

INDEED



© Компания «Индид», 2009–2018.
Все права защищены.

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 EA RDP Windows Logon

Руководство по установке и эксплуатации
версия 2.0.0

Содержание

Введение	2
Условные обозначения	2
О компоненте Indeed EA RDP Windows Logon	2
Установка и настройка Indeed EA RDP Windows Logon	3
Предварительные условия установки	3
Системные требования	3
Порядок установки	3
Настройка Indeed EA RDP Windows Logon	4
Настройка параметров аутентификации	4
Настройка провайдеров	4
Аутентификация с использованием Indeed EA RDP Windows Logon	7
Сбор программных логов	9
Часто задаваемые вопросы	9

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Это руководство поможет вам ознакомиться с принципом работы компонента **Indeed EA RDP Windows Logon**, 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 EA RDP Windows Logon

Модуль Indeed EA RDP Windows Logon реализует возможность двухфакторной аутентификации с помощью технологии Indeed ID в процессе подключения по RDP или Remote App. В качестве второго фактора поддерживается использование:

- Статического мастер-пароля
- Одноразового пароля, сгенерированного мобильным приложением
- Одноразового пароля, отправленного по SMS или Email.

Установка и настройка Indeed EA RDP Windows Logon

Предварительные условия установки

Для корректной установки и работы Indeed EA RDP Windows Logon 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
- Консоль управления Indeed EMC

Системные требования

Аппаратные требования для установки

Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО.

Поддерживаемые операционные системы

- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows 7 SP1 32/64bit
- Windows 8.1 32/64bit
- Windows 10 32/64bit

Порядок установки

Indeed EA RDP Windows Logon устанавливается на сервере с компонентом **Узел сеансов удаленных рабочих столов** (Remote Desktop Session Host) роли **Службы удалённых рабочих столов** (Remote Desktop Services) или на рабочих станциях, к которым пользователи будут подключаться по RDP.

На каждом сервере Indeed EA устанавливаются провайдеры Indeed (один или несколько), необходимые для аутентификации пользователей.

Для установки Indeed EA RDP Windows Logon выполните следующие действия:

1. Запустите файл Indeed.EA.RDPWindowsLogon.ru-ru.msi в соответствии с разрядностью операционной системе из дистрибутив и выполните установку, следуя указаниям мастера.
2. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.
3. Установка, настройка, удаление и обновление провайдеров аутентификации осуществляется в соответствии с руководством по установке и эксплуатации соответствующего провайдера.

Настройка Indeed EA RDP Windows Logon

Настройка параметров аутентификации

Аутентификация пользователей без лицензии на Indeed EA

По умолчанию Indeed EA RDP Windows Logon работает с пользователями, обладающими лицензией на использование технологии аутентификации Indeed.

Для включения аутентификации пользователей без лицензии Indeed EA выполните следующие действия:

1. Откройте редактор реестра Windows.
2. Создайте в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\` ключ **Indeed-ID** с вложенным ключом **RemoteAuth**.
3. В созданном ключе **RemoteAuth** создайте параметр DWORD с именем **AllowNonEAUsers**
4. Определите значение параметра **AllowNonEAUsers** равное **1**. Если параметр не задан или его значение 0, то Indeed EA RDP Windows Logon будет работать только с пользователями, обладающими лицензией Indeed EA.

Настройка провайдеров

Поддерживаются два режима работы Indeed EA RDP Windows Logon: с провайдером аутентификации, заданным на сервере или с провайдером, выбранным пользователем в момент подключения.

Настройка провайдера аутентификации на сервере Indeed EA RDP Windows Logon

1. В разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth` реестра Windows создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру:

{F696F05D-5466-42B4-BF52-21BEE1CB9529} – для Passcode Provider

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} – для Google Authenticator Provider

{093F612B-727E-44E7-9C95-095F07CBB94B} – для Email OTP Provider

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} – для SMS OTP Provider



Допустимо только одно значение **ProviderId**. Для работы с несколькими провайдерами аутентификации используйте вариант подключения, при котором провайдер выбирается пользователем в процессе подключения.

Если **ProviderId** не задан, то будет использоваться Indeed-Id Passcode Provider.

2. В случае использования Indeed-Id Email OTP Provider задайте имя атрибута Active Directory, в котором содержится адрес электронной почты пользователя для отправки одноразового пароля.

По умолчанию используется атрибут **mail**. Для изменения атрибута создайте в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth` строковый параметр **EmailAttribute** и укажите в качестве его значения имя атрибута, в котором хранится адрес электронной почты пользователя.

На Рисунке 1 приведен пример настройки для провайдера Email OTP с получением адреса электронной почты пользователя из атрибута **otherMailbox**.

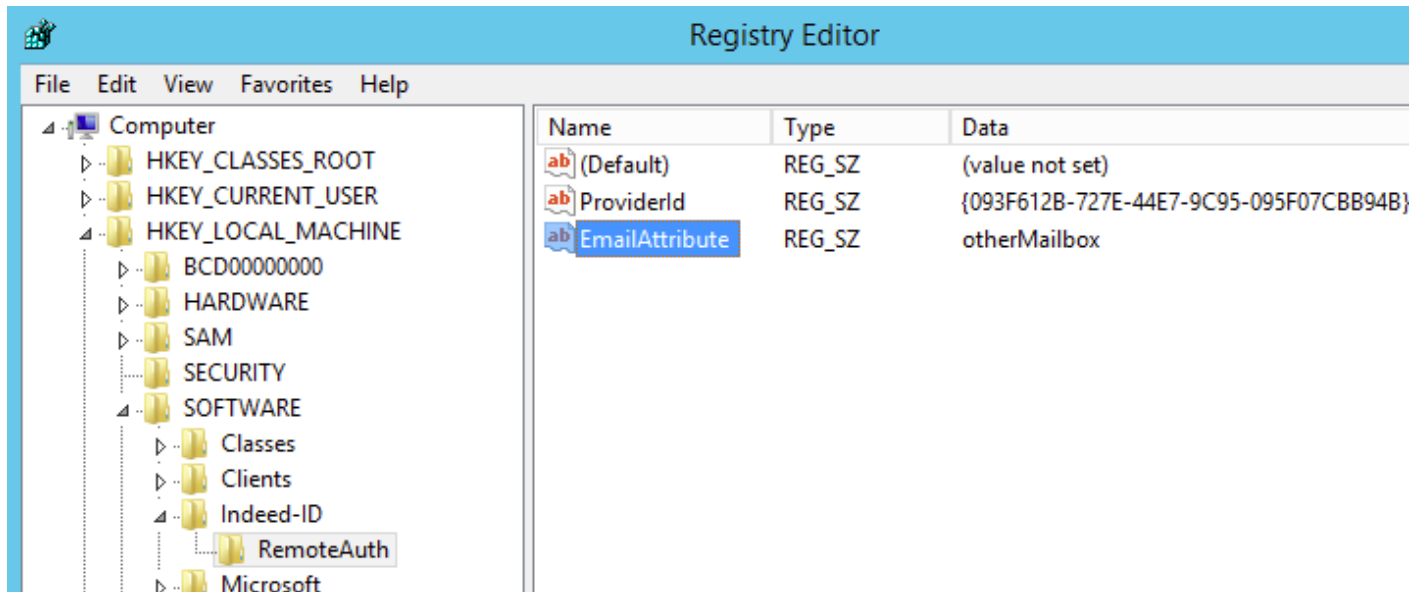


Рисунок 1 – Настройка для провайдера Email OTP с получением адреса электронной почты пользователя из атрибута otherMailbox.

