GreenOrbit

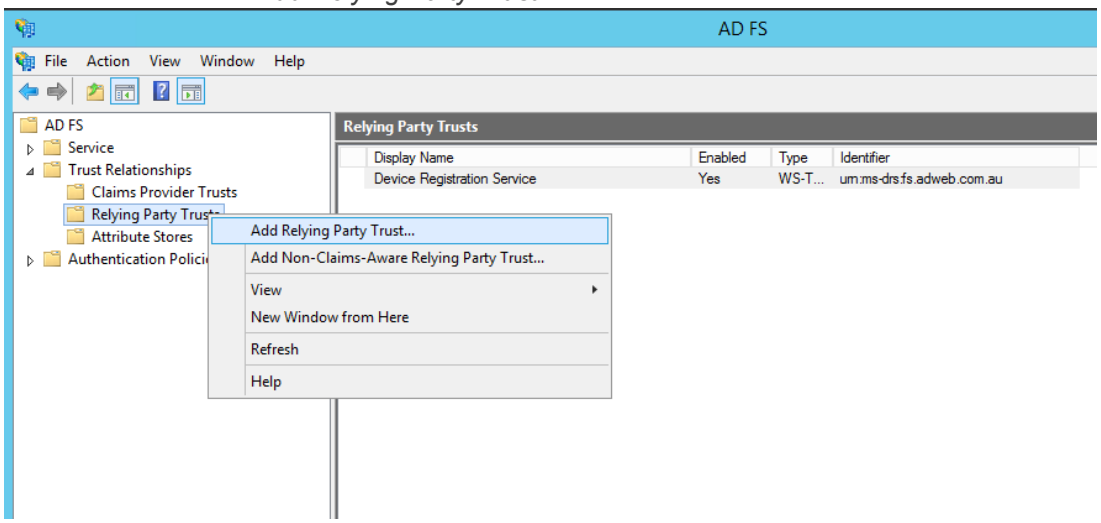
GREENORBIT GUIDE

Integrate GreenOrbit with ADFS

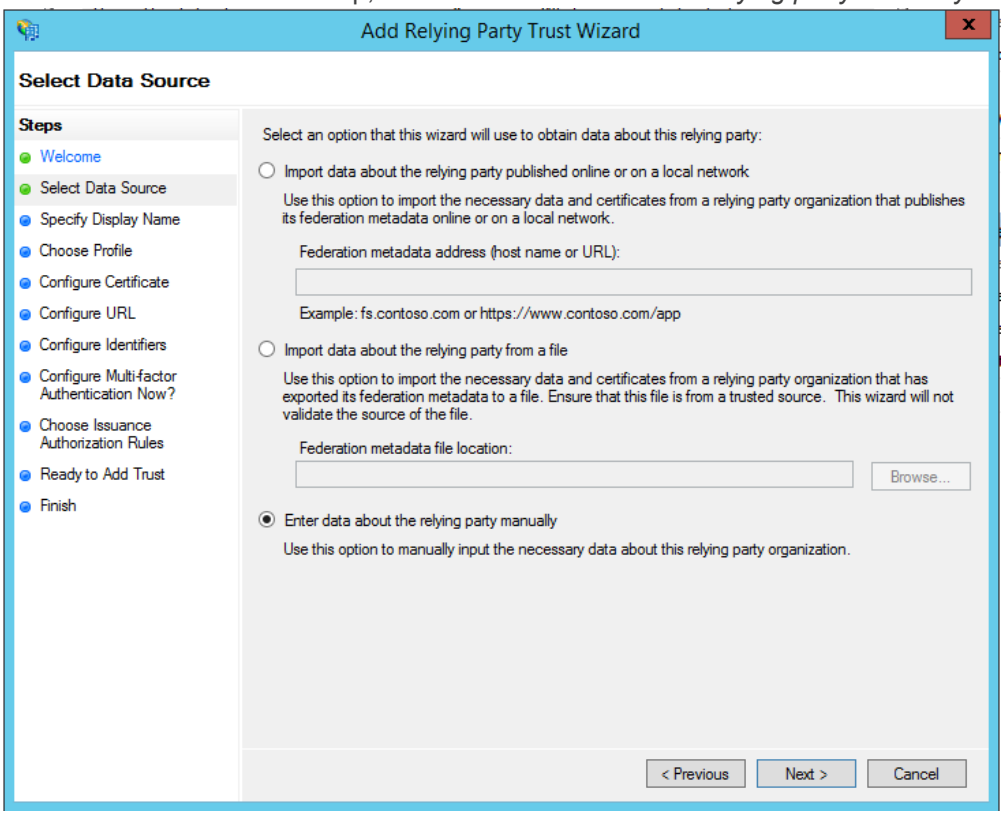
INTEGRATE WITH ADFS

Note: This guide assumes that ADFS is already implemented on your company network. For users to seamlessly be authenticated you will also need to ensure the URL of your ADFS server is added to the local intranet zone of the end users' computer.

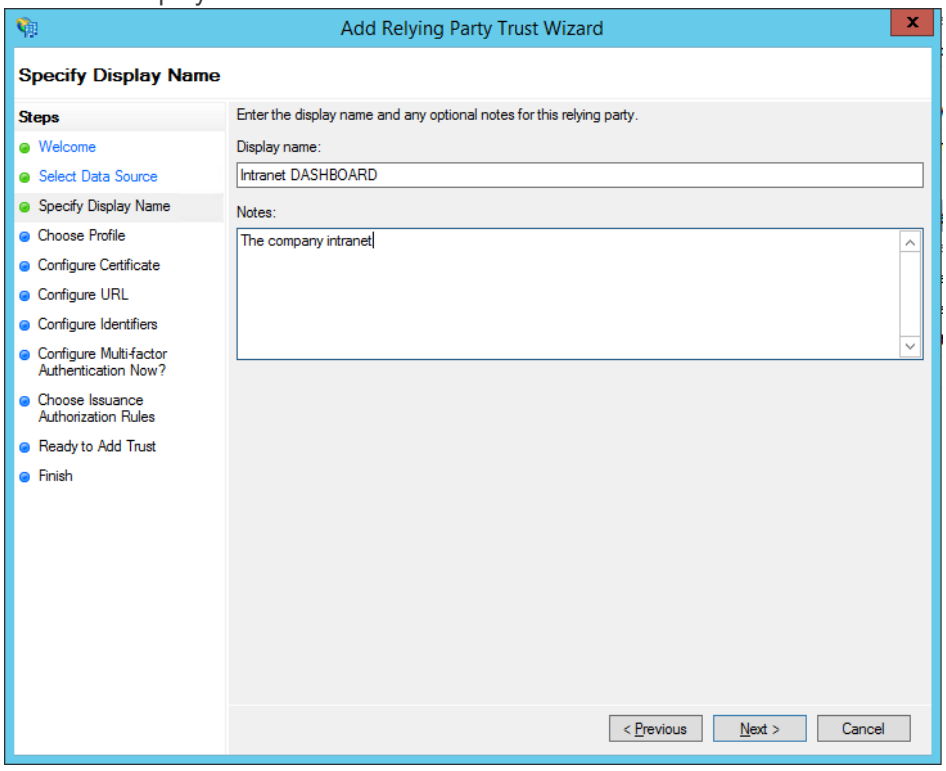
1. Open the ADFS Management Console and select *Trust Relationships* > *Relying Party Trusts*. Right click this folder and select *Add Relying Party Trust*



