Indeed AM Self Service

Indeed AM Self Service - это Web-приложение, которое работает на базе IIS. В данном модуле пользователь может осуществлять управление своими аутентификаторами.

Информация

Файлы для indeed AM Self Service расположены: *indeed AM <Homep версии>\Indeed AM Self Service\<Homep версии>*

• Indeed.SelfService-<номер версии>.x64.ru-ru.msi - Пакет для установки Indeed AM Self Service.

Установка

1. Выполнить установку Indeed AM Self Service через запуск пакета для установки Indeed AM Self Service.

🗥 Информация

Опциональная настройка. Генерация сертификата необходима при аутентификации в Indeed AM Self Service с использованием Indeed AM SAML IDP Provider.

Данный сертификат не предназначен для организации SSL соединения.

Если данный сертификат был сгенерирован ранее, то необходимо убрать флажок.

По завершению установки будет предложено сгенерировать новый IDP сертификат. Если флажок будет выставлен, то сгенерируется и установится в хранилище сертификатов (*Local Machine -> Personal*) новый самоподписанный сертификат. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.

 \times

😹 Программа установки Indeed Self Service x64



2. Добавить привязку https в настройках Default Web Site в IIS Manager.

🛈 Информация

Self Service 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 Self Service.

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

Настройка

🛈 Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

По умолчанию компонент **Indeed AM Self Service** настроен на использование SAML аутентификации, при необходимости можно настроить прозрачную Windows аутентификацию.

Аутентификация с Windows Authentication

- Откройте конфигурационный файл Self Service Web.config (C: \inetpub\wwwroot\iidselfservice\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 "**islgnoreCertErrors**" на значение "**true**" в файле "**applicationSettings. config**" (iidselfservice\Config).

Пример

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

- 3. Откройте IIS Manager, выберете "Default Web Site" и откройте приложение "iidselfservice".
- 4. Откройте "Проверка подлинности" и включите следующие методы:
 - а. Олицетворение ASP.NET.
 - b. Проверка подлинности Windows.

Проверка подлинности

Сгруппировать по: Без группирования 🔹				
Имя	Состояние	Тип ответа		
Анонимная проверка подлинности	Отключен			
Обычная проверка подлинности	Отключен	Вызов НТТР 401		
Олицетворение ASP.NET	Включен			
Проверка подлинности Windows	Включен	Вызов НТТР 401		
Проверка подлинности с помощью форм	Отключен	Вход-перенаправлени		

- 5. Отключите все остальные методы.
- 6. Откройте конфигурационный файл Self Service **Web.config** (**C**: **\inetpub\wwwroot\iidselfservice\Web.config**).
- 7. Для тега "amAuthentication" в параметре "mode" укажите "Windows".

🛈 Информация

Параметр "loginUrl" оставьте без изменений, при использовании Windows аутентификации данный параметр не учитывается.

Пример

<amAuthentication mode="Windows" loginUrl="" enableLogout="true" />

 Перезапустите IIS сервер. SelfService будет доступен по адресу: "http(s):// полное_dns_имя_cepвepa/iidselfservice/".

Аутентификация с помощью SAML idp

- 1. Откройте конфигурационный файл Self Service Web.config (C:

 \inetpub\wwwroot\iidselfservice\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 "**islgnoreCertErrors**" на значение "**true**" в файле "**applicationSettings. config**" (iidselfservice\Config).

Пример

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

- 3. В теге amAuthentication выполните следующие:
 - **а.** В параметре **mode** укажите значение **Saml**.
 - **b.** В параметре **loginUrl** кажите **URL** в формате http(s)://полное_dns_имя_сервера /iidsamlidp/ для подключения к серверу **Indeed SAML**.

<amAuthentication mode="Saml" loginUrl="http://saml.demo.local/iidsamlidp"/>

c. В параметре identityProviderCertificateThumbprint укажите отпечаток сертификата Indeed AM Saml Idp. Сертификат необходимо экспортировать без закрытого ключа с сервера SAML на сервер с Indeed AM Self Service. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата Saml Idp через PS

Get-Childitem Cert:\LocalMachine\My\ | Where-Object {\$_.Subject -eq "CN=idp"}

- **d.** В параметре **serviceProviderCertificateThumbprint** укажите отпечаток сертификата IDP клиента Indeed AM Self Service, который был сгенерирован при установке.
 - 🛈 Информация

Сертификат устанавливает в хранилище сертификатов (*Local Machine -> Personal*) с общем именем "**ucsp**".

Получить отпечаток можно с помощью Power Shell запроса:

Get-Childitem Cert:\LocalMachine\My\ | Where-Object {\$_.Subject -eq "CN=ucsp"}

e. Параметр enableLogout (Не обязательный) - включает возможность выполнять выход из Self Service.

Пример

<amAuthentication mode="Saml" loginUrl="https://logserver.indeed.local/iidsamlidp/" identityProviderCertificateThumbprint=" C72DF64AE6E039445C8ED53FD83F75A9A2BA37E9" serviceProviderCertificateThumbprint=" 3A1663D905E543782DD84B50391DEBC5178269D7" enableLogout="true"/>

- 4. Откройте конфигурационный файл Indeed AM Saml Idp Web.config (C:

 \inetpub\wwwroot\iidsamlidp\Web.config).
 - а. В тегt **amPartnerServiceProviderSettings** укажите следующие:
 - i. В параметре **SelfServiceUrl** укажите URL сервера с компонентом Indeed AM Self Service в формате http(s)://полное_dns_имя_cepвepa/iidselfservice/
 - В параметре SelfServiceCertificateThumbprint укажите отпечаток сертификата Indeed AM Self Service. Сертификат необходимо экспортировать без закрытого ключа с сервера Indeed AM Self Service на сервер с Indeed AM Saml Idp. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата Admin Console через PS

Get-Childitem Cert:\LocalMachine\My\ | Where-Object {\$_.Subject -eq "CN=ucsp"}

Пример

<amPartnerServiceProviderSettings SelfServiceUrl="https://server.indeed.local/iidselfservice/" EmcServiceUrl="" SelfServiceCertificateThumbprint=" 3A1663D905E543782DD84B50391DEBC5178269D7" EmcCertificateThumbprint=""/>

5. Сохраните изменения в конфигурационных файлах и перезапустите IIS сервера с Indeed AM Saml и с Indeed AM Self Service.

Вход в Self Service с использованием SAML

1. Откройте в браузере Web интерфейс консоли Self Service.

2. В появившемся окне аутентификации SAML нажмите "**Back**" для выбора способа аутентификации, по умолчанию используется последний используемый способ.





Enter the windows password

Enter the windows password

Back

Next

3. Выберите способ аутентификации и нажмите "Select".

🛈 Информация

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

🗥 Информация

Выход в сессии пользователя из SAML idp не влечет за собой выход пользователя из Self Service, до перезапуска браузера или истечения срока хранения cookie. Время хранения cookie для SAML idp - 30 минут.



Способ входа Passcode Windows Token Passcode

Passcode



Choose an authentication method you want to use

- Passcode
- Windows Password + Passcode
- Hardware OTP + Passcode
- Hardware TOTP

Select

4. Введите пароль и нажмите "**Sing in**". Если ввод данных был успешный, то отобразится карточка пользователя.

16.05.2019 11:35:45

	Admin Indeed		
	Имя учетной записи	Admin-Indeed@demo.local	
	Путь	demo.local/Users/Admin Indeed	
	E-mail	Admin-Indeed@demo.local	
	Телефон		
История входов	Аутентификаторы (2)		
Модуль		Время входа	
Self Service		16.05.2019 15:44:54	
Enterprise Managem	ent Console	16.05.2019 14:53:39	
SAML Identity Provid	ler	16.05.2019 13:15:48	

RDP Windows Logon

5. Для выхода из Self Service выполните:

\land Информация

Данная опция будет активна если в пункте 3.b раздела "**Установка**", был настроен параметр **enableLogout**. По умолчанию отключена.

- а. Нажмите на имя пользователя в верхней части окна.
- b. Выберите "**Выйти**" из выпадающего списка.

🛈 Информация		
При выходе из Self Service происходит автоматический выход из SAML idp.		
	DEMOVAdmin-Indeed - Рус Быйти	
	Вы успешно вышли из сервиса самообслуживания Indeed Enterprise Authentication.	
	Войти	