Indeed AM NPS RADIUS Extension

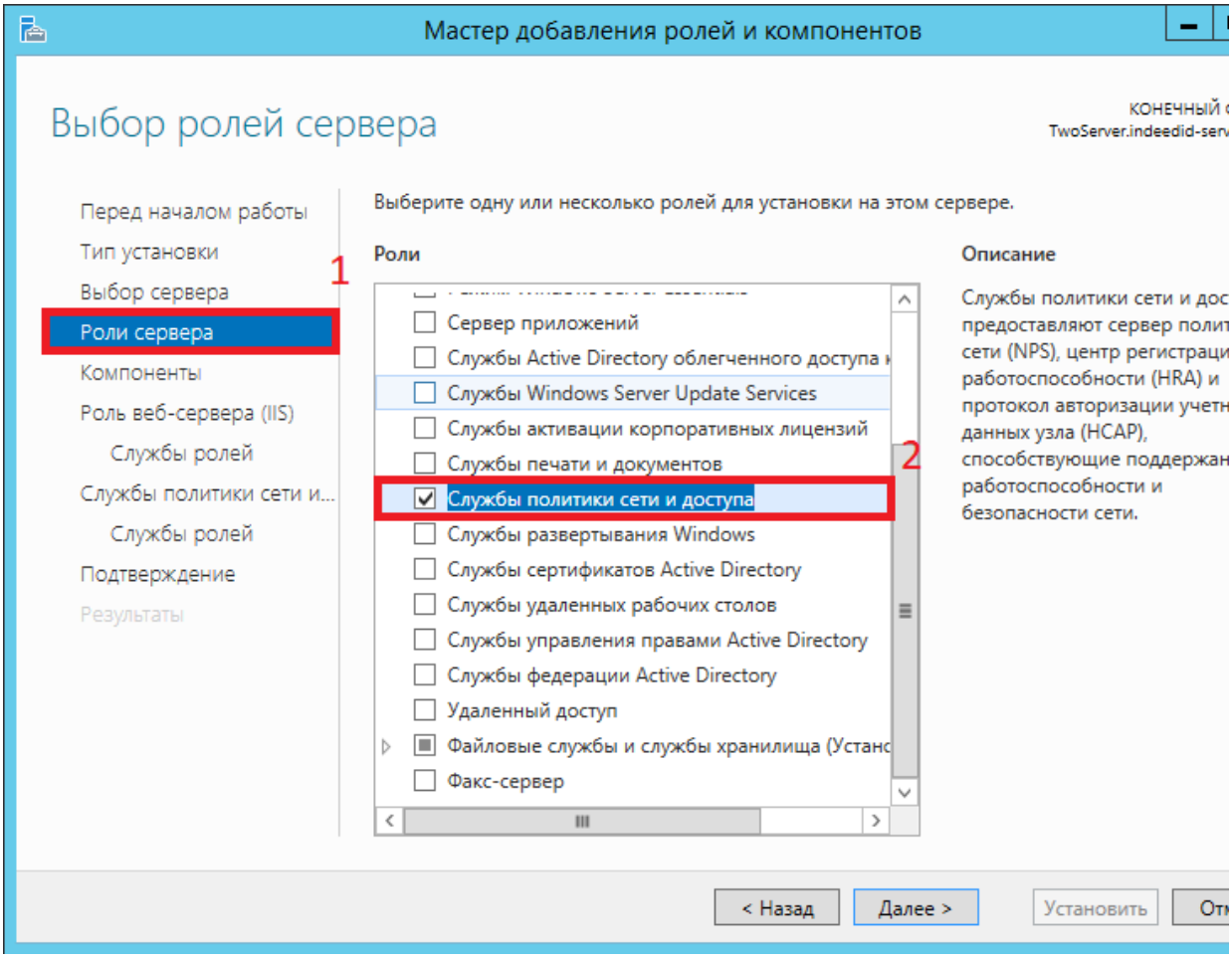
Indeed AM NPS RADIUS Extension (RADIUS Extension) представляет собой модуль расширения Microsoft Network Policy Server (NPS, входит в состав Windows Server) и позволяет реализовать для RADIUS-совместимых сервисов и приложений технологию двухфакторной аутентификации.

> **Информация**
>
> Файлы для Indeed AM NPS Radius Extension расположены: ***indeed AM <Номер версии>\Indeed AM RADIUS Extension\<Номер версии>***
>
> - **IndeedID.EA.RADIUS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM NPS Radius Extension.
>
> Файлы шаблонов политик расположены: ***indeed AM <номер версии>*\Misc\ADMX Templates**.

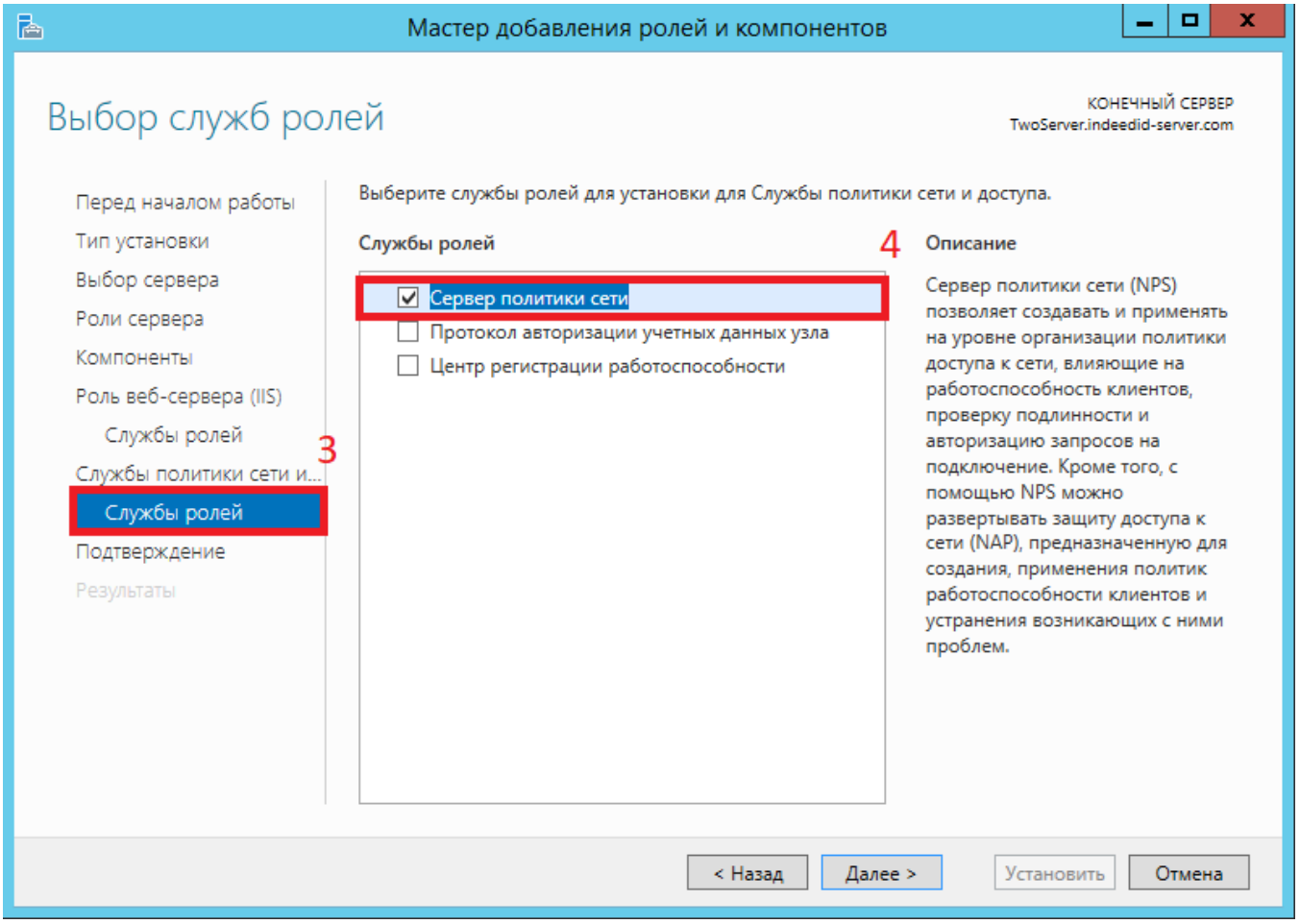
Установка Network Policy Server

1. Запустить **Мастер добавления ролей и компонентов (Add Roles and Features Wizard)**.

2. Из списка ролей выбираем роль **Службы политики сети и доступа (Network Policy and Access Services)**, соглашаемся с установкой дополнительных компонентов.



3. Из списка **"Службы ролей"** выбираем **"Сервер политики сети (Network Policy Server)"**.



4. В окне **"Подтверждение установки компонентов"** нажимаем **"Установить"**.

Настройка NPS Сервера

Добавление Radius-клиента

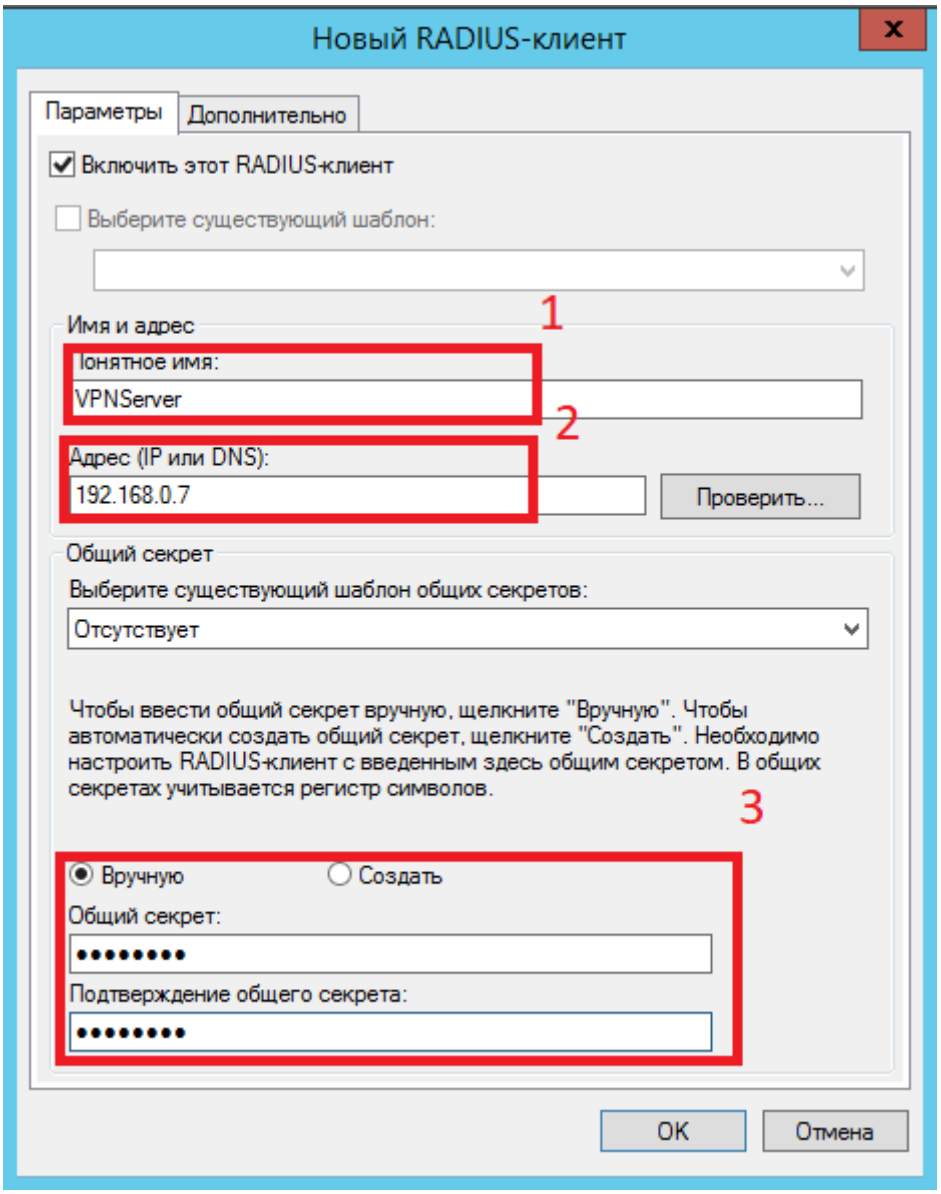
1. Запустите **"Сервер сетевых политик"**.
2. Добавьте в "RADIUS-клиенты" необходимый VPN клиент. Для создания создания клиента нажмите правой кнопкой мыши по **"RADIUS - Клиенты"** и выберете **"Новый документ"**.