3. В случае использования Indeed-Id SMS OTP Provider задайте имя атрибута Active Directory, в котором содержится номер телефона пользователя для отправки одноразового пароля. По умолчанию используется атрибут **telephoneNumber**. Для изменения атрибута создайте в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth строковый параметр **PhoneAttribute** и укажите в качестве его значения имя атрибута, в котором хранится номер телефона пользователя.
- На Рисунке 2 приведен пример настройки для провайдера SMS OTP с получением номера телефона пользователя из атрибута **mobile**.

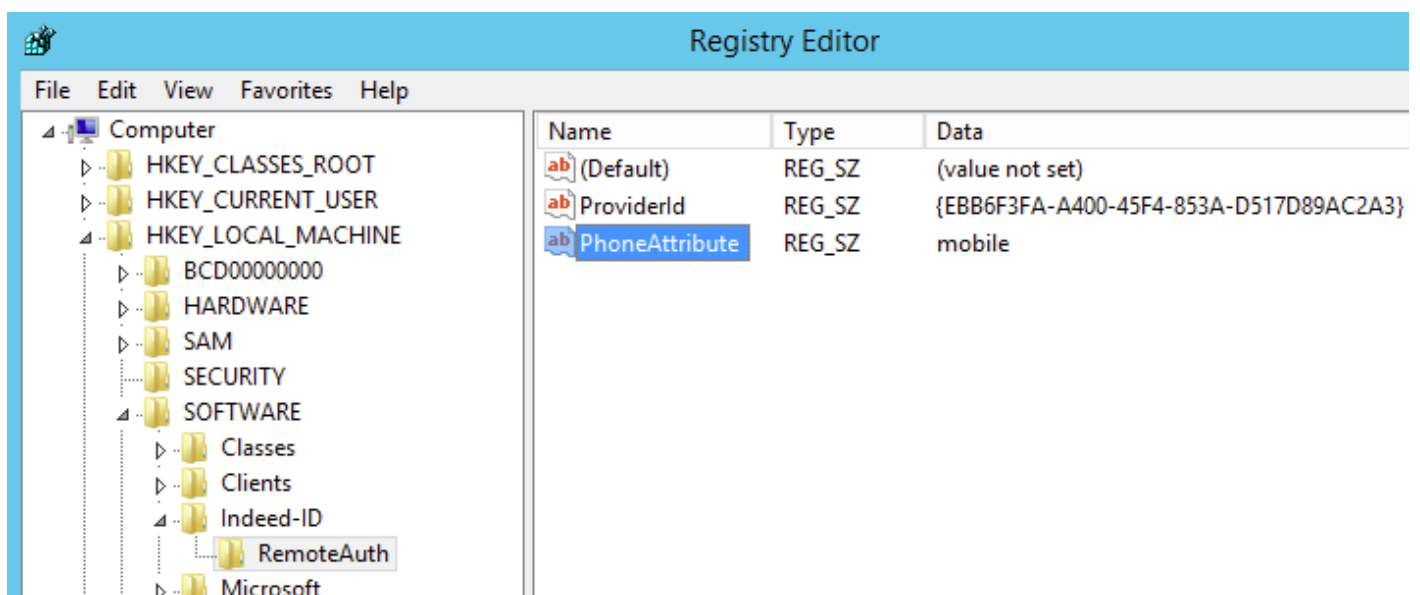


Рисунок 2 – Настройка для провайдера SMS OTP с получением адреса электронной почты пользователя из атрибута mobile.

Выбор провайдера аутентификации на стороне пользователя

По умолчанию выбор провайдера аутентификации отключен. Для включения выполните на сервере Indeed EA RDP Windows Logon следующие действия:

1. В разделе HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth реестра Windows создайте параметр DWORD с именем **IsAuthSelectionEnabled**
2. 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-Id 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.

На Рисунке 3 приведен пример настройки Indeed EA RDP Windows Logon:

- Разрешено подключение пользователей без лицензией Indeed EA (AllowNonEAUsers=1)
- В качестве провайдера по умолчанию определен Indeed-Id Email OTP Provider (его ID указан в ProviderId) и определен атрибут, содержащий адрес электронной почты пользователя (EmailAttribute=mail)
- Разрешен выбор провайдера аутентификации пользователем (IsAuthSelectionEnabled=1)
- В случае, если пользователь выберет для аутентификации Indeed-Id SMS OTP Provider, то телефонный номер будет взят из атрибута mobile (PhoneAttribute=mobile)

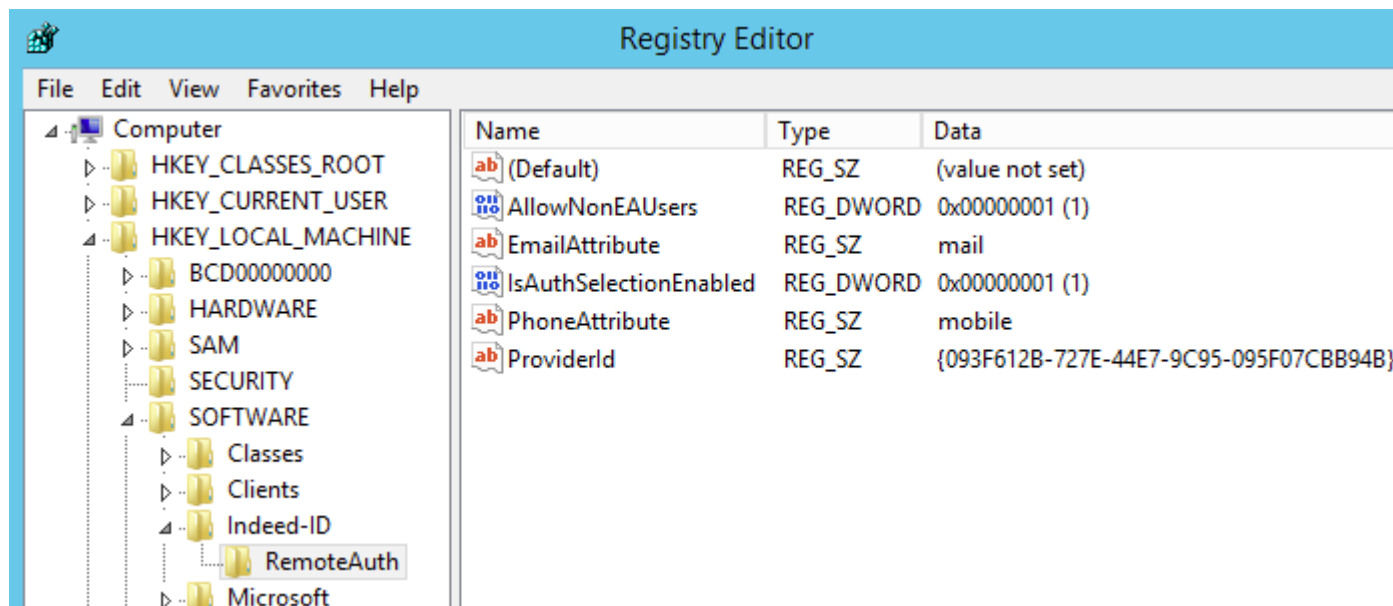


Рисунок 3 – Пример конфигурации Indeed EA Remote Authentication.

Аутентификация с использованием Indeed EA RDP Windows Logon

1. Выполните вход на портал RD Web Access и выберите опубликованное RDP подключение.



В сценарии без использования RD Web Access Indeed EA RDP Windows Logon устанавливается на рабочей станции, к которой требуется подключение по RDP (сервер), настроенное таким образом, чтобы запрос учетных данных происходил на рабочей станции, с которой подключается пользователь (клиент).

2. В появившемся окне введите доменные логин и пароль (Рисунок 4).

