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 IIS Extension

Руководство по установке и эксплуатации

версия 1.3.1

Содержание

Введение 2

Условные обозначения 2

О компоненте Indeed IIS Extension 2

Установка и настройка Indeed IIS Extension 3

- Предварительные условия установки . . . 3
- Порядок установки и настройки . . . 4
- Установка Indeed IIS Extension . . . 5
- Включение зарегистрированного модуля аутентификации Indeed . . . 5
- Настройка проверки подлинности приложений . . . 7
  - Проверка подлинности Windows (Windows Authentication) . . . 7
  - Проверка подлинности с помощью форм (Forms Authentication) . . . 8
- Настройка однофакторной аутентификации . . . 9
- Настройка двухфакторной аутентификации . . . 10
- Настройка приложений на работу с различными провайдерами аутентификации Indeed . . . 13

Примеры настройки приложений для работы с Indeed IIS Extension 14

- Outlook Web App . . . 14
- Exchange Active Sync . . . 18
- Remote Desktop Web Access . . . 20
- Microsoft Lync/Skype for Business . . . 23
- Directum . . . 24

Сбор программных логов 26

Часто задаваемые вопросы 26

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное руководство поможет вам ознакомиться с принципом работы компонента **Indeed IIS 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 IIS Extension

Продукт Indeed IIS Extension обеспечивает возможность аутентификации пользователей в web-приложениях, развернутых на платформе Microsoft Internet Information Services (IIS) с использованием технологии аутентификации Indeed, таких как:

- Outlook Web Access
- Lync/Skype for Business
- Directum
- Remote Desktop Web Access
- Прочих приложениях, использующих платформу IIS

Это позволяет вместо пароля доменной учетной записи использовать специальный (отдельный) пароль. Пароль может быть одноразовым или статическим. При этом возможность аутентификации по доменному паролю сохраняется. Также возможно использование одноразового пароля в качестве второго фактора аутентификации, наряду с доменным паролем.
Indeed IIS Extension поддерживает работу с web-приложениями использующими следующие методы проверки подлинности пользователей:

- Обычная проверка подлинности (Basic Authentication)
- Дайджест-проверка подлинности (Digest Authentication)

- Windows-проверка подлинности (Windows Authentication)
- Проверка подлинности с помощью форм (Forms Authentication)

Поддерживаемые форматы передачи данных для Forms Authentication:

- SOAP XML
- JSON
- HTML forms

Совместимые провайдеры аутентификации Indeed:

- Indeed-Id Google Authenticator Provider без поддержки PIN-кода (для одно- и двухфакторной аутентификации)
- Indeed-Id Passcode Provider (для одно- и двухфакторной аутентификации)
- Indeed-Id SMS OTP Provider (только для двухфакторной аутентификации)
- Indeed-Id Email OTP Provider (только для двухфакторной аутентификации)

Установка и настройка Indeed IIS Extension

Предварительные условия установки

Для корректной установки и работы Indeed IIS Extension необходимо следующее окружение:

- Microsoft Internet Information Services (версии 7.5 -8.5)
- Продукты Indeed, установленные в следующей конфигурации:
  - Indeed-Id Enterprise Server
  - Indeed-Id Windows Logon[1]
  - Провайдеры аутентификации Indeed-Id:
    - Indeed-Id Passcode Provider
    - Indeed-Id Google Authenticator Provider
    - Indeed-Id SMS OTP Provider
    - Indeed-Id Email OTP Provider

[1]Не требуется при использовании с Indeed-Id Email OTP Provider и Indeed-Id SMS OTP Provider.

Порядок установки и настройки

Установку необходимых компонентов рекомендуется выполнять в следующем порядке:

1. Установка модуля Indeed-Id Enterprise Server.
2. Установка провайдеров аутентификации Indeed на каждой рабочей станции, где установлен модуль Indeed-Id Enterprise Server.
3. Установка провайдеров аутентификации Indeed (только Indeed-Id Passcode Provider или Indeed-Id Google Authenticator Provider) на рабочих станциях пользователей, где будет производиться регистрация аутентификаторов.
4. Установка компонента Indeed IIS Extension на сервер с развернутой ролью IIS[2].

[2]Для работы с Lync(Skype for Business) модуль должен быть установлен на FrontEnd сервере Lync.

Установка Indeed IIS Extension

Для установки компонента пользователь, от имени которого выполняется установка, должен обладать правами администратора (быть членом локальной группы «Администраторы»).

1. Запустите файл Indeed.EA.IIS.Extension.x64.msi и выполните установку, следуя указаниям мастера.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

При удалении продукта модуль аутентификации Indeed будет удален из всех сайтов и приложений IIS. Аутентификация пользователей на этих ресурсах по технологии Indeed будет невозможна.

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение (для Outlook Web Access – это owa), которое будет использовать Indeed IIS Extension и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей. . .** (Configure Native Modules. . .), включите модули Indeed в соответствии с Рисунком 1 и нажмите OK.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

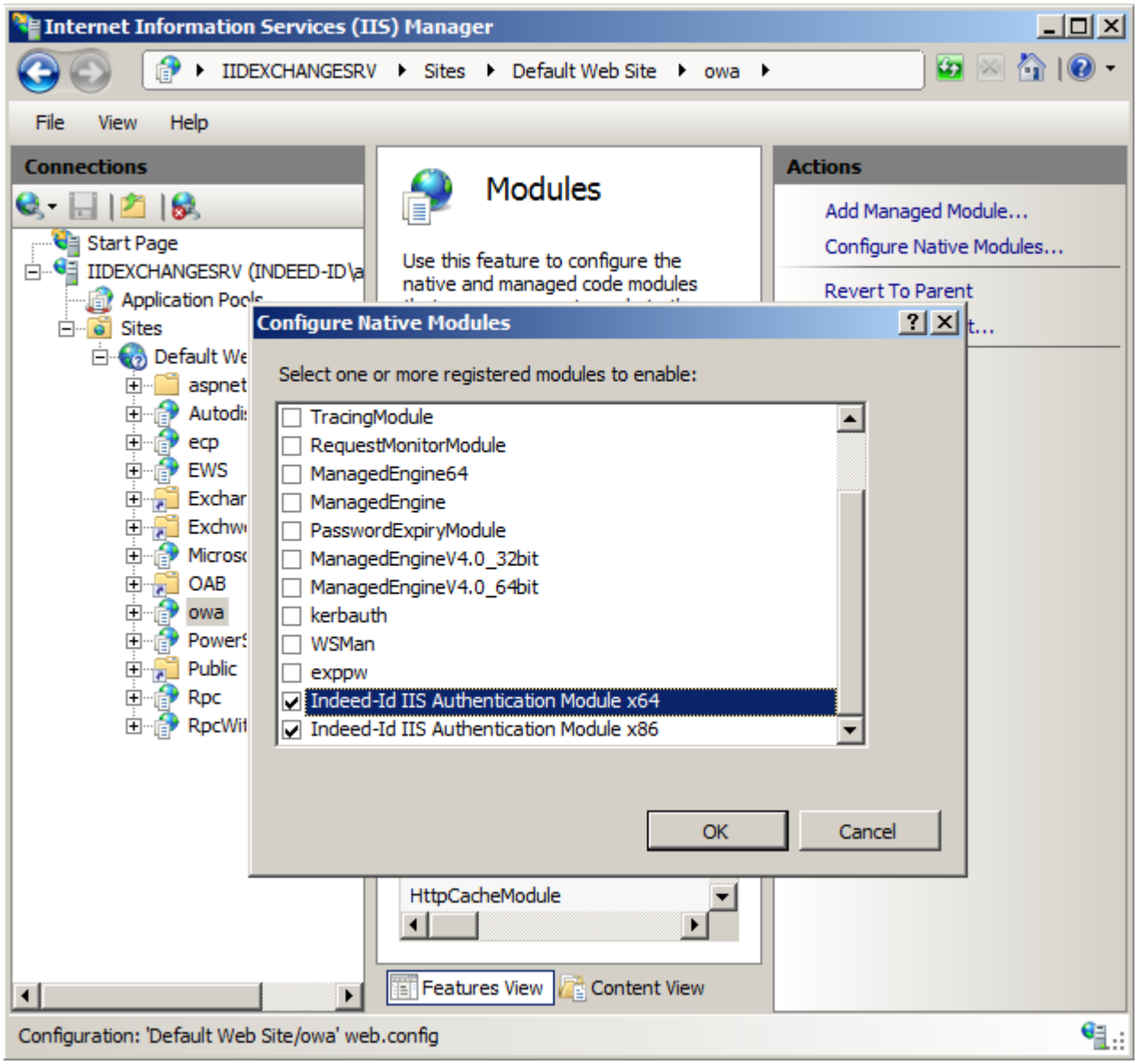

Рисунок 1 – Включение модулей аутентификации Indeed на примере Outlook Web Access.