> ⚠ **Информация**
>
> При использовании проверки подлинности **Chap** необходимо, в параметрах учетной записи пользователя, включить "**Хранить пароль, используя обратимое шифрование**" и обновить пароль пользователю.

3. В окне "**Новый Radius-клиент**" выполните настройку клиента.

a. Добавьте произвольное понятное имя для добавляемого клиента **(1)**.
b. Укажите **IP адрес (2)**.
c. Задайте **секретный ключ** для соединения **(3)**.

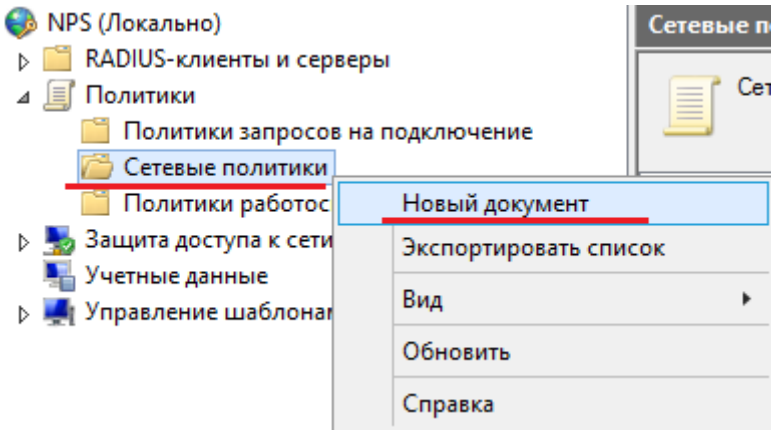
> **Информация**
>
> Необходимо указать секретный ключ, который был создан на клиенте. Если подключение со стороны клиента ещё не было настроено, задайте произвольный ключ и запомните его. Данный ключ потребуется указать при настройке подключения со стороны клиента.



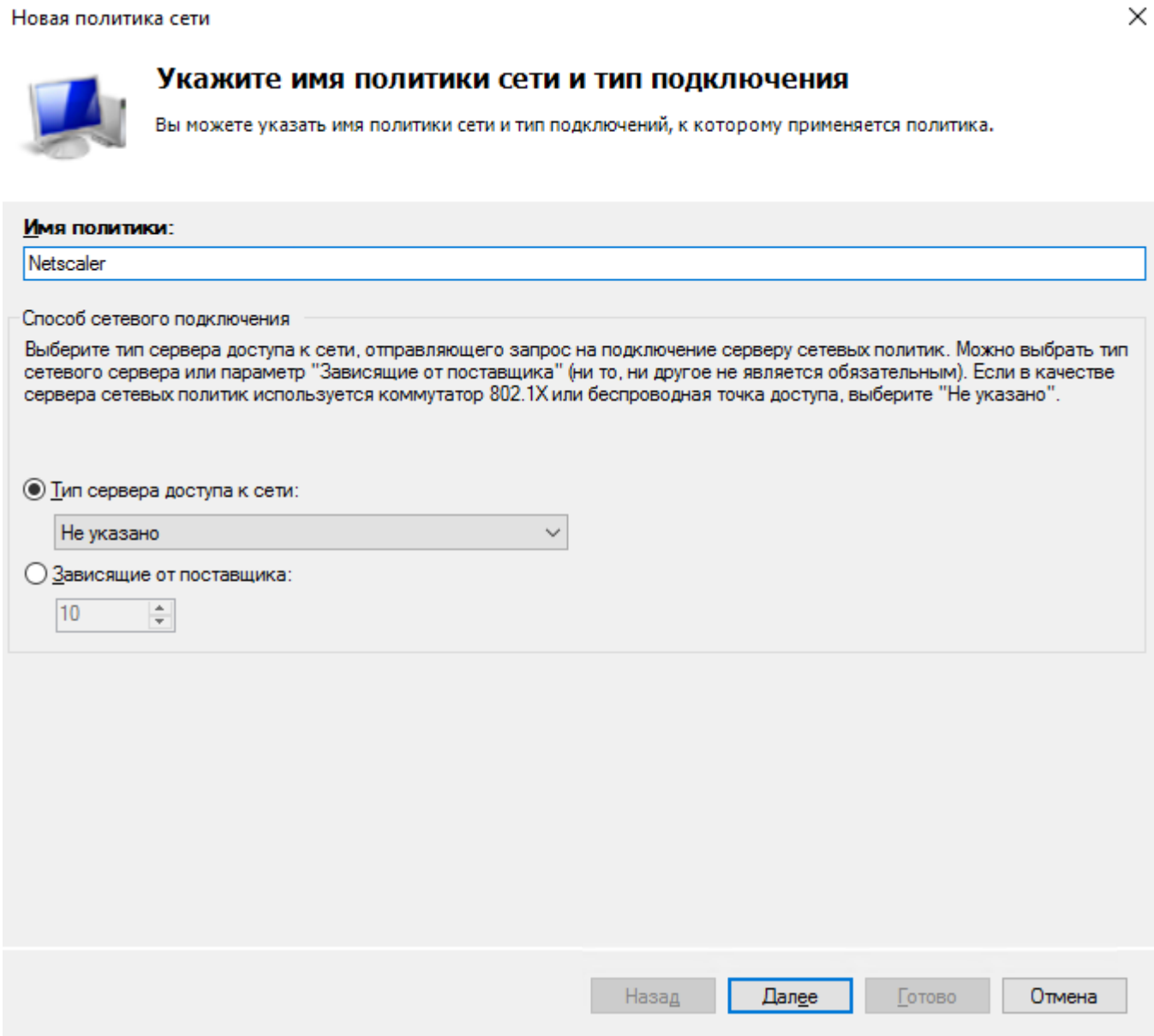
Добавление сетевой политики

1. Запустите **"Сервер сетевых политик"**.

2. Раскройте раздел "**Политики**".
3. Нажмите правой кнопкой мыши по разделу "**Сетевые политики**" и выберете "**Новый документ**".

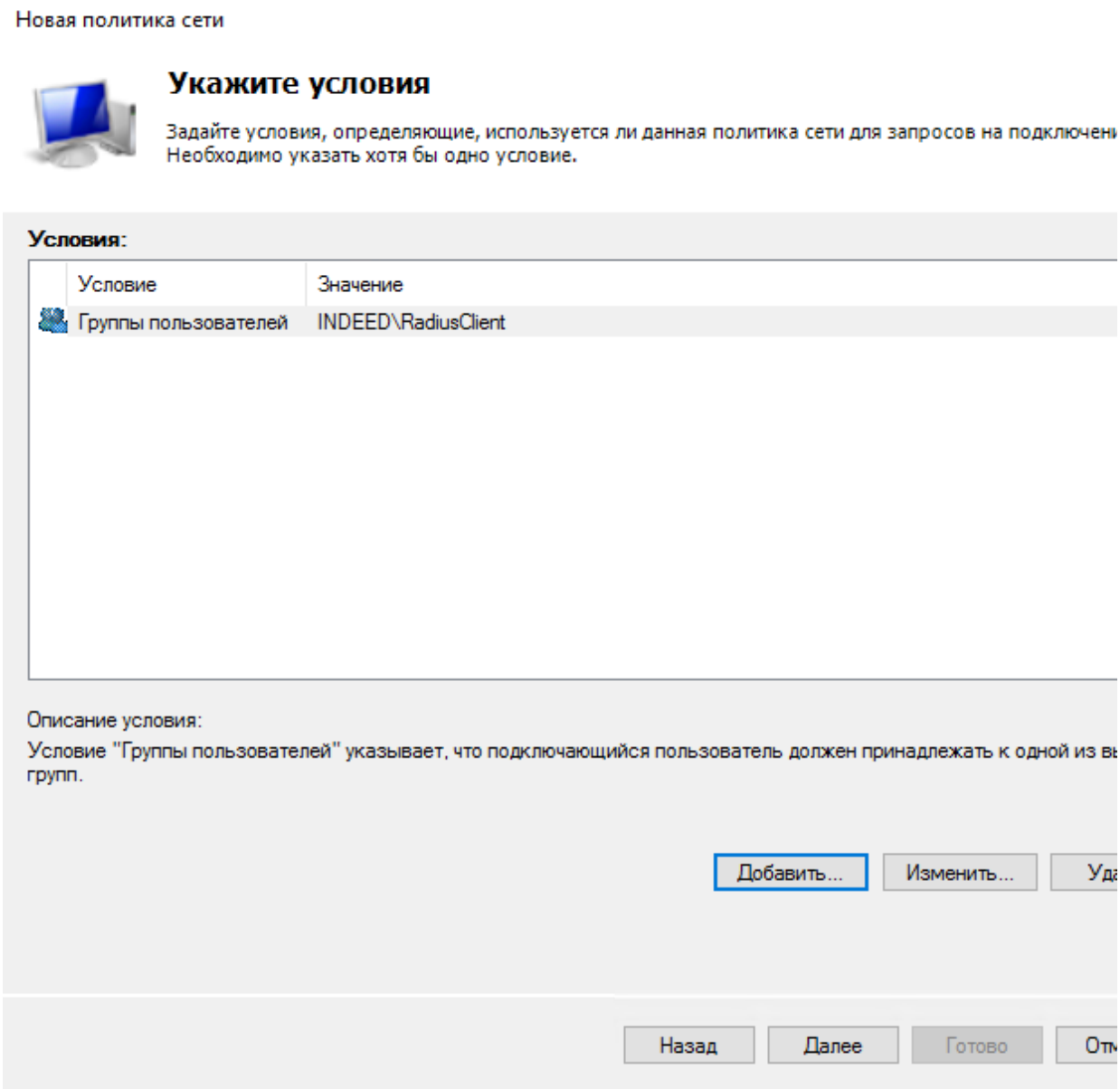


4. В поле "**Имя политики**" укажите произвольное понятное имя для создаваемой политики и нажмите "**Далее**".



5. В окне "**Укажите условия**" добавьте необходимые условия, которые будут проверяться при подключении клиентов. Для добавления нажмите кнопку "**Добавить...**" и выберете необходимое условие. После добавления условия нажмите "**Далее**".

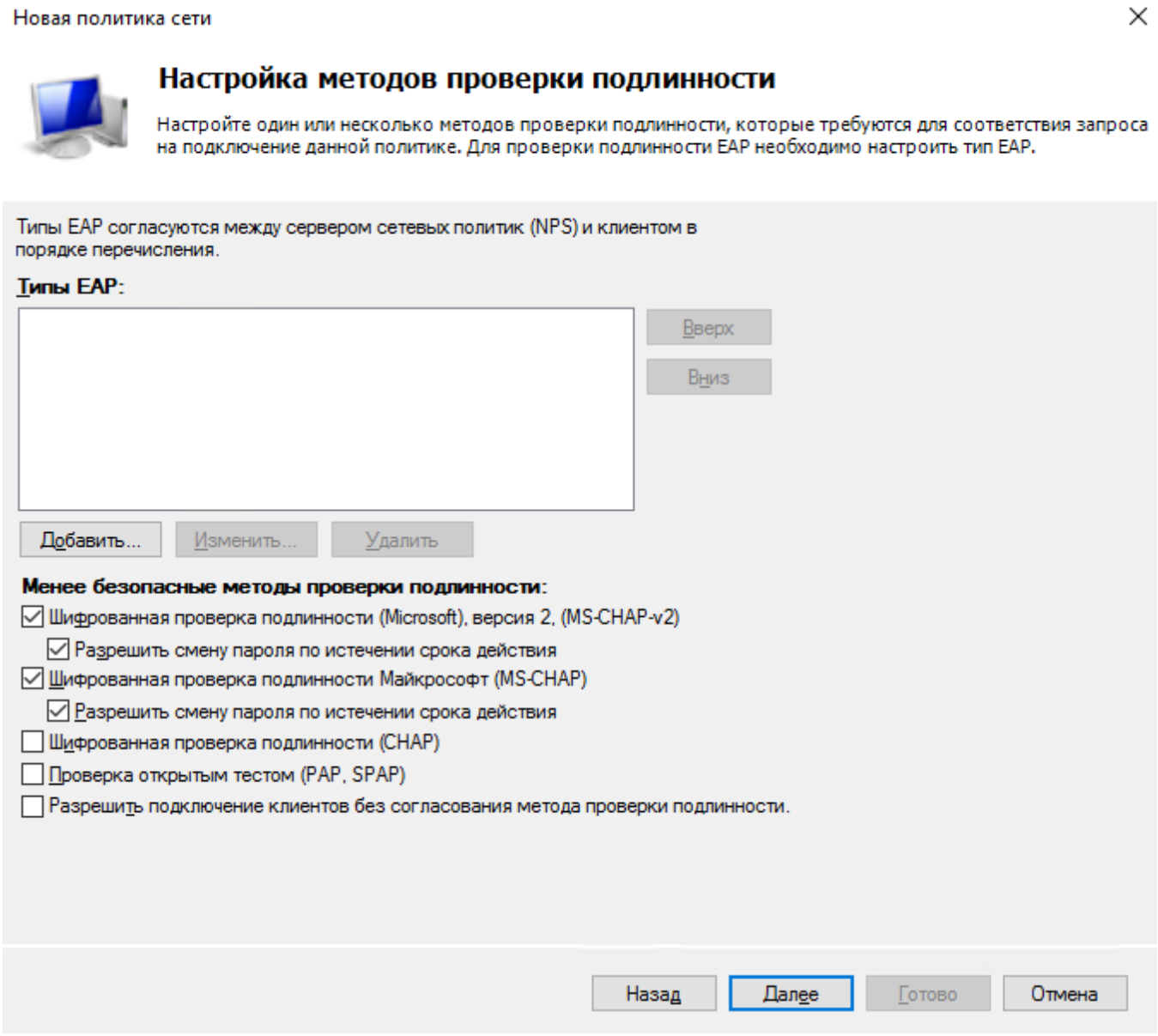
> **Информация**
>
> В качестве примера будет добавлено условие "**Группы пользователей**". При добавлении группы, потребуется указать имя группы пользователей из AD.



6. В окне "**Укажите разрешения доступа**" выберете "**Доступ разрешен**" и нажмите "**Далее**".

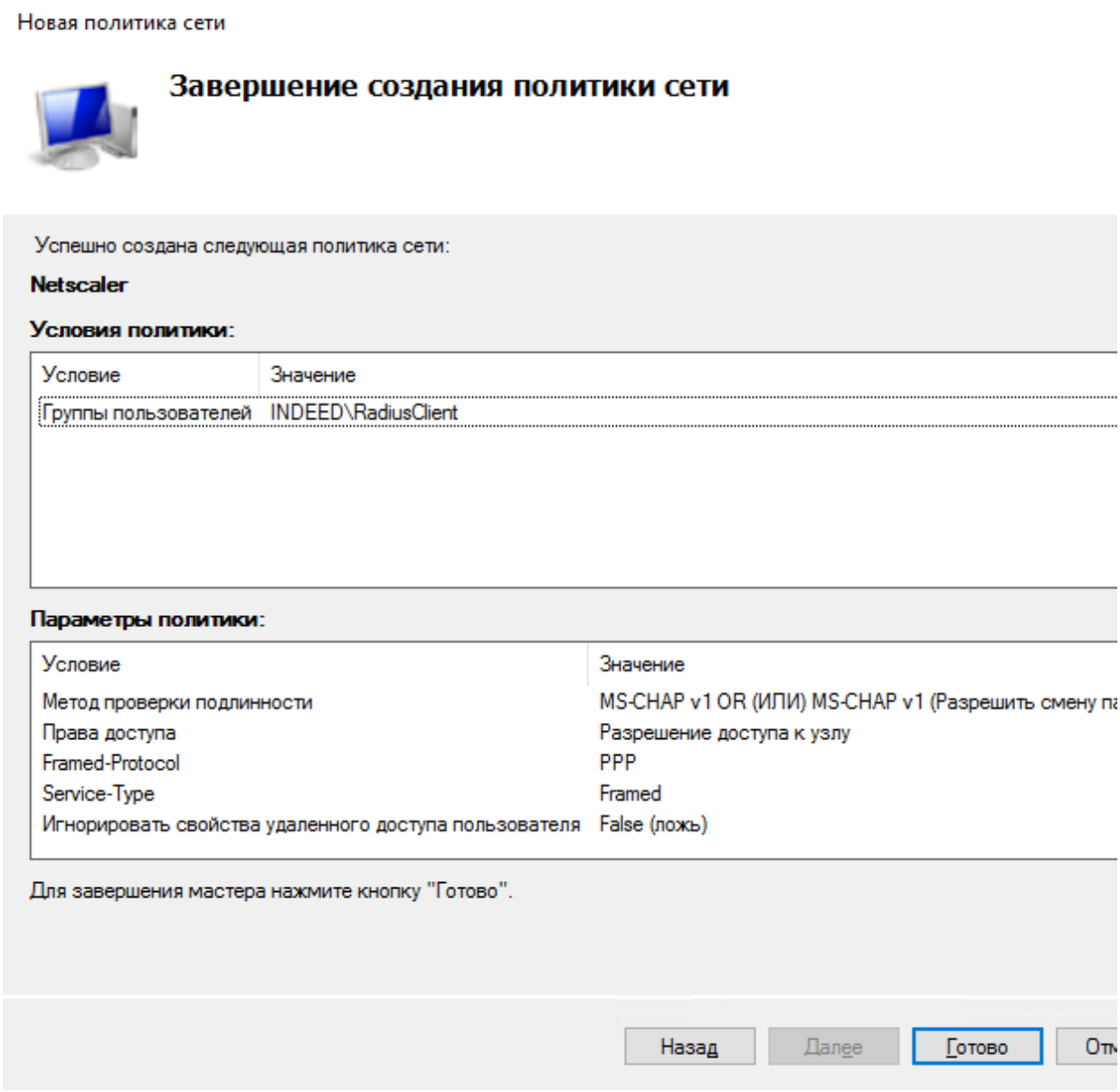
7. В окне "**Настройка методов проверки подлинности**" укажите методы проверки подлинности, которые настроены на клиенте, и нажмите "**Далее**".

> **Информация**
>
> Методы проверки подлинности со стороны Radius сервера и клиента должны совпадать, в противном случае возникнет ошибка аутентификация.



8. В окнах "**Настройка ограничений**" и "**Настройка параметров**" оставьте значения по умолчанию и нажмите "**Далее**".

9. В окне "**Завершение создания политики сети**" проверьте данные и нажмите "**Готово**".



Установка Indeed AM NPS RADIUS Extension

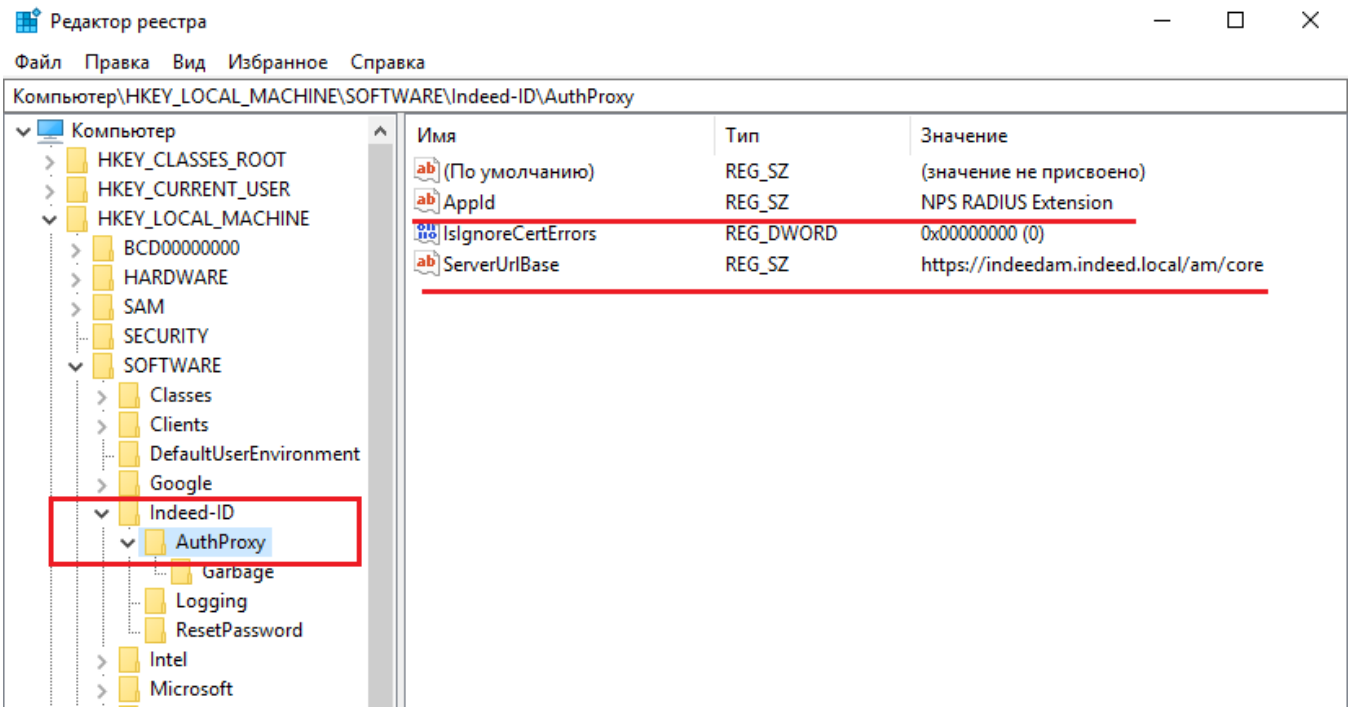
1. Выполните установку NPS RADIUS через запуск соответствующего пакета из дистрибутива.
2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy.** Измените параметры:
    a. Параметр **ServerUrlBase.** В значении для параметра укажите адрес вашего сервера **Indeed** в формате **http(s)://<DNS_IndeedAM_Server>/am/core/**.

> **Информация**
>
> При использовании https соединения требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

    b. Параметр **IsIgnoreCertErrors,** указать значение **0** или **1.**

> **Информация**
>
> Данный параметр предназначен для игнорирования ошибок сертификата проверки подлинности сервера **Indeed**, при значении **1** про исходит игнорирование ошибок сертификата.

    c. Параметр **AppId** со значением **NPS RADIUS Extension.**

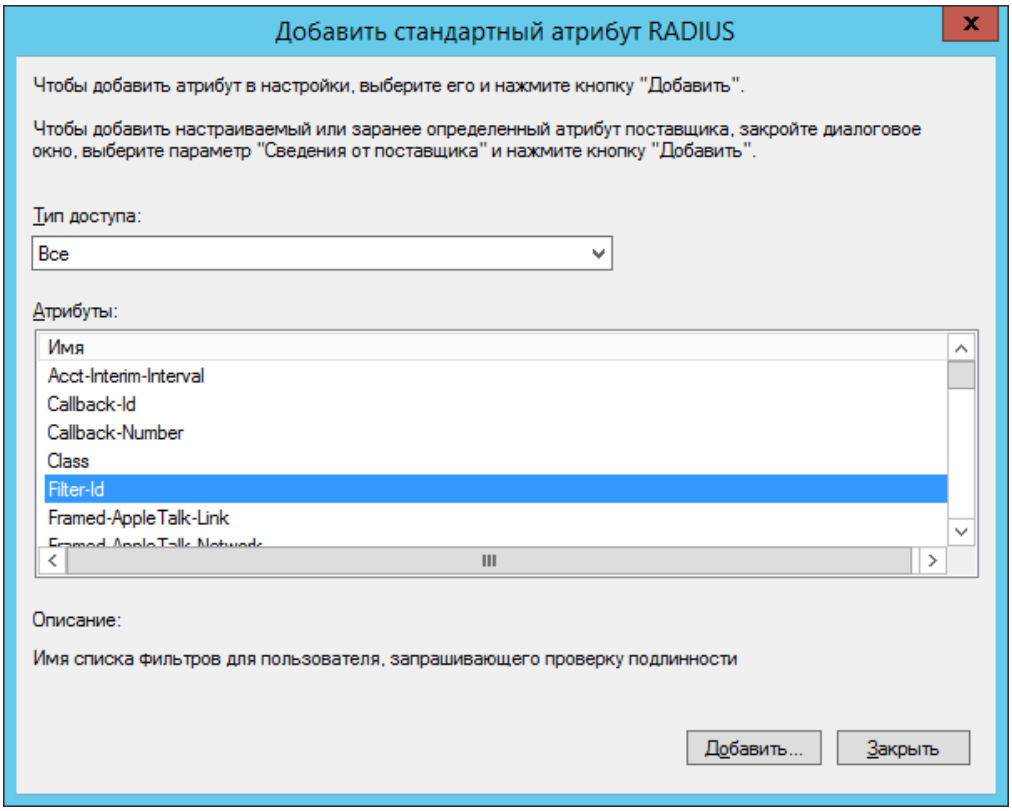


Настройка проброса атрибутов Radius

> **Информация**
>
> Данная настройка является опциональной и выполняется только при необходимости проброса атрибутов Radius для клиента.

> **Информация**
>
> Данная настройка позволяет добавить атрибуты в ответ "Access-Accept", которые указаны в сетевой политике NPS сервера.

1. Откройте "**Политику запросов на подключение**".
2. Выберите имеющуюся или создайте новую политику и откройте вкладку "**Параметры**".
3. Выберите параметр "**Стандарт**" и нажмите "**Добавить**".
4. В окне "**Добавить стандартный атрибут Radius**" выберете "**Filter-Id**" и нажмите "**Добавить**".

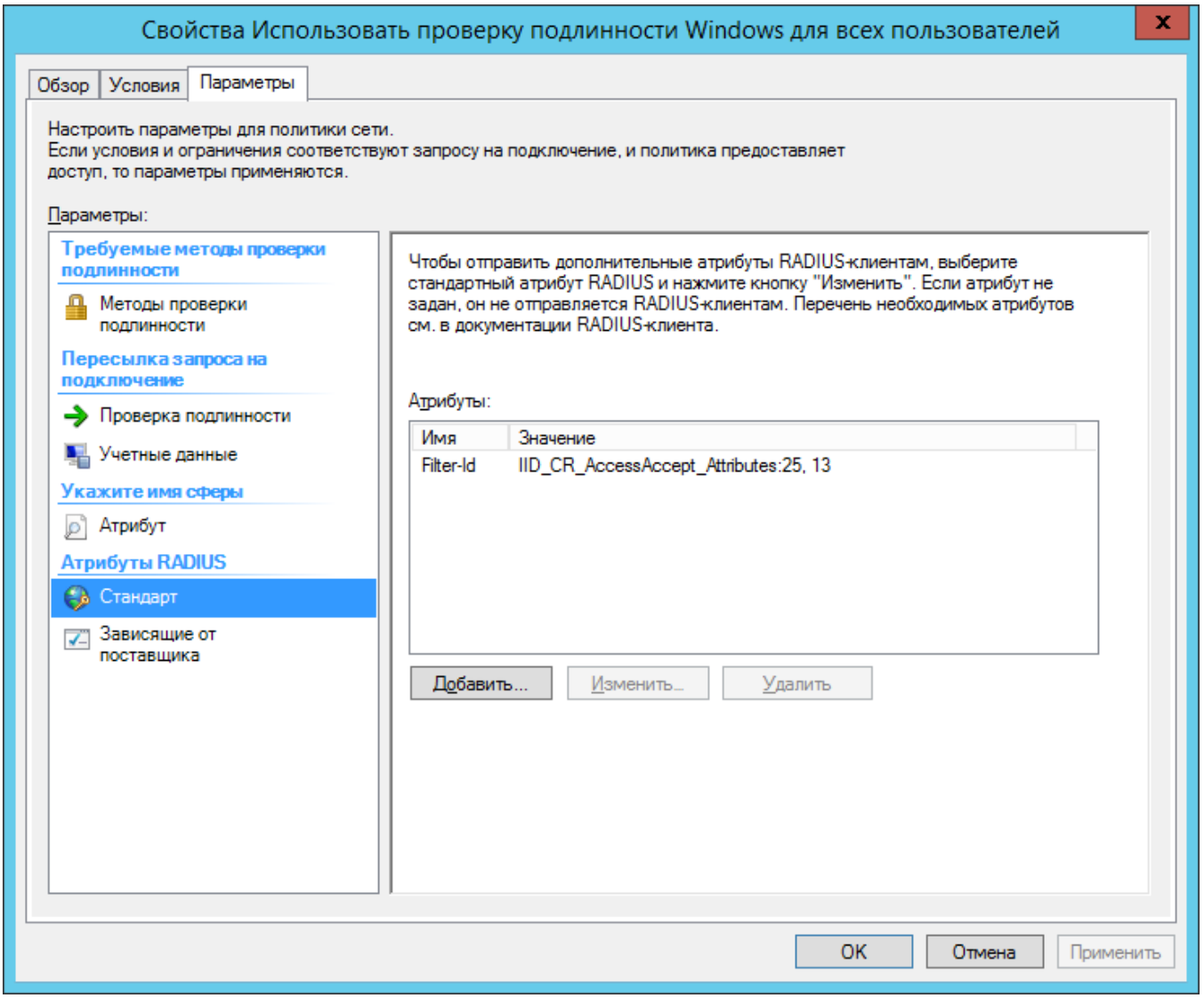


5. В окне "**Сведения об атрибуте**" нажмите "**Добавить**". Убедитесь, что параметр "**Формат ввода атрибута**" - строковый, и введите строку формата: **IID_CR_AccessAccept_Attributes:<id требуемого атрибута 1>, <id требуемого атрибута 1>**

> **Информация**
>
> Если атрибутов несколько, то id атрибутов требуется указывать через запятую.

Пример
IID_CR_AccessAccept_Attributes:25, 13

6. Закройте все окна и нажмите "**Применить**".



7. Перезапустите службу NPS.

Настройка параметров доступа в политиках на сервере политики сети (NPS)

> **Информация**
>
> Опциональная настройка.

