CAPITA

one

Setting up Single Sign On

last updated for the Summer 2016 release

Technical Guide

Revision History

Version	Published on
Summer 2016 (3.60) - 1.0	31/05/2016

Doc Ref

Setting up Single Sign On Technical Guide/Summer 2016/2016-05-31

www.capita-one.co.uk

Contacting the Service Desk

You can log a call with the Service Desk via the Customer Service tool available on My Account.

Providing Feedback on Documentation

We always welcome comments and feedback on the quality of our documentation including online help files and handbooks. If you have any comments, feedback or suggestions regarding the module help file, this handbook (PDF file) or any other aspect of our documentation, please email:

onepublications@capita.co.uk

Please ensure that you include the document name, version and aspect of documentation on which you are commenting.

Contents

01 **| Introduction 1**

02 **| Installing the SSO Authentication Website 2**

Introduction 2

Prerequisites for the SSO website 2

02.1 Create an application pool 2

02.2 Install the SSO website 2

03 **| Configuring the SSO Authentication Website 3**

Settings 3

04 **| Configuring Exclusion web site 5**

05 **| Configuring the Client Machine 6**

06 **| Configuring the Application Server 8**

Settings 8

Granting Permission to Read the Service Certificate's Private Key 9

07 **| Configuring ADFS 13**

End Point Enabled on ADFS 13

Adding SSOAuthentication as a Relying Party 13

Adding the Application Server as a Relying Party 18

Configuring Communication Between the SSOAuthentication Website and the AppServer 22

Changes to the Application Server Relying Party 22

Changes to the SSOAuthentication Relying Party 25

Appendix – Obtaining ADFS Details 28

Index 30

01 | Introduction

This document details the configuration changes that must be made in order to use One Single Sign On (SSO) in a v4 environment. There are four areas in which you need to make changes:

- The SSO authentication website/server.
- The application server website/server.
- Your client machine.
- Active Directory Federation Services (ADFS).

Example Environment

This document details SSO configuration in an example v4 environment with the following settings. You must adjust the values to suit your own One server environment.

- The **domain name** is `LAB-LA02.COM`**.**
- The **SSOAuthentication** website is installed on a machine with the name `LAB-ONEALL.LAB-LA02.COM`
- The **SSOAuthentication URL** is `https://LAB-ONEALL/SSOAuthentication/`
- The **AppServer**, **Session Server**, **Report Server** and **CCS Enterprise Online** are installed on a machine with the name `LAB-DEV01.LAB-LA02.COM`
- The **Application Server URL** is `https://LAB-DEV01/CCSEnterprise_ApplicationService_Debug358/`
- The **CCS Enterprise Online URL** is: `https://LAB-DEV01/CCSEnterprise.RIA.WEB358/`
- **The Exclusion App URL is**: `https://LAB-DEV01/CCSEnterpriseExclusion/`
- The **ADFS server** is installed on a machine with the name `LAB-DC8R26401.LAB-LA02.COM`
- The **ADFS URL** is `https://adfs.lab-la02.com/adfs`
- To check if ADFS is working you can use `https://adfs.lab-la02.com/adfs/ls/IdpInitiatedSignon.aspx`

02 | Installing the SSO Authentication Website

Introduction

This chapter details the installation the SSO authentication website. After installing the website, you must enter the details into the **SSO Authentication** tab of the CCS Enterprise Server Configuration utility.

IMPORTANT NOTE: *After configuring your One environment to use SSO, you should direct end users to access v4 Online Silverlight modules via the new SSO website URL instead of the existing v4 Online Silverlight URL. If users access the existing v4 Online Silverlight URL, they will have to enter their One user credentials to log in.*

Prerequisites for the SSO website

An existing One infrastructure is required, including an application server. You can install the SSO website on any server in your environment.

02.1 Create an application pool

The SSO website should be run within its own application pool.

On the server that will host the SSO website, add an application pool with the following settings:

- **Name:** This can be any valid name, but you should write it down as it will be required later.
- **.NET framework version**: 4.0
- **Managed pipeline mode:** Integrated.
- **Identify:** NetworkService

In advanced settings for the application pool, enter the following value:

- **IdleTime-out**: 480
- **Identity:** NetworkService

02.2 Install the SSO website

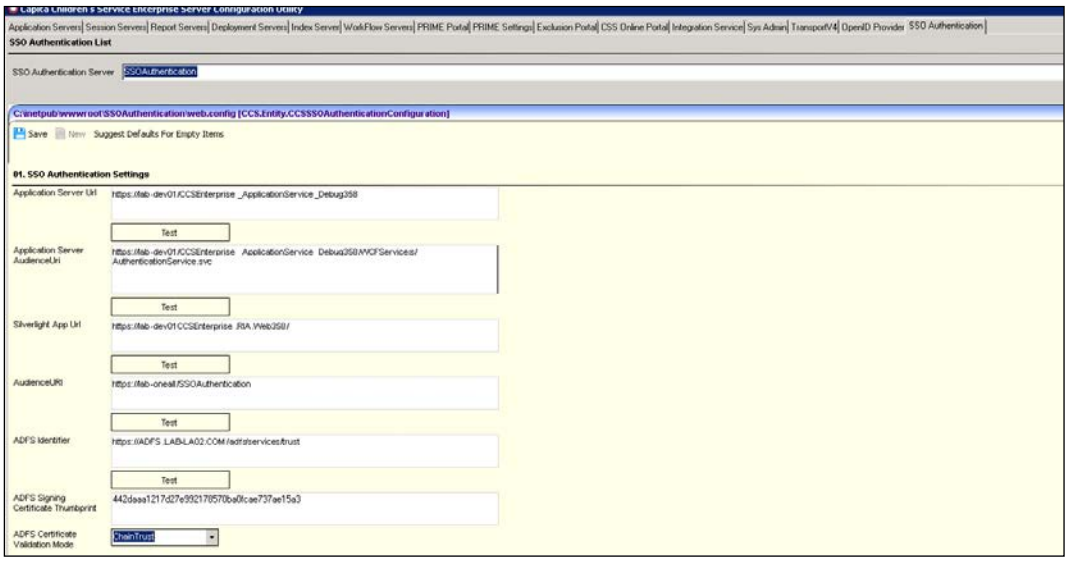
Install the website by running the SSOAuthenticationSetup.msi. You will be prompted for the following information

- Select IIS Destination page:
  - **Site**: typically **Default Web Site**
  - **Virtual Directory**: typically **SSOAuthentication.**
  - **Application Pool**: The application pool created in step 2.1.

03 | Configuring the SSO Authentication Website

Settings

This chapter details the settings for the SSO authentication website. These settings are entered on the **SSO Authentication** tab of the CCS Enterprise Server Configuration utility.



- **Application Server URL:** You must provide a valid application server URL.

  The URL for the example environment is `https://LAB-DEV01/CCSEnterprise_ApplicationService_Debug358/`

- **CCS Enterprise Online URL:** You must provide a valid URL for CCS Enterprise Online.

  The URL for the example environment is `https://LAB-DEV01/CCSEnterprise.RIA.WEB358/`

- **Exclusion App Url:** You must provide a valid URL for Exclusion App in the following format.

  https://[Web Server]/[Exclusion WebSite]/Login.aspx

  The URL for the example environment is

  `https://LAB-DEV01/CCSEnterpriseExclusion/Login.aspx`

- **Audience URL:** This is the base URL for the current SSOAuthentication website.

  It must be in the following format: `https://[WebServer]/SSOAuthentication`

  It must also match the **Relying Party Identifier**. For more information on relying parties, see Appendix – Obtaining ADFS Details on page *28*.

  The URL for the example environment is `https://LAB-ONEALL/SSOAuthentication`

- **ADFS Identifier:** You must provide an ADFS identifier in the following format: `https://[ADFS]/adfs/services/trust`

  For information on finding the ADFS identifier, see Appendix – Obtaining ADFS Details on page *28.*

  The identifier for the example environment is `https://adfs.lab-la02.com/adfs/services/trust`

- **Thumbprint:** This is the thumbprint of the certificate used by ADFS to sign the token. For information on how to obtain the correct thumbprint, see Appendix – Obtaining ADFS Details on page *28.*
- **Certificate Validation Mode:** This option is used to determine the validity of the certificate that is used by ADFS to sign the token. Select one of the following values:
  - **ChainTrust:** The certificate is valid if the chain builds to a certification authority in the trusted root store.

    > ***NOTE:*** *The certificate must meet the following requirements in order for you to use the* ***ChainTrust*** *option.*
    >
    > *- The certificate must be issued from a CA in Capita's trusted CA list (in the machine certificate store).*
    >
    > *- The intended purpose of that CA must include* ***Client Authentication****.*

  - **PeerOrChainTrust:** The certificate is valid if it is in the trusted people store, or if the chain builds to a certification authority in the trusted root store.
  - **PeerTrust:** The certificate is valid if it is in the trusted people store.
  - **None:** The certificate is not validated.

  By default, the certificate validation mode is set to **None**. If this setting is changed, you must install the ADFS certificate (public key only).
- **Application Server Audience URL:** This is the URL of the application server website. It must be in the following format:
  `https://[AppServer]/WCFServices/AuthenticationService.svc`

