



## **РУСТЭК.VDI**

Инструкция по настройке SAML в ADFS для Single Sign-On

Релиз 4.1

## Оглавление

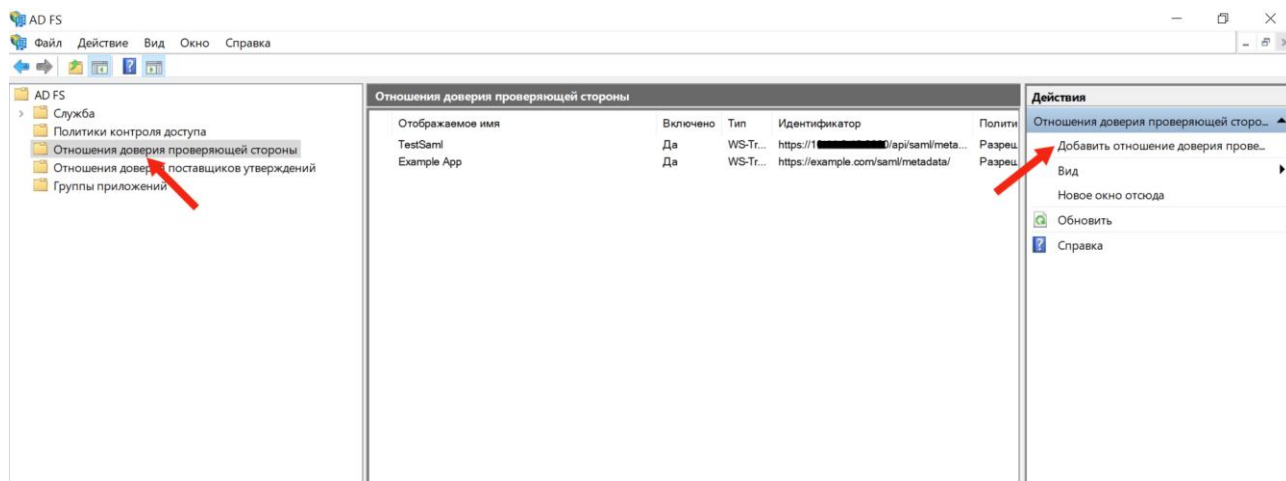
1. Настройка SAML в ADFS.....	3
2. Включение поддержки CORS в ADFS.....	14
3. Просмотр логов.....	14

Если предполагается использование функционала Single Sign-On (далее - SSO), прежде, чем начать работу в панели управления РУСТЭК.VDI, необходимо выполнить данную инструкцию.

