

# SAML SSO Using ADFS

Version: Dec 30, 2022

## Table of Contents

<b>Introduction</b> .....	<b>2</b>
<b>Prerequisites</b> .....	<b>2</b>
<b>SAML Authentication Workflow with ADFS</b> .....	<b>2</b>
<b>Configuring ADFS and Vectra</b> .....	<b>3</b>
<b>1. Get SAML Profile Information for ADFS</b> .....	<b>3</b>
<b>2. Add a Relying Party Trust</b> .....	<b>4</b>
<b>3. Add a Claim Description</b> .....	<b>9</b>
<b>4. Add Rules Claim</b> .....	<b>10</b>
a. Add the SSO rule Claim.....	11
b. Add Role rule Claim.....	12
<b>5. Create SAML Profile</b> .....	<b>15</b>
<b>6. Test your new SAML Single Sign-On Functionality</b> .....	<b>16</b>
<b>Worldwide Support Contact Information</b> .....	<b>17</b>

## Introduction

This document describes the process to integrate the Cognito Platform (Brain) with Microsoft ADFS to perform Single Sign On (SSO) using SAML 2.0. This was tested using Microsoft ADFS server version 3 or later.

- ▼ *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.*

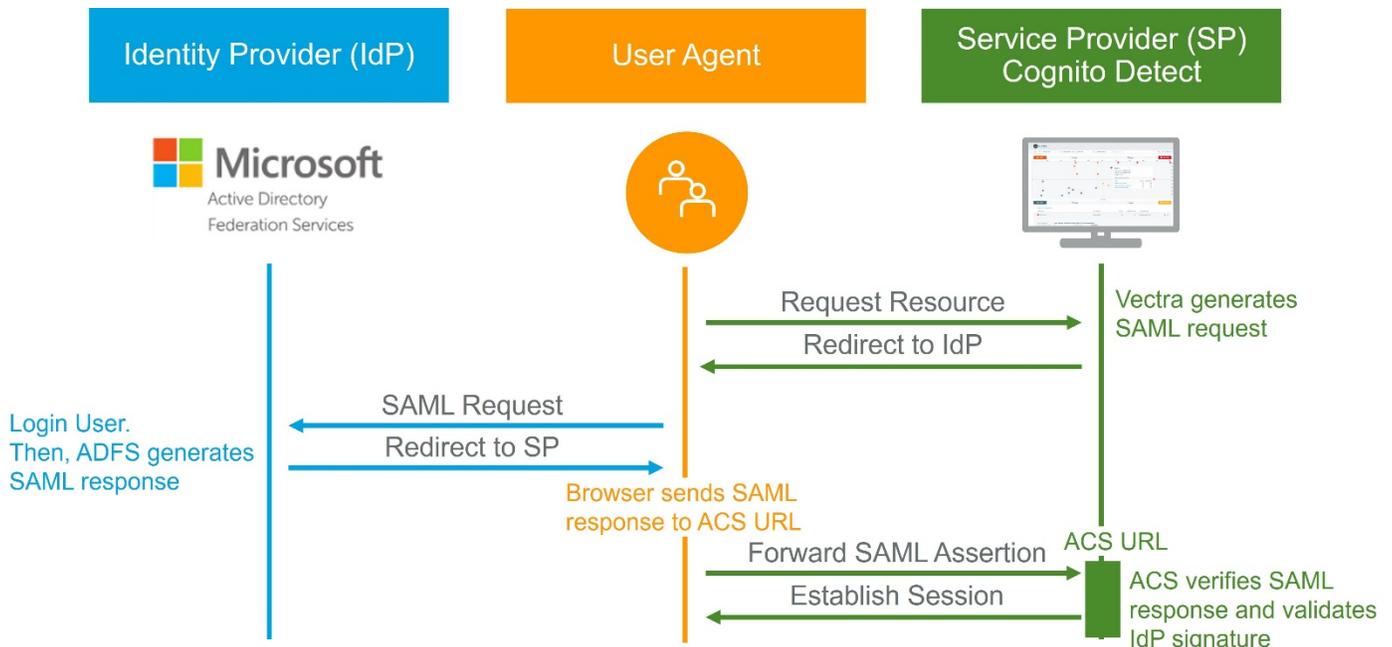
## Prerequisites

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}
```

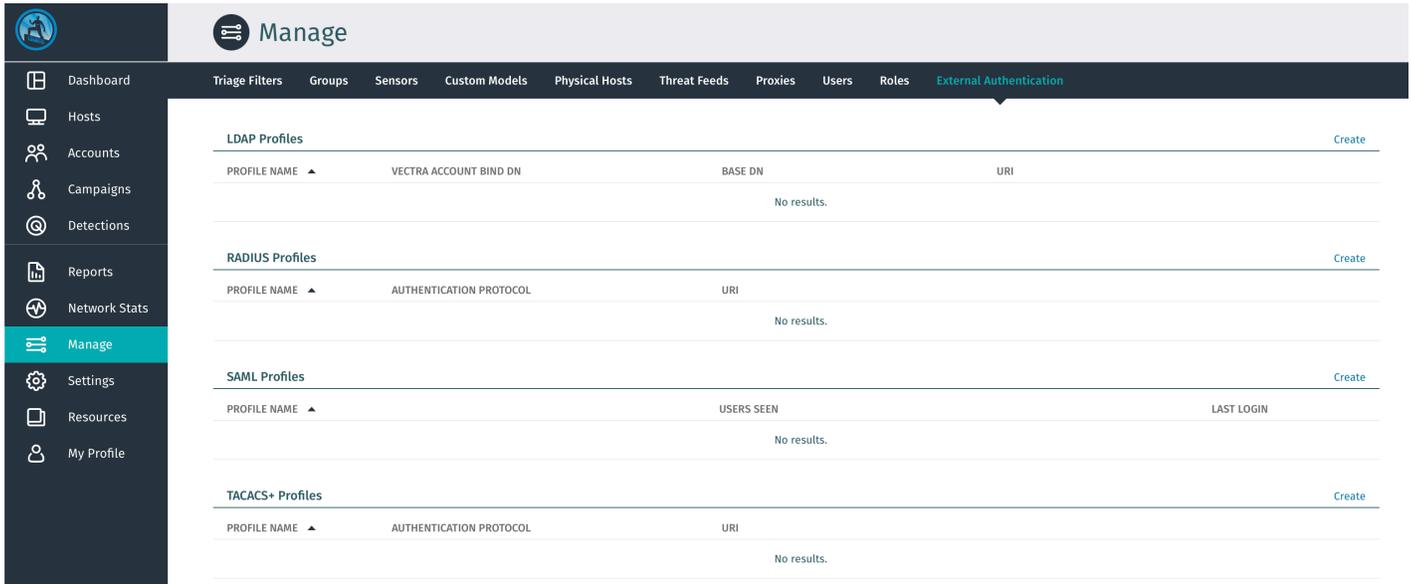
## SAML Authentication Workflow with ADFS



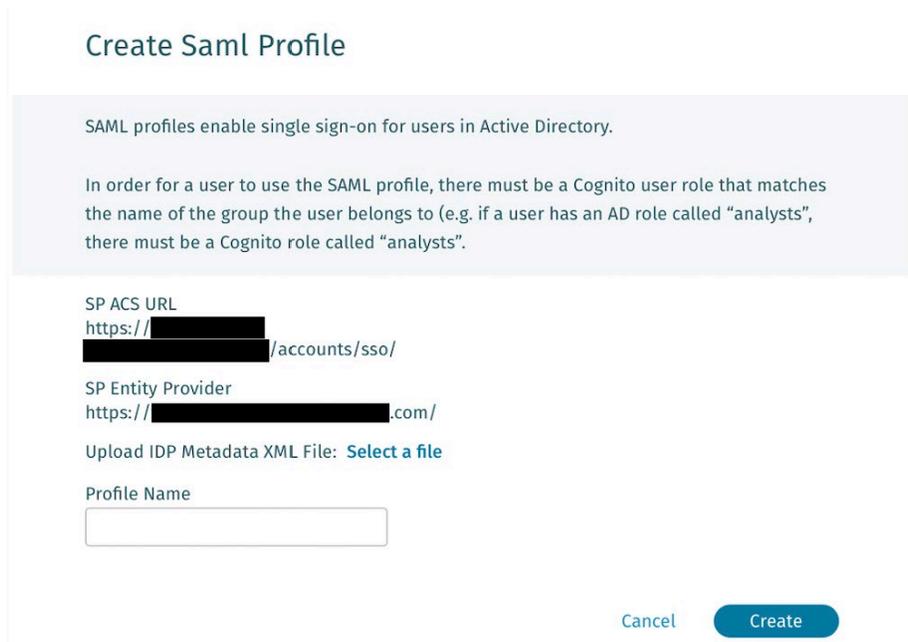
# Configuring ADFS and Vectra

## 1. Get SAML Profile Information for ADFS

Log in to your Cognito Platform (Brain) as you normally do and navigate to **Manage > External Authentication**. Click on **“Create”** in the **SAML Profiles** section.



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



- ▼ The SP ACS URL is the Assertion Consumer Service URL. It represents the endpoint on the service provider (Vectra side) where ADFS will redirect to with its authentication response. This URL will be of the following format: **https://<Vectra Brain IP or FQDN>/accounts/sso/**.

- ▼ The SP Entity Provider represents the entity of the Vectra Service Provider.

Click Next. Take note of these information as they will be needed in the next steps to configure the corresponding fields in the ADFS SAML SSO setup flow.

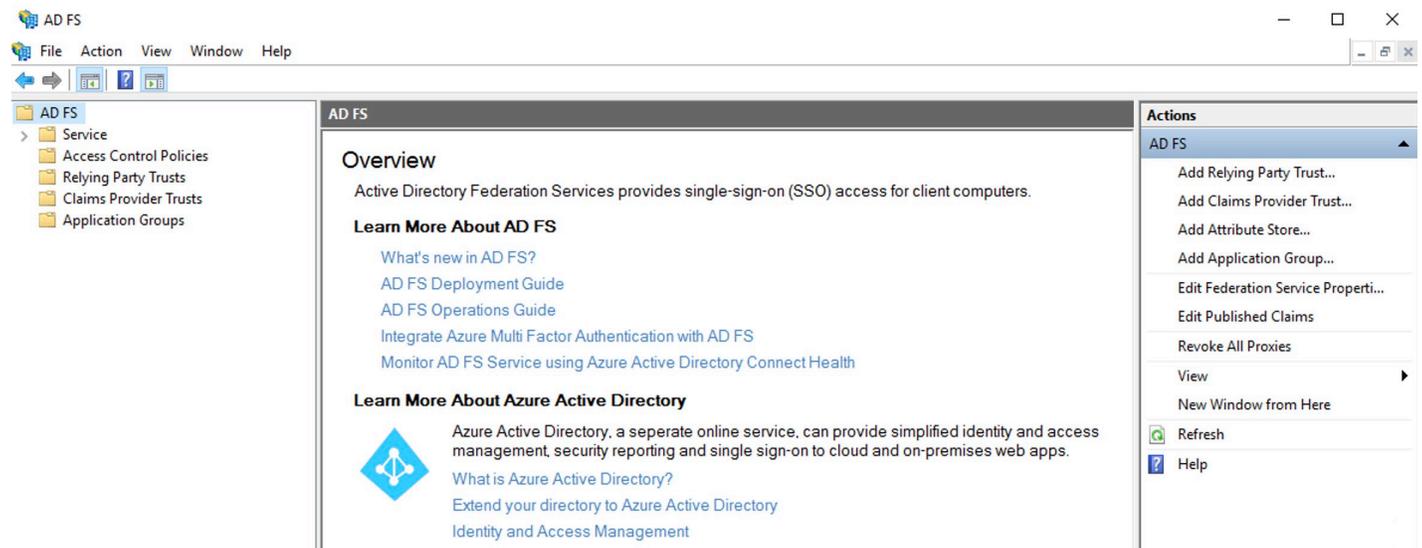
- ▼ *Note: If you want a hostname-based entry instead of IP-based for the SP ACS URL and SP Entity Provider, then you should:*
  - Configure on Vectra the Brain FQDN, in Settings > General > Brain > DNS Name in the Cognito Platform (Brain) UI.
  - Check the "DNS Name" radio button for the "For linking in alerts/notifications (except AWS SecurityHub)" section
  - 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 the 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...**



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

Add Relying Party Trust Wizard ✕

### Welcome

Steps	Content
<ul style="list-style-type: none"> <li><span style="color: green;">●</span> Welcome</li> <li><span style="color: blue;">●</span> Select Data Source</li> <li><span style="color: blue;">●</span> Choose Access Control Policy</li> <li><span style="color: blue;">●</span> Ready to Add Trust</li> <li><span style="color: blue;">●</span> Finish</li> </ul>	<p><b>Welcome to the Add Relying Party Trust Wizard</b></p> <p>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. <a href="#">Learn more</a></p> <p> <input checked="" type="radio"/> Claims aware  <input type="radio"/> Non claims aware         </p>

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

Add Relying Party Trust Wizard ✕

### Select Data Source

Steps	Content
<ul style="list-style-type: none"> <li><span style="color: green;">●</span> Welcome</li> <li><span style="color: green;">●</span> Select Data Source</li> <li><span style="color: blue;">●</span> Specify Display Name</li> <li><span style="color: blue;">●</span> Configure Certificate</li> <li><span style="color: blue;">●</span> Configure URL</li> <li><span style="color: blue;">●</span> Configure Identifiers</li> <li><span style="color: blue;">●</span> Choose Access Control Policy</li> <li><span style="color: blue;">●</span> Ready to Add Trust</li> <li><span style="color: blue;">●</span> Finish</li> </ul>	<p>Select an option that this wizard will use to obtain data about this relying party:</p> <p> <input type="radio"/> 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):  <input type="text"/>            Example: fs.contoso.com or https://www.contoso.com/app         </p> <p> <input type="radio"/> 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:  <input type="text"/> <span style="float: right;">Browse...</span> </p> <p> <input checked="" type="radio"/> Enter data about the relying party manually            Use this option to manually input the necessary data about this relying party organization.         </p> <p style="text-align: right;"> <input style="border: none;" type="button" value=" &lt; Previous "/> <input style="border: none;" type="button" value=" Next &gt; "/> <input style="border: none;" type="button" value=" Cancel "/> </p>

Enter a display name (like “*Vectra\_Cognito\_Detect*”) and any optional notes, then click **Next**

The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. On the left, a 'Steps' list includes: Welcome, Select Data Source, Specify Display Name (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the instruction: 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' text box containing 'Vectra\_Cognito\_Detect' and a 'Notes:' text area. At the bottom, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

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

The screenshot shows the 'Configure Certificate' step of the 'Add Relying Party Trust Wizard'. The 'Steps' list on the left now highlights 'Configure Certificate'. The main area contains the instruction: '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.' Below this, there is a text box with labels for 'Issuer:', 'Subject:', 'Effective date:', and 'Expiration date:'. Underneath the text box are three buttons: 'View...', 'Browse...' (highlighted), and 'Remove'. At the bottom, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

Select **Enable support for the SAML 2.0 WebSSO Protocol**.

Enter the **SP ACS URL** retrieved from Cognito Detect SAML Profile configuration page in Step 1, then click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The wizard has a 'Steps' sidebar on the left with the following items: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main content area contains the following text and controls:

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/

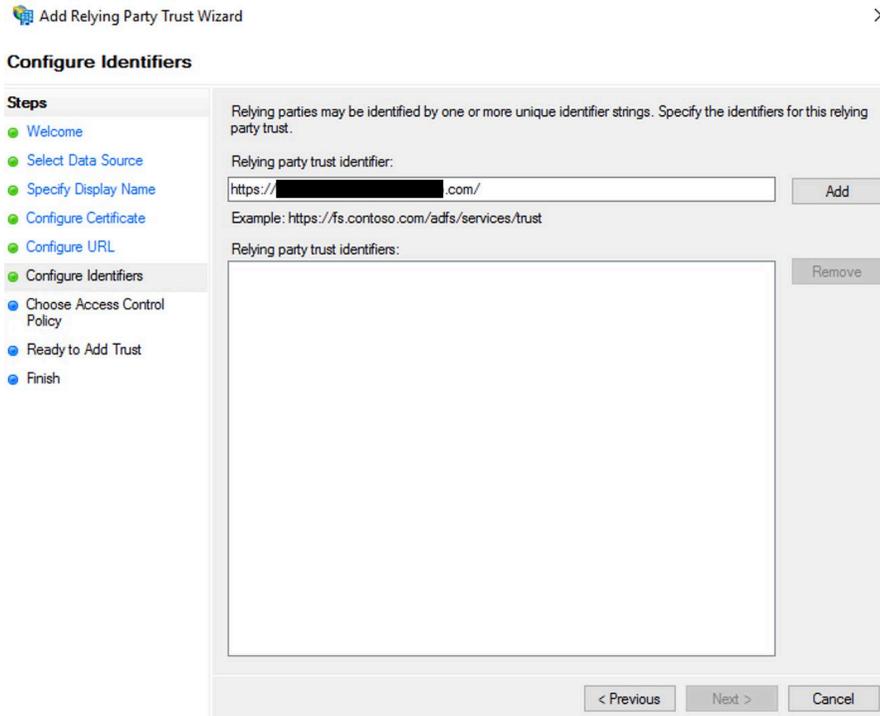
Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

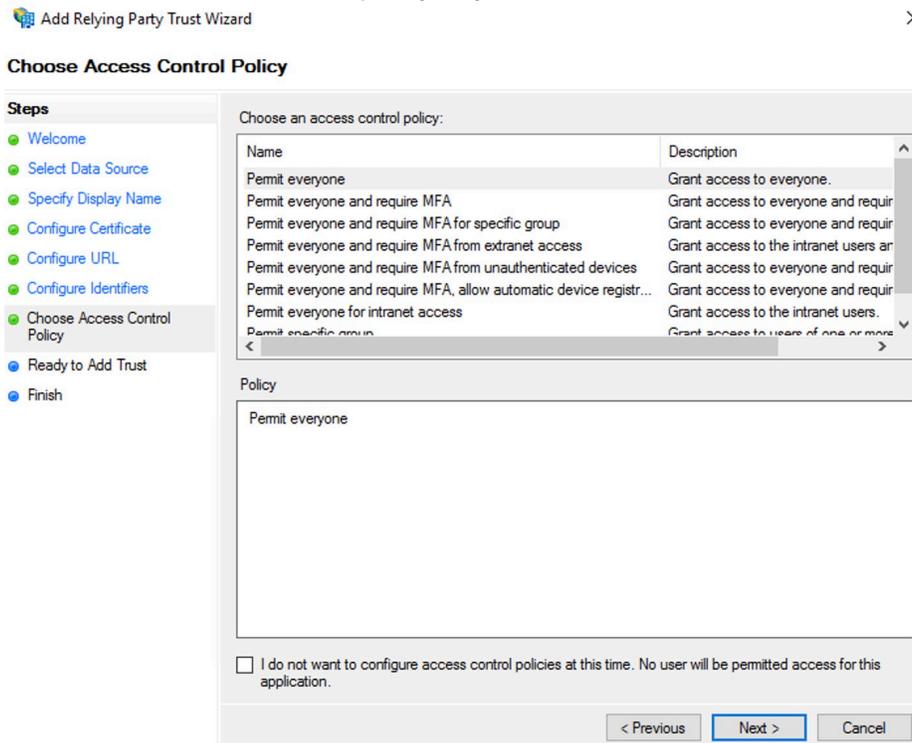
Relying party SAML 2.0 SSO service URL:  
  
 Example: https://www.contoso.com/adfs/ls/

At the bottom of the dialog are three buttons: '< Previous', 'Next >', and 'Cancel'.

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



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



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

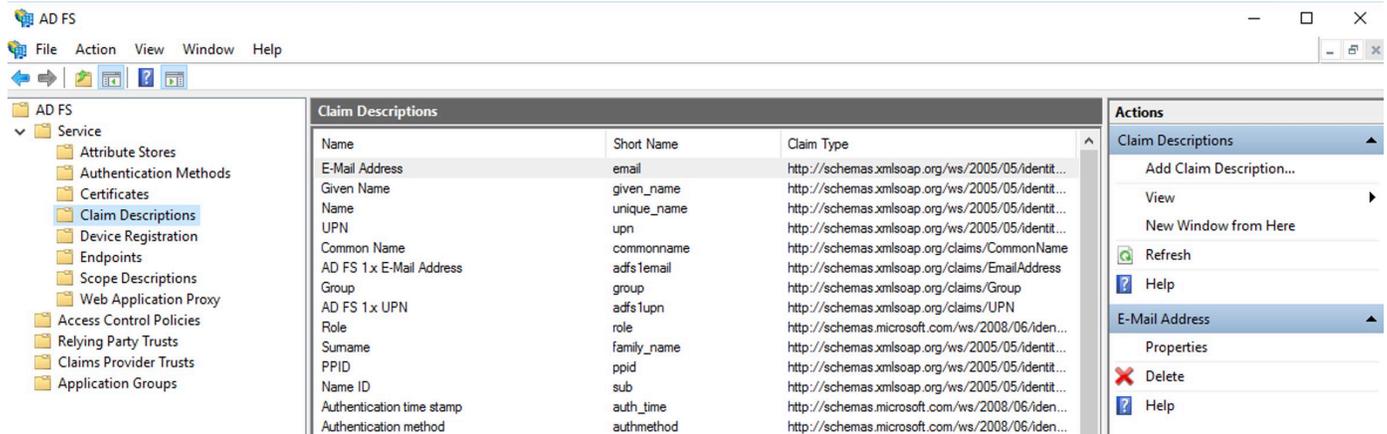
At the Finish screen, uncheck **Configure claims issuance policy for this application**, then click **Close**.

Next, we will configure a custom attribute to use as a claim to assigned roles.

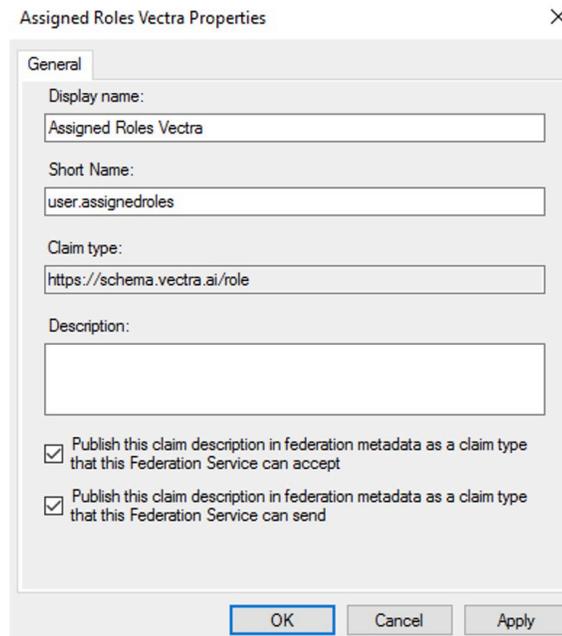
### 3. Add a Claim Description

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 an attribute corresponding to standardized name of a Vectra role, so that the Brain 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



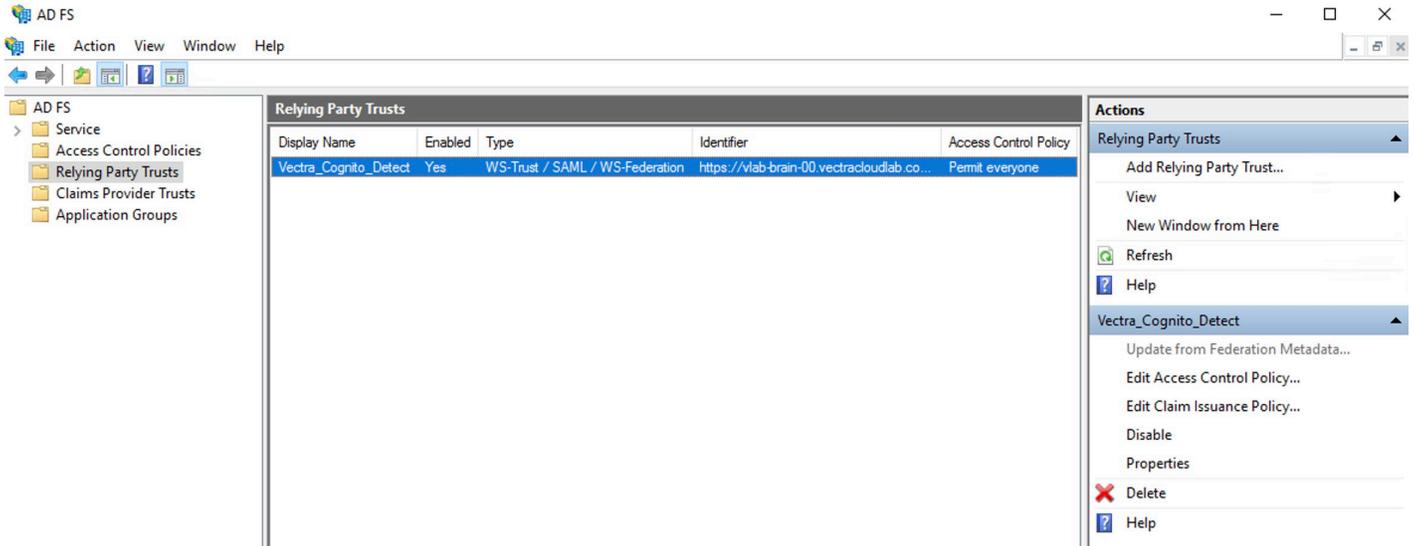
Enter a **Display name** like **“Assigned Roles Vectra”**  
 then enter the **Short Name** **“user.assignedroles”**  
 then enter the **Claim Type** **“https://schema.vectra.ai/role”**  
 Finally check the two **Publish...** box and finish by clicking **Ok**



## 4. Add Rules Claim

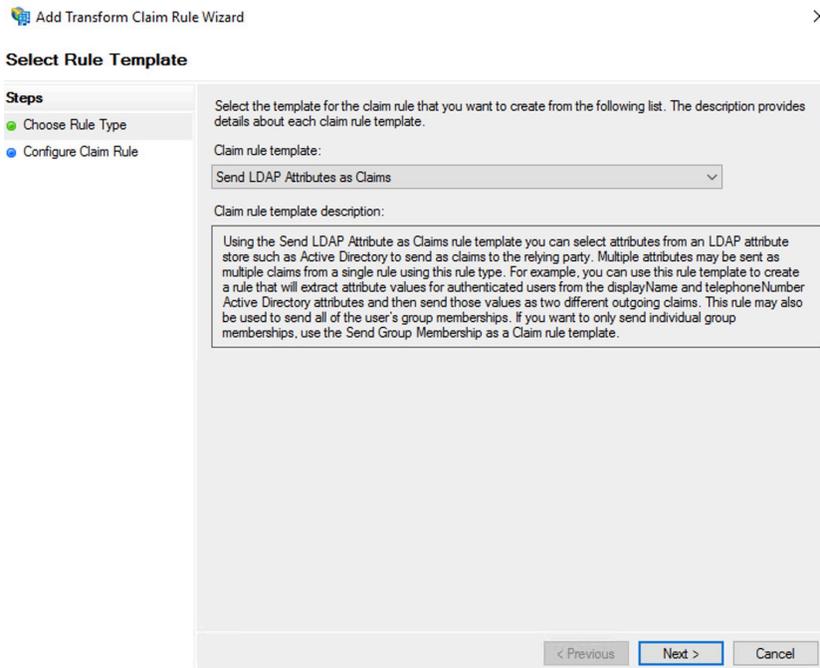
In ADFS, the Claims Issuance Policy defines what pieces of information about a user go where in a claim.

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



a. Add the SSO rule Claim

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



Enter a **Claim rule name** like **Cognito\_Detect\_SSO**

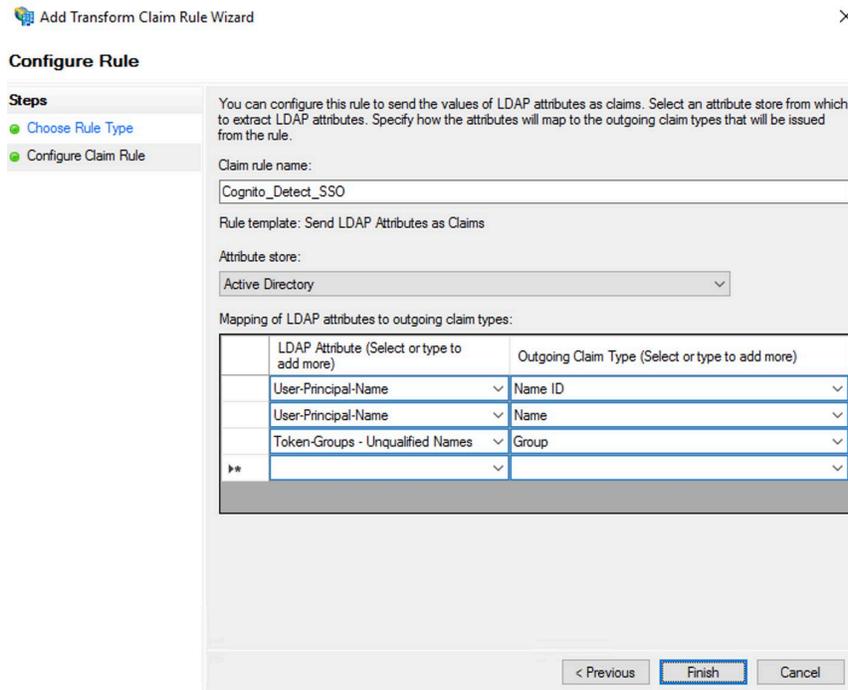
Then select **Active Directory Attribute Store**

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 **Name** as **Outgoing Claim Type**

Then select **Token-Groups – Unqualified Names** as **LDAP Attribute** and map it to **Group** as **Outgoing Claim Type**

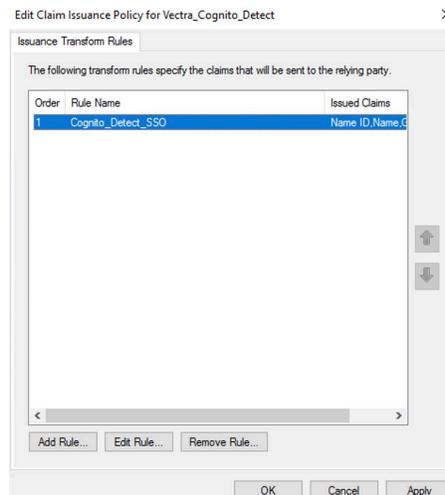
- ▼ *Note: The “User-Principal-Name” contains the value of the email address of the user. The “Name ID” outgoing claim should always be present to ensure correct session handling and can be seen as the login field in SAML.*



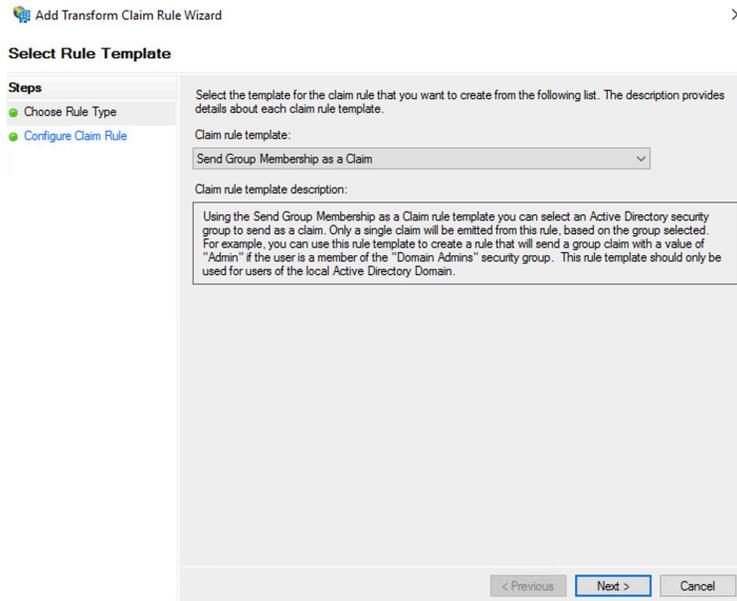
## b. Add Role rule Claim

Now, go to Edit Claim Issuance Policy window to create a 2<sup>nd</sup> 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...**



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



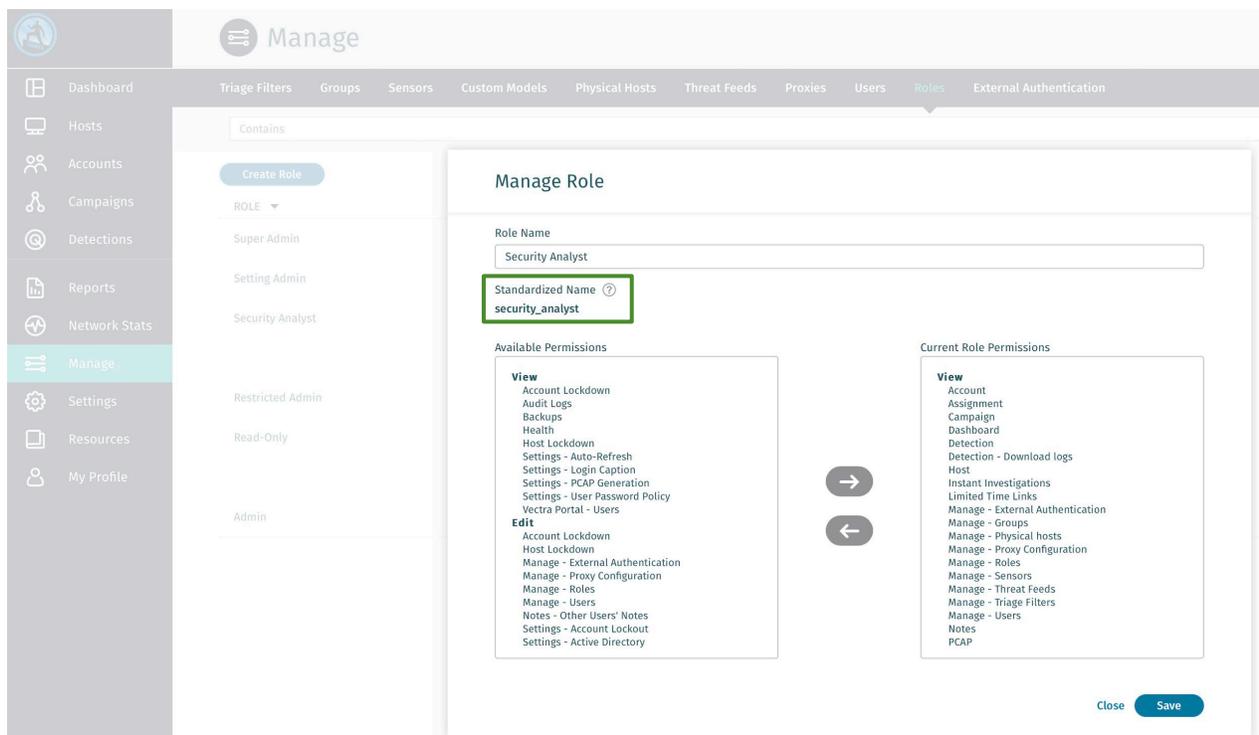
Enter a **Claim rule name**

Browse the Active Directory and select the group to map

Select the **Outgoing claim type** newly created **Assigned Roles Vectra** 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 Cognito Detect 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"**



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

**Add Transform Claim Rule Wizard** [Close]

**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:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

Outgoing name ID format:

Outgoing claim value:

< Previous **Finish** Cancel

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

**Edit Claim Issuance Policy for Vectra ADFS** [Close]

**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, Group
2	Cognito_Detect_security_analyst_role_m...	Assigned Roles Vectra

▼ *Note: Please ensure the users are only mapped to one Vectra Cognito Detect 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.

To Download **ADFS federation metadata xml**, go to the following URL:

[https://adfs\\_server.domain.com/FederationMetadata/2007-06/FederationMetadata.xml](https://adfs_server.domain.com/FederationMetadata/2007-06/FederationMetadata.xml)

It should give you a file of this type:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="..." entityID="http://...adfs/services/trust">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#e83c5589-c41b-40b6-bc42-ebb3ddd2927e">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
        <ds:DigestValue>...XCM=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>...0u5TX19TSYXncvz4zdShkAgTa/c6Xr0N1WVds9TGICe9DEbgSSbXsRFV+vb5R2p1l1Ra97eNAopxBv3bERzxVpbMli4tX7ophSZOP70JFpCt918
  </ds:Signature>
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <X509Data>
      <X509Certificate>...smcgLSBKYZAxLmFyY2hlcj5sb2NhbdAeFw0yMTEExMTYxOTM5SMTVaFw0yMjExMTYxOTM5SMTVaNCsXKI
    </X509Data>
  </KeyInfo>
</ds:Signature>
</EntityDescriptor>
</RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsrf/federation/200706" xsi:type="fed:ApplicationServiceType" protocolSupportEnum=
```

