

Развертывание ADFS на Windows Server для авторизации на внешних площадках

Подготовительные действия

- 1.1. Добавить и настроить роль AD, завести пользователей.
- 1.2. Добавить роли IIS
- 1.3. Сгенерировать самоподписанный SSL сертификат ([как сгенерировать самоподписанный SSL сертификат](#)), либо использовать выпущенный для имеющегося домена
- 1.4. Если будет использоваться выпущенный сертификат, то необходимо выполнить его импорт

←  Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

To continue, click Next.

 Next

Cancel

File to Import

Specify the file you want to import.

File name:

C:\[redacted]

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

Certificate store:

Personal

Browse...

Select Certificate Store ×

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

Show physical stores

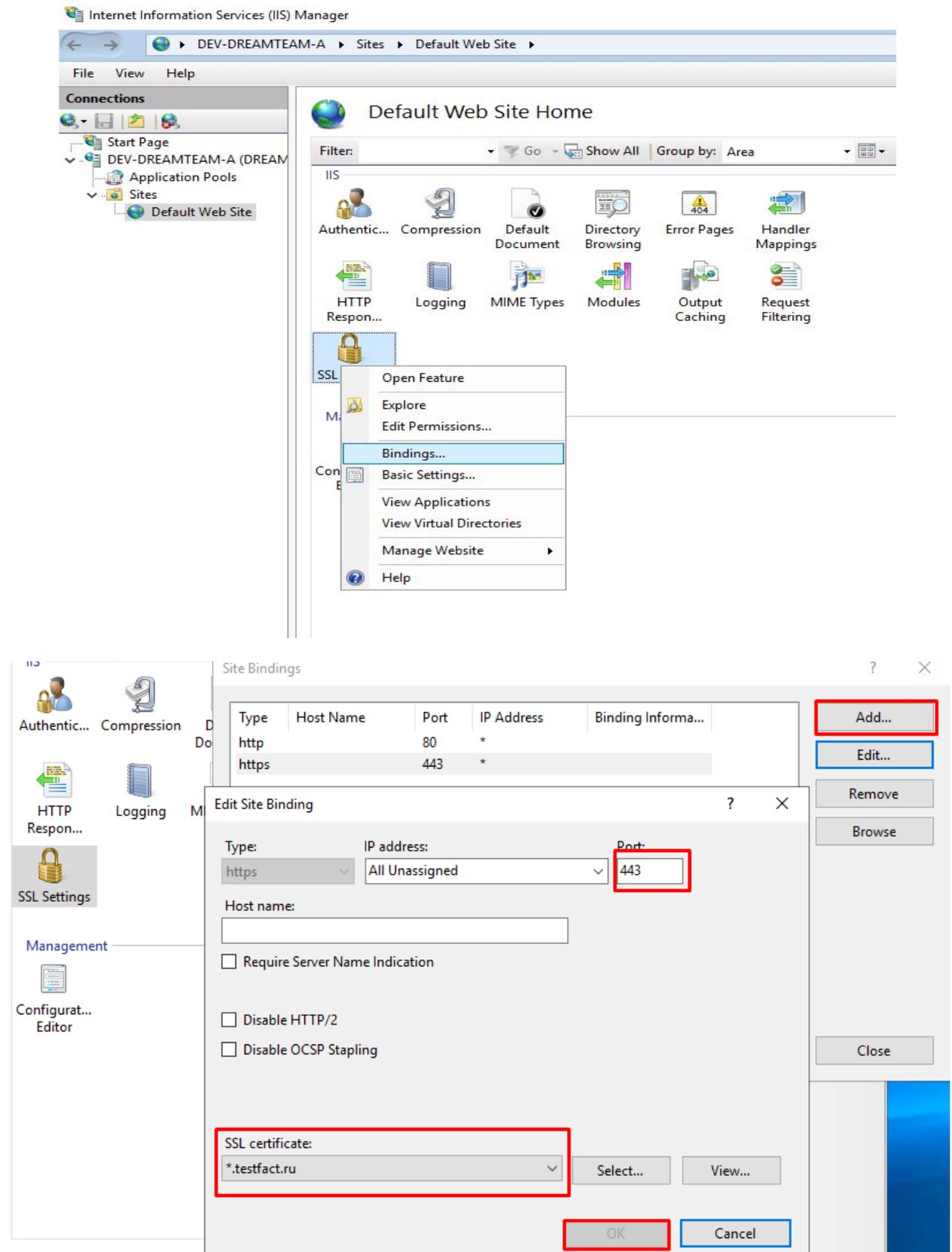
OK Cancel

Next

Cancel

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

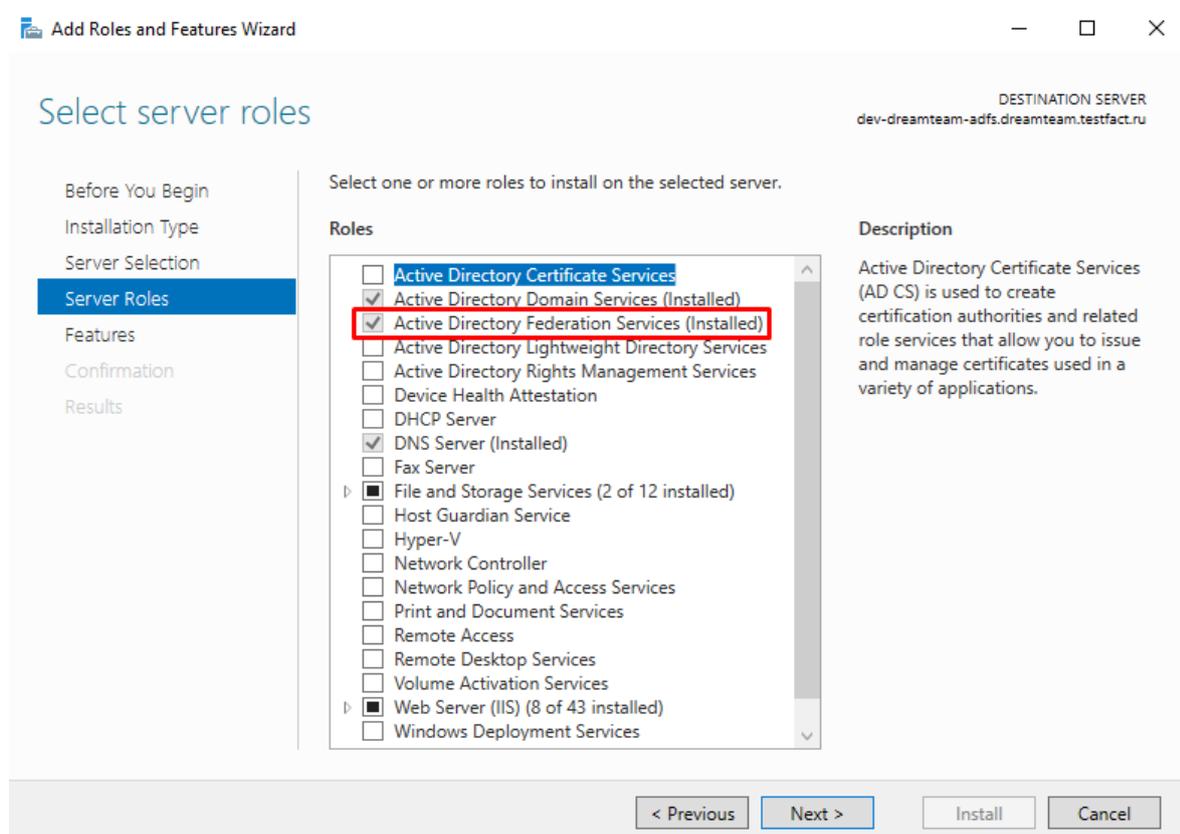
1.5. Открыть оснастку управления IIS и для «Default Web Site» в секции SSL Settings выбрать пункт «Bindings...», добавить порт 443 и выбрать импортированный ранее сертификат.



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

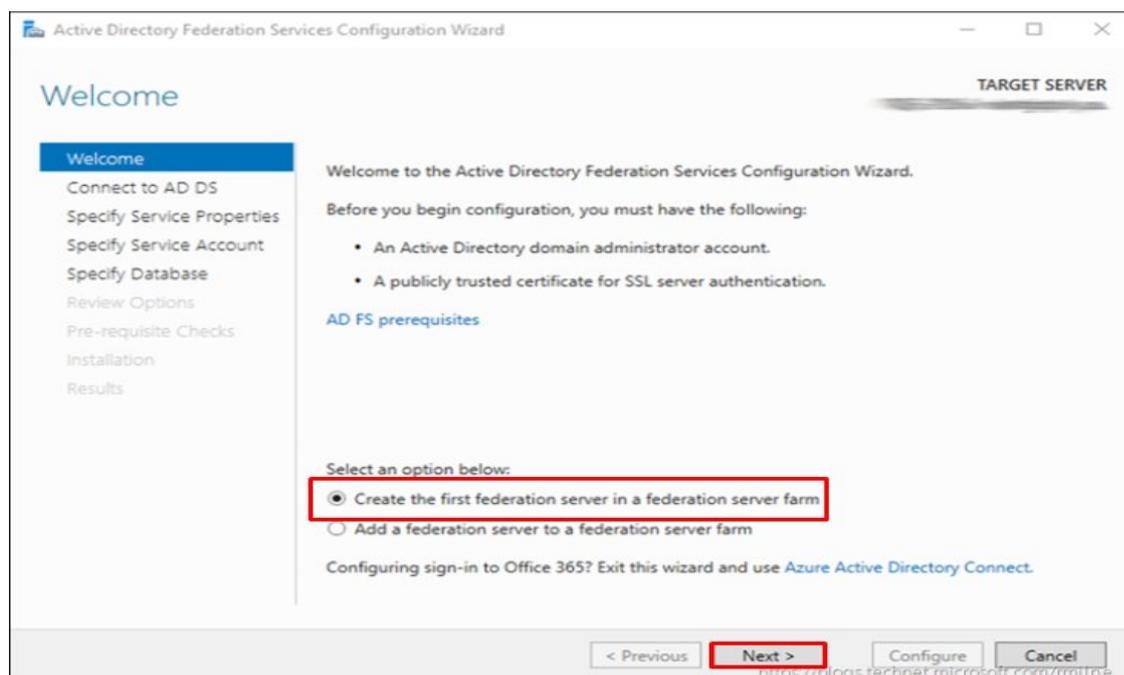
Добавление и настройка ADFS

2.1. Добавить роль ADFS

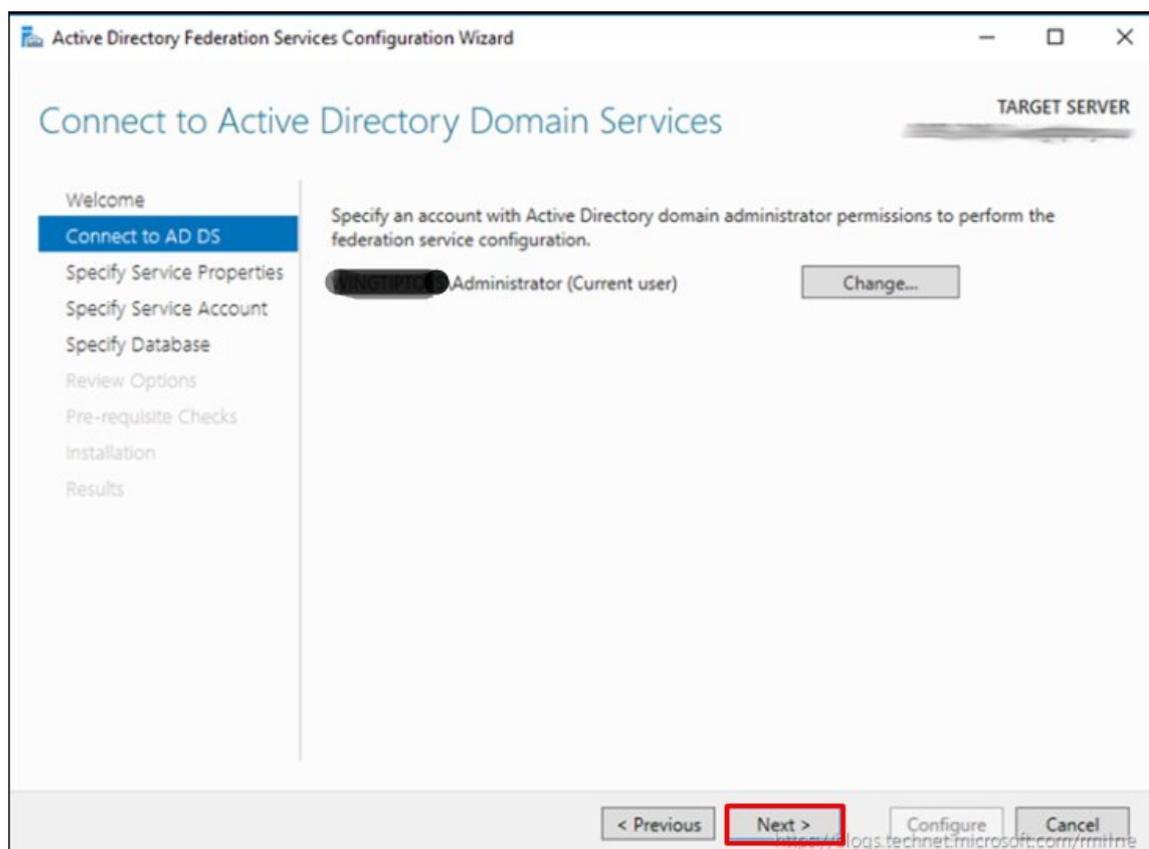


2.2. После установки необходимо вызвать мастер конфигурирования ADFS

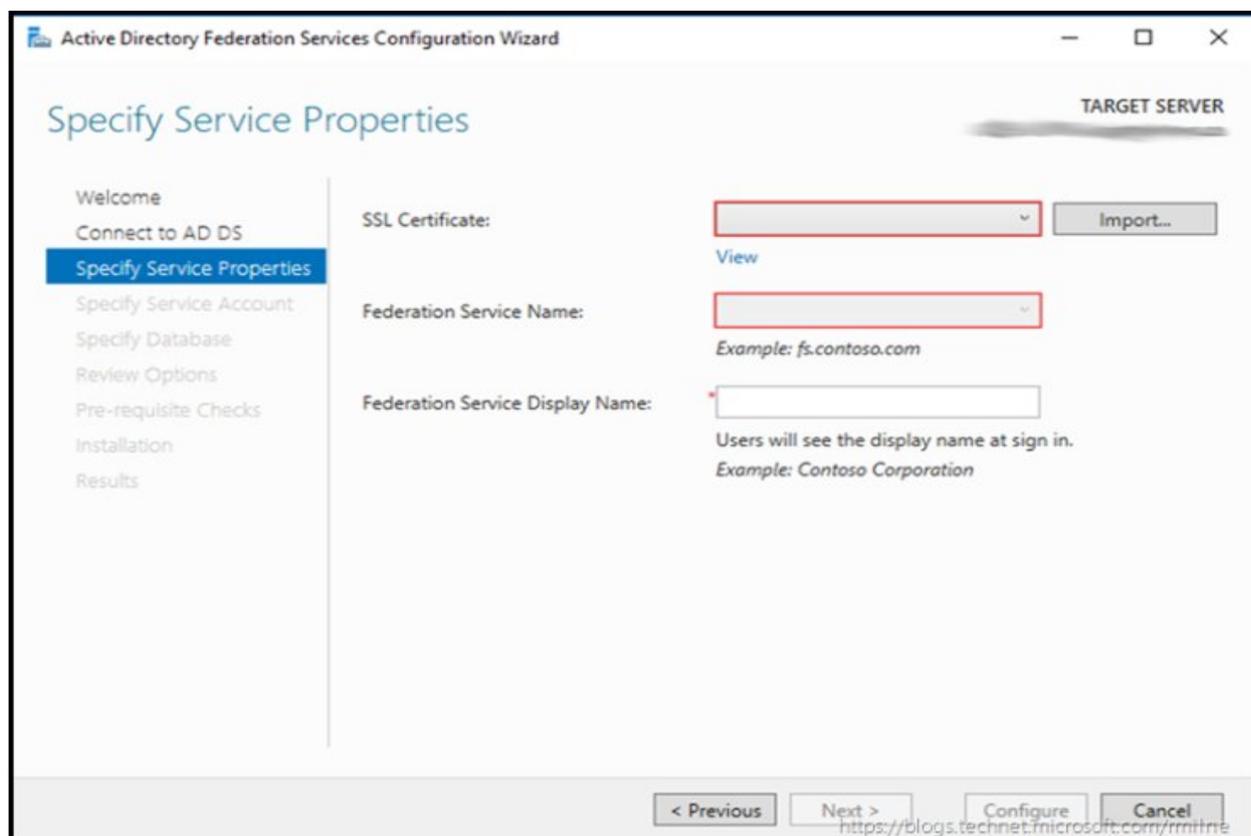
2.3. Шаги мастера настройки следующие:



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



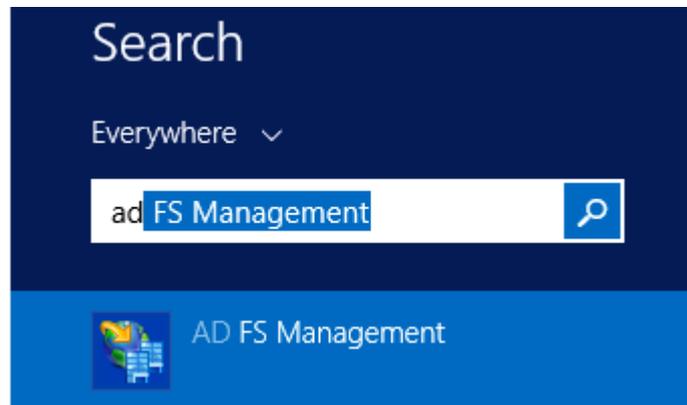
Выбираем сертификат, который мы импортировали на шаге 1.4, имя (например adfs.yourdomain.ru) и выводимое имя (оно будет отображаться на странице авторизации).



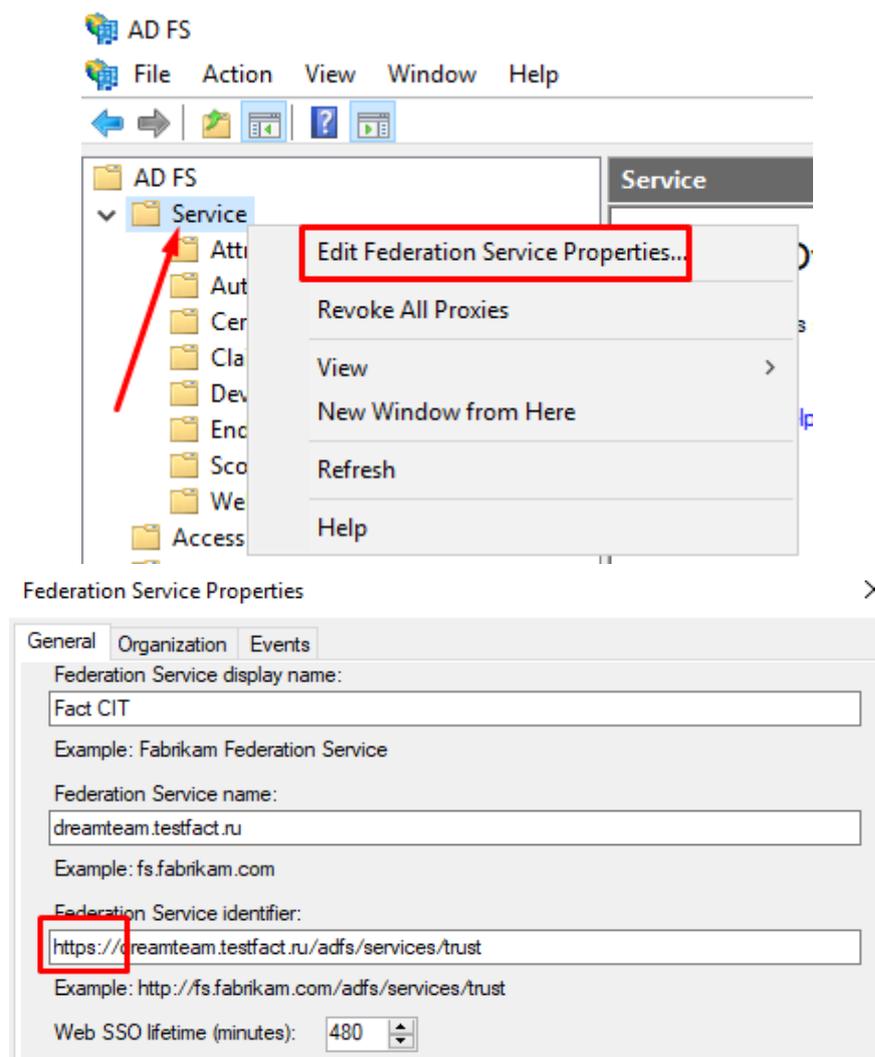
Далее выбираем тип БД, создаем ее и завершаем настройку, пройдя по оставшимся шагам мастера (на этих шагах уже никаких параметров менять/выбирать не нужно).

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)

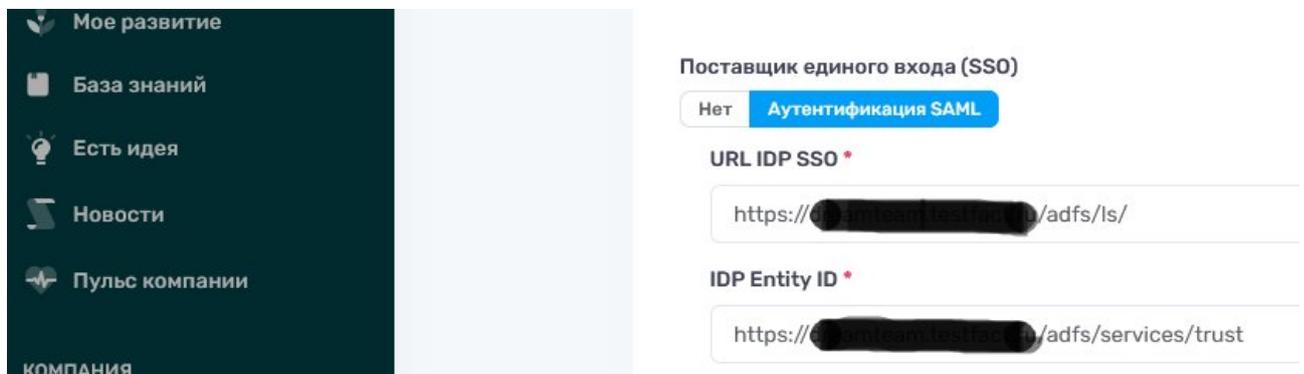


3.3 Выполнить вход в <https://dev1.dreamteam.fact.digital> под своей учетной записью