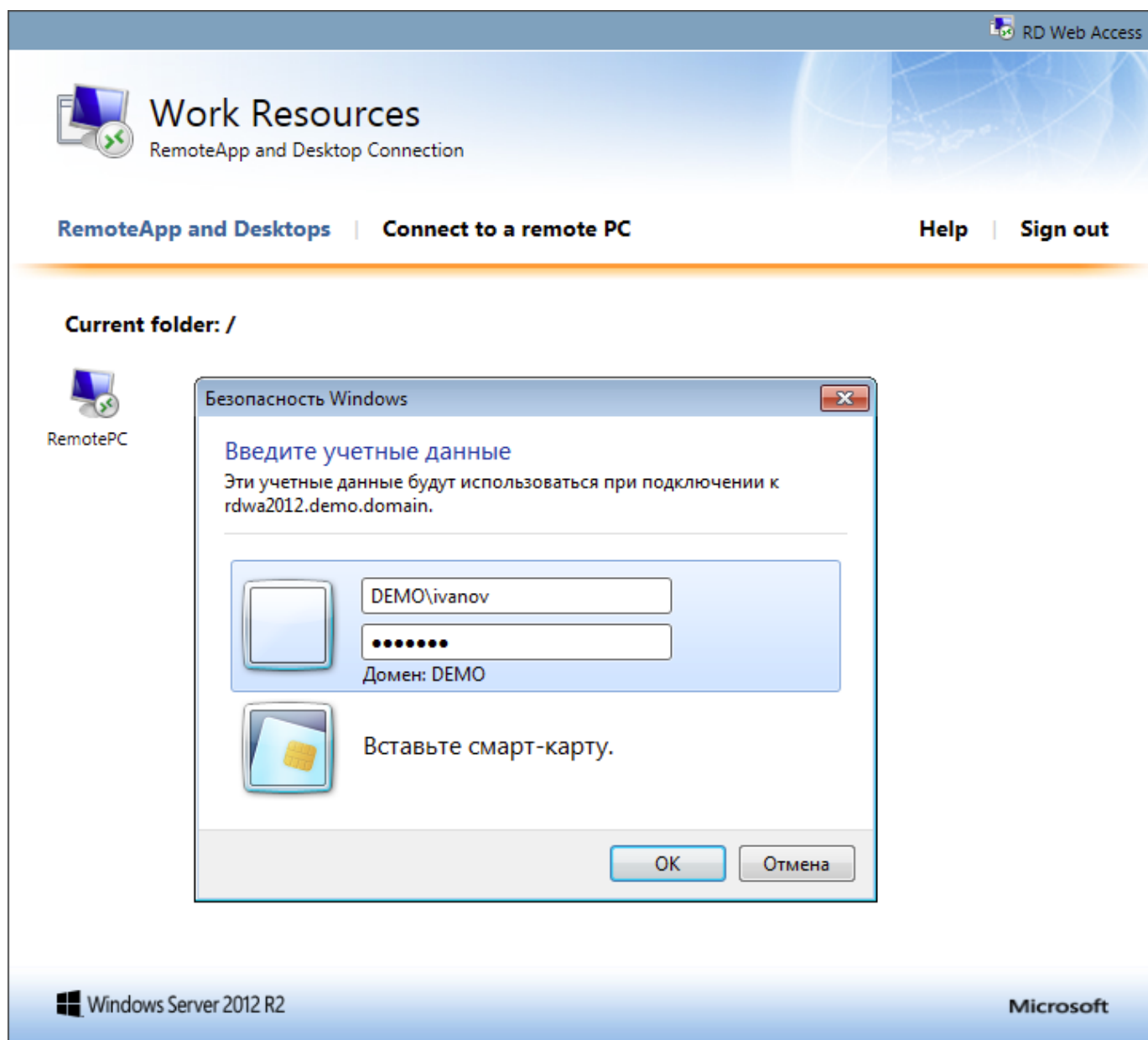


Рисунок 4 – Ввод учетных данных пользователя в RD Web Access.

