

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

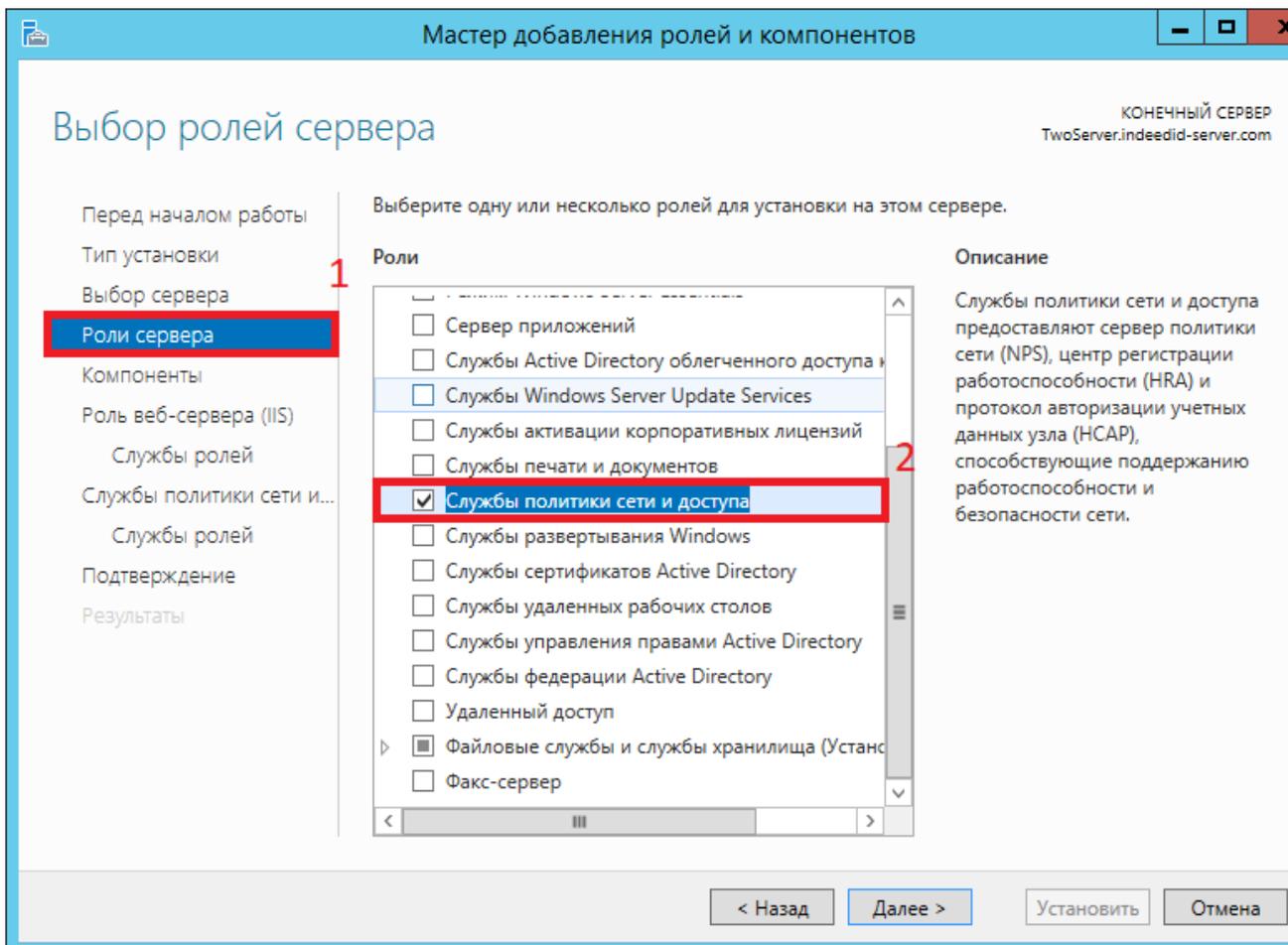
Файлы для Indeed AM NPS Radius Extension расположены: ***indeed AM <Номер версии>\Indeed AM RADIUS Extension\<Номер версии>***

- **IndeedID.EA.RADIUS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM NPS Radius Extension.
- **Misc** - Файлы шаблонов групповых политик для дополнительной настройки сервера и провайдеров.

