Setting up NEXL and ADFS.

NEXL CRM

https://nexlcrm.com

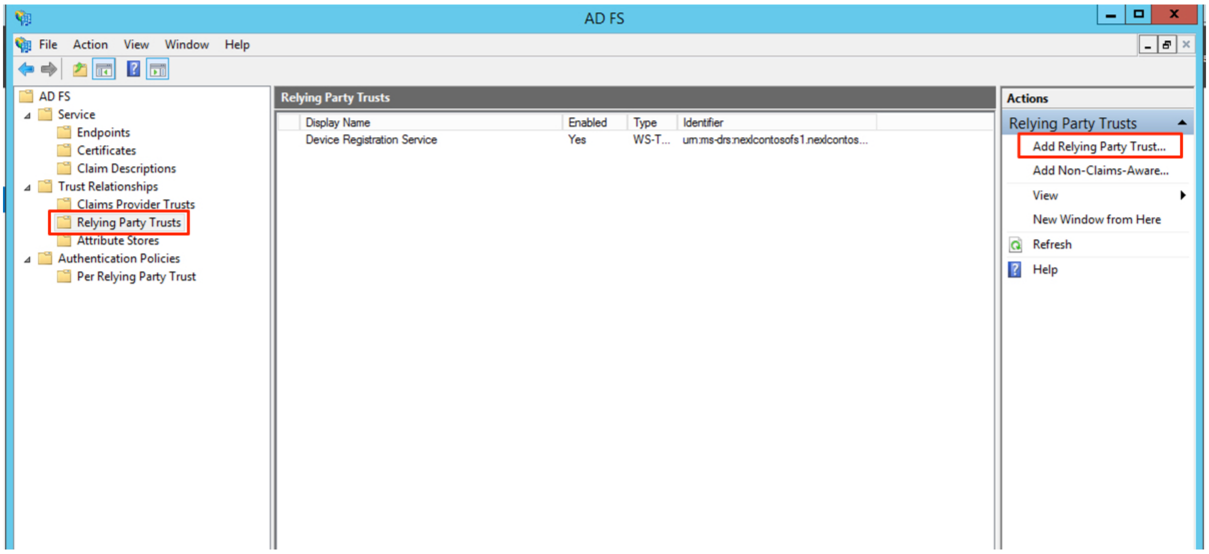
AUSTRALIA • USA • MEXICO• UK

Table of Contents

Create a new Relaying Party Trust

Getting started

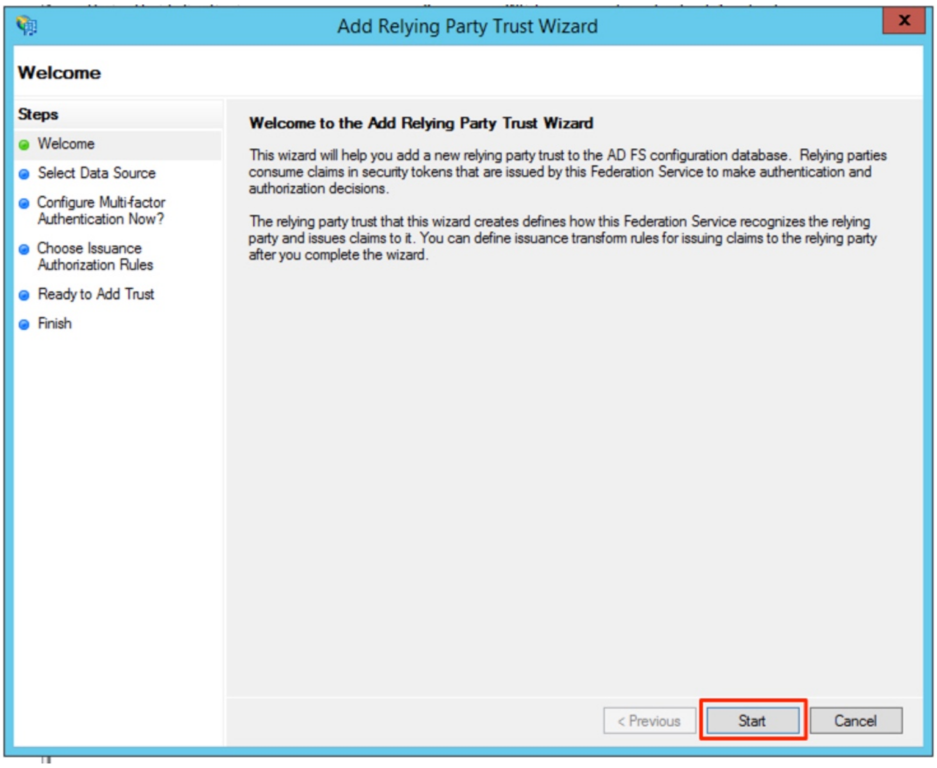
To get started with your ADFS setup, open the ADFS management console, open the Relying Party Trusts folder and click on “Add Relying Party Trust”



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:nexlcontosofs1.nexlcontos...

The Add Replying Party Trust Wizard will open. Please click on “Start”


Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Start
Cancel

Welcome to the Add Relying Party Trust Wizard

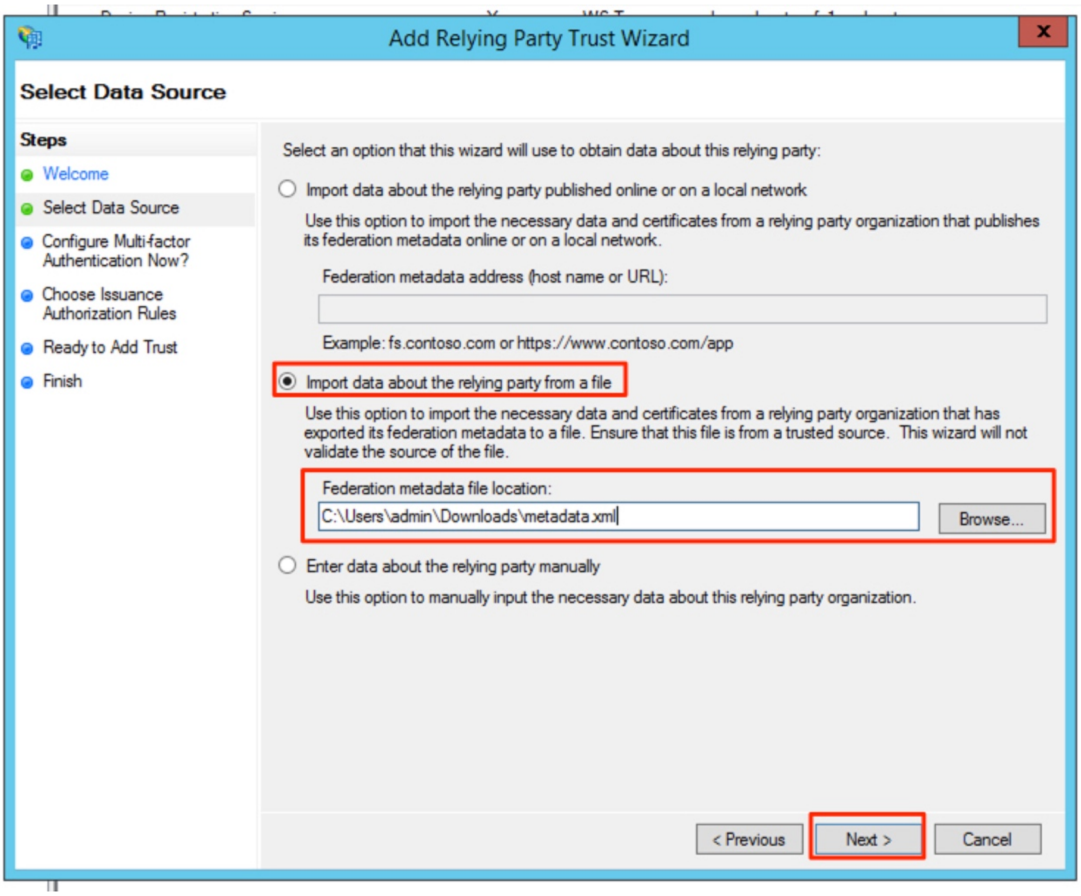
This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

Download and select data source

The wizard will ask you to provide a data source for the configuration XML file. Please download NEXL's federation metadata file here: https://360.nexl.io/saml/1b959aa5-baa4-4b32-a6f4-15b315df8729/metadata.xml

Save the XML on your ADFS server and select to "Import data about the relying party from a file" and click browse and select the downloaded XML.



Add Relying Party Trust Wizard

Select Data Source

Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
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

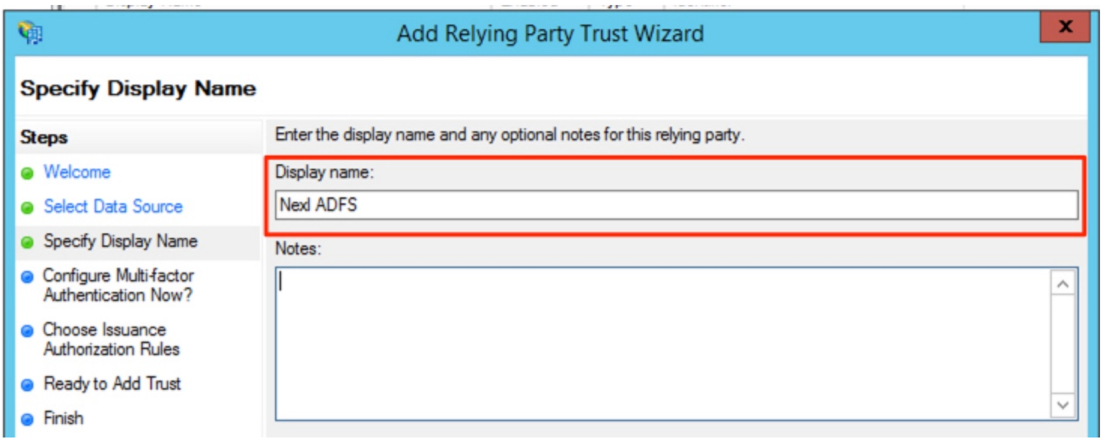
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location: C:\Users\admin\Downloads\metadata.xml

○ Enter data about the relying party manually

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

Please specify a Display Name. The display name has no impact on the configuration and is for your internal use only.



Add Relying Party Trust Wizard

Specify Display Name

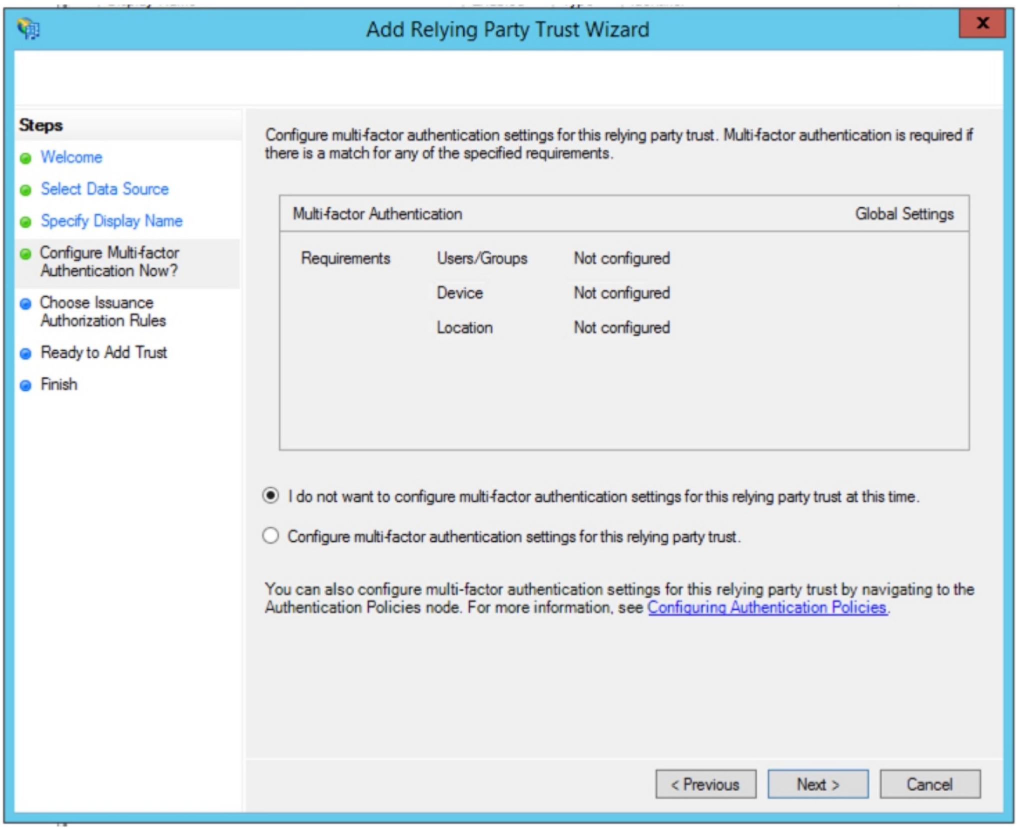
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

Enter the display name and any optional notes for this relying party.

