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\Indeed AM RADIUS Extension\<Номер версии>***

- **Indeed.AM.RADIUS.Extension-x64.ru-ru.msi** - Пакет для установки Indeed AM NPS Radius Extension
- **/Misc/GroupPolicyTemplates (ADMX)** - Шаблоны групповых политик для дополнительной настройки сервера и провайдеров.

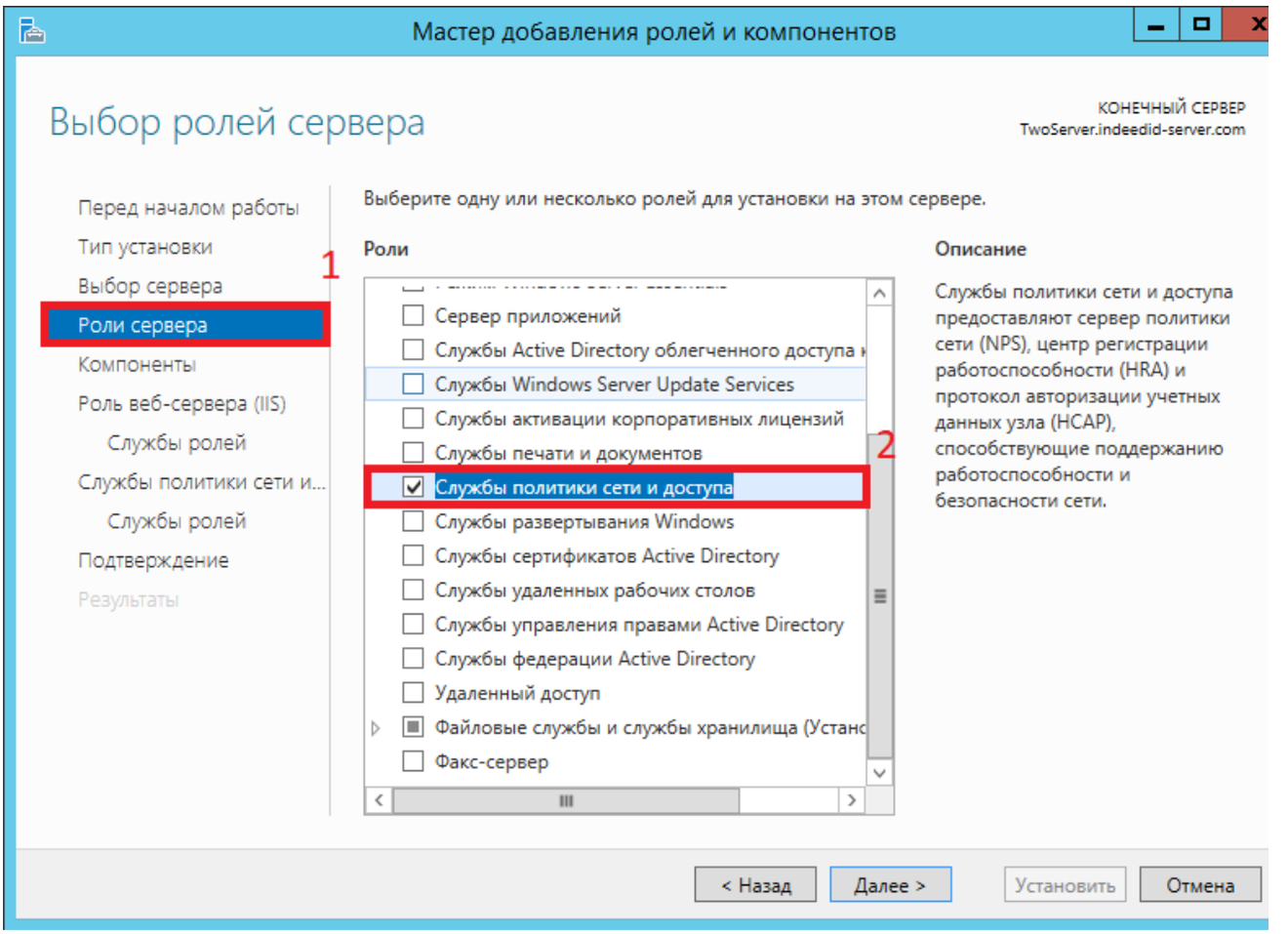
Установка Network Policy Server

Информация

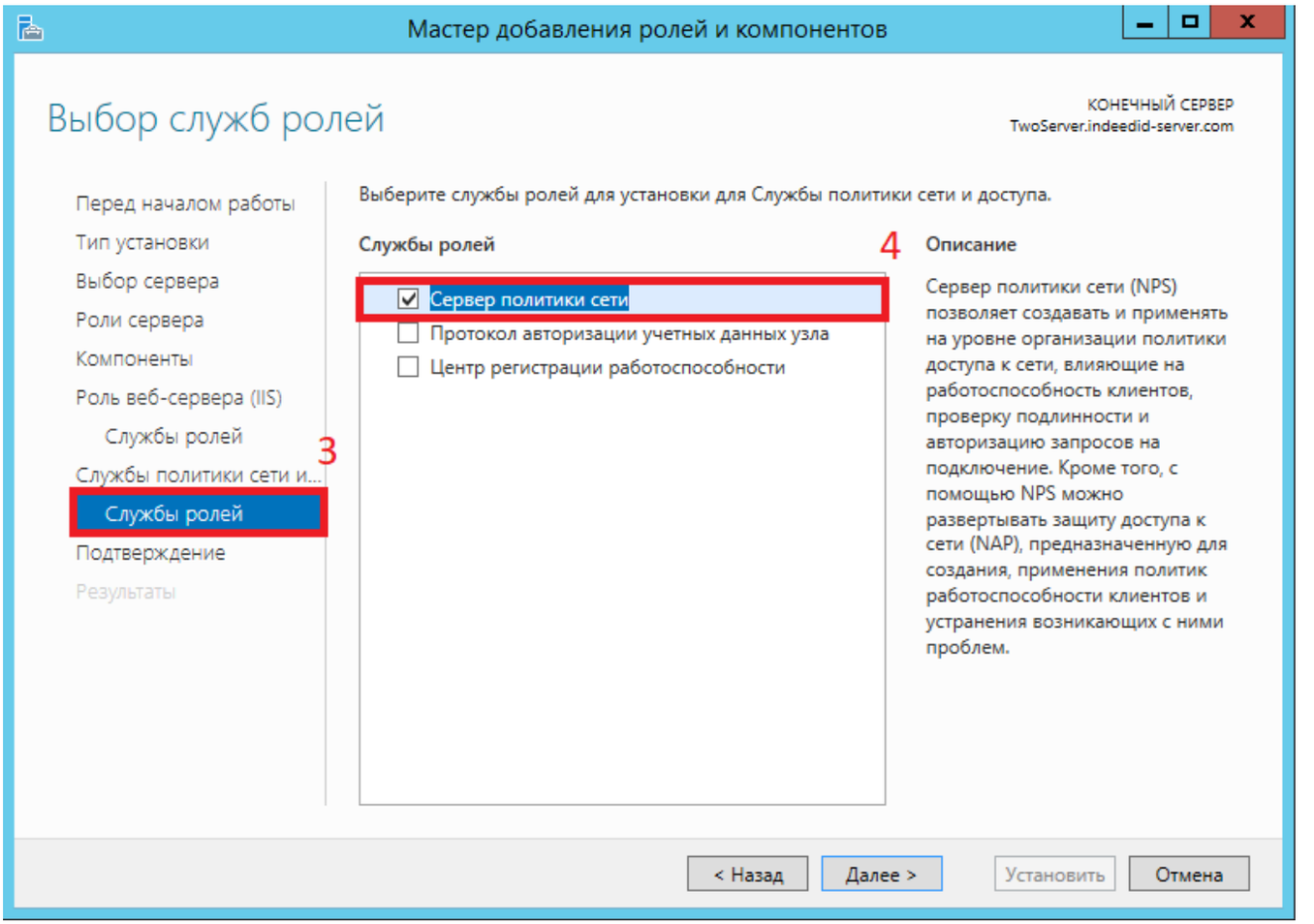
После установки кроме самой роли будет установлен Web-Server (IIS) и внутренняя база данных Windows.

