Indeed AM ADFS Extension (2016)

Компонент **ADFS Extension** реализует провайдер мультифакторной аутентификации для сервера **Microsoft ADFS**, добавляя в процесс получения доступа второй фактор.

> **Информация**
>
> Файлы для Indeed AM ADFS Extension расположены: ***indeed AM <Номер версии>\Indeed AM ADFS Extension\<Номер версии>***
>
> - **IndeedId.ADFS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed ADFS Extension.

Установка и настройка ADFS Extension.

1. Выполнить установку ADFS Extension через запуск пакета для установки Indeed ADFS Extension.

2. Создайте конфигурационный файл **MFAAdapter.json**, содержащий следующие параметры.

> **Информация**
>
> **ModeId** 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**
>
> {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} **- AirKey Provider**

Пример

```
{
"ServerType":"eaNet",
"EANetServerURL":"http://YourDomainName/easerver/",
"ModeId":"{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}",
"LSEventCacheDirectory": "C:\\EventCacheEa\\"
}
```

> **Информация**
>
> При использовании https соединения требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

3. Запустите **PowerShell** с правами администратора. Для регистрации адаптера введите следующие данные:

   Информация

   YourPath\MFAAdapter.json - укажите свой полный путь к конфигурационному файлу созданному ранее.

   Информация

   В переменной **$typeName**, в параметре **Version** указывается номер версии используемого **Indeed ADFS Extension.**

   Пример

   ```
   $typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter, IndeedId.ADFS.MFAAdapter, Version=1.0.6.0, Culture=neutral, PublicKeyToken=1ebb0d9282100d91"
   Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id MFA Adapter" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
   ```

4. Для удаления адаптера необходимо выполнить следующую команду:

   Пример

   ```
   Unregister-AdfsAuthenticationProvider -Name "Indeed Id MFA Adapter"
   ```

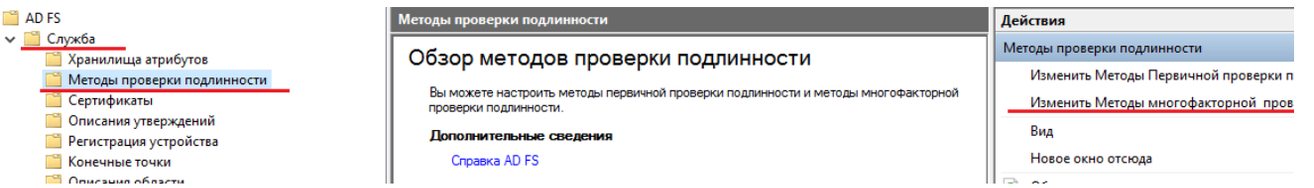
5. Для обновления конфигурации необходимо выполнить следующую команду:

   Пример

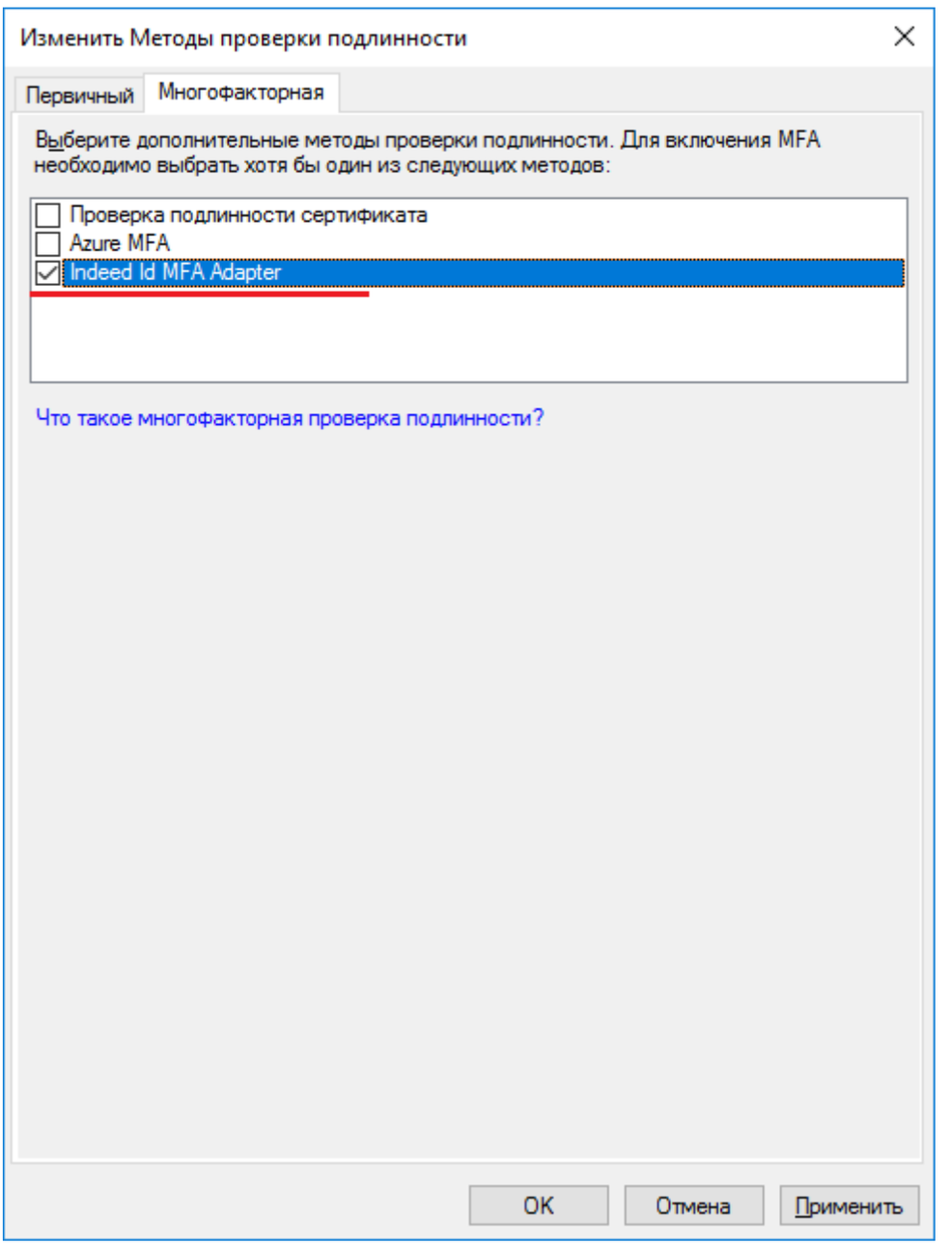
   ```
   Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter" -FilePath 'YourPath\MFAAdapter.json'
   ```

Включение многофакторной аутентификации для ADFS.

1. Откройте консоль управления AD FS.
2. Выберите "**Служба Методы проверки подлинности**", в окне "**Действия**" выберите "**Изменить Методы многофакторной проверки...**"



3. В вкладке "**Многофакторная**" выберите созданный ранее провайдер и нажмите "**Применить**".



4. Для применения изменений перезапустите службу AD FS.

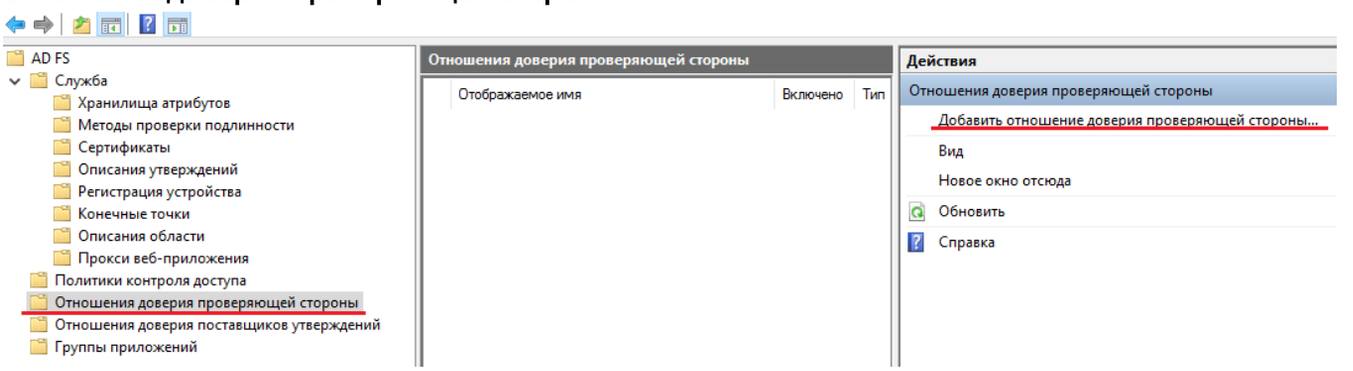
Пример работы расширения.

Пример работы расширения на idpinitiatedsignon странице ADFS

> **Информация**
>
> Пример работы расширения показан на странице ADFS **idpinitiatedsignon.htm**. По умолчанию данная страница не настроена (Настройка данной страницы не обязательна).

Настройка тестовой страницы

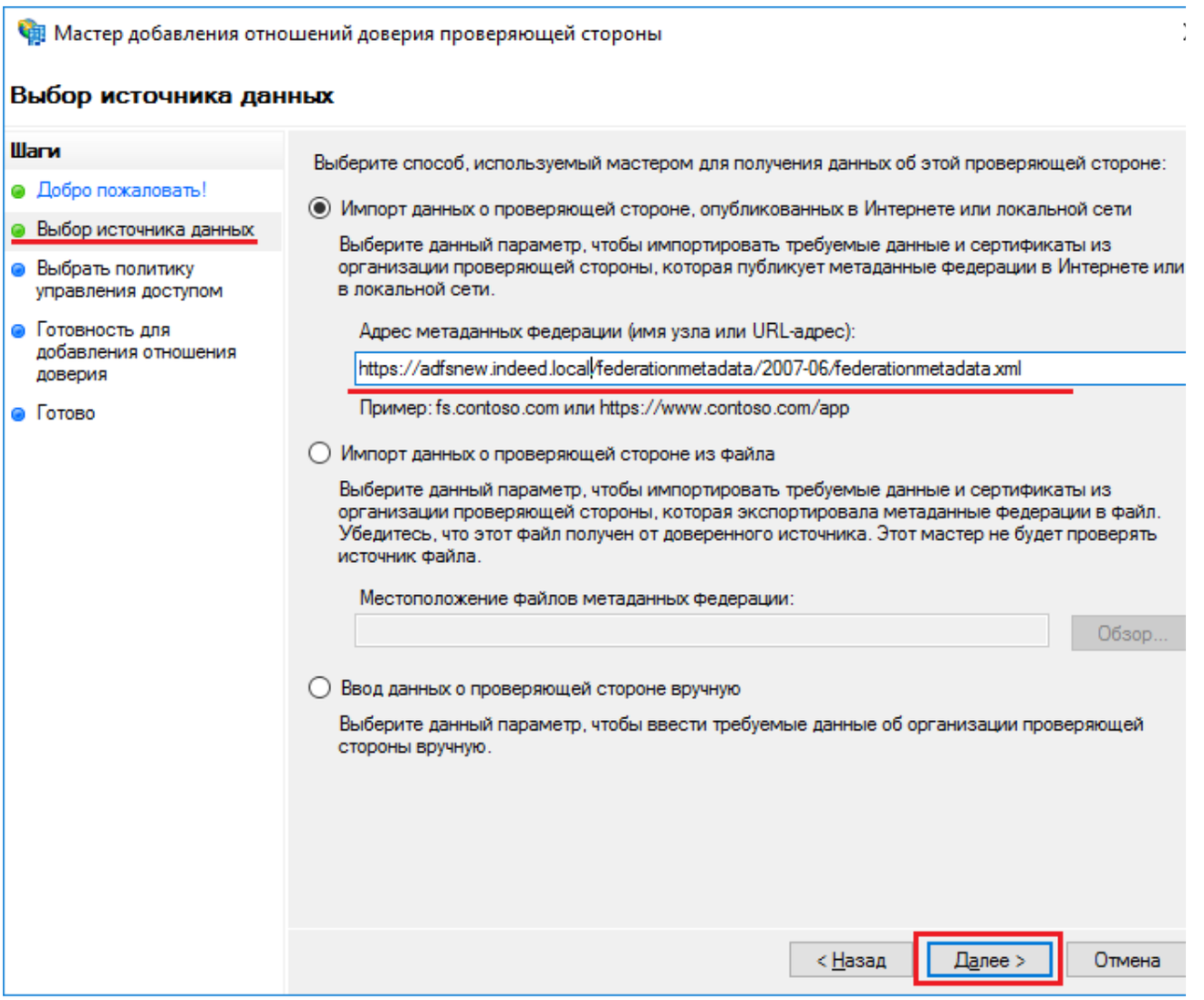
1. Выберите "**Отношение доверия проверяющей стороны**" и нажмите "**Добавить отношение доверия проверяющей стороны...**".



