Indeed AM RDP Windows Logon

Модуль **Indeed AM RDP Windows Logon** позволяет реализовать возможность двухфакторной аутентификации с помощью технологии Indeed AM в процессе подключения по **RDP или Remote App**. В качестве второго фактора могут выступать мастер-пароль (**провайдер Passcode**), одноразовый пароль, сгенерированный мобильным приложением (**провайдер Software OTP**), одноразовый пароль, отправленный по SMS или email.

Информация

Файлы для Indeed AM RDP Windows Logon расположены: ***indeed AM\Indeed AM RDP Windows Logon\<Номер версии>***

- **Indeed.AM.RDPWindowsLogon-x64.ru-ru.msi** - Пакет для установки RDP Windows Logon для x64 битных машин.
- **Indeed.AM.RDPWindowsLogon-x86.ru-ru.msi** - Пакет для установки RDP Windows Logon для x32 битных машин.

Установка и настройка RDP Windows Logon.

Информация

Для работы расширения требуется включение NLA для пользователя.

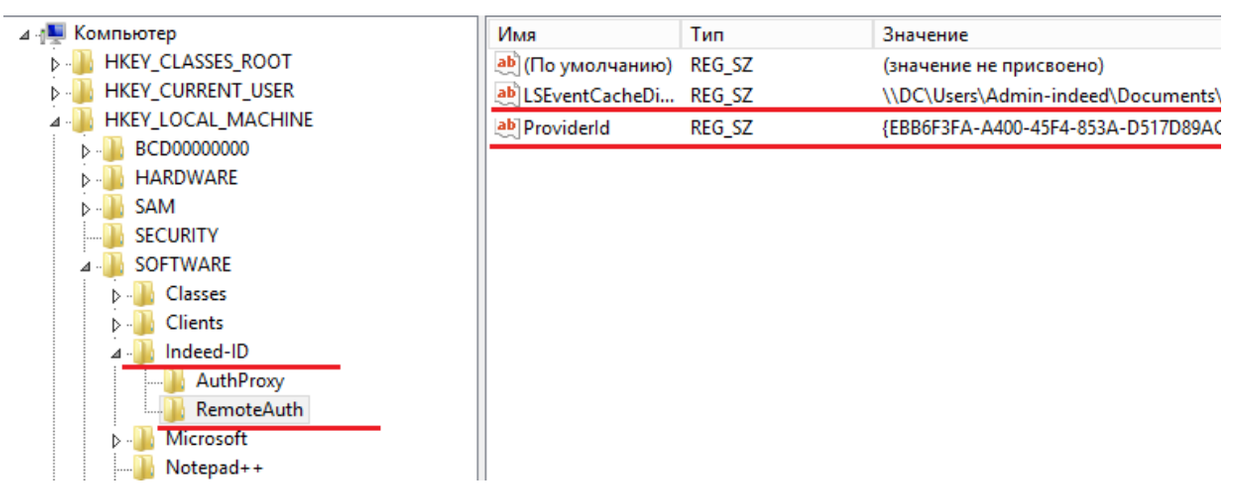
1. Выполнить установку RDP Windows Logon в зависимости от битности системы через запуск инсталлятора.
2. Открыть редактор реестра **Windows.**
3. Создать в разделе **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **RemoteAuth.**
4. В разделе **RemoteAuth** создать:

a. Строковый параметр **ProviderId** и задать значение, соответствующее используемому провайдеру.

> **Информация**
>
> **ProviderId** может иметь разные **ID** провайдеров:
>
> {EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**
>
> {093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**
>
> {F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**
>
> {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**
>
> {AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**
>
> {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**
>
> {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**

b. Строковый параметр **LSEventCacheDirectory** в значении укажите путь к папке для хранения локального кеша.

