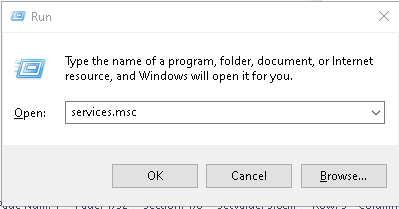
**Server best practices**

# Security patch update

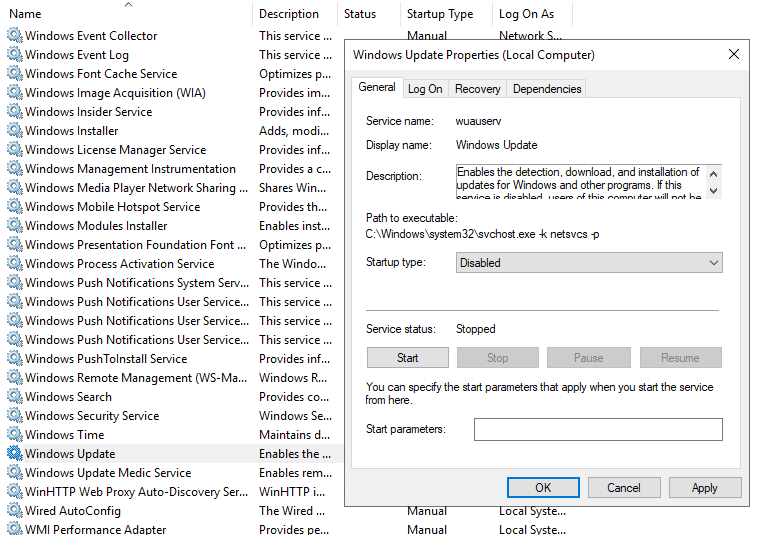
* Goto RUN and type **services.msc** press enter key.



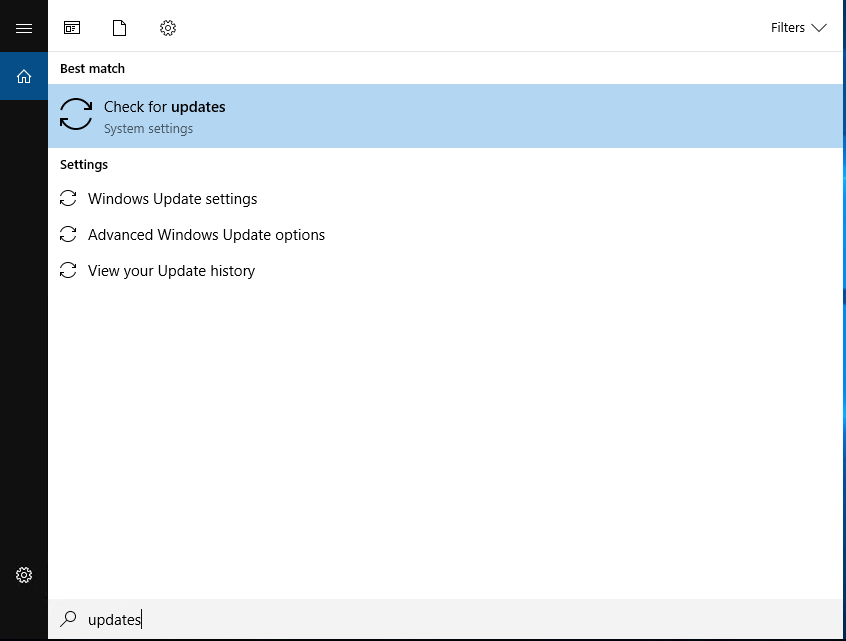
In services window, Enable the below services to automatic and start them.

1. Background Intelligent Transfer Service
2. Windows Installer
3. Windows Modules Installer
4. Windows Update

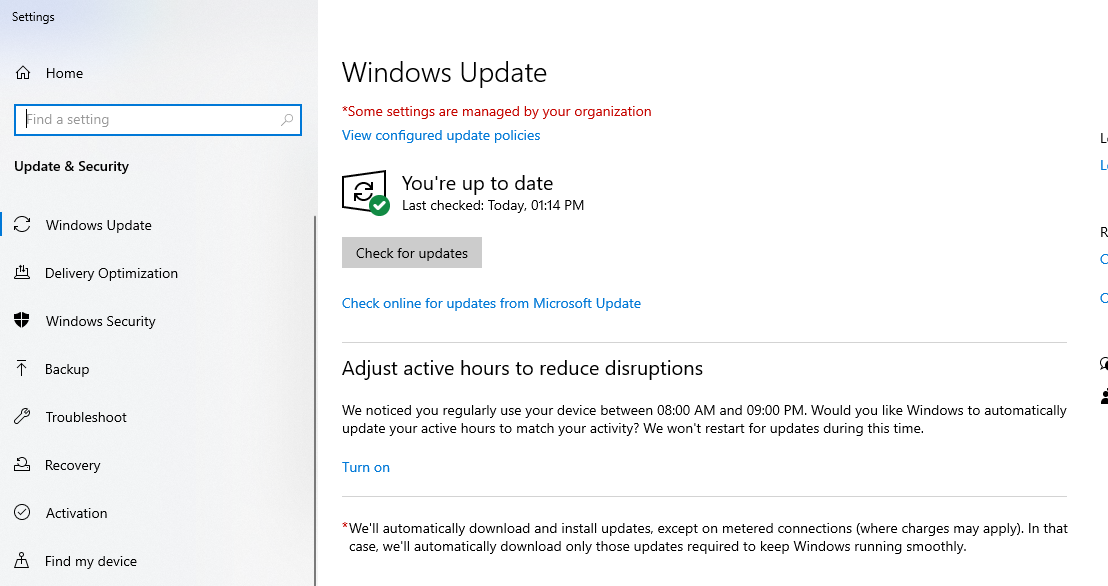
* To enable a service, Right click on the service, Goto properties and click on start-up type and select automatic and click on start.
* After starting a service, click apply and OK.



* After starting all the services, Goto search and type “**updates”**

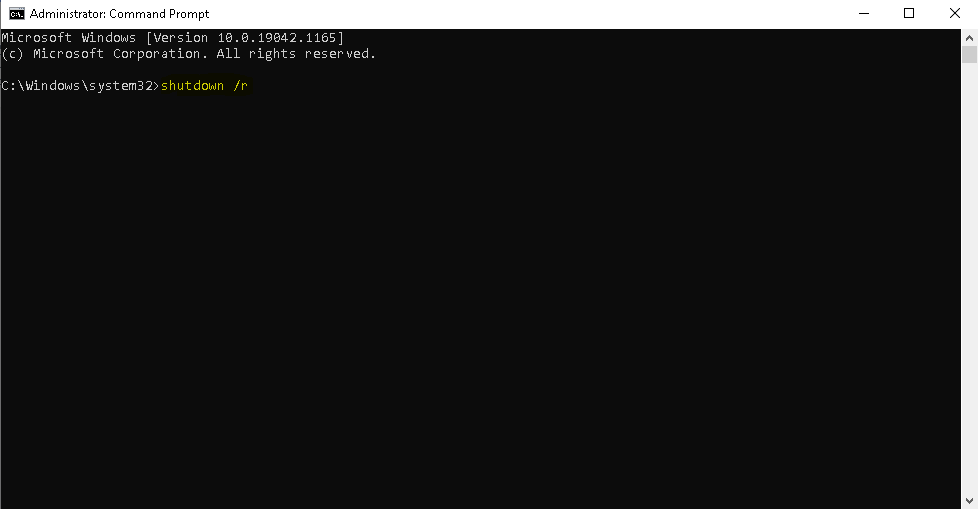


* Click on check for updates.



* If any updates are available, then download and install it.
* After installation, server should be restarted.
* To restart a server after installation, goto command prompt and type

‘**shutdown /r**” and press enter.



# Pre-requisite Installation Check

Please ensure that, the below mentioned Software are installed in the server before you start deployment:

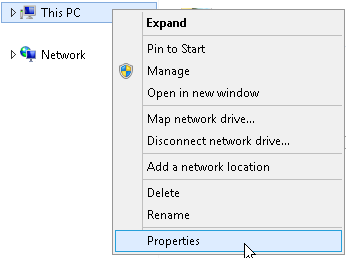
|  |  |  |
| --- | --- | --- |
| SL NO. | Software Name | Notes |
| 1. | SQL Server Installation | **Reporting Service should be Enabled** |
| 2. | Microsoft .Net Frameworks | **Versions 2.0, 3.0, 4.0 & 4.5 to be Installed** |
| 3. | ASP.NET MVC’s | **Versions 1.0, 2, 3, 4 to be Installed** |
| 4. | Microsoft Report Viewer Redistributable | **Versions 2005, 2008, 2010 to be installed** |
| 5. | Notepad ++ | **NA** |
| 6. | 7zip | **NA** |
| 7. | IIS (Internet Information Services) | **Make sure all the Components are Installed.** |

Please ensure the below mentioned items are available in the server to proceed with deployment:

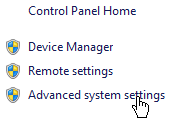
|  |  |  |
| --- | --- | --- |
| SL NO. | Server Specific Pre-requisite | Notes |
| 1. | DNS Name | Create DNS Name if Necessary.(DNS Name OR Public IP for Accessing Application Outside Network) |
| 2. | SSL (HTTPS) | Create SSL Certificate if Necessary |
| 3. | Configure SMTP Details | Configure SMTP Details if Necessary |
| 4. | LDAP Enabling | Enable the Ports, if LDAP is Required |
| 5. | Load Balancer | Configure Load Balancer if it is under Multiple App Servers |

# Setting Server to Adjust for Best Performance

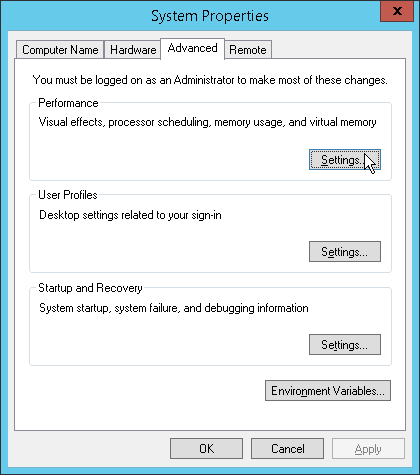
Follow the steps below to set server to adjust for the best performance:



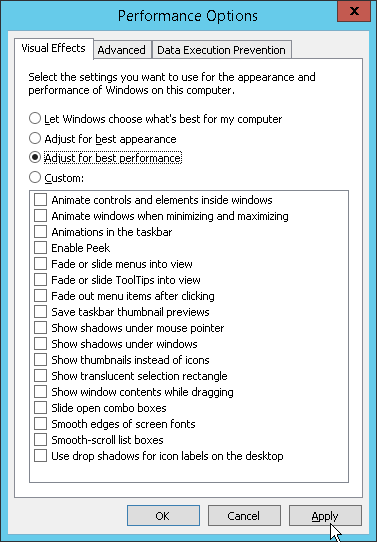
1. Go **My Computer** ->**Right** Click -> Select **Properties**.



1. On the **Properties** Window Navigate to **Advanced system settings**.



