Подключение AD FS как клиент (Service Provider) для Blitz IDP

AD FS (Active Directory Federation Services) - компонент Windows Server, обеспечивающий федеративное управление удостоверениями и доступом. Он позволяет использовать единый вход (SSO) для безопасного доступа к внешним веб-приложениям, облачным сервисам и ресурсам партнеров, используя учетные данные корпоративной Active Directory

Основная настройка интеграции заключается в обмене файлами метаданных с параметрами подключения между AD FS и Blitz IDP:

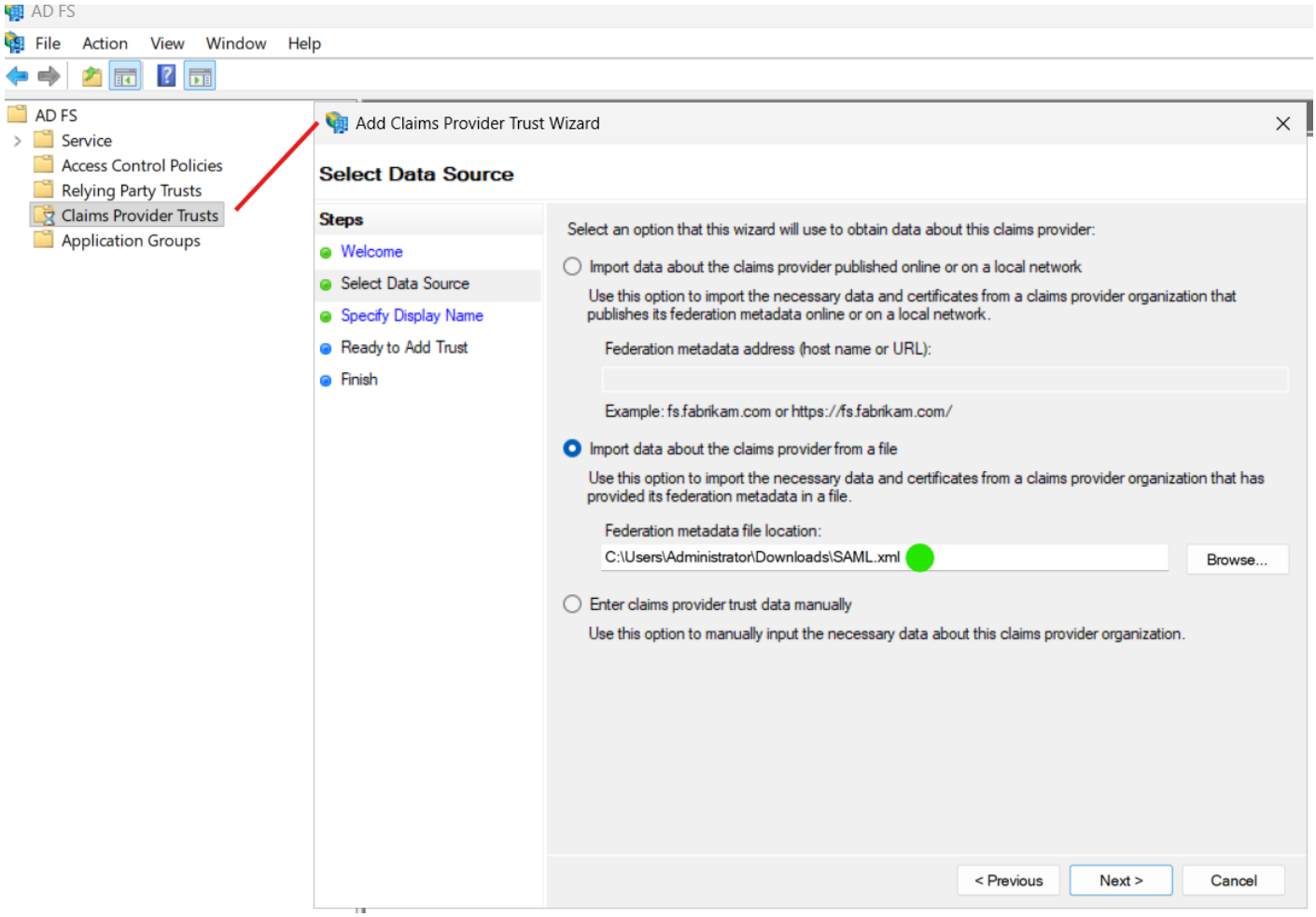
- URL метаданных Blitz IDP: `https://login.company.com/blitz/saml/profile/Metadata/SAML`
- URL метаданных AD FS: `https://adfs.company.com/FederationMetadata/2007-06/FederationMetadata.xml`

Подключение AD FS к Blitz Identity Provider выполняется по протоколу SAML и состоит из двух этапов:

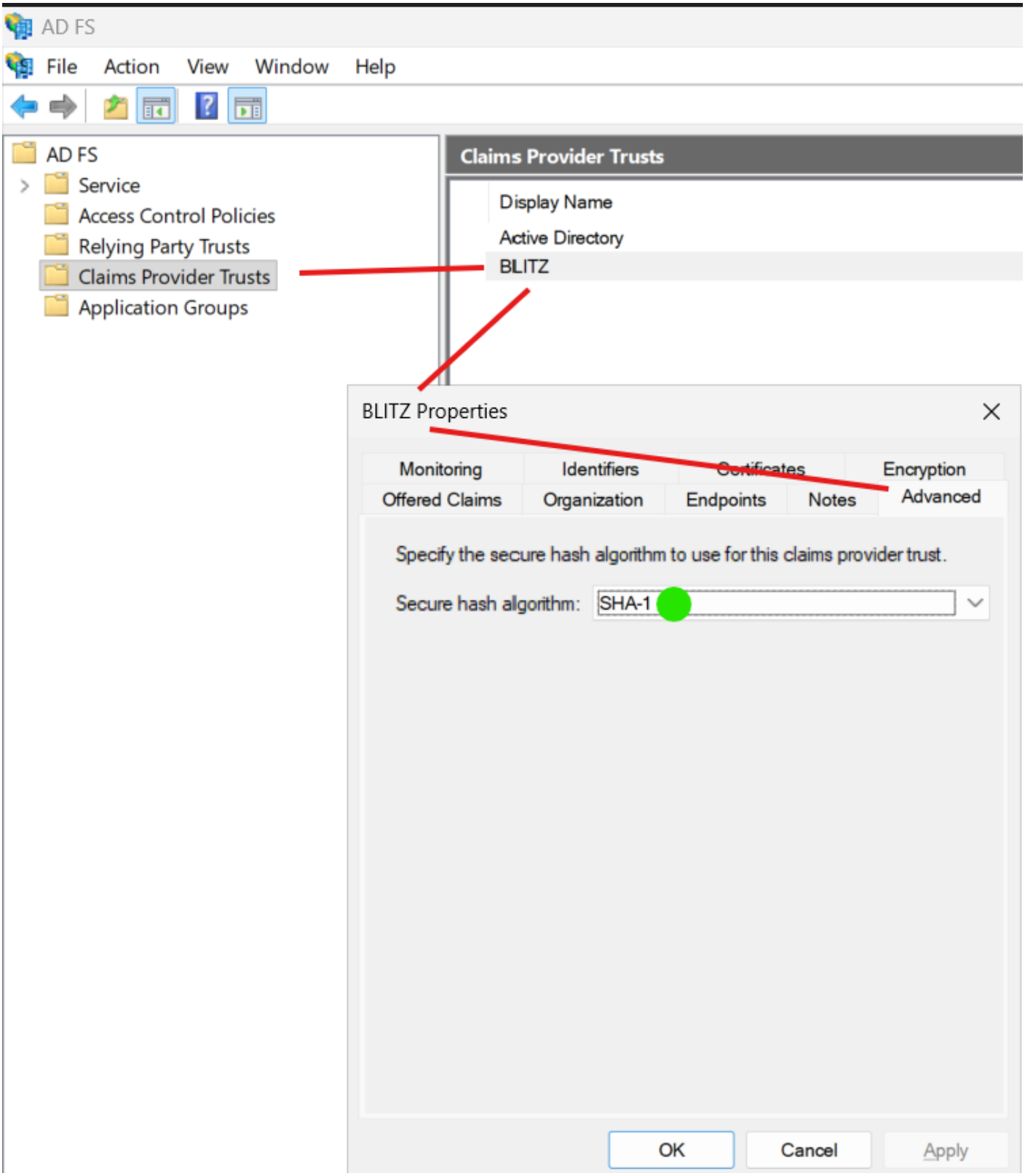
- Этап 1. Настройки на стороне AD FS
- Этап 2. Настройки на стороне Blitz Identity Provider
- Этап 3. Настройка атрибутов AD FS

Этап 1. Настройки на стороне AD FS

1. В оснастке управления AD FS необходимо добавить внешний провайдер, данные для настройки импортируйте из файла метаданных Blitz IDP. Название на следующем шаге - произвольное, например - Blitz IDP.



2. После создания провайдера в его настройках необходимо изменить алгоритм хэширования на **SHA-1 .**



Этап 2. Настройки на стороне Blitz IDP

1. В Консоли администратора создайте новое приложение с идентификатором `http://adfs.company.com/adfs/services/trust` и значением домена `adfs.company.com`. Проверить идентификатор можно в метаданных ADFS, значение параметра `entityID`.
2. После создания приложения необходимо сконфигурировать протокол SAML:

- **Метаданные**: в метаданные загрузите метаданными AD FS `FederationMetadata.xml`.
- **SAML профиль**: выберите `SAML 2.0 Web SSO Profile` и задайте параметры:
  - Подписывать утверждения: `always`
  - Шифровать утверждения: `never`
  - Шифровать идентификаторы (NameIds): `never`

3. Отметьте чек-бокс *Включить передачу SAML-утверждений о пользователе в специальном блоке Attribute Statement*. В **Атрибуты пользователя** указать атрибуты, которые необходимо передавать в AD FS.

Этап 3. Настройка передачи атрибутов Blitz IDP -> ADFS -> Приложение

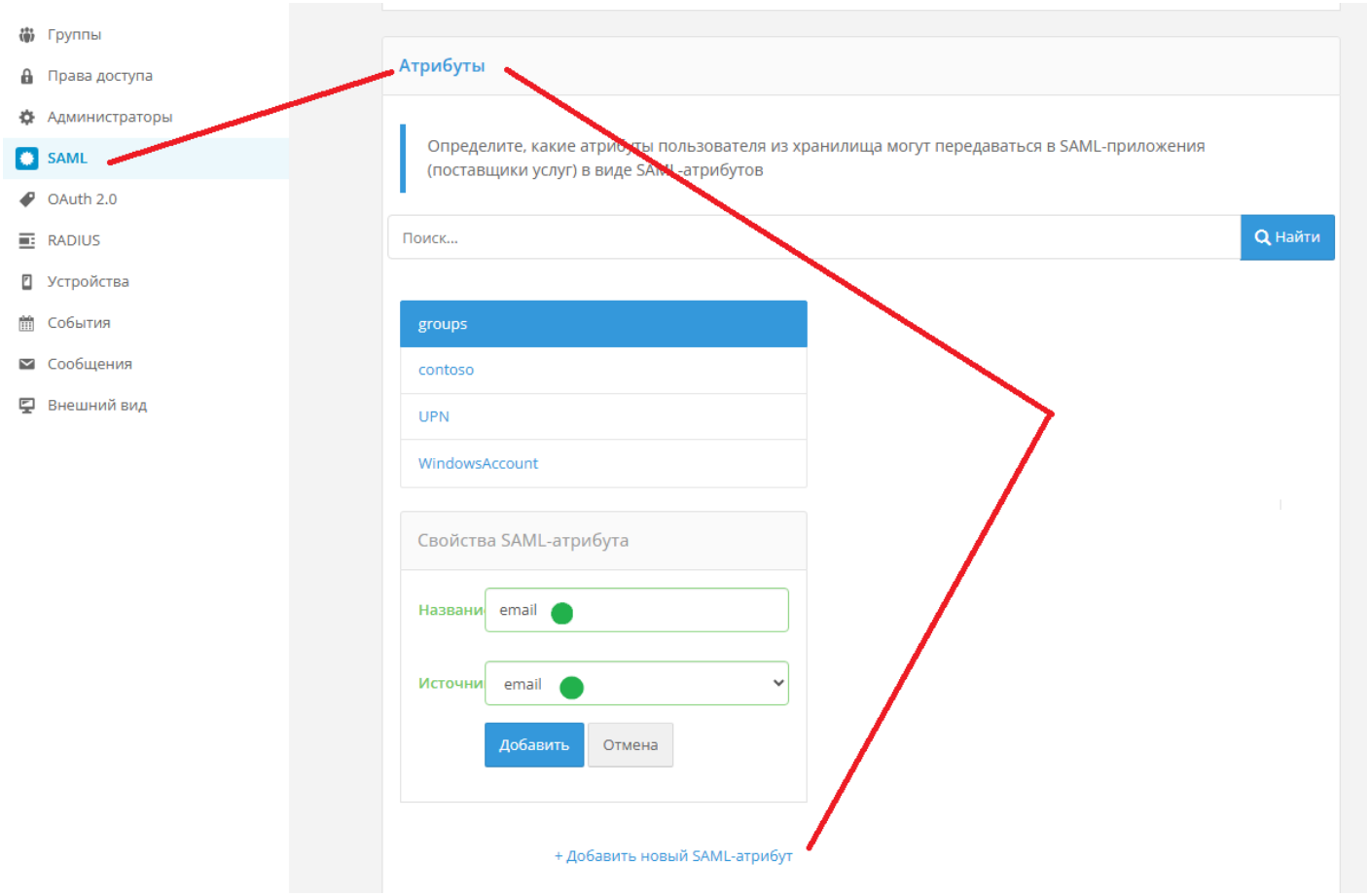
Есть две схемы передачи атрибутов из Blitz IDP в Клиентское приложение через ADFS. Их можно использовать как совместно, так и по отдельности:

