SAML SSO Using ADFS

Version: Dec 30, 2022

Table of Contents

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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.*

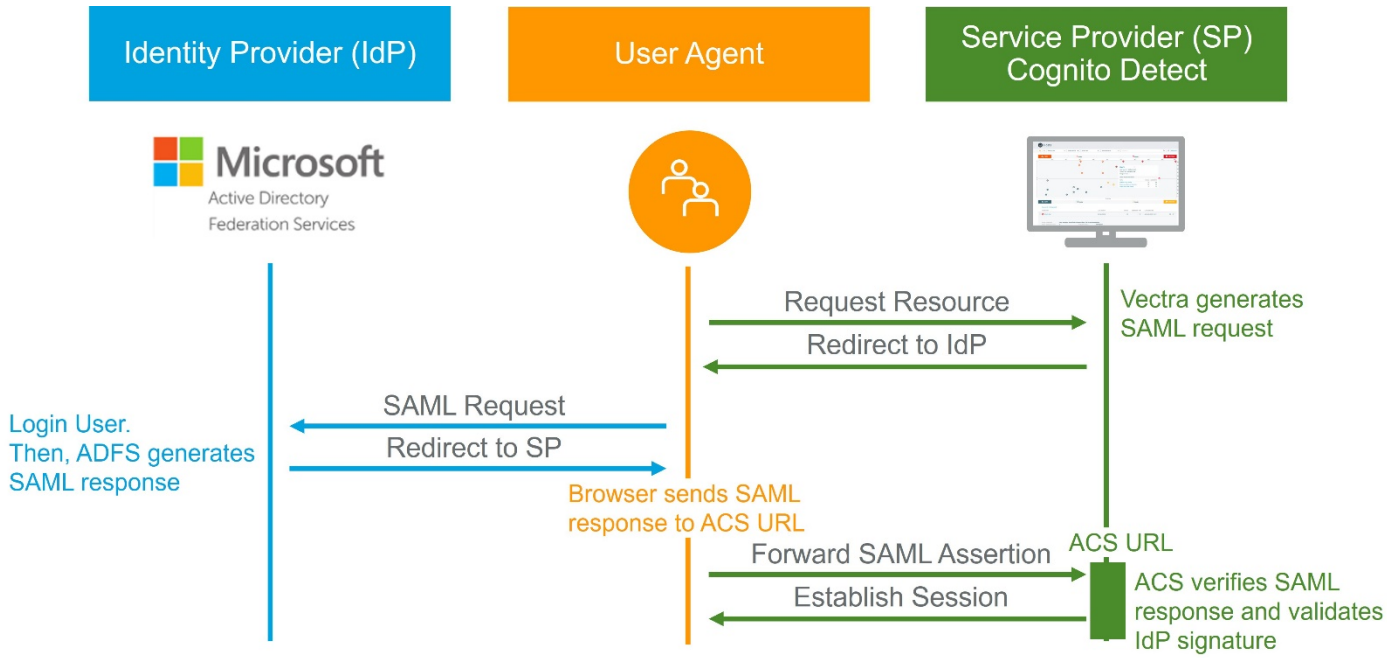
Prerequisites

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



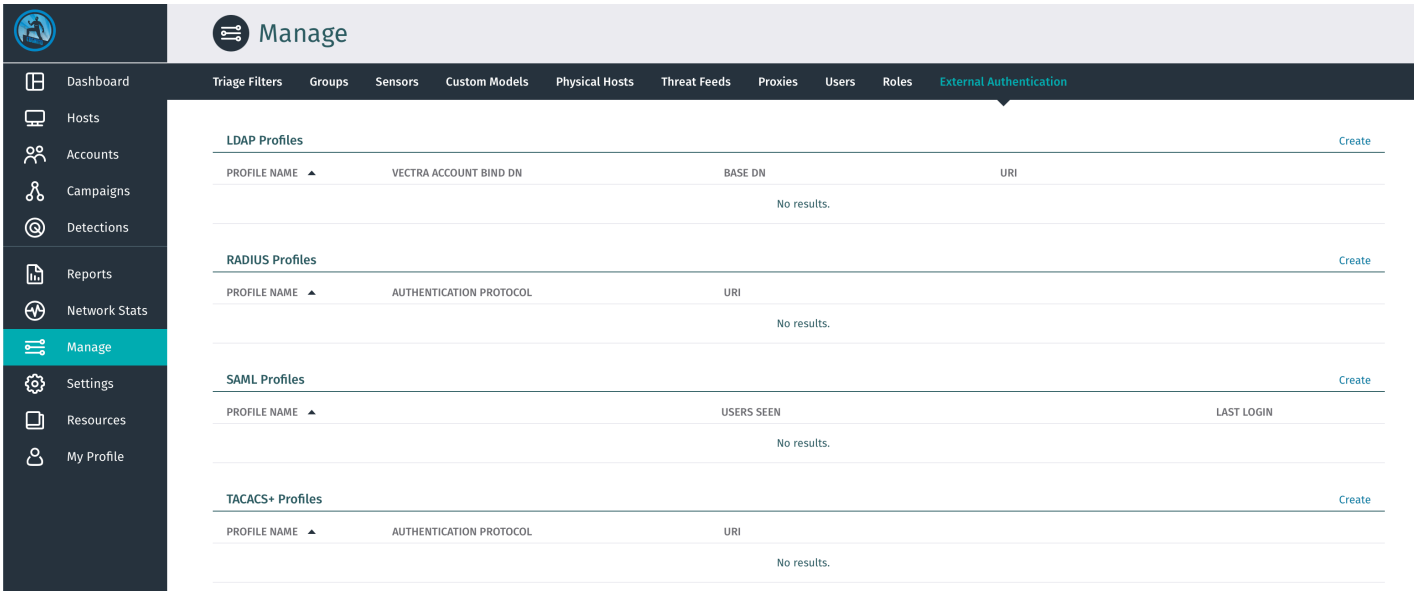
© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Configuring ADFS and Vectra

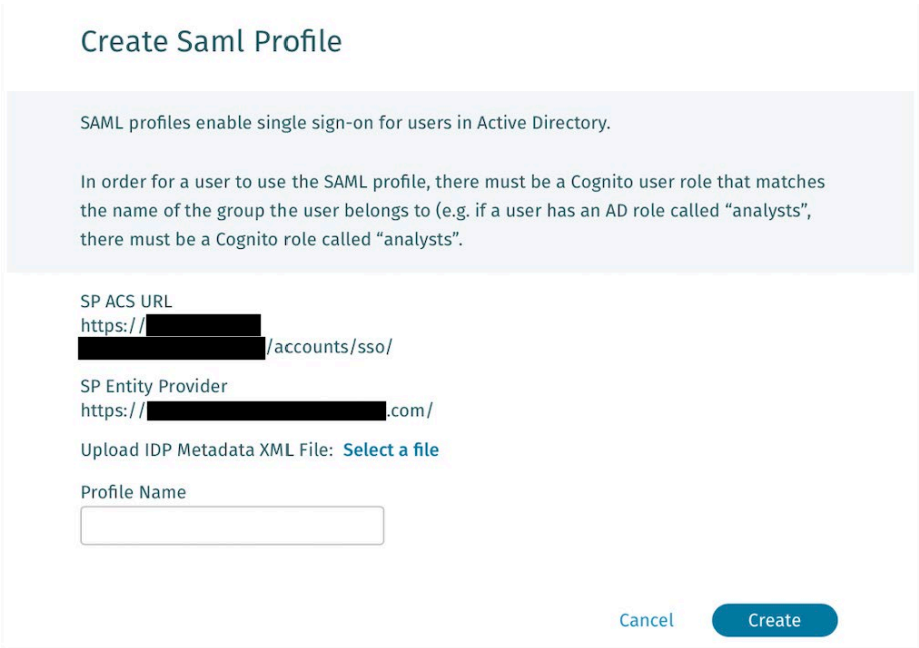
1. Get SAML Profile Information for ADFS

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/.

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

- 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.

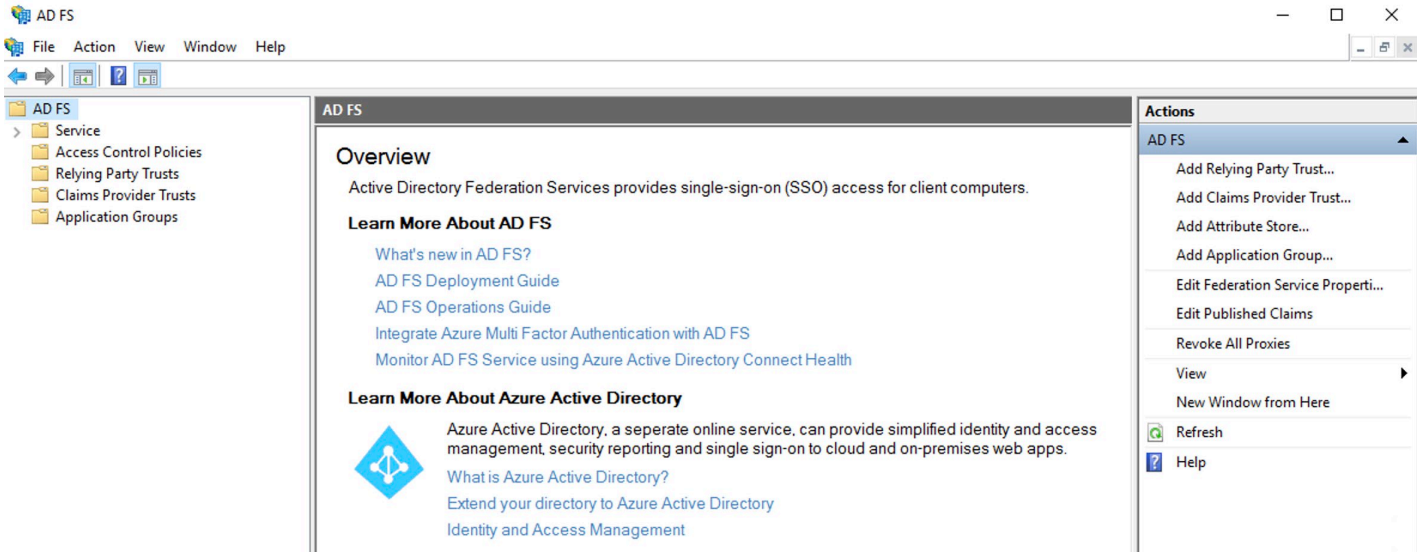
- *Note: If you want a hostname-based entry instead of IP-based for the SP ACS URL and SP Entity Provider, then you should:*
  - *Configure on Vectra the Brain FQDN, in Settings > General > Brain > DNS Name in the Cognito Platform (Brain) UI.*
  - *Check the "DNS Name" radio button for the "For linking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

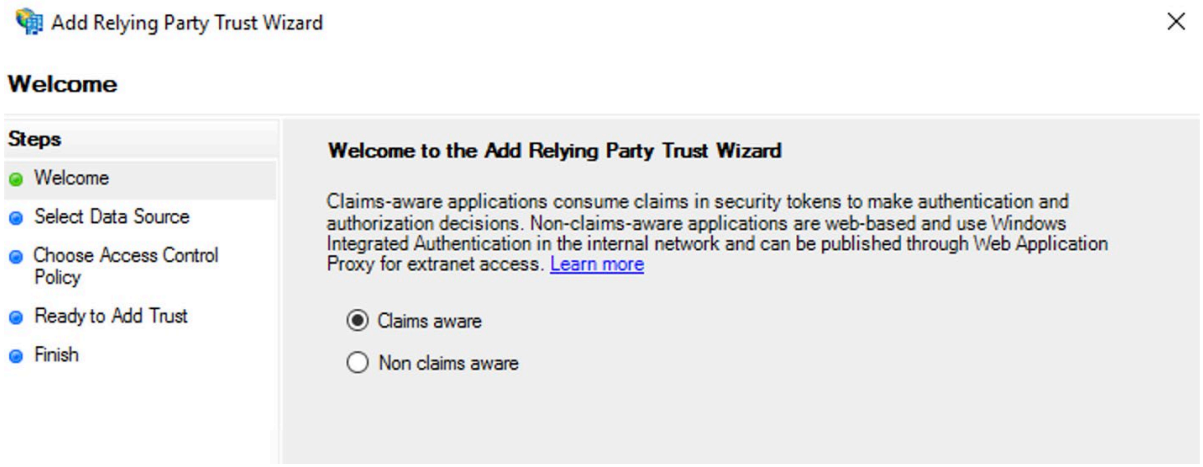
Relying party trust is a term used in ADFS to identify service providers (in our case Vectra) that can communicate with an ADFS endpoint.

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...**

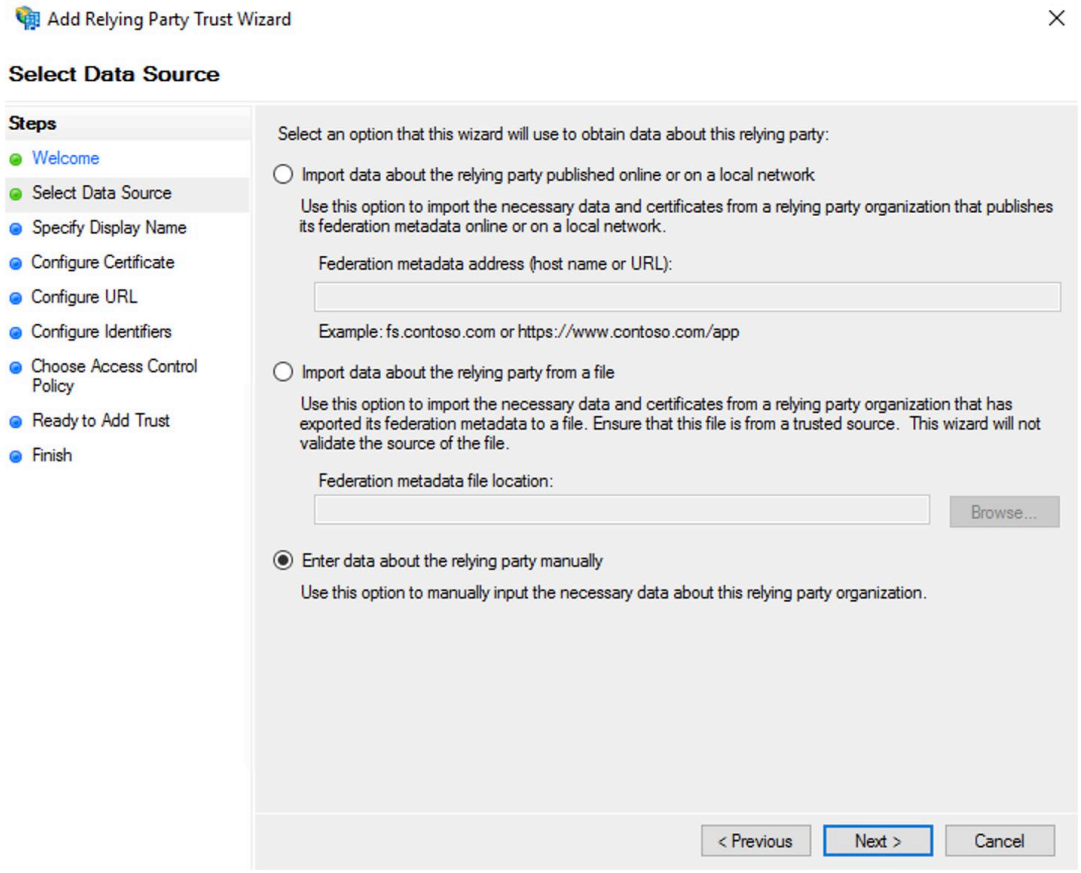


© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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

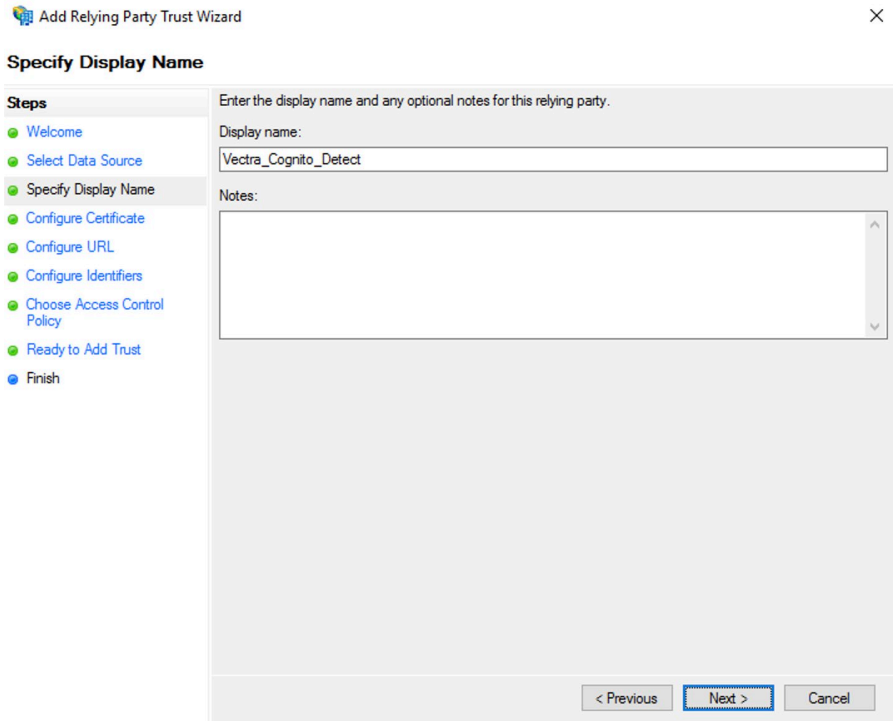


Select **Enter data about the relying party manually**, then click **Next**

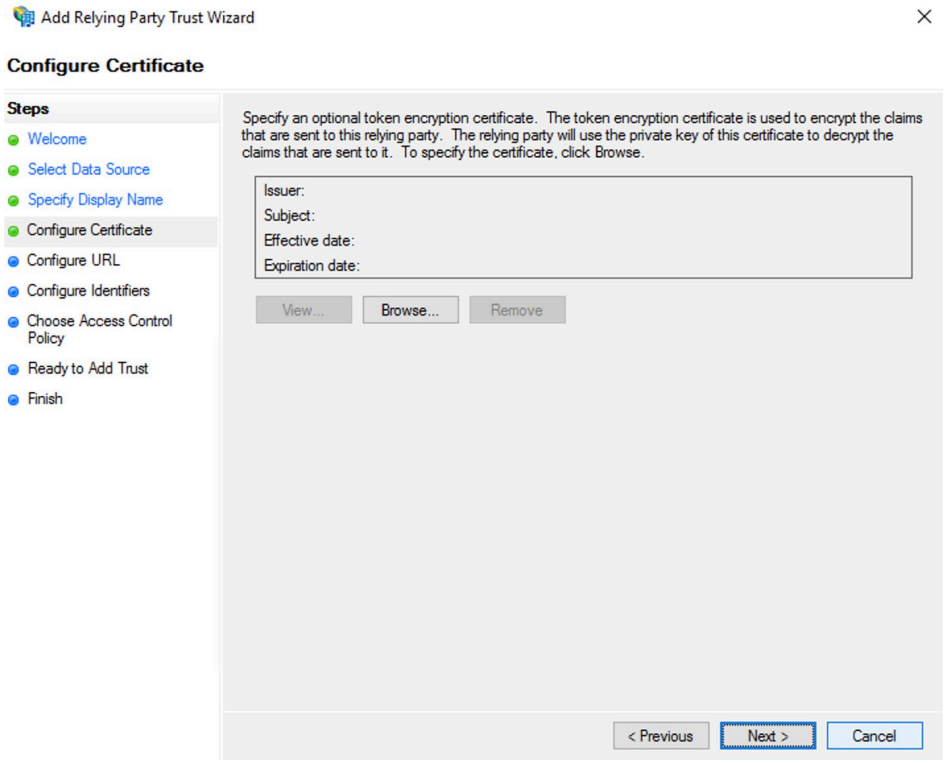


© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Enter a display name (like "***Vectra_Cognito_Detect***") and any optional notes, then click **Next**

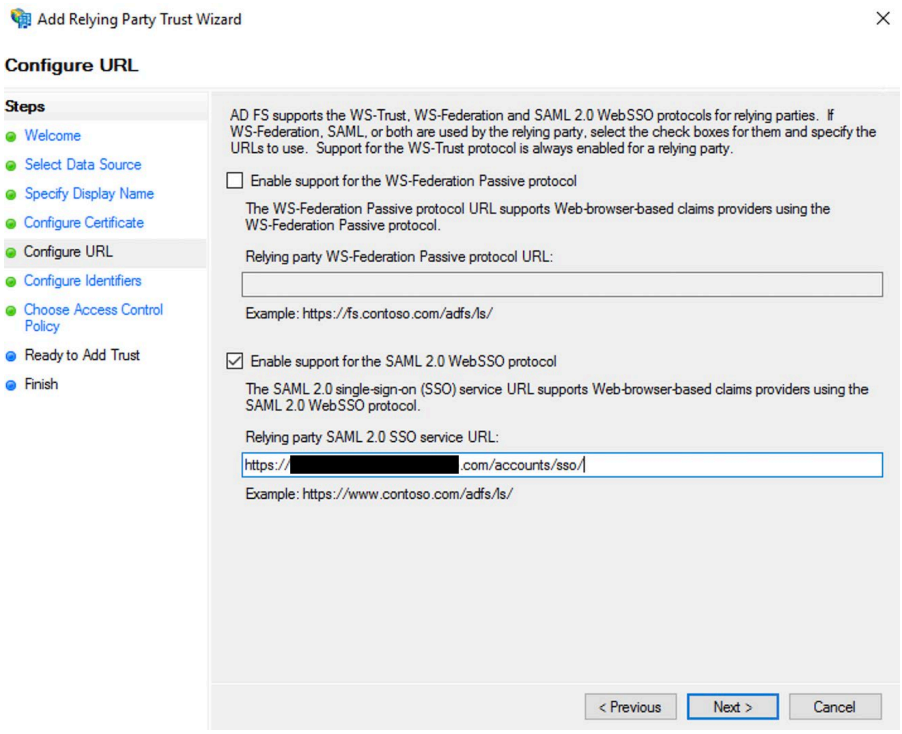


Click ***Next*** to accept the defaults for the ***Configure Certificate*** step.



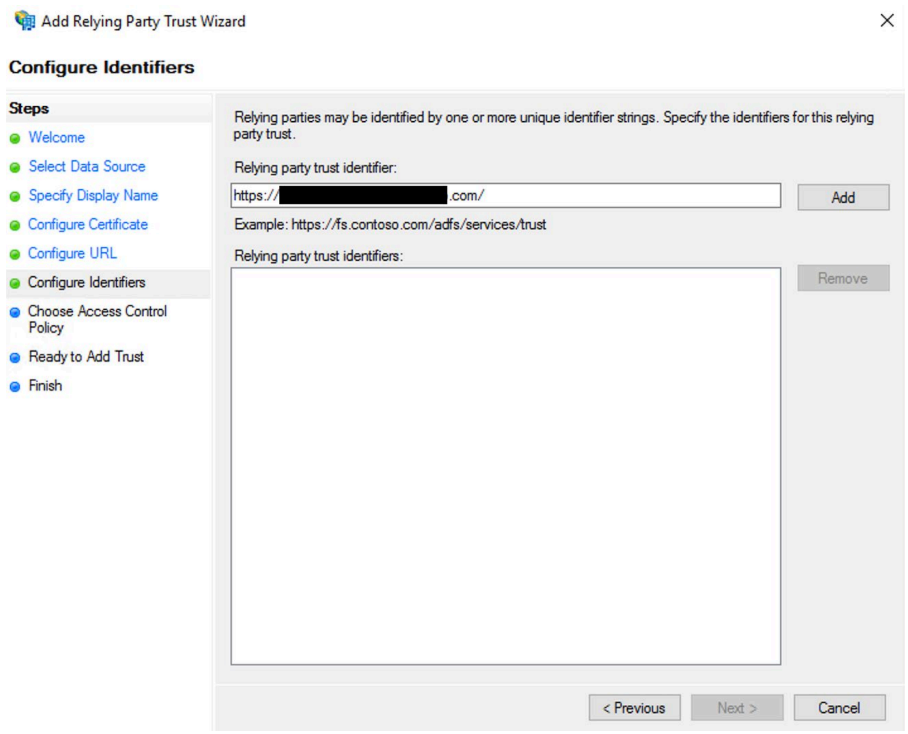
© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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***.

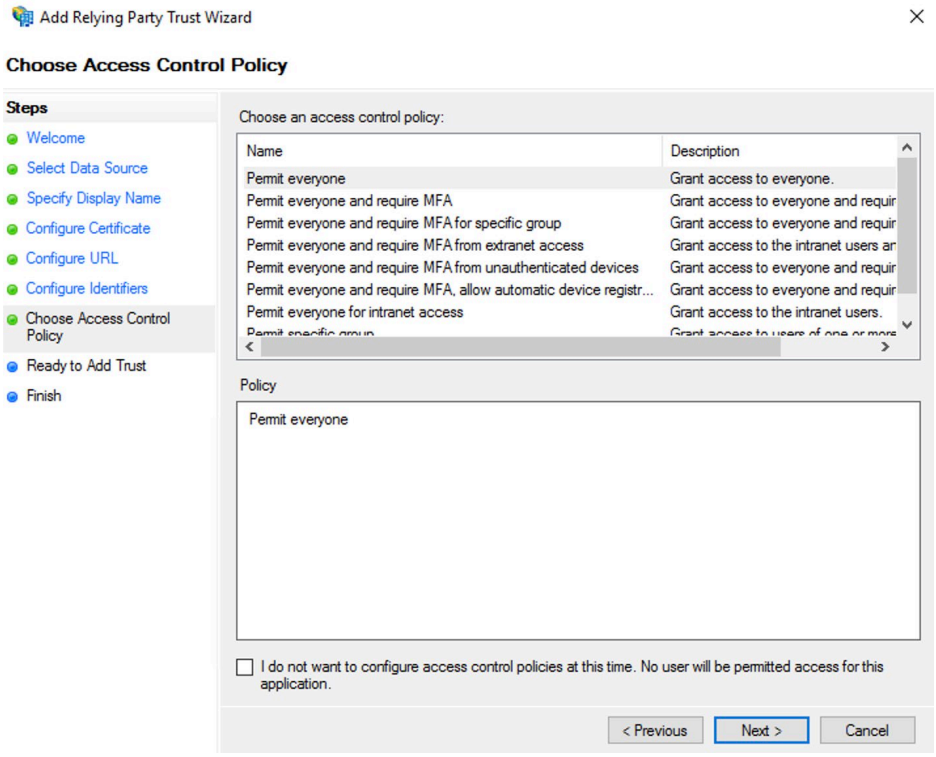


In the ***Relay party trust identifier***, enter the ***SP Entity Provider*** retrieved from Cognito Detect SAML Profile configuration page in Step 1. Click ***Add***, then Click ***Next***.

