

Indeed AM IIS Extension

Продукт **Indeed AM IIS Extension** обеспечивает возможность добавления второго фактора аутентификации пользователей в web приложениях, использующих проверку подлинности с помощью форм (**Forms Authentication**), развернутых на платформе **Microsoft Internet Information Services (IIS)** с использованием технологии аутентификации **Indeed**.

Информация

Файлы для Indeed AM IIS Extension расположены: ***indeed AM\Indeed AM IIS Extension\<Номер версии>***

- **Indeed.AM.IIS.Extension-x64.ru-ru.msi** - Пакет для установки Indeed AM IIS Extension.
- **/Misc/Server2008/Indeed.AdminConsole.IIS.Install.MSServer2008.ps1** - Скрипт для установки необходимых компонентов IIS сервера для Windows Server 2008.
- **/Misc/Server2008/NDP452-KB2901907-x86-x64-AllOS-ENU.exe** - Пакет с обновлением Microsoft .NET Framework 4.5.2 для Windows Server 2008.
- **/Misc/Server2012/AccessControlInitialConfig/Indeed.AdminConsole.IIS.Install.MSServer2012.ps1** - Скрипт для установки необходимых компонентов IIS сервера для Windows Server 2012.

Установка и настройка Indeed AM IIS Extension

Информация

Indeed AM 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 поддерживается только для приложений, использующих проверку подлинности с помощью форм (Forms Authentication).

Двухфакторная аутентификация реализована с помощью аутентификации по доменному паролю и по второму фактору – одноразовому паролю.

Информация

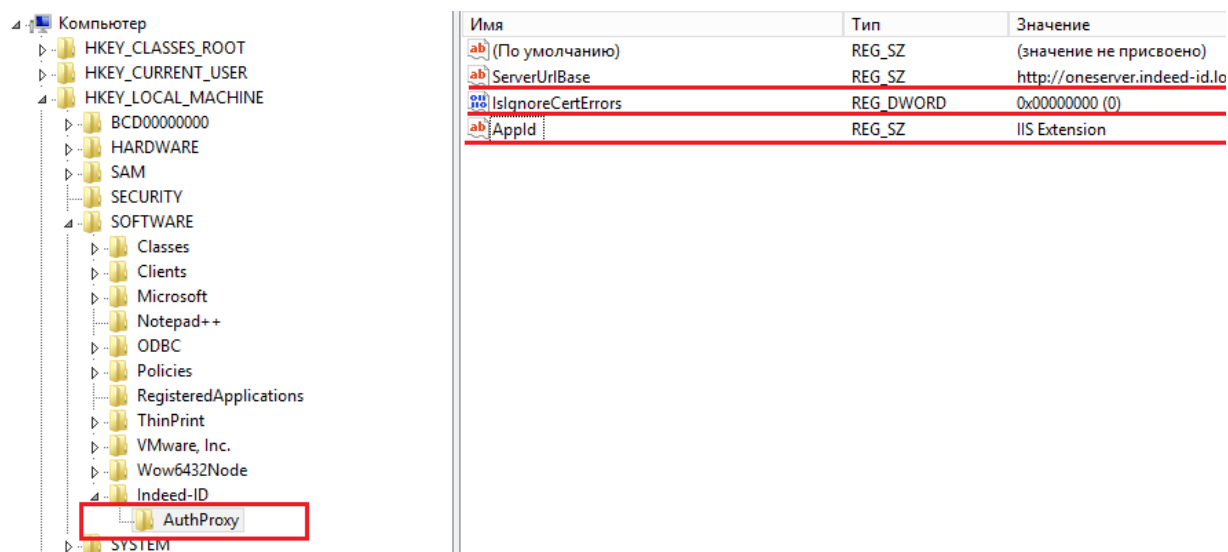
Для использования расширения необходимо установить **Indeed AM Windows Password Provider** на сервер **Indeed AM**.

1. Выполнить установку IIS Extension через запуск инсталлятора **Indeed.AM.IIS.Extension-v1.2.7.x64.ru-ru.msi**.
2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy**. Измените параметры:
 - а. Параметр **ServerUrlBase**. В данном параметре указывается URL Вашего сервера Indeed AM.

Примечание

В настройках приложения, в URL не должно быть символов "/" в конце

- б. Параметр **IgnoreCertErrors** со значением **0**. Данный параметр предназначен для проверки сертификата сервера **Indeed AM**, при значении **1** происходит игнорирование ошибок сертификата.
- с. Параметр **Appld** со значением **IIS Extension**. В данном параметре задается название используемого компонента.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
ServerUrlBase	REG_SZ	http://oneserver.indeed-id.io
IgnoreCertErrors	REG_DWORD	0x00000000 (0)
Appld	REG_SZ	IIS Extension

3. Создайте в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID** ключ **IISHTTPModule**. В созданном ключе создайте:

- а. Строковый параметр **LSUrl**. В данном параметре указывается URL Вашего лог сервера.



Примечание

В настройках приложения, в URL не должно быть символов "/" в конце

- б. Создайте строковый параметр **LSEventCacheDirectory** в значении укажите путь к папке для хранения локального кеша.



Информация

Папка **LSEventCacheDirectory** должна быть доступна для всех пользователей **IIS Extension**.

- с. Строковый параметр **ProviderId**. Укажите **ID** провайдера который будет использоваться при аутентификации.



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**

Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
COMPONENTS
HARDWARE
SAM
Schema
SECURITY
SOFTWARE
Classes
Clients
Indeed-ID
AuthProxy
IISHTTPModule
Exchange
iisconfig
Logging

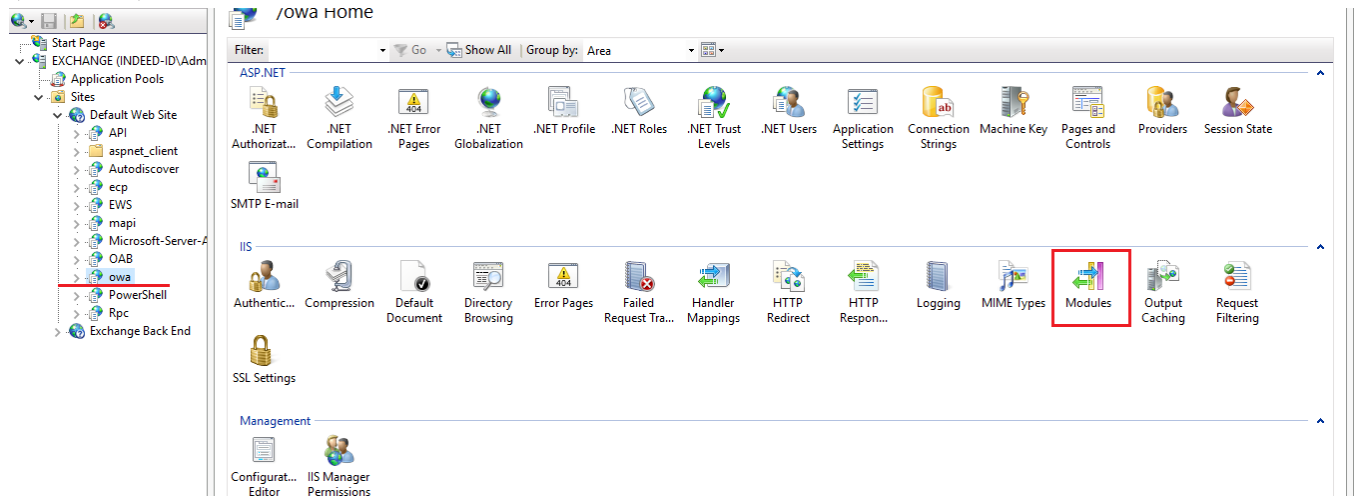
Name	Type	Data
(Default)	REG_SZ	(value not set)
LSEventCacheDi...	REG_SZ	\\IIS\Users\Public\Documents\LocalCache
LSUrl	REG_SZ	http://dc.demo.local/ils/api
ProviderId	REG_SZ	{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

Настройка IIS.

