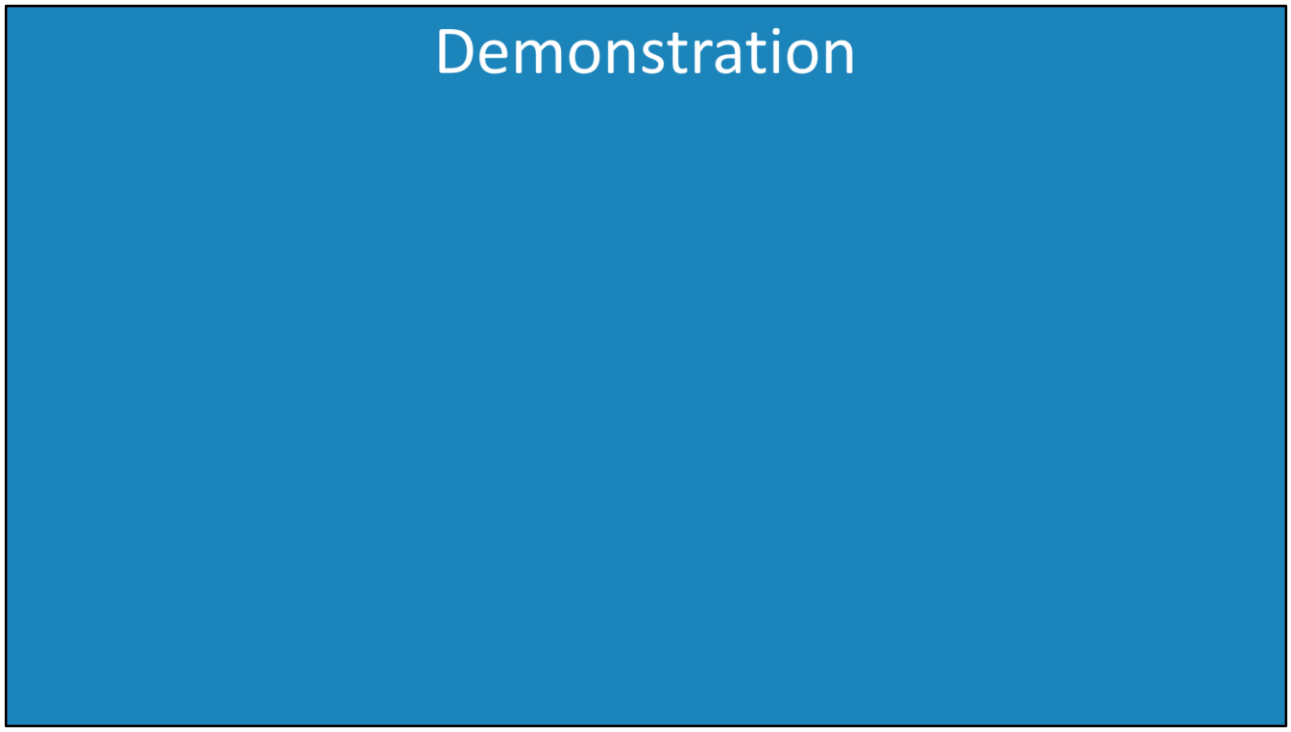
This video from ITFreeTraining will look at how to install Active Directory Federation Services. The install requires a certificate. If you do not have certificate services installed, see our previous video on how to install Active Directory Certificate Services.



Demonstration installing Active Directory Federation Services role

00:42 To start the install, open Server Manager by selecting the shortcut in the quick launch bar.

00:50 From the Server manager home screen, select the option “Add roles and features”.

00:58 Skip the welcome screen and on installation type select “Role-based or feature-based installation” and press next.

01:04 On the select destination server screen, select the server that you wish to install the role on and press next. In this case the server “ITADFS2012R2.ITFreeTraining.local” was selected.

01:12 On the select server roles screen select the option “Active Directory Federation Services” and press next.

01:24 On the select features screen, no additional features are required so press next to continue.

01:30 The AD FS home screen contains information about AD FS, press next to continue.

01:40 At the confirm installation selection screen press install to install the role.

Demonstration requesting and installing a certificate

02:04 To request a certificate from an Enterprise CA, right click the start menu and select run. Enter in the run box mmc and press ok.

02:30 For the certificate management, select “Add/Remove snap-in” from the file

menu.
02:35 From the list of snap-ins select the certificate snap-in and press add.
02:44 You will then be prompted for the scope for the certificate snap-in. Since the certificate will be used by the server, the option for computer account needs to be selected and press next.
02:55 On the select computer screen leave it on the default option of “Local computer” and press finish and then o.k to complete the wizard.
03:05 If you open the Personal container, this will show all the certificates that are currently installed on that server.
03:13 Certificate is not present and needs to be requested. The default view is not the best view to request the certificate with. To change the view, right click on the container Personal and select options under the view menu. Refresh the view if the option is not present.
03:30 The default mode will be “Logical certificate stores”. Change this to “Certificate purpose” and press o.k.
03:45 Select the container “Server Authentication”, right click it and select the option “Request New Certificate” under “all Tasks”.
04:05 On the certificate enrollment wizard, press next to skip the welcome screen.
04:09 The “Select Certificate Enrollment Policy” screen will ask which enrollment policy you want to use. It is possible to create multiple enrollment policies, however in this case the default enroll policy “Active Directory Enrollment Policy” will be selected and next pressed.
04:56 The new screen will ask which template will be used to create the certificate. In previous videos the “ADFS SSL Certificate” template was created. In this case it will be selected and the button enroll pressed. Windows Server will now renew the certificate as required using auto enrollment.
05:30 To complete the wizard press finish and the certificate will be added to the container “Server Authentication” and MMC can be closed.

Demonstration Configuration Active Directory Federation Services
05:38 To configure the Active Directory Federation Services role, select the exclamation mark at the top of Server Manager and select the option “Configure the federation service on this server”.
05:53 On the welcome screen of the configuration wizard there is an option to configure the farm options for the server. The default option “Create the first federation server in a federation server farm” will create a new farm with only that Federation server in it. If you an existing Federation Server Farm and want to add this server to that Federation’s server farm, select the second option “Add a federation server to a federation server farm”. In previous versions of Active Directory Federations Servers, there was an option for stand-alone, in Windows Server 2012 R2 this option is no longer available. Once you have chosen the option, press next to continue.

06:52 The next screen will ask which user account will be used to perform the install. A domain administrator account is required to create a key distributed key management object during the install which will also need administrator rights on the local computer. Once the account has been selected, press next to move on to the next screen of the wizard.
07:05 On the next screen the certificate to be used with Active Directory Federation Services needs to be selected. Since this has already been created it can be selected from the pull down menu. If the certificate has not been installed and is available in a file, the import option can be used to import the certificate.
07:27 On this screen a Federation Service Display Name needs to be entered. This should be a friendly name as the user will see this name. Once this has been entered, press next to move on to the next screen of the wizard.
07:40 On specify service account screen, a service account needs to be selected or created to be used with Active Directory Federation Services. In this case there is a warning message saying “Group Managed Services account are not available because the KDS root key has not been set....”. If a root key does not exist in Active Directory this message will appear. This key is required to keep the randomize passwords used between different servers the same when they are used in the same farm. This step is required to be performed in PowerShell.
08:45 To create a Root Key, go to Server Manager and select the option on the left hand side “All servers”. Select a Domain Controller, right click it and select PowerShell. This will run PowerShell on the Domain Controller. The command will not work on member servers as they do not have Active Directory Services installed.
09:07 From PowerShell run the command “Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)” The command should only take a few seconds to run. The Root key will be created on that Domain Controller and will need to be replicated to the other Domain Controllers in your domain. This can be run before Active Directory Federation Services is installed if the administrator wants to prepare ahead of time.
09:40 Once the PowerShell command has been run, enter exit twice to exit PowerShell.
09:48 Since the PowerShell command has just been run the option to create a service account will be grayed out. Press back and next again to refresh the screen.
10:00 Select the option “Create a Group Managed Service Account”. For the name, in this case, FsGmsa was used for Federation Services Group Managed Service account and then press next.
10:15 The next screen will ask if SQL Server will be used or the internal Windows database. In this case there is no SQL server on the network so the option “Create a database on this server using Windows Internal Database” will be used. Once selected, press next to move on.
10:31 The next screen will allow you to review the settings that have been selected. If you are happy with the settings press next to continue to the next screen of the wizard.

10:43 The next screen will perform a pre-requisite check to make sure everything it ready. If you have only just created the root key using PowerShell you may get a warning message. This will disappear after 10 hours, however it will not prevent the wizard from being able to be completed.
11:18 Press configure to complete the wizard.
11:50 Press close to close the wizard.

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
"Windows Server 2012: Group Managed Service Accounts"
http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx