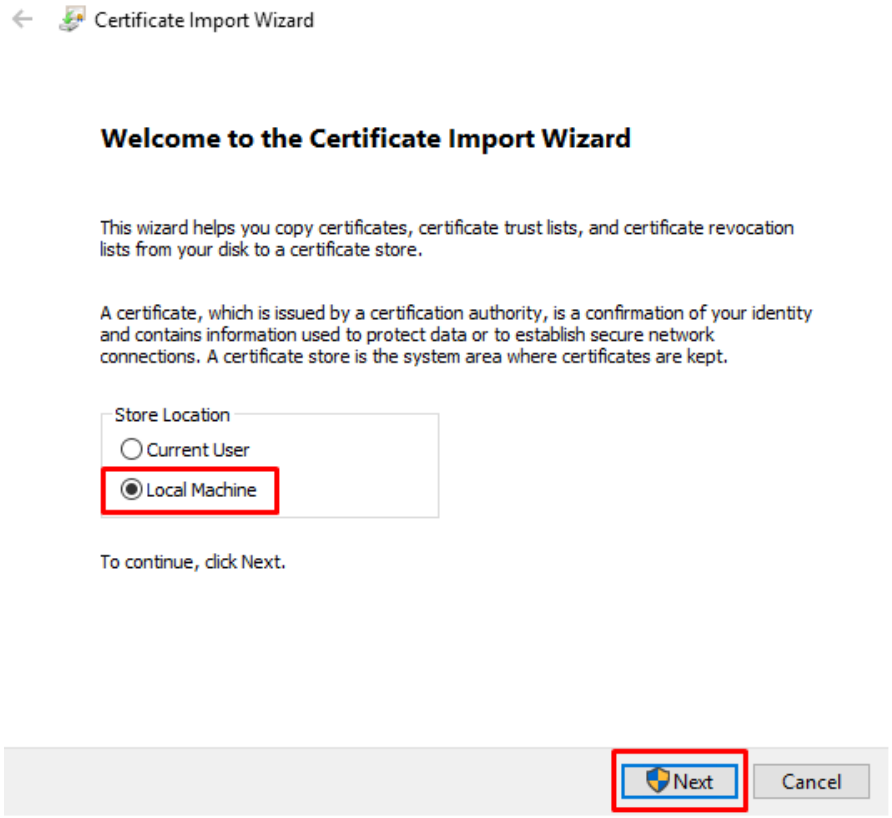
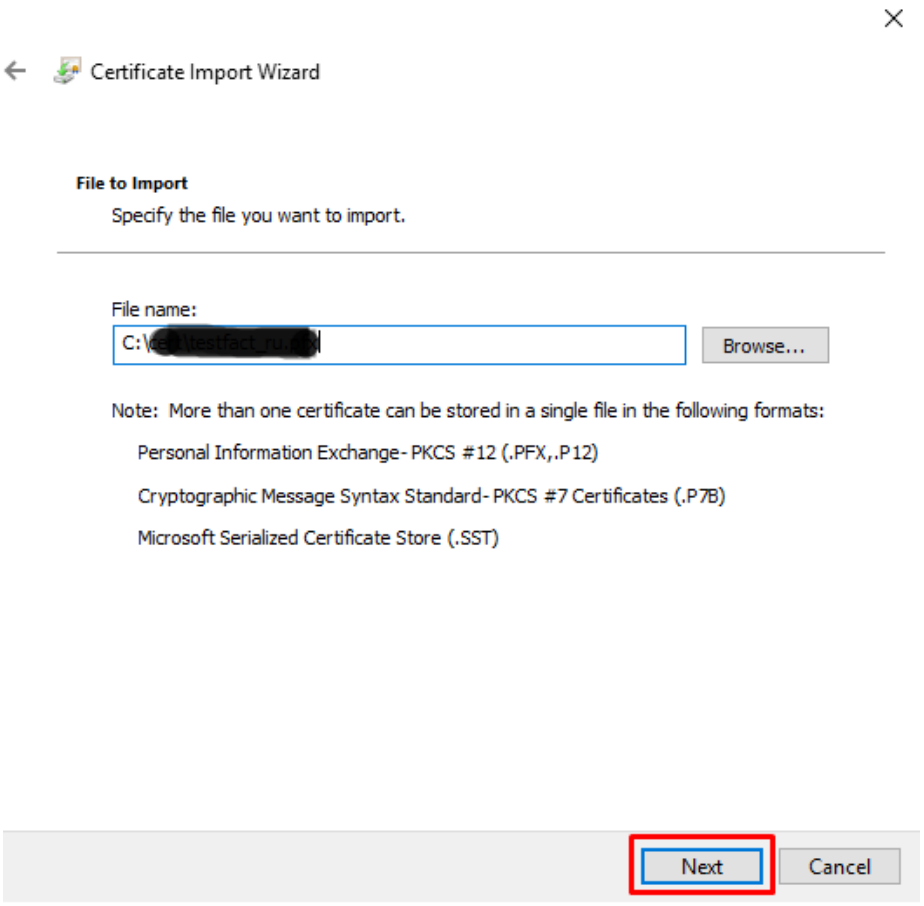
Развертывание ADFS на Windows Serverдля авторизации на внешних площадках

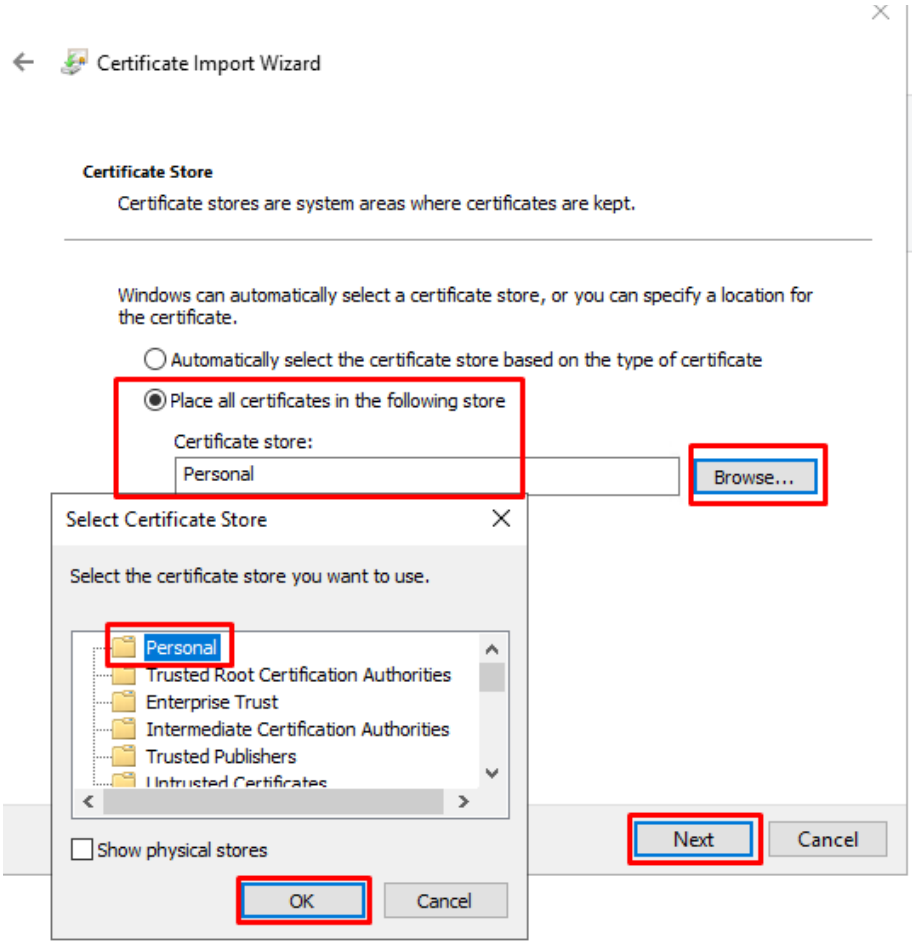
Подготовительные действия

1.1. Добавить и настроить роль AD, завестипользователей.
1.2. Добавить ролыIIS
1.3. Сгенерировать самоподписанный SSL сертификат (как сгенерировать самодписаный SSL сертификат),либо использовать выпущенный для имеющегося домена

1.4. Если будет использоваться выпущенный сертификат, то необходимо выполнить его импорт

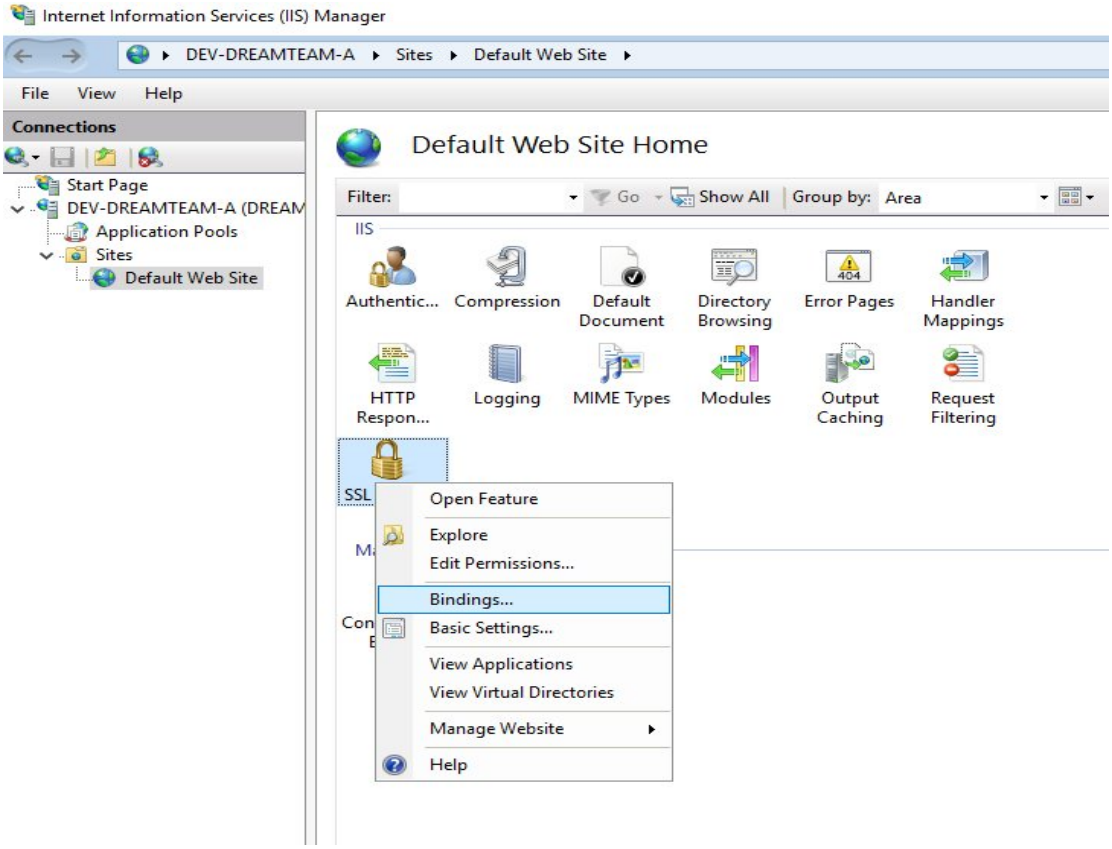


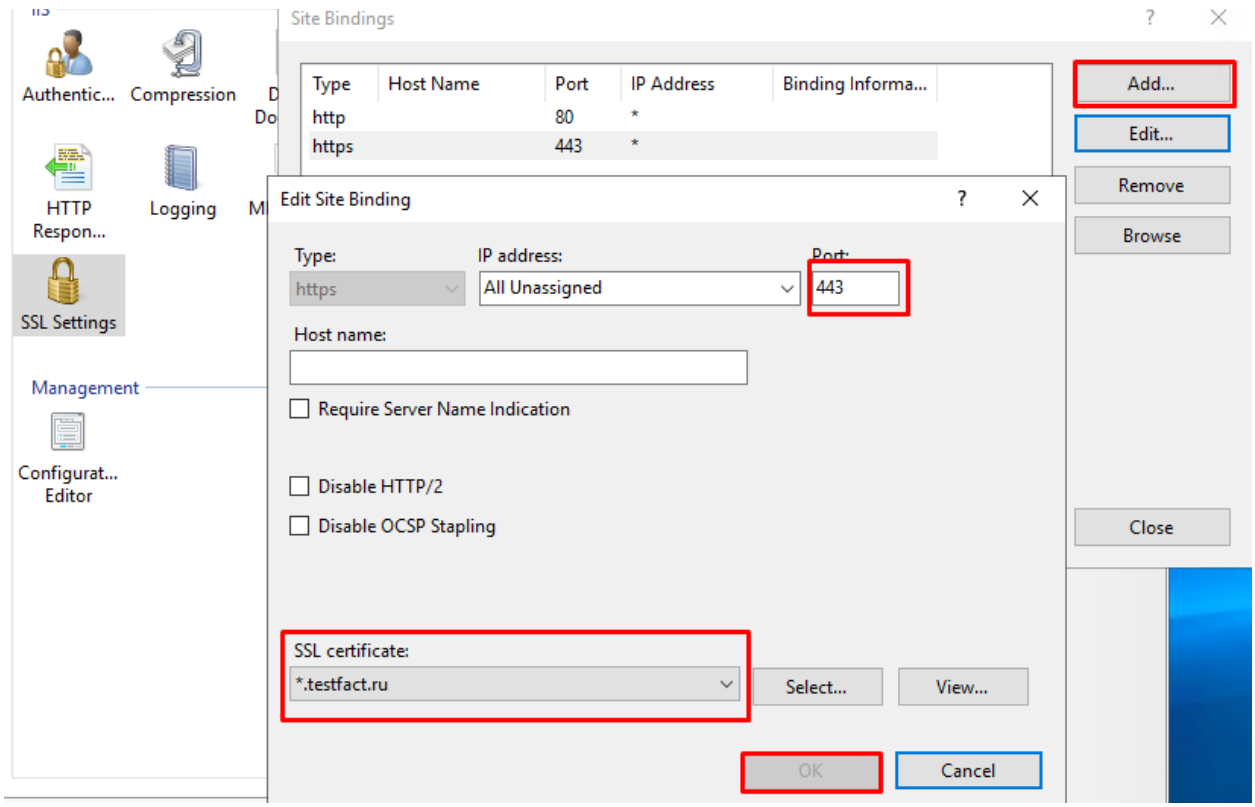




Нажать «Next», а на следующем экране «Finish».

1.5. Открыть оснастку управления IIS и для «Default Web Site» в секции SSL Settings выбрать пункт «Bindings...», добавить порт 443 и выбрать импортированный ранее сертификат.

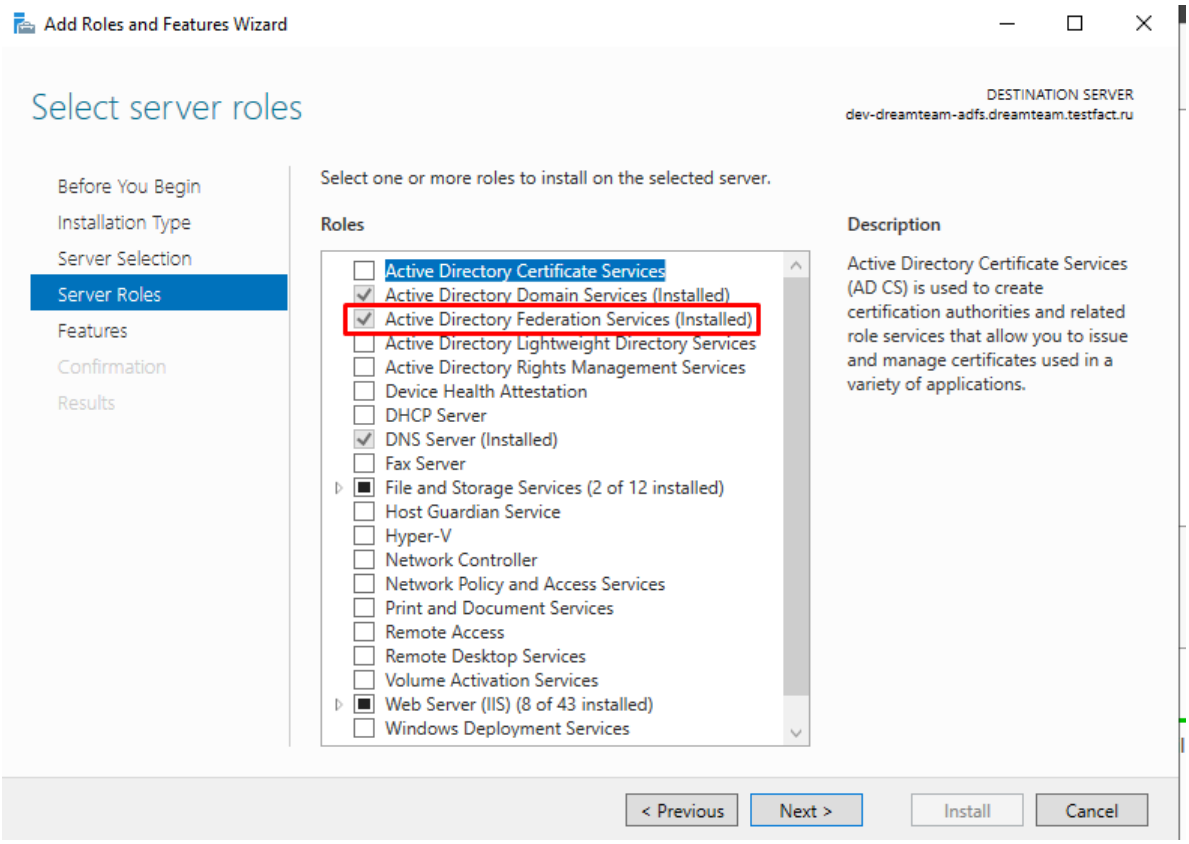




1.6. Создать пользователя в AD (например ADFS_SVC). Это специальный сервисный аккаунт для подключения к AD.

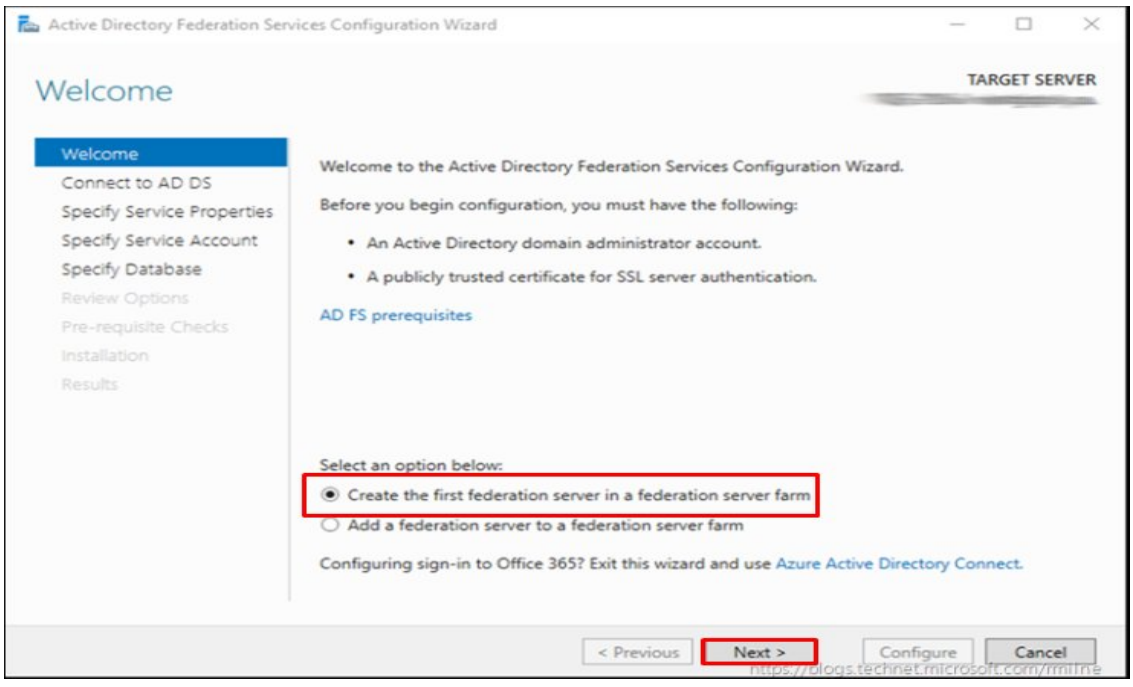
Добавление и настройка ADFS

2.1. Добавить роль ADFS

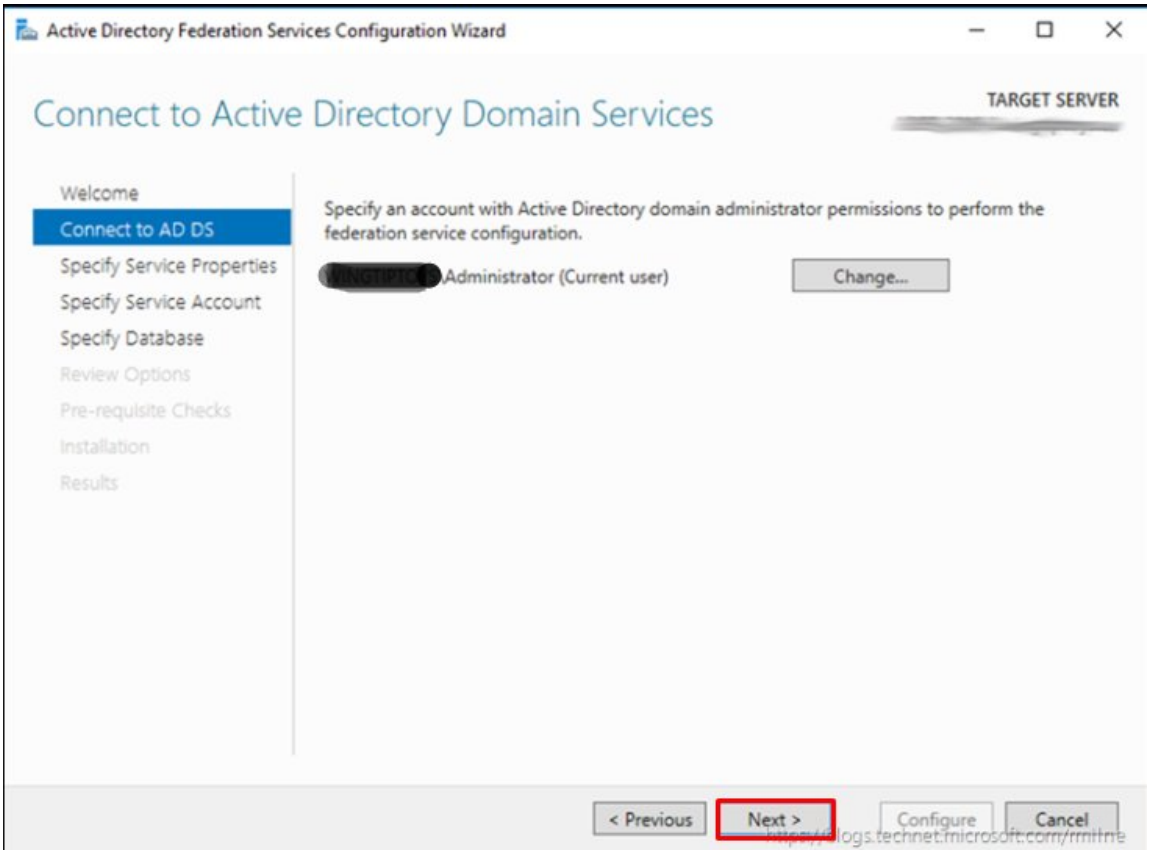


2.2. После установки необходимо вызвать мастер конфигурирования ADFS

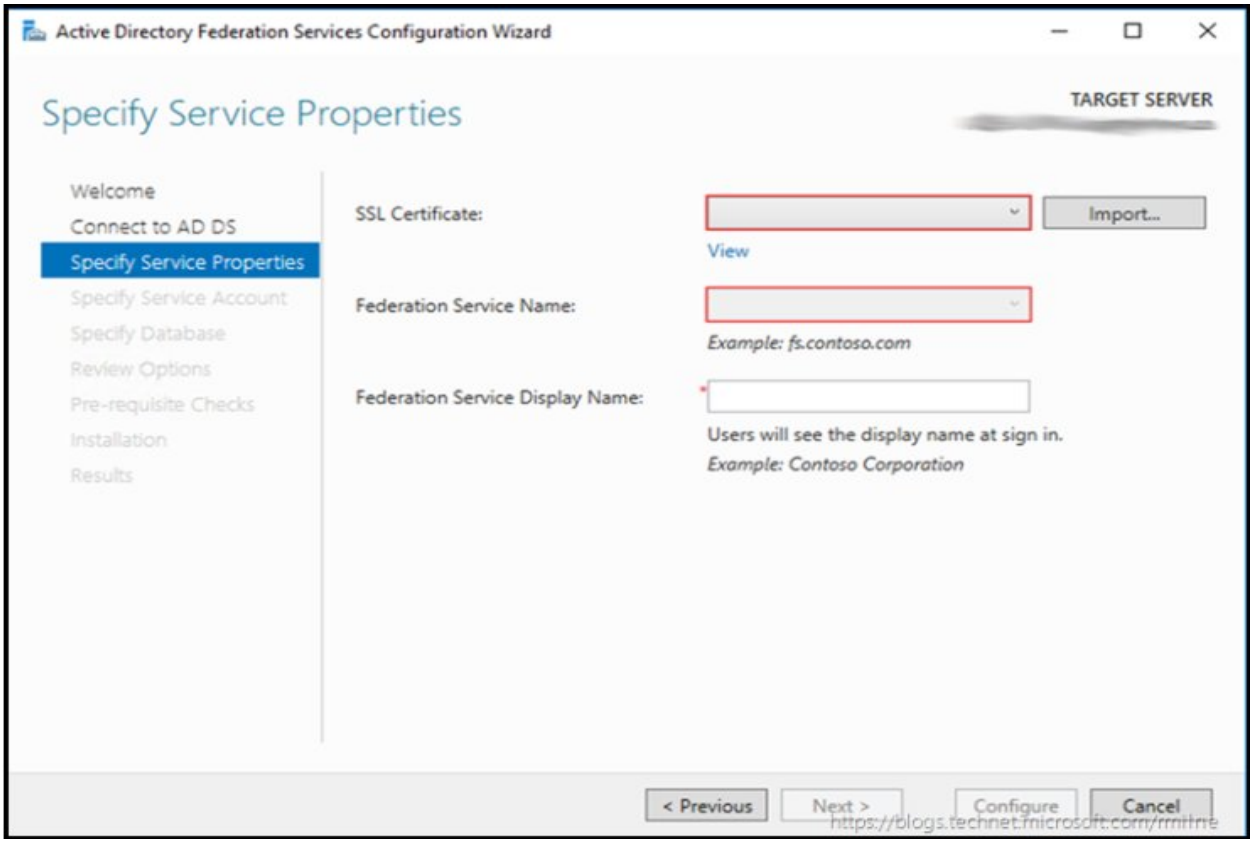
2.3. Шаги мастера настройки следующие:



Указываем УЗ с правами администратора домена, от имени которой будем выполнять конфигурирование



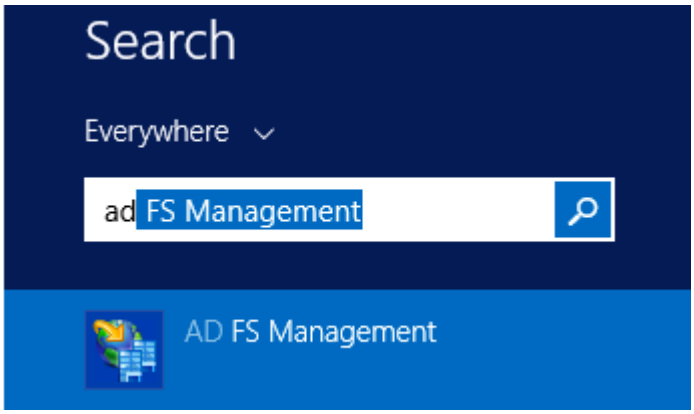
Выбираем сертификат, который мы импортировали на шаге 1.4, имя (например adfs.yourdomain.ru) и выводимое имя (оно будет отображаться на странице авторизации).



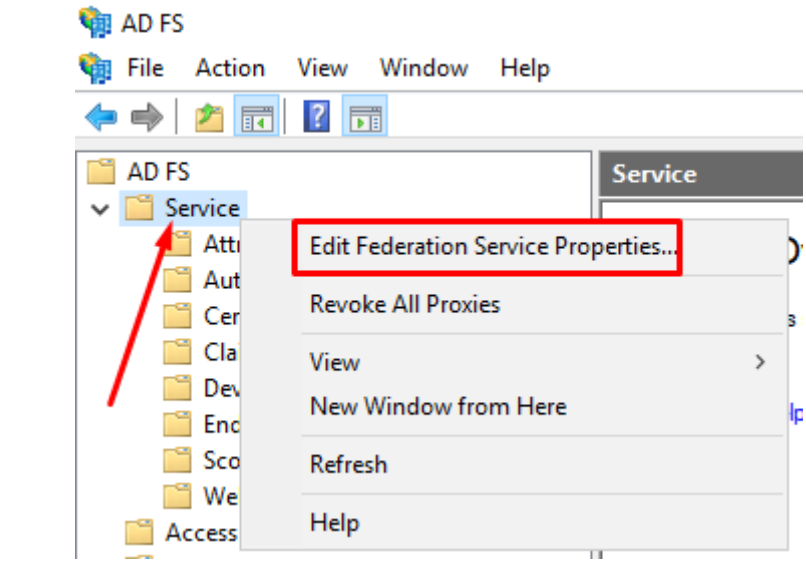
Далее выбираем тип БД, создаем ее и завершаем настройку, пройдя по оставшимся шагам мастера (на этих шагах уже никаких парамеров менять/выбирать не нужно).