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

1. Запустить **"Сервер сетевых политик"**.
2. Добавить в **RADIUS** - Клиенты Ваш **VPN сервер**. (**Правая кнопка мыши по RADIUS - Клиенты ->Новый документ**).

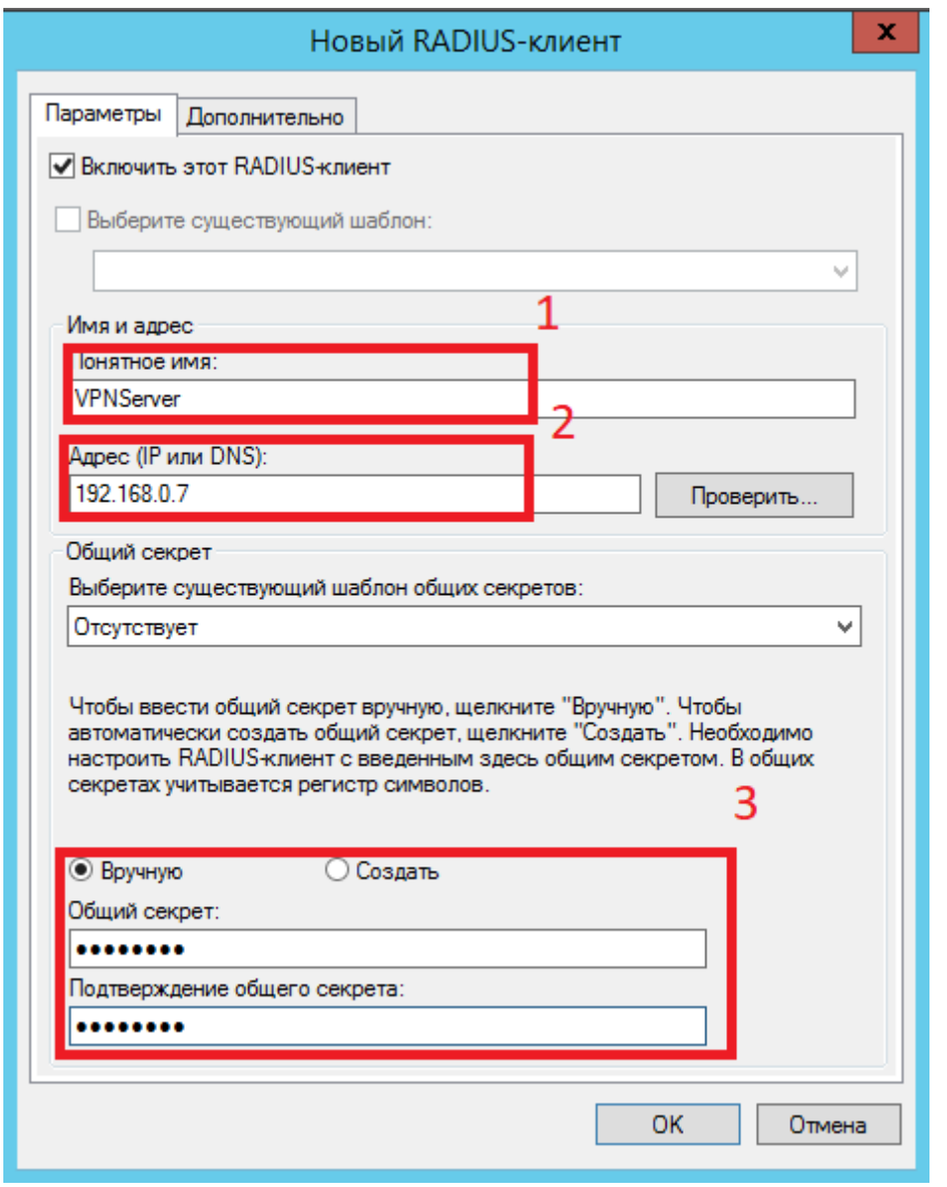
   Информация

   При использовании проверки подлинности **Chap** необходимо, в параметрах учетной записи пользователя, включить "**Хранить пароль, используя обратимое шифрование**" и обновить пароль пользователю.
3. Настроить нового клиента.

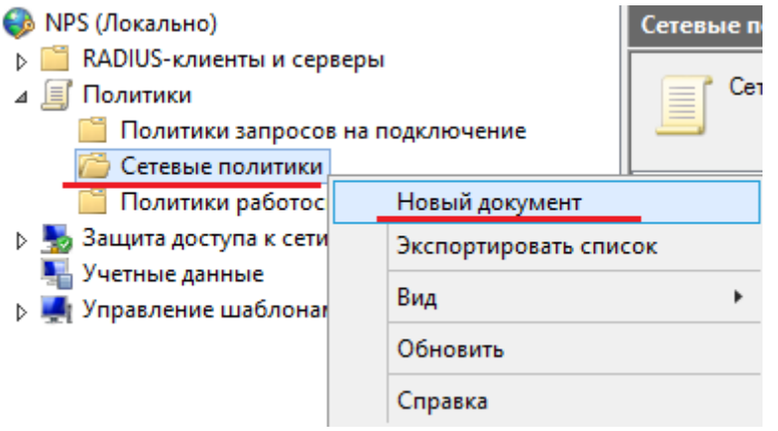
a. Добавить **имя** для нашего сервера **VPN (1)**.
b. Указать **IP адрес** нашего сервера **VPN (2)**.
c. Задать **секретный ключ** для соединения с сервером **(3)**.

Информация

Общий секретный ключ задается на сервере и на клиенте при подключении.



4. Добавьте сетевую политику для подключения Radius-клиентов.



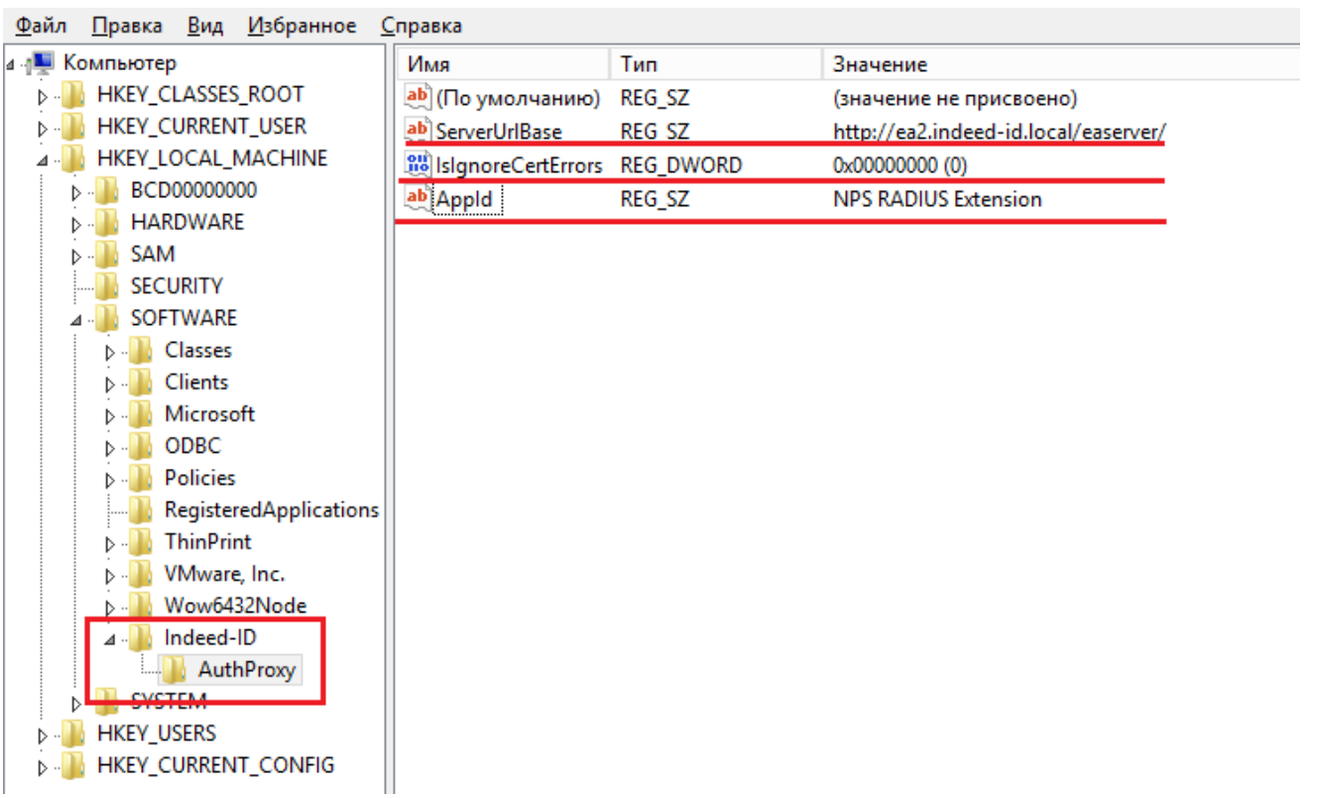
Установка Indeed AM NPS RADIUS Extension

1. Выполнить установку NPS RADIUS через запуск инсталлятора **Indeed.AM.RADIUS.Extension-x64.ru-ru.msi.**
2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy.** Измените параметры:
   a. Параметр **ServerUrlBase.** В значении для параметра укажите адрес вашего сервера **Indeed** .
   b. Параметр **IsIgnoreCertErrors,** указать значение **0** или **1.**

      Информация

      Данный параметр предназначен для проверки сертификата сервера **Indeed**, при значении **1** происходит игнорирование ошибок сертификата.

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



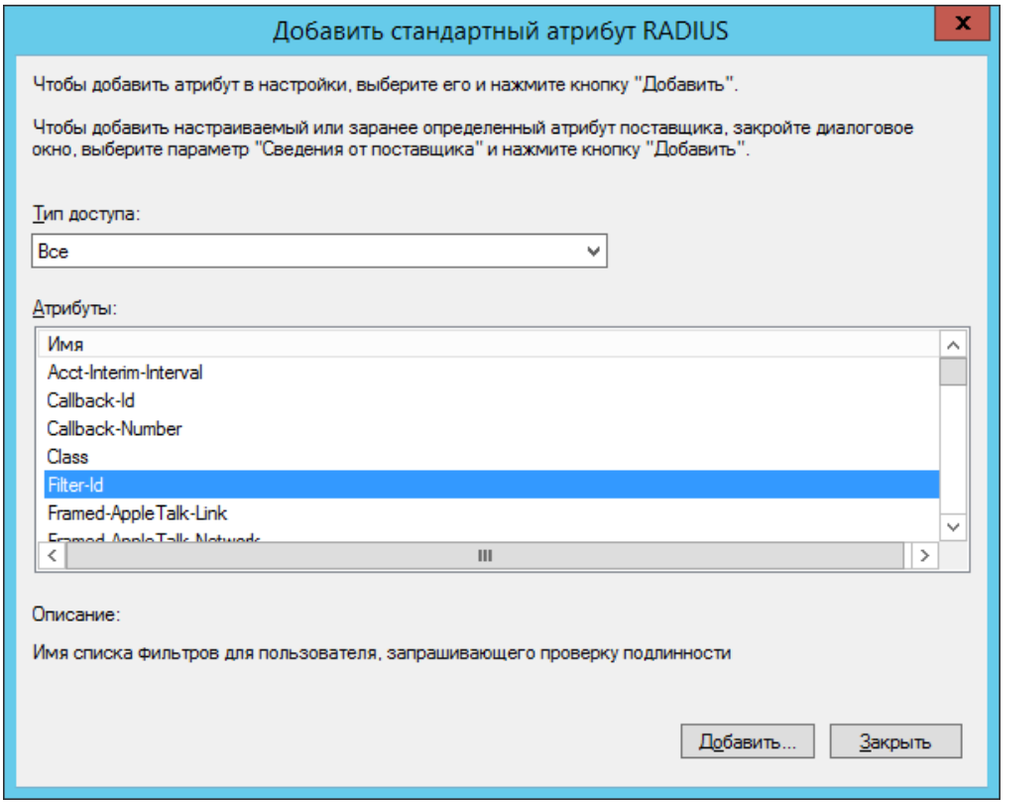
Настройка проброса атрибутов Radius

Информация

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

1. Откройте "**Политику запросов на подключение**".
2. Выберете имеющуюся или создайте новую политику и откройте вкладку "**Параметры**".

3. Выберете параметр "**Стандарт**" и нажмите "**Добавить**".
4. В окне "**Добавить стандартный атрибут Radius**" выберете "**Filter-Id**" и нажмите "**Добавить**".



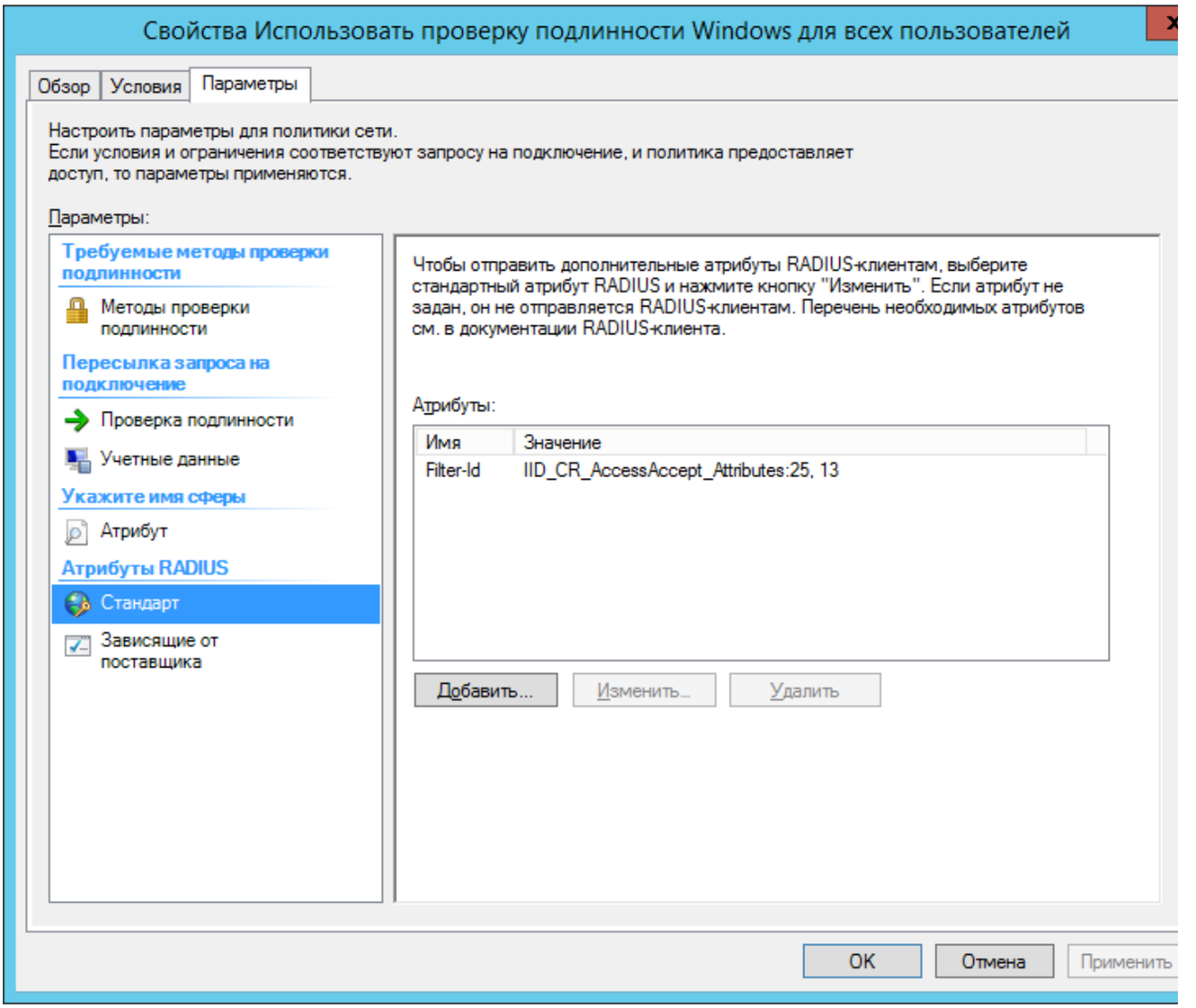
5. В окне "**Сведения об атрибуте**" нажмите "**Добавить**". Убедитесь, что параметр "**Формат ввода атрибута**" - строковый, и введите строку формата:
IID_CR_AccessAccept_Attributes:<id требуемого атрибута 1>, <id требуемого атрибута 1>

   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 политики

Информация

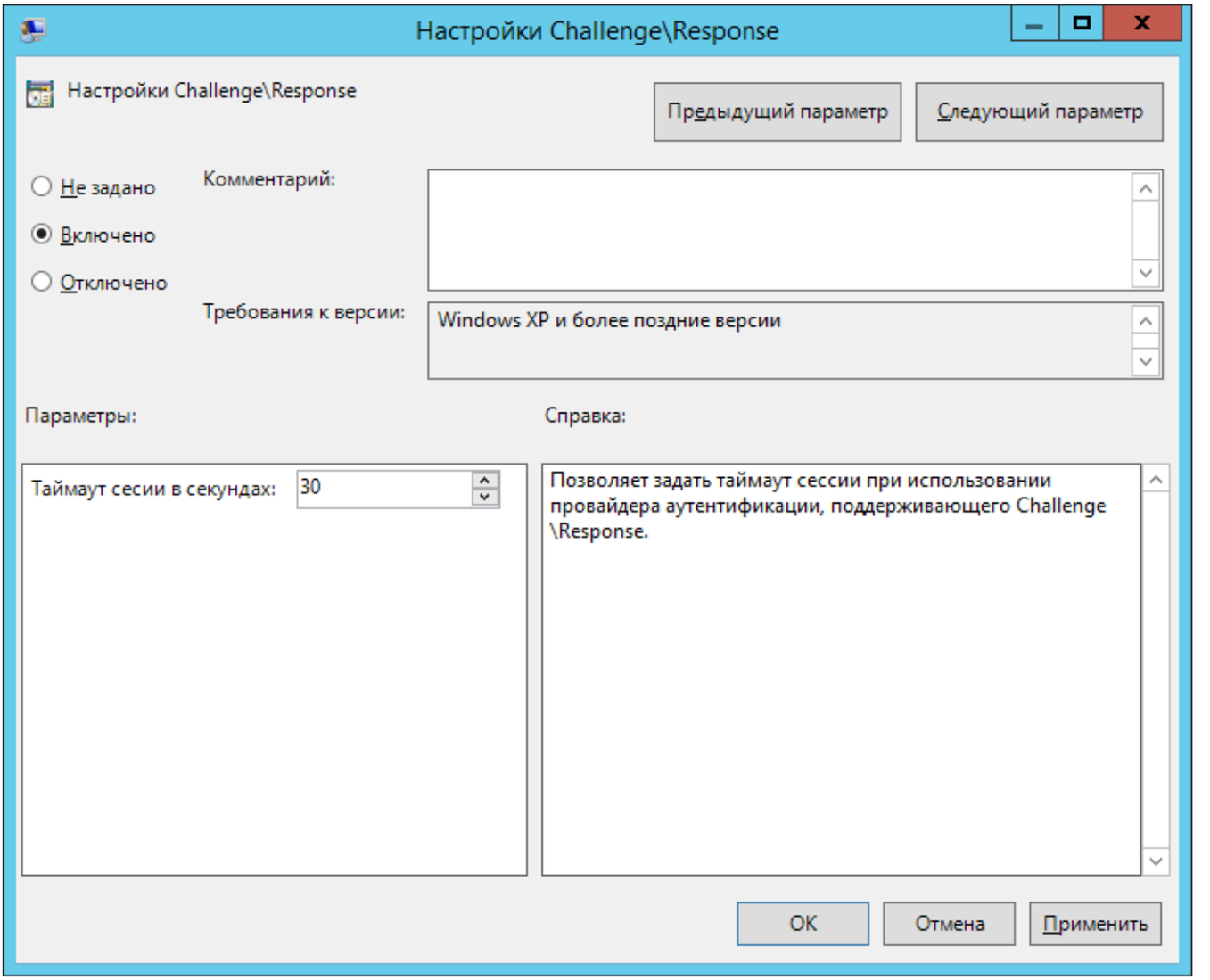
Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Информация

Политики применяется к серверам с развернутой ролью NPS и позволяет изменять настройки компонента.

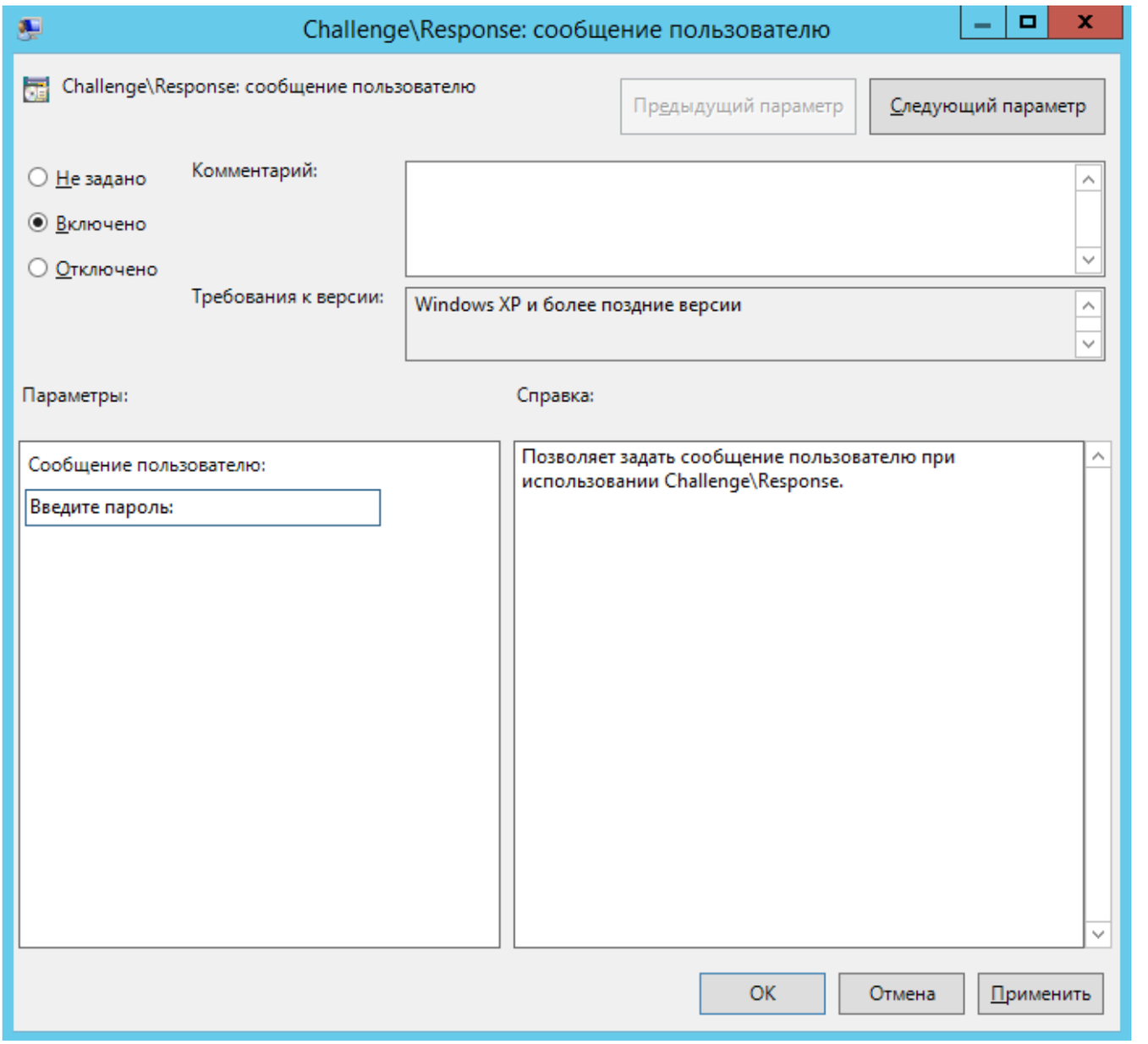
Настройки Challenge\Response

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



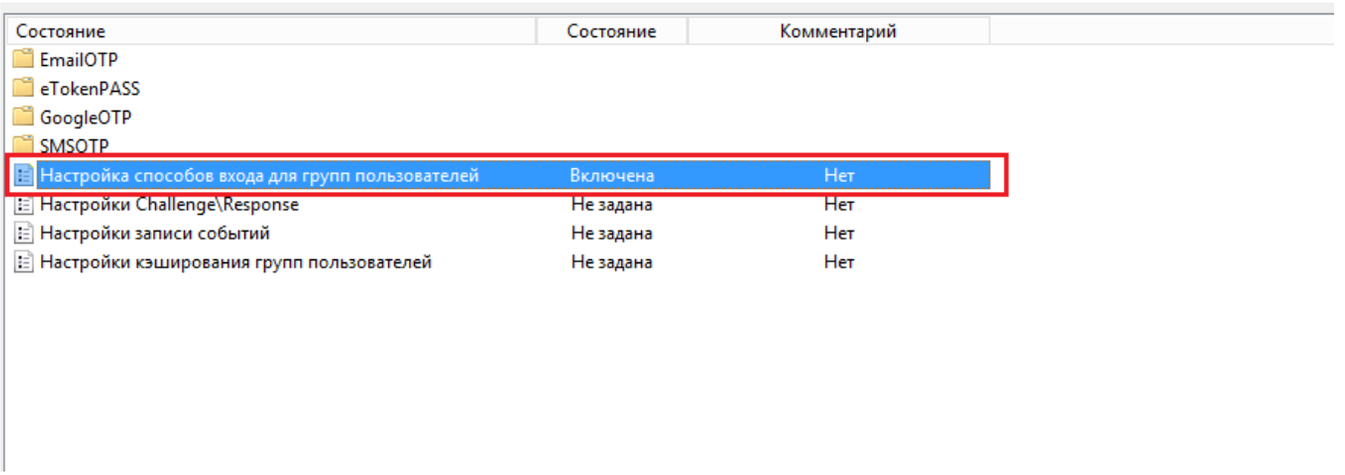
Challenge\Response: сообщение пользователю

Политика позволяет задать сообщение пользователю, которые отображается при запросе второго фактора.

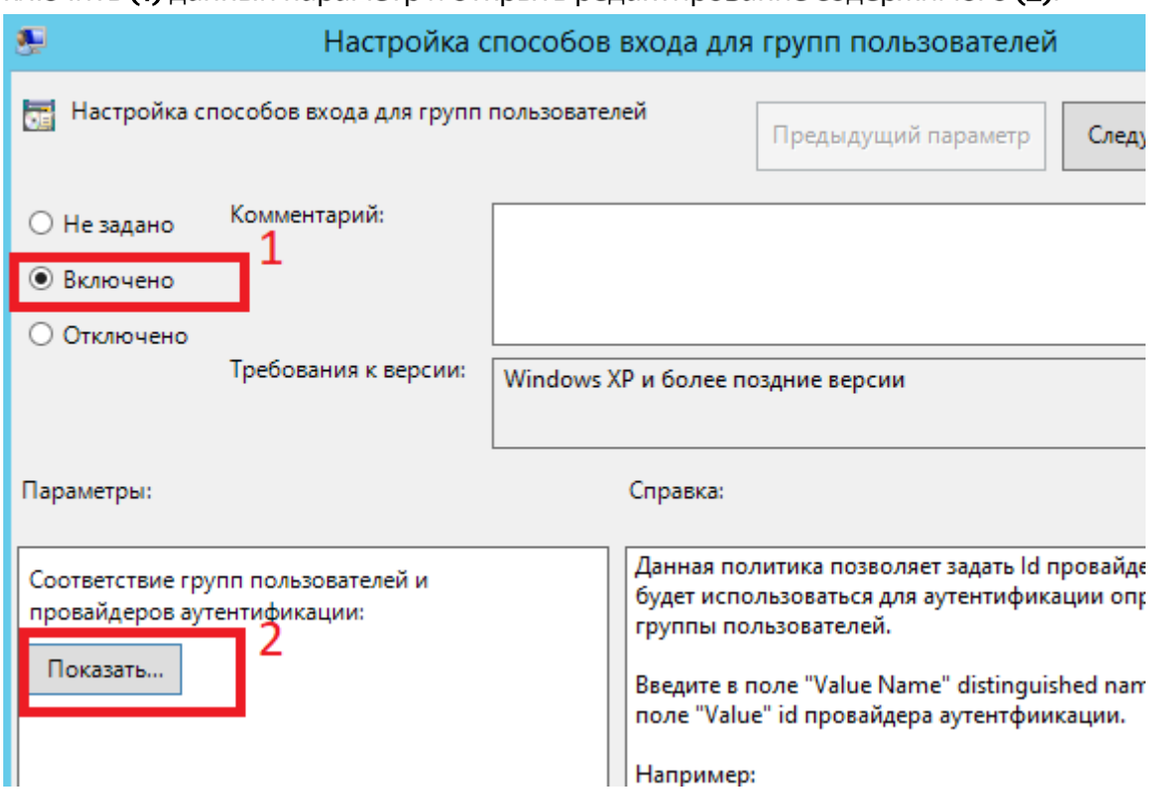


Настройка способов входа для групп пользователей