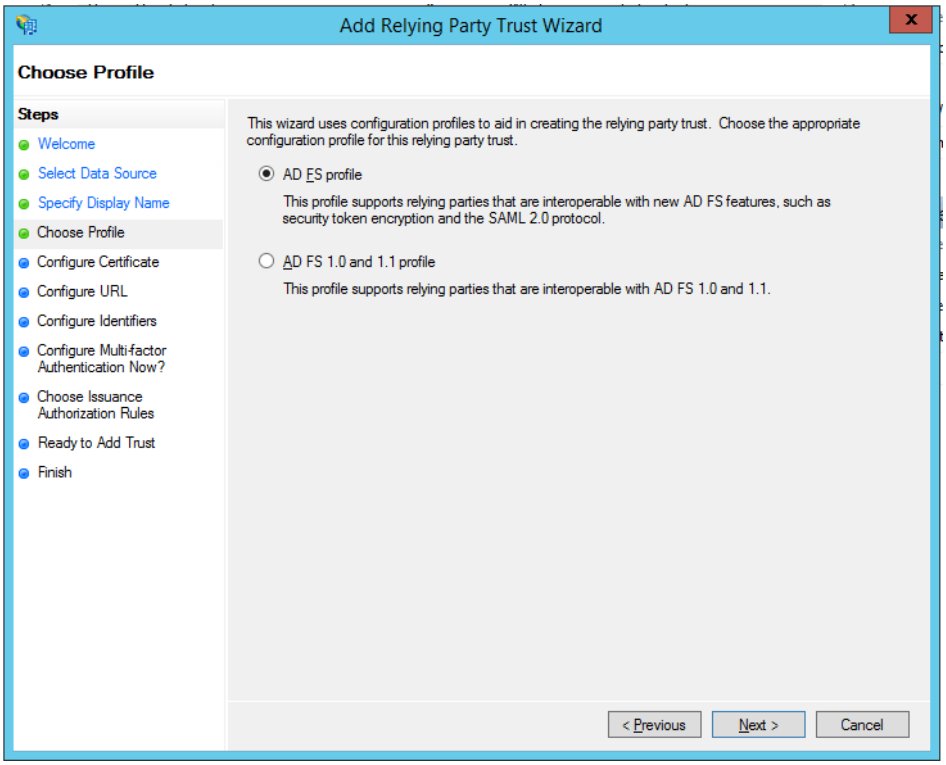
2. At the *Select Data Source* step, select *Enter data about the relying party manually*



3. Provide a display name and some notes about the item



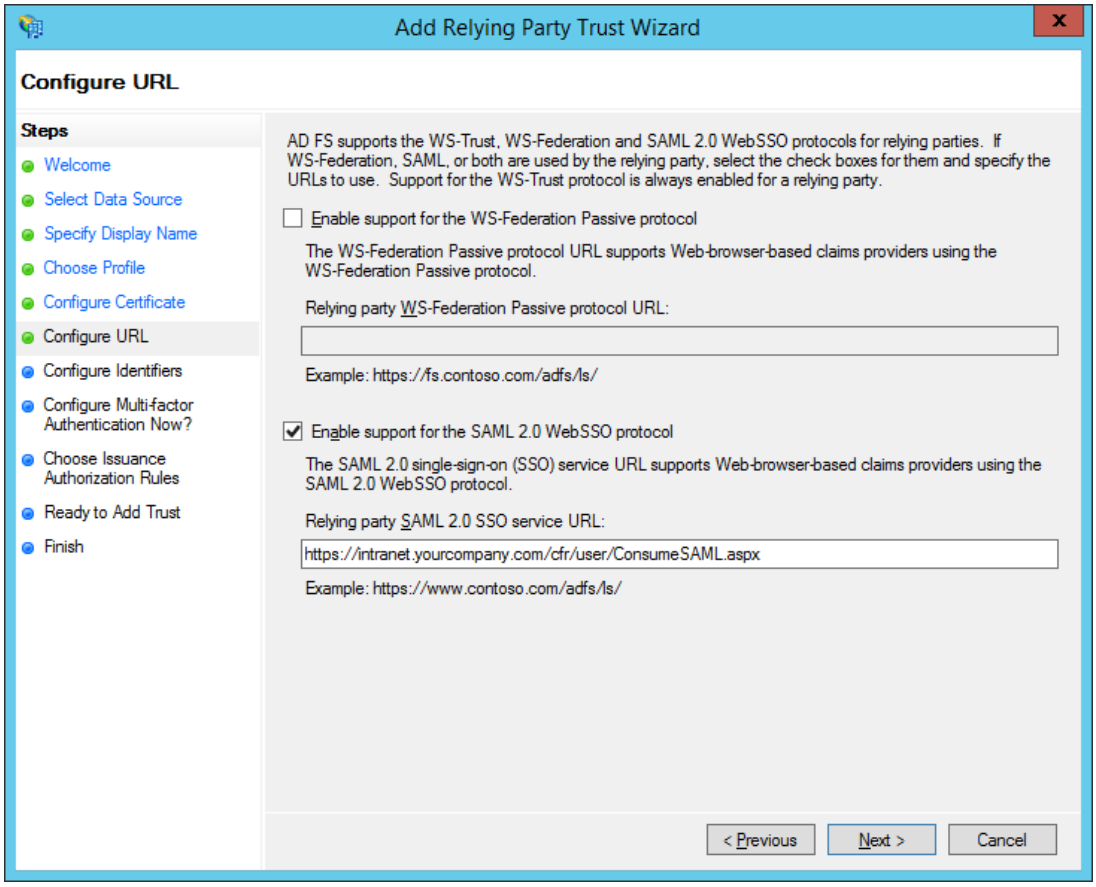
4. Select *AD FS profile* at the *Choose Profile* step as this profile supports the SAML 2.0 protocol which is required for integration with GO.



