Configuring Vault For Single Sign On

Overview

Vault provides integration with Microsoft's Active Directory Federation Services (AD FS) to enable your users to have a Single Sign On experience when they access your organisation's Web-based Vault application.
As well as giving users a single sign on capability, AD FS also gives you the security control and management of the access credentials of your users without having to share these with a third party.

In its simplest form, AD FS operates in the following manner

1. Your user attempts to log into Vault
2. Vault refers the request to your Single Sign On server
3. Your Single Sign On servers verify the user against your Active Directory credentials
4. The verified details are passed back to Vault for Vault authorisation
5. If the user exists in Vault, the user is presented with the Vault home page

Responsibilities

Vault GRC are responsible for;

- Providing the SAML interface in Vault
- Configuring the Vault interface with details supplied by you

You are responsible for;

- Provision and configuration of all AD FS components
- Provision of appropriately skilled resources for the above
- Maintaining a valid token signing certificate and notifying Vault of any changes to the certificate used prior to rollover

Vault GRC will assist with integration of your AD FS services with Vault, however the skills and resources to configure ADFS / SAML are your responsibility.

Configuring Vault As a Trusted

Linking Vault with your Active directory using ADFS requires the setup of a two-way trust using SAML. ADFS has to be configured to trust Vault as a relying party and Vault needs to trust the ADFS as an identity provider.

Prerequisites

ADFS 2.0 (3.o) installed. Setup of the ADFS infrastructure is outside the scope of the document.

Note: Windows 2008 R2 ADFS role installs ADFS version 1.0. You will need to download and install ADFS 2.0 (3.0) from Microsoft.

Initial Vault Information

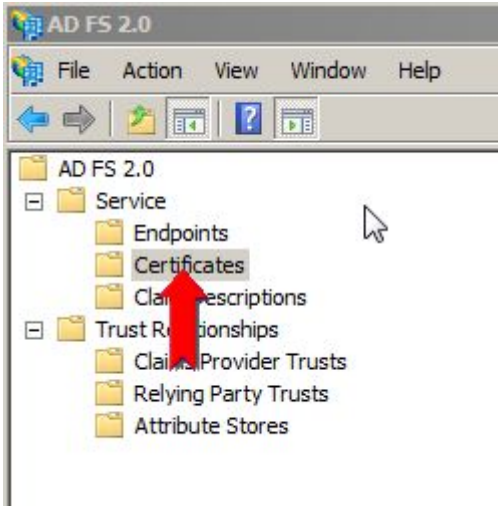
Vault GRC requires the following information before it can setup the relaying trust.

ADFS Domain: e.g. adfs.ngbigroup.com
ADFS Token Signing Thumbprint e.g. 9d4e231cbb110d41181a25612191e73baf2087ac

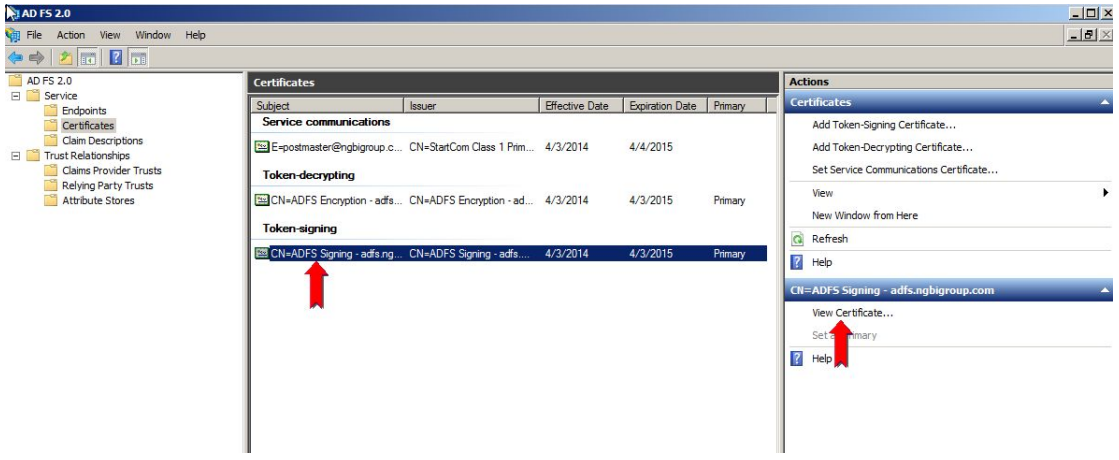
Send this information to support@vaultgrc.com

To get the Token signing thumbprint perform the following

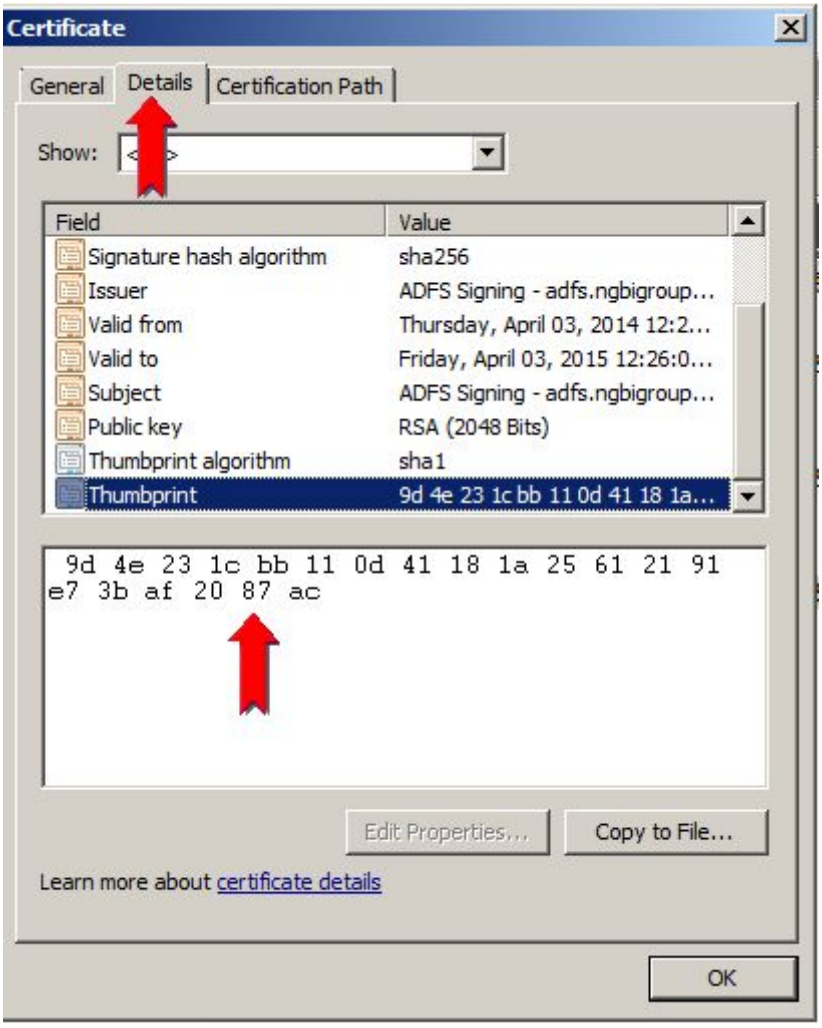
1. Open the ADFS 2.0 (3.0) Management Screen and click on the Service -> Certificates



2. Click on the Token-signing certificate and then click on View Certificate on the right



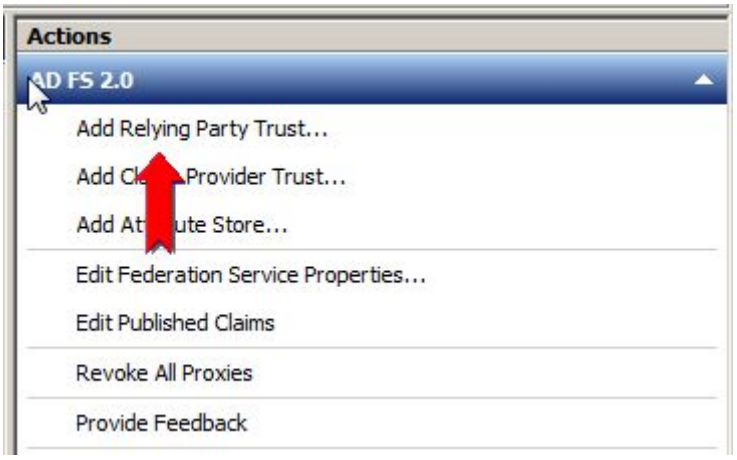
3. Click on the Details tab then go to the last item which is the Thumbprint. In the text box below select the text and press Ctrl + C to copy the value



Setup Vault Relying Party Trust

After Vault GRC has the previous information continue below

1. **From the ADFS Management Console, right-click ADFS 2.0 (3.0) and select Add Relying Party Trust.**

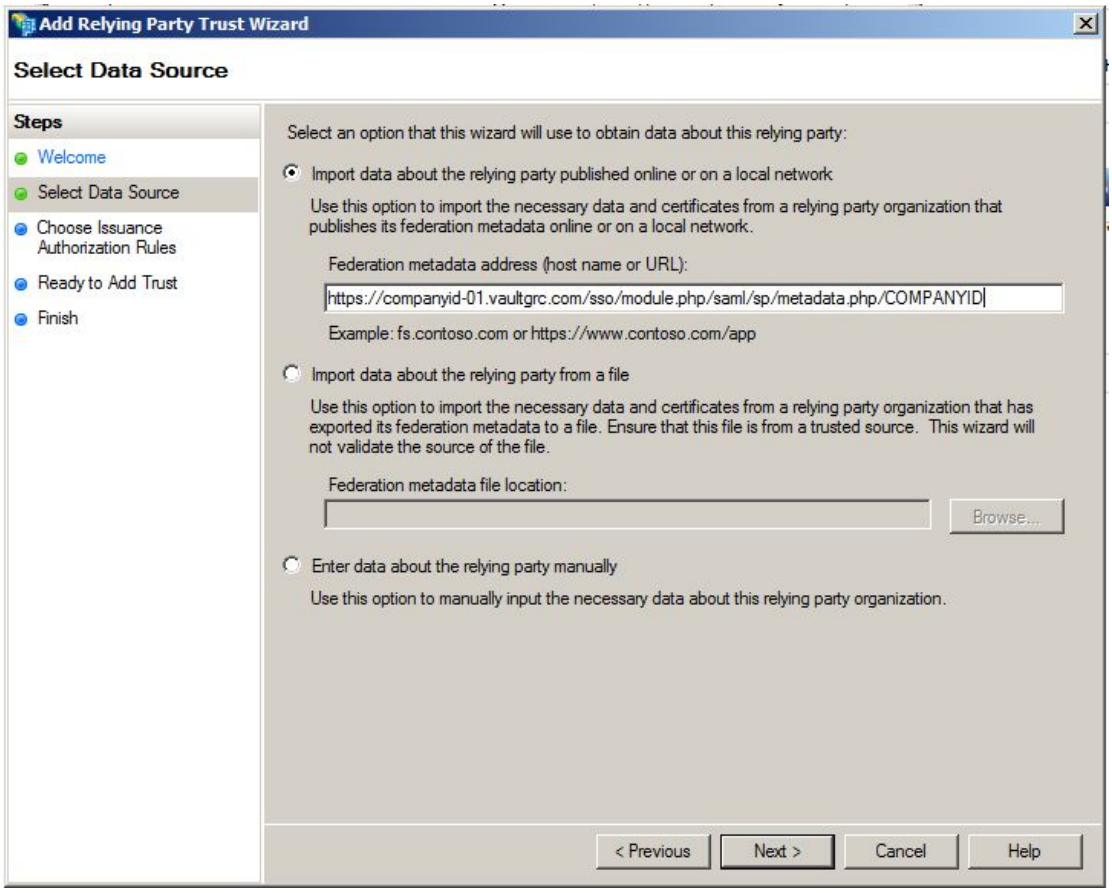


2. In the Add Relying Party Trust Wizard, click Start.

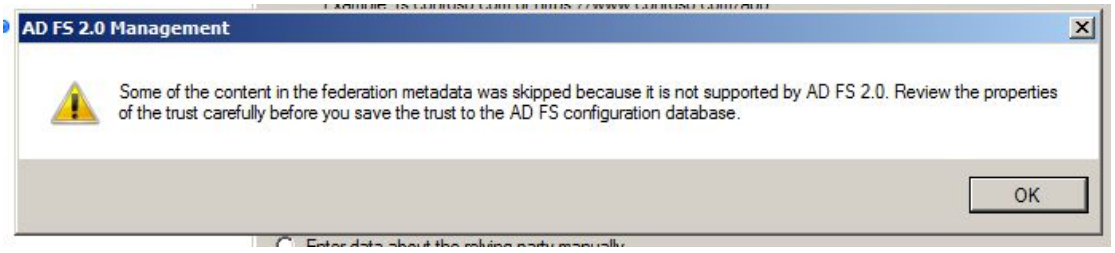
3. Check Import data about the relying party published online or on a local network, Use the provided Federation metadata. It will have the following format

https://companyid-01.vaultgrc.com/sso/module.php/saml/sp/metadata.php/COMPANYID

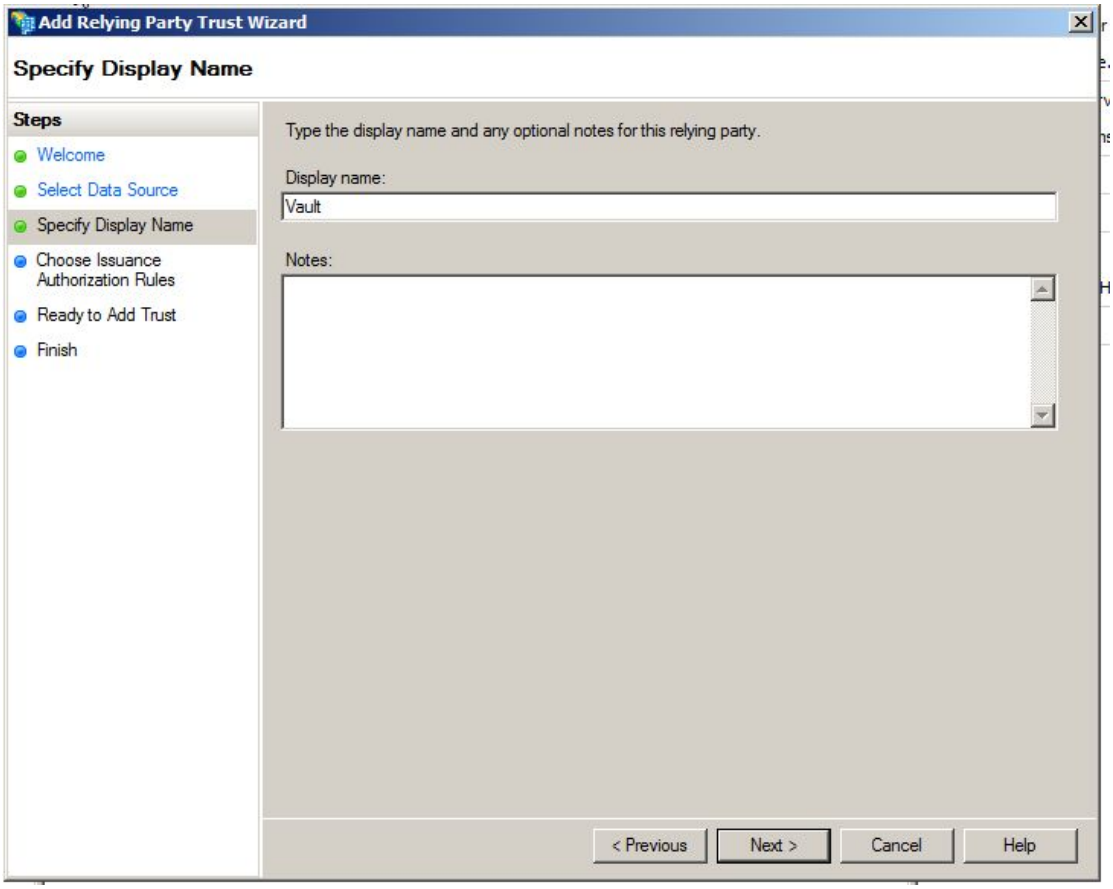
Then click Next. The metadata XML file is a standard SAML metadata document that describes Vault as a relying party.



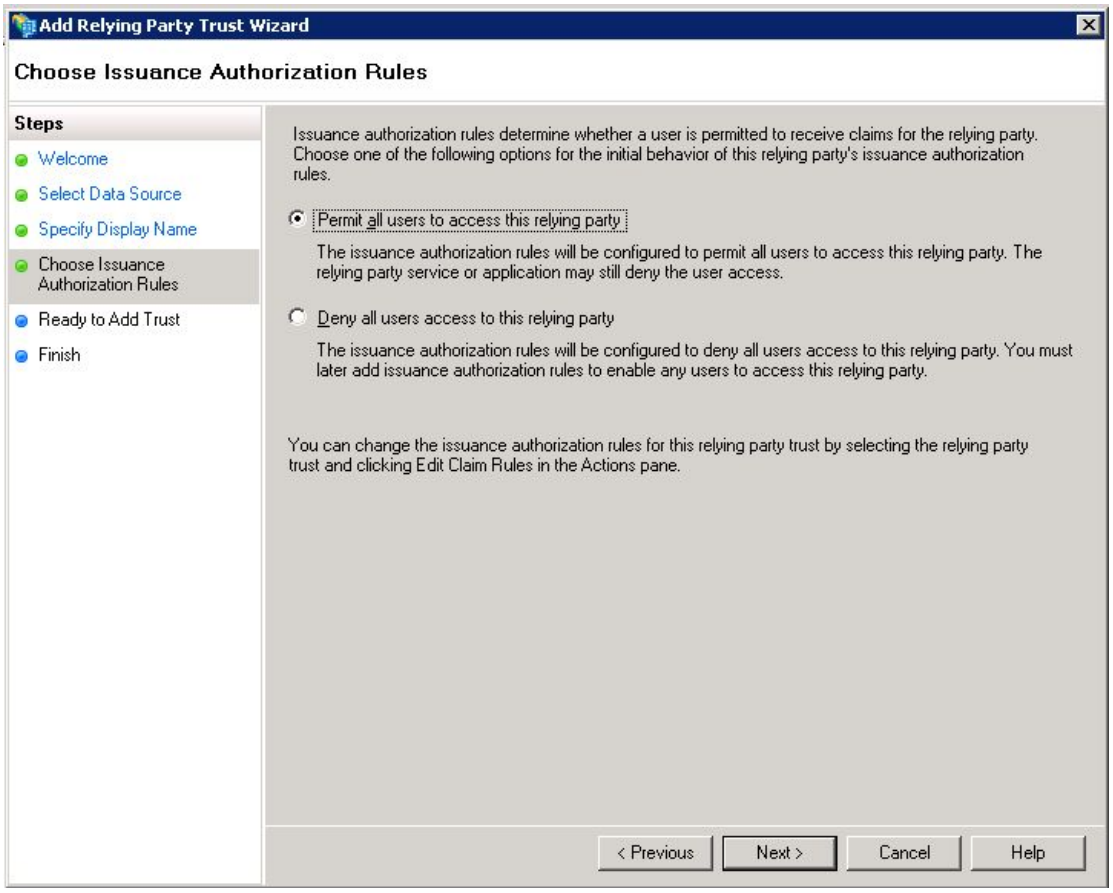
4. Click OK on the notice message



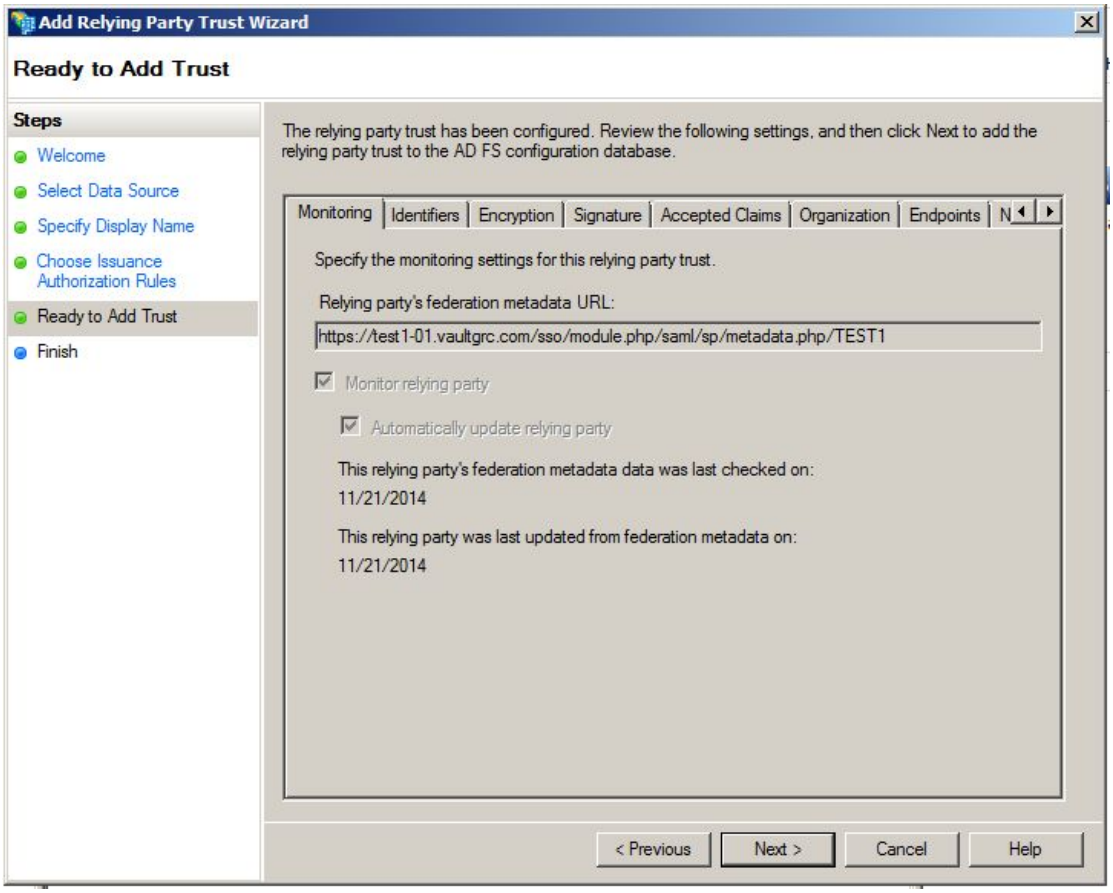
5. **Set the display name for the relying party and then click Next.**



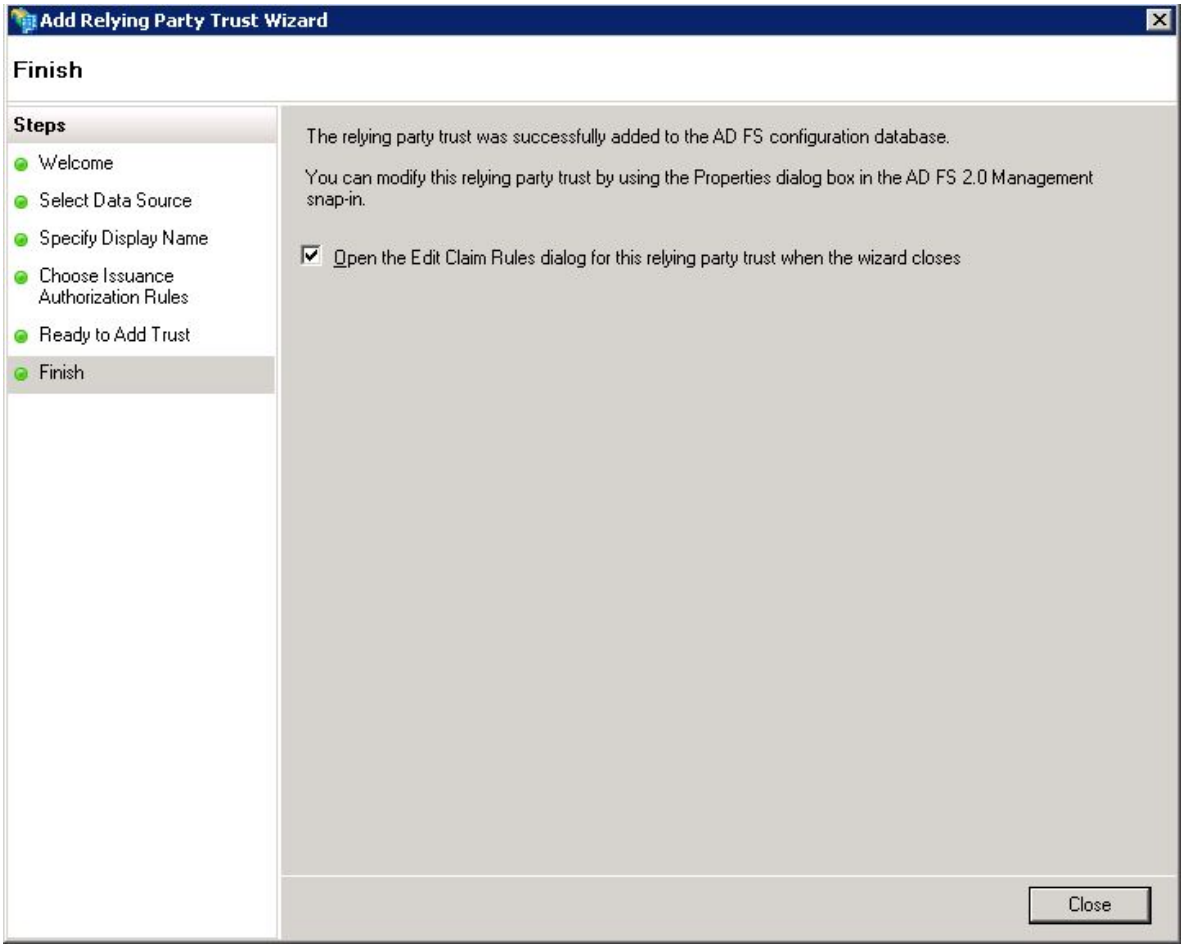
6. Choose your authorization rules. For my scenario, I chose Permit all users to access this relying party. When you're done, click Next.



7. **Review your settings and then click Next.**



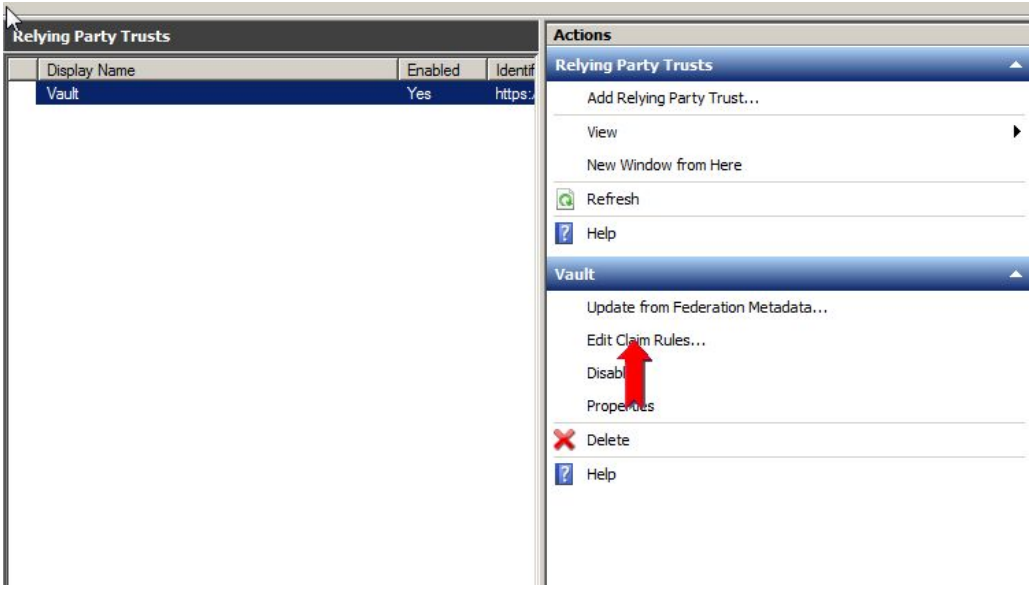
8. Check Open the Edit Claim Rules dialog for this relying part trust when the wizard closes and then click Close.



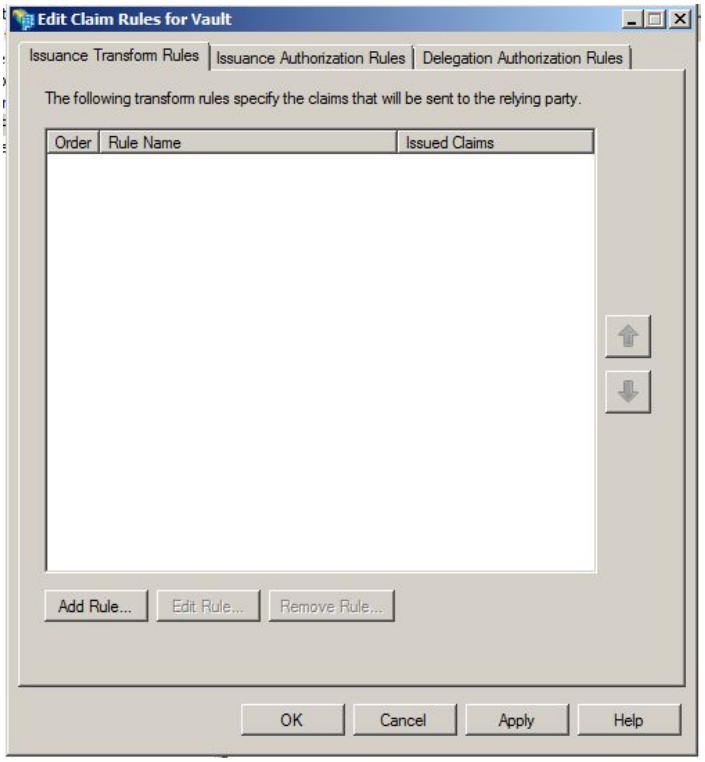
You're done configuring Vault as a relying party.

