

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.

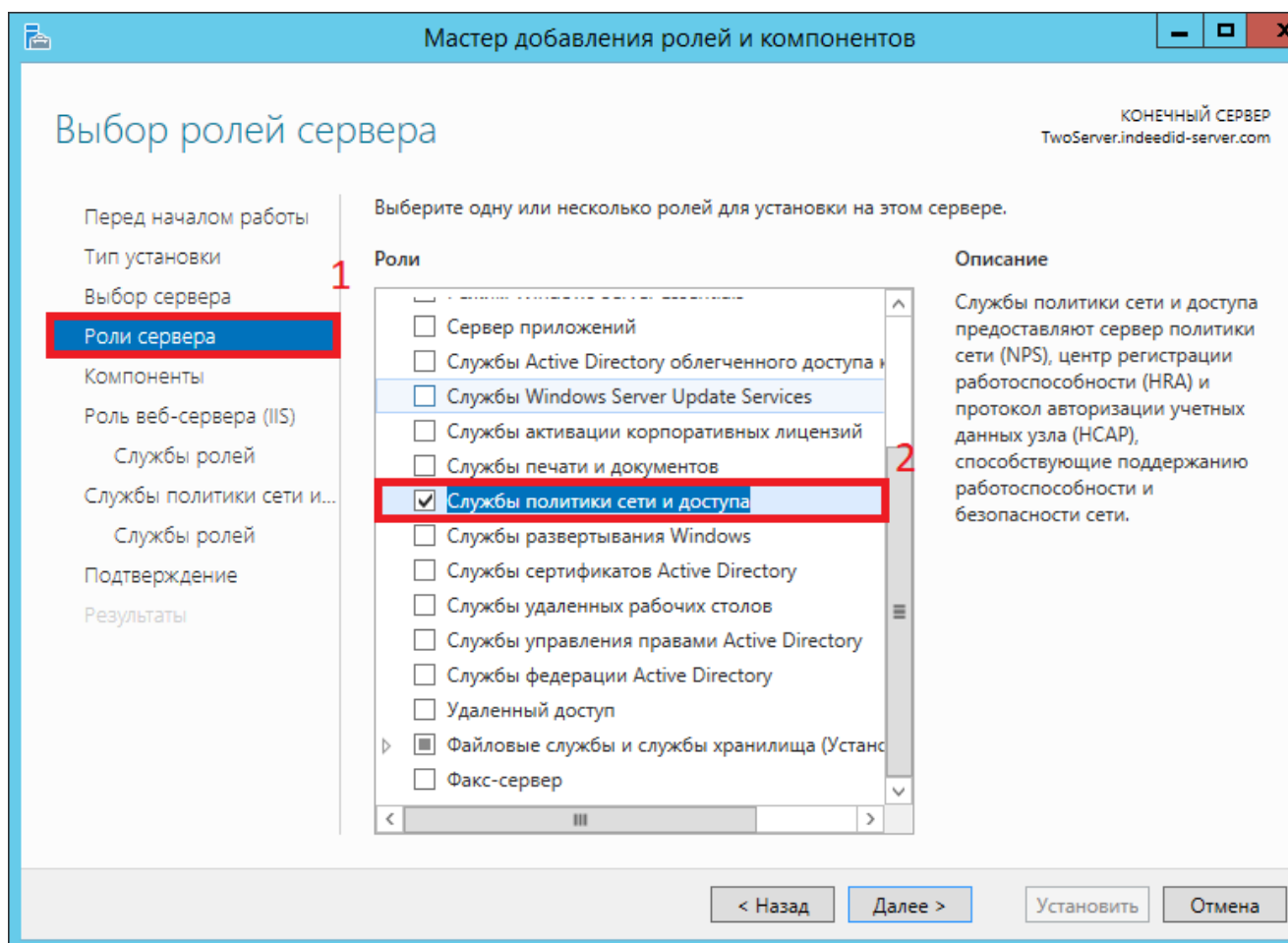
Установка Network Policy Server

Информация

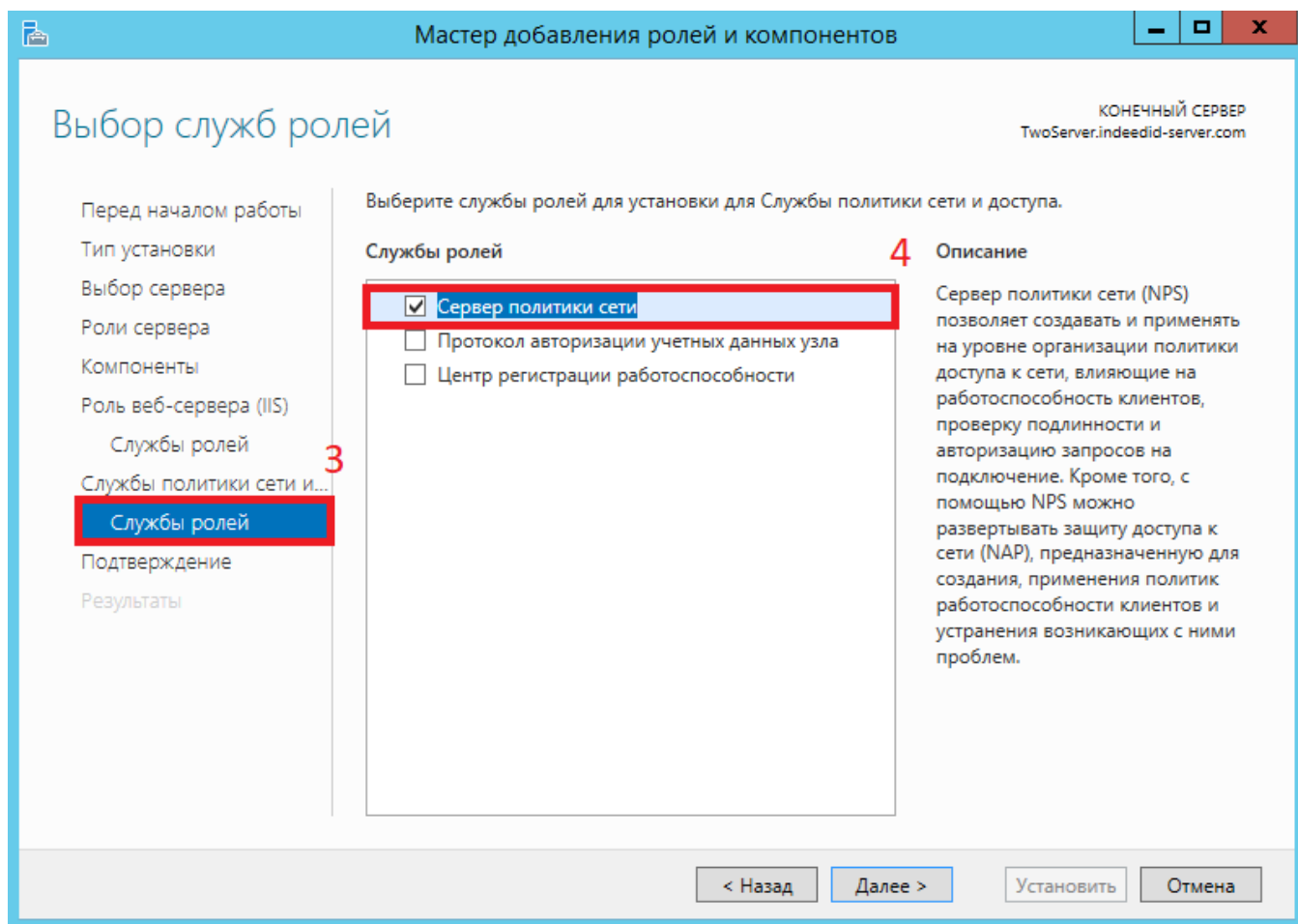
После установки кроме самой роли будет установлен Web-Server (IIS) и внутренняя база данных Windows.

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.

Новый RADIUS-клиент

Параметры Дополнительно

☒ Включить этот RADIUS-клиент

☐ Выберите существующий шаблон:

Имя и адрес

Имя сервера:
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.

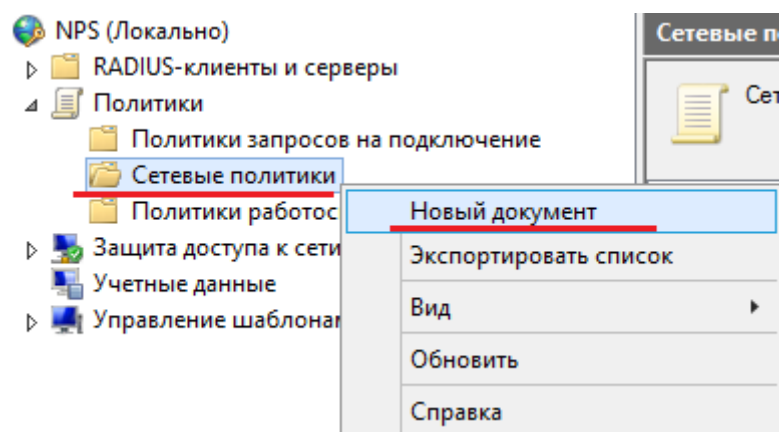
☒ Вручную ☐ Создать

Общий секрет:
.....

Подтверждение общего секрета:
.....

ОК Отмена

4. Добавьте сетевую политику для подключения Radius-клиентов.



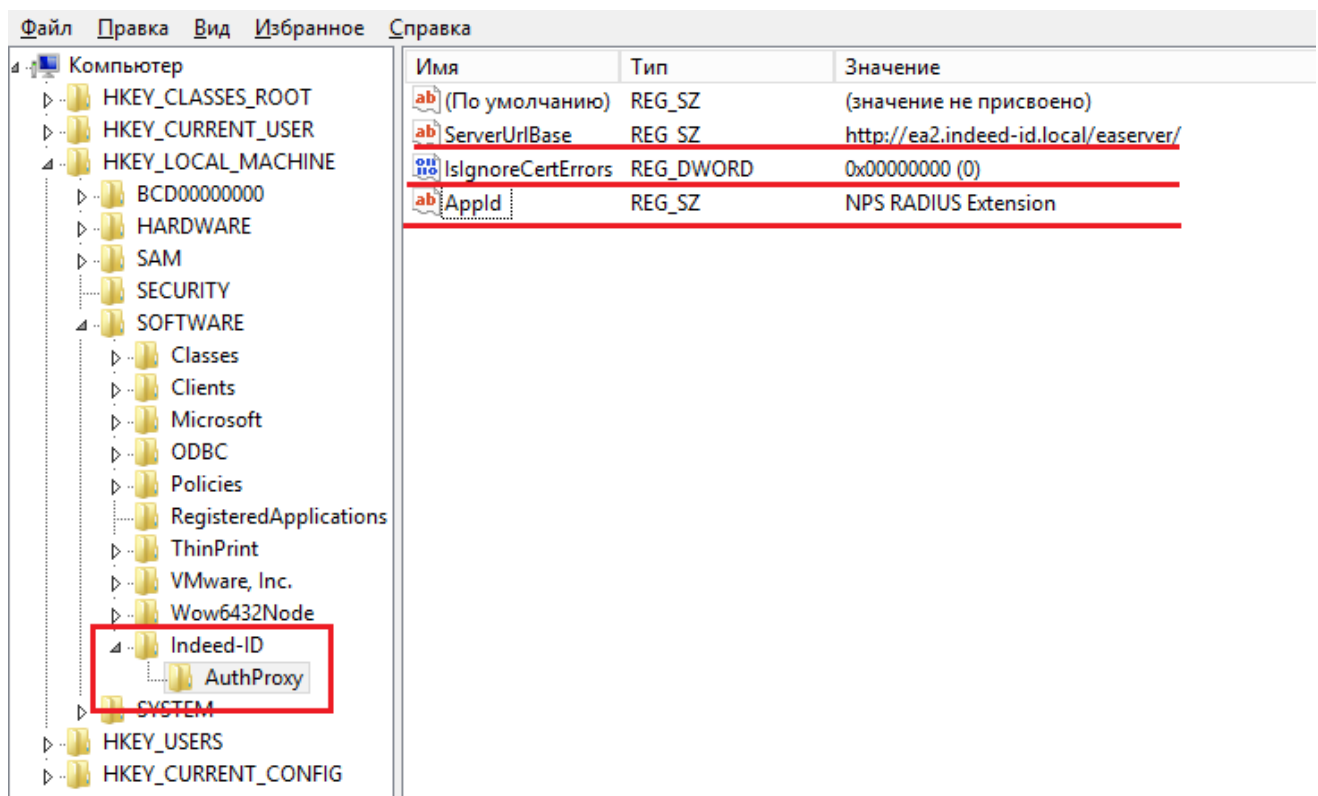
Установка Indeed AM NPS RADIUS Extension

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 **ApplId** со значением **NPS RADIUS Extension**.

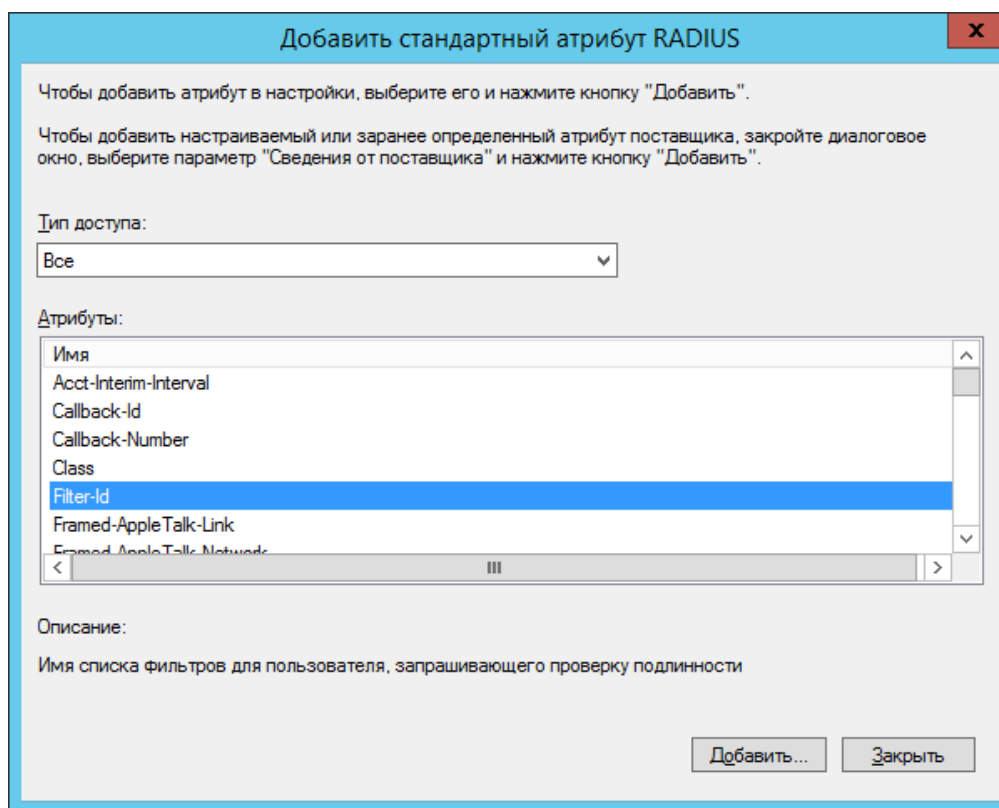


Настройка проброса атрибутов Radius

Информация

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

1. Откройте "**Политику запросов на подключение**".
2. 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>

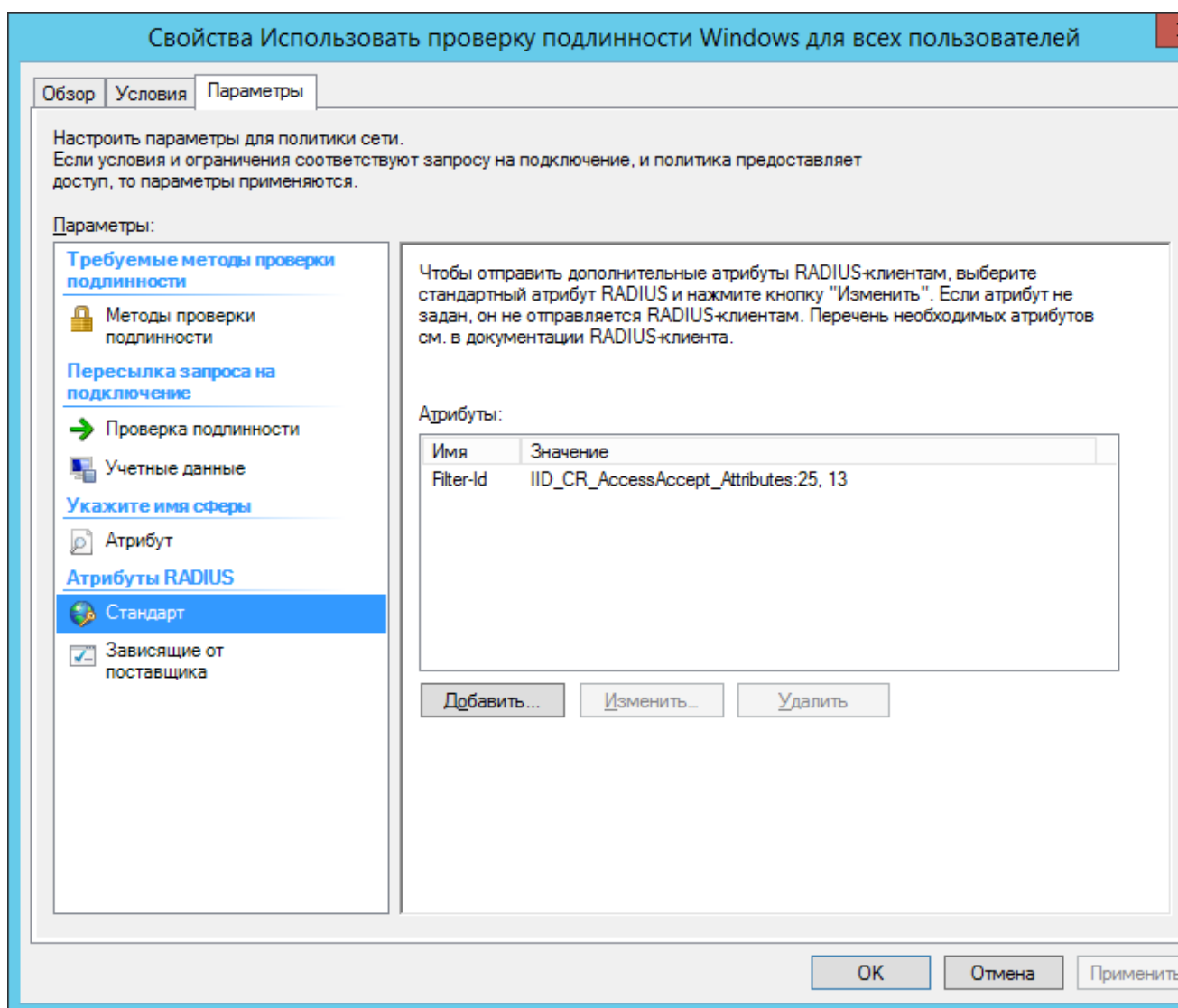
Информация

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 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.

Настройки Challenge\Response

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Таймаут сессии в секундах: 30

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

ОК Отмена Применить

Challenge\Response: сообщение пользователю

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

Challenge\Response: сообщение пользователю

Challenge\Response: сообщение пользователю

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Сообщение пользователю:

Введите пароль:

Позволяет задать сообщение пользователю при использовании Challenge\Response.

OK Отмена Применить

Настройка способов входа для групп пользователей

- а. Открыть для редактирования "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

- б. Включить (1) данный параметр и открыть редактирование содержимого (2).

Настройка способов входа для групп пользователей

Настройка способов входа для групп пользователей

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено 1

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Соответствие групп пользователей и провайдеров аутентификации:

Показать... 2

Данная политика позволяет задать Id провайдера, который будет использоваться для аутентификации определенных групп пользователей.

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

Например:

- с. 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**

Вывод содержания

Соответствие групп пользователей и провайдеров аутентификации:

	Имя значения	Значение
	CN=Radius-clients,CN=Users,DC=indeed-id,DC=local	{B772829C-4076-482B-B9BD-53B55EA1A302}
>>		

OK Отмена

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 имени пользователя

Настройка имени пользователя

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

☒ Использовать NetBIOS имя домена в случае указания имени пользователя без домена

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

OK Отмена Применить

Настройка кэширования сессий запросов пользователей

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

Настройки кэширования сессий запросов пользователей

Настройки кэширования сессий запросов пользователей

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Время жизни сессии запроса в секундах:

60

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

OK Отмена Применить

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