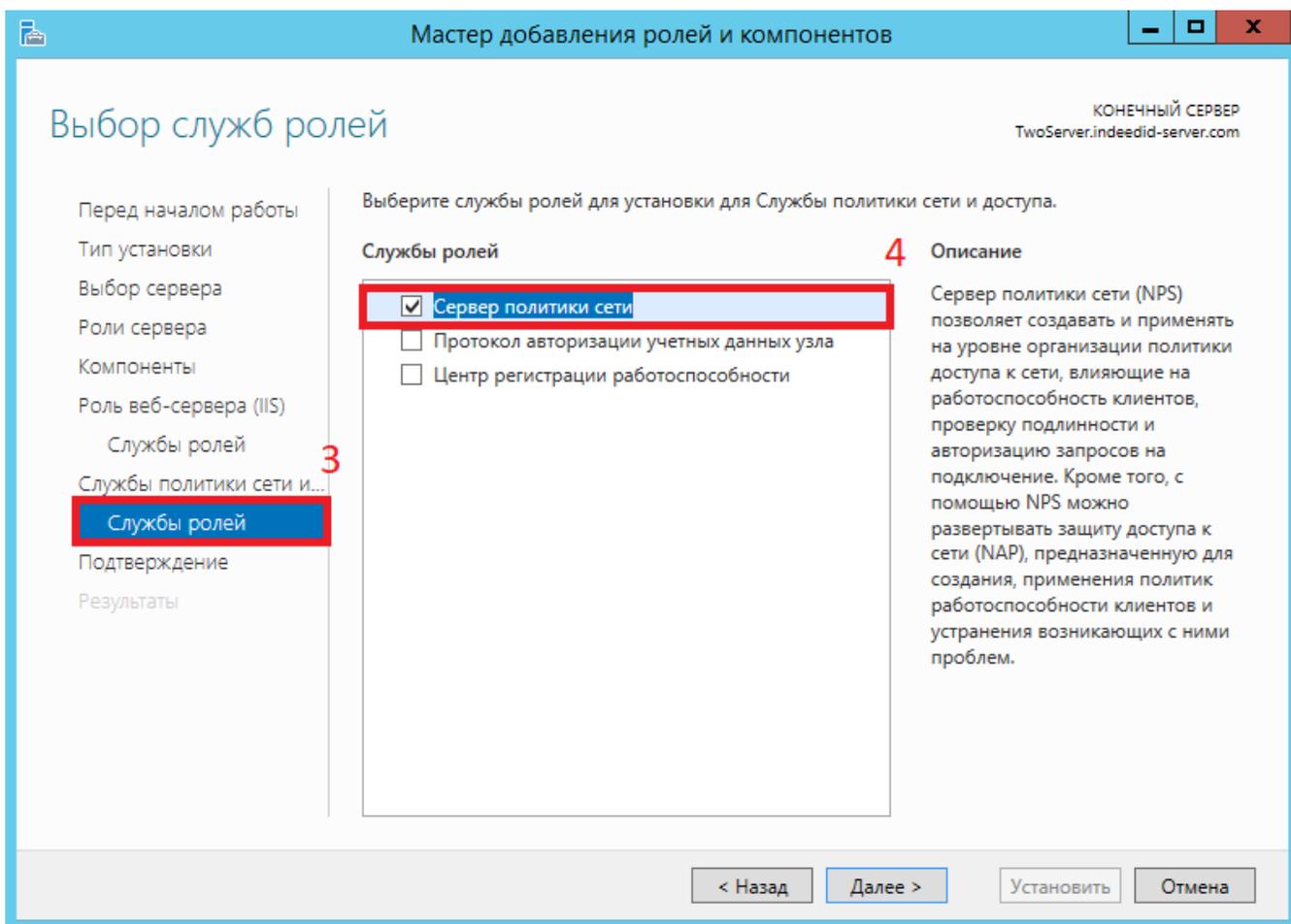
Установка Network Policy Server

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).

И 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.

Новый RADIUS-клиент

Параметры Дополнительно

Включить этот RADIUS-клиент

Выберите существующий шаблон:

Имя и адрес

Понятное имя:
VPNServer

Адрес (IP или DNS):
192.168.0.7

Проверить...

Общий секрет

Выберите существующий шаблон общих секретов:
Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

Вручную Создать

Общий секрет:
.....

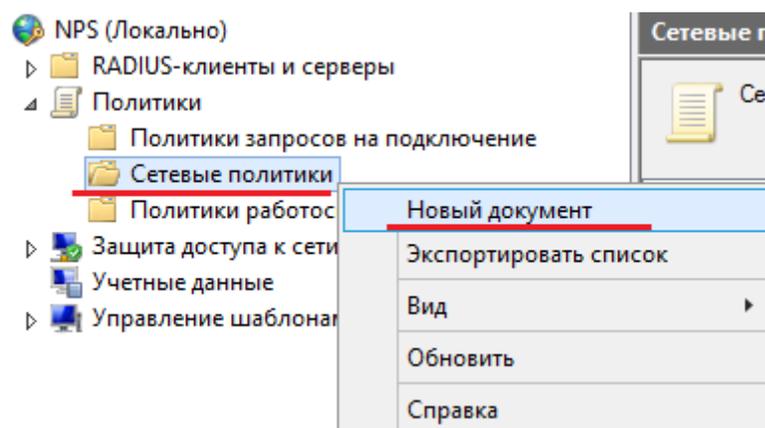
Подтверждение общего секрета:
.....

ОК Отмена

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".

Новая политика сети



Укажите имя политики сети и тип подключения

Вы можете указать имя политики сети и тип подключений, к которому применяется политика.

Имя политики:

Способ сетевого подключения

Выберите тип сервера доступа к сети, отправляющего запрос на подключение серверу сетевых политик. Можно выбрать тип сетевого сервера или параметр "Зависящие от поставщика" (ни то, ни другое не является обязательным). Если в качестве сервера сетевых политик используется коммутатор 802.1X или беспроводная точка доступа, выберите "Не указано".

Тип сервера доступа к сети:

Не указано

Зависящие от поставщика:

10

Назад **Далее** Готово Отмена

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.

Новая политика сети



Укажите условия

Задайте условия, определяющие, используется ли данная политика сети для запросов на подключение. Необходимо указать хотя бы одно условие.

Условия:

Условие	Значение
 Группы пользователей	INDEED\RadiusClient

Описание условия:

Условие "Группы пользователей" указывает, что подключающийся пользователь должен принадлежать к одной из выбранных групп.

Добавить...

Изменить...

Удалить

Назад

Далее

Готово

Отмена

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".

И Информация

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

Новая политика сети



Настройка методов проверки подлинности

Настройте один или несколько методов проверки подлинности, которые требуются для соответствия запроса на подключение данной политике. Для проверки подлинности EAP необходимо настроить тип EAP.

Типы EAP согласуются между сервером сетевых политик (NPS) и клиентом в порядке перечисления.

Типы EAP:

Вверх

Вниз

Добавить...

Изменить...

Удалить

Менее безопасные методы проверки подлинности:

- Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2)
 - Разрешить смену пароля по истечении срока действия
- Шифрованная проверка подлинности Майкрософт (MS-CHAP)
 - Разрешить смену пароля по истечении срока действия
- Шифрованная проверка подлинности (CHAP)
- Проверка открытым тестом (PAP, SPAP)
- Разрешить подключение клиентов без согласования метода проверки подлинности.

Назад

Далее

Готово

Отмена

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".

Новая политика сети



Завершение создания политики сети

Успешно создана следующая политика сети:

Netscaler

Условия политики:

Условие	Значение
Группы пользователей	INDEED\RadiusClient

Параметры политики:

Условие	Значение
Метод проверки подлинности	MS-CHAP v1 OR (ИЛИ) MS-CHAP v1 (Разрешить смену паро...
Права доступа	Разрешение доступа к узлу
Framed-Protocol	PPP
Service-Type	Framed
Игнорировать свойства удаленного доступа пользователя	False (ложь)

Для завершения мастера нажмите кнопку "Готово".

Назад

Далее

Готово

Отмена

Установка Indeed AM NPS RADIUS Extension

1. Выполните установку NPS RADIUS через запуск пакета для установки Indeed AM NPS Radius Extension.
2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy**. Измените параметры:

- a. Параметр **ServerUrlBase**. В значении для параметра укажите адрес вашего сервера **Indeed**.