Configuring Claim Rules for the Vault Relying Party

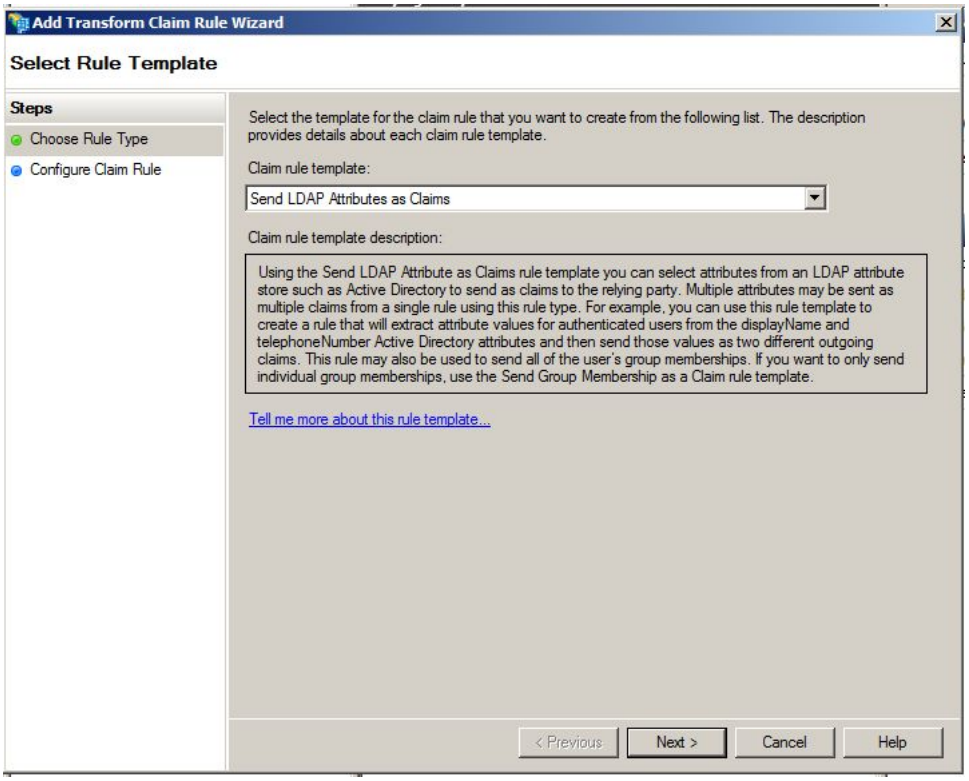
In these steps we're going to add the claim rules so that the elements Vault requires and ADFS doesn't provide by default (Name Id, principal) are added to the SAML authentication response. If you forgot to check the box to launch the claim rule dialog, right-click on the relying party (in this case Vault) and then click Edit Claim Rules.



Click on Add Rule...



Select Send LDAP Attributes as Claims (Default) and press Next

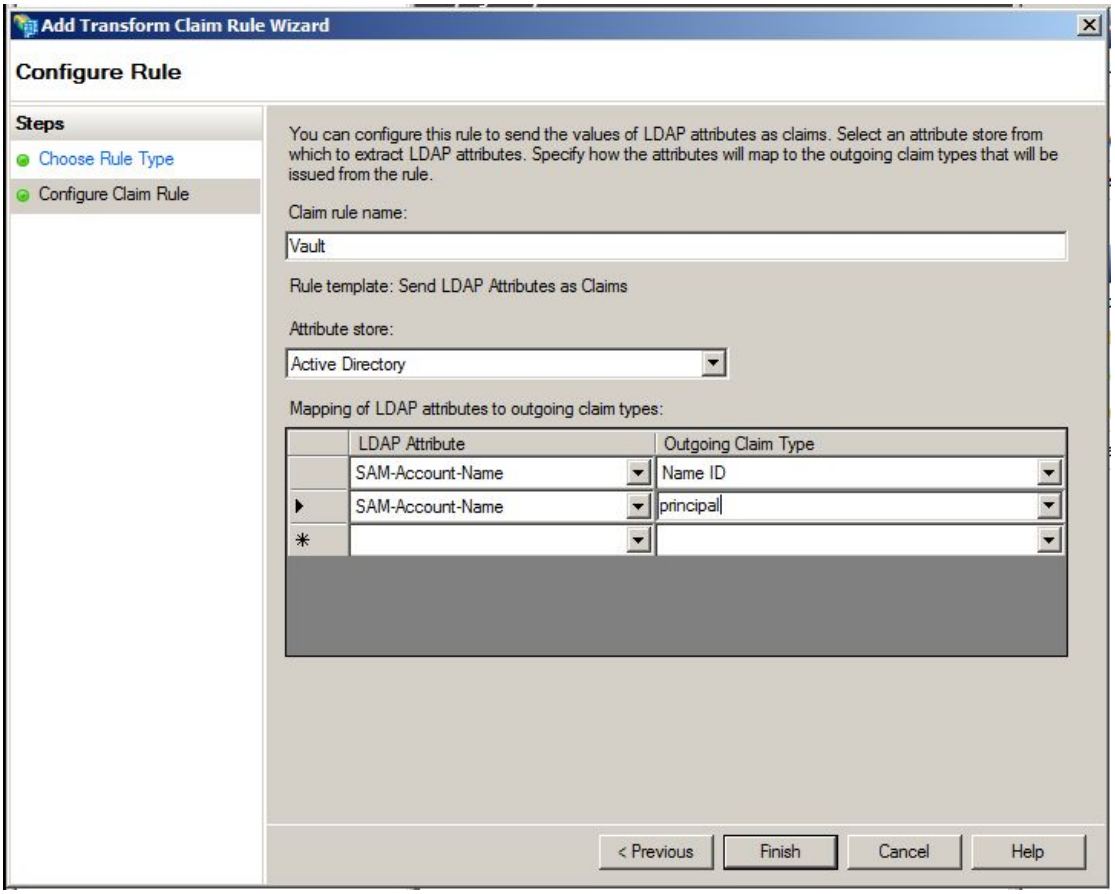


Add a Rule Name and Select Active Directory as the Attribute Store.

