

ADFS Integration for Silent Circle Enterprise Customers

System Requirements

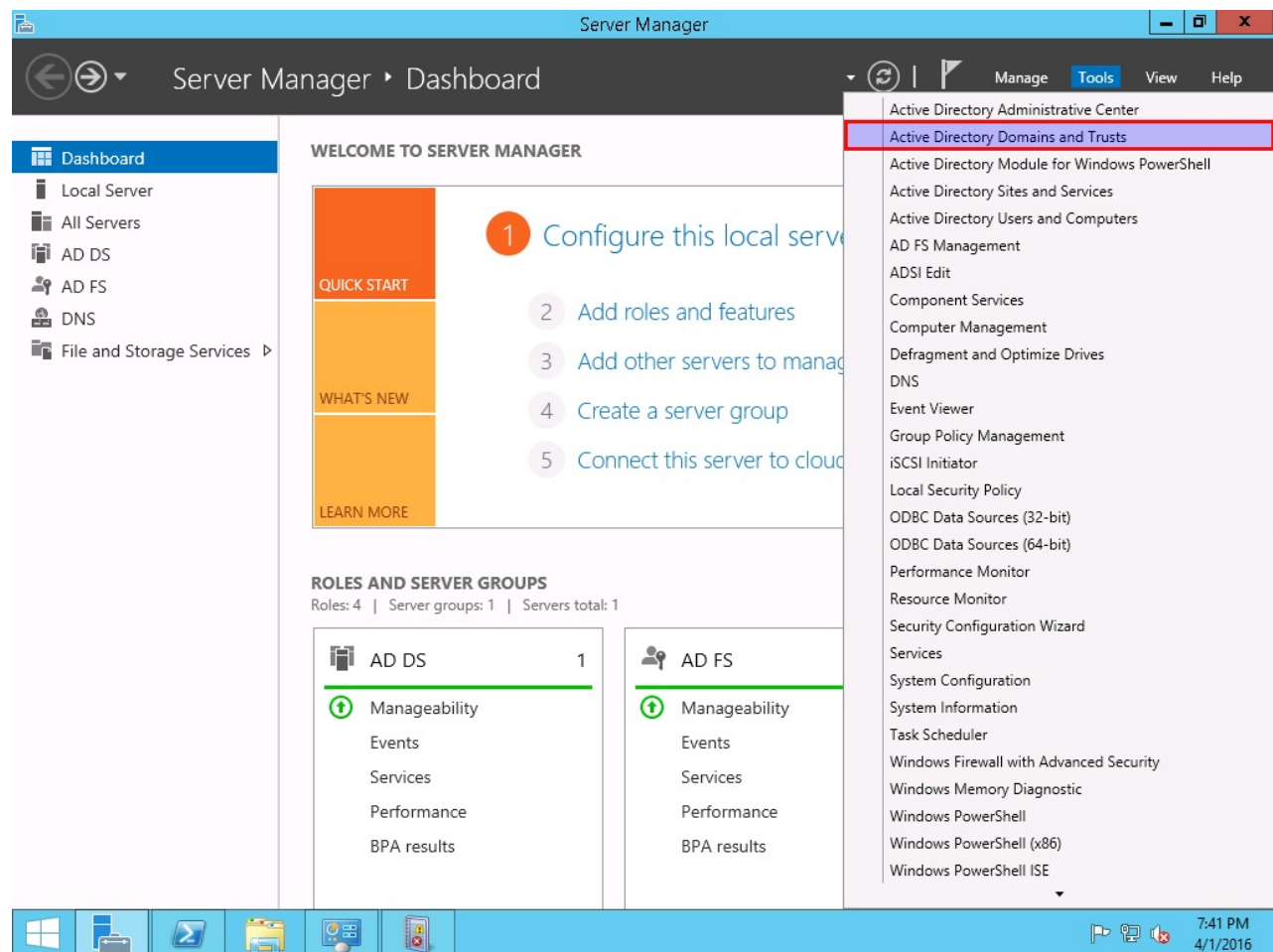
- Microsoft Windows Server 2012 R2
- Microsoft Active Directory Federation Services 3.0

Configuration Steps

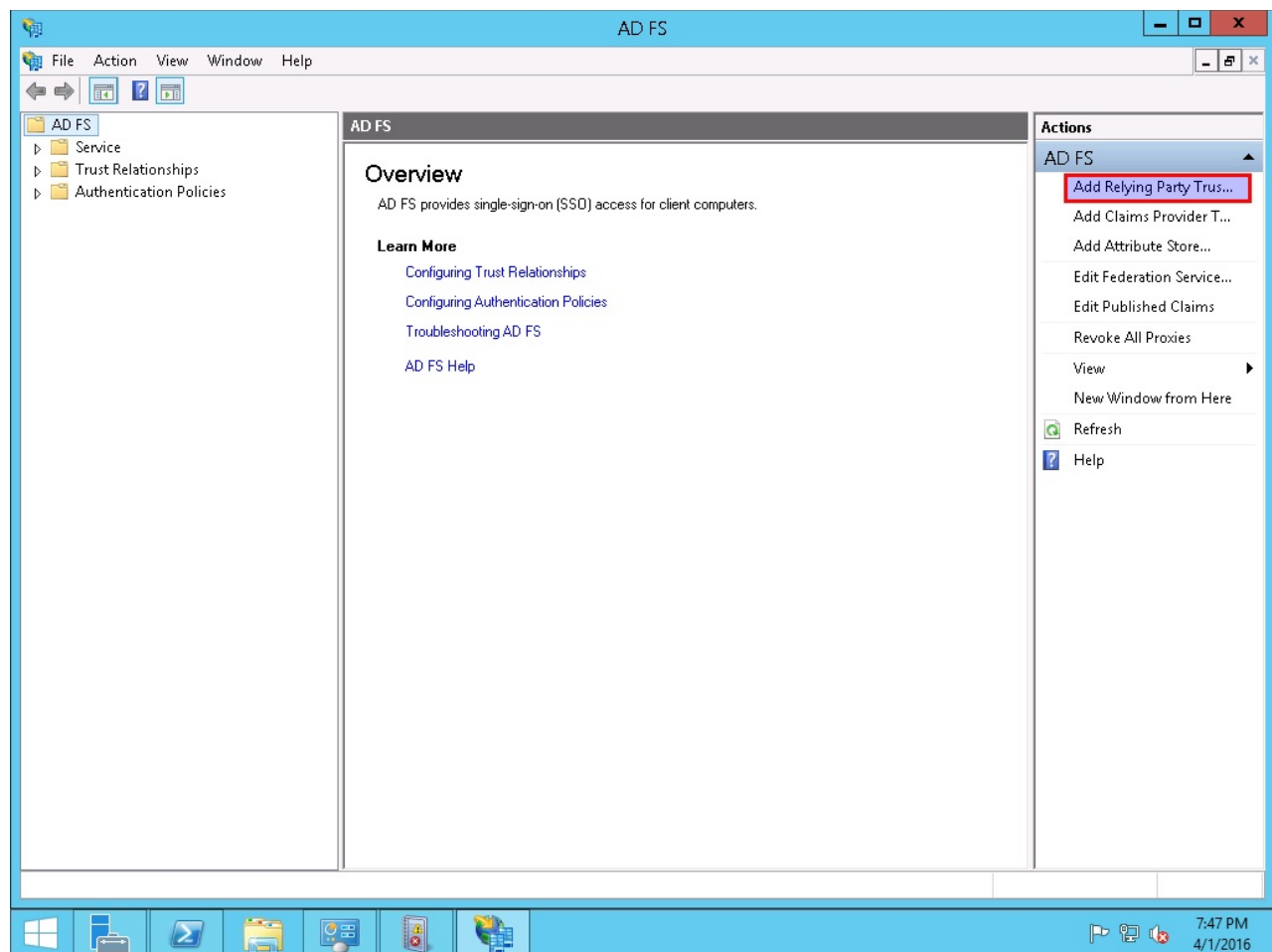
Configure Active Directory Federation Services (ADFS)

This is where we add the Silent Circle trust relationship.