 **Информация**

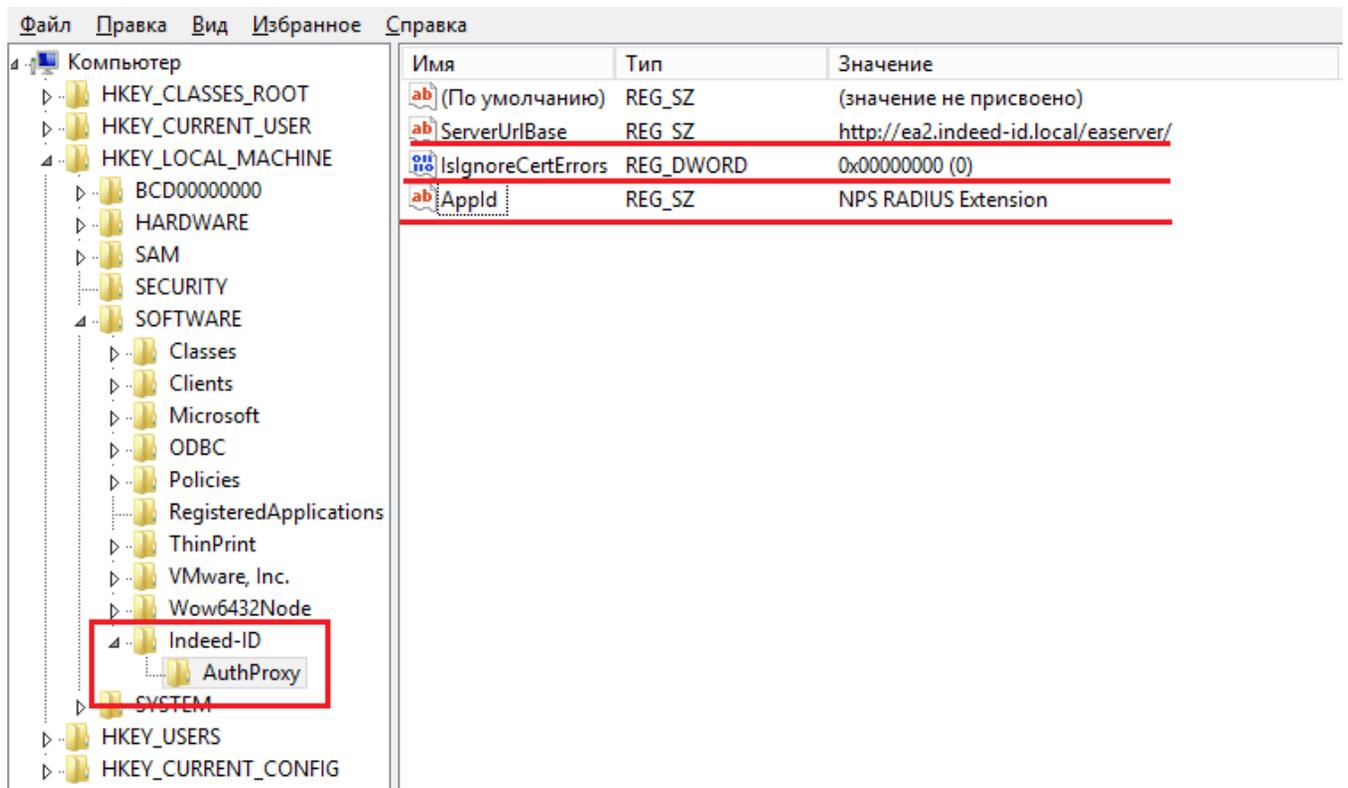
При использовании https соединения требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

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

 **Информация**

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

- c. Параметр **Appld** со значением **NPS RADIUS Extension**.



The screenshot shows the Windows Registry Editor with the following configuration:

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
ServerUrlBase	REG_SZ	http://ea2.indeed-id.local/easerver/
IsIgnoreCertErrors	REG_DWORD	0x00000000 (0)
Appld	REG_SZ	NPS RADIUS Extension

Настройка проброса атрибутов Radius

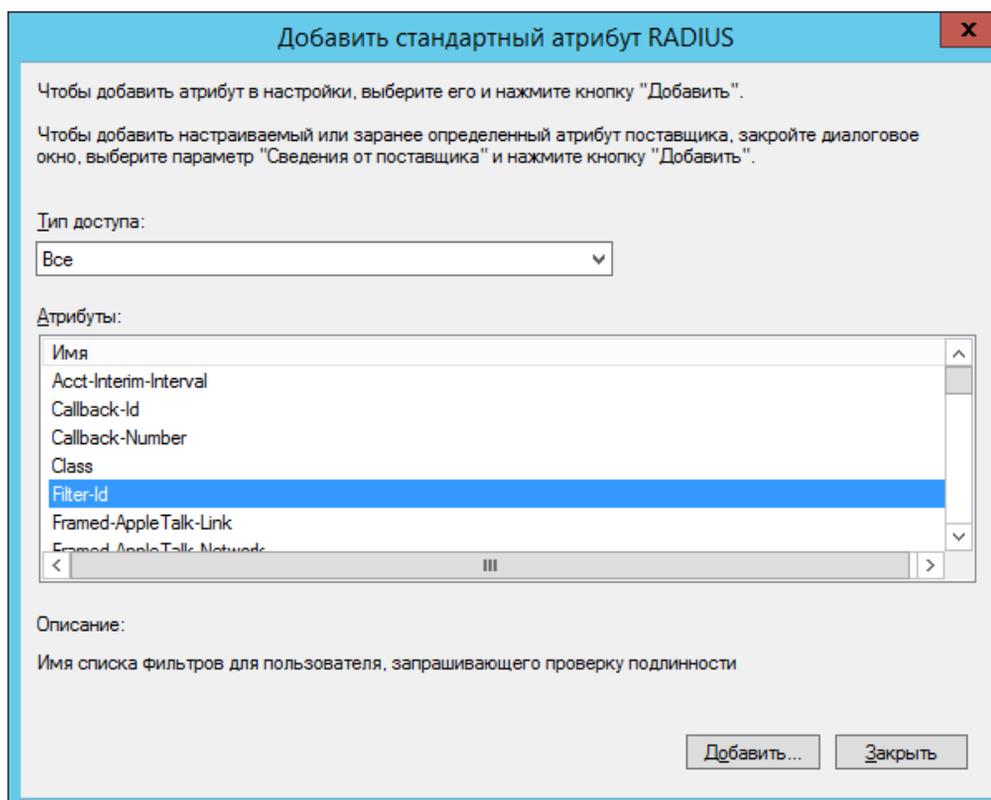
Информация

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**" выберите "**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>