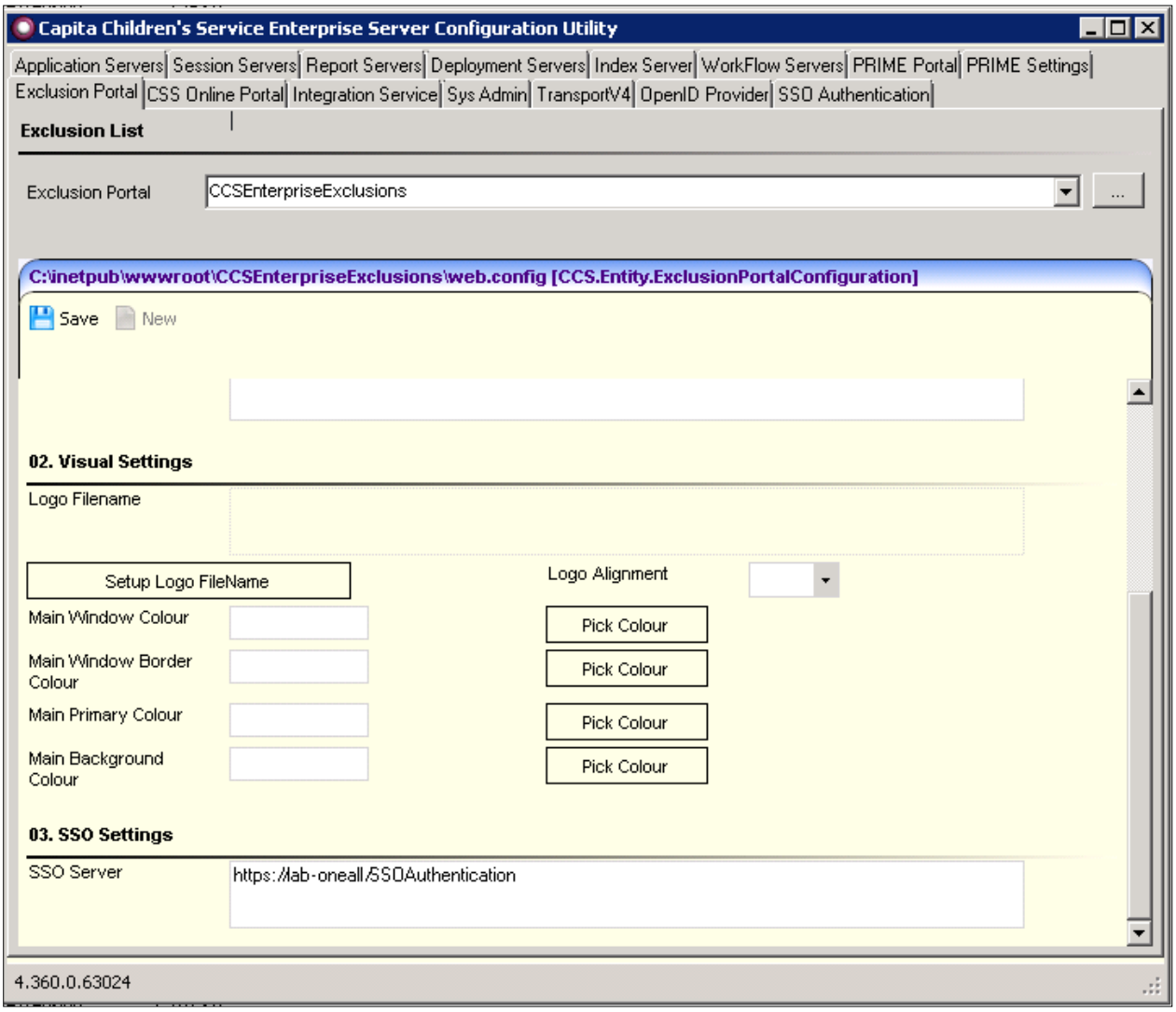
  It must also match the **Audience URL** in the application server configuration.

  The correct URL for the example environment is `https://LAB-DEV01/CCSEnterpirse_ApplicationService_Debug358/WCFServices/AuthenticationService.svc`

> ***NOTE:*** *You must also install the application server certificate on the SSOAuthentication machine.*

04 | Configuring Exclusion web site

This chapter details the settings for the Exclusion Portal website. These settings are entered on the **Exclusion Portal** tab of the CCS Enterprise Server Configuration utility.



- **SSO Server:** This is the base URL for the current SSOAuthentication website.

It must be in the following format: `https://[WebServer]/SSOAuthentication`

The URL for the example environment is https://LAB-ONEALL/SSOAuthentication.

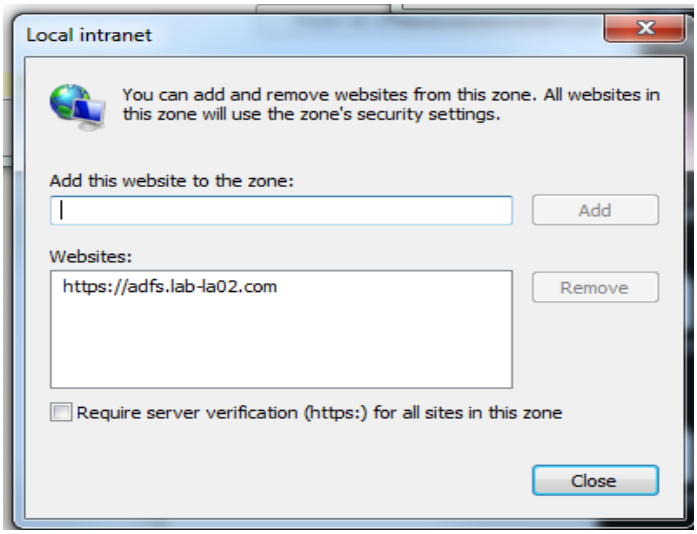
05 | Configuring the Client Machine

1. If applicable, install the ADFS service certificate on the client machine.

   This step is not required if the ADFS certificate is created using a certificate that is already known to the client.

2. If you are prompted for credentials, add the ADFS website to the Intranet websites:

   a. Open Internet Explorer and select **Internet Options | Security | Sites | Advanced**.

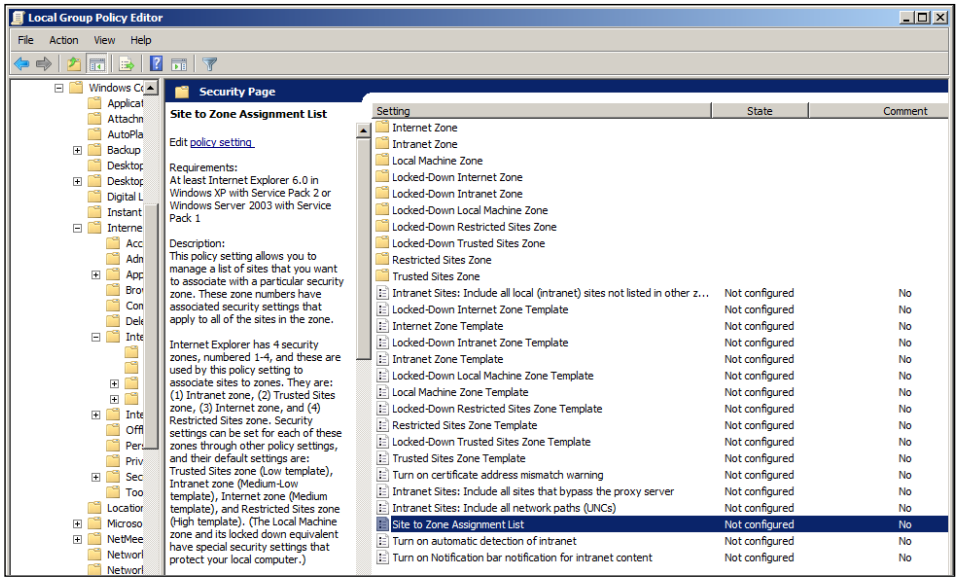


   b. Enter the address of the website into the **Add this website to the zone** field and then click the **Add** button to add that site.

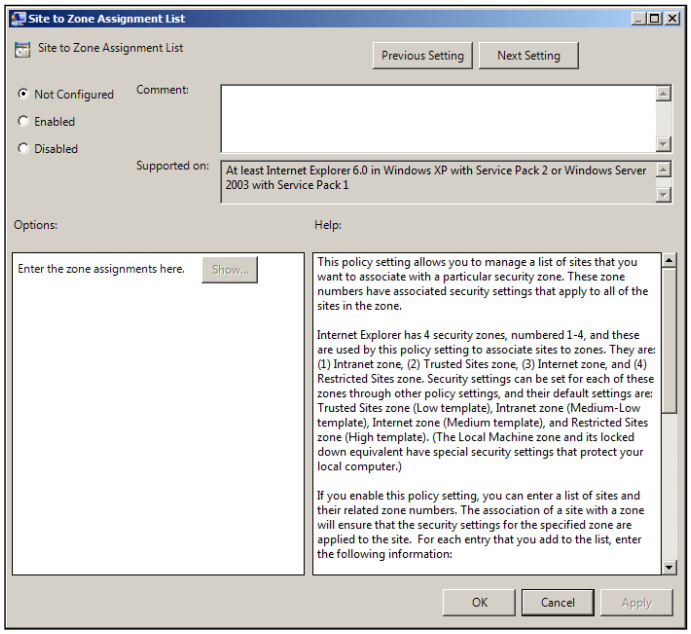
   c. Use Windows Group Policy to add the site URL into the client's Local Intranet Zone:

      i. Open the Group Policy client and select a policy that applies to authenticated users.

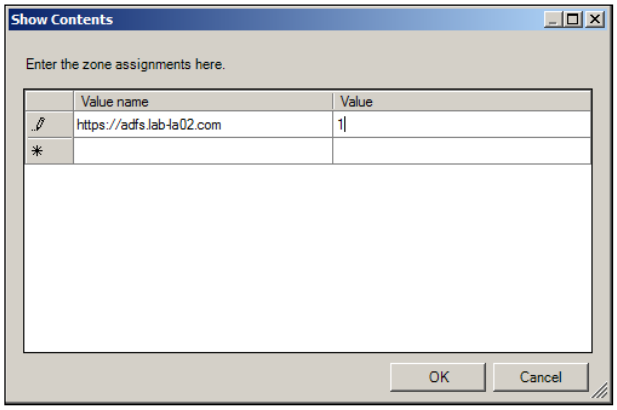
      ii. Select **User config | Administrative Templates | Windows Components | Internet Explorer | Internet Control Panel | Security Page**.



      iii. Double-click the **Site to Zone Assignment List** button to display properties for that setting.



iv. Ensure that the **Enabled** radio button is selected and then click the **Show** button to display the **Show Contents** dialog.



v. Enter the URL of the site into the **Value Name** field.

vi. Enter “1” into the **Value** field to assign the site to the Local Intranet Zone.

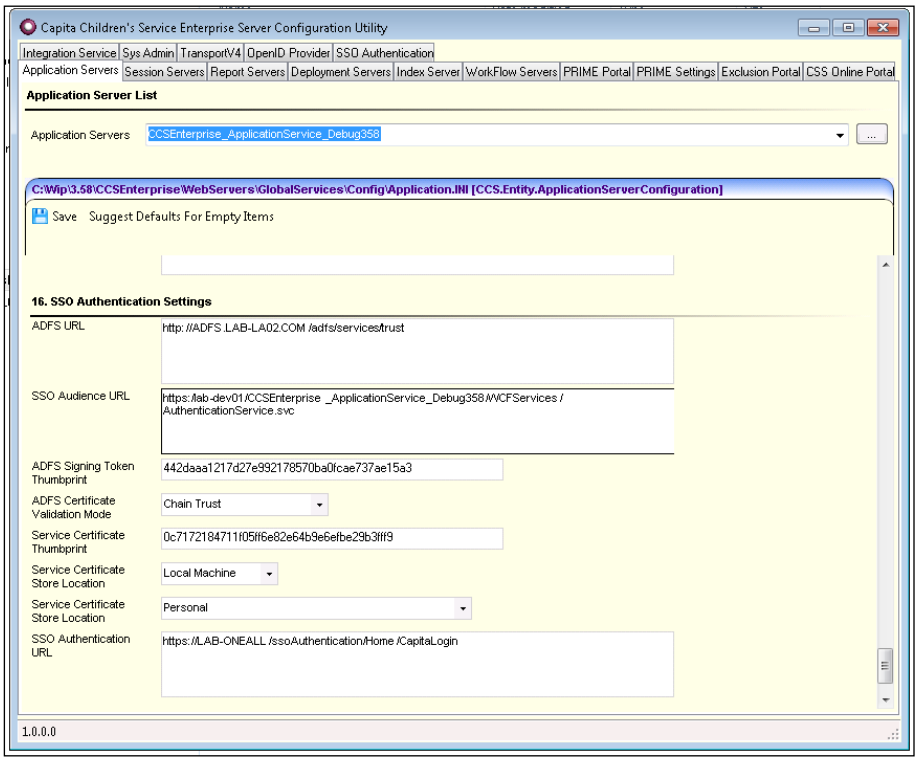
vii. Click the **OK** button to close the dialog, and then click **OK** again to save your changes.

