

# Saml SSO настройка

Настройка Relying Party для ADFS на стороне Клиента:

Создание Relying Party Trust

Откройте консоль управления ADFS и выберите в левом дереве консоли **Trust Relationships**, а затем **Relying Party Trusts** В правом меню **Actions** нажмите **Add Relying Party Trust**. С  
клеймами

**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

## Данные вводим вручную

 Add Relying Party Trust Wizard ✕

**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):

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.

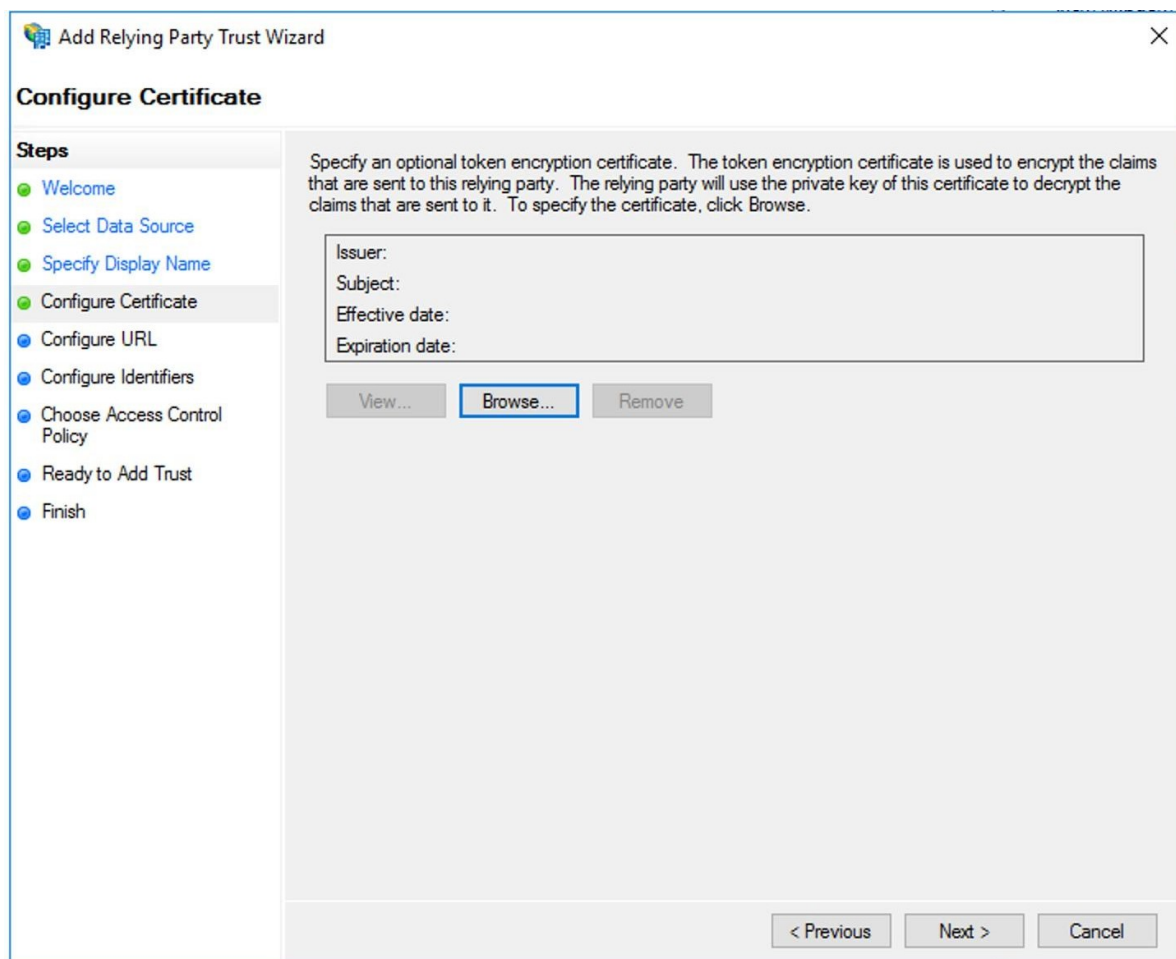
Federation metadata file location:

☒ Enter data about the relying party manually

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

## Без сертификата



**Add Relying Party Trust Wizard**

**Configure Certificate**

**Steps**

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

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

Issuer:  
Subject:  
Effective date:  
Expiration date:

View... Browse... Remove

< Previous Next > Cancel

Включаем SAML 2.0 и **указываем** следующий сервис URL:

`https://домен-портала/local/adfs/?acs`

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Configure URL' step. The window has a title bar with a close button. On the left, there is a 'Steps' pane with a list of steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains instructions and configuration options. It starts with a paragraph explaining that AD FS supports WS-Trust, WS-Federation, and SAML 2.0 WebSSO protocols. Below this, there are two checkboxes. The first checkbox, 'Enable support for the WS-Federation Passive protocol', is unchecked. Below it, a text box is labeled 'Relying party WS-Federation Passive protocol URL:' with an example URL 'https://fs.contoso.com/adfs/ls/'. The second checkbox, 'Enable support for the SAML 2.0 WebSSO protocol', is checked. Below it, a text box is labeled 'Relying party SAML 2.0 SSO service URL:' with the URL 'https://k-team-tst.mr-group.ru/?acs' entered. An example URL 'https://www.contoso.com/adfs/ls/' is also provided. At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'. A red text overlay 'Введите текст' is positioned over the 'Relying party WS-Federation Passive protocol URL' text box.

**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:

`https://k-team-tst.mr-group.ru/?acs`

Example: `https://www.contoso.com/adfs/ls/`

< Previous   **Next >**   Cancel

# Идентификатор

https://домен-портала/

https://домен-портала/adfs/



Add Relying Party Trust Wizard



## Configure Identifiers

### Steps

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

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Add

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

https://k-team-tst.mr-group.ru/  
https://k-team-tst.mr-group.ru/adfs/

Remove

< Previous

Next >

Cancel

**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 require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specific groups.

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

Алгоритм хэша, должен быть

SHA-256

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.

MonitoringIdentifiersEncryptionSignatureAccepted ClaimsOrganizationEndpointsNotes

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

**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.

Encryption	Signature	Accepted Claims	Organization	Endpoints	Notes	Advanced	◀ ▶
<p>Specify the secure hash algorithm to use for this relying party trust.</p> <p>Secure hash algorithm: <span style="border: 1px solid #ccc; padding: 2px 10px;">SHA-256</span> ▼</p>							