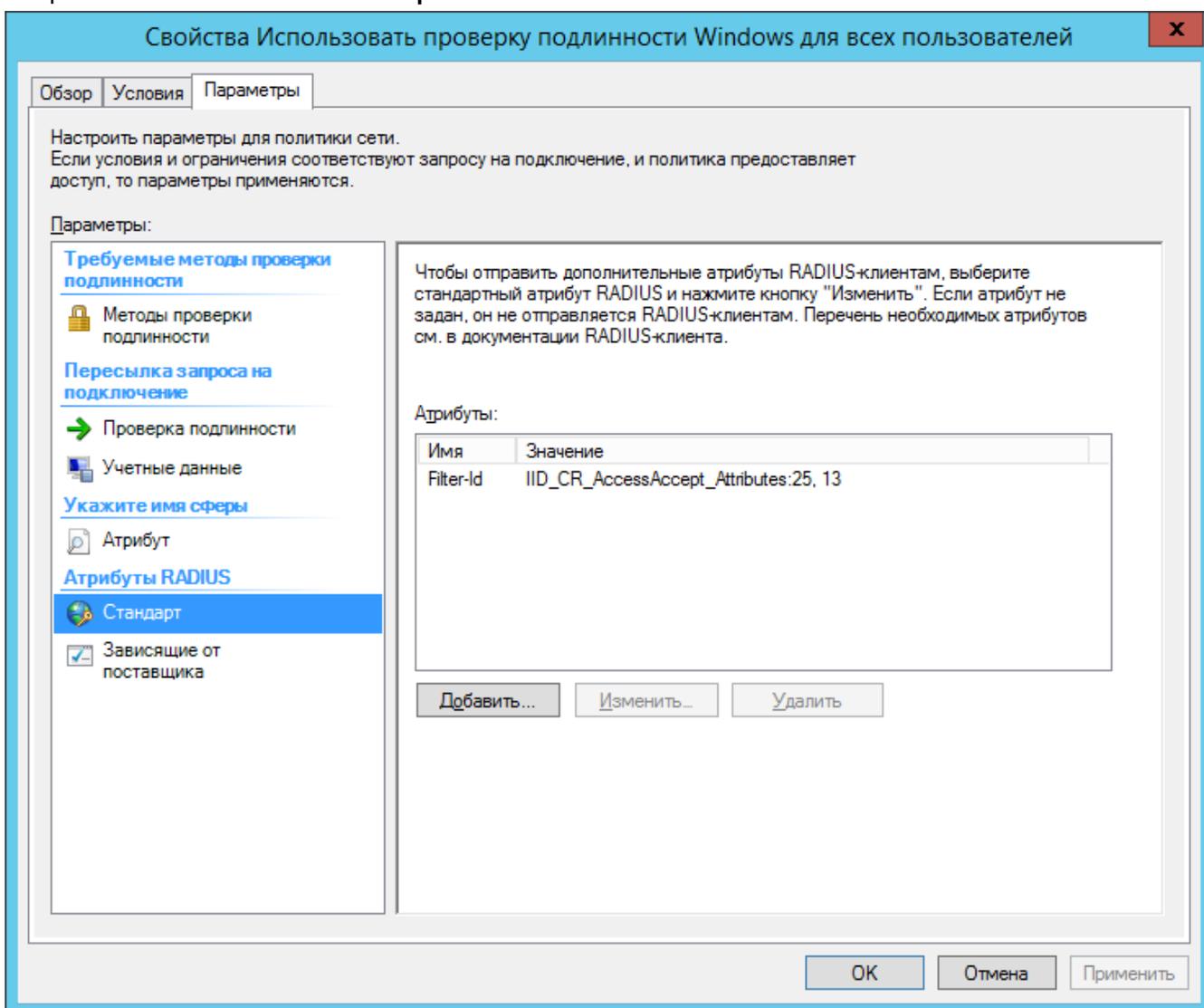
Информация

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:

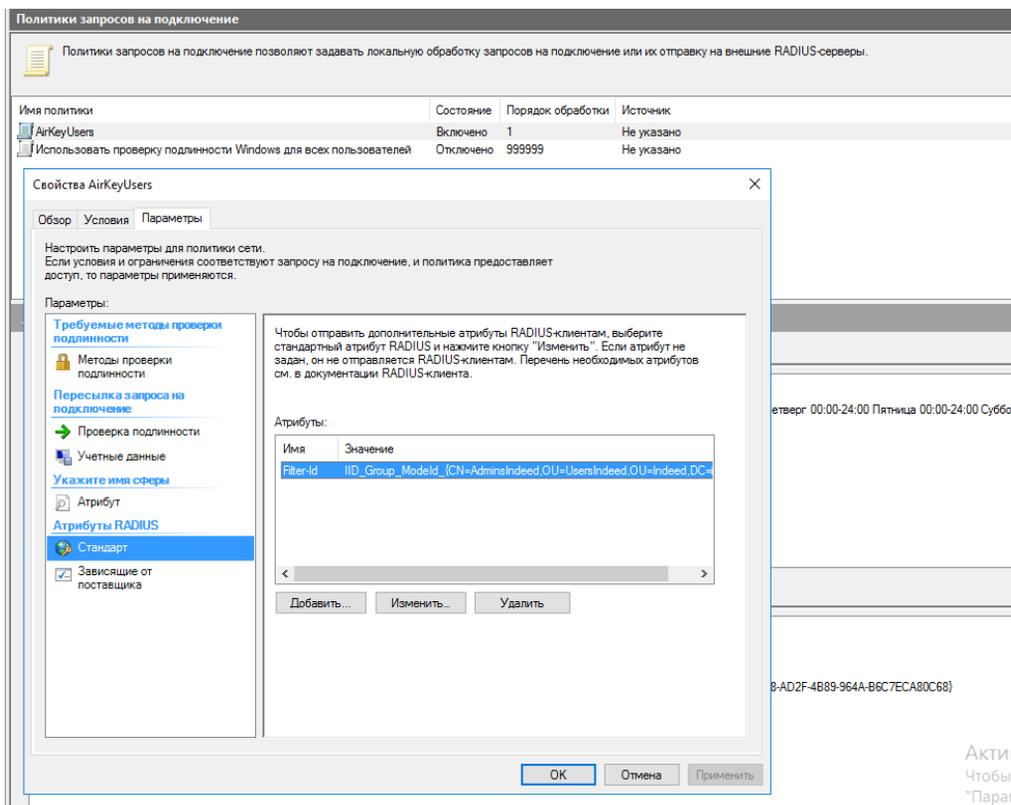
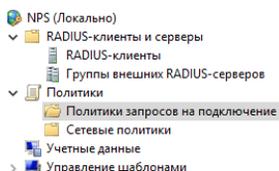
- Общая настройка способа входа
- Настройка способов входа для групп пользователей

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 имеющуюся 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
ID_Modeld_{ProviderId}	<p>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".</p> <p>Пример значения атрибута с Indeed AM Software OTP Provider: IID_Modeld_{B772829C-4076-482B-B9BD-53B55EA1A302}</p>
ID_Group_Modeld_{DN}_{ProviderId}	<p>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.</p> <p>Значение DN – различающееся имя группы (Distinguished Name).</p> <p>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.</p> <p>Пример значения с Indeed AM AirKey Provider: IID_Group_Modeld_{CN=AdminsIndeed,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local}_{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}</p>



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".

Состояние	Состояние	Комментарий
📁 EmailOTP		
📁 eTokenPASS		
📁 GoogleOTP		
📁 SMSOTP		
🔗 Настройка способов входа для групп пользователей	Включена	Нет
🔗 Настройки Challenge\Response	Не задана	Нет
🔗 Настройки записи событий	Не задана	Нет
🔗 Настройки кэширования групп пользователей	Не задана	Нет

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

Настройка способов входа для групп пользователей

Настройка способов входа для групп пользователей

○ Не задано Комментарий:

Включено 1

○ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Соответствие групп пользователей и провайдеров аутентификации:

 2

Данная политика позволяет задать Id провайдера, который будет использоваться для аутентификации опр. группы пользователей.

Введите в поле "Value Name" distinguished name, а в поле "Value" id провайдера аутентификации.

Например:

5. Укажите в "Имя значения" значение атрибута "distinguishedName" 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**

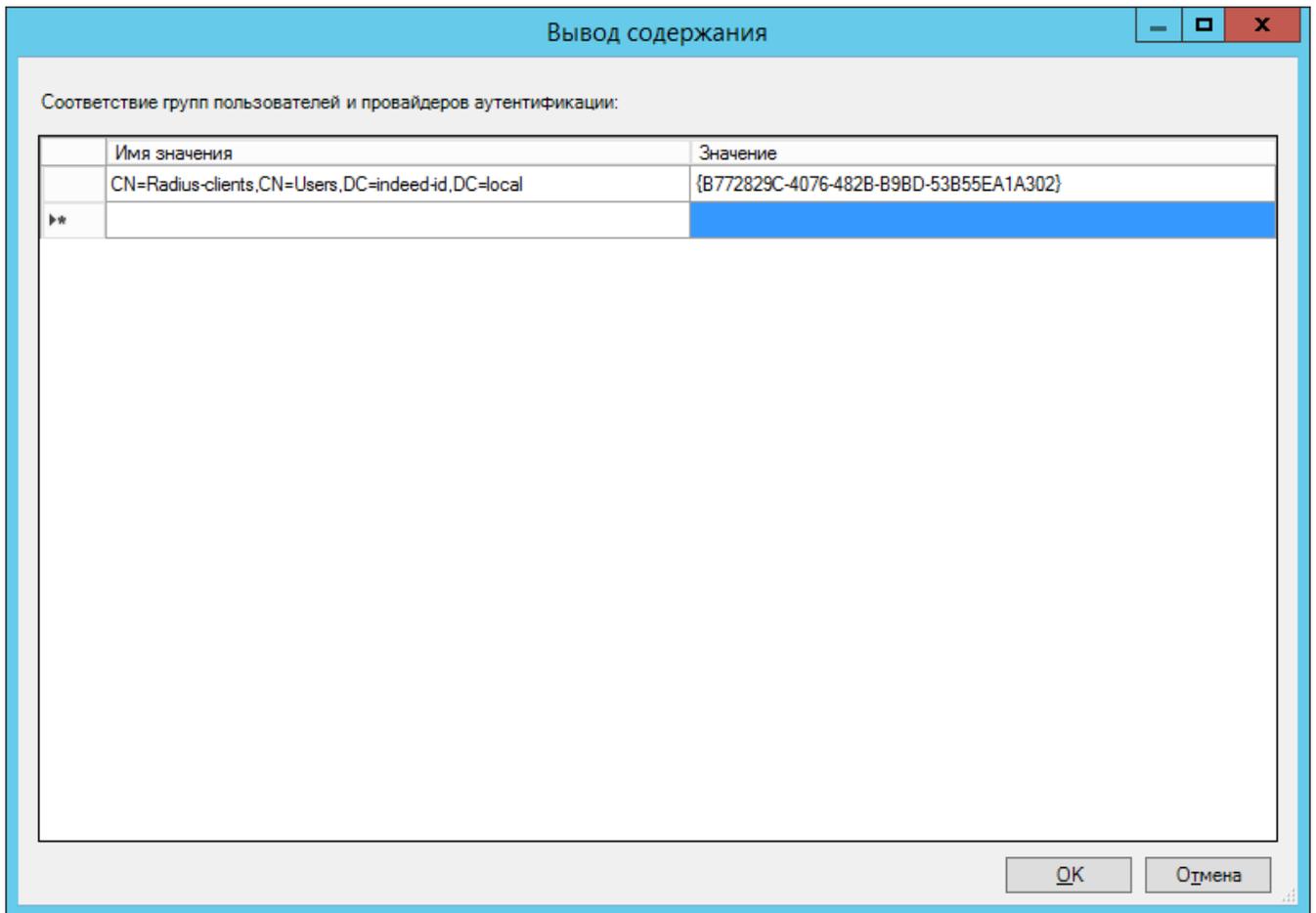
{CA4645CC-5896-485E-A6CA-011FCC20DF1D} - **Telegram OTP**



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" целевой группы пользователей, в значении укажите ID используемого параметра.