> **Информация**
>
> Папка **LSEventCacheDirectory** должна быть доступна для всех пользователей **RDP Windows Logon.**

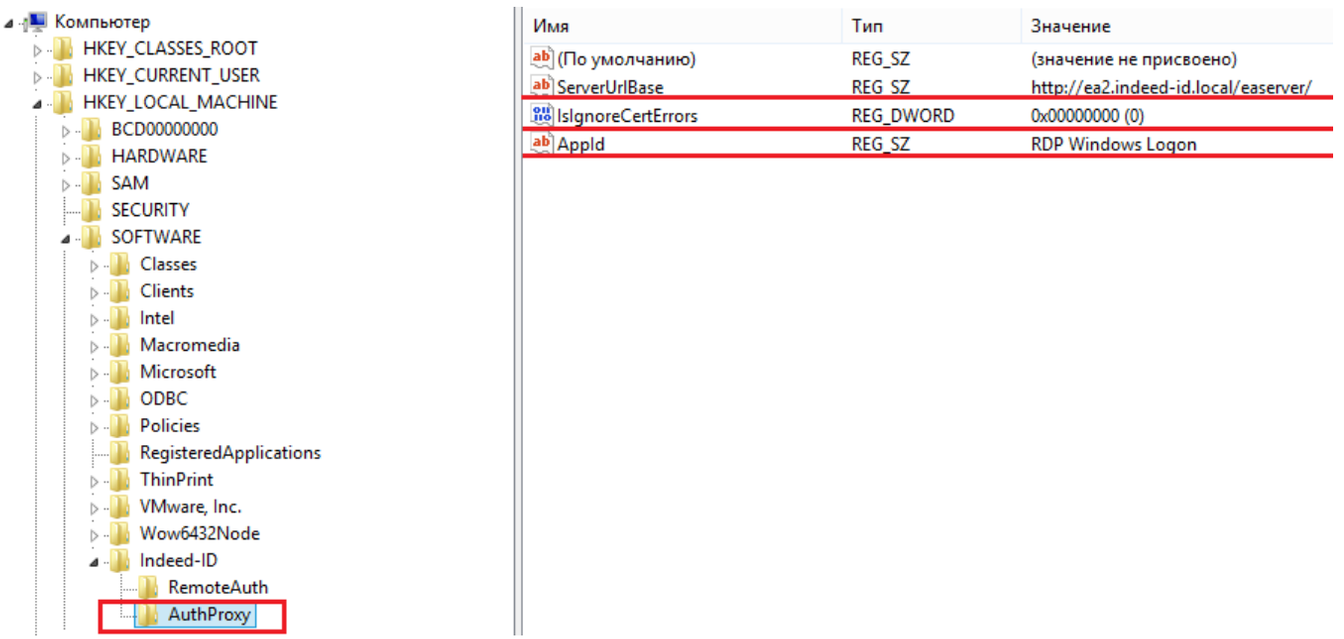


5. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy.** Измените параметры:

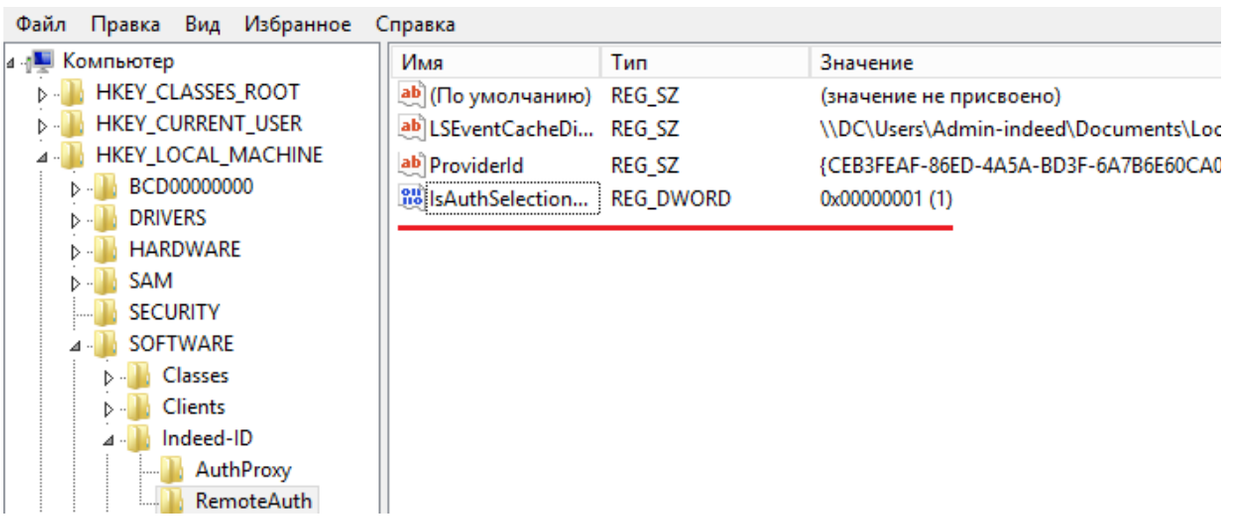
a. Параметр **ServerUrlBase.** В значении для параметра укажите адрес вашего сервера **Indeed**.
b. Параметр **IsIgnoreCertErrors,** указать значение **0** или **1.**

