РУСТЭК.VDI

Инструкция по настройке SAML в ADFS для Single Sign-On

Релиз 4.1

2024

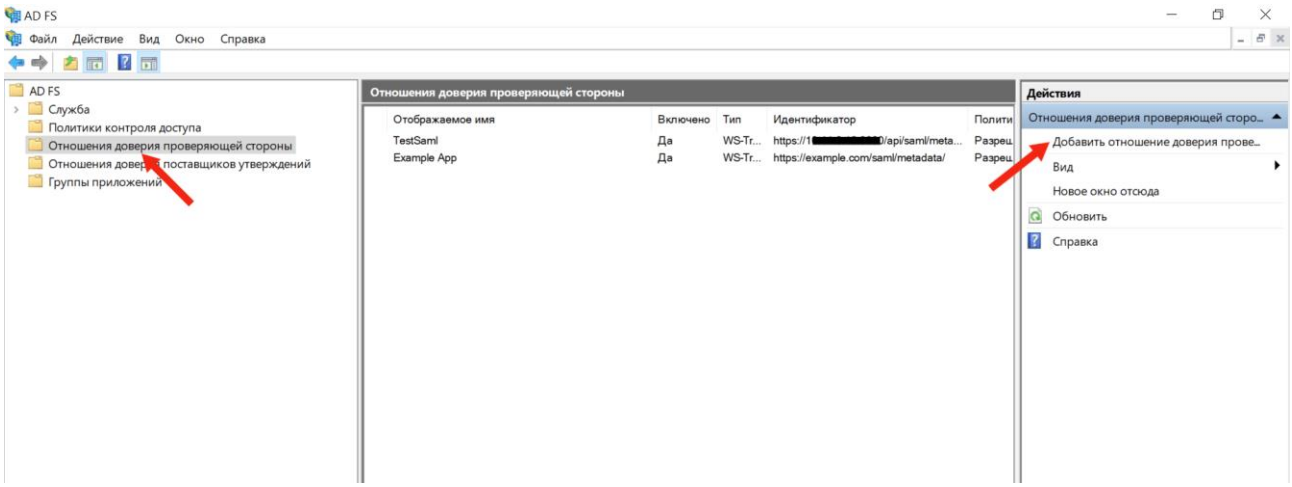
Оглавление

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

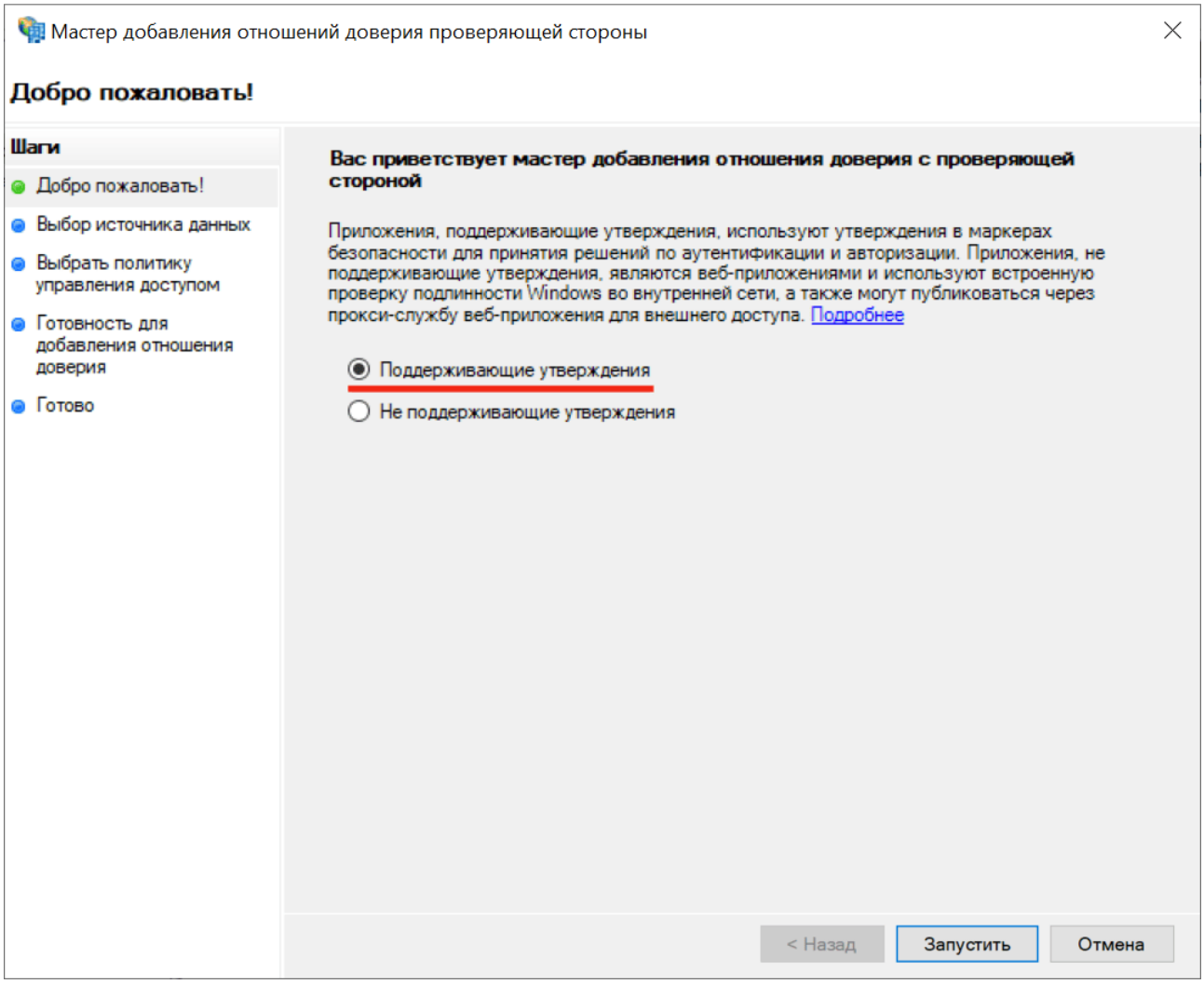
1. Настройка SAML в ADFS

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:

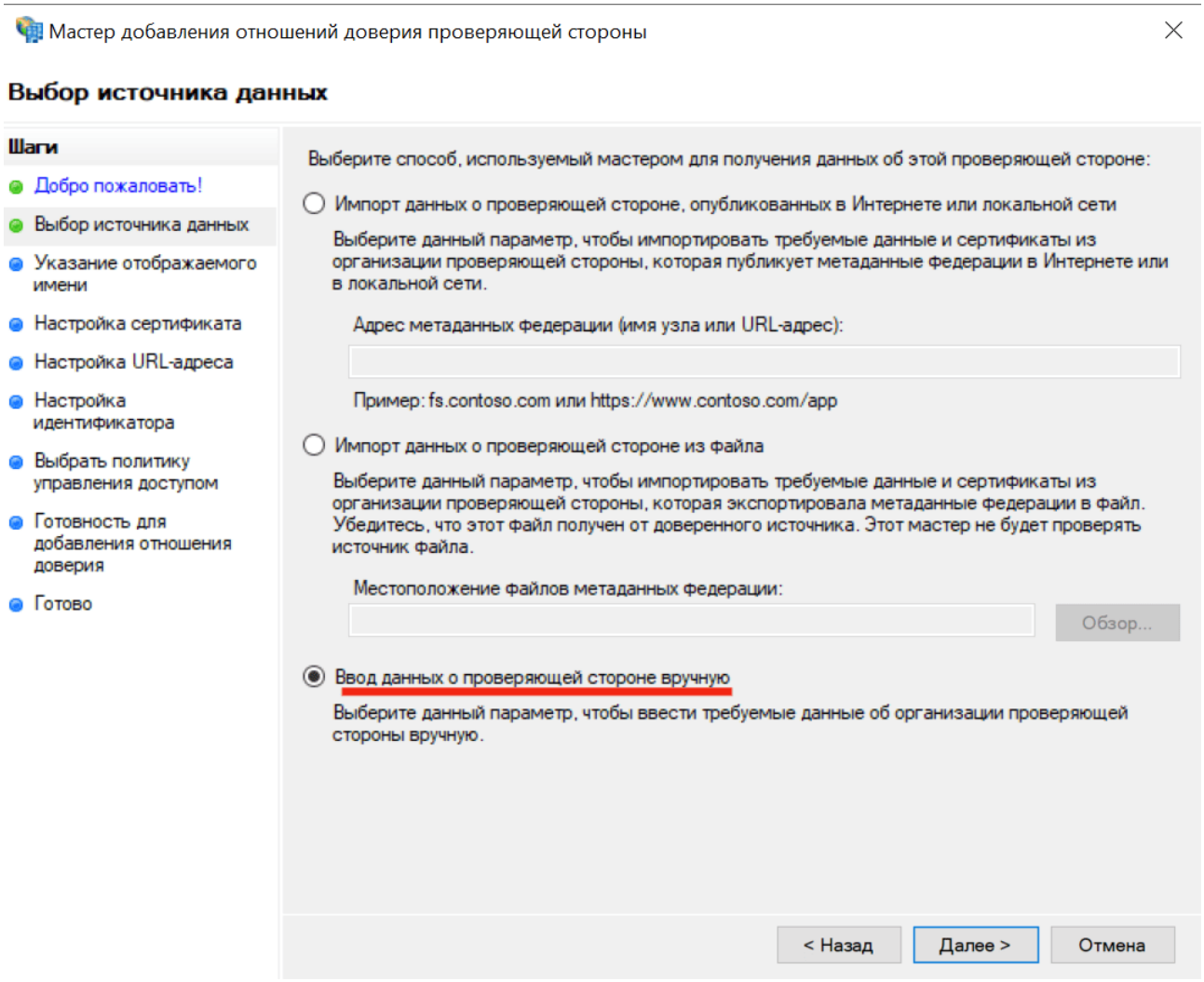
1. Подключитесь к ВМ, где установлена ADFS.
2. Откройте приложение **Управление ADFS**.
3. В открывшемся окне выберите **Отношение доверия проверяющей стороны** и нажмите **Добавить отношение доверия проверяющей стороны**.