In the example environment, the URL `https://adfs.lab-la02.com` was added to the zone.

06 | Configuring the Application Server

Settings

This section details the settings for the application server. These settings are entered on the **Application Server** tab of the CCS Enterprise Server Configuration Utility.



- **ADFS Identifier:** You must provide the correct ADFS identifier in the following format: `https://[ADFS]/adfs/services/trust`.

  For information on finding the ADFS identifier, see Appendix – Obtaining ADFS Details on page *28*.

  The URL for the example environment is `https://adfs.lab-la02.com/adfs/services/trust`

- **Audience URL:** The **Audience URL** is used by ADFS to identify the application server, and should match the **Relying Party Identifier** as configured in ADFS. It should be entered in the following format: `https://[AppServer]/WCFServices/AuthenticationService.svc`

  The correct URL for the example environment is `https://LAB-DEV01/CCSEnterpirse_ApplicationService_Debug358/WCFServices/AuthenticationService.svc`

- **Thumbprint:** This is the thumbprint of the certificate used by ADFS to sign the token. For information on how to obtain the correct thumbprint, see Appendix – Obtaining ADFS Details on page *28*.

- **Certificate Validation Mode:** This option is used to determine the validity of the certificate that is used by ADFS to sign the token. Select from the following values:

  - **ChainTrust:** The certificate is valid if the chain builds to a certification authority in the trusted root store.

> ***NOTE:*** *The certificate must meet the following requirements in order for you to use the* ***ChainTrust*** *option.*
>
> *- The certificate must be issued from a CA in Capita's trusted CA list (in the machine certificate store).*
>
> *- The intended purpose of that CA must include* ***Client Authentication****.*

- **PeerOrChainTrust:** The certificate is valid if it is in the trusted people store, or if the chain builds to a certification authority in the trusted root store.
- **PeerTrust:** The certificate is valid if it is in the trusted people store.
- **None:** The certificate is not validated.

By default, the certificate validation mode is set to **None**. If this setting is changed, you must install the ADFS certificate (public key only).

- **Service Certificate:** These fields enable you to record information about the certificate that is used by the service to decrypt the incoming request. The following information is required:
  - **Thumbprint:** The thumbprint of the certificate used by the WCF authentication service.
  - **Folder:** The folder in which the certificate resides.
  - **Store Location:** Whether the certificate is a machine / service or a user certificate.

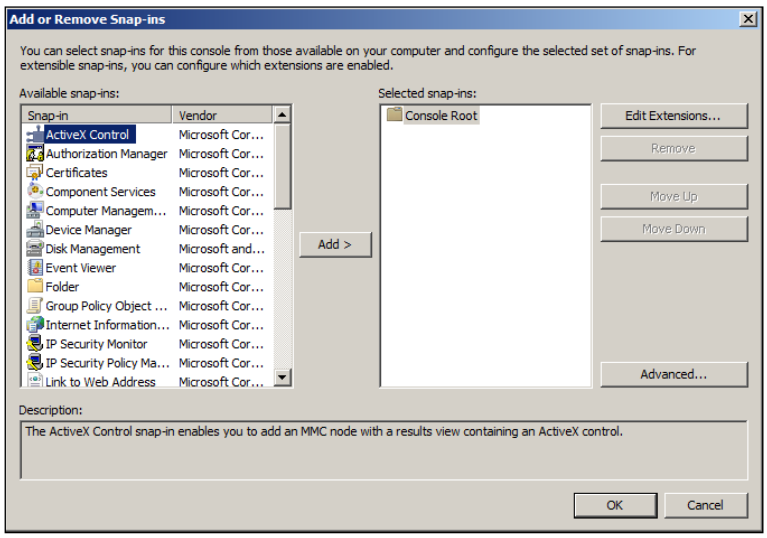
> ***NOTE:*** *You must export this certificate and copy it to the ADFS machine. This is required while configuring the application server as a relying party.*

- **SSO Authentication URL:** The URL of the SSOAuthentication website. Must be in the following format: `https://[SSOAuthenticationWebServer]/SSOAuthentication/Home/CapitaLogin`

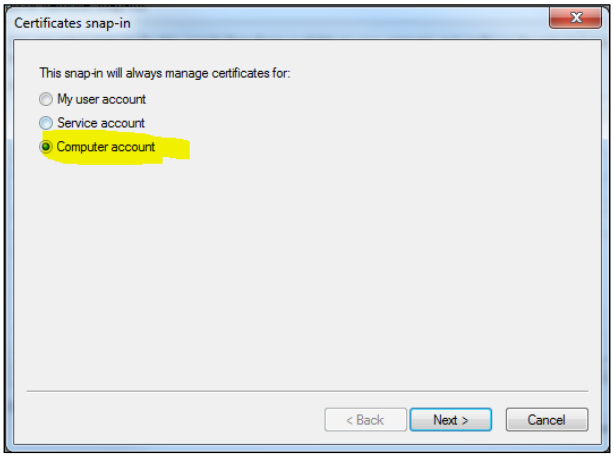
Granting Permission to Read the Service Certificate's Private Key

You must grant the application pool under which the application server is running read permission for the service certificate's private key. To do so:

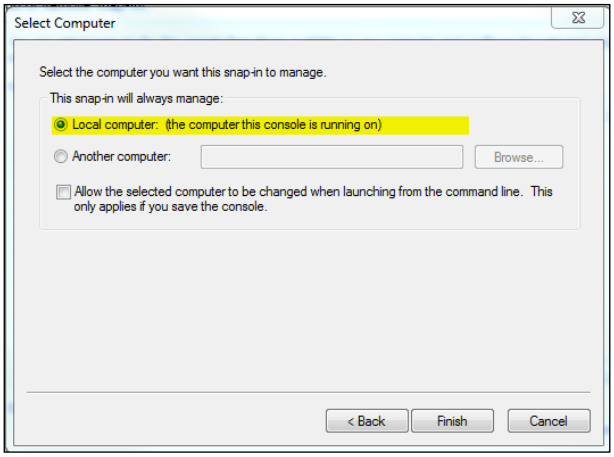
1. Open the Microsoft Management Console
2. Add the Certificates snap-in for your local computer:
   a. Select **File | Add / Remove Snap-In** to display the **Add or Remove Snap-ins** dialog.



b. Select **Certificates** from the **Available snap-ins** list and then click the **Add** button to add it to the **Selected Snap-ins** list and display the **Certificates snap-in** dialog.



c. Select the **Computer account** radio button and then click the **Next** button to display the **Select Computer** dialog.

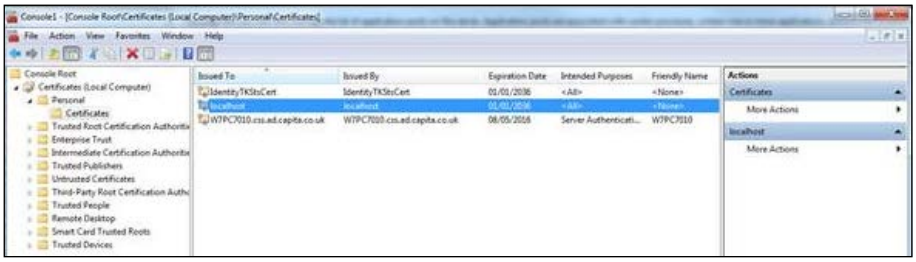


d. Select the **Local Computer** radio button and then click the **Finish** button to close the **Select Computer** dialog and return to the **Add or Remove snap-ins** dialog.

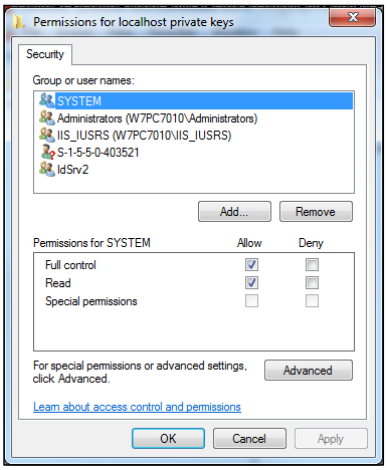
e. Click the **OK** button to close the **Add or Remove snap-ins** dialog and save your changes.

3. Grant permission to the private key:

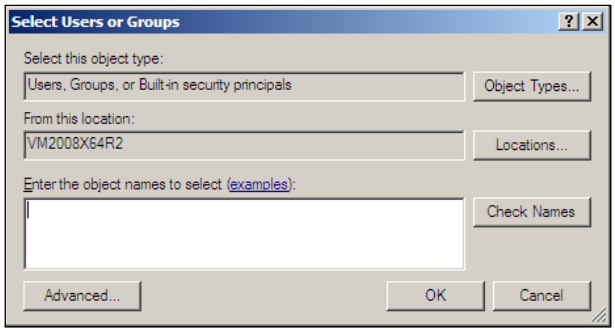
a. In the left-hand panel, select **Certificates | Personal | Certificates** to display a list of available certificates.



b. Right-click on the desired certificate and select **All Tasks | Manage Private Keys** to display the **Permissions** dialog.

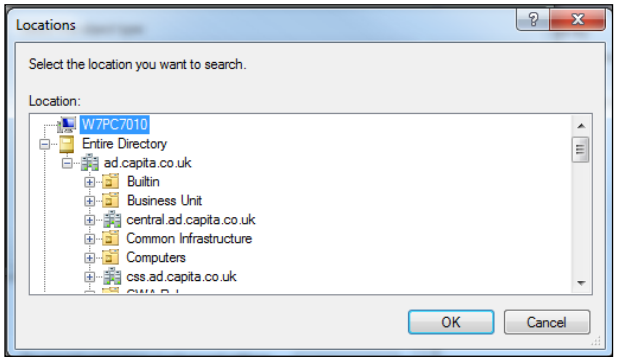


c. Click the **Add** button to display the **Select Users or Groups** dialog.



d. If your application pool is running under the default application pool identity (**AppPoolIdentity**), change the **Location** to your current computer:

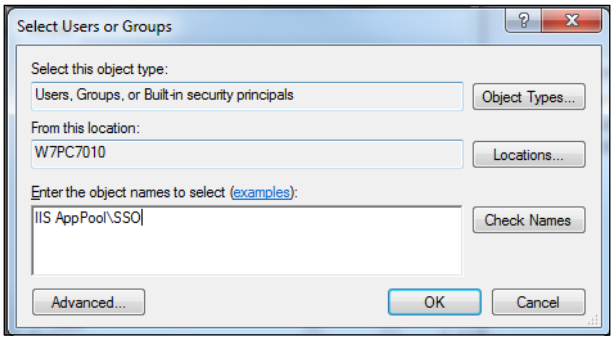
   i. Click the **Locations** button to display the **Locations** dialog.



