SAML SSO Using ADFS for RUX Deployments

Version: April 3, 2025

Table of Contents

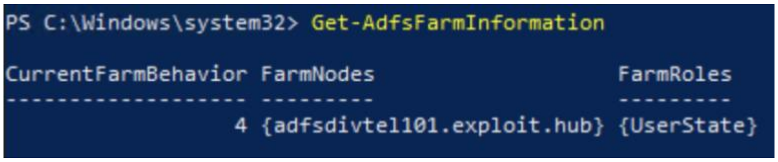
Introduction

This document describes the process to integrate a Vectra Respond UX (RUX) deployment of the Vectra AI platform with Microsoft ADFS to perform Single Sign On (SSO) using SAML 2.0. This was tested using Microsoft ADFS server version 10.

- *Note: SSO may also work on lower versions of Microsoft ADFS supporting SAML 2.0 (i.e. from version ADFS 2.0), but this was not tested by Vectra and is not supported.*

Prerequisites

Verify the version of your Microsoft ADFS server. The "**`CurrentFarmBehavior`**" value must be 3 or 4.
To do so, you can run PowerShell command to get ADFS version: *Get-AdfsFarmInformation*



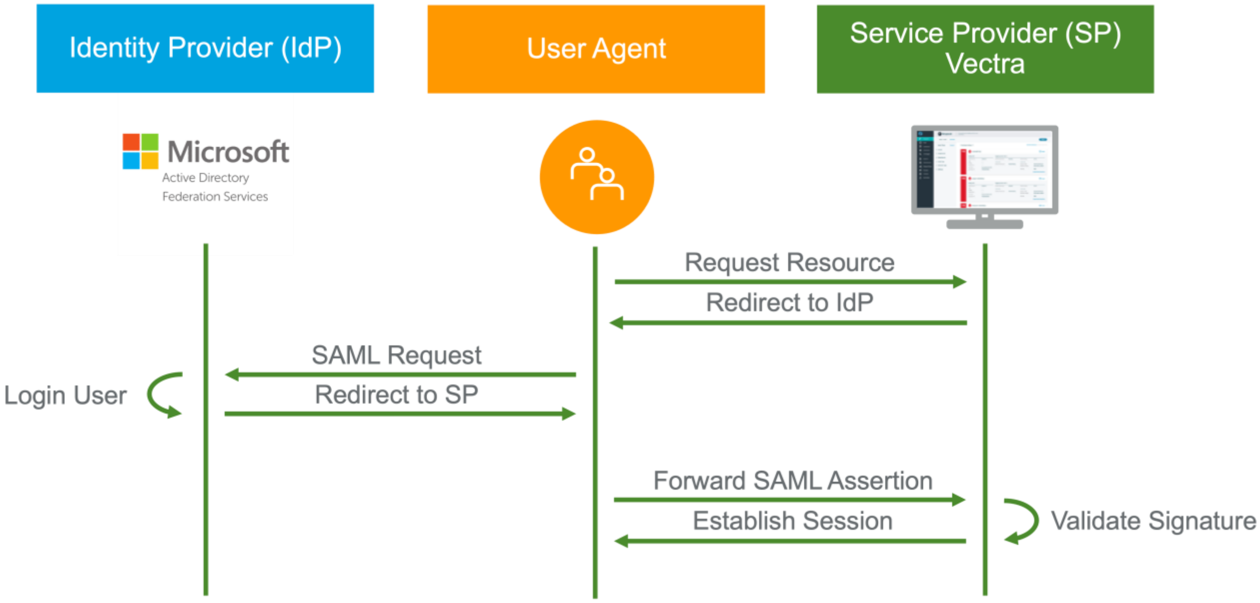
```
PS C:\Windows\system32> Get-AdfsFarmInformation

CurrentFarmBehavior FarmNodes                     FarmRoles
------------------- ---------                     ---------
                  4 {adfsdivtel101.exploit.hub} {UserState}
```

SSL Requirements

Respond UX requires that the SSL Certificate of the ADFS server be publicly signed to allow for certificate validation.

SAML Authentication Workflow with ADFS

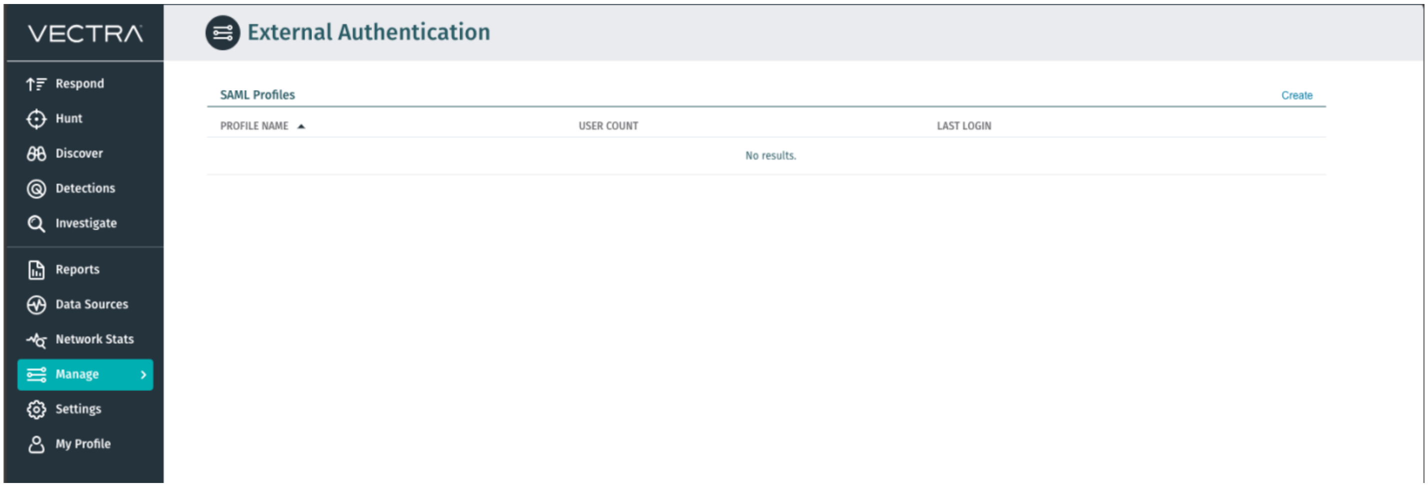


Configuring ADFS and Vectra

1. Get SAML Profile Information for ADFS

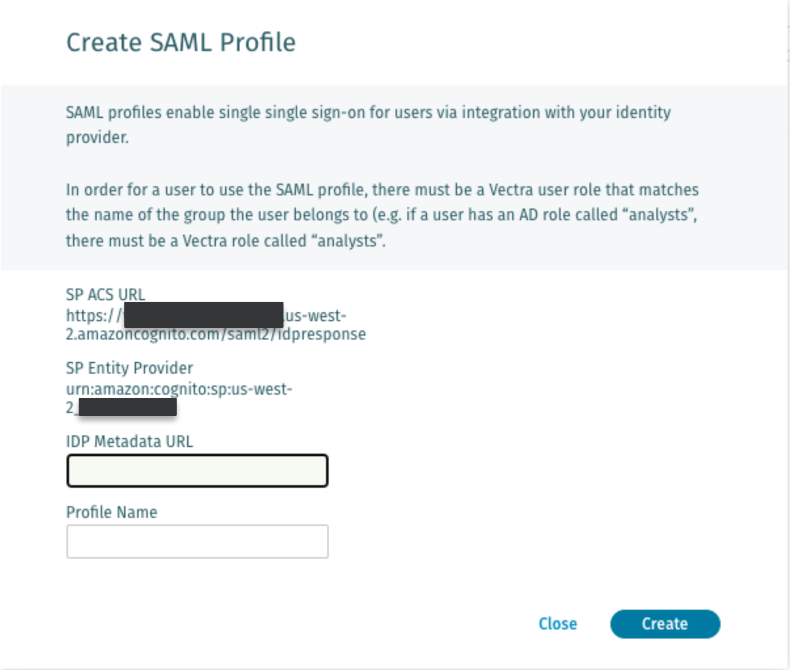
Log in to your RUX Vectra UI as you normally do and navigate to ***Manage > External Authentication***.

Click on "***Create***" in the ***SAML Profiles*** section.



PROFILE NAME	USER COUNT	LAST LOGIN
No results.		

A dialog will open with the following information: ***SP Entity Identifier*** and ***SP ACS URL***.



Create SAML Profile

SAML profiles enable single single sign-on for users via integration with your identity provider.

In order for a user to use the SAML profile, there must be a Vectra user role that matches the name of the group the user belongs to (e.g. if a user has an AD role called "analysts", there must be a Vectra role called "analysts".

SP ACS URL
https://[redacted]us-west-2.amazoncognito.com/saml2/idpresponse

SP Entity Provider
urn:amazon:cognito:sp:us-west-2[redacted]

IDP Metadata URL

Profile Name

- The SP ACS URL is the Assertion Consumer Service URL. It represents the endpoint on the service provider (Vectra side) where ADFS will redirect the user agent (browser) to with its authentication response. This URL will be of the following format: **https://<Brain URL and AWS Region>.amazoncognito.com/saml2/idpresponse**.
- The SP Entity Provider represents the entity of the Vectra Service Provider.

Click Next. Take note of these data points as they will be needed later to configure the corresponding fields in the ADFS SAML SSO setup flow.

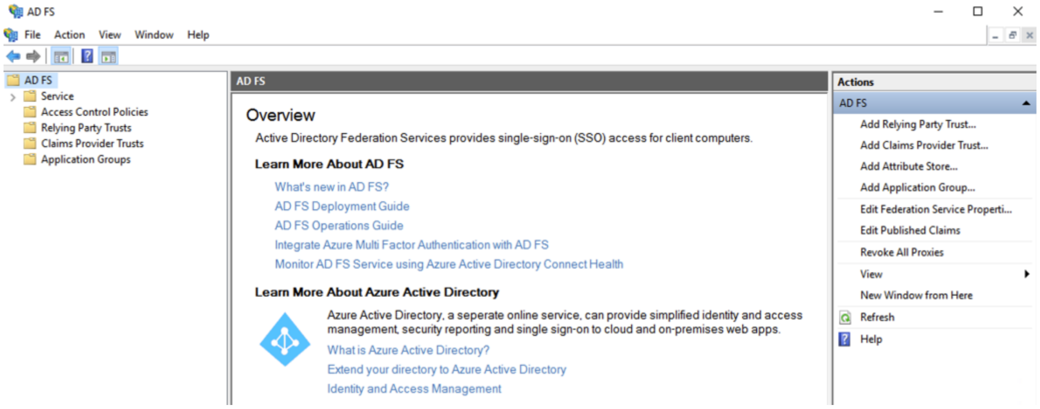
- *Note: If you want a hostname-based entry instead of IP-based for the SP ACS URL and SP Entity Provider, then you should:*
  - Configure this option in Vectra, at *Data Sources > Network > Brain Setup > Brain.*
  - Check the "DNS Name" radio button for the "For linking in alerts/notifications (except AWS SecurityHub)" option instead of the default of “Management IP Address”
  - This will populate the SP entries using hostname instead of IP.
- **Please also note that the "DNS Name" should be in lowercase in this area and any place you see it in ADFS.**

Next, we will configure ADFS with these values.

2. Add a Relying Party Trust

Relying party trust is a term used in ADFS to identify service providers (in our case Vectra) that can communicate with an ADFS endpoint.

Go to **AD FS Management**, select in the left navigation pane **Relying Party Trust**, then on the right navigation pane click **Add Relying Party Trust...**



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Learn More About AD FS

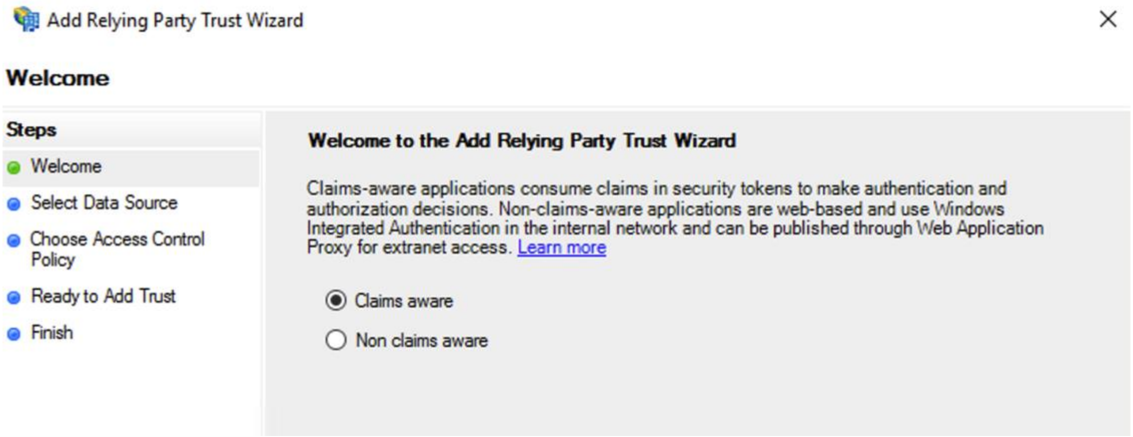
What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

What is Azure Active Directory?
Extend your directory to Azure Active Directory
Identity and Access Management

On the Wizard '**Welcome page**', select the option ***Claim Aware***, then click **Start.**



Welcome

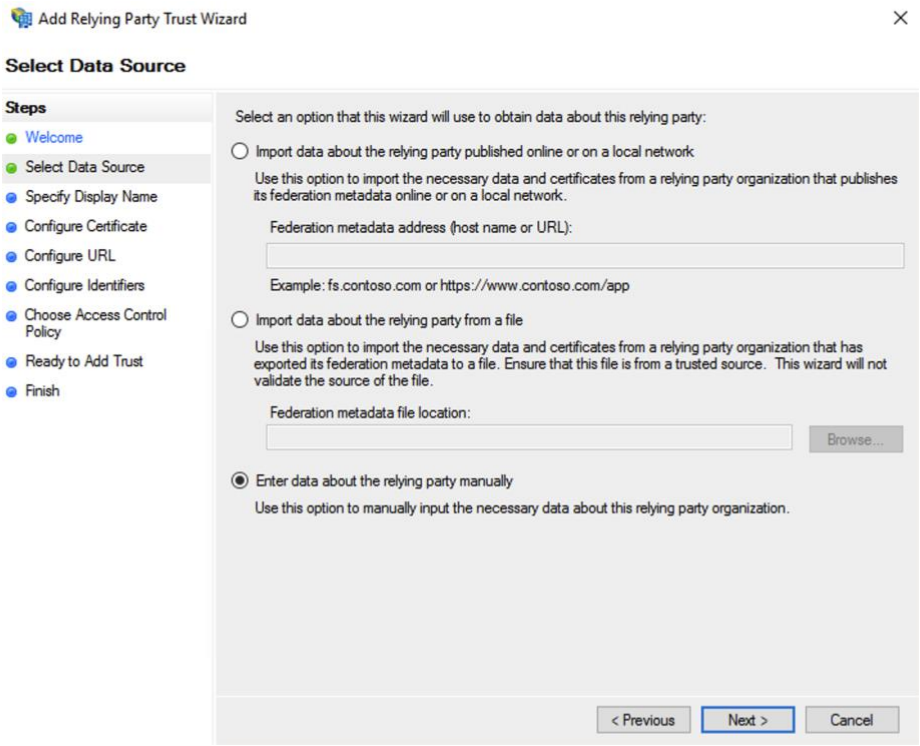
Welcome to the Add Relying Party Trust Wizard

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

Select **Enter data about the relying party manually**, then click **Next.**



Add Relying Party Trust Wizard

Select Data Source

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

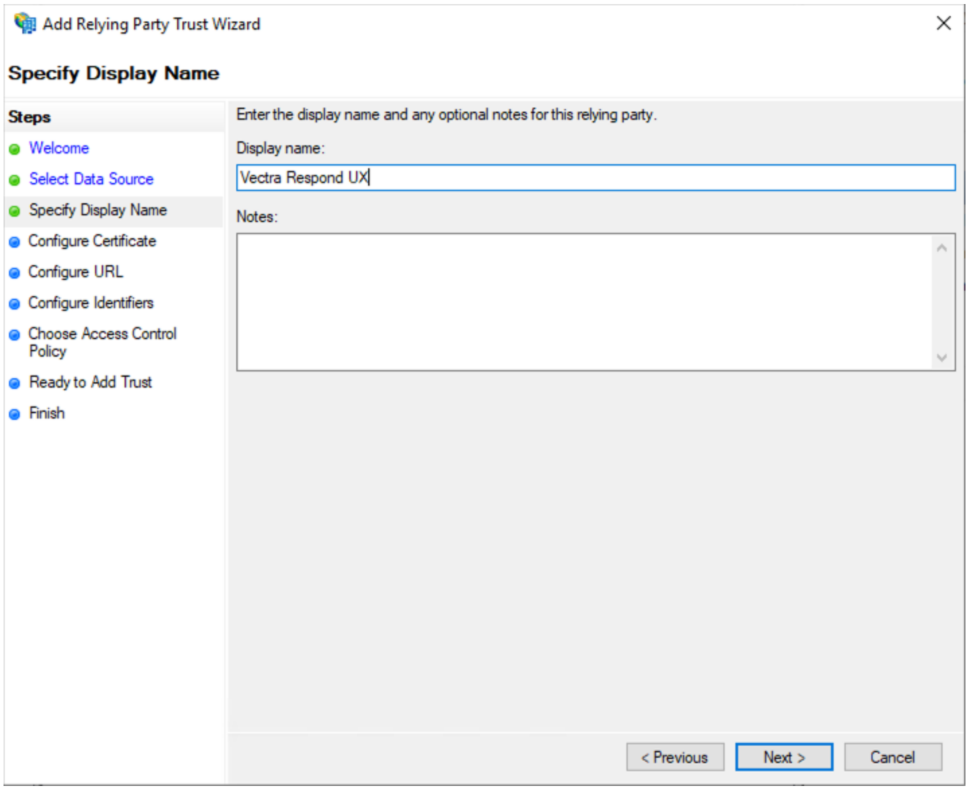
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

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.

Enter a display name (like "***Vectra Respond UX"*** and any optional notes, then click **Next.**



Add Relying Party Trust Wizard

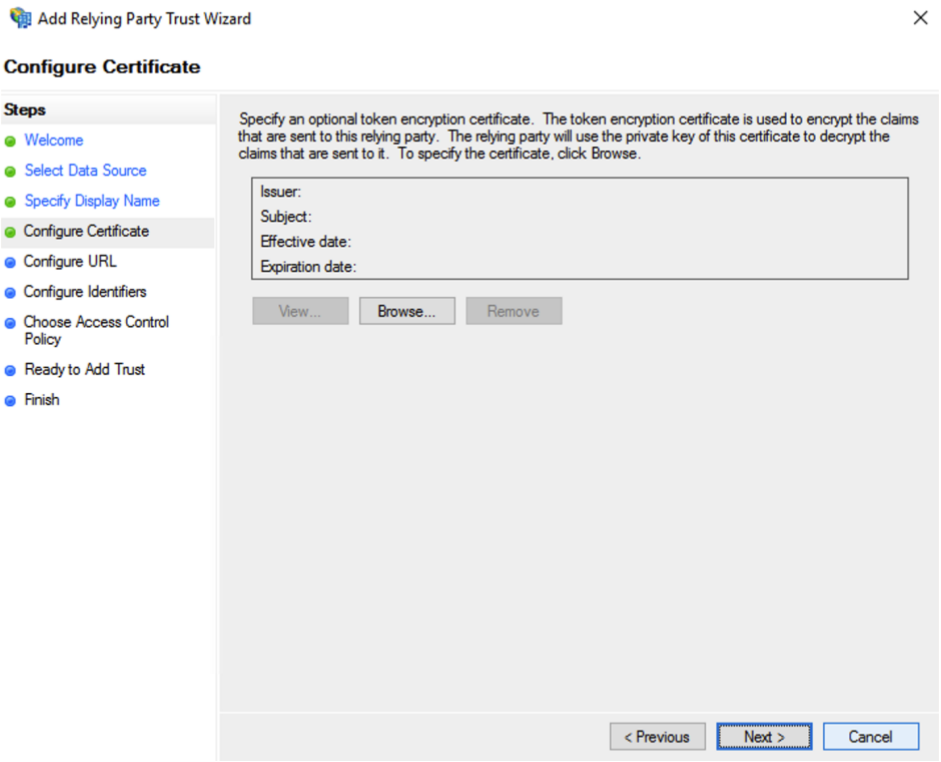
Specify Display Name

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

Display name: Vectra Respond UX

Notes:

Click ***Next*** to accept the defaults for the ***Configure Certificate*** step.

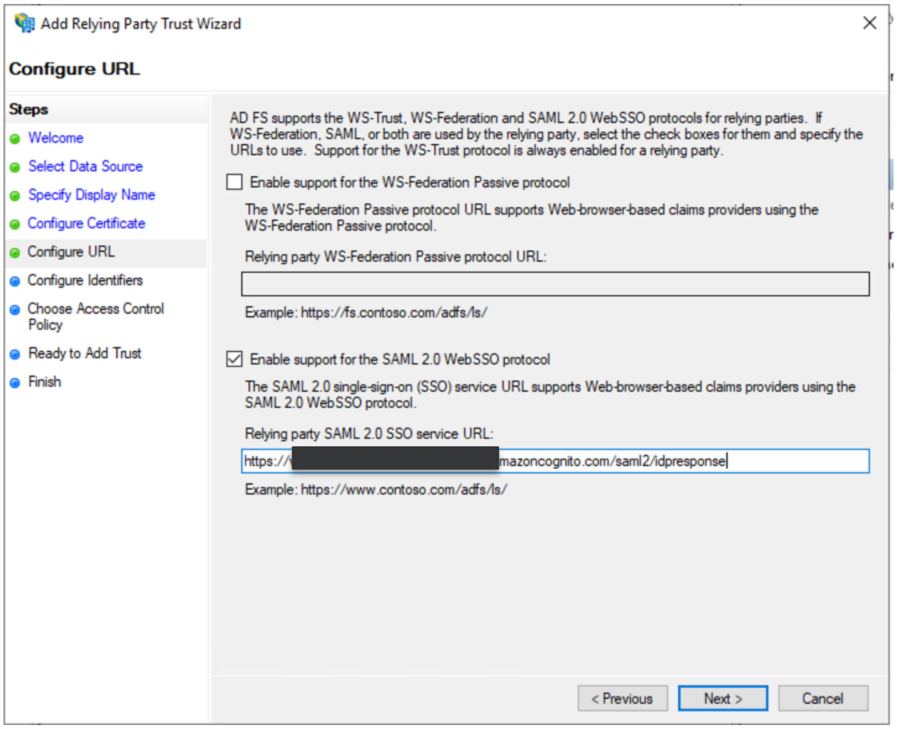


Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

Issuer:
Subject:
Effective date:
Expiration date:

Select ***Enable support for the SAML 2.0 WebSSO Protocol***.
Enter the ***SP ACS URL*** retrieved from Vectra SAML Profile configuration page in Step 1, then click ***Next***.



Configure URL

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.

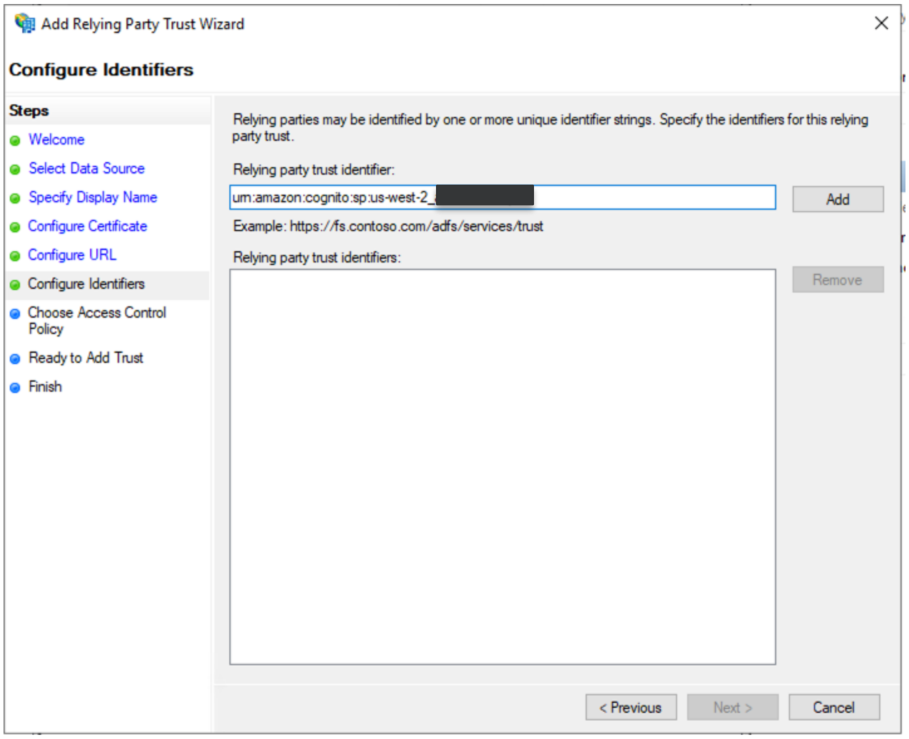
Relying party SAML 2.0 SSO service URL:

https://[redacted]mazoncognito.com/saml2/idpresponse

Example: https://www.contoso.com/adfs/ls/

© 2025 Vectra AI, Inc.

In the ***Relay party trust identifier***, enter the ***SP Entity Provider*** retrieved from Vectra SAML Profile configuration page in Step 1. Click ***Add***, then Click ***Next***.



Add Relying Party Trust Wizard

Configure Identifiers

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- 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.

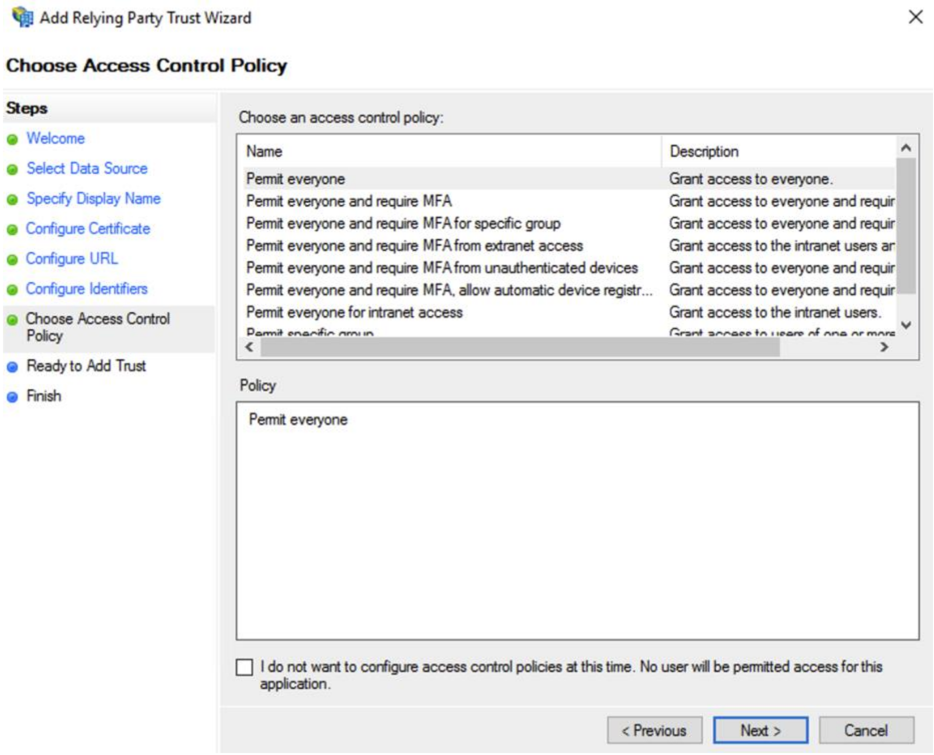
Relying party trust identifier:

urn:amazon:cognito:sp:us-west-2_[redacted]

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

Relying party trust identifiers:

Select ***Permit Everyone*** (or other access control policy of your choice), then click ***Next***.



Add Relying Party Trust Wizard

Choose Access Control Policy

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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 requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

No changes are needed for the **Ready to Add Trust** section. Click ***Next***.

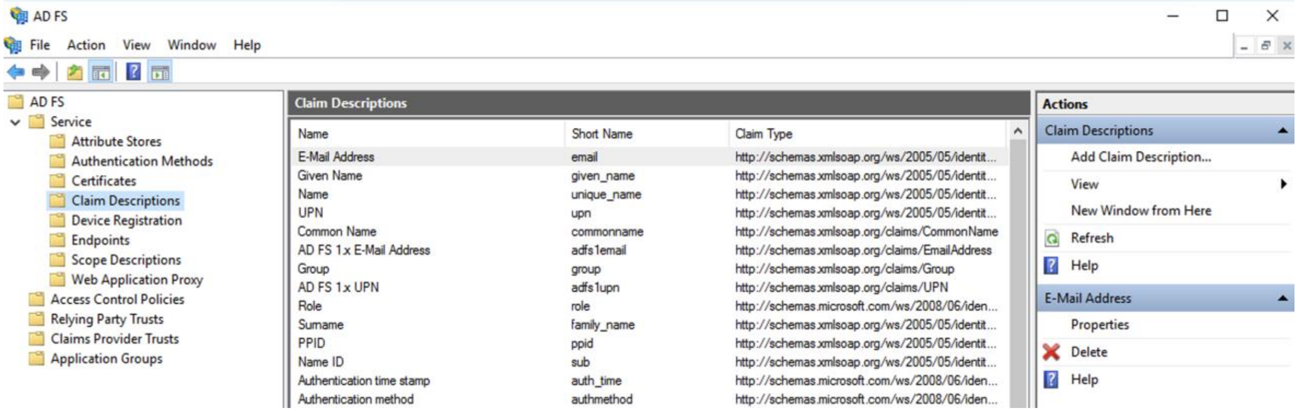
At the Finish screen, uncheck **Configure claims issuance policy for this application,** then click ***Close***.

Next, we will configure custom attributes to use as a claims.

3. Add a Claim Description

Claim descriptions will allow us to create a custom attribute that will be sent by ADFS in its SAML response. In our case, we need to create attributes corresponding to standardized name of a Vectra role, email address, and name, so that Vectra can then give the right permissions associated to the role indicated in the SAML response. Thus, once authenticated, users are assigned by Vectra the application role defined in the ADFS.

Go to **AD FS Management**, select **Service** from the left navigation pane then **Claim Descriptions**.
Click **Add Claim Description...** on the right navigation pane and add new claims for role, emailaddress, and name.



Claim Descriptions

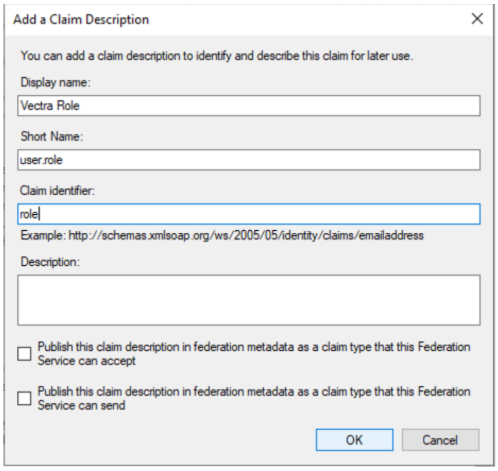
Name	Short Name	Claim Type
E-Mail Address	email	http://schemas.xmlsoap.org/ws/2005/05/identit...
Given Name	given_name	http://schemas.xmlsoap.org/ws/2005/05/identit...
Name	unique_name	http://schemas.xmlsoap.org/ws/2005/05/identit...
UPN	upn	http://schemas.xmlsoap.org/ws/2005/05/identit...
Common Name	commonname	http://schemas.xmlsoap.org/claims/CommonName
AD FS 1.x E-Mail Address	adfs1email	http://schemas.xmlsoap.org/claims/EmailAddress
Group	group	http://schemas.xmlsoap.org/claims/Group
AD FS 1.x UPN	adfs1upn	http://schemas.xmlsoap.org/claims/UPN
Role	role	http://schemas.microsoft.com/ws/2008/06/iden...
Surname	family_name	http://schemas.xmlsoap.org/ws/2005/05/identit...
PPID	ppid	http://schemas.xmlsoap.org/ws/2005/05/identit...
Name ID	sub	http://schemas.xmlsoap.org/ws/2005/05/identit...
Authentication time stamp	auth_time	http://schemas.microsoft.com/ws/2008/06/iden...
Authentication method	authmethod	http://schemas.microsoft.com/ws/2008/06/iden...

Enter a **Display name** like “***Vectra Role***”.

then enter the **Short Name** “***user.assignedrole***”.

then enter the **Claim Type** "***role***".

Finally leave the two **Publish**… boxes unchecked and finish by clicking ***Ok.***



You can add a claim description to identify and describe this claim for later use.

Display name: Vectra Role

Short Name: user.role

Claim identifier: role

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Description:

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

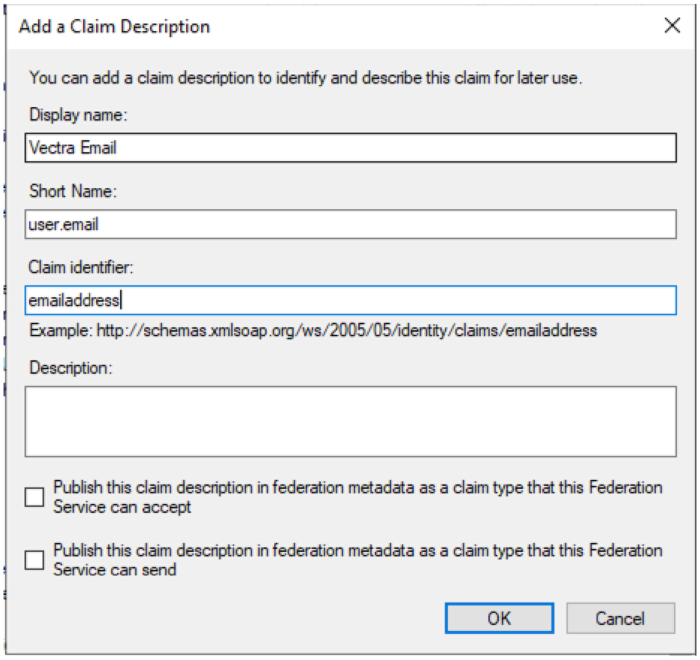
☐ Publish this claim description in federation metadata as a claim type that this Federation Service can send

Enter a **Display name** like “***Vectra Email***”.

then enter the **Short Name** “***user.email***”.

then enter the **Claim Type** "***emailaddress***".

Finally leave the two **Publish**… box unchecked and finish by clicking “OK”.



Add a Claim Description

You can add a claim description to identify and describe this claim for later use.

Display name: Vectra Email

Short Name: user.email

Claim identifier: emailaddress

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Description:

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

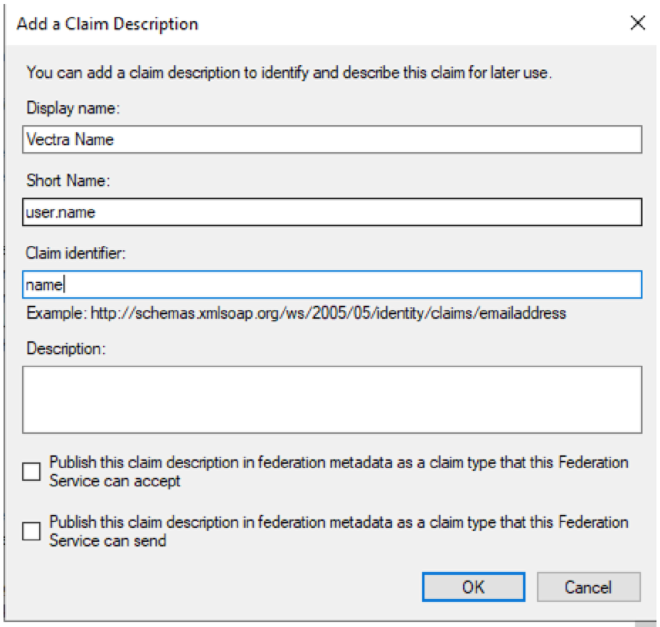
□ Publish this claim description in federation metadata as a claim type that this Federation Service can send

Enter a **Display name** like “***Vectra Name***”.

then enter the **Short Name** “***user.name***”.

then enter the **Claim Type** "***name***".

Finally leave the two **Publish**… boxes unchecked and finish by clicking “OK”.



Add a Claim Description

You can add a claim description to identify and describe this claim for later use.

Display name: Vectra Name

Short Name: user.name

Claim identifier: name

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Description:

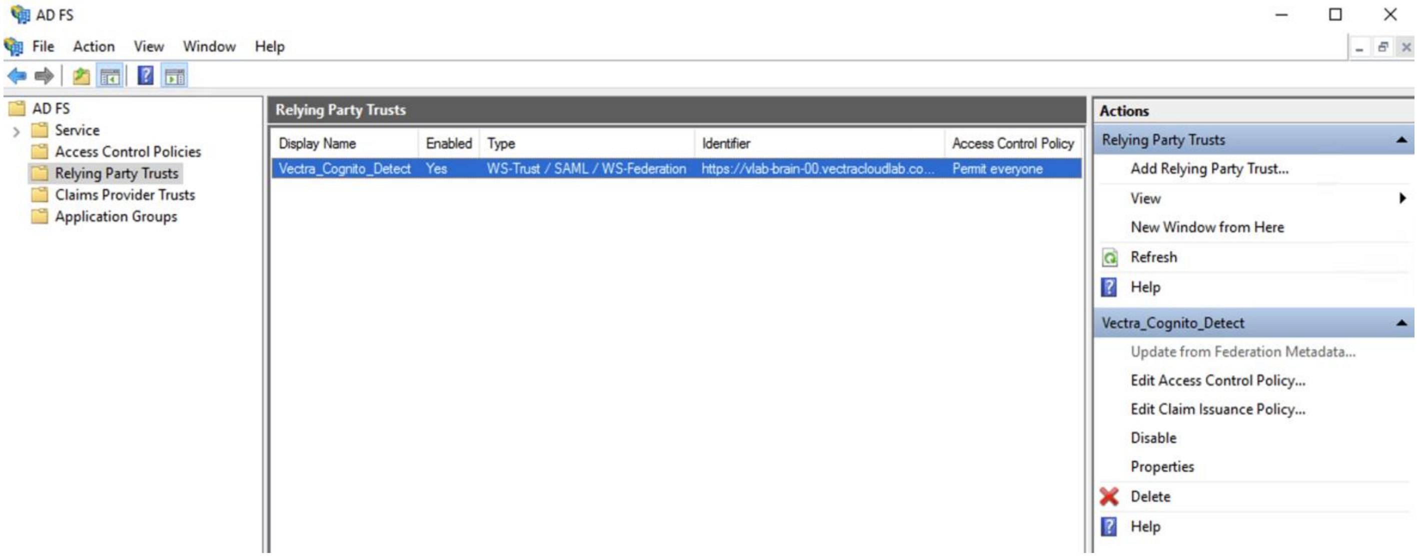
□ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

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

4. Add Rules Claim

In ADFS, the Claims Issuance Policy defines what pieces of information about a user go where in a claim.

To define it, go to **AD FS Management**, select **Relying Party Trusts** from the left navigation pane then **Edit Claim Issuance Policy…** from right navigation pane.

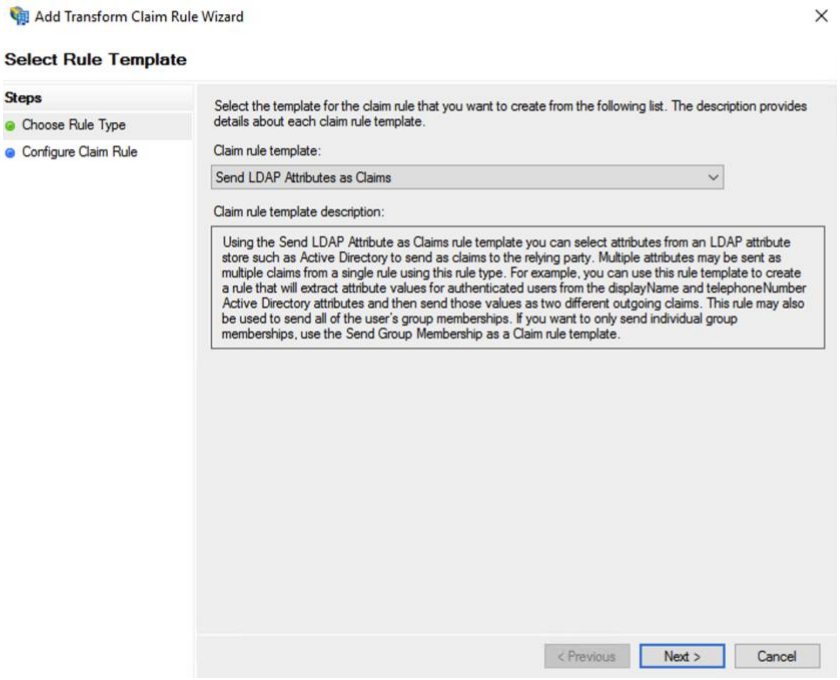


Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Vectra_Cognito_Detect	Yes	WS-Trust / SAML / WS-Federation	https://vlab-brain-00.vectracloudlab.co...	Permit everyone

a. Add the SSO rule Claim

Select ***Send LDAP Attributes as a Claim***, then click ***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:

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.

Enter a **Claim rule name** like ***Vectra Respond UX.***

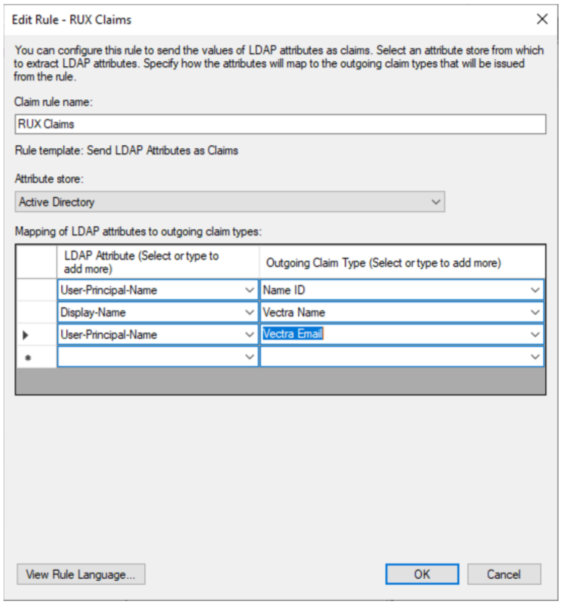
Then select ***Active Directory*** **Attribute Store.**

Then select ***User-Principal-Name*** as **LDAP Attribute** and map it to ***Name ID*** as **Outgoing Claim Type.**

Then select ***User-Principal-Name*** as **LDAP Attribute** and map it to ***Vectra Email*** as **Outgoing Claim Type.**

Then select ***Display-Name*** as **LDAP Attribute** and map it to ***Vectra Name*** as **Outgoing Claim Type.**

- *Note: The "User-Principal-Name" contains the value of the email address of the user. The "Name ID" outgoing claim should always be present to ensure correct session handling and can be seen as the login field in SAML.*



Edit Rule - RUX Claims

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: RUX Claims

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

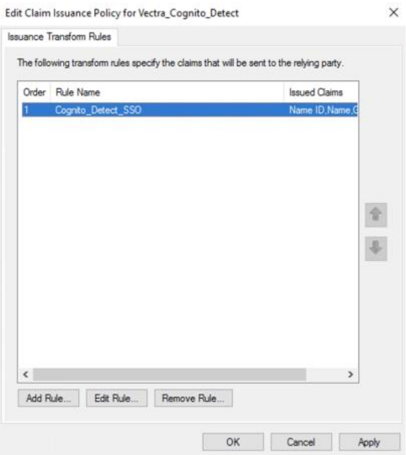
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	Name ID
	Display-Name	Vectra Name
▸	User-Principal-Name	Vectra Email
*		

b. Add Role rule Claim

Now, go to Edit Claim Issuance Policy window to create a 2nd claim rule, which will map the AD group to the standardized Vectra role name. This will map to a role (and permissions) defined on the Vectra Brain.

Add a new rule Claim ***Add Rule…***



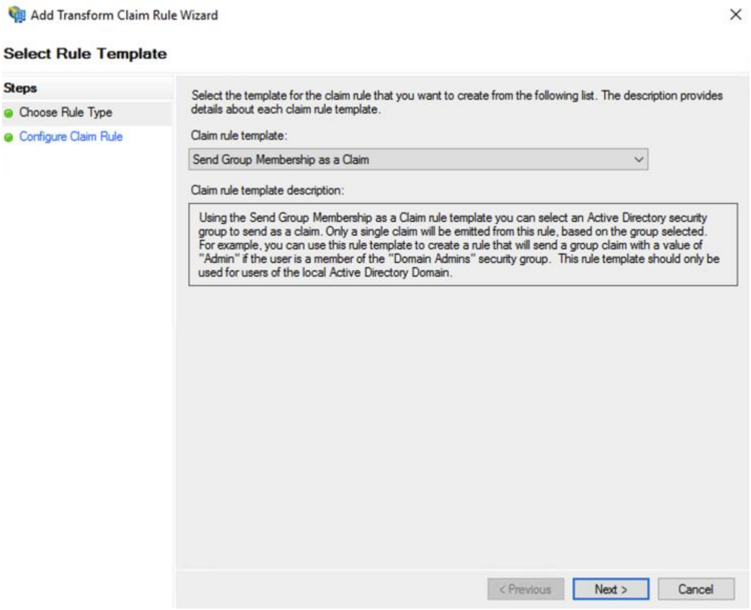
Edit Claim Issuance Policy for Vectra_Cognito_Detect

Issuance Transform Rules

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

Order	Rule Name	Issued Claims
1	Cognito_Detect_SSO	Name ID,Name,G

Select ***Send Group Membership as a Claim***, then click ***Next.***



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:

Send Group Membership as a Claim

Claim rule template description:

Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this rule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.

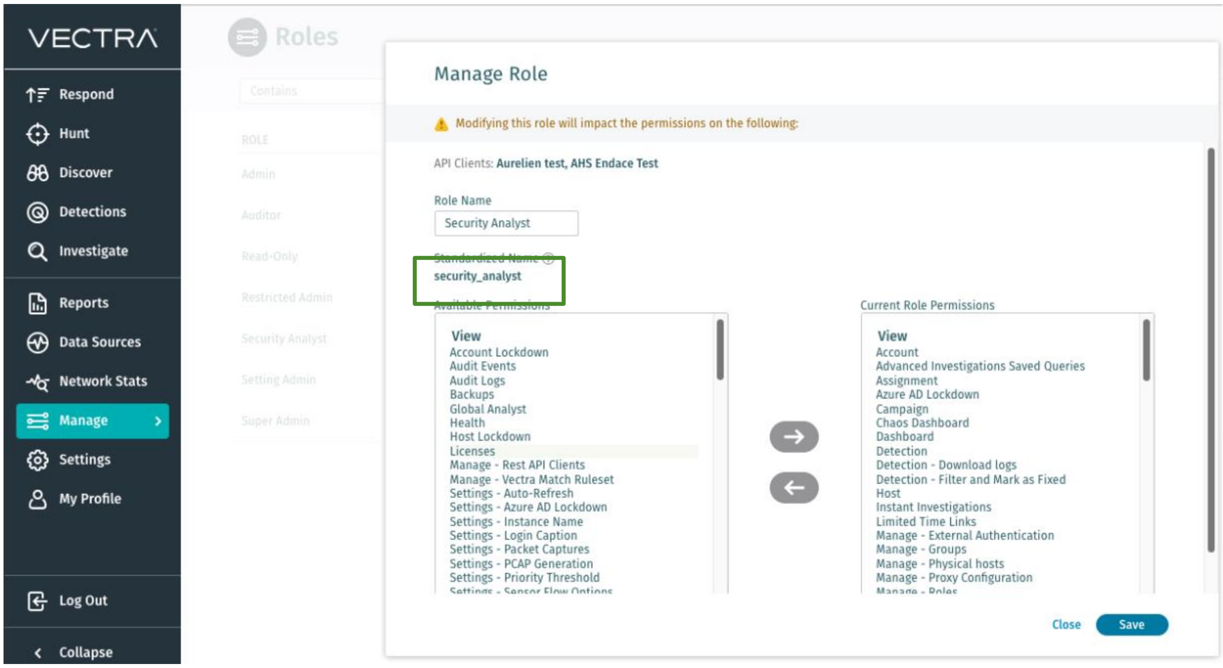
Enter a **Claim rule name.**

Browse the Active Directory and select the group to map.

Select the **Outgoing claim type** newly created ***Vectra Role*** in our example.

Then, we need to indicate the **Outgoing claim value** which will be the standardized name of your role to be assigned. To find this value, go back in your Vectra tab, navigate to the ***Manage > Roles*** screen.

Click on each role that your SAML users will be using and make note of the specific **Standardized Name** for each role. For example, the Security Analyst role has a Standardized name of "***security_analyst***".



Manage Role

⚠ Modifying this role will impact the permissions on the following:

API Clients: Aurelien test, AHS Endace Test

Role Name: Security Analyst

Standardized Name: security_analyst

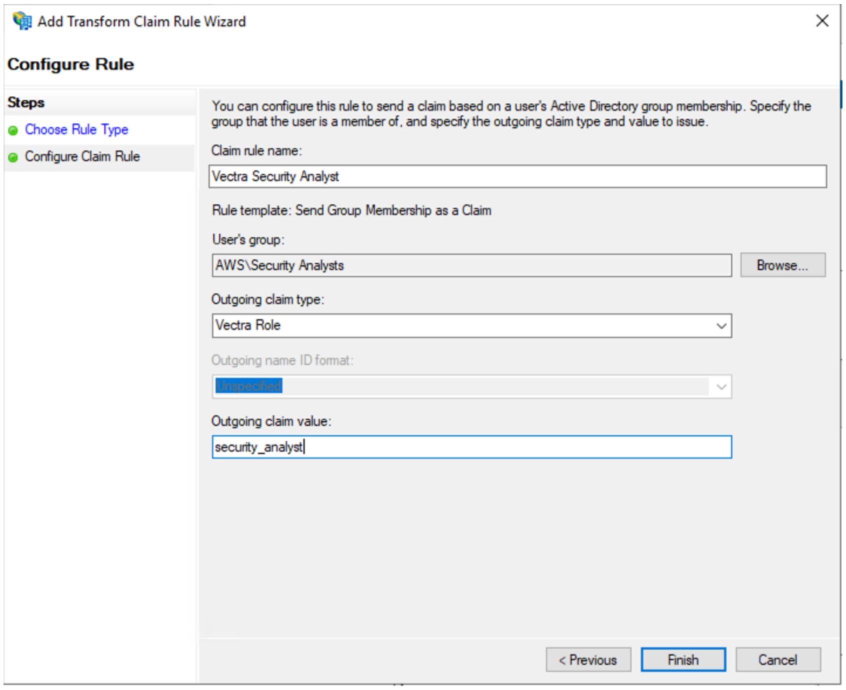
Available Permissions

View
Account Lockdown
Audit Events
Audit Logs
Backups
Global Analyst
Health
Host Lockdown
Licenses
Manage - Rest API Clients
Manage - Vectra Match Ruleset
Settings - Auto-Refresh
Settings - Azure AD Lockdown
Settings - Instance Name
Settings - Login Caption
Settings - Packet Captures
Settings - PCAP Generation
Settings - Priority Threshold
Settings - Sensor Flow Options

Current Role Permissions

View
Account
Advanced Investigations Saved Queries
Assignment
Azure AD Lockdown
Campaign
Chaos Dashboard
Dashboard
Detection
Detection - Download logs
Detection - Filter and Mark as Fixed
Host
Instant Investigations
Limited Time Links
Manage - External Authentication
Manage - Groups
Manage - Physical hosts
Manage - Proxy Configuration
Manage - Roles

Enter the specific **Standardized Vectra Role Name** to map then click ***Finish.***



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: Vectra Security Analyst

Rule template: Send Group Membership as a Claim

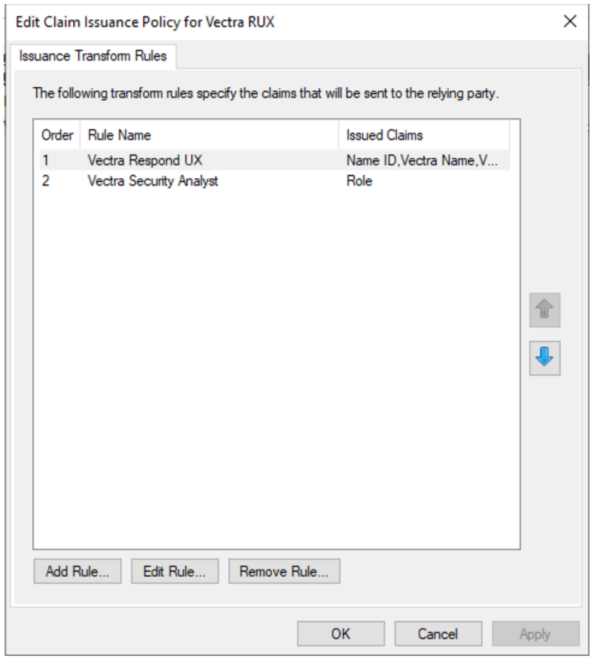
User's group: AWS\Security Analysts

Outgoing claim type: Vectra Role

Outgoing name ID format: Unspecified

Outgoing claim value: security_analyst

- *Note: for each role assignment a rule needs to be created.*



Edit Claim Issuance Policy for Vectra RUX

Issuance Transform Rules

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

Order	Rule Name	Issued Claims
1	Vectra Respond UX	Name ID,Vectra Name,V...
2	Vectra Security Analyst	Role

- *Note: Please ensure the users are only mapped to one Vectra Role in the IdP.*
    - *If a user is mapped to more than 1 role, the user may not be assigned the preferred role.*

5. Create SAML Profile

SAML metadata is an XML document which contains information necessary for interaction with SAML-enabled identity or service providers. The document contains e.g. URLs of endpoints, information about supported bindings, identifiers and public keys.

Use the following URL for the IDP Metadata URL (this must be reachable from your Vectra RUX instance):

https://adfs_server.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

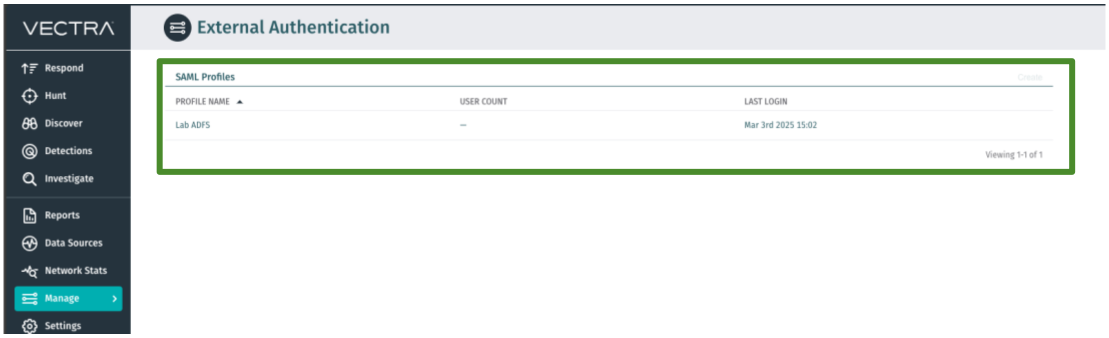
Open a new browser tab and log in to your Vectra UI as you normally do and navigate to ***Manage > External Authentication.***

Click on “***Create***” in the ***SAML Profiles*** section.

A dialog will open with the ***SP Entity Identifier*** and ***SP ACS URL*** will be displayed there.

Input the URL for the ***ADFS federation metadata xml.***

And finally add the **Profile Name** like ***ADFS***, then click ***Create.***



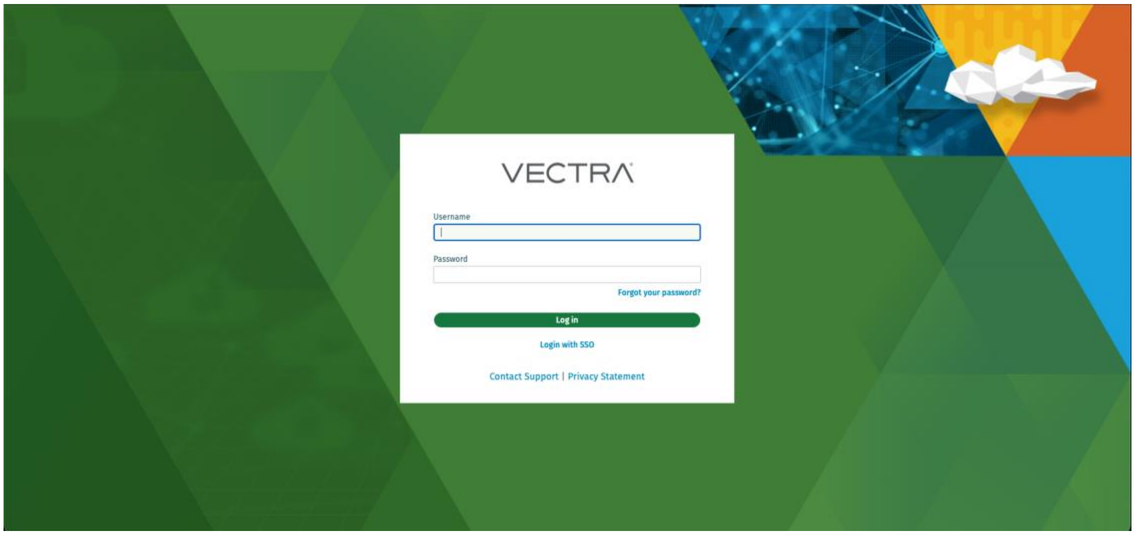
SAML Profiles

PROFILE NAME ▲	USER COUNT	LAST LOGIN
Lab ADFS	–	Mar 3rd 2025 15:02

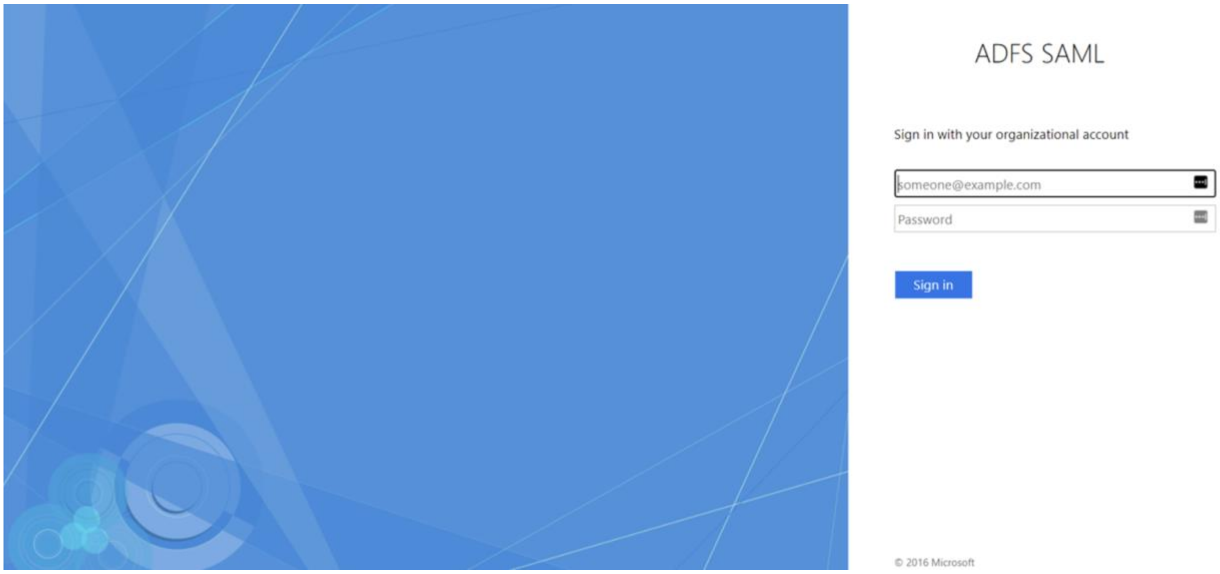
Viewing 1-1 of 1

6. Test your new SAML Single Sign-On Functionality

The Respond URL you have been previously using now works with SAML SSO when a user clicks the “Login with SSO” link.



They will then be redirected to the ADFS login page:

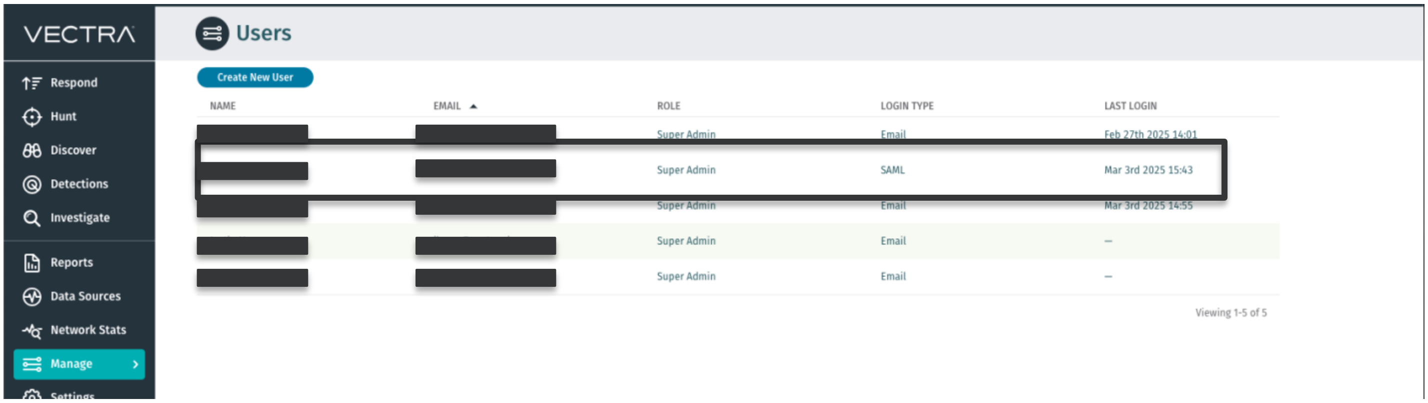


ADFS SAML

Sign in with your organizational account

Once connected, the user has access to the Vectra UI with the proper permissions of their role.

Users logged in with SAML are listed in ***Manage > Users*** screen with prefix **SAML.**



NAME	EMAIL ▲	ROLE	LOGIN TYPE	LAST LOGIN
[redacted]	[redacted]	Super Admin	Email	Feb 27th 2025 14:01
[redacted]	[redacted]	Super Admin	SAML	Mar 3rd 2025 15:43
[redacted]	[redacted]	Super Admin	Email	Mar 3rd 2025 14:55
[redacted]	[redacted]	Super Admin	Email	–
[redacted]	[redacted]	Super Admin	Email	–

Viewing 1-5 of 5

Note: local authentication can be performed using URL ***https://<Brain URL and AWS region>.portal.vectra.ai/signIn?local=True***

Worldwide Support Contact Information

- Support portal: https://support.vectra.ai
- Email: support@vectra.ai (preferred contact method)
- Additional information: https://www.vectra.ai/support