Для обеспечения аутентификации пользователей в web-приложениях по технологии Indeed должны выполняться следующие условия:

- Серверы Indeed должны быть запущены и доступны по сети для модуля Indeed IIS Extension, развернутого на сервере с ролью Internet Information Services и целевыми web-приложениями.
- Пользователи должны иметь разрешение на использование Indeed Enterprise Authentication (соответствующая опция располагается на вкладке **Настройки** в карточке пользователя в **консоли управления Indeed EMC**). Для получения подробной информации обратитесь к документу *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.
- Пользователи должны иметь обученный аутентификатор в системе Indeed EA. Обучение аутентификатора осуществляется пользователем самостоятельно с помощью приложения **Управление аутентификаторами**, входящего в состав Indeed-Id Windows Logon.

- Целевые приложения, в случае необходимости, должны быть настроены на работу с Indeed IIS Extension(см. **Примеры настройки приложений для работы с Indeed IIS Extension**).

Настройка проверки подлинности приложений

Перед началом использования Indeed IIS Extension может потребоваться настройка способов проверки подлинности целевых web-приложений (зависит от используемых способов проверки подлинности вашего приложения). Для способов проверки подлинности **Digest** и **Basic** дополнительная настройка не требуется. Настройки для проверки подлинности Windows и проверки подлинности при помощи форм приведены ниже.

Проверка подлинности Windows (Windows Authentication)

В случае проверки подлинности Windows Indeed IIS Extension работает через провайдер NTLM. Поэтому необходимо в IIS определить приоритет использования провайдеров в данном способе проверки подлинности.
Установите провайдер **NTLM** первым в списке используемых провайдеров в разделе **Проверка подлинности** (Authentication) **Диспетчера служб IIS** (IIS Manager), Рисунок 2:

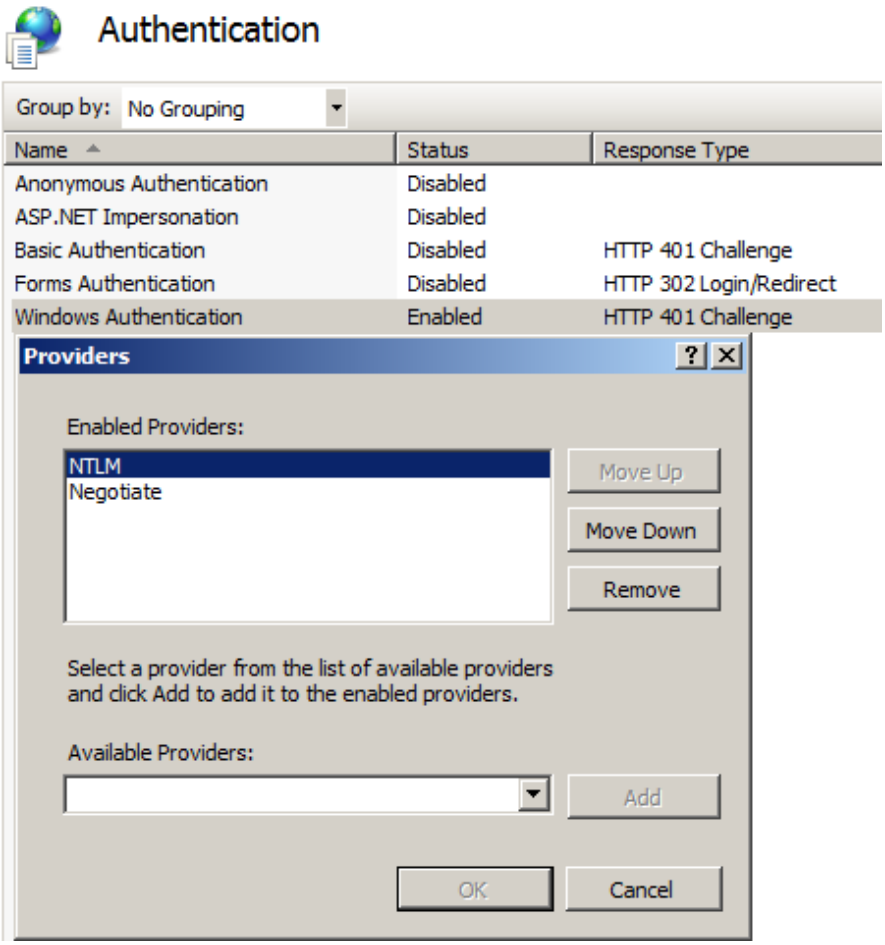

Рисунок 2 – Настройка проверки подлинности Windows.

В разделе **Дополнительные параметры** (Advanced Settings) для **проверки подлинности Windows** (Windows Authentication) отключите опцию **Включить проверку подлинности в режиме ядра** (Enable Kernel-mode authentication).

Проверка подлинности с помощью форм (Forms Authentication)

Indeed IIS Extension совместим с любым приложением или web-страницей, использующим html-форму для аутентификации пользователей. При этом включение проверки подлинности с помощью форм (Forms Authentication) в настройках IIS для такого приложения не обязательно.

Для обеспечения аутентификации по технологии Indeed необходимо выполнить настройку forms-аутентификации на сервере IIS для используемого приложения:

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте ключ с именем приложения или сайта в IIS (может иметь произвольное значение) в разделе реестра Windows**HKEY_LOCAL_MACHINE \SOFTWARE\Indeed-ID\IISHTTPModule**
3. Создайте в ключе с именем приложения следующие строковые параметры:
   LoginURL – относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
   UsernameField – значение атрибута **name** поля имени пользователя формы входа приложения.
   PasswordField – значение атрибута **name** поля пароля формы входа приложения.

Значения всех перечисленных параметров содержатся в форме аутентификации целевого приложения могут быть получены, например, при помощи инструмента Internet Explorer F12 Developer Tools. На Рисунке 3 приведен пример значений всех параметров для приложения Outlook Web App.

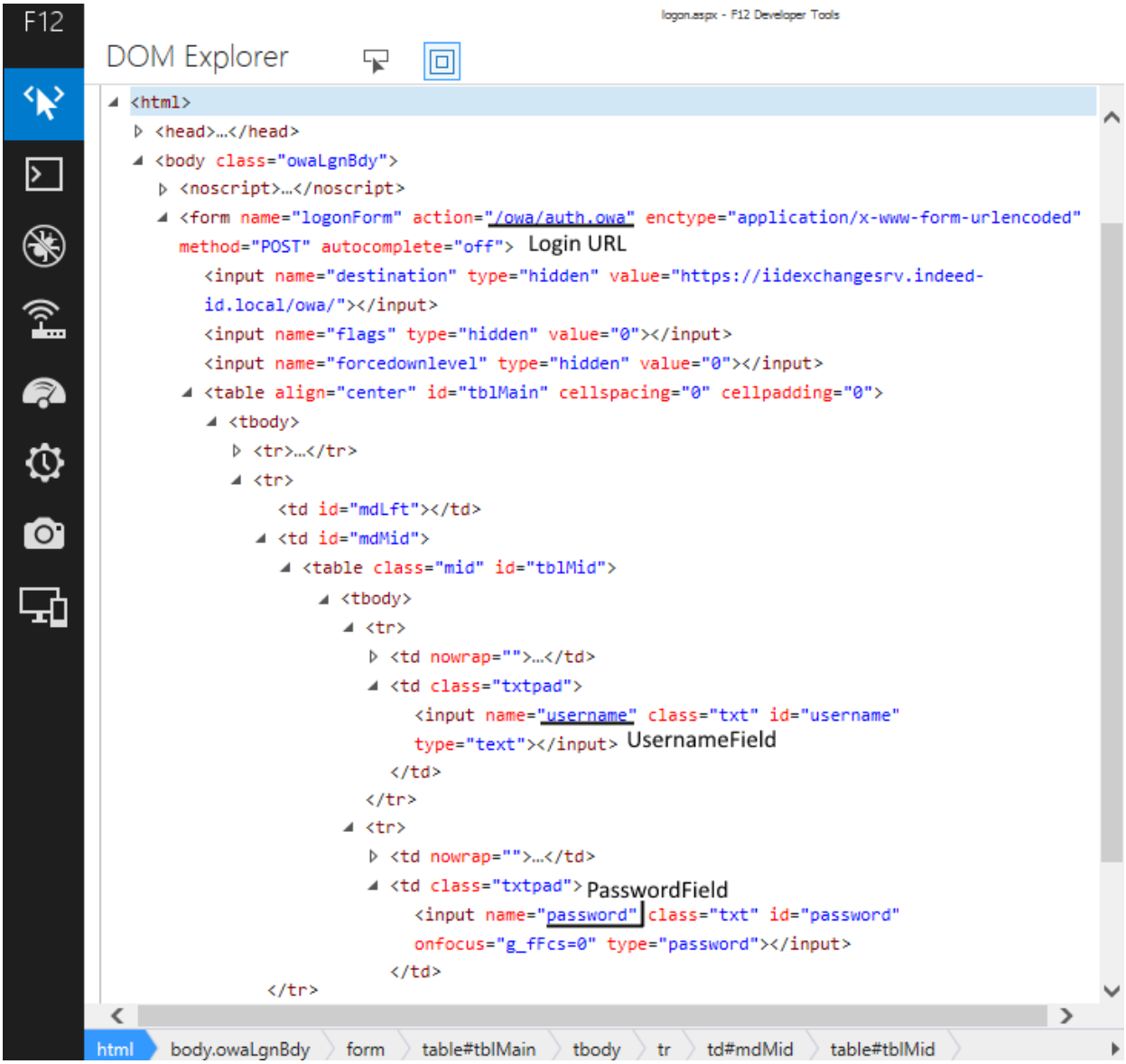

Рисунок 3 – Значения параметров LoginURL, UsernameField и PasswordField для Outlook Web App.