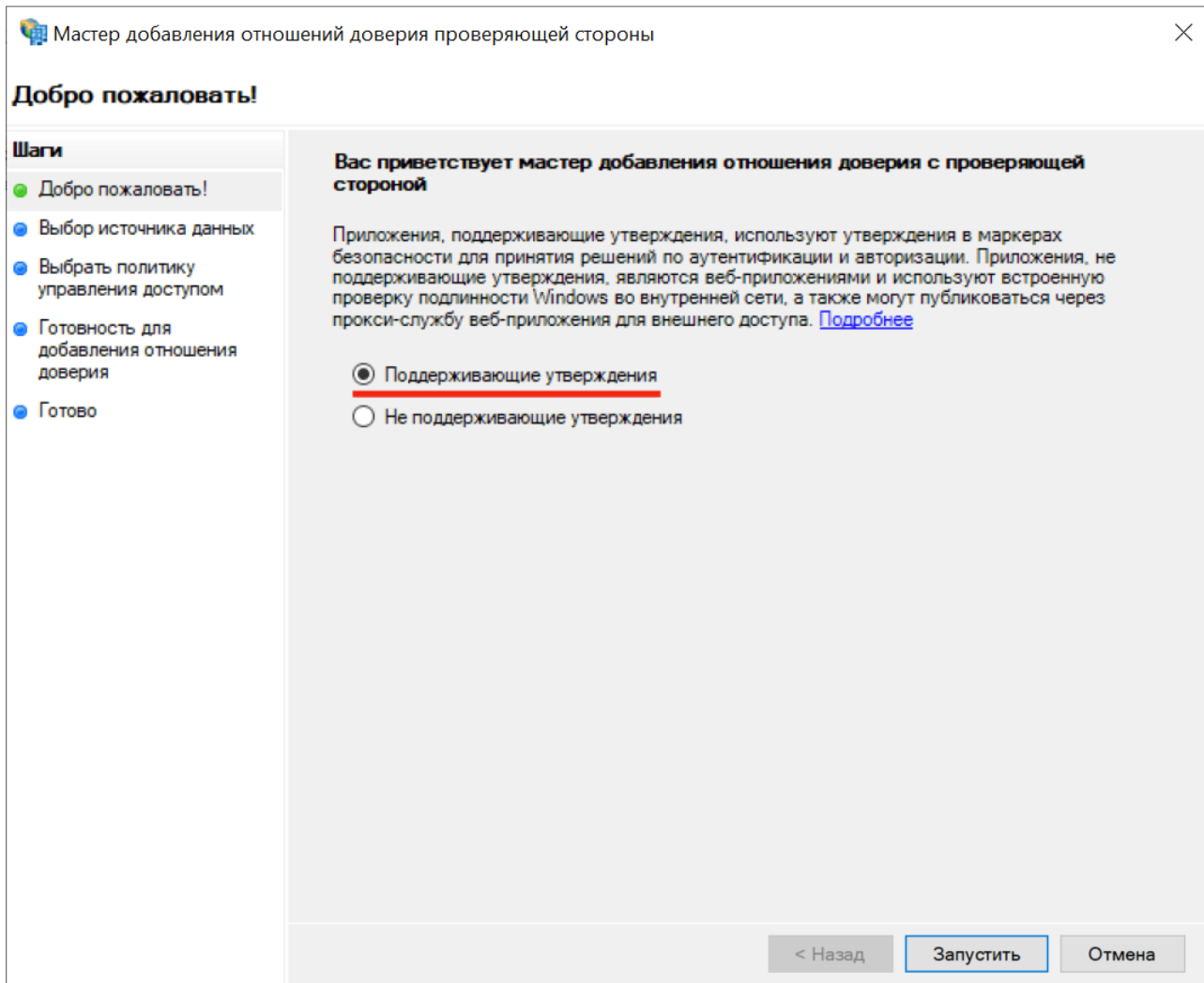
## 1. Настройка SAML в ADFS

Раздел описывает настройку Security Assertion Markup Language (далее SAML) в Active Directory Federation Services (далее ADFS) для реализации Single Sign-On (SSO) между Identity Provider и Service Provider:

1. Подключитесь к ВМ, где установлена ADFS.
2. Откройте приложение **Управление ADFS**.
3. В открывшемся окне выберите **Отношение доверия проверяющей стороны** и нажмите **Добавить отношение доверия проверяющей стороны**.



4. Убедитесь, что в открывшемся мастере переключатель установлен на значении **Поддерживающие утверждения**. Нажмите **Запустить** для продолжения настройки.



5. В окне выбора источника данных выберите **Ввод данных о проверяющей стороне вручную** и нажмите **Далее**.

Мастер добавления отношений доверия проверяющей стороны

### Выбор источника данных

**Шаги**

- Добро пожаловать!
- Выбор источника данных**
- Указание отображаемого имени
- Настройка сертификата
- Настройка URL-адреса
- Настройка идентификатора
- Выбрать политику 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 в локальной сети.

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

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 источник файла.

Местоположение файлов метаданных федерации:

 Обзор...

**Ввод данных о проверяющей стороне вручную**

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

< Назад    **Далее >**    Отмена

6. Введите отображаемое имя для проверяющей стороны и нажмите **Далее**.

Мастер добавления отношений доверия проверяющей стороны

### Указание отображаемого имени

Для этой проверяющей стороны введите отображаемое имя и любые примечания.

Отображаемое имя:

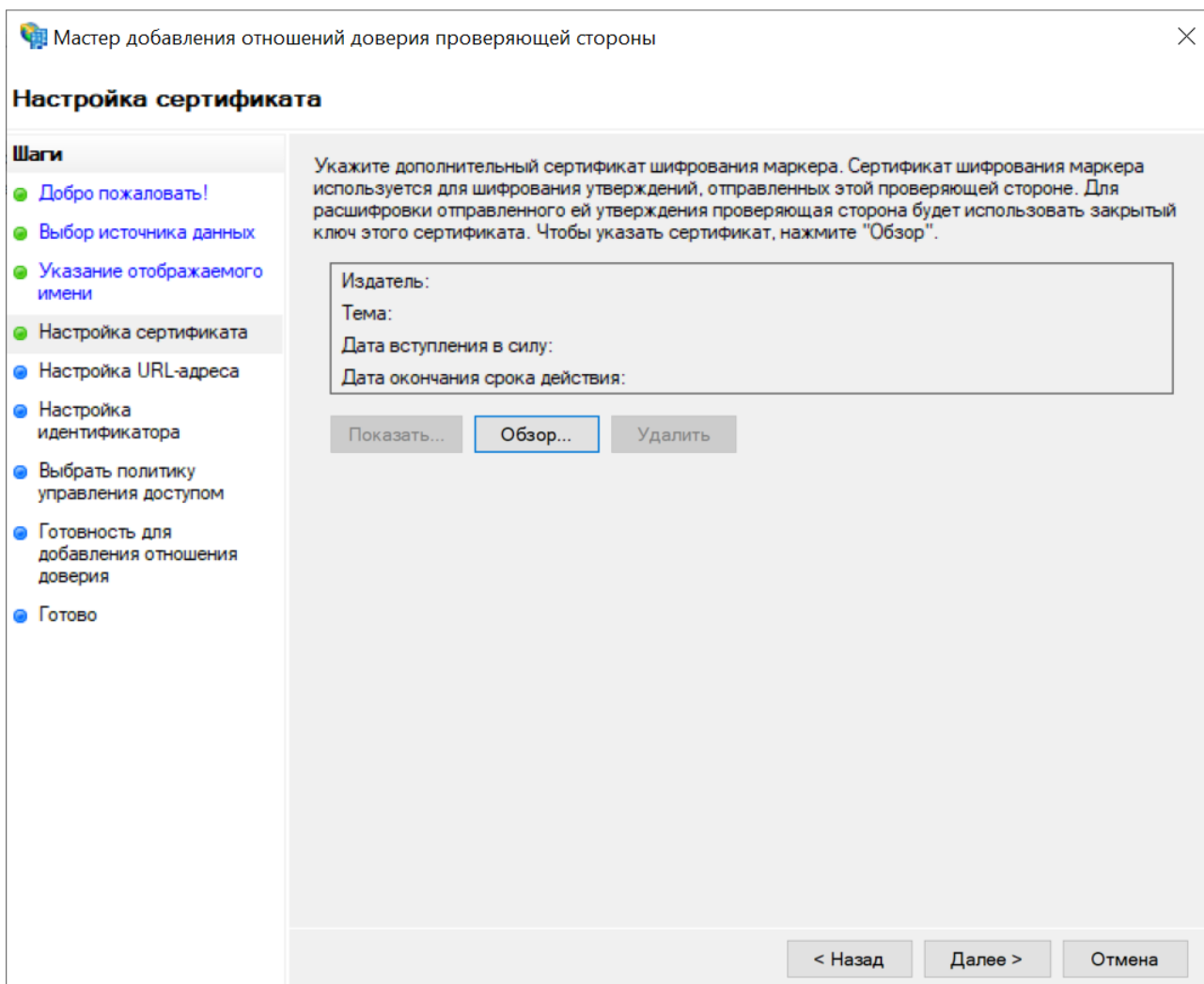
Примечания:

**Шаги**

- Добро пожаловать!
- Выбор источника данных
- Указание отображаемого имени**
- Настройка сертификата
- Настройка URL-адреса
- Настройка идентификатора
- Выбрать политику управления доступом
- Готовность для добавления отношения доверия
- Готово

< Назад **Далее >** Отмена

7. Выберите сертификат Service Provider в формате .CER и нажмите **Далее**.