Display name: Nexl ADFS

Notes:

Depending on your internal configuration and requirements, you can enable 2FA. In our case, we will skip this step and click on "Next".



Add Relying Party Trust Wizard

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

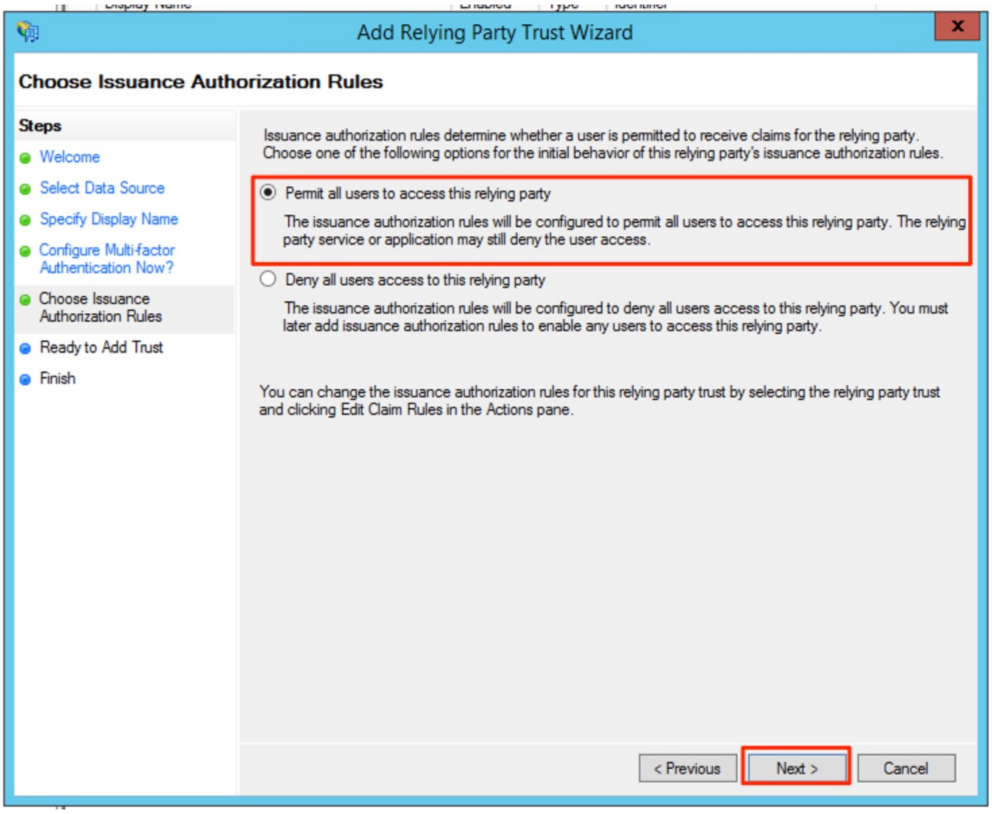
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

On the next screen, please "Permit all users to access this relying party" and click next.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

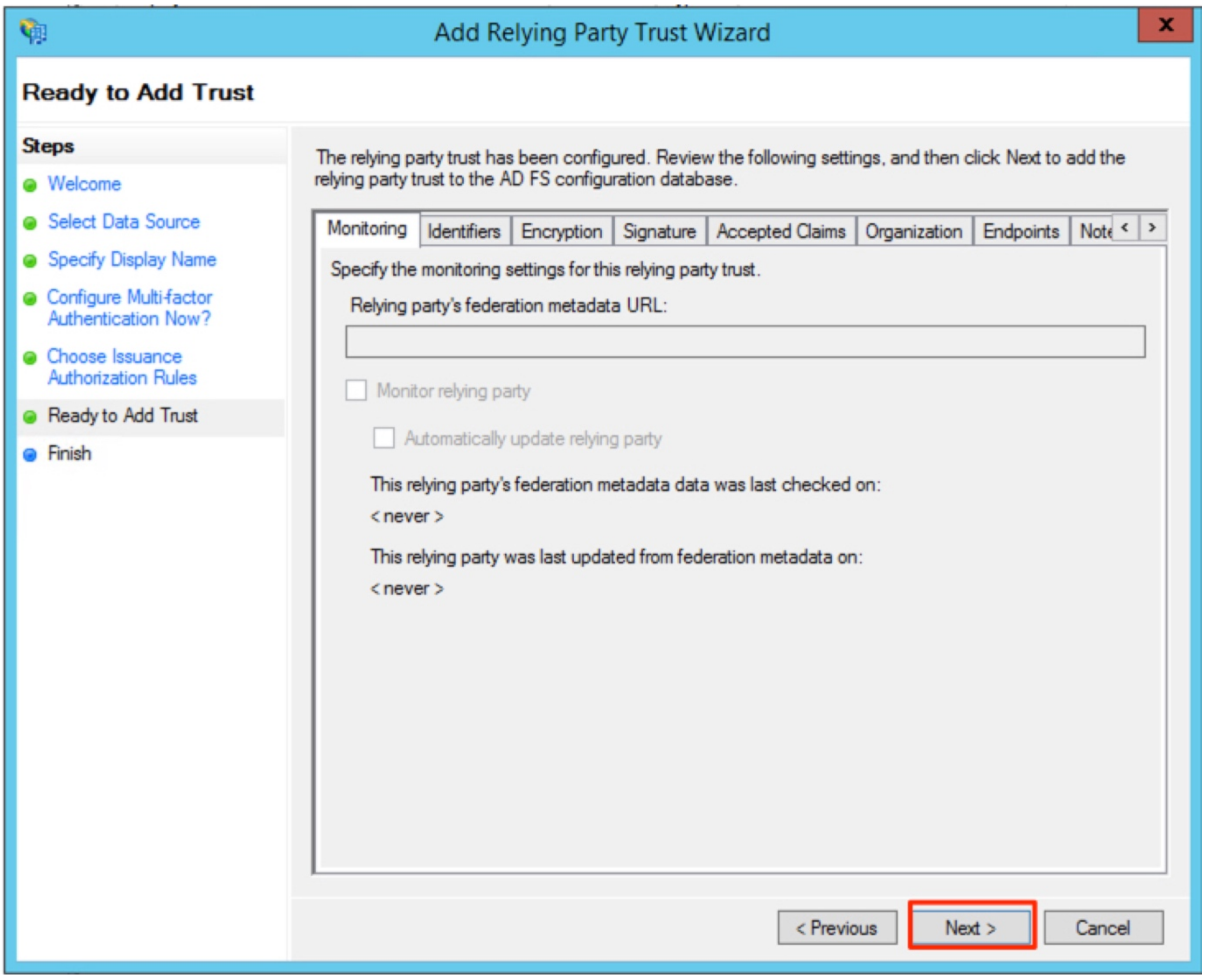
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