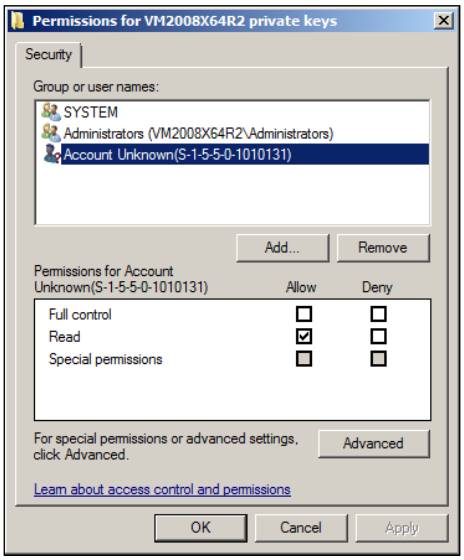
   ii. Highlight the name of your local computer and then click the **OK** button to select that computer and return to the **Select Users or Groups** dialog.

   If your application pool is not running under the default identity, move to step **e**.

e. Type the name of your required application pool into the **Enter the object names to select** field in the following format: `IIS AppPool\MyAppPoolName`



f. Click the **Check Names** button to validate the name of the application pool and then click the **OK** button to save your changes and close the **Select users or Groups** dialog. The **Permissions** dialog is displayed.



g. Select the **Read** permission from the **Allow** column, and ensure that all other check boxes in both columns are deselected. Click **OK** to close the dialog and save your changes.

07 | Configuring ADFS

The following ADFS configuration tasks must be undertaken in order to run SSO:

- Adding the SSOAuthentication website as a relying party.
- Adding the application server as a relying party.
- Configuring communication between the SSOAuthentication website and the application server.

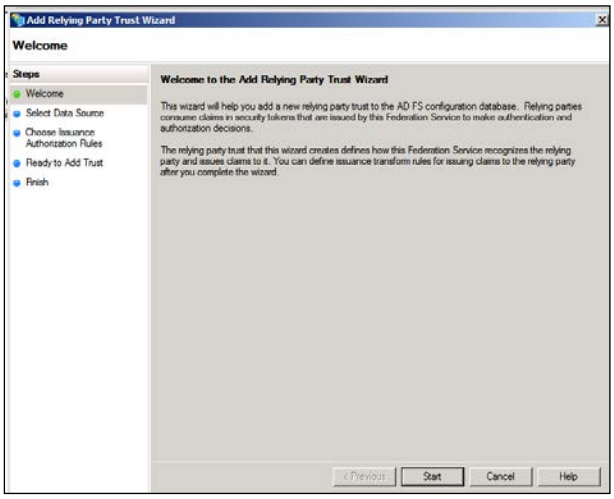
End Point Enabled on ADFS

Please make sure the following end points are enabled on ADFS:

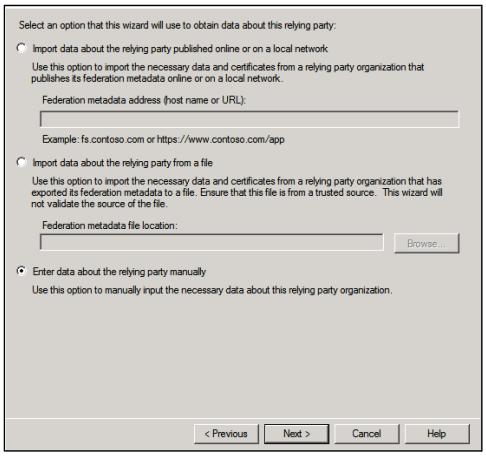
- /adfs/ls/
- /adfs/services/trust/13/windowstransport
- /adfs/services/trusttcp/windows

Adding SSOAuthentication as a Relying Party

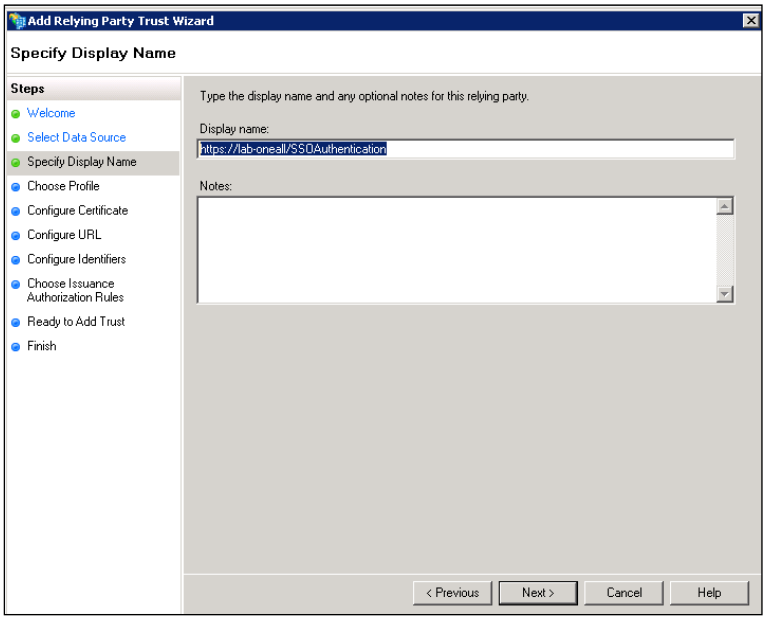
1. On the ADFS server, run the ADFS Management console.
2. Select **Trust Relationships | Relying Party Trust | Add Relying Party Trust** to display the **Add Relying Party Trust** wizard.



3. Click the **Start** button to run the wizard and display the **Select Data Source** page.

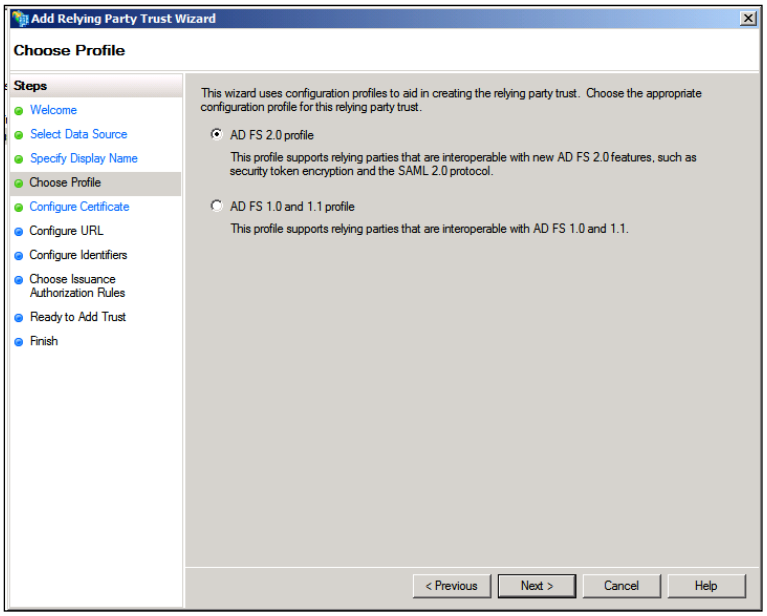


4. Select the **Enter data about the relying party manually** radio button and then click the **Next** button to display the **Specify Display Name** page.

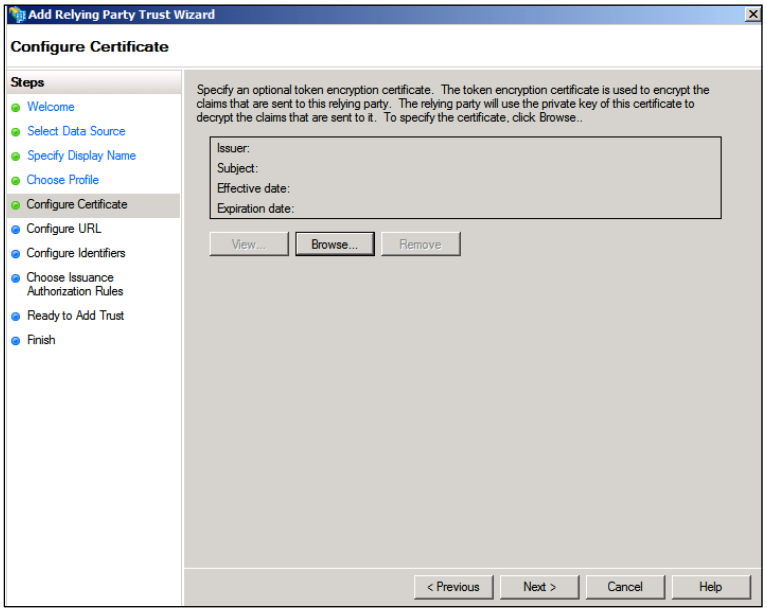


5. Enter the SSOAuthentication **Audience URL** (as configured during the SSOAuthentication configuration process) into the **Display name** field. The URL should be entered in the following format:
`https://[SSOAuthenticationWebServer]/SSOAuthentication`
The URL for the example environment is `https://lab-oneall/SSOAuthentication`.

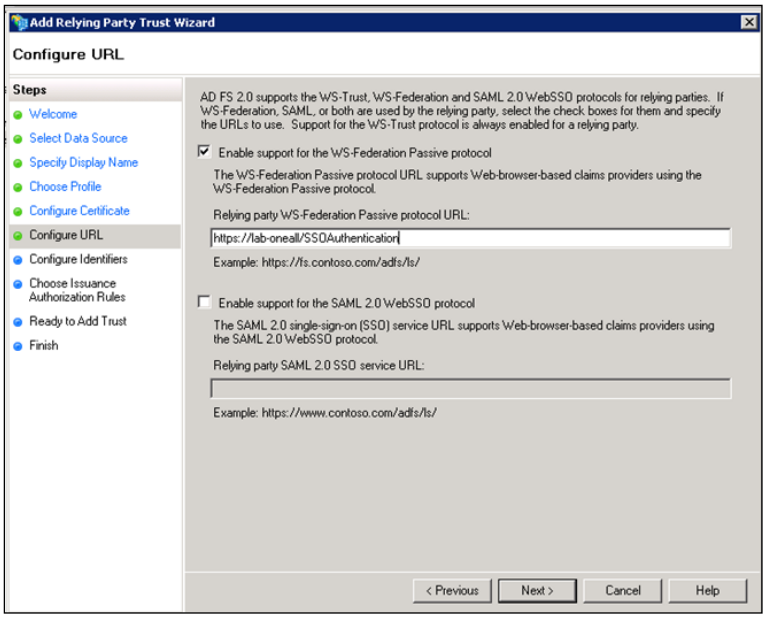
6. Click the **Next** button to display the **Choose Profile** page.



7. Select the **ADFS 2.0 profile** radio button and then click the **Next** button to display the **Configure Certificate** page.