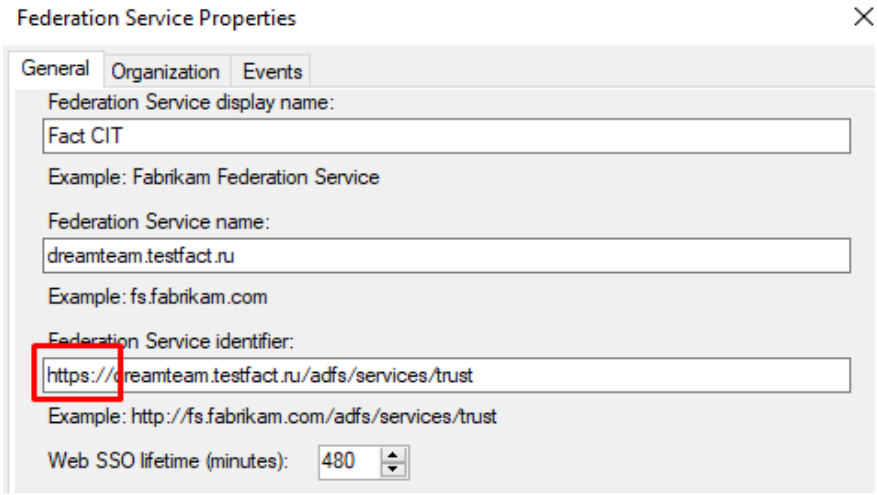
Настройка ADFS

3.1. Запускаем оснастку управления



3.2. Убедимся, что используется протокол HTTPS. Если HTTP, то меняем на HTTPS (иначе при отправке запросов на авторизацию будем получать ошибку)

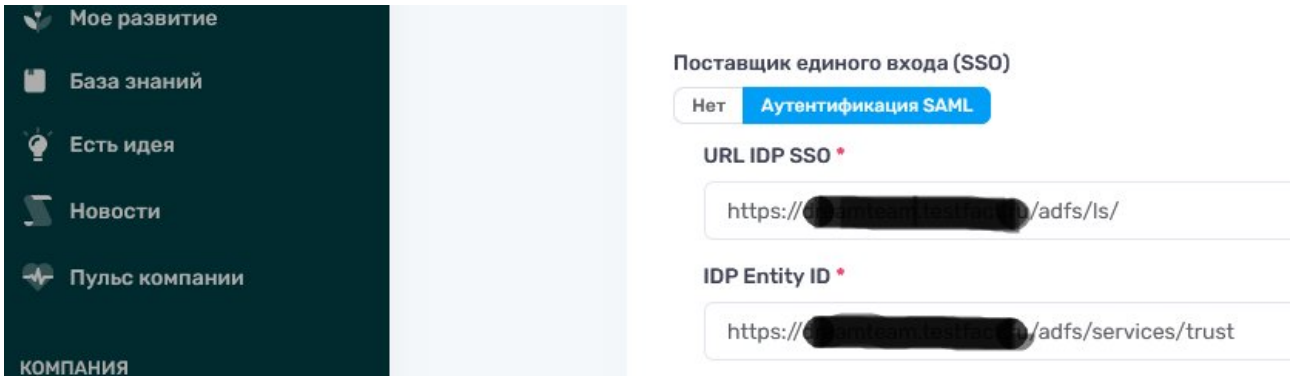




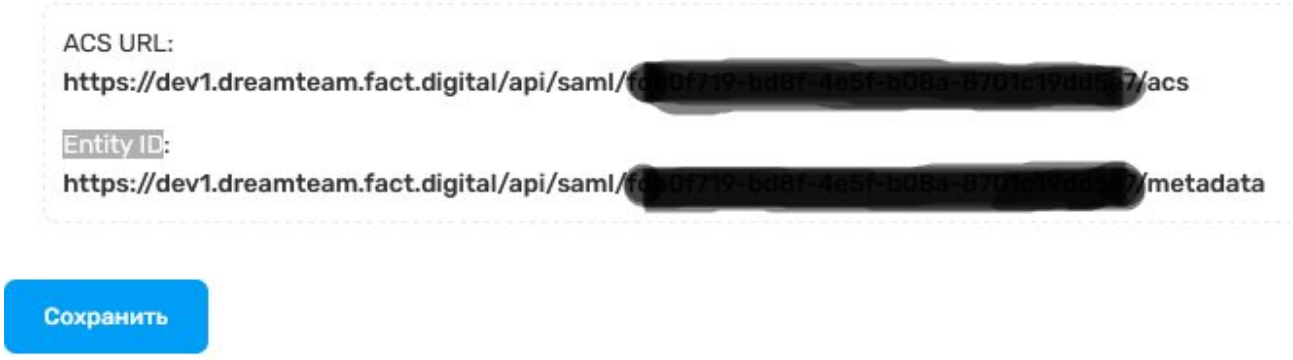
3.3 Выполнить вход в https://dev1.dreamteam.fact.digital под своей учетной записью

3.4. Перейти в меню «Настройки» - «Аутентификация», активировать «Аутентификация SAML», внести информацию в следующие поля и нажать «Сохранить».

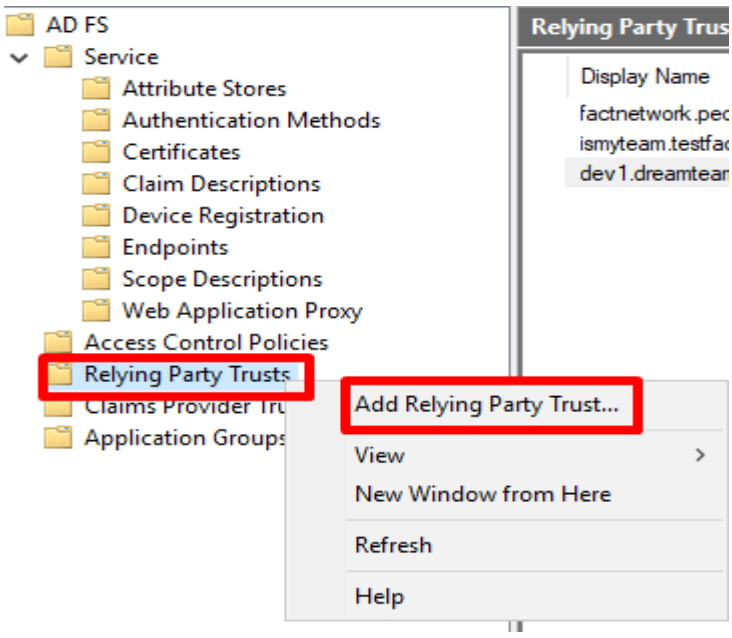
URL IDP SSO https://adfs.yourdomain.ru/adfs/ls/
IDP Entity ID https://adfs.yourdomain.ru/adfs/services/trust



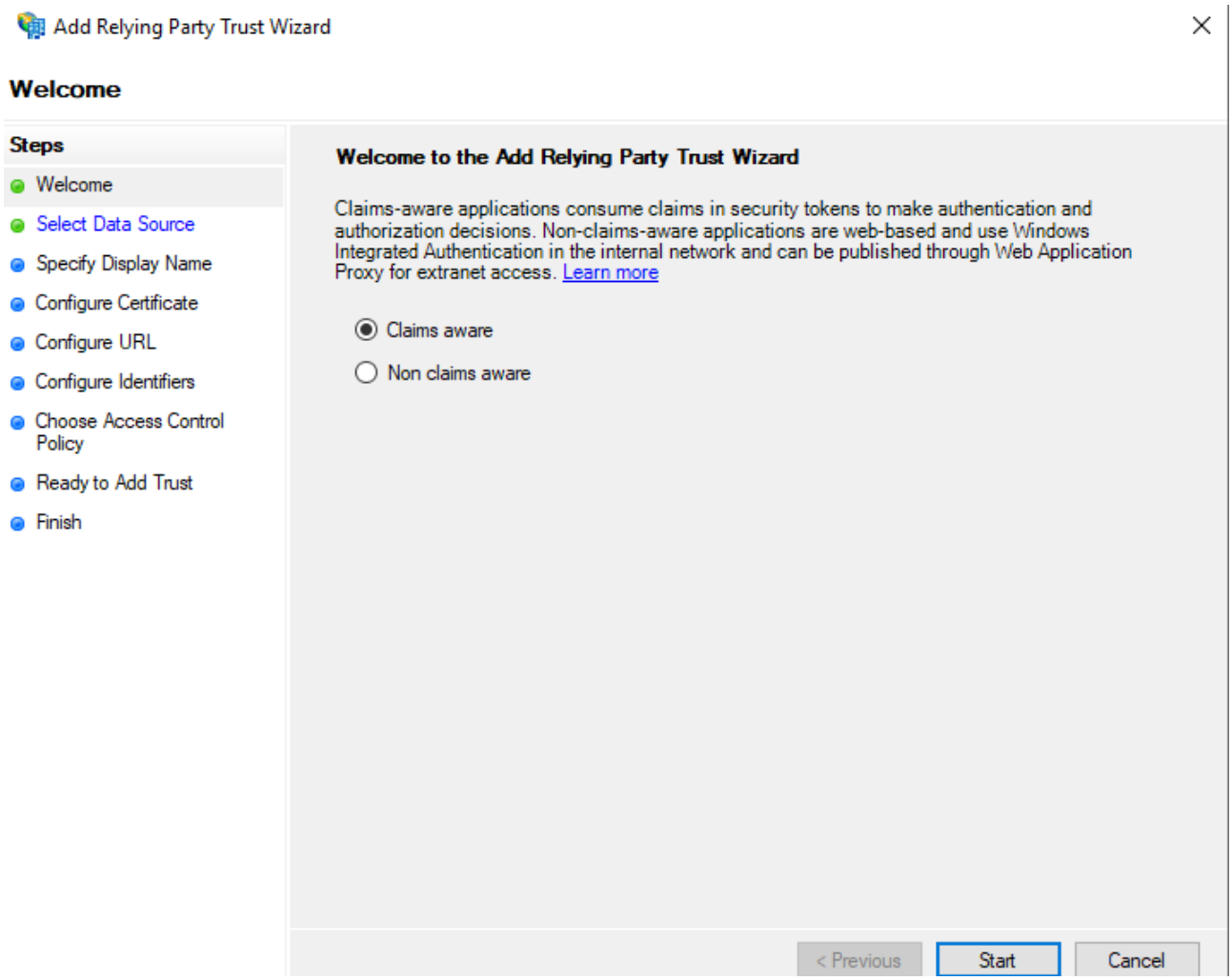
3.5. После нажатия на кнопку «Сохранить» в полях **ACS URL** и **Entity ID** появятся ссылки, которые нам потребуются позже

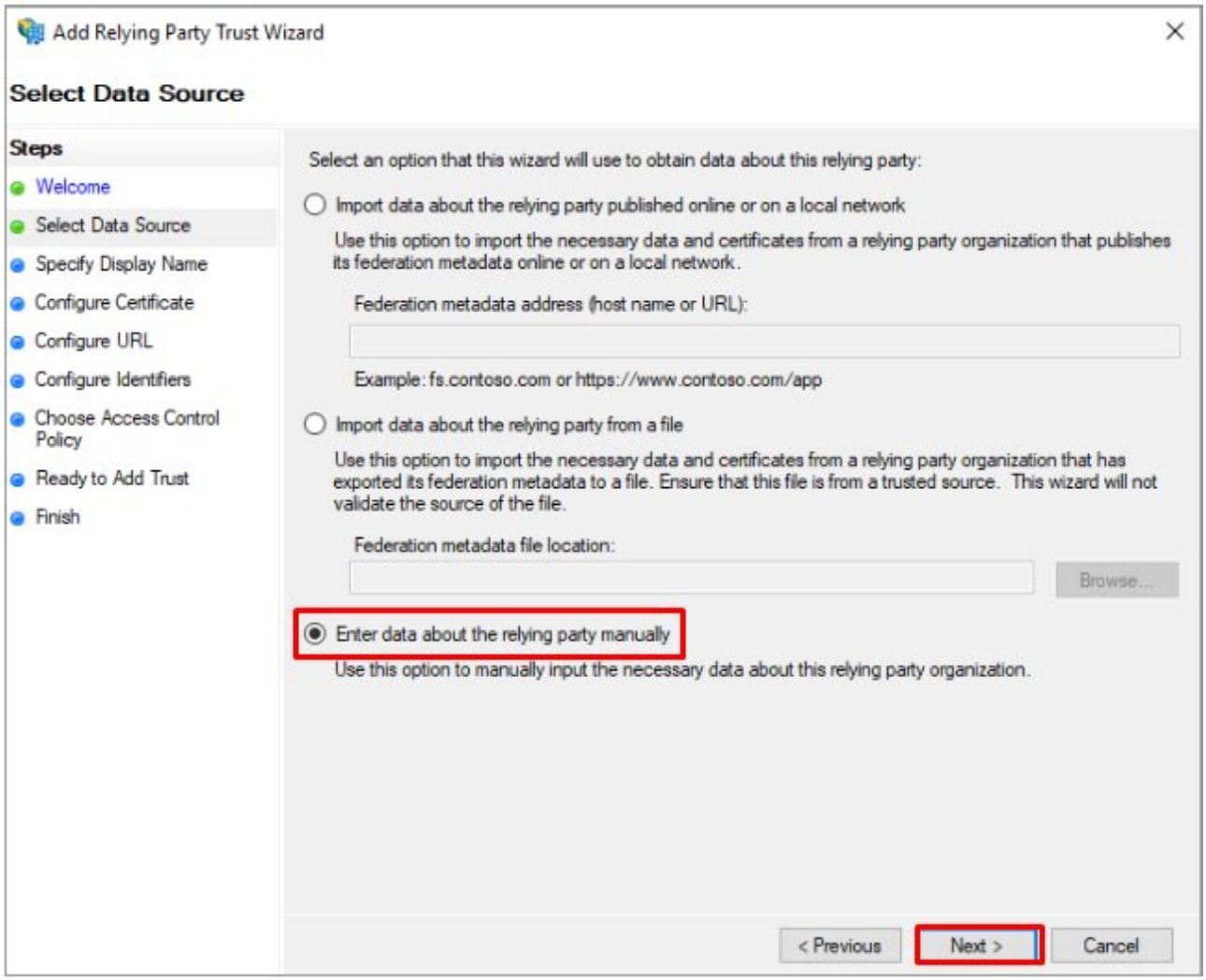


3.6. Возвращаемся в консоль управления ADFS и создаем новый Relying Party Trust



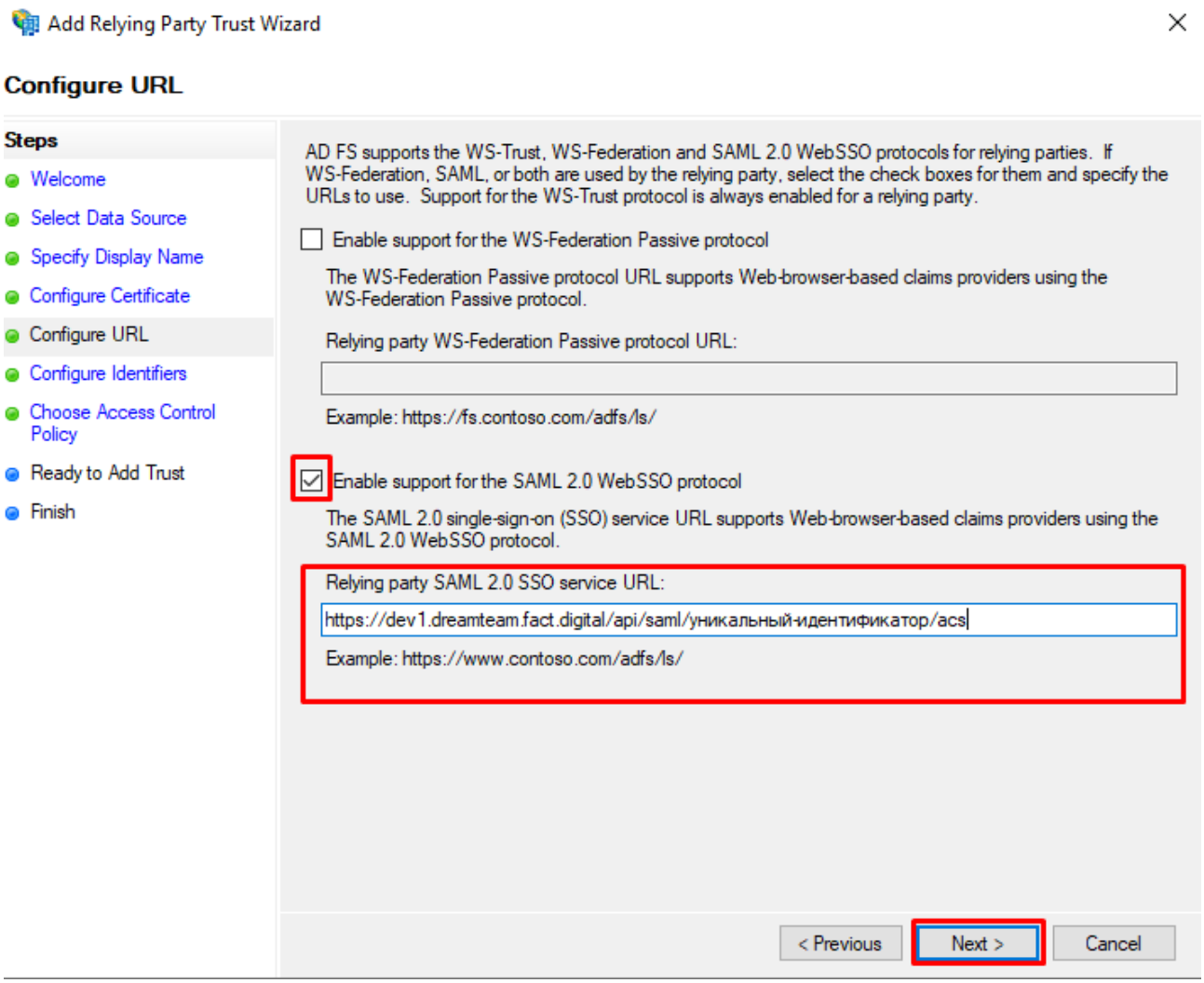
Выбираем тип «Claim aware»