Примеры настройки проверки подлинности с помощью форм для различных приложений приведены в разделе **Примеры настройки приложений для работы с Indeed IIS Extension**.

Настройка однофакторной аутентификации

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ Indeed-ID с вложенным ключом IISHTTPModule.
3. В созданном ключе **IISHTTPModule** создайте строковый параметр ProviderId и задайте для него значение, соответствующее используемому провайдеру (Рисунок 4):
   {F696F05D-5466-42B4-BF52-21BEE1CB9529} – для Indeed-Id Passcode Provider
   {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} – для Indeed-Id Google Authenticator Provider

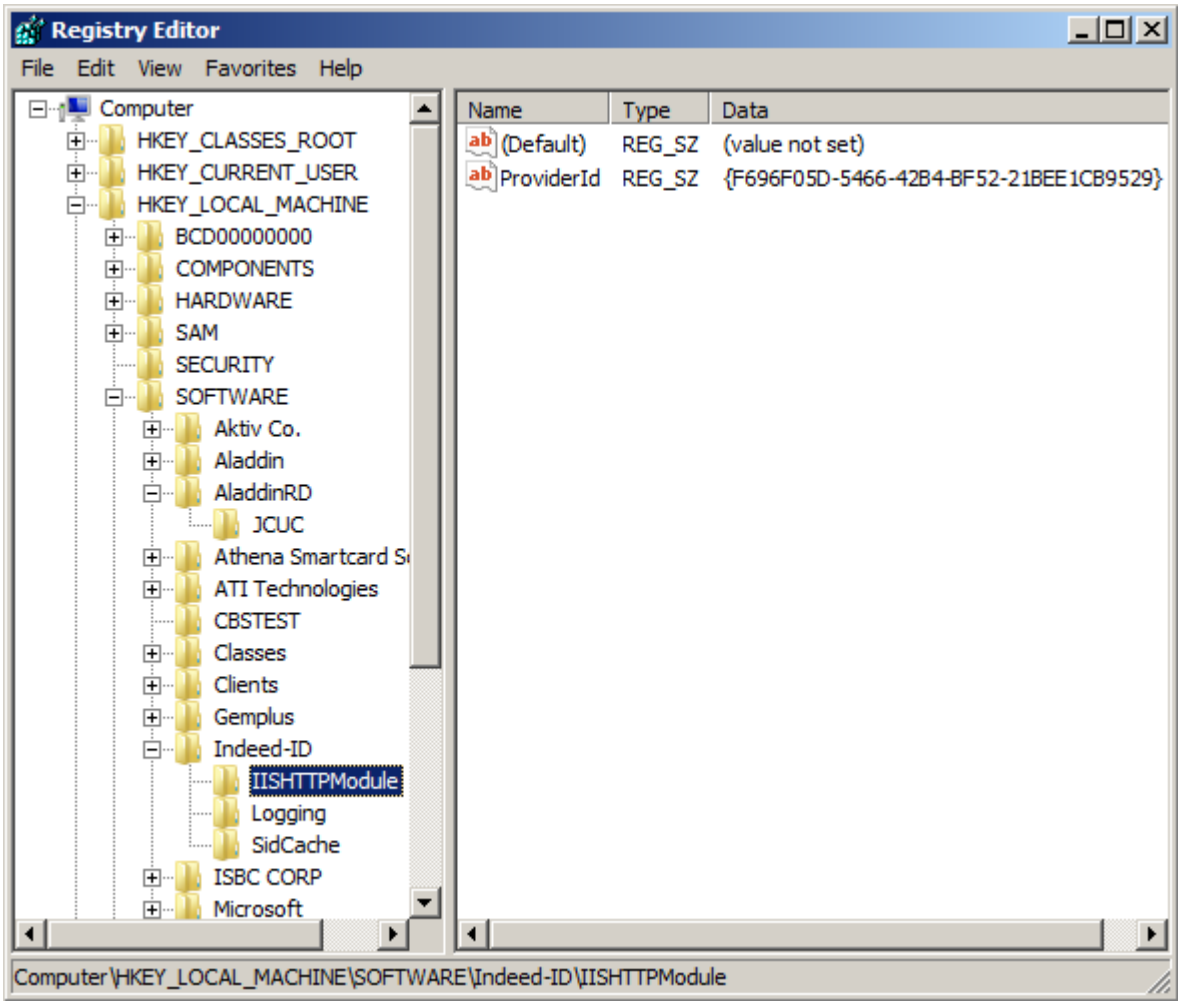

Рисунок 4 – Настройка однофакторной аутентификации в Indeed IIS Extension.

Настройка двухфакторной аутентификации

Indeed IIS Extension позволяет настроить двухфакторную аутентификацию для доступа к удаленным рабочим столам и приложениям через web с использованием службы Microsoft Remote Desktop Web Access (RD Web Access). Двухфакторная аутентификация реализована с помощью аутентификации по доменному паролю и по второму фактору – одноразовому паролю.

Двухфакторная аутентификация поддерживается только для приложений, **использующих проверку подлинности с помощью форм** (Forms Authentication).

Провайдеры Indeed-Id, поддерживающие двухфакторную аутентификацию:

- Indeed-Id Passcode Provider
- Indeed-Id Google Authenticator Provider
- Indeed-Id SMS OTP Provider
- Indeed-Id Email OTP Provider

Для обеспечения аутентификации по технологии Indeed необходимо выполнить настройку forms-аутентификации на сервере IIS для используемого приложения.

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule**.
3. В созданном ключе IISHTTPModule 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
4. Задайте строковые параметры **EmailAttribute** (определяет имя атрибута Active Directory, содержащего адрес электронной почты пользователя) и **PhoneAttribute** (определяет имя атрибута Active Directory, содержащего номер мобильного телефона пользователя). На Рисунке 5 приведен пример настроек для провайдера SMS OTP.

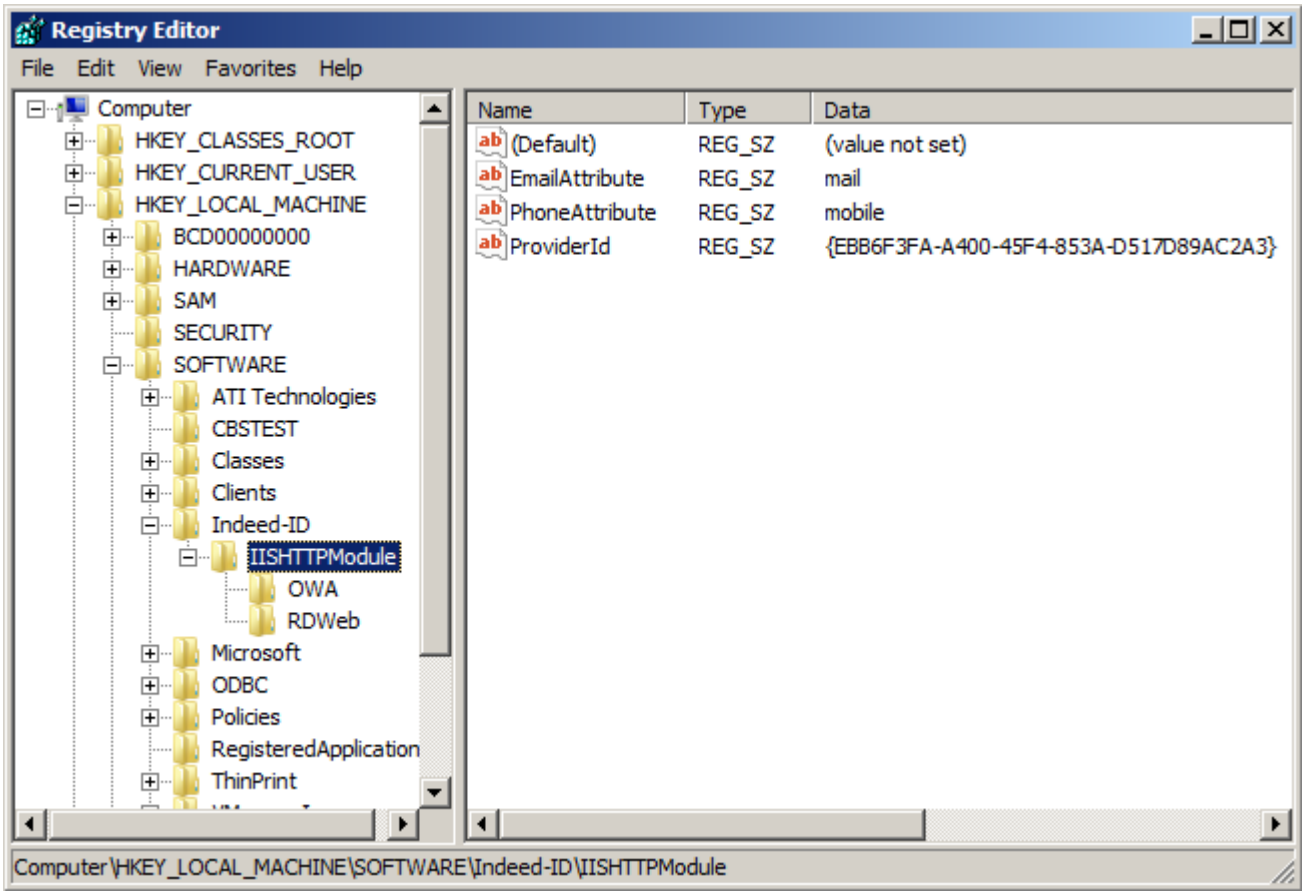

Рисунок 5 – Настройка двухфакторной аутентификации в Indeed IIS Extension.

