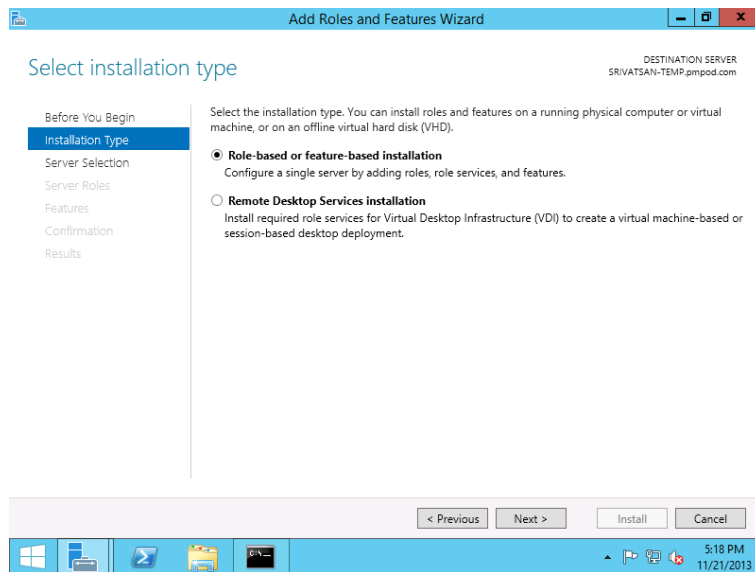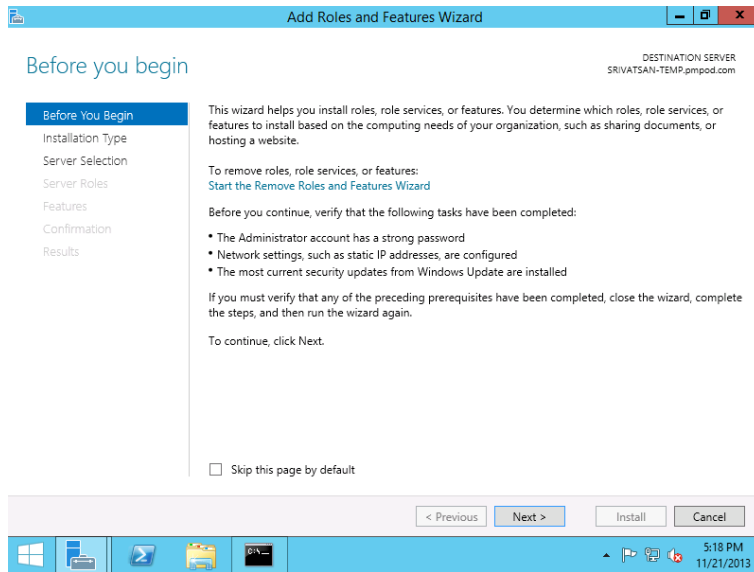# Configuring AD FS in Windows Server 2012 R2

Go to Server Manager --> Add Roles & Features wizard

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter: [   ]

Name	IP Address	Operating System
SRIVATSAN-TEMP.pmpo...	172.18.10.13	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous | Next > | Install | Cancel

5:19 PM
11/21/2013

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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
- ☑ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▷ ☑ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services

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.

< Previous | Next > | Install | Cancel

5:20 PM
11/21/2013

Add Roles and Features Wizard

Select features

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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

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

Features

- ▷ ☐ .NET Framework 3.5 Features
- ▷ ☑ .NET Framework 4.5 Features (2 of 7 installed)
- ▷ ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☐ IIS Hostable Web Core
- ☐ Ink and Handwriting Services
- ☐ Internet Printing Client

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous | Next > | Install | Cancel

5:22 PM
11/21/2013

Add Roles and Features Wizard

Active Directory Federation Services (AD FS)

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

< Previous   Next >   Install   Cancel

5:22 PM
11/21/2013

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Add Roles and Features Wizard ✕

⚠ If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes   No

Export configuration settings
Specify an alternate source path

< Previous   Next >   Install   Cancel

5:22 PM
11/21/2013

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
SRIVATSAN-TEMP.pmpod.com

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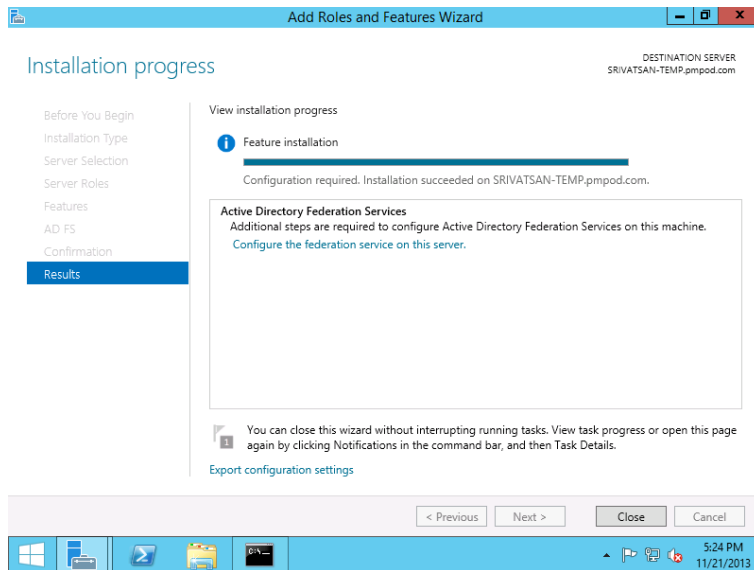
View installation progress

ⓘ Starting installation

Active Directory Federation Services

🗋 You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
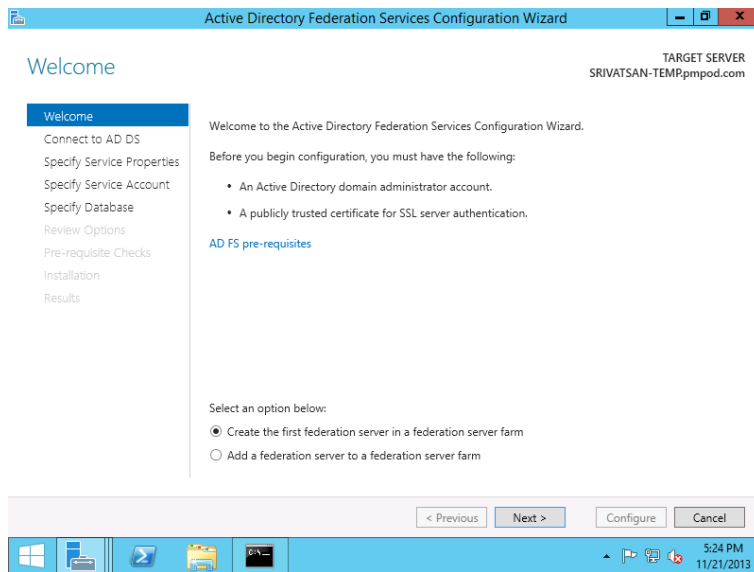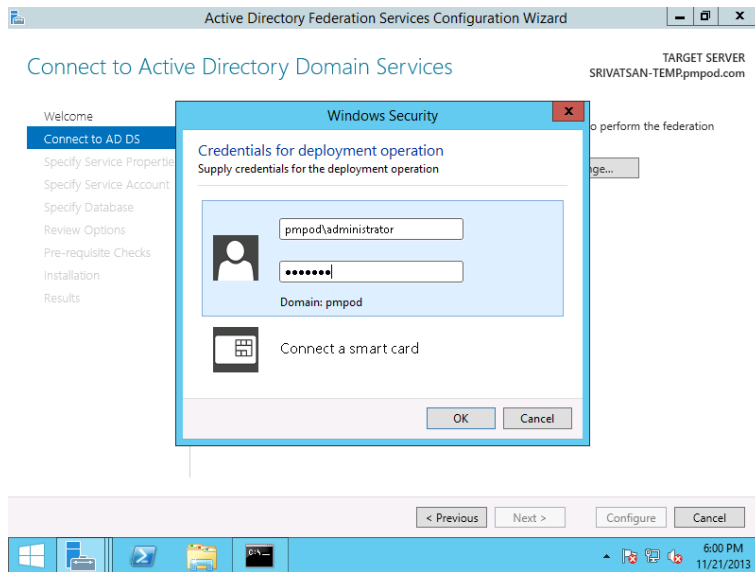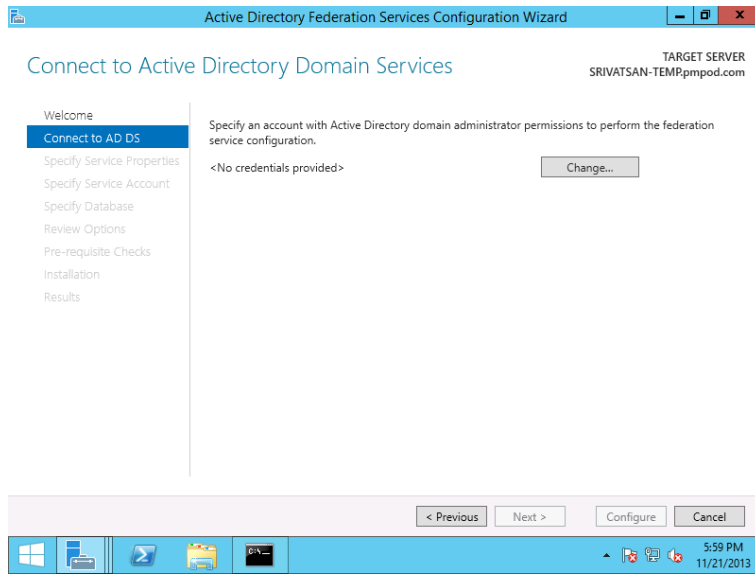
Export configuration settings