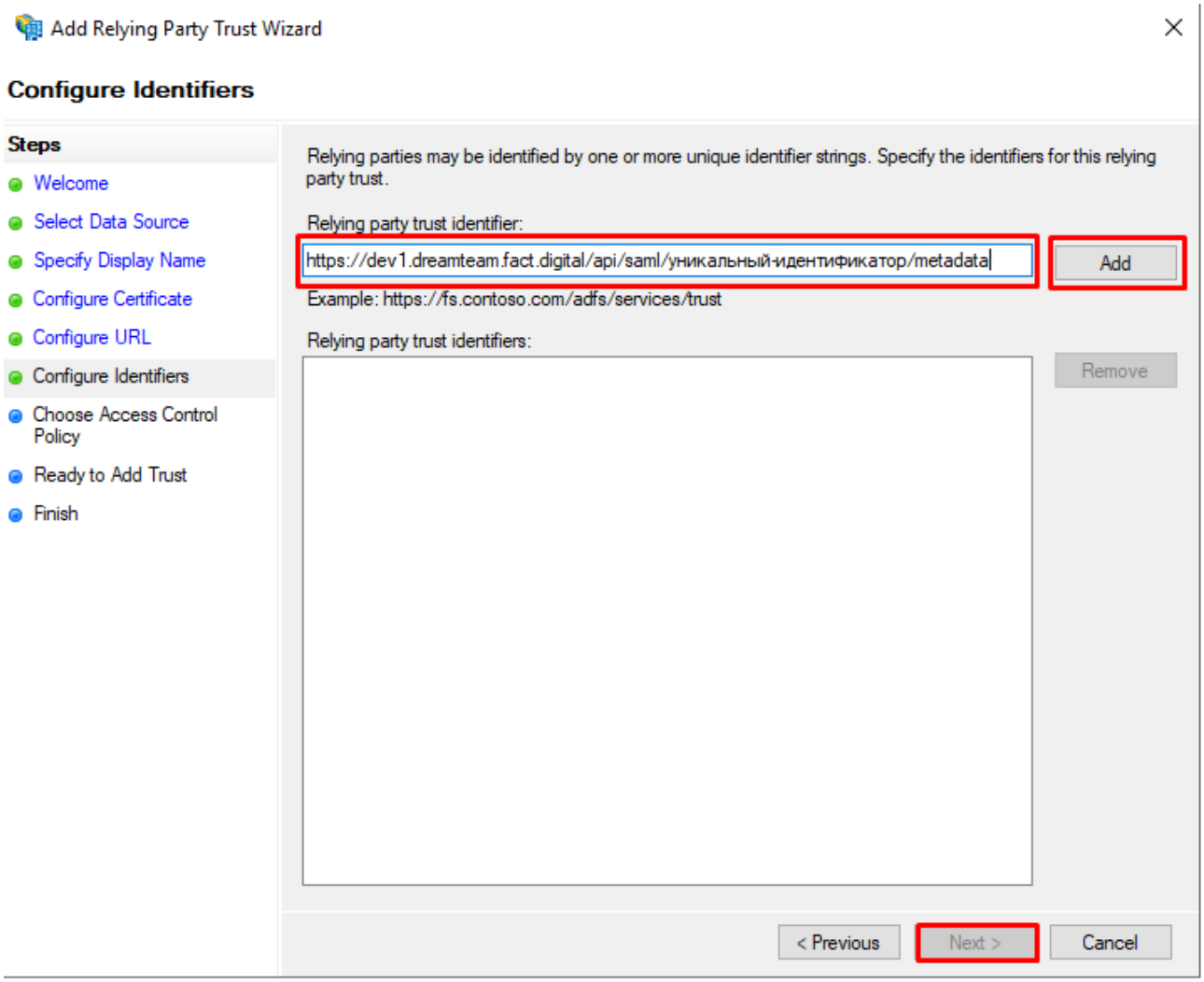


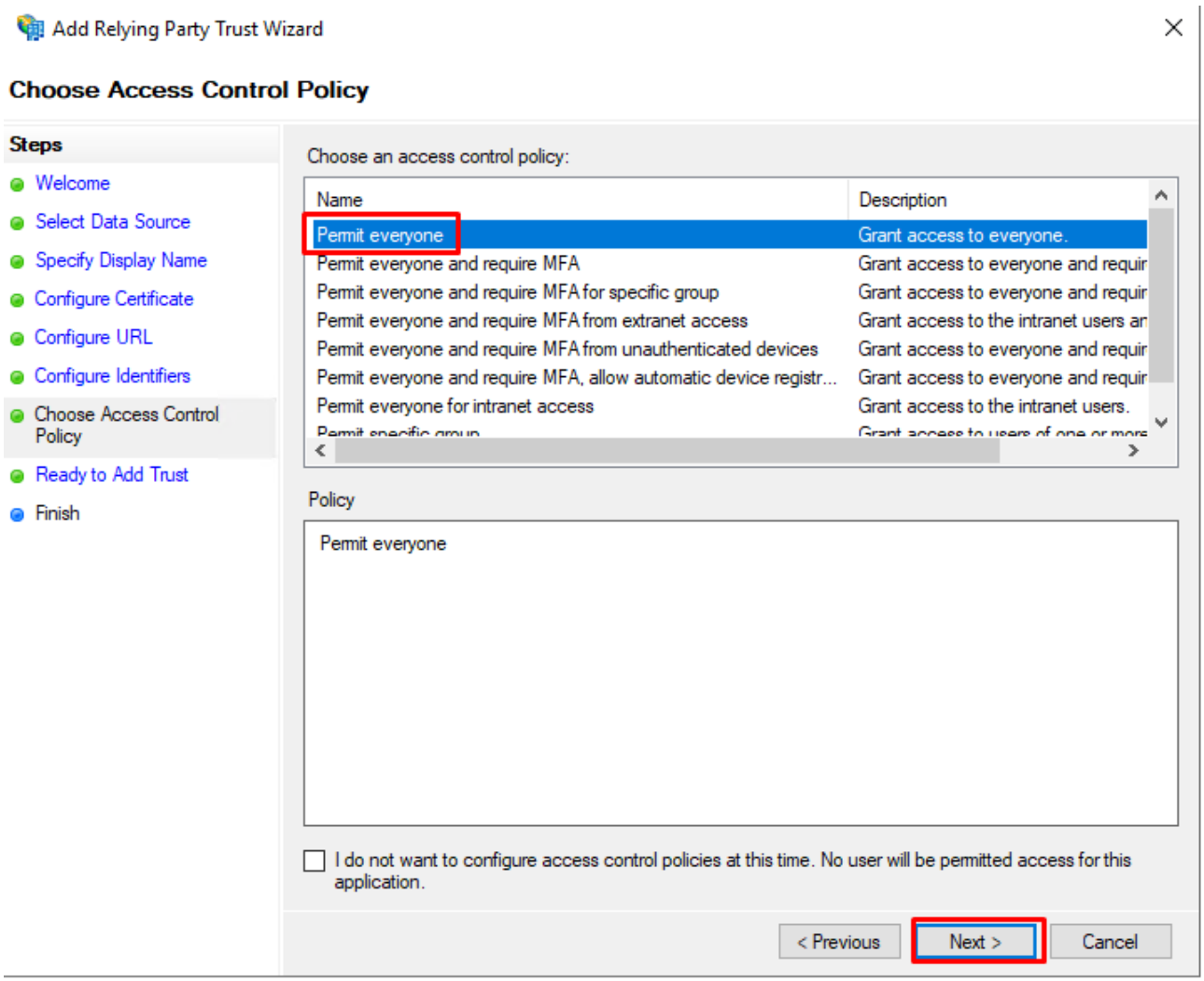
На следующем экране вводим отображаемое имя (можно использовать любое, это ни на что не влияет), нажимаем 2 раза «Next».

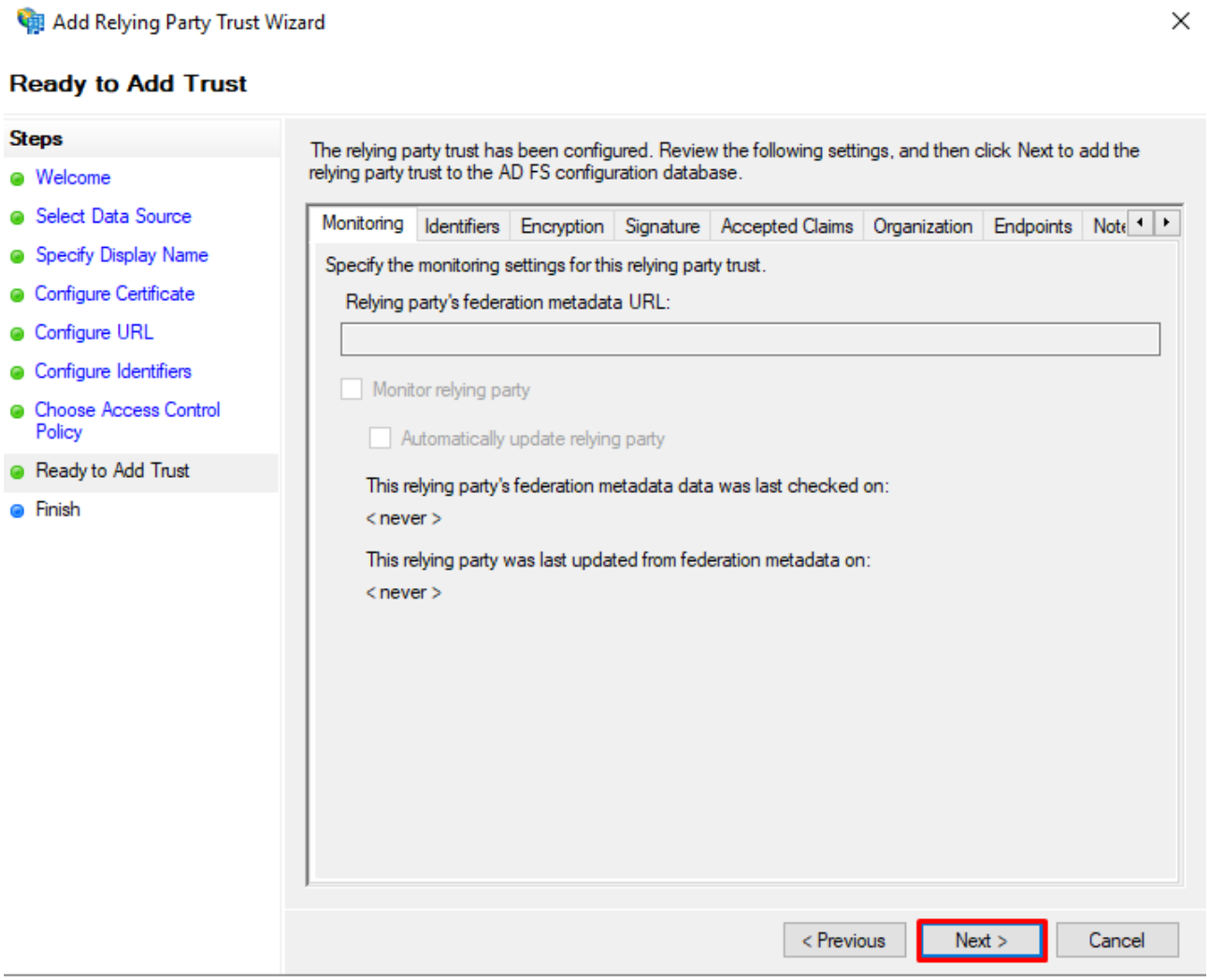
Активируем протокол SAML 2.0 и вставляем ссылку вида https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs из поля **ACS URL** МоейКоманды

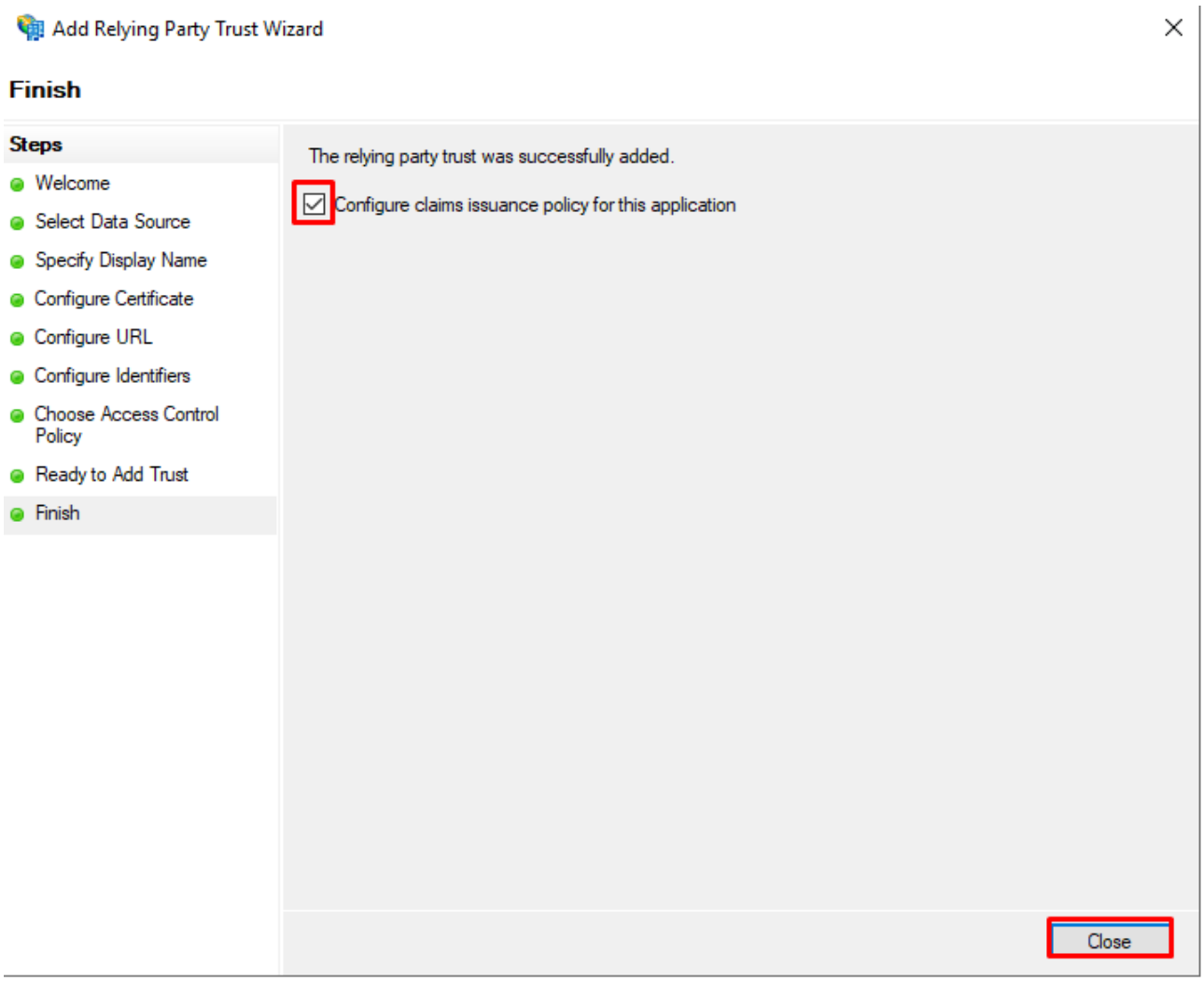


Вставляем ссылку вида https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs из поля **Entity ID** МоейКоманды

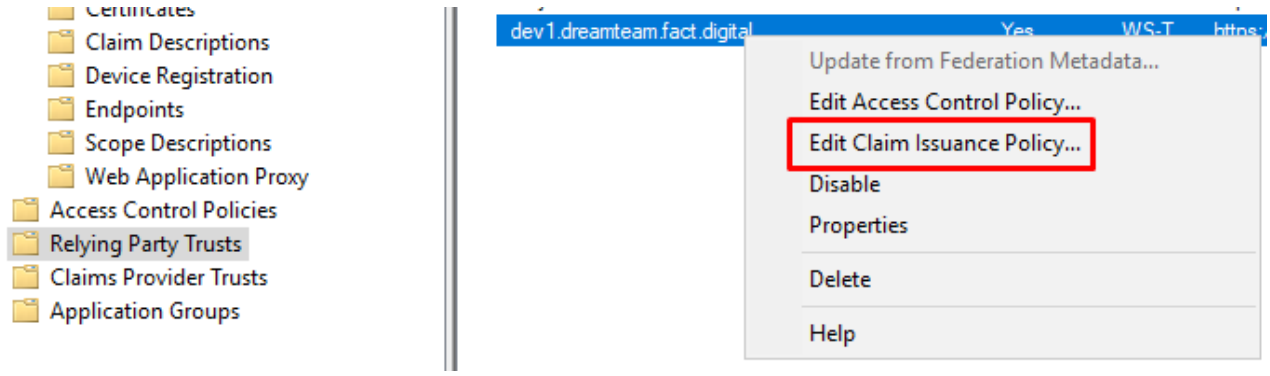



Add Relying Party Trust Wizard
Choose Access Control Policy
Steps
Welcome
Select Data Source
Specify Display Name
Configure Certificate
Configure URL
Configure Identifiers
Choose Access Control Policy
Ready to Add Trust
Finish
Choose an access control policy:
Name
Description
Permit everyone
Grant access to everyone.
Permit everyone and require MFA
Grant access to everyone and requir
Permit everyone and require MFA for specific group
Grant access to everyone and requir
Permit everyone and require MFA from extranet access
Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices
Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...
Grant access to everyone and requir
Permit everyone for intranet access
Grant access to the intranet users.
Policy
Permit everyone
I do not want to configure access control policies at this time. No user will be permitted access for this application.
< Previous
Next >
Cancel

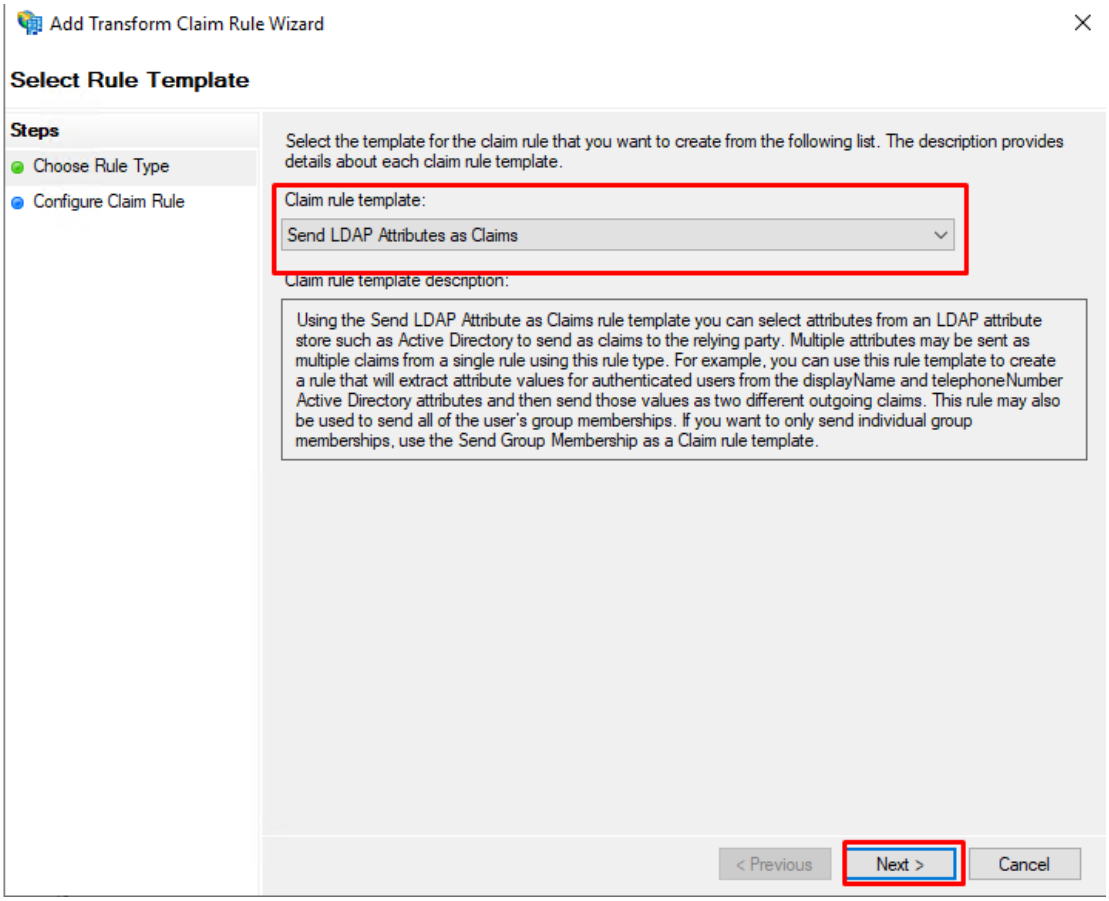

Add Relying Party Trust Wizard
Ready to Add Trust
Steps
Welcome
Select Data Source
Specify Display Name
Configure Certificate
Configure URL
Configure Identifiers
Choose Access Control Policy
Ready to Add Trust
Finish
The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
Monitoring
Identifiers
Encryption
Signature
Accepted Claims
Organization
Endpoints
Note
Specify the monitoring settings for this relying party trust.
Relying party's federation metadata URL:
Monitor relying party
Automatically update relying party
This relying party's federation metadata data was last checked on:
< never >
This relying party was last updated from federation metadata on:
< never >
< Previous
Next >
Cancel

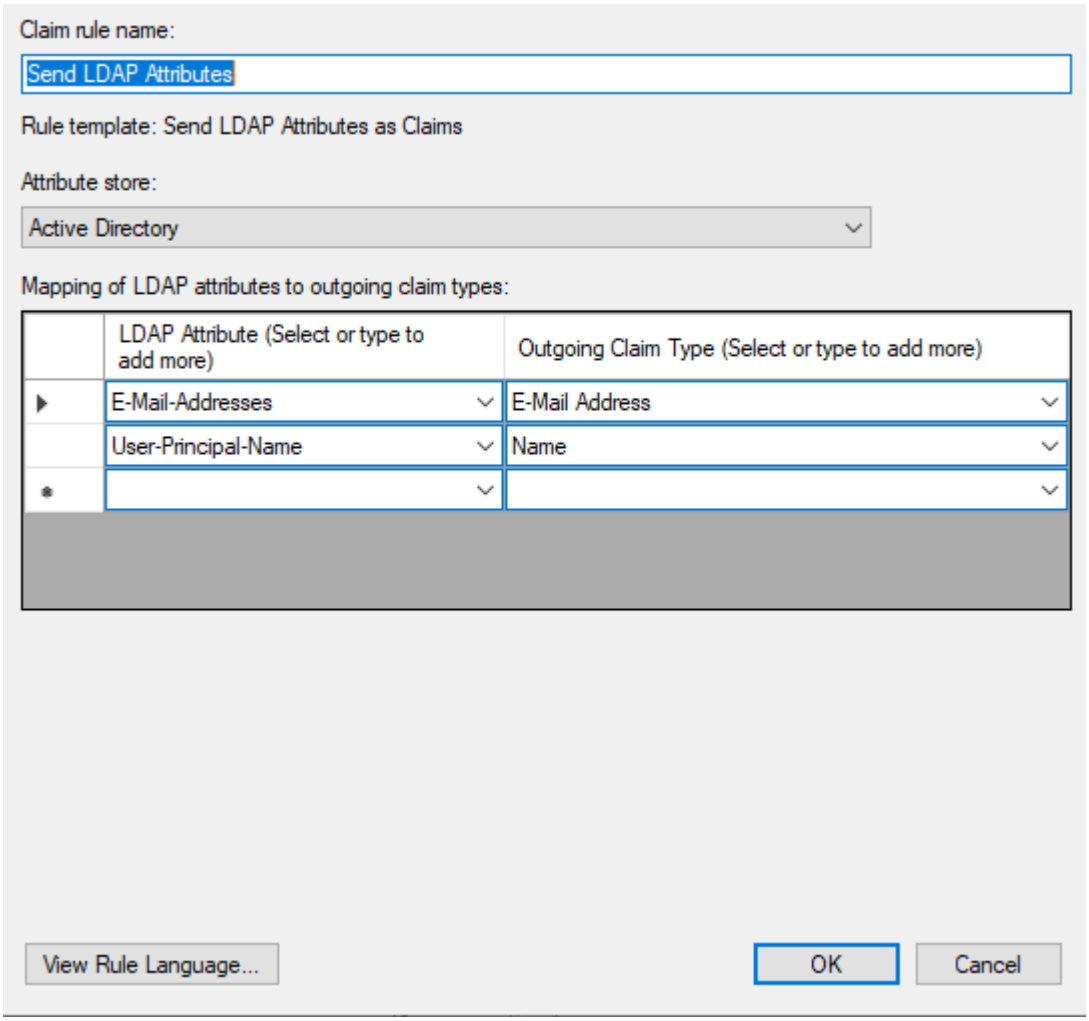


3.7. Создание правил трансформации отпечатка авторизации

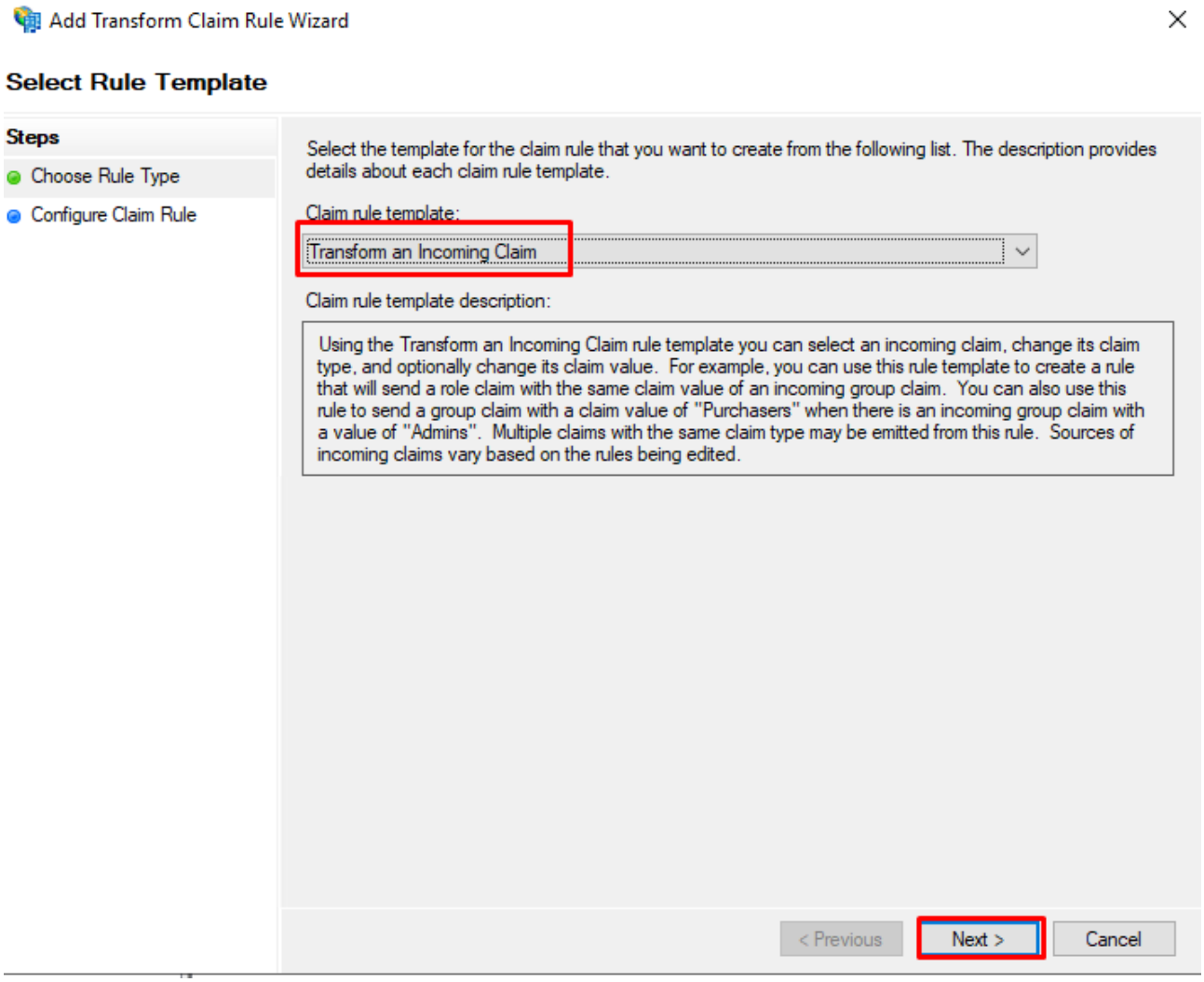


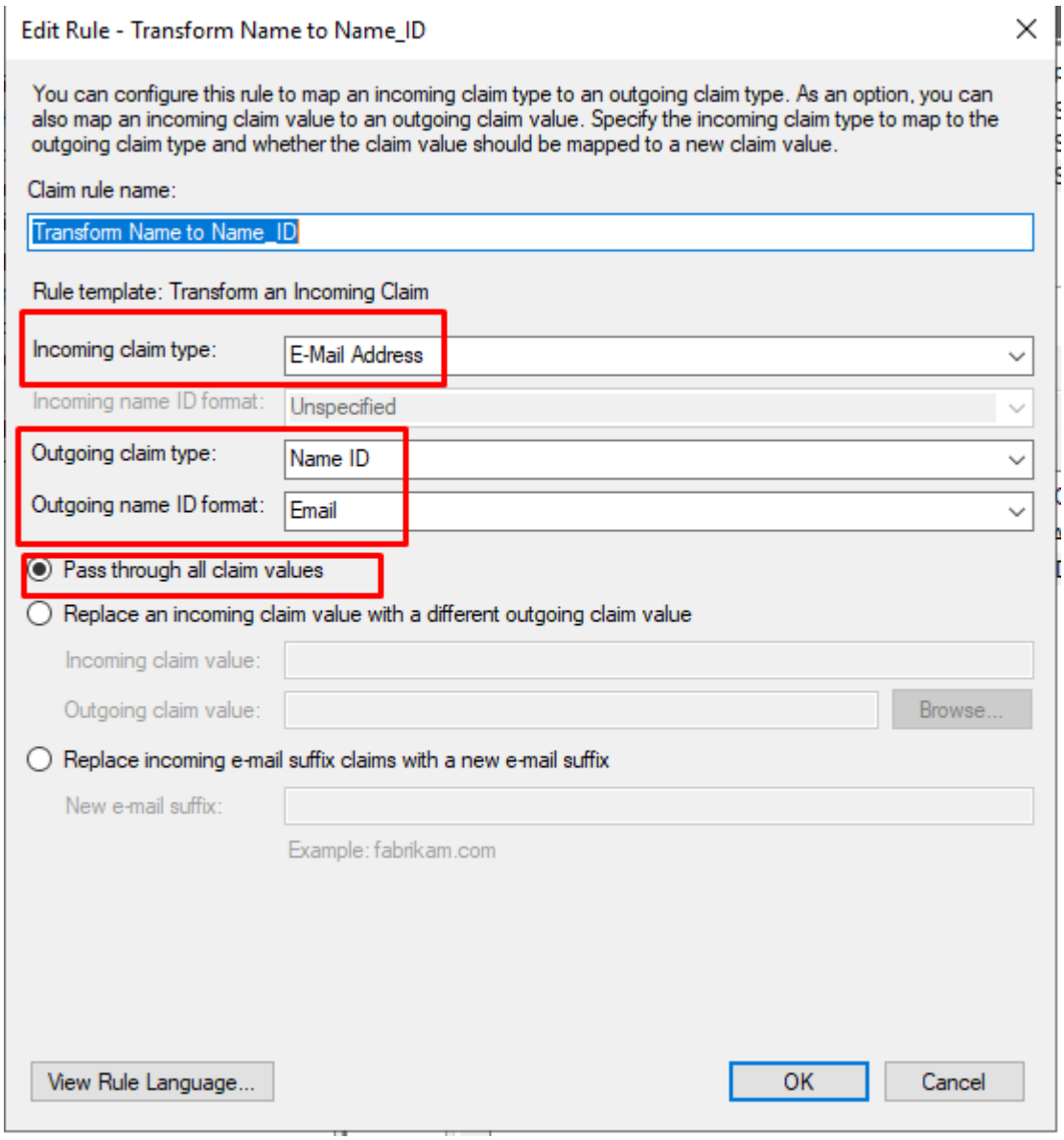
Нажимаем «Add» и выбираем шаблон


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Send LDAP Attributes as Claims
Claim rule template description:
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
< Previous
Next >
Cancel

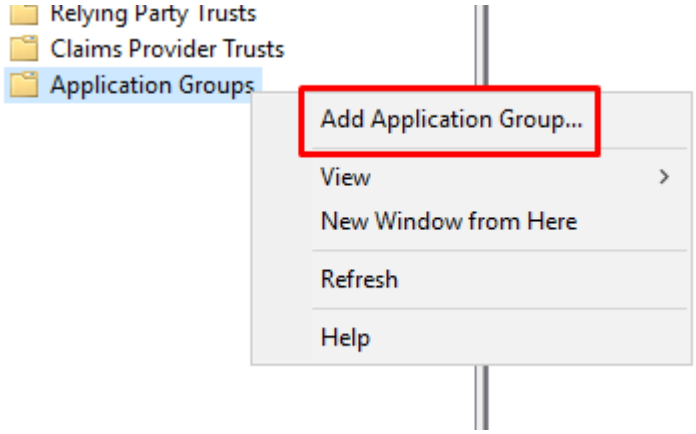

Claim rule name:
Send LDAP Attributes
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoing claim types:
LDAP Attribute (Select or type to add more)
Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses
E-Mail Address
User-Principal-Name
Name
View Rule Language...
OK
Cancel

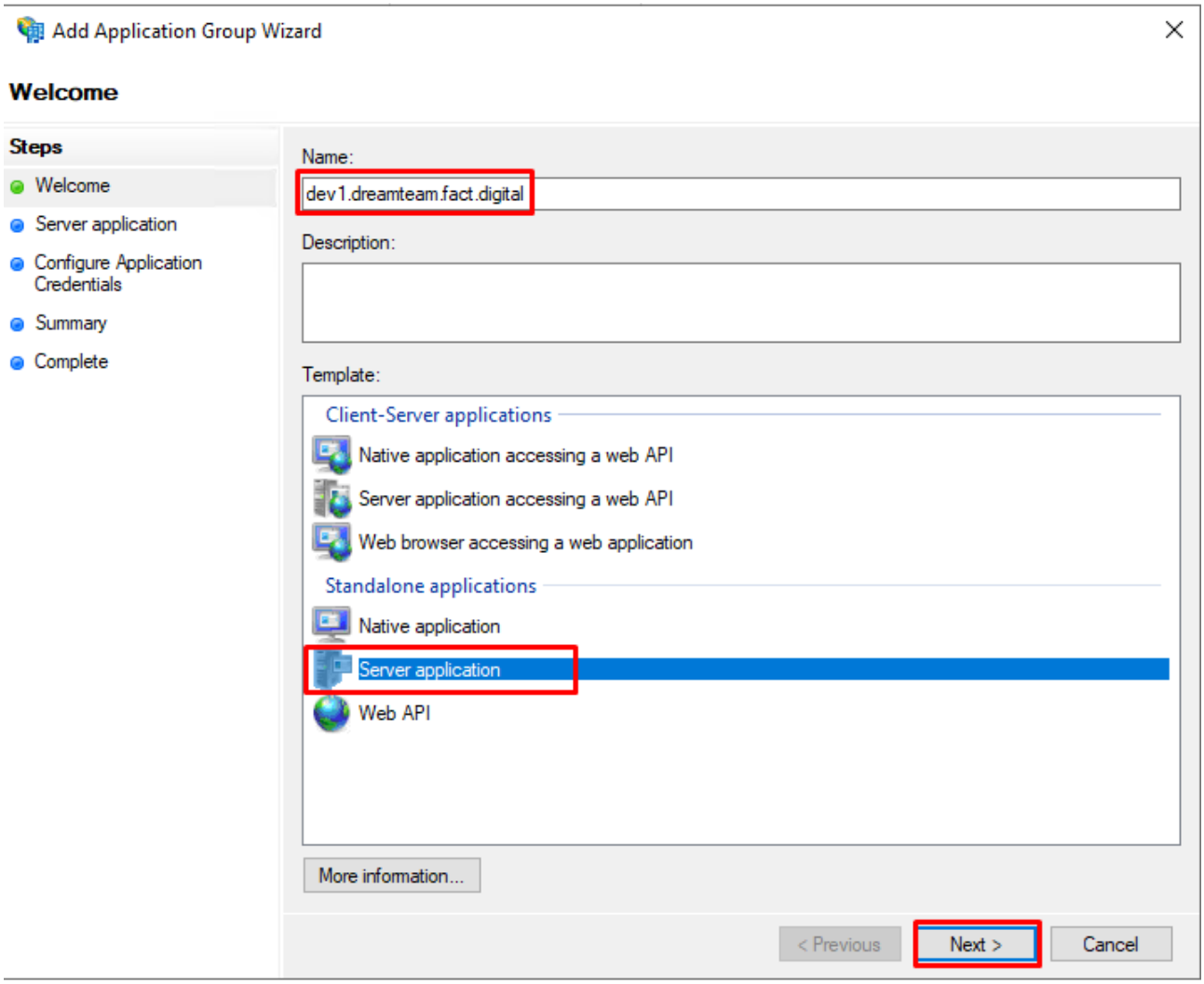
Нажимаем «Add» и выбираем шаблон

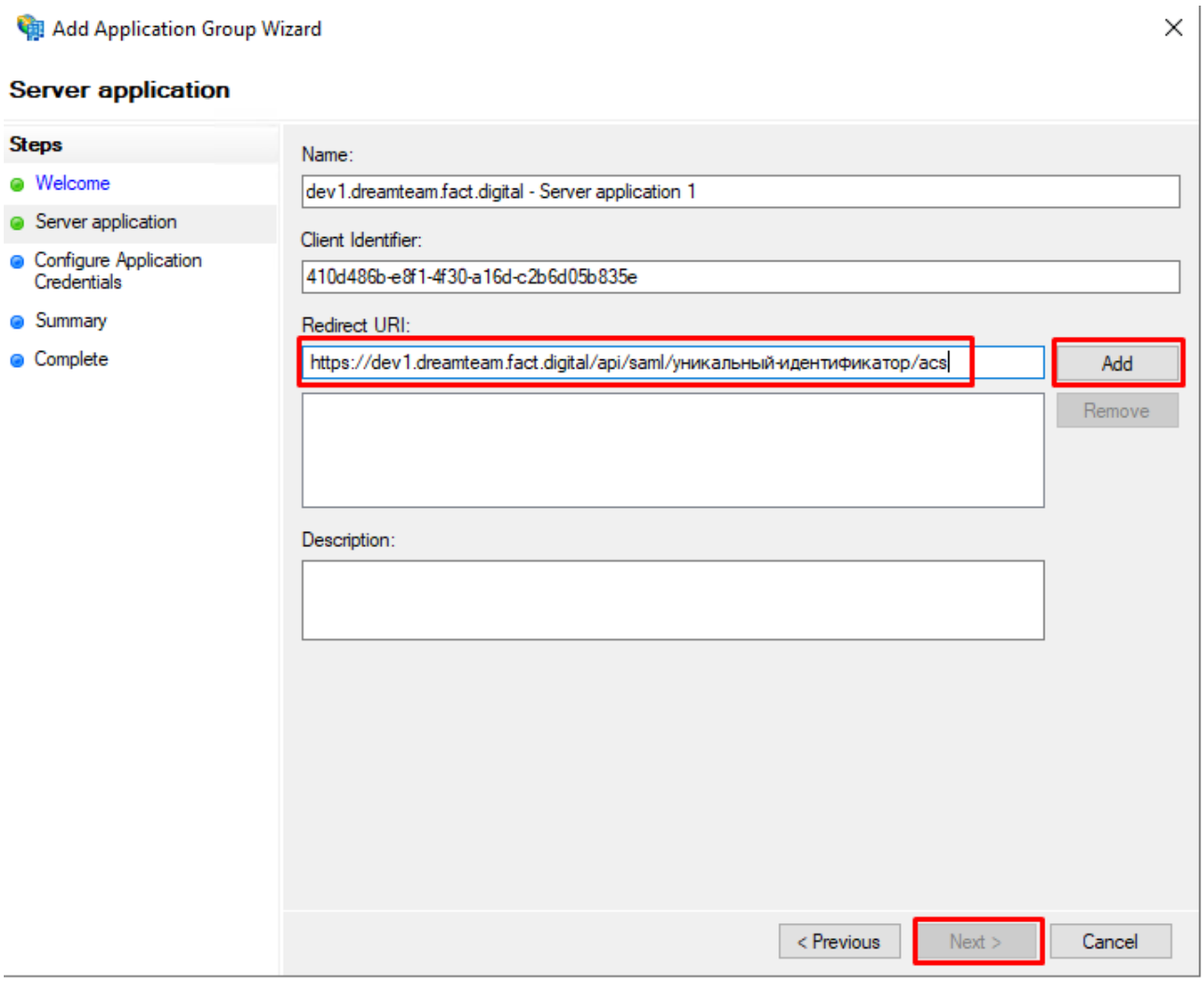




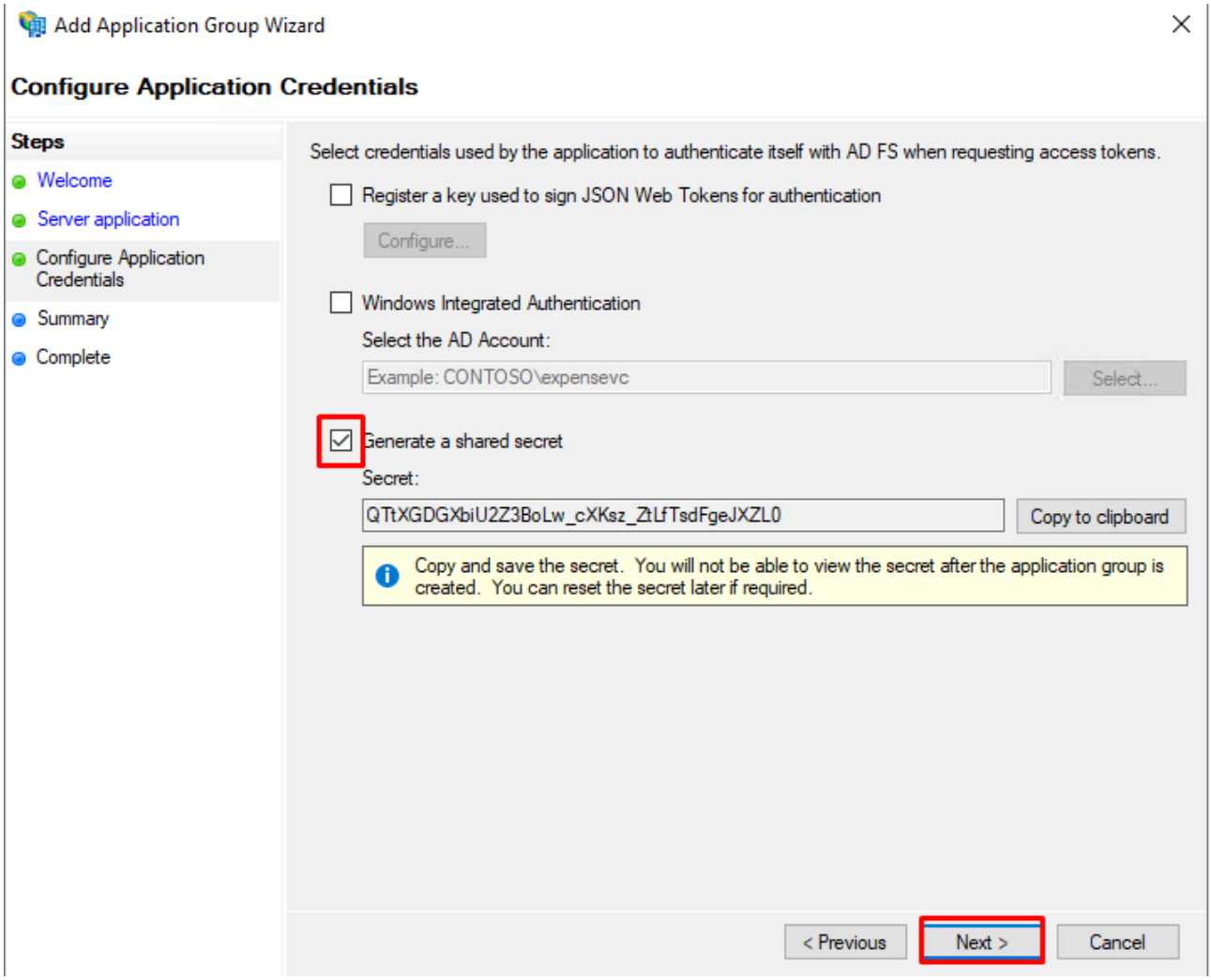
3.8. Создание группы приложений




Add Application Group Wizard
Welcome
Steps
Welcome
Server application
Configure Application Credentials
Summary
Complete
Name:
dev1.dreamteam.fact.digital
Description:
Template:
Client-Server applications
Native application accessing a web API
Server application accessing a web API
Web browser accessing a web application
Standalone applications
Native application
Server application
Web API
More information...
< Previous
Next >
Cancel

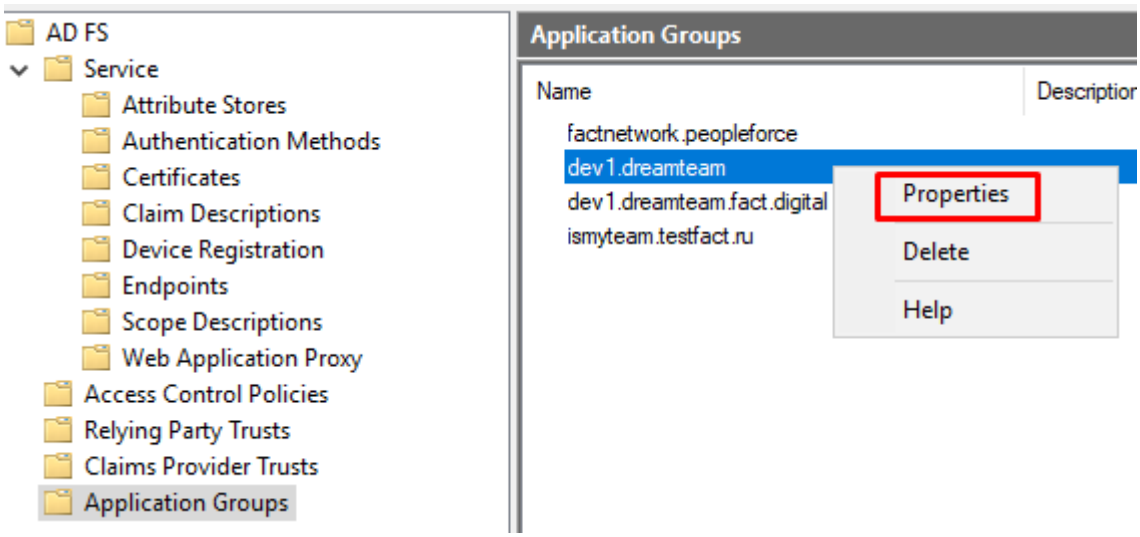

Add Application Group Wizard
Server application
Steps
Welcome
Server application
Configure Application Credentials
Summary
Complete
Name:
dev1.dreamteam.fact.digital - Server application 1
Client Identifier:
410d486b-e8f1-4f30-a16d-c2b6d05b835e
Redirect URI:
https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs
Add
Remove
Description:
< Previous
Next >
Cancel

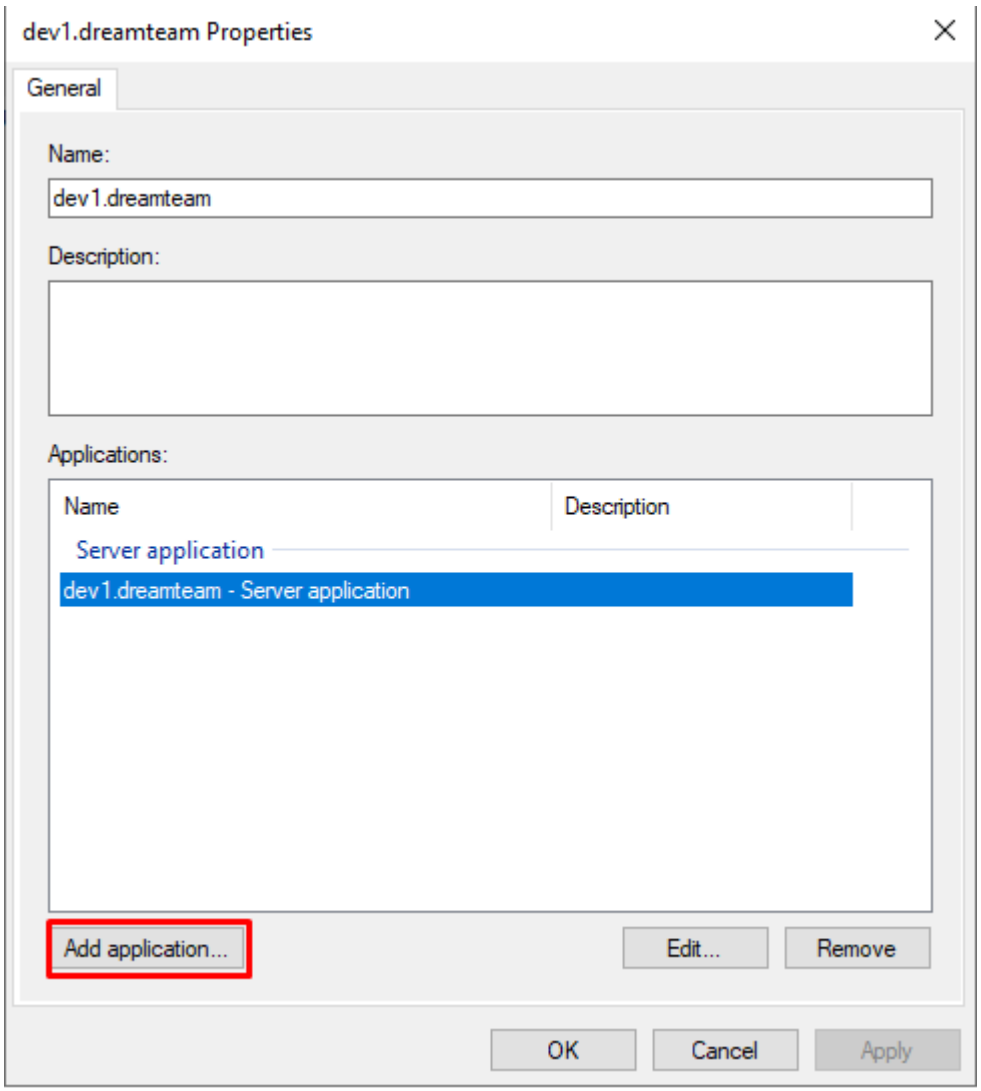
Нужно отметить поле «Generate a shared secret». Сам этот секрет нигде прописывать не нужно, но без него нельзя завершить настройку.

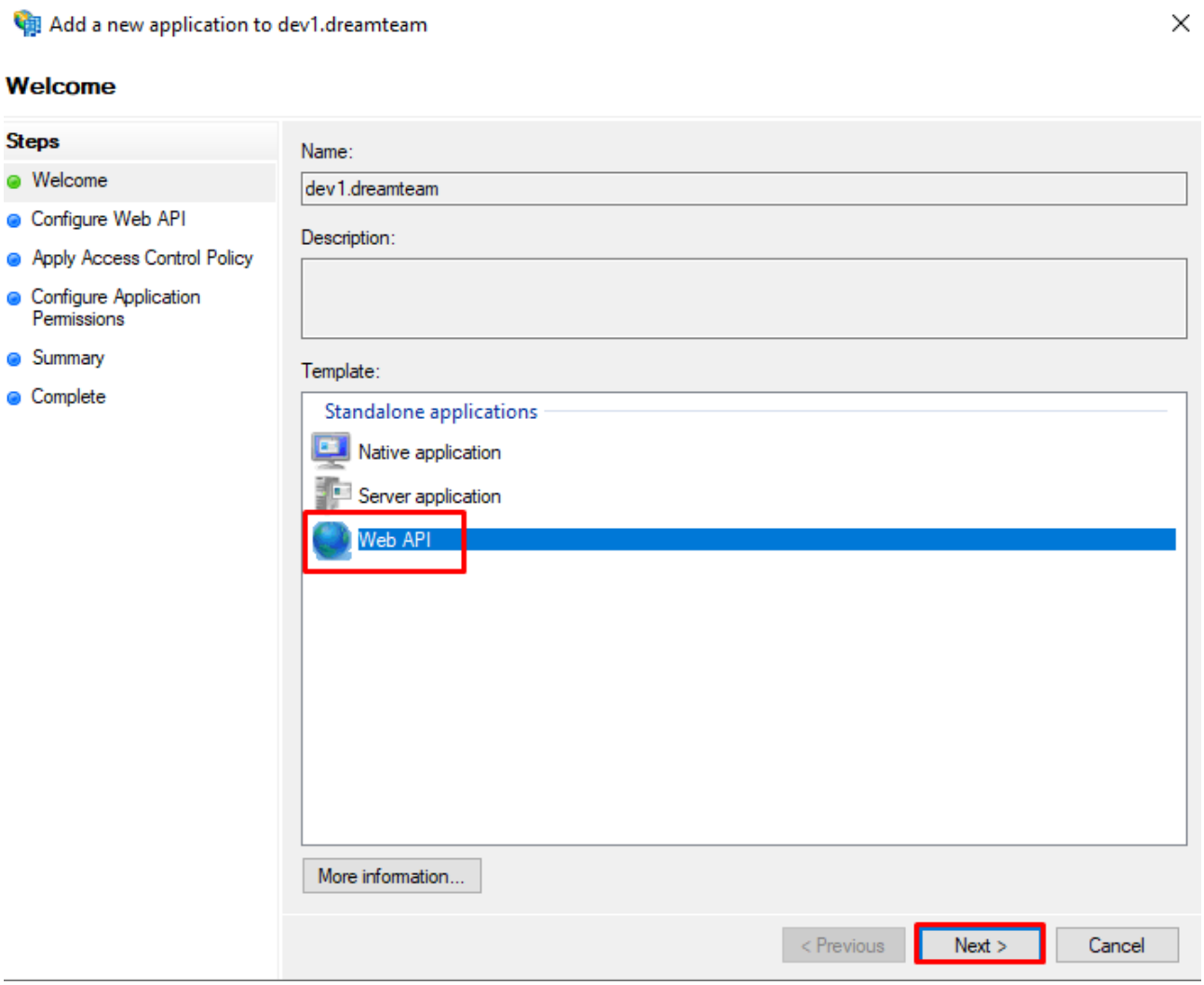


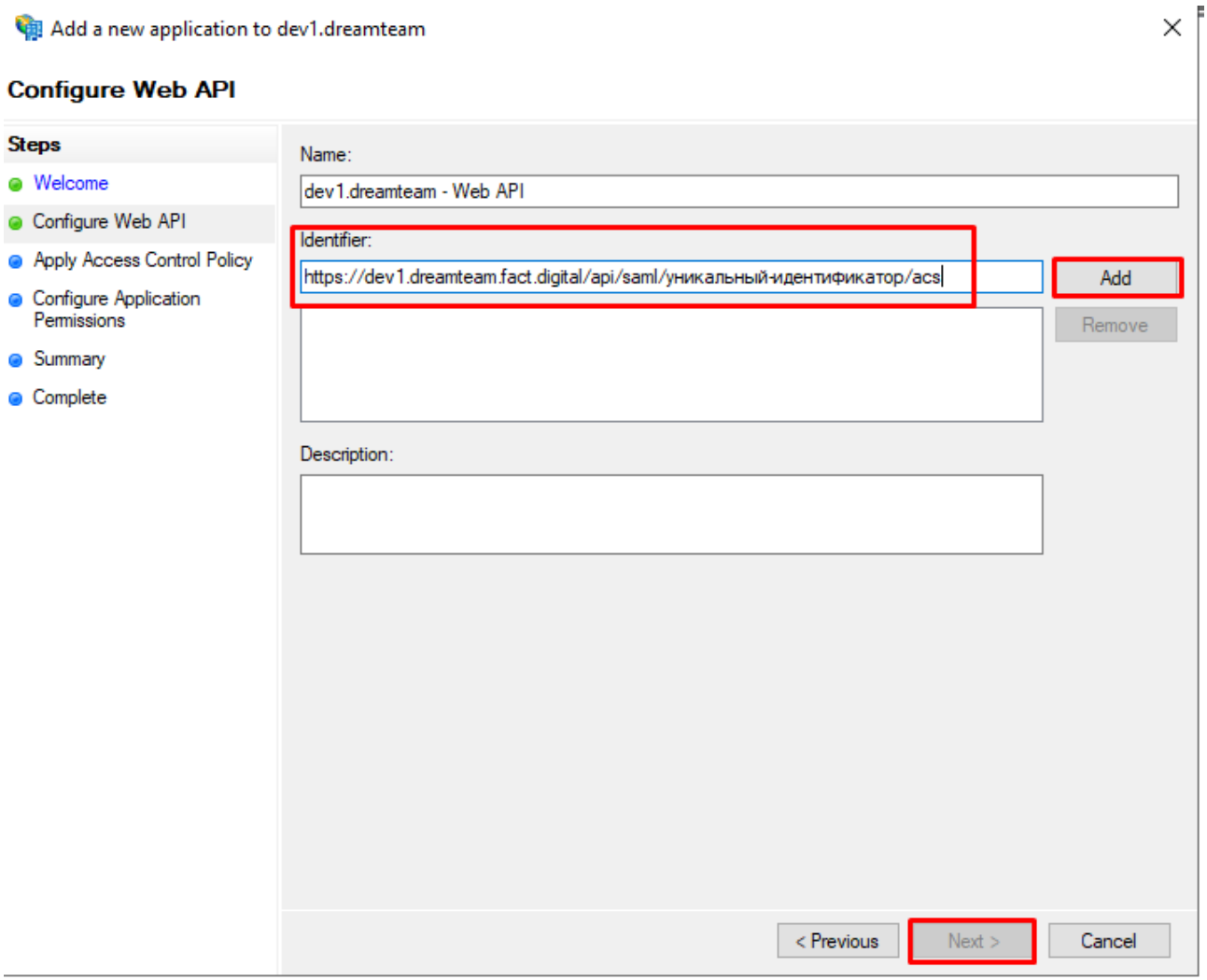
На следующем экране нажимаем «Next», а затем «Close».

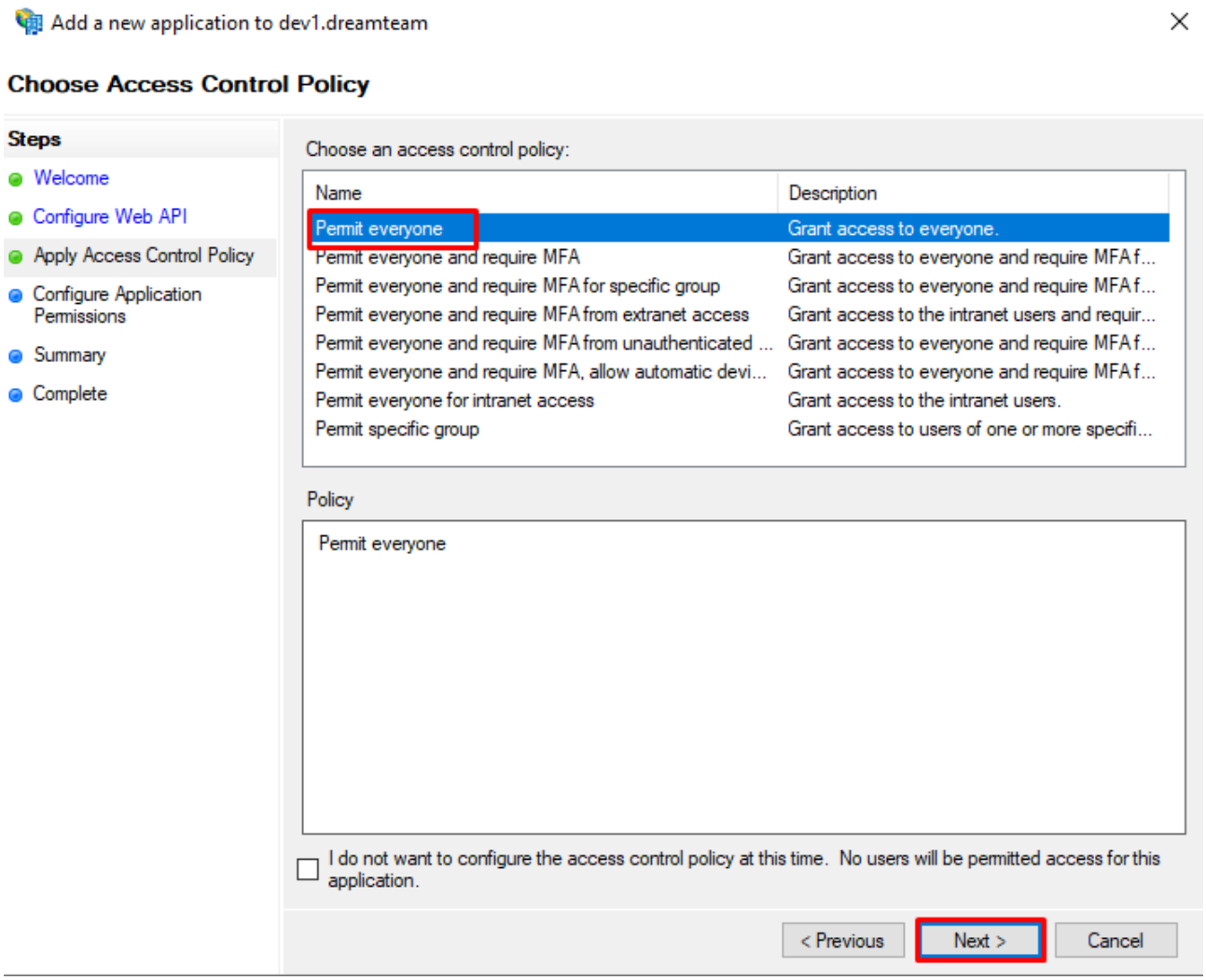
Правый щелчок мыши на вновь созданном Application Group и выбираем «Properties»

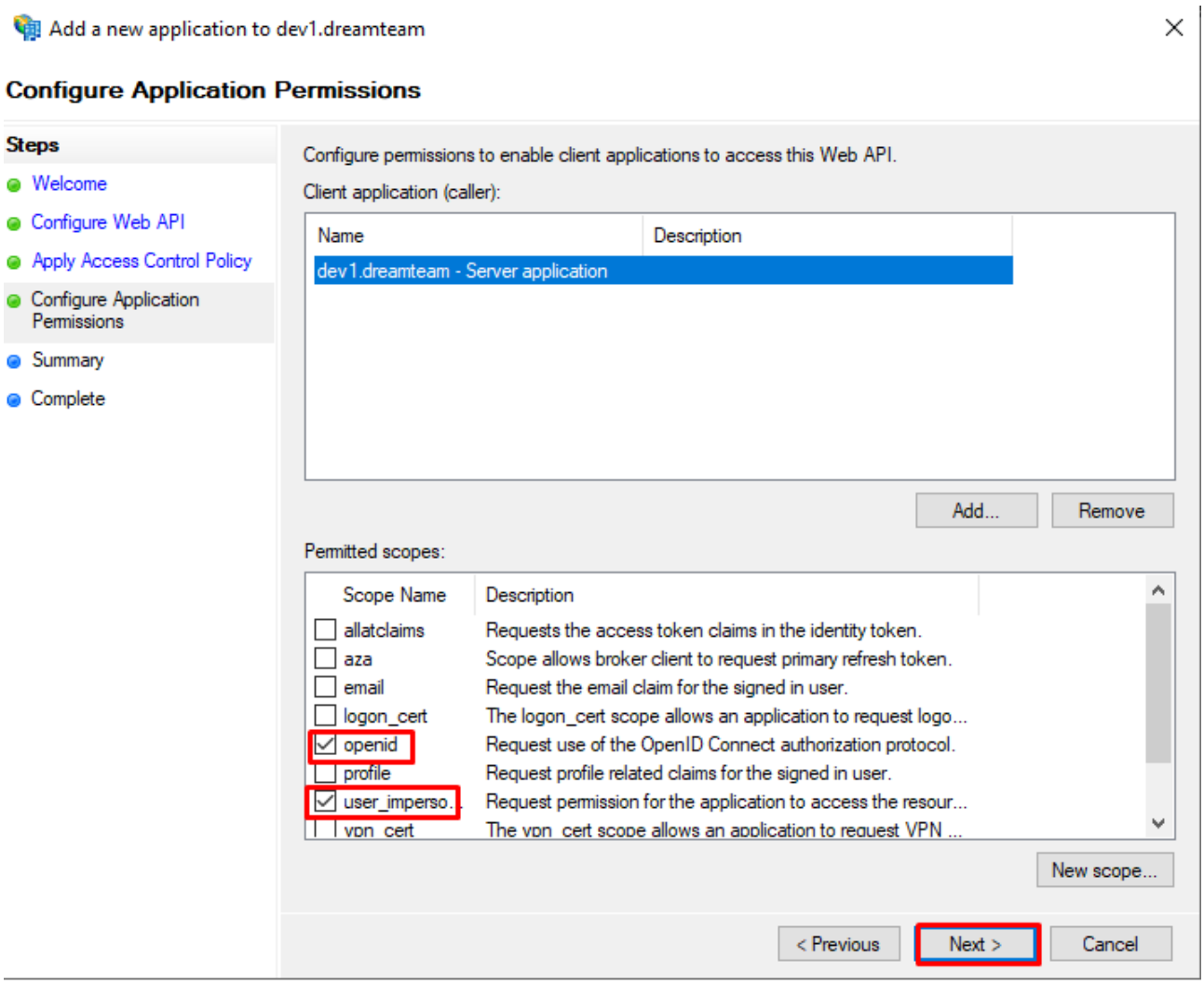



dev1.dreamteam Properties
General
Name:
dev1.dreamteam
Description:
Applications:
Name
Description
Server application
dev1.dreamteam - Server application
Add application...
Edit...
Remove
OK
Cancel
Apply


Add a new application to dev1.dreamteam
Welcome
Steps
Welcome
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Name:
dev1.dreamteam
Description:
Template:
Standalone applications
Native application
Server application
Web API
More information...
< Previous
Next >
Cancel

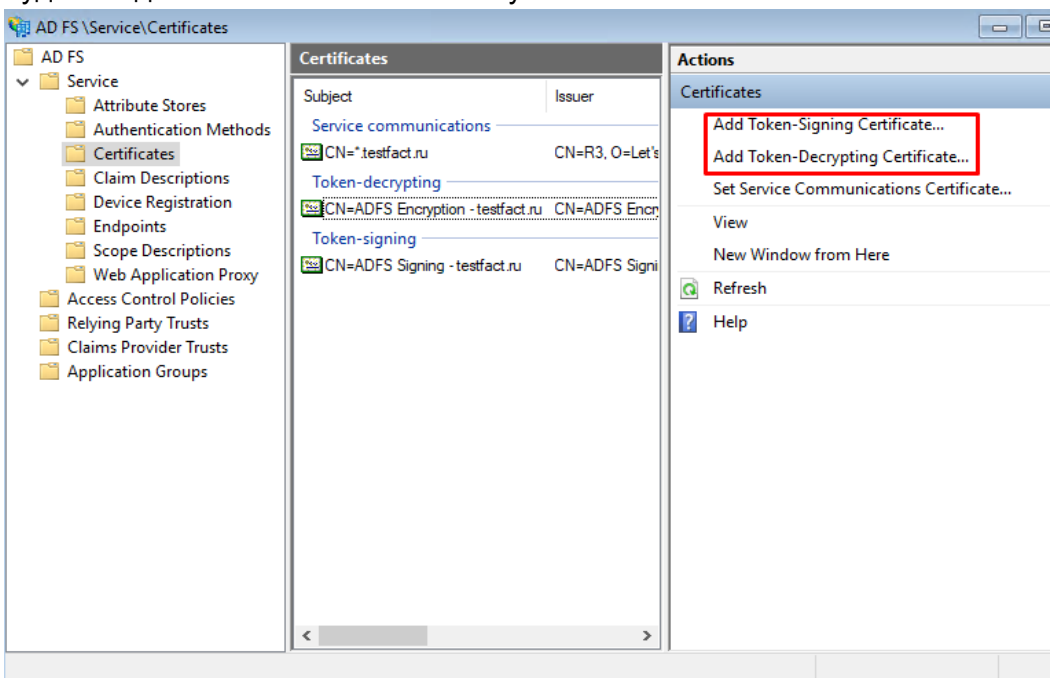

Add a new application to dev1.dreamteam
Configure Web API
Steps
Welcome
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Name:
dev1.dreamteam - Web API
Identifier:
https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs
Add
Remove
Description:
< Previous
Next >
Cancel


Add a new application to dev1.dreamteam
Choose Access Control Policy
Steps
Welcome
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Choose an access control policy:
Name
Description
Permit everyone
Grant access to everyone.
Permit everyone and require MFA
Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group
Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access
Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...
Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...
Grant access to everyone and require MFA f...
Permit everyone for intranet access
Grant access to the intranet users.
Permit specific group
Grant access to users of one or more specifi...
Policy
Permit everyone
I do not want to configure the access control policy at this time. No users will be permitted access for this application.
< Previous
Next >
Cancel

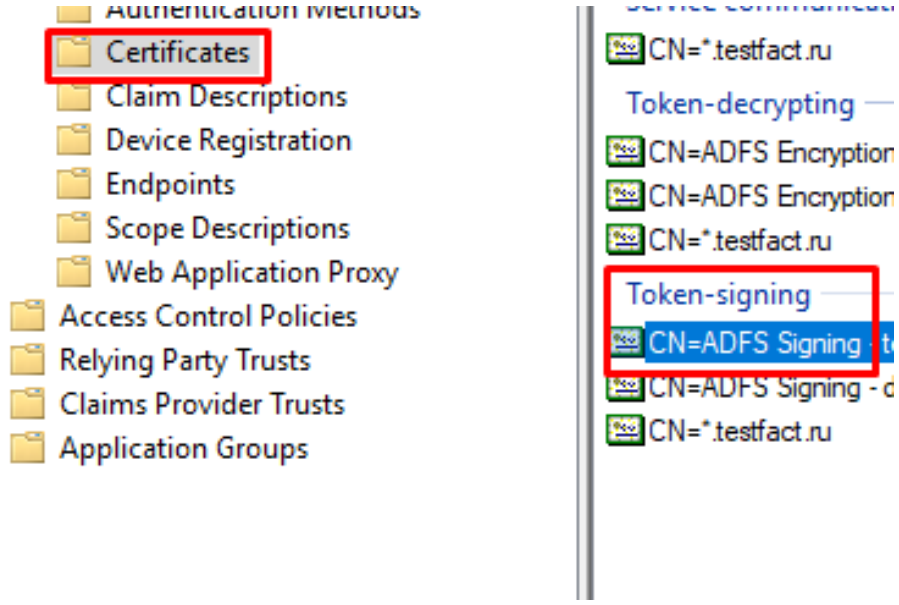


Еще раз нажимаем «Next» и «Close».

3.9. В процессе настройки, мастером, возможно, будет предложено выпустить сертификаты, которые используется для подписи и шифрования. Если этого не произойдет, то нужно будет создать их самостоятельно. и указать его в личном кабинете «МояКоманды».

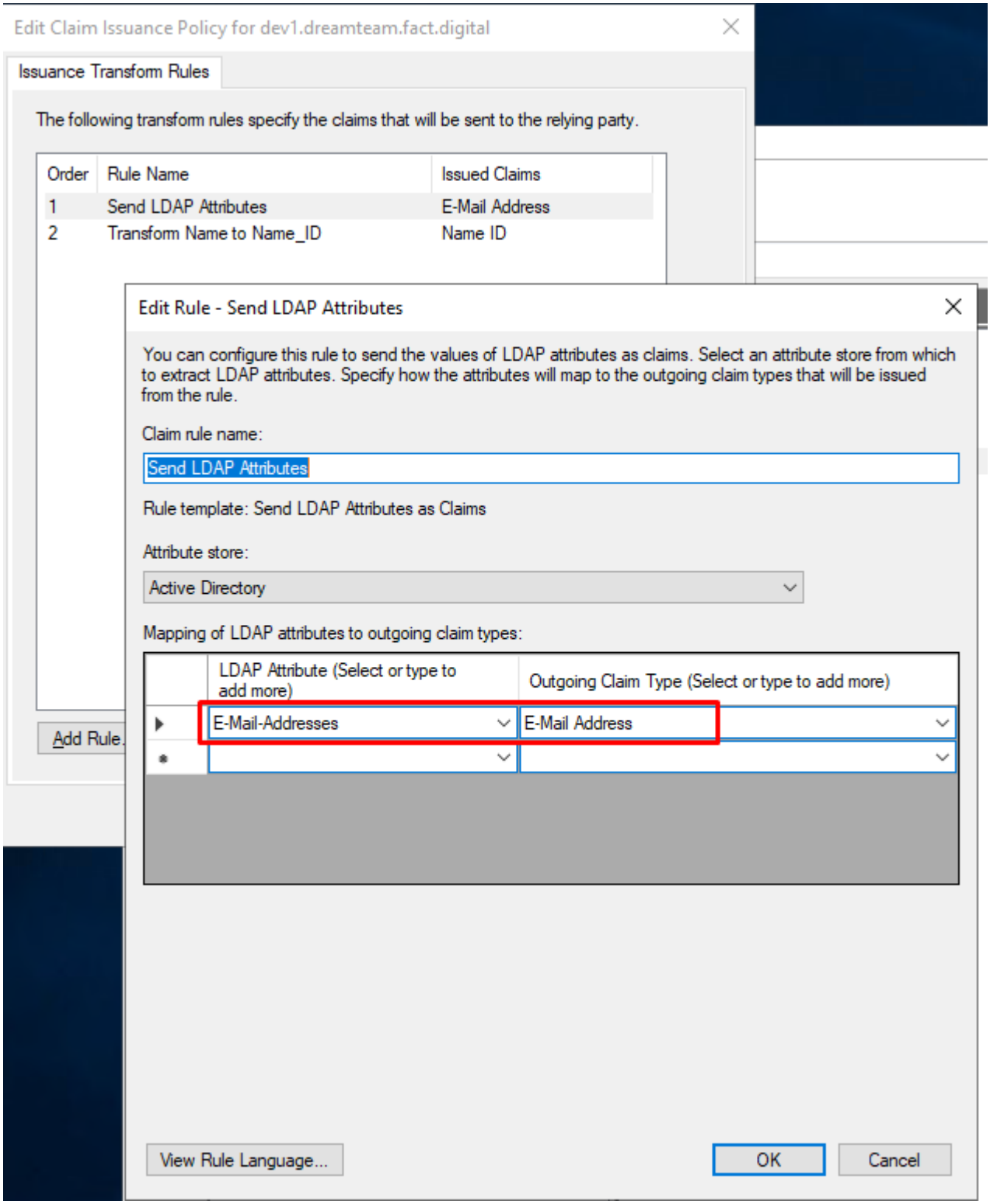


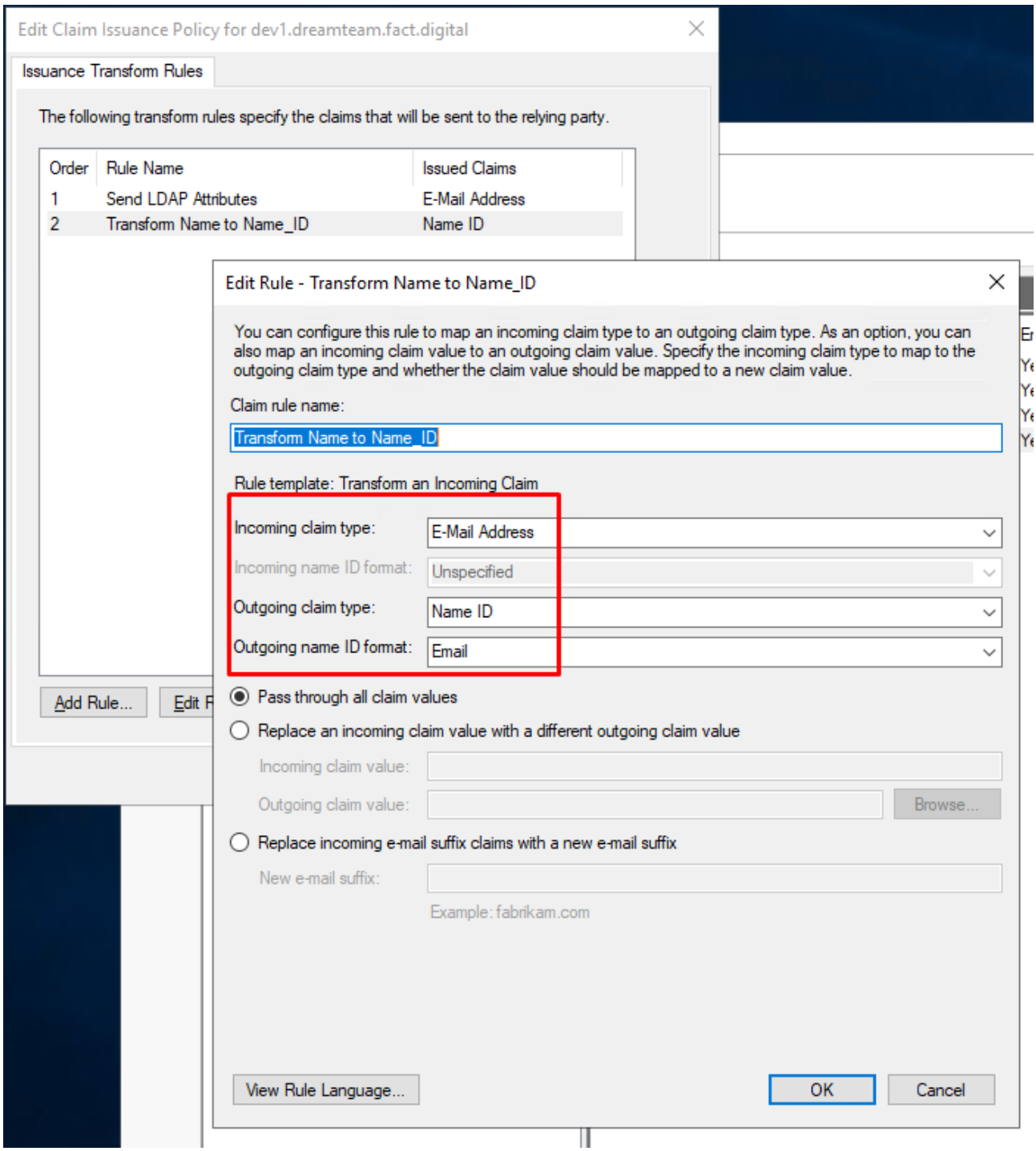
Сертификат для подписи необходимо сохранить в файл, конвертировать в формат pem и в текстовом виде вставить в поле «Сертификат» (только сам сертификат без секций «BEGIN CERTIFICATE» и «END CERTIFICATE») в личном кабинете «МояКоманды».



!!!_____!!!

Еще один вариант, при котором заработала авторизация:




Edit Claim Issuance Policy for dev1.dreamteam.fact.digital
Issuance Transform Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Send LDAP Attributes
E-Mail Address
2
Transform Name to Name_ID
Name ID
Add Rule...
Edit R
Edit Rule - Transform Name to Name_ID
You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.
Claim rule name:
Transform Name to Name_ID
Rule template: Transform an Incoming Claim
Incoming claim type:
E-Mail Address
Incoming name ID format:
Unspecified
Outgoing claim type:
Name ID
Outgoing name ID format:
Email
Pass through all claim values
Replace an incoming claim value with a different outgoing claim value
Incoming claim value:
Outgoing claim value:
Browse...
Replace incoming e-mail suffix claims with a new e-mail suffix
New e-mail suffix:
Example: fabrikam.com
View Rule Language...
OK
Cancel

При этом, в УЗ пользователя в AD должно быть корректное значение в поле E-mail: