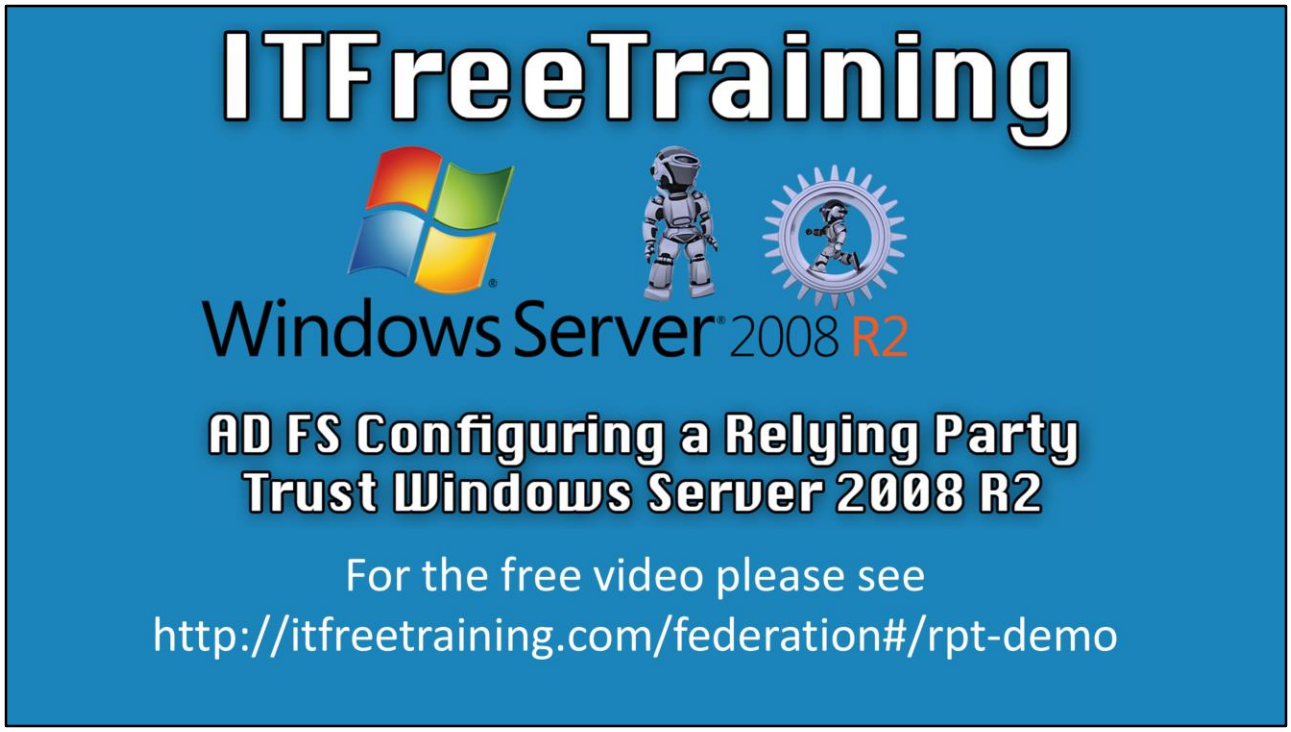

This video looks at how to create a relying party trust on Windows Server 2008 R2 using Active Directory Federation Services. The relying party trust is the configuration that is used to create a claim.

Demonstration

In the previous videos, a basic install of Active Directory Federation Services has been performed. This video will look at configuring an existing Active Directory Federation Services install with a relying party trust.

1)To create the relying party trust, open AD FS 2.0 Management from under Administrative Tools under the start menu.
2)To start the wizard to create the trust, expand down through trust relationship until you reach the container “Relying Party Trusts”. Right click this container and then select the option “Add Relying Party Trust”.
3)When the welcome screen appears, press the start button.
4)The “select data source” screen of the wizard requests when to import the configuration data that will be used with the relying party trust. There are 3 different ways this data can be imported. The first option “Import data about the relying party published online or on a local network” will contact the other Active Directory Federation Server and transfer the data from that server. This option requires a direct network connection between the two servers. The second option “Import data about the relying party trust” requires that the data from the other Federation Server be exported in a file. Once this file has been exported, it needs to be transferred to the other server using a medium like e-mail or a flash drive. The last option “Enter data about the relying party manually” requires the administrator to enter in the data for the relying party trust manually.

5)In this case, the option “Import data about the relying party published online on a local network” will be used. In order to do this, a secure connection is required so the remote server requires the certificate from the local server. See below how to add the certificate.
6)On the next screen, enter in a friendly name for the relying party trust. This will assist other administrators working out what the trust is for. After entering the friendly name, move on to the next screen.
7)The next screen will ask what the default rule is for the Issuance Authorization. If the permit rule is used, by default users will be given access. If the deny rule is selected, a rule will have to be created before the user will be granted access. This provides better security but also means more work for the administrator. In this case the deny rule will be used.
8)The next screen will show all the information that was obtained and will be used to create the wizard. This is read only and cannot be changed.
9)Once the wizard is complete, the relying party trust has been created and is ready to be used.

Adding a certificate for SSL
In order for a direct connection to be made between the 2 Federation Servers, a certificate needs to be imported on the remote server and local server from the other server. This will allow a secure connection from the local server to the remote server to transfer the relying party trust configuration.
1)Run MMC from the start menu.
2)Select the option “Add/Remove snap-in” from under the file menu.
3)Add the snap-in certificates.
4)When prompted, select the option “Computer account” to access the certificates on the local server.
5)When asked each computer you want to manage, leave it on the default option of “Local computer” and press finish to complete the wizard.
6)Press o.k. to go back to the console.
7)Expand down to certificates located under “Trusted Root Certification Authority”. Select the certificate for Active Directory Federation Services and double click to open it.
8)To export the certificate, select the details tab and then press the button “Copy to File” to start the certificate export wizard.
9)Once past the welcome screen, leave it on the default option of “DER encoded binary X.509 (.CER)” and move on to the next screen.
10)The next screen saves the certificate to the location of your choice. This file will next need to be transferred to the remote server.
11)Complete the wizard to export the certificate to the location that was specified.
12)To import the certificate on the remote server, open MMC and add the

certificate snap-in by running steps 1 to 6 on the remote server.
13)The certificate for this remote server needs to be export. Repeat steps 7 to 11 above.
14)To import the certificate from the other server, make sure the Certificates container under Trust Root Certification Authority is open. Right click the white space and select import under all tasks.
15)Browse to the location of the ITFreeTraining certificate.
16)Make sure the store is “Trusted Root Certification Authorities” and complete the wizard.
17)Repeat steps 14 to 16 on the other server to import the certificate.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com
for our always free training videos. This is only one video from the many free courses available on YouTube.

References
none