LEGALINTELLIGENCE

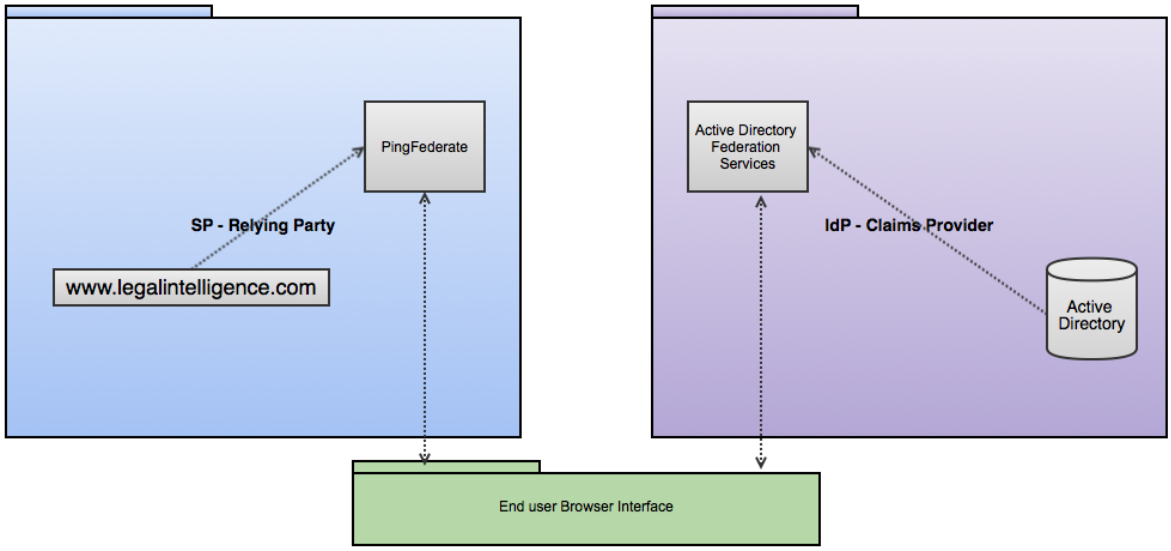
Single Sign On AD FS 2.0 QuickGuide

For Single Sign-On to Legal Intelligence

Introduction

This QuickGuide describes the steps needed to setup a SSO connection between your AD FS 2.0 server and Legal Intelligence. In this context, your AD FS 2.0 server is the Claims Provider and the Ping Federate server at Legal Intelligence acts as the Relying Party.

Package Structure



The instructions are based on the Microsoft guide at http://technet.microsoft.com/en-us/library/gg466930(WS.10).aspx.

Requirements
http://technet.microsoft.com/nl-nl/ff678034%28WS.10%29.aspx

Prerequisites

Check Internet Information Services (IIS) to make sure your server has a Default Web Site with an https binding. If the certificate used for the binding is not suitable for SSO, create a new https binding at a different port. More information available at http://social.technet.microsoft.com/wiki/contents/articles/2554.ad-fs-2-0-how-to-replace-the-ssl-service-communications-token-signing-and-token-decrypting-certificates.aspx and http://blogs.technet.com/b/canitpro/archive/2013/06/13/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365.aspx

To avoid conflicts it is strongly recommended to install ADFS on a server with a clean IIS i.e. without other websites.

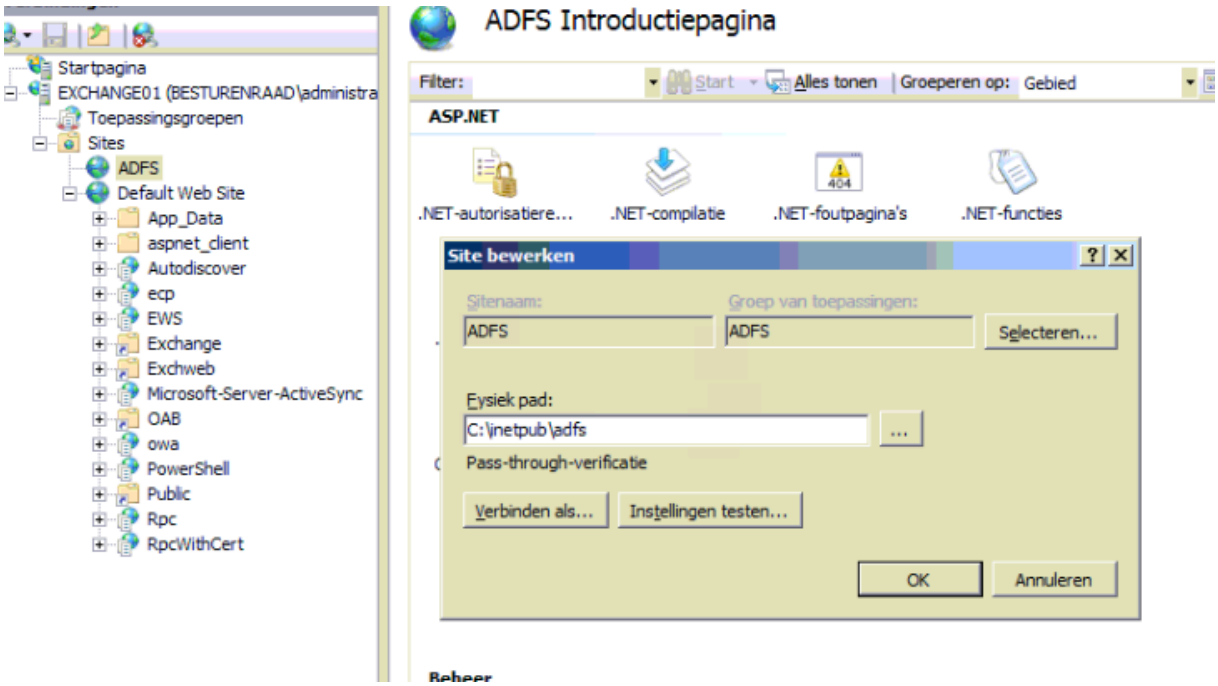
Test IIS by entering the https://{full_servername} in the browser, you should see the Startscreen of IIS.

