Этот документ входит в комплект поставки продукта.
Информация, содержащаяся в этом документе, может быть изменена разработчиком без уведомления пользователя.

Контактная информация:

+7 (495) 640-06-09
Москва
+7 (812) 640-06-09
Санкт-Петербург

inbox@indeed-id.com
почта

8 800 333-09-06
support@indeed-id.com
техническая поддержка

Indeed NPS RADIUS Extension

Руководство по установке и эксплуатации

версия 1.1.0

Содержание

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное руководство поможет вам ознакомиться с принципом работы компонента **Indeed NPS RADIUS Extension**, параметрами его установки и настройки.

Условные обозначения

В Руководстве используются следующие условные обозначения:

Важная информация
Указания, требующие особого внимания при развертывании, настройке, работе или обновлении продукта.

Дополнительная информация
Указания, способные упростить развертывание, настройку, работу или обновление продукта.

О компоненте Indeed NPS RADIUS Extension

Indeed NPS RADIUS Extension представляет собой модуль расширения Microsoft Network Policy Server (NPS) и позволяет системе Indeed EA участвовать в процессе аутентификации пользователей при запросах на подключение к внутренним ресурсам организации.
Возможны два сценария реализации доступа пользователей:

- Однофакторная аутентификация
- Двухфакторная аутентификация

Однофакторная аутентификация реализуется путем замены входа пользователя по доменному паролю входом по аутентификатору Indeed (постоянному или одноразовому паролю). Такая схема аутентификации поддерживается провайдерами:

- Indeed-Id Passcode Provider
- Indeed-Id Google Authenticator Provider
- Indeed-Id eToken PASS Provider

Двухфакторная аутентификация реализуется при помощи механизма Запрос\Ответ (challenge\response) и подразумевает, что при входе в RADIUS-приложение пользователю необходимо будет ввести учетные свои данные (логин и доменный пароль) и дополнительный одноразовый пароль. Одноразовый пароль может быть доставлен пользователю по разным каналам: SMS, Email, eToken PASS или сгенерирован приложением в мобильном устройстве. Такая схема аутентификации поддерживается провайдерами:

- Indeed-Id SMS OTP Provider

- Indeed-Id Email OTP Provider
- Indeed-Id Google Authenticator Provider (challenge\response)
- Indeed-Id eToken PASS Provider (challenge\response)

Установка и настройка Indeed NPS RADIUS Extension

Предварительные условия установки

Для корректной установки и работы Indeed NPS RADIUS Extension необходимы продукты компании Indeed, установленные в следующей конфигурации:

- Indeed-Id Enterprise Server
- Провайдеры аутентификации Indeed-Id (один или несколько):
  - Indeed-Id SMS OTP Provider (без PIN-кода)
  - Indeed-Id Email OTP Provider
  - Indeed-Id Google Authenticator Provider (без PIN-кода)
  - Indeed-Id Passcode Provider
  - Indeed-Id eToken PASS Provider (без PIN-кода)
- Консоль управления Indeed EMC
- Зарегистрированные пользовательские лицензии системы Indeed Enterprise Authentication

Поддерживаемые методы (протоколы) аутентификации:

- PAP
- CHAP
- MSCHAPv2

Порядок установки

Компоненты системы Indeed Enterprise Authentication для аутентификации на RADIUS-совместимых сервисах необходимо устанавливать в следующем порядке:

- Indeed NPS RADIUS Extension устанавливается на сервере с компонентом **Сервер сетевых политик** (Network Policy Server, NPS) роли **Политика сети и службы доступа** (Network Policy and Access Services, NPAS)
- На каждом сервере Indeed EA устанавливаются провайдеры Indeed (один или несколько), необходимые для аутентификации в RADIUS-сервисах.

Для установки Indeed NPS RADIUS Extension выполните следующие действия:

1. Запустите файл IndeedID.EA.RADIUS.Extension.x86.ru-ru.msi[1] из дистрибутива и выполните установку, следуя указаниям мастера.

2. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Установка, настройка, удаление и обновление провайдеров аутентификации осуществляется в соответствии с руководством по установке и эксплуатации соответствующего провайдера.

[1]Для установки на 64-битных ОС следует использовать инсталлятор IndeedID.EA.RADIUS.Extension.x64.ru-ru.msi.

Особенности аутентификации с использованием Indeed NPS RADIUS Extension

Indeed NPS RADIUS Extension может быть настроен для работы по следующим сценариям аутентификации пользователей:

- Способ входа в RADIUS-приложение един для всех пользователей
- Способ входа в RADIUS-приложение задается для каждой группы пользователей

При этом возможна комбинация настроек: для всех пользователей домена действует один способ аутентификации, но для указанных групп пользователей применяется свой, отличный от общего способ аутентификации.

Перед началом использования Indeed NPS RADIUS Extension необходимо соответствующим образом настроить RADIUS-клиент и RADIUS-сервер. Аутентификация с использованием Challenge\Response поддерживаться не всеми RADIUS-клиентами.

Настройка Indeed NPS RADIUS Extension

В этом разделе содержится описание настраиваемых параметров работы модуля и способах их изменения. Изменение параметров работы модуля осуществляется следующим образом:

- В политиках на сервере NPS задаются параметра доступа
- В групповых политиках Active Directory задаются параметры провайдеров аутентификации Indeed-Id.

Настройка параметров доступа в политиках на Сервере политики сети (NPS)

В политике на сервере NPS задаются параметры:

- Разрешать RADIUS-аутентификацию для пользователей без лицензии Indeed EA
- Разрешать пользователям Indeed EA использование доменного пароля для RADIUS-аутентификации
- Общая настройка способа входа
- Настройка способов схода 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 перейдите в свойства ранее созданной.
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 1 и нажмите **ОК**.
6. Для применения внесенных в политику изменений нажмите **Применить** (Apply).
7. Перезапустите службу NPS.

Таблица 1 – Значения атрибута Filter-Id для работы с Indeed NPS RADIUS Extension

Значение	Описание
IID_AllowUseDomainPassword	**Разрешать RADIUS-аутентификацию для пользователей без лицензии Indeed EA**. Если указано, то пользователи, не обладающие лицензией на использование Indeed EA смогут использовать RADIUS-аутентификацию.
IID_AllowWLUserUseDomainPassword	**Разрешать пользователям Indeed EA использование доменного пароля для RADIUS-аутентификации**. Если указано, то пользователи, обладающие лицензией на использование Indeed EA, смогут входить в RADIUS-приложения используя только доменный пароль.
IID_ModeId_{ProviderId}	**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 приведено в Таблице 2. **Пример значения атрибута с Indeed-Id Passcode Provider:** IID_ModeId_{F696F05D-5466-42b4-BF52-21BEE1CB9529}
IID_Group_ModeId_{DN}_{ProviderId}	**Настройка способов схода для групп пользователей**. Если задано, то пользователи указанной группы Active Directory будут использовать указанный провайдер Indeed для аутентификации в RADIUS-приложениях. Значение **DN** – различающееся имя группы (Distinguished Name). 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. **Пример значения с Indeed-Id Email OTP Provider:** IID_Group_ModeId_{CN=group,DC=demo,DC=com}_{093F612B-727E-44E7-9C95-095F07CBB94B}

Таблица 2 – Значения ProviderId провайдеров аутентификации Indeed.

Название провайдера Indeed	**ProviderId**
SMS OTP Provider (без PIN-кода)	{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
Email OTP Provider	{093F612B-727E-44E7-9C95-095F07CBB94B}
Google Authenticator Provider	{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Google Authenticator Provider (challenge\response)	{B772829C-4076-482B-B9BD-53B55EA1A302}
Passcode Provider	{F696F05D-5466-42B4-BF52-21BEE1CB9529}
eToken PASS Provider	{EA588135-CED1-4922-B640-924C94A91904}
eToken PASS Provider (challenge\response)	{631F1011-2DEE-47C5-95D8-75B9CAED7DC7}

Пример настроек атрибута Filter-Id приведен на Рисунке 1.

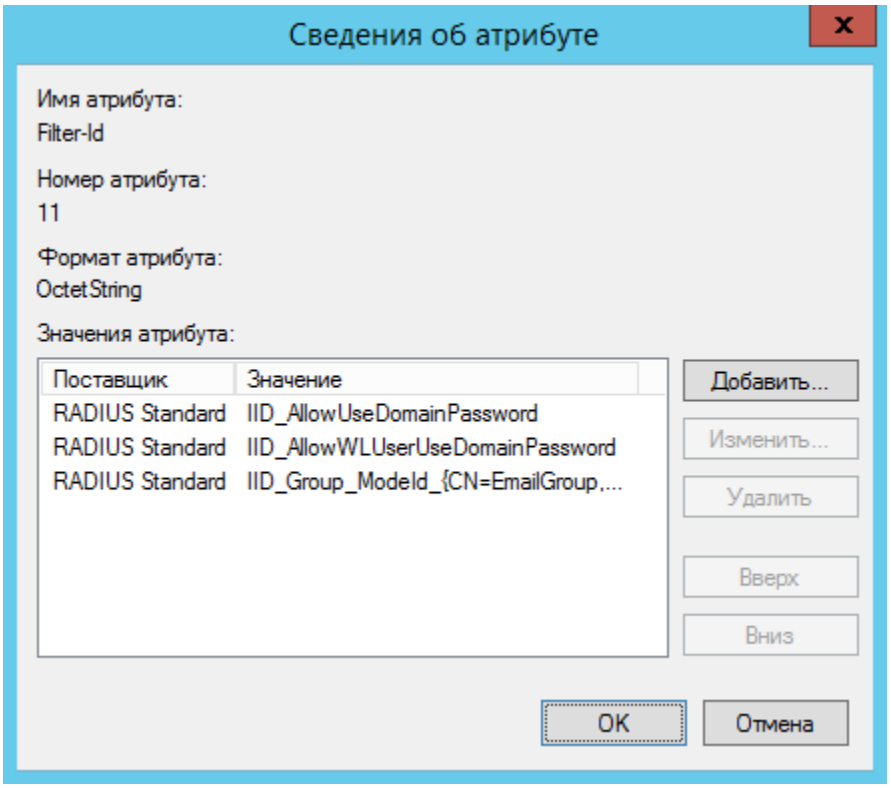

Рисунок 1 – Пример настроек атрибута Filter-Id.

Особенности работы Indeed NPS RADIUS Extension без Indeed-Id Windows Logon при однофакторной аутентификации пользователей

Для регистрации аутентификаторов Passcode, eToken PASS, Google Authenticator при использовании однофакторной аутентификации требуется доменный пароль пользователя: он используется для входа в утилиту *Indeed-Id Управление аутентификаторами*.

После регистрации первого аутентификатора доменный пароль пользователя записывается в хранилище данных Indeed и проверяется сервером Indeed EA при каждой аутентификации пользователя (при этом пользователь не вводит пароль, а использует аутентификатор Indeed). При изменении доменного пароля его новое значение должно быть также записано в хранилище системы Indeed. Такую операцию (синхронизацию пароля) выполняет компонент Indeed-Id Windows Logon. В случае, если Indeed-Id Windows Logon не используется в вашей организации, то при смене доменного пароля пользователя его новое значение не попадёт в базу данных Indeed. Это приведет к рассинхронизации пароля при попытке входа в RADIUS-приложение по ранее зарегистрированному аутентификатору Indeed. В этом случае в доступе будет отказано.

Рассинхронизации пароля можно избежать, если проверка учетных данных пользователей будет отключена на Сервере политик сети (NPS). В этом случае Сервер политик сети будет игнорировать введенный пользователем доменный пароль.

