*D:\Downloads\adfsConfig.xml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

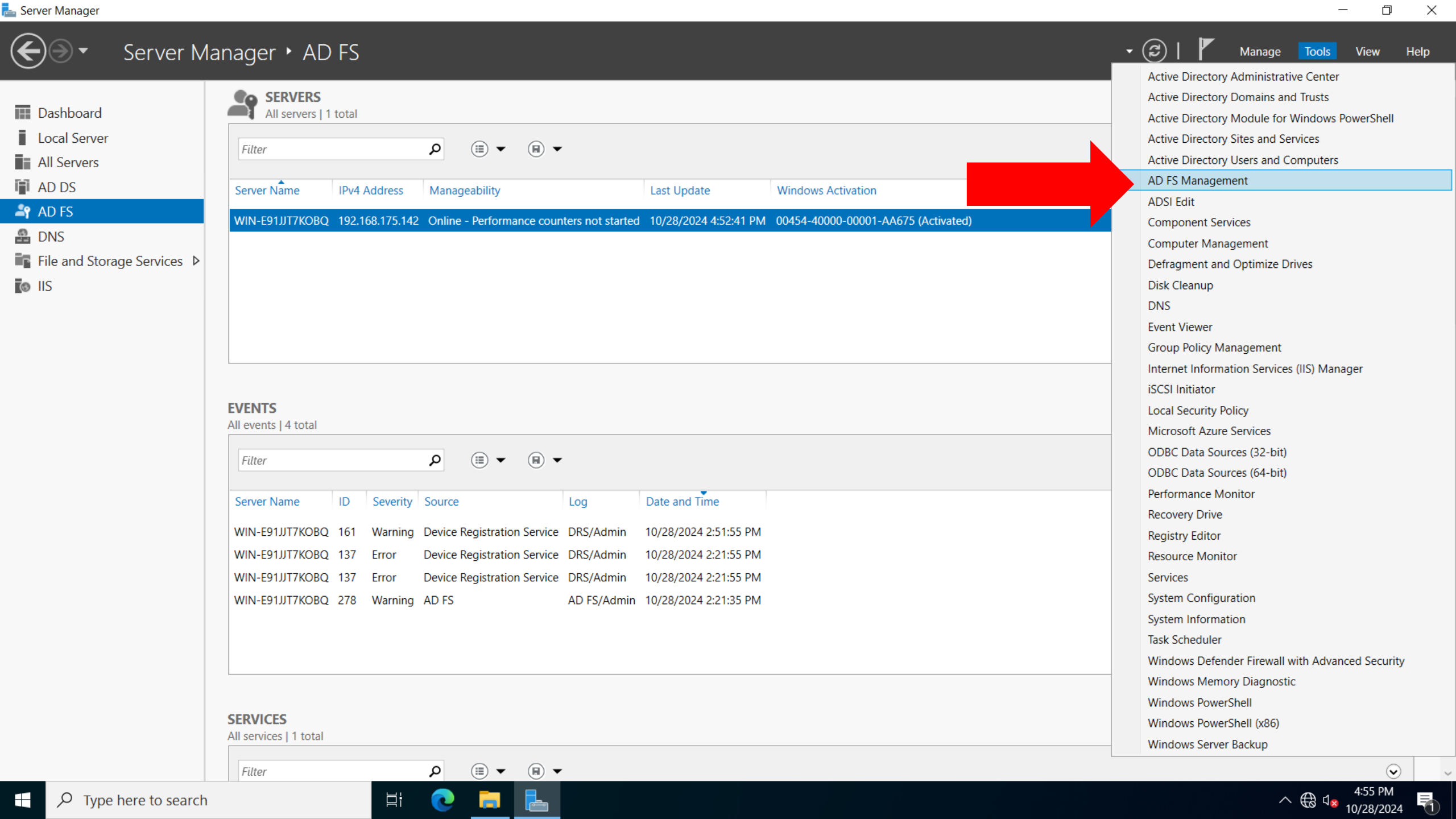
.env.example | adfsConfig.xml

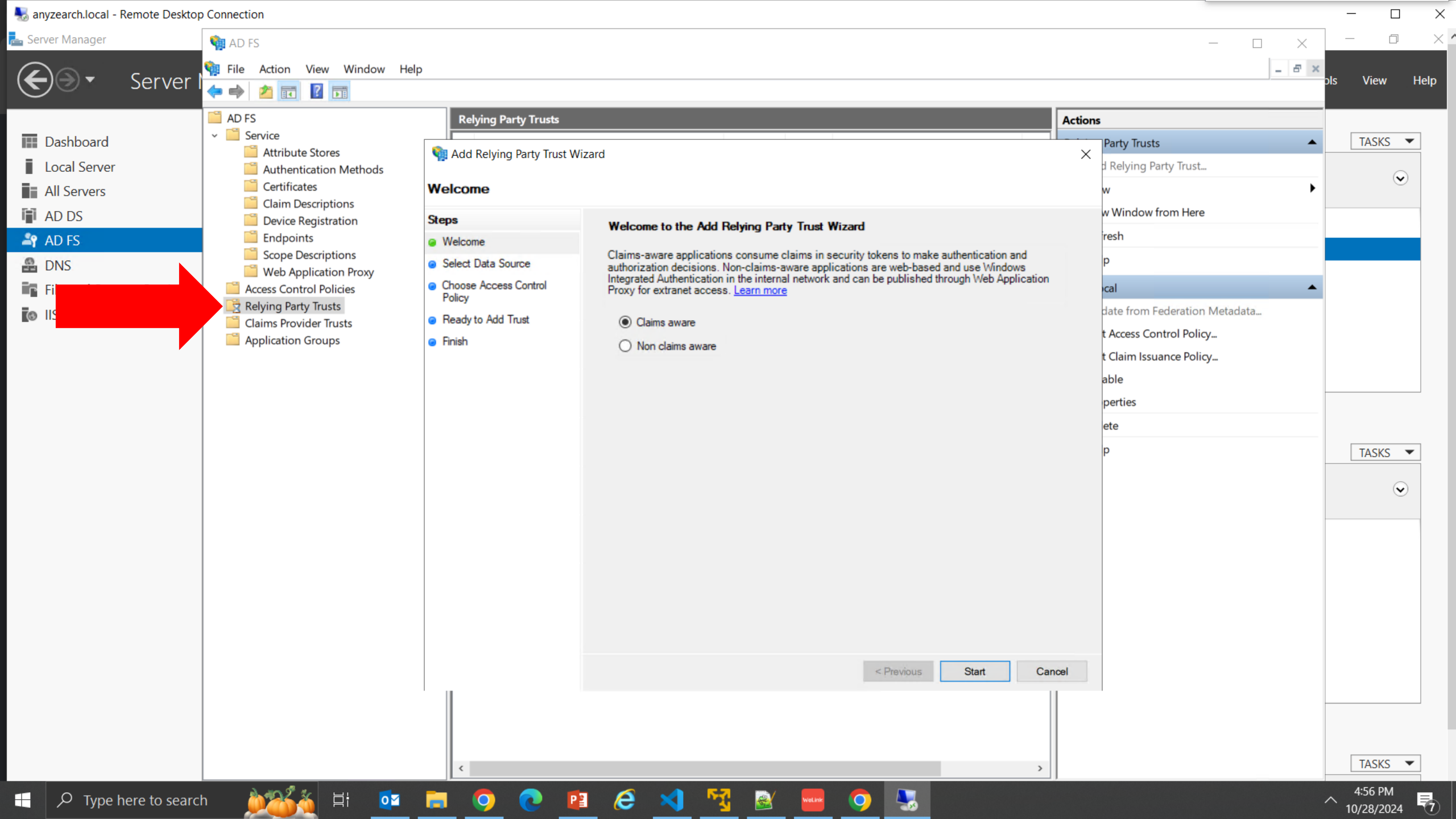
```
<EntityDescriptor entityID="win10.local" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            [redacted]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://win10.local:3001/adfs/auth/logout"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://win10.local:3001/adfs/auth/postResponse" index="0"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

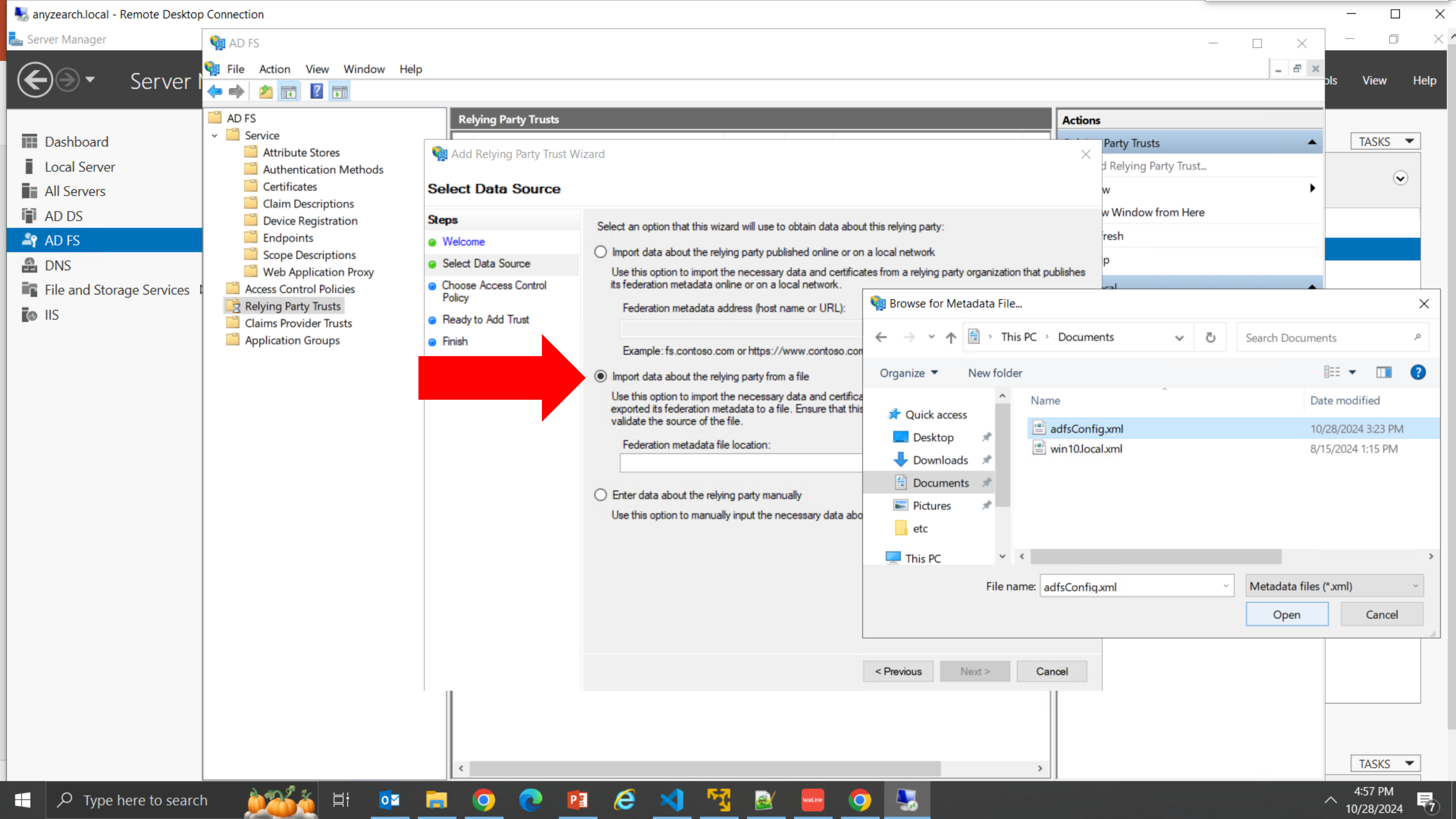
eXtensible Markup Language file | length : 1,788 lines : 30 | Ln : 7 Col : 13 Pos : 375 | Unix (LF) | UTF-8 | INS

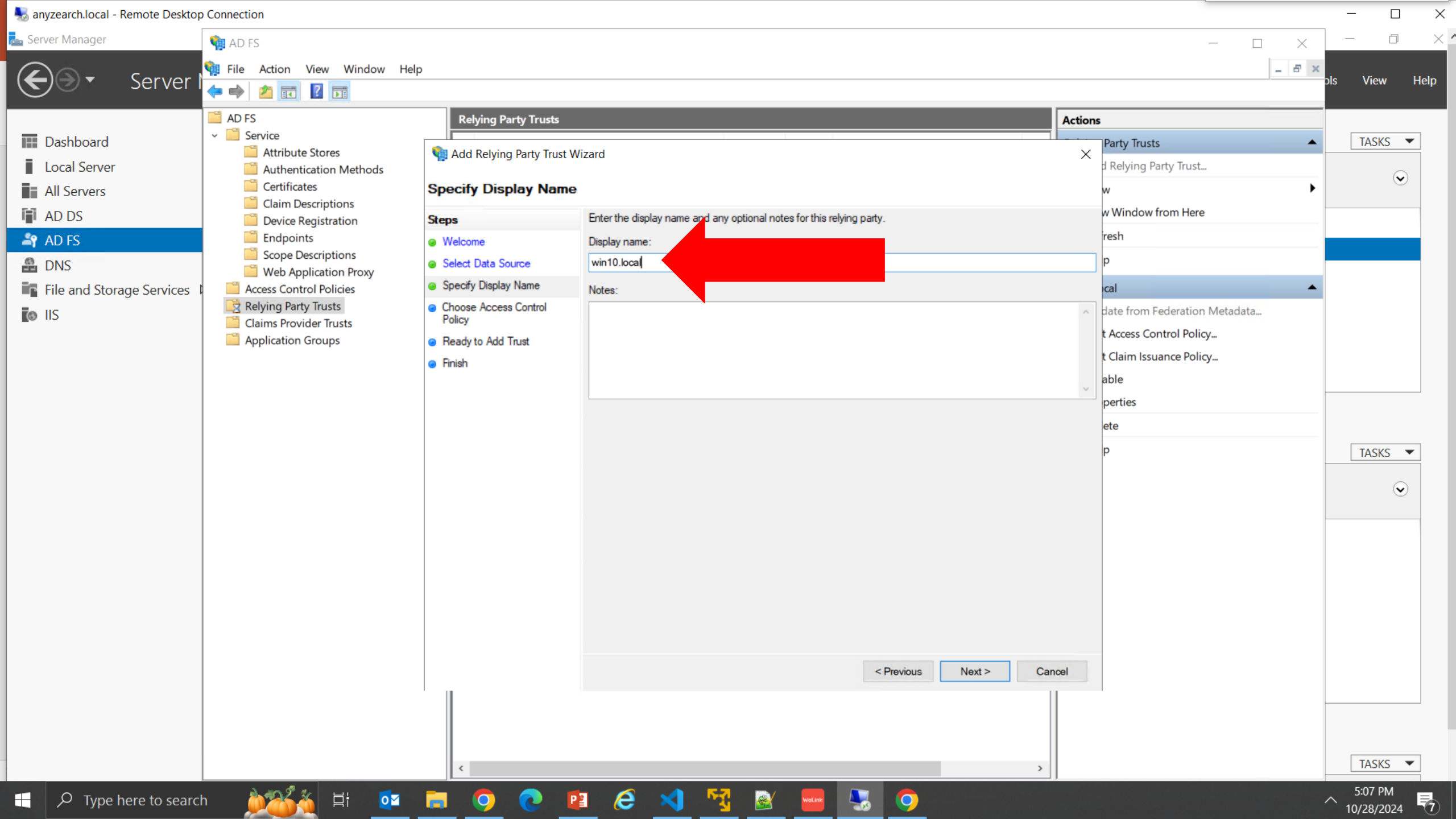
Type here to search

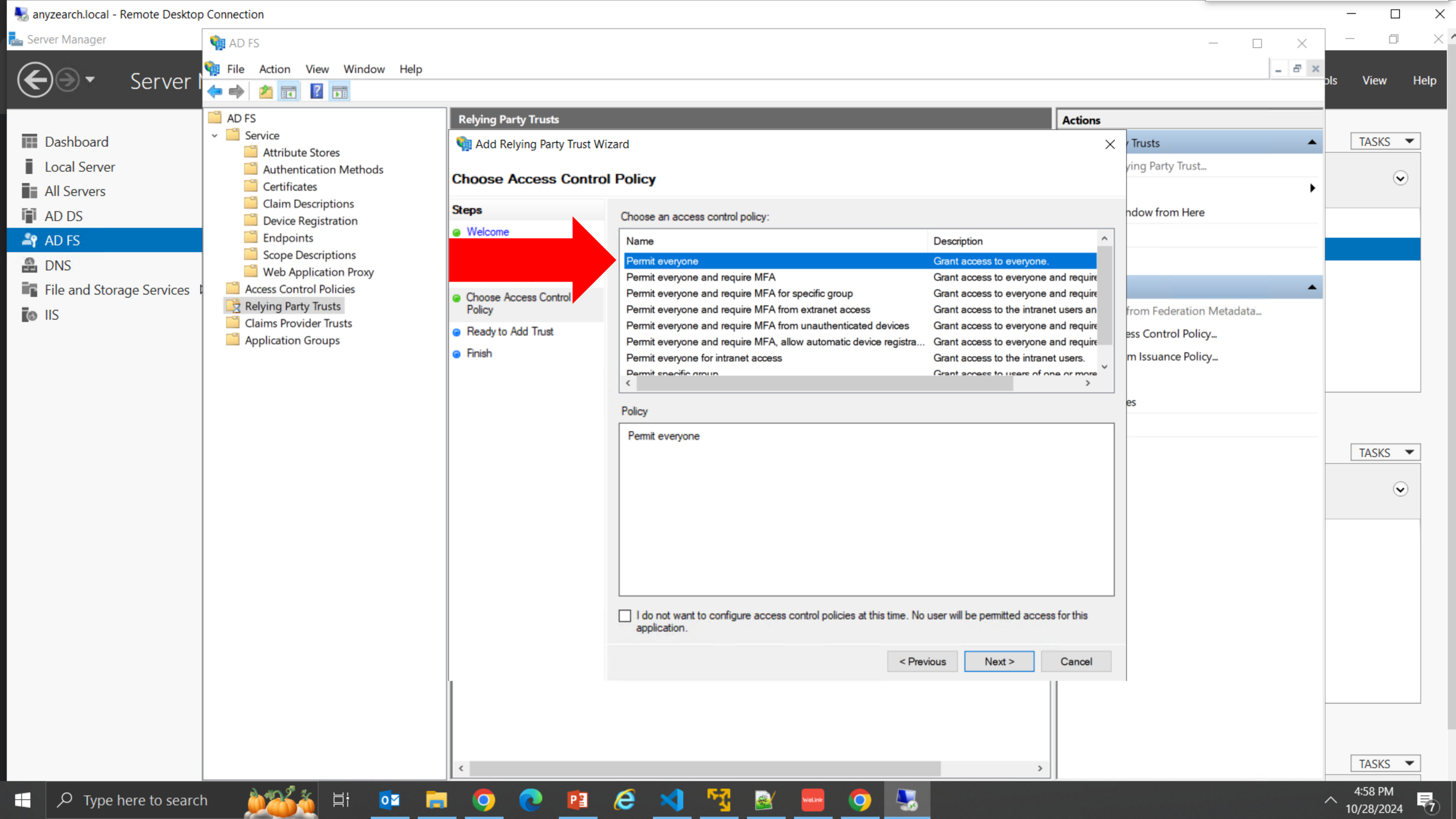
5:05 PM
10/28/2024

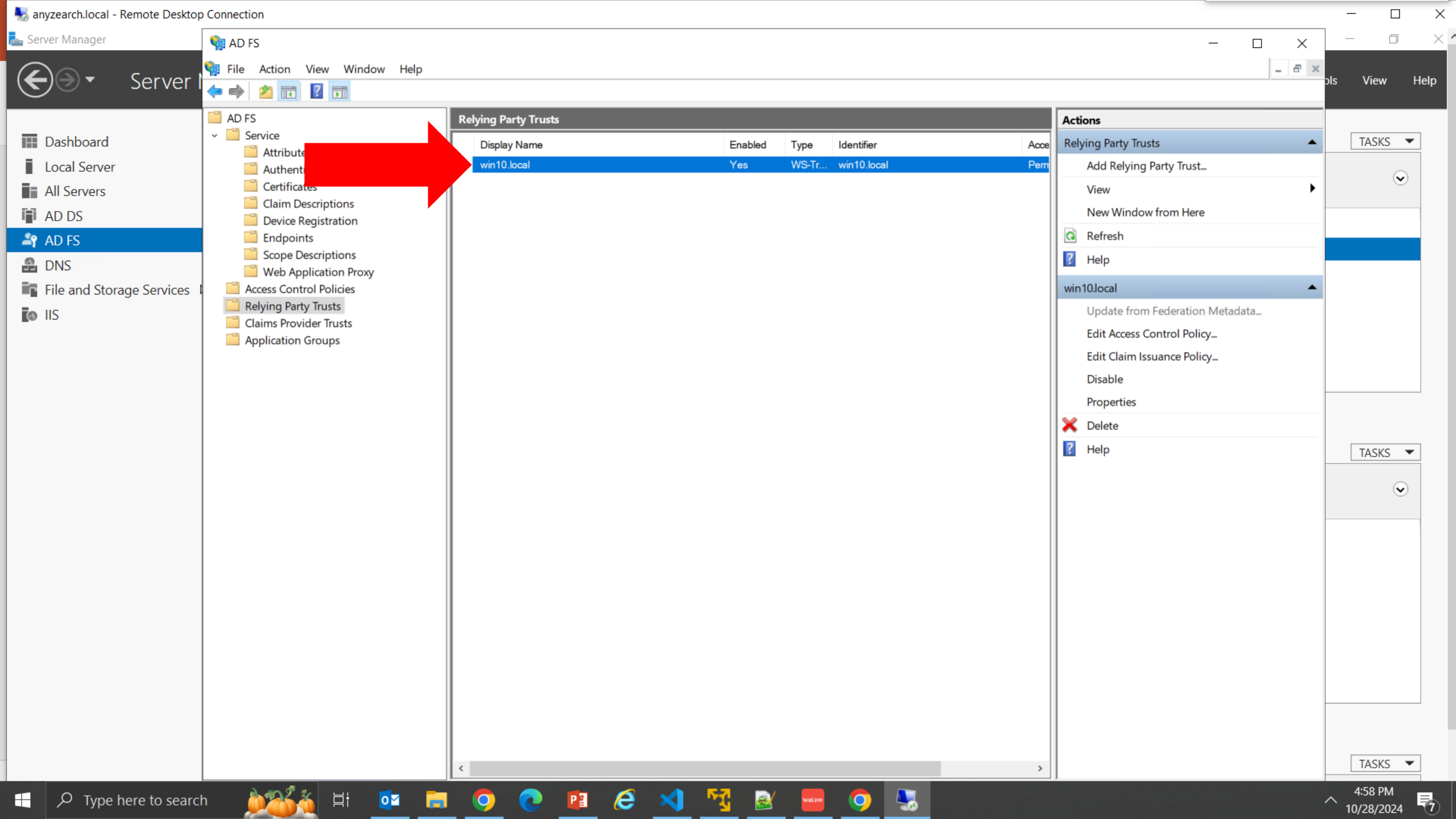

Server Manager
Server Manager ▸ AD FS
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
SERVERS
All servers | 1 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
WIN-E91JJT7KOBQ
192.168.175.142
Online - Performance counters not started
10/28/2024 4:52:41 PM
00454-40000-00001-AA675 (Activated)
EVENTS
All events | 4 total
Filter
Server Name
ID
Severity
Source
Log
Date and Time
WIN-E91JJT7KOBQ 161 Warning Device Registration Service DRS/Admin 10/28/2024 2:51:55 PM
WIN-E91JJT7KOBQ 137 Error Device Registration Service DRS/Admin 10/28/2024 2:21:55 PM
WIN-E91JJT7KOBQ 137 Error Device Registration Service DRS/Admin 10/28/2024 2:21:55 PM
WIN-E91JJT7KOBQ 278 Warning AD FS AD FS/Admin 10/28/2024 2:21:35 PM
SERVICES
All services | 1 total
Filter
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows Server Backup
Type here to search
4:55 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Server
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Actions
Party Trusts
Relying Party Trust...
w Window from Here
resh
p
cal
date from Federation Metadata...
t Access Control Policy...
t Claim Issuance Policy...
able
perties
ete
p
TASKS
Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
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
Type here to search
4:56 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Server
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Actions
Party Trusts
Relying Party Trust...
w Window from Here
resh
TASKS
Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
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
Import data about the relying party from a file
Use this option to import the necessary data and certifica
exported its federation metadata to a file. Ensure that this
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 abo
< Previous
Next >
Cancel
Browse for Metadata File...
This PC › Documents
Search Documents
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
etc
This PC
Name
Date modified
adfsConfig.xml
10/28/2024 3:23 PM
win10.local.xml
8/15/2024 1:15 PM
File name: adfsConfig.xml
Metadata files (*.xml)
Open
Cancel
Type here to search
4:57 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Server
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Actions
Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Choose Access Control Policy
Ready to Add Trust
Finish
Enter the display name and any optional notes for this relying party.
Display name:
win10.local
Notes:
< Previous
Next >
Cancel
TASKS
Type here to search
5:07 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Server
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Actions
Add Relying Party Trust Wizard
Choose Access Control Policy
Steps
Welcome
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
Permit everyone and require MFA for specific group
Grant access to everyone and require
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 require
Permit everyone and require MFA, allow automatic device registra...
Grant access to everyone and require
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
TASKS
Type here to search
4:58 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Server
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
AD FS
Service
Attribute
Authent
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Acce
win10.local
Yes
WS-Tr...
win10.local
Perm
Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
win10.local
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
TASKS
Type here to search
4:58 PM
10/28/2024

anyzearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

- AD FS
  - Service
    - Attribute Stores
    - Authentication Methods
    - Certificates
    - Claim Descriptio
    - Device Registrati
    - Endpoints
    - Scope Descriptions
    - Web Application Proxy
  - Access Control Policies
  - Relying Party Trusts
  - Claims Provider Trusts
  - Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Acce
win10.local	Yes	WS-Tr...	win10.local	Perm

Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help

Actions

Relying Party Trusts
- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

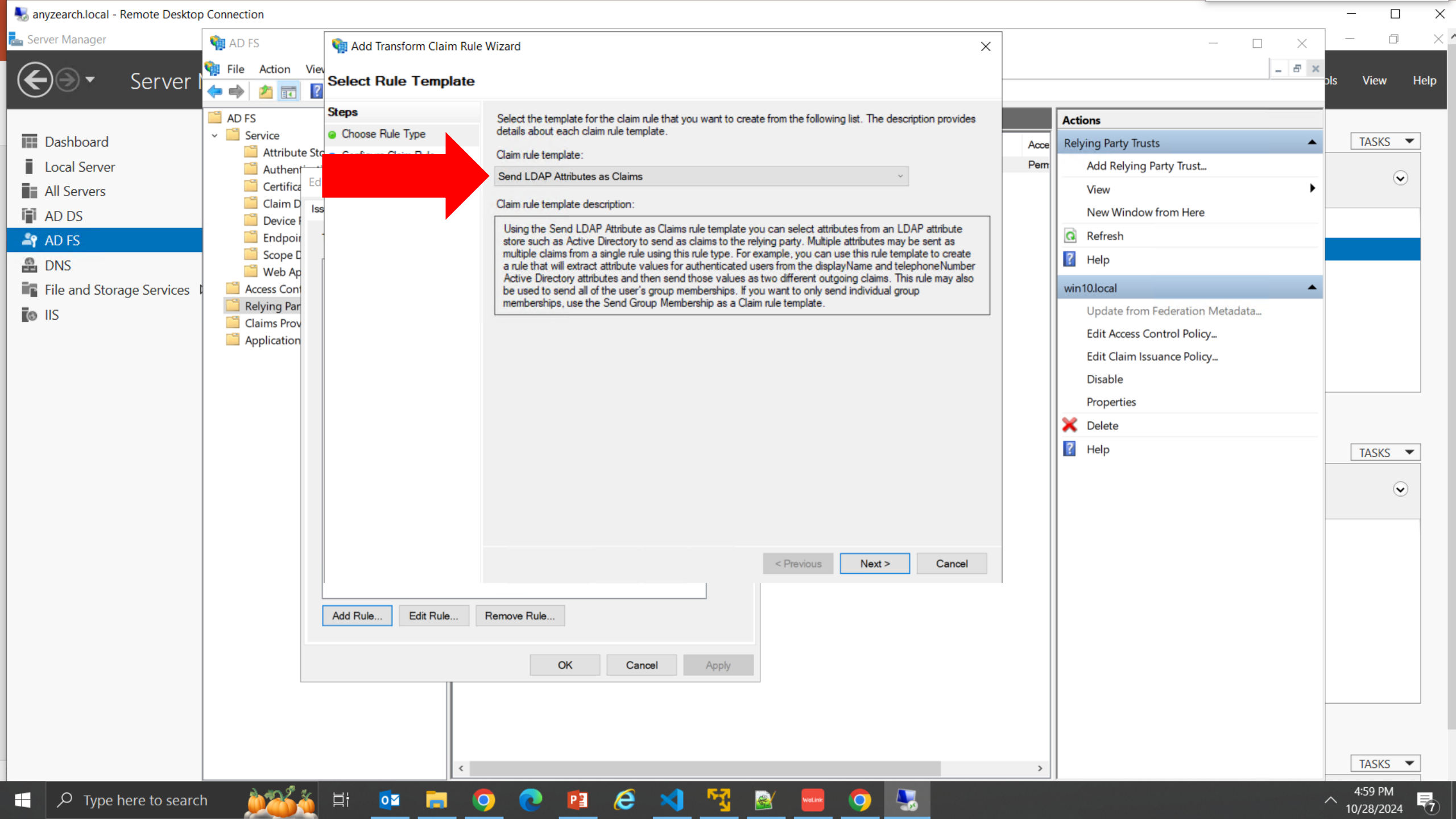
win10.local
- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...
- Disable
- Properties
- Delete
- Help

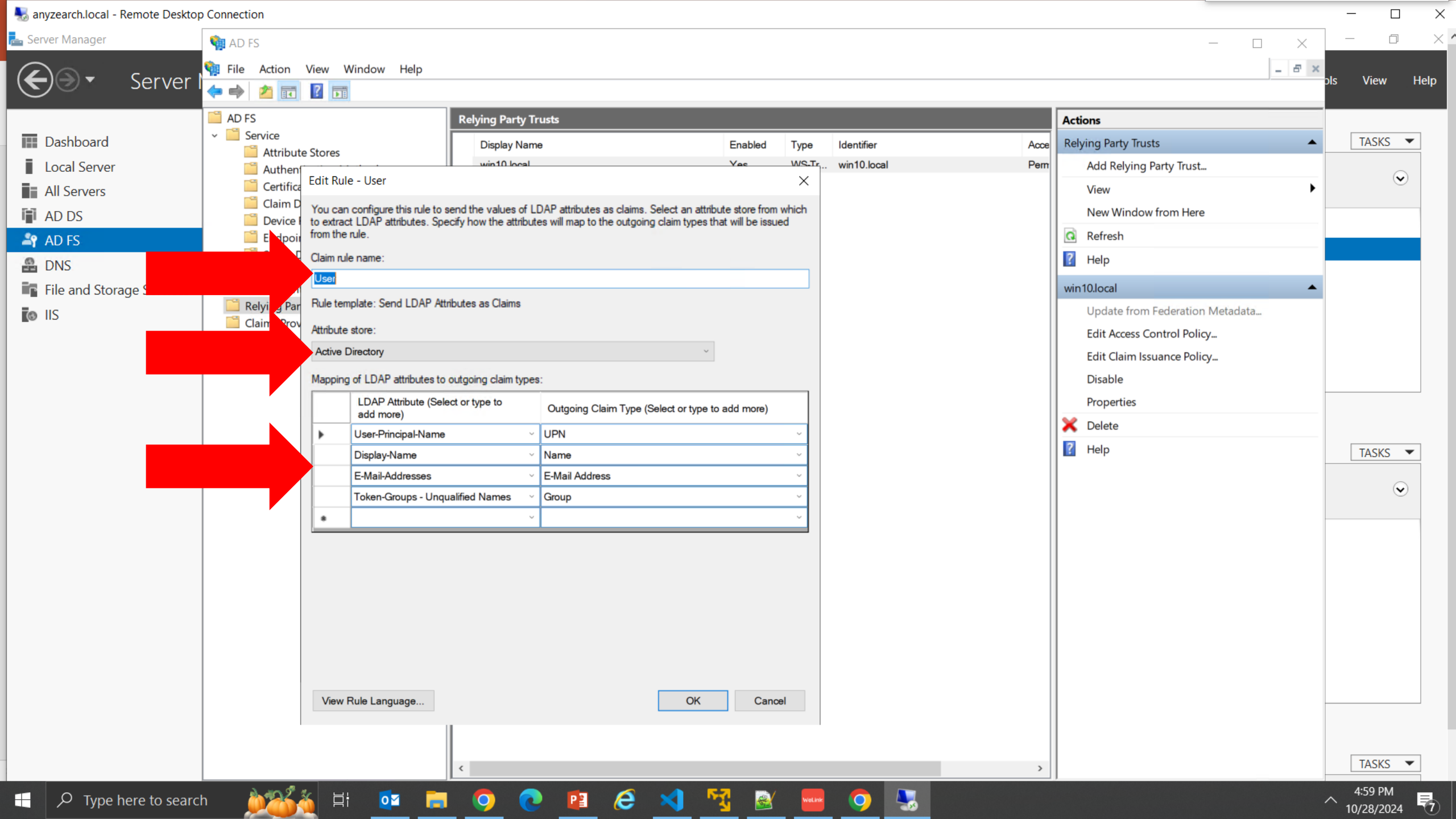
Server Manager
- Dashboard
- Local Server
- All Servers
- AD DS
- AD FS
- DNS
- File and Storage Services
- IIS

TASKS

Type here to search

4:59 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
AD FS
File Action View
AD FS
Service
Relying Party Trusts
Claims Provider Trusts
Application Groups
Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
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
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
win10.local
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
TASKS
Type here to search
4:59 PM
10/28/2024


anyzearch.local - Remote Desktop Connection
Server Manager
AD FS
File Action View Window Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage S
IIS
AD FS
Service
Attribute Stores
Relying Party Trusts
Display Name
Enabled
Type
Identifier
win10.local
Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
win10.local
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
TASKS
Edit Rule - User
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:
User
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)
User-Principal-Name
UPN
Display-Name
Name
E-Mail-Addresses
E-Mail Address
Token-Groups - Unqualified Names
Group
View Rule Language...
OK
Cancel
Type here to search
4:59 PM
10/28/2024