Daemon Directory Services (DDS)

Collaboration Service

How To: Configure ADFS 2.0 on existing Active Directory

Test Lab: dds-gws.co.uk

Version: 1.0 June 2011

Table of Contents

1 Contents

Document Control/Change History

Version	Date	Author	Changes
1.0	*07/06/2011*	*SH*	*Created document*

2 Overview

This how-to details how to add a single AD FS 2.0 server to your existing infrastructure to provide Secure Token Services for your domain users in order to access applications provided through the GWS Identity Federation Service.

You can view a screencast of this process on our website here:

http://www.g-sphere.co.uk/videos/configure-adfs-for-federation.html

3 Prerequisites:

- □ Windows 2008 or Windows 2008 R2
- □ Domain joined
- □ Web Server Role installed
- □ SSL Certificate that will be trusted by your client browsers
- □ Copy of DDS Federation Metadata XML document

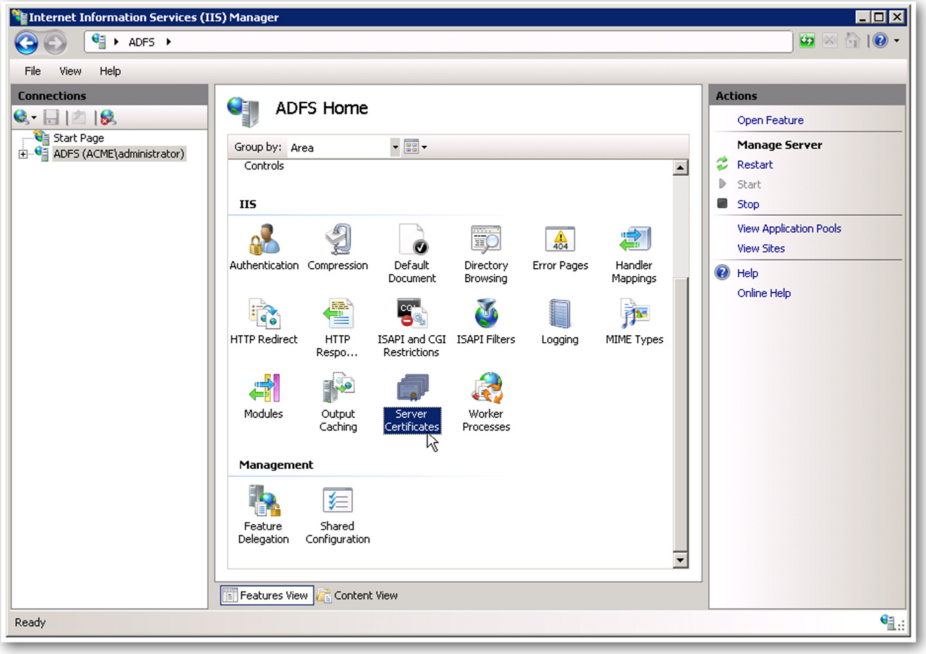
4 Step 1 – Install SSL Certificate

A SSL certificate must be installed on the server before running the AD FS 2.0 configuration wizard, as this is required to secure communications with the AD FS 2.0 server and provide token signing and encryption.

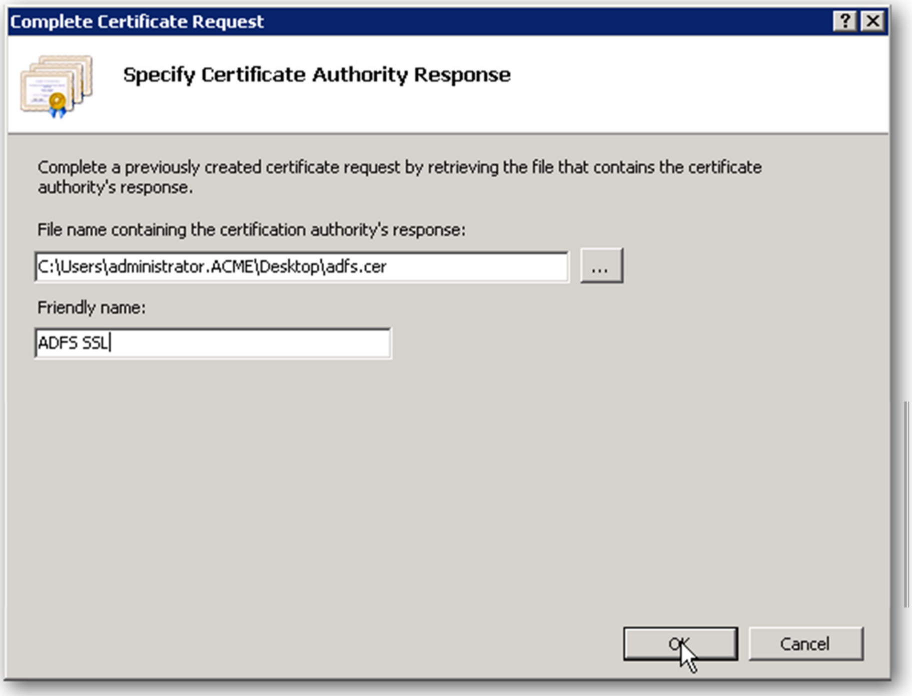
You should obtain the SSL Certificate from a Certification Authority whose root certificate is installed in your client machines browser. This will either be a domain CA where you have pushed the root certificate out to all clients, or a public CA such as Thawte or VeriSign.

Once obtained, follow these steps to install the SSL Certificate on the Default Web Site in IIS:

1. Open IIS Manager
2. Click on the server name
3. Double click on Server Certificates



4. Click on Complete Certificate Request (under Actions)



Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\Users\administrator.ACME\Desktop\adfs.cer

Friendly name:

ADFS SSL

5. Select the .CER file issued by the CA
6. Enter a friendly name (e.g. ADFS SSL)
7. Click OK

You have now added the SSL Certificate.

5 STEP 2 – INSTALL AD FS 2.0

AD FS 2.0 is an additional piece of software freely available from Microsoft. Use the following link to download the installer, taking care to select the correct package for your Windows version and processor architecture:

http://www.microsoft.com/downloads/details.aspx?familyid=118c3588-9070-426a-b655-6cec0a92c10b

Once downloaded simply double click on the installer and follow the prompts through – installation takes about 20 minutes and installs all necessary dependencies.

6 STEP 3 – CONFIGURE AD FS 2.0

Configuring AD FS 2.0 is a straightforward process however there is an important decision to be made early on with regards to redundancy. You can choose to configure AD FS 2.0 in one of two modes: Single Server or Farm. Single Server does what it says – a single server instance of AD FS 2.0. In Farm mode you can either create a new farm or join an existing farm. This allows you to have multiple AD FS 2.0 servers for redundancy and load balancing. This guide will show you how to configure a single server – see the following Microsoft TechNet article for more details on planning your AD FS 2.0 architecture:

http://technet.microsoft.com/en-us/library/gg982491(WS.10).aspx

1. Launch ADFS 2.0 Management Console
2. Click ADFS 2.0 Federation Server Configuration Wizard

3. Select Create a new Federation Service
4. Select Stand-alone federation server
5. Select the SSL Certificate that you installed
6. Click Next to start the configuration process

Once the configuration process has completed follow these steps to add the DDS ADFS server as a Trusted Relying Party:

1. Click Add Relying Party Trust…
2. Select Import data about the relying party from a file
3. Click Browse and select the Federation Metadata XML document supplied by DDS
4. Enter DDS ADFS as the display name and click Next
5. Select Permit all users to access this relying party and click Next
6. Check the Identifiers tab to ensure the Federation Metadata has loaded correctly and click Next
7. Click Close and the Edit Claims dialog will load

At this point you have added the DDS ADFS server as a trusted relying party – this means that your ADFS will issue tokens to the DDS ADFS server when requested.

The next step (for demonstration purposes) is to add a claim mapping:

1. Click Add Rule
2. Select Pass Through or Filter an Incoming Claim from the Claim rule template drop-down list and click Next
3. Enter Pass Through Email in the Claim rule name box
4. Select E-Mail Address from the Incoming Claim Type drop-down list and click Finish

You have now completed the configuration steps required.

7 Export Federation Metadata

The final stage is to export the federation metadata XML document so that DDS can configure your ADFS server as a Claims Provider.

1. Open a web browser on the server and enter the address: https://<your-server-name>/FederationMetadata/2007-06/FederationMetadata.xml
2. Right click on the document and click View Source
3. Click File > Save and save the file

Send the file to DDS at collabsupport@dds-labs.co.uk