Steps

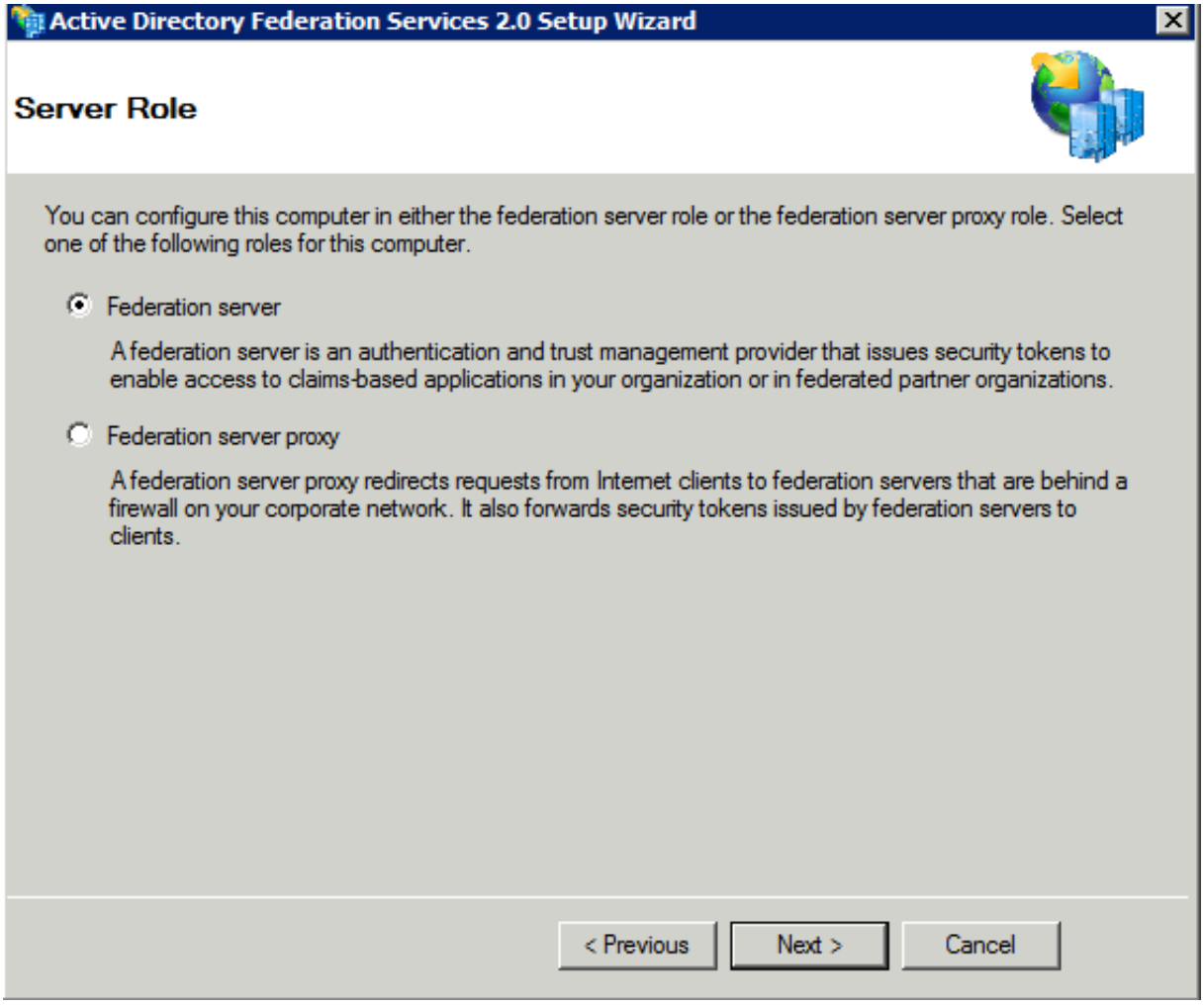
1. Install AD FS 2.0

   Download installation file from
   http://www.microsoft.com/en-us/download/details.aspx?id=10909
   Select the language and OS version before download.

   After installation, one should have a folder like C:\inetpub\adfs which is assigned to a website as can be seen in IIS.

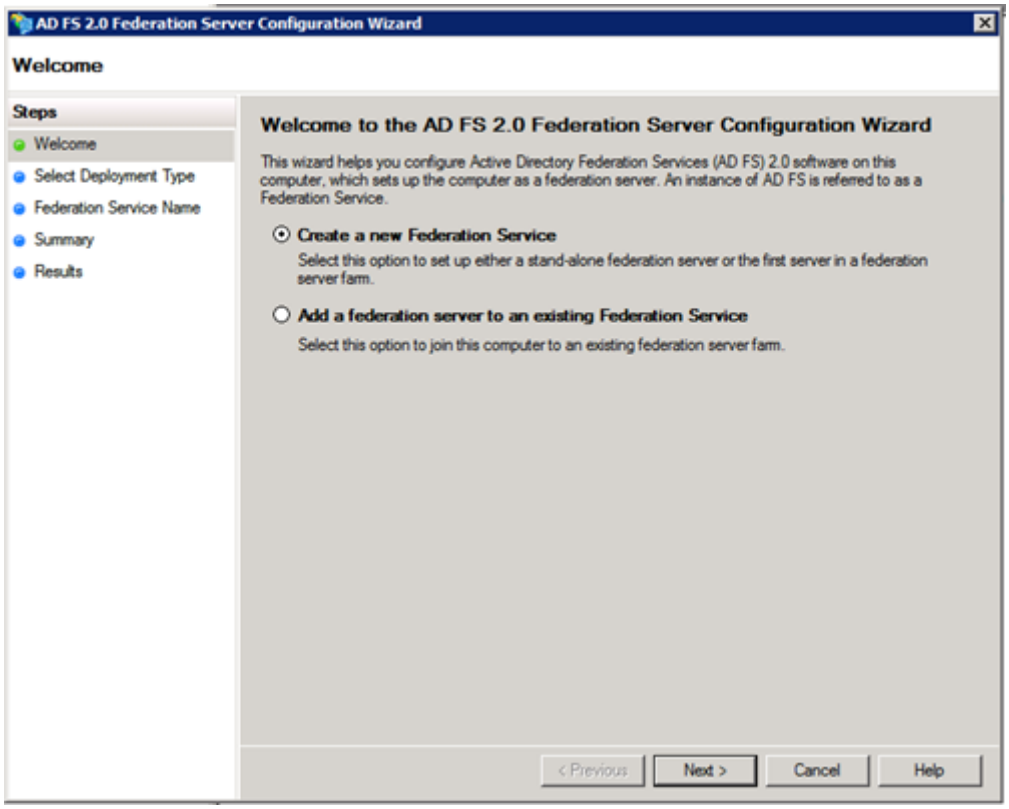


   In the Federation Server Configuration Wizard, choose Create a new Federation Service.