8. Click the **Next** button to display the **Configure URL** page.



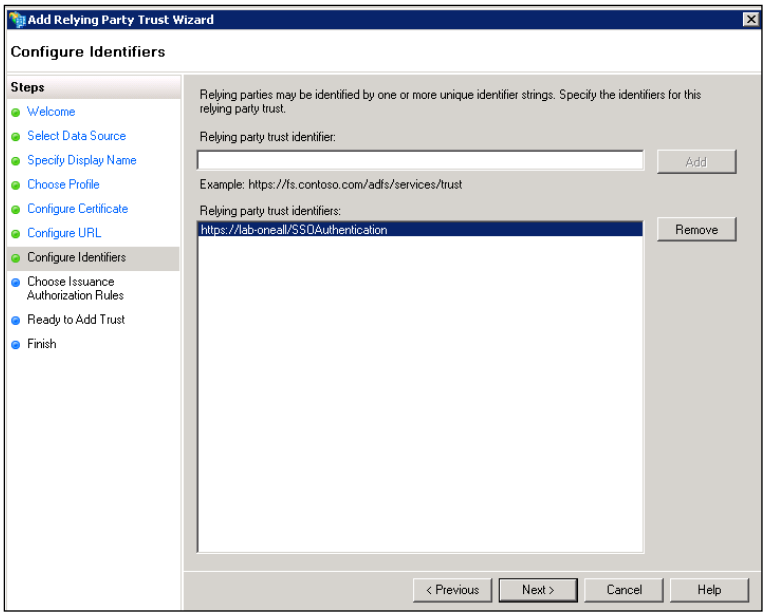
9. Select the **Enable support for Ws-Federation Passive protocol** check box and then enter the **Relying Party WS-Federation Passive protocol URL**.

   The URL must be in the following format:

   `https://[SSOAuthenticationWebServer]/SSOAuthentication`

   For the example environment, the URL is `https://lab-oneall/SSOAuthentication.`

10. Click the **Next** button to display the **Configure Identifiers** page.



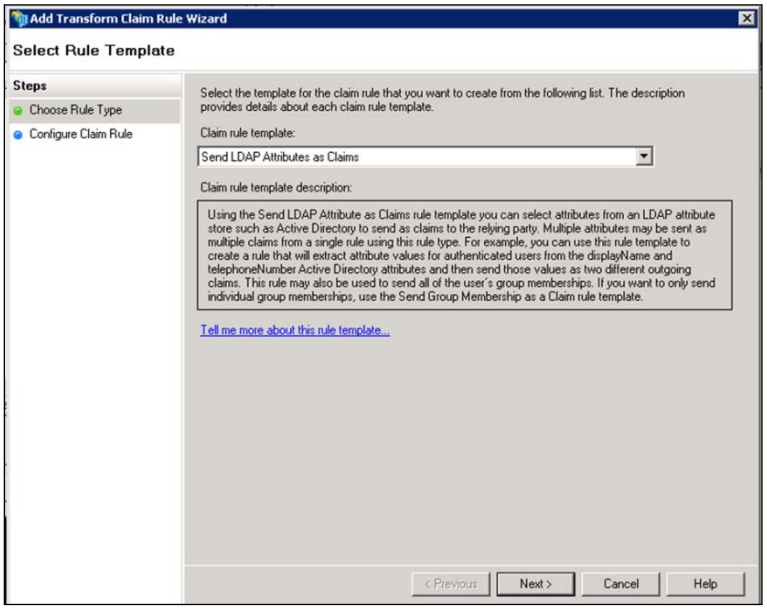
11. Enter the **Audience URL** (as configured during the SSOAuthentication configuration process) into the **Relying party trust identifier** field.

    The URL must be in the following format:
    `https://[SSOAuthenticationWebServer]/SSOAuthentication`

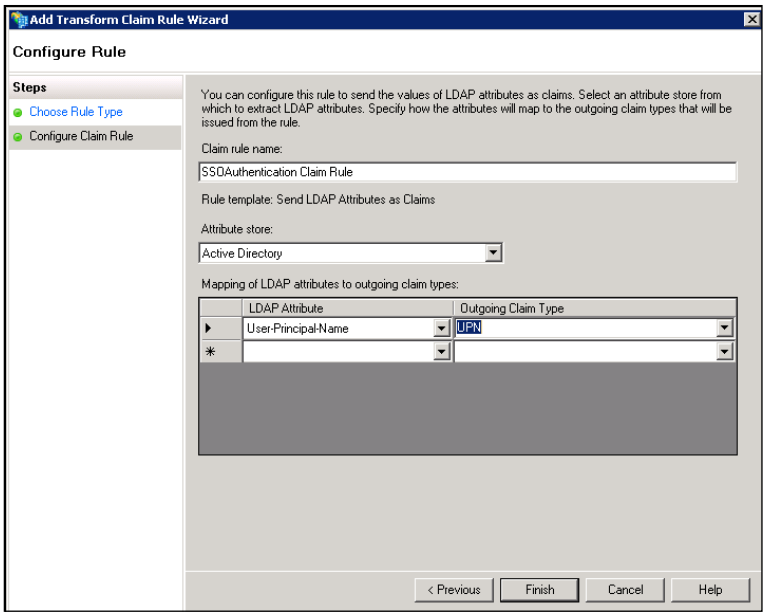
    For the example environment, the Audience URL is
    `https://lab-oneall/SSOAuthentication`

12. Click the **Next** button three more times to move through to the end of the wizard.

13. On the **Finish** page, select the option to configure claims to display the **Add Transform Claim Rule** wizard.



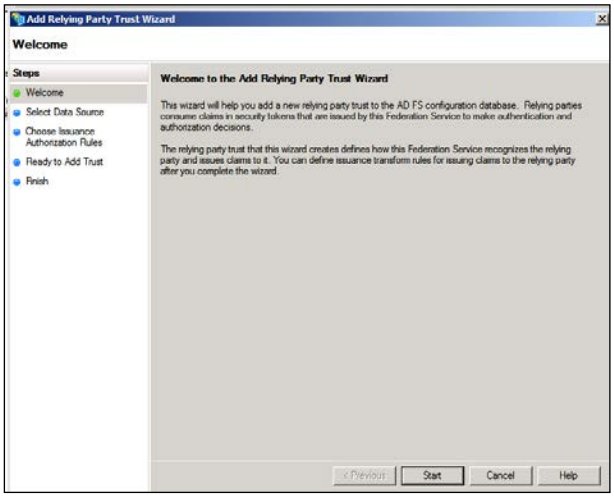
14. Select **Send LDAP Attributes as Claims** from the **Claim rule** template field and then click the **Next** button to display the **Configure Claim Rule** page.



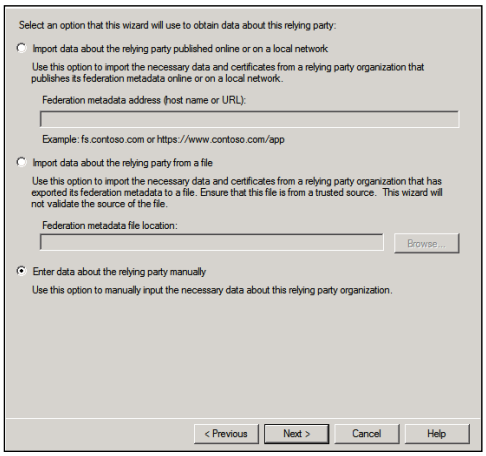
15. Enter a unique name into the **Claim Rule name** field (Capita suggests using the name "SSOAuthentication Claim Rule").
16. Select **Active Directory** from the **Attribute store** drop-down list.
17. Select **User Principal Name** from the **LDAP Attribute** drop-down list and then select **UPN** from **Outgoing Claim Type** drop-down list.
18. Click the **Finish** button to close the wizard and then click the **OK** button to save your changes.

Adding the Application Server as a Relying Party

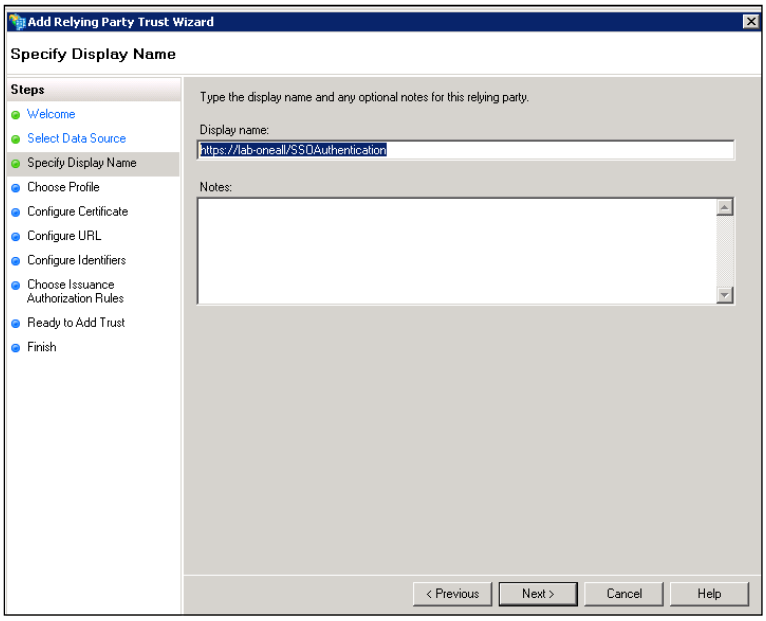
1. On the ADFS server, run the ADFS Management console.
2. Select **Trust Relationships | Relying Party Trust | Add Relying Party Trust** to display the **Add Relying Party Trust** Wizard.



3. Click the **Start** button to run the wizard and display the **Select Data Source** page.

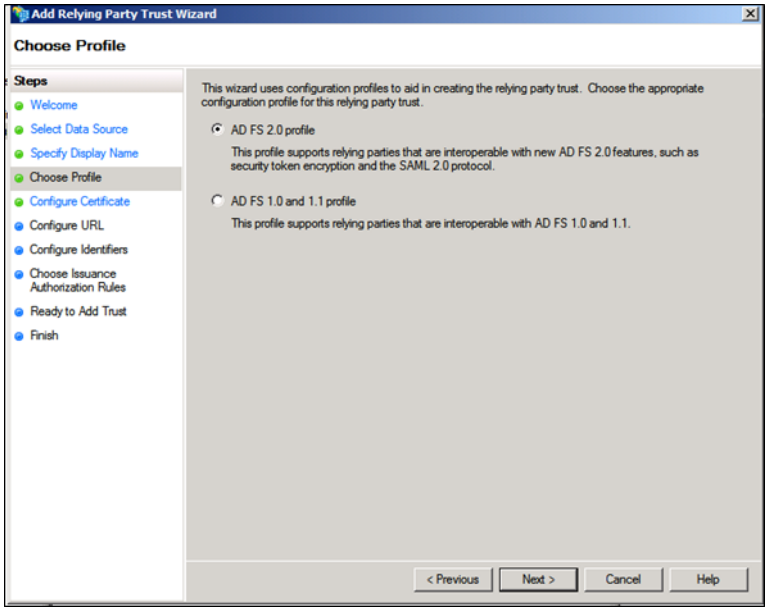


4. Select the **Enter data about the relying party manually** radio button and then click the **Next** button to display the **Specify Display Name** page.