a. Открыть для редактирования **"Настройка способов входа для групп пользователей "**.



b. Включить **(1)** данный параметр и открыть редактирование содержимого **(2)**.



c. Добавьте в **"Имя значения"** значение атрибута **"distinguishedName"** вашей группы пользователей.

d. Вставьте в **"Значение"** 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**

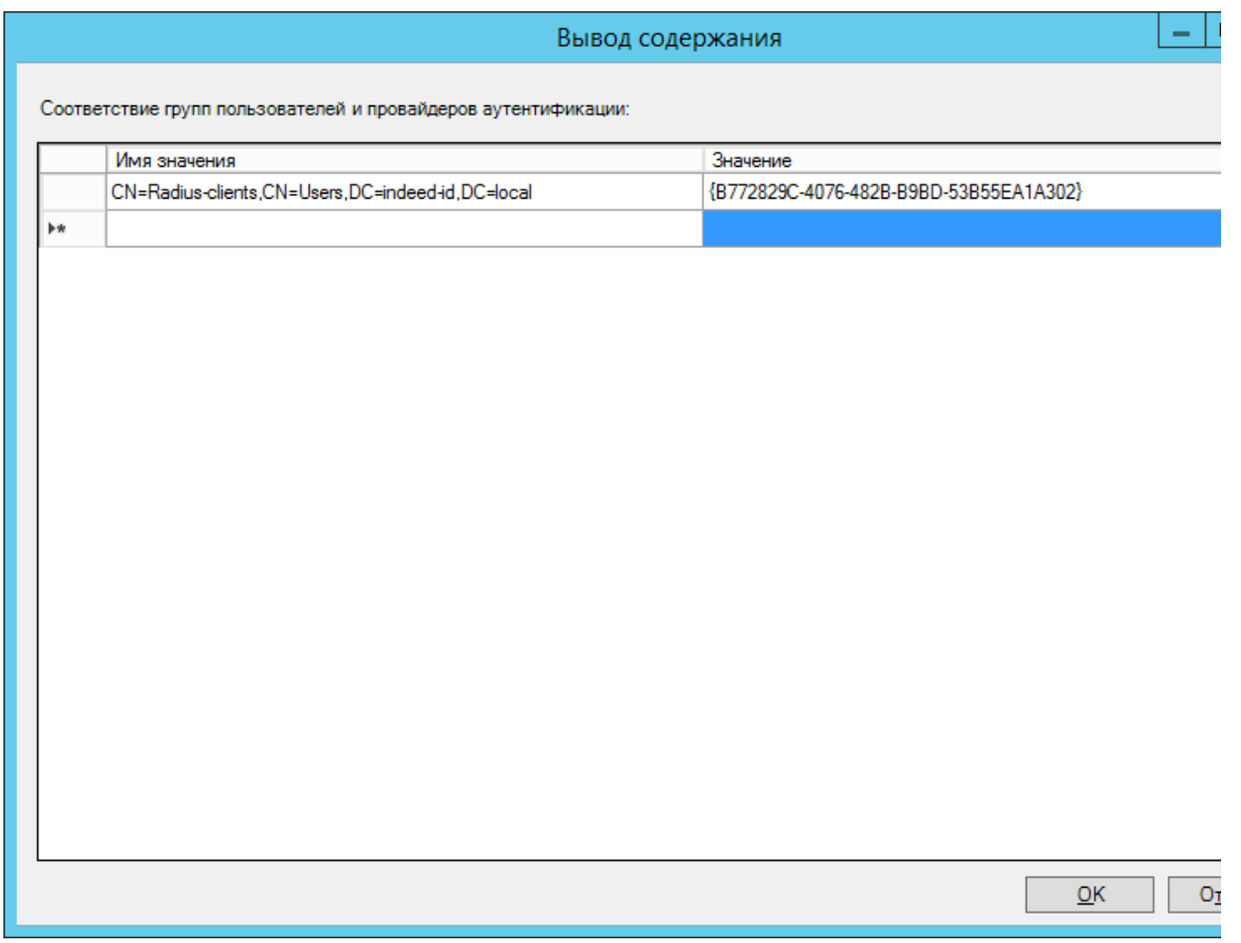
{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

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

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

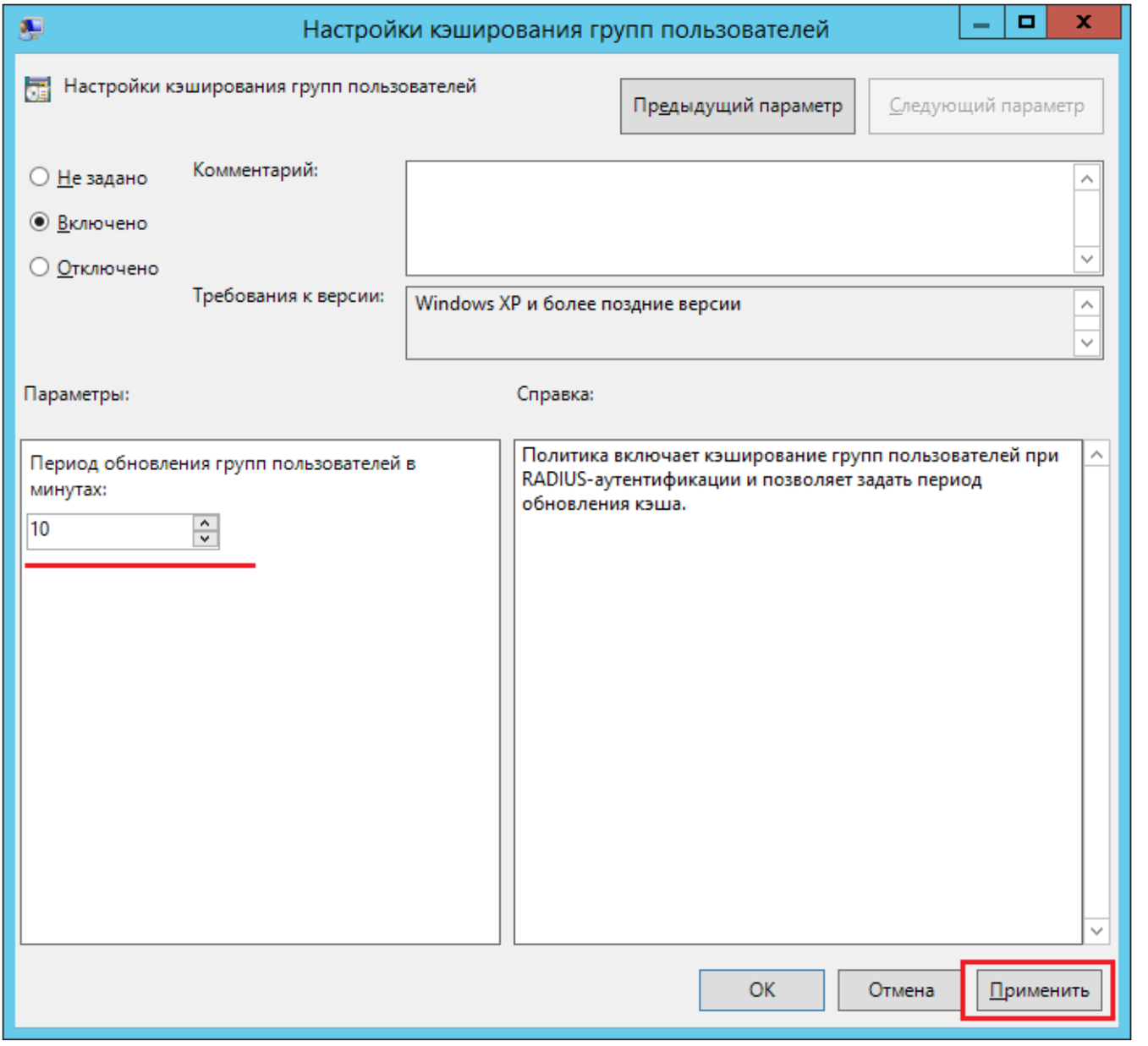
{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **HTOTP Provider**

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



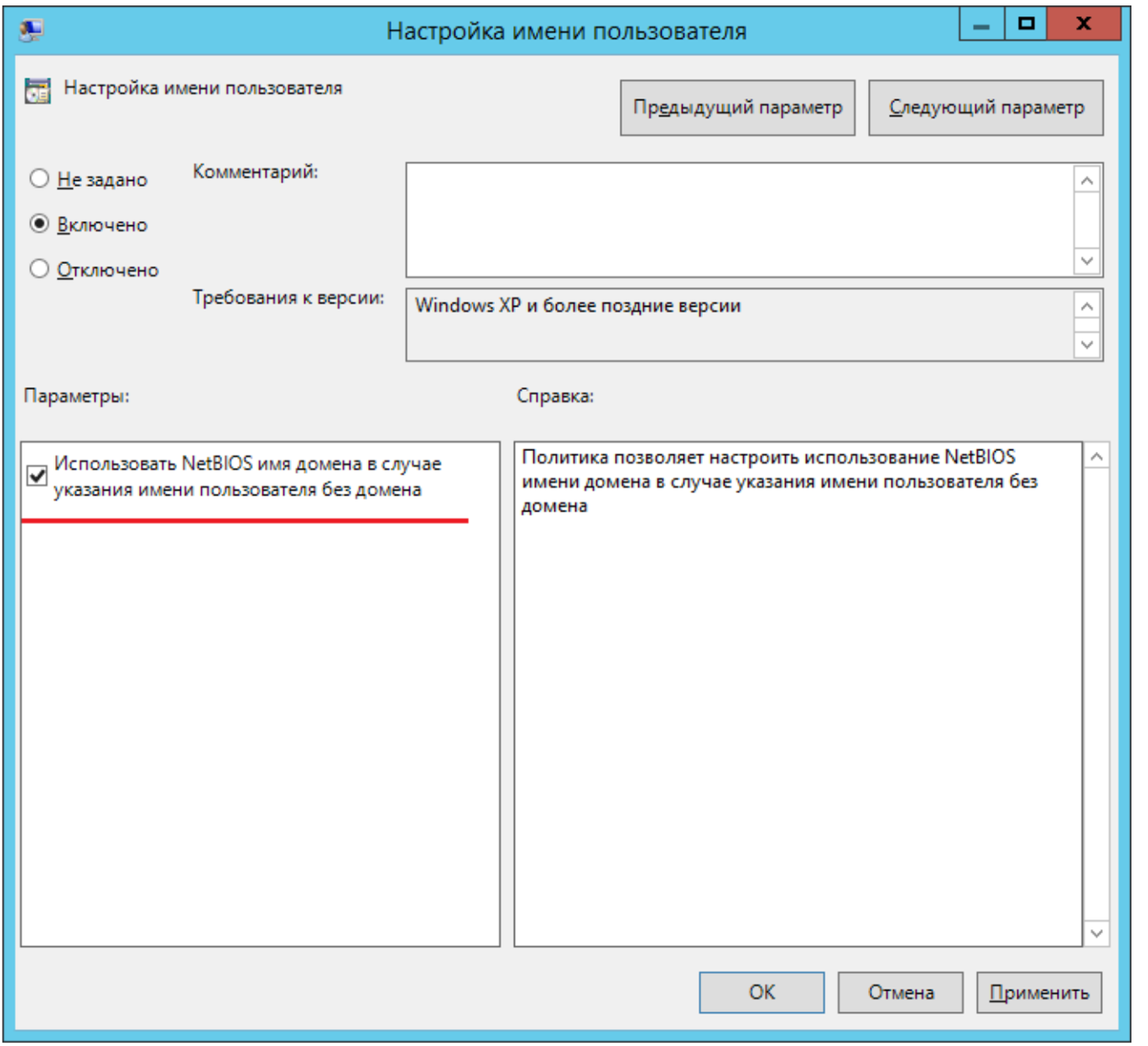
Кэширование групп пользователей

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



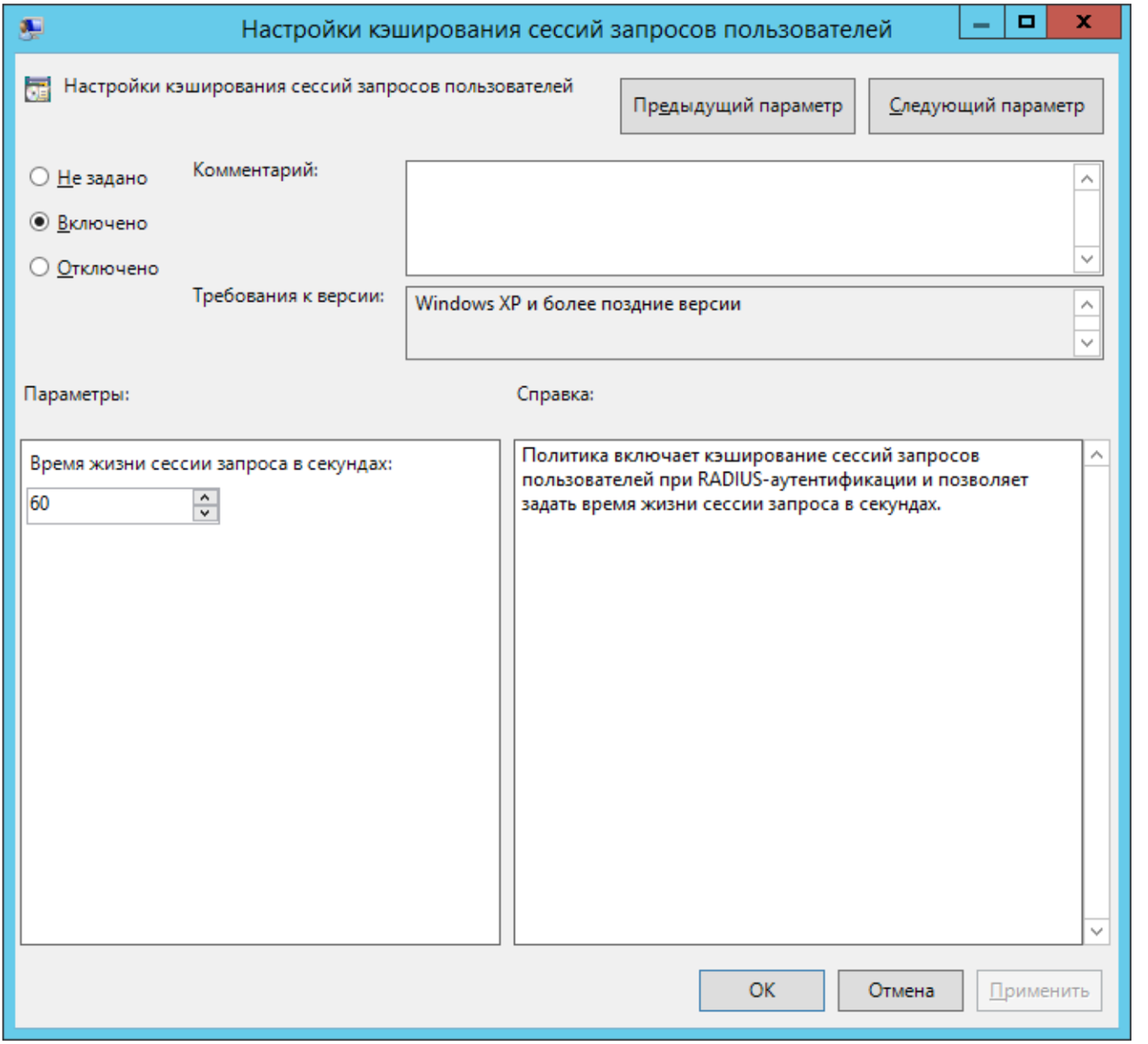
Настройка имени пользователя

Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена. Для включения политики активируйте параметр: "**Использовать NetBIOS имя домена в случае указания имени пользователя без домена**"



Настройка кэширования сессий запросов пользователей

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



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**