

Indeed ADFS Extension

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

Информация

Файлы для Indeed ADFS Extension расположены: **indeed AM 7.0\Indeed ADFS Extension\<Номер версии>**

- **IndeedId.ADFS.Extension-v1.0.2.x64.ru-ru.msi** - Пакет для установки Indeed ADFS Extension

Установка и настройка ADFS Extension.

1. Выполнить установку Indeed ADFS Extension через запуск инсталлятора **IndeedId.ADFS.Extension-v1.0.2.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 TOTP**

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

Пример

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

- а. Настройка при использовании **SMS OTP Provider**.

Информация

По умолчанию номер телефона получается из атрибута **"telephoneNumber"**.

Для смены атрибута по умолчанию необходимо добавить параметры в конфигурационный файл сервера (C:\inetpub\wwwroot\easerver\Web.config).

- Добавить тег **"userMapRules"** в теге **"adUserCatalogProvider"**.
Добавить тег **"adObjectMapRule"** в теге **"userMapRules"** с параметрами:
 - **"attribute="Phone"** - Указывает на изменяемый параметр.
 - **"adAttribute="mobile"** - Указывает с какого атрибута AD брать значение.
- Добавить тег **"objectTypeSettings"**.
- Добавить тег **"objectSetting"** с параметрами **"category="person" class="user"**

Пример

```
<adUserCatalogProvider id="userId" serverName="ind.
loc" containerPath="DC=ind,DC=loc" userName="
userAdmin" password="Q1q2E3e4">
    <userMapRules>

    <adObjectMapRule attribute="Phone" adAttribute="mobile"
/>

    <objectTypeSettings>

    <objectSetting category="person" class="user"><
/objectSetting>
        <
/objectTypeSettings>
            </userMapRules>
    </adUserCatalogProvider>
```

b. Настройка при использовании EMAIL OTP Provider.



Информация

По умолчанию адрес электронной почты получается из атрибута "mail".

Для смены атрибута по умолчанию необходимо добавить параметры в конфигурационный файл сервера (C:\inetpub\wwwroot\easerver\Web.config).

- Добавить тег "userMapRules" в теге "adUserCatalogProvider".
Добавить тег "adObjectMapRule" в теге "userMapRules" с параметрами:
 - "attribute="Email" - Указывает на изменяемый параметр.
 - "adAttribute="otherMailbox" - Указывает с какого атрибута AD брать значение.
- Добавить тег "objectTypeSettings".
- Добавить тег "objectSetting" с параметрами "category="person" class="user"

Пример

```
<adUserCatalogProvider id="userId" serverName="ind.
loc" containerPath="DC=ind,DC=loc" userName="
userAdmin" password="Q1q2E3e4">
    <userMapRules>

    <adObjectMapRule attribute="Email" adAttribute="
otherMailbox" />

    <objectTypeSettings>

    <objectSetting category="person" class="user"><
/objectSetting>
        <
/objectTypeSettings>
            </userMapRules>
    </adUserCatalogProvider>
```

3. Запустите PowerShell с правами администратора. Введите следующие данные:



Информация

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

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter, IndeedId.ADFS.MFAAdapter, Version=1.0.0.0, Culture=neutral, PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id MFA Adapter" -ConfigurationFilePath 'YourPatch\MFAAdapter.json'
```

4. Для удаления адаптера необходимо выполнить следующую команду:

Пример

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

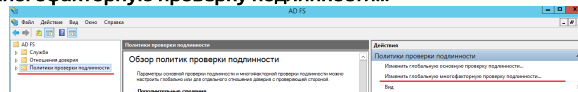
5. Для обновления конфигурации необходимо выполнить следующую команду:

Пример

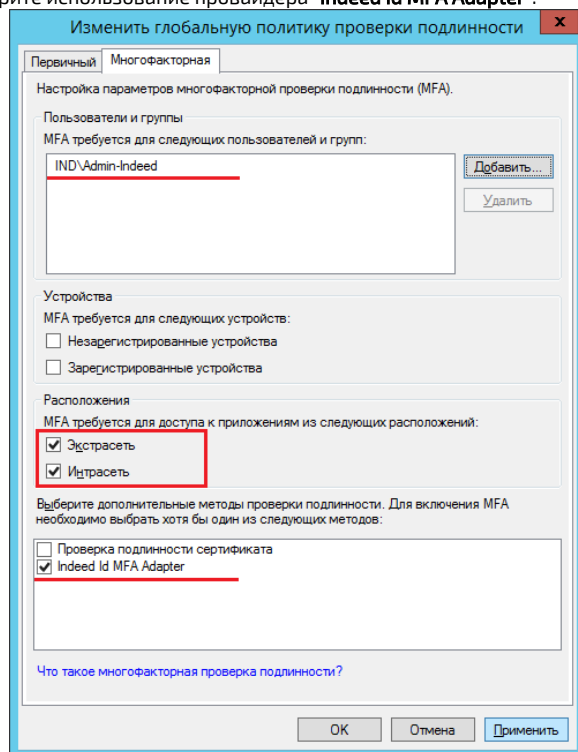
```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter" -FilePath 'YourPatch\MFAAdapter.json'
```

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".



Пример работы расширения.

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.

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

4. После корректного ввода данных будет выполнен вход.

ADFS

Вы выполнили вход.

Выход