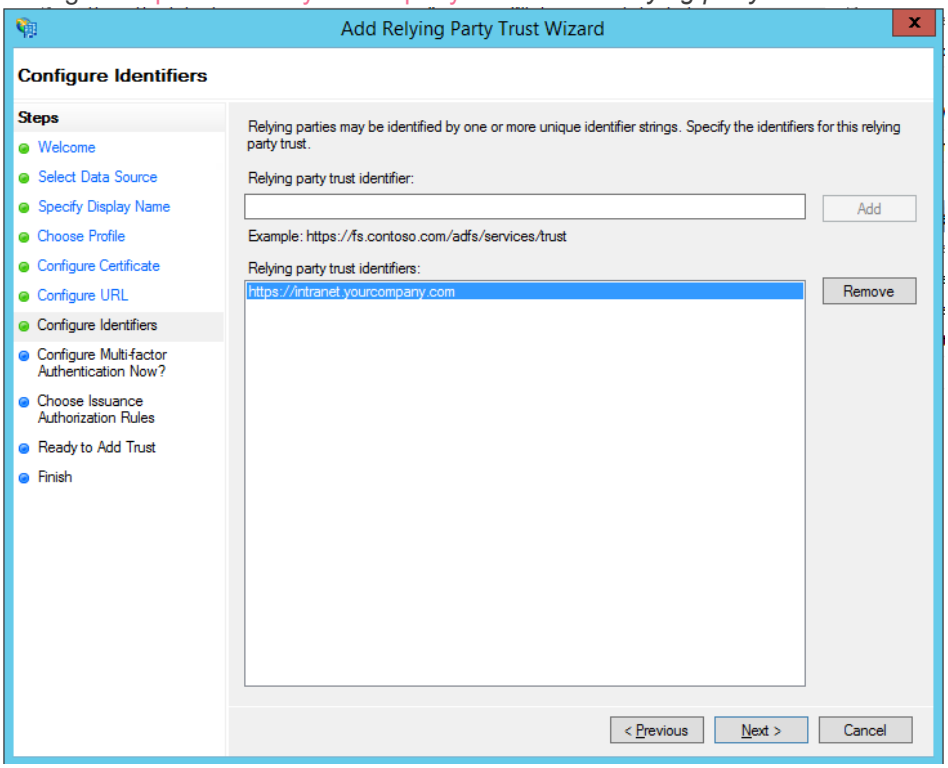
5. Skip over the *Configure Certificate step*

6. At the *Configure URL* step select *Enable support for the SAL 2.0 WebSSO protocol* and enter in the address of your intranet, eg. https://intranet.yourcompany.com/cfr/user/ConsumeSAML.aspx

   Please note that this URL is case-sensitive and should match the casing of the example above exactly – ie. all lower case except for “ConsumeSAML.aspx” at the end.

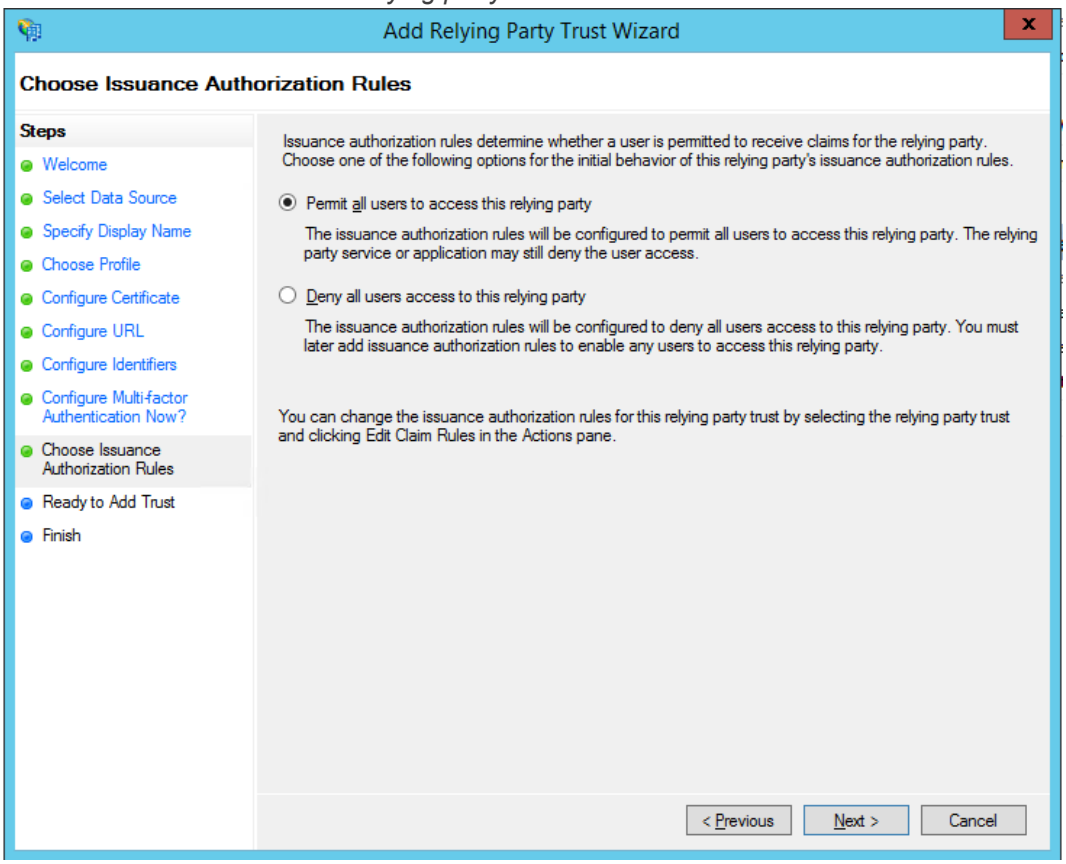


7. Configure https://intranet.yourcompany.com as the *Relying party trust identifier*



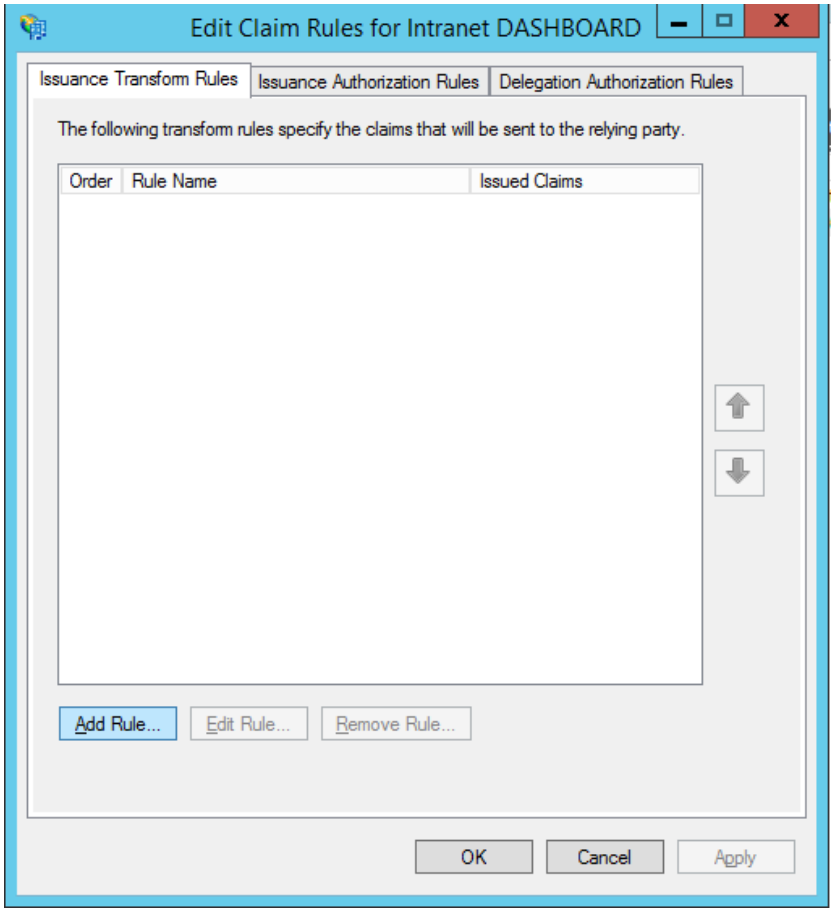
8. Do not configure *multi-factor authentication* when prompted.

9. *Permit all users to access the relying party* when at the *Choose issuance authorization rules* step.



10. Click next through to the end of the wizard and when prompted at the end, open *Edit Claim Rules* to setup the transformation rules.

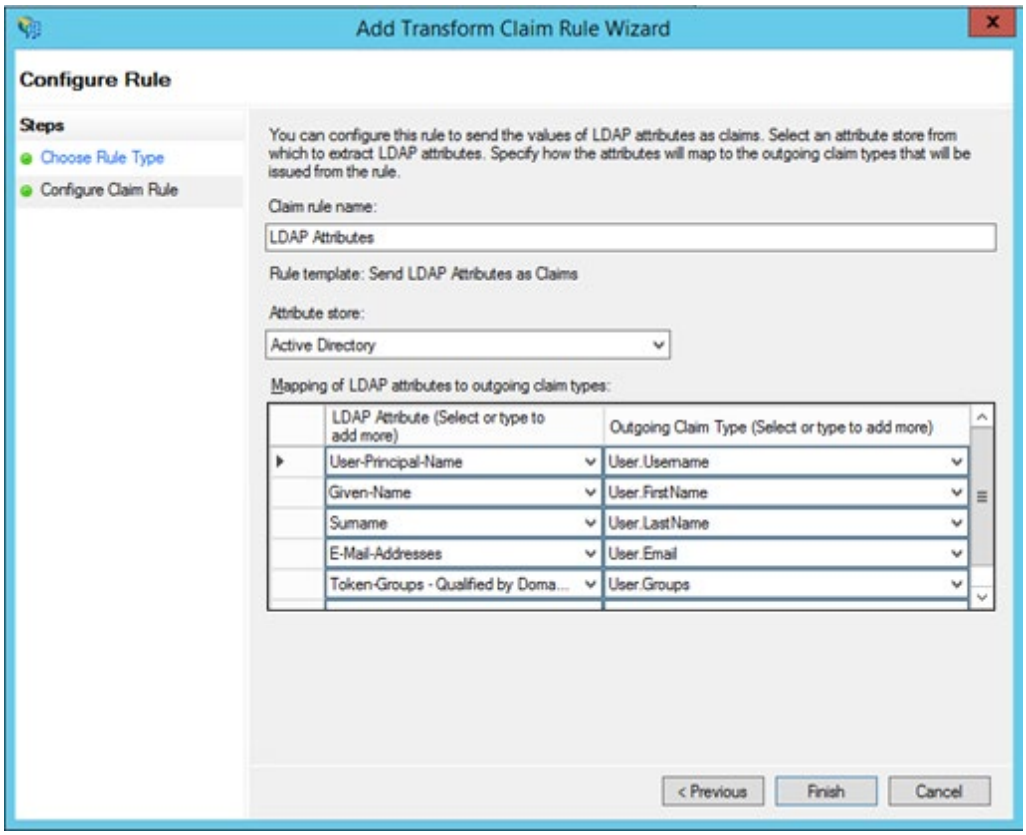
11. In the *Issuance Transform Rules* interface, click *Add Rule* to add a new transformation.



12. Choose the option *Send LDAP attributes as claims* when prompted and fill in the details as required.

    Claim Rule Name: LDAP Attributes
    Attribute Store: Active Directory

    and add in the following mappings:
    - User-Principal-Name → User.Username
    - Given-Name → User.FirstName
    - Surname → User.LastName
    - E-Mail-Addresses → User.Email
    - Token-Groups – Qualified by Domain Name → User.Groups



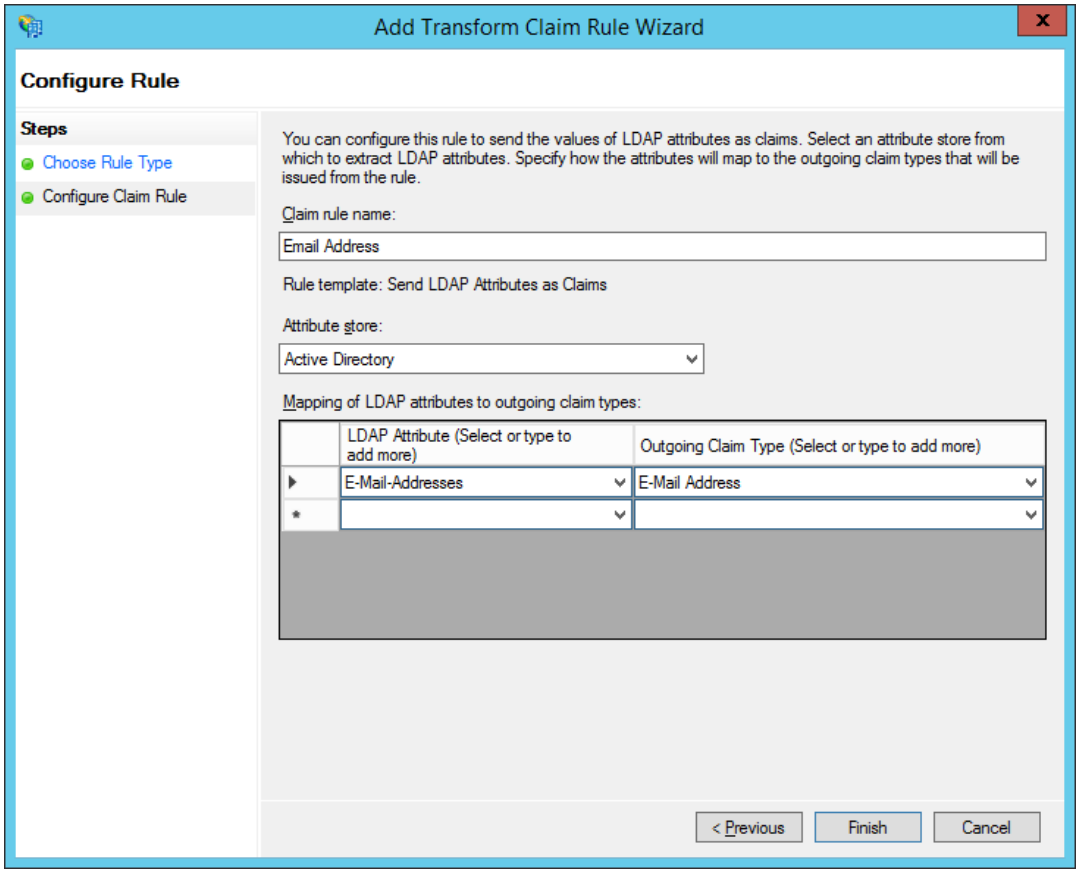
13. Click *Finish* to add the rule.

