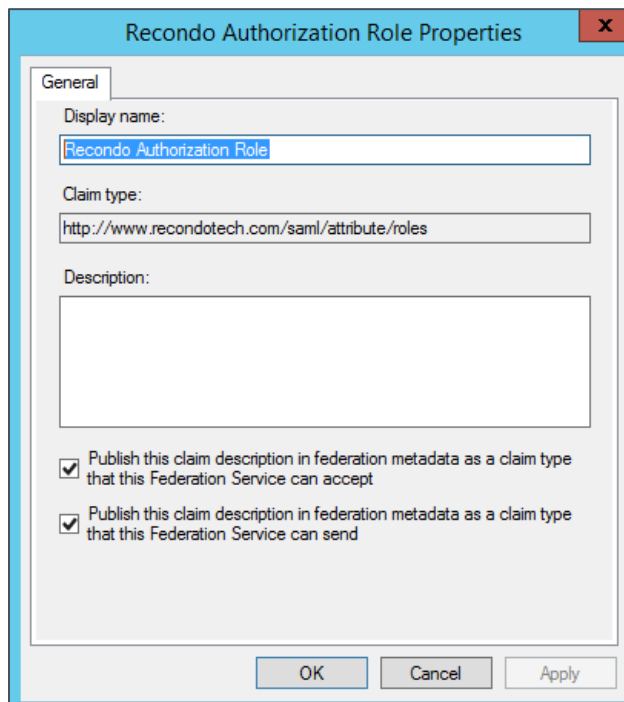


Overview

This document explains how to configure custom claim rules in ADFS for Waystar single sign-on (SSO) integration.

1. Update ADFS > Service > Claim Descriptions

- a. Add Recondo Authorization Role.
- b. Name: **Recondo Authorization Role**.
- c. Claim type: **<http://www.recondotech.com/saml/attribute/roles>**.
- d. Enable both **Publish** checkboxes.
- e. Click the **OK** button.



Recondo Authorization Role Properties

General

Display name:
Recondo Authorization Role

Claim type:
<http://www.recondotech.com/saml/attribute/roles>

Description:

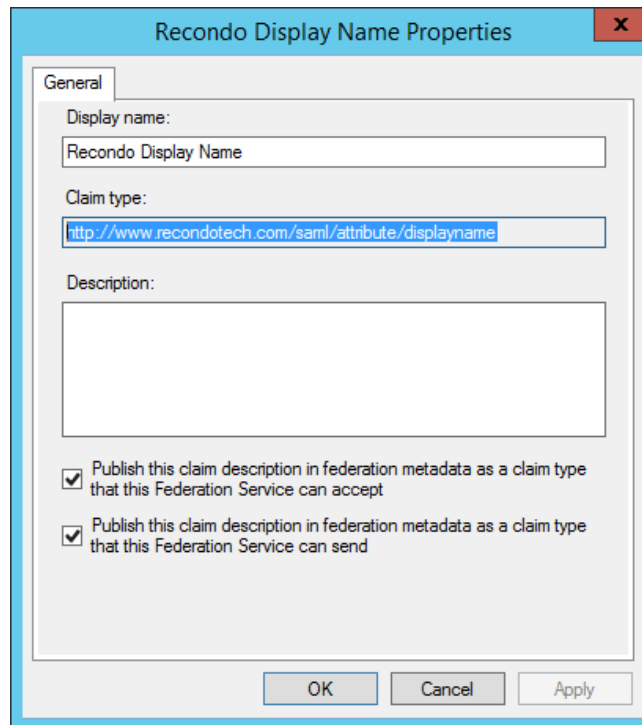
☒ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

☒ Publish this claim description in federation metadata as a claim type that this Federation Service can send

OK Cancel Apply

2. Update ADFS > Service > Claim Descriptions

- Add Recondo Display Name.
- Name: **Recondo Display Name**.
- Claim type: **<http://www.recondotech.com/saml/attribute/displayname>**
- Enable both **Publish** checkboxes.
- Click the **OK** button.



Recondo Display Name Properties

General

Display name:
Recondo Display Name

Claim type:
<http://www.recondotech.com/saml/attribute/displayname>

Description:

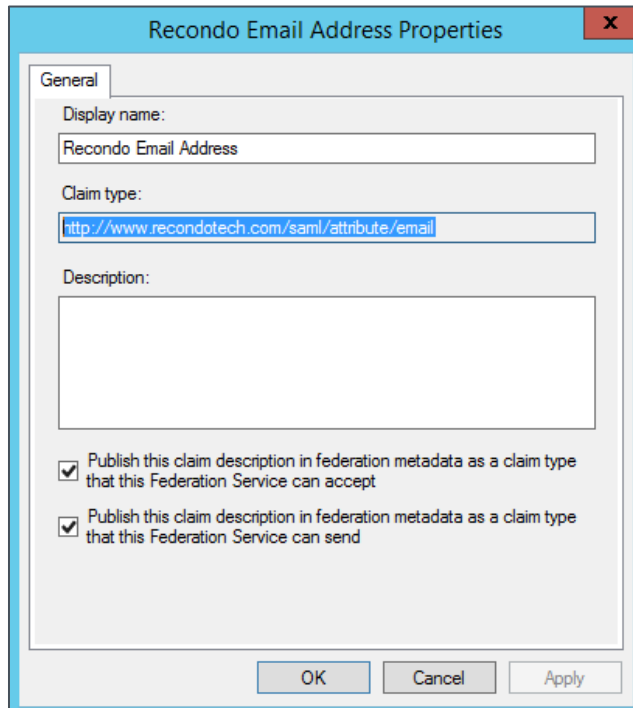
☒ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

☒ Publish this claim description in federation metadata as a claim type that this Federation Service can send

OK Cancel Apply

3. Update ADFS -> Service -> Claim Descriptions

- Add Recondo Email Address.
- Name: **Recondo Email Address**.
- Claim type: **<http://www.recondotech.com/saml/attribute/email>**.
- Enable both **Publish** checkboxes.
- Click the **OK** button.



Recondo Email Address Properties

General

Display name:
Recondo Email Address

Claim type:
<http://www.recondotech.com/saml/attribute/email>

Description:

☒ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

☒ Publish this claim description in federation metadata as a claim type that this Federation Service can send

OK Cancel Apply

4. Add Relying Party

Use the ADFS documentation; there are no special instructions.

5. Edit Claim Rules for Relying Party

- Add Send Name ID.
- Set Claim rule name: **Send Name ID**.
- Set Rule template: **Send LDAP Attributes as Claims**.
- Set LDAP Attribute: **User-Principal-Name**.
- Set Outgoing Claim Type: **Name ID**.
- Click the **OK** button.

Edit Rule - Send NameID

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:

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	Name ID
*		

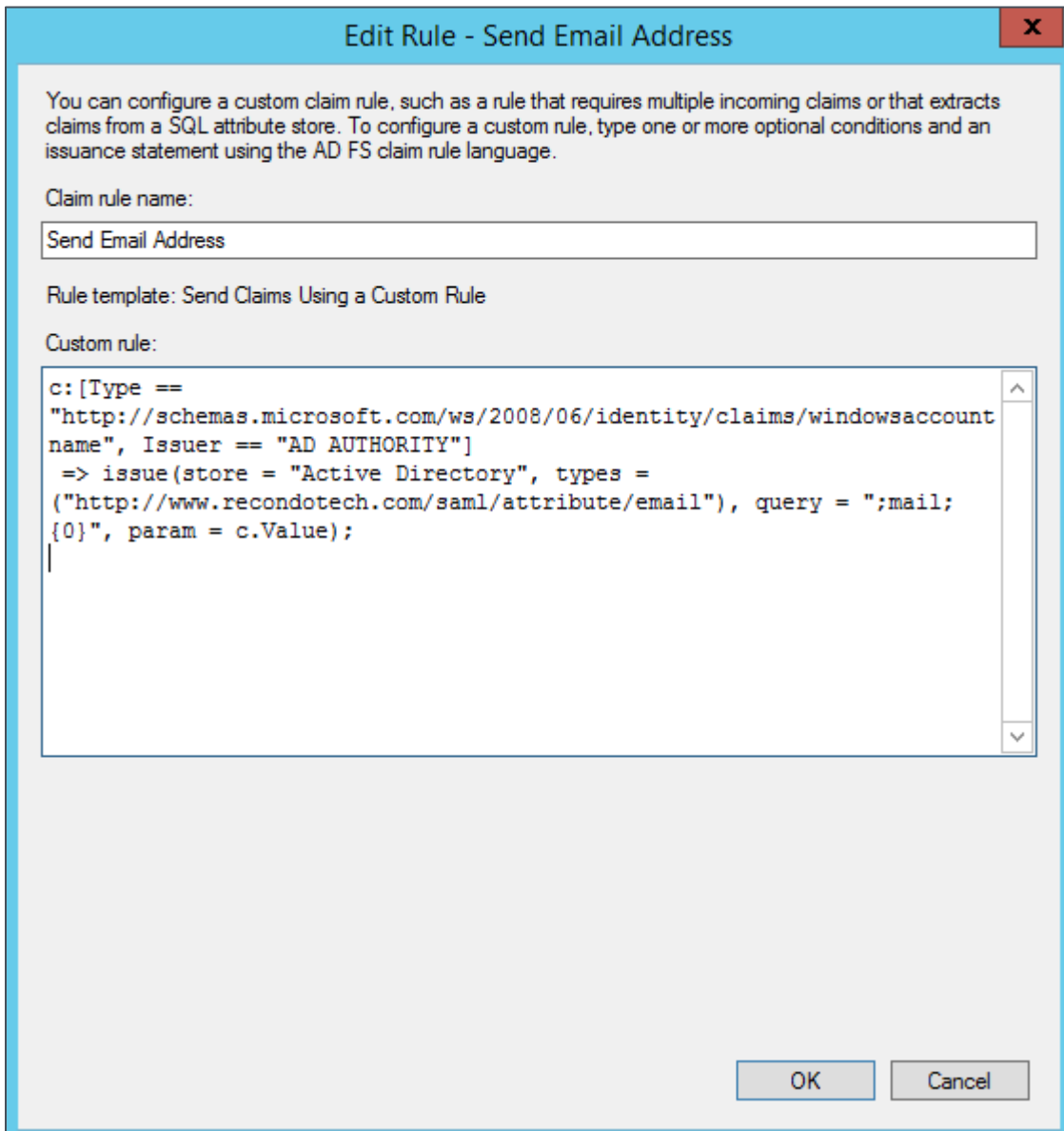
View Rule Language...
OK
Cancel

6. Edit Claim Rules for Relying Party

- a. Add Send Email Address.
- b. Set Rule template: **Send Claims Using a Custom Rule.**
- c. Set Claim rule name: **Send Email Address.**
- d. Set Custom rule:


```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
== "AD AUTHORITY"]

=> issue(store = "Active Directory", types =
("http://www.recondotech.com/saml/attribute/email"), query = ";mail;{0}", param =
c.Value);
```
- e. Click the **OK** button.



Edit Rule - Send Email Address

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 Email Address

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 =
("http://www.recondotech.com/saml/attribute/email"), query = ";mail;
{0}", param = c.Value);
```

OK Cancel

7. Edit Claim Rules for Relying Party

- a. Add Send Display Name.
- b. Set Rule template: **Send Claims Using a Custom Rule.**
- c. Set Claim rule name: **Send Display Name.**

Note: Custom rule is using the email as the display name, you can use a different directory value if desired.

- d. Set Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
== "AD AUTHORITY"]

=> issue(store = "Active Directory", types =
("http://www.recondotech.com/saml/attribute/displayname"), query = ";mail;{0}", param
= c.Value);
```

- e. Click the **OK** button.

Edit Rule - Send Display Name

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:

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 =
("http://www.recondotech.com/saml/attribute/displayname"), query =
";mail;{0}", param = c.Value);
```

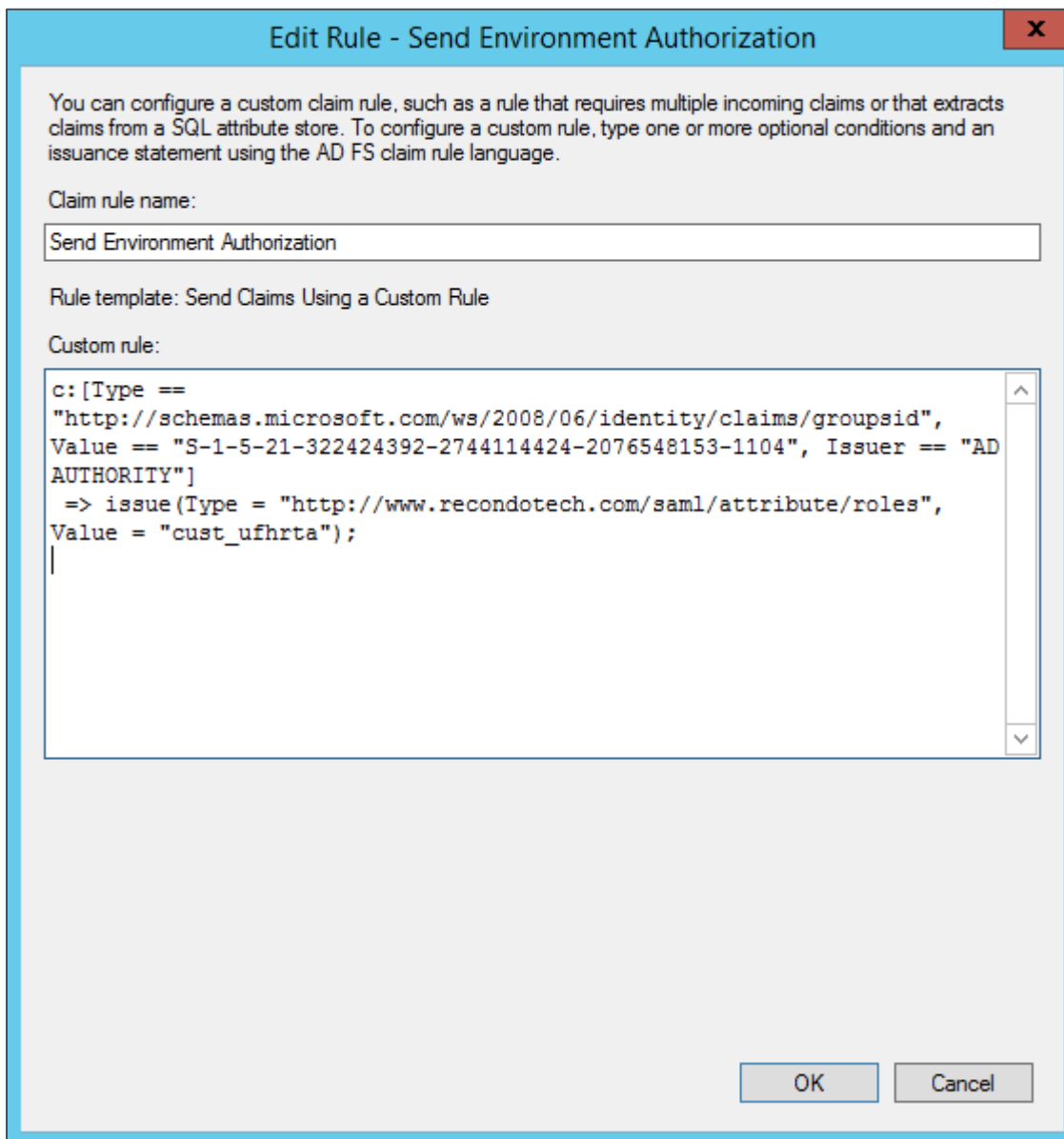
OKCancel

8. Edit Claim Rules for Relying Party

- a. Add Send Environment Authorization.
- b. Set Rule template: **Send Claims Using a Custom Rule.**
- c. Set Claim rule name: **Send Environment Authorization.**
- d. Custom rule requires a **groupsid**; see the [How to get a groupsid](#) section for how to use it in this rule.
- e. Set Custom rule:


```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value ==
  "S-1-5-21-322424392-2744114424-2076548153-1104", Issuer == "AD AUTHORITY"]

=> issue(Type = "http://www.recondotech.com/saml/attribute/roles", Value =
  "cust_ufhrta");
```
- f. Click the **OK** button.



Edit Rule - Send Environment Authorization

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 Environment Authorization

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value == "S-1-5-21-322424392-2744114424-2076548153-1104", Issuer == "AD
AUTHORITY"]
=> issue(Type = "http://www.recondotech.com/saml/attribute/roles",
Value = "cust_ufhrta");
```

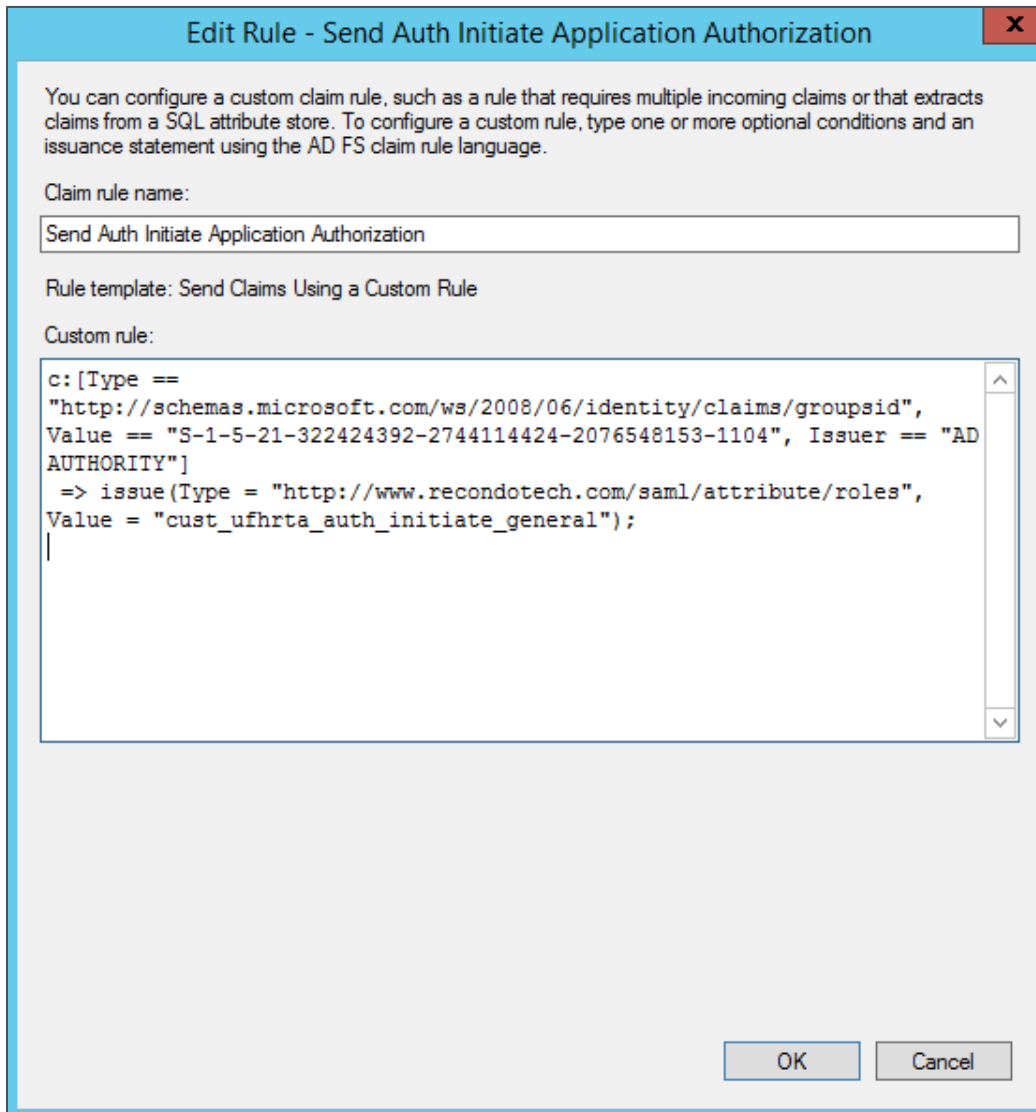
OK Cancel

9. Edit Claim Rules for Relying Party

- a. Send Auth Initiate Application Authorization.
- b. Set Rule template: **Send Claims Using a Custom Rule.**
- c. Set Claim rule name: **Send Auth Initiate Application Authorization.**
- d. Custom rule requires a **groupid**; see the [How to get a groupid](#) section for how to use it in this rule.
- e. Set Custom rule:


```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupid", Value ==
"S-1-5-21-322424392-2744114424-2076548153-1104", Issuer == "AD AUTHORITY"]

=> issue(Type = "http://www.recondotech.com/saml/attribute/roles", Value =
"cust_ufhrta_auth_initiate_general");
```
- f. Click the **OK** button.



Edit Rule - Send Auth Initiate Application Authorization

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:

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupid",
Value == "S-1-5-21-322424392-2744114424-2076548153-1104", Issuer == "AD
AUTHORITY"]
=> issue(Type = "http://www.recondotech.com/saml/attribute/roles",
Value = "cust_ufhrta_auth_initiate_general");
```

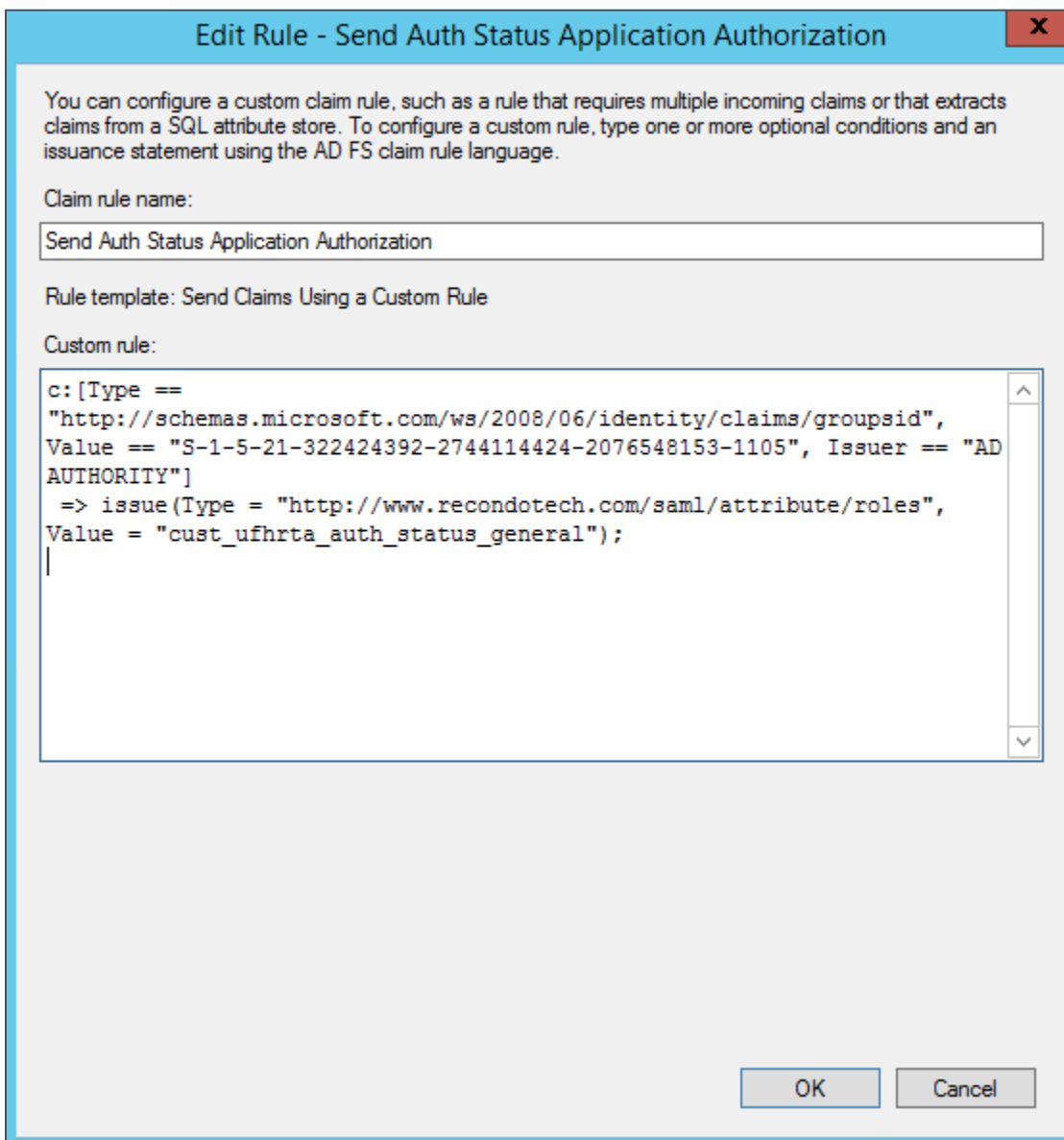
OK Cancel

10. Edit Claim Rules for Relying Party

- a. Send Auth Status Application Authorization.
- b. Set Rule template: **Send Claims Using a Custom Rule.**
- c. Set Claim rule name: **Send Auth Status Application Authorization.**
- d. Custom rule requires a **groupsid**; see the [How to get a groupsid](#) section for how to use it in this rule.
- e. Set Custom rule:


```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-21-322424392-2744114424-2076548153-1105", Issuer == "AD AUTHORITY"]

=> issue(Type = "http://www.recondotech.com/saml/attribute/roles", Value = "cust_ufhrta_auth_status_general");
```
- f. Click the **OK** button.



Edit Rule - Send Auth Status Application Authorization [X]

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 Auth Status Application Authorization

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value == "S-1-5-21-322424392-2744114424-2076548153-1105", Issuer == "AD
AUTHORITY"]
=> issue(Type = "http://www.recondotech.com/saml/attribute/roles",
Value = "cust_ufhrta_auth_status_general");
```

OK Cancel

How to get a groupsid

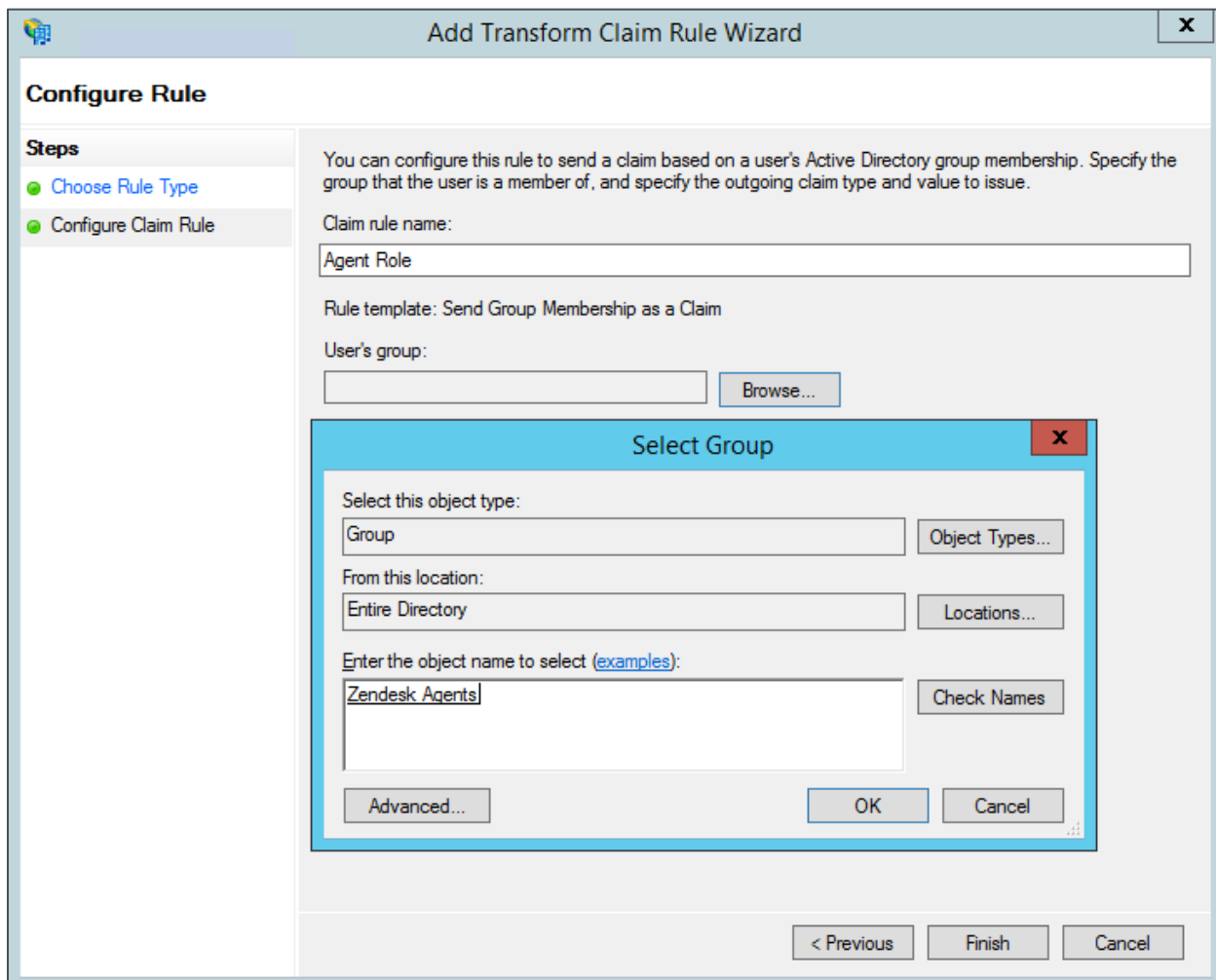
Note: Most of this section was copied from:

<https://support.zendesk.com/hc/en-us/articles/203663896-Mapping-attributes-from-Active-Directory-with-ADFS-and-SAML>

Setting the role of a user based on their membership in a group is a two-step process. First, you create a new rule using the **Send Group Membership as a Claim** template. Second, you modify the definition generated by that rule slightly to create a custom rule that correctly passes the information to Zendesk.

To create the group membership rule and get the groupsid:

1. Add a new rule and **Select Send Group Membership as a Claim** for the template.
2. Locate the group that you wish to map to the role by using the **Browse** button.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.

Claim rule name:
Agent Role

Rule template: Send Group Membership as a Claim

User's group:
Browse...

Select Group

Select this object type:
Group Object Types...

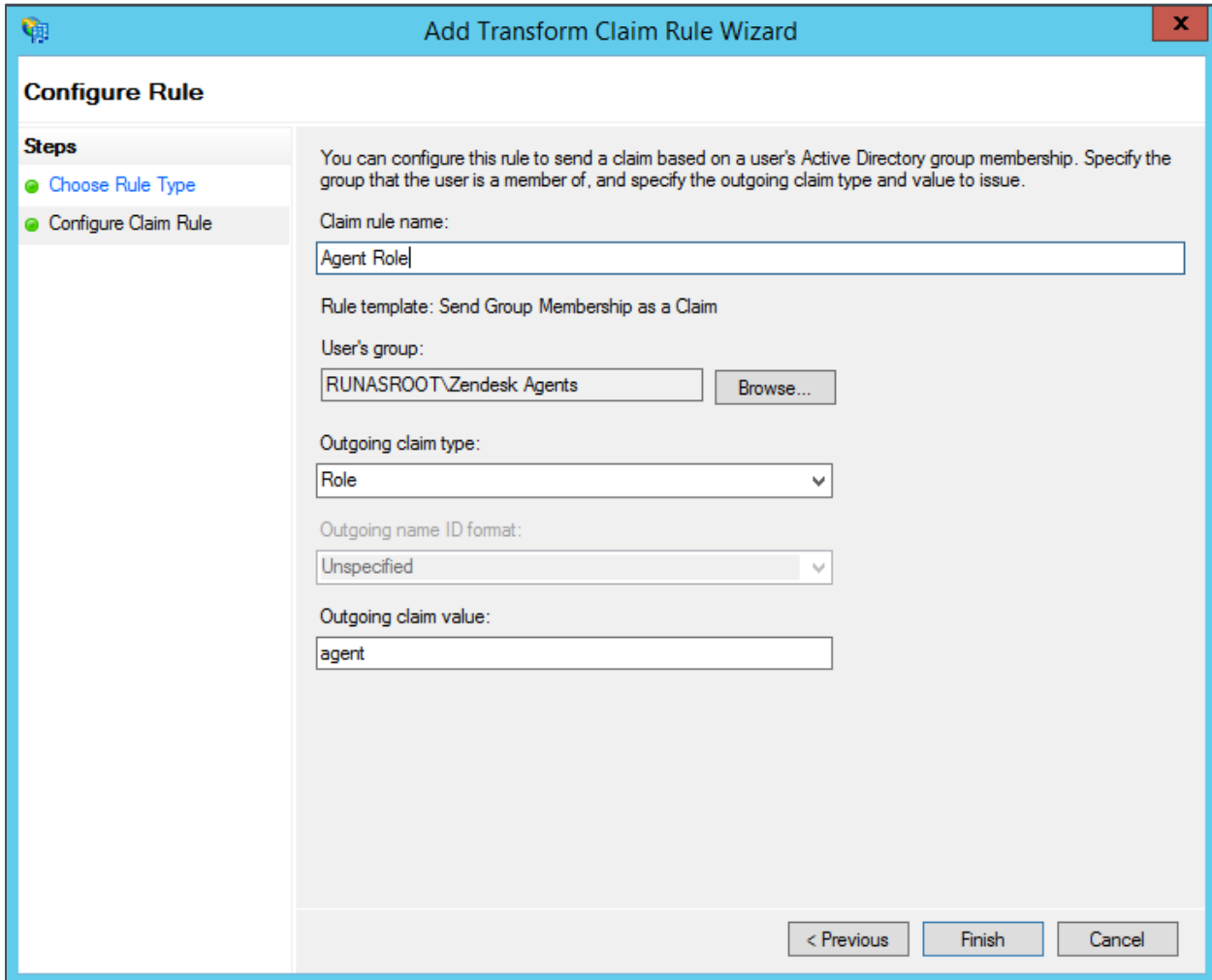
From this location:
Entire Directory Locations...

Enter the object name to select (examples):
Zendesk Agents Check Names

Advanced... OK Cancel

< Previous Finish Cancel

- For **Outgoing claim type**, select **Role**.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.

Claim rule name:
Agent Role

Rule template: Send Group Membership as a Claim

User's group:
RUNASROOT\Zendesk Agents Browse...

Outgoing claim type:
Role

Outgoing name ID format:
Unspecified

Outgoing claim value:
agent

< Previous Finish Cancel

- For **Outgoing claim value**, use test. This rule will be deleted once we get the groupsid so what value we use ultimately does not matter.
- Click **Finish**, then click **Edit Rule** for the rule you just created.

- Use the **View Rule Language** button to get the raw code for the rule. Copy the groupsid value to a location later use. In the example below, the groupsid for the selected group RUNASROOT\Zendesk Agents is:

S-1-5-21-4093502798-4122876194-85005858-1114.

This groupsid will be the value used in the custom claim rules above.

Edit Rule - Agent Role

You can use the following claim rule language to build a custom rule. To do this, copy the text below, create a new custom rule using the Send Claims Using a Custom Rule template, and then paste the text into the Custom Rule text box on the Configure Rule Template page in the Add Rule Wizard.

Claim rule language:

```

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value == "S-1-5-21-4093502798-4122876194-85005858-1114",
Issuer == "AD AUTHORITY"]
=> issue(Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
Value = "agent", Issuer = c.Issuer, OriginalIssuer =
c.OriginalIssuer, ValueType = c.ValueType);

```

OK