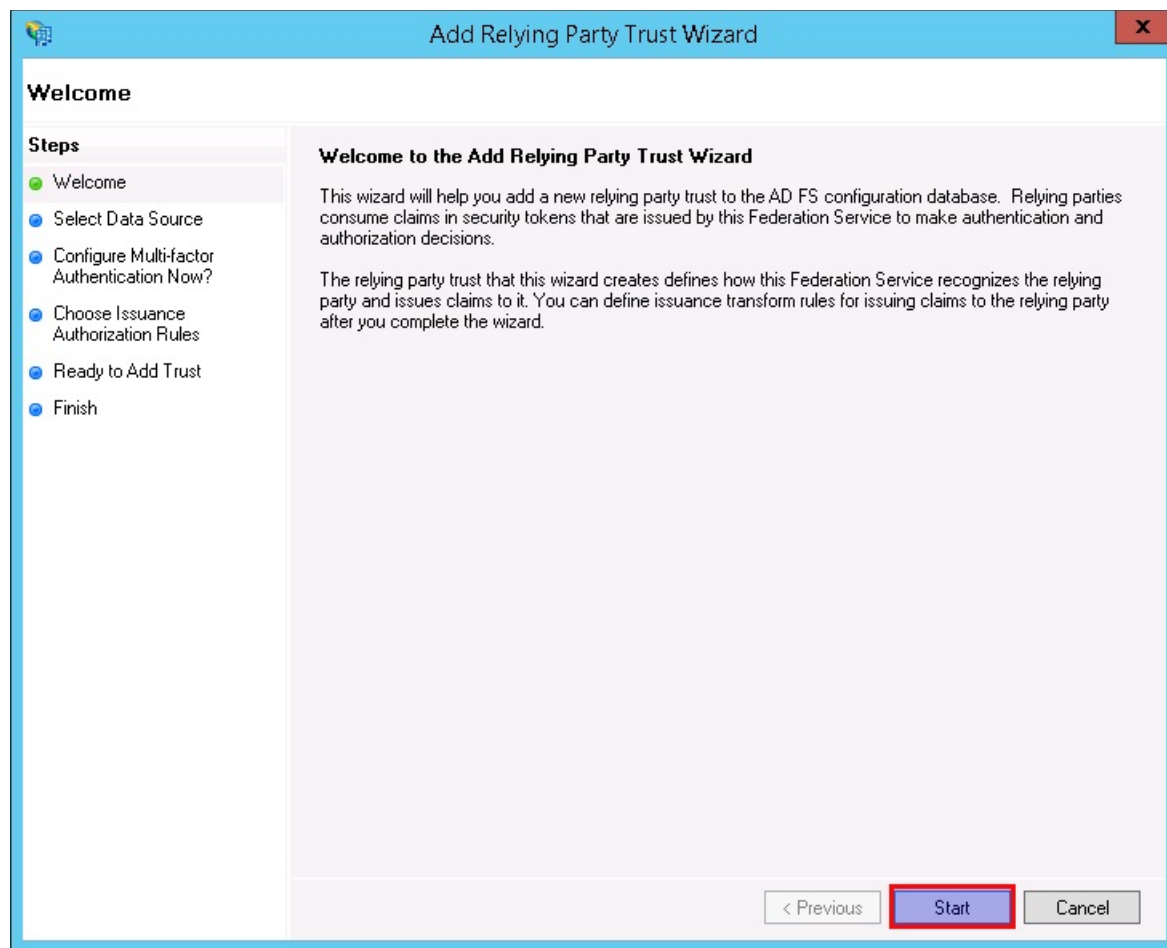
In Server Manager, select **Tools > AD FS Management**.



Launch the **Add Relying Party Trust Wizard**



Start the **Add Relying Party Trust Wizard**



Select **Enter data about the relying party manually**

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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:

☒ Enter data about the relying party manually

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

1

2

Add Silent Circle information

- Enter "Silent Circle Enterprise Client" in **Display name**, and any notes that might be of interest.
- Click **Next**.

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name**
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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:

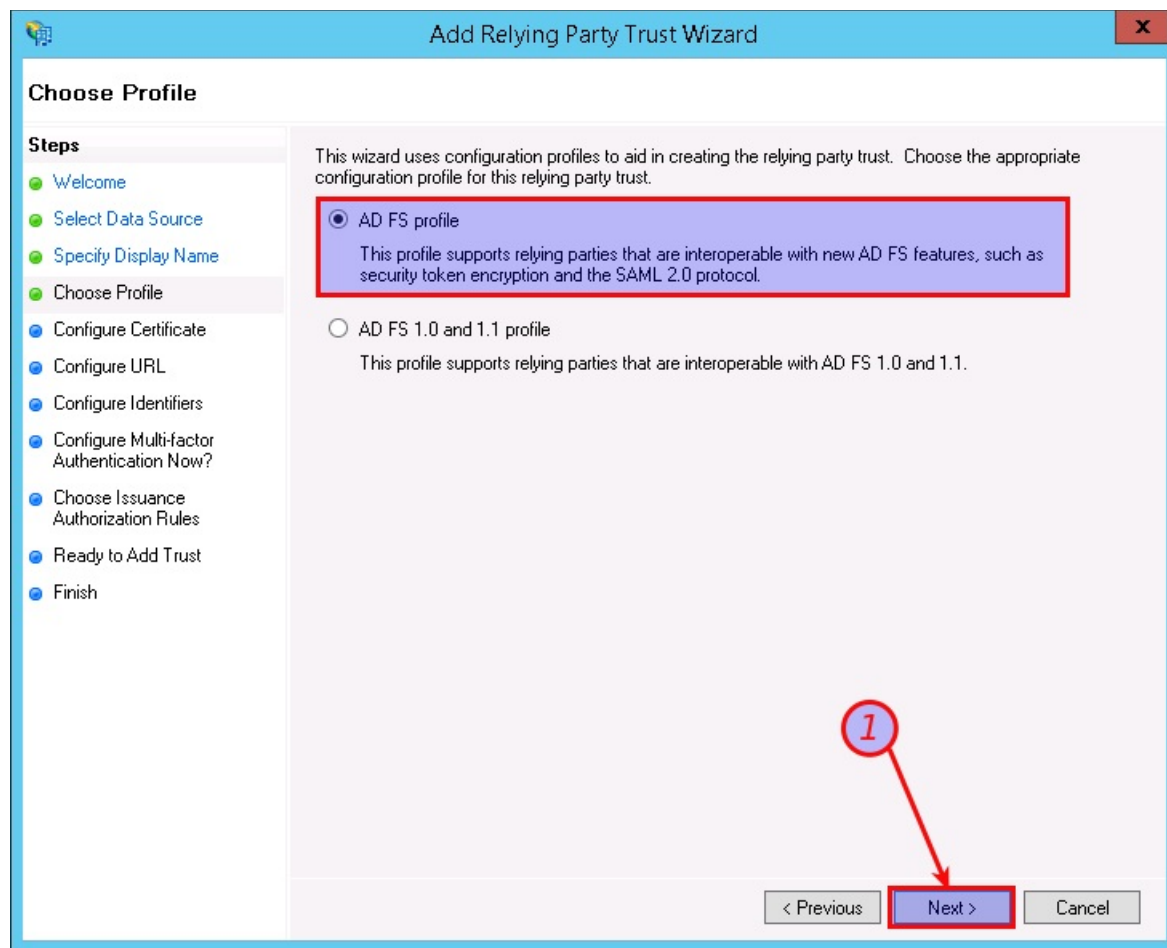
Silent Circle Enterprise Client

Notes:

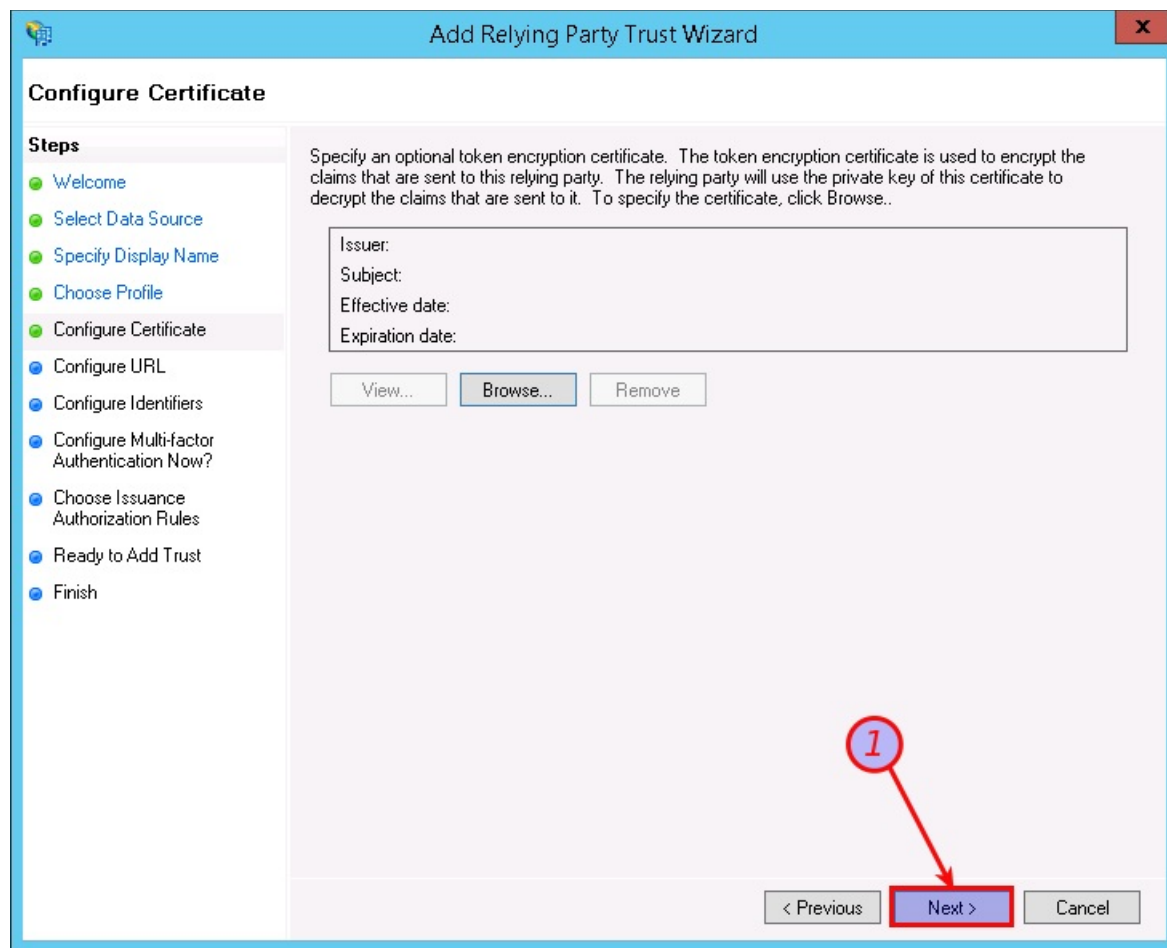
This is the Relying Party for the Silent Circle web site and Silent Phone application.

< Previous **Next >** Cancel

Select AD FS Profile



Skip Token Encryption Certificate



Skip WS-Federation and SAML

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- 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

Add Relying Party trust identifier

- Enter `silentcircle-entapi://rpId` in **Relying party trust identifier** and click **Add**

Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- 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:

silentcircle-entapi://tpid

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

Relying party trust identifiers:

Add

Remove

< Previous Next > Cancel

- Click **Next** to accept the trust identifier.

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Configure Identifiers' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard' and a close button. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, 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 is a text box for 'Relying party trust identifier:' with an 'Add' button. An example is provided: 'Example: https://fs.contoso.com/adfs/services/trust'. Below that is a list box for 'Relying party trust identifiers:' containing the entry 'silentcircle-entapi://rpId', with a 'Remove' button to its right. At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a red box and a red arrow pointing to it from a red circle with the number '1'), and 'Cancel'.

Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- 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:

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

Relying party trust identifiers:

silentcircle-entapi://rpId

< Previous **Next >** Cancel

Optional: Configure MFA

- We skip this step here, but you are free to configure MFA as desired.

Add Relying Party Trust Wizard

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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](#).

1 → **Next >**

< Previous **Next >** Cancel

Choose Issuance Authorization Rules

- We will restrict access in a later step; for now, permit all users to access this Relying Party.

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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.

1

< Previous **Next >** Cancel

Add Trust to the database

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main area is titled 'Ready to Add Trust'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust (highlighted), and Finish. The main content area has a message: '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.' Below this is a tabbed interface with tabs for Monitoring, Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Not. The 'Monitoring' tab is active. It contains the text 'Specify the monitoring settings for this relying party trust.' followed by 'Relying party's federation metadata URL:' and an empty text box. Below this are two checkboxes: 'Monitor relying party' and 'Automatically update relying party', both of which are unchecked. Further down, it says 'This relying party's federation metadata data was last checked on:' followed by '< never >'. Below that, it says 'This relying party was last updated from federation metadata on:' followed by '< never >'. At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a red box and a red arrow pointing to it from a red circle with the number 1), and 'Cancel'.

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- 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 | Not < >

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 >

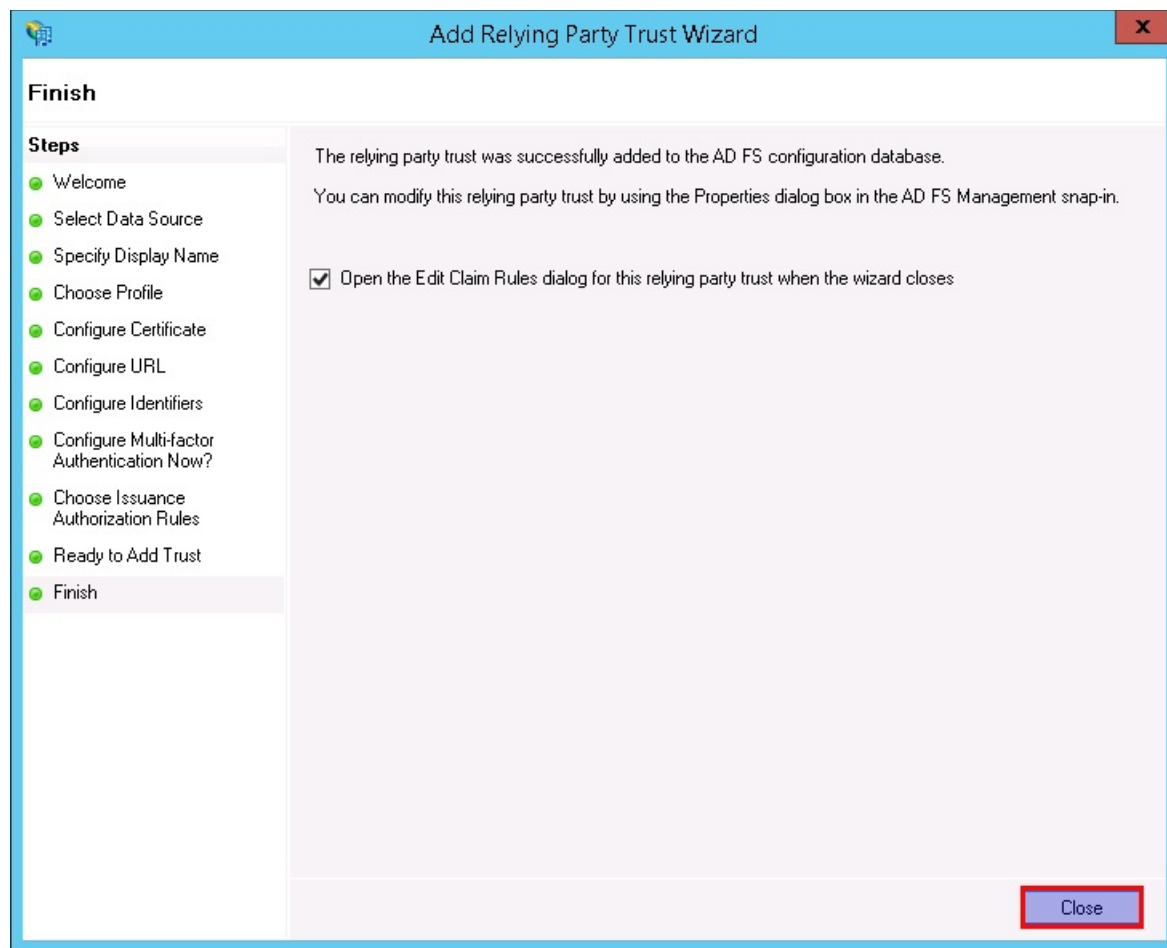
This relying party was last updated from federation metadata on:

< never >

< Previous **Next >** Cancel

Close the wizard

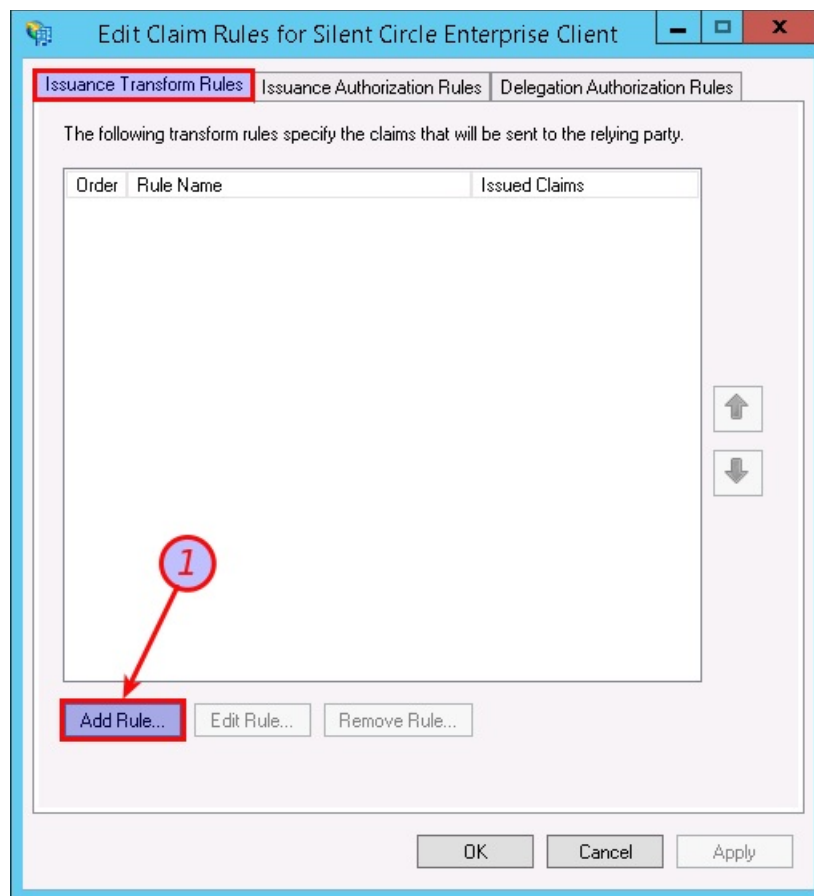
- Click **Close**. This will launch the **Edit Claims Rules Dialog**.



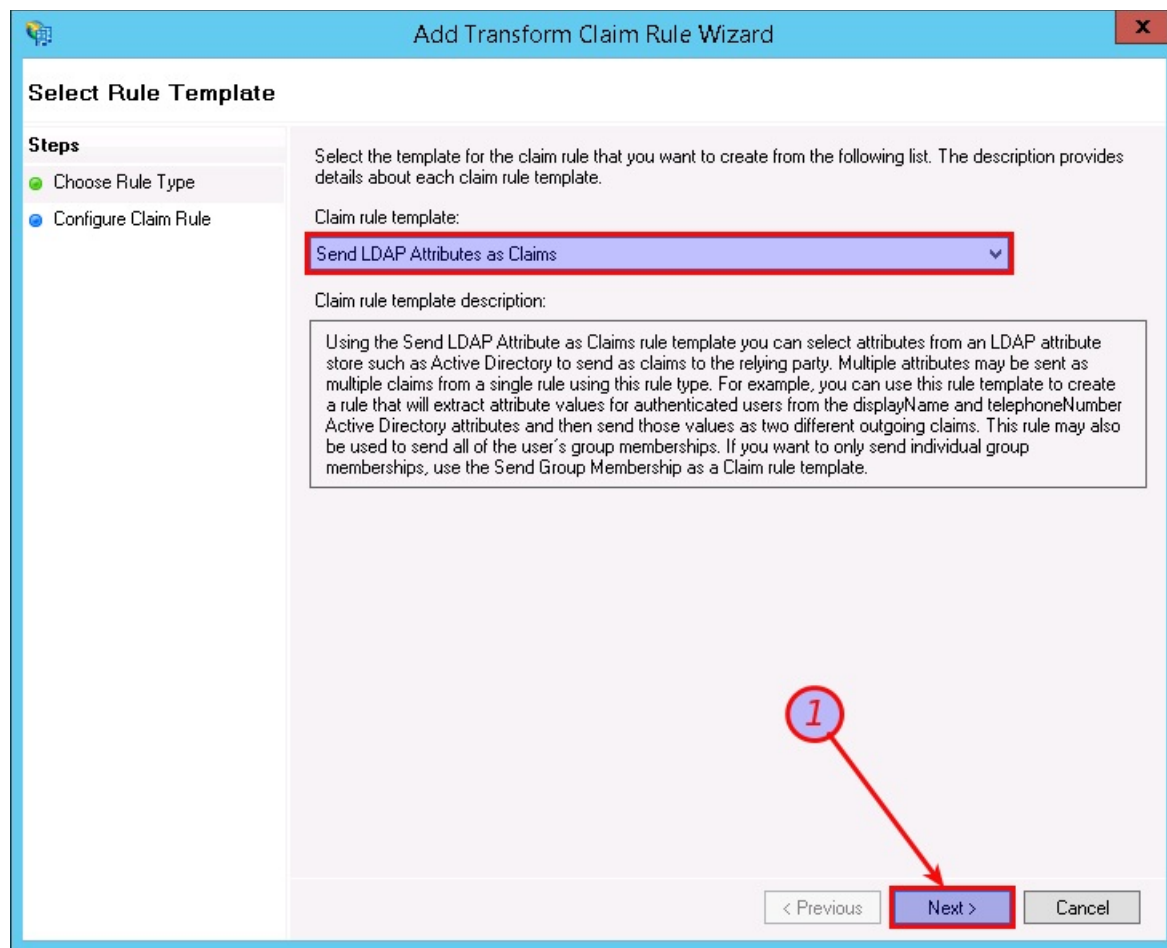
Configure Claims Rules

Add Issuance Transform Rule

- The **Edit Claims Rules for Silent Circle Enterprise Client** wizard should be running now.
- On the **Issuance Transform Rules** tab, click on **Add Rule...**



Accept the **Send LDAP Attributes as Claims** template.



Configure Temp Claim Rule

- Type "Temp" as the claim rule name (we'll be copying this later and deleting it).
- Select **Active Directory** as the attribute store.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Select an attribute store
Active Directory

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| * | <input type="text"/> | <input type="text"/> |

Add LDAP attributes

- Add the following LDAP attribute to Outgoing claim type mappings:
- `objectGUID` to `sub`
- `User-Principal-Name` to `email`
- `displayName` to `name` (note that the Wizard keeps changing this to `Name` - allow it to do so for now; we'll change it later).

Add Transform Claim Rule Wizard

X

Configure Rule

Steps

Choose Rule Type

Configure Claim Rule

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:

Temp

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) |
|---|---|--|
| ▶ | objectGUID | subject |
| * | | |

1

2

< Previous

Finish

Cancel

Add Transform Claim Rule Wizard

X

Configure Rule

Steps

Choose Rule Type

Configure Claim Rule

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:

Temp

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) |
|----|---|--|
| | objectGUID | sub |
| | User-Principal-Name | email |
| »* | | |

1

2

< Previous

Finish

Cancel

Add Transform Claim Rule Wizard

X

Configure Rule

Steps

Choose Rule Type

Configure Claim Rule

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:

Temp

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) |
|---|---|--|
| | objectGUID | sub |
| | User-Principal-Name | email |
| ▶ | Display-Name | name |
| * | | |

1

2

< Previous

Finish

Cancel

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:
Temp

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) |
|---|---|--|
| | objectGUID | sub |
| ▶ | User-Principal-Name | email |
| | Display-Name | Name |
| * | | |

1

< Previous Finish Cancel

- Click **Finish**.

Copy Claim Rule Language

- Click **Edit Rule...** and then **View Rule Language**. Copy the selected text (right-click, then **Copy**).

Edit Claim Rules for Silent Circle Enterprise Client

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 | Temp | sub,email.Name |

↑

↓

Add Rule...

Edit Rule...

Remove Rule...

OK

Cancel

Apply

Edit Rule - Temp

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:

Temp

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

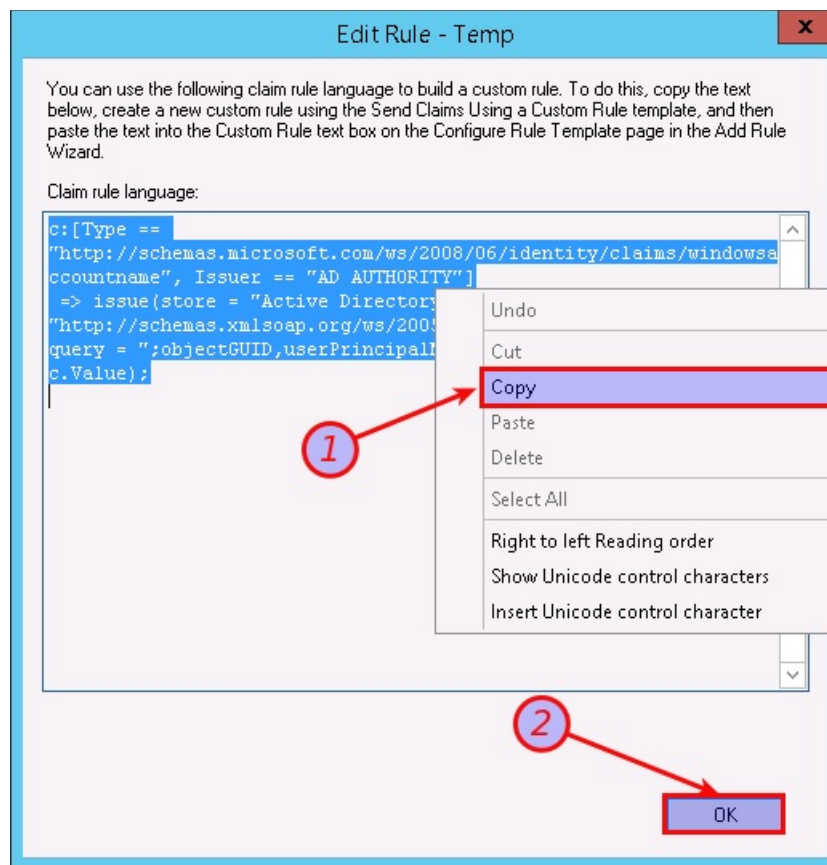
| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | objectGUID | sub |
| | User-Principal-Name | email |
| | Display-Name | Name |
| * | | |

1

View Rule Language...

OK

Cancel



- Click **OK**, then **Cancel** to exit the rule editor.

Edit Rule - Temp

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:

Temp

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) |
|---|---|--|
| ▶ | objectGUID | sub |
| | User-Principal-Name | email |
| | Display-Name | Name |
| * | | |

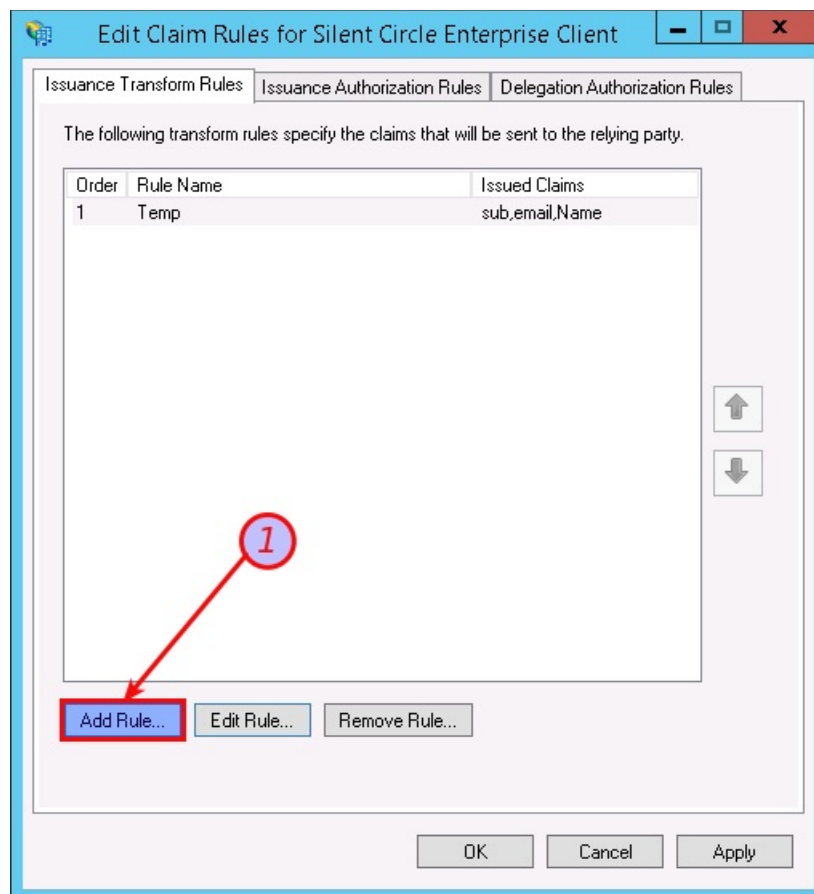
View Rule Language...

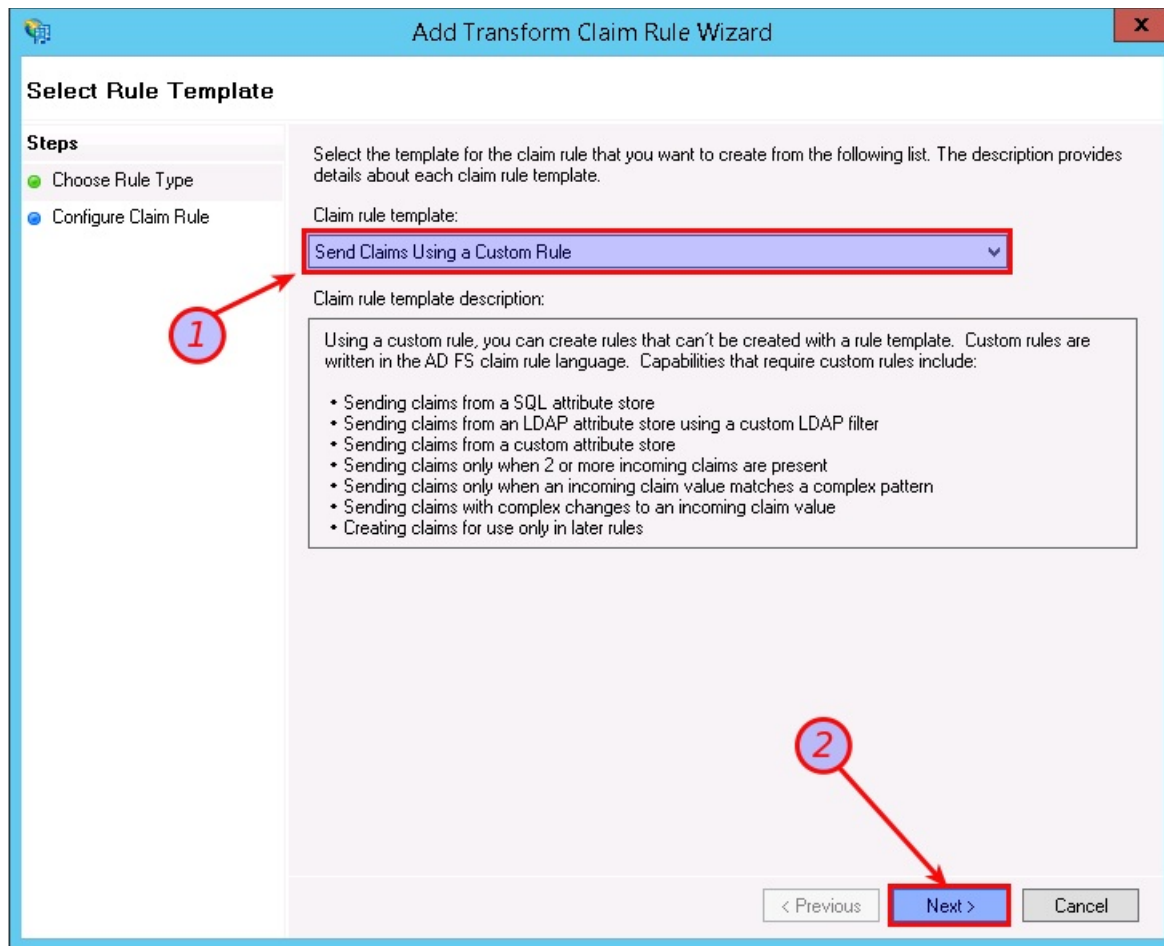
OK

Cancel

Add Custom Rule

- Add rule... to create a new rule based on Send Claims Using a Custom Rule.





- Name it "Send Silent Circle Enterprise Client Claims" and paste the copied text into it.
- Delete the text `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/`.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
Send Silent Circle Enterprise Client Claims

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount  
name". Issuer == "AD AUTHORITY"]  
=> issue(store = "Active Directory", types = ("sub", "email"  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name") query =  
";objectGUID,userPrincipalName,displayName;0}", param = c.Value);
```

Delete highlighted text

< Previous Finish Cancel

- What should be left is `name`.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
Send Silent Circle Enterprise Client Claims

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount  
name", Issuer == "AD AUTHORITY"]  
=> issue(store = "Active Directory", types = ("sub", "email", "name"),  
query = ";objectGUID,userPrincipalName,displayName;0", param =  
c.Value);
```

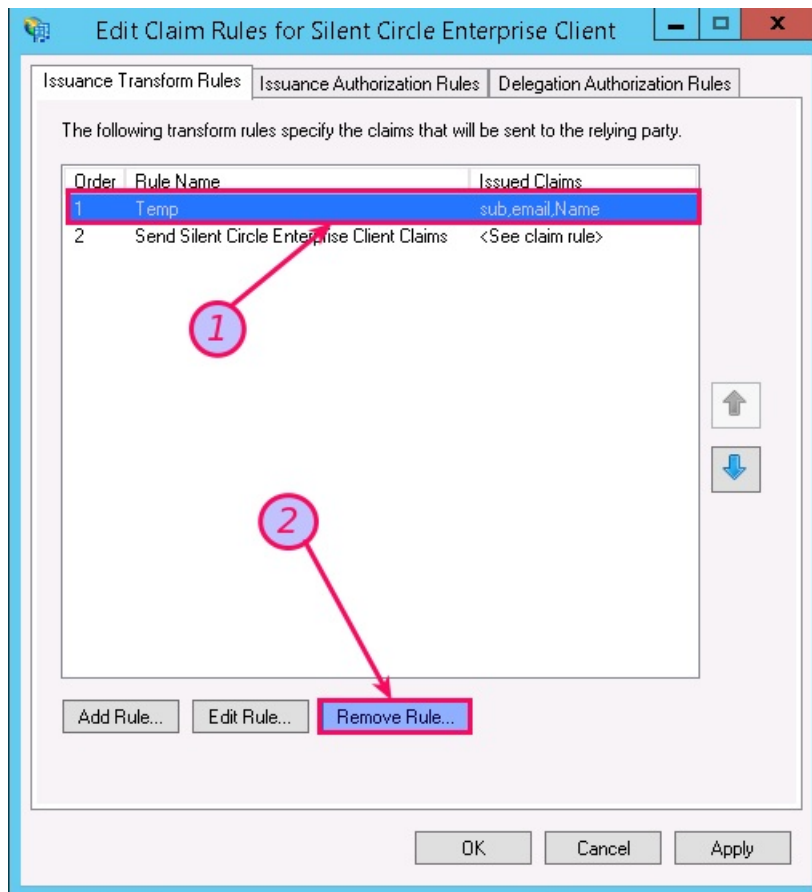
1

2

< Previous Finish Cancel

- Click **Finish**.

Delete temp rule



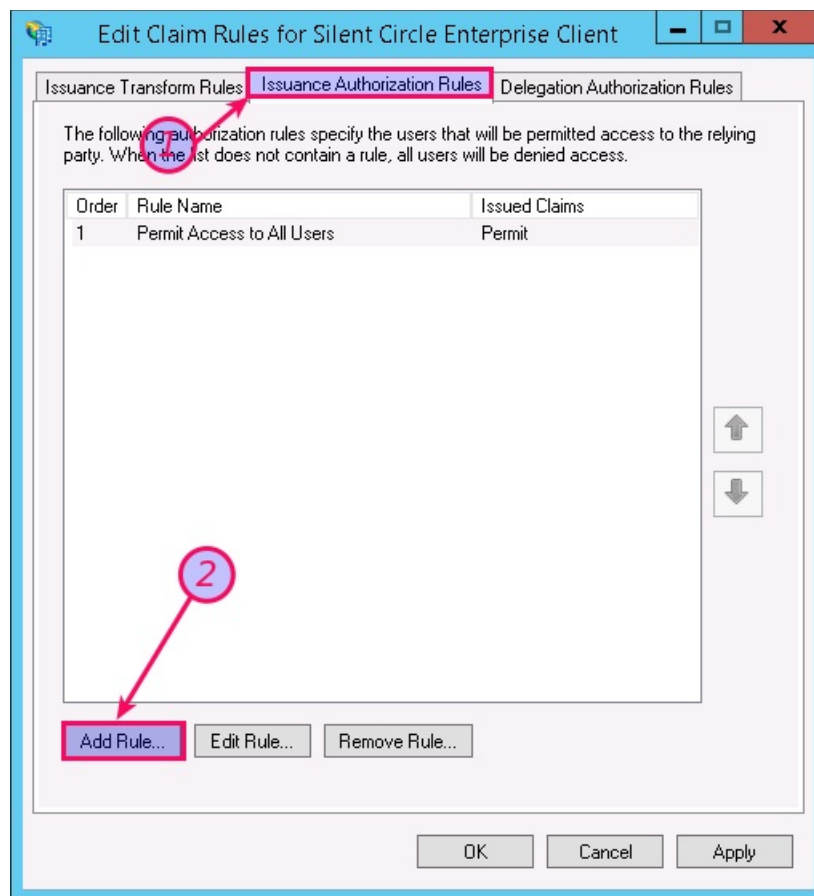
- Delete the `Temp` rule.
- Press `OK`.

Add Issuance Authorization Rules

The precise details will vary widely, but most companies will want to restrict which employees can use Silent Circle. This can be done using Issuance Authorization Rules. If an employee tries to authenticate for a Silent Circle resource (like Silent Phone), but is blocked by this rule, the employee will be prevented from authenticating, and will not be authorized to use Silent Circle.

In this chapter we add a simple rule based on a user group that was previously added. No doubt more elaborate rules will be desired, but this is a good starting point.

- Select the `Issuance Authorization Rules` tab in `Edit Claim Rules`, and click on `Add Rule...`.



- Select **Permit or Deny Users Based on an Incoming Claim**.

Add Issuance Authorization 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.

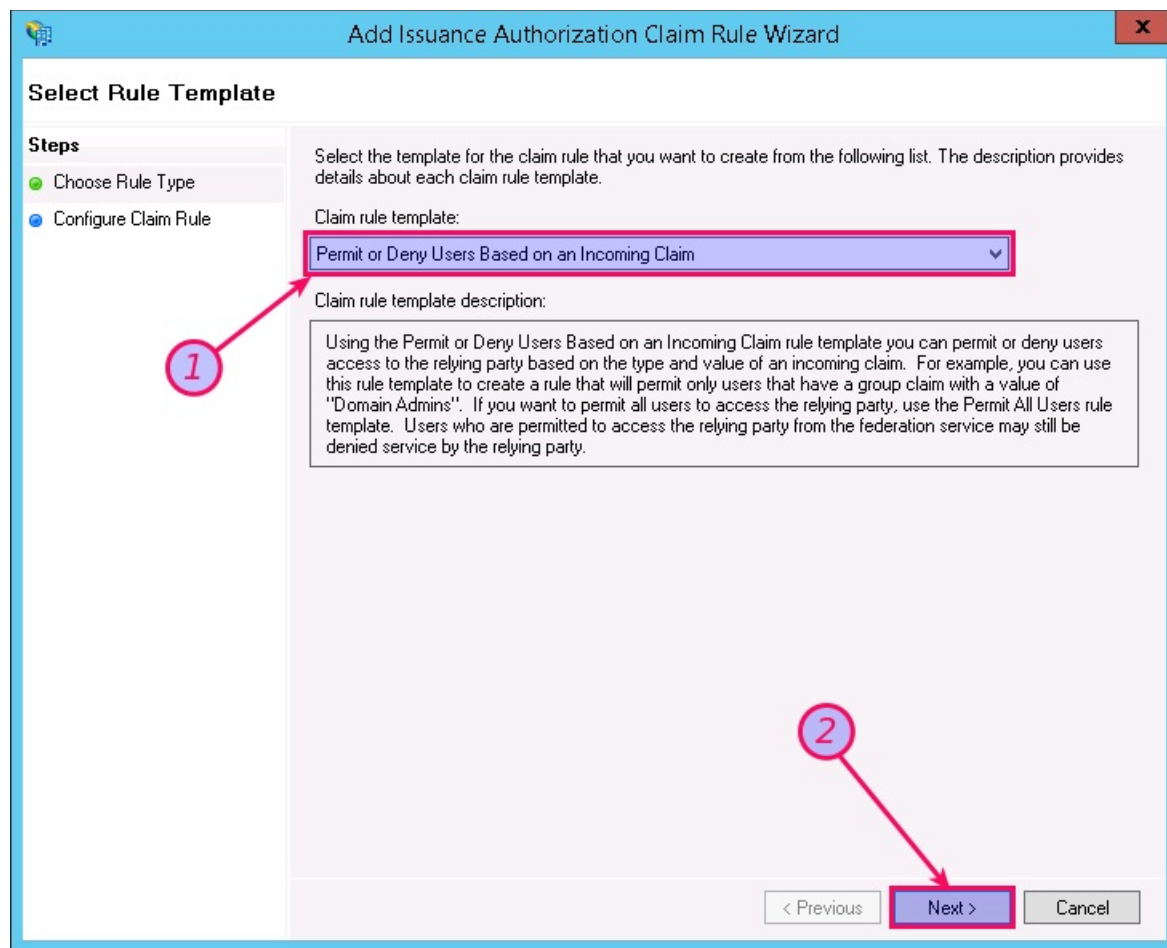
Claim rule template:

Permit or Deny Users Based on an Incoming Claim

Claim rule template description:

Using the Permit or Deny Users Based on an Incoming Claim rule template you can permit or deny users access to the relying party based on the type and value of an incoming claim. For example, you can use this rule template to create a rule that will permit only users that have a group claim with a value of "Domain Admins". If you want to permit all users to access the relying party, use the Permit All Users rule template. Users who are permitted to access the relying party from the federation service may still be denied service by the relying party.

< Previous **Next >** Cancel



- Type in a rule name like `Authorize Silent Circle group members`.
- Select `Group SID` as an Incoming Claim Type.

Add Issuance Authorization Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to permit or deny users based on an incoming claim. Specify the incoming claim type, claim value, and whether the users should be permitted or denied access to the relying party.

Claim rule name: **Authorize Silent Circle group members**

Rule template: Authorize Users Based on an Incoming Claim

Incoming claim type:

AD FS 1.x E-Mail Address

Deny only primary group SID
Deny only primary SID
Device Identifier
Device OS type
Device OS Version
Device Registration DisplayName
Device Registration Identifier
E-Mail Address
Endpoint Path
Enhanced Key Usage
Forwarded Client IP
Given Name
Group
Group SID
Inside Corporate Network
Is Managed Device
Is Registered User
Issuer
Issuer Name
Key Usage
Name
Name ID
Not After
Not Before
Password Expiration Days
Password Expiration Time
PPID
Primary group SID

Browse...

her users with this claim will be permitted or denied access

< Previous Finish Cancel

- Ensuring that the claim type is still **Group SID**, click **Browse** to select an incoming claim rule.

Add Issuance Authorization Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to permit or deny users based on an incoming claim. Specify the incoming claim type, claim value, and whether the users should be permitted or denied access to the relying party.

Claim rule name:
Authorize Silent Circle group members

Rule template: Authorize Users Based on an Incoming Claim

Incoming claim type:
Group SID

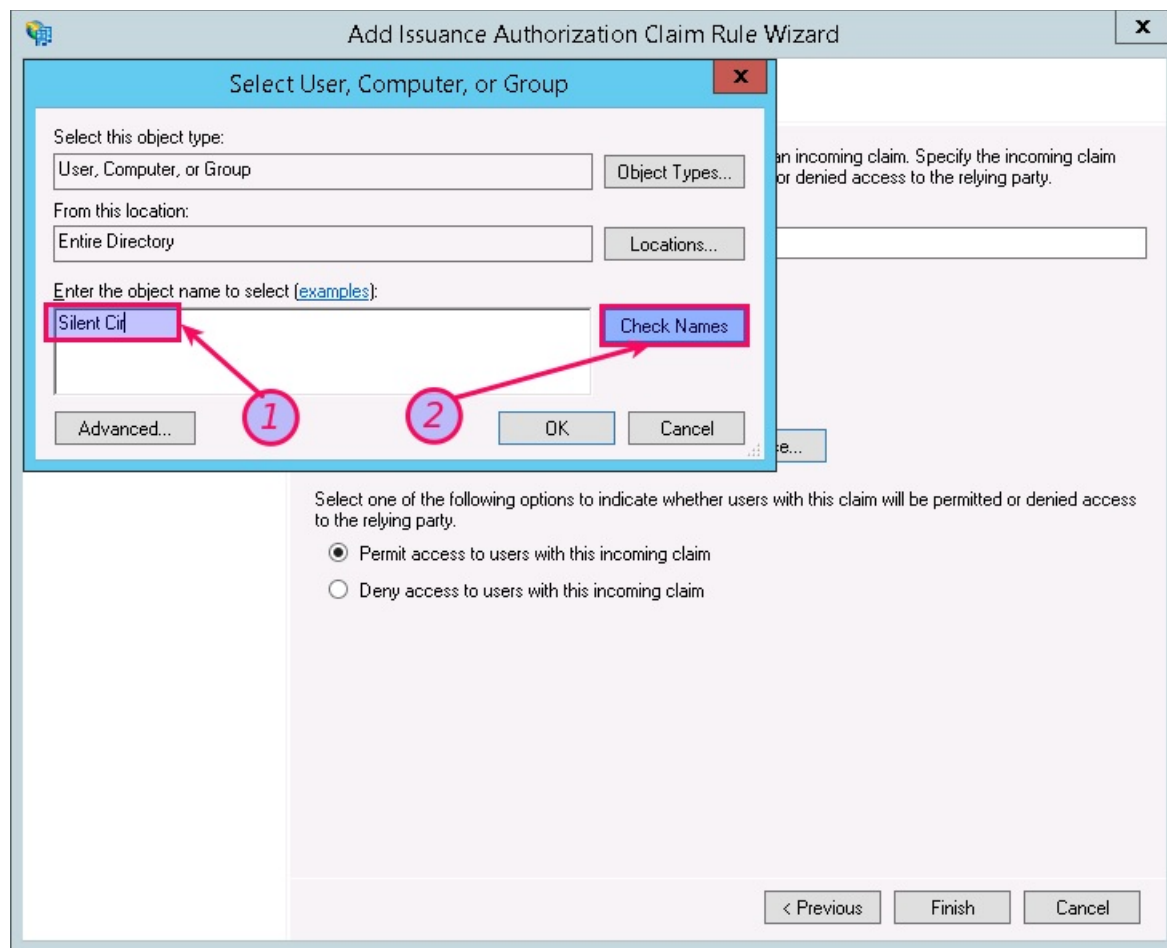
Incoming claim value:
 Browse...

Select one of the following options to indicate whether users with this claim will be permitted or denied access to the relying party.

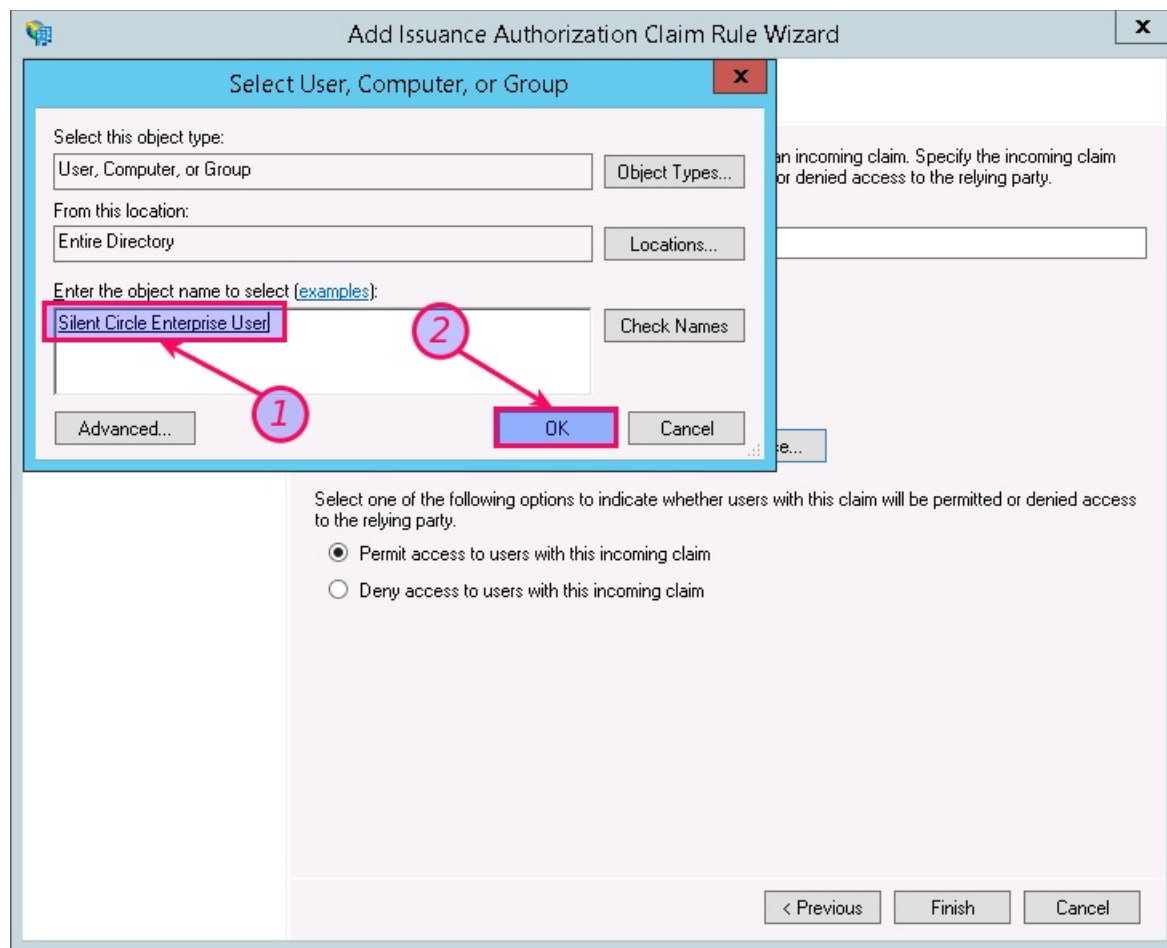
☒ Permit access to users with this incoming claim
☐ Deny access to users with this incoming claim

< Previous Finish Cancel

- In the **Select User, Computer, or Group** dialog box, start typing in the group name. In this example, we've typed in **Silent Cir** and deliberately not completed it.



- Now, click **Check Names** and the name will be auto-completed if possible. Otherwise, type in the full group name and click **Check names** again, followed by **OK**.



- Ensure that all the fields are correct as shown:
 - Incoming claim type: **Group SID**
 - Incoming claim value: (varies by installation)
 - Radio button selected: **Permit access to users with this incoming claim**.
- Click **Finish**.

Add Issuance Authorization Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to permit or deny users based on an incoming claim. Specify the incoming claim type, claim value, and whether the users should be permitted or denied access to the relying party.

Claim rule name:
Authorize Silent Circle group members

Rule template: Authorize Users Based on an Incoming Claim

Incoming claim type:
Group SID

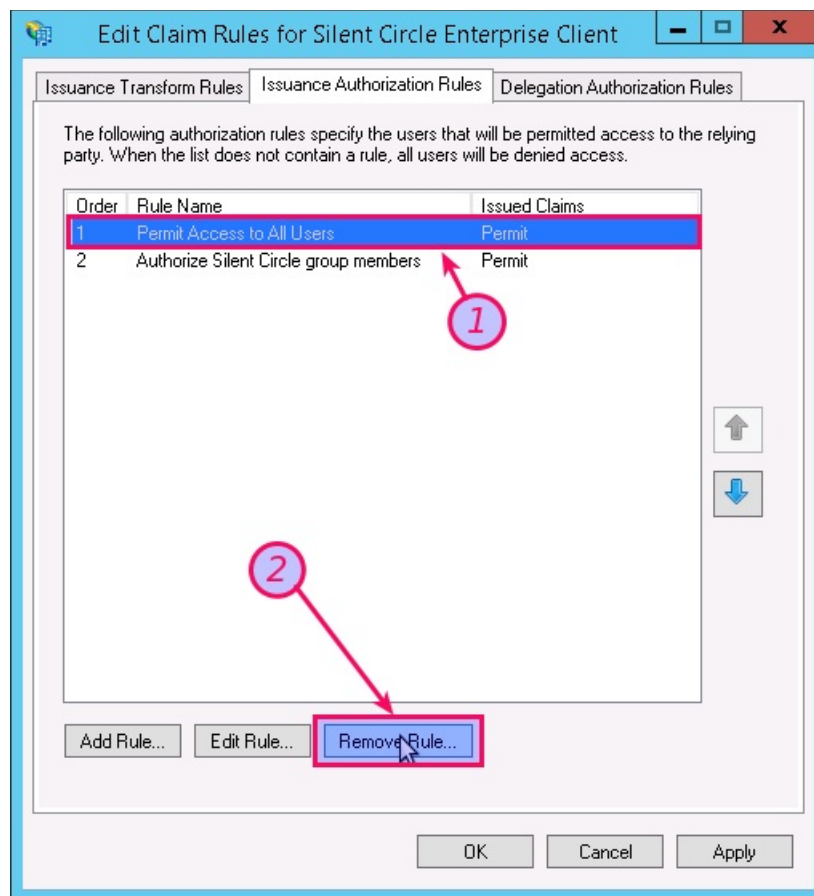
Incoming claim value:
SSO-DEV0\Silent Circle Enterprise User Browse...

Select one of the following options to indicate whether users with this claim will be permitted or denied access to the relying party.

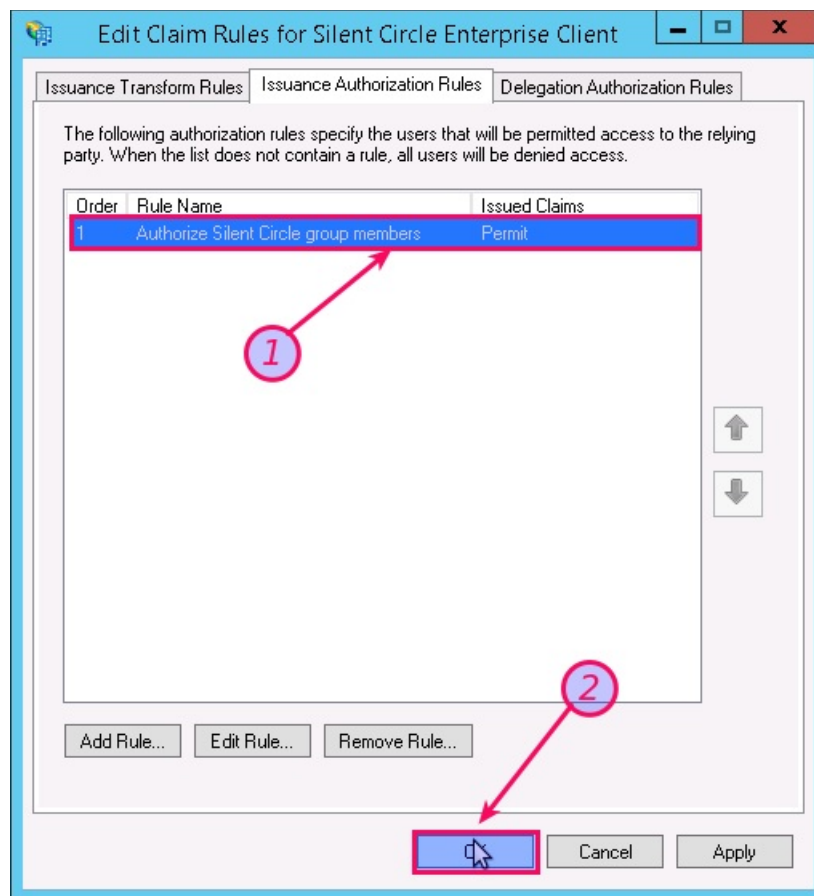
☒ Permit access to users with this incoming claim
☐ Deny access to users with this incoming claim

< Previous **Finish** Cancel

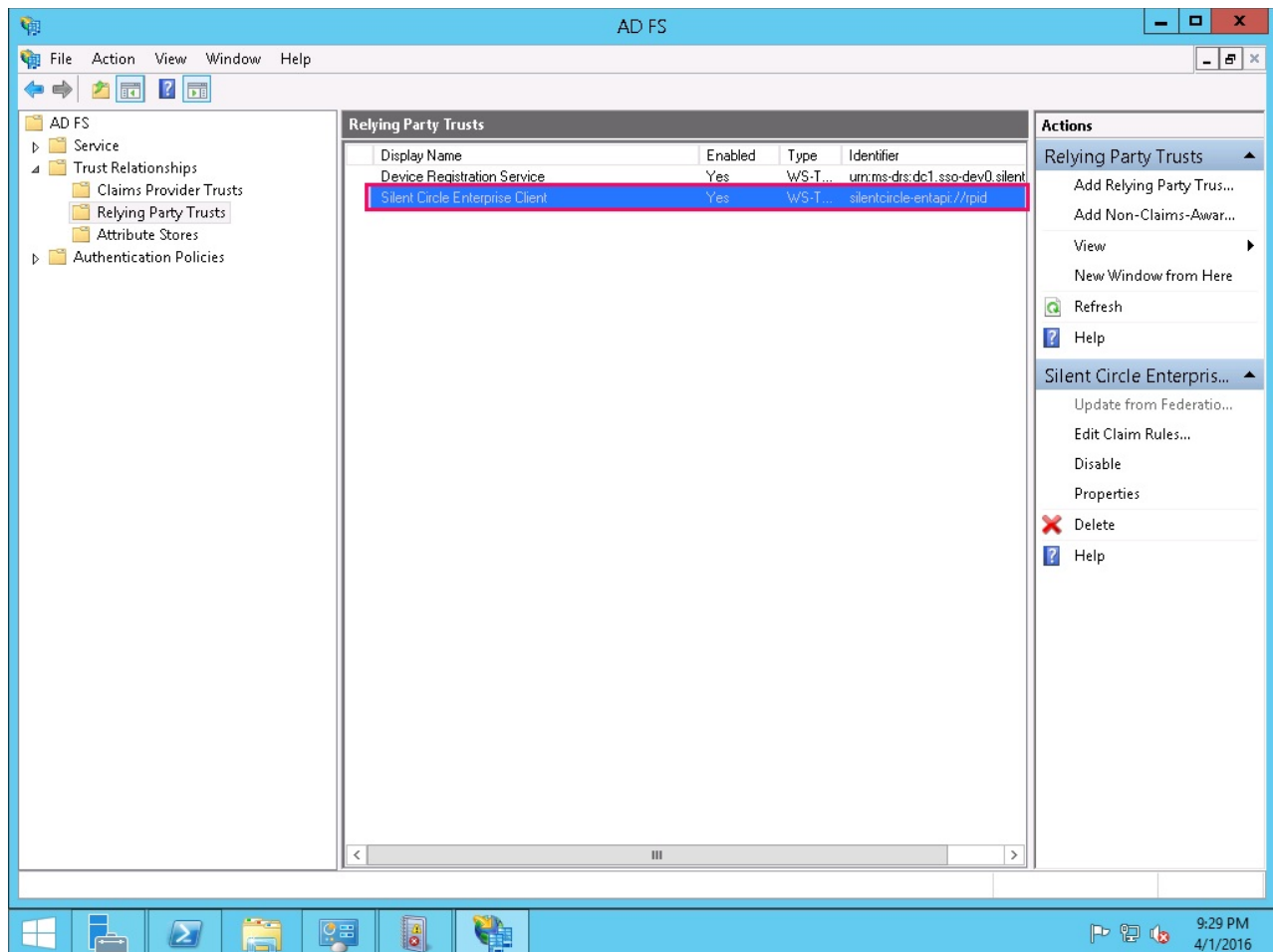
- Remove the default rule, **Permit Access to All Users**.



- There should only be one rule left; the one we just added. Click **OK**.



- Finally, we see the **Silent Circle Relying Party** Enterprise Trust rule we've been working on.



Configure Silent Circle ADFS OAuth2 Client

This is the last step. In this step we need to configure the Silent Circle OAuth2 client.

In a PowerShell window, type in the following command:

```
Add-AdfsClient -ClientId SCEntClient `
  -Name 'Silent Circle Enterprise Client' `
  -Description 'Silent Circle Enterprise Client' `
  -RedirectURI https://accounts.silentcircle.com/sso/oauth2/return/,https://accounts-dev.silentcircle.com/sso/oauth2/return/,https://localsc.ch/sso/oauth2/return/,http://localsc.ch:8000/sso/oauth2/return/
```

To check it, type in

```
Get-AdfsClient 'Silent Circle Enterprise Client'
```

Sample output is shown below.

```
PS C:\Users\Administrator> Get-AdfsClient 'Silent Circle Enterprise Client'
```



```
RedirectUri : {http://localsc.ch:8000/sso/oauth2/return/, https://accounts.silentcircle.com/sso/oauth2/return/,  
              https://accounts-dev.silentcircle.com/sso/oauth2/return/, https://  
localsc.ch/sso/oauth2/return/}  
Name       : Silent Circle Enterprise Client  
Description : Silent Circle Enterprise Client  
ClientId   : SCEntClient  
BuiltIn    : False  
Enabled    : True  
ClientType : Public
```