

Indeed AM ADFS Extension (2012)

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\Indeed AM ADFS Extension\<Номер версии>***

- **IndeedAM.ADFS.Extension-x64.ru-ru.msi** - Пакет для установки Indeed ADFS Extension

Установка и настройка ADFS Extension.

1. Выполнить установку ADFS Extension через запуск инсталлятора **IndeedAM.ADFS.Extension-x64.ru-ru.msi**.

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

 Информация

ModelId 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/",
  "ModelId": "{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}",
  "LSEventCacheDirectory": "C:\\\\EventCacheEa\\"
}
```

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 **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"
```

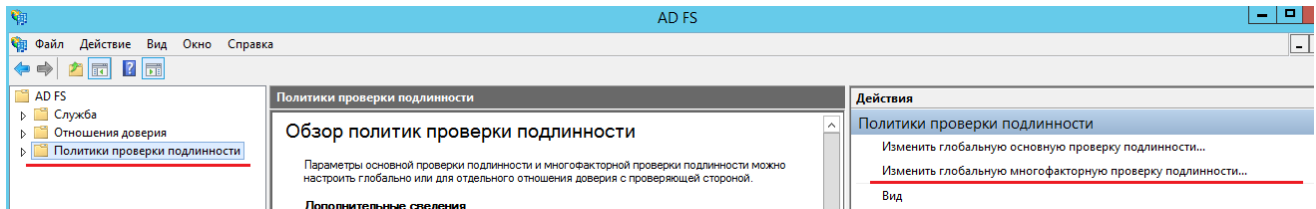
5. Для обновления конфигурации необходимо выполнить следующую команду:

Пример

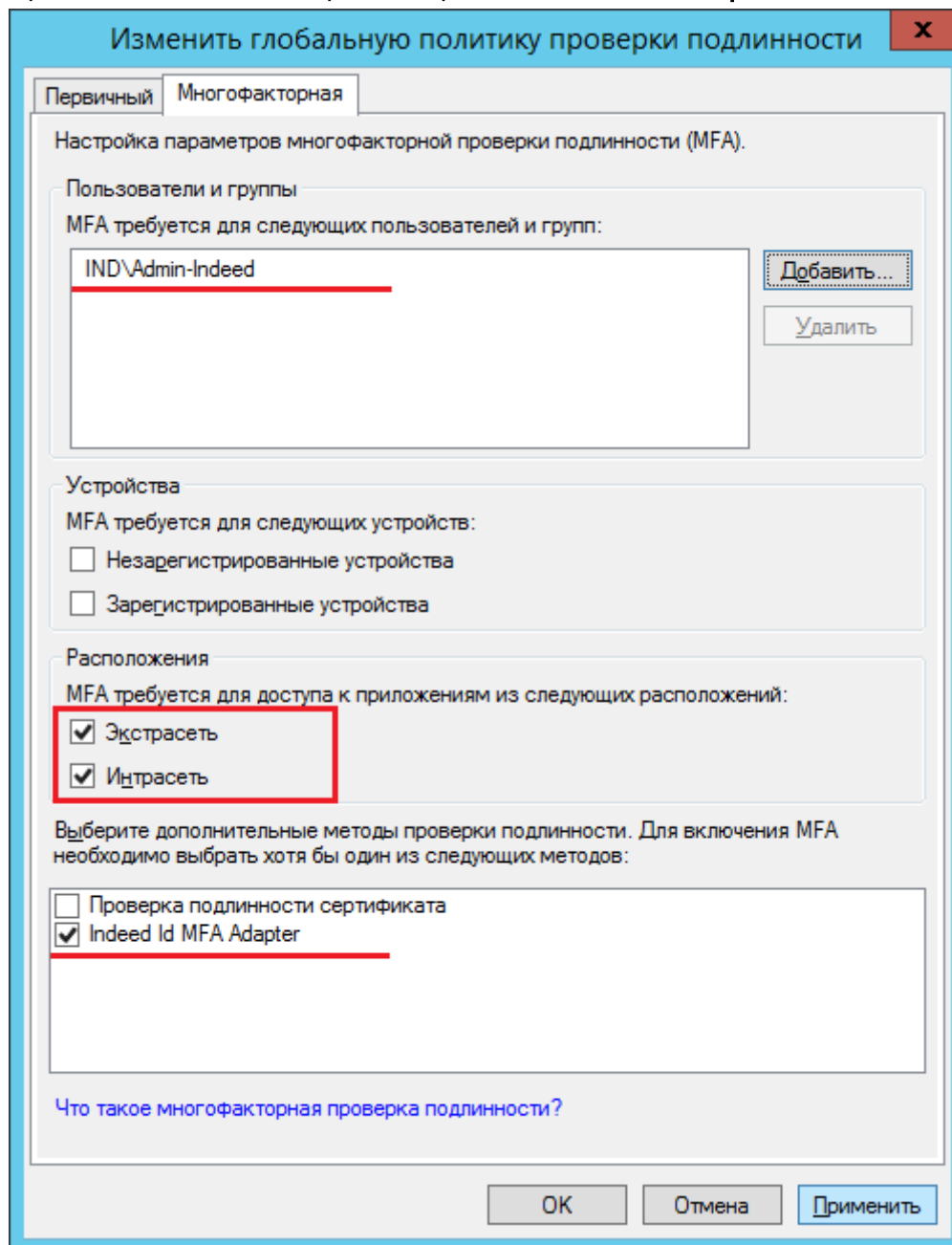
```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter" -FilePath 'YourPath\MFAAdapter.json'
```

Включение многофакторной аутентификации для ADFS.

1. Откройте консоль управления AD FS.
2. Выберите "Политики проверки подлинности", в окне "Действия" выберите "Изменить глобальную многофакторную проверку подлинности..."



3. Добавьте пользователя/группу и включите следующие параметры:
 - a. В пункте "Расположение" выберите "Экстрасеть" и "Интрасеть".
 - b. Выберите использование провайдера "Indeed Id MFA Adapter".



4. Для применения изменений перезапустите службу AD FS.

Пример работы расширения.

Пример настройки расширения в сценариях

1. Настройка двухфакторной аутентификации для приложений опубликованных в WAP
2. Инструкция по настройке двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016

Пример работы расширения на странице ADFS

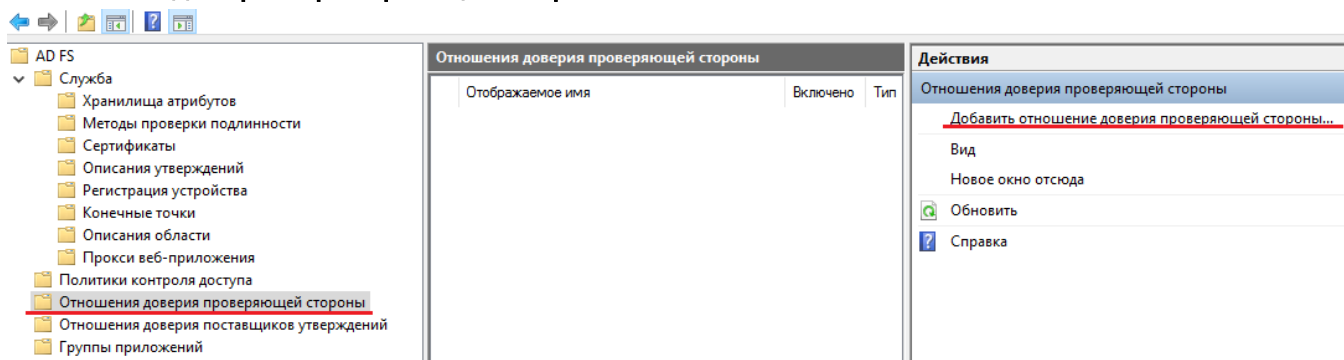


Информация

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

1. Настройка тестовой страницы

- а. Выберите "Отношение доверия проверяющей стороны" и нажмите "Добавить отношение доверия проверяющей стороны...".



- б. На вкладке "Добро пожаловать!" выберите "Поддерживающие утверждения" и нажмите "Запустить".

- с. 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.

Мастер добавления отношений доверия проверяющей стороны

Выбор источника данных

Шаги

- Добро пожаловать!
- Выбор источника данных**
- Выбор политики управления доступом
- Готовность для добавления отношения доверия
- Готово

Выберите способ, используемый мастером для получения данных об этой проверяющей стороне.

☒ Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети

Выберите данный параметр, чтобы импортировать требуемые данные и сертификаты из организации проверяющей стороны, которая публикует метаданные федерации в Интернете или локальной сети.

Адрес метаданных федерации (имя узла или URL-адрес):

<https://adfsnew.indeed.local/federationmetadata/2007-06/federationmetadata.xml>

Пример: fs.contoso.com или https://www.contoso.com/app

☐ Импорт данных о проверяющей стороне из файла

Выберите данный параметр, чтобы импортировать требуемые данные и сертификаты из организации проверяющей стороны, которая экспортировала метаданные федерации в файл. Убедитесь, что этот файл получен от доверенного источника. Этот мастер не будет проверять файл.

Местоположение файлов метаданных федерации:

☐ Ввод данных о проверяющей стороне вручную

Выберите данный параметр, чтобы ввести требуемые данные об организации проверяющей стороны вручную.

< Назад **Далее >** Отмена

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

- е. 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.

The screenshot shows the 'Master of Trust Relationships' wizard in Windows Server. The title bar reads 'Мастер добавления отношений доверия проверяющей стороны'. The main heading is 'Выбрать политику управления доступом'. On the left, a 'Шаги' (Steps) pane shows a sequence of steps: 'Добро пожаловать!', 'Выбор источника данных', 'Указание отображаемого имени', 'Выбрать политику управления доступом' (which is highlighted with a red underline and a blue selection dot), 'Готовность для добавления отношения доверия', and 'Готово'. The main area is titled 'Выберите политику управления доступом:' and contains a table with two columns: 'Имя' (Name) and 'Описание' (Description). The first row, 'Разрешение для каждого и запрос MFA', is highlighted in blue. Below the table, a preview box labeled 'Политика' shows the selected policy: 'Разрешение пользователям и требуется многофакторная проверка подлинности'. At the bottom, there is a checkbox labeled 'Не настраивать политики управления доступом в этот раз. Ни один пользователь не получит доступ к этому приложению.' and three buttons: '< Назад', 'Далее >' (highlighted with a red rectangle), and 'Отмена'.

Имя	Описание
Разрешение для каждого и запрос MFA	Предоставьте доступ всем и запрос MFA
Разрешение для каждого и запрос MFA для внешних поль...	Предоставление доступа пользов...
Разрешение для каждого и запрос MFA для определенной г...	Предоставление доступа каждому...
Разрешение для каждого и запрос MFA с непроверенных у...	Предоставьте доступ всем и за...
Разрешение для каждого.	Предоставление доступа каждому...
Разрешение для определенной группы	Предоставление доступа пользов...
Разрешение доступа через интрасеть для каждого	Предоставьте доступ пользовате...
Разрешить всем и требовать MFA, разрешить автоматичес...	Предоставить доступ всем и треб...

Политика

Разрешение пользователям
и требуется многофакторная проверка подлинности

☐ Не настраивать политики управления доступом в этот раз. Ни один пользователь не получит доступ к этому приложению.

< Назад **Далее >** Отмена

- f. Остальные параметры оставьте по умолчанию.
- g. Для применения изменений перезапустите службу AD FS.

Работа расширения

- a. Откройте тестовую страницу ADFS: <https://YourDomainName/adfs/ls/idpinitiatedsignon.htm>
- b. Выполните вход.

с. После ввода доменного логин/пароля укажите данные для второго фактора.

ADFS

Добро пожаловать IND\Admin-Indeed

В целях безопасности необходимо указать
дополнительные данные для проверки учетной
записи

Indeed Id Enterprise Authentication
One Time Password

•••••

Submit

d. После корректного ввода данных будет выполнен вход.

ADFS

Вы выполнили вход.

Выход

