SharePoint Federation and Extranet Workshop
Unit 5
SharePoint On Premises

Presented by Peter Carson
President, Envision IT

June 18, 2014

envision IT
Leaders in SharePoint Solutions

Agenda

Morning Session

- Unit 0 – Introductions
- Unit 1 – Federation
- Unit 2 – Reference Scenarios
- Unit 3 – Customer Case Studies

Afternoon Session

- Unit 4 - Office 365
- Unit 5 – SharePoint On Premises
- Unit 6 – Open Discussion

SharePoint On Premise Authentication Options

Windows Authentication

Active Directory

Windows Claims
Or
Classic Mode

Forms-Based Authentication

.NET Providers

AD

SQL

Claims

Federated Identity

Relying Party

Trusted Identity Provider

AD

User Store

Claims

Trusted Identity Providers

- Active Directory Federation Services (AD FS)
- Thinktecture Identity Server
- Social Identities
  - Facebook
  - Linkedin
  - Microsoft Account
  - Google+

Authentication Providers

BROWSE | WEB APPLICATIONS | SHARE

New | Extend | Delete | General Settings | Manage Features | Managed Paths | Service Connections | Authentication Providers | Self-Service Site Creation | Blocked File Types | User Permissions | Web Part Security | User Policy | Anonymous Policy | Permission Policy

Contribute | Manage | Security | Policy

Central Administration
- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Apps
- Configuration Wizards

Name	URL	Port
SharePoint - thinktecturedev.eitdev.org443	https://thinktecturedev.eitdev.org/	443
SharePoint Central Administration v4	https://thinktecturedev:19000/	19000

Edit Authentication

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

- [x] Enable Windows Authentication
  - [x] Integrated Windows authentication
    - NTLM
  - [ ] Basic authentication (credentials are sent in clear text)
- [ ] Enable Forms Based Authentication (FBA)
  - ASP.NET Membership provider name
  - ASP.NET Role manager name
- [x] Trusted Identity provider
  - Trusted Identity Provider
    - [x] Thinktecture IP-STS

SharePoint Infrastructure

- SharePoint Farm (one or more servers)
  - Web Application
    - Site Collection
      - Subsites
        - Lists and Libraries
  - Application Pools
  - IIS Sites
  - Content Databases

Web Application Zones

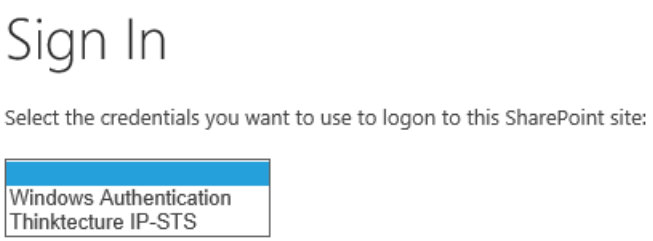
- Authentication methods are defined for each zone of a web application
- Each web app can have up to five zones
  - Default
  - Intranet
  - Extranet
  - Internet
  - Custom
- Multiple authentication methods can be applied to a single zone

When to Use Zones

- In general we recommend not to use multiple zones
- Everyone (internal and external users) should share a single https url (https://portal.contoso.com)
- Confusion results otherwise
  - Emailed links are broken for some of your users
  - Workflows, tasks, and alerts point to the wrong URL (unless you are in the Default zone)
- The only exception is where you also need an anonymous http zone
  - Mixed public and private sites
  - This is the only scenario that Microsoft recommends
  - Secure https zone should always be the default zone

Authentication Chooser

- Users decides what method to use to authenticate
- Goal should be to hide this from the user
  - Use the IP address
  - Check the email domain of the login email address



AD FS and SharePoint On Premises

AD FS and SharePoint On Premises

- Same AD FS infrastructure is needed as Office 365
- Complete the AD FS Configuration Checklist
  - http://blog.petercarson.ca/Documents/ADFS Configuration Checklist.zip
- Export the token signing certificate
- Setup the Relying Party (SharePoint) in AD FS
- Run the PowerShell to configure SharePoint to trust AD FS as an identity provider
- Select the Trusted Identity Provider in Central Admin
- http://technet.microsoft.com/en-us/library/hh305235(v=office.15).aspx#Phase2

AD FS Configuration Checklist

Relying Party Definition	
Item	**Value**
Display Name	Extranet
URL	https://adfsportal.eitdev.org/_trust/
Identifier	extranet
Full Identifier	urn:extranet:sharepoint
Claim Rule	
LDAP Attribute	**Outgoing Claim Type**
E-Mail Addresses	E-Mail Address
Token Groups - Unqualified Names	Role
SharePoint Trusted Identity Provider	
Token Issuer	ADFS LAB LOCAL
Certificate File	C:\Install\ADFS\adfs.cer
Certificate Name	Token Signing Cert Lab Local
Realm	urn:extranet:sharepoint
Description	SharePoint secured by SAML (ADFS) Lab Local
ADFS Signin URL	https://adfs.eitdev.org/adfs/ls

Token Signing Certificate

AD FS

File Action View Window Help

- AD FS
  - Service
    - Endpoints
    - Certificates
    - Claim Descriptions
  - Trust Relationships
    - Claims Provider Trusts
    - Relying Party Trusts
    - Attribute Stores

Certificates

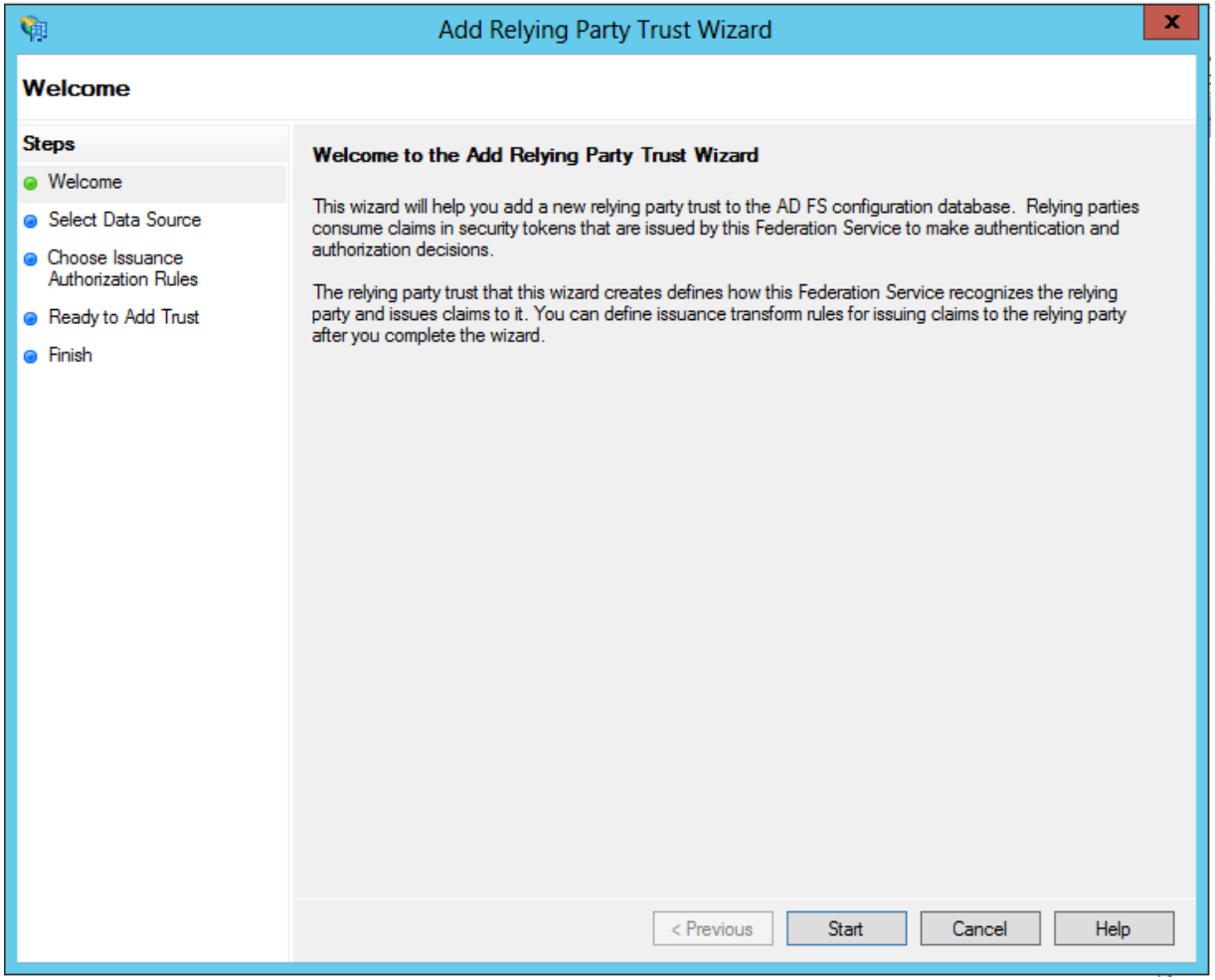
Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=*.eitdev.org, OU=Domain Control Validated	SERIALNUMBER=07969...	2/2/2014	2/2/2015		
Token-decrypting					
CN=ADFS Encryption - adfs.eitdev.org	CN=ADFS Encryption - ad...	5/14/2014	5/14/2015		Primary
Token-signing					
CN=ADFS Signing - adfs.eitdev.org	CN=ADFS Signing - adfs....	5/14/2014	5/14/2015		Primary

Actions

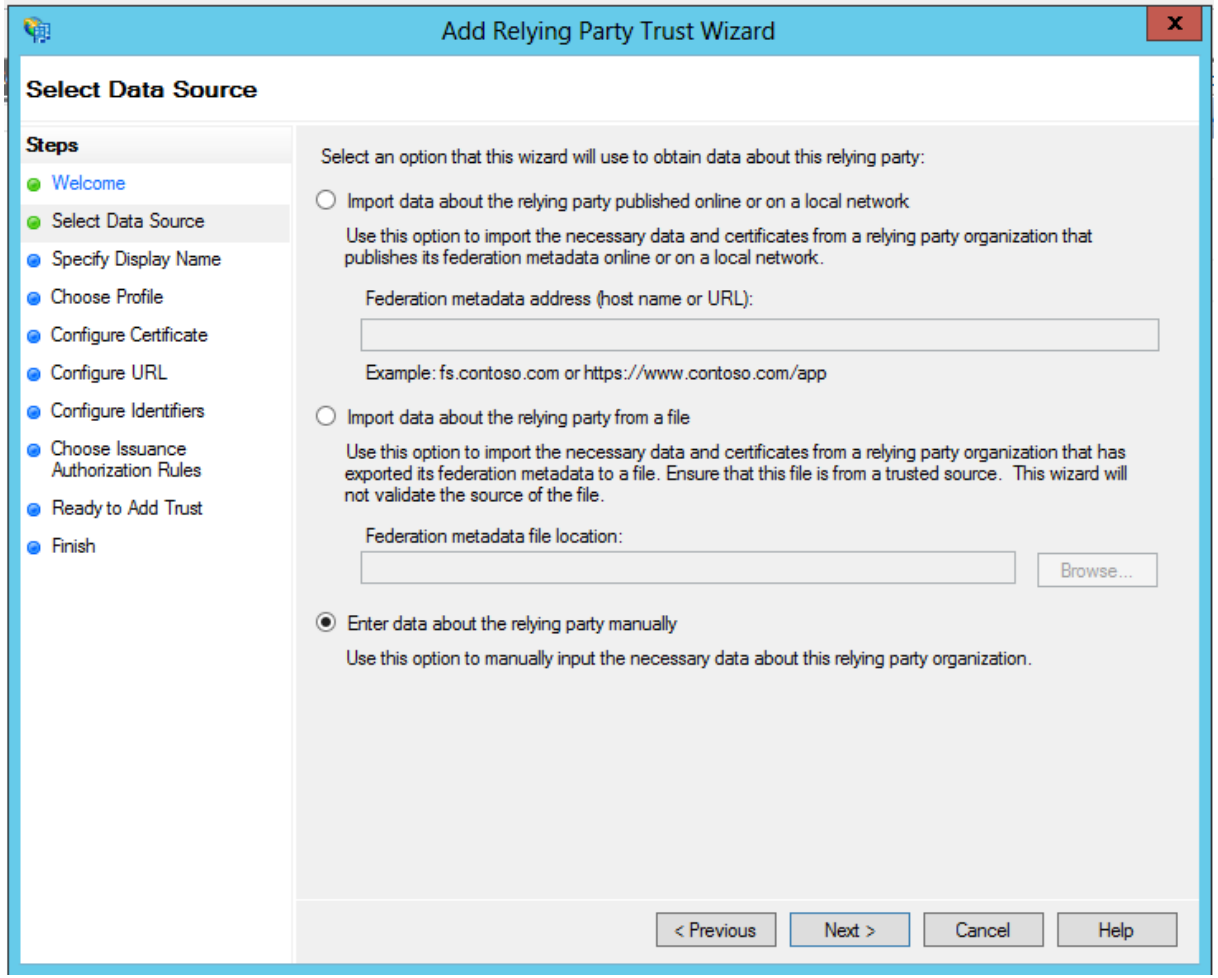
Certificates
- Add Token-Signing Certificate...
- Add Token-Decrypting Certificate...
- Set Service Communications Certific...
- View
- New Window from Here
- Refresh
- Help

CN=ADFS Encryption - adfs.eitde...
- View Certificate...
- Set as Primary
- Help

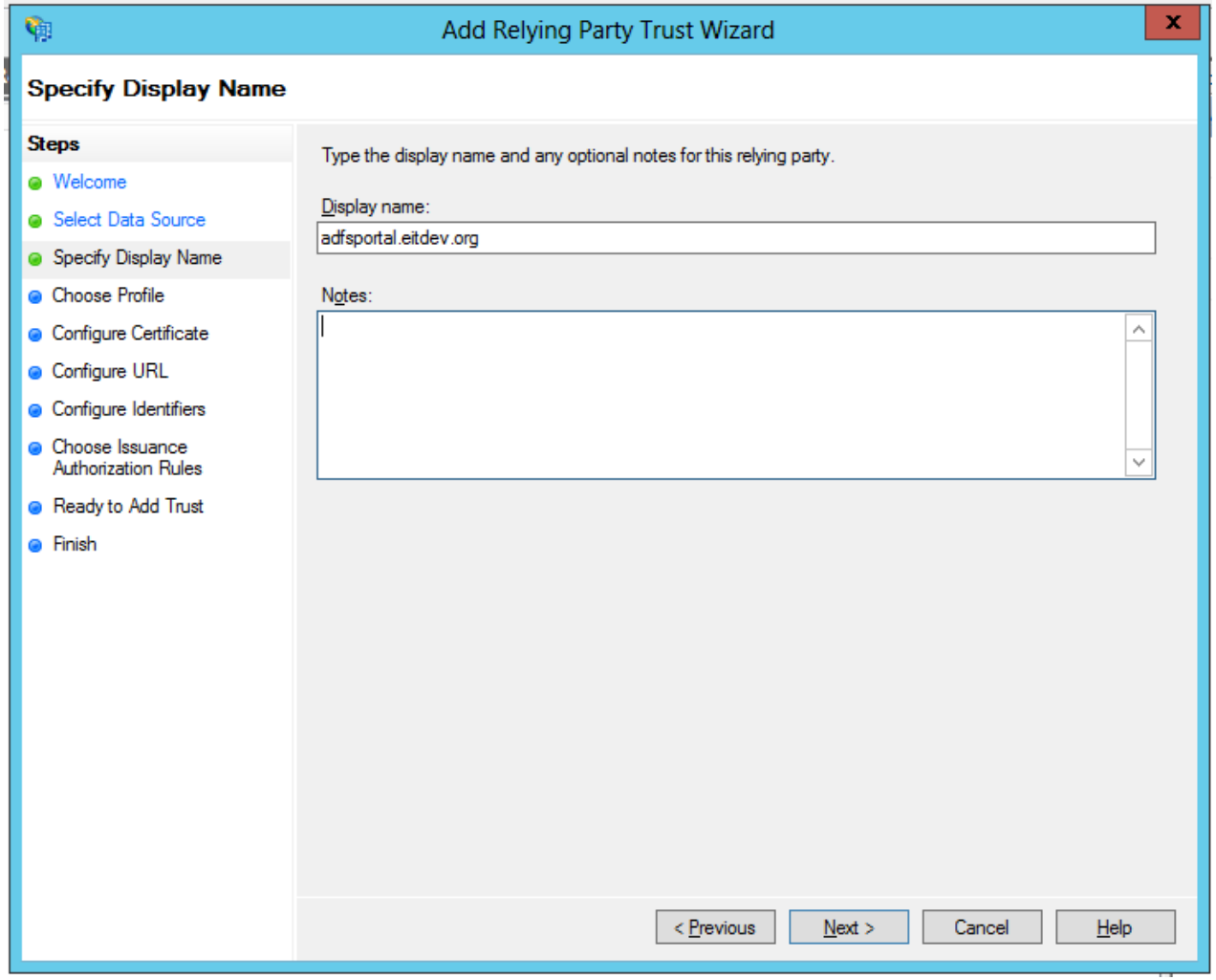
Relying Party Trust



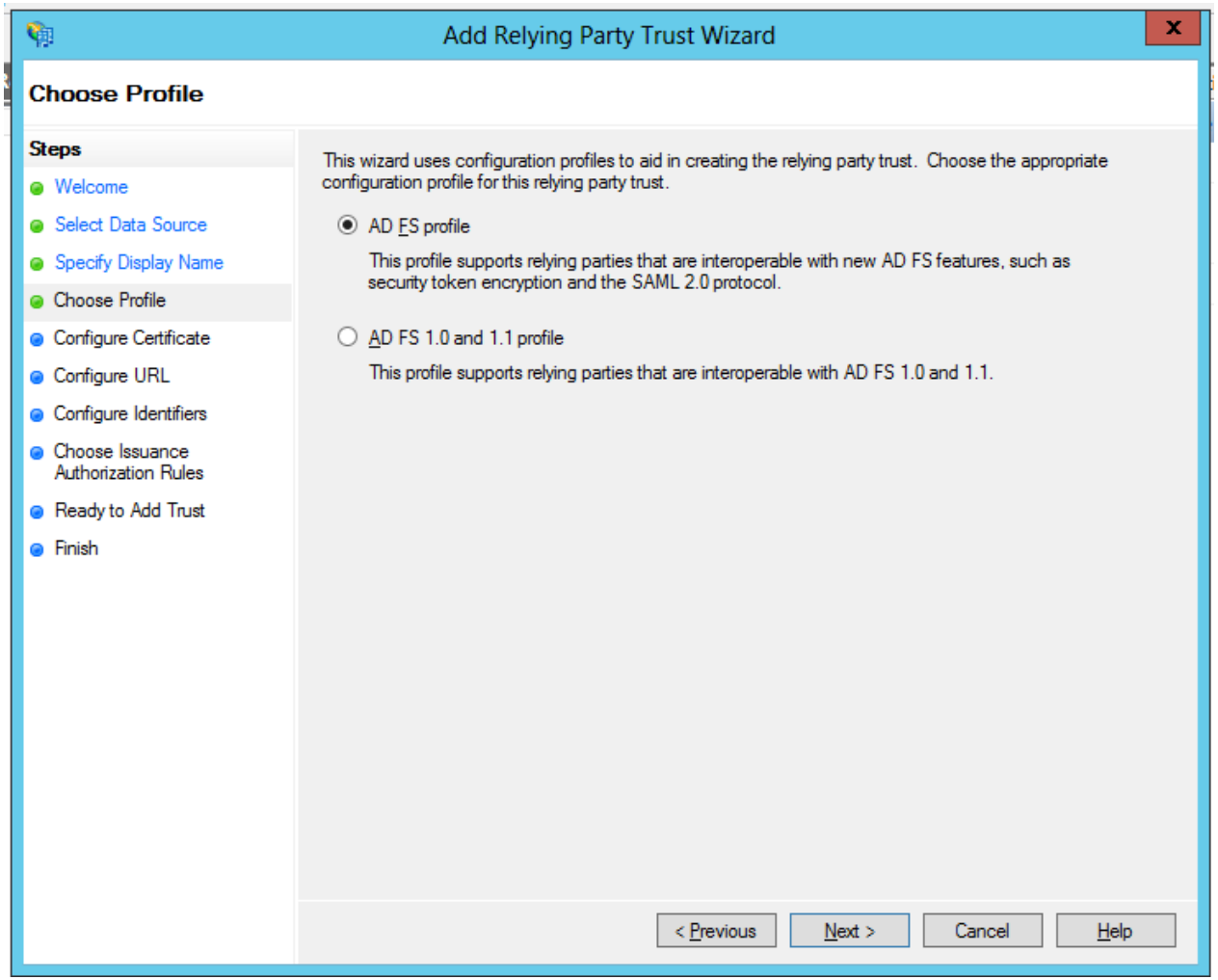
Relying Party Trust



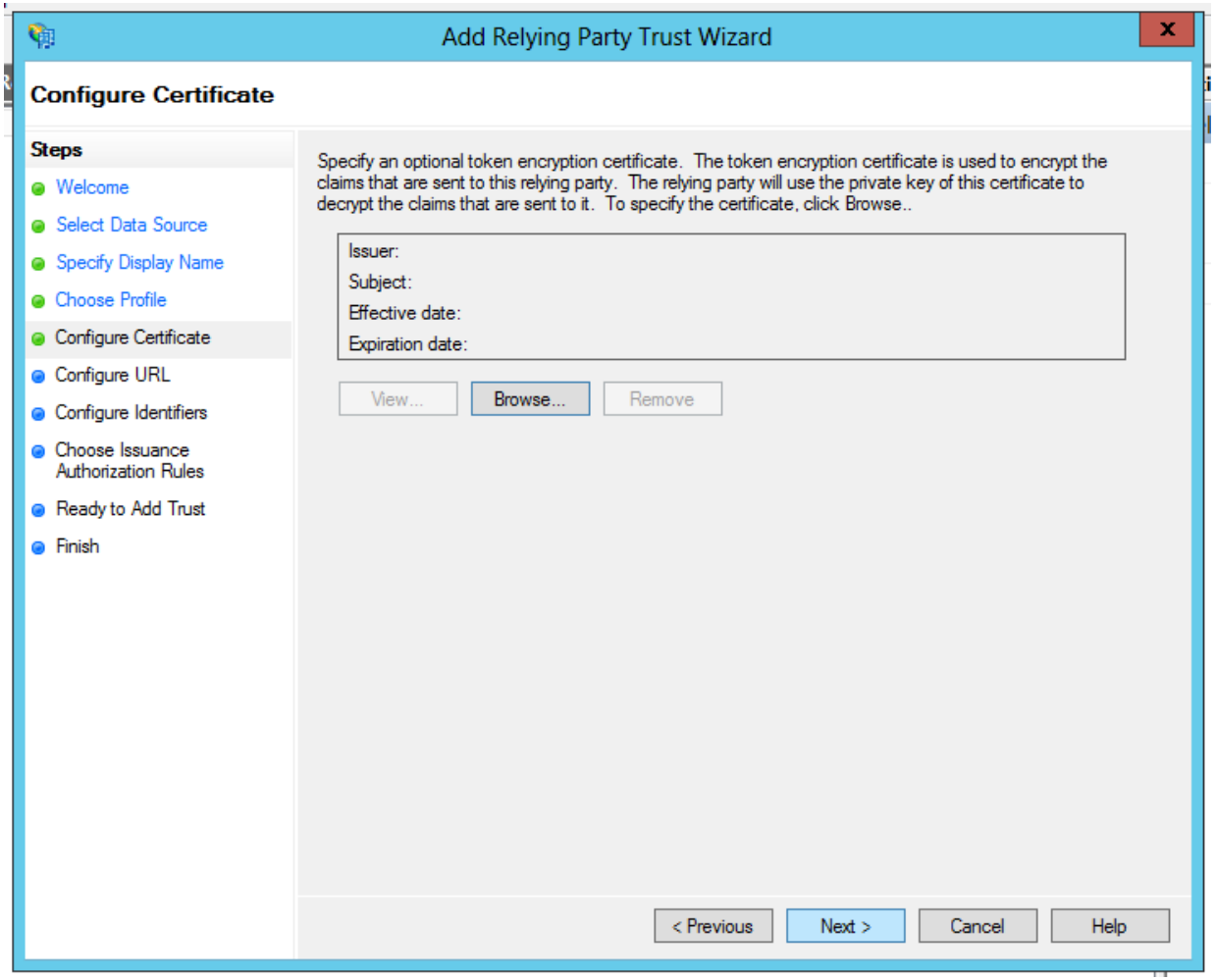
Relying Party Trust



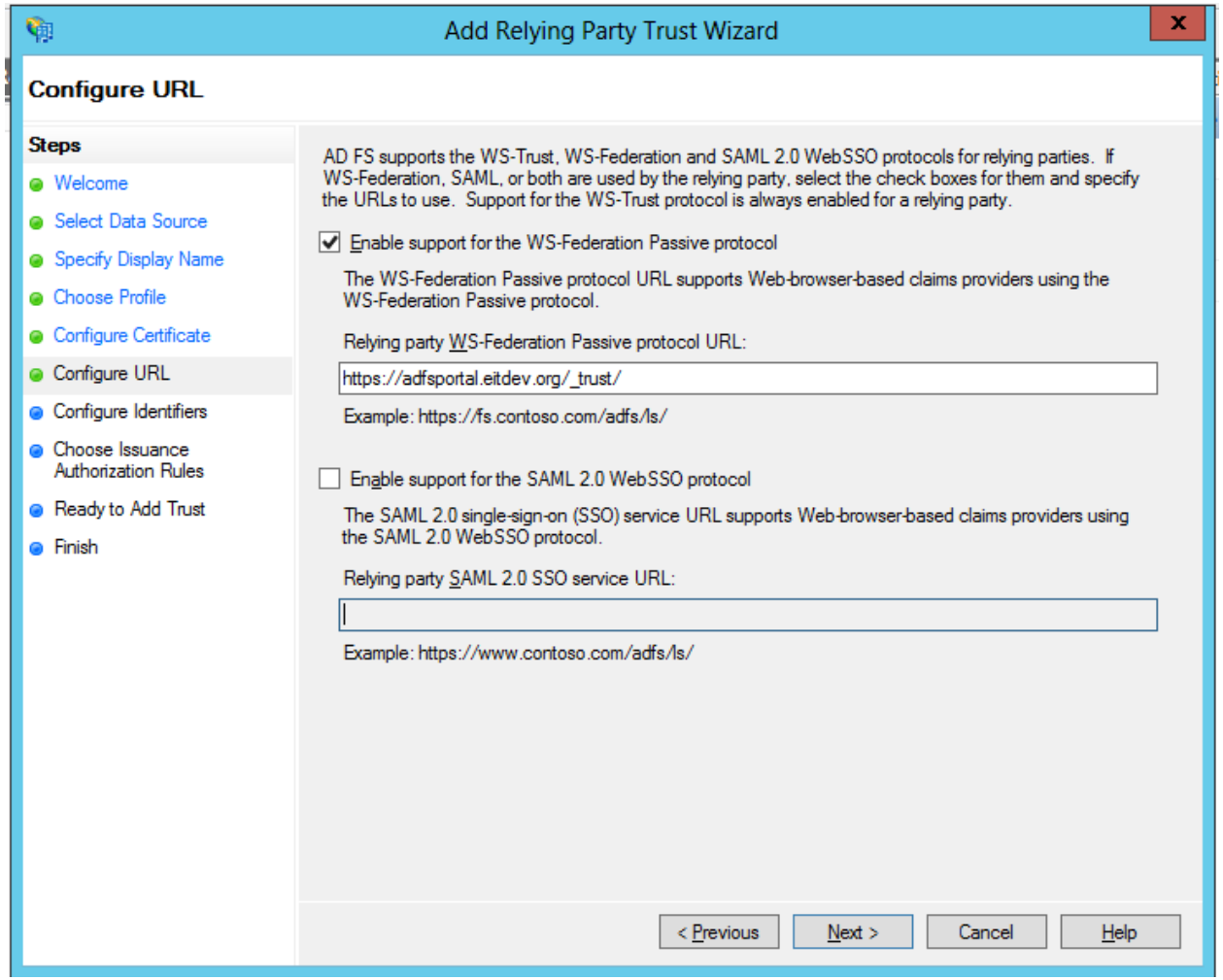
Relying Party Trust



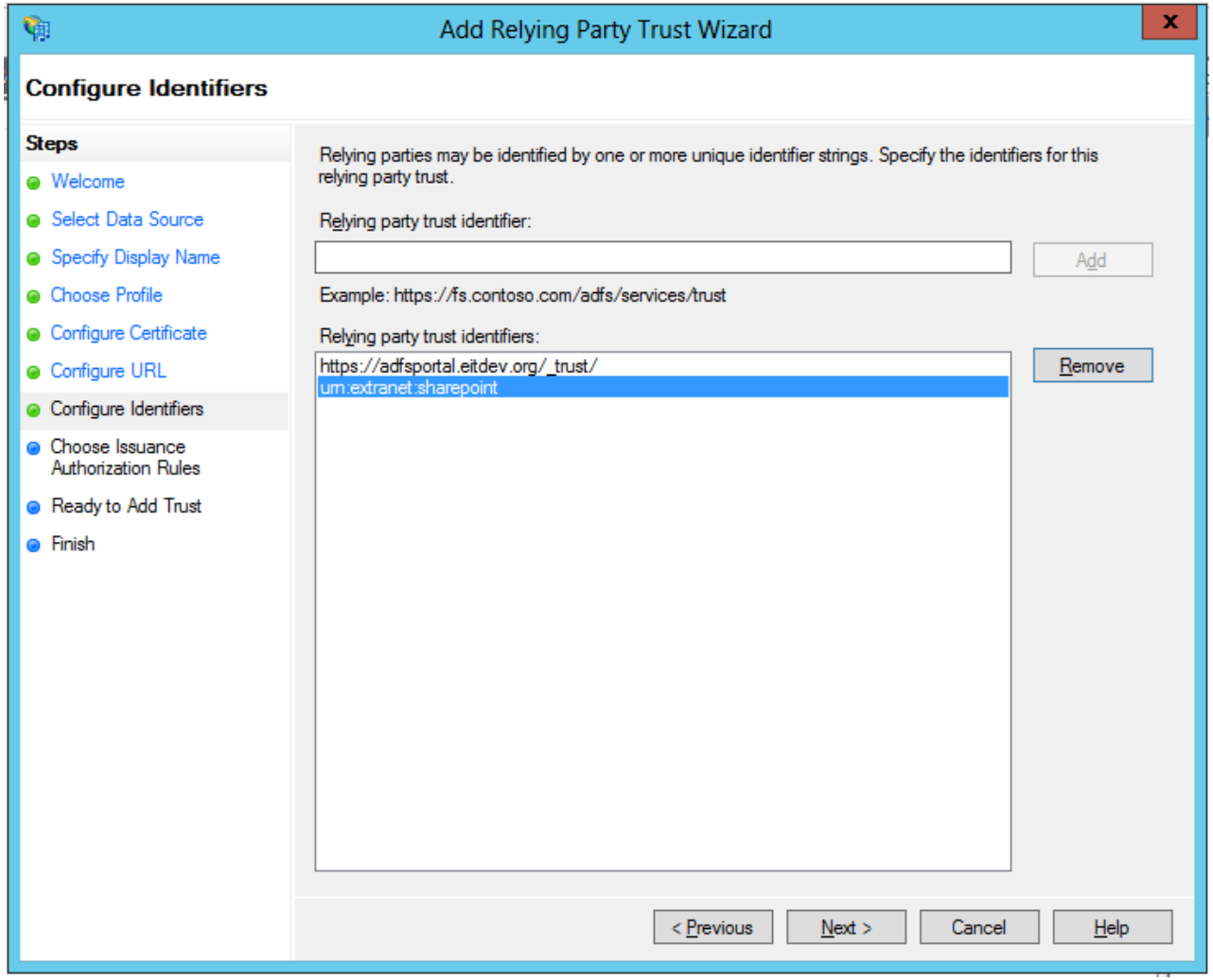
Relying Party Trust



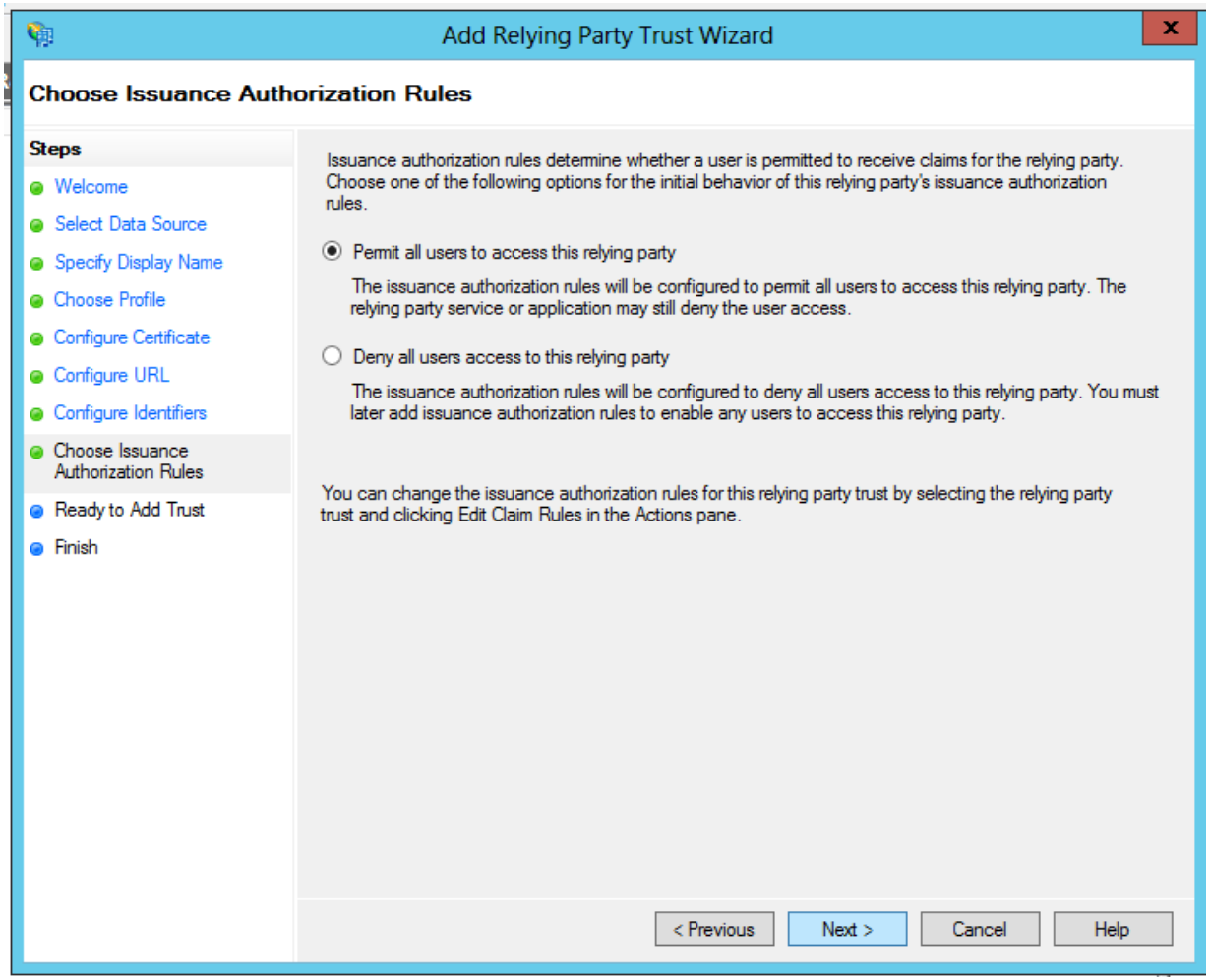
Relying Party Trust



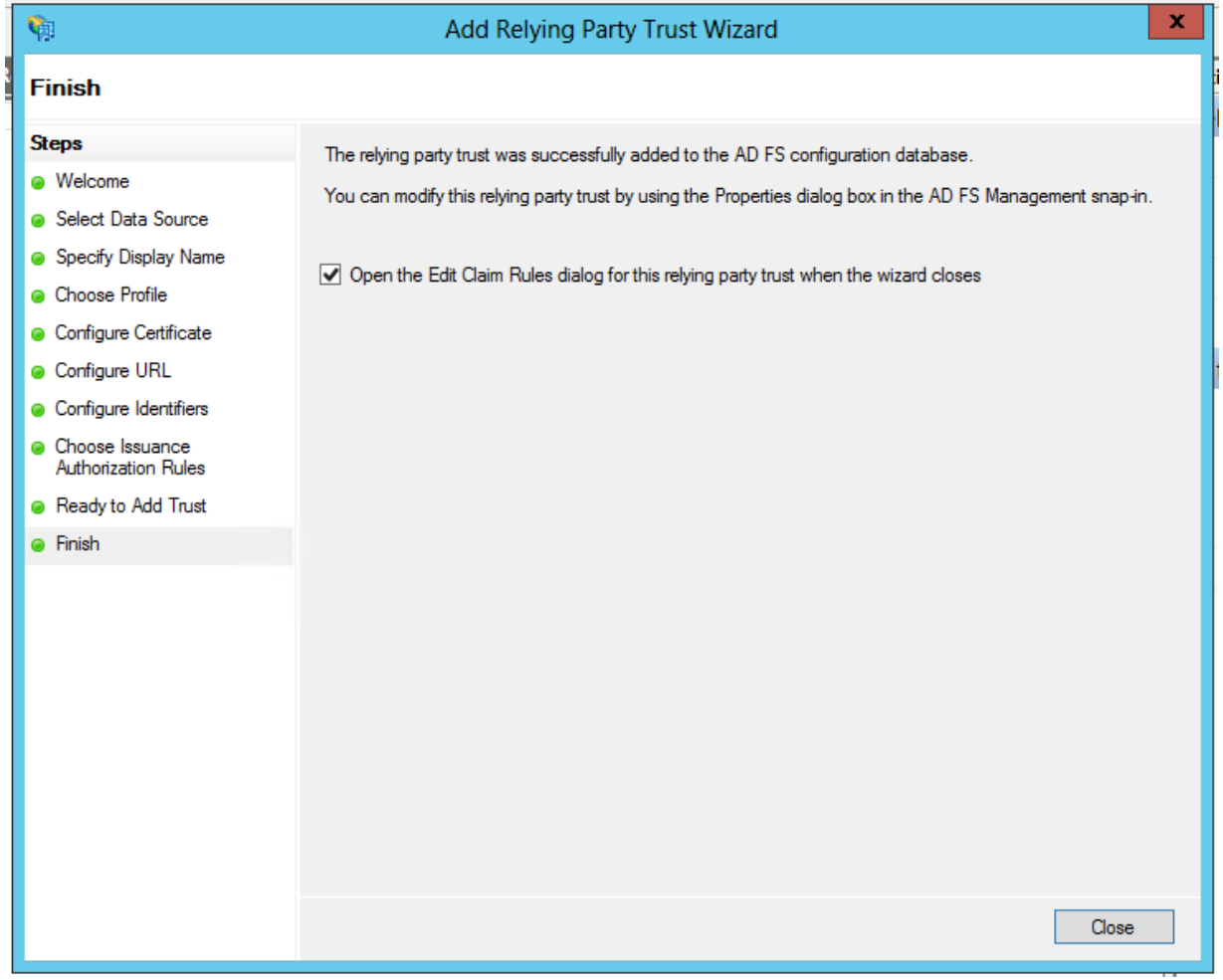
Relying Party Trust



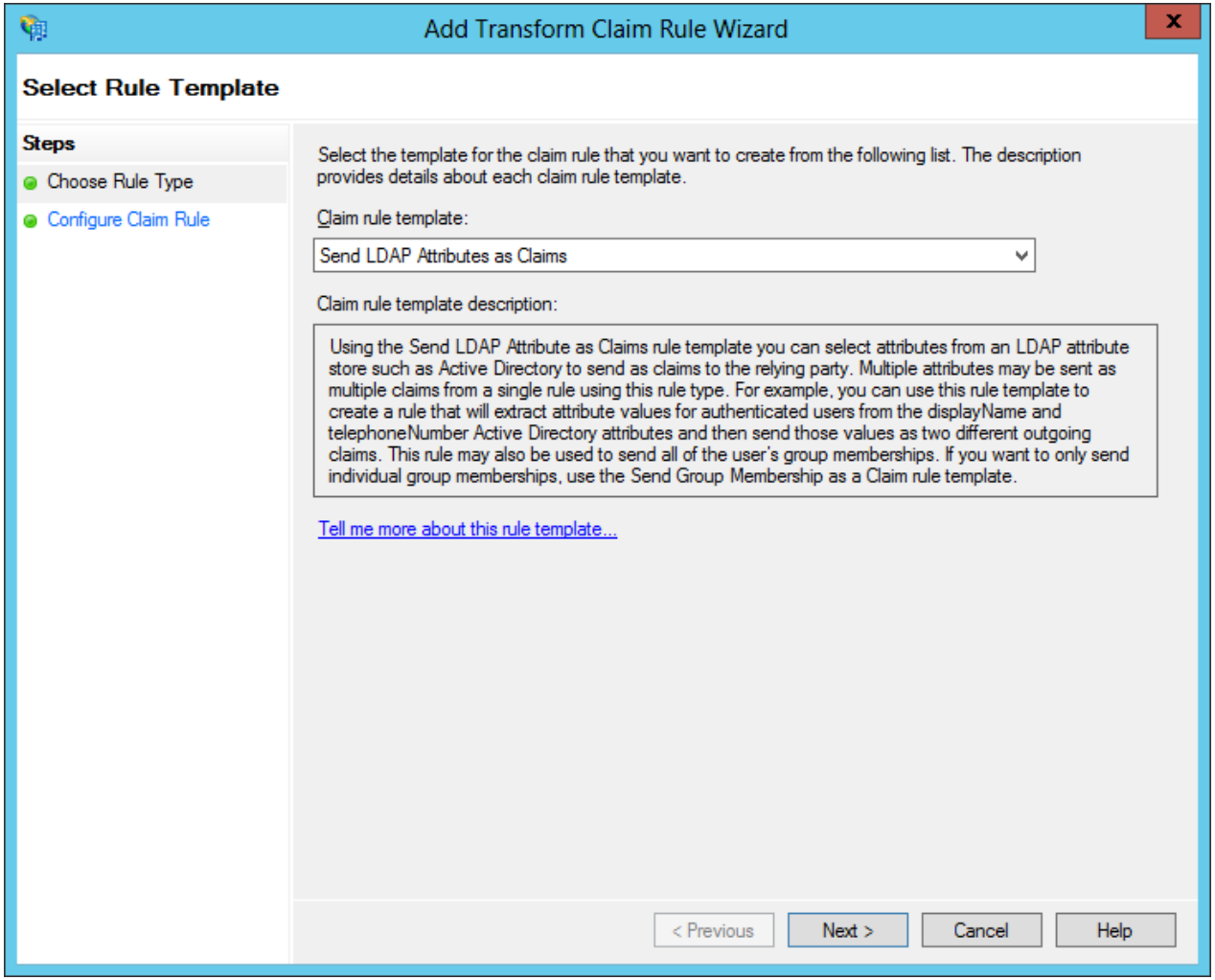
Relying Party Trust



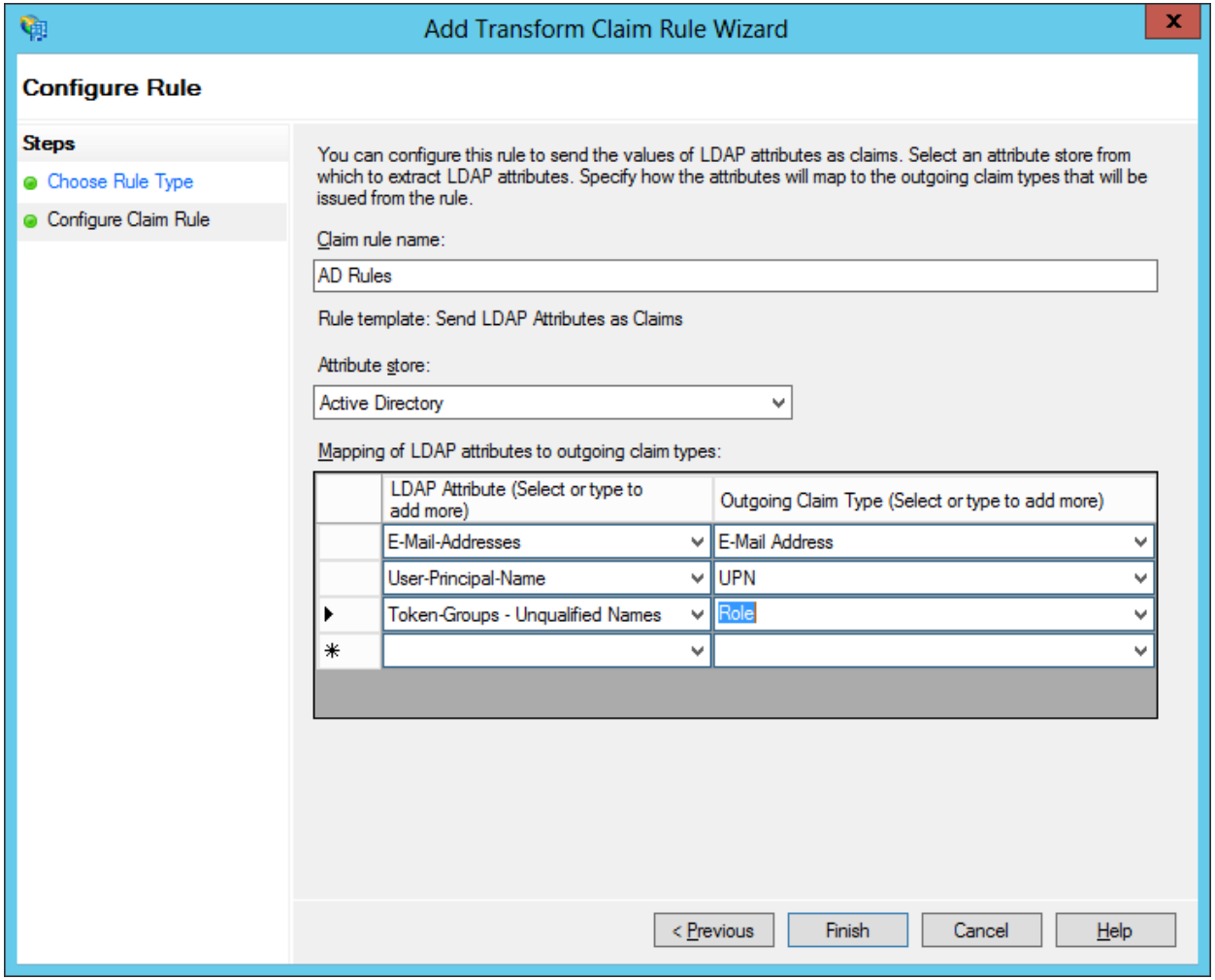
Relying Party Trust



Relying Party Trust



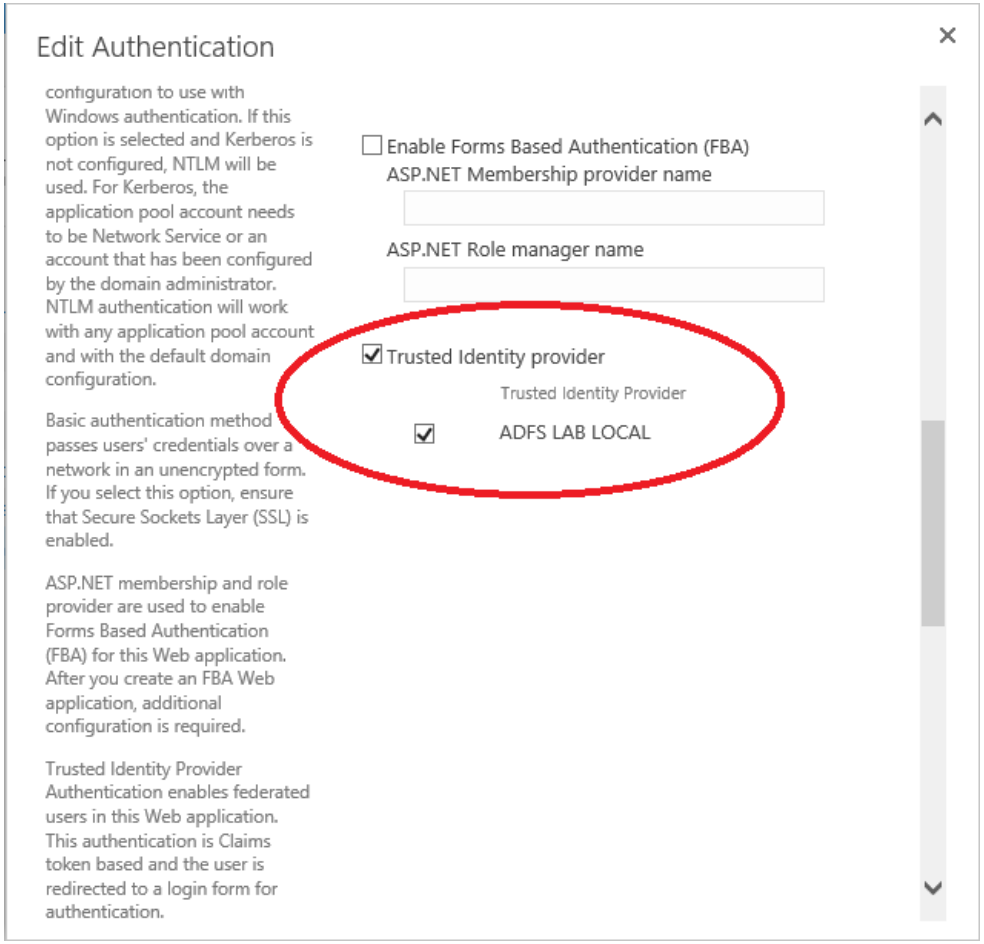
Relying Party Trust



PowerShell to Configure SharePoint

```
$TokenIssuer = "ADFS LAB LOCAL"
$CertFile = "C:\Install\ADFS\adfs.cer"
$CertName = "Token Signing Cert Lab Local"
$realm = "urn:extranet:sharepoint"
$descript = "SharePoint secured by SAML (ADFS) Lab Local"
$ADFSSigninURL = "https://adfs.eitdev.org/adfs/ls"

if ($args[0] -eq "-Install")
{
   Write-host "INSTALL Certificate - $CertName"
   $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2($CertFile)
   New-SPTrustedRootAuthority -Name $CertName -Certificate $cert

   Write-host "INSTALL Token Issuer - $TokenIssuer"
   $map = New-SPClaimTypeMapping   -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -
SameAsIncoming;
   $map2 = New-SPClaimTypeMapping  -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role"
-IncomingClaimTypeDisplayName "Role" -SameAsIncoming;

   $ap = New-SPTrustedIdentityTokenIssuer -Name $TokenIssuer -Description $descript  -realm $realm   -
ImportTrustCertificate $cert   -ClaimsMappings $map,$map2 -SignInUrl $ADFSSigninURL   -IdentifierClaim
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress";
}
elseif ($args[0] -eq "-Uninstall")
{
    Write-host "UnINSTALL $TokenIssuer and $CertName"

    Remove-SPTrustedIdentitytokenissuer $TokenIssuer
    Remove-SPTrustedRootAuthority -Identity $CertName
```

Select the Trusted Identity Provider



EUM and SharePoint

EUM and SharePoint

- Full details in the Deployment and Configuration Guide
- High-level steps
  - Create an IIS site to install into
  - Run the installer
  - Configure the Extranet Identity Server
  - Complete the EUM configuration
  - Add SharePoint as a Relying Party
  - Integrate AD FS as an Identity Provider
  - Configure other Relying Parties