2. На вкладке "**Добро пожаловать!**" выберите "**Поддерживающие утверждения**" и нажмите "**Запустить**".

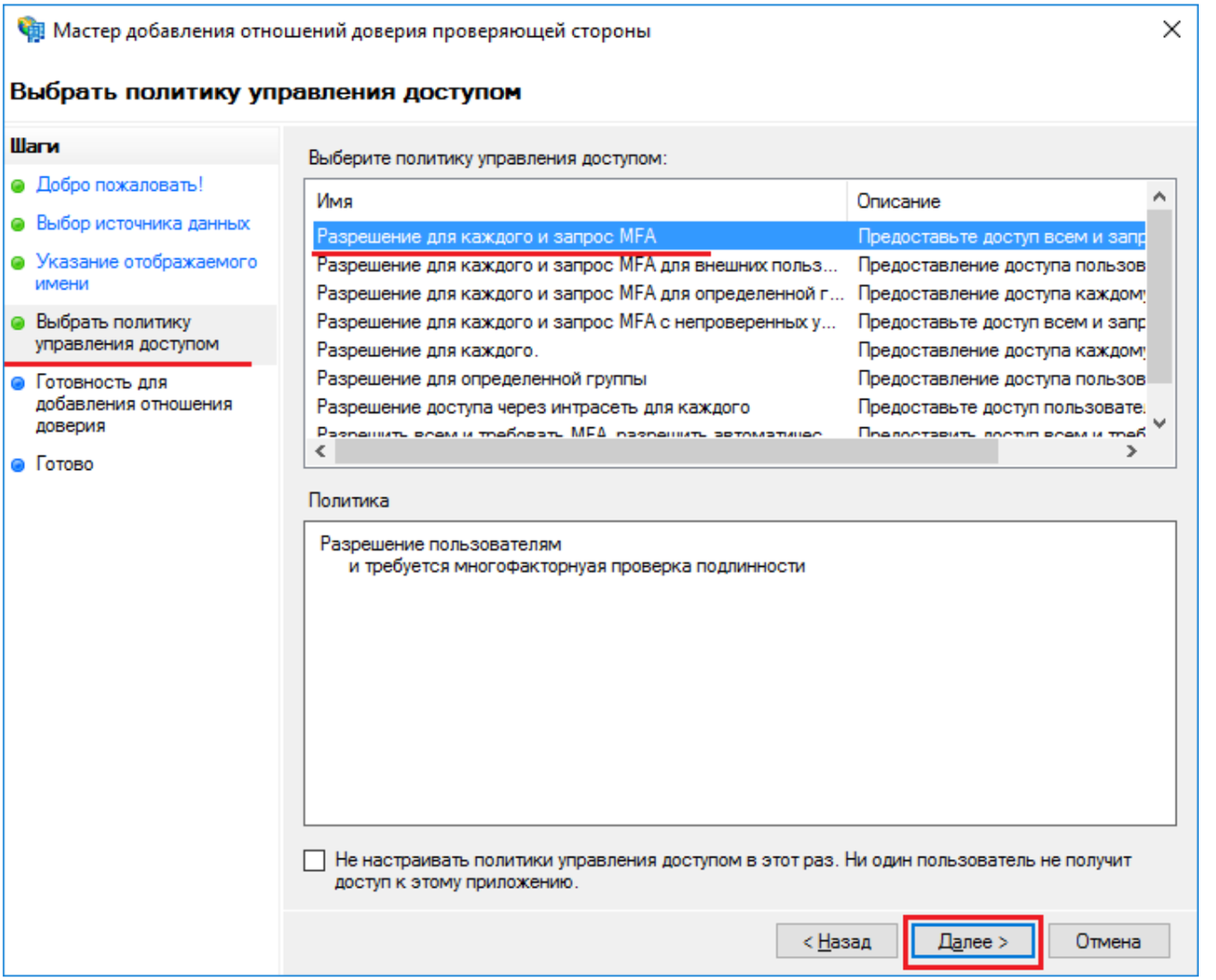
3. На вкладке "**Выбор источника данных**" укажите URL адрес вашего приложения и нажмите "**Далее**".

> **Информация**
>
> В качестве примера работы расширения используется стандартная страница ADFS **idpinitiatedsignon.htm**. Адрес метаданных используется для данной страницы.



4. На вкладке "**Указание отображаемого имени**" введите имя и описание для вашего отношения доверия и нажмите "**Далее**".

5. На вкладке "**Выбрать политику управления доступом**" выберите подходящую вам политику с запросом MFA, из предложенных по умолчанию, также вы можете добавить произвольные политики контроля доступа.



6. Остальные параметры оставьте по умолчанию.
7. Для применения изменений перезапустите службу AD FS.

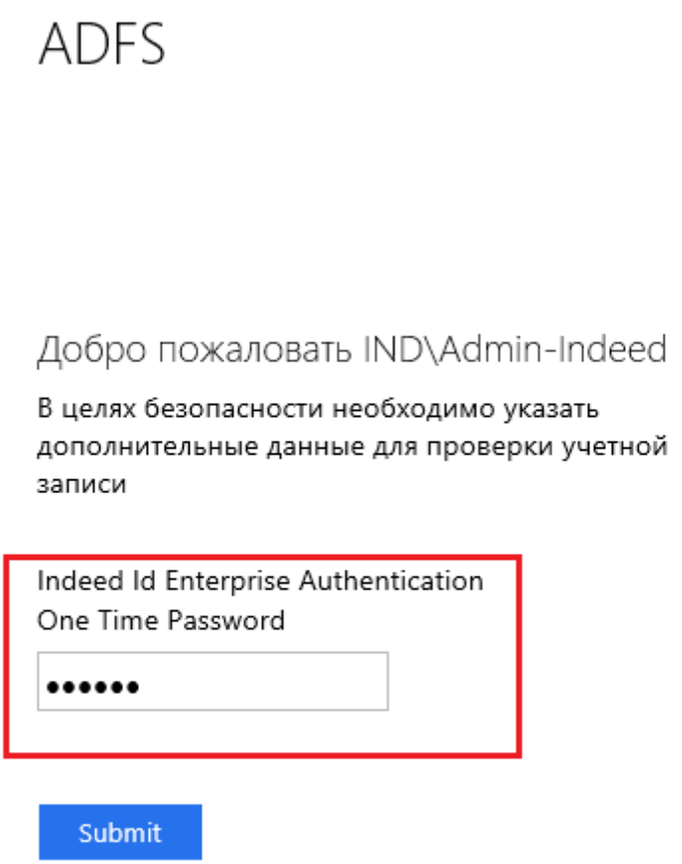
Работа расширения

Информация

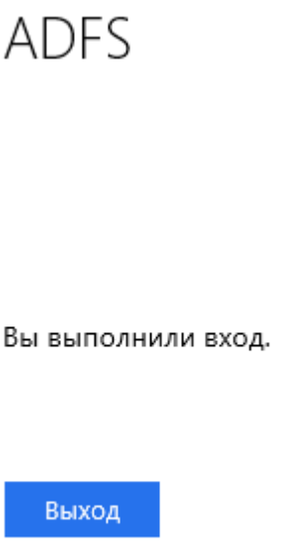
По умолчанию страница **idpinitiatedsignon.htm** отключена в AD FS 2016, для включения запустите PowerShell от имени администратора и выполните команду:

```
Set-AdfsProperties –EnableIdpInitiatedSignonPage $True
```

1. Откройте тестовую страницу ADFS: **https://YourDomainName/adfs/ls/idpinitiatedsignon.htm**
2. Выполните вход.
3. После ввода доменного логин/пароля укажите данные для второго фактора.



4. После корректного ввода данных будет выполнен вход.



Примеры внедрения расширения

1. Настройка двухфакторной аутентификации для приложений опубликованных в WAP
2. Настройка двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016
3. Настройка двухфакторной аутентификации в Microsoft Office 365 при помощи Indeed AM ADFS Extension