В политике на сервере NPS задаются параметры:

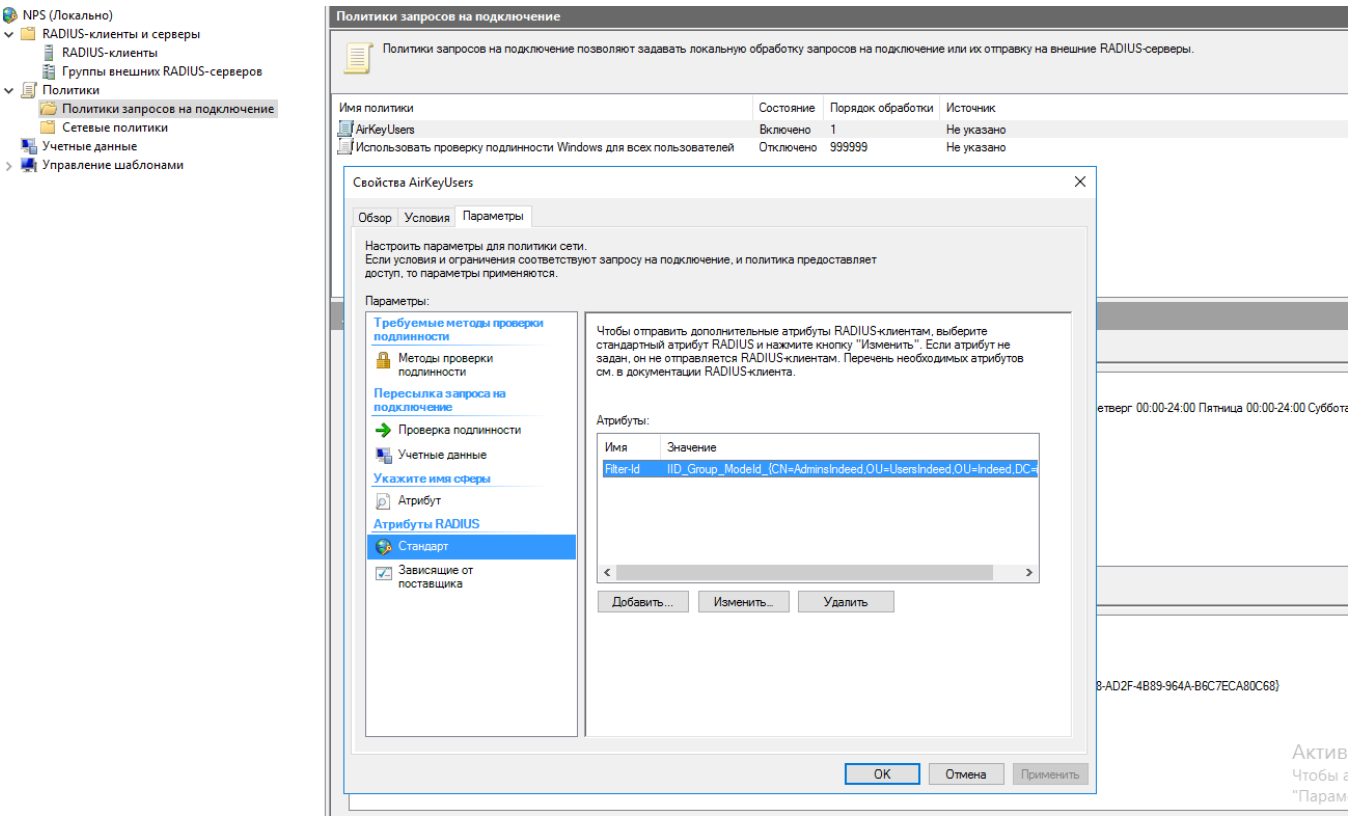
- Общая настройка способа входа
- Настройка способов входа для групп пользователей

Для настройки параметров доступа выполните следующие действия:

1. На сервере сетевых политик (Network Policy Server, NPS) запустите консоль "**Сервер политики сети (Network Policy Server)**" и перейдите в раздел **Политики (Policies)** **Политики запросов на подключение (Connection Request Policies)**.
2. Создайте новую политику или используйте имеющеюся и перейдите в её свойства.
3. На вкладке "**Параметры (Settings)**" перейдите в раздел **Атрибуты RADIUS (RADIUS Attributes)** **Стандарт (Standard)**.
4. Нажмите "**Добавить... (Add..)**", выберите атрибут "**Filter-Id**" и нажмите "**Добавить... (Add...)**".

5. В окне "**Сведения об атрибуте (Attribute Information)**" укажите необходимые значения, в соответствии с таблицей ниже.

Значение	Описание
IID_ModeId_{ProviderId}	**Общая настройка способа входа**. Если указано, то пользователи (кроме тех, на которых распространяется действие настройки "**Настройка способов входа для групп пользователей**") будут использовать указанный провайдер аутентификации Indeed в RADIUS-приложениях. Значение "**ProviderId**" уникально для каждого провайдера и перечислены в политике "**Настройка способов входа для групп пользователей**". Пример значения атрибута с Indeed AM Software OTP Provider: **IID_ModeId_{B772829C-4076-482B-B9BD-53B55EA1A302}**
ID_Group_ModeId_{DN}_{ProviderId}	**Настройка способов входа для групп пользователей.** Если задано, то пользователи указанной группы Active Directory будут использовать указанный провайдер Indeed AM для аутентификации в RADIUS приложениях. Значение **DN** – различающееся имя группы (Distinguished Name). При использовании кириллических символов в названиях групп на каждом Сервере политик сети (NPS) необходимо установить русский язык как язык для программ, не поддерживающих Юникод. Без данной настройки членам таких групп будет отказано в аутентификации Сервером политик сети. Пример значения с Indeed AM AirKey Provider: **IID_Group_ModeId_{CN=AdminsIndeed,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local}_{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}**



6. Для применения внесенных в политику изменений нажмите "**Применить (Apply)**".

7. Перезапустите службу NPS.

Настройка политик

> **Информация**
>
> Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива и расположены в каталоге Misc.
>
> Политики применяется к серверам с развернутой ролью NPS и позволяет выполнить дополнительные настройки.
>
> Политики можно настроить как через доменные групповые политики, так и через локальную групповую политику на сервере NPS.
>
> После настройки политик необходимо выполнить перезагрузку службы NPS.

> **Информация**
>
> Действие политики представляет из себя добавление определенных ключей в реестр, при необходимости значения политик можно добавить в реестр вручную.

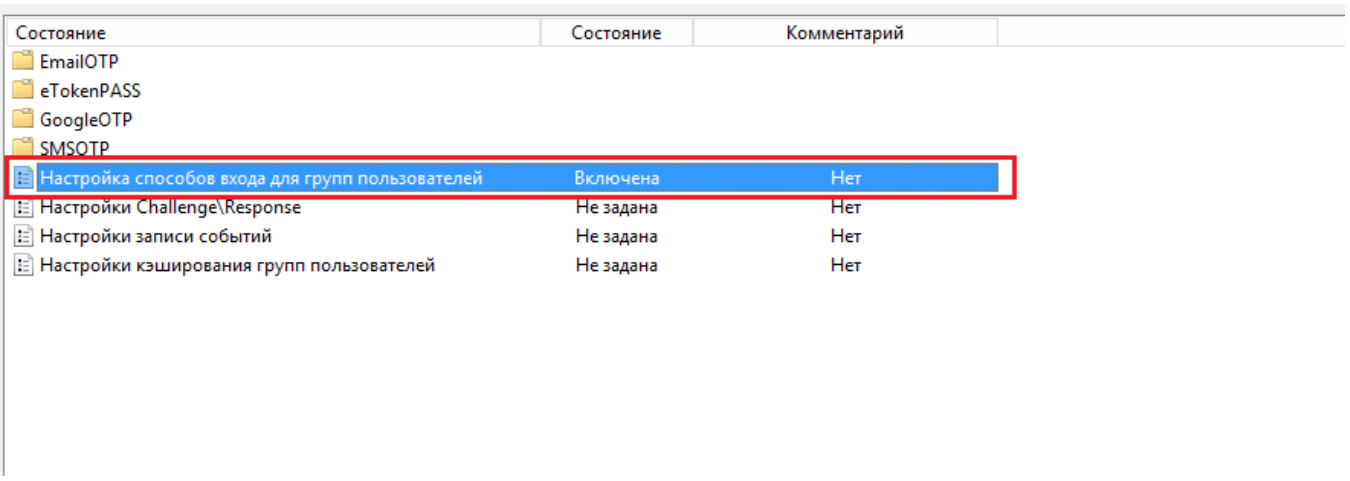
Настройка способов входа для групп пользователей

Политика задает Id провайдера, который будет использоваться для аутентификации определенной группы пользователей.

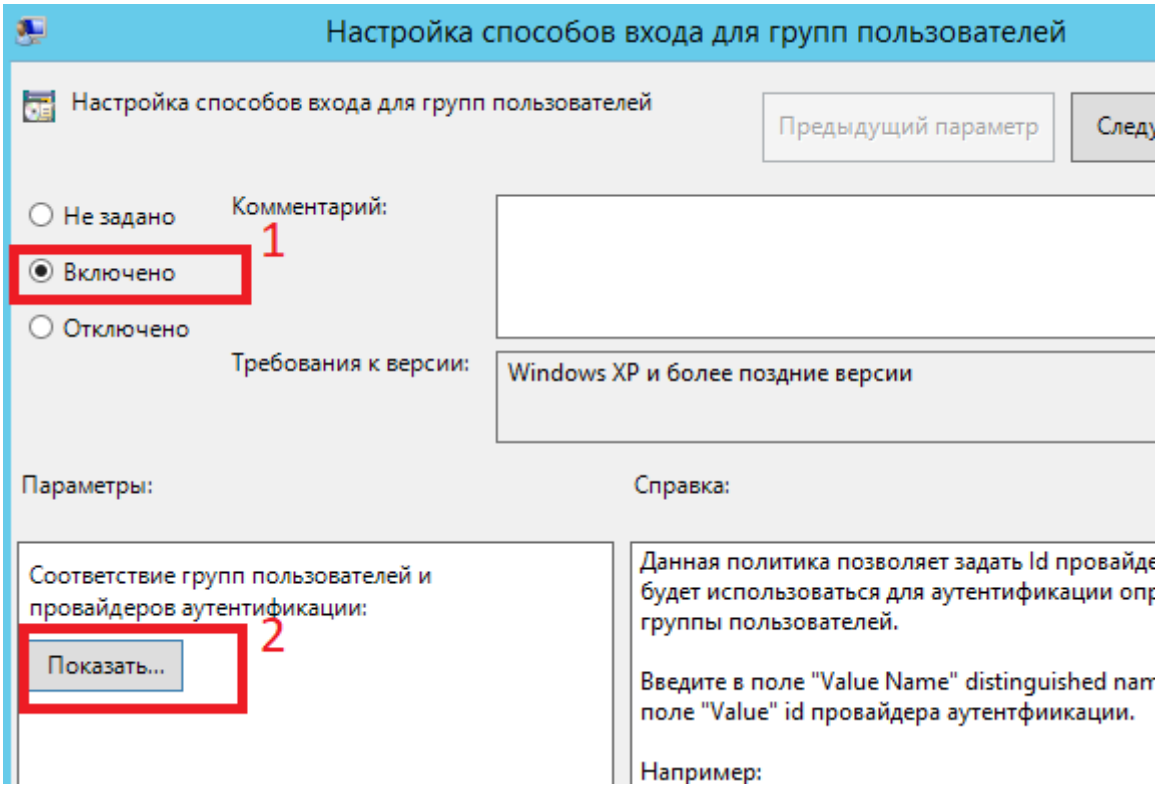
Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".

3. Откройте политику "**Настройка способов входа для групп пользователей**".



4. Включите **(1)** данную политику и нажмите "**Показать...**" для настройки **(2)**.



5. Укажите в **"Имя значения"** значение атрибута **"DistinguishedName"**, "**ObjectGUID**" или "**SID**" целевой группы пользователей.
6. В **"Значение"** укажите ключ используемого провайдера.

Информация

Параметр **"Значение"** может иметь разные **ID** провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{3F2C1156-B5AF-4643-BFCB-9816012F3F34} - **StorageSms OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{B772829C-4076-482B-B9BD-53B55EA1A302} - **Software OTP**

{631F1011-2DEE-47C5-95D8-75B9CAED7DC7} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **HTOTP Provider**

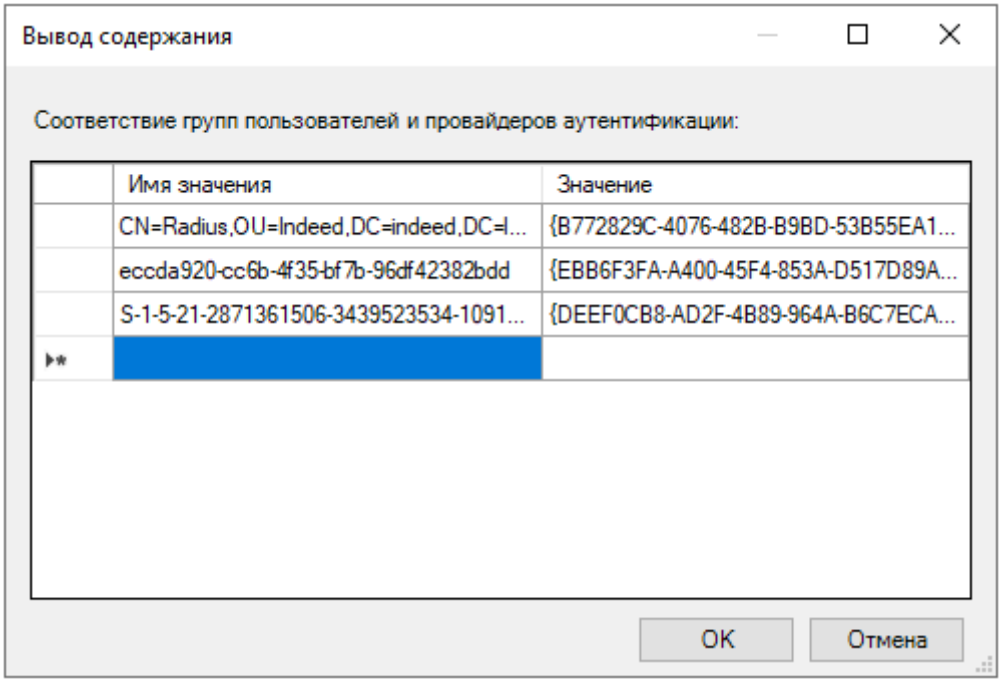
{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**

{CA4645CC-5896-485E-A6CA-011FCC20DF1D} **- Telegram OTP**

Для настройки данных провайдеров требуется отключение проверки подлинности запросов на сервере NPS. Настройка выполняется в политике запросов на подключение.

{CB3D3B0A-29C6-4BA4-939D-09B126C10C2E} - **Passcode + GoogleOTP**

{E5D3185C-9A13-4538-BE8F-D4E1C50A329E} - **Passcode + AirKey**



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте раздел с именем "**GroupDNProviderId**".
4. Создайте строковый параметр, в качестве имени параметра укажите **"DistinguishedName"**, "**ObjectGUID**" или "**SID**" целевой группы пользователей, в значении укажите ID используемого параметра.

   Пример

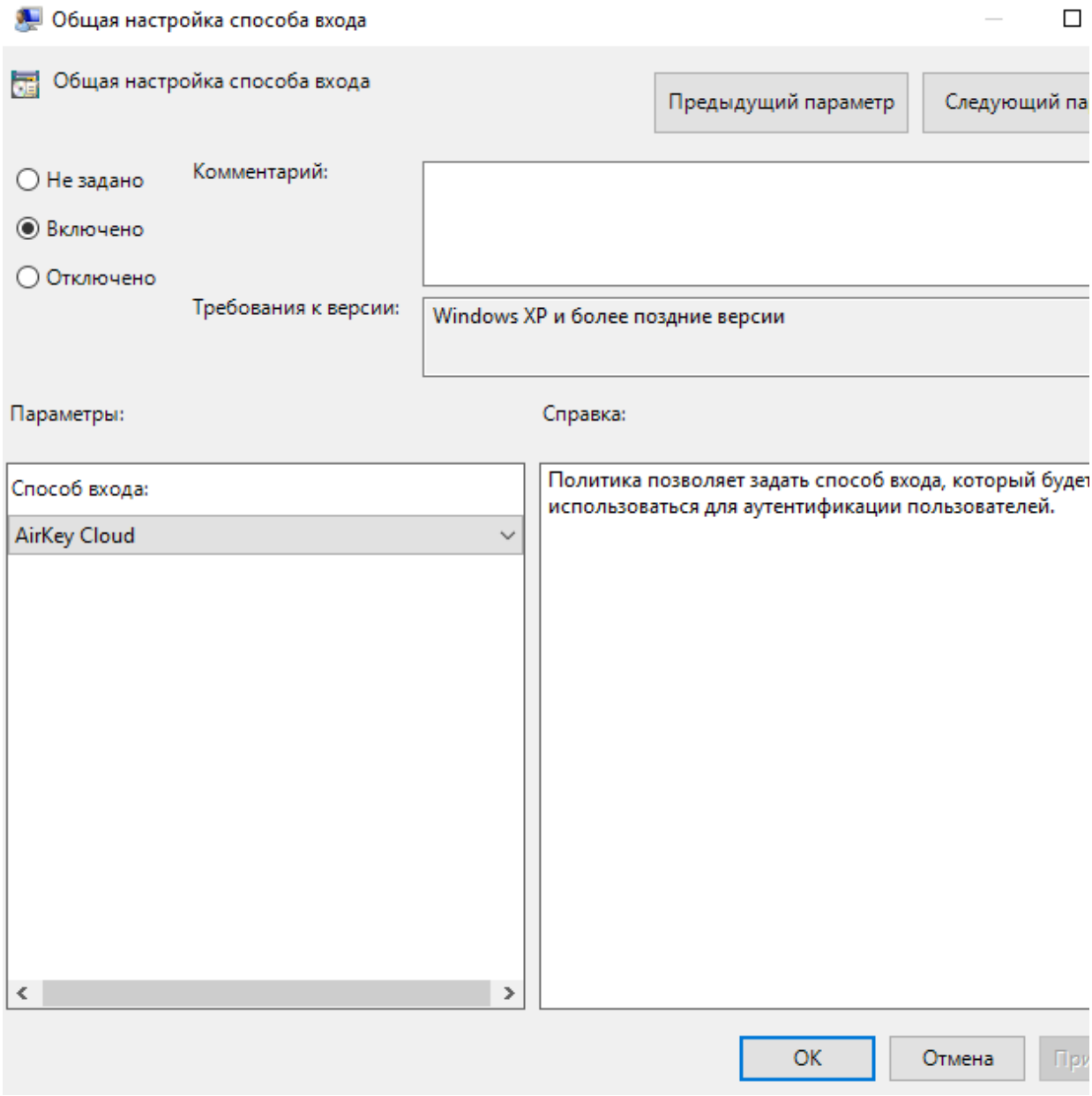
   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\GroupDNProviderId]
   "CN=RadiusClient,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local"="{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}"
   ```

Общая настройка способа входа

Настройка политики позволяет задать способ входа, который будет использоваться для аутентификации пользователей.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".
3. Откройте политику "**Общая настройка способа входа**".
4. Включите политику и в поле "**Способ входа**" выберете требуемый провайдер.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте строковый параметр с именем "**ProviderId**" в значении укажите требуемый ID провайдера.

   > **Информация**
   >
   > ID провайдеров указаны выше, в информационном блоке политики "**Настройка способов входа для групп пользователей**".

   Пример

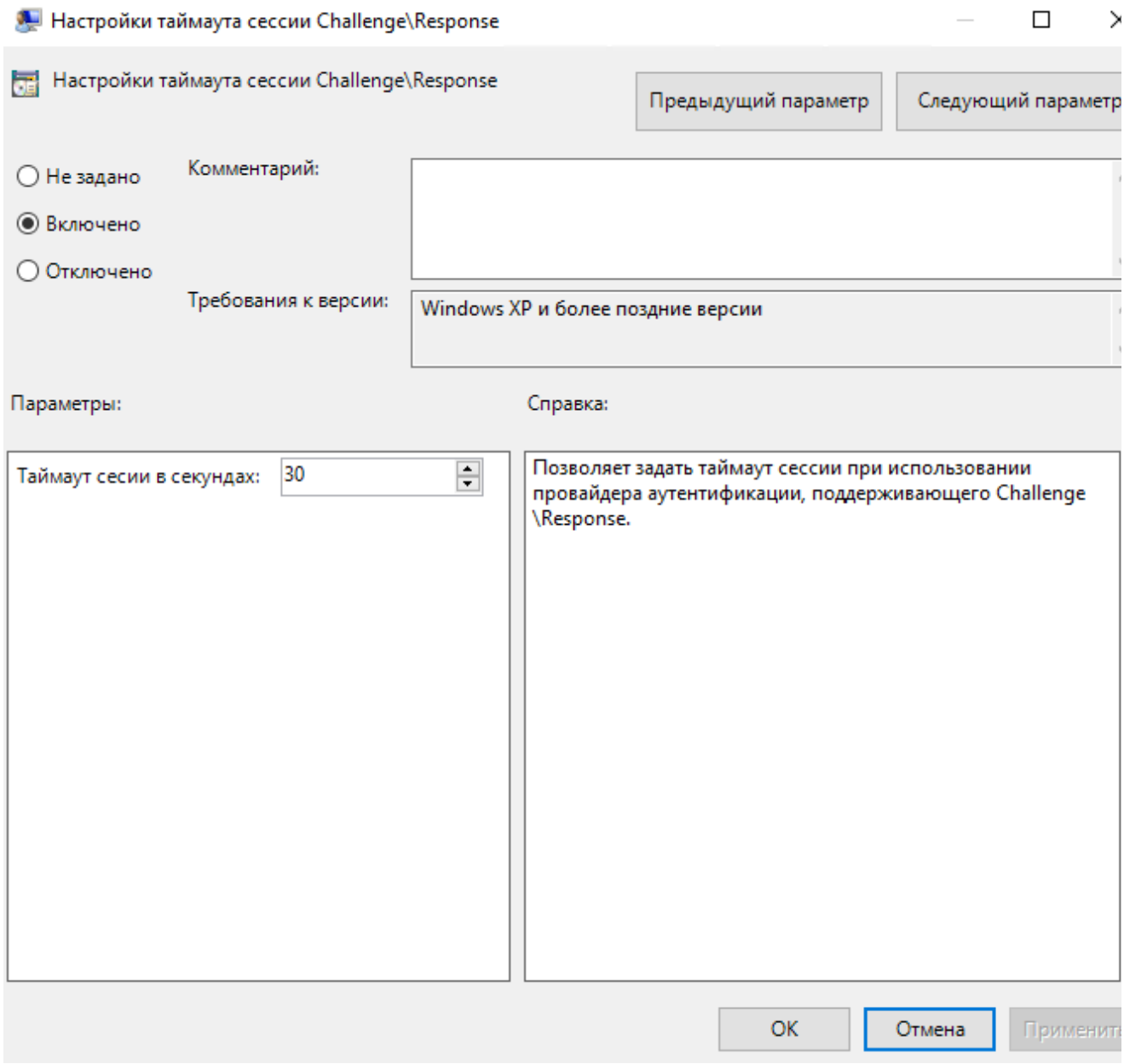
   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
   "ProviderId"="{B772829C-4076-482B-B9BD-53B55EA1A302}"
   ```

Настройка таймаута сессии Challenge\Response

Позволяет задать таймаут сессии при использовании провайдера аутентификации, поддерживающего Challenge\Response.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".
3. Откройте политику "**Настройка таймаута сессии Challenge\Response**".
4. Включите политику и в поле "**Таймаут сессии в секундах**" укажите необходимое значение.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "**DWORD**" с именем "**SessionLifetimeSec**" в качестве значения укажите таймаут сессии в секундах в десятичном формате.

   Пример

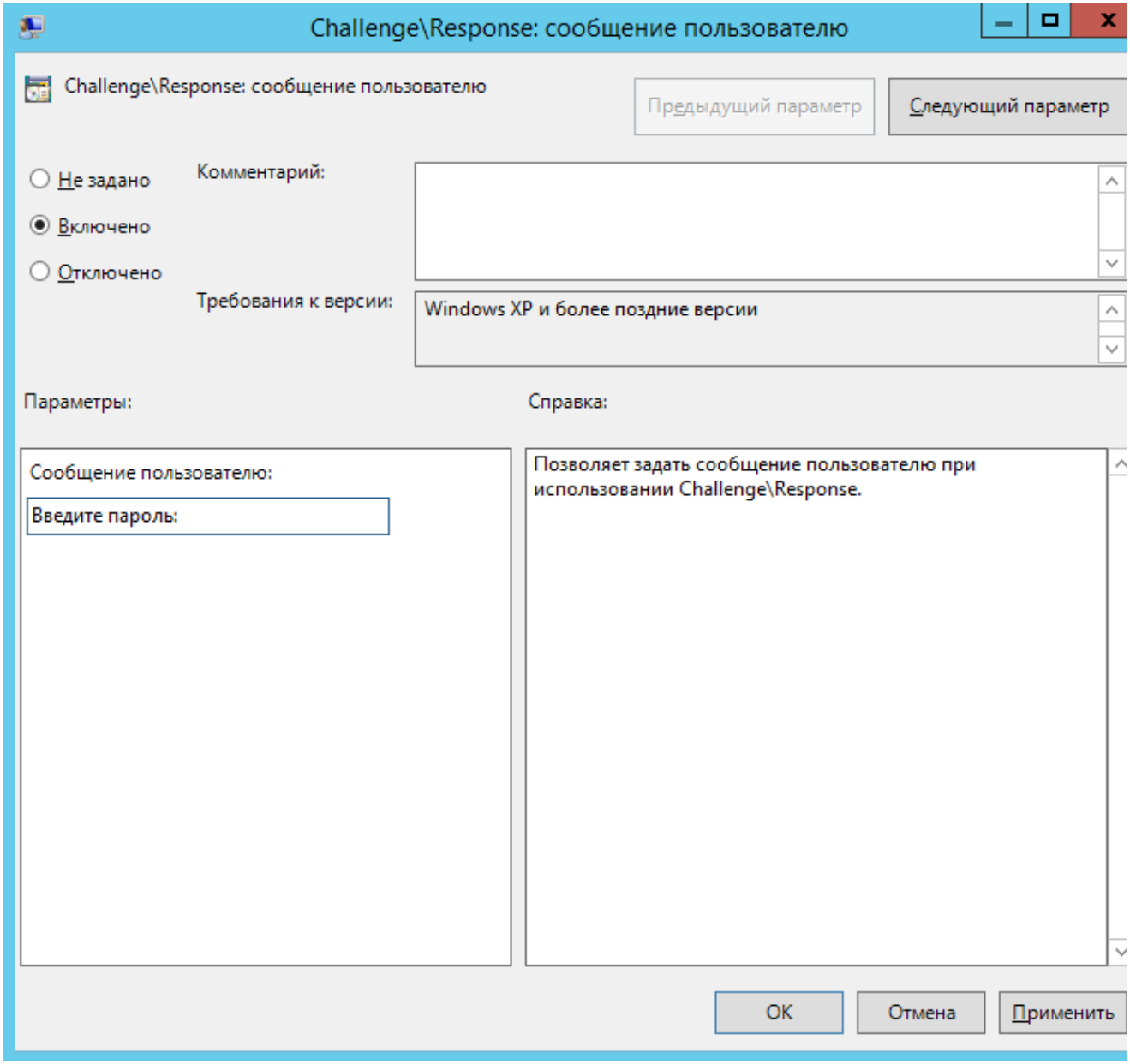
   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
   "SessionLifetimeSec"=dword:0000001e
   ```

Challenge\Response: сообщение пользователю

Политика позволяет задать сообщение пользователю при использовании Challenge\Response.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**" "**<Имя используемого провайдера>**".
3. Откройте политику "**Challenge\Response сообщение пользователю**".
4. Включите политику и в поле "**Сообщение пользователю**" введите необходимый текст.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте раздел с именем необходимого провайдера: **EmailOTP**, **eTokenPASS**, **GoogleOTP**, **SMSOTP**.
4. Создайте строковый параметр с именем формата "**<имя используемого провайдера>ChallengeResponseReplyMessage**", например, "**eTokenPassChallengeResponseReplyMessage**".
5. В качестве значения укажите текст, который будет отображаться пользователю.

   Пример

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\EmailOTP]
   "EmailOTPChallengeResponseReplyMessage"="EmailOTP:"

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\eTokenPASS]
   "eTokenPassChallengeResponseReplyMessage"="eTokenPASS OTP: "

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\GoogleOTP]
   "GoogleOTPChallengeResponseReplyMessage"="Software TOTP OTP: "

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\SMSOTP]
   "SMSOTPChallengeResponseReplyMessage"="SMS OTP: "
   ```

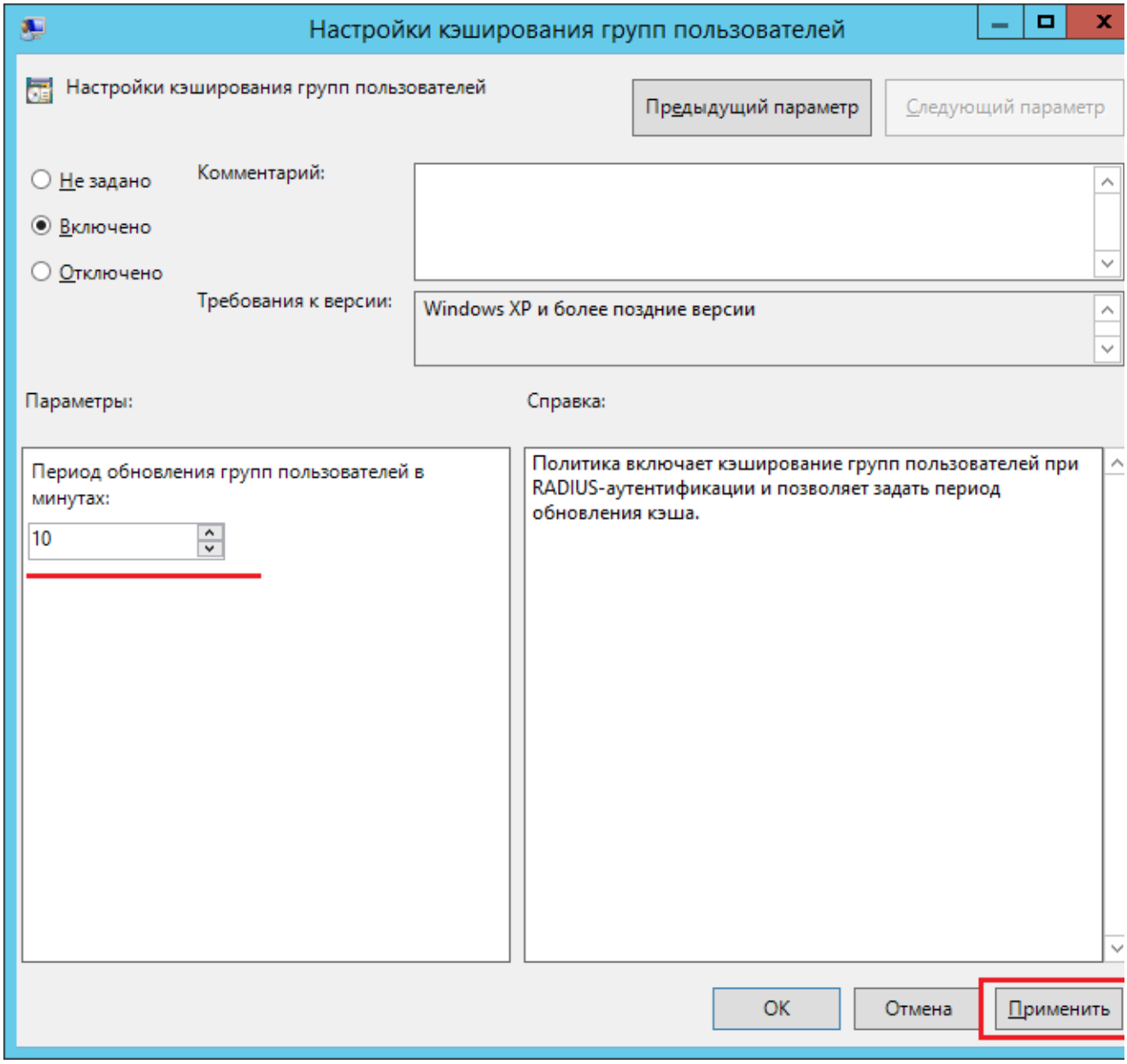
Кэширование групп пользователей

Политика включает кэширование групп пользователей при RADIUS-аутентификации и позволяет задать период обновления кэша.

