daptiv™

Daptiv SSO and AFDS 2.0

ADFS 2.0 Setup Guide for Daptiv SSO

INTRODUCTION

ADFS 2.0 is a widely used SSO software available free from Microsoft. Because of the prevalence of this software, we have found that many of our clients utilize ADFS 2.0. This guide is provided as general guidance on how to configure ADFS 2.0 with Daptiv only; Daptiv does not provide support for ADFS 2.0. If you need software or hardware troubleshooting, please contact Microsoft directly.
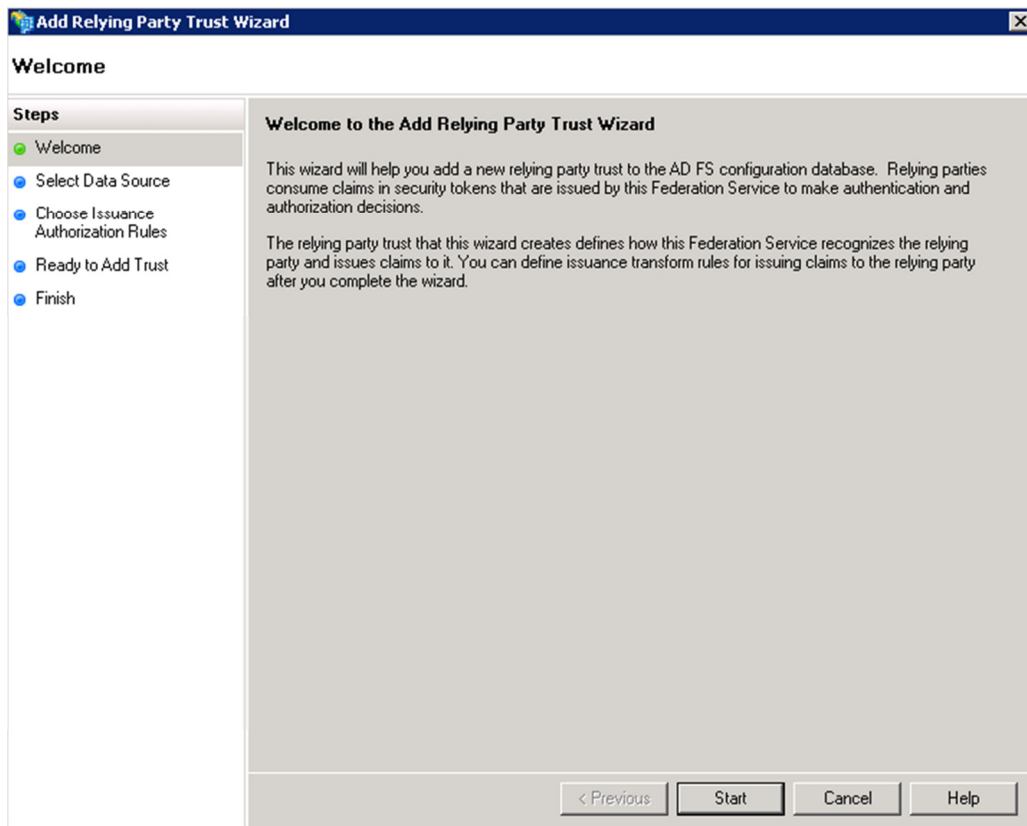
This guide assumes that you have ADFS 2.0 installed on a machine already, with or without other SSO integrations set up.

Steps:

1) Open the ADFS 2.0 Management Console from the Administrative Tools menu, and choose to 'Add Relying Party Trust...'
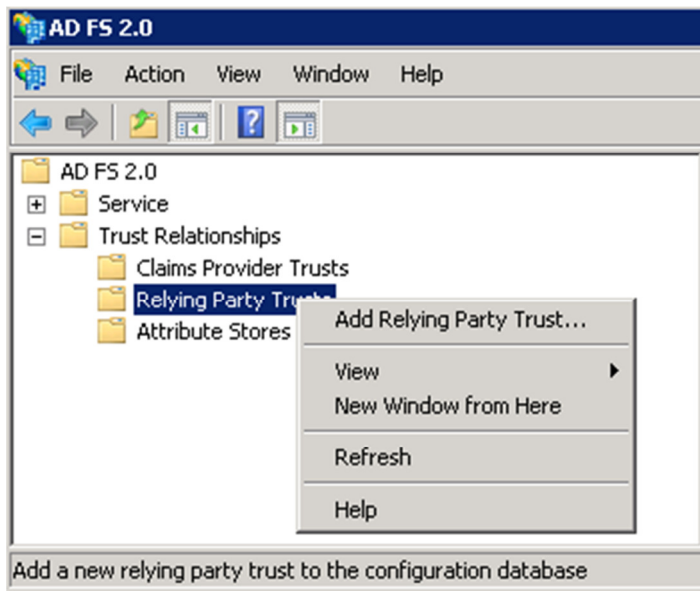
2) Click through the introductory screen.

Add Relying Party Trust Wizard

Welcome

Steps
- Welcome
- Select Data Source
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

< Previous   Start   Cancel   Help

3) Choose to import data from a file, and select the location of the metadata XML file.

4) Choose a display name for this integration.

5) Choose your configuration for access; it is usually to allow all users access.
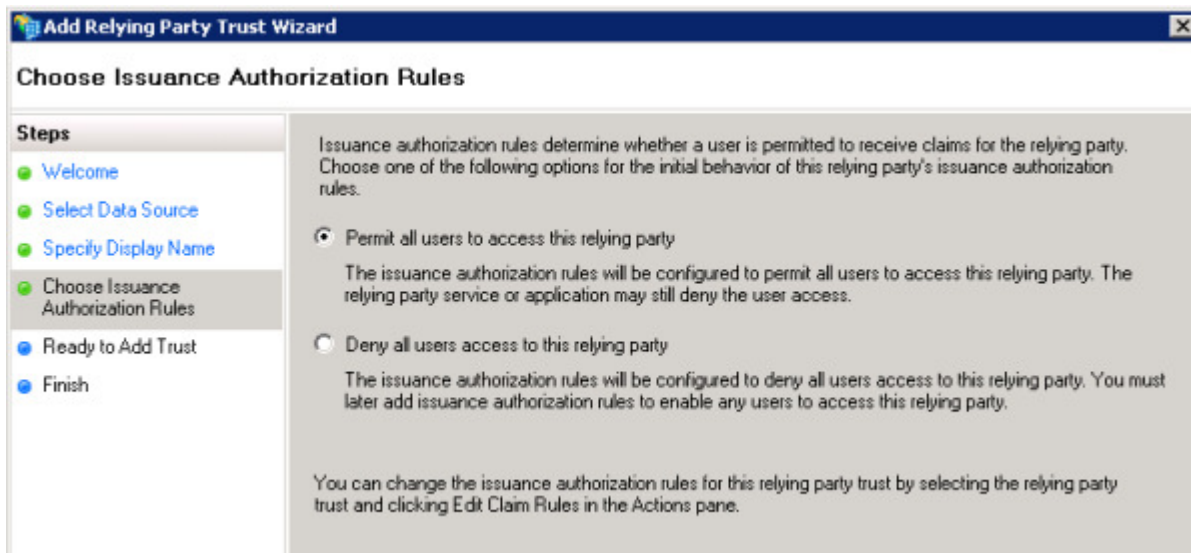
6) View a summary of the information. Note that in this summary page, some settings cannot be changed and we must come back to the configuration page later.

7) Choose to open the Claims window when complete.

8) Choose to add a new rule.

9) Choose to send LDAP Attributes as Claims.

Add Transform Claim Rule Wizard ☒

Select Rule Template

Steps
- ● Choose Rule Type
- ● Configure Claim Rule

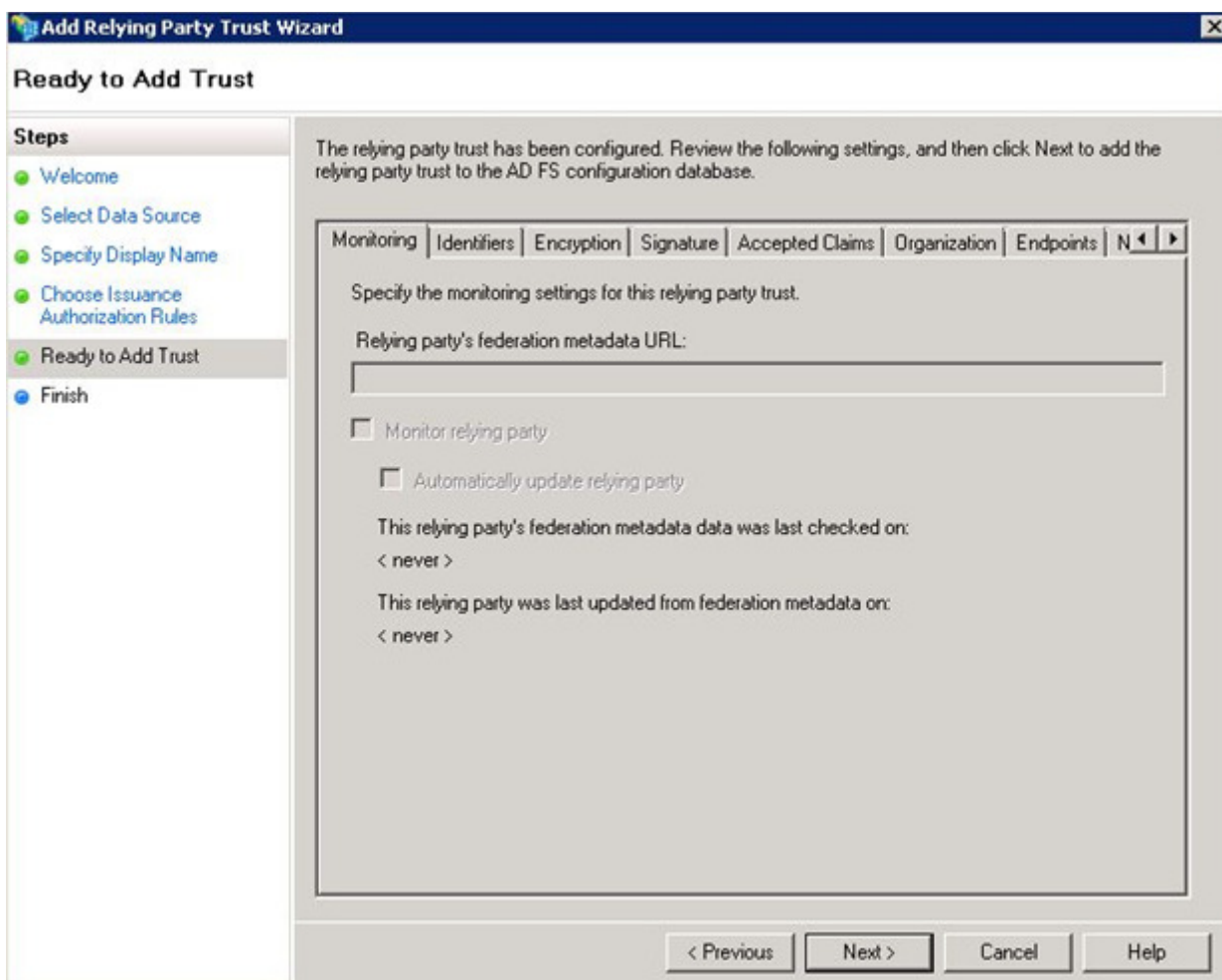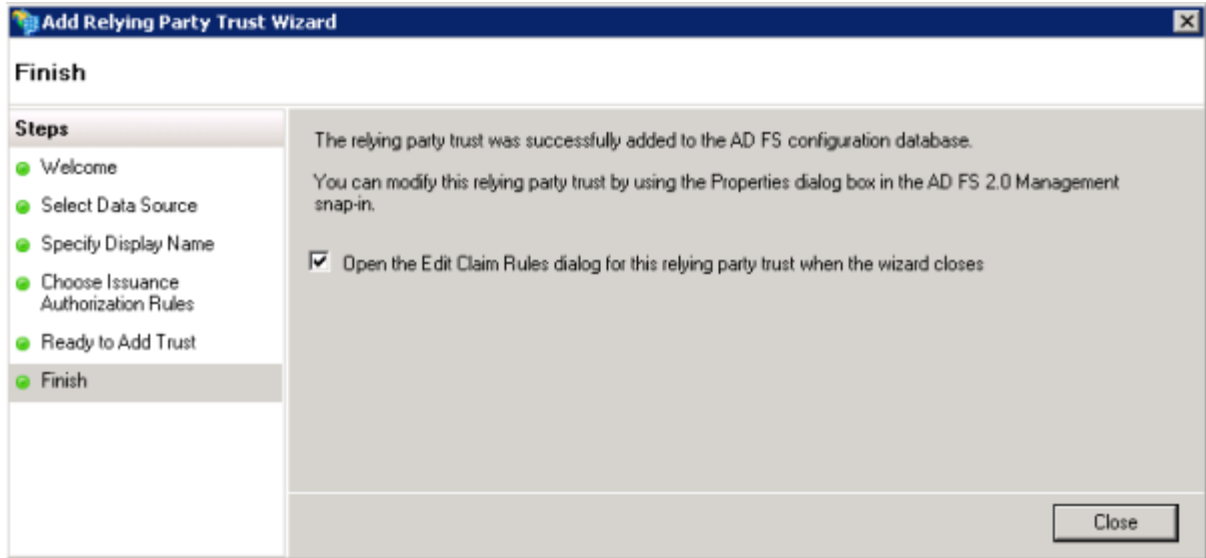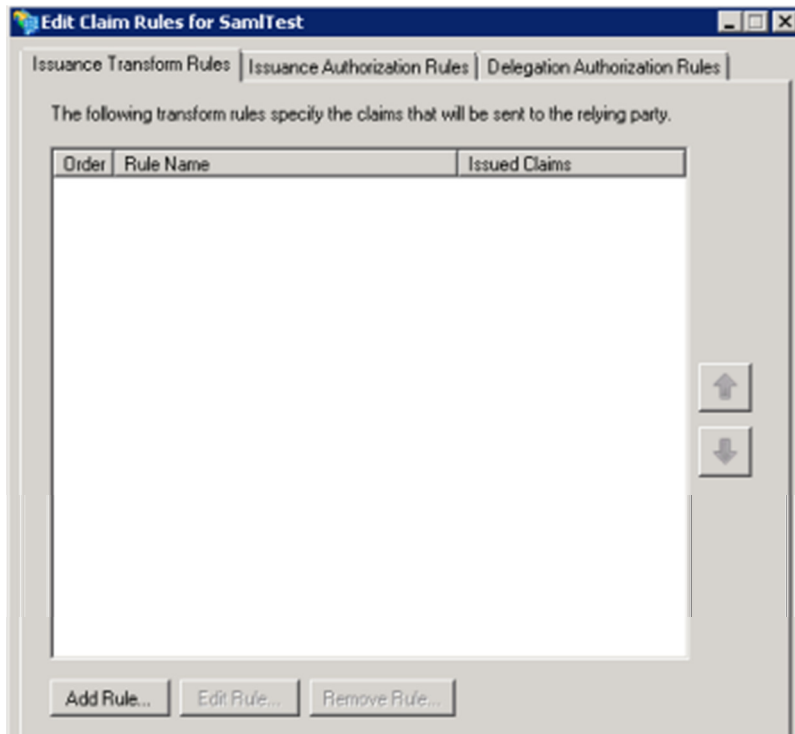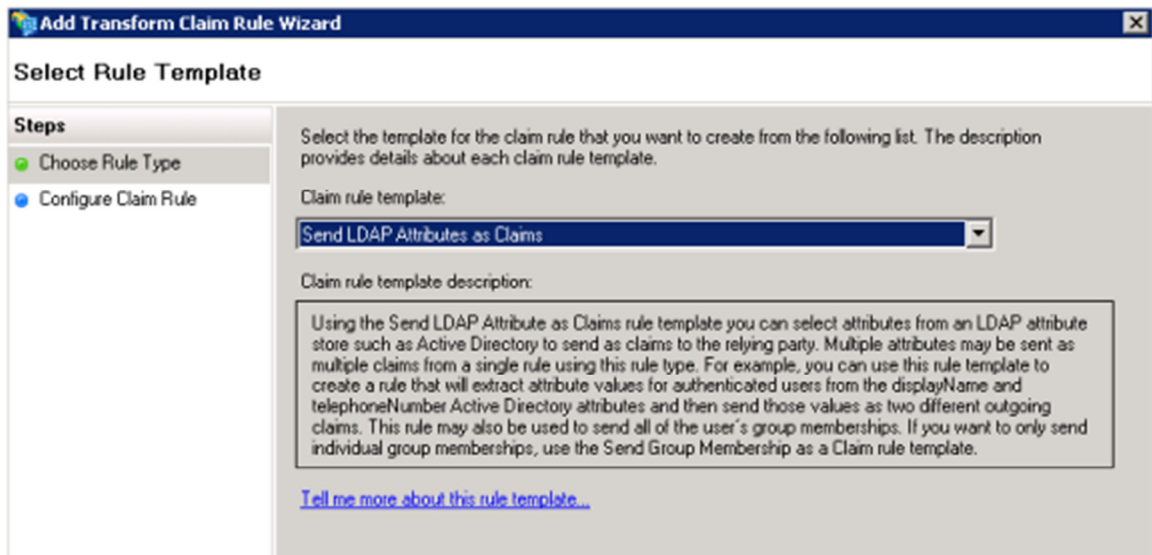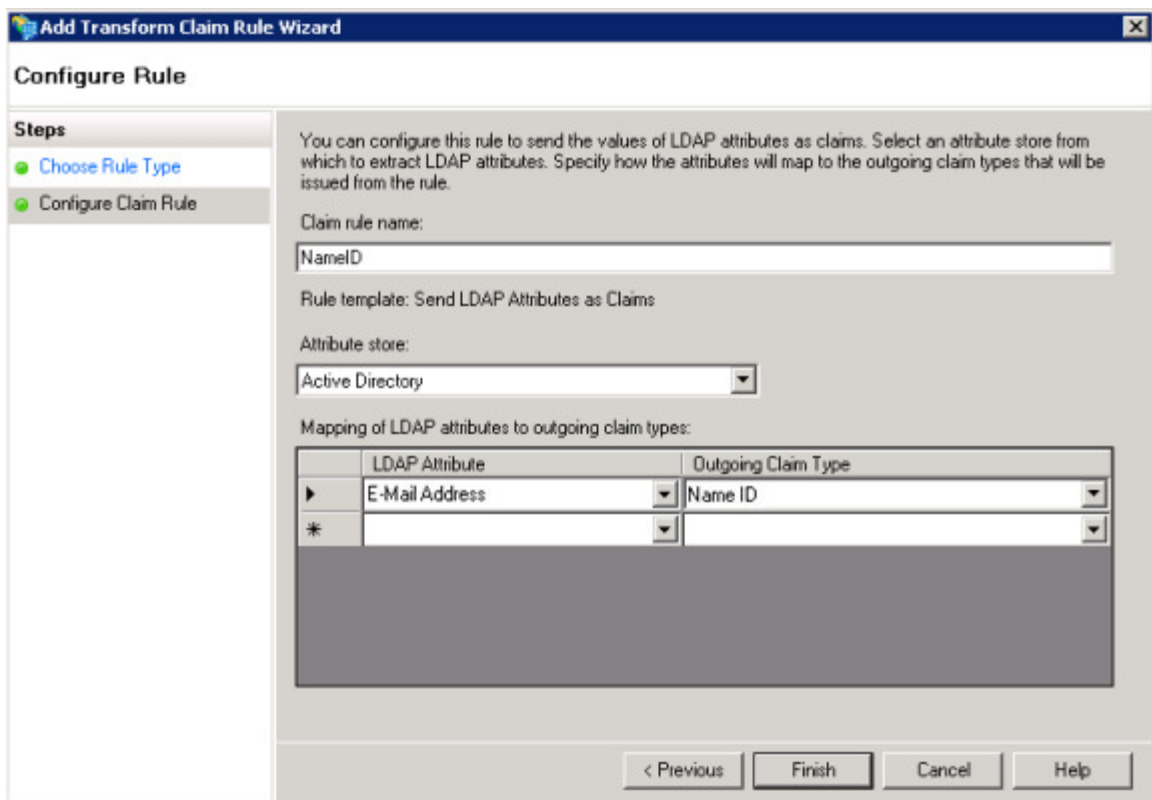Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send 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.

Tell me more about this rule template...

10) Name the Claim, and then set the attributes below so that it pulls from the Active Directory. Additionally, map the E-mail Addresses attribute as the NameID.

Add Transform Claim Rule Wizard ☒

Configure Rule

Steps
- ● Choose Rule Type
- ● Configure Claim Rule

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:

NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory ▾

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	E-Mail Address ▾	Name ID ▾
✳	▾	▾

< Previous   Finish   Cancel   Help

11) Click Finish in the Claim Rule Wizard, and go back to the ADFS 2.0 Management Console. View the Properties for the Daptiv entry. You'll see a screen with multiple tabs.

12) On the Signature tab, make sure that the certificate listed here is the same as the certificate you have sent to Daptiv Support (as one of the required pieces of information). If no certificate is listed, then you'll need to select one. Note that the example below contains a certificate, but you will have a different name/value.
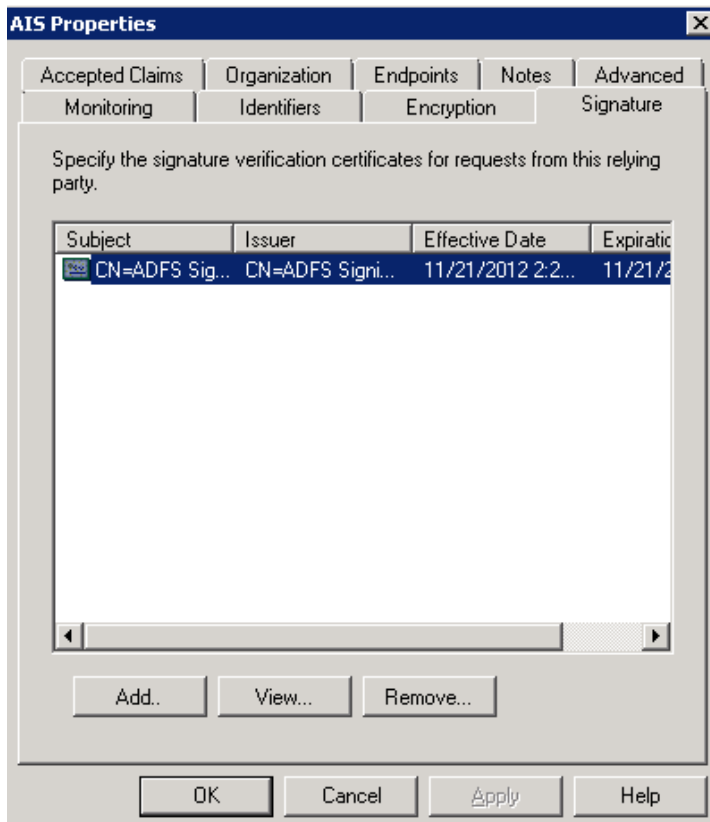
13) On the Advanced tab, change the algorithm to SHA1. This is the encryption algorithm
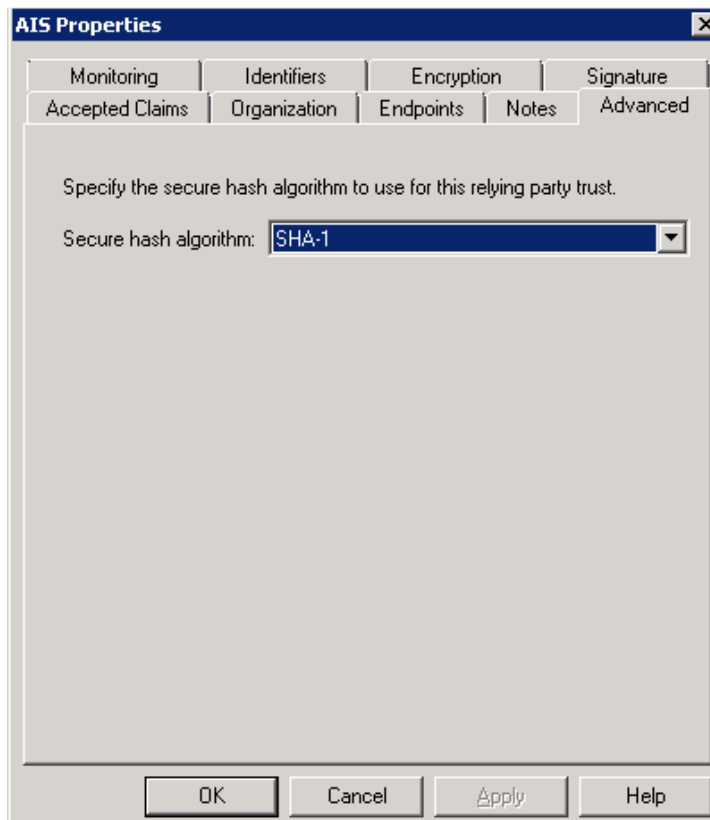
14) After saving the changes to the properties, you are ready to send the required information to Daptiv Support, if you haven't already.

15) After Daptiv Support confirms that the SSO information has been entered, test your Daptiv SSO integration. By default, ADFS 2.0 has a sign-in URL of: <https://**<ADFS FQDN>**/adfs/ls/IdpInitiatedSignon.aspx> where <ADFS FQDN> is the address of your ADFS 2.0 server.