5. Двухфакторная аутентификация настраивается отдельно для каждого целевого приложения. В процессе настройки необходимо создать в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule** реестра Windows ключ с именем приложения или сайта в IIS (может иметь произвольное значение), создать в этом ключе следующие параметры и определить их значения:

   AuthCookie – название Cookie, которое используется для аутентификации в целевом приложении. Определяется экспериментальным путем для каждого приложения. Значение параметра можно получить из консоли F12 IE Developer Toolbar выполнив следующие действия:

   - В разделе **Сеть** (Network) запустите **Сбор сетевого трафика** (Enable network traffic capturing)
   - Выполните аутентификацию в приложении
   - Перейдите в раздел **Подробности** (Details) на вкладку **Файлы Cookie** (Cookies).
   - Искомое значение указано в столбце **Ключ** (Key).

   На Рисунке 6 приведен пример значения для приложения RD Web Access. В данном случае значение параметра AuthCookie будет **TSWAAuthHttpOnlyCookie**.

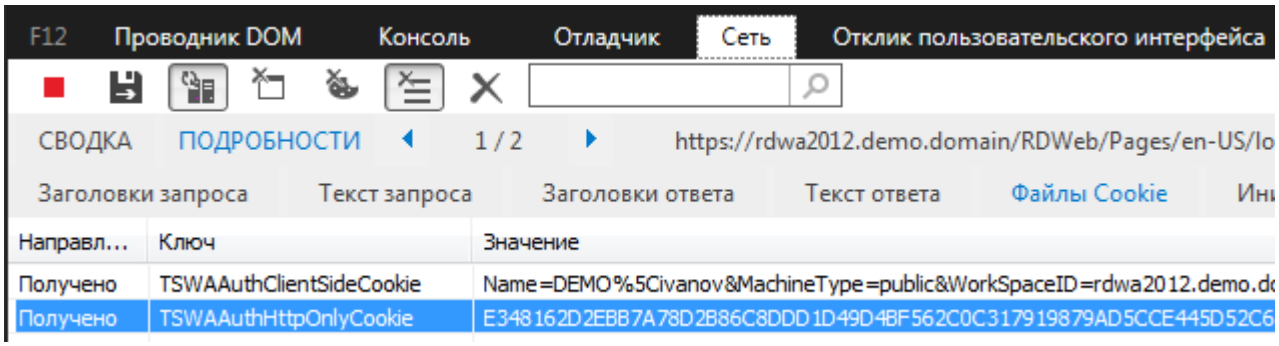

Рисунок 6 – Значение параметра AuthCookie для приложения RD Web Access.

IsMFAEnabled – включение двухфакторной аутентификации.
LoginURL – относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
OTPURL – альтернативный URL для отправки данных формы аутентификации Indeed второго фактора. По умолчанию данные формы отправляются на тот же URL, что и данные формы целевого приложения. Их перехватывает IIS модуль и подменяет на оригинальные данные, если аутентификация Indeed прошла успешно или же не подменяет их, если аутентификация Indeed не прошла и целевое приложение отображает собственную ошибку аутентификации. Значение необходимо использовать, если целевое приложение не трактует данные формы Indeed как ошибочные для аутентификации или необходимо явным образом демонстрировать ошибки аутентификации Indeed пользователю. Таким образом, значение можно оставить пустым или указать ссылку на страницу **/RDWeb/iidotp.aspx**.
PasswordField – значение атрибута **name** поля пароля формы входа приложения.
TargetURL – URL целевой страницы, на которую пользователь попадает после аутентификации в приложении.
UsernameField – значение атрибута **name** поля имени пользователя формы входа приложения.

Настройка приложений на работу с различными провайдерами аутентификации Indeed

Indeed IIS Extension позволяет задать провайдер аутентификации для целевого приложения, отличный от провайдера, используемого для аутентификации во всех других приложениях.
К примеру, модуль настроен на однофакторную аутентификацию с использованием провайдера Passcode (в секции IISHTTPModule), но для приложения OWA необходимо использовать провайдер SMS OTP.

Настройка провайдера аутентификации для конкретного приложения осуществляется следующим образом:

1. В ветке реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig** перейдите в раздел с именем приложения.
2. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру для данного приложения:
   - **{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

При указанном значении ProviderId в секции IISConfig для целевого приложения аутентификация будет осуществляться с использованием указанного идентификатора провайдера. ProviderId, указанный в секции IISHTTPModule в этом случае использоваться не будет.

Примеры настройки приложений для работы с Indeed IIS Extension

Outlook Web App

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение **owa** и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей...** (Configure Native Modules...), включите модули **Indeed-Id IIS Authentication Module (x64 и x86)** и нажмите **OK**.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

Настройка способов аутентификации, обрабатываемых IIS Extension

Настройка необходима для корректной работы Outlook Web App, настроенного на проверку подлинности при помощи форм.

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule\IISConfig**.
3. Создайте в ключе **IISConfig** ключ с точным именем сайта или приложения IIS – **Default Web Site/owa**.
4. Создайте в этом ключе DWORD значение **IsBasicDisabled=dword:00000001**
   На Рисунке 7 приведен пример настроек в реестре:

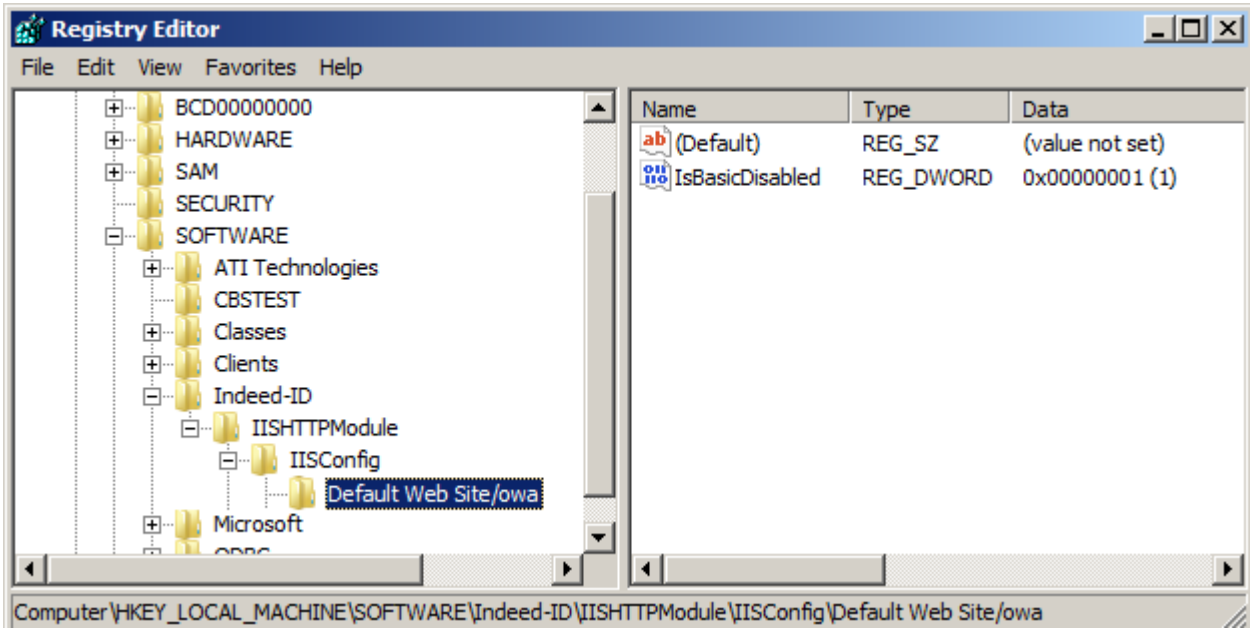

Рисунок 7 – Настройка способов аутентификации, обрабатываемых IIS Extension для Outlook Web App.

Настройка работы с заданным провайдером аутентификации Indeed

1. В ветке реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig** перейдите в раздел **Default Web Site/owa**
2. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру для данного приложения:
   - **{F696F05D-5466-42B4-BF52-21BEE1CB9529}** – для Passcode Provider
   - **{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}** – для Google Authenticator Provider

   На Рисунке 8 приведен пример настроек в реестре для аутентификации с использованием Indeed-Id Google Authenticator Provider.