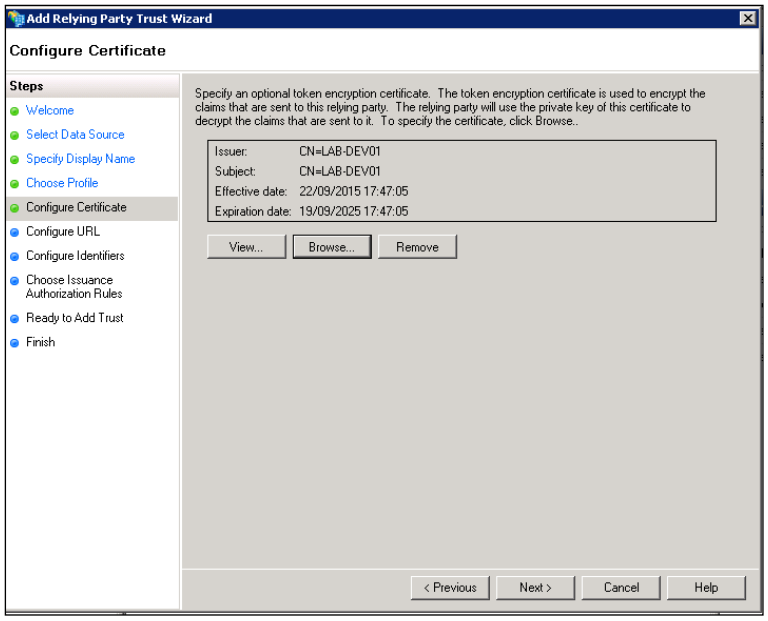


5. Enter the application server Audience URL (as configured during the application server configuration process) into the **Display name** field. It must be in the following format: `https://[AppServer]/WCFServices/AuthenticationService.svc`
The value for the example environment is `https://LAB-DEV01/CCSEnterpirse_ApplicationService_Debug358/WCFServices/AuthenticationService.svc`.

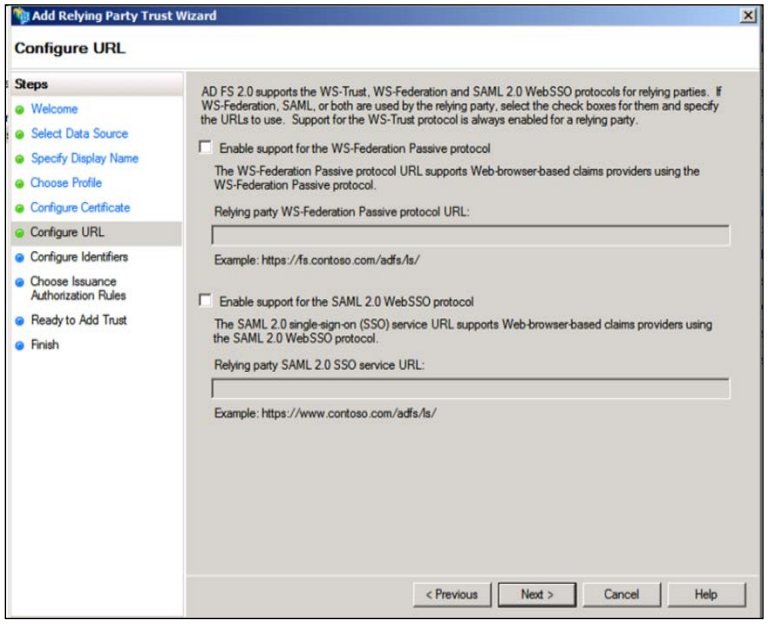
6. Click the **Next** button to display the **Choose Profile** page.



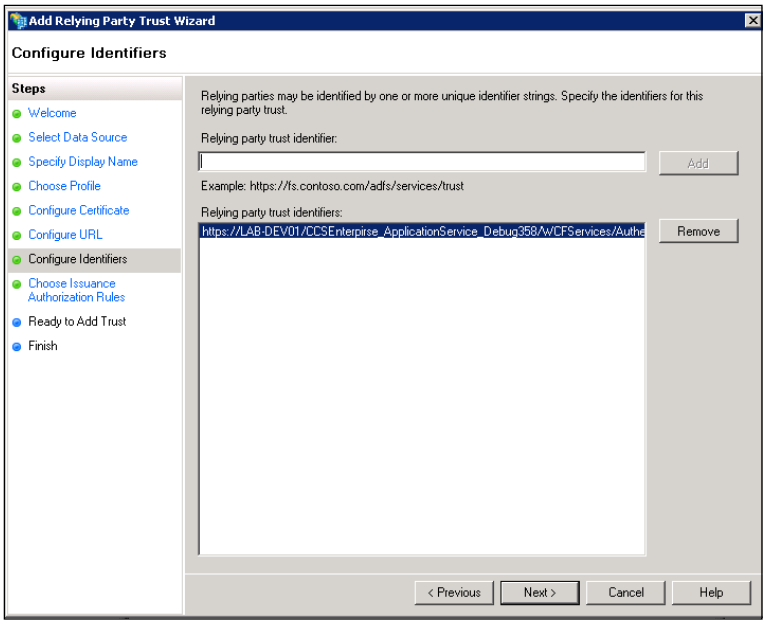
7. Select the **ADFS 2.0 profile** radio button and then click the **Next** button to display the **Configure Certificate** page.



8. Click the **Browse** button and select the certificate that you copied during the application server configuration process.
9. Click the **Next** button to display the **Configure URL** page.



10. Click the **Next** button to display the **Configure Identifiers** page.

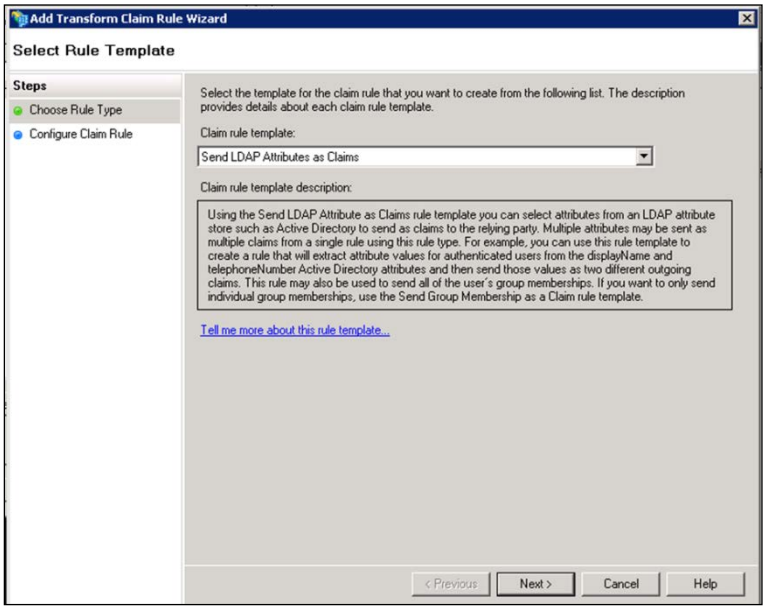


11. Enter the audience URL that you set during the application server configuration process into the **Relying party trust identifier** field. The URL must be entered in the following format: `https://[AppServer]/WCFServices/AuthenticationService.svc`

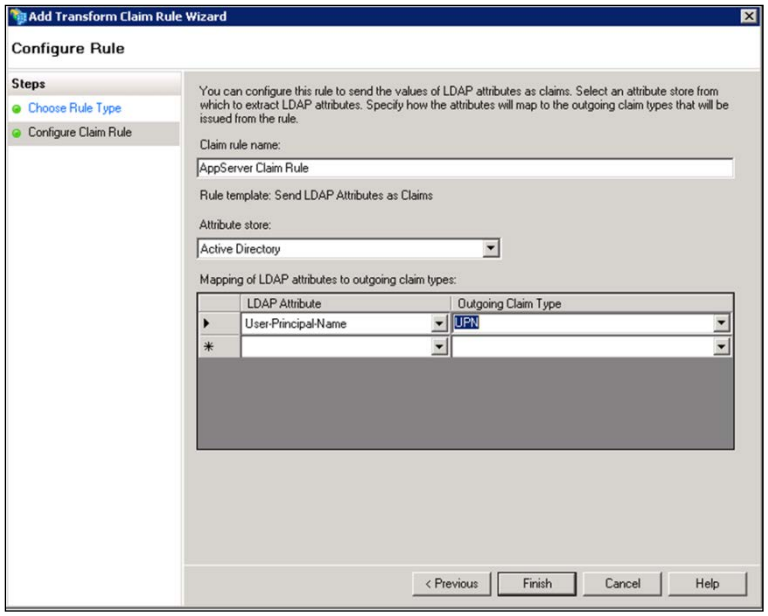
    The value for the example environment is `https://LAB-DEV01/CCSEnterpirse_ApplicationService_Debug358/WCFServices/AuthenticationService.svc`

12. Click the **Next** button three more times to move through to the end of the wizard.

13. On the **Finish** page, select the option to configure claims to display the **Add Transform Claim Rule** wizard.



14. Select **Send LDAP Attributes as Claims** from the **Claim rule** template field and then click the **Next** button to display the **Configure Claim Rule** page.

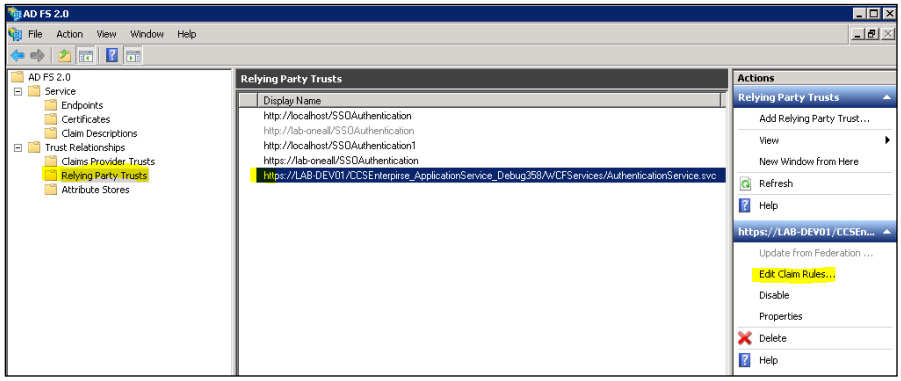


15. Enter a unique name into the **Claim Rule name** field (Capita suggests using the name "AppServer Claim Rule").
16. Select **Active Directory** from the **Attribute store** drop-down list.
17. Select **User Principal Name** from the **LDAP Attribute** drop-down list and then select **UPN** from **Outgoing Claim Type** drop-down list.
18. Click the **Finish** button to close the wizard and then click the **OK** button to save your changes.