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.



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.

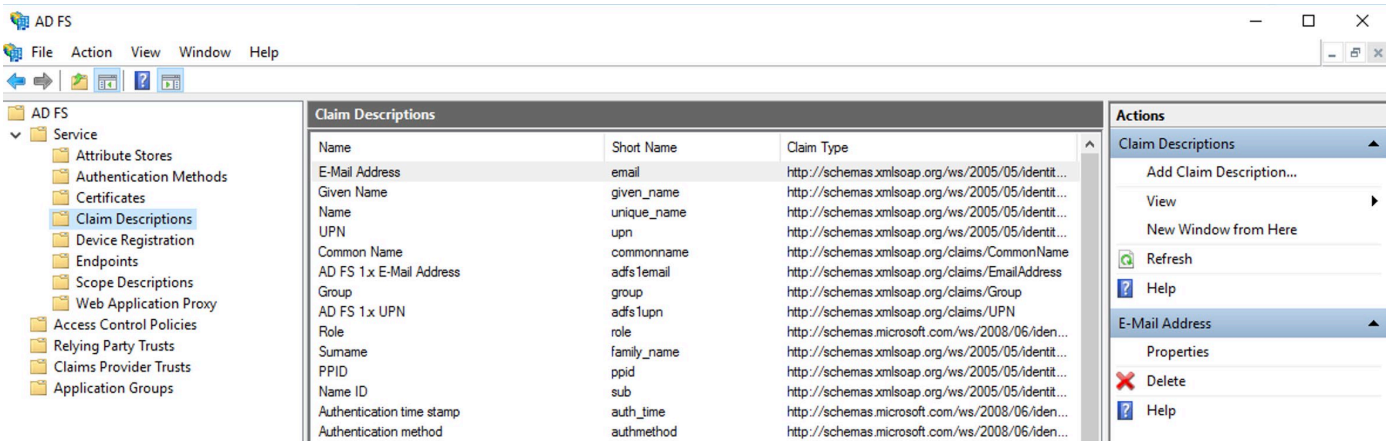
© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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.

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Go to **AD FS Management**, select **Service** from the left navigation pane then **Claim Descriptions**.
Click **Add Claim Description...** on the right navigation pane

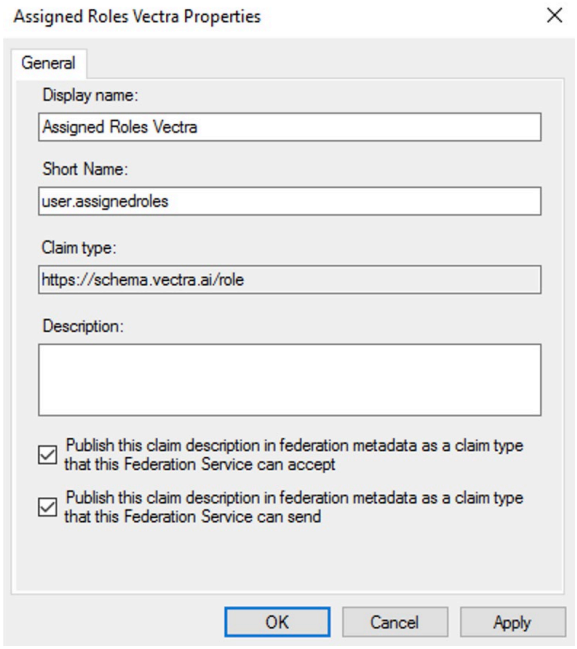


Enter a **Display name** like "***Assigned Roles Vectra***"

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***

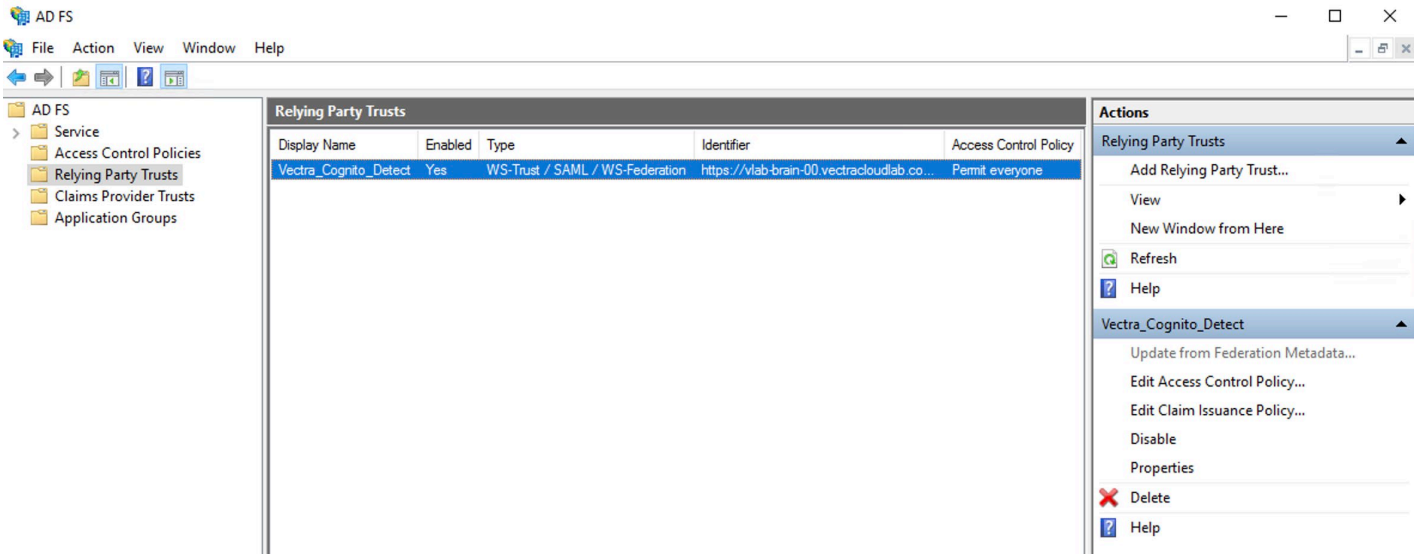


4. Add Rules Claim

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

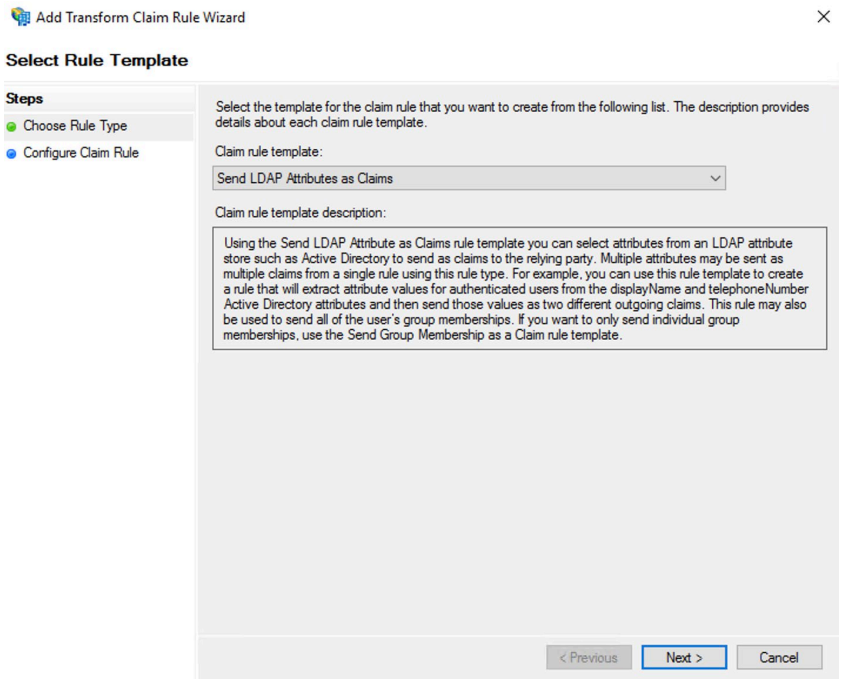
© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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**

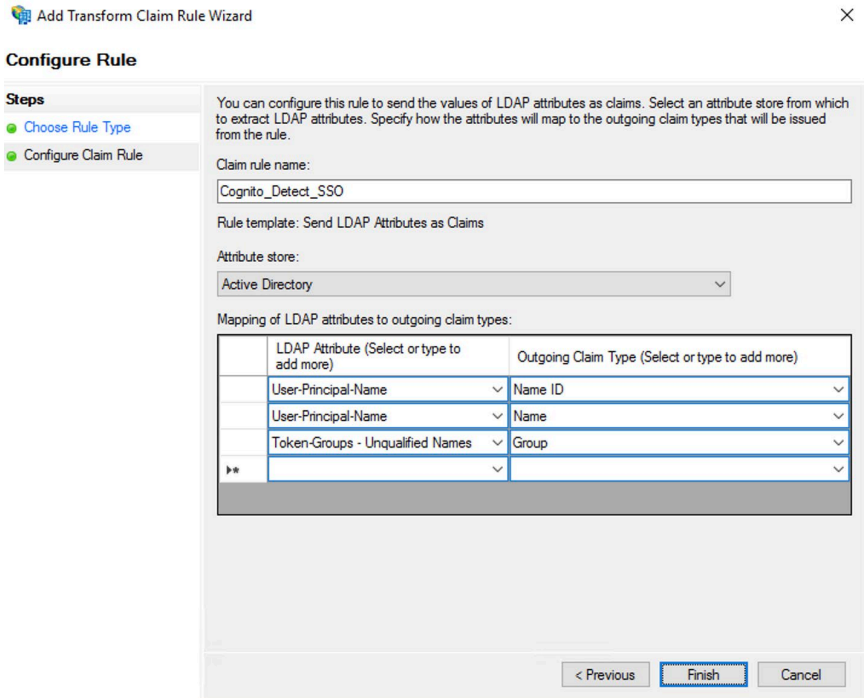
Then select ***User-Principal-Name*** as **LDAP Attribute** and map it to ***Name ID*** as **Outgoing Claim Type**

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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**

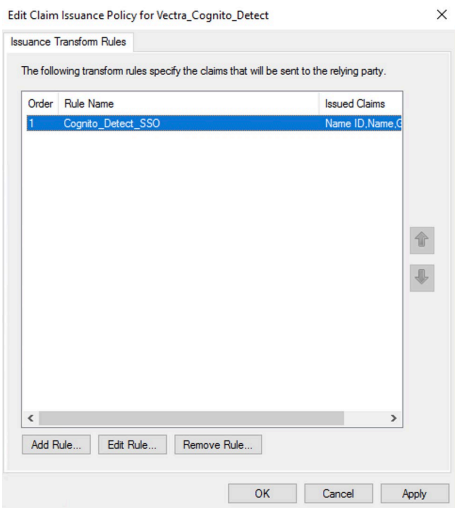
- *Note: The "User-Principal-Name" contains the value of the email address of the user. The "Name ID" outgoing claim should always be present to ensure correct session handling and can be seen as the login field in SAML.*



b. Add Role rule Claim

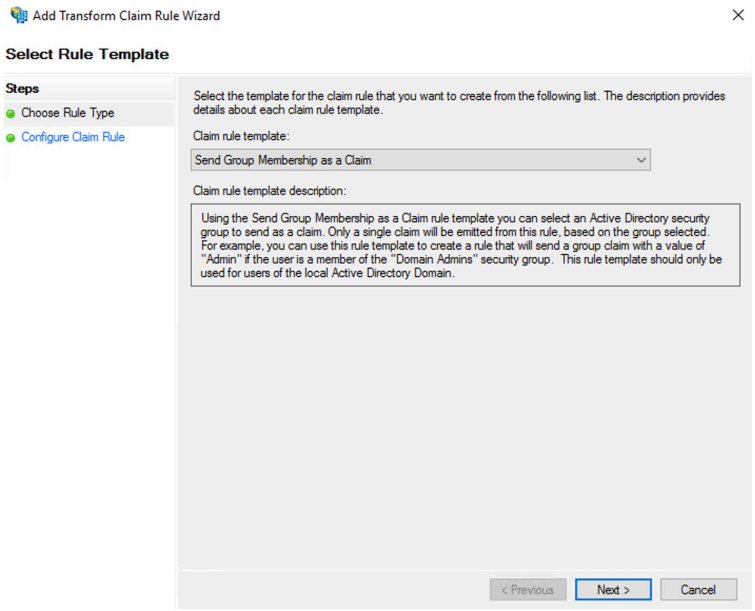
Now, go to Edit Claim Issuance Policy window to create a 2nd claim rule, which will map the AD group to the standardized Vectra role name. This will map to a role (and permissions) defined on the Vectra Brain.

Add a new rule Claim ***Add Rule…***



© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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



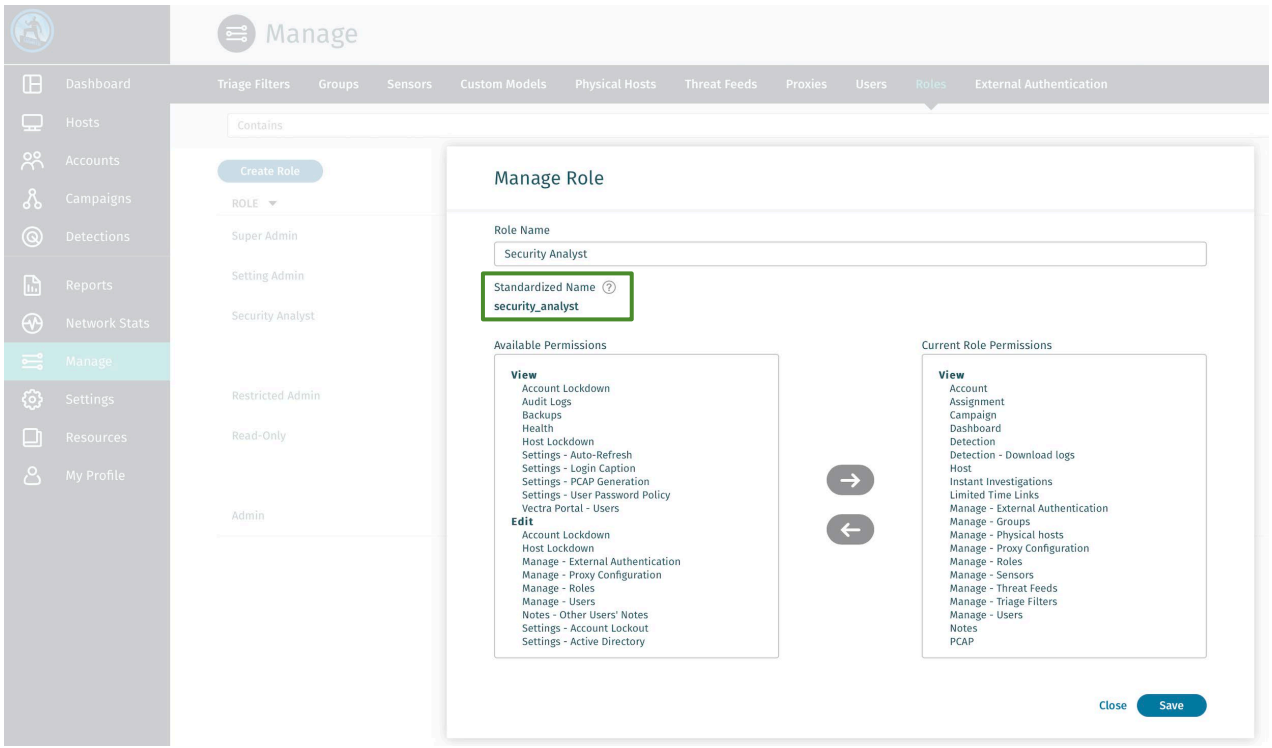
Enter a **Claim rule name**

Browse the Active Directory and select the group to map

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

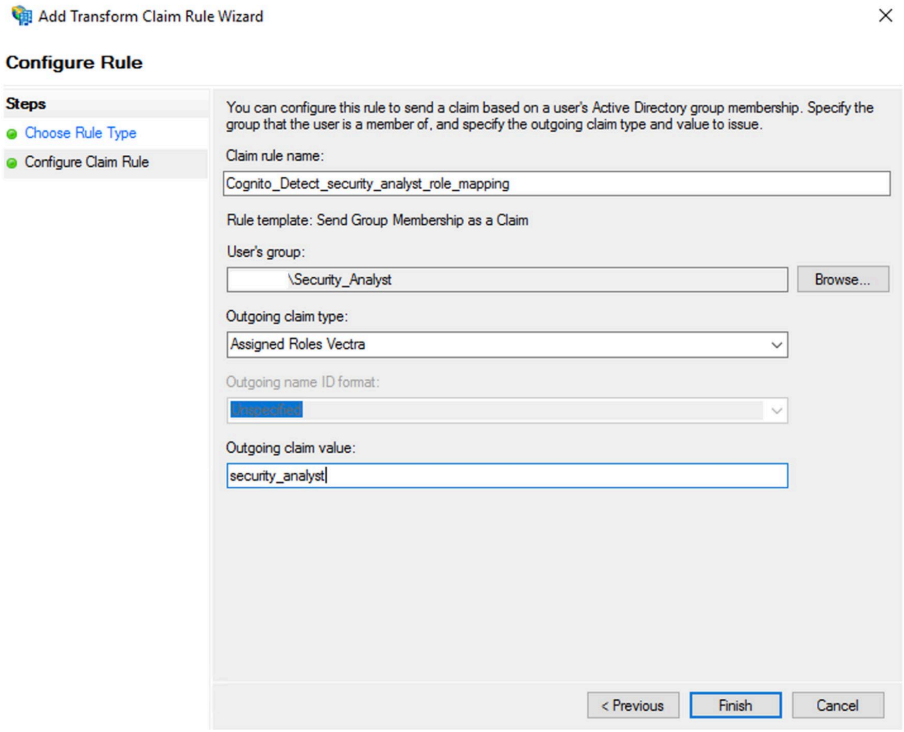
Then, we need to indicate the **Outgoing claim value** which will be the standardized name of your role to be assigned. To find this value, go back in your Cognito Detect tab, navigate to the ***Manage > Roles*** screen.

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***"

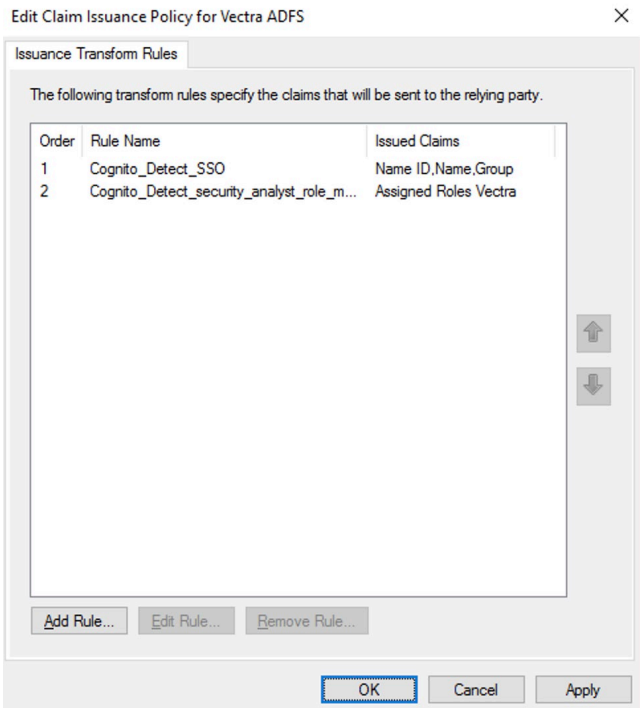


© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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



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



- *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*

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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

It should give you a file of this type:

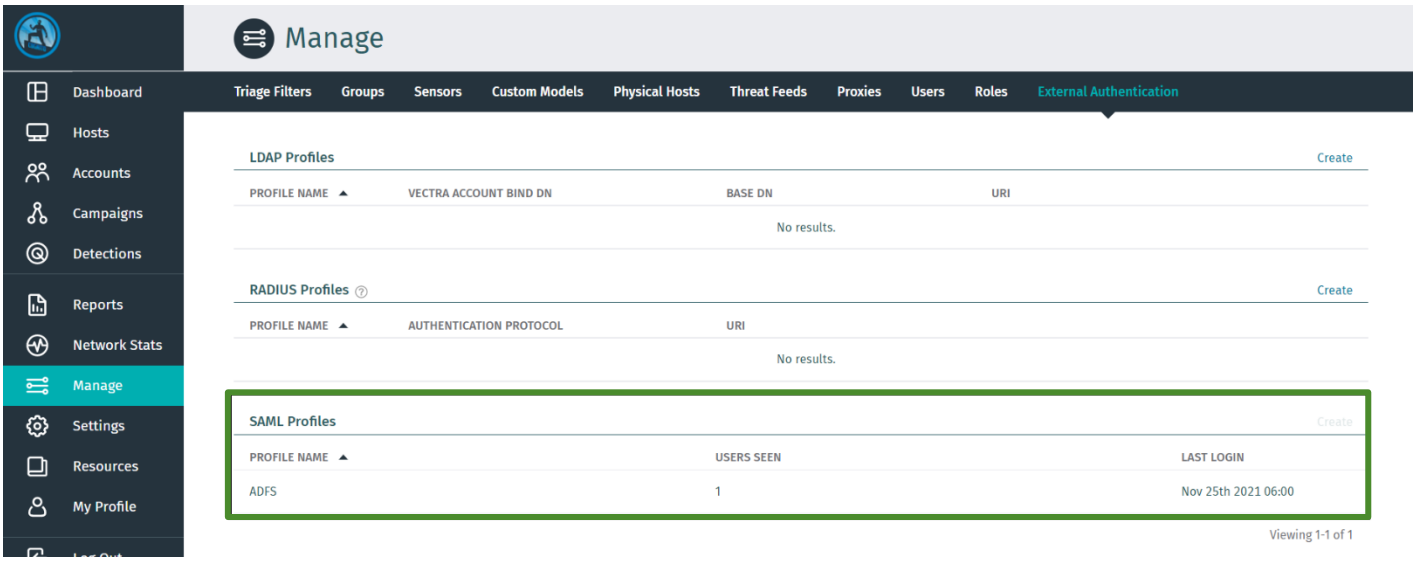
Open a new browser tab and log in to your Cognito Platform (Brain) as you normally do and navigate to ***Manage > External Authentication.***

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***



© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

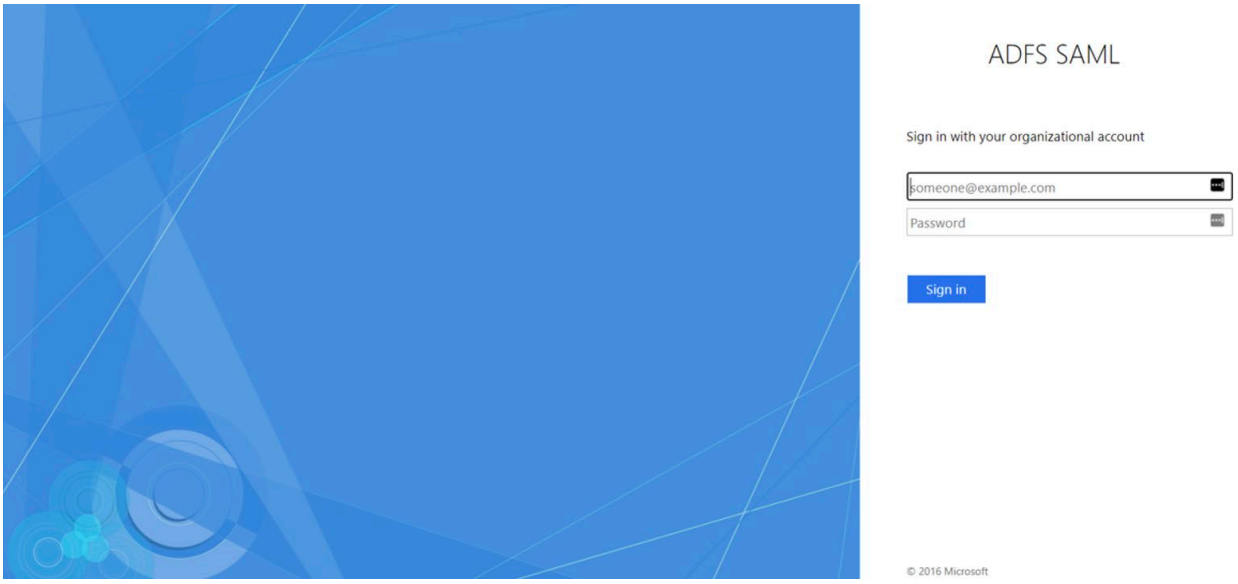
6. Test your new SAML Single Sign-On Functionality

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”.

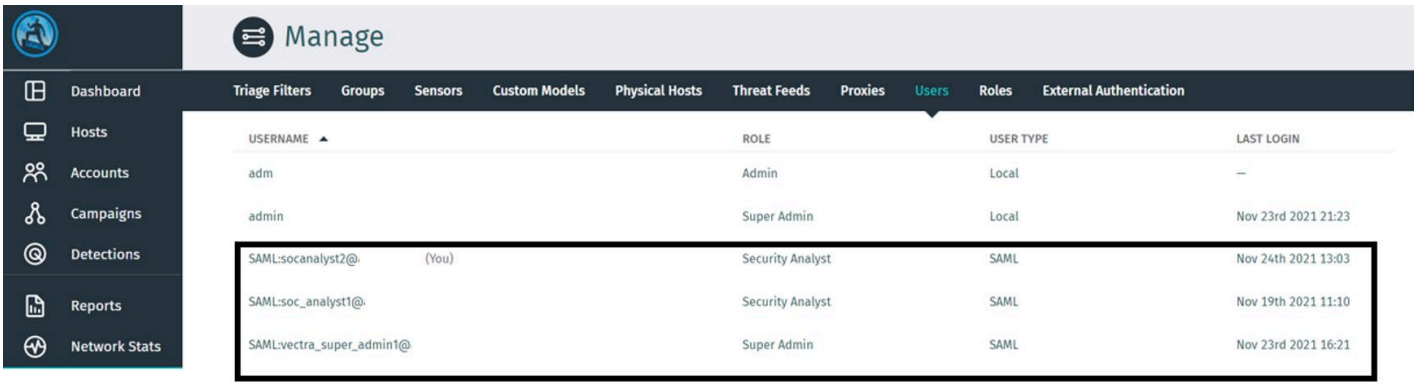
They will then be redirected to the ADFS login page:



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

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

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



Note: local authentication can be performed using URL https://brain_ip_or_fqdn/accounts/login/?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

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.