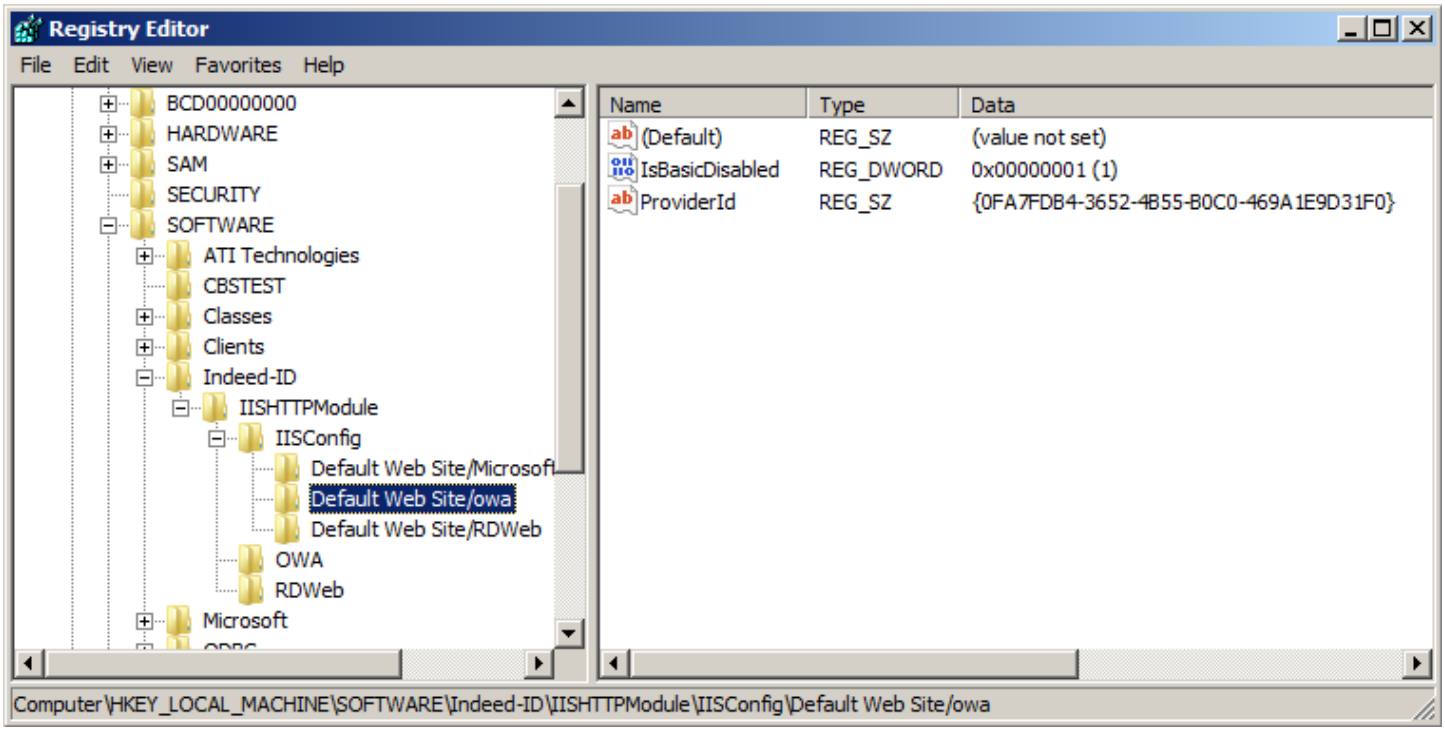

Рисунок 8 – Пример настроек в реестре для Outlook Web App для аутентификации с использованием Indeed-Id Google Authenticator Provider.

Итого, в разделе **...IISConfig/Default Web Site/owa** должны быть следующие параметры (на примере провайдера Google:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\Default Web
 Site/owa]
"IsBasicDisabled"=dword:00000001
"ProviderId"="{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}"
```

Настройка проверки подлинности

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule** ключ с именем приложения или сайта в IIS (может иметь произвольное значение).
   Например, **[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\OWA]**
3. Создайте следующие строковые параметры:
   LoginURL – относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
   UsernameField – значение атрибута **name** поля имени пользователя формы входа приложения.
   PasswordField – значение атрибута **name** поля пароля формы входа приложения.
4. В итоге реестр Windows должен содержать следующее (Рисунок 9):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\OWA]
"LoginURL"="/owa/auth.owa"
"UsernameField"="username"
"PasswordField"="password"
```

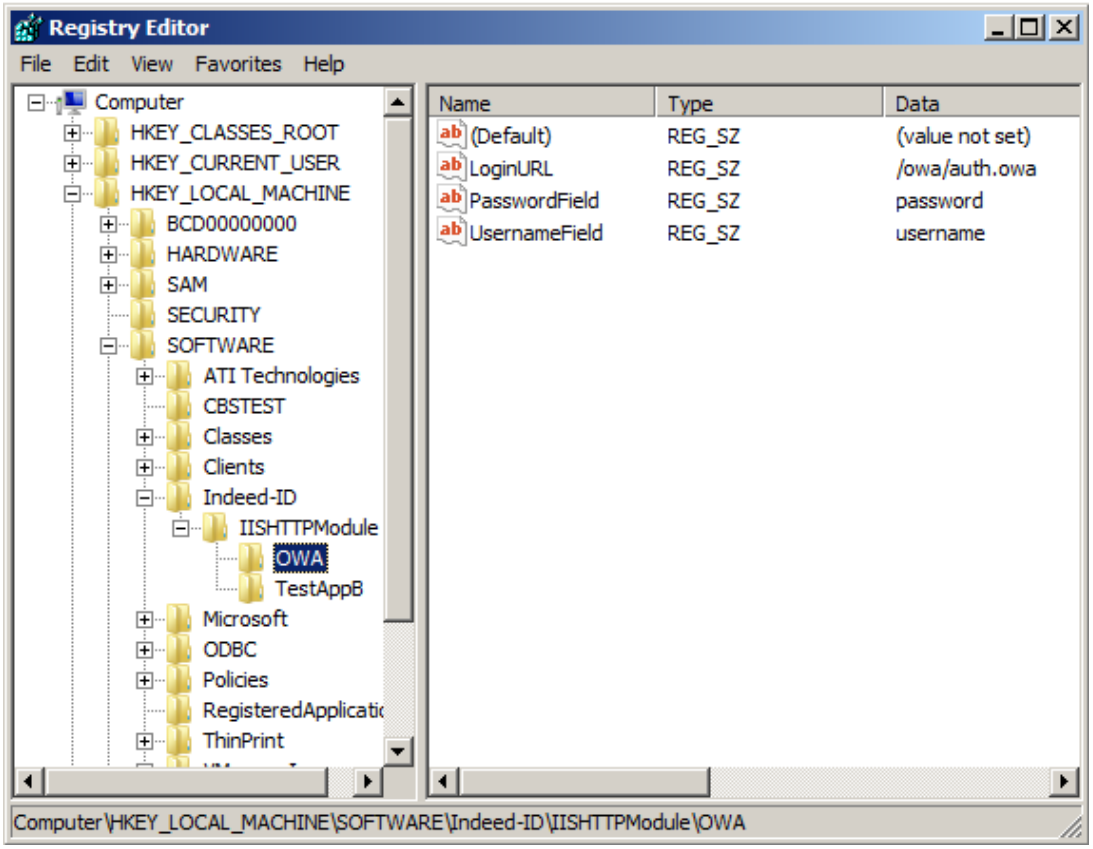

Рисунок 9 – Настройки Indeed IIS Extension для доступа в Outlook Web App.

5. Теперь для доступа в Outlook Web App пользователи смогут вместо доменного пароля использовать самостоятельно заданный пароль (в случае использования Indeed-Id Passcode Provider) или одноразовый пароль (в случае использования Indeed-Id Google Authenticator Provider).

   На Рисунке 10 приведен пример формы входа Outlook Web App, где доменный пользователь Ivan.Ivanov в качестве пароля использует одноразовый пароль, выданный приложением Google Authenticator, которое установлено на его смартфоне.

