

3.1.3.3. Настройка доступа к сетям VPN по предъявлению токена

Раздел содержит инструкцию по настройке доступа к сетям VPN по предъявлению токена.

Для настройки необходим компьютер с установленной операционной системой **Windows 2019 Server Rus** и драйверами **Рутокен**, а также **дистрибутив этой ОС**.

Операционная система должна быть настроена как **Контроллер домена**. В системе должны быть установлены **Службы Сертификации**, **Служба Маршрутизация и удаленный доступ** (в брандмауэре Windows должно быть настроено разрешающее правило для этой службы), а пользователям выданы сертификаты типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.

Все описанные далее действия производятся с правами администратора системы.

Для примера используется учетная запись **Admin**.

Этапы настройки доступа к сетям VPN по предъявлению токена:

1 этап: Настройка маршрутизации и удаленного доступа.

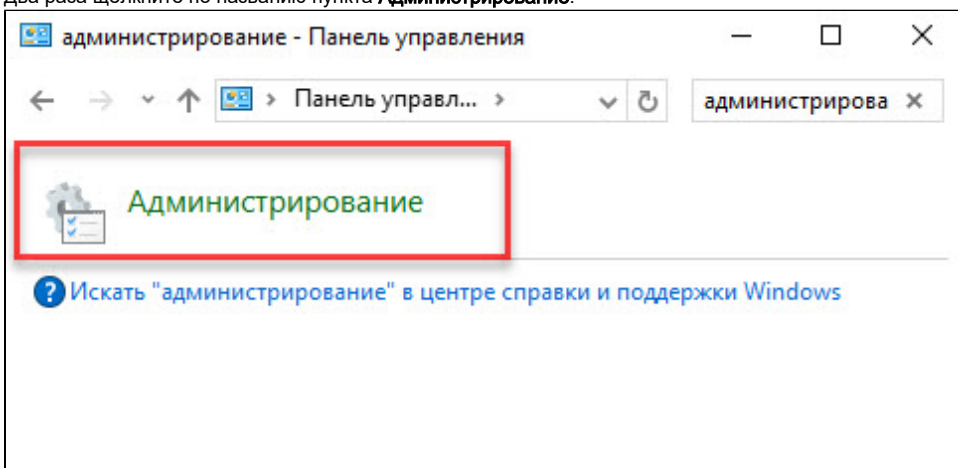
2 этап: Настройка учетных записей пользователей.

Настройка маршрутизации и удаленного доступа

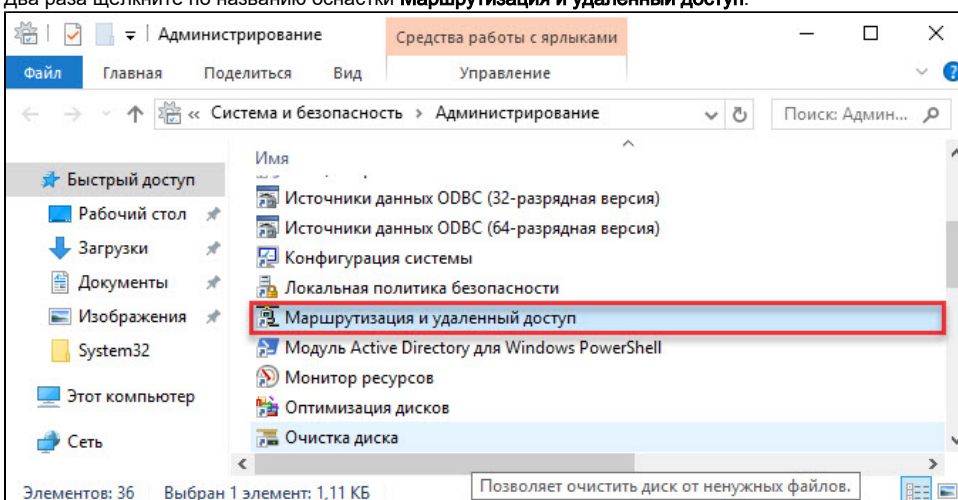
Перед настройкой маршрутизации и удаленного доступа необходимо убедиться, что на сервере установлены роли **Службы политики сети и доступа** и **Удаленный доступ**.

Для настройки маршрутизации и удаленного доступа:

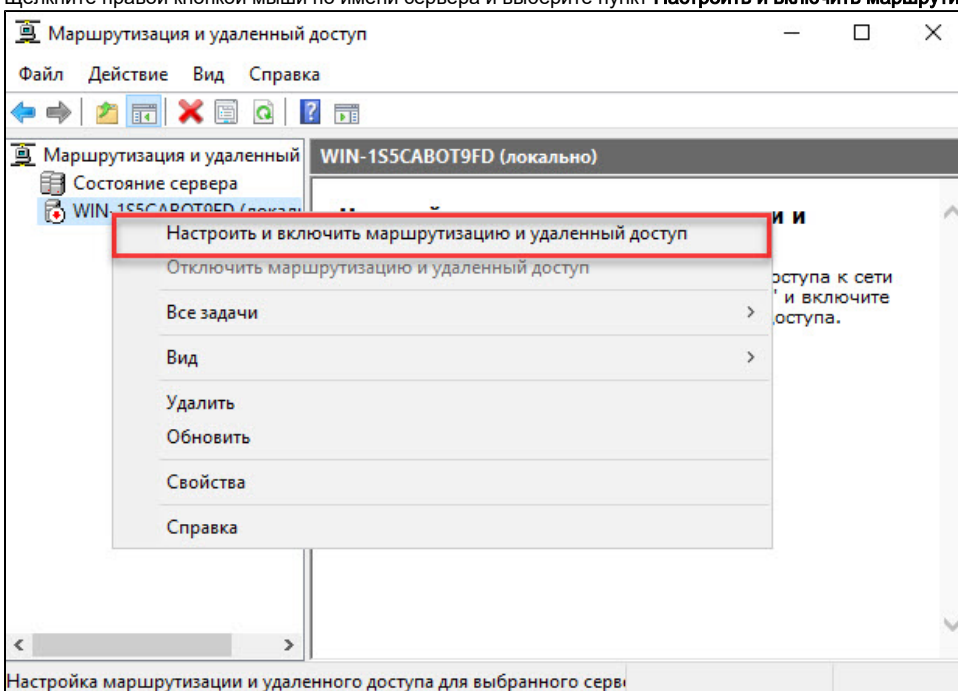
1. Откройте **Панель управления**.
2. В поле поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.



4. Два раза щелкните по названию оснастки **Маршрутизация и удаленный доступ**.



5. Щелкните правой кнопкой мыши по имени сервера и выберите пункт **Настроить и включить маршрутизацию и удаленный доступ**.



6. В окне **Мастер настройки сервера маршрутизации и удаленного доступа** нажмите **Далее**.

Мастер настройки сервера маршрутизации и удаленного доступа

Мастер установки сервера маршрутизации и удаленного доступа

Этот мастер помогает настроить сервер так, чтобы вы могли подключаться к другим сетям и разрешать подключения удаленных клиентов.

Для продолжения нажмите кнопку "Далее".

< Назад **Далее >** Отмена

7. Установите переключатель в положение **Особая конфигурация**, нажмите **Далее**.

Мастер настройки сервера маршрутизации и удаленного доступа

Конфигурация

Вы можете включить указанные службы в любом из этих сочетаний или выполнить настройку данного сервера.

- ☐ Удаленный доступ (VPN или модем)
Позволяет удаленным клиентам подключаться к этому серверу через удаленное подключение или безопасное подключение виртуальной частной сети (VPN)
- ☐ Преобразование сетевых адресов (NAT)
Позволяет внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.
- ☐ Доступ к виртуальной частной сети (VPN) и NAT
Позволяет удаленным клиентам подключаться к данному серверу через Интернет и внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.
- ☐ Безопасное соединение между двумя частными сетями
Позволяет подключить данную сеть к удаленной сети, например, к сети филиала.
- ☒ **Особая конфигурация**
Любая комбинация возможностей маршрутизации и удаленного доступа.

< Назад **Далее >** Отмена

8. Установите флажок **Доступ к виртуальной частной сети (VPN)** и нажмите **Далее**.

Мастер настройки сервера маршрутизации и удаленного доступа

Настраиваемая конфигурация
После закрытия этого мастера вы можете настроить выбранные службы на консоли маршрутизации и удаленного доступа.

Выберите службы, которые вы хотите включить на данном сервере.

☒ **Доступ к виртуальной частной сети (VPN)** **1**

☐ Удаленный доступ (через телефонную сеть)

☐ Подключения по требованию (для маршрутизации филиалов)

☐ Преобразование сетевых адресов (NAT)

☐ Маршрутизация локальной сети

2

< Назад **Далее >** Отмена

9. Убедитесь, что все необходимые функции сервера маршрутизации и удаленного доступа выбраны (поле **Сводка выбранных параметров**). Нажмите **Готово**.

Мастер настройки сервера маршрутизации и удаленного доступа

Завершение мастера сервера маршрутизации и удаленного доступа

Успешно завершена работа мастера сервера маршрутизации и удаленного доступа

Сводка выбранных параметров:

доступ к виртуальной частной сети (VPN)

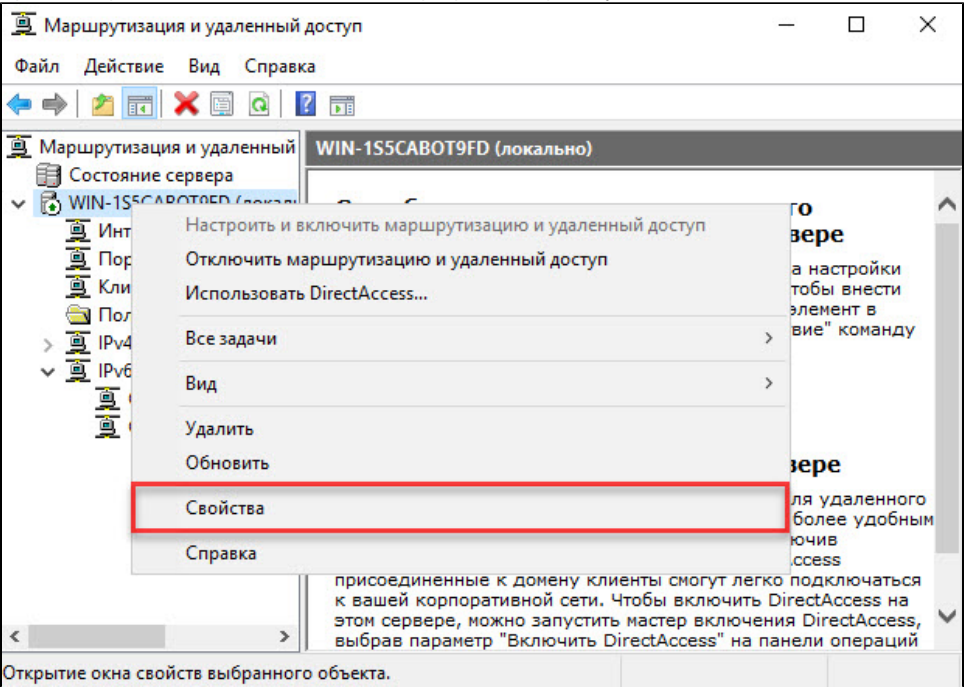
Закройте мастер и затем настройте выбранные службы на консоли маршрутизации и удаленного доступа.

Для закрытия мастера нажмите кнопку "Готово".

< Назад **Готово** Отмена

10. Нажмите **Запустить службу** и дождитесь завершения процесса запуска службы.

11. Щелкните правой кнопкой мыши по имени сервера и выберите пункт меню **Свойства**.



12. В окне со свойствами сервера перейдите на вкладку **Безопасность** и нажмите на кнопку **Методы проверки подлинности**.

