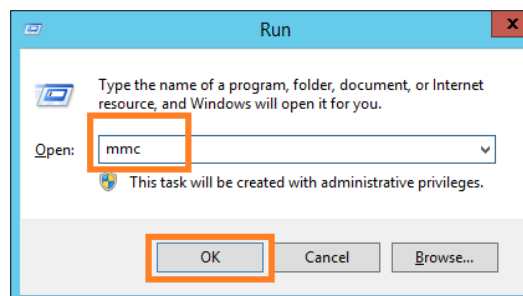
 В нашем примере, для значения vdi, отобразятся все пользователи и группы, содержащие "vdi" в своём названии.



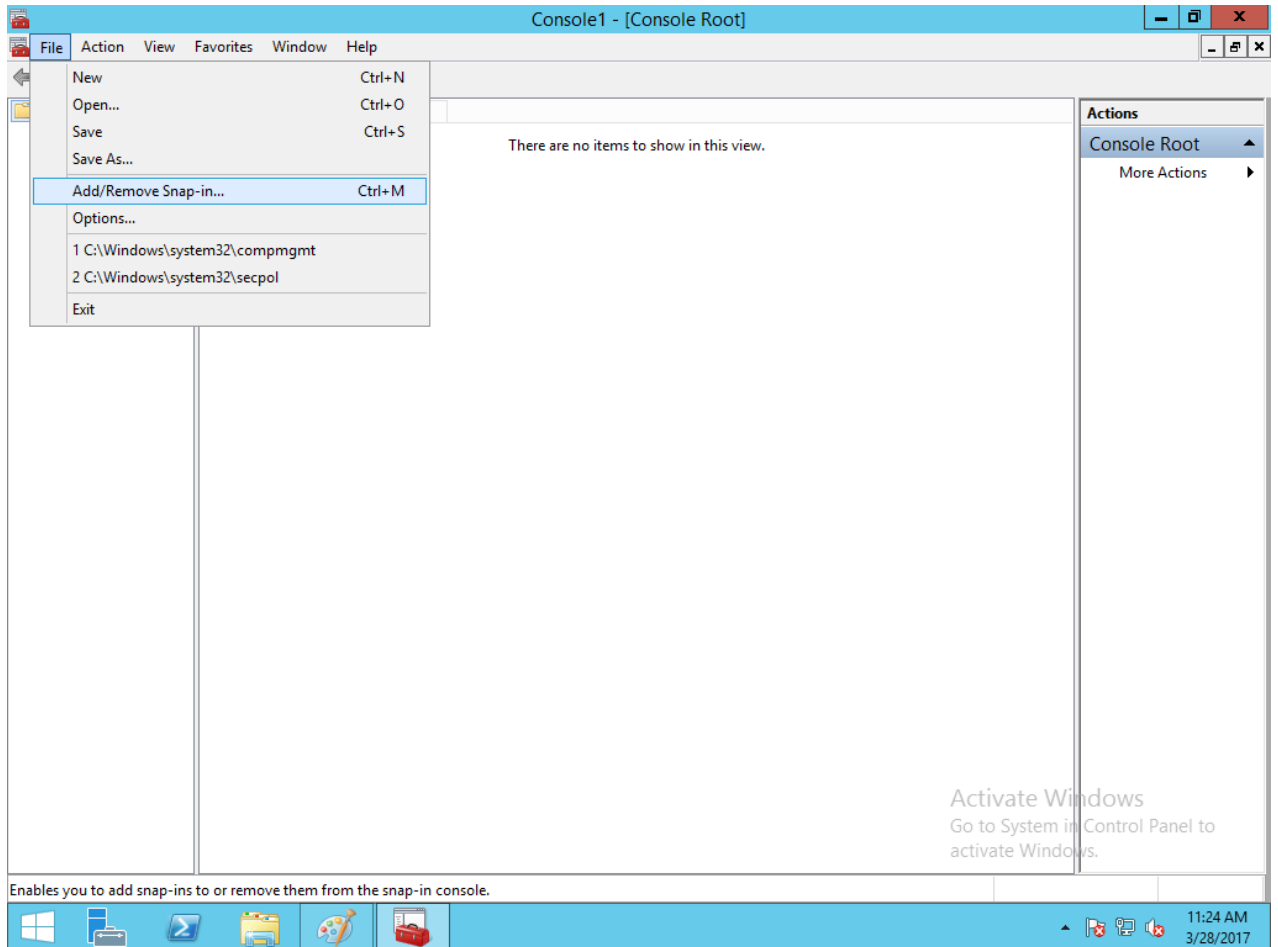
Настройка политик безопасности домена (AD)

На сервере с ролью домен контроллера необходимо выполнить следующие действия.

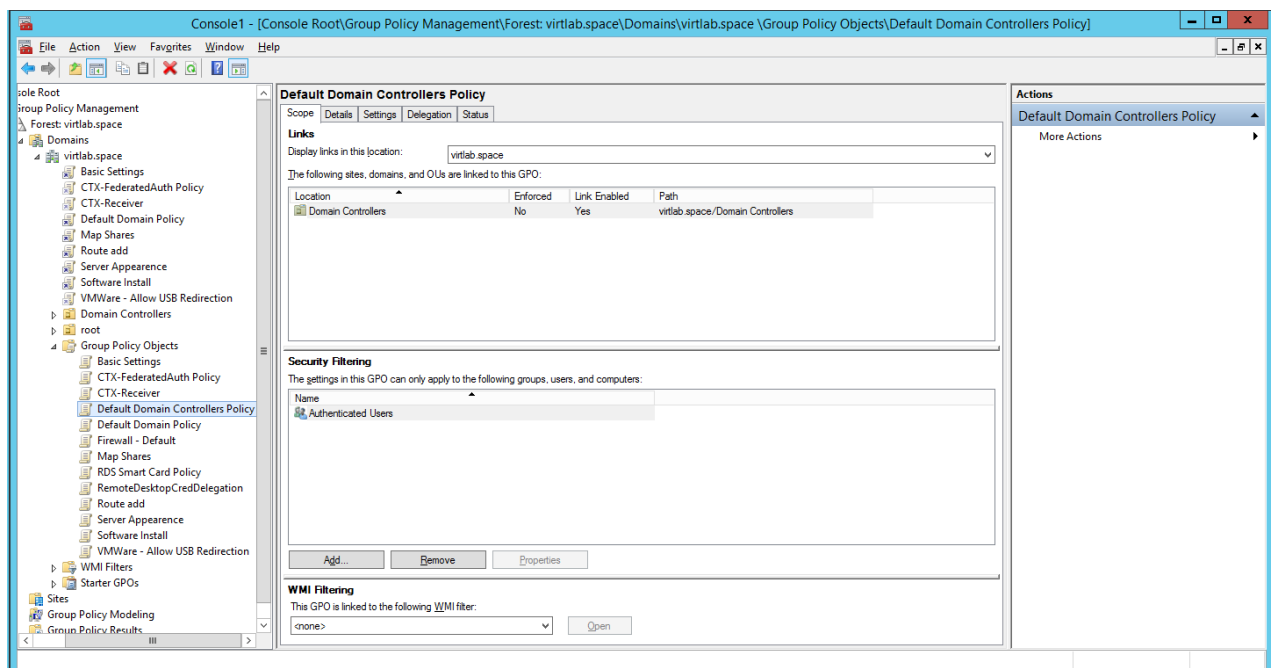
Откройте **Microsoft Management Console (MMC (Консоль Управления Microsoft))**, для этого щёлкните правой кнопкой меню **Пуск**, в открывшемся окне щёлкните **Run (Выполнить)**, в отображившемся окне наберите **mmc** и нажмите **OK**.



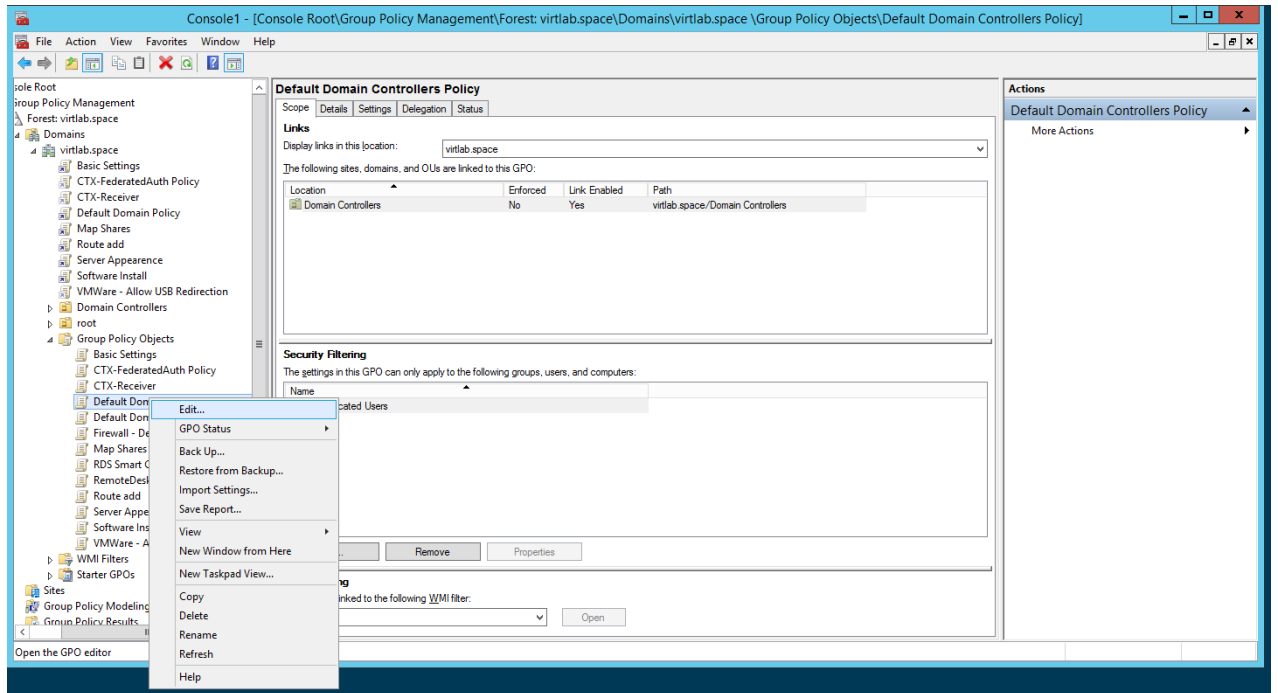
В отображившемся окне выберите **File (Файл) -> Add/Remove Snap-in...** (Добавить или удалить оснастку...)



В отобразившемся окне выберите настройку **GroupPolicyManagement (Управление групповой политикой)**, нажмите **Add (Добавить)** -> **ОК**. В лесу нужного домена выберите **DefaultDomainControllersPolicy (Объекты групповой политики)**.

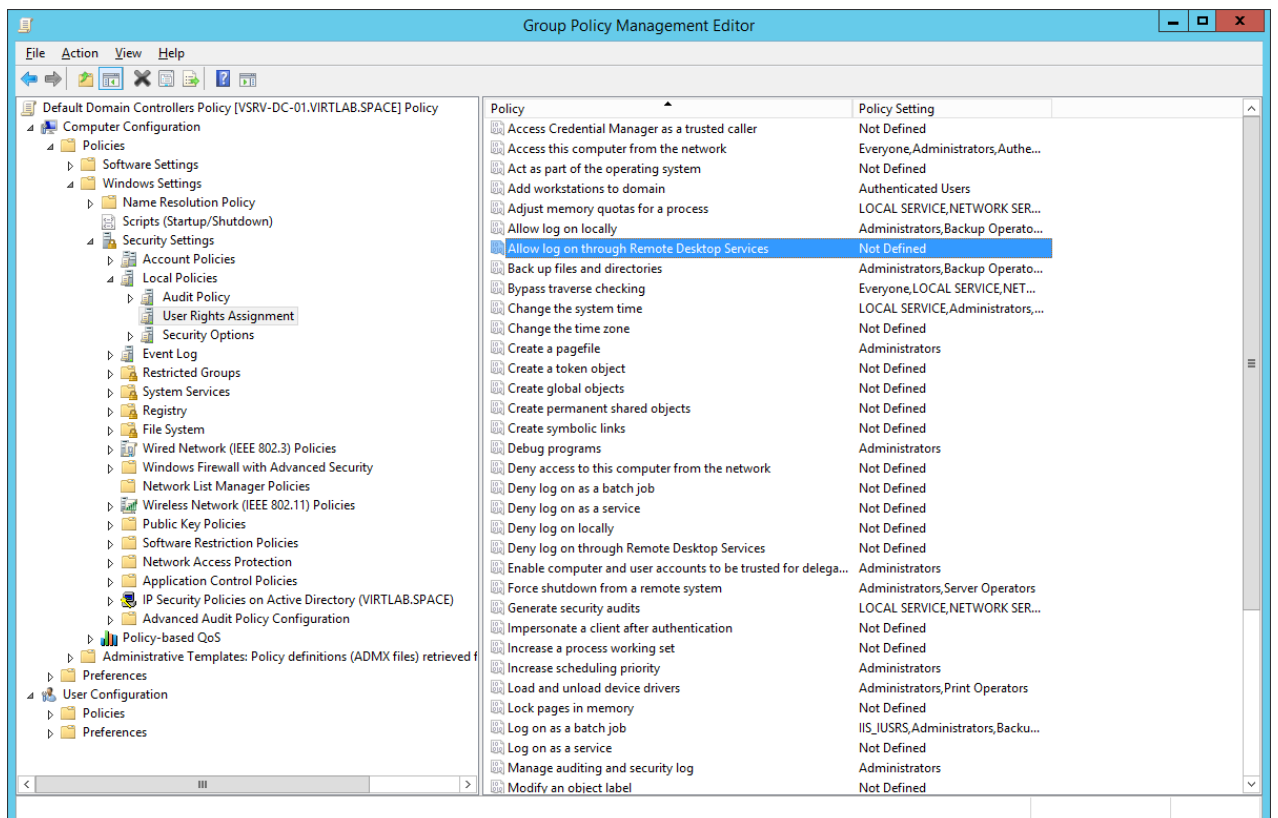


Щёлкните правой кнопкой мыши по **Default Domain Controllers Policy** и выберите **Edit... (Изменить...)**

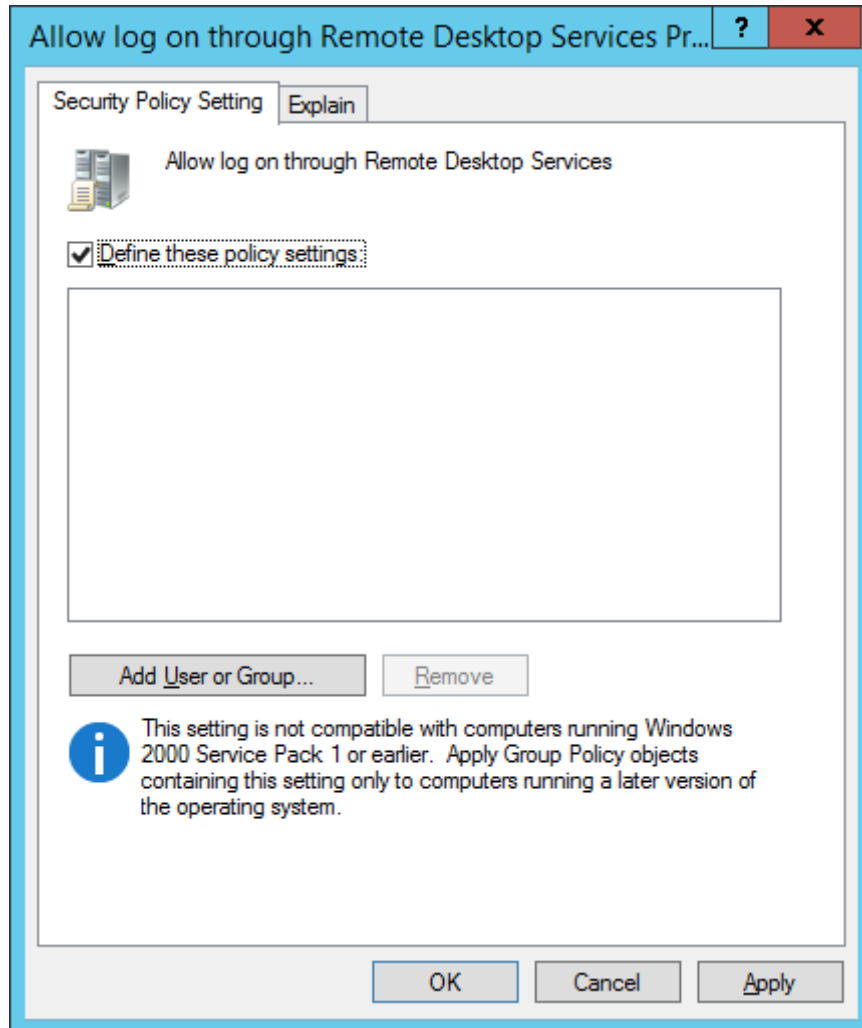


Откроется **Group Policy Management Editor** (Редактор управления групповыми политиками), перейдите в категорию **Computer Configuration** (Конфигурация компьютера) -> **Policies** (Политики) -> **Windows Settings** (Конфигурация Windows) -> **Security Settings** (Параметры безопасности) -> **Local Policies** (Локальные политики) -> **User Rights Assignment** (Назначение прав пользователей).

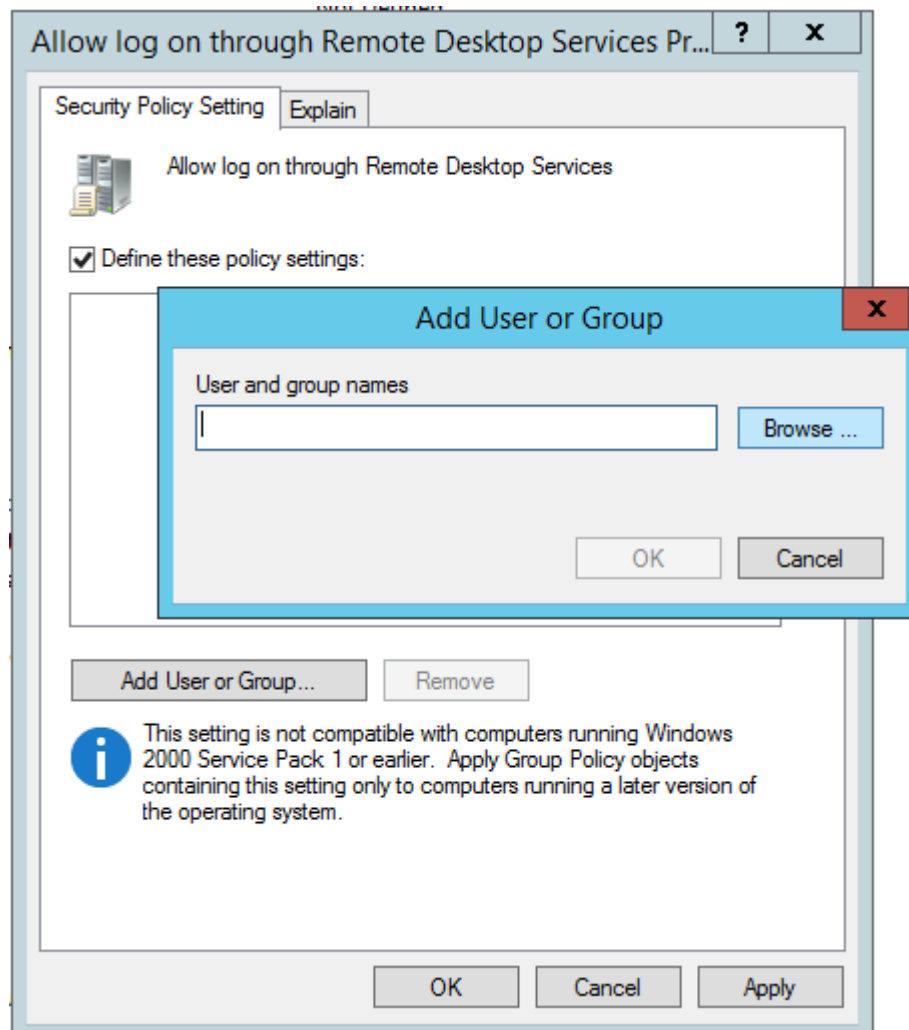
Выберите настройки политики **Allow log on through Remote Desktop Services** (Разрешить вход в систему через службу удалённых рабочих столов).



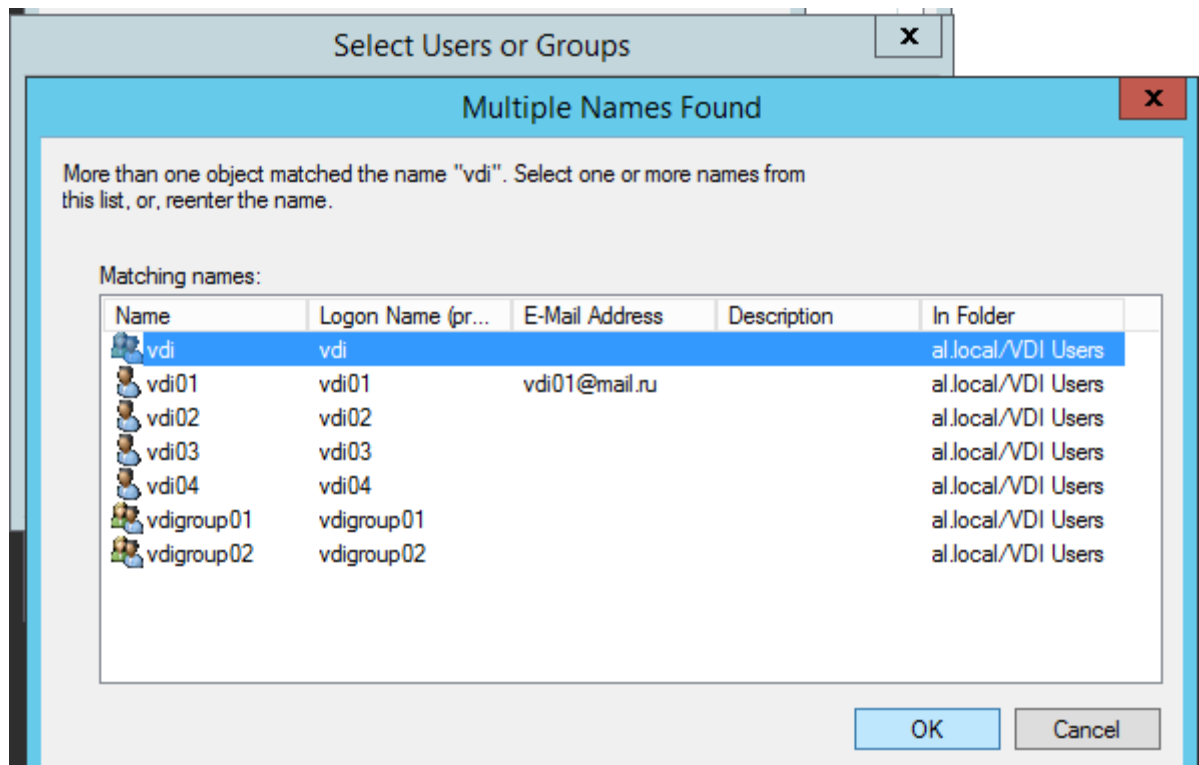
Поставьте галку напротив **Define these policy settings** (Определить следующие параметры политики) и нажмите **Add User or Group** (Добавить пользователя или группу).



Нажмите **Browse... (Открыть...)**.



Выберите нужного пользователя или группу, примените изменения.



Закройте **Group Policy Management Editor (Редактор управления групповыми политиками)** и все остальные окна.

Выполните перезагрузку.