Now we are ready to add the new Relying Party Trust. Simple click on Next and then finish the setup.



Ready to Add Trust

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.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

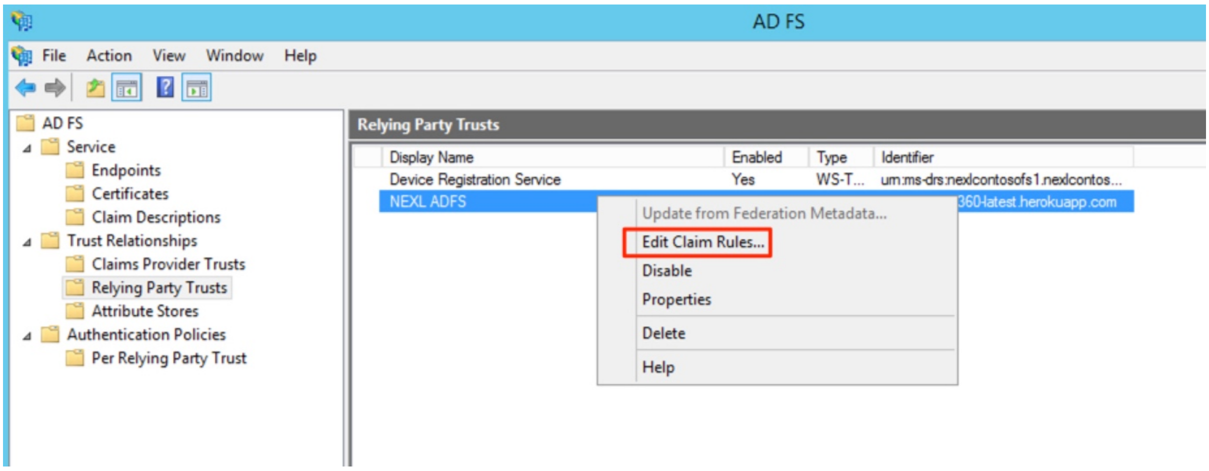
□ Automatically update relying party

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

This relying party was last updated from federation metadata on:
< never >

Adding Claim rules for your newly created Relying Party Trust.

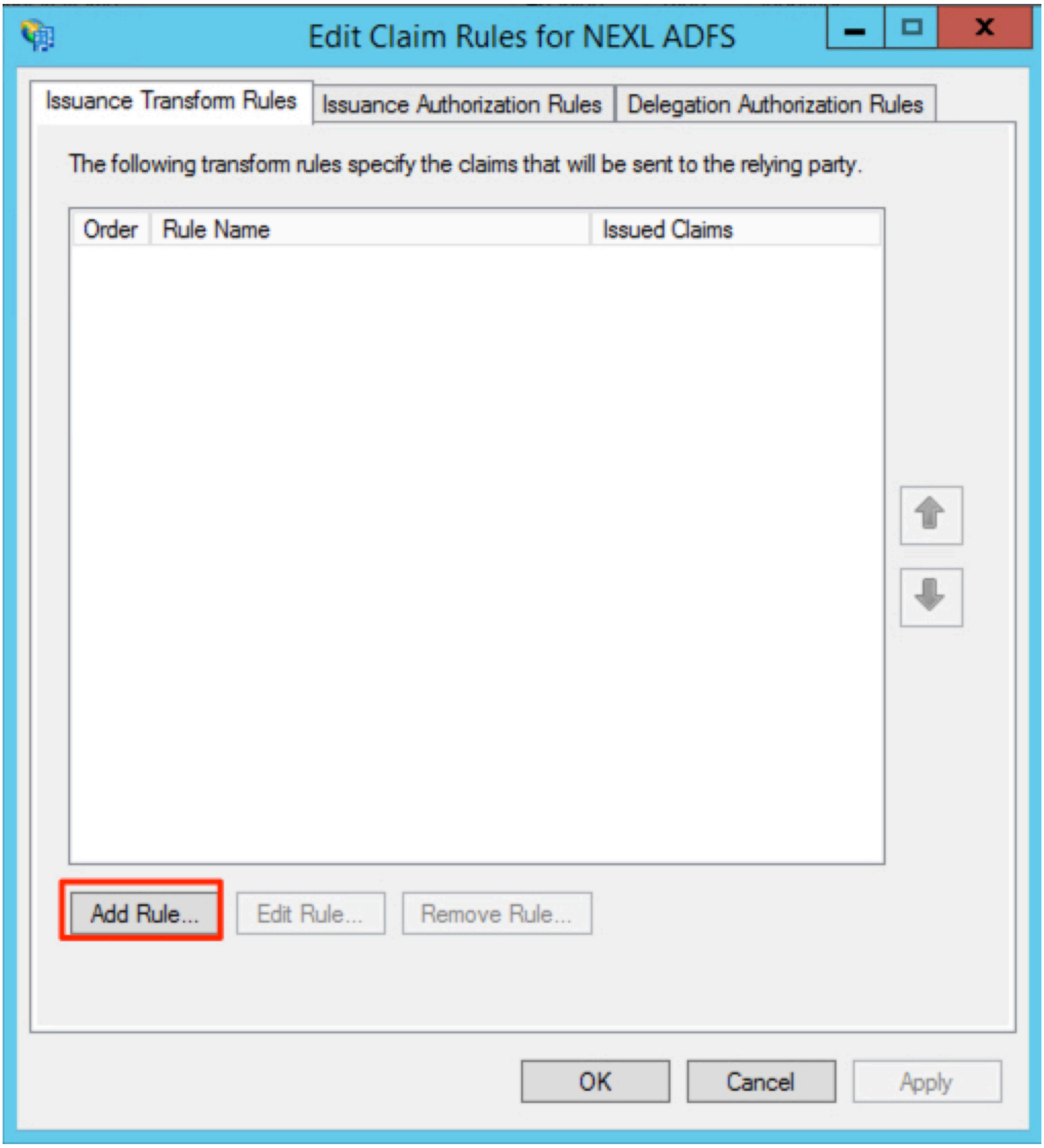
For the next step, we will need to add the required Claim Rules to the newly created Relying Party Trust. Please right click on the party trust and select "Edit Claim Rules…"



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:nexlcontosofs1.nexlcontos...
NEXL ADFS			360-latest.herokuapp.com

Click on “Add Rule..”

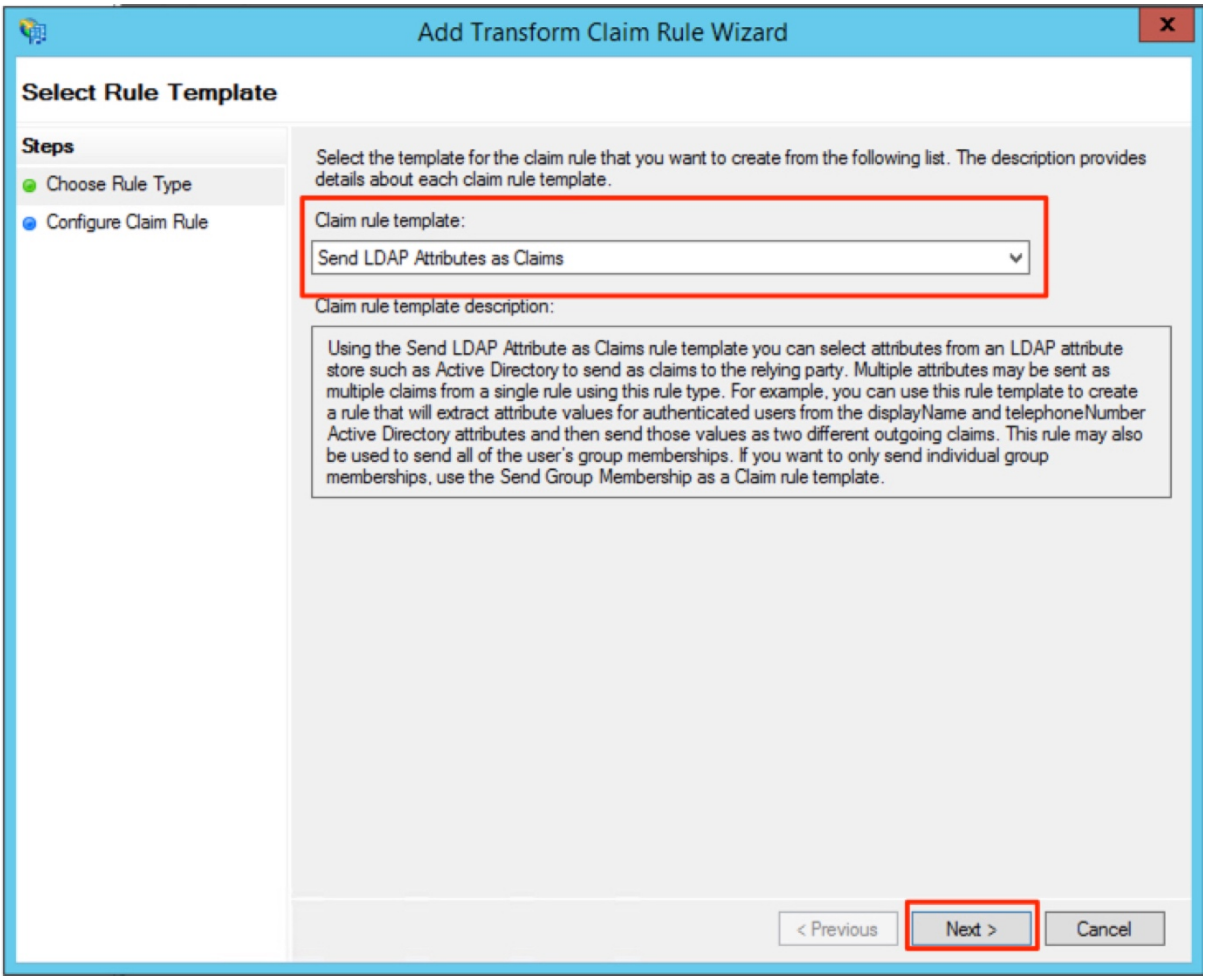

Edit Claim Rules for NEXL ADFS
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

Please select the “Send LDAP Attributes as Claims” rule template and click “Next”.



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

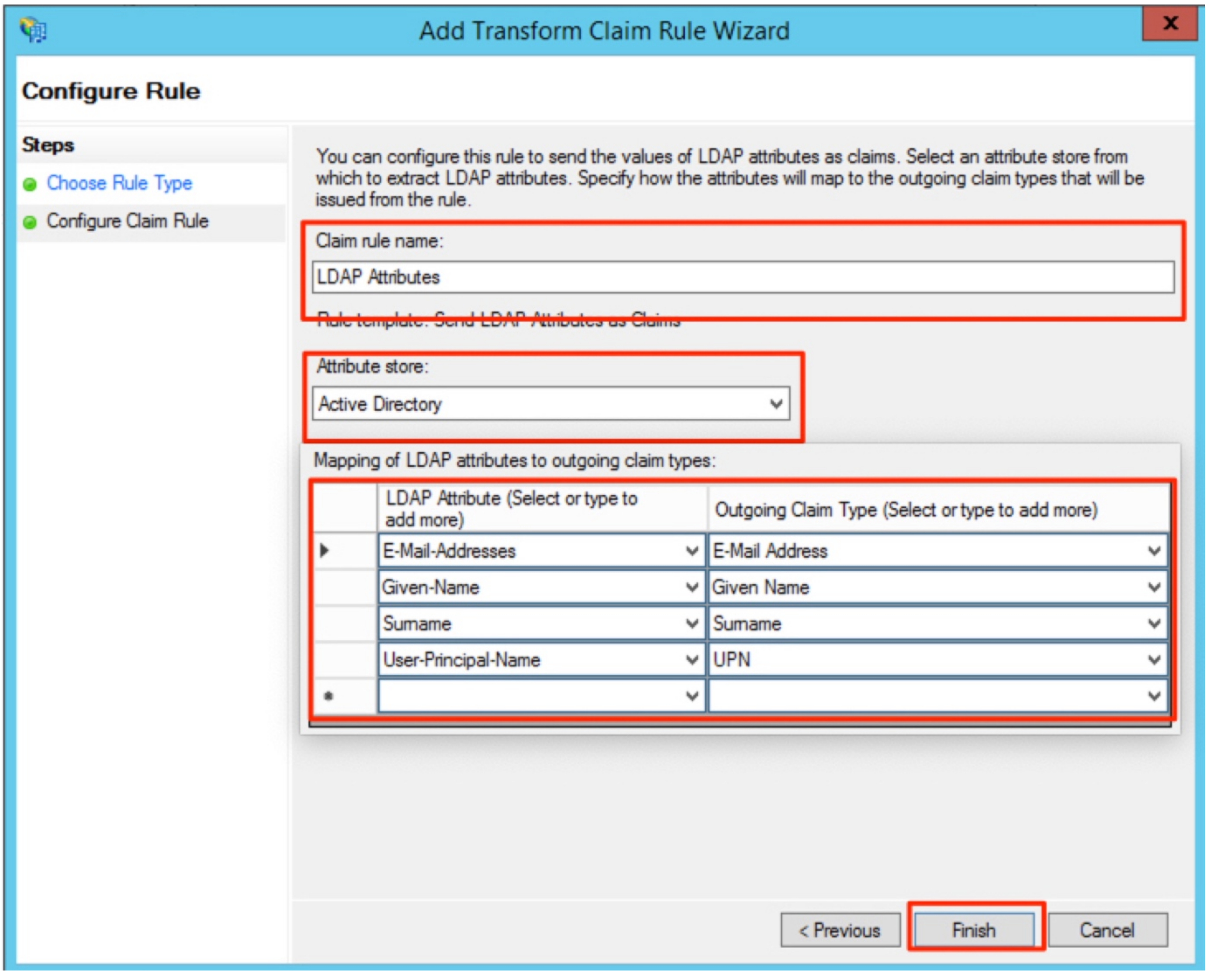
Claim rule template description:

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.

Next, we will configure the Claim Rules. Add a Rule name (which is for your internal use only) and select “Active Directory” for the attribute store. Then use the drop down in the “Mapping of LDAP attributes…” to add the following mapping:

- **Email Addresses -> E-Mail Address**
- **Given-Name -> Given Name**
- **Surname -> Surname**
- **User-Principal-Name -> UPN**

Then click on finish.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
LDAP Attributes

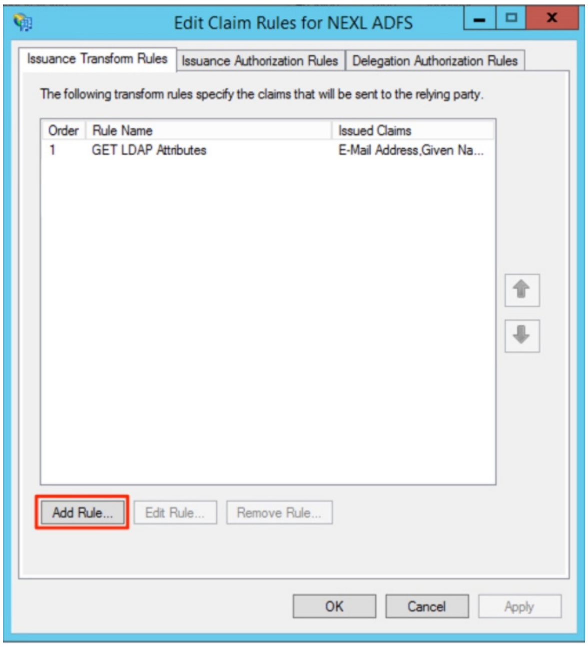
Rule template: Send LDAP Attributes as Claims

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
Given-Name	Given Name
Surname	Surname
User-Principal-Name	UPN

Add a second rule. Click on “Add Rule…” again.

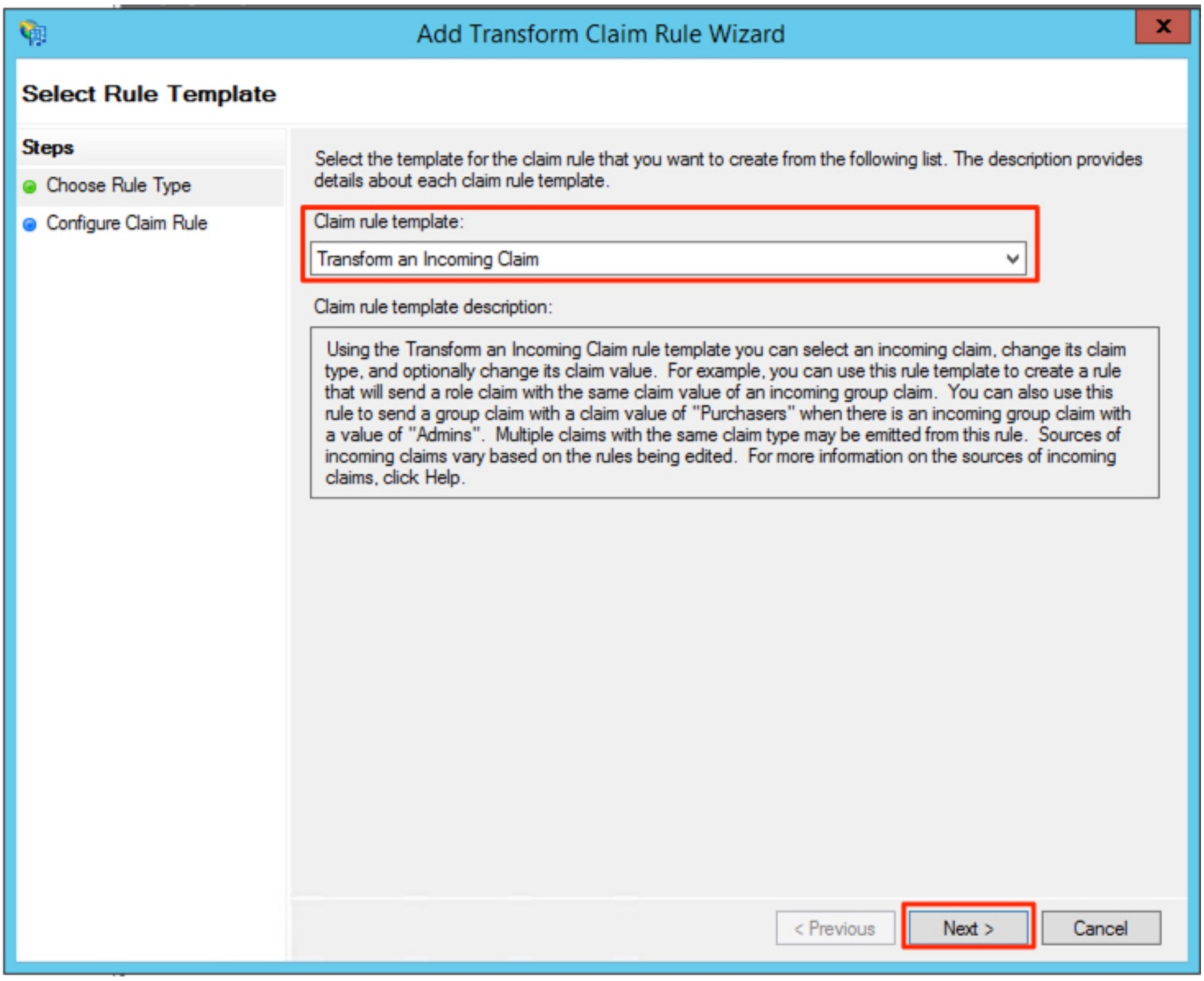

Edit Claim Rules for NEXL ADFS
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	GET LDAP Attributes	E-Mail Address,Given Na...

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

This time select the “Transform an Incoming Claim” rule template and click on “Next



Select Rule Template

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

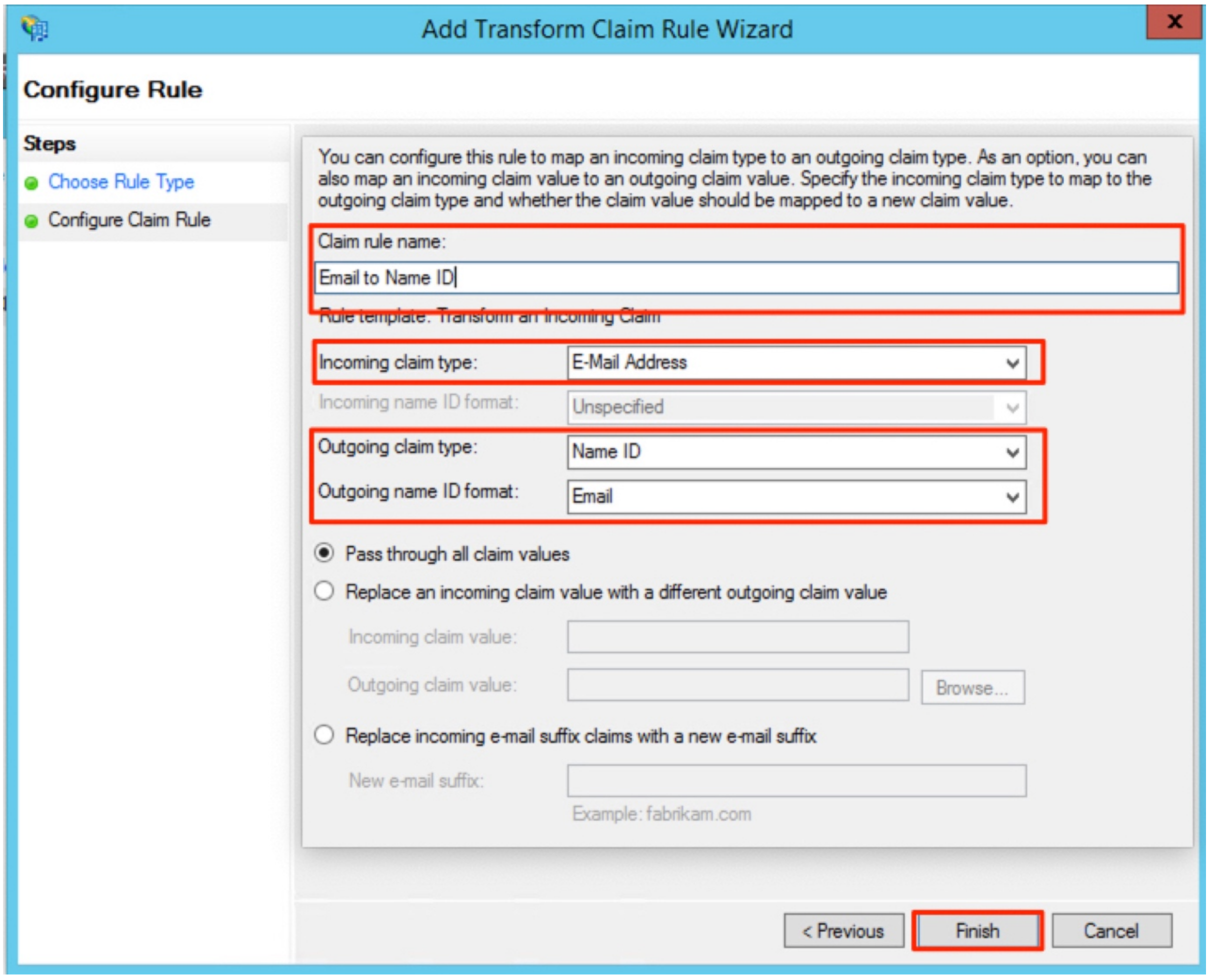
Claim rule template description:

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. For more information on the sources of incoming claims, click Help.

Please enter a Claim rule name. This is for internal use only. Please set the

- “Incoming claim type” to “E-Mail Address”
- “Outgoing claim type” to “Name ID”
- “Outgoing name ID format” to “Email”

Then click on “Finish”



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:

Email 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

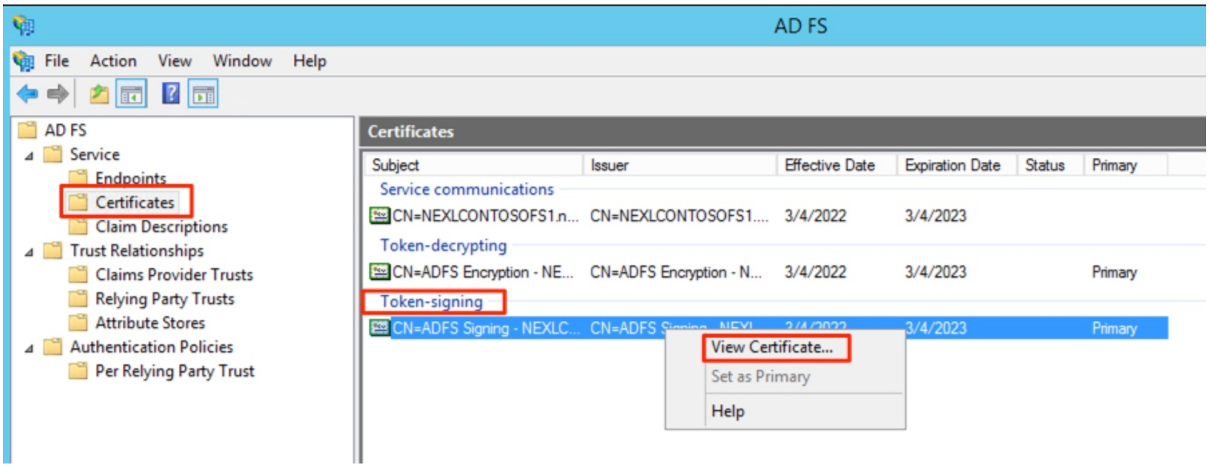
New e-mail suffix:

Example: fabrikam.com

Export your Token-signing certificate

As for last step, please export your Token-signing certificate and send it to a team member at NEXL.

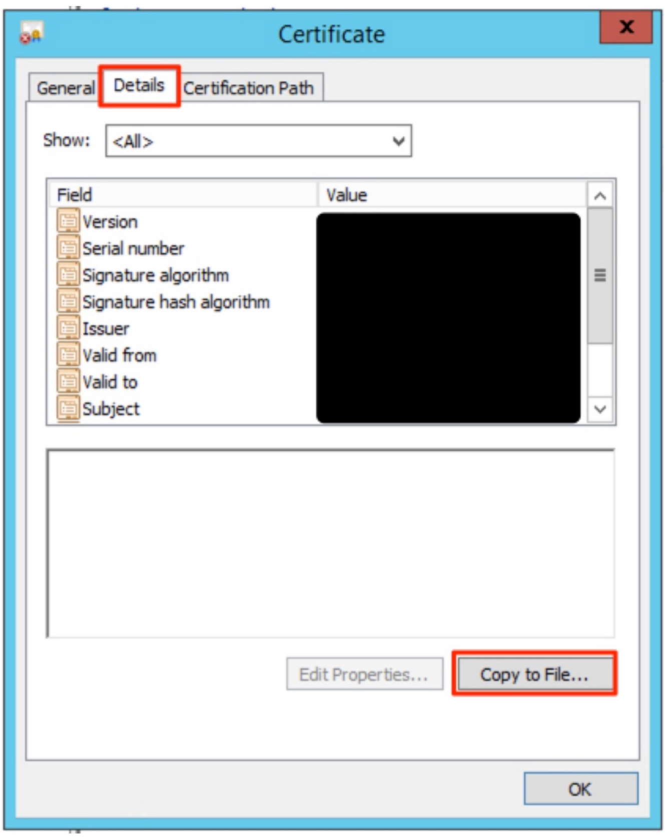
To export the certificate, go to the “Service” -> “Certificates” folder and right click on the certificate under “Token-singing” and click on “View Certificate”



Certificates

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=NEXLCONTOSOFS1.n...	CN=NEXLCONTOSOFS1....	3/4/2022	3/4/2023		
Token-decrypting					
CN=ADFS Encryption - NE...	CN=ADFS Encryption - N...	3/4/2022	3/4/2023		Primary
Token-signing					
CN=ADFS Signing - NEXLC...	CN=ADFS Signing - NEXL...	3/4/2022	3/4/2023		Primary

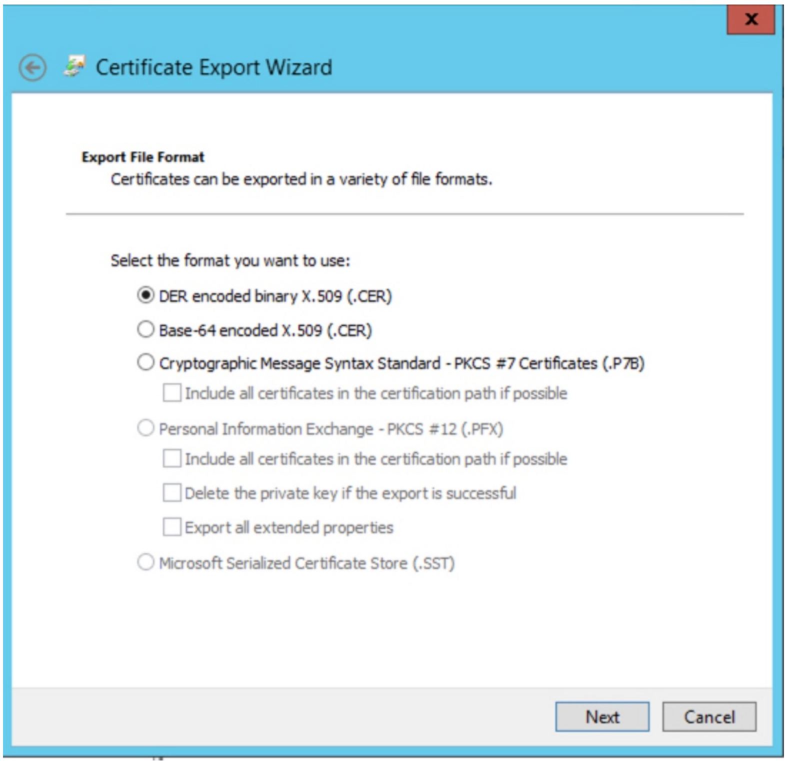
Then open the “Details” tab and click on “Copy to File”



Show: <All>

Field	Value
Version	[redacted]
Serial number	[redacted]
Signature algorithm	[redacted]
Signature hash algorithm	[redacted]
Issuer	[redacted]
Valid from	[redacted]
Valid to	[redacted]
Subject	[redacted]

Export the certificate in DER format, save it to your desktop and then share the resulting .cer file with NEXL.



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)