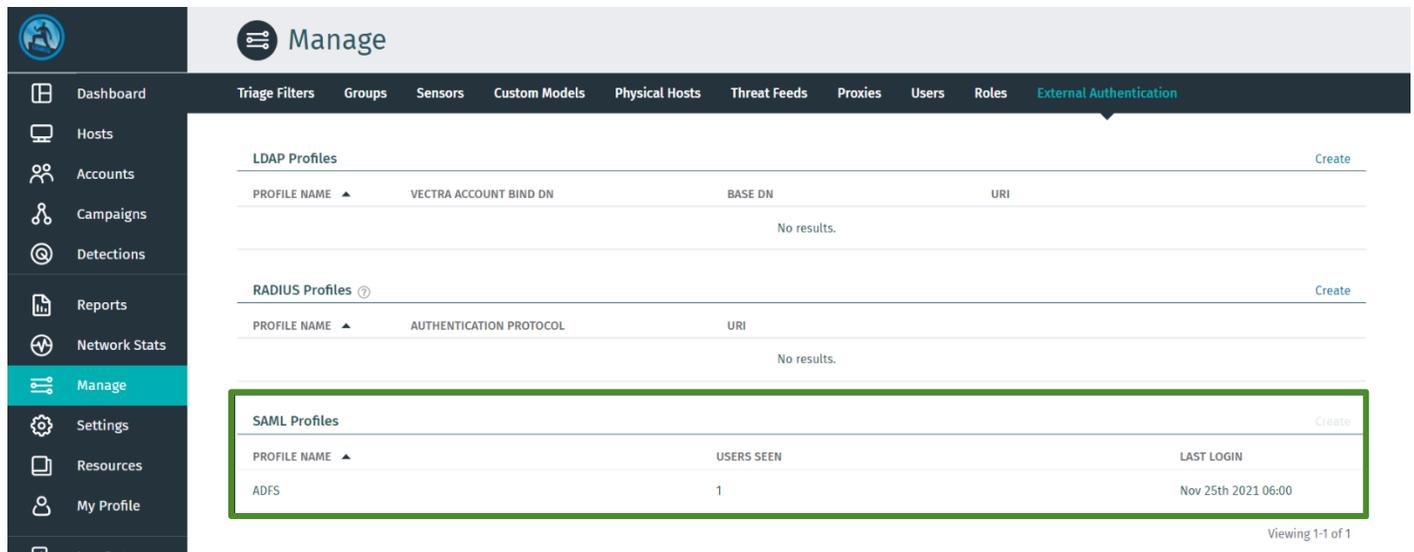
Open a new browser tab and log in to your Cognito Platform (Brain) as you normally do and navigate to **Manage > External Authentication**.