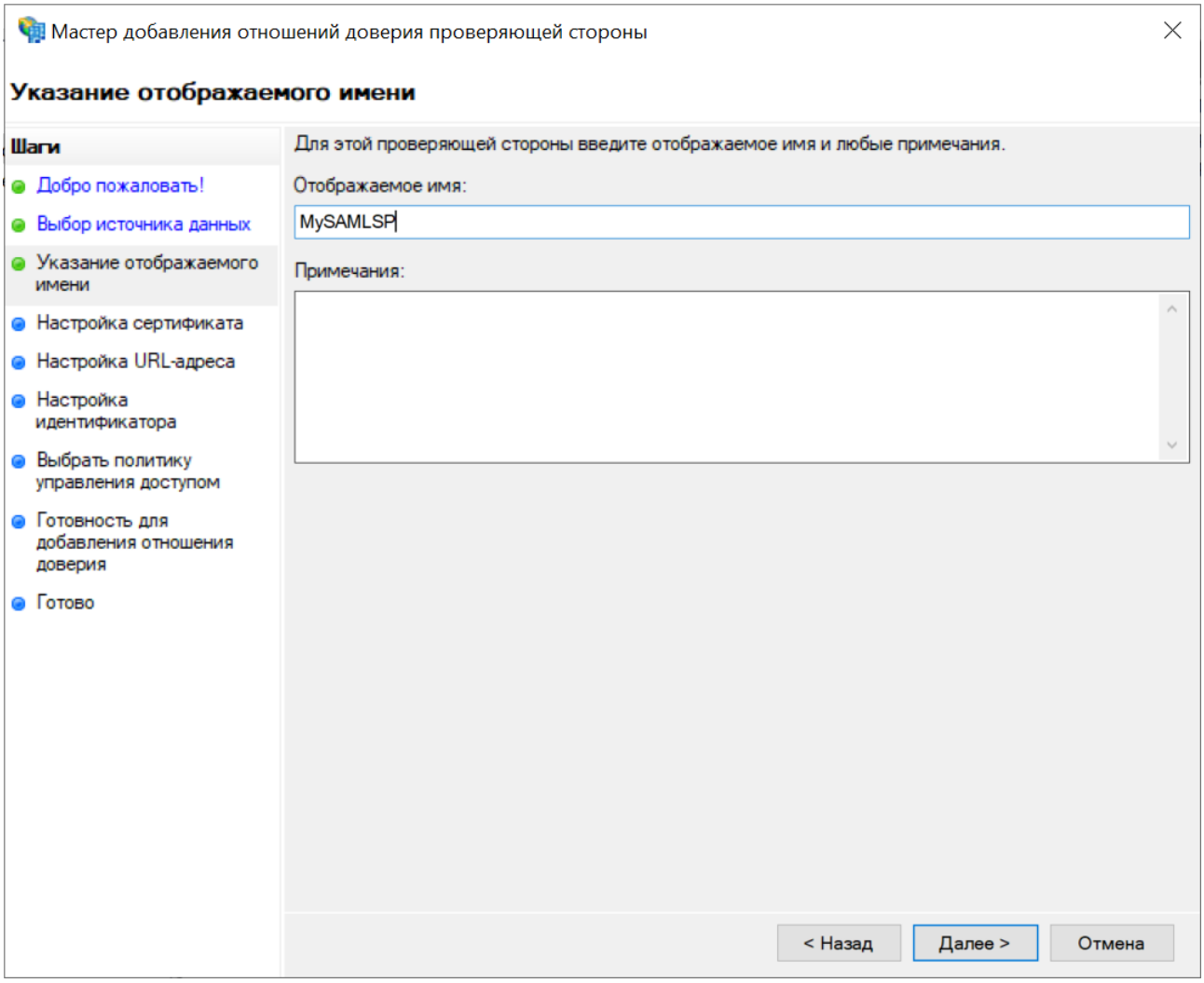
4. Убедитесь, что в открывшемся мастере переключатель установлен на значении **Поддерживающие утверждения**. Нажмите **Запустить** для продолжения настройки.



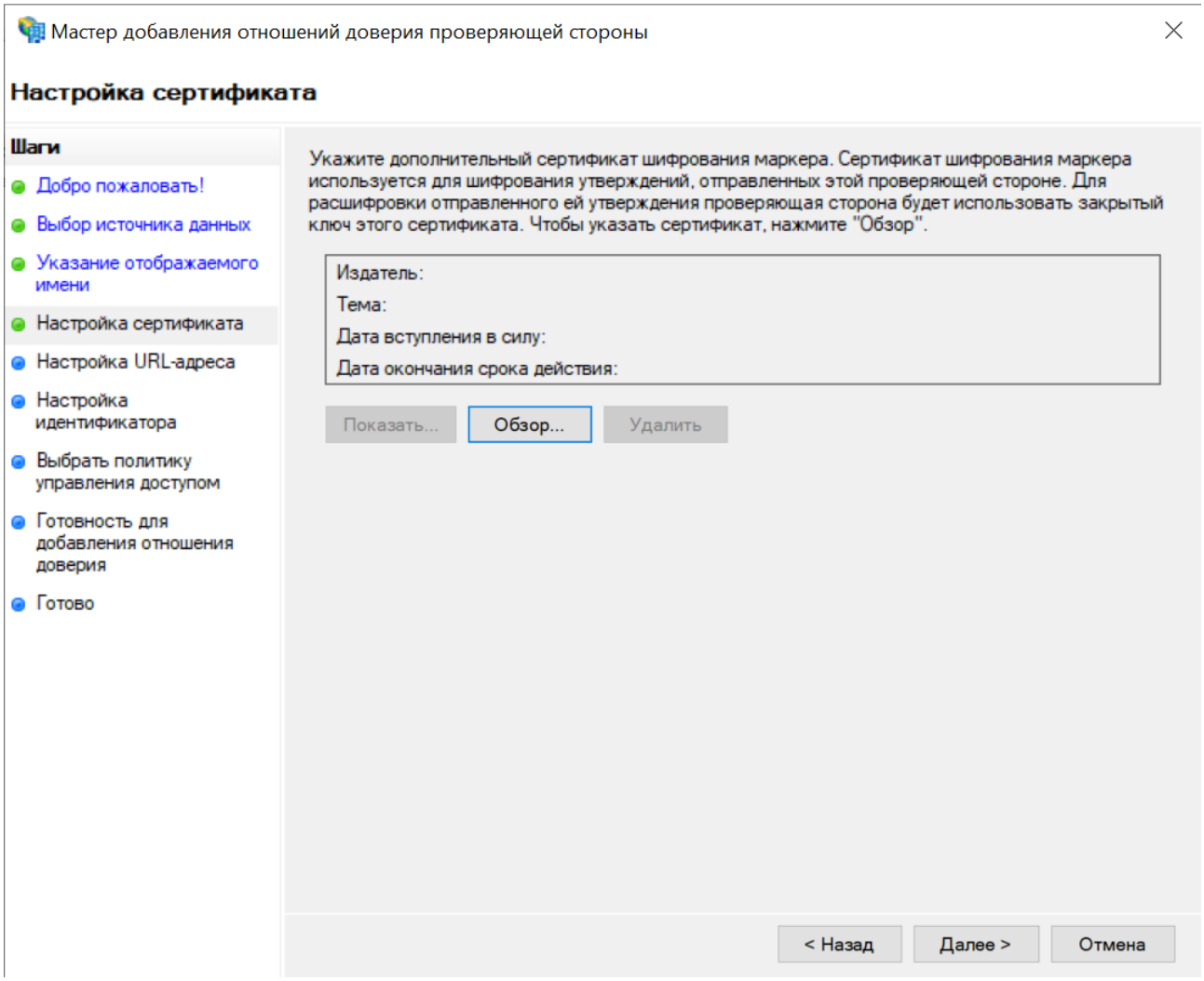
5. В окне выбора источника данных выберите **Ввод данных о проверяющей стороне вручную** и нажмите **Далее**.



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

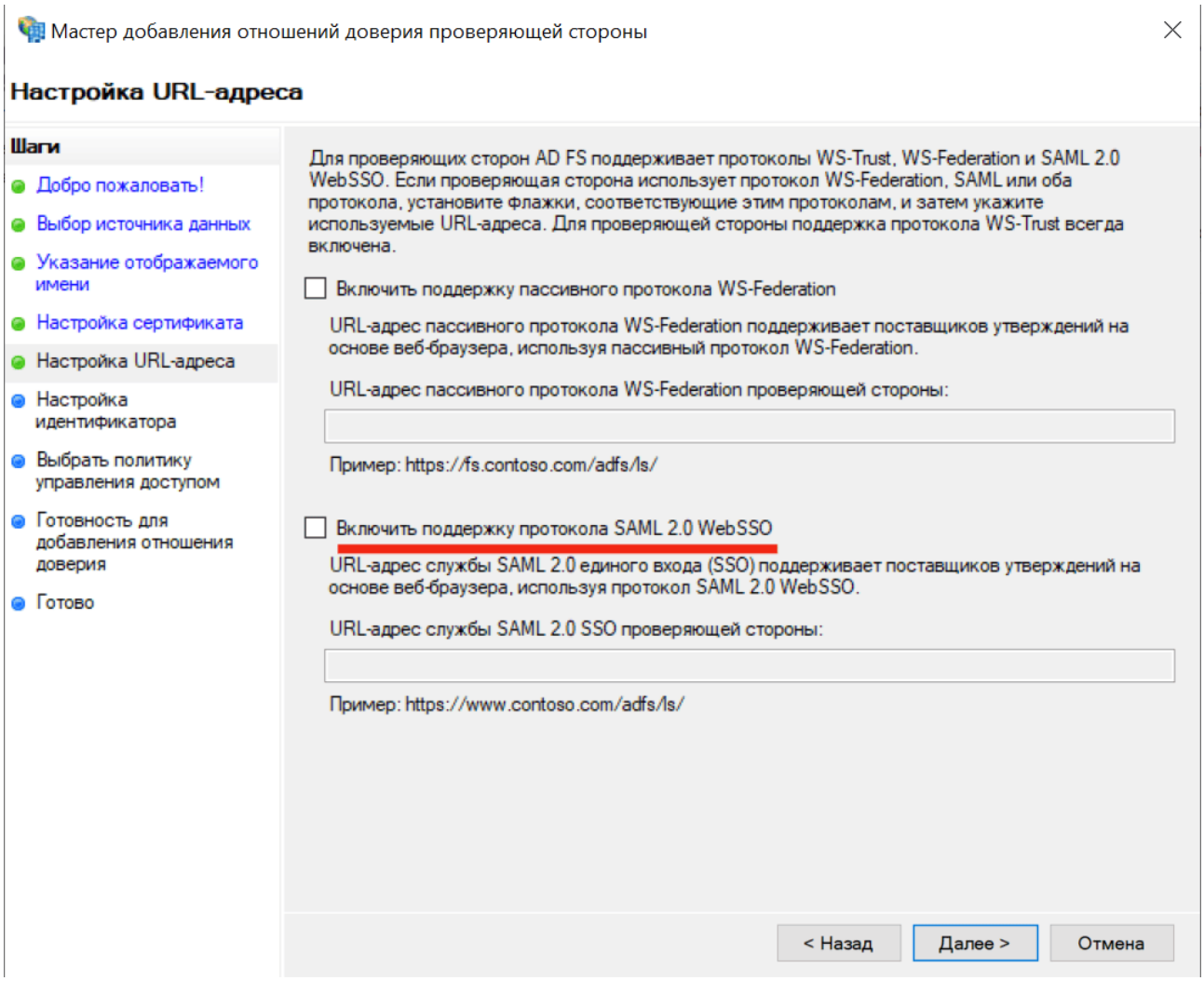


7. Выберите сертификат Service Provider в формате .CER и нажмите **Далее**.

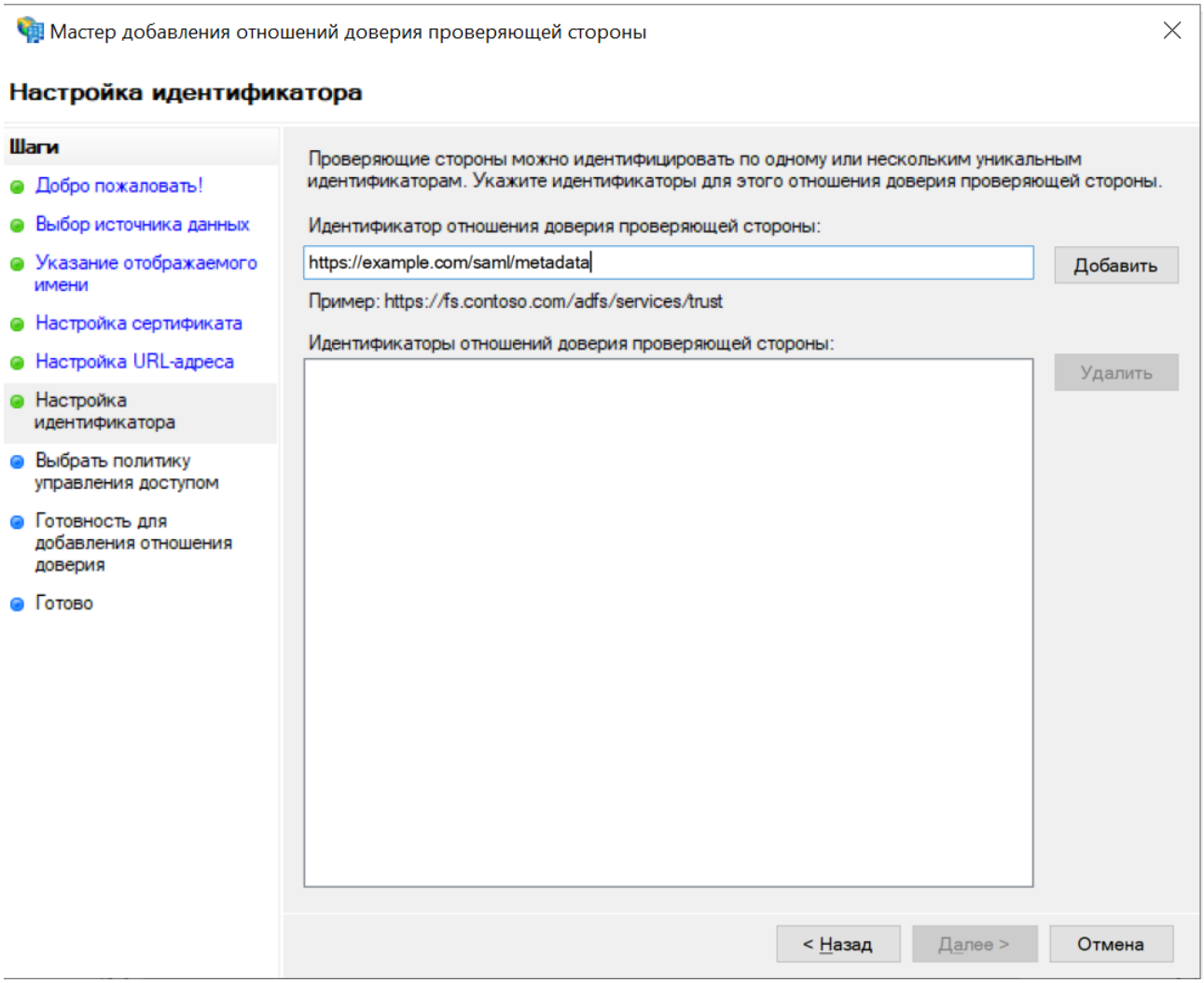


8. (Опционально) Если файл в формате .CRT, то его необходимо конвертировать в .CER.
   Для конвертации сертификата выполните следующие действия:
   - Нажмите дважды на сертификат .CRT.
   - Перейдите в раздел **Состав** и нажмите **Копировать в файл...**.
   - В открывшемся мастере экспорта:
     a.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

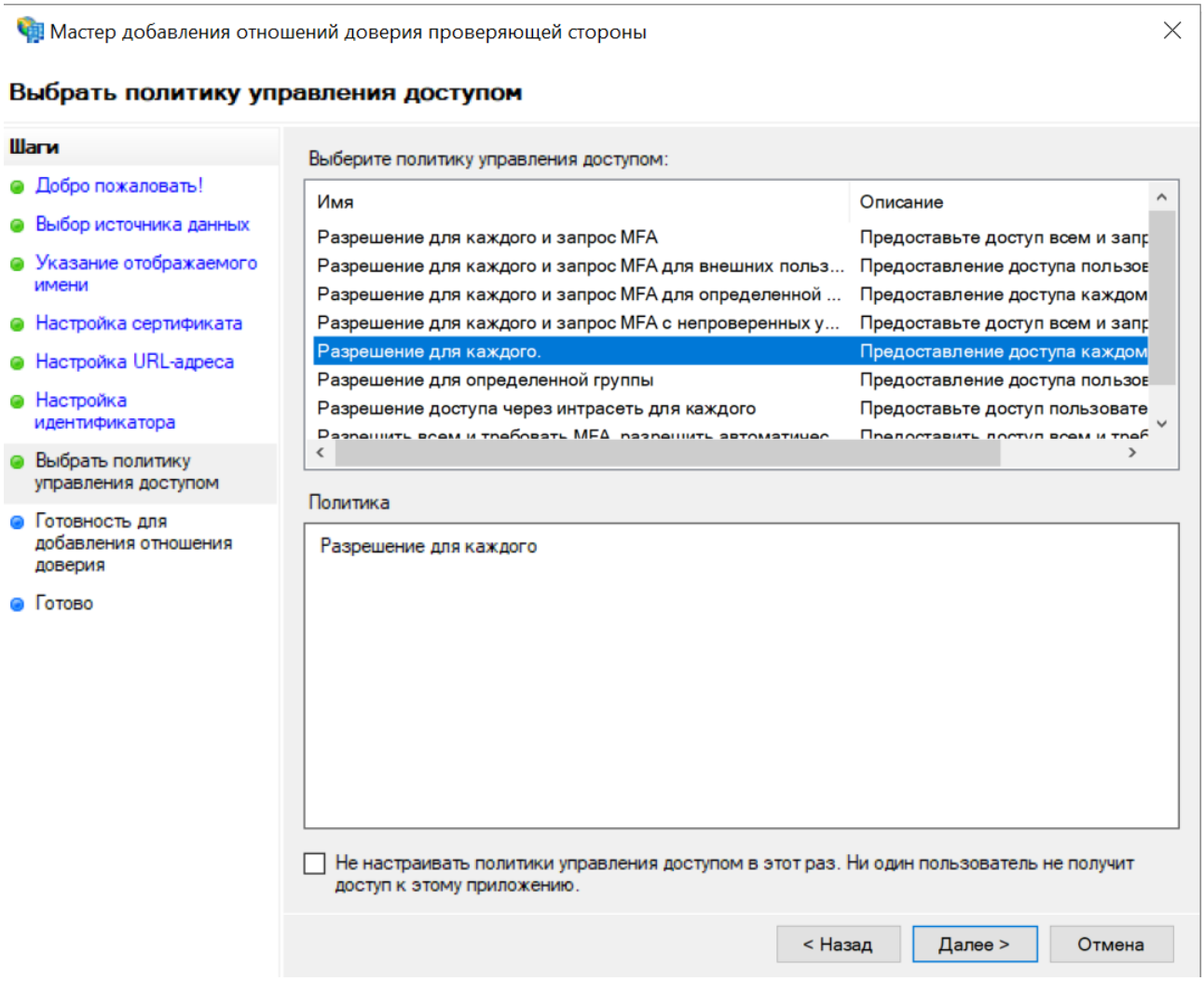
9. Включите поддержку протокола SAML 2.0 WebSSO и укажите ASC URL вашего Service Provider.



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

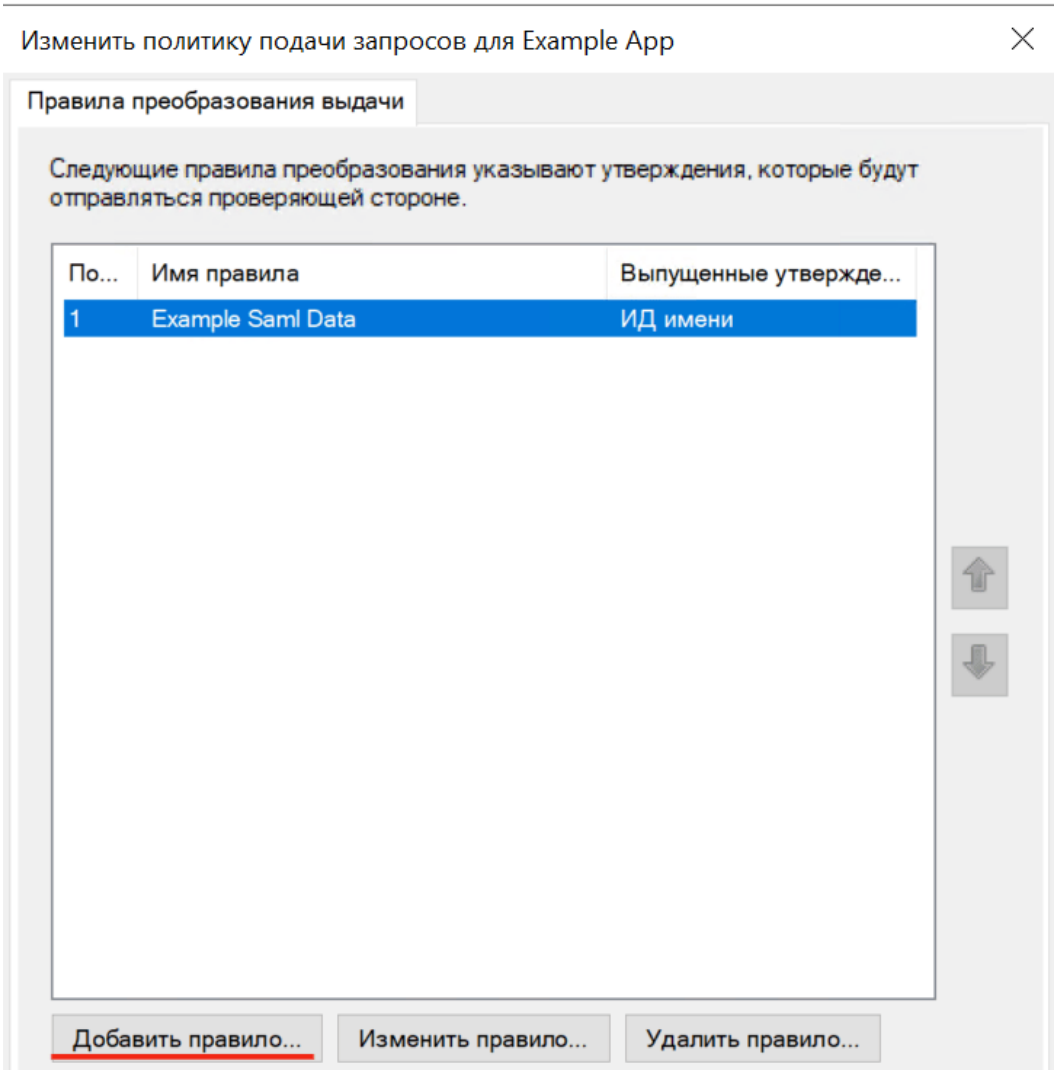


11. Выберите **Разрешение для каждого** в окне политики управления доступом и нажмите **Далее**.



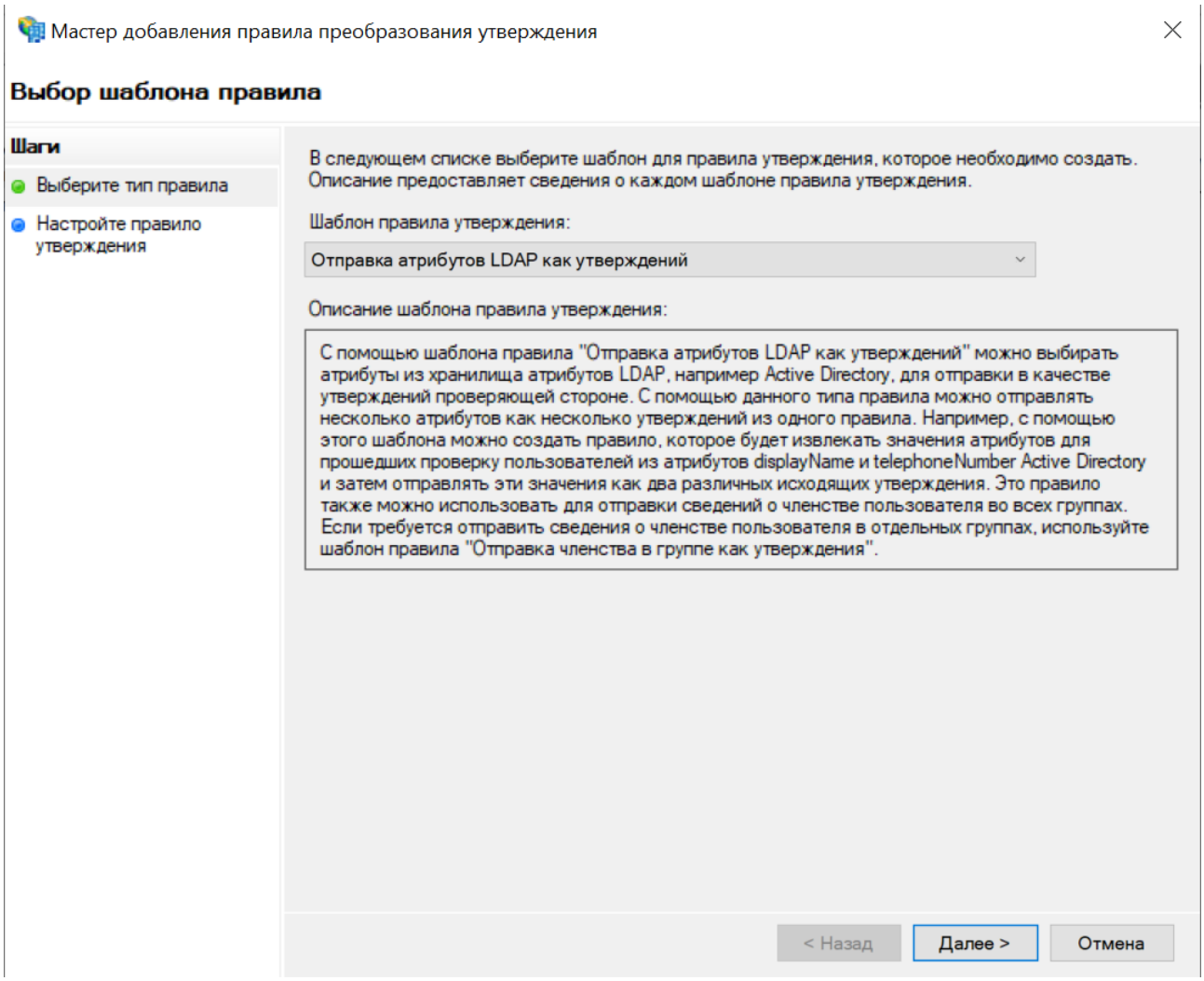
12. Нажмите **Далее**, а затем нажмите **Готово**.

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

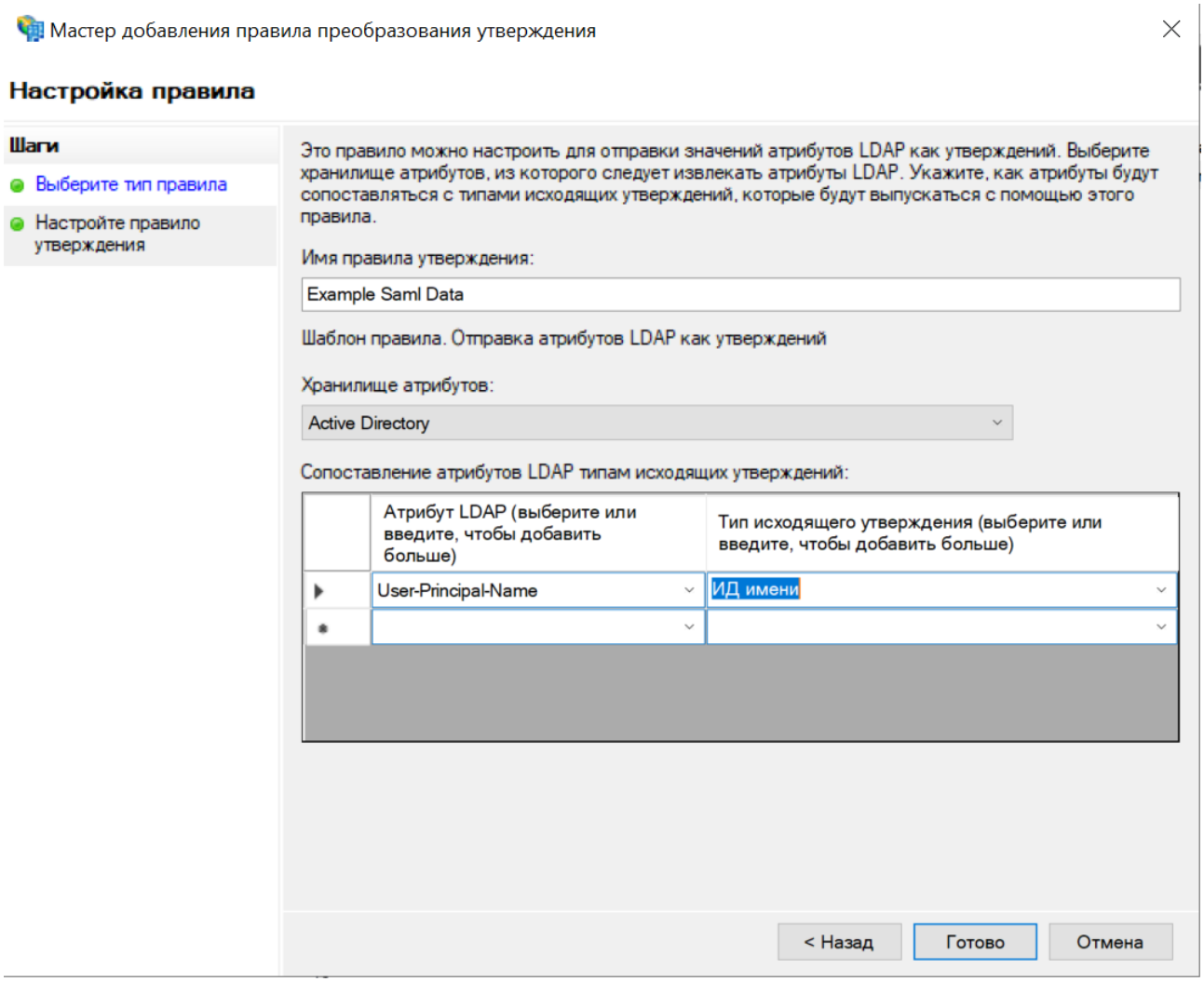


Если окно изменения политики подачи запросов не открылось, выберите ваш Service Provider, затем нажмите **Изменить политику подачи запросов**.

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



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**.



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.