3. Если учетные данные введены верно, то отобразится окно с запросом одноразового пароля (способ получения зависит от настроенного провайдера аутентификации), Рисунок 5.

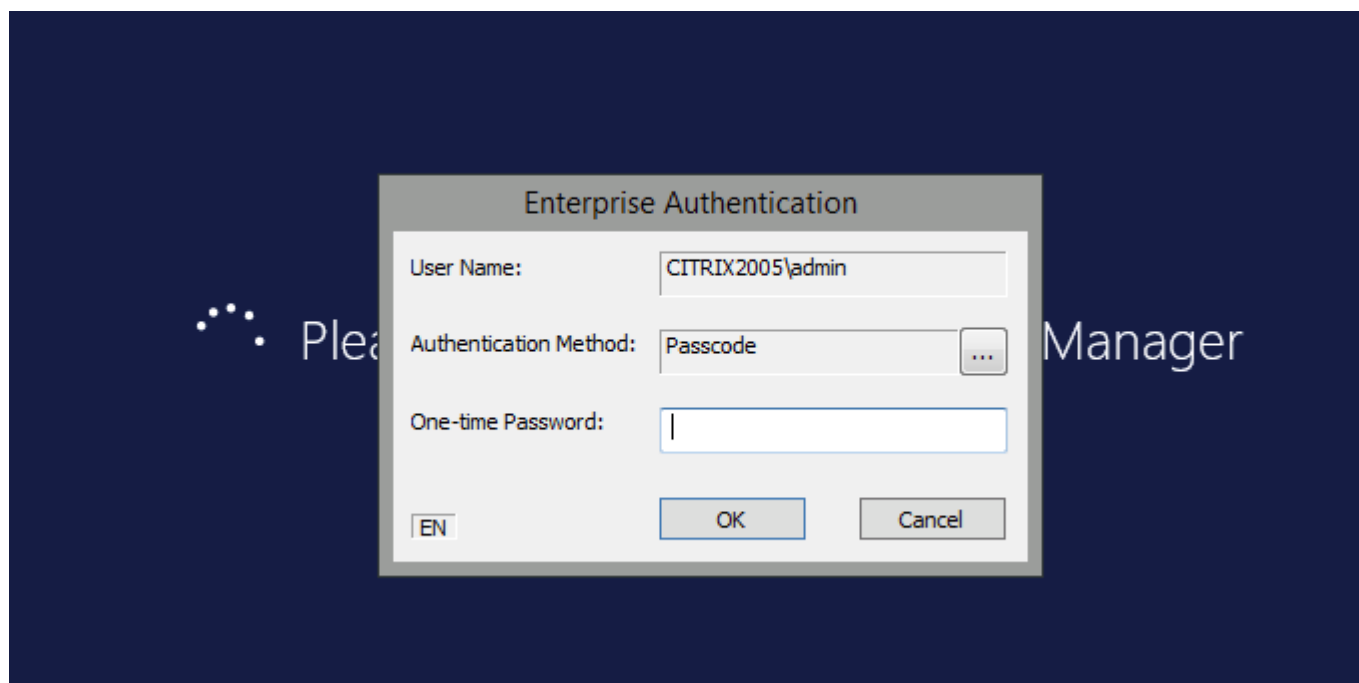


Рисунок 5 – Окно Indeed EA RDP Windows Logon.

4. Для выбора провайдера аутентификации (если он разрешен) нажмите .
5. Введите пароль и нажмите **OK**. После проверки пароля сервером Indeed EA произойдет переход к RDP сессии.



Для входа по Passcode и Google Authenticator пользователь должен обладать соответствующим аутентификатором в системе Indeed EA.

Для входа по одноразовому паролю, отправляемому по email или в виде SMS, регистрация аутентификатора не требуется.

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.