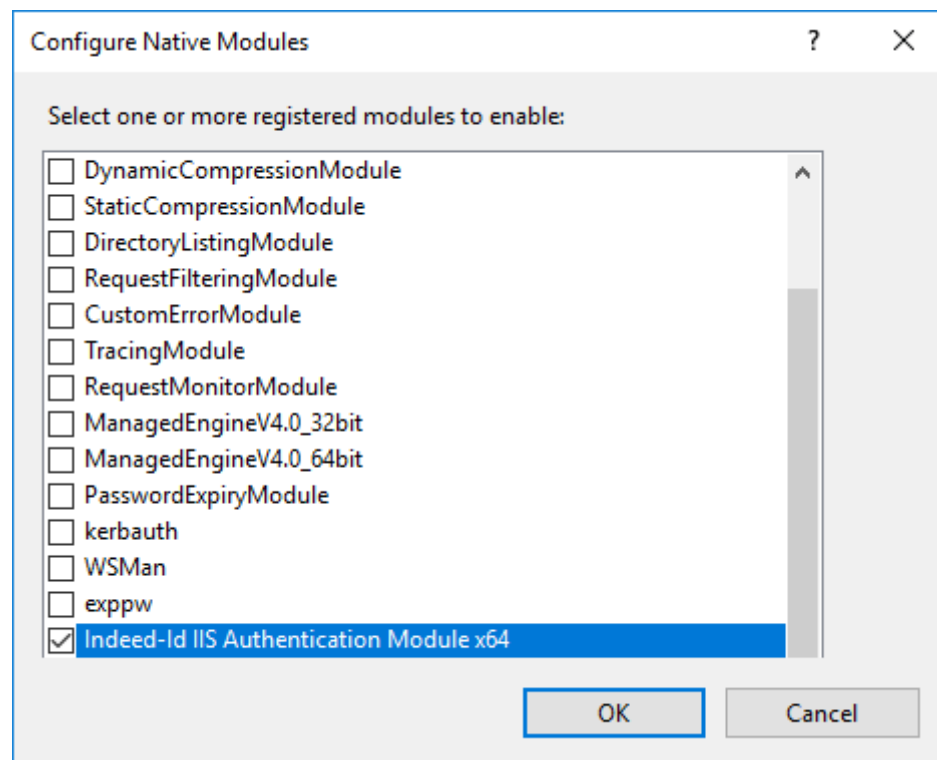
Информация

В данном руководстве рассмотрен пример настройки для Exchange 2016.

1. Откройте в **Диспетчере служб IIS (IIS Manager)** приложение (для Outlook Web Access – это owa), которое будет использовать **IIS Extension** и перейдите в раздел **Модули (Modules)**.



2. В меню Действия (Actions) нажмите **Выполняется настройка собственных модулей...** (Configure Native Modules...), включите модули Indeed и нажмите Ок.

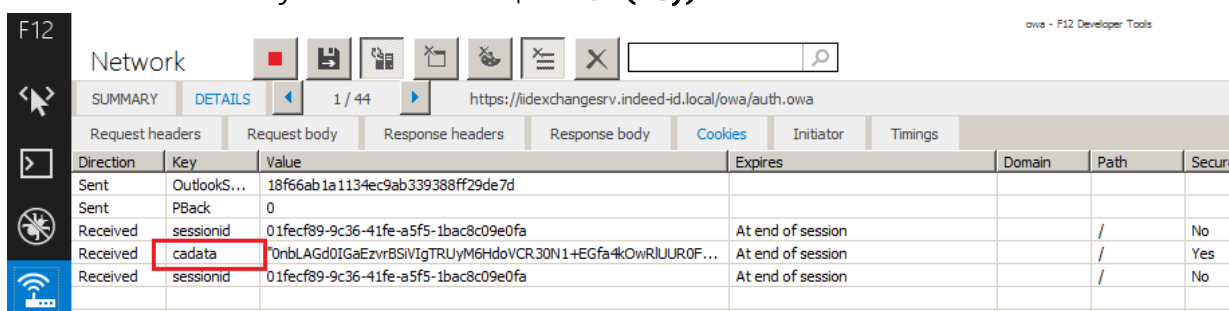


Настройка компонента

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:

1. **AuthCookie** – Строковый параметр. 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 **Cookie (Cookies)**.
- Искомое значение указано в столбце **Ключ (Key)**.



- isMFAEnabled** – DWORD параметр. Включение двухфакторной аутентификации.
- LoginURL** – Строковый параметр. Относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
- MatchTargetRedirect** - DWORD параметр. При значении 1, страница для ввода второго фактора отображается до перехода на основную страницу. Целевая страница не сохраняется в буфере, после ввода второго фактора происходит редирект на основную страницу (Параметр: TargetURL).
- OTPURL** – Строковый параметр. 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.
- PasswordField** – Строковый параметр. Значение атрибута name поля пароля формы входа приложения.
- RedirectToTarget** - DWORD параметр. Редирект на целевую страницу.

8. TargetURL – Строковый параметр. URL целевой страницы, на которую пользователь попадает после аутентификации в приложении.



Информация

Для Exchange 2013 и 2016 указывается **"/owa"** (без завершающего /), для Exchange 2010 указывается **"/owa/"** (с завершающим /)

9. UsernameField – Строковый параметр. Значение атрибута name поля имени пользователя формы входа приложения.

Значения всех параметров: **LoginURL, PasswordField, UsernameField** содержатся в форме аутентификации целевого приложения могут быть получены, например, при помощи инструмента Internet Explorer F12 Developer Tools.

```

└─ <body class="owaLgnBdy">
  └─ <noscript>...</noscript>
  └─ <form name="logonForm" action="/owa/auth.owa" enctype="application/x-www-form-urlencoded"
    <input name="destination" type="hidden" value="https://iidexchangesrv.indeed-id.1"
    <input name="flags" type="hidden" value="0"></input>
    <input name="forcedownlevel" type="hidden" value="0"></input>
  └─ <table align="center" id="tblMain" cellspacing="0" cellpadding="0">
    └─ <tbody>
      └─ <tr>...</tr>
      └─ <tr>
        └─ <td id="mdLft"></td>
        └─ <td id="mdMid">
          └─ <table class="mid" id="tblMid">
            └─ <tbody>
              └─ <tr>...</tr>
              └─ <tr>...</tr>
              └─ <tr>...</tr>
              └─ <tr>...</tr>
              └─ <tr>...</tr>
              └─ <tr>...</tr>
            └─ <tr>
              └─ <td>
                └─ <table class="nonMSIE">
                  └─ <colgroup>...</colgroup>
                  └─ <tbody>
                    └─ <tr>
                      └─ <td nowrap="">...</td>
                      └─ <td class="txtpad">
                        <input name="username" class="txt" id="username" type="password" value="" />
                      </td>
                    </tr>
                    └─ <tr>
                      └─ <td nowrap="">...</td>
                      └─ <td class="txtpad">
                        <input name="password" class="txt" id="password" type="password" value="" />
                      </td>
                    </tr>
                  </tbody>
                </table>
              </td>
            </tr>
          </tbody>
        </td>
      </tr>
    </tbody>
  </table>

```

LoginURL

UsernameField

PasswordField

Computer		
HKEY_CLASSES_ROOT		
HKEY_CURRENT_USER		
HKEY_LOCAL_MACHINE		
BCD00000000		
COMPONENTS		
HARDWARE		
SAM		
Schema		
SECURITY		
SOFTWARE		
Classes		
Clients		
Indeed-ID		
AuthProxy		
IISHTTPModule		
Exchange		
iisconfig		
Logging		

Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthCookie	REG_SZ	cadata
IsMFAEnabled	REG_DWORD	0x00000001 (1)
LoginURL	REG_SZ	/owa/auth.owa
MatchTargetRe...	REG_DWORD	0x00000001 (1)
OTPURL	REG_SZ	/owa/iidotp.aspx
PasswordField	REG_SZ	password
RedirectToTarget	REG_DWORD	0x00000000 (0)
TargetURL	REG_SZ	/owa
UsernameField	REG_SZ	username

Информация

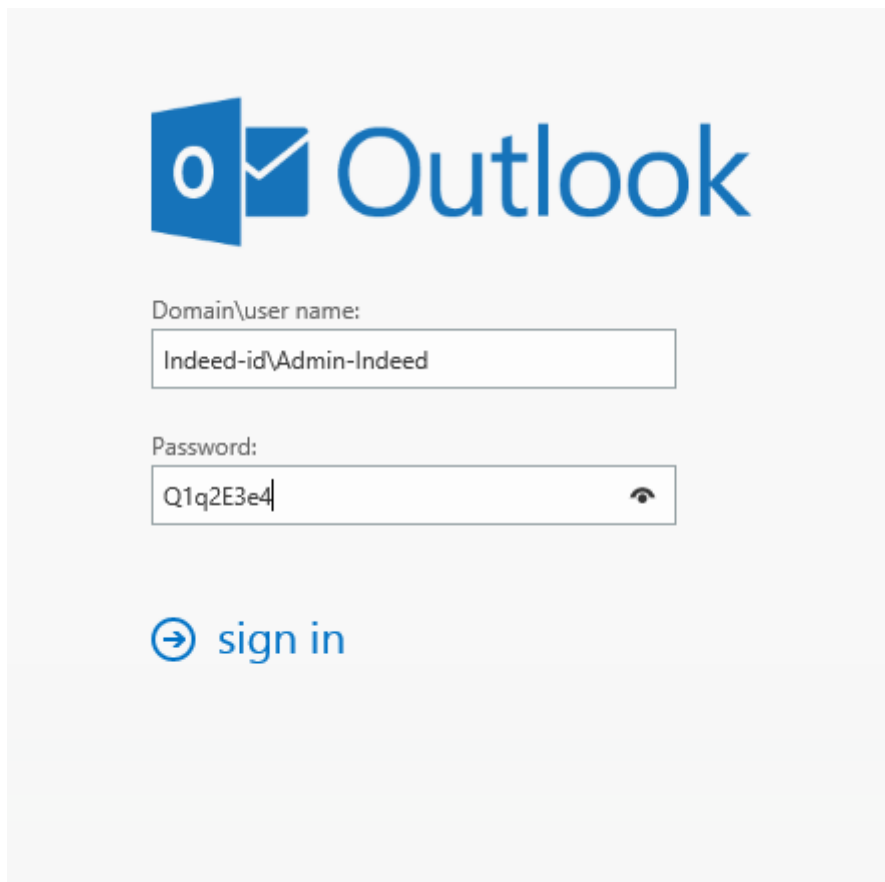
Для приложения OWA необходимо в реестре отключить **Basic** аутентификацию. Создайте DWORD параметр: "**IsBasicDisabled**" со значение "**1**", по пути: HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\owa

Пример работы расширения.

Информация

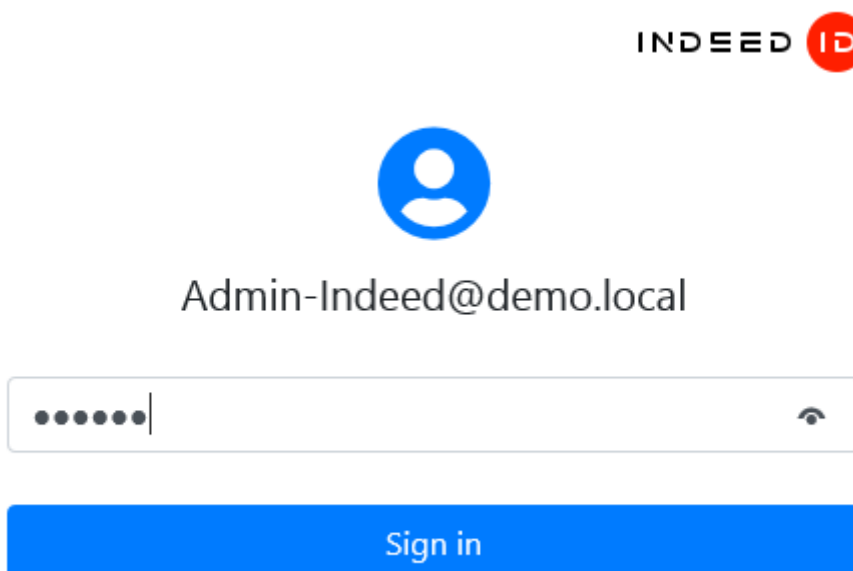
В IIS Extension не поддерживается настройка входа в OWA по "**User name only**".

1. Открыть приложение OWA и ввести доменный логин/пароль.



The image shows the Outlook login interface. At the top is the Outlook logo. Below it, there are two input fields. The first is labeled 'Domain\user name:' and contains the text 'Indeed-id\Admin-Indeed'. The second is labeled 'Password:' and contains the text 'Q1q2E3e4'. Below the password field is a blue circular icon with a right-pointing arrow and the text 'sign in'.

2. После корректного ввода появится окно с запросом второго фактора.



The image shows the second factor authentication screen. At the top right is the 'INDEED ID' logo. In the center is a blue circular icon with a white person silhouette. Below it is the email address 'Admin-Indeed@demo.local'. At the bottom is a blue button with the text 'Sign in'.

3. После успешного ввода откроется приложение.