8. (Опционально) Если файл в формате .CRT, то его необходимо конвертировать в .CER. Для конвертации сертификата выполните следующие действия:
  - Нажмите дважды на сертификат .CRT.
  - Перейдите в раздел **Состав** и нажмите **Копировать в файл....**
  - В открывшемся мастере экспорта:
    - а. Нажмите **Далее**.
    - б. Выберите **Файлы x.509 (.CER) в кодировке Base-64**.
    - с. Нажмите **Далее**.
  - Укажите расположения для сохранения конвертированного .CER, нажмите **Далее** и **Готово**.

9. Включите поддержку протокола SAML 2.0 WebSSO и укажите ASC URL вашего Service Provider.

Мастер добавления отношений доверия проверяющей стороны

### Настройка URL-адреса

**Шаги**

- Добро пожаловать!
- Выбор источника данных
- Указание отображаемого имени
- Настройка сертификата
- Настройка URL-адреса**
- Настройка идентификатора
- Выбрать политику управления доступом
- Готовность для добавления отношения доверия
- Готово

Для проверяющих сторон AD FS поддерживает протоколы WS-Trust, WS-Federation и SAML 2.0 WebSSO. Если проверяющая сторона использует протокол WS-Federation, SAML или оба протокола, установите флажки, соответствующие этим протоколам, и затем укажите используемые URL-адреса. Для проверяющей стороны поддержка протокола WS-Trust всегда включена.

Включить поддержку пассивного протокола WS-Federation

URL-адрес пассивного протокола WS-Federation поддерживает поставщиков утверждений на основе веб-браузера, используя пассивный протокол WS-Federation.

URL-адрес пассивного протокола WS-Federation проверяющей стороны:

Пример: <https://fs.contoso.com/adfs/ls/>

Включить поддержку протокола SAML 2.0 WebSSO

URL-адрес службы SAML 2.0 единого входа (SSO) поддерживает поставщиков утверждений на основе веб-браузера, используя протокол SAML 2.0 WebSSO.

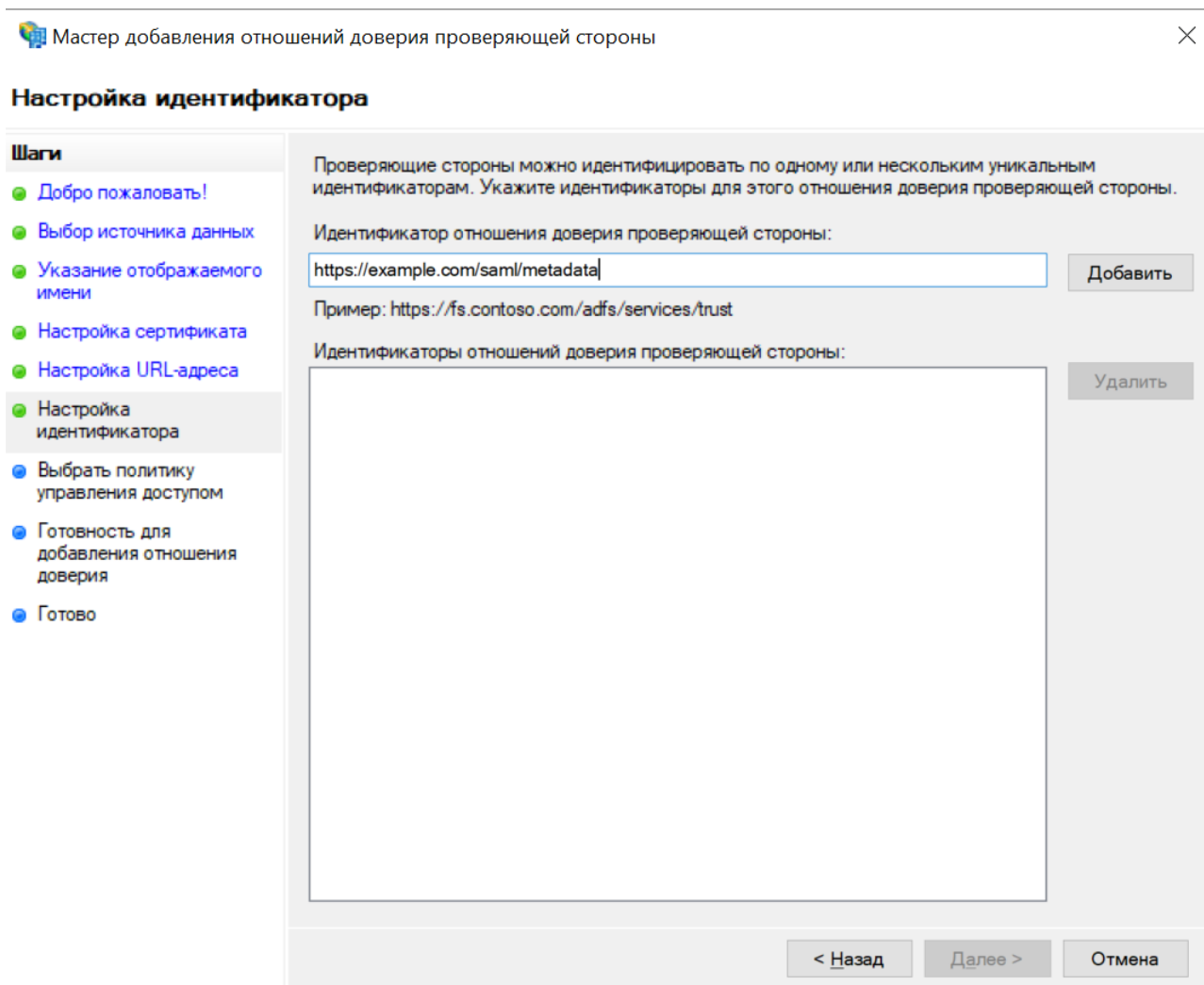
URL-адрес службы SAML 2.0 SSO проверяющей стороны:

Пример: <https://www.contoso.com/adfs/ls/>

< Назад    Далее >    Отмена



10. Вставьте Entity ID вашего Service Provider в поле **Идентификатор отношения доверия проверяющей стороны**, нажмите **Добавить** и затем **Далее**.



