

Indeed SAML idp



Информация

По умолчанию Indeed SAML idp настроен на использование Windows аутентификации, для вне доменных сценариев требуется включить анонимную аутентификацию в IIS для iidsamlidp.



Информация

Файлы для indeed SAML idp расположены: *indeed AM 7\Indeed SAML idp \<Homep версии>*

- **EA.SAMLidP-v7.1.0.x64.ru-ru.msi** - Пакет для установки indeed SAML idp.
- **/Misc/Server2012/Indeed.SAML.IIS.Install.MSServer2012.ps1** - Скрипт для установки необходимых компонентов IIS сервера для Windows Server 2012.

Установка

1. Выполнить установку Indeed SelfService через запуск инсталлятора **EA.SAMLidP-v7.1.0.x64.ru-ru.msi**
2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.



Информация

Indeed SelfService является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для SAML idp.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Редактирование конфигурационного файла

1. Откройте конфигурационный файл SAML idp **Web.config** (C:\inetpub\wwwroot\iidservice\Web.config).
2. Укажите **URL** для подключения к серверу **Indeed** для параметра **Url** в тэге **amAuthServer**.
 - a. **Параметр Url** - url адрес сервера Indeed в формате **http(s)://полное_dns_имя_сервера/easerver/**



Информация

Для игнорирования ошибок сертификата сервера необходимо изменить параметр **"IsIgnoreCertErrors"** на значение **"true"** в файле **"applicationSettings.config"** (iidsamlidp\Config).

Пример

```
<amAuthServer Url="https://amserv.indeed-id.local/easerver"/>
```

3. В тэге **amAuthMethods** укажите ID провайдера в формате:

- a. Если для входа используется 1 провайдер.

Пример

```
<amAuthMethod id="SMSOTP"> <amAuthProviders> <amAuthProvider  
id="ebb6f3fa-a400-45f4-853a-d517d89ac2a3" /> <  
/amAuthProviders> </amAuthMethod>
```

- b. Если для входа используется несколько провайдеров.

Пример

```
<amAuthMethod id="HOTP_Passcode_SMS"> <amAuthProviders>  
<amAuthProvider id="AD3FBA95-AE99-4773-93A3-6530A29C7556" />  
<amAuthProvider id="F696F05D-5466-42b4-BF52-21BEE1CB9529" />  
<amAuthProvider id="ebb6f3fa-a400-45f4-853a-d517d89ac2a3" /> <  
/amAuthProviders> </amAuthMethod>
```

- Параметр **id** тега **amAuthMethod** - Произвольное уникальное значение.
- Параметр **id** тега **amAuthProvider** - id используемого провайдера.



Параметр **id** тега **amAuthProvider** 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**

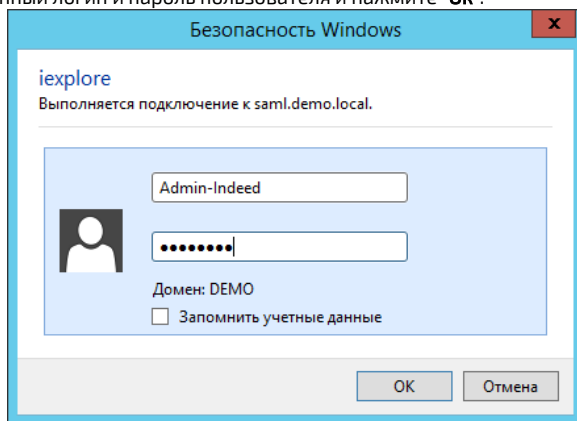
{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software TOTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

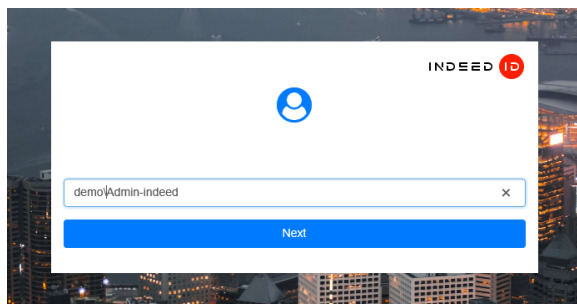
{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

Пример работы расширения

1. Для аутентификации в SAML откройте URL **http(s)://полное_имя_сервера/iidsamlidp/**
2. Введите доменный логин и пароль пользователя и нажмите "Ок".



3. В появившемся окне аутентификации SAML введите имя пользователя в формате: **Имя_домена\имя_пользователя** и нажмите "Next".

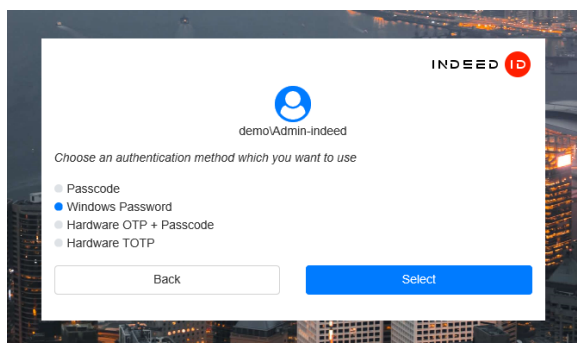


4. Выберите способ аутентификации и нажмите **"Select"**.



Информация

Если у пользователя нет обученного аутентификатора, то выберите **"Windows Password"**.



5. Введите пароль и нажмите **"Sing In"**. Если ввод данных был успешный, то произойдет вход.