< Previous   Next >   Install   Cancel

5:22 PM
11/21/2013

In the above screenshot, click on the "Configure the federation service on this server". You will get the below screen

To create a self-signed certificate, use makecert.exe and pvk2pfx.exe available with Windows SDK.
After installing Windows SDK,
1. Open a command prompt
2. Run the following commands :

- makecert -r -pe -n "CN=adfs.yourdomain.com" -b 01/01/2013 -e 01/01/2014 -sky exchange Server.cer -sv Server.pvk
(Instead of "adfs.yourdomain.com" give the fully qualified name of the AD FS system in the above command)

- pvk2pfx.exe -pvk Server.pvk -spc Server.cer -pfx Server.pfx

Now, click "Import" button and select the "Server.pfx" file that you created using above commands
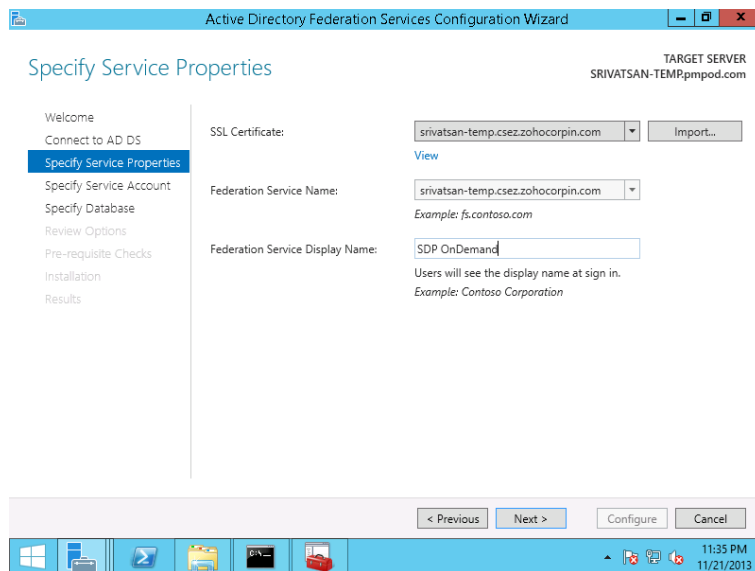
Active Directory Federation Services Configuration Wizard

Specify Service Account

TARGET SERVER
SRIVATSAN-TEMP.pmpod.com

⊗ Error determining whether gMSA is available: Group Managed Service Accounts require a domain with at least one... Show more ✕

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

Account Name: PMPOD\ [   ]

● Use an existing domain user account or group Managed Service Account

Account Name: PMPOD\administrator   [Clear]   [Select...]

Account Password: [●●●●●●]

[< Previous] [Next >]   [Configure] [Cancel]

11:39 PM
11/21/2013

Active Directory Federation Services Configuration Wizard

Specify Configuration Database

TARGET SERVER
SRIVATSAN-TEMP.pmpod.com

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a database to store the Active Directory Federation Service configuration data.

● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

Database Host Name: [   ]

Database Instance: [   ]

To use the default instance, leave this field blank.

[< Previous] [Next >]   [Configure] [Cancel]

11:39 PM
11/21/2013

Active Directory Federation Services Configuration Wizard

Review Options

TARGET SERVER
SRIVATSAN-TEMP.pmpod.com

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'srivatsan-temp.csez.zohocorpin.com'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

Federation service will be configured to run as PMPOD\administrator.

These settings can be exported to a Windows PowerShell script to automate additional installations

[View script]

[< Previous] [Next >]   [Configure] [Cancel]

11:39 PM
11/21/2013

Active Directory Federation Services Configuration Wizard

Pre-requisite Checks

TARGET SERVER
SRIVATSAN-TEMP.pmpod.com

✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.   Show more ✕

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Rerun prerequisites check

▲ View results

ⓘ Prerequisites Check Completed
✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

< Previous   Next >   Configure   Cancel

11:40 PM
11/21/2013

Active Directory Federation Services Configuration Wizard

Results

TARGET SERVER
SRIVATSAN-TEMP.pmpod.com

✓ This server was successfully configured   Show more ✕

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

▲ View detailed operation results

Next steps required for completing your federation service deployment

< Previous   Next >   Close   Cancel

11:42 PM
11/21/2013

Running the Powershell Script

Powershell script for configuring AD FS 3.0 is:

https://sdpondemand.manageengine.com/html/adfsscript_2012_r2.ps1

1. Download the adfsscript.ps1 and save it in C:\ drive in the AD FS installation system
2. Open a "Command Prompt" ("Run as Administrator")
3. Type the following commands :
    - powershell
    - Set-ExecutionPolicy RemoteSigned
    - C:\adfsscript_2012_r2.ps1 <Your Verified Primary Domain Name>
4. Make sure the powershell script ran successfully. Any errors encountered while running the script will be printed in "red" color in the console.
5. If you are unable to set the execution policy to RemoteSigned because of domain policy, you might need to set the same policy in your Domain Controller.
    Refer here on how to set the execution policy in Domain controller.
    (http://www.techrepublic.com/blog/datacenter/set-the-powePrshell-executionpolicy-via-group-policy/3305)

Configure SAML in SDP On-Demand

1. Go to Admin page in SDP On-Demand
2. Configure Login url as : https://<AD FS Host Name>/adfs/ls
3. Logout url as : https://<AD FS Host Name>/adfs/ls/idpinitiatedsignon?SingleSignOut=SingleSignOut
4. Certificate will be saved as C:\certificate.cer. Browse and select it
5. Algorithm will be RSA
6. Save the settings

Logging out
    On Logout, you will not be redirected to the Login page again. Please close your browser when you finish your work with SDP On-Demand.