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.

Then upload the **ADFS federation metadata xml**

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



## 6. Test your new SAML Single Sign-On Functionality

The Detect URL you have been previously using now works with SAML SSO

When a user accesses the URL and does not already have a valid authentication session open, they will be redirected to the IdP.



From here, the user can connect via SAML, by clicking on “Log in via SSO”.

They will then be redirected to the ADFS login page:



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

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

USERNAME ▲	ROLE	USER TYPE	LAST LOGIN
adm	Admin	Local	—
admin	Super Admin	Local	Nov 23rd 2021 21:23
SAML:socanalyst2@ (You)	Security Analyst	SAML	Nov 24th 2021 13:03
SAML:soc_analyst1@	Security Analyst	SAML	Nov 19th 2021 11:10
SAML:vectora_super_admin1@	Super Admin	SAML	Nov 23rd 2021 16:21

Note: local authentication can be performed using URL [https://brain\\_ip\\_or\\_fqdn/accounts/login/?local=true](https://brain_ip_or_fqdn/accounts/login/?local=true)



## Worldwide Support Contact Information

- ▼ Support portal: <https://support.vectora.ai>
- ▼ Email: [support@vectora.ai](mailto:support@vectora.ai) (preferred contact method)
- ▼ Additional information: <https://www.vectora.ai/support>