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

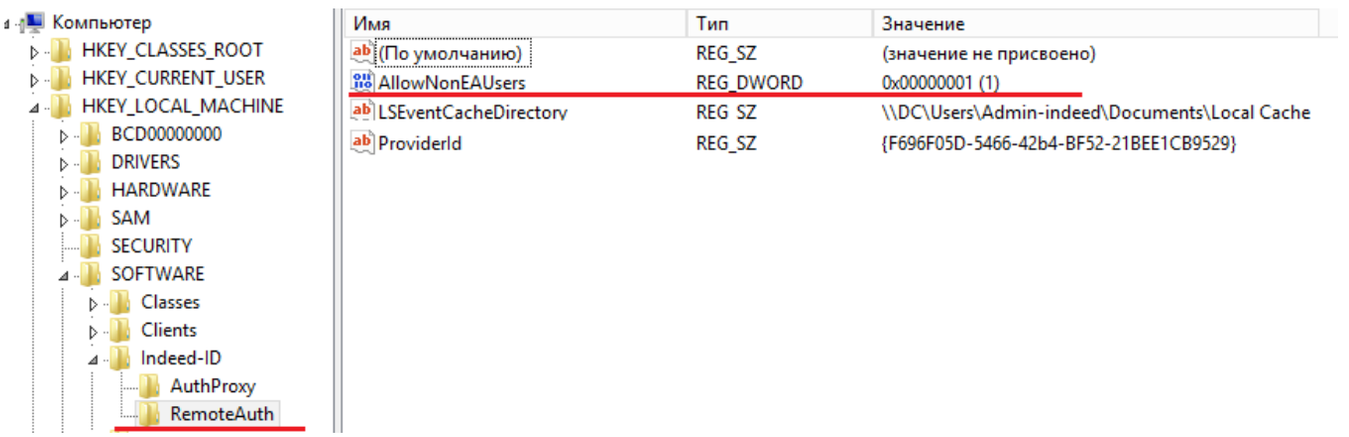
c. Параметр **AppId** со значением **RDP Windows Logon.**



6. Для настройки выбора провайдера аутентификации на стороне пользователя выполните:
    a. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth** реестра Windows создайте параметр **DWORD** с именем **IsAuthSelectionEnabled**
    b. Определите значение параметра **IsAuthSelectionEnabled** равное **1**. Если параметр не задан или его значение **0**, то выбор провайдера аутентификации предоставляться не будет. В этом случае будет использоваться провайдер, указанный в значении **ProviderId** или **Indeed AM Passcode Provider**, если **ProviderId** не указан. Если **IsAuthSelectionEnabled=1** и указан провайдер в **ProviderId**, то при подключении пользователя будет выбран указанный провайдер, но пользователь сможет выбрать любой другой из числа поддерживаемых.

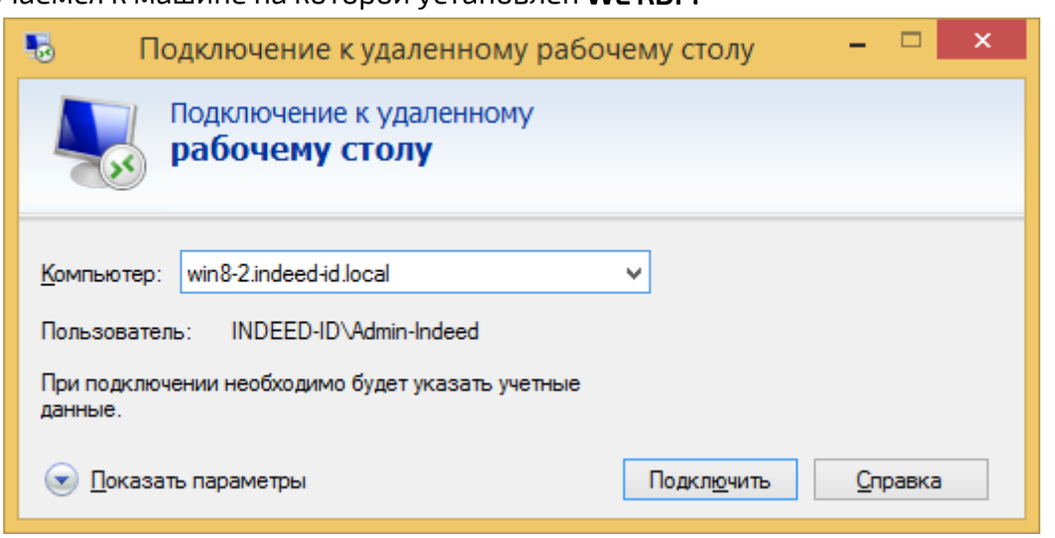


7. Аутентификация пользователей без лицензии на Indeed AM.
   По умолчанию **Indeed AM RDP Windows Logon** работает с пользователями, обладающими лицензией **AM RDP Windows Logon**. Для включения аутентификации пользователей без лицензии **RDP Windows Logon** выполните следующие действия:
   a. Откройте редактор реестра Windows.
   b. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth** создайте параметр **DWORD** с именем **AllowNonEAUsers**.
      - Если значение параметра **AllowNonEAUsers** равно **1**, то пользователи без лицензии RDP WL смогут аутентифицироваться по доменному паролю (Без использования технологии Indeed).
      - Если значение параметра **AllowNonEAUsers** равно **0** или **не задано**, то аутентификация осуществляется только для пользователей с лицензией RDP WL. Пользователь без лицензии аутентифицироваться не сможет.

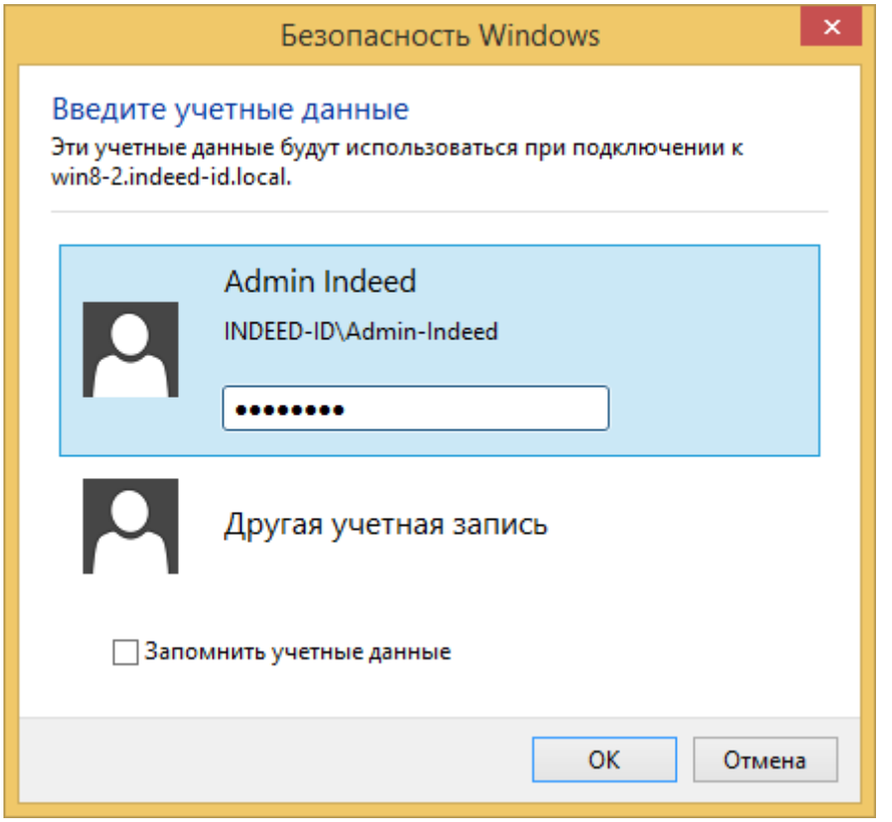


Пример работы расширения.

1. Подключаемся к машине на которой установлен **WL RDP.**



2. Указываем пользователя и доменный пароль и нажимаем **"Ок".**



3. Вводим одноразовый пароль.