Отключение проверки учетных данных пользователей на Сервере политик сети (NPS) приведет к следующим последствиям:

- При отсутствии в политике NPS общей настройки способа входа пользователи без лицензии Indeed EA, а также пользователи, обладающие лицензией на использование Indeed EA, но не принадлежащие ни к одной из групп Active Directory, на которые распространяется действие способа входа через Indeed NPS RADIUS Extension **будут беспрепятственно и бесконтрольно получать доступ к RADIUS-приложениям**.
- При использовании OTP-провайдеров Indeed-Id:
  - EmailOTP
  - SMSOTP
  - GoogleOTP (challenge\response)
  - eToken PASS(challenge\response)

  двухфакторная аутентификация **фактически превращается в однофакторную** т.к. вместо доменного пароля может быть использована любая комбинация символов.
- Параметры, определенные в разделе **Политики Сети (Network Policies)** сервера NPS, будут игнорироваться как при использовании совместно с Indeed NPS RADIUS Extension, так и без него.

Для отключения проверки учетных данных пользователей 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 перейдите в свойства ранее созданной.
3. На вкладке **Параметры** (Settings) перейдите в раздел **Пересылка запроса на подключение** (Forwarding Connection Request) – **Проверка подлинности** (Authentication).
4. Включите опцию **Принимать пользователей без проверки учетных данных** (Accept users without validating credentials) и нажмите **Применить** (Apply).
5. Настройте общий способ входа для всех пользователей RADIUS-приложений. При необходимости настройте способы входа для различных групп пользователей (см. **Настройка параметров доступа в политиках на Сервере политики сети (NPS)**).

Настройка параметров провайдеров аутентификации Indeed-Id

Перед настройкой групповой политики необходимо добавить в список административных шаблонов Active Directory шаблоны политик Indeed. Файлы шаблонов политик входят в состав дистрибутива Indeed NPS RADIUS Extension.

Настройки Challenge\Response
Политика применяется к рабочим станциям с установленным компонентом **Сервер сетевых политик** (Network Policy Server, NPS) роли **Политика сети и службы доступа** (Network Policy and Access Services, NPAS) и позволяет задать временной период, в течение которого будет действителен одноразовый пароль, при использовании двухфакторной аутентификации с поддержкой механизма Challenge\Response.

Не задан (Not Configured) или *Отключен (Disabled)*
Время действия пароля 30 секунд. Значение умолчанию - Не задан.

Включен (Enabled)
При включении политики необходимо указать период действия одноразового пароля в секундах.

Настройки политик провайдеров аутентификации для работы с Indeed NPS RADIUS Extension
Политики применяется к рабочим станциям с установленным компонентом **Сервер сетевых политик** (Network Policy Server, NPS) роли **Политика сети и службы доступа** (Network Policy and Access Services, NPAS).

Основные настройки провайдеров аутентификации Indeed-Id задаются через механизм групповых политик и **применяются к серверам Indeed EA**. См. руководства по установке и настройке провайдеров аутентификации Indeed-Id (входят в состав дистрибутива системы Indeed Enterprise Authentication).

Email OTP
Политика **Challenge\Response: сообщение пользователю** позволяет задать сообщение пользователю при использовании Challenge\Response.

Не задан (Not Configured) или *Отключен (Disabled)*
Отображается значение "OTP:". Значение умолчанию - Не задан.

Включен (Enabled)
Отображается значение, указанное в строке **Сообщение пользователю**. Сообщение по умолчанию – "OTP:".
На Рисунке 2 приведен пример отображения значения политики в интерфейсе приложения Citrix NetScaler с поддержкой двухфакторной аутентификации. Вторым фактором служит одноразовый пароль, присланный пользователю на адрес электронной почты, после того, как он прошел первый этап аутентификации по доменному логину и паролю.

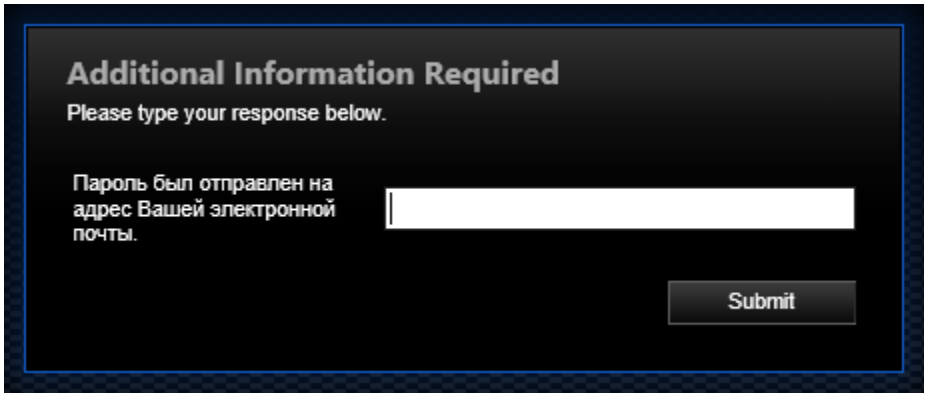

Рисунок 2 – Действие политики Email OTP Challenge\Response: сообщение пользователю.

Политика **Имя атрибута с email пользователя** позволяет задать имя атрибута Active Directory, в котором содержится адрес электронной почты пользователя. При использовании провайдера Email OTP адрес из указанного атрибута будет использоваться для отправки на него одноразовых паролей.

Не задан (Not Configured) или *Отключен (Disabled)*
Имя атрибута – mail. Значение умолчанию - Не задан.

Включен (Enabled)
Используется адрес, указанный в параметре **Имя атрибута**. Атрибут по умолчанию – mail.

eToken PASS
Политика **Challenge\Response: сообщение пользователю** позволяет задать сообщение пользователю при использовании Challenge\Response.

Не задан (Not Configured) или *Отключен (Disabled)*
Отображается значение "OTP:". Значение умолчанию - Не задан.

Включен (Enabled)
Отображается значение, указанное в строке **Сообщение пользователю**. Сообщение по умолчанию – "OTP:". Значение политики в RADIUS-приложении отображается по аналогии с Рисунком 2.

Google OTP
Политика **Challenge\Response: сообщение пользователю** позволяет задать сообщение пользователю при использовании Challenge\Response.

Не задан (Not Configured) или *Отключен (Disabled)*
Отображается значение "OTP:". Значение умолчанию - Не задан.

Включен (Enabled)
Отображается значение, указанное в строке **Сообщение пользователю**. Сообщение по умолчанию – "OTP:". Значение политики в RADIUS-приложении отображается по аналогии с Рисунком 2.

SMS OTP
Политика **Challenge\Response: сообщение пользователю** позволяет задать сообщение пользователю при использовании Challenge\Response.

Не задан (Not Configured) или *Отключен (Disabled)*
Отображается значение "OTP:". Значение умолчанию - Не задан.

Включен (Enabled)
Отображается значение, указанное в строке **Сообщение пользователю**. Сообщение по умолчанию – "OTP:". Значение политики в RADIUS-приложении отображается по аналогии с Рисунком 2.

Политика **Имя атрибута с номером телефона** позволяет задать имя атрибута Active Directory, содержащего номер телефона пользователя. Формат номера зависит от используемого SMS-шлюза. Некоторые шлюзы могут не поддерживать пробелы или отдельные виды разделителей (тире, скобки), а также символ "+". При использовании провайдера SMS OTP телефонный номер из указанного атрибута будет использоваться для отправки на него одноразовых паролей.

Не задан (Not Configured) или *Отключен (Disabled)*
Имя атрибута – mobile. Значение умолчанию - Не задан.

Включен (Enabled)
Используется номер телефона пользователя, указанный в параметре **Имя атрибута**. Атрибут по умолчанию – mobile.

Сбор программных логов

Сбор логов приложений

Наличие программных логов позволяет специалистам службы поддержки определить причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты GetLog, поставляемой в составе дистрибутива Indeed Enterprise Authentication. Для получения подробной информации обратитесь к документу *Indeed-Id GetLog. Руководство по эксплуатации.pdf*.

Часто задаваемые вопросы

Ознакомиться со списком часто задаваемых вопросов и ответов на них можно в **Базе знаний** по продукту Indeed Enterprise Authentication.