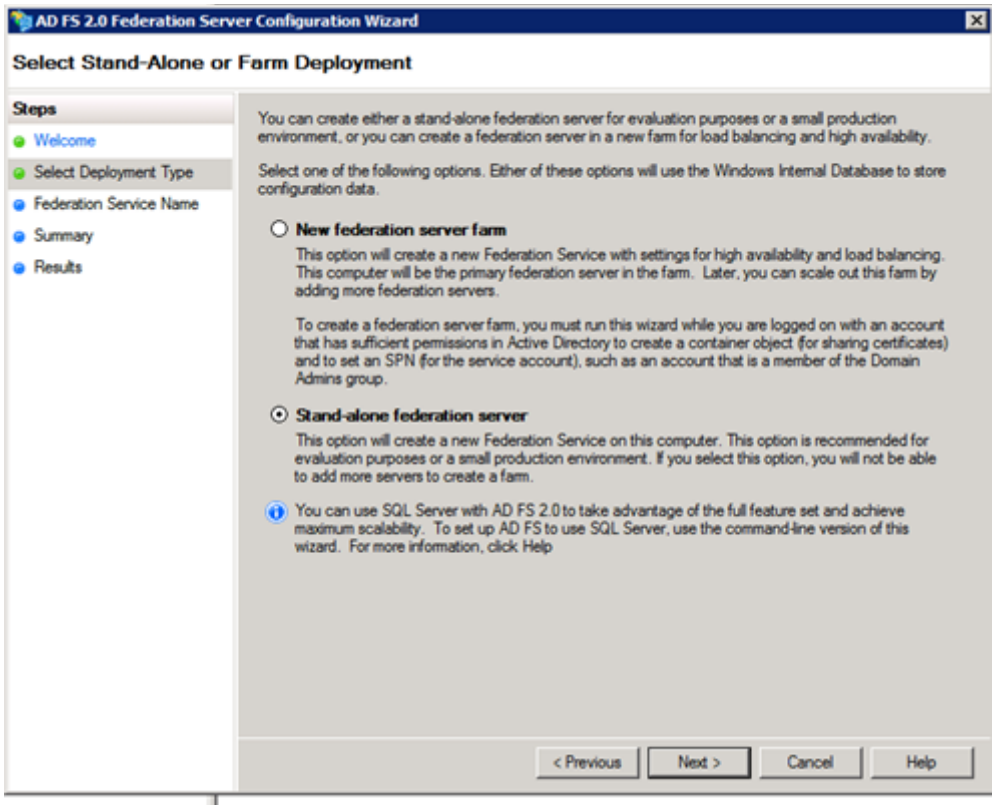


Start AD FS 2.0 Federation Server Configuration Wizard.
See http://www.syfuhs.net/post/2010/08/13/Installing-ADFS-2-and-Federating-an-Application.aspx for more information.

Choose Create a new Federation Service.

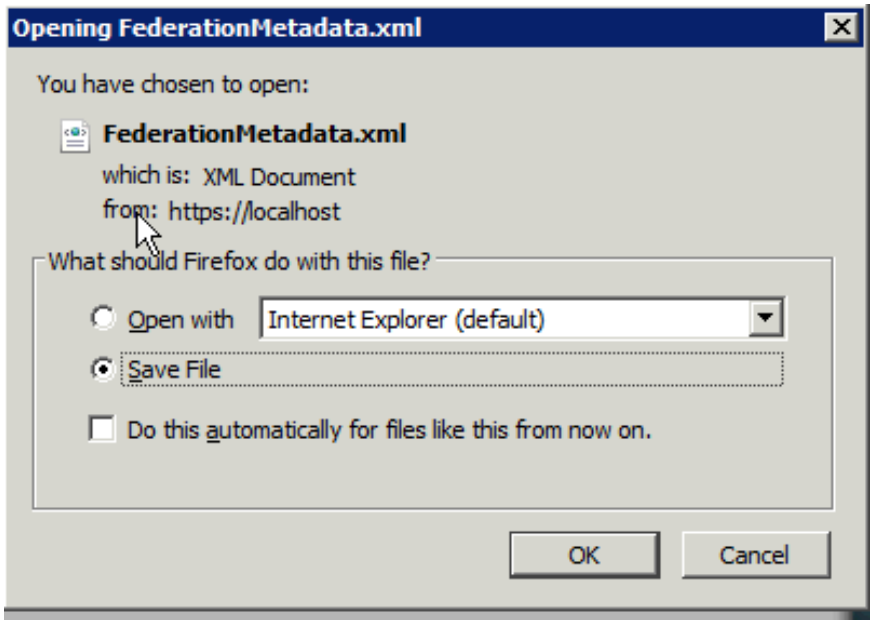


Select Stand-alone federation server.



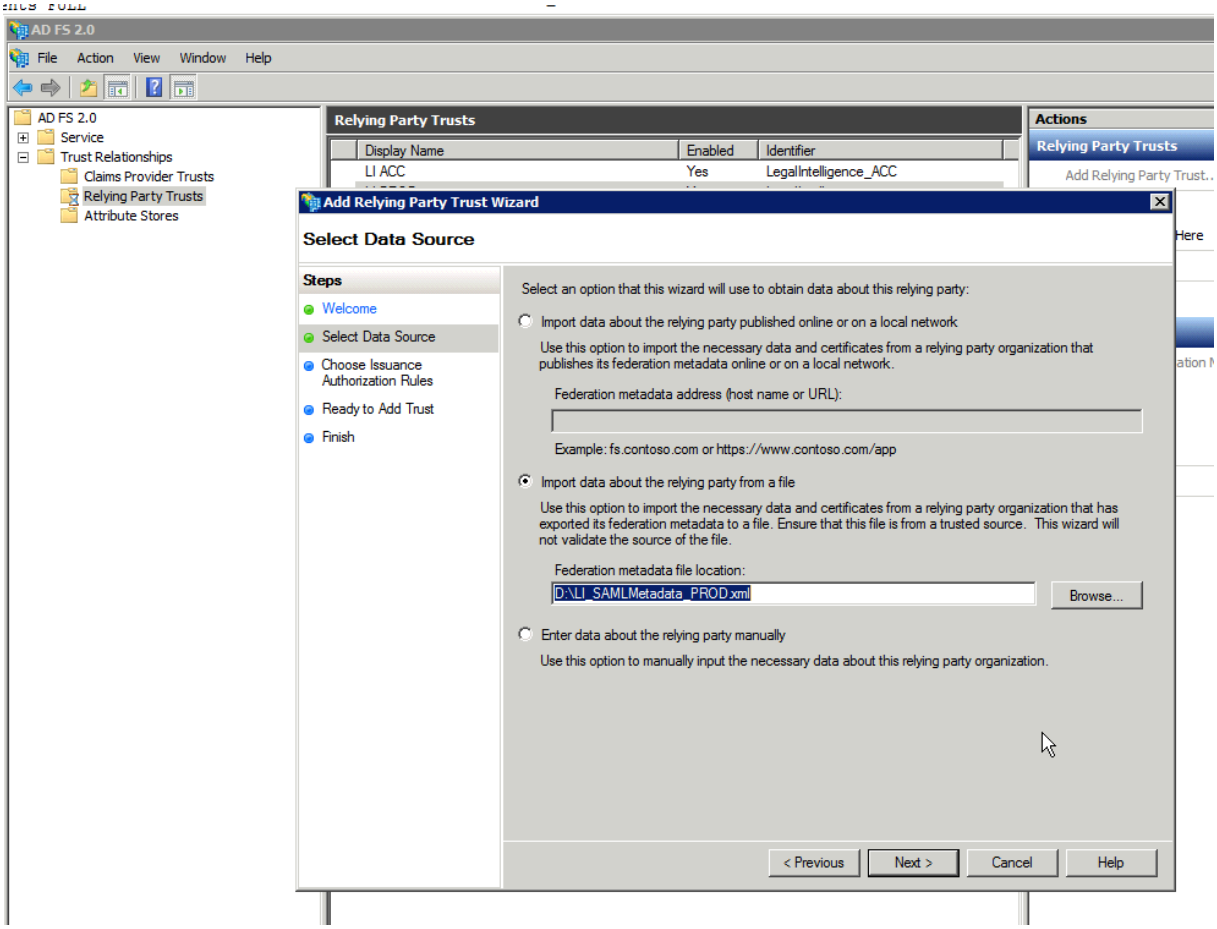
Note1: The wizard can also be manually started by running C:\Program Files\Active Directory Federation Services 2.0\ FsConfigWizard.exe.
Note2: To uninstall ADFS 2, select Active Directory Federation Services 2.0 at Installed Updates.

2. Export the AD FS 2.0 metadata by opening https://localhost/FederationMetadata/2007-06/FederationMetadata.xml. The federation service name is usually the Full Computer Name which can be find in the Server Manager. Save the xml-file directly to a file i.e. do NOT copy paste the metadata from the browser!

