Setting up AD FS

Instructions for Windows Server 2012 R2 running Active Directory.

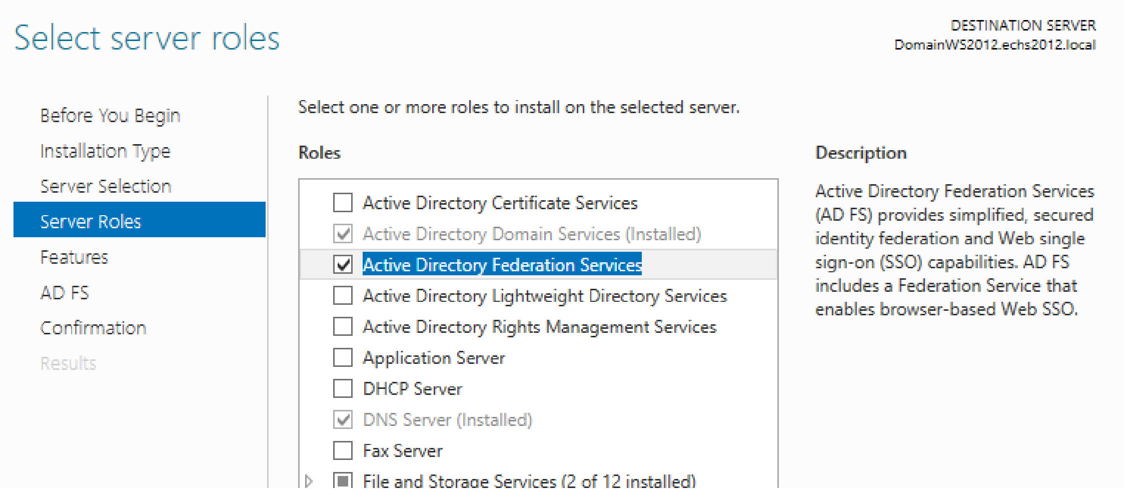
Enroll an SSL certificate for AD FS

Before you can use SSO, you will have to get an SAML certificate and set up your eCompliance management system account to use it. See the “SSO SAML Instructions” document for details on this process.

Install AD FS

Detailed instructions at http://technet.microsoft.com/en-us/library/dn486802.aspx

- Open Server Manager
- Click Add Roles and Features
- Select "Role-based or feature-based installation"
- Select your server (default is the server that you're running on)
- Select Active Directory Federation Services



Select server roles

DESTINATION SERVER
DomainWS2012.echs2012.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

Select one or more roles to install on the selected server.

Roles

□ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☑ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
☑ DNS Server (Installed)
□ Fax Server
▣ File and Storage Services (2 of 12 installed)

Description

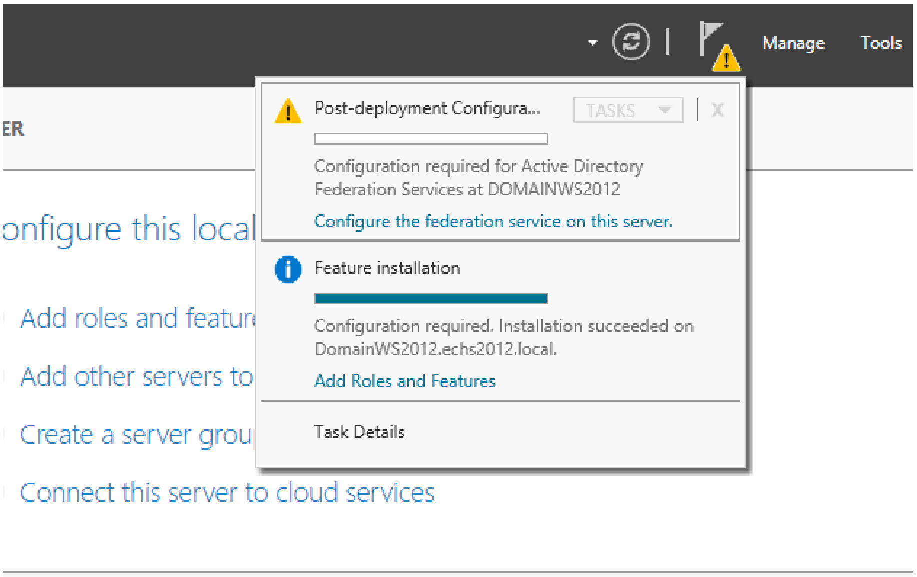
Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

- Finish the wizard

Configure AD FS

Detailed instructions at https://technet.microsoft.com/en-us/library/dn486807.aspx

In Server Manager, click the notification that appears after AD FS is installed



Post-deployment Configura...

Configuration required for Active Directory Federation Services at DOMAINWS2012

Configure the federation service on this server.

Feature installation

Configuration required. Installation succeeded on DomainWS2012.echs2012.local.

Add Roles and Features

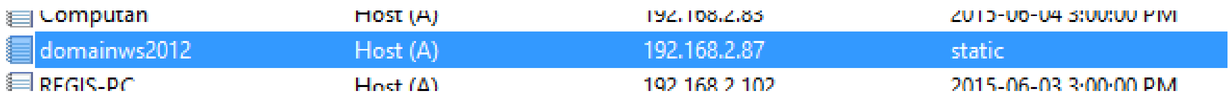
Task Details

- Accept "Create the first federation server..."
- Select the Active Directory administrator user
- Import the SSL certificate you generated or requested in the first step
- Pick a display name for the Federation Service
- Pick an account for the AD FS service (eCompliance recommends using a gMSA)
    - If you see a yellow information bar, you will have to add the instructions to create a KDS root key before you can use a gMSA
- Choose either internal or SQL database
- Carefully review your selections
- Click until finished

Configure DNS

Verify that your DNS has an A record (not a CNAME) for your AD FS server.

In DNS Manager, there should be an entry like this (where the zone is your AD FS server, and the name matches your domain).



Computan	Host (A)	192.168.2.83	2015-06-04 3:00:00 PM
domainws2012	Host (A)	192.168.2.87	static
REGIS-PC	Host (A)	192.168.2.102	2015-06-03 3:00:00 PM

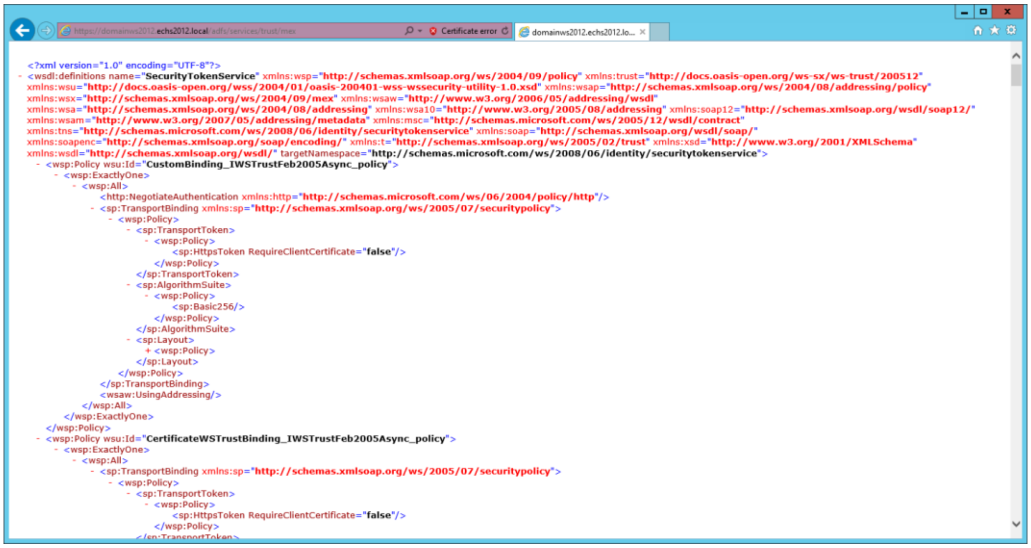
Verify Federation Server

Detailed instructions at https://technet.microsoft.com/en-us/library/dn486821.aspx

Ensure that the federation server is set as an intranet site on all client machines

In a browser, navigate to https://<federationserver>/adfs/services/trust/mex

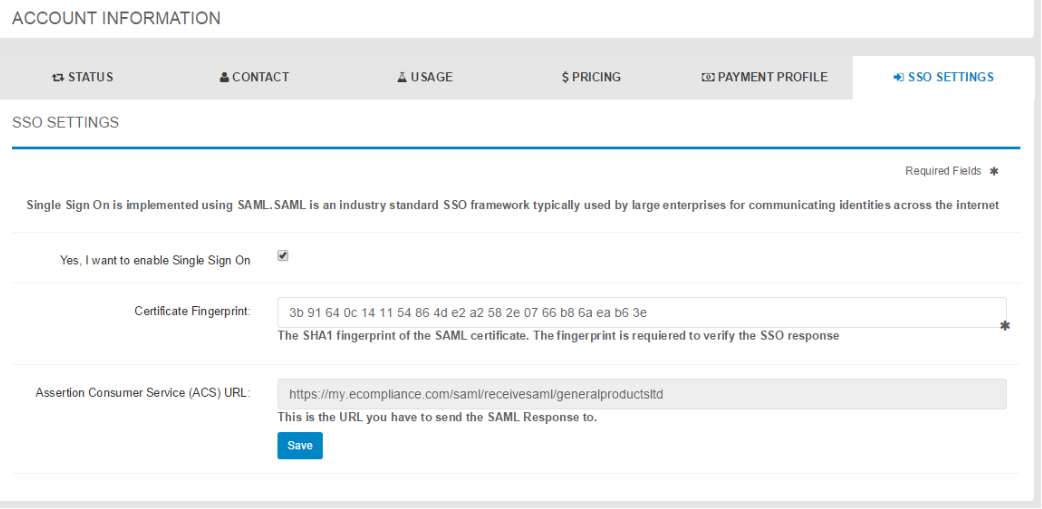
It should look something like this:


https://domainws2012.echs2012.local/adfs/services/trust/mex
Certificate error
domainws2012.echs2012.lo...

```
  <?xml version="1.0" encoding="UTF-8"?>
- <wsdl:definitions name="SecurityTokenService" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
  xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex" xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa10="http://www.w3.org/2005/08/addressing" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
  xmlns:tns="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" targetNamespace="http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice">
  - <wsp:Policy wsu:Id="CustomBinding_IWSTrustFeb2005Async_policy">
    - <wsp:ExactlyOne>
      - <wsp:All>
          <http:NegotiateAuthentication xmlns:http="http://schemas.microsoft.com/ws/06/2004/policy/http"/>
        - <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          - <wsp:Policy>
            - <sp:TransportToken>
              - <wsp:Policy>
                  <sp:HttpsToken RequireClientCertificate="false"/>
                </wsp:Policy>
              </sp:TransportToken>
            - <sp:AlgorithmSuite>
              - <wsp:Policy>
                  <sp:Basic256/>
                </wsp:Policy>
              </sp:AlgorithmSuite>
            - <sp:Layout>
              + <wsp:Policy>
              </sp:Layout>
            </wsp:Policy>
          </sp:TransportBinding>
          <wsaw:UsingAddressing/>
        </wsp:All>
      </wsp:ExactlyOne>
    </wsp:Policy>
  - <wsp:Policy wsu:Id="CertificateWSTrustBinding_IWSTrustFeb2005Async_policy">
    - <wsp:ExactlyOne>
      - <wsp:All>
        - <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          - <wsp:Policy>
            - <sp:TransportToken>
              - <wsp:Policy>
                  <sp:HttpsToken RequireClientCertificate="false"/>
                </wsp:Policy>
              </sp:TransportToken>
```

SSO Setup

You will need your eCompliance ACS URL for this step. You can find this in your eCompliance account settings, in the SSO Settings tab:



SSO SETTINGS

Required Fields *

Single Sign On is implemented using SAML.SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet

Yes, I want to enable Single Sign On ☑

Certificate Fingerprint: 3b 91 64 0c 14 11 54 86 4d e2 a2 58 2e 07 66 b8 6a ea b6 3e *
The SHA1 fingerprint of the SAML certificate. The fingerprint is requiered to verify the SSO response

Assertion Consumer Service (ACS) URL: https://my.ecompliance.com/saml/receivesaml/generalproductsltd
This is the URL you have to send the SAML Response to.

While you are at this stage, verify the SSO SAML URL in your eCompliance settings, this should be of the form https://<federationserver>/adfs/ls

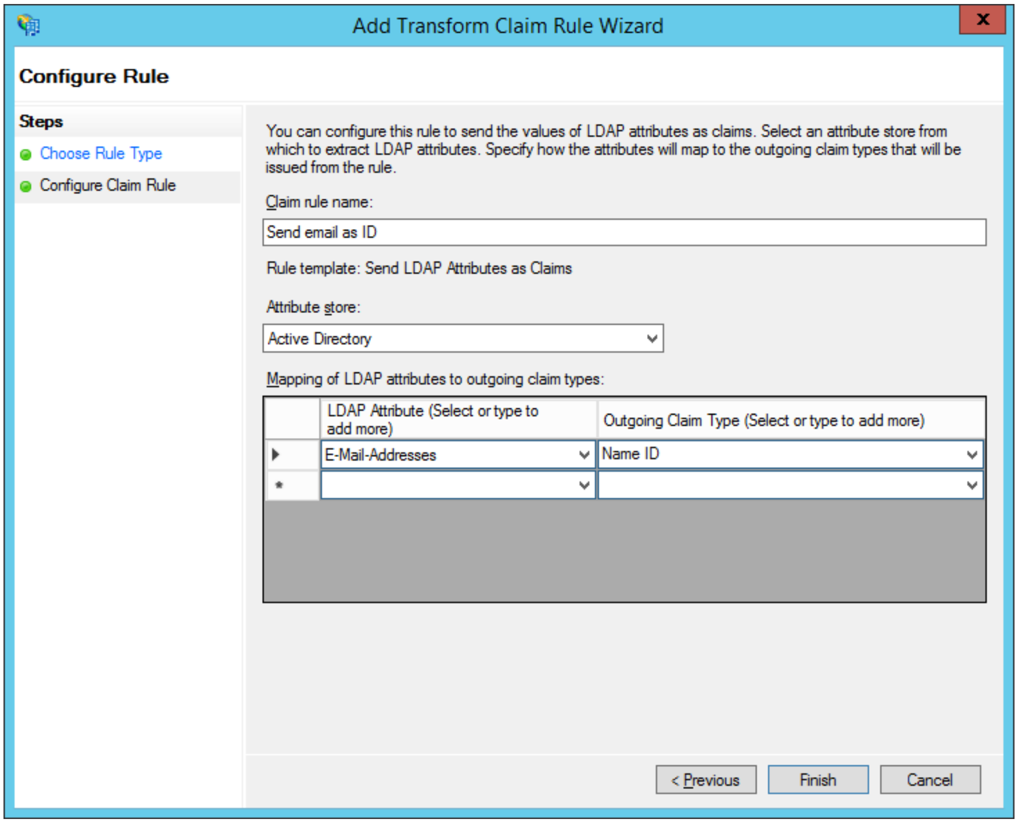
In Server Manager, select Tools > AD FS Management

- Select Service > Endpoints and confirm that /adfs/ls is present and enabled
- Confirm that the Certificates view contains certificates for Service communications, Token-decrypting and Token-signing
- Go to Trust Relationships > Relying Party Trusts and select Add Relying Party Trust...
- Select "Enter data about the relying party manually"
- Specify eCompliance as the display name
- Leave AD FS profile selected

- You do not need a token encryption certificate
- Select the SAML 2.0 WebSSO protocol and specify the ACS URL from eCompliance
- Add "http://ecompliance.com" as a Relying party trust identifier
    - If you are setting SSO up on an eCompliance staging server (such as robot), the trust identifier should be changed accordingly (such as http://robot.ecompliance.com).
- Skip past multi-factor authentication unless you're feeling really ambitious
- Choose your preferred authorization rules (if unsure, select Permit all)
- Click until finished

In the window that appears after adding the trust (if you have closed this window, you can get it back by right-clicking on the eCompliance trust and selecting Edit Claim Rules).

- Select the Issuance Transform Rules tab and click Add Rule...
- Leave Send LDAP Attributes as Claims selected
- Set these settings:



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: Send email as ID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	Name ID
*		

- Finish

eCompliance requres that both the SAML response and assertion are signed. To enable this, open PowerShell and run this command:

```
Set-AdfsRelyingPartyTrust -TargetName eCompliance -SamlResponseSignature MessageAndAssertion
```

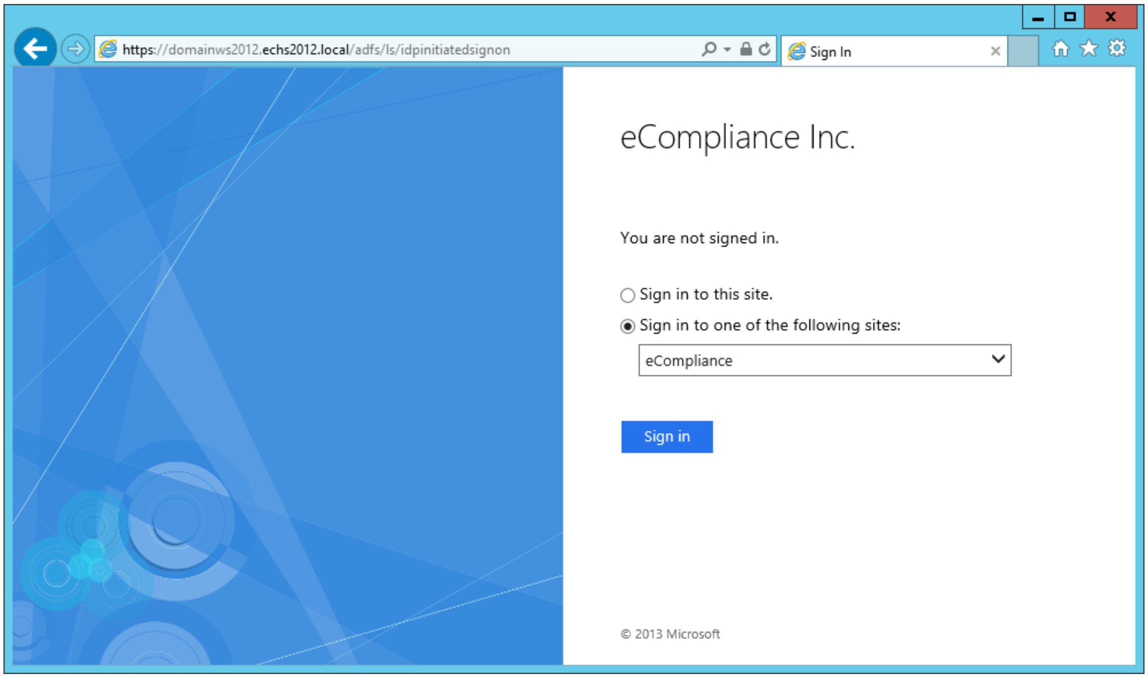
This setup will work in Internet Explorer. If automatic sign in is required for Chrome or Firefox, run the following:

```
Set-AdfsProperties -ExtendedProtectionTokenCheck Allow
```

Then, restart the Active Directory Federation Services service

Verify SSO setup

In a client browser, go to https://<federationserver>/adfs/ls/idpinitiatedsignon


https://domainws2012.echs2012.local/adfs/ls/idpinitiatedsignon
Sign In
Sign in

eCompliance Inc.

You are not signed in.

○ Sign in to this site.

● Sign in to one of the following sites:

eCompliance

© 2013 Microsoft

Troubleshooting

Some common problems and fixes

The AD FS service will not start

- Make sure that the user running the service has the correct SPN. It should have one for **HOST/name.of.federation.service.name** .
- Make sure that Microsoft Key Distribution Service starts before the AD FS service by setting its startup type to Automatic