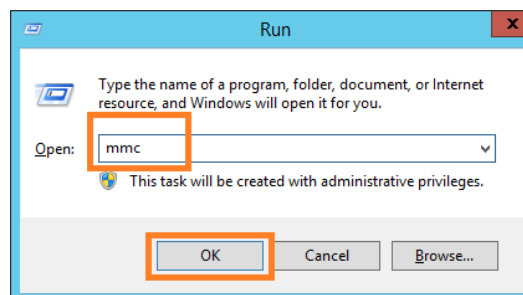
На этом настройка сервера окончена.

Отключение парольной аутентификации

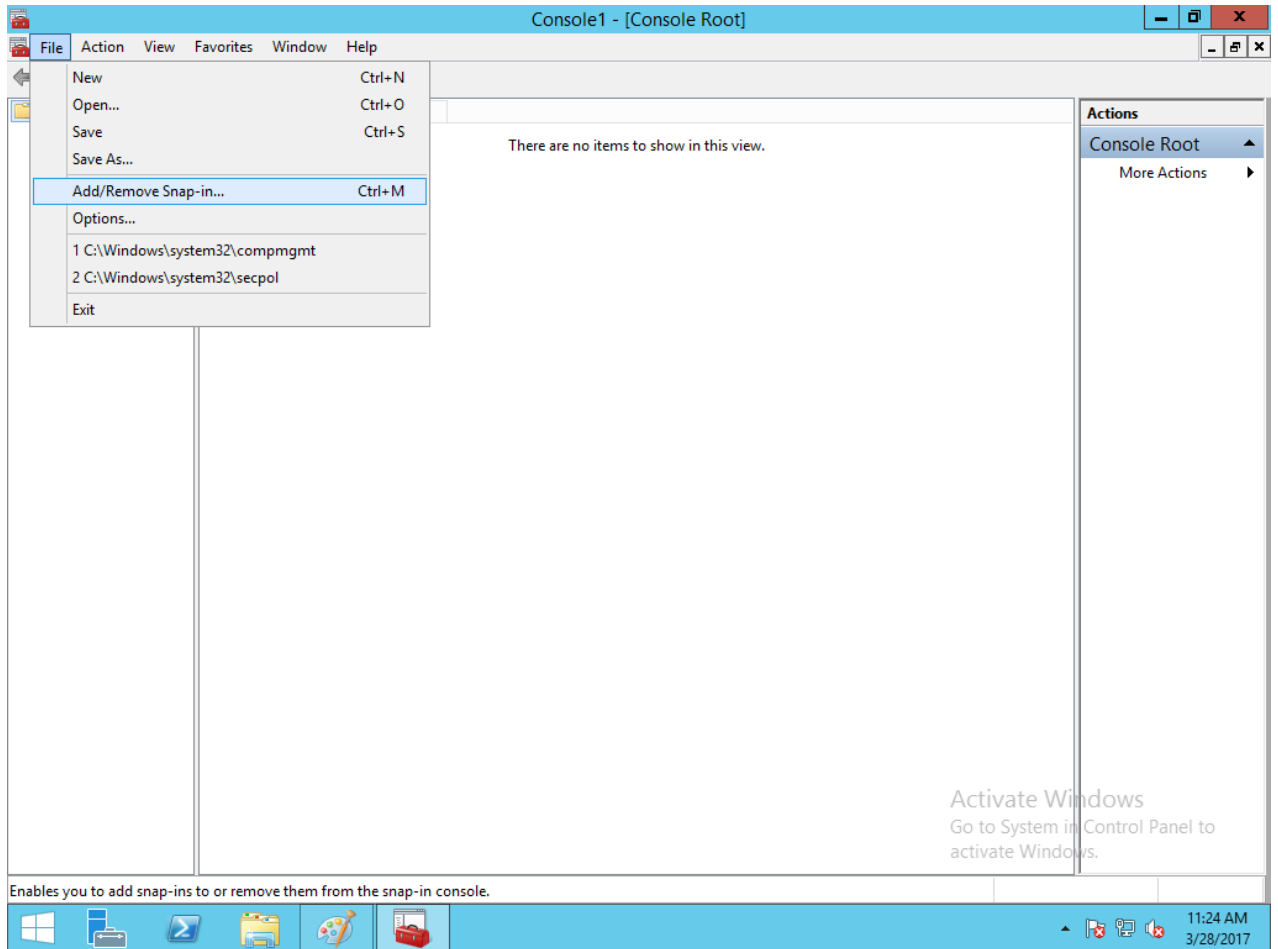
Существует возможность отключить аутентификацию пользователя по паре логин/пароль и оставить только аутентификацию по сертификатам на электронном ключе. В этом случае без смарт-карты или USB-токена **JaCarta** аутентифицироваться будет невозможно.

Для выполнения этой настройки необходимо на сервере с ролью домен контроллера выполнить следующие действия.

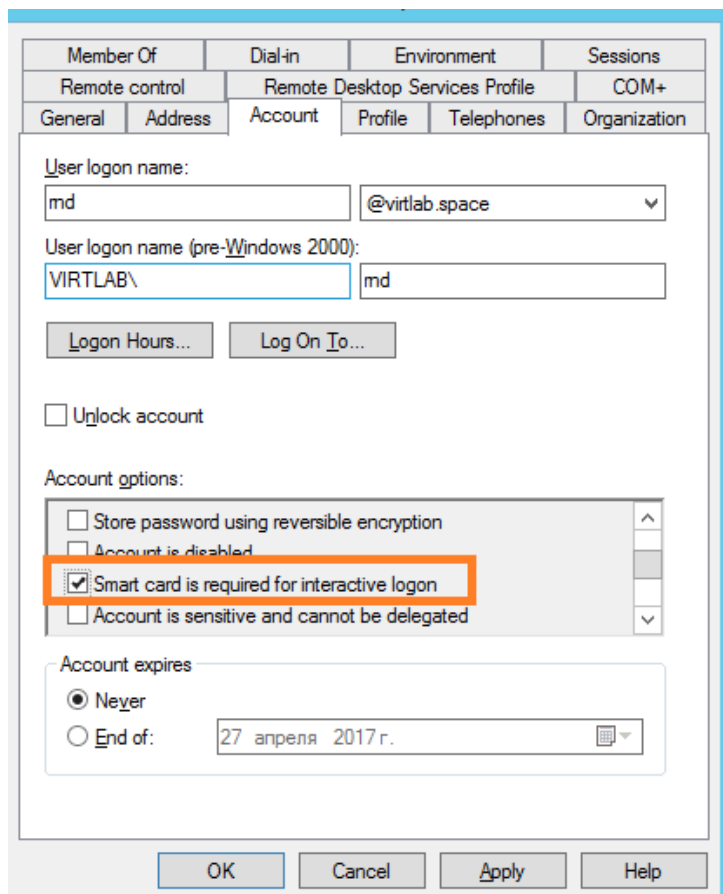
Откройте **MicrosoftManagementConsole (MMC(Консоль Управления Microsoft))**, для этого щёлкните правой кнопкой меню **Пуск**, в открывшемся окне щёлкните **Run (Выполнить)**, в отобразившемся окне наберите **mmc** и нажмите **OK**.



В отобразившемся окне выберите **File (Файл) ->Add/RemoveSnap-in... (Добавить или удалить оснастку...)**




В отобразившемся окне выберите оснастку **Active Directory Users and Computers (Active Directory — пользователи и компьютеры)**, выберите **Users (Пользователи)** и для пользователей, которым требуется запретить аутентификацию по паролю, выберите в их свойствах параметров **SmartCardisrequiredforinteractivelogon (Для интерактивного входа в сеть требуется смарт-карта)**.



После выполнения этих настроек аутентификация пользователя будет возможна только при наличии электронного ключа **JaCarta** и сертификата пользователя на нём. Обычный вход по паролю и логину работать не будет.


Настройка клиента

Для аутентификации по смарт-картам в RemoteDesktopServices со стороны клиента требуется настроенная на работу со смарт-картами рабочая станция. Это может быть полноценный ПК, ноутбук или тонкий клиент.

 Поддерживаются различные типы ОС, включая Linux, а также некоторые специализированные прошивки тонких клиентов, например, Dell/WyseThinOS.

Настройка подразумевает установку пакета драйверов и утилит для работы с электронными ключами **JaCarta** и сам клиент для RDP-соединения. Во всех современных ОС семейства Windows RDP-клиент встроен по умолчанию, по сути остаётся только настроить ярлык соединения или каждый раз открывать утилиту **RemoteDesktopConnection (Подключение к удалённому рабочему столу)** и вводить адрес сервера вручную. Настройка соединения в Windows будет показано ниже.


В следующей главе будет описан пример настройки соединения для Windows 7 и 10.

 Из-за многообразия и разрозненности дать однозначную инструкцию по настройке других операционных систем невозможно, поэтому следует эти сценарии рассматривать отдельно.

Проверка работоспособности

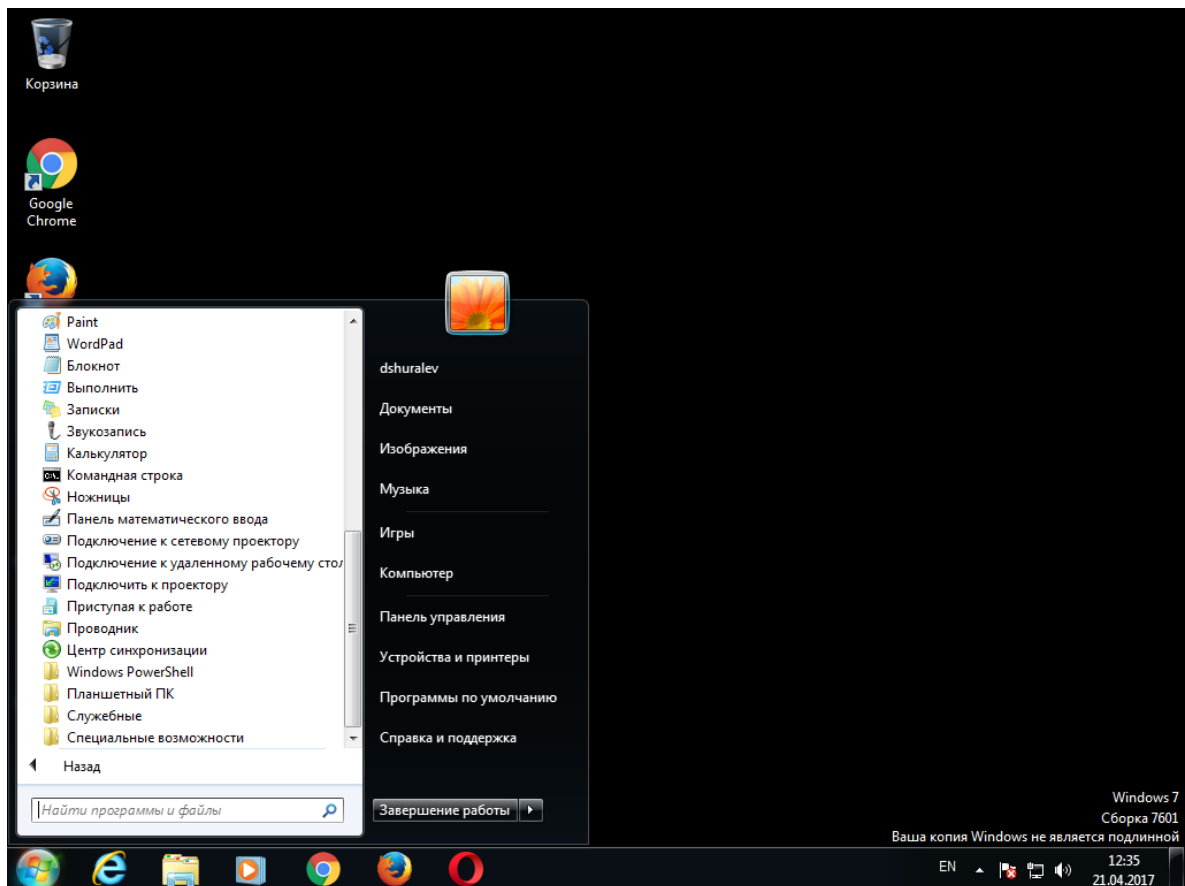
Для проверки работоспособности решения необходимо запустить две одновременно активных сессии двух разных пользователей. В настоящем примере это пользователь 1 с клиентской машиной Windows 7 и пользователь 2 клиентской машиной Windows 10.