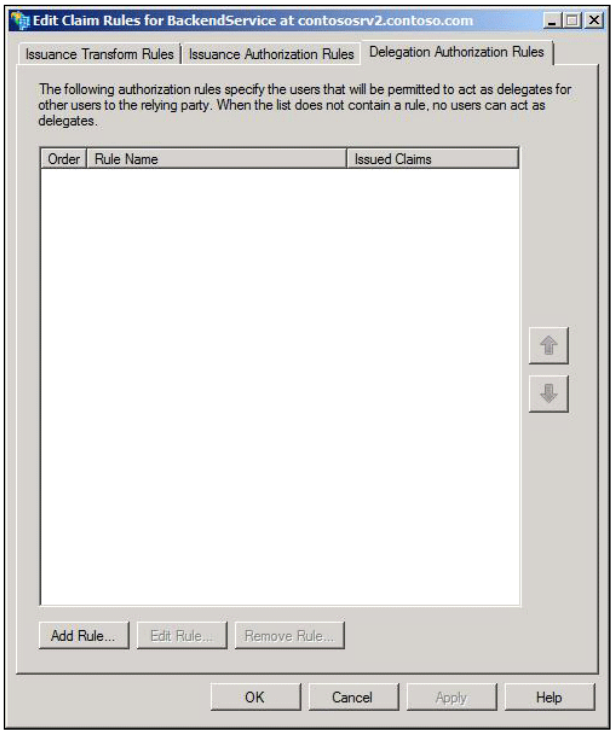
Configuring Communication Between the SSOAuthentication Website and the AppServer

Changes to the Application Server Relying Party

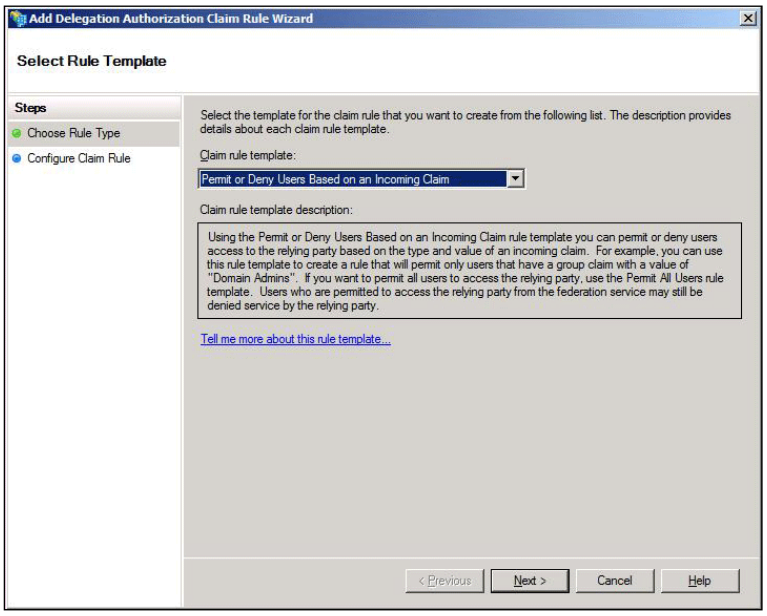
1. Within the Microsoft Management Console, select the **Relying Party Trusts** folder from the left-hand panel to display a list of relying party addresses in the centre panel.



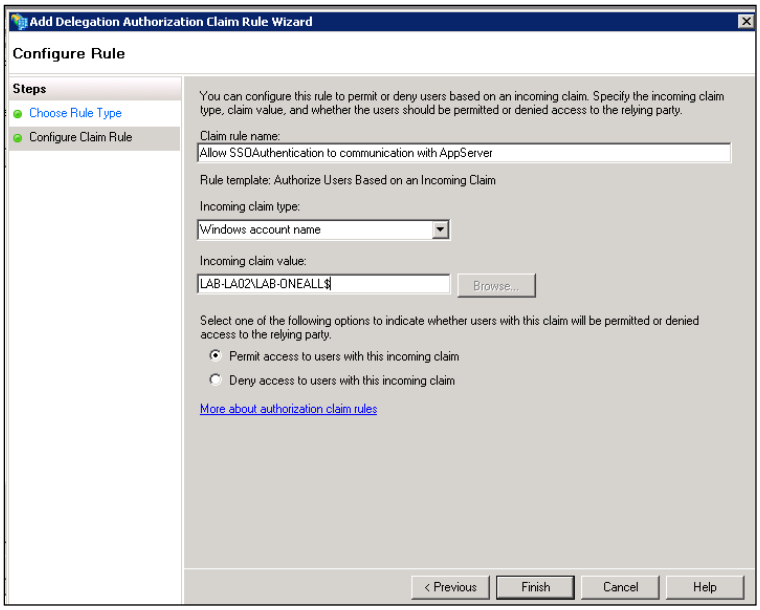
2. Highlight the application server relying party (https://LAB-DEV01/CCSEnterprise_ApplicationService_Debug358/WCFServices/AuthenticationService.svc in the example) and then click the **Edit Claim Rules** hyperlink to display the **Edit Claim Rules** dialog.



3. Select the **Delegation Authorization Rules** tab and then click the **Add Rule** button to display the **Add Delegation Authorization Claim Rule** wizard.

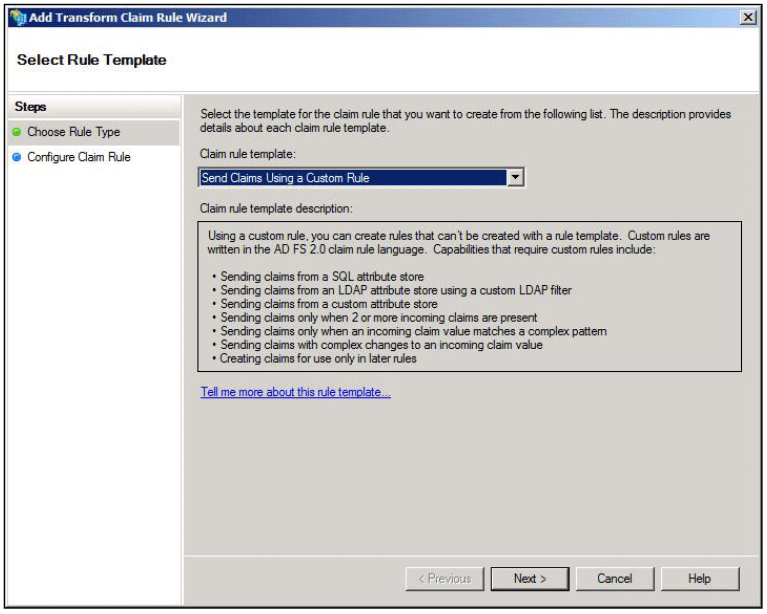


4. Select **Permit or Deny Users Based on an Incoming Claim** from the **Claim rule template** drop-down menu and then click the **Next** button to display the **Configure Claim Rule** page.

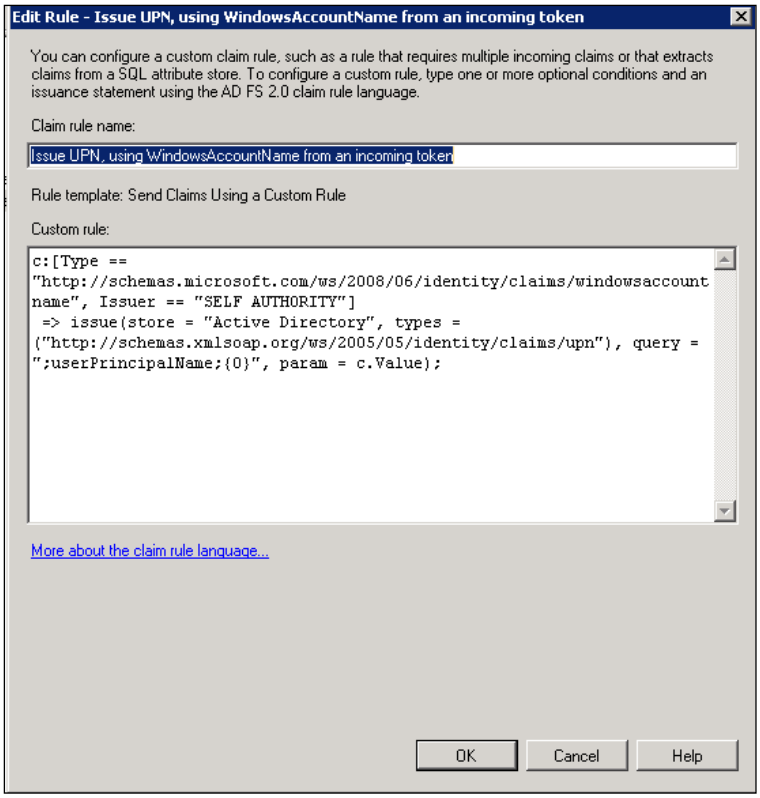


5. Select **Allow SSOAuthentication to communicate with AppServer** from the **Claim rule name** drop-down menu.
6. Select **Windows account name** from the **Incoming claim type** drop-down menu.
7. Enter the name of the SSOAuthentication Web Server into the **Incoming claim** value field, using the following format: `DOMAIN\WEBSERVER$ (all uppercase letters)`

   The SSOAuthentication Web Server for the example environment is `LAB-LA02\LAB-ONEALL$`.
8. Ensure that the **Permit access to users with this incoming claim** radio button is selected, and then click the **Finish** button to close the wizard and return to the **Edit Claim Rules** dialog.
9. Select the **Issuance Transform Rules** tab and then click the **Add Rule** button to display the **Add Transform Claim Rule** wizard.



10. Select **Send Claims Using a Custom Result** from the **Claim rule template** drop-down menu and then click the **Next** button to display the **Edit Rule** page.



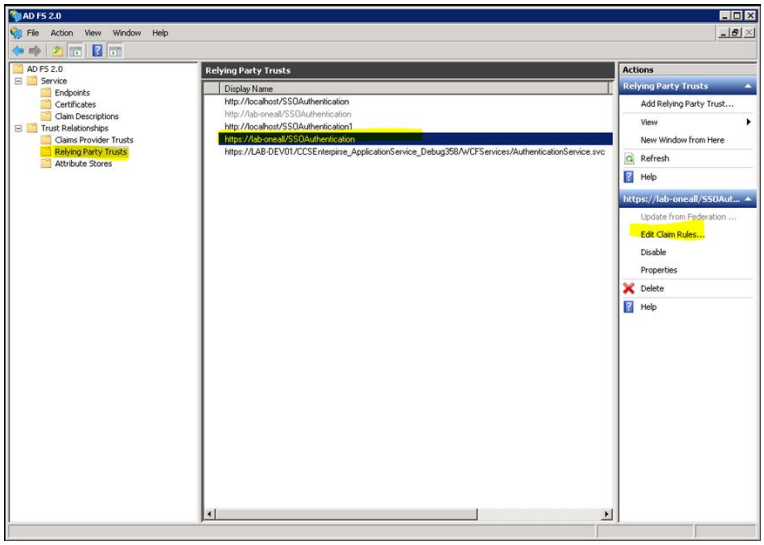
11. Type “Issue UPN, using WindowsAccountName from an incoming token” into the **Claim rule name** field.
12. Copy the following code and paste it into the **Custom rule** text box.

