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).

- При рас

- Уст
 Ser
- Had
- Уст
- RAI
 Нас атр
- Had
 - (

 - (
 - (
 - (

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)".

L	Мастер добавления ролей и компонен	тов	_ D X
Выбор служб ро	лей		КОНЕЧНЫЙ СЕРВЕР TwoServer.indeedid-server.com
Перед началом работы Тип установки	выоерите служоы ролеи для установки для служоы по Службы ролей	литики 4	о сети и доступа. Описание
Выбор сервера Роли сервера Компоненты Роль веб-сервера (IIS) Службы ролей Службы политики сети и Службы ролей Подтверждение Результаты	Сервер политики сети Протокол авторизации учетных данных узла Центр регистрации работоспособности		Сервер политики сети (NPS) позволяет создавать и применять на уровне организации политики доступа к сети, влияющие на работоспособность клиентов, проверку подлинности и авторизацию запросов на подключение. Кроме того, с помощью NPS можно развертывать защиту доступа к сети (NAP), предназначенную для создания, применения политик работоспособности клиентов и устранения возникающих с ними проблем.
	< Назад	Далее :	> Установить Отмена

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 **Сhap** необходимо, в параметрах учетной записи пользователя, включить "**Хранить пароль, используя обратимое шифрование**" и обновить пароль пользователю.

3. Настроить нового клиента.

- а. Добавить имя для нашего сервера VPN (1).
- b. Указать IP адрес нашего сервера VPN (2).
- с. 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:
1
Имя и адрес
VPNServer
2
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 Осоздать Общика сократ:
Подтверждение общего секрета:
••••••
ОК Отмена

4. Добавьте сетевую политику для подключения Radius-клиентов.

 NPS (Локально) ПАDIUS-клиенты и серв Политики Политики запросов 	веры Сетевые по Сетевы
Сетевые политики Политики работос	Новый документ
В Защита доступа к сети	Экспортировать список
Учетные данные Управление шаблоная	Вид
	Обновить
	Справка

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.

с. Параметр **Appld** со значением **NPS RADIUS Extension**.

<u>Ф</u> айл <u>П</u> равка <u>В</u> ид <u>И</u> збранное <u>С</u>	правка		
🛯 📲 Компьютер	Имя	Тип	Значение
HKEY_CLASSES_ROOT	赴 (По умолчанию)	REG_SZ	(значение не присвоено)
▶ 🔐 HKEY_CURRENT_USER	ab ServerUrlBase	REG SZ	http://ea2.indeed-id.local/easerver/
A HKEY_LOCAL_MACHINE	IsignoreCertErrors	REG_DWORD	0x00000000 (0)
▶	ab Appld	REG_SZ	NPS RADIUS Extension
▶ • HARDWARE			
D - SAM			
SECURITY			
Microsoft			
DDBC			
Policies			
⊳ 📲 ThinPrint			
VMware, Inc.			
Wow6432Node			
⊿ 🔒 Indeed-ID			
AuthProxy			
D SYSTEM			
D. B HKEY_CUKKENT_CONFIG			

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

rna: v sim-Interval i-Id i-Number Apple Talk-Link	ип доступа: Все ✓ прибуты: Имя Acct-Interim-Interval Callback-Id Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link Framed-AppleTalk-Link
	Все ✓ птрибуты: Имя /// Acct-Interim-Interval ////////////////////////////////////
:	атрибуты: Имя Acct-Interim-Interval Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link Framed-AppleTalk-Link
erim-Interval :-Id :-Number AppleTalk-Link	Acct-Interim-Interval Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link Framed-AppleTalk-Link
-Id -Number AppleTalk-Link	Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link
-Number -Number Apole Talk-Link	Callback-Number Class Filter-Id Framed-AppleTalk-Link
Apple Talk-Link	Class Filter-Id Framed-AppleTalk-Link Framed-AppleTalk-Link
Apple Talk-Link	Filter-Id Framed-AppleTalk-Link Framed-AppleTalk-Link
Apple Talk-Link	Framed-AppleTalk-Link
	Espend Apple Talk Network
Apple Talk Metwork	
111 7	
Apple Talle Naturade	

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".

Настроить параметры для политики се Если условия и ограничения соответст доступ, то параметры применяются. Параметры: Требуемые методы проверки подлинности	ети. вуют запросу на подключение, и политика предоставляет Чтобы отправить дополнительные атрибуты RADIUS-клиентам, выберите стандартный атрибут RADIUS и нажмите кнопку "Изменить", Если атрибут не
Методы проверки подлинности Пересылка запроса на подключение	задан, он не отправляется RADIUS-клиентам. Перечень необходимых атрибутов см. в документации RADIUS-клиента. А <u>т</u> рибуты:
 Учетные данные Укажите имя сферы Атрибут Атрибуты RADIUS Стандарт 	Имя Значение Filter-Id IID_CR_AccessAccept_Attributes:25, 13
Зависящие от поставщика	<u>Добавить</u> <u>И</u> зменить_ <u>У</u> далить

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.

Позволяет задать таймаут сессии при использовании провайдера аутентификации,

поддерживающего Challenge\Response.

9	ł	łастройки Challenge\Response 📃 🗕 💌 🗙
📷 Настройки С	hallenge\Response	Пр <u>е</u> дыдущий параметр <u>С</u> ледующий параметр
○ <u>Н</u> е задано	Комментарий:	
<u>В</u> ключено		
○ <u>О</u> тключено	Требования к версии:	
	преосования к версии.	Windows XP и более поздние версии
Параметры:		Справка:
Таймаут сесии в	секундах: 30	Позволяет задать таймаут сессии при использовании провайдера аутентификации, поддерживающего Challenge \Response.
		ОК Отмена <u>П</u> рименить

Challenge\Response: сообщение пользователю

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

۶	Challenge	e\Response	: сообще	ние пользоват	гелю	Ŀ	_ D X
Challenge\Re	sponse: сообщение польз	ователю		Пр <u>е</u> дыдущий па	раметр	<u>С</u> ледующі	ий параметр
 <u>Н</u>е задано <u>В</u>ключено 	Комментарий:						^
○ <u>О</u> тключено	Требования к версии:	Windows XP	и более по	здние версии			×
Параметры:		(Справка:				
Сообщение поль Введите пароль:	зователю:		Позволяет : использова	задать сообщение нии Challenge\Re	e пользова sponse.	телю при	
				ОК		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

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

Настройка	способов входа для	я групп пользователей
📷 Настройка способов входа для груп	п пользователей	Предыдущий параметр Следу
 Не задано Включено Отключено Требования к версии: 	Windows XP и более п	юздние версии
Параметры:	Справка:	
Соответствие групп пользователей и провайдеров аутентификации: 2 Показать	Данная по будет испо группы по Введите в поле "Valu Например	олитика позволяет задать ld провайде ользоваться для аутентификации опр ользователей. поле "Value Name" distinguished nam ие" id провайдера аутентфиикации. о:

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

".

d. Вставьте в "Значение" ключ используемого провайдера.



	5550	д содержании		
ооте	етствие групп пользователей и провайдеров аутентификаци	и:		
	Имя значения	Значение		
	CN=Radius-clients,CN=Users,DC=indeed-id,DC=local	{B772829C-4076-482B-B9BD-53B55EA1A302	ł	
*				
				-
			<u>0</u> K	1

Кэширование групп пользователей

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

.	Настройк	ки кэшир	ования гру	упп пол	іьзователе	й	L	_ □	x
📷 Настройки кэш	ирования групп пользо	вателей		Пр <u>е</u> ды,	дущий парам	етр	<u>С</u> ледуюц	ций параме	етр
○ <u>Н</u> е задано	Комментарий:								<u> </u>
<u> Включено</u>									
О <u>О</u> тключено	Гребования к версии:								
	греоования к версии.	Windows	ХР и более по	оздние ве	рсии				÷
Параметры:			Справка:						
Период обновлени минутах: 10	ия групп пользователей	Б	Политика в RADIUS-аут обновлени	включает гентифик ія кэша.	г кэшировани ации и позво	е групп п ляет зада	пользова	ателей при	∧

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 Пр <u>е</u> дыдущий параметр <u>С</u> ледующий параметр					
○ <u>Н</u> е задано	Комментарий:				
○ <u>О</u> тключено	Треборания к версии				
	треоования к версии:	Windows XP и более поздние версии			
Параметры:		Справка:	1		
Использовать указания имен	NetBIOS имя домена в сл	учае на Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена			
ОК Отмена <u>П</u> рименить					

Настройка кэширования сессий запросов пользователей

Политика включает кэширование сессий запросов пользователей при RADIUS-

аутентификации и позволяет задать время жизни сессии запроса в секундах.

.	Настройки кэц	ирования сессий запросов пользователей 🛛 💻 🗙		
Настройки кэширования сессий запросов пользователей Пр <u>е</u> дыдущий параметр <u>С</u> ледующий параметр				
○ <u>Н</u> е задано	Комментарий:			
<u>В</u> ключено				
○ <u>О</u> тключено	T			
	требования к версии:	Windows XP и более поздние версии		
Параметры:		Справка:		
Время жизни сес 60	ссии запроса в секундах:	Политика включает кэширование сессий запросов пользователей при RADIUS-аутентификации и позволяет задать время жизни сессии запроса в секундах.		
		ОК 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 ОТР в Citrix Netscaler