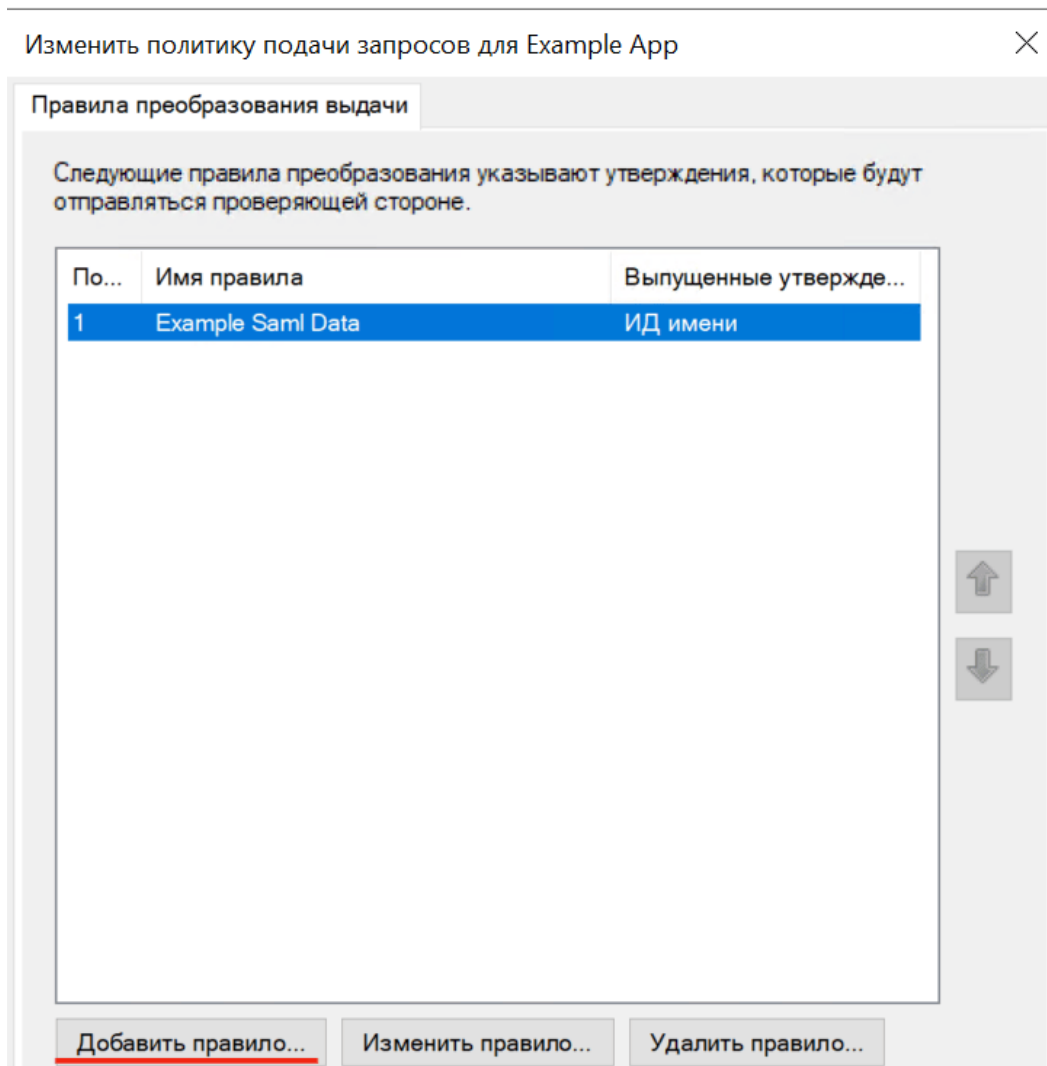
11. Выберите **Разрешение для каждого** в окне политики управления доступом и нажмите **Далее**.

The screenshot shows the 'Master of Trust Relationships' wizard window. 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 lists the following steps: 'Добро пожаловать!', 'Выбор источника данных', 'Указание отображаемого имени', 'Настройка сертификата', 'Настройка URL-адреса', 'Настройка идентификатора', 'Выбрать политику управления доступом' (highlighted), '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 table lists several policies, with 'Разрешение для каждого.' (Allow for everyone) selected. Below the table, the 'Политика' (Policy) section shows 'Разрешение для каждого'. 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.' (Do not configure access control policies this time. No user will get access to this application.) and three buttons: '< Назад', 'Далее >' (highlighted), and 'Отмена'.

Имя	Описание
Разрешение для каждого и запрос MFA	Предоставьте доступ всем и запрос MFA
Разрешение для каждого и запрос MFA для внешних польза...	Предоставление доступа пользо...
Разрешение для каждого и запрос MFA для определенной ...	Предоставление доступа каждо...
Разрешение для каждого и запрос MFA с непроверенных у...	Предоставьте доступ всем и за...
<b>Разрешение для каждого.</b>	<b>Предоставление доступа каждо...</b>
Разрешение для определенной группы	Предоставление доступа пользо...
Разрешение доступа через интрасеть для каждого	Предоставьте доступ пользовате...
Разрешить всем и требовать MFA, разрешить автоматичес...	Предоставить доступ всем и треб...

