

Indeed 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 NPS Radius Extension расположены: **indeed AM 7\Indeed RADIUS Extension\<Номер версии>**

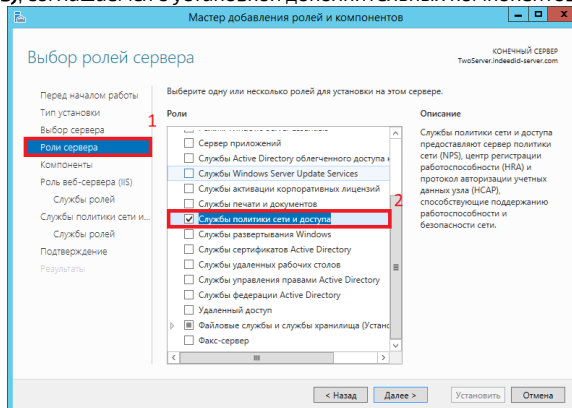
- **IndeedID.EA.RADIUS.Extension-v1.0.13.x64.ru-ru.msi** - Пакет для установки Indeed NPS Radius Extension
- **/Misc/GroupPolicyTemplates (ADMX)** - Шаблоны групповых политик для дополнительной настройки сервера и провайдеров.

Установка Network Policy Server.

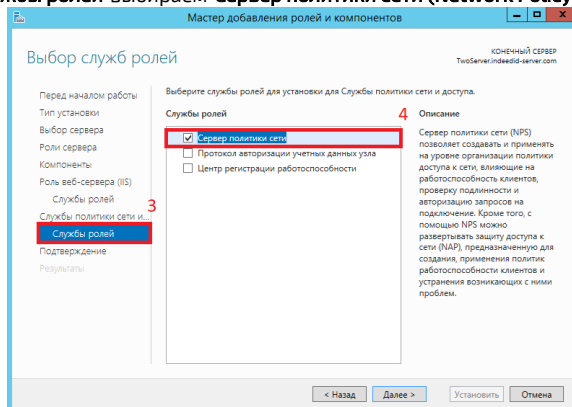
Информация

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.

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

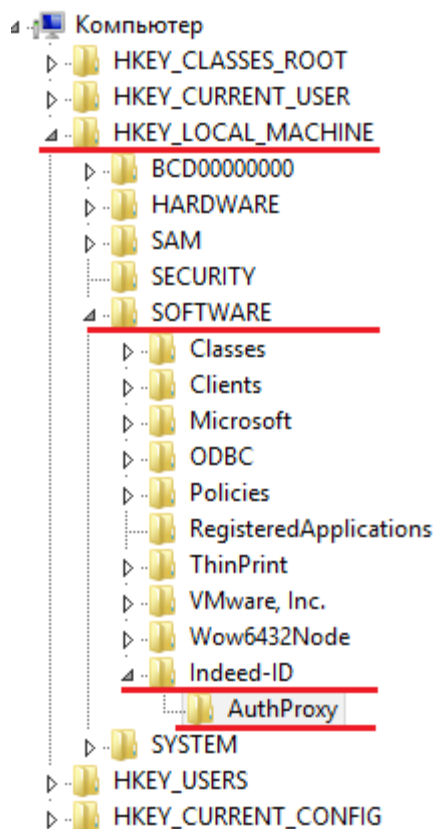


Информация

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

Установка Indeed NPS RADIUS Extension.

- Выполнить установку Indeed NPS RADIUS через запуск инсталлятора **IndeedID.EA.RADIUS.Extension-v1.0.13.x64.ru-ru.msi**.
- Создать в реестре **HKEY_LOCAL_MACHINE\SOFTWARE** раздел **Indeed-ID**, с вложенным разделом **AuthProxy**.



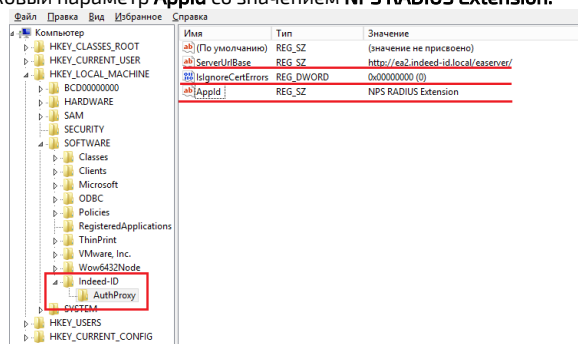
3. Создать в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID** ключ **AuthProxy**. В созданном ключе создайте:
- Строковый параметр **ServerUrlBase**. В значении для параметра укажите адрес вашего сервера **Indeed**.
 - DWORD** параметр **IsIgnoreCertErrors**, указать значение **0** или **1**.



Информация

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

- с. Строковый параметр **AppId** со значением **NPS RADIUS Extension**.



Настройка политики.



Информация

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



Информация

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

Challenge\Response: сообщение пользователю

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

Имя атрибута с email пользователя

Политика позволяет изменить атрибут из которого будет получаться email пользователя. По умолчанию получается из **mail**.

Имя атрибута с номером телефона

Политика позволяет изменить атрибут из которого будет получаться телефон пользователя. По умолчанию получается из **mobile**.

Настройка способов входа для групп пользователей

- а. Открыть для редактирования **"Настройка способов входа для групп пользователей"**.

Состояние	Состояние	Комментарий
	EmailOTP	
	eTokenPASS	
	GoogleOTP	
	SMSTOTP	
	Настройка способов входа для групп пользователей	Включено
	Настройка Challenge\Response	Не задана
	Настройка записи событий	Не задана
	Настройка шифрования групп пользователей	Не задана

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

Настройка способов входа для групп пользователей

Настройка способов входа для групп пользователей

☐ Не задано
☒ **Включено**
☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Соответствие групп пользователей и провайдеров аутентификации:

Показать...

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

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

Например:

- 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**

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

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

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

Вывод содержания

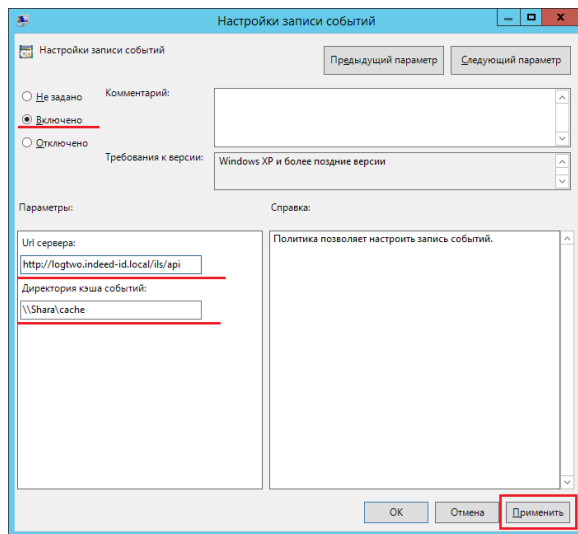
Соответствие групп пользователей и провайдеров аутентификации:

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

OK Отмена

Настройка записи событий

В политике указывается **Url** адрес **Log-сервера** и путь кеш-директории для записи события, в случае недоступности основного Log-сервера.



Кеширование групп пользователей.

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