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "SELF AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);
```

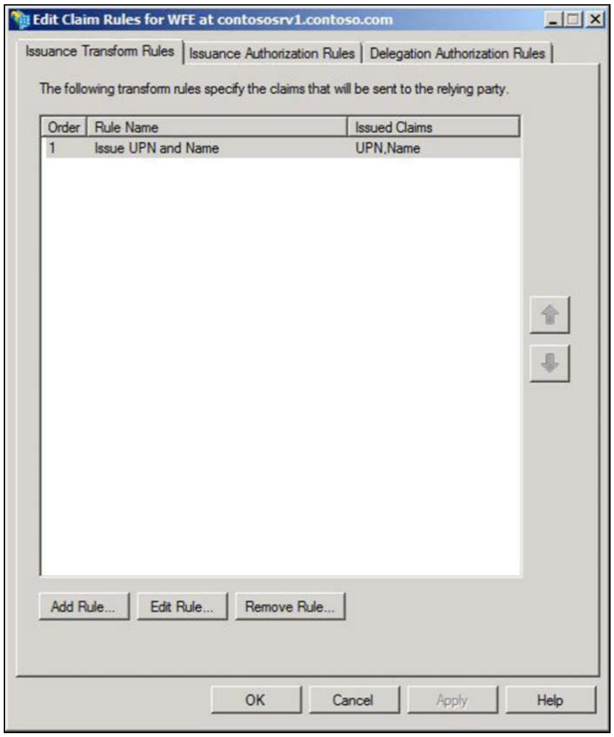
13. Click the **OK** button to the **Edit Claim Rules** dialog, and then click the **OK** button again to save your changes.

Changes to the SSOAuthentication Relying Party

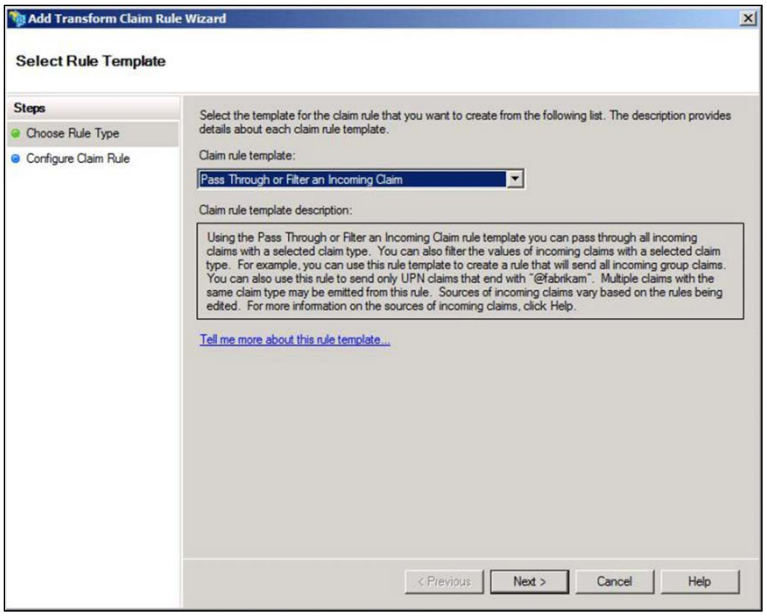
1. Within the Microsoft Management Console, select the **Relying Party Trusts** folder from the left-hand panel to display a list of relying party addresses in the centre panel.



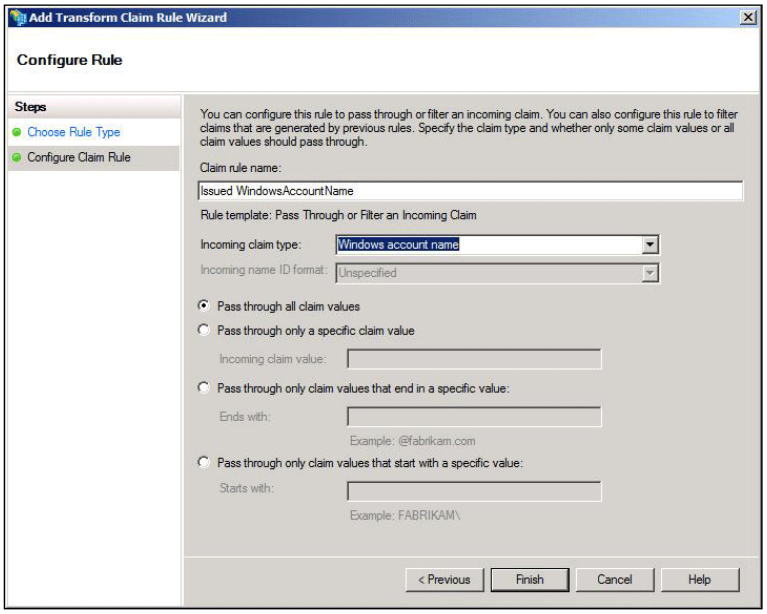
2. Select the SSOAuthentication relying party (https:lab-oneall/SSOAuthentication is the example environment) and then click the **Edit Claim Rules** hyperlink to display the **Edit Claim Rules** dialog.



3. Select the **Issuance Transform Rules** tab and then click the **Add Rule** button to display the **Add Transform Claim Rule** wizard.



4. Select **Pass Through or Filter an Incoming Claim** from the **Claim rule template** drop-down list and then click the **Next** button to display the **Configure Claim Rule** page.

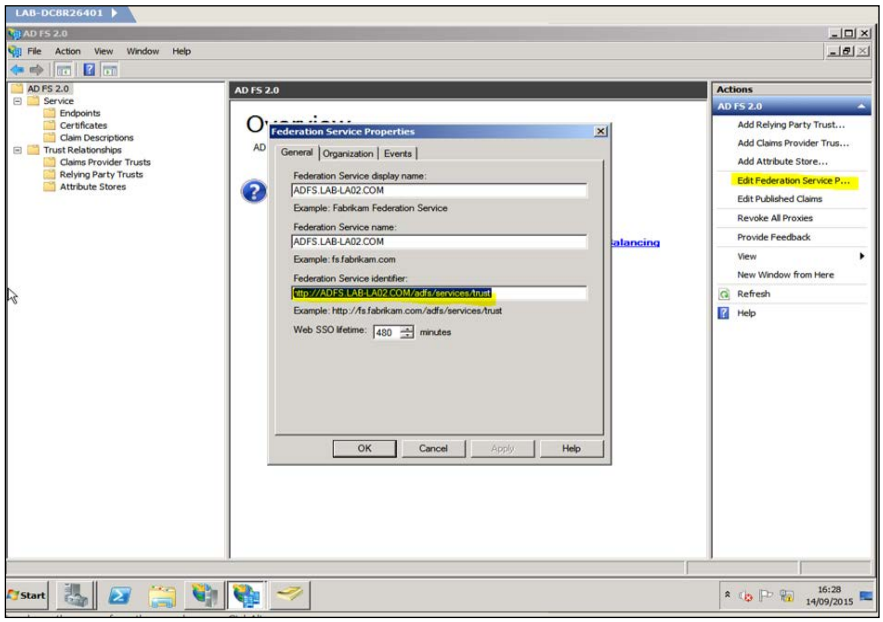


5. Enter “Issued WindowsAccountName” into the **Claim rule name** field.
6. Select **Windows account name** from the **Incoming claim type** drop-down menu.
7. Ensure that the **Pass through all claim values** radio button is selected, and then click the **Finish** button to add the rule and return to the **Edit Claim Rules** dialog.
8. Click the **OK** button to save your changes.

Appendix – Obtaining ADFS Details

Obtaining the ADFS Identifier

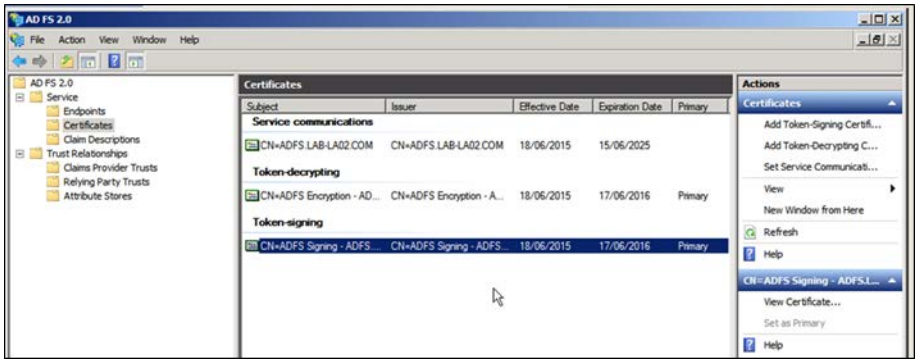
In the ADFS Management application, highlight **ADFS2.0** in the left-hand panel and then click **the Edit Federation Service Properties** hyperlink to display the **Federation Services Properties** dialog.



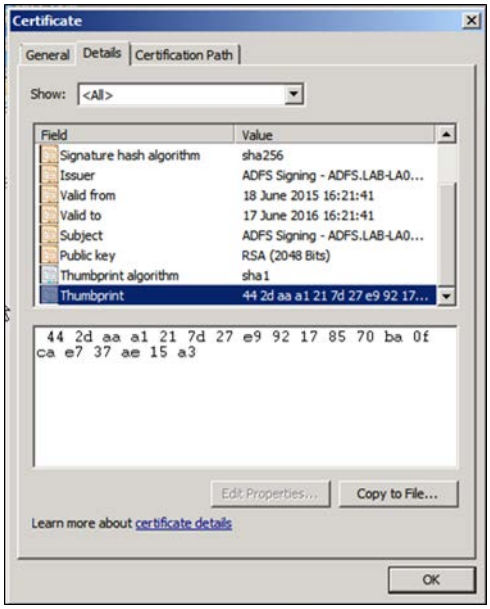
The **Federation Service Identifier** is displayed toward the bottom of the dialog. You can copy this value to use elsewhere if required.

Obtaining the ADFS Signing Token Certificate

1. On the machine hosting the ADFS server, open the ADFS Management application.
2. Select **Certificates** from the left-hand panel to display a list of certificates in the centre panel.



3. Double-click the token-signing certificate to display the **Certificate** dialog.
4. Select the **Details** tab. The thumbprint is displayed in the field at the bottom.



5. Copy and paste the thumbprint into Notepad
6. Remove any spaces and hidden characters that were displayed when you copied the thumbprint into Notepad.

   The thumbprint is now ready for use.

Index

Adding SSOAuthentication as a Relying Party 13
Adding the Application Server as a Relying Party 18
Application Pool 2
CCS OpenID Provider Installer 2
Changes to the Application Server Relying Party 22
Changes to the SSOAuthentication Relying Party 25
Configuring Communication Between the SSOAuthentication Website and the AppServer 22
End Point Enabled on ADFS 13
Granting Permission to Read the Service Certificate's Private Key 9
installing server components prerequisites 2
Introduction 2
Prerequisites for the SSO website 2
server components, installing 2
Settings 3, 8