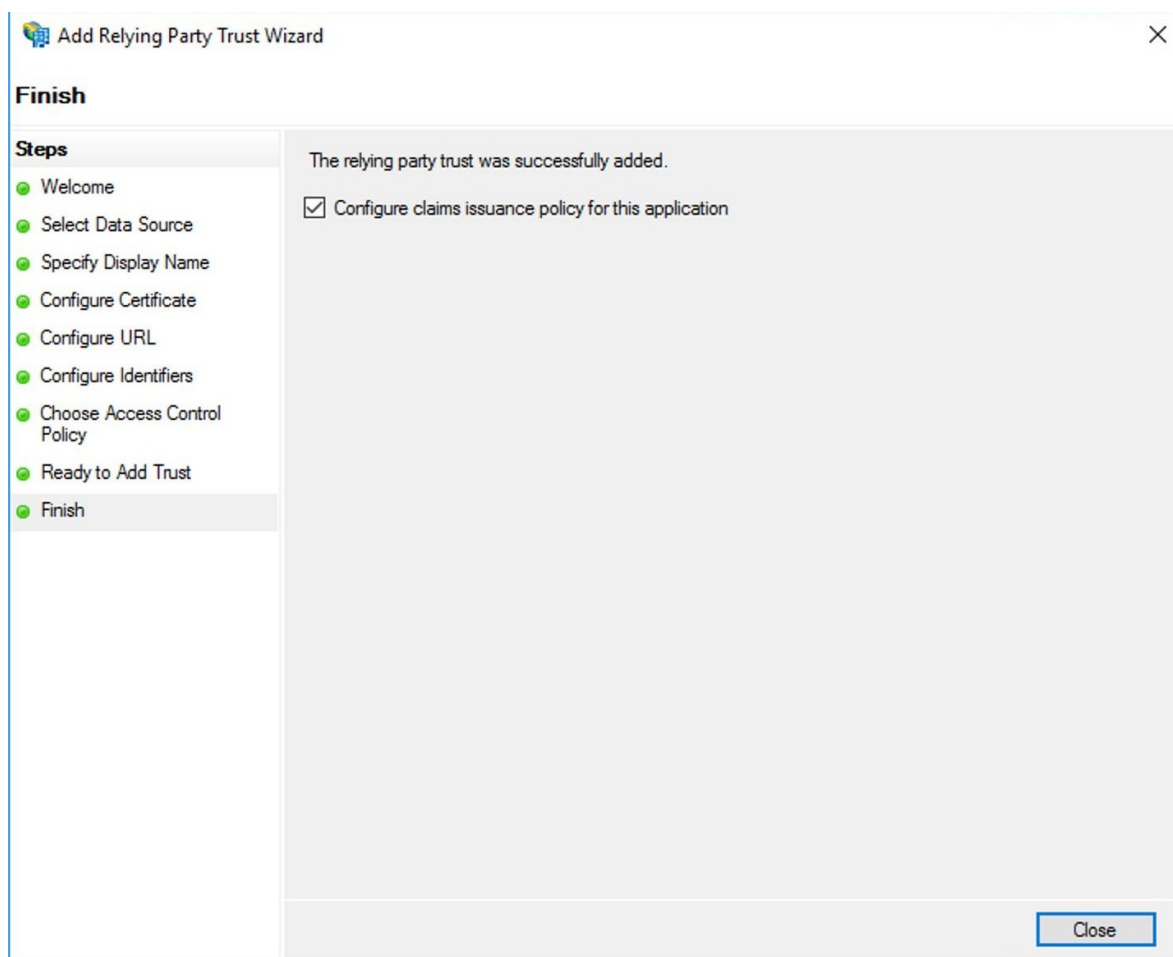
&lt; Previous

Next &gt;

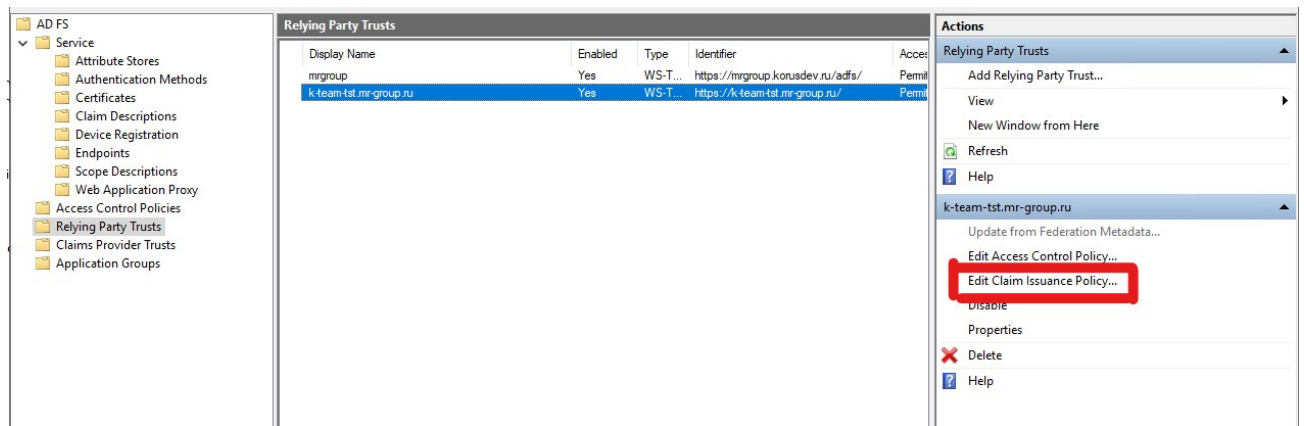
Cancel



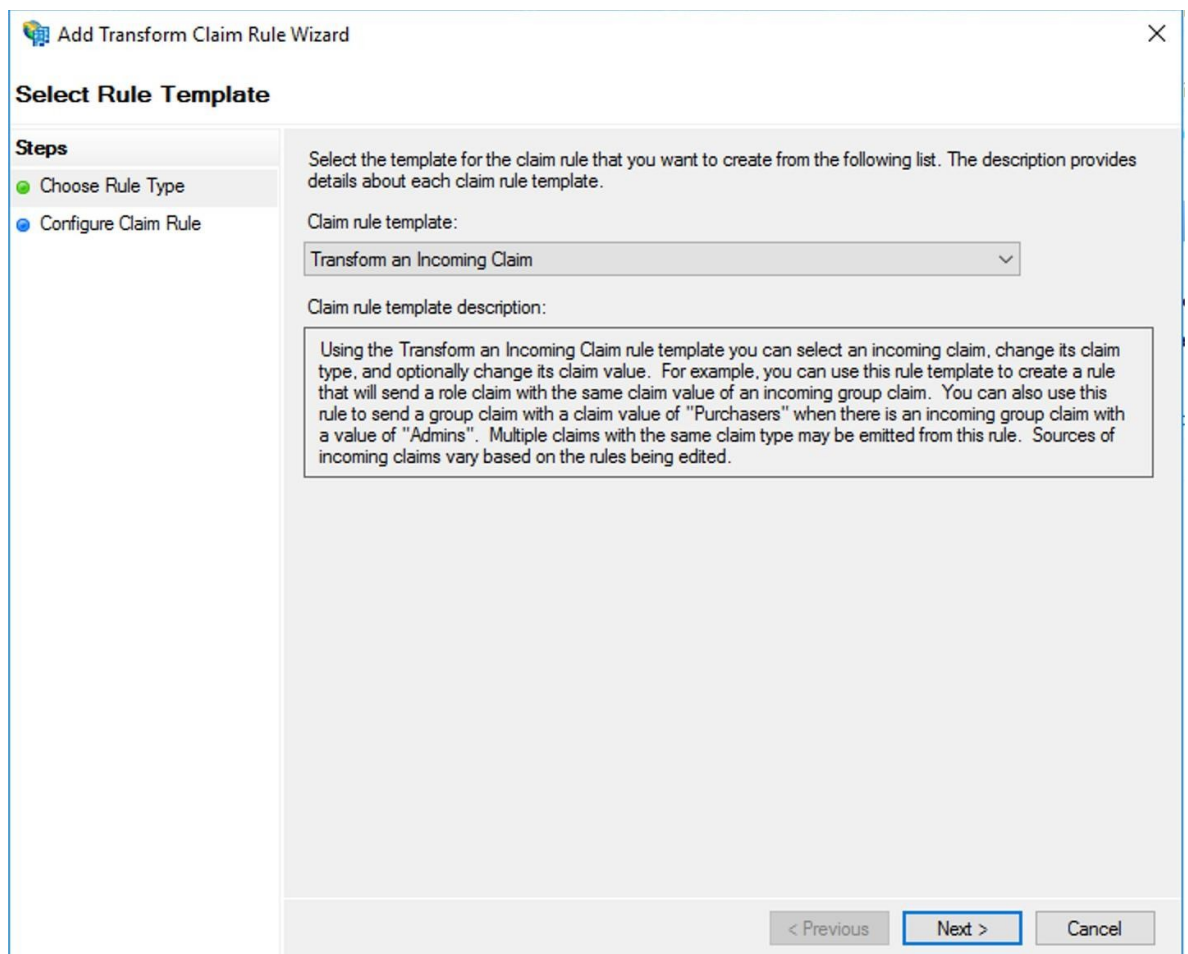
Если все верно, то подтверждаем



# Настройка Claims




## 1. NameId



## 2. Имя исходящего клейма (если нет в выпадающем списке)

Name ID

 Add Transform Claim Rule Wizard ✕

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

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. LDAP атрибуты

**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

LDAP	исходящий claim
SAM-Account-Name	AuthNRequestID

Claim rule name:

LDAP

Rule template: Send LDAP Attributes as Claims

Attribute store:

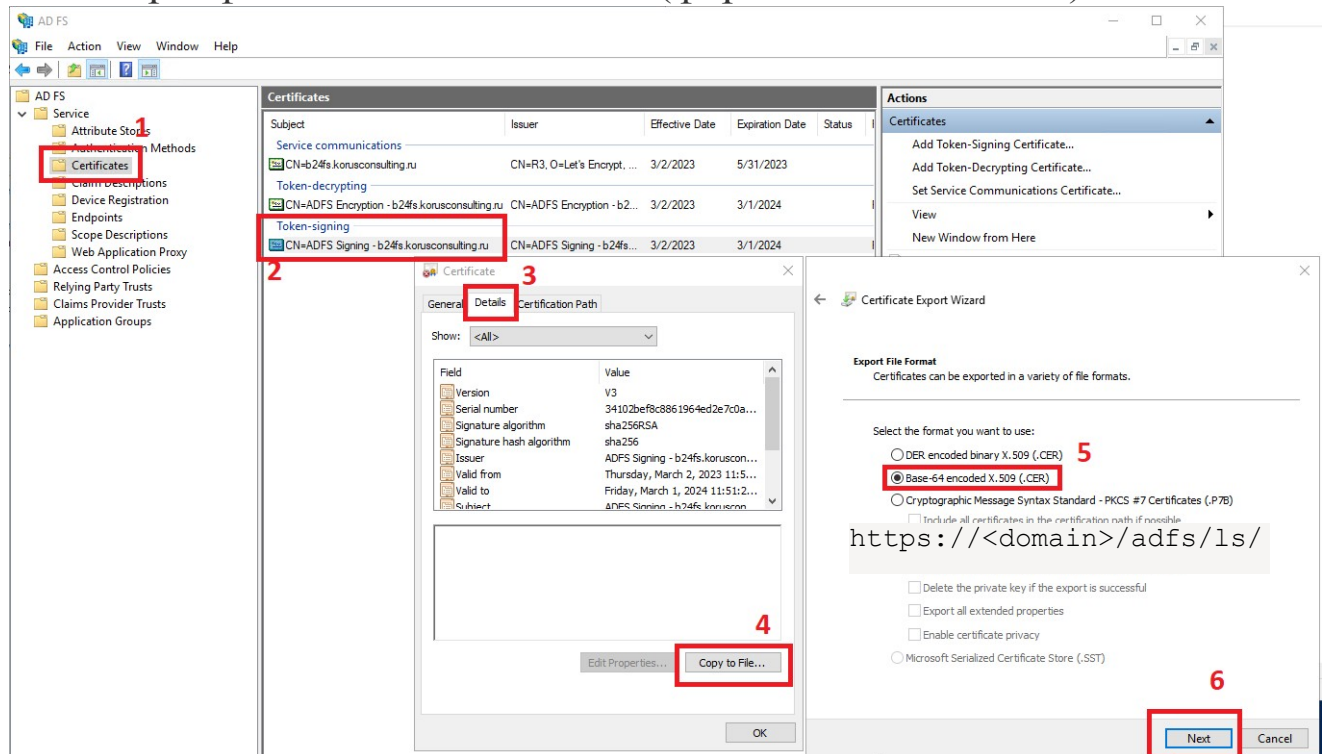
Active Directory

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)
▶	SAM-Account-Name	AuthNRequestID
*		

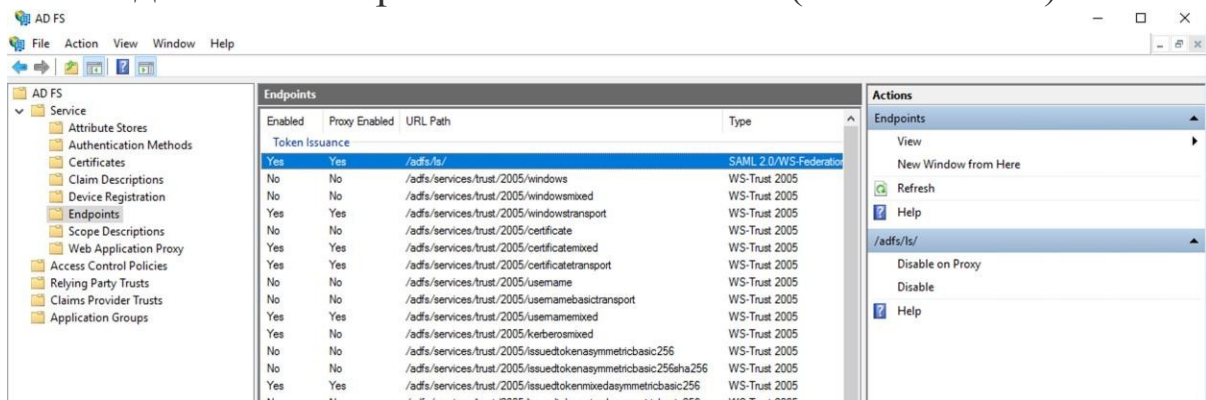
Передача данных для настройки:

### 1. Сертификат подписи токенов (формат x509 в base64)



### 2. адрес точки входа в логин, это обычно

надо чтоб эта прокси была включена (Enabled - Yes)



### 3. Entity Id домена, посмотреть можно в свойствах ADFS, обычно это `http://<domain>/ads/services/trust`

Federation Service Properties ✕

General Organization Events

Federation Service display name:  
KorusDev ADFS

Example: Fabrikam Federation Service

Federation Service name:  
b24fs.korusconsulting.ru

Example: fs.fabrikam.com

Federation Service identifier:  
<http://b24fs.korusconsulting.ru/adfs/services/trust>

Example: <http://fs.fabrikam.com/adfs/services/trust>

Web SSO lifetime (minutes): 480 ▲ ▼

☐ Enable delegation for service administration

Delegate name:

Edit...

☐ Allow Local System account for service administration

☒ Allow Local Administrators group for service administration

OK Cancel Apply