> **Информация**
>
> Если NPS RADIUS Extension или Indeed AM Server долго отвечают во время работы под нагрузкой с большим количеством пользователей, то необходимо отключить данную настройку.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".
3. Откройте политику "**Настройки кэширования групп пользователей**".
4. Включите политику и в поле "**Период обновления групп пользователей в минутах**" укажите требуемое значение в минутах.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "**DWORD**" с именем "**UserGroupsCachingEnabled**", в значении параметра укажите 1.
4. Создайте параметр типа "**DWORD**" с именем "**UserGroupsCacheUpdateMin**", в значении параметра укажите десятичное число в минутах.

   Пример

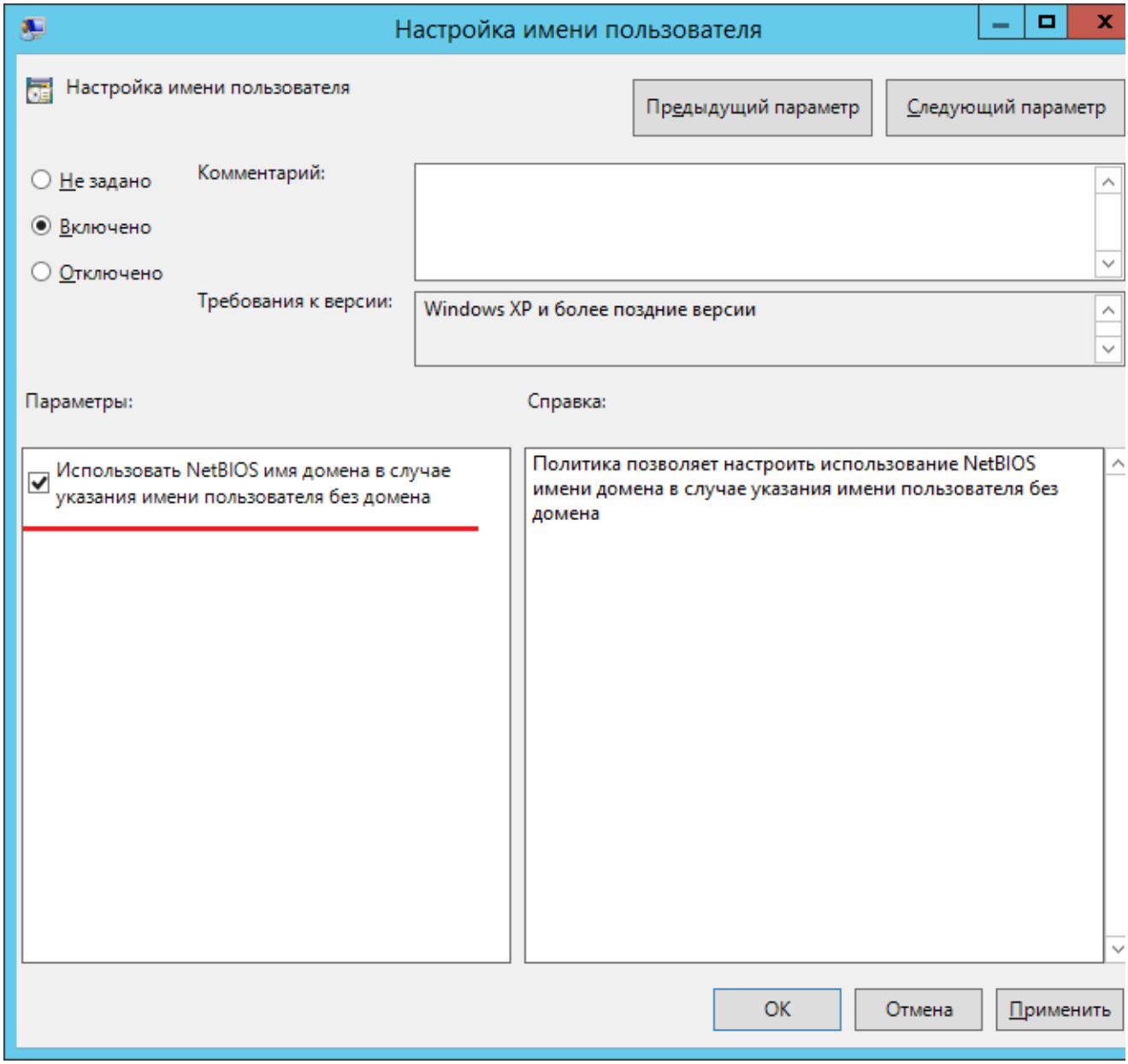
   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
   "UserGroupsCachingEnabled"=dword:00000001
   "UserGroupsCacheUpdateMin"=dword:00000021
   ```

Настройка имени пользователя

Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".
3. Откройте политику "**Настройка имени пользователя**".
4. Включите политику и активируйте параметр: "**Использовать NetBIOS имя домена в случае указания имени пользователя без домена**".



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "**DWORD**" со значением "**1**" и с именем "**UseNetBiosDomainName**".

   Пример

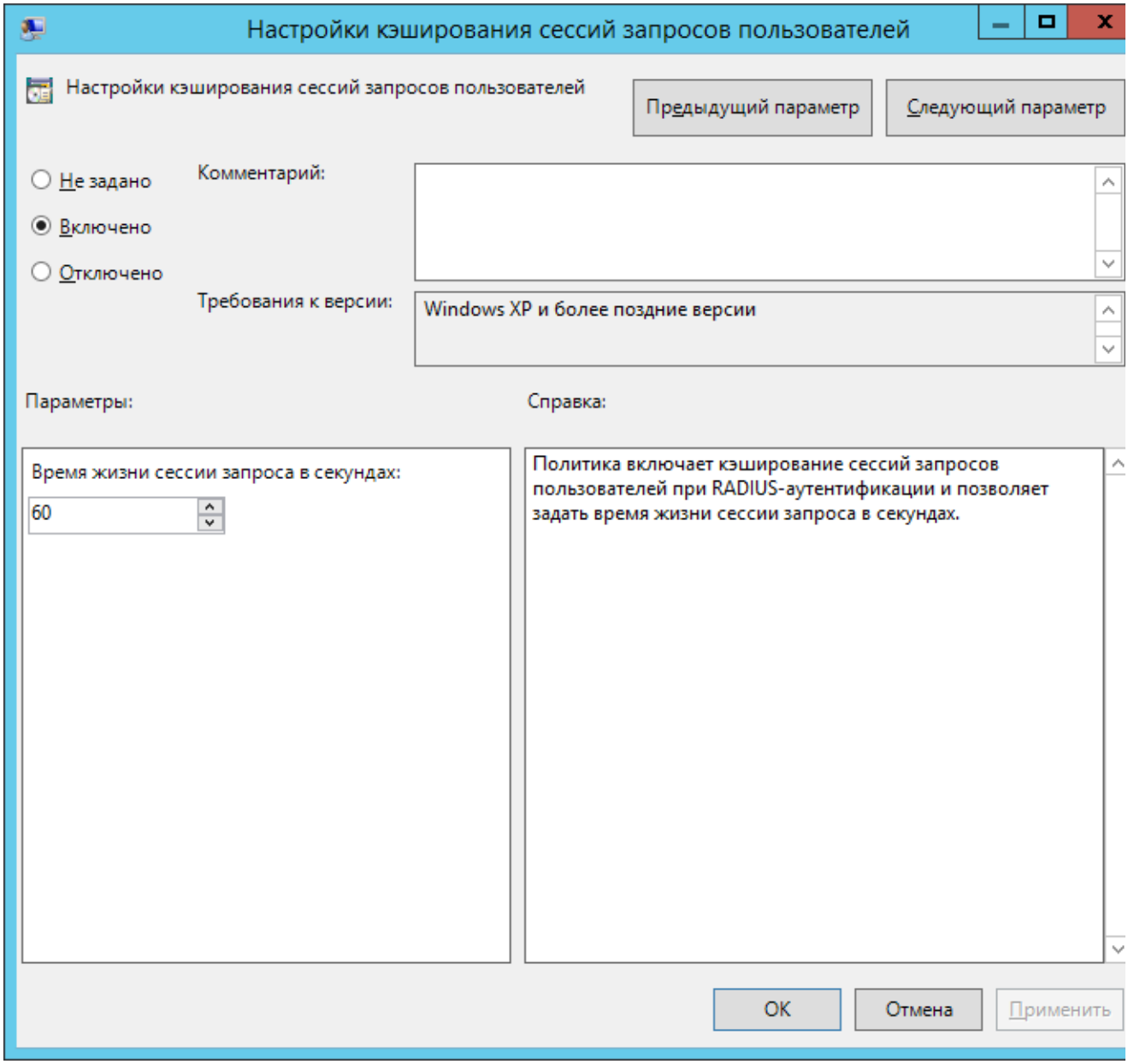
   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
   "UseNetBiosDomainName"=dword:00000001
   ```

Настройка кэширования сессий запросов пользователей

Политика включает кэширование сессий запросов пользователей при RADIUS-аутентификации и позволяет задать время жизни сессии запроса в секундах.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "**Конфигурация компьютера**" "**Административные шаблоны**" "**Indeed ID**" "**Radius**".
3. Откройте политику "**Настройка кэширования сессий запросов пользователей**".
4. Включите политику и в поле "**Время жизни сессии запроса в секундах**" укажите значение.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius**".

   > **Информация**
   >
   > При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "**DWORD**" с именем "**RequestSessionCachingEnabled**", в значении параметра укажите 1.
4. Создайте параметр типа "**DWORD**" с именем "**RequestSessionLifetimeSec**", в значении параметра укажите десятичное число в секундах.

   Пример

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
   "RequestSessionCachingEnabled"=dword:00000001
   "RequestSessionLifetimeSec"=dword:0000003c
   ```

Примеры внедрения расширения

1. **Настройка Cisco ASA для аутентификации через Indeed NPS RADIUS Extension**
2. **Настройка FortiGate VM для двухфакторной аутентификации через Indeed NPS Radius Extension**
3. **Установка и настройка аутентификации по OTP в Citrix Netscaler**