Свойства: WIN-1S5CABOT9FD (локально) ? X

IKEv2	PPP	Ведение журнала	
Общие	Безопасность	IPv4	IPv6

Поставщик службы проверки подлинности проверяет учетные данные клиентов удаленного доступа и маршрутизаторов вызова по требованию.

Поставщик службы проверки подлинности:

Windows - проверка подлинности [Настроить...]

Методы проверки подлинности...

Поставщик учета ведет журнал сеансов и запросов на подключение.

Поставщик учета:

Windows - учет [Настроить...]

Пользовательская политика IPsec задает общий ключ для L2TP- и IKEv2-подключений. Чтобы настроить данный параметр, следует запустить службу маршрутизации и удаленного доступа. Инициаторы IKEv2, настроенные на проверку подлинности на этом сервере с помощью сертификата, не смогут выполнить подключение.

☐ Разрешить пользовательские политики IPsec для L2TP- и IKEv2-подключения

Общий ключ:

Привязка сертификата SSL

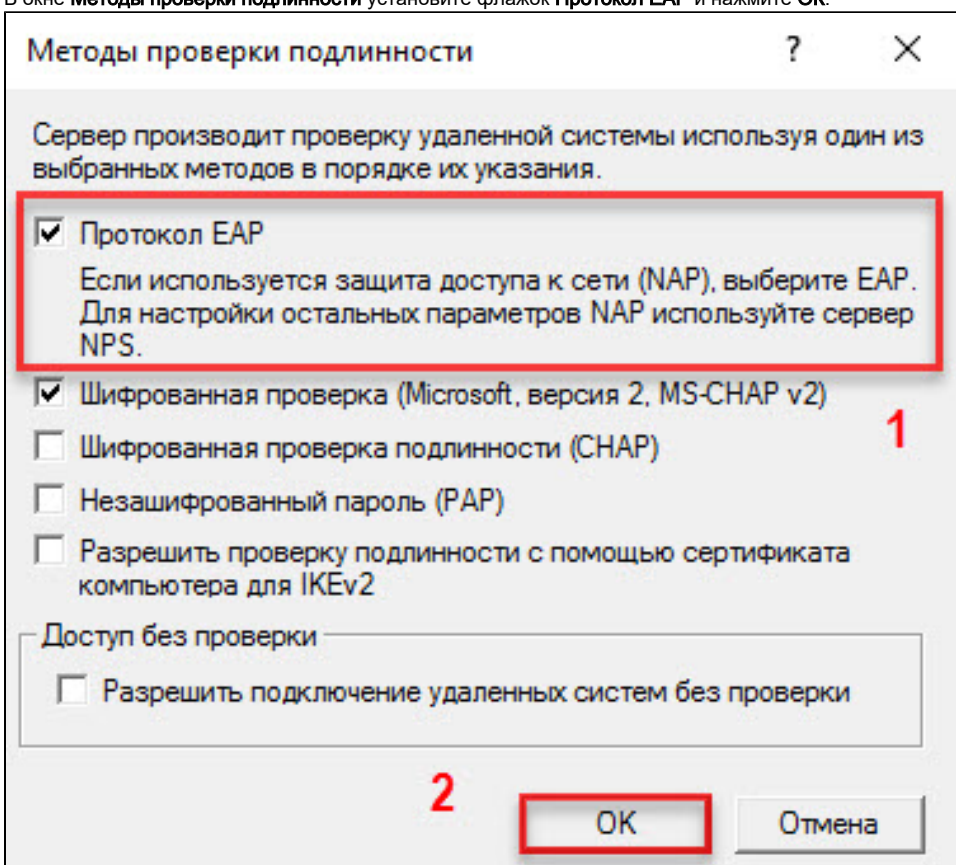
☐ Использовать HTTP

Выберите сертификат, который должен использовать SSTP-сервер для привязки SSL (веб-прослушиватель)

Сертификат: По умолчанию [Просмотр]

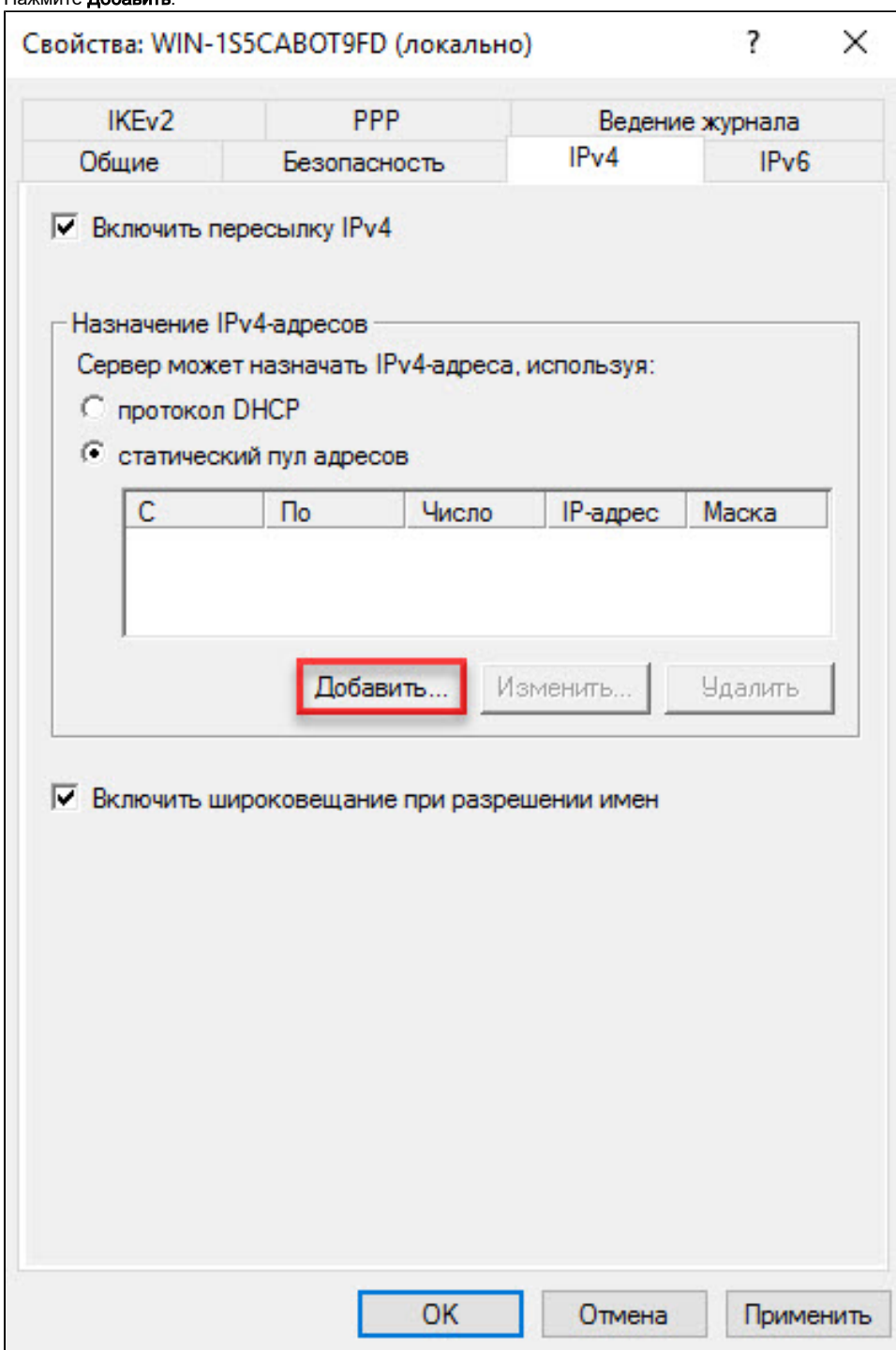
OK Отмена Применить

13. В окне **Методы проверки подлинности** установите флажок **Протокол EAP** и нажмите **ОК**.



14. В нашем примере на компьютере не настроена служба DHCP. Поэтому удаленным клиентам сначала необходимо назначить IP-адреса из заданного диапазона. Перейдите на вкладку **IPv4** и установите переключатель в положение **статистический пул адресов**.

15. Нажмите **Добавить**.



16. Введите начало и конец диапазона IP-адресов, нажмите **ОК**.

Новый диапазон IPv4-адресов?×

Введите начальный IP-адрес и либо конечный IP-адрес, либо количество адресов в непрерывном диапазоне.

Начальный IP-адрес:

192 . 168 . 60 . 0

Конечный IP-адрес:

192 . 168 . 60 . 254

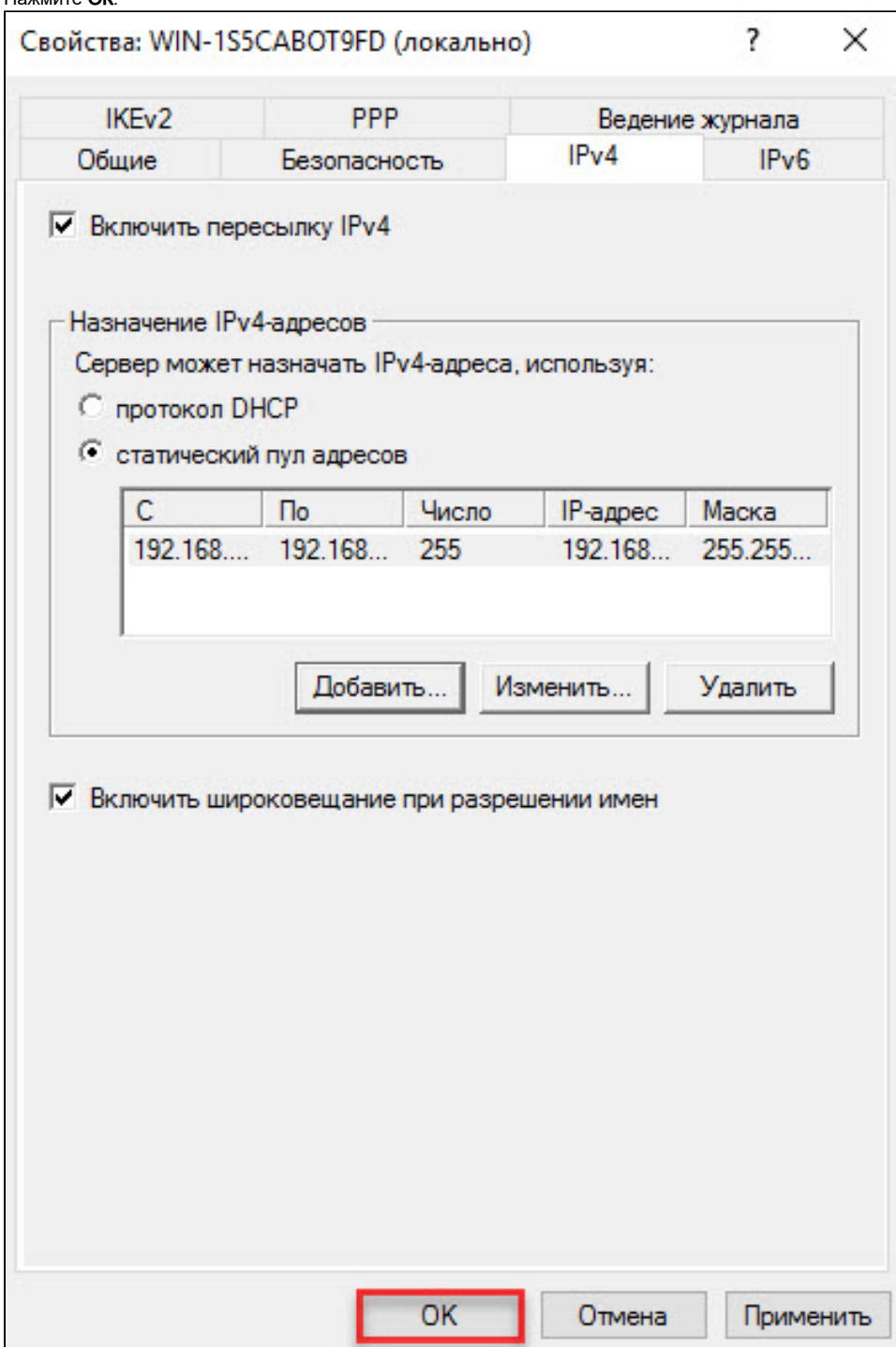
Количество адресов:

255

ОК

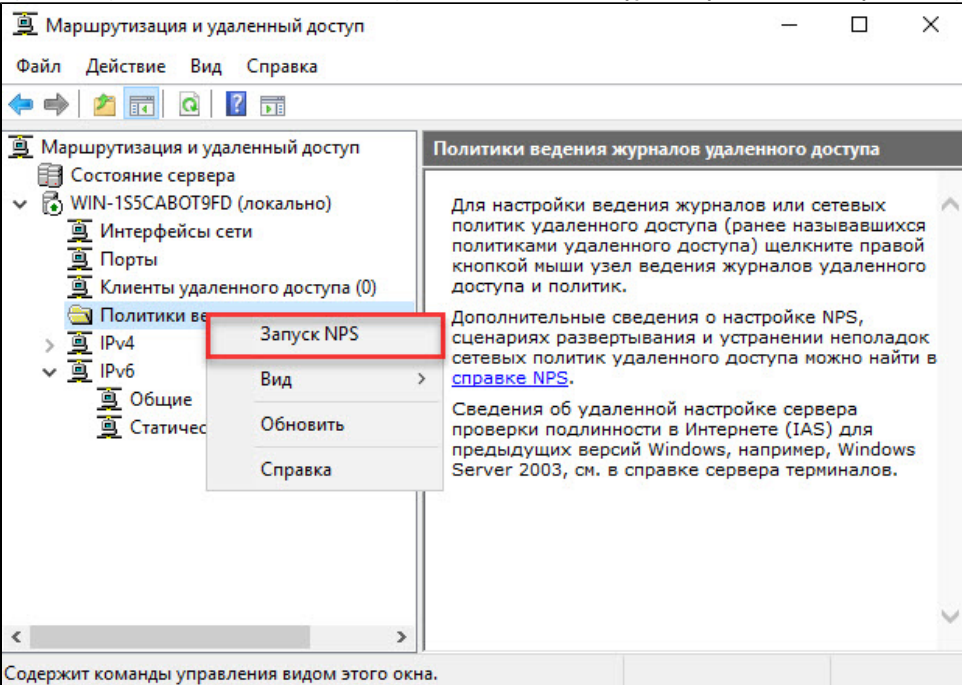
Отмена

17. Нажмите ОК.

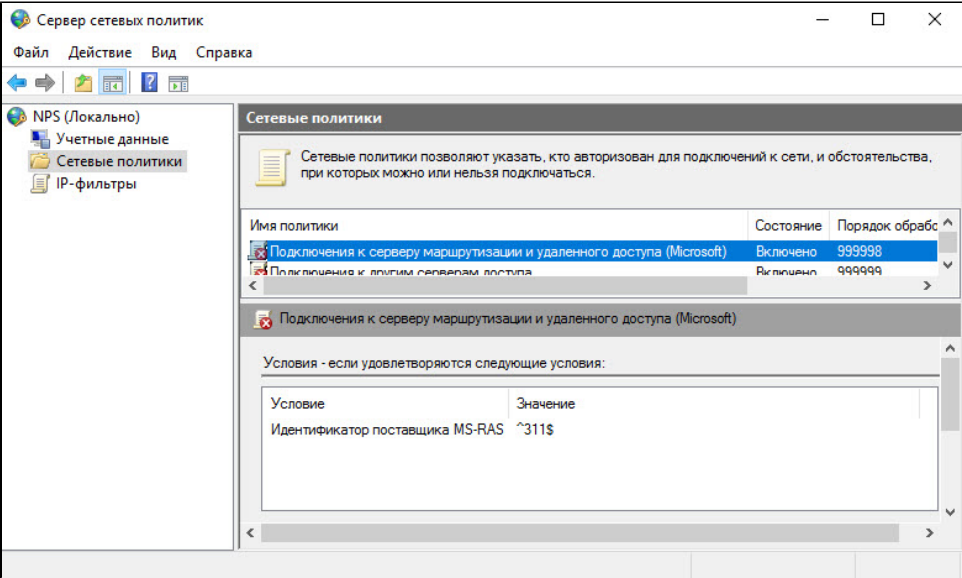


18. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Обновить**.

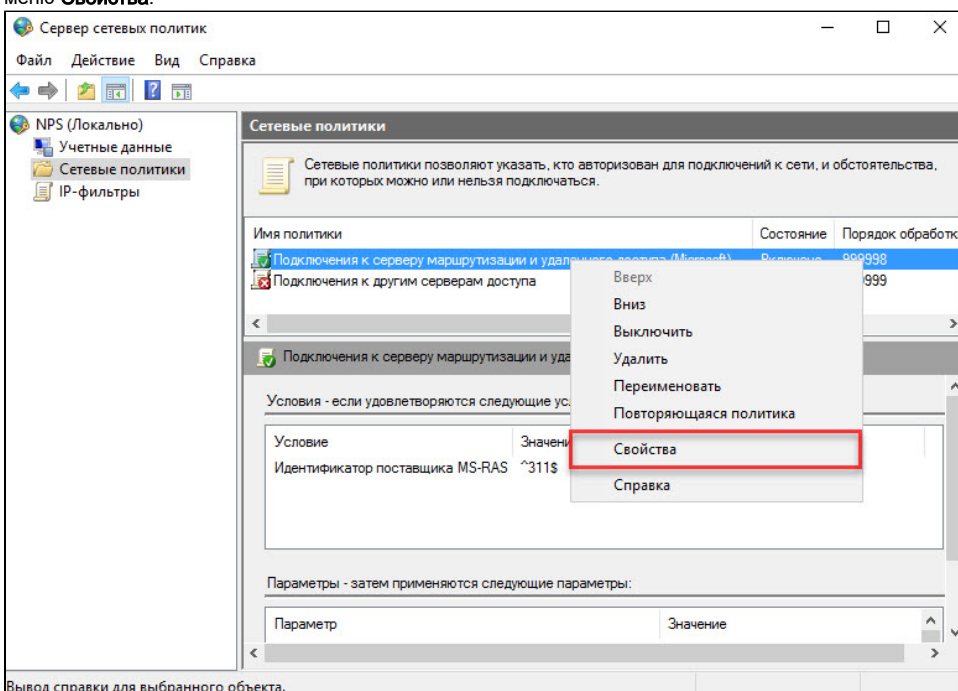
19. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Запуск NPS**.



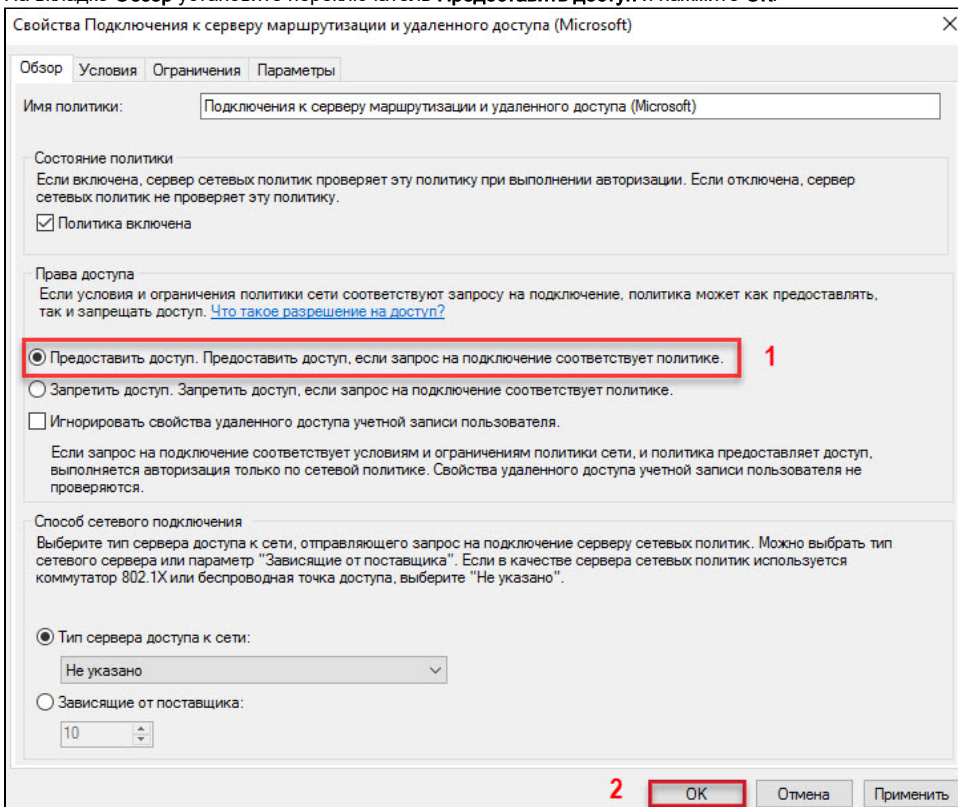
20. В окне **Сервер сетевых политик** щелкните по названию категории **Сетевые политики**.



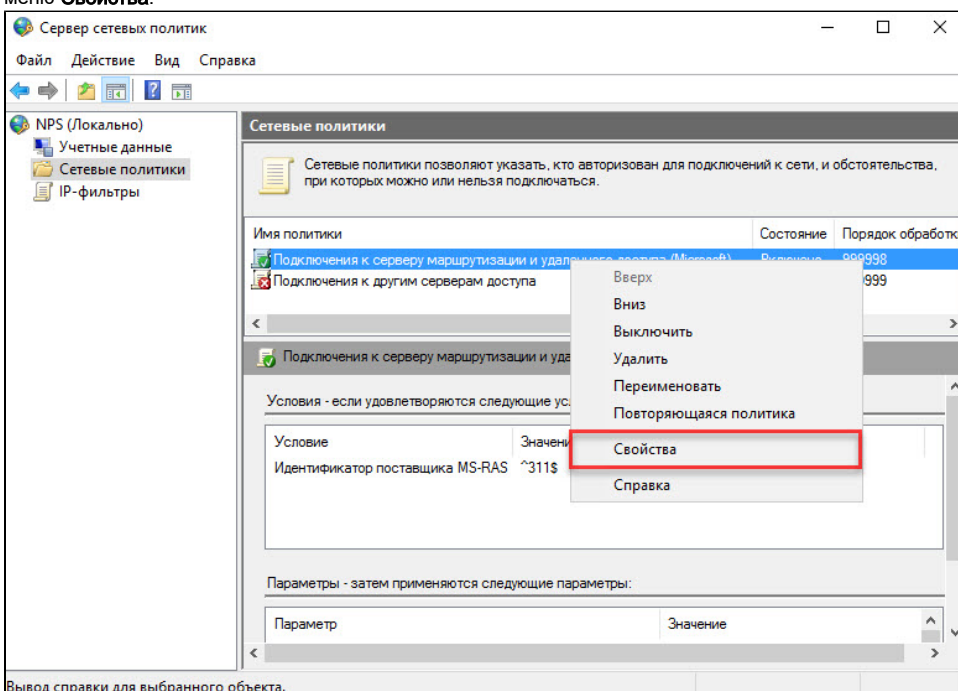
21. Кликните правой кнопкой мыши по строке **Подключение к серверу маршрутизации и удаленного доступа (Microsoft)** и выберите пункт меню **Свойства**.



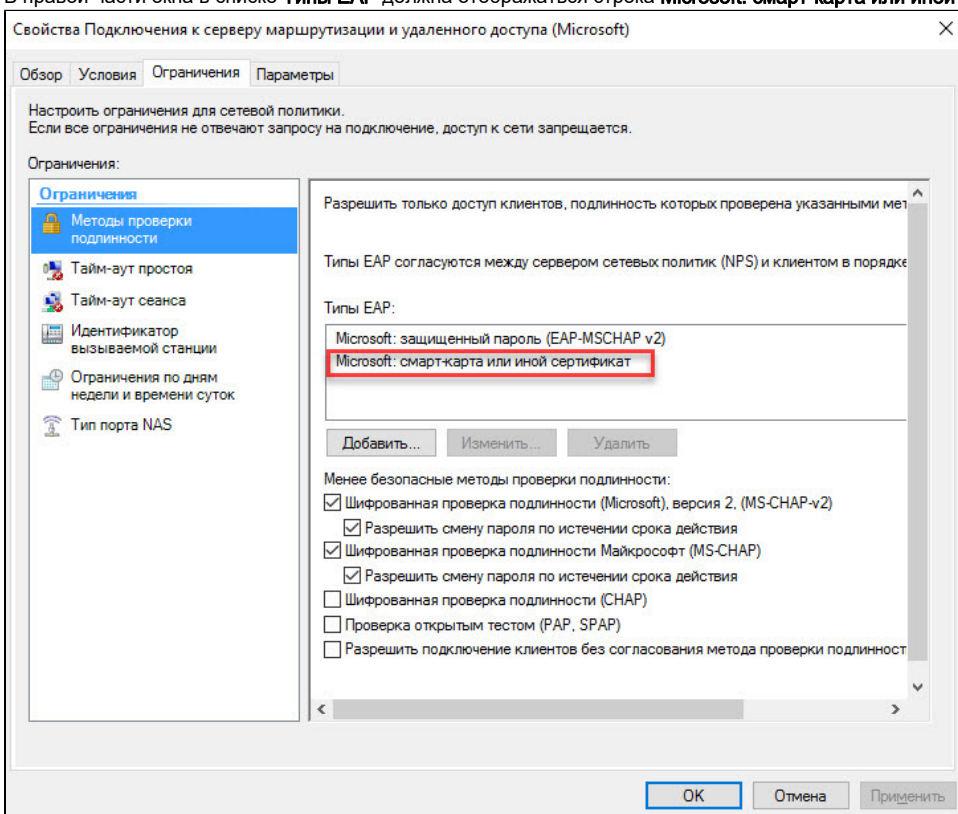
22. На вкладке **Обзор** установите переключатель **Предоставить доступ** и нажмите **ОК**.



23. Кликните правой кнопкой мыши по строке **Подключение к серверу маршрутизации и удаленного доступа (Microsoft)** и выберите пункт меню **Свойства**.

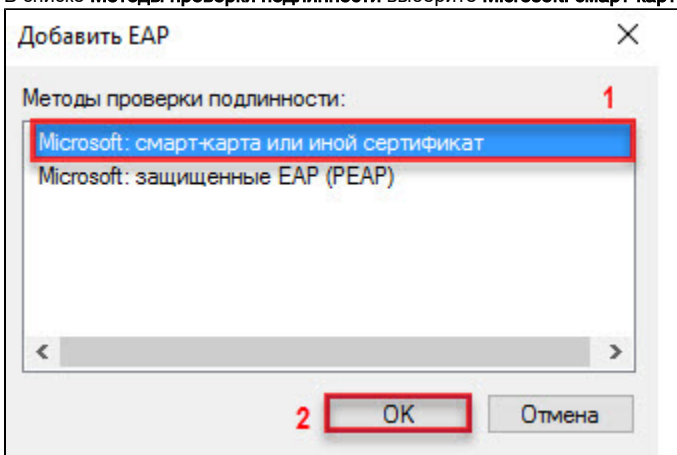


24. На вкладке **Ограничения** в левой части окна щелкните по названию ограничения **Методы проверки подлинности**.
25. В правой части окна в списке **Типы EAP** должна отображаться строка **Microsoft: смарт-карта или иной сертификат**.



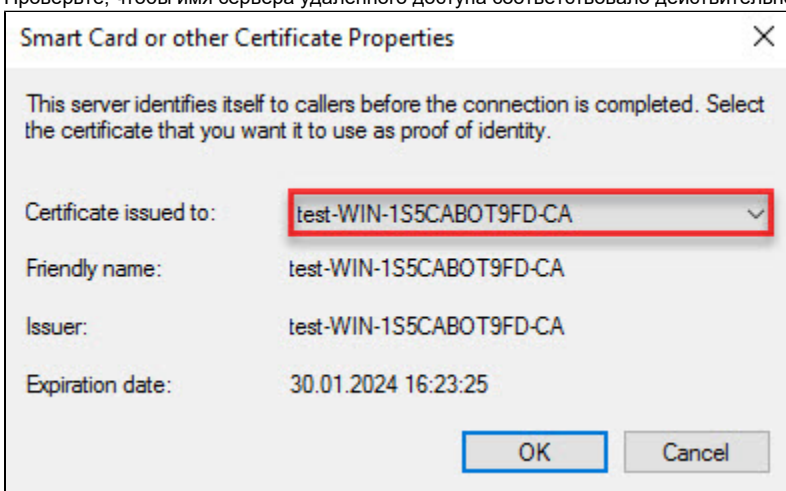
26. Если эта строка не отображается, то нажмите **Добавить**.

27. В списке **Методы проверки подлинности** выберите **Microsoft: смарт-карта или иной сертификат**, нажмите **ОК**.



28. Далее укажите сервер для аутентификации. Для этого щелкните по строке **Microsoft: смарт-карта или иной сертификат** и нажмите **Изменить**.

29. Проверьте, чтобы имя сервера удаленного доступа соответствовало действительности.



30. Нажмите **ОК**.

31. Закройте оснастку **Сервер сетевых политик**.

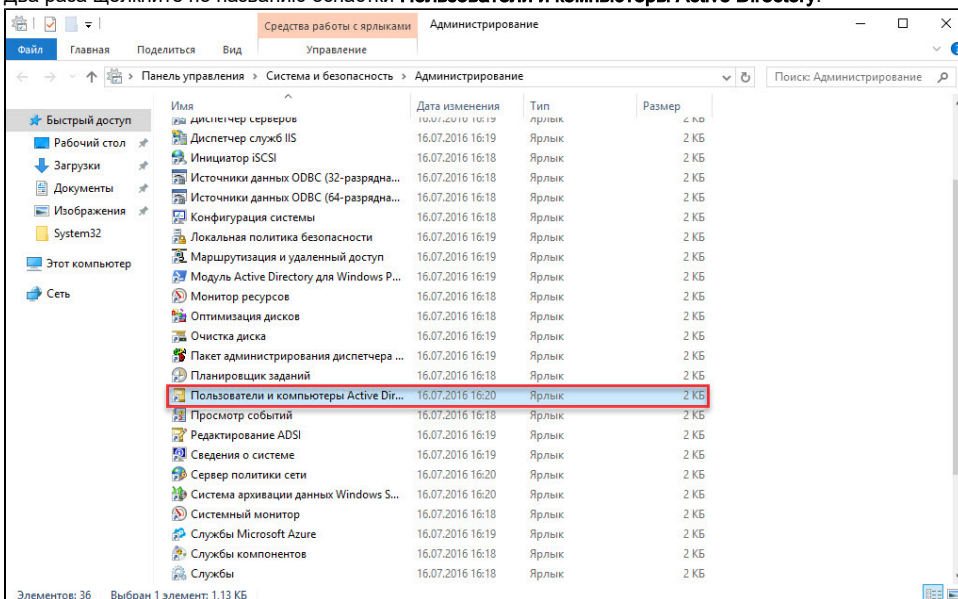
Настройка учетных записей пользователей

После настройки удаленного доступа пользователям необходимо дать права на подключение к VPN.

Для настройки учетных записей пользователей:

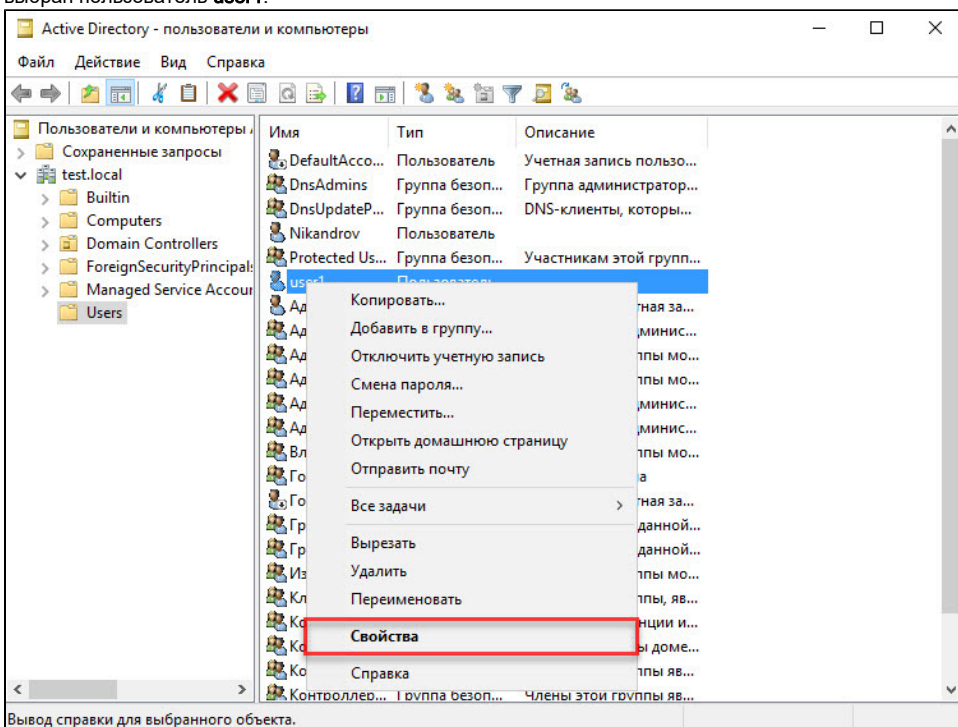
1. Зайдите в **Панель управления**.
2. В поле для поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.

4. Два раза щелкните по названию оснастки **Пользователи и компьютеры Active Directory**.



5. В окне **Active Directory - пользователи и компьютеры** щелкните по названию папки **Users**.

6. В правой части окна, в строке с именем пользователя щелкните правой кнопкой мыши и выберите пункт **Свойства**. В данном примере выбран пользователь **user1**.



7. В окне **Свойства:[Имя пользователя]** перейдите на вкладку **Входящие звонки**.

8. Установите переключатель в положение **Разрешить доступ** и нажмите **ОК**.

Свойства: user1

Профиль служб удаленных рабочих столов COM+

Общие Адрес Учетная запись Профиль Телефоны Организация

Член групп Входящие звонки Среда Сеансы Удаленное управление

Права доступа к сети

☒ Разрешить доступ

☐ Запретить доступ

☐ Управление доступом на основе политики сети NPS

☐ Проверять код звонящего:

Ответный вызов сервера

☒ Ответный вызов не выполняется

☐ Устанавливается вызывающим (только для RAS)

☐ Всегда по этому номеру:

☐ Назначить статические IP-адреса

Определите IP-адреса, разрешенные для этого входящего подключения.

☐ Использовать статическую маршрутизацию

Определите маршруты, работающие с входящим подключением.

9. Закройте оснастку **Пользователи и компьютеры Active Directory**.

Настройка сервера завершена. Теперь необходимо настроить удаленное подключение к виртуальной частной сети (VPN) [на клиентском компьютере](#).