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>

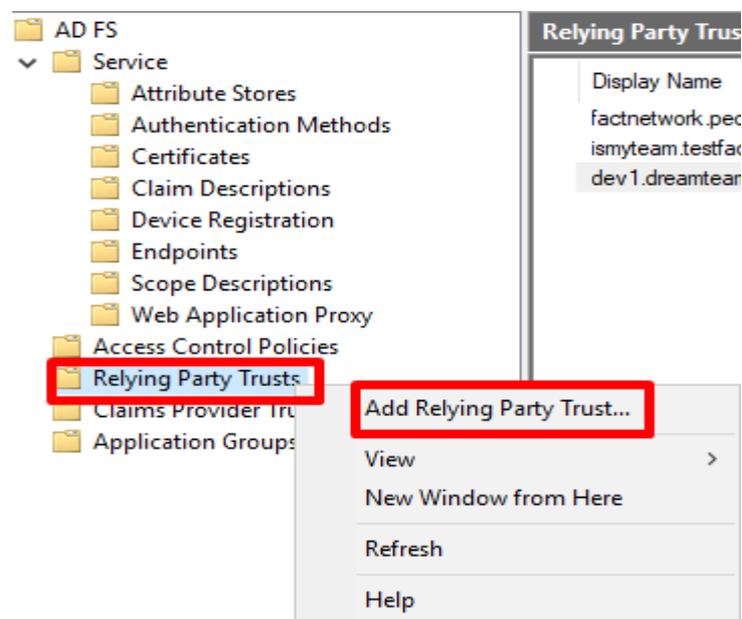


3.5. После нажатия на кнопку «Сохранить» в полях **ACS URL** и **Entity ID** появятся ссылки, которые нам потребуются позже



Сохранить

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



Выбираем тип «Claim aware»

 Add Relying Party Trust Wizard ✕

Welcome

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. [Learn more](#)

Claims aware

Non claims aware

< Previous Start Cancel

Add Relying Party Trust Wizard [Close]

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
[Text Box]
Example: fs.contoso.com or https://www.contoso.com/app

Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:
[Text Box] [Browse...]

Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.

[< Previous] [Next >] [Cancel]

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

Add Relying Party Trust Wizard



Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

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

Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

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

< Previous

Next >

Cancel

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

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure Identifiers' step. The window title is 'Add Relying Party Trust Wizard' with a close button (X) in the top right corner. On the left, a 'Steps' sidebar lists the following steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this, there is a label 'Relying party trust identifier:' followed by a text input field containing the URL 'https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/metadata'. To the right of the input field is an 'Add' button. Below the input field is an example: 'Example: https://fs.contoso.com/adfs/services/trust'. Underneath, there is a label 'Relying party trust identifiers:' followed by a large empty list box. To the right of the list box is a 'Remove' button. At the bottom of the dialog, there are three buttons: '< Previous', 'Next >' (highlighted with a red box), and 'Cancel'.

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 an
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.
Permit specific group	Grant access to users of one or more

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

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:

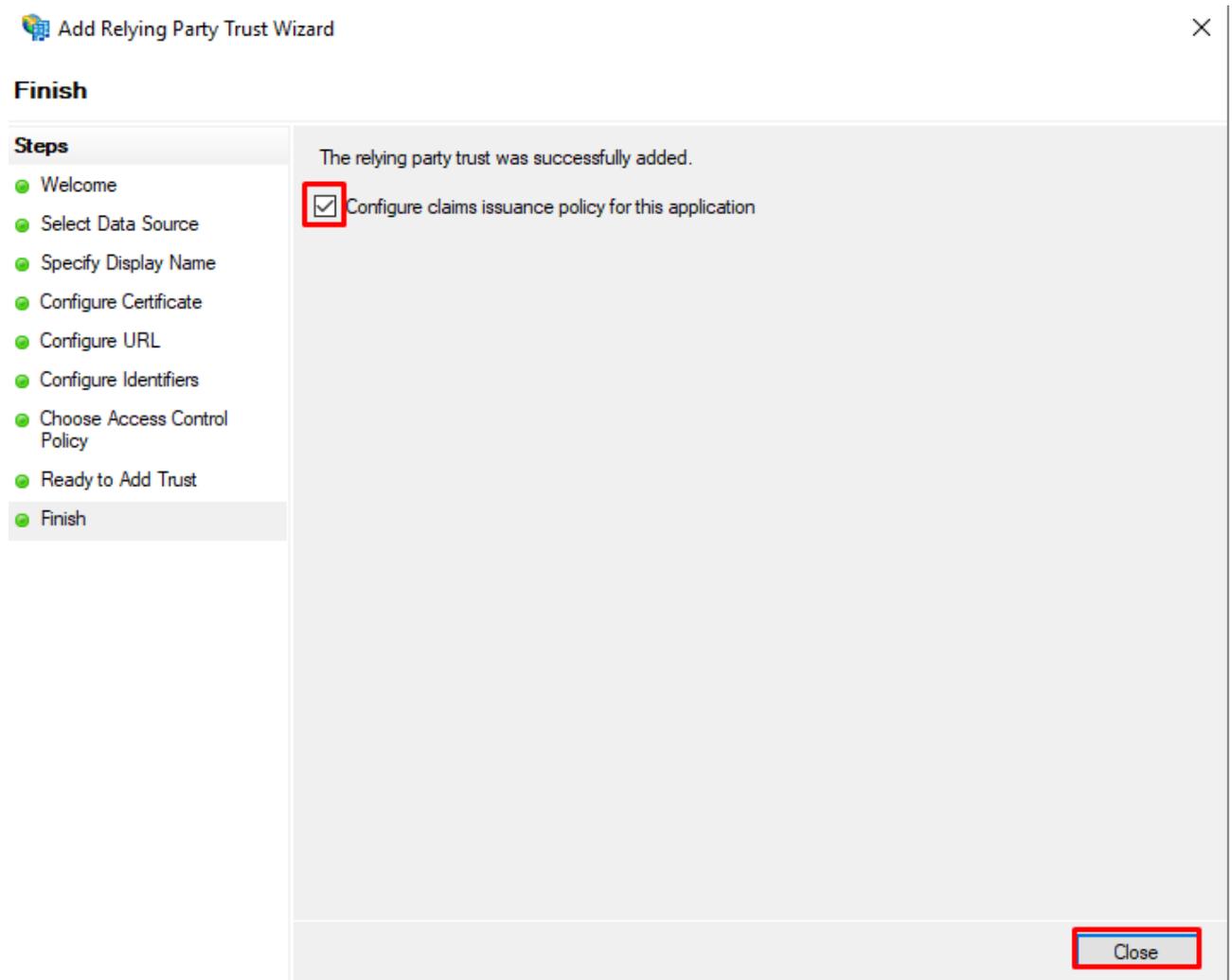
Monitor relying party

Automatically update relying party

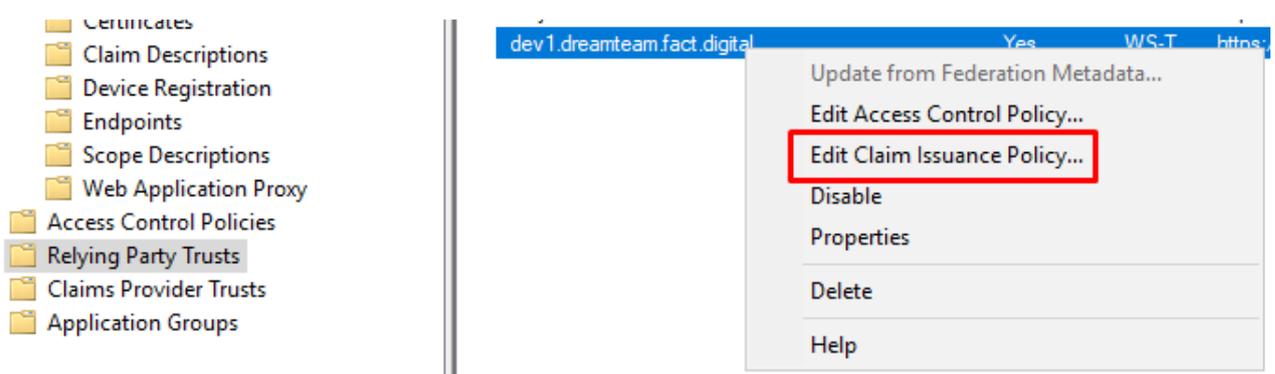
This relying party's federation metadata data was last checked on:
< never >

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

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

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:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous

Next >

Cancel

Edit Rule - Transform Name to Name_ID X

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:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

Pass through all claim values

Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

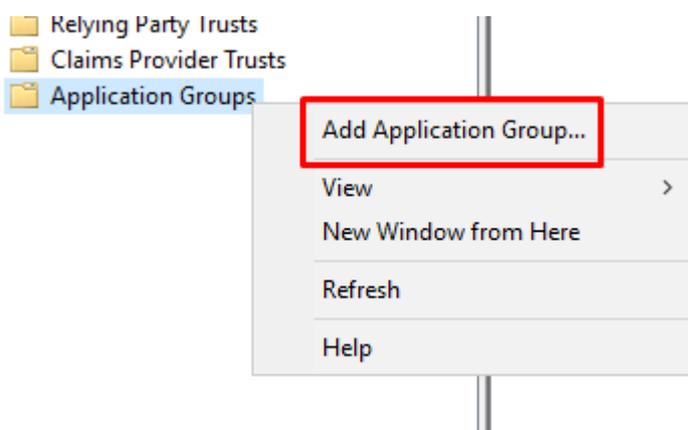
Outgoing claim value:

Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

3.8. Создание группы приложений





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

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

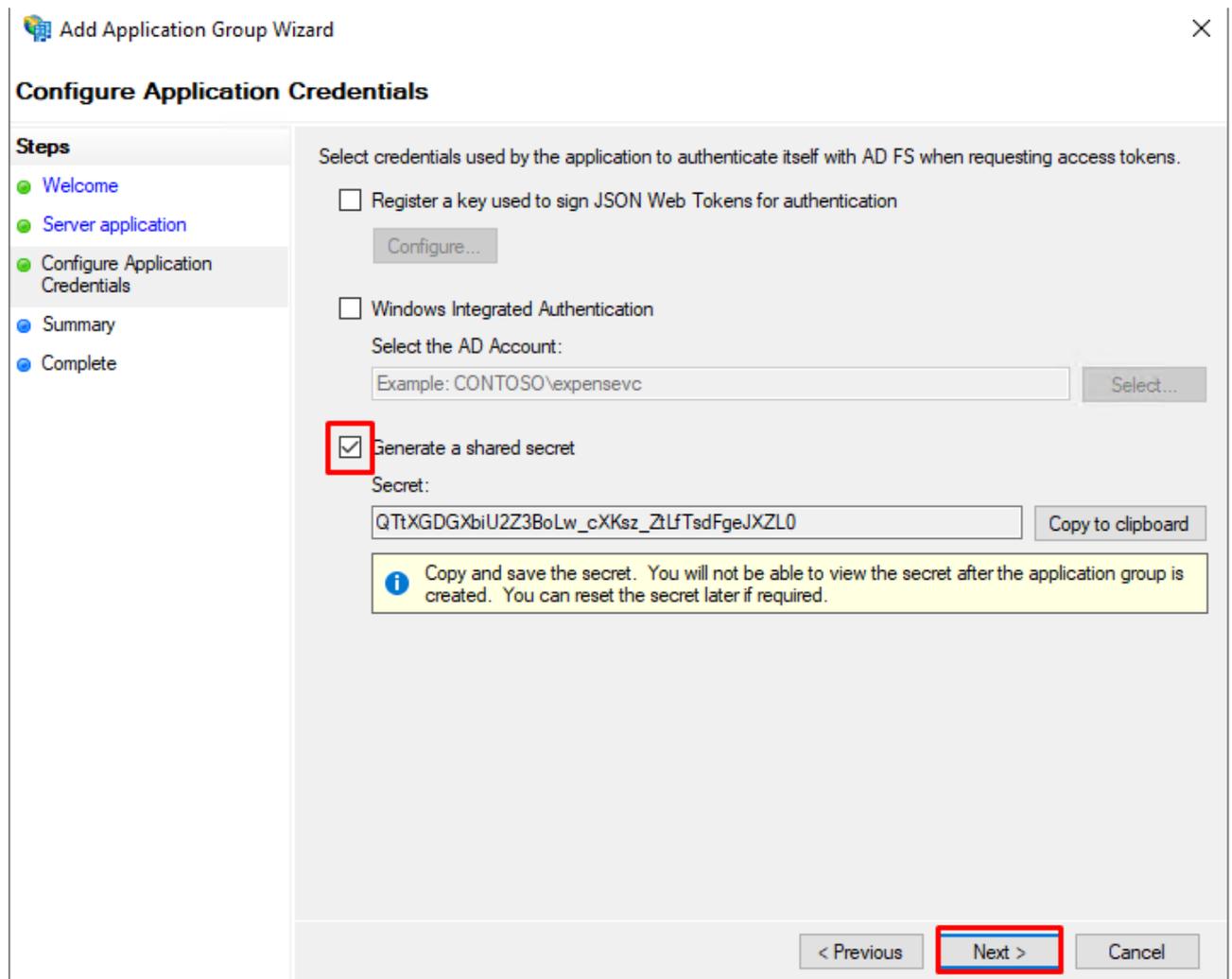
Description:

< Previous

Next >

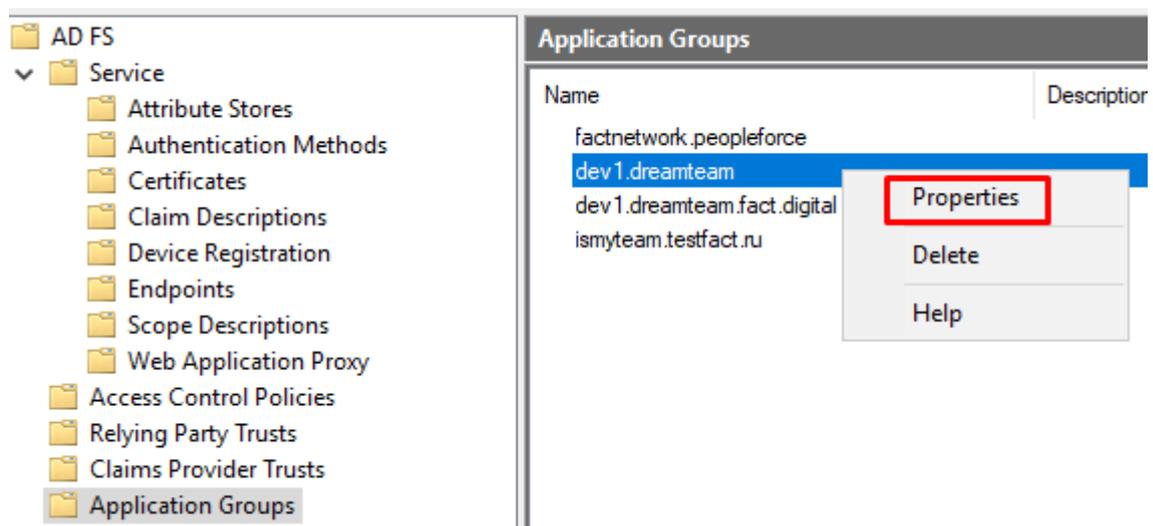
Cancel

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

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

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

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...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA...
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...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA...
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

Configure Application Permissions

Steps

- Welcome
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
dev1.dreamteam - Server application	

Add... Remove

Permitted scopes:

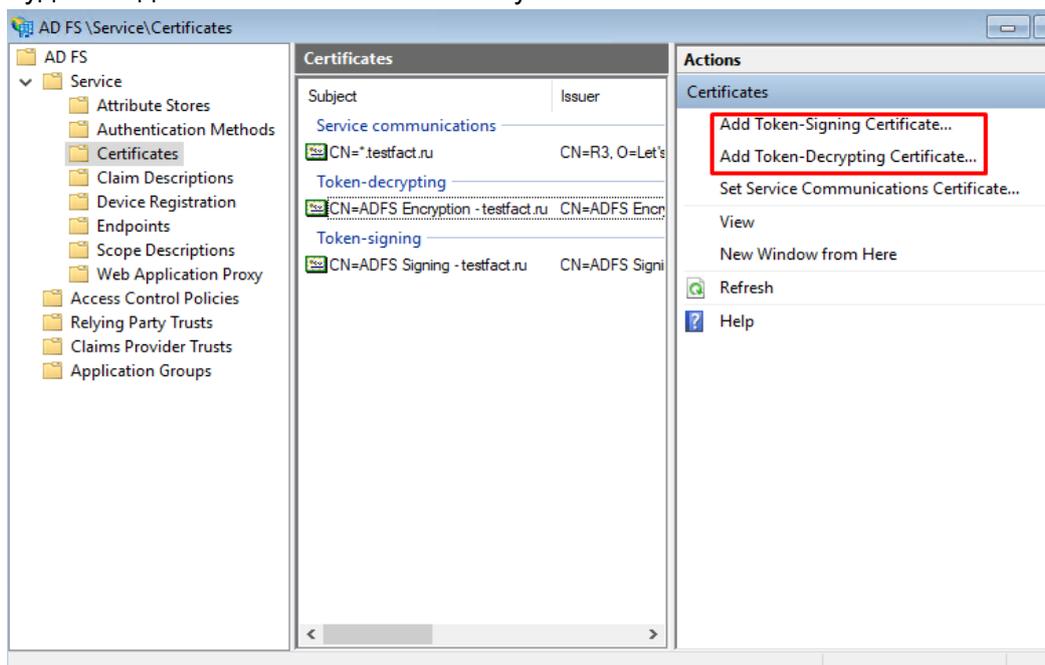
Scope Name	Description
<input type="checkbox"/> allatclaims	Requests the access token claims in the identity token.
<input type="checkbox"/> aza	Scope allows broker client to request primary refresh token.
<input type="checkbox"/> email	Request the email claim for the signed in user.
<input type="checkbox"/> logon_cert	The logon_cert scope allows an application to request logon...
<input checked="" type="checkbox"/> openid	Request use of the OpenID Connect authorization protocol.
<input type="checkbox"/> profile	Request profile related claims for the signed in user.
<input checked="" type="checkbox"/> user_imperso.	Request permission for the application to access the resour...
<input type="checkbox"/> von_cert	The von_cert scope allows an application to request VPN ...

New scope...

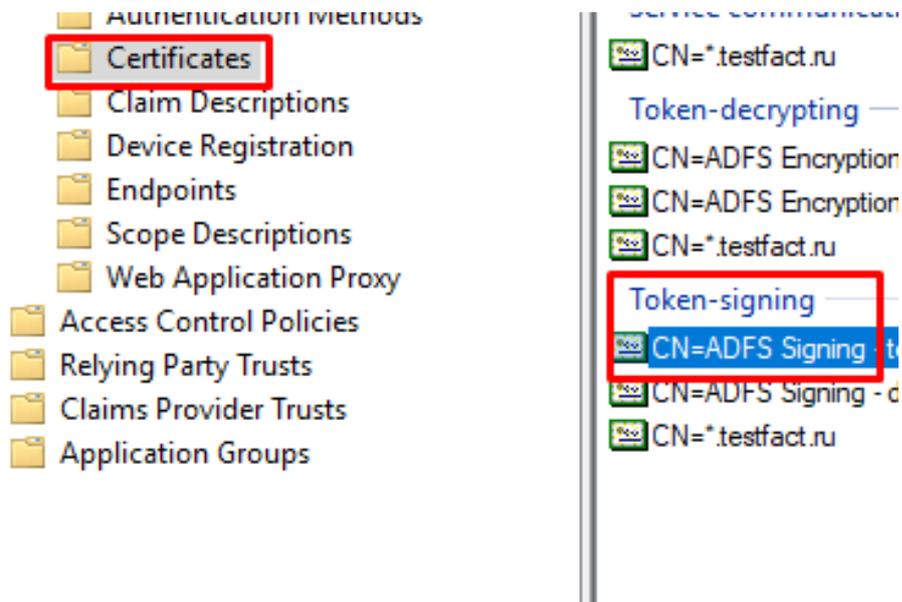
< Previous **Next >** Cancel

Еще раз нажимаем «Next» и «Close».

3.9. В процессе настройки, мастером, возможно, будет предложено выпустить сертификаты, которые используются 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:

The screenshot shows a software interface for editing claim issuance policies. The main window is titled "Edit Claim Issuance Policy for dev1.dreamteam.fact.digital". It features a tab labeled "Issuance Transform Rules" and a text area stating: "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

An "Add Rule..." button is visible on the left side of the main window.

An "Edit Rule - Send LDAP Attributes" dialog box is open in the foreground. It contains the following information:

- Claim rule name:
- Rule template: Send LDAP Attributes as Claims
- Attribute store:
- 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
*		

At the bottom of the dialog box, there are buttons for "View Rule Language...", "OK", and "Cancel".

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

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:

- Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

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

First name:	<input type="text" value="Oleg"/>	Initials:	<input type="text" value="T.A."/>
Last name:	<input type="text" value="Test"/>		
Display name:	<input type="text" value="Test Oleg"/>		
Description:	<input type="text"/>		
Office:	<input type="text"/>		
<hr/>			
Telephone number:	<input type="text" value="+78000000000"/>	<input type="button" value="Other..."/>	
E-mail:	<input type="text" value="test@fact.digital"/>		
Web page:	<input type="text"/>	<input type="button" value="Other..."/>	
<hr/>			
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>	<input type="button" value="Apply"/>
<input type="button" value="Help"/>			