In the grid add the items below. Note: principal is not in the drop down list and must be added manually.

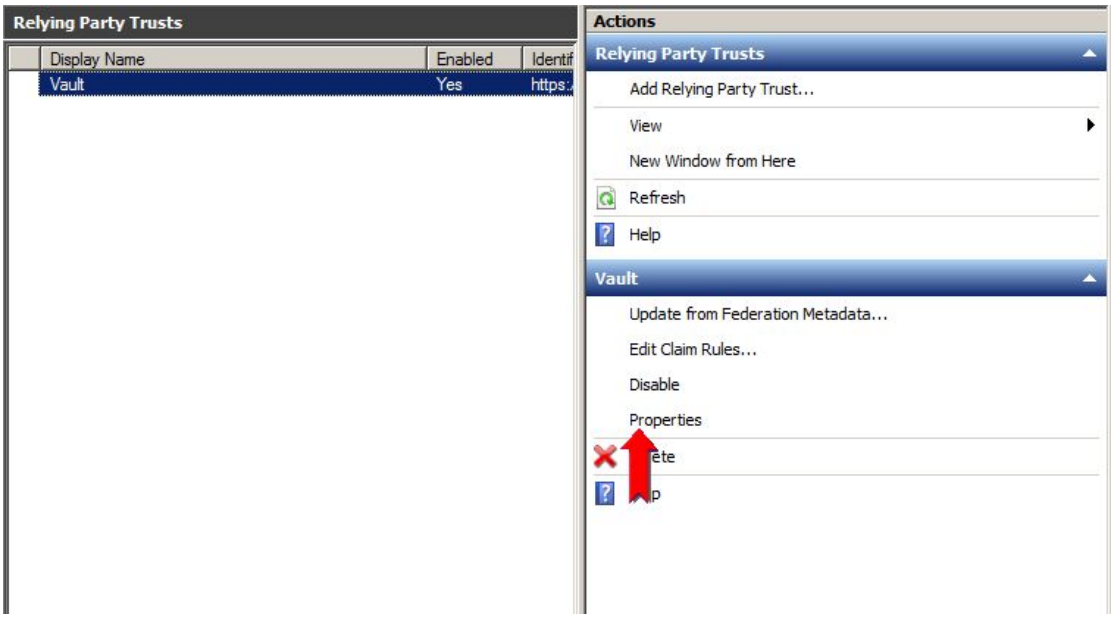
'User-Principal-Name', 'Employee Number' or 'SAM Account Name' can be used

SAM Account Name	Name ID
SAM Account Name	Principal

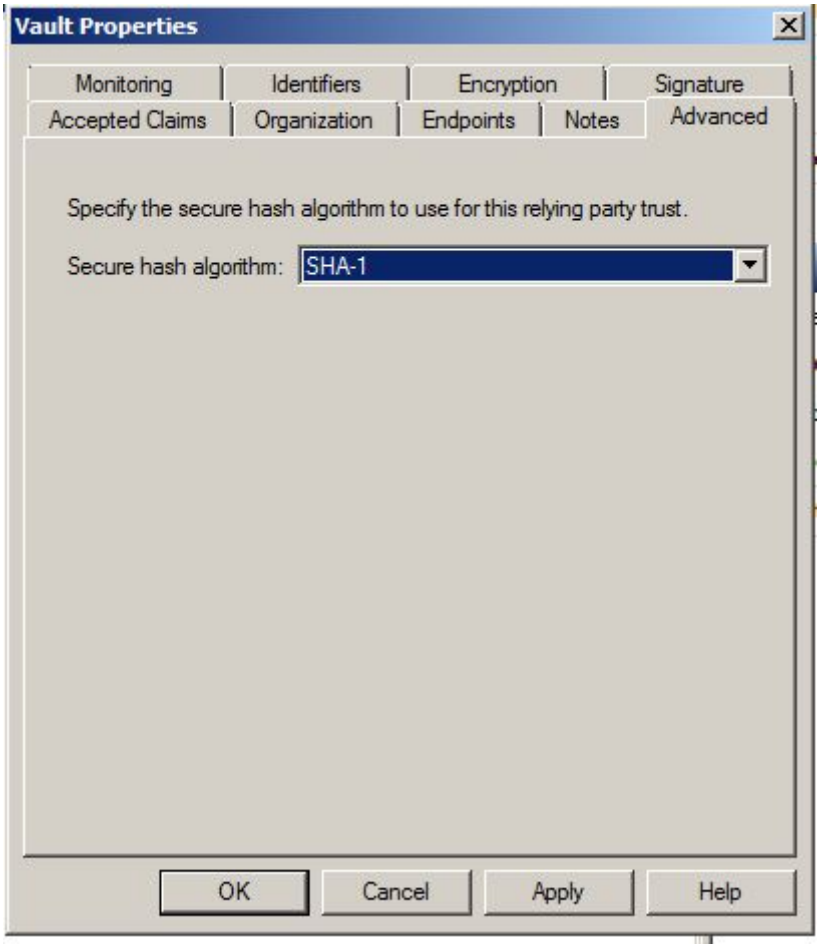


Click on Finish.

Now click on the Properties



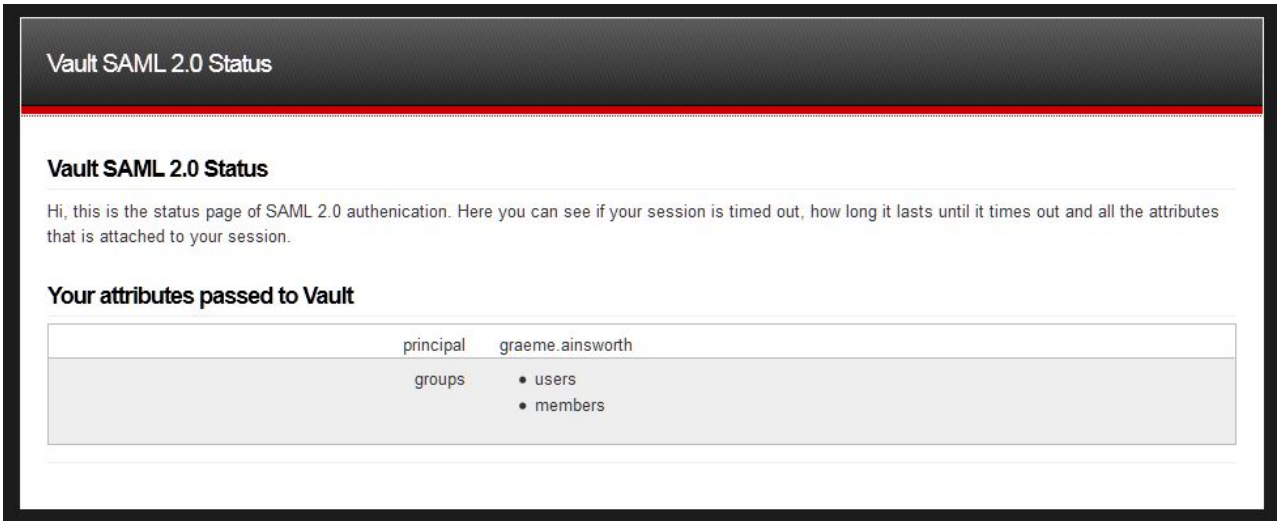
Select the Advanced tab and change the hash algorithm to SHA-1



Test with the link provided. It will have the following format.

https://[companyid]-01.vaultgrc.com/sso/module.php/core/authenticate.php?as=[COMPANYID]

If successful you will get to the following page.



If you get any other page then recheck the settings and contact Vault GRC support with the error message.

Token Signing Certificate Rollover

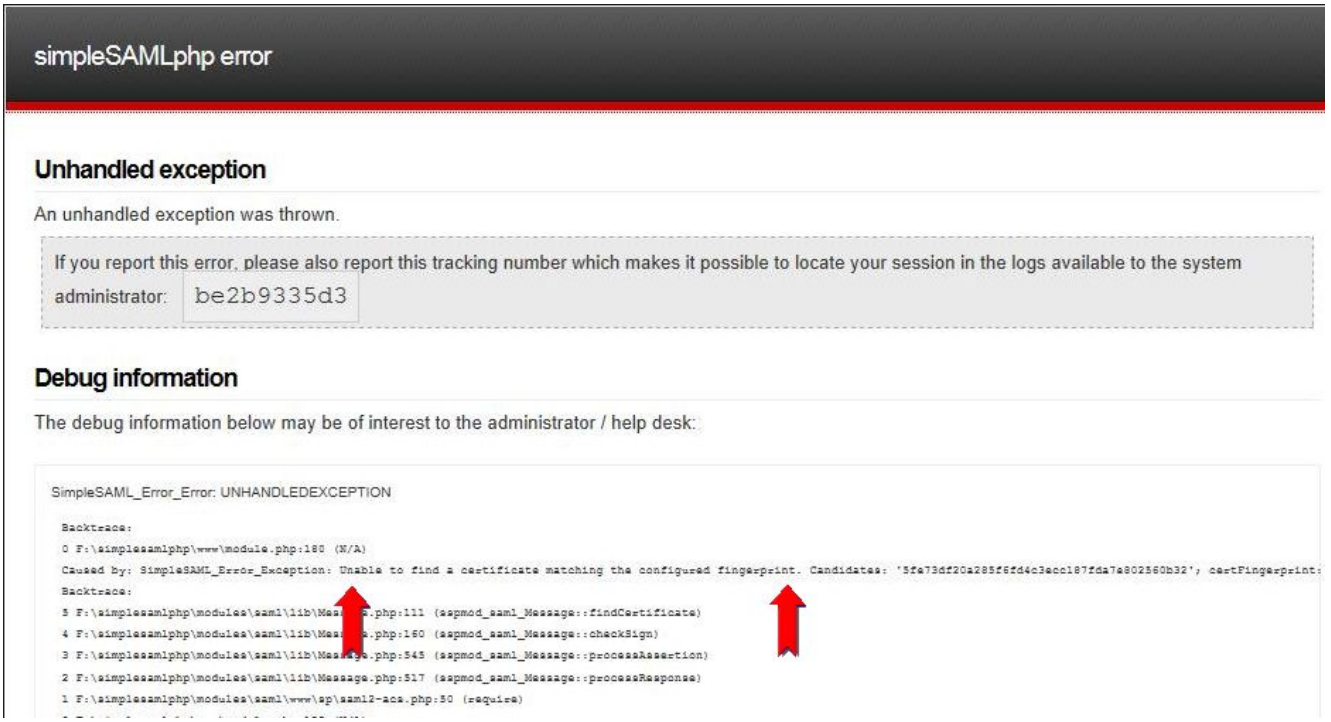
ADFS Default Behaviour

ADFS automatically creates a new Token Signing Certificate 20 days before the current token signing certificate expires. ADFS will automatically switch to use the new signing certificate as the primary signing certificate after 5 more days (15 days until the expiry of old signing certificate).

Error Condition

If Vault is not notified of the new certificate is used as primary without notifying Vault all attempts to login will fail with message in the stack trace:

Unable to find a certificate matching the configured fingerprint.



New Token Signing Key Procedure

Once the new key is generated (automatically or manually) the new certificate thumbprint is required to be sent to Vault (support@vaultgrc.com) for addition to the allowed list of thumbprints. At this stage both thumbprints will be valid. Once the rollover is complete and the old certificate is removed from ADFS contact support to remove the old thumbprint.

By following this method users should not experience any downtime logging into Vault.