12. Нажмите **Далее**, а затем нажмите **Готово**.

13. В открывшемся окне изменения политики подачи запросов, нажмите **Добавить правило**.



Если окно изменения политики подачи запросов не открылось, выберите ваш Service Provider, затем нажмите **Изменить политику подачи запросов**.

14. Оставьте параметр **Отправка атрибутов LDAP** неизменным и нажмите **Далее**.

Мастер добавления правила преобразования утверждения

### Выбор шаблона правила

**Шаги**

- Выберите тип правила
- Настройте правило утверждения**

В следующем списке выберите шаблон для правила утверждения, которое необходимо создать. Описание предоставляет сведения о каждом шаблоне правила утверждения.

Шаблон правила утверждения:

Отправка атрибутов LDAP как утверждений

Описание шаблона правила утверждения:

С помощью шаблона правила "Отправка атрибутов LDAP как утверждений" можно выбирать атрибуты из хранилища атрибутов LDAP, например Active Directory, для отправки в качестве утверждений проверяющей стороне. С помощью данного типа правила можно отправлять несколько атрибутов как несколько утверждений из одного правила. Например, с помощью этого шаблона можно создать правило, которое будет извлекать значения атрибутов для прошедших проверку пользователей из атрибутов displayName и telephoneNumber Active Directory и затем отправлять эти значения как два различных исходящих утверждения. Это правило также можно использовать для отправки сведений о членстве пользователя во всех группах. Если требуется отправить сведения о членстве пользователя в отдельных группах, используйте шаблон правила "Отправка членства в группе как утверждения".

< Назад    **Далее >**    Отмена

15. Введите любое название в поле **Имя правила утверждения**. В списке **Хранилище атрибутов** выберите **Active Directory** и укажите необходимые данные пользователя, которые должен отправить ADFS вашему Service Provider после его авторизации. Затем нажмите **Готово**.

Мастер добавления правила преобразования утверждения

### Настройка правила

**Шаги**

- Выберите тип правила
- Настройте правило утверждения

Это правило можно настроить для отправки значений атрибутов LDAP как утверждений. Выберите хранилище атрибутов, из которого следует извлекать атрибуты LDAP. Укажите, как атрибуты будут сопоставляться с типами исходящих утверждений, которые будут выпускаться с помощью этого правила.

Имя правила утверждения:

Шаблон правила. Отправка атрибутов LDAP как утверждений

Хранилище атрибутов:

Сопоставление атрибутов LDAP типам исходящих утверждений:

	Атрибут LDAP (выберите или введите, чтобы добавить больше)	Тип исходящего утверждения (выберите или введите, чтобы добавить больше)
▶	User-Principal-Name	ИД имени
*		

< Назад    Готово    Отмена

## 2. Включение поддержки CORS в ADFS

Поддержка Cross-Origin Resource Sharing (далее CORS) в ADFS необходима, когда ADFS и бэкенд приложения находятся на разных доменах, а также для обеспечения безопасного обмена ресурсами между ними через браузеры.

1. Выполните следующую команду для включения поддержки CORS

```
Set-AdfsResponseHeaders -EnableCORS $true
```

2. Для определения списка доменов, которым разрешается доступ к ресурсам ADFS через CORS, выполните следующую команду:

```
Set-AdfsResponseHeaders -CORSTrustedOrigins https://example1.com,https://example2.com
```

Для предоставления доступа всем доменам вы можете использовать символ "\*".

## 3. Просмотр логов

Для просмотра логов ADFS:

1. Включите журналирование. Нажмите правой кнопкой мыши на **Admin** и выберите **Включить журнал**.
2. Откройте приложение **Просмотр событий**.
3. Перейдите в Журналы приложений и служб → ADFS → Admin.