Windows 7 (Пользователь 1)

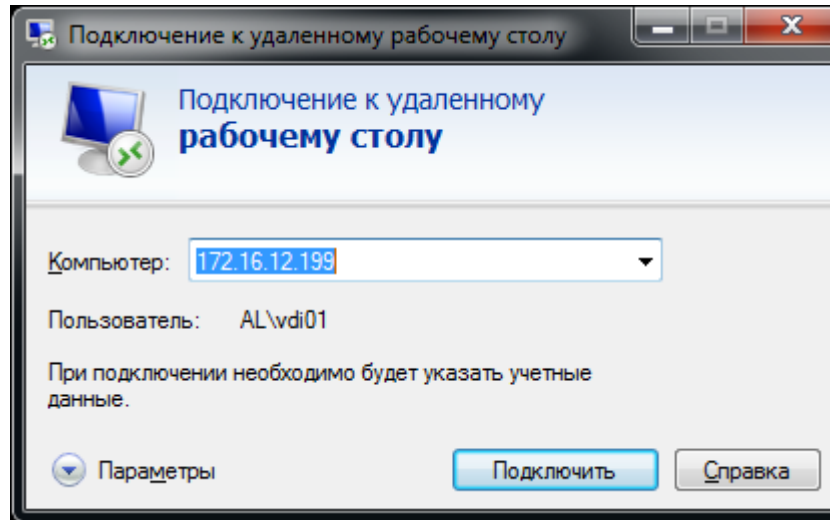
 Перед началом настройки убедитесь в том, что установлены драйвера и утилиты JaCarta — "Единый Клиент JaCarta" или "JC-Client". На самом ключе JaCarta должен находиться сертификат пользователя, выпущенный MSCA по шаблону "Пользователь со смарт-картой" или "Вход со смарт-картой".

Настройка подключения

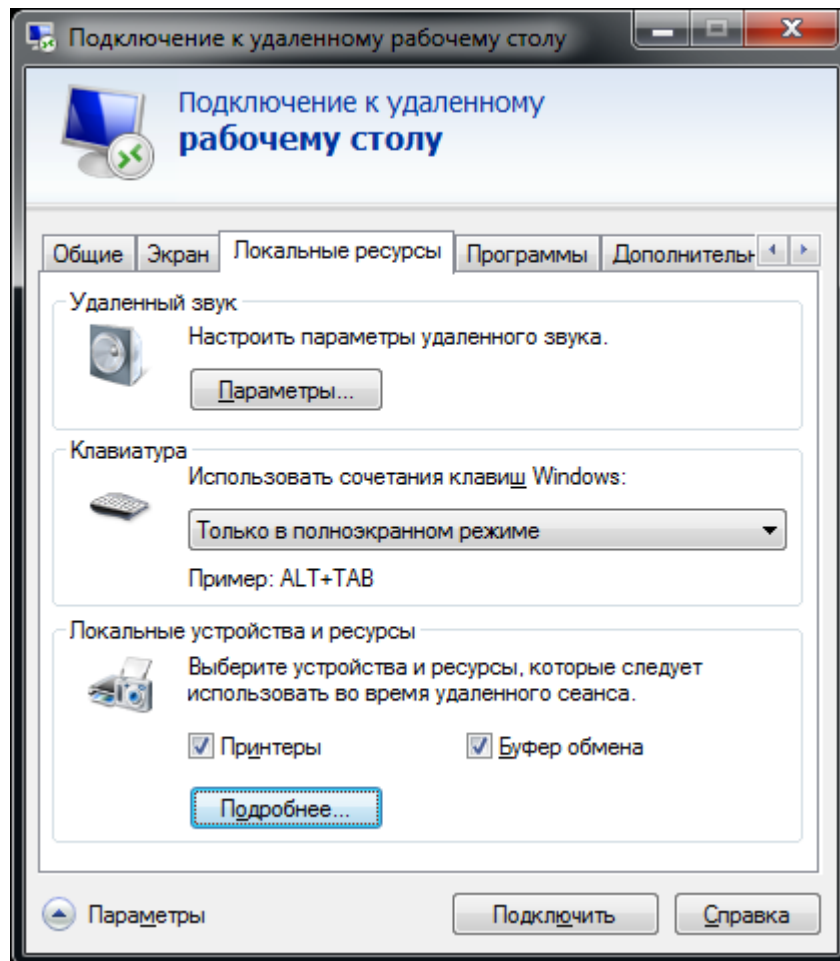
Для подключения к серверу откройте утилиту **Подключение к удалённому рабочему столу**, для этого нажмите **Пуск -> Все программы -> Стандартные -> Подключение к удалённому рабочему столу**.



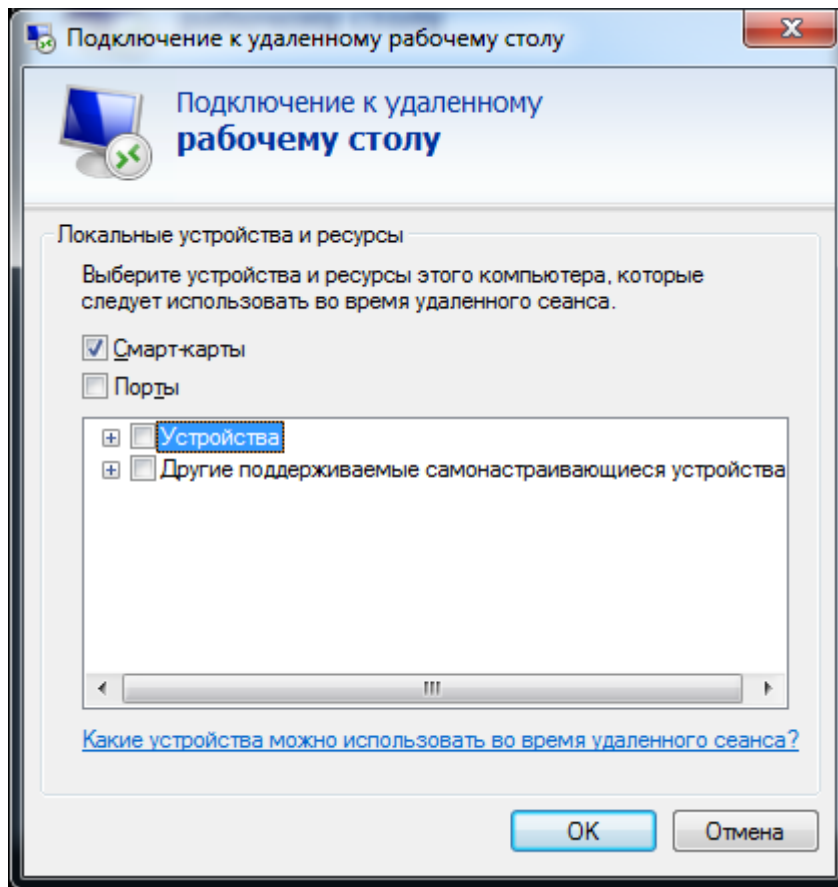
В отобразившемся окне выберите **Параметры**.



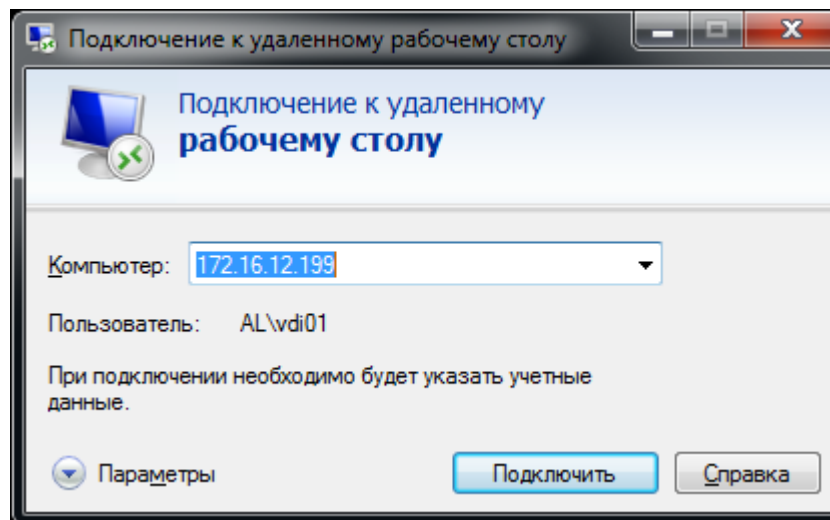
Перейдите на вкладку **Локальные ресурсы** и в поле **Локальные устройства и ресурсы** нажмите **Подробнее**.



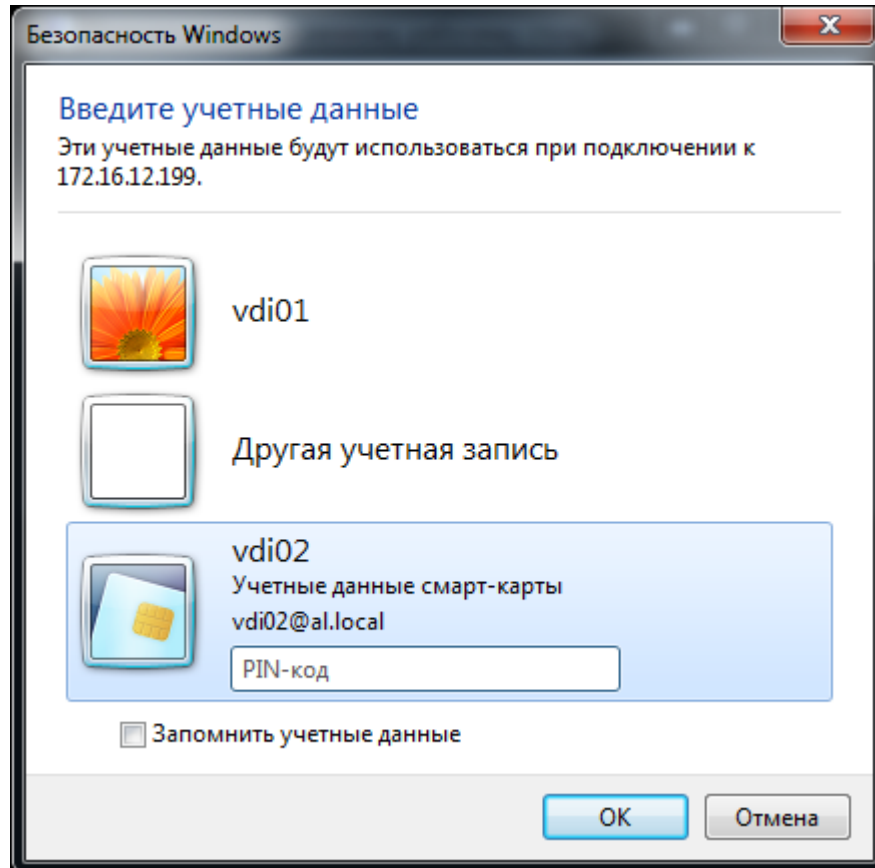
Если поле **Смарт-карты** не отмечено, отметьте его.



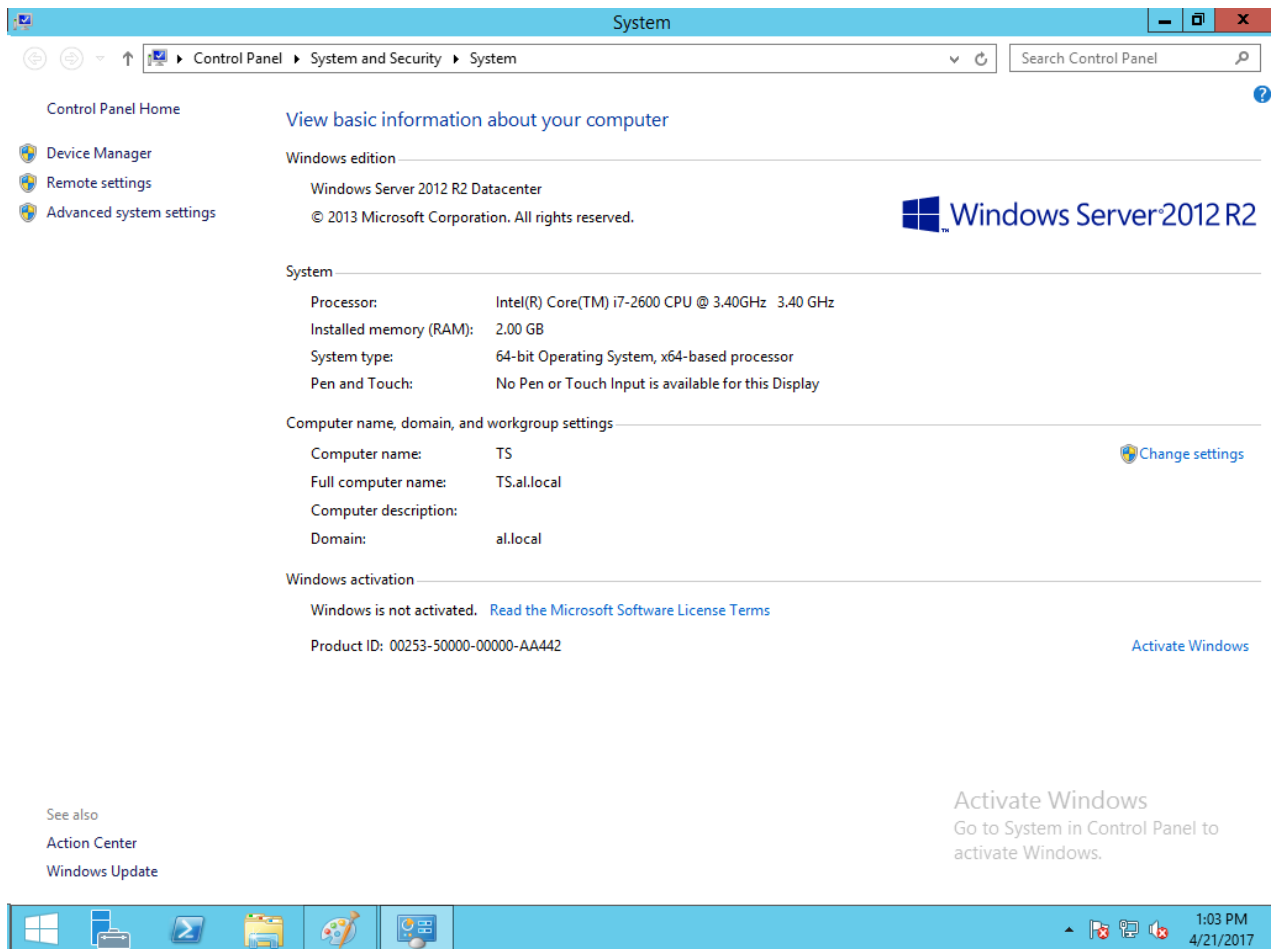
Сохраните изменения и выполните подключение к серверу, нажав **Подключить**.



В отобразившемся окне выберите **Учётные данные смарт-карты**, введите PIN-код и нажмите **ОК**.



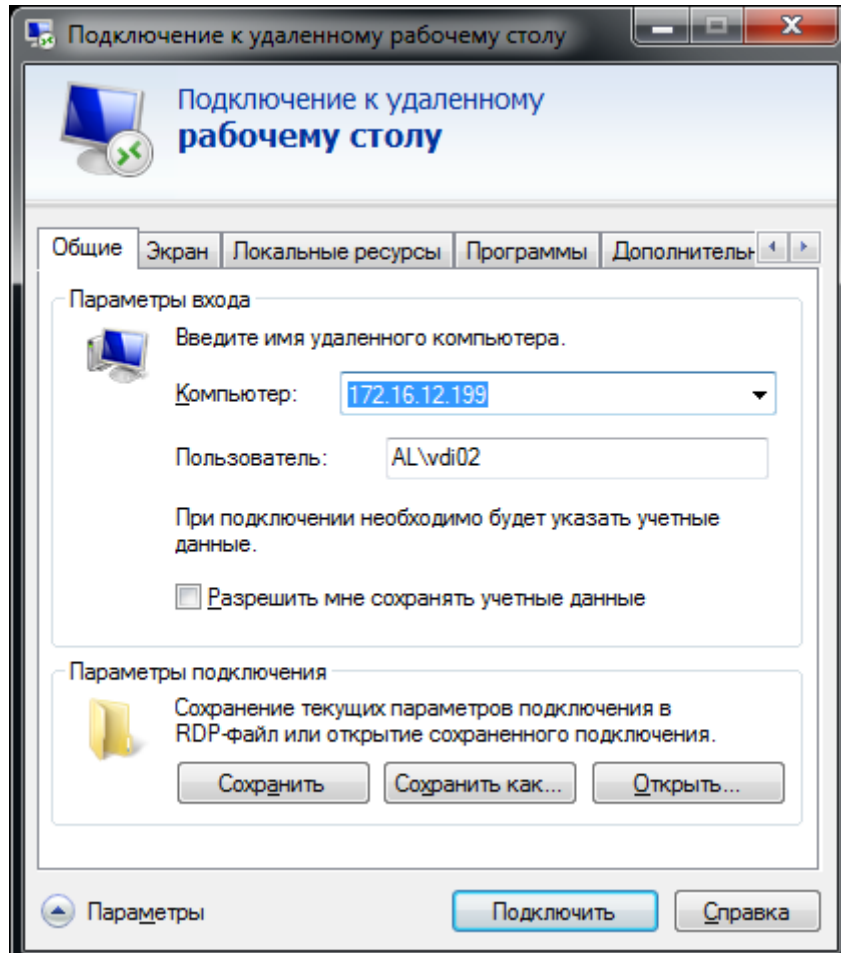
После аутентификации пользователь попадёт на свой виртуальный рабочий стол.



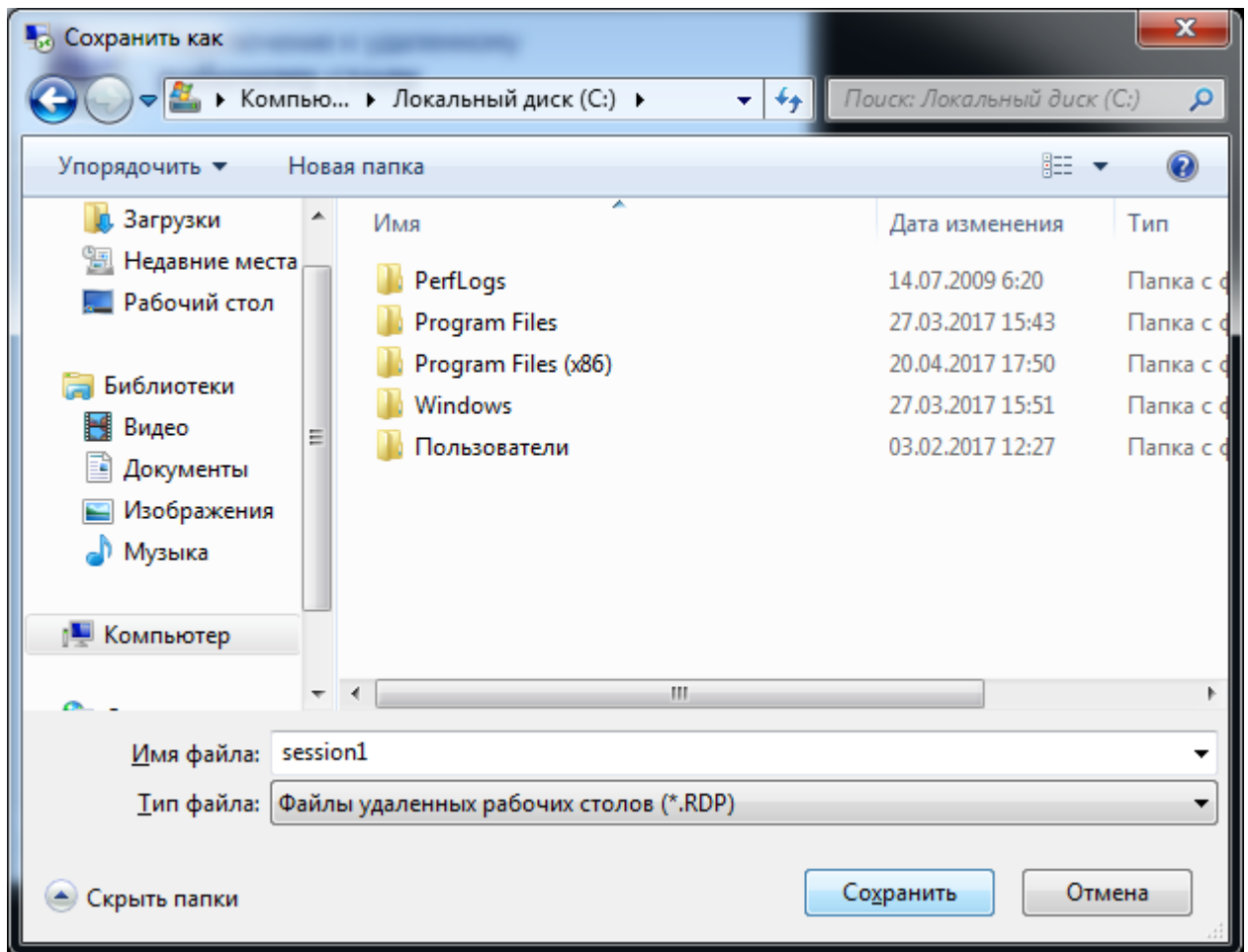
Создание ярлыка для быстрого подключения

Для того, чтобы каждый раз не вводить адрес сервера или другие настройки вручную, существует возможность создать ярлык быстрого доступа.

Для этого, открыв **Параметры**, перейдите во вкладку **Общее**. В поле **Параметры подключения** нажмите **Сохранить как...**



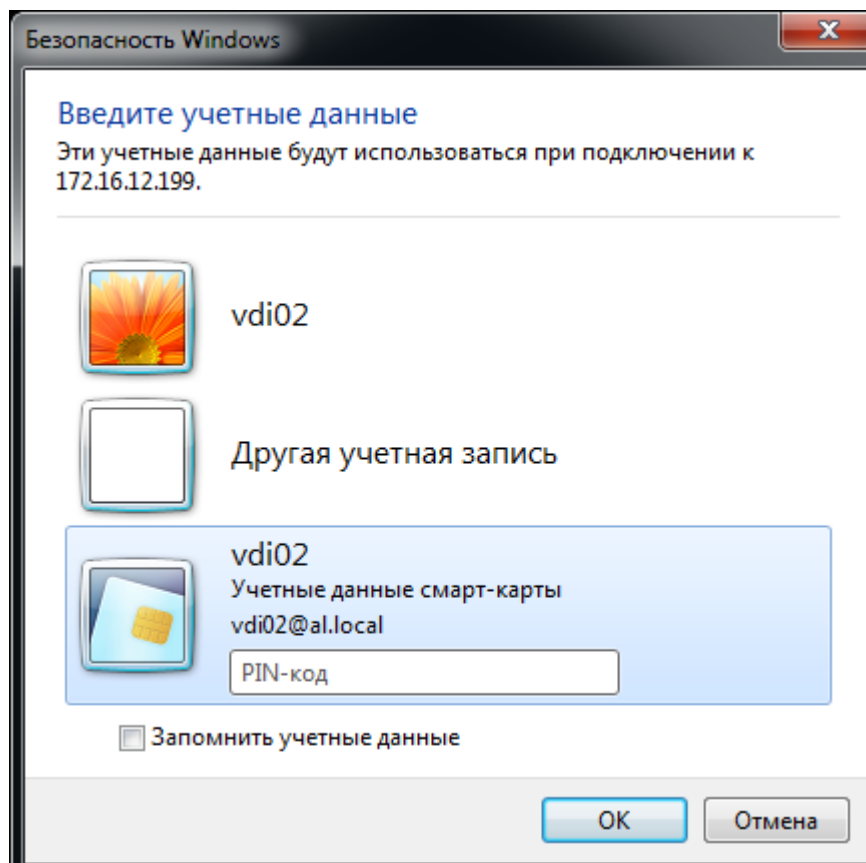
В отобразившемся окне укажите путь, куда следует сохранить ярлык быстрого доступа.



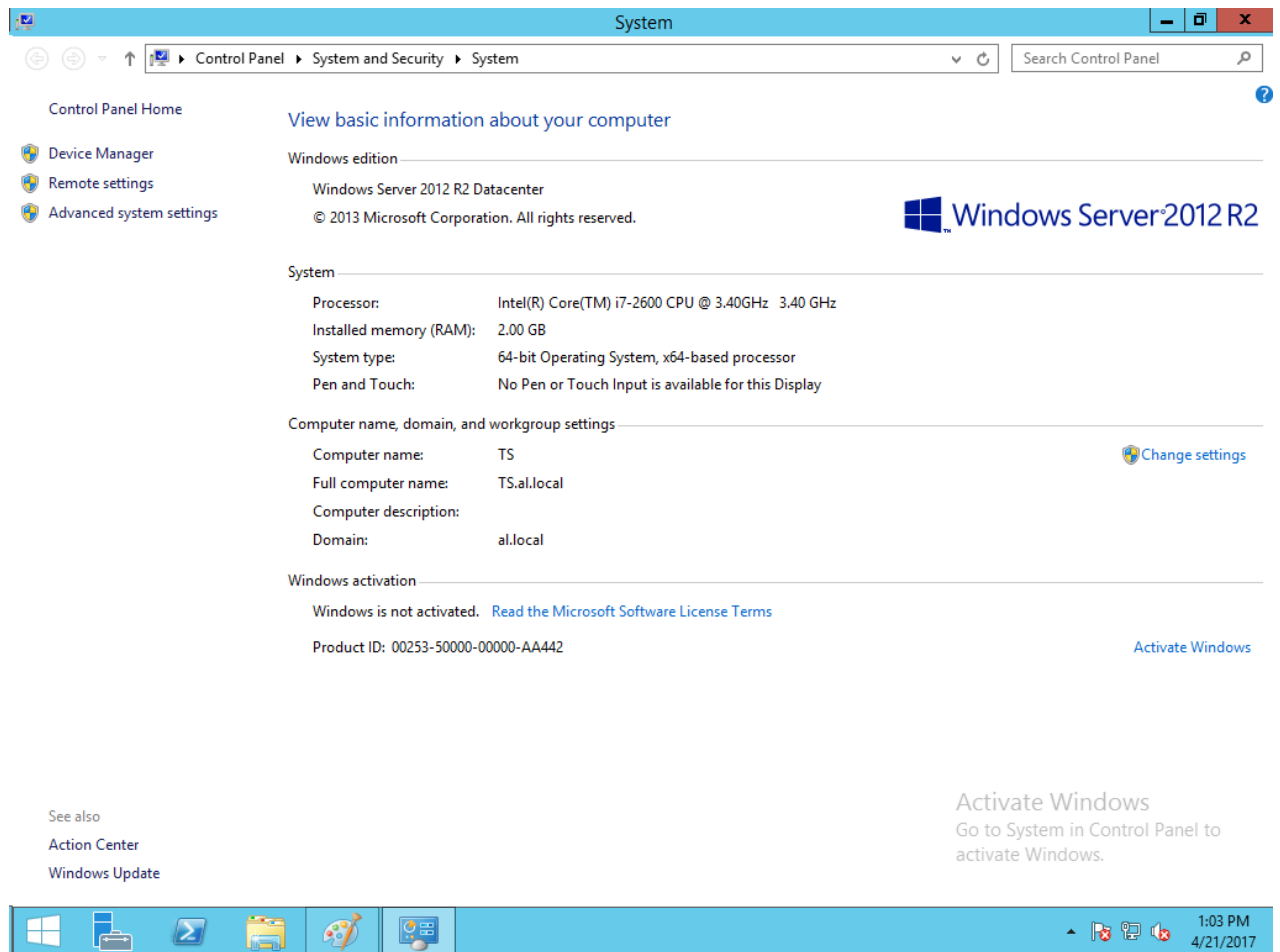
В настоящем примере файл помещён на рабочий стол.




Дважды щёлкнув по нему, система попросит предъявить PIN-код от JaCarta.




А после аутентификации пользователь попадёт на свой виртуальный рабочий стол.



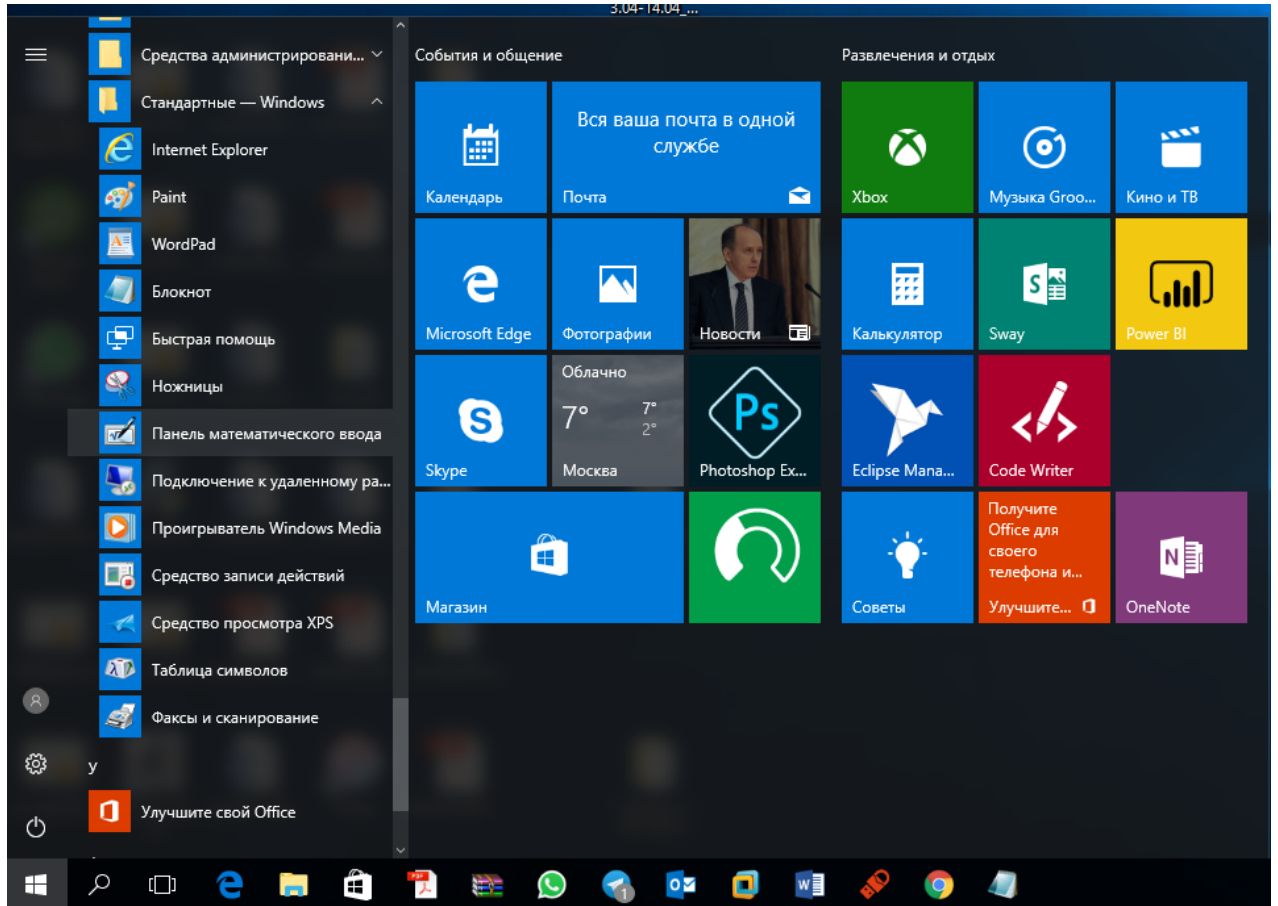
 Пользователь попадает в ту же сессию, из которой вышел в прошлый раз. Перезапуска программ и процессов не происходит.

Windows 10 (Пользователь 2)

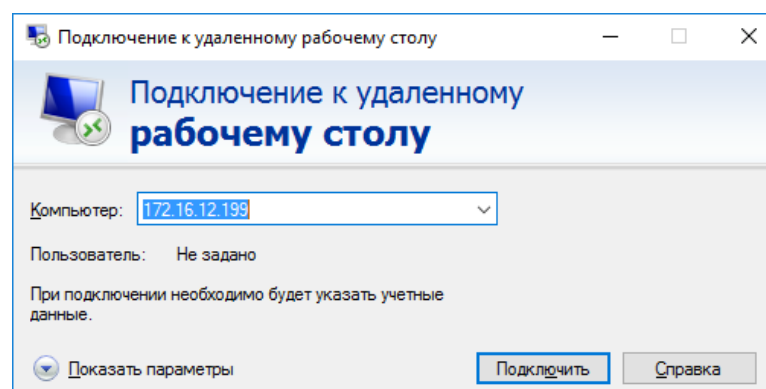
 Перед началом настройки убедитесь в том, что установлены драйвера и утилиты JaCarta — "Единый Клиент JaCarta" или "JC-Client". На самом ключе JaCarta должен находиться сертификат пользователя, выпущенный MSCA по шаблону "Пользователь со смарт-картой" или "Вход со смарт-картой".

Настройка подключения

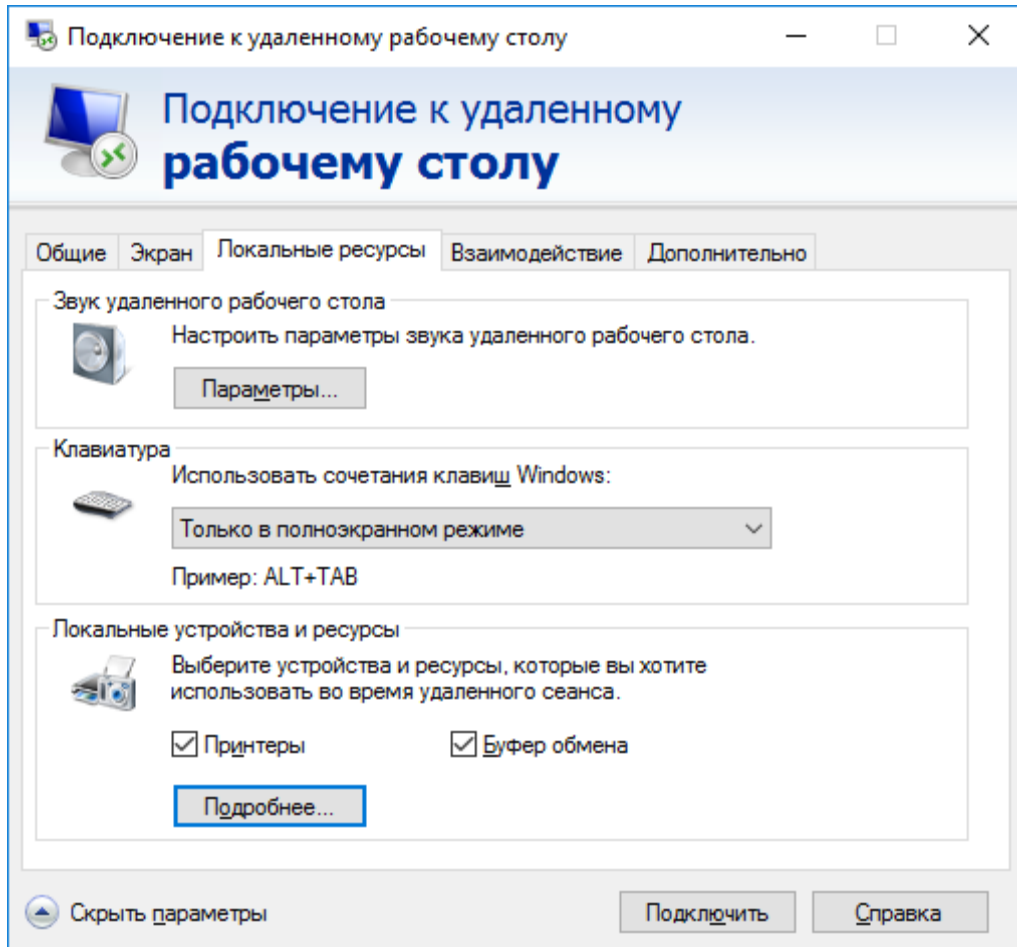
Для подключения к серверу откройте утилиту **Подключение к удалённому рабочему столу**, для этого нажмите **Пуск -> Все программы -> Стандартные -> Подключение к удалённому рабочему столу**.



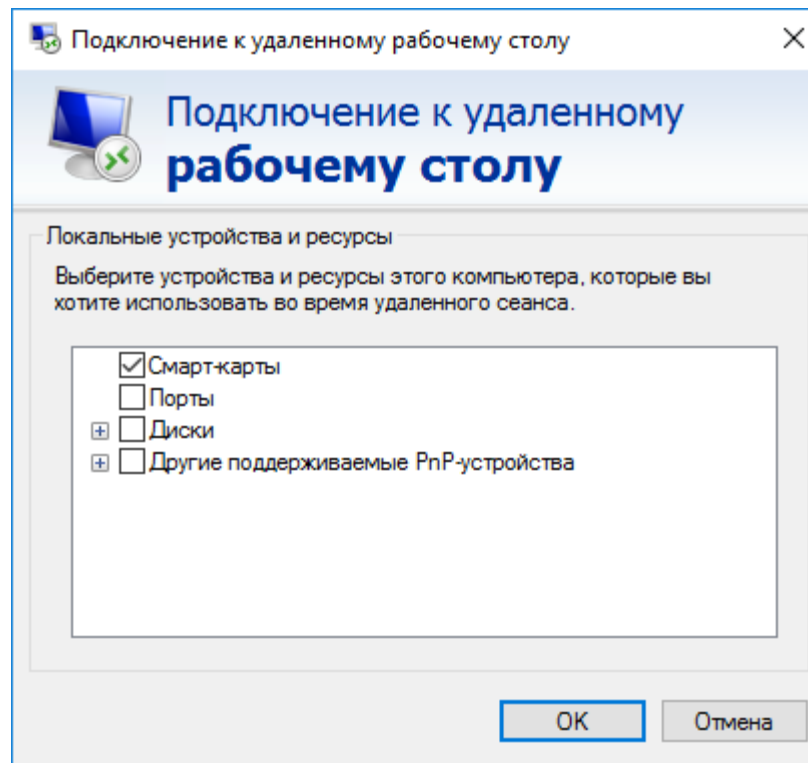
В отобразившемся окне выберите **Параметры**.



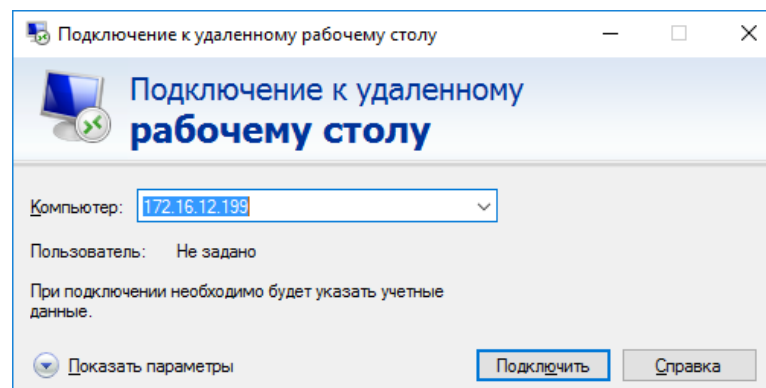
Перейдите на вкладку **Локальные ресурсы** и в поле **Локальные устройства и ресурсы** нажмите **Подробнее**.



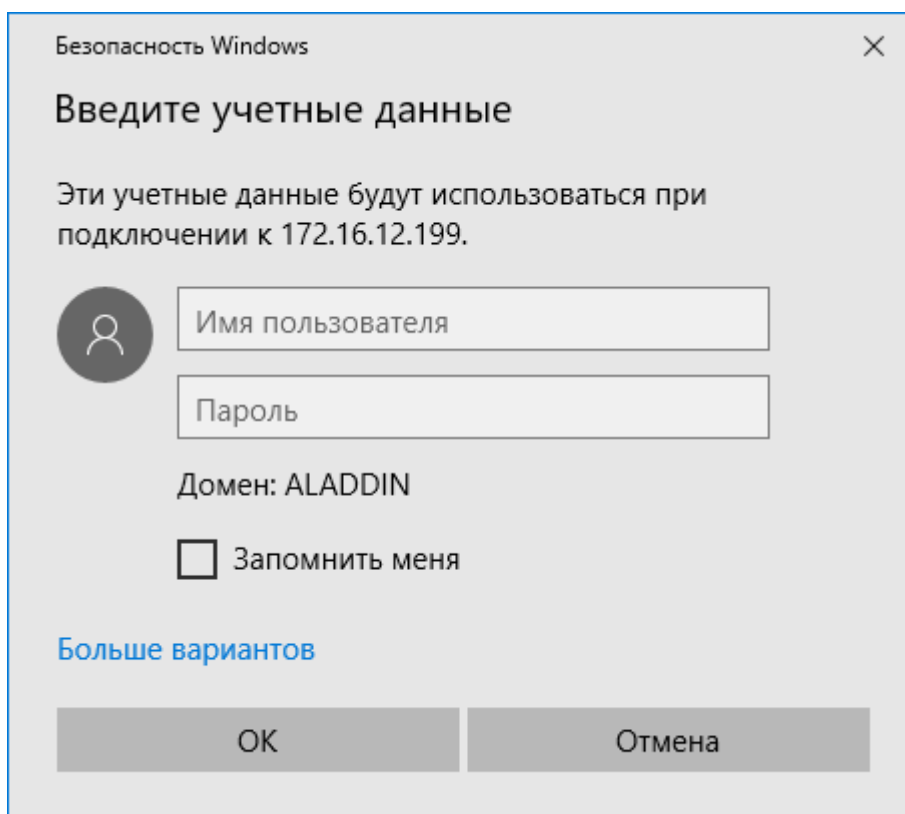
Если поле **Смарт-карты** не отмечено, отметьте его.



Сохраните изменения и выполните подключение к серверу, нажав **Подключить**.

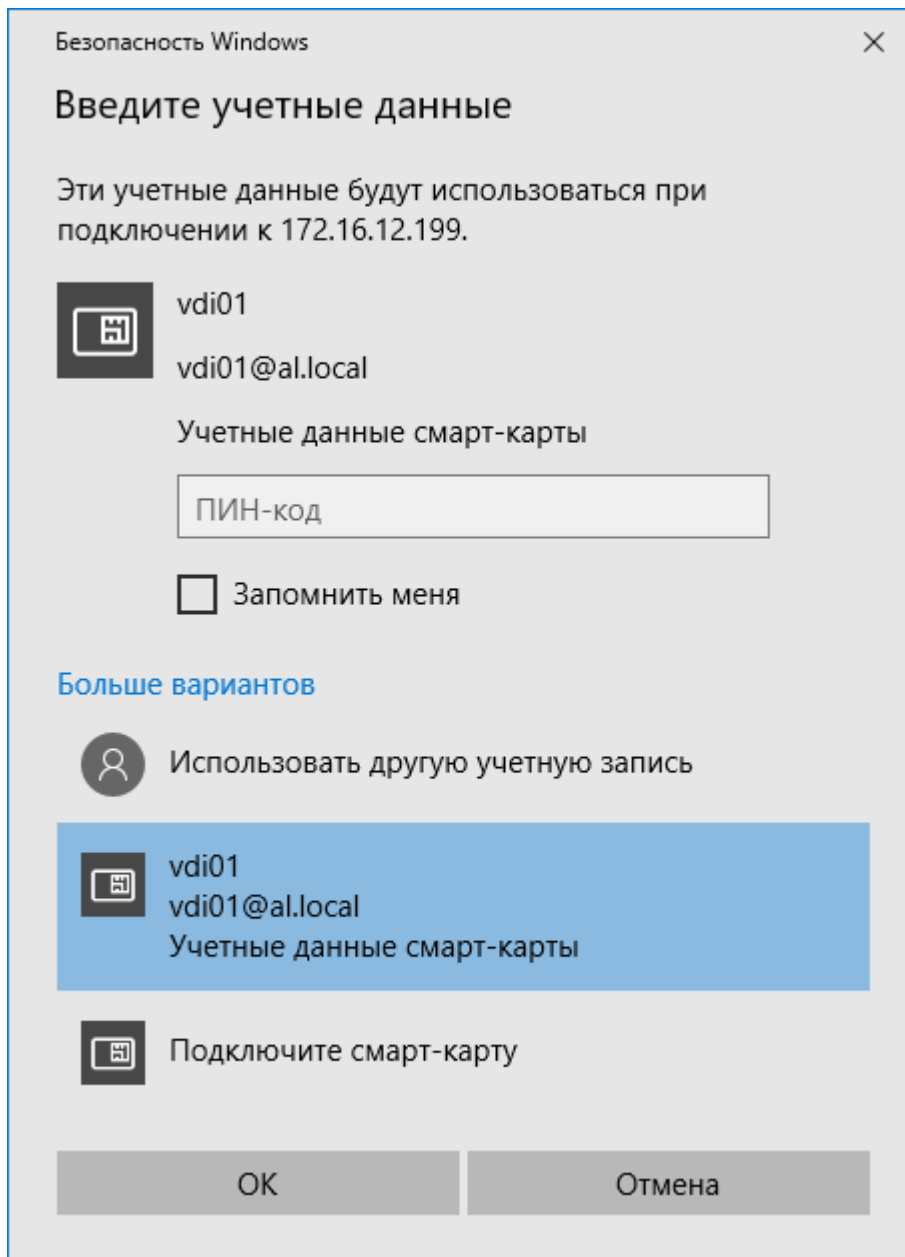


В отобразившемся окне выберите **Больше вариантов**.

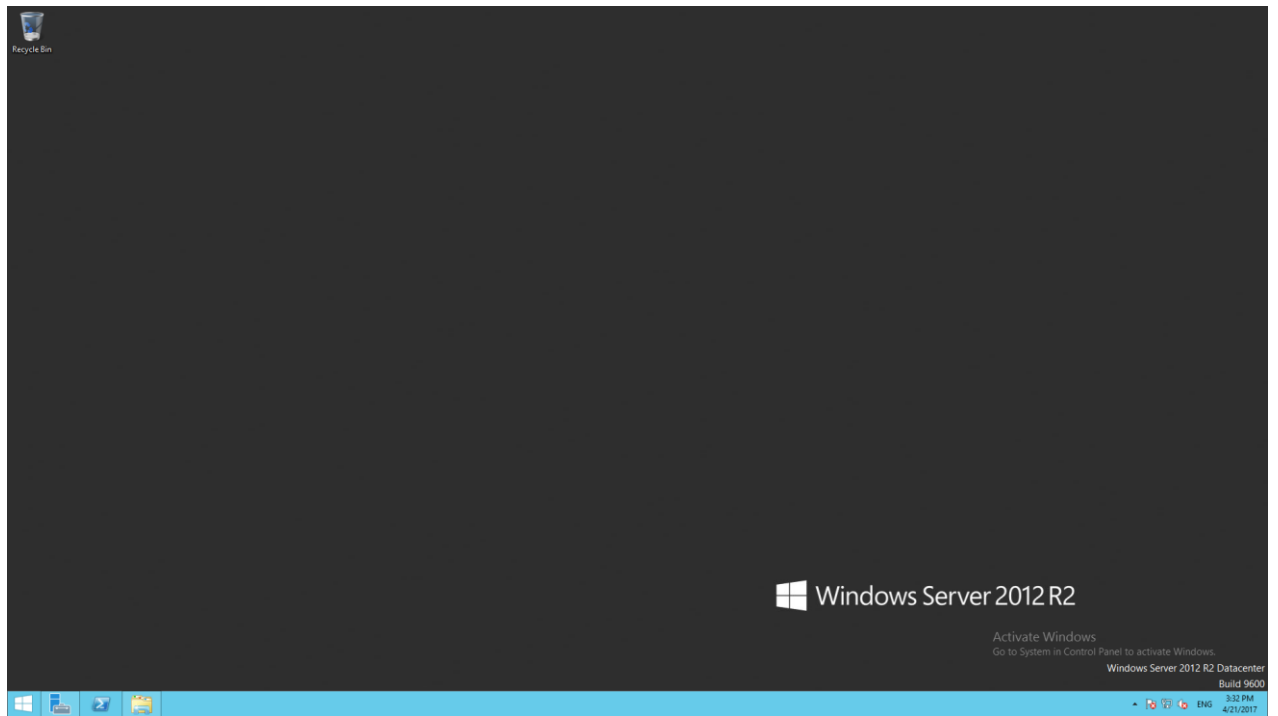


The image shows a Windows Security dialog box titled "Безопасность Windows" (Windows Security) with a close button (X) in the top right corner. The main heading is "Введите учетные данные" (Enter credentials). Below this, it states: "Эти учетные данные будут использоваться при подключении к 172.16.12.199." (These credentials will be used when connecting to 172.16.12.199.). There are two input fields: "Имя пользователя" (User name) and "Пароль" (Password). To the left of these fields is a circular icon containing a person silhouette. Below the password field, it says "Домен: ALADDIN" (Domain: ALADDIN). There is a checkbox labeled "Запомнить меня" (Remember me) which is currently unchecked. At the bottom left, there is a blue link that says "Больше вариантов" (More options). At the bottom, there are two buttons: "ОК" (OK) and "Отмена" (Cancel).

В отобразившемся окне выберите **Учётные данные смарт-карты**, введите PIN-код и нажмите **ОК**.



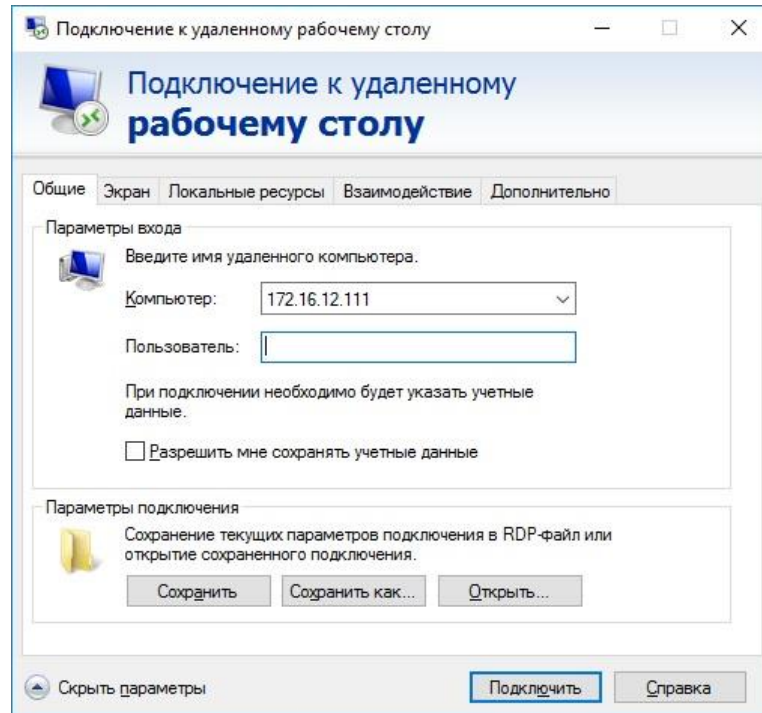
После аутентификации пользователь попадёт на свой виртуальный рабочий стол.



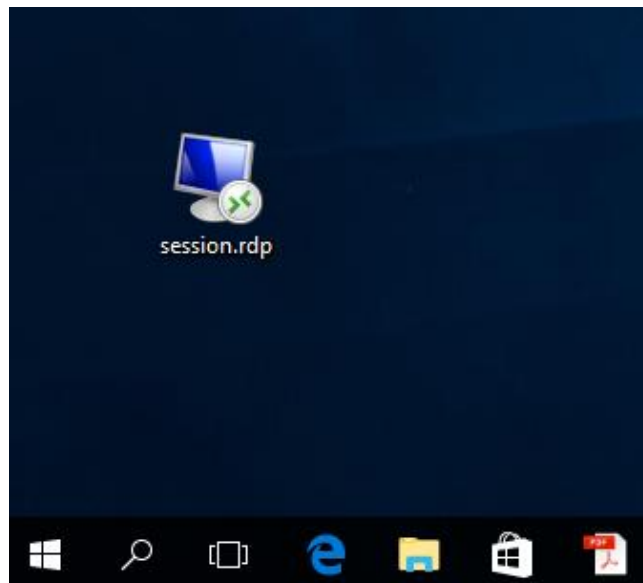
Создание ярлыка для быстрого подключения

Для того, чтобы каждый раз не вводить адрес сервера или другие настройки вручную, существует возможность создать ярлык быстрого доступа.

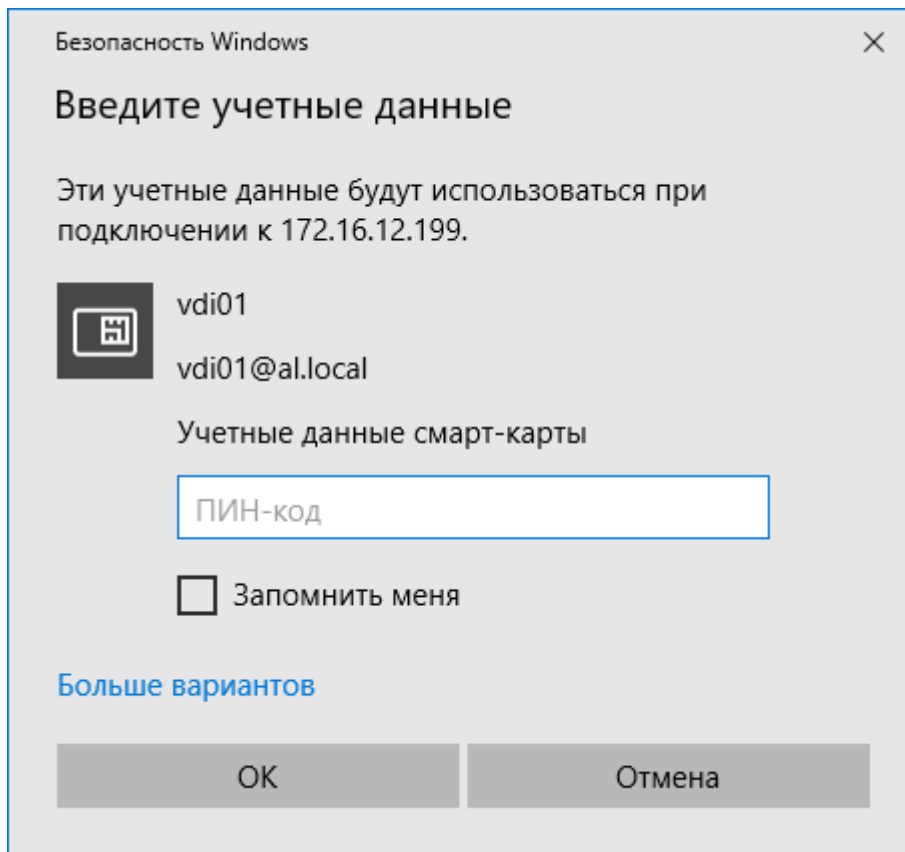
Для этого, открыв **Параметры**, перейдите во вкладку **Общее**. В поле **Параметры подключения** нажмите **Сохранить как...** и укажите путь для сохранения ярлыка быстрого доступа.



В настоящем примере полученный файл помещён на рабочий стол. Дважды щёлкнув по нему, система попросит предъявить PIN-код от JaCarta.




Введите PIN-код от **JaCarta**.



Безопасность Windows

Введите учетные данные

Эти учетные данные будут использоваться при подключении к 172.16.12.199.

 vdi01
vdi01@al.local

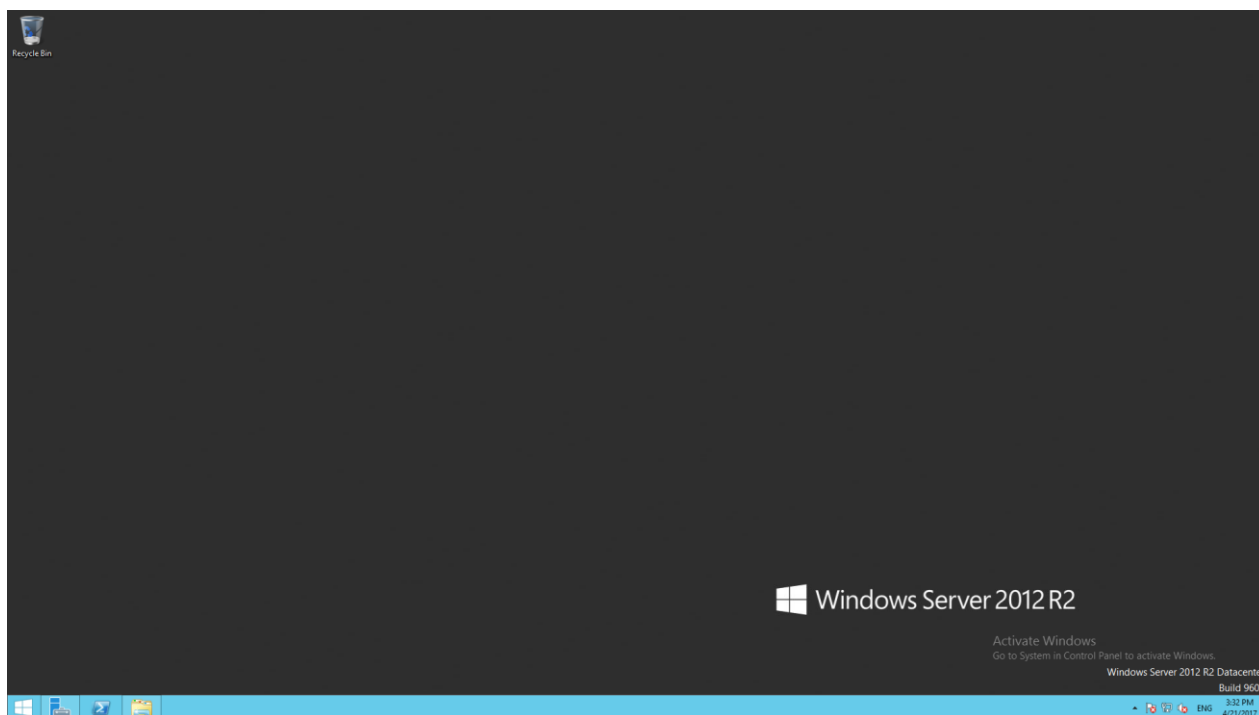
Учетные данные смарт-карты

Запомнить меня

[Больше вариантов](#)

ОК Отмена

После аутентификации пользователь попадёт на свой виртуальный рабочий стол.



 Пользователь попадает в ту же сессию, из которой вышел в прошлый раз. Перезапуска программ и процессов не происходит.

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
Лицензия Министерства обороны РФ № 1384 от 22.08.16
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 "АладдинР.Д.", 1995–2017. Все права защищены.

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