14. In the *Issuance Transform Rules* interface, click *Add Rule* again to add a second new transformation.

15. Choose the option *Send LDAP attributes as claims* when prompted and fill in the details as required.

    Claim Rule Name: Email Address
    Attribute Store: Active Directory

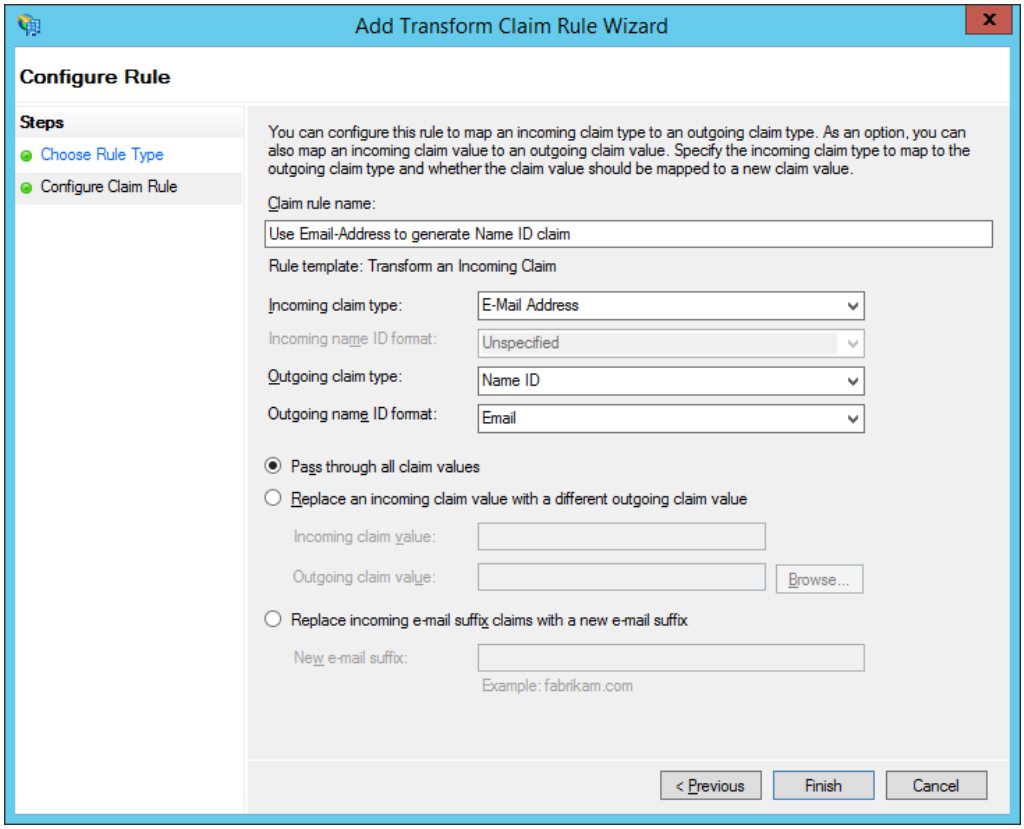
    and add in the following mapping:
    - E-Mail-Addresses → E-Mail Address



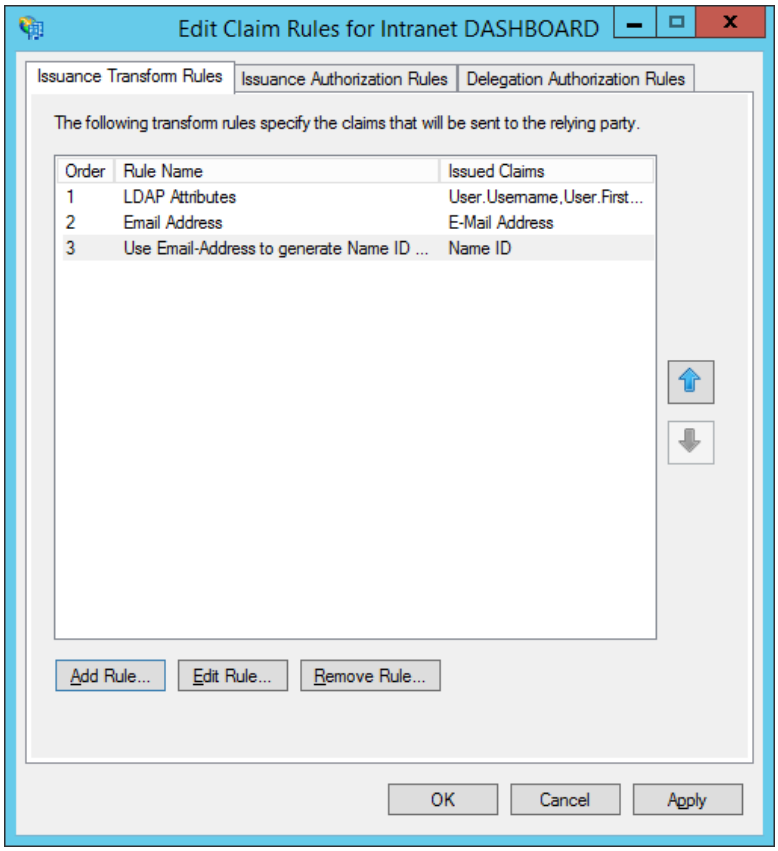
16. Click *Finish* to add the rule.

17. In the *Issuance Transform Rules* interface, click *Add Rule* again to add a third new transformation.

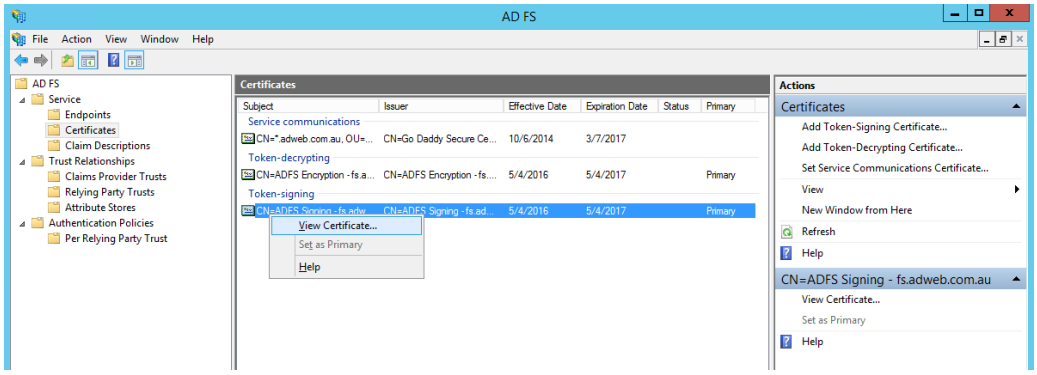
18. Choose the option *Transform an Incoming Claim* when prompted and fill in the details as required.
    Claim Rule Name: Use Email-Address to generate Name GO claim
    Incoming claim type: E-mail Address
    Outgoing claim type: Name GO
    Outgoing name GO format: Email
    Pass through all claim values