- Вариант 1. AD FS работает просто как "передатчик" - присланный из Blitz IDP атрибут передает в клиентское приложение с таким же или измененным названием.
- Вариант 2. Blitz передает определенный атрибут (с именем `http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname` и значением `ДОМЕН\пользователь`), по которому ADFS может найти пользователя в AD и отправить в клиентское приложение атрибуты из AD этого пользователя. Этот вариант менее затратный, т.к. не потребует настройки передачи всех атрибутов из Blitz, настройки их приёма в ADFS и изменения настроек всех клиентских приложений ADFS на новые атрибуты.

Вариант 1. Передача атрибута в Приложение через AD FS

Шаг 1. Настройка со стороны Blitz IDP

1. В консоли администратора **SAML -> Атрибуты -> Добавить новый SAML-атрибут**:
   - Название: произвольное,
   - Источник: название атрибута пользователя, значение из которого будет отправлено Кодировщик.



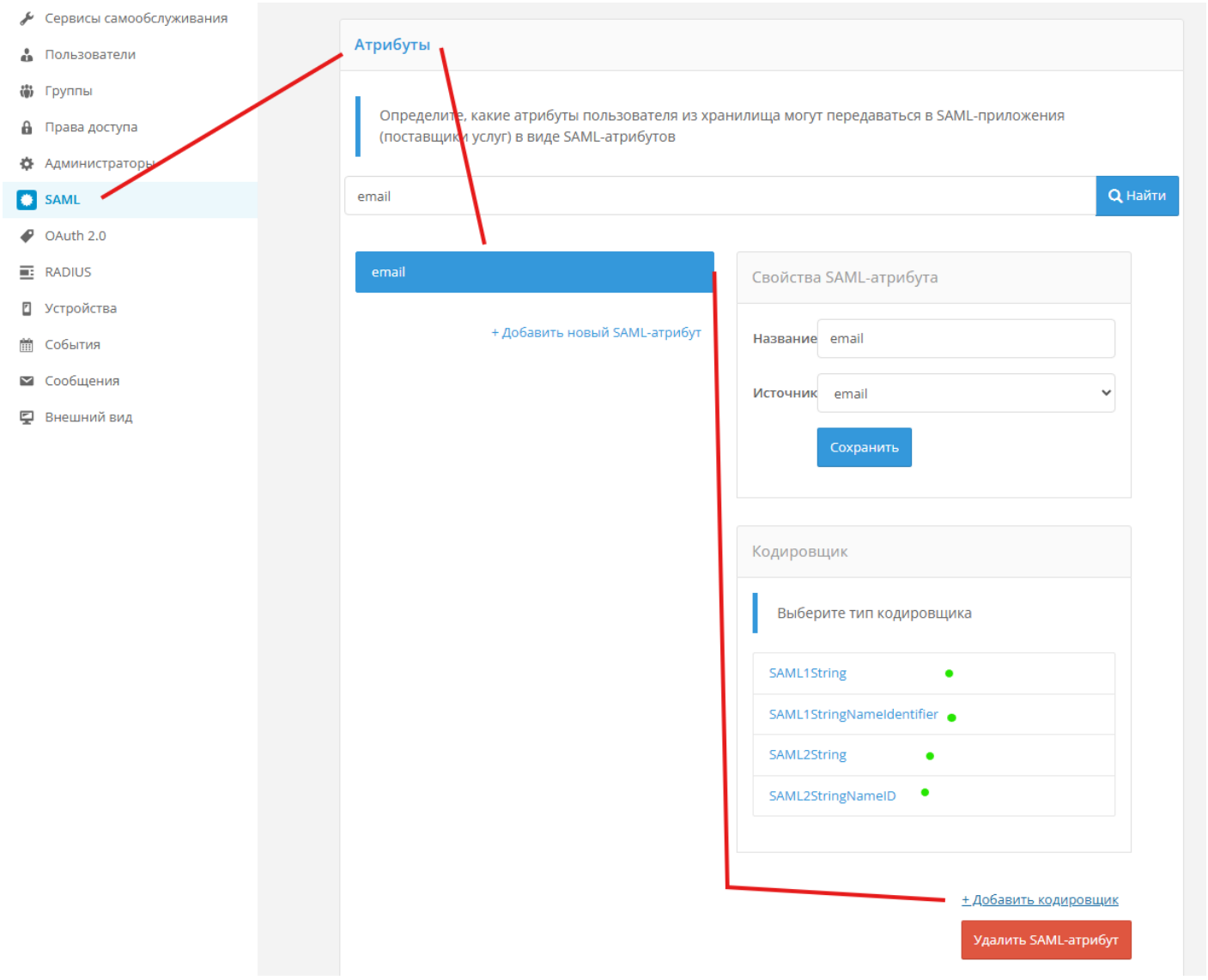
2. В SAML помимо значения атрибута передается еще и его тип. Для вновь созданного SAML атрибута необходимо настроить как минимум один кодировщик, иначе атрибут передан не будет.
   Для AD FS нужно выбирать кодировщик SAML2. Для SAML2 есть два кодировщика: **String** и **StringNameID**.

Важно:

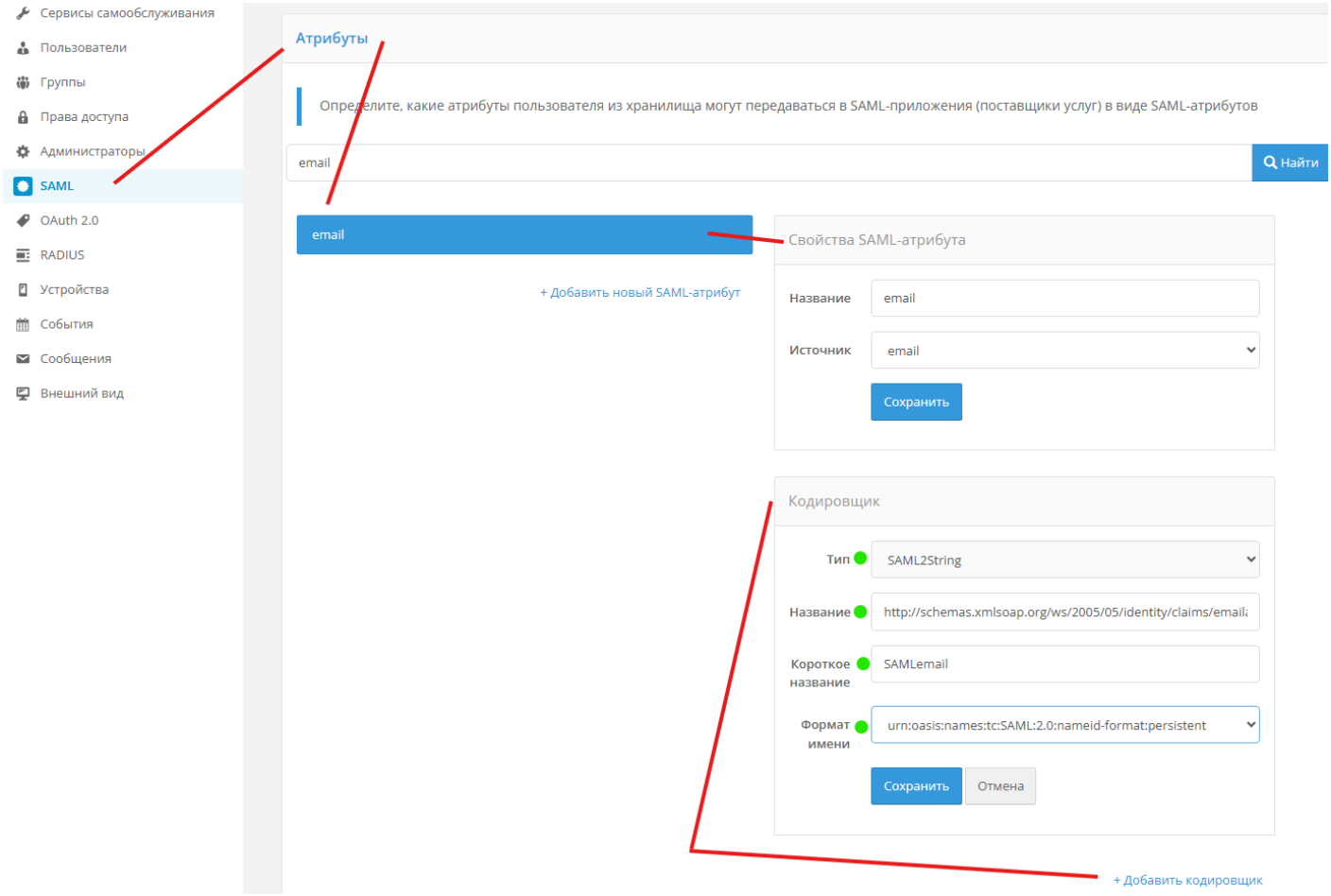
По спецификации SAML в ответе должен быть один атрибут **NameID** (не ноль и не два и более), иначе ответ будет считаться ошибочным и принят клиентом не будет.

Настройте хотя бы один кодировщик для типа **NameID**, тогда значение передаваемого в нем атрибута будет сопоставлено с внутренним атрибутом AD FS под названием **Name** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`.

Правильным будет в **NameID** передавать атрибут `sub` из Blitz IDP, таким образом будет выполнено сопоставление уникальных идентификаторов в обеих системах. Количество атрибутов с кодировщиком String не ограничено.



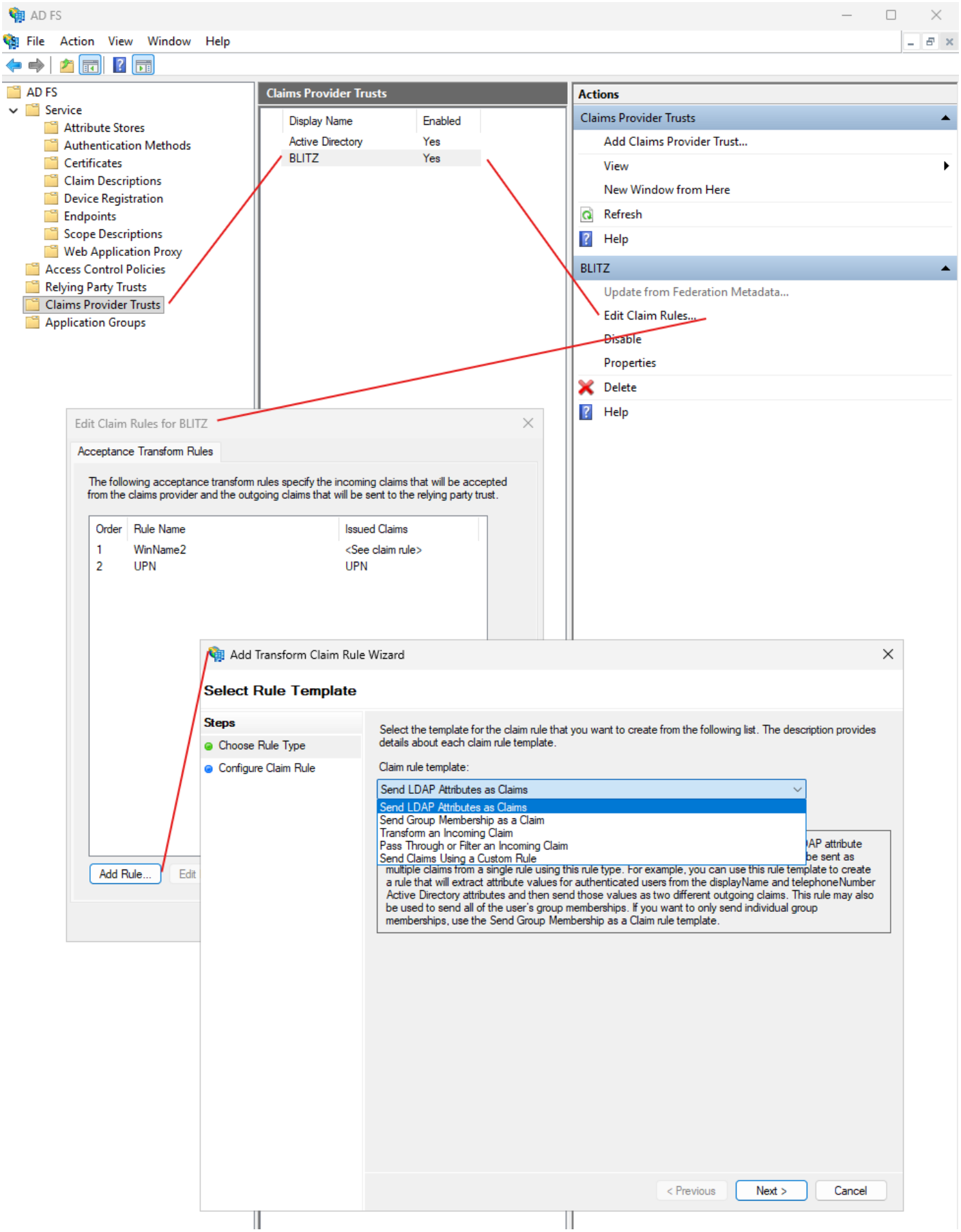
3. После выбора типа кодировщика нужно выбрать Название из Приложения 1 - по нему AD FS определяет к какому внутреннему атрибуту AD FS относится входящий атрибут из SAML-Response, который формирует Blitz IDP. Формат имени обычно `persistent`, проверить можно в метаданных AD FS по пути `/EntityDescriptor/SPSSODescriptor/` - тут перечислены допустимые **NameID**.



Шаг 2. Настройка на стороне AD FS

1. Помимо известного для AD FS названия атрибута нужно настроить его приём в AD FS для возможности дальнейшей обработки\передачи. В **Claim Provider Trusts** выберите настроенный ранее провайдер Blitz IDP, справа нажмите **Редактировать правила обработки утверждений**, добавьте новое правило из имеющихся шаблонов, а также введите дополнительную информацию, нужную для работы правила.

   Полное описание правил.

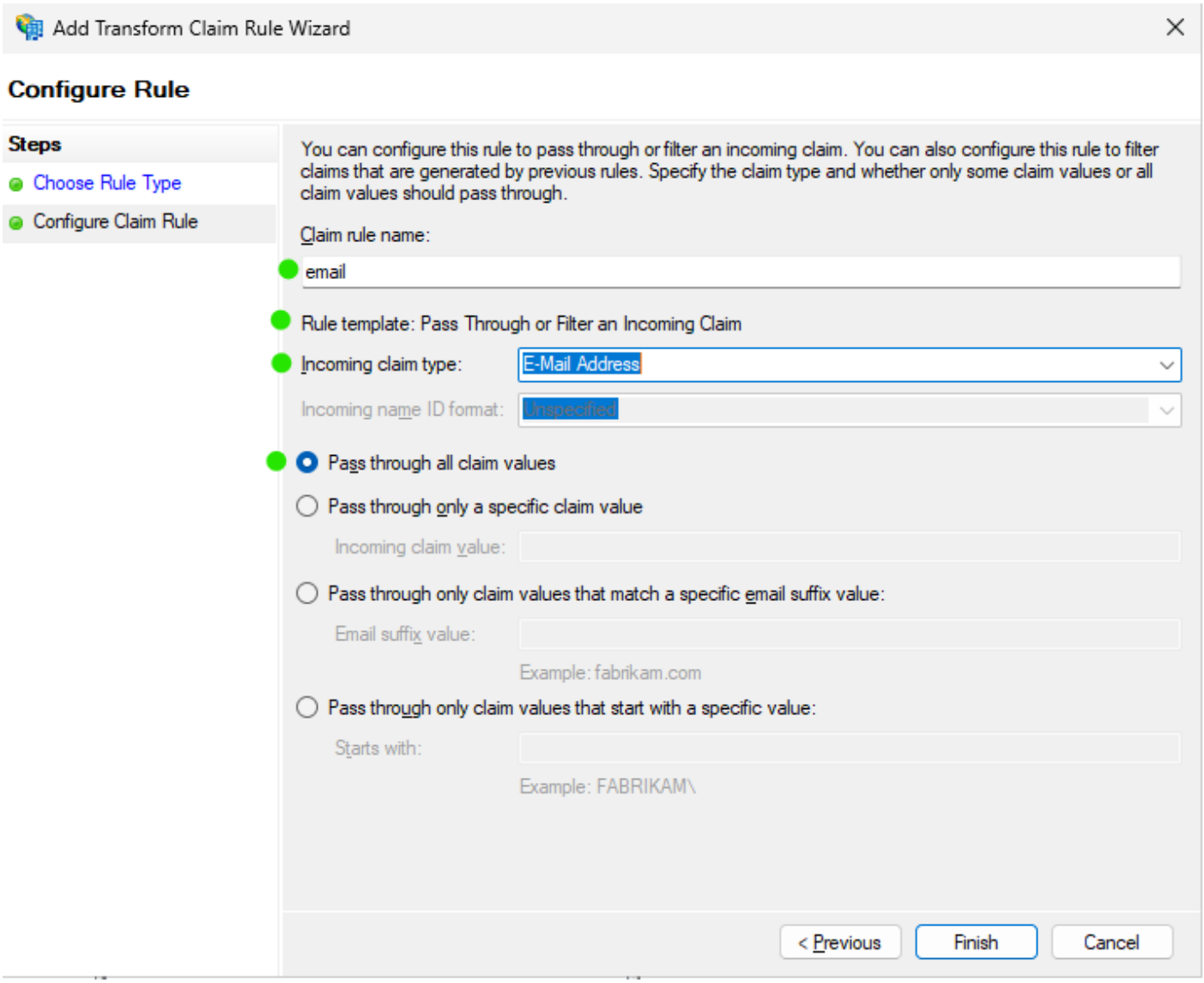


2. Для простого приёма атрибута в AD FS без его изменения выберите правило "*Проход через входящие утверждение или его фильтрация*":

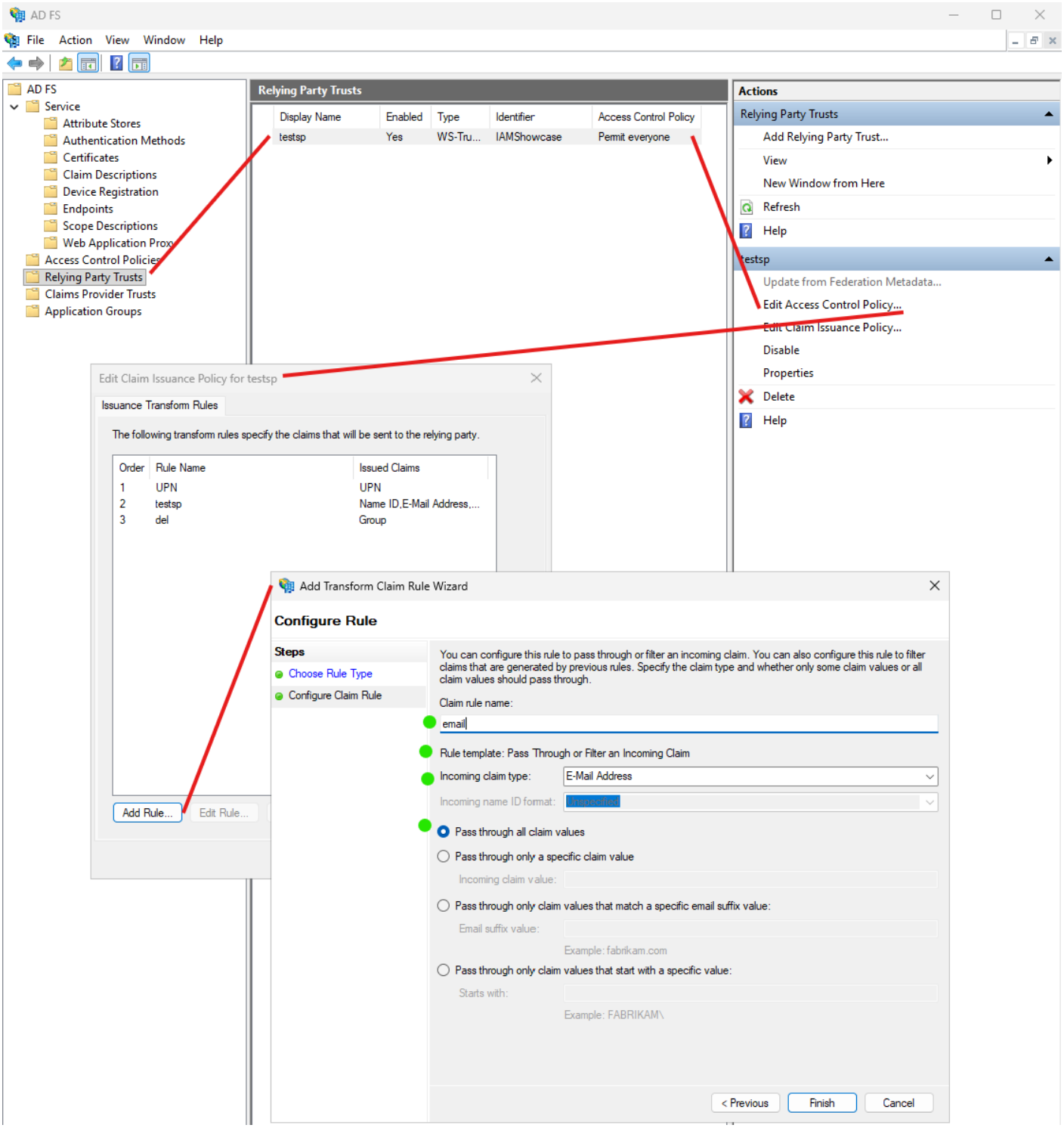
   Название: любое понятное,

ниже - выбранный ранее **шаблон**,

Тип входящего утверждения должен соответствовать "Имени в ADFS" из Приложения 1

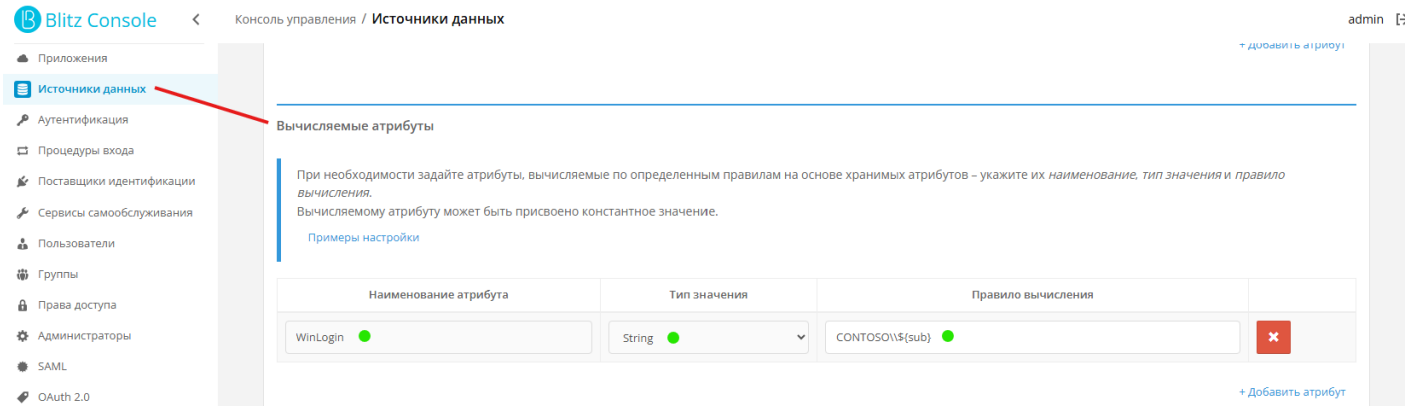


3. Для простой передачи атрибута в клиентское приложение нужно добавить правило "*Проход через входящие утверждение или его фильтрация*" в политику выдачи утверждений в настройках приложения:

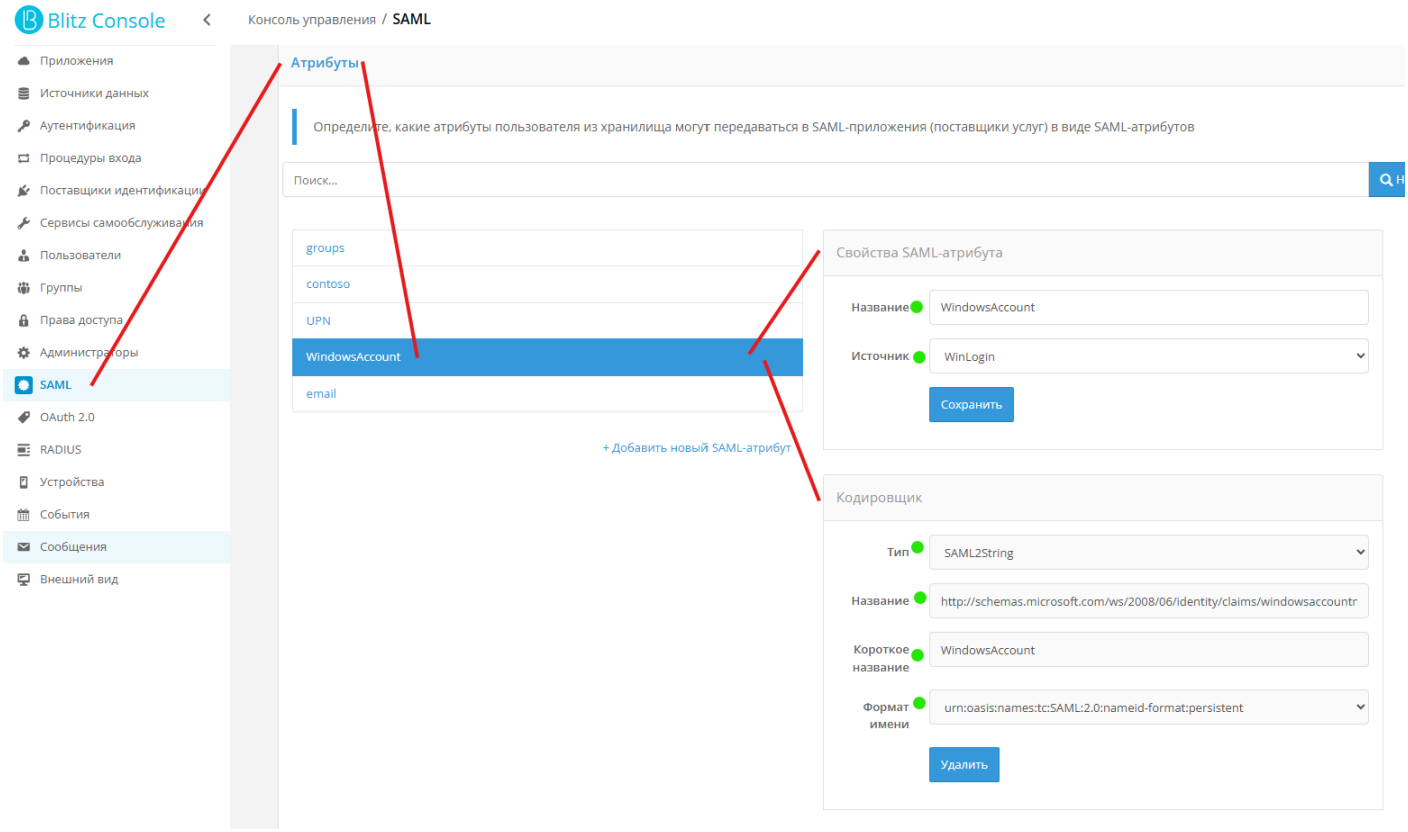


Вариант 2. Настройка передачи данных из AD при аутентификации через внешний провайдер

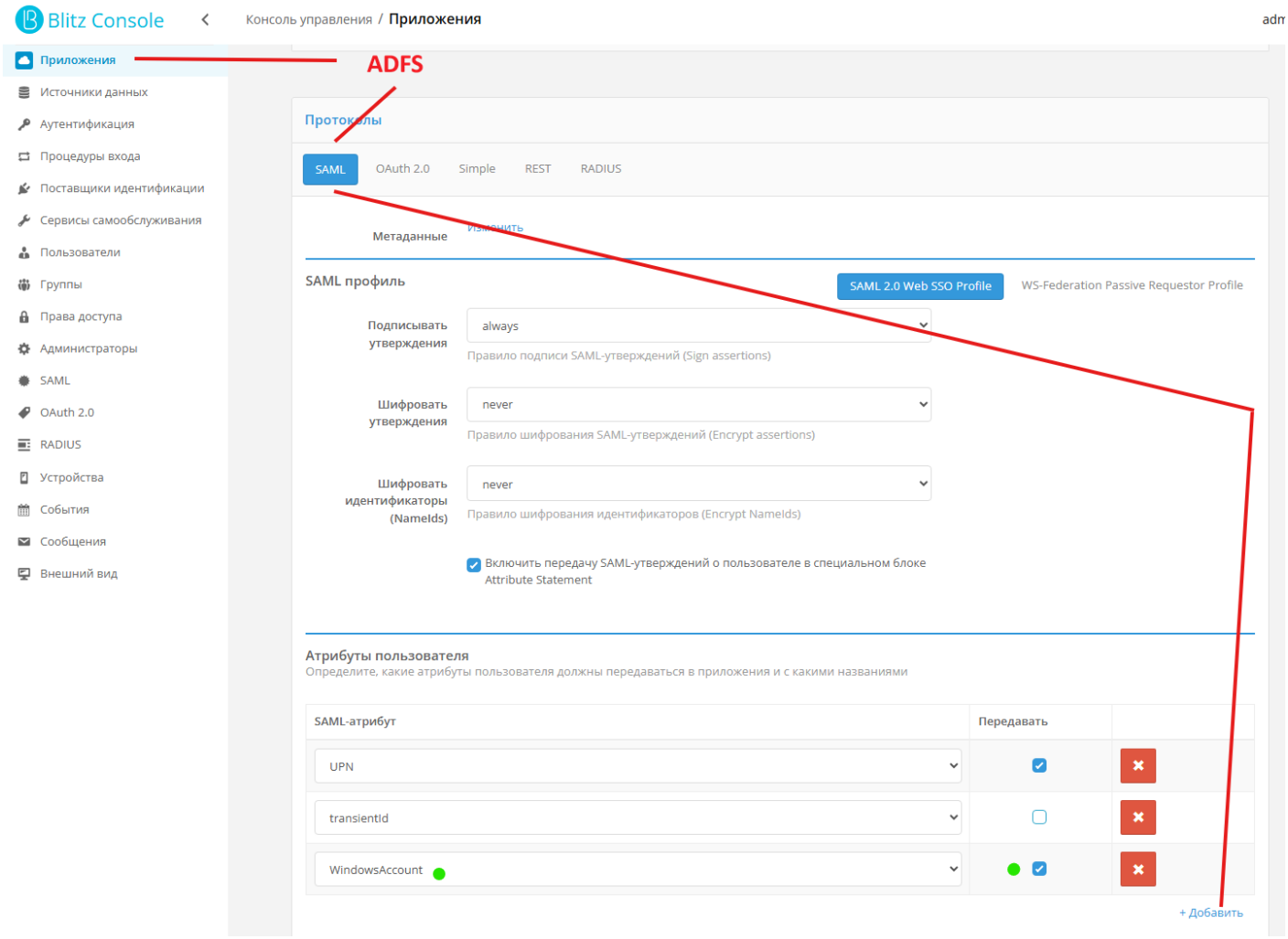
1. В Blitz IDP надо настроить передачу атрибута с названием в кодировщике `http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname` и значением `NetBIOS-имя-домена\пользователь: CONTOSO\user`. В AD атрибута с таким значением у пользователя нет, поэтому будем использовать вычисляемый атрибут в Blitz IDP. Создаём вычисляемый атрибут с правилом вычисления `CONTOSO\\${sub}`:



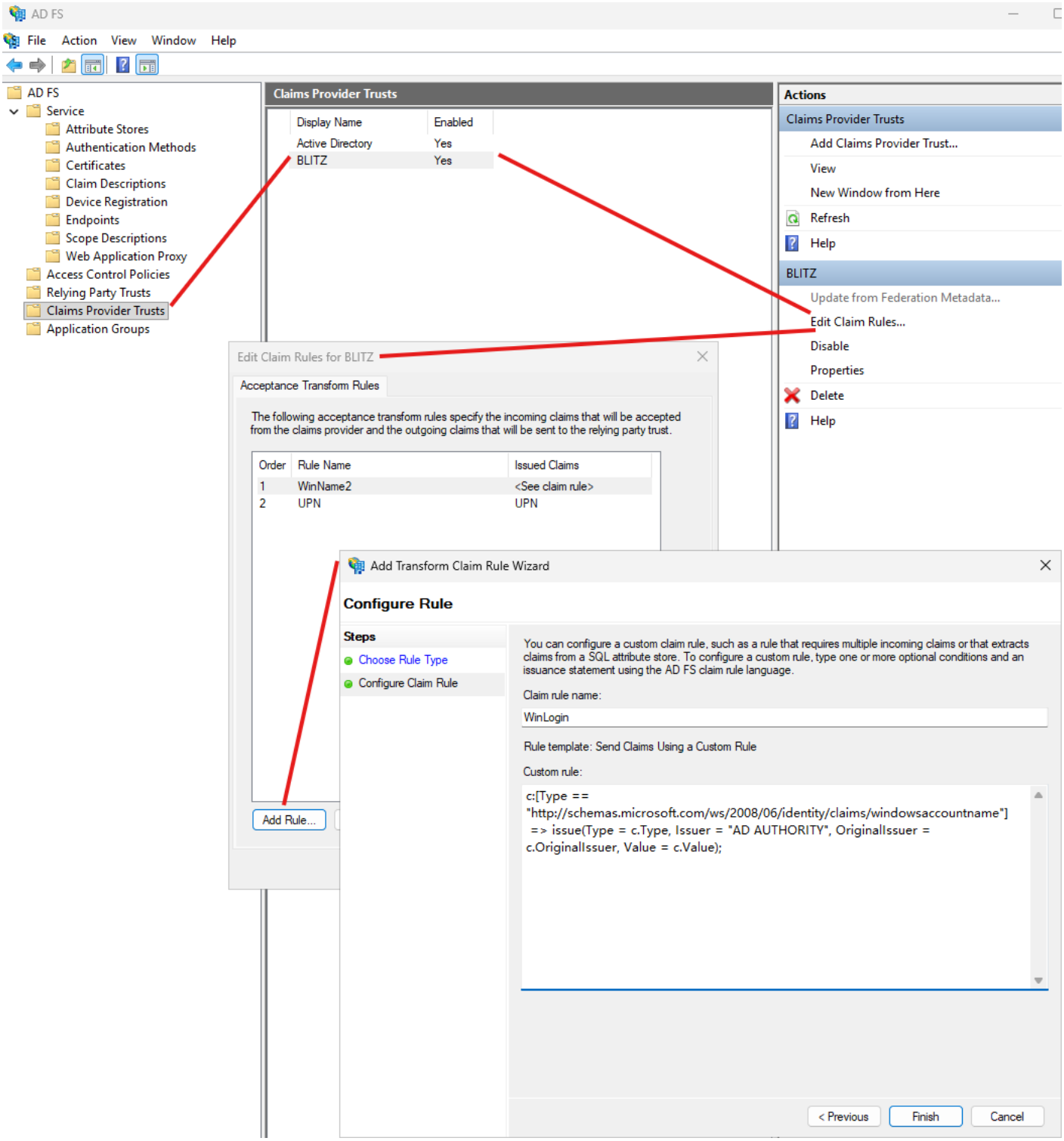
2. Настройте SAML-атрибут и Кодировщик для него:



3. В приложении для подключения AD FS настройте передачу созданного атрибута:



4. В AD FS для провайдера нужно создать кастомное правило обработки утверждений, которое меняет подпись для утверждения `http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname` из внешнего провайдера на "AD AUTHORITY" - без такой подписи AD поиск пользователя отклонит:



Правило:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type = c.Type, Issuer = "AD AUTHORITY", OriginalIssuer = c.OriginalIssuer, Value = c.Value);
```

Дополнительно

Атрибуты и названия claim внешнего провайдера для их автоматического маппинга в AD FS

Имя в ADFS	Описание	Название атрибута для передачи
E-Mail Address	The e-mail address of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Given Name	The given name of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Name	The unique name of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
UPN	The user principal name (UPN) of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
Common Name	The common name of the user	http://schemas.xmlsoap.org/claims/CommonName
AD FS 1.x E-Mail Address	The e-mail address of the user when interoperating with AD FS 1.1 or AD FS 1.0	http://schemas.xmlsoap.org/claims/EmailAddress
Group	A group that the user is a member of	http://schemas.xmlsoap.org/claims/Group
AD FS 1.x UPN	The UPN of the user when interoperating with AD FS 1.1 or AD FS 1.0	http://schemas.xmlsoap.org/claims/UPN
Role	A role that the user has	http://schemas.microsoft.com/ws/2008/06/identity/claims/role
Surname	The surname of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
PPID	The private identifier of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
Name Identifier	The SAML name identifier of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
Authentication Method	The method used to authenticate the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod
Deny Only Group SID	The deny-only group SID of the user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid
Deny only primary SID	The deny-only primary SID of the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarysid

Имя в ADFS	Описание	Название атрибута для передачи
Deny only primary group SID	The deny-only primary group SID of the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarygroupsid
Group SID	The group SID of the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid
Primary group SID	The primary group SID of the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid
Primary SID	The primary SID of the user	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid
Windows account name	The domain account name of the user in the form of <domain>\\<user>	http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname

---

Версия #22
Андрей Гордеев создал 2026-04-16 15:19:18 UTC
Обновлено 2026-05-08 15:24:19 UTC