Пример

Windows Registry Editor Version 5.00

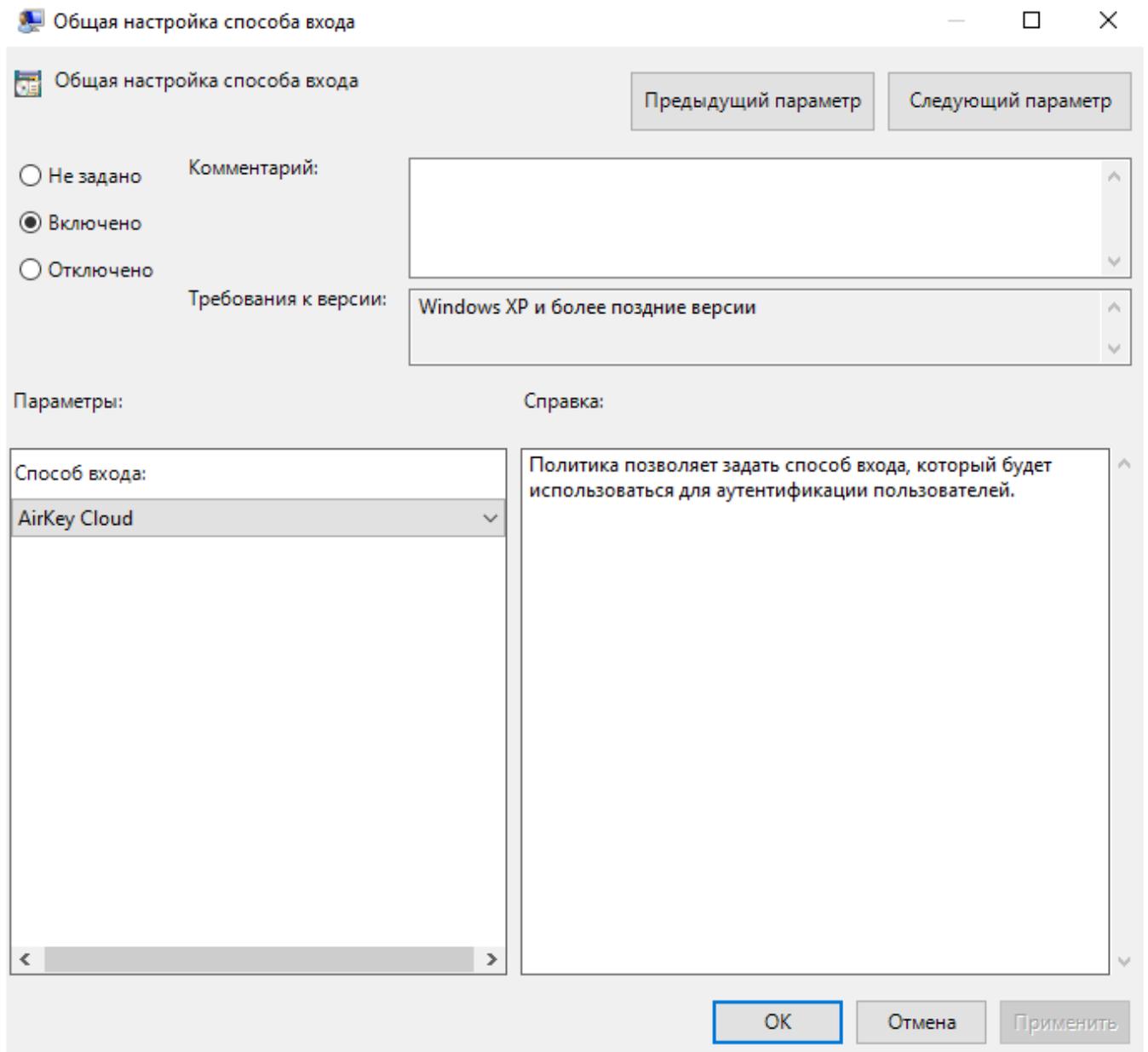
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\GroupDNProviderId]
"CN=RadiusClient,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local"="{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}"
```

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" выберите 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

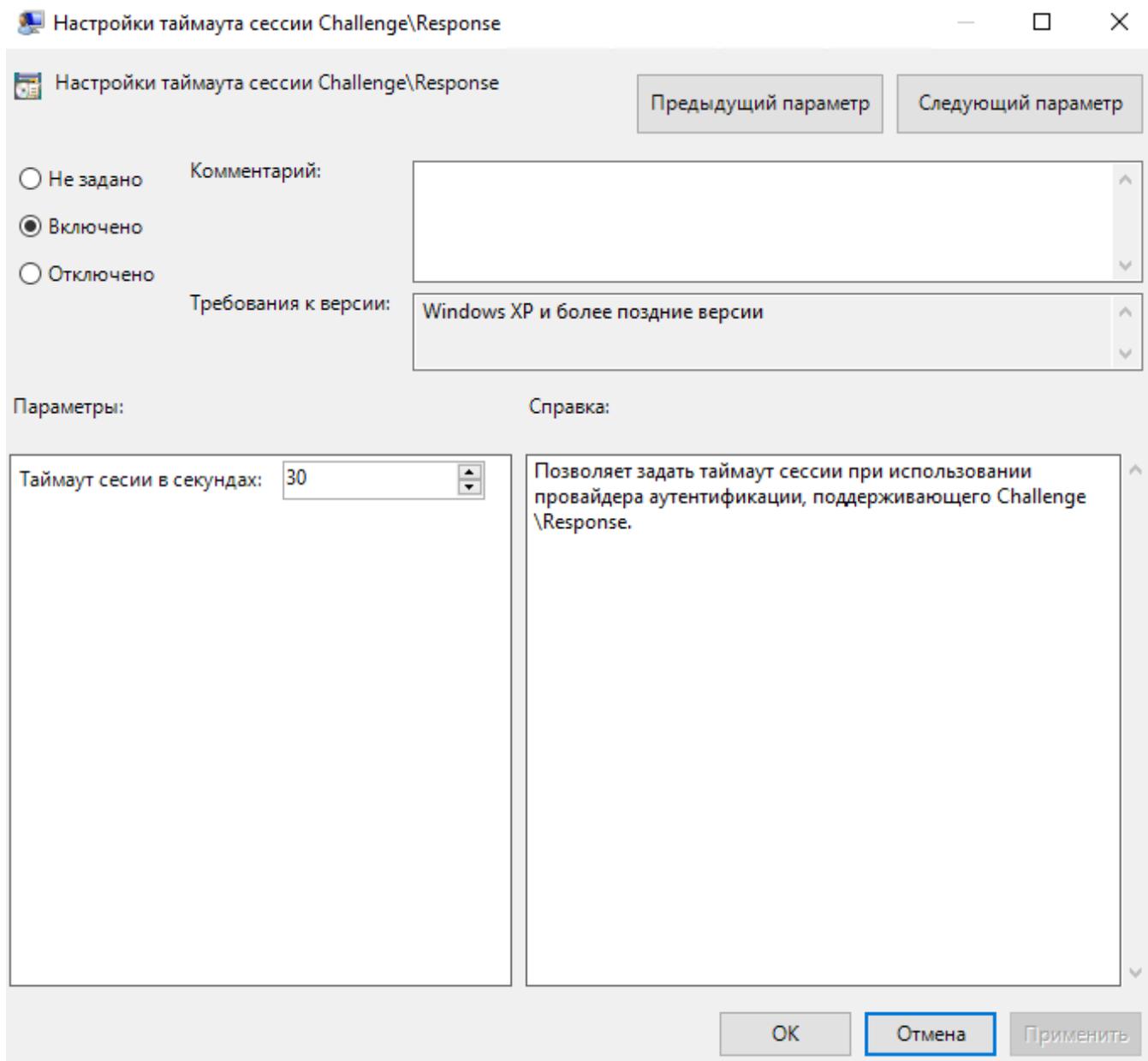
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"ProviderId"="{B772829C-4076-482B-B9BD-53B55EA1A302}"
```

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

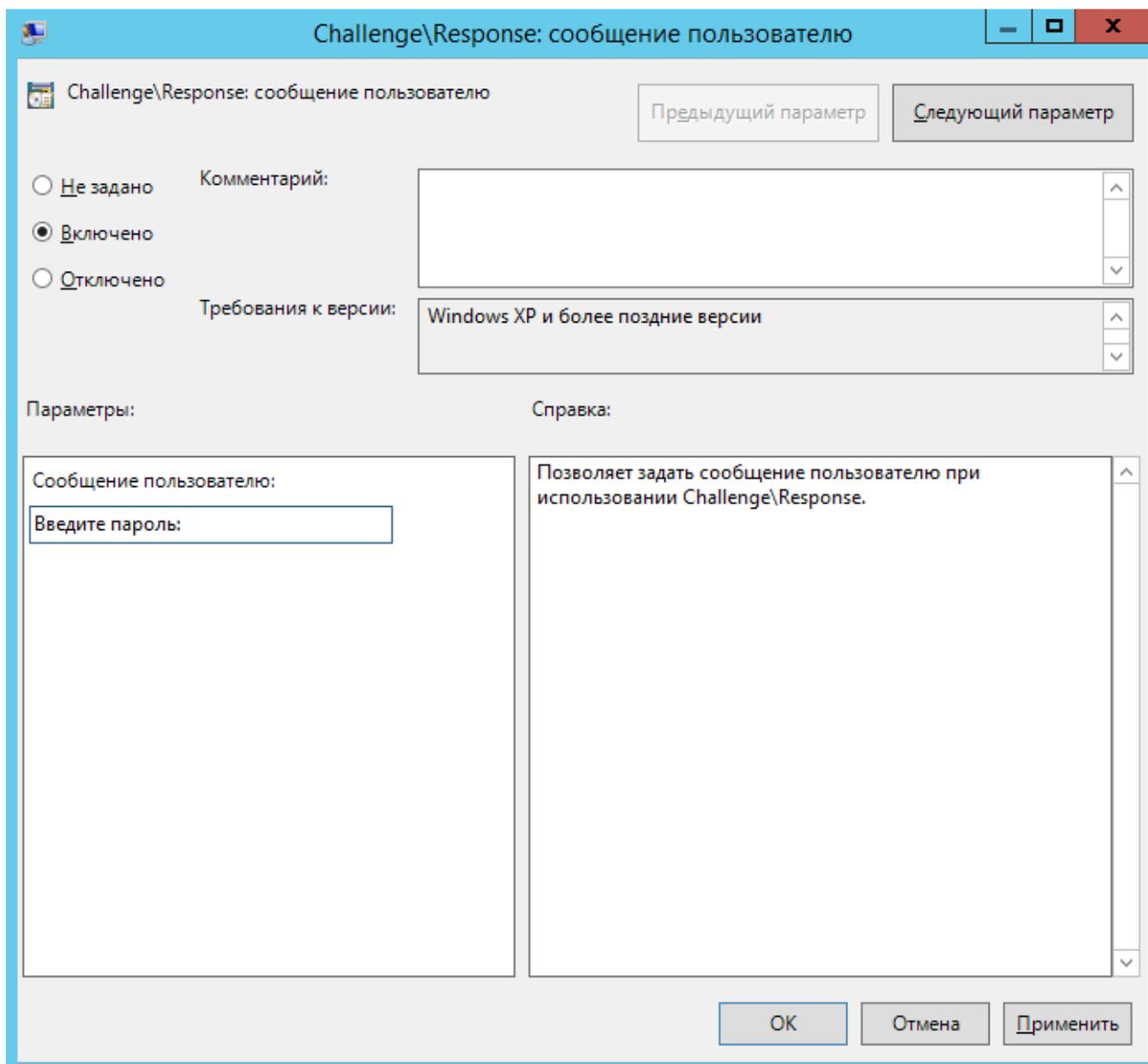
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"SessionLifetimeSec"=dword:0000001e
```

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: "
```