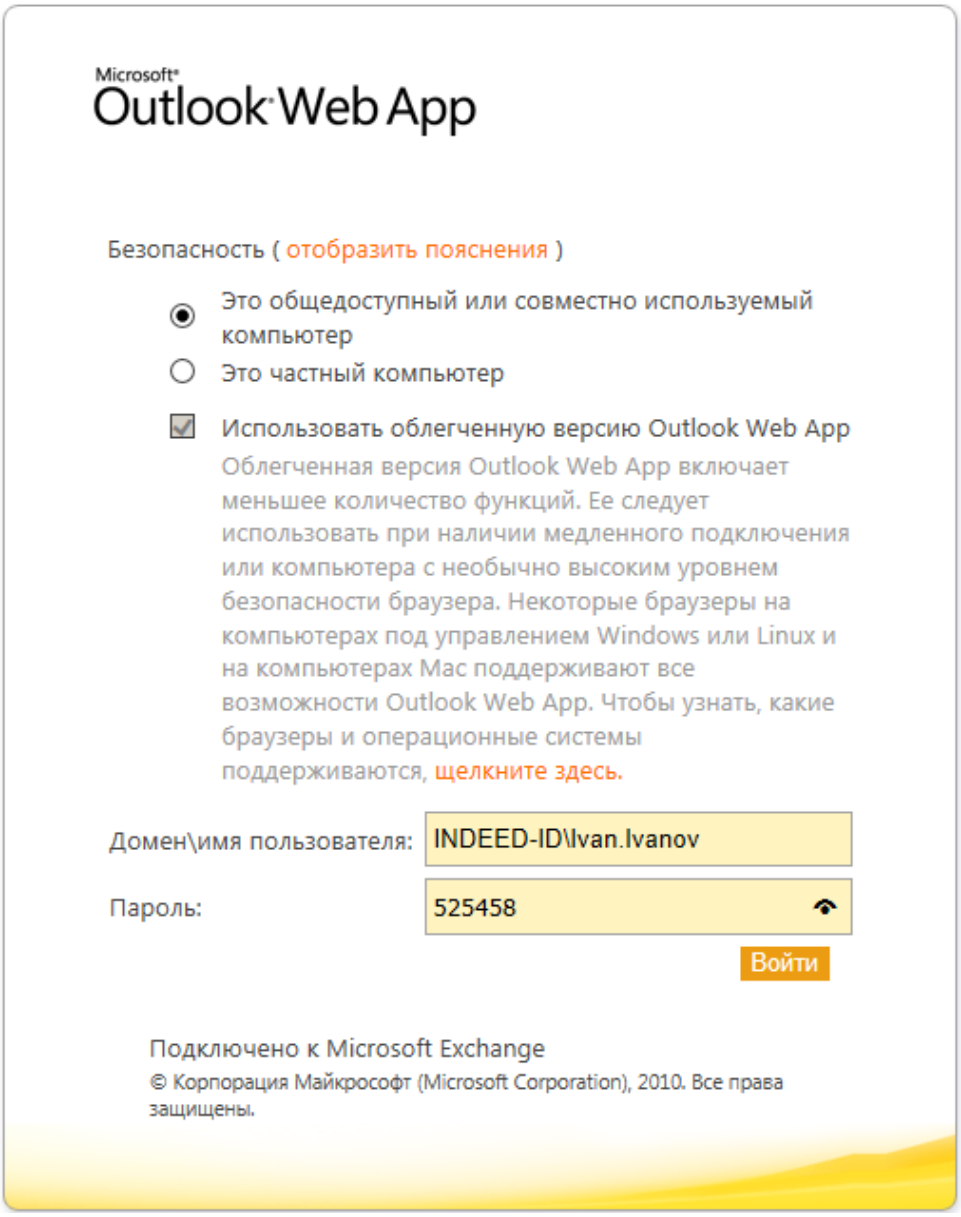

Рисунок 10 – Использование одноразового пароля Google для доступа доменного пользователя в Outlook Web App.

Exchange Active Sync

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение **Microsoft-Server-ActiveSync** и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей...** (Configure Native Modules...), включите модули **Indeed-Id IIS Authentication Module (x64 и x86)** и нажмите **OK**.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

Настройка способов аутентификации, обрабатываемых IIS Extension

Настройка необходима для корректной работы Exchange Active Sync с IIS Extension

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule\IISConfig**.
3. Создайте в ключе IISConfig ключ с точным именем сайта или приложения IIS – **Default Web Site/Microsoft-Server-ActiveSync**.
4. Создайте в этом ключе DWORD значение **IsFormsDisabled =dword:00000001**
   На Рисунке 11 приведен пример настроек в реестре.

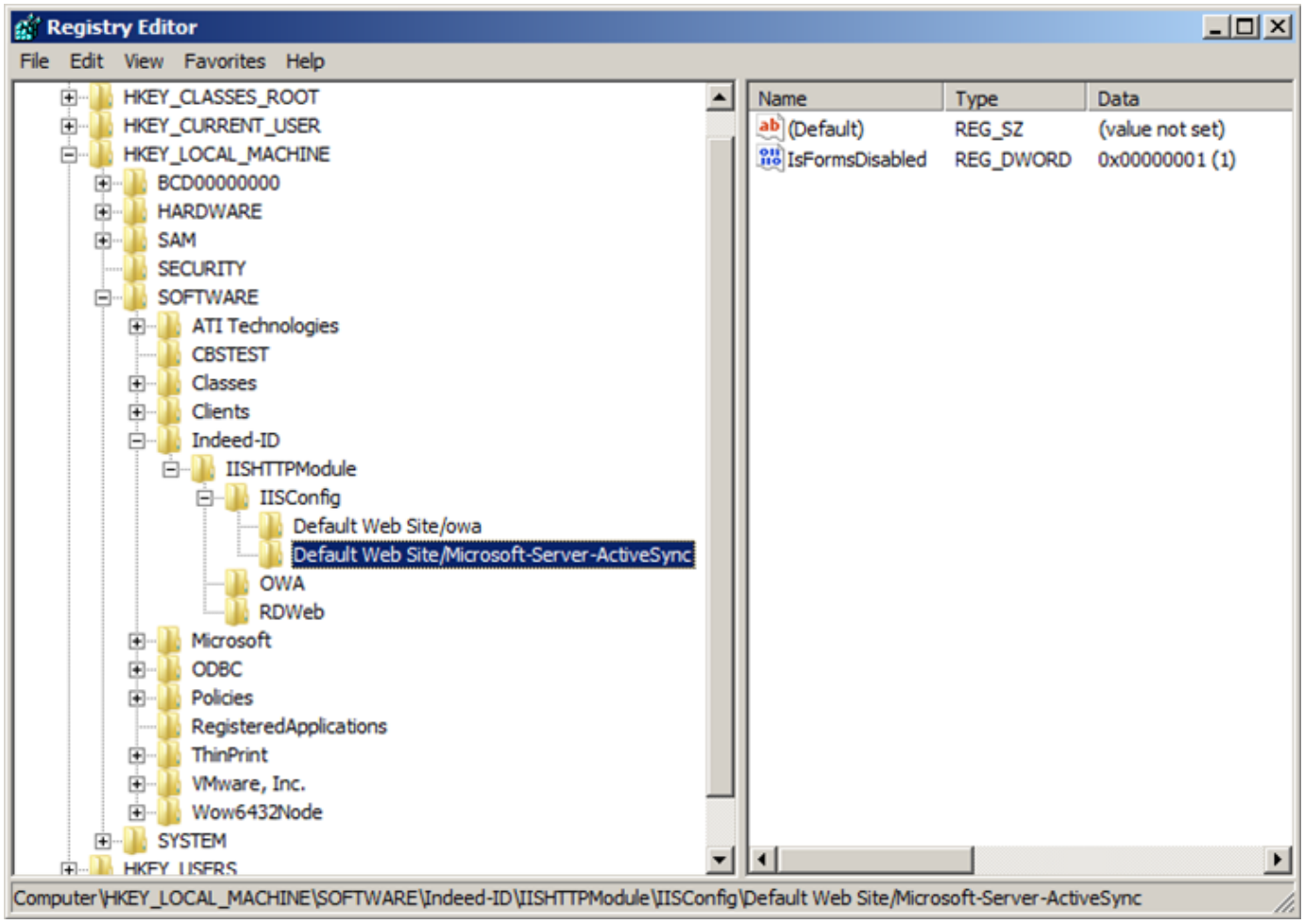

Рисунок 11 – Настройка способов аутентификации, обрабатываемых IIS Extension для Exchange Active Sync.

Настройка работы с заданным провайдером аутентификации Indeed

1. В ветке реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed- ID\IISHTTPModule\IISConfig** перейдите в раздел **Default Web Site/Microsoft-Server-ActiveSync**
2. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру Passcode **{F696F05D-5466-42B4-BF52-21BEE1CB9529}**

На Рисунке 12 приведен пример настроек в реестре для аутентификации с использованием Indeed-Id Passcode Provider. Обе описанные выше настройки приложения Exchange Active Sync в реестре Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\Default Web Site/Microsoft-Server-ActiveSync]
"IsFormsDisabled"=dword:00000001
"ProviderId"="{F696F05D-5466-42B4-BF52-21BEE1CB9529}"
```

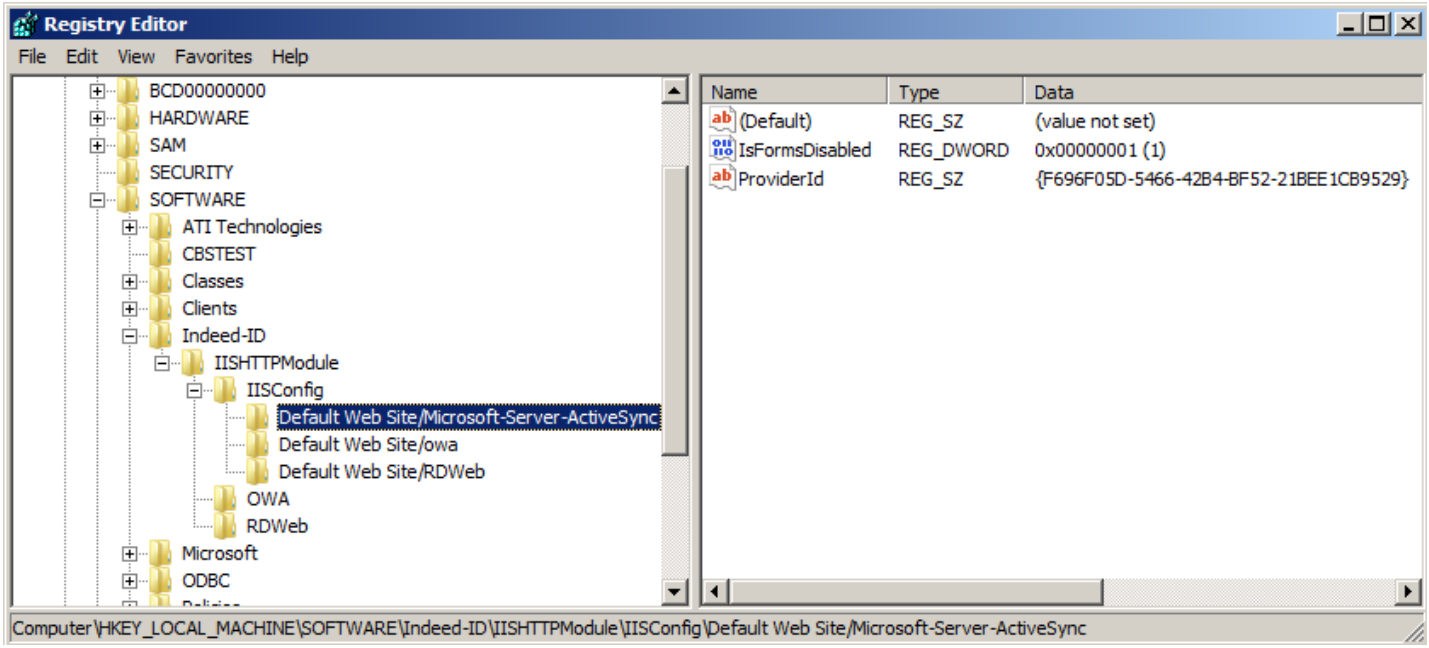

Рисунок 12 – Пример настроек в реестре для Exchange Active Sync для аутентификации с использованием Indeed-Id Passcode Provider.

Remote Desktop Web Access

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение **RDWeb** и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей...** (Configure Native Modules...), включите модули **Indeed-Id IIS Authentication Module (x64 и x86)** и нажмите **OK**.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

Настройка работы с заданным провайдером аутентификации Indeed

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule\IISConfig**.
3. Создайте в ключе IISConfig ключ с точным именем сайта или приложения IIS – **Default Web Site/RDWeb**.
4. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру для данного приложения:
   - **{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

Итого, в разделе **. . . IISConfig\Default Web Site/RDWeb** должны быть следующие параметры (на примере провайдера Email OTP (Рисунок 13):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\Default Web
 Site/RDWeb]
"ProviderId"="{093F612B-727E-44E7-9C95-095F07CBB94B}"
```

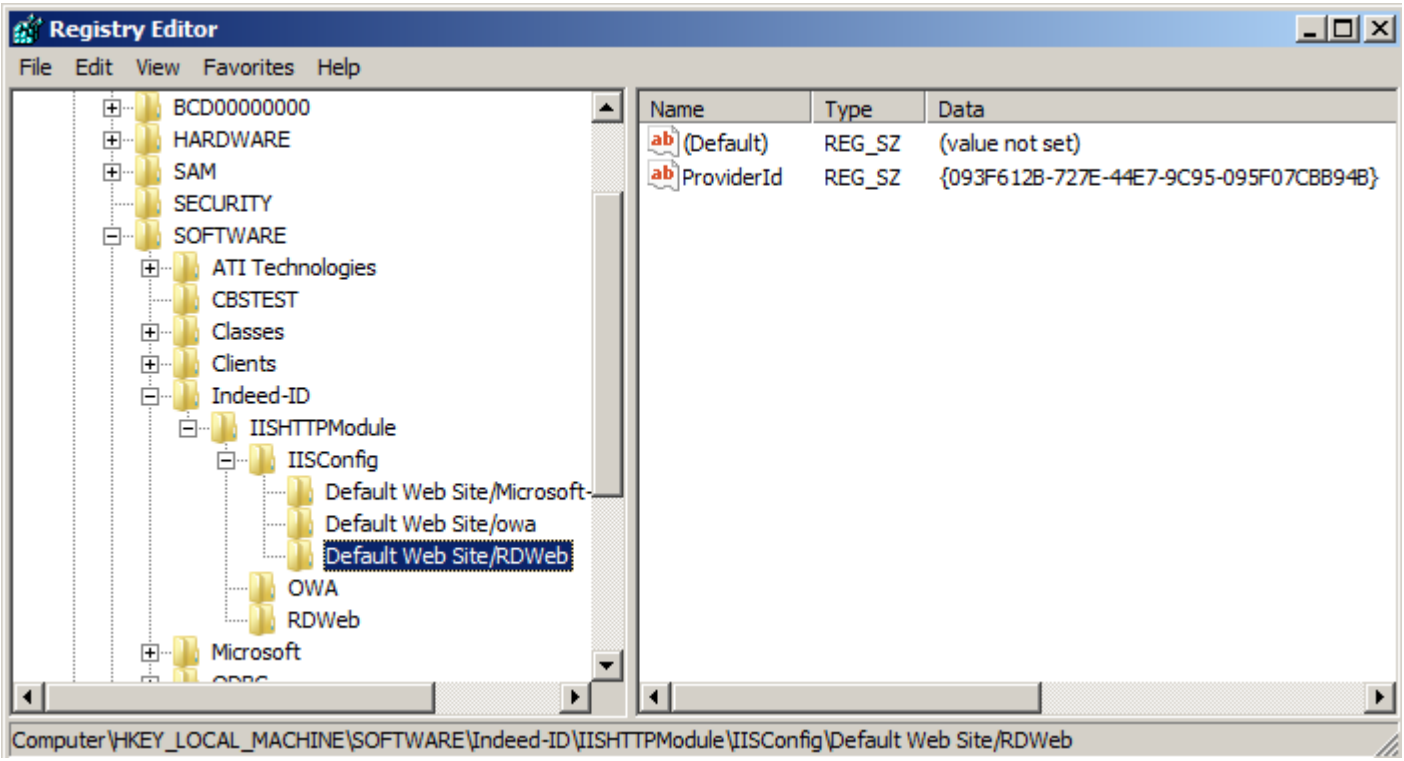

Рисунок 13 – Пример настроек в реестре для Remote Desktop Web Access для аутентификации с использованием Indeed-Id Email OTP Provider.

Настройка проверки подлинности и двухфакторной аутентификации

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule** ключ с именем приложения или сайта в IIS (может иметь произвольное значение).
   Например: **[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\RDWeb]**
3. Создайте следующие параметры и определите их значения (см. **Настройка двухфакторной аутентификации**):
   - **AuthCookie**
   - **IsMFAEnabled**
   - **LoginURL**
   - **OTPURL**
   - **PasswordField**
   - **TargetURL**
   - **UsernameField**
4. В итоге реестр Windows должен содержать следующее (Рисунок 14):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\RDWeb]
"LoginURL"="/RDWeb/Pages/en-US/login.aspx"
"PasswordField"="UserPass"
"UsernameField"="DomainUserName"
"TargetURL"="/RDWeb/Pages/en-US/default.aspx"
"AuthCookie"="TSWAAuthHttpOnlyCookie"
"IsMFAEnabled"=dword:00000001
"OTPURL"="/RDWeb/iidotp.aspx"
```

5. Теперь при подключении через Remote Desktop Web Access пользователи должны будут помимо доменного пароля использовать самостоятельно заданный пароль (в случае использования Indeed-Id Passcode Provider) или одноразовый пароль (SMS OTP, Email OTP или Google Authenticator Provider).
   Ввод дополнительного пароля осуществляется после ввода доменного пароля на странице аутентификации Indeed (Рисунок 15).

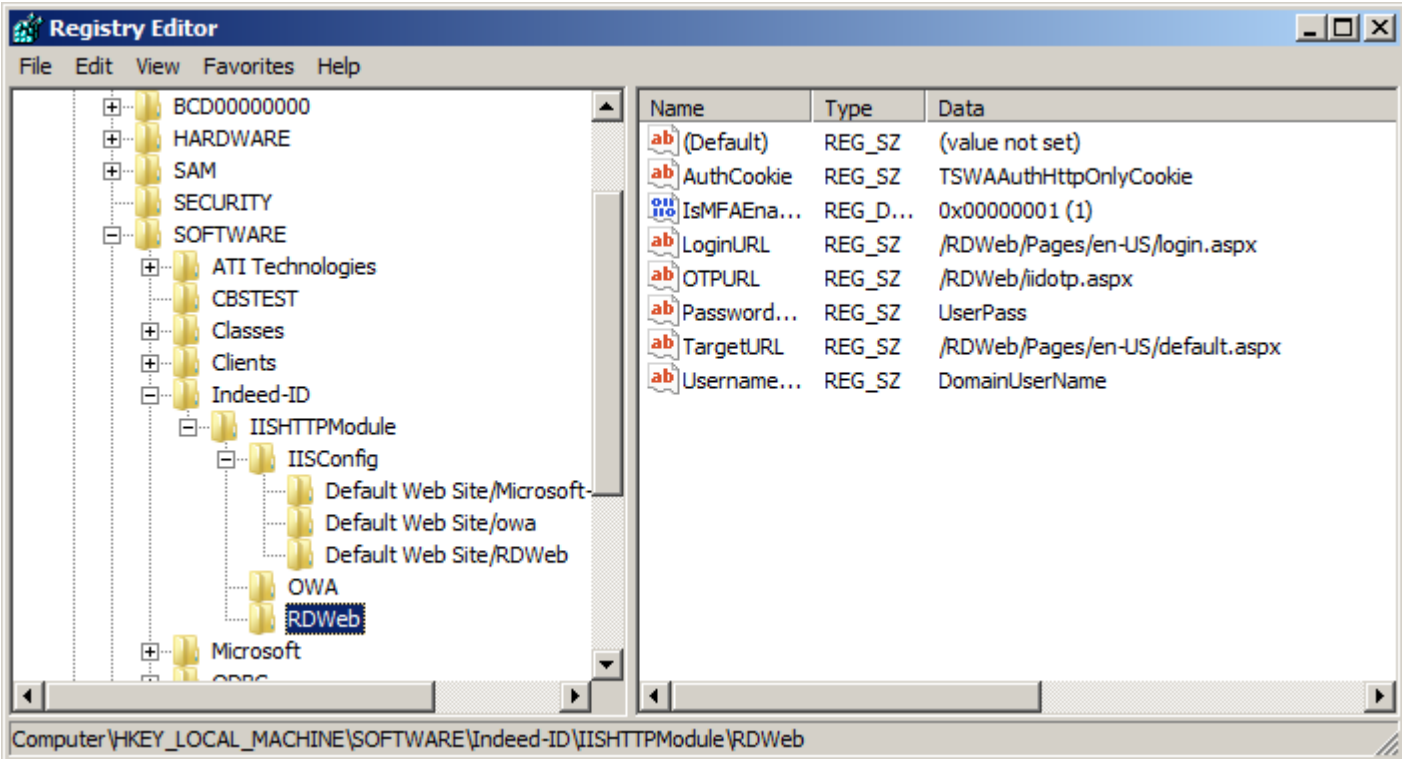

Рисунок 14 – Настройки Indeed IIS Extension для доступа в RD Web Access с использованием двухфакторной аутентификации.

Microsoft Lync/Skype for Business

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение **WebTicket** на **Lync Server External Web Site** и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей. . .** (Configure Native Modules. . .), включите модули **Indeed-Id IIS Authentication Module (x64 и x86)** и нажмите **OK**.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

Настройка работы с заданным провайдером аутентификации Indeed

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule\IISConfig**.
3. Создайте в ключе IISConfig ключ с точным именем сайта или приложения IIS – **Lync Server External Web Site/WebTicket**.
4. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру Passcode **{F696F05D-5466-42B4-BF52-21BEE1CB9529}**

Итого, в разделе **. . . IISConfig\Lync Server External Web Site/WebTicket** должны быть следующие параметры (на примере провайдера Passcode :

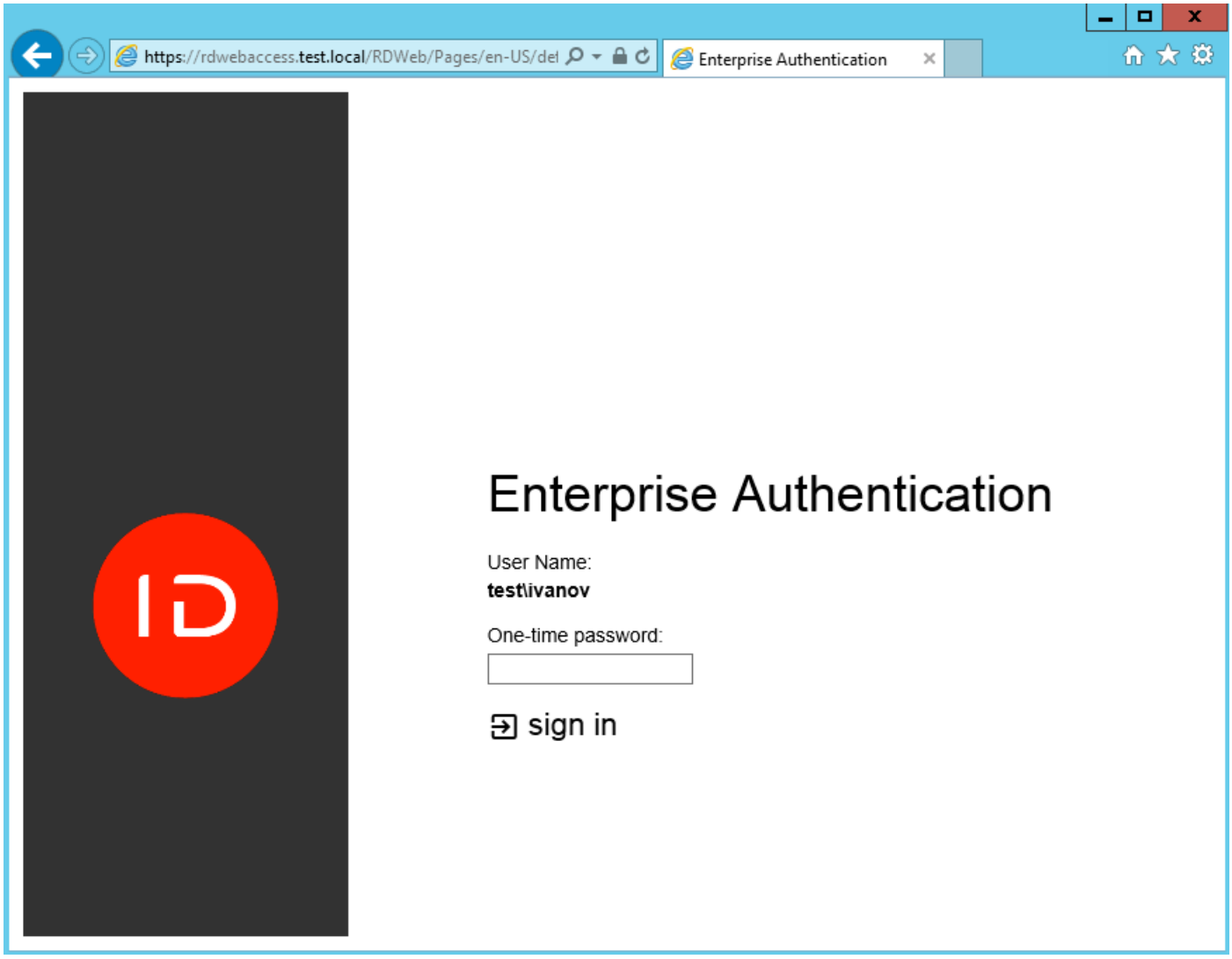

Рисунок 15 – Страница аутентификации Indeed по дополнительному фактору.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\
Lync Server External Web Site/WebTicket]
"ProviderId"="{F696F05D-5466-42B4-BF52-21BEE1CB9529}"
```

Directum

Включение зарегистрированного модуля аутентификации Indeed

1. Откройте в **Диспетчере служб IIS** (IIS Manager) приложение **Directum Web**(для web-версии) или **Directum PDA**(для мобильной версии) и перейдите в раздел **Модули** (Modules).
2. В меню **Действия** (Actions) нажмите **Выполняется настройка собственных модулей...** (Configure Native Modules...), включите модули **Indeed-Id IIS Authentication Module (x64 и x86)** и нажмите **OK**.
3. Перезапустите сервер IIS в **Диспетчере служб IIS** (IIS Manager).

Настройка работы с заданным провайдером аутентификации Indeed

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **IISHTTPModule\IISConfig**.
3. Создайте в ключе IISConfig ключ с точным именем сайта или приложения IIS – **Default Web Site/Directum Web** для web-версии или **Default Web Site/Directum PDA** для мобильной версии.
4. Создайте строковый параметр **ProviderId** и задайте для него значение, соответствующее используемому провайдеру для данного приложения:
   - **{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

Настройка проверки подлинности

1. Выполните вход на сервер с установленным компонентом Indeed IIS Extension с учетной записью, обладающей правами локального администратора.
2. Создайте в разделе реестра Windows **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule** ключ с именем приложения или сайта в IIS (может иметь произвольное значение).

   Например:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\Directum Web] для web-версии
   [HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\Directum PDA] для мобильной версии.
3. Создайте следующие строковые параметры:
   LoginURL – относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
   UsernameField – значение атрибута **name** поля имени пользователя формы входа приложения.
   PasswordField – значение атрибута **name** поля пароля формы входа приложения.
   DomainField – необязательное поле с именем домена, к которому принадлежит пользователь.

В итоге реестр Windows должен содержать следующее:
Для Directum Web:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\Directum Web]
"LoginURL"="/UserLogin.asmx"
"UsernameField"="Username"
"PasswordField"="Password"
"DomainField"="Domain"
```

Для Directum PDA:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\Directum PDA]
"LoginURL"="/pda/Login.aspx"
"UsernameField"="sLogin"
"PasswordField"="sPwd"
"DomainField"="sDomain"
```

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 Single Sign-On. 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.