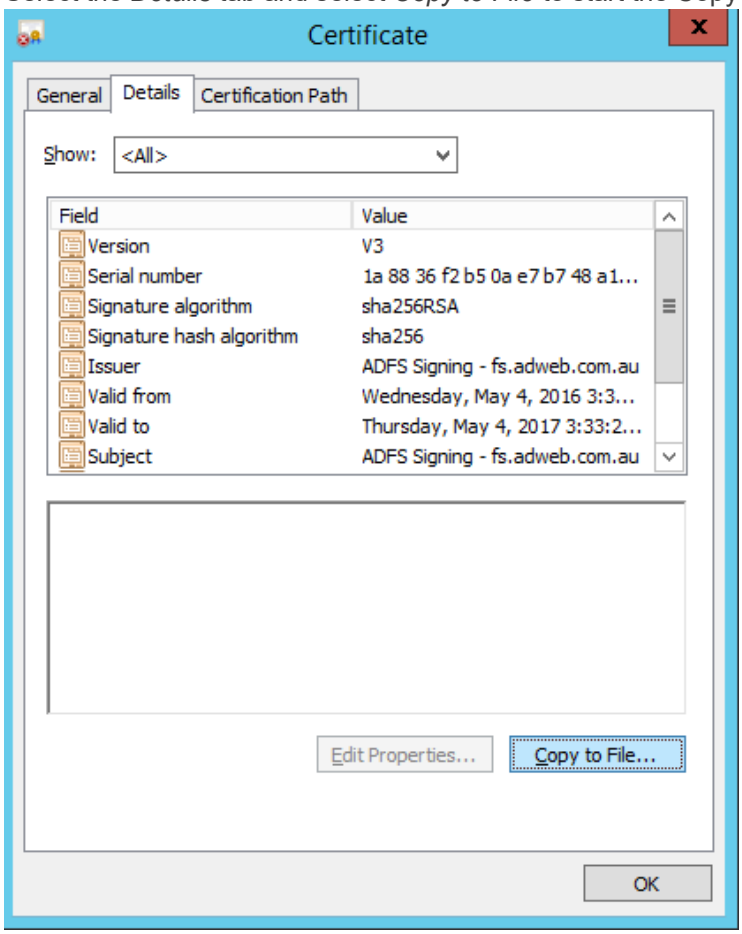
19. Save all changes by selecting *Finish* and *Apply* to go back to the main ADFS Management Console.



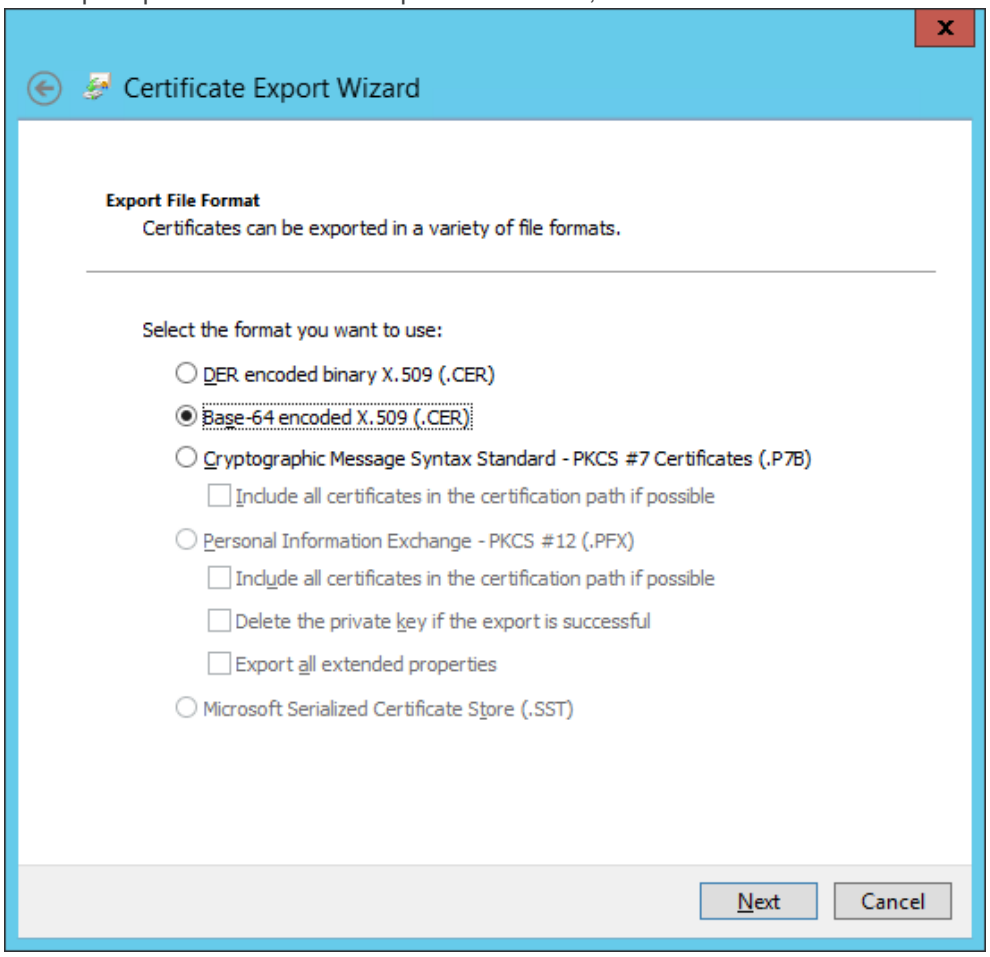
20. We now need to get the signing token to place into GO. Right click on the *Token-Signing* certificate and select *View Certificate*



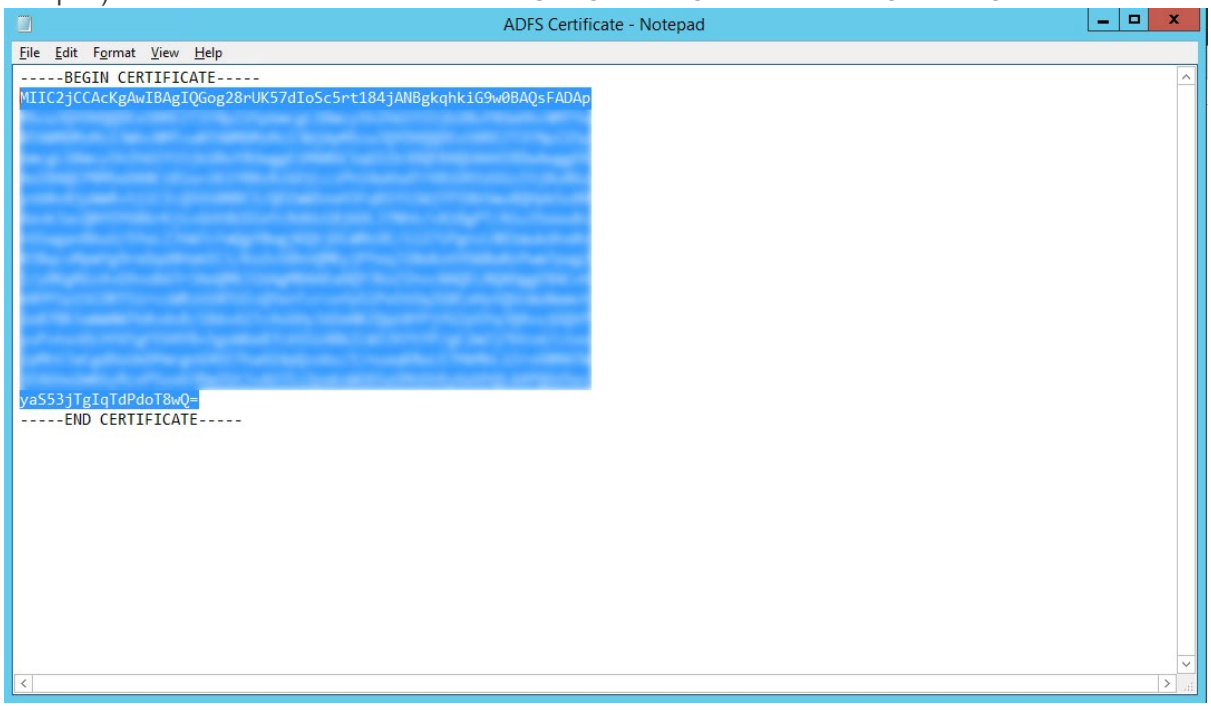
21. Select the *Details* tab and select *Copy to File* to start the Copy Wizard



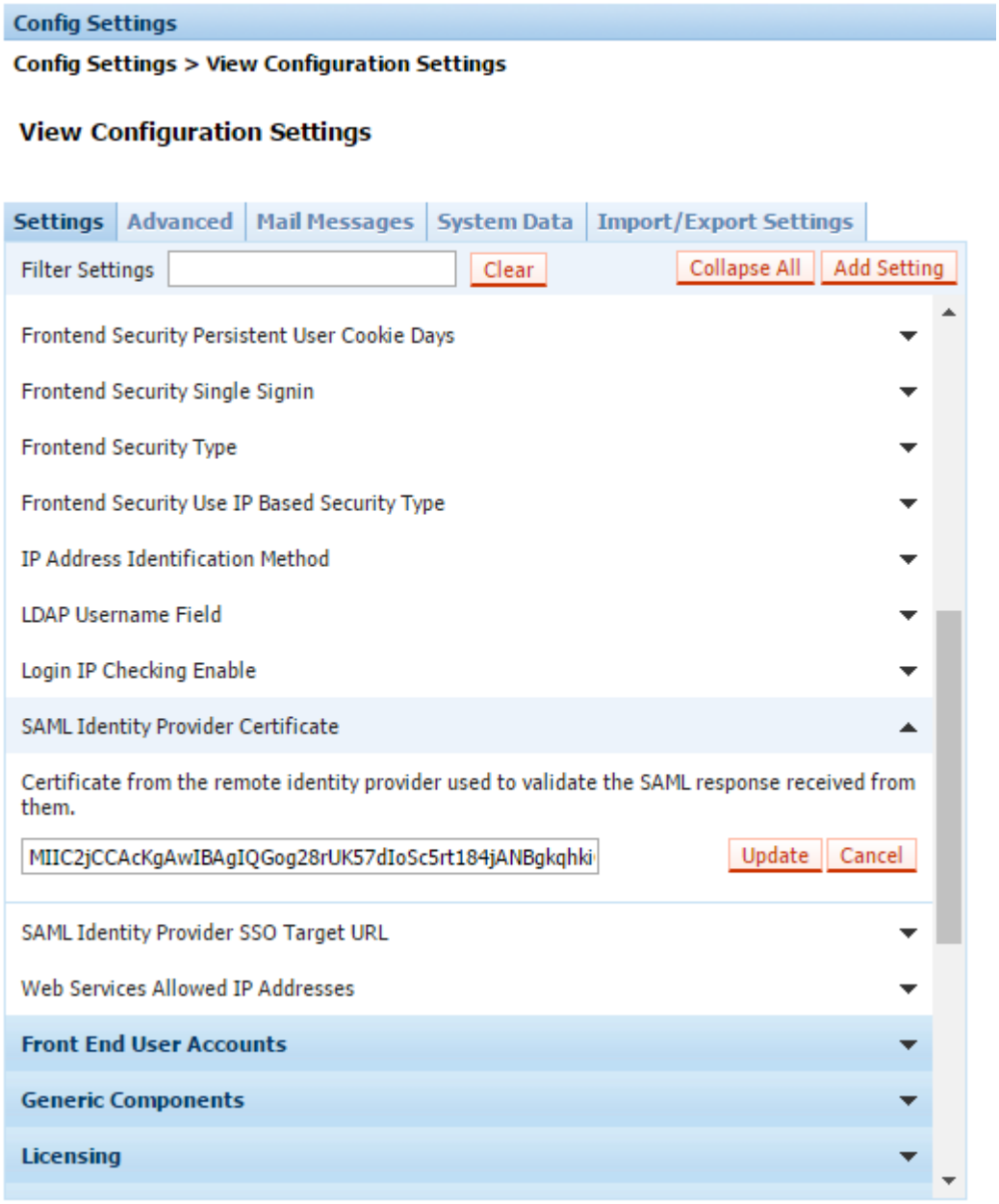
22. When prompted to choose the Export File Format, choose *Base-64 encoded X.509 option*



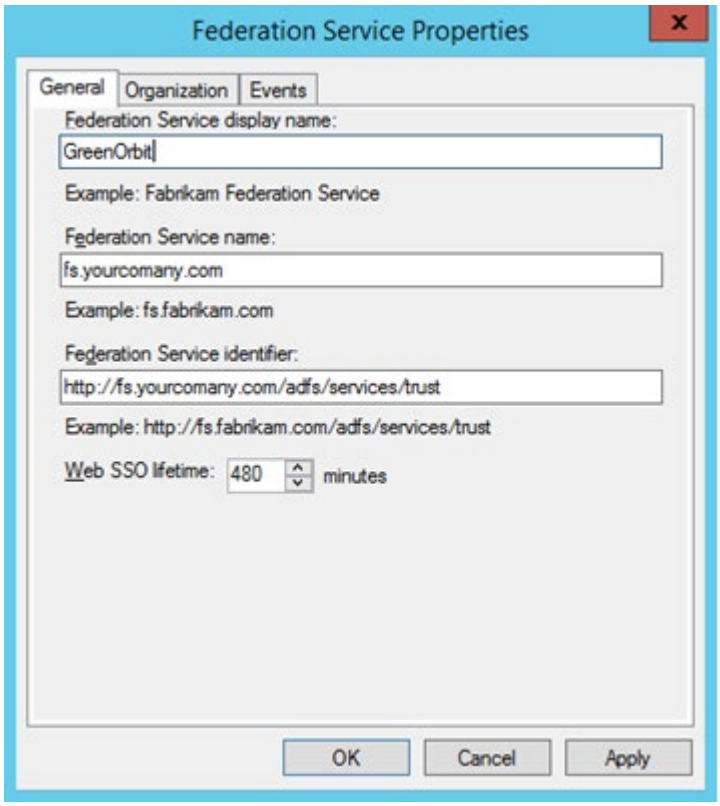
23. Save the file to an easy to access location and then open it with your preferred text editor (such as notepad) and select the text between the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines.

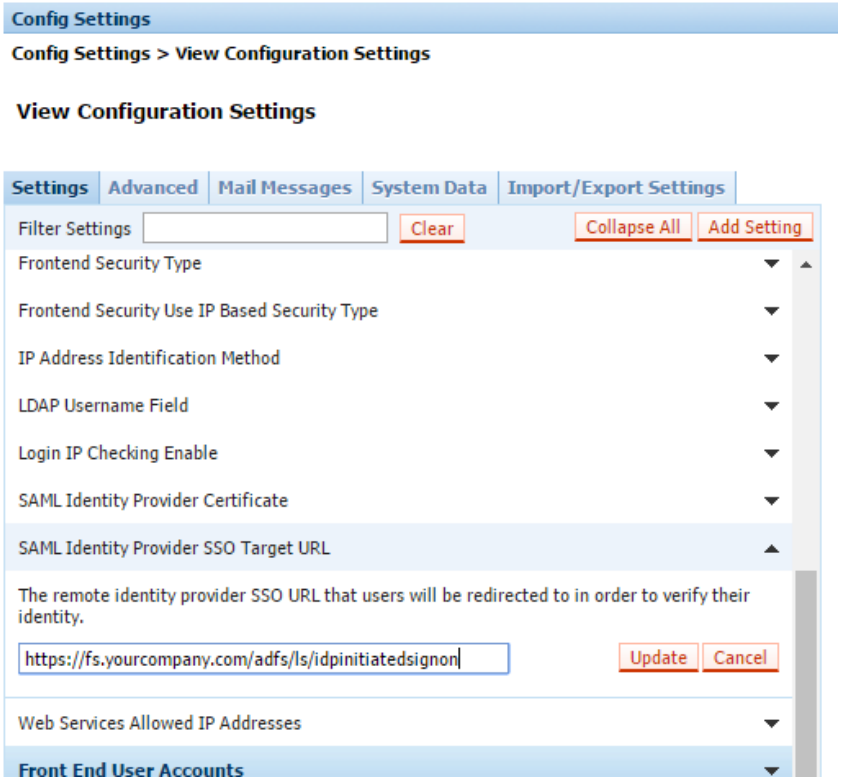


24. Login to your GO Administration interface and navigate to *Utilities* > *Config Settings* and find the setting called *SAML Identity Provider Certificate* and paste the certificate string into the text field and choose *Update*



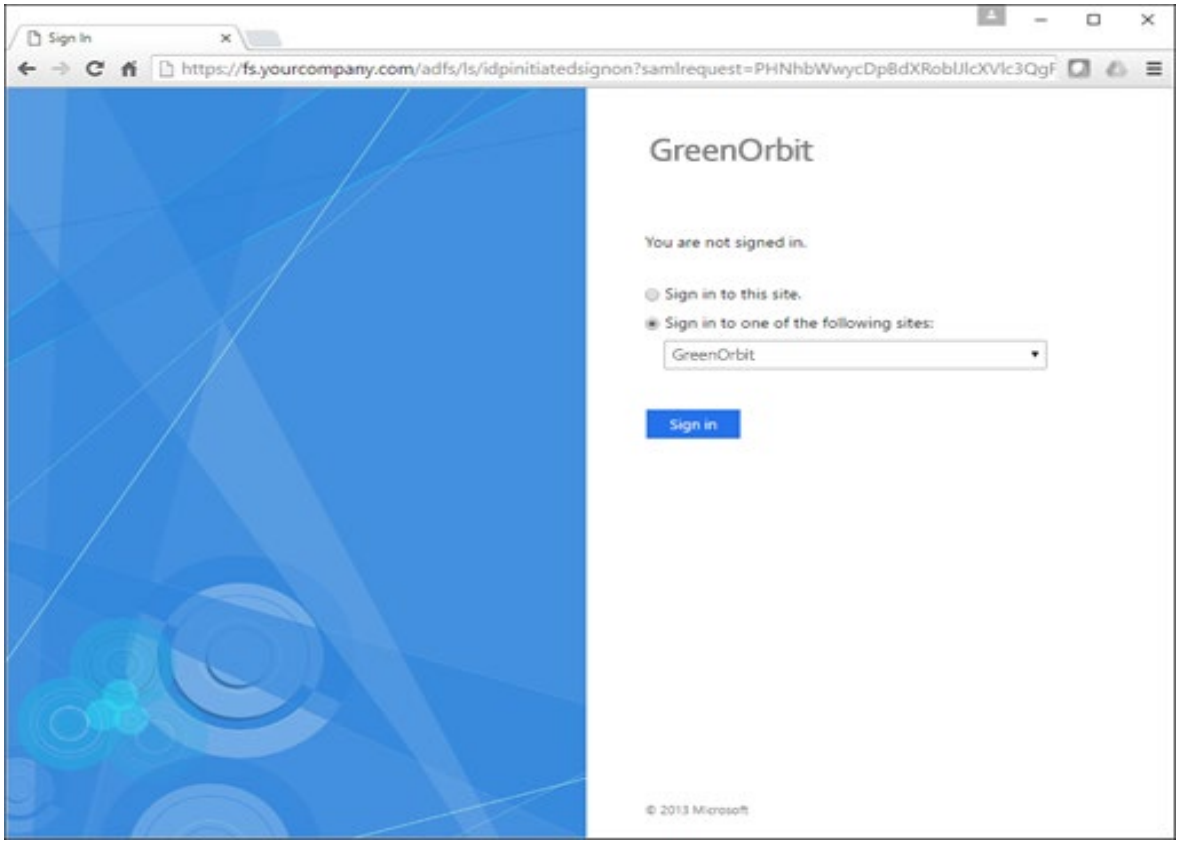
25. Now select the Config Setting *SAML Identity Provider SSO Target URL*, this is the URL of your ADFS server endpoint, and can be found in the *Federation Service Name* of the *Federation Service Properties* in ADFS. Get this name and then put it into GO's config setting as: https://fs.yourcompany.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https://intranet.yourcompany.com





26. If you haven't already done so, also change the Frontend Security Type to *Login using SAML*. Follow the guide on our help site to learn how to do this: http://help.intranetdashboard.com/systemadmin/Security/ChangingtheFrontendSecurityType.html

27. Now when accessing your intranet address, eg https://intranet.yourcompany.com you'll be redirected to authenticate by ADFS prior to being logged into the site.



28.

TROUBLESHOOTING

1. If there is an authentication error when GO is loaded after entering credentials within ADFS you may need to adjust a *Config Settings* called *SAML Authentication Request Format* and change it from *Default* to *Deflate and Base64* by clicking *Edit* making the change from the dropdown and clicking *Update*.

ADDITIONAL INFORMATION

If you have been unsuccessful configuring ADFS to act as an SAML Identity Provider for GO, please reach out to our support team at support@greenorbit.com.