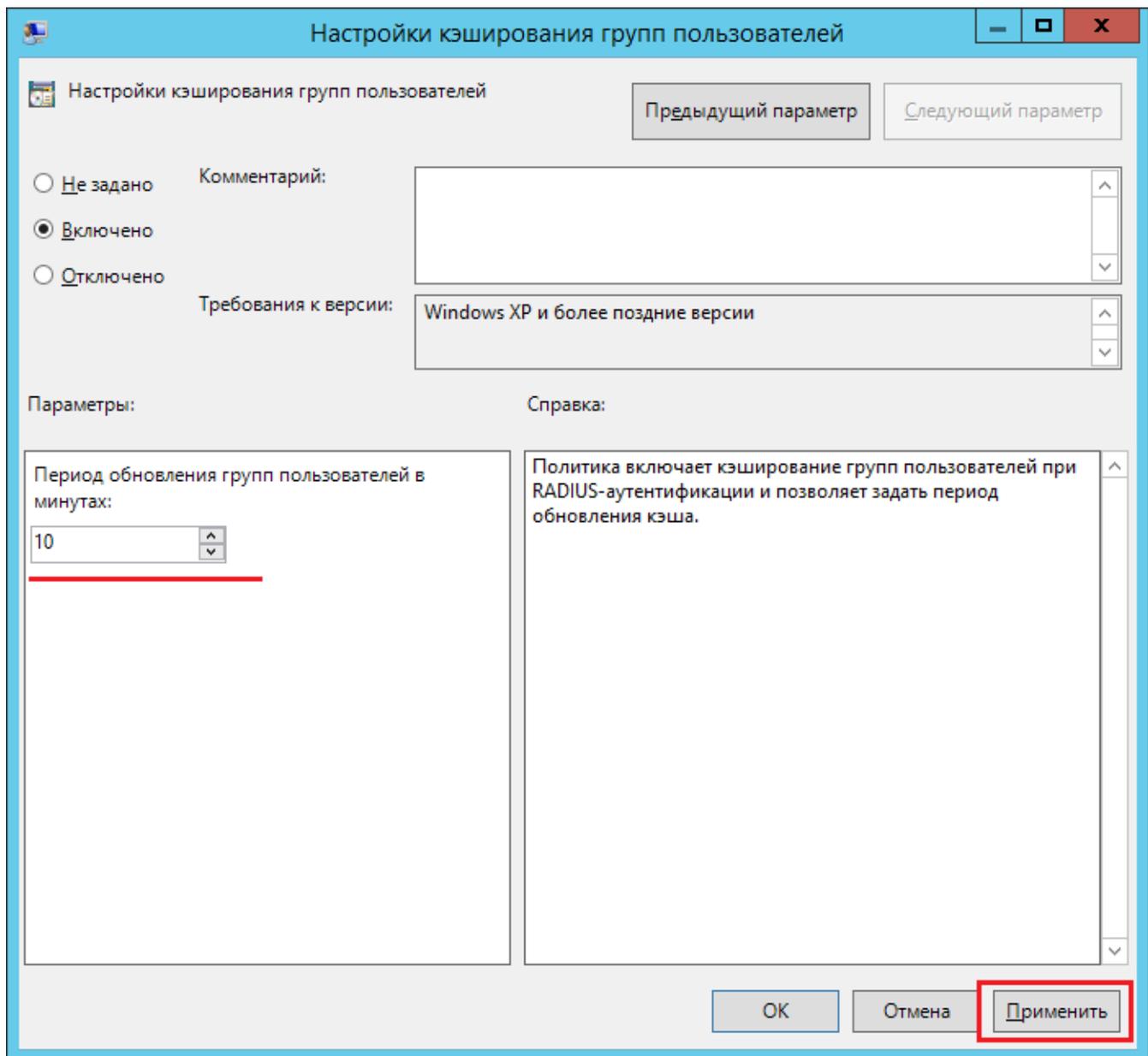
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\SMSOTP]
"SMSOTPChallengeResponseReplyMessage"="SMS OTP: "
```

Кэширование групп пользователей

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

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

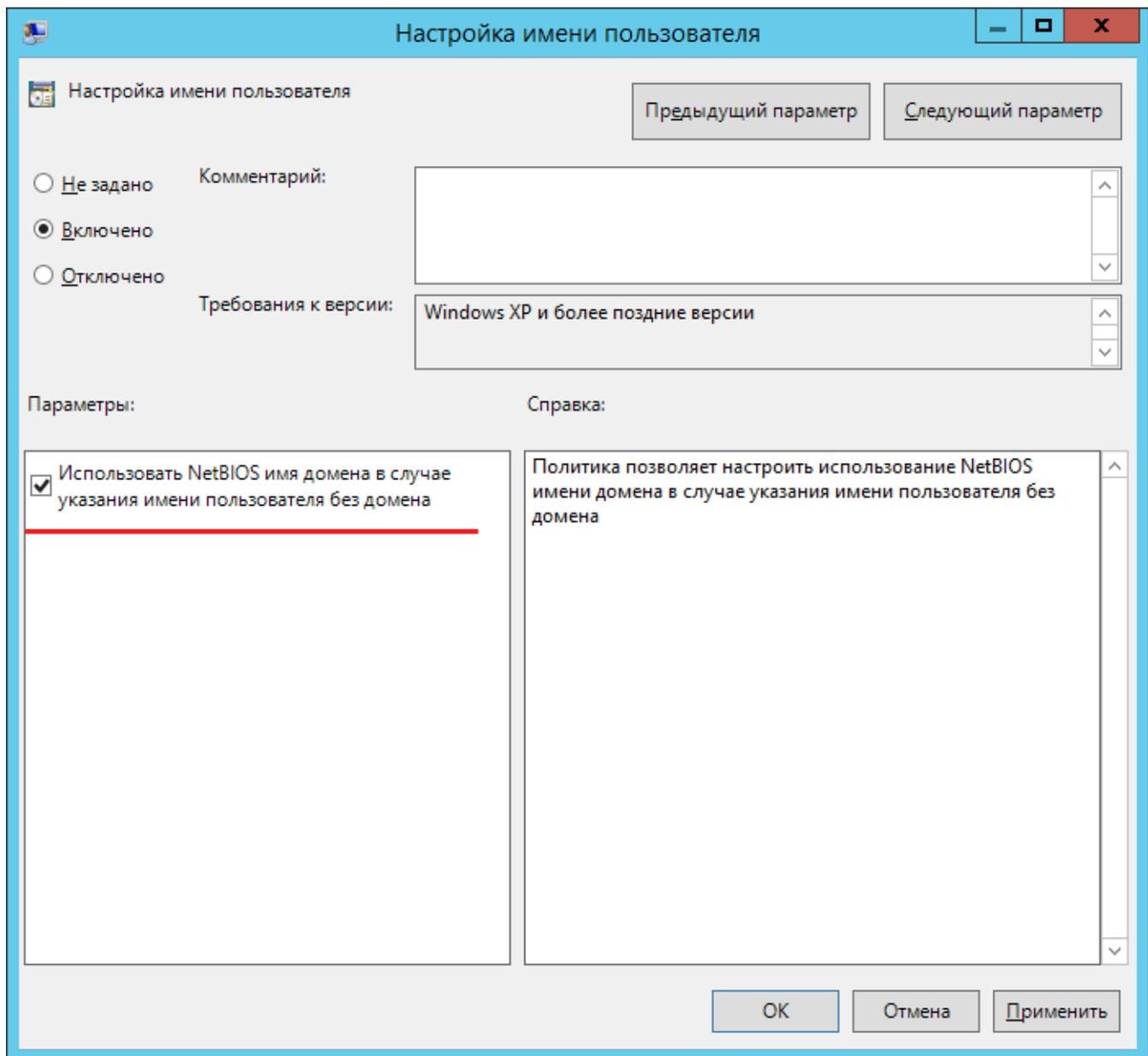
"UserGroupsCacheUpdateMin"=dword:00000021

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

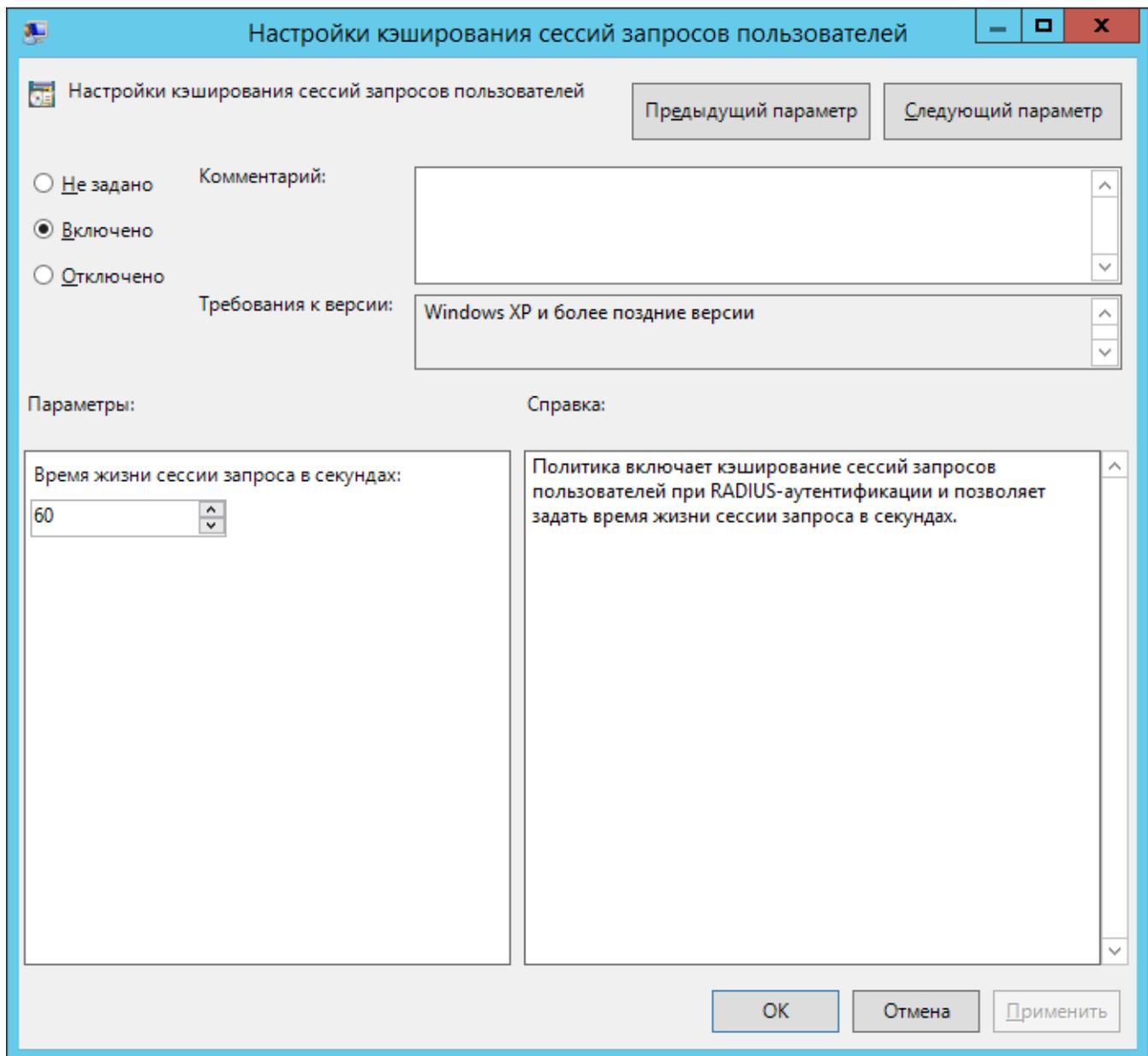
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"UseNetBiosDomainName"=dword:00000001
```

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