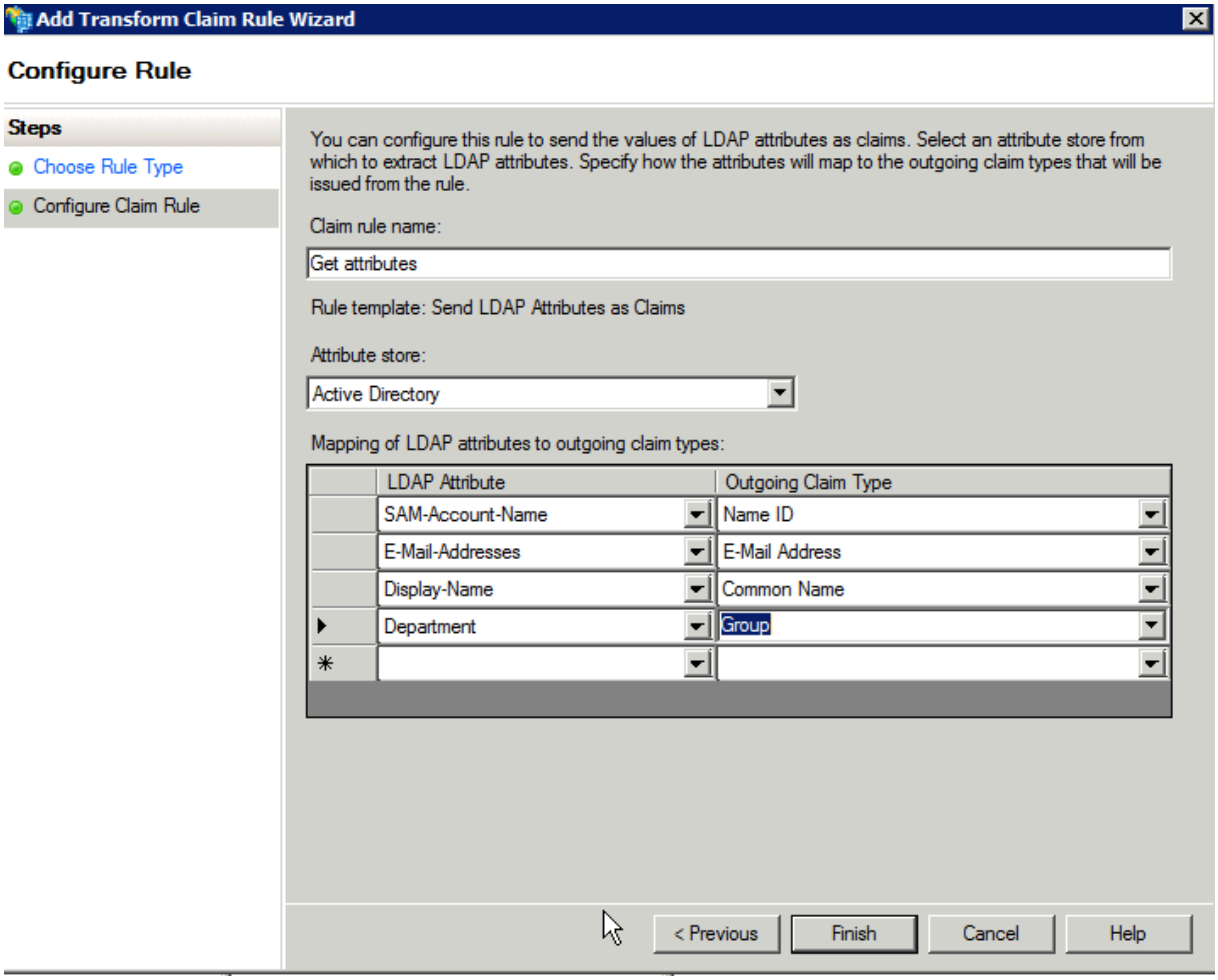


3. Send the XML-file together with your IP-address to Legal Intelligence (to be found at http://whatismyipaddress.com/). The metadata is needed to setup the connection in PingFederate.

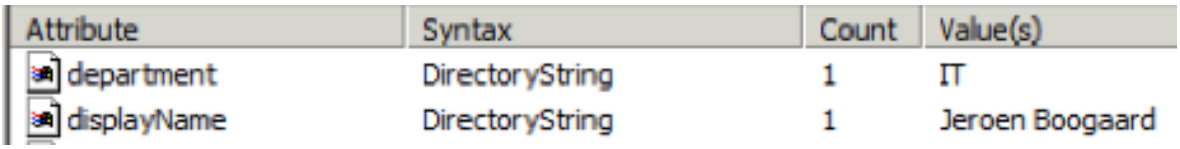
4. Add a Relying Party Trust
Follow the instructions on http://technet.microsoft.com/en-us/library/adfs2-federation-with-ping-identity-ping-federate%28v=ws.10%29.aspx under 'Configure AD FS 2.0 as the Claims Provider and PingFederate as the Reling Party -> Configure AD FS 2.0'. You will need to import the metadata sent by Legal Intelligence.



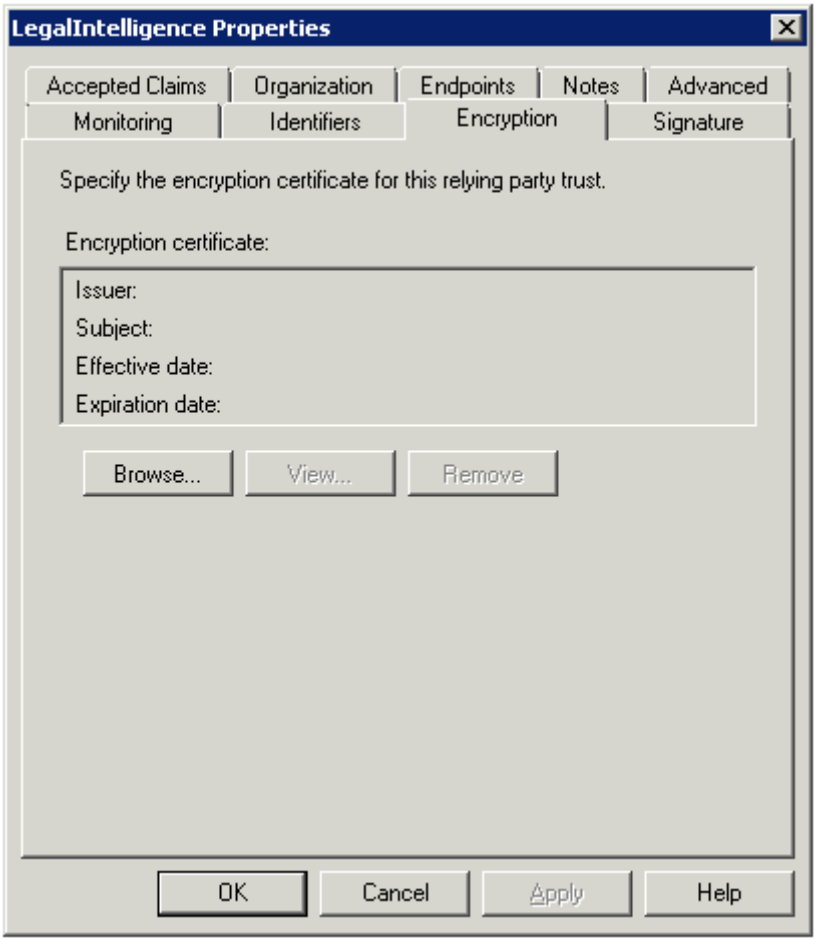
5. Add claim rule named “LI PRD” and select Send LDAP Attributes as claims. Choose Active Directory as Attribute store. Define the attribute mapping as shown below, the attribute department is optional. The Outgoing Claim Type attributes (right column) represent the attributes defined in the SSO contract.



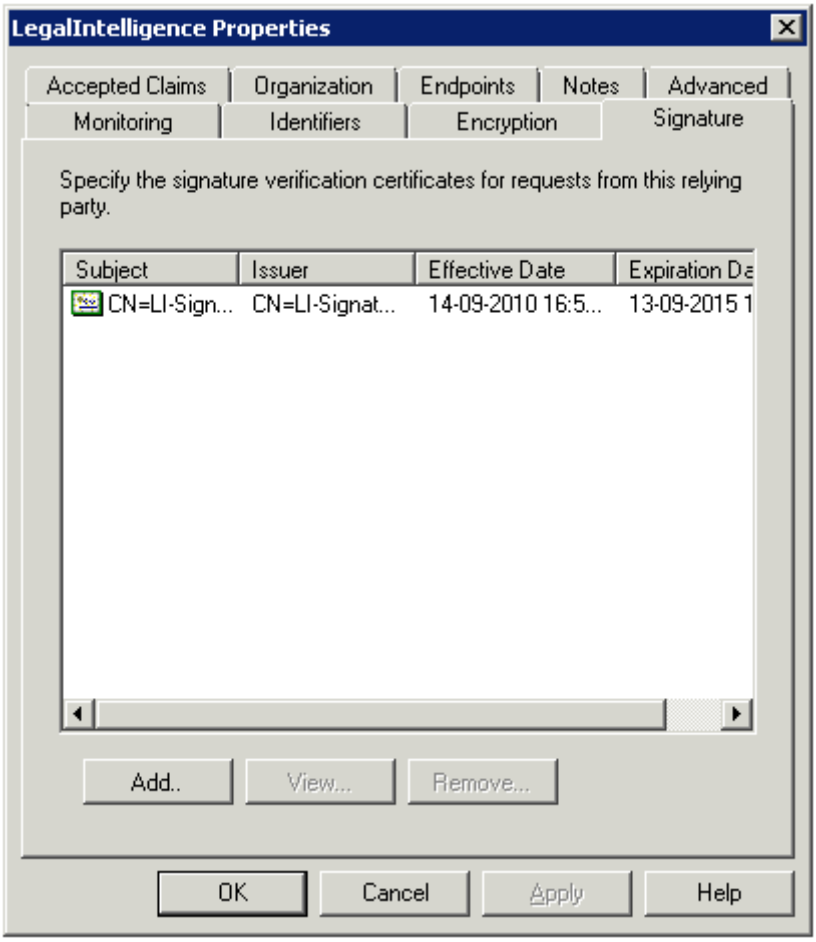
The LDAP attributes may be different in your network. Use AD Explorer (download.sysinternals.com/files/AdExplorer.zip) to find out the exact attribute names used in your network.



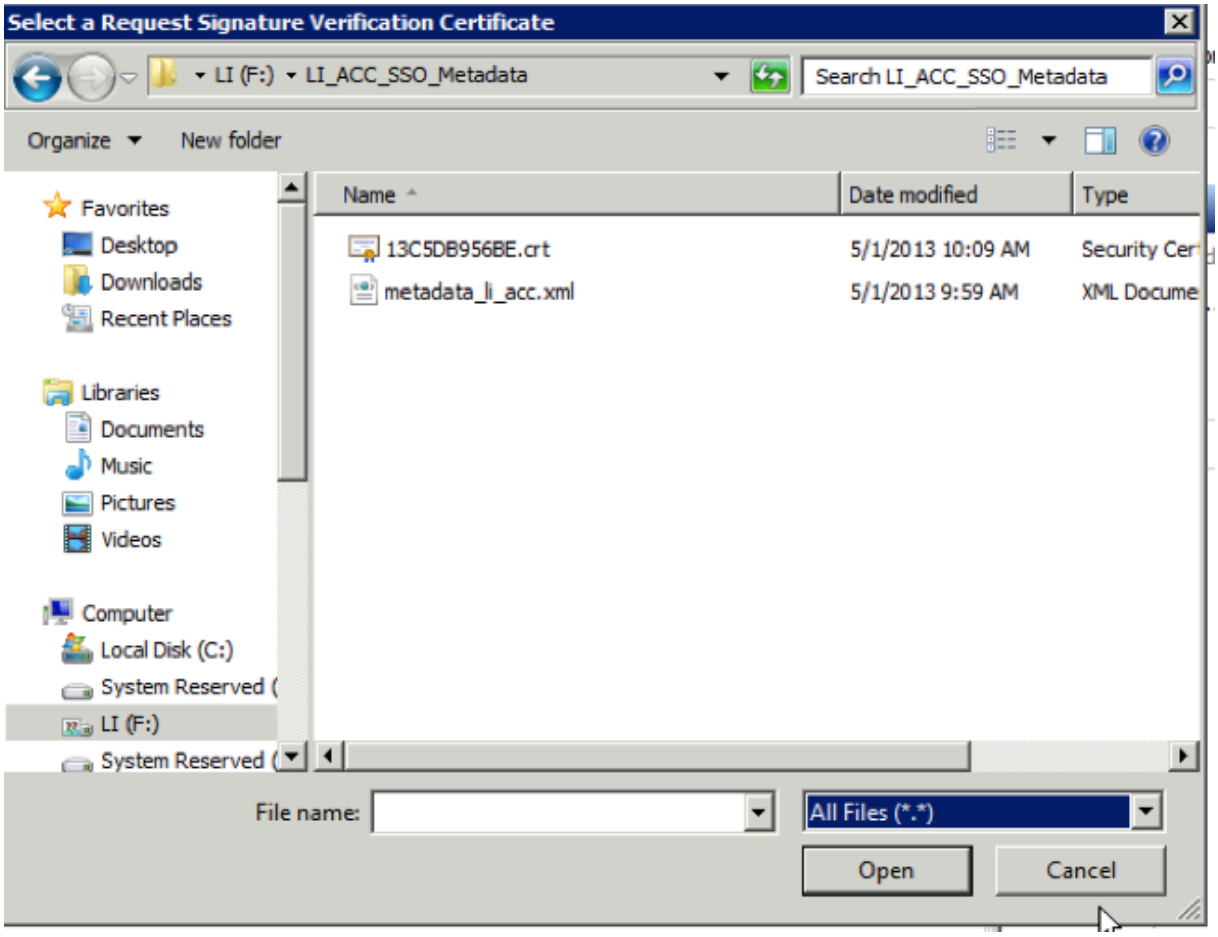
6. Configure the certificate settings by editing the properties of the Relying Party Trust. Make sure that there is no certificate at Encryption (if there is, remove it).



In Signature, add the certificate that you received from Legal Intelligence.



To be able to select the certificate, first select ‘All files (*.*)’ since the certificate has a different extension.



7. Prepare the browser; follow the instructions in chapter Windows Authentication.

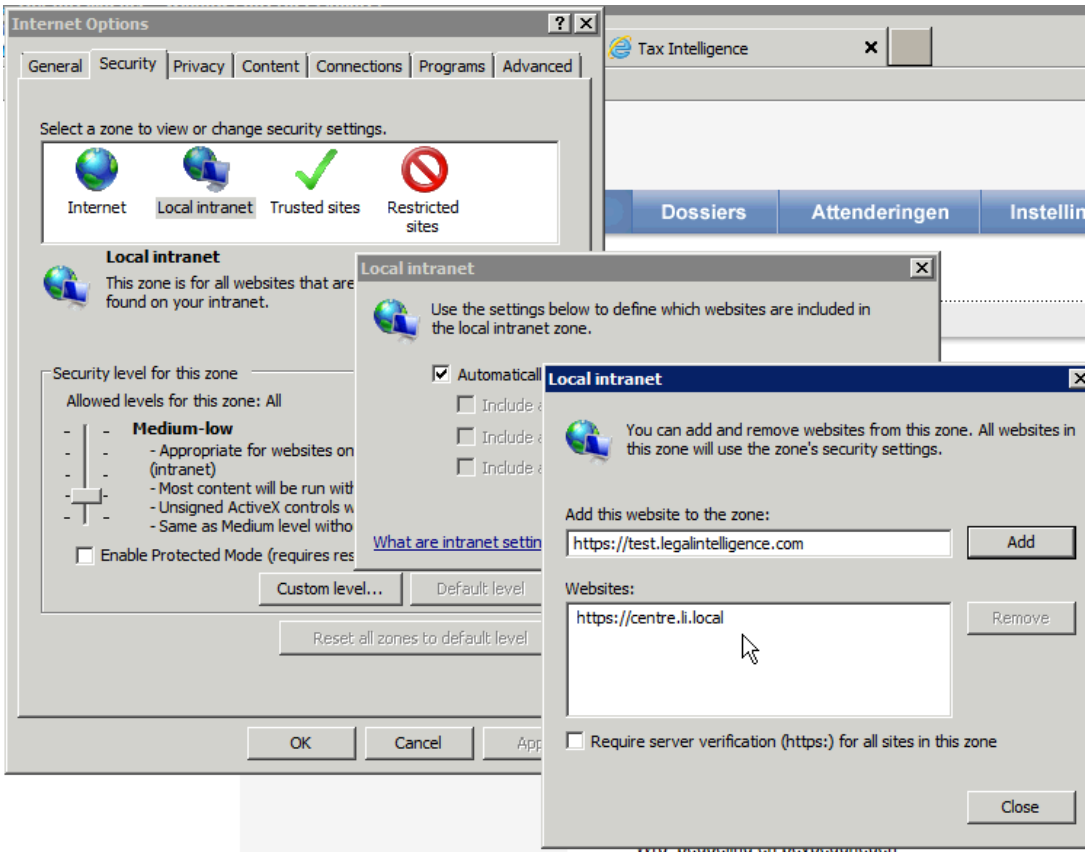
8. Once Legal Intelligence has updated the LI WebSite access configuration with your IP-addresses, test the following URL:
http://www.legalintelligence.com/sso/test

Windows Authentication

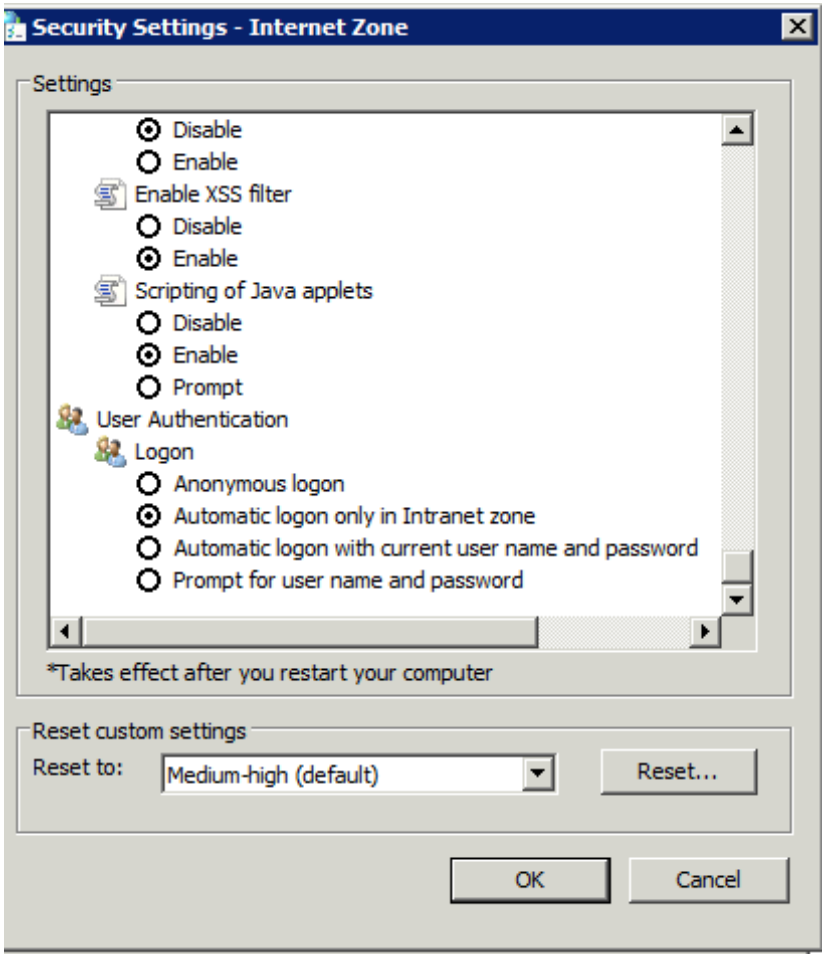
If your browser does not continue to login on the Legal Intelligence website, probably the Integrated Windows Authentication settings needs to be reconfigured.

Internet Explorer and Chrome

Navigate to Control Panel -> Network and Internet -> Internet options -> Security and add https://www.legalintelligence.com and your IIS Server URL to the Local intranet zone as shown below.



Next, click *Custom level*, scroll down and select *Automatic logon with current user name and password*.



More information at https://sysadminspot.com/windows/google-chrome-and-ntlm-auto-logon-using-windows-authentication and http://support.microsoft.com/kb/258063

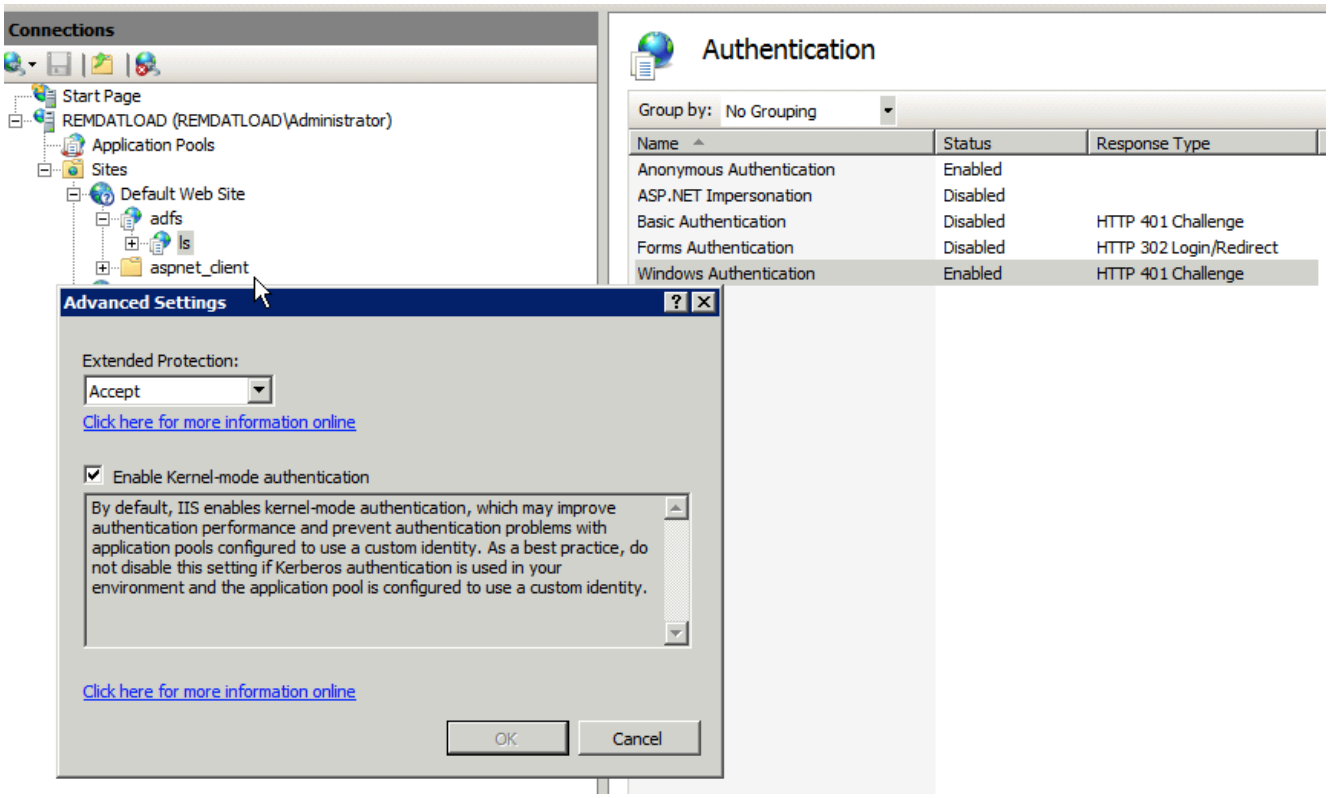
Firefox

1. Open Firefox
2. In the address bar type: about:config
3. Firefox3.x and later requires you to agree that you will proceed with caution.
4. After the config page loads, in the filter box type: network.automatic
5. Modify network.automatic-ntlm-auth.trusted-uris by double clicking the row and enter http://www.replacewithyoursite.com or http://your-intranet-server-name
6. Note 1: Multiple sites can be added by comma delimiting them such as http://www.replacewithyoursite.com, http://www.replacewithyourintranetsite.com
   Note 2: If your ADFS uses a different port, add the portnumber such as http://your-intranet-server-name:8843

More information at http://markmonica.com/2007/11/20/firefox-and-integrated-windows-authentication

Extended Protection

Open Internet Information Services, select Is in the left column and click at *Authentication* in the middle column. Right click at *Windows Authentication* and select Advanced Settings. Make sure that Extended Protection is set to *Accept*.


Connections
Start Page
REMDATLOAD (REMDATLOAD\Administrator)
Application Pools
Sites
Default Web Site
adfs
ls
aspnet_client
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Enabled
ASP.NET Impersonation
Disabled
Basic Authentication
Disabled
HTTP 401 Challenge
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Windows Authentication
Enabled
HTTP 401 Challenge
Advanced Settings
Extended Protection:
Accept
Click here for more information online
Enable Kernel-mode authentication
By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.
Click here for more information online
OK
Cancel

Replace Token Signing certificate

The ADFS Token Signing certificate will expire someday, so it needs to be replaced without interrupting the current SSO configuration. Follow the steps below to replace the ADFS Token Signing Certificate.

1. Inform Legal Intelligence that you planned to replace the certificate.

2. Run Windows **Powershell** as Administrator and enter the following commands.

Add-PSSnapin "microsoft.adfs.powershell" ; this will add ADFS commands to Powershell

Get-ADFSCertificate -CertificateType token-signing ; shows the current Token-SigningCertificate

set-adfsproperties -CertificateDuration 730 ; renew Token-SigningCertificate

The next command will activate the new certificate, Intelligence, SSO will no longer work until this certificate is not yet known by Legal Intelligence. This will not be noticed by users that are already logged in.

update-adfscertificate -CertificateType: Token-Signing -Urgent:$True ; this update your ADFS configuration

Get-ADFSCertificate -CertificateType token-signing ; shows the new Token-SigningCertificate

3. Export the certificate by following the instructions at http://microscoff.com/2013/09/19/renewing-adfs-2-0-certificates-in-sharepoint-2013/

4. Send the exported certificate to Legal Intelligence ASAP

Important: If the certificate is not being replaced before 15 days before the expiration date, it will be renewed automatically without notifying!

This can be turned off by the following Powershell commands

Add-PSSnapin Microsoft.Adfs.Powershell

Set-ADFSProperties -AutoCertificateRollover $false

More info can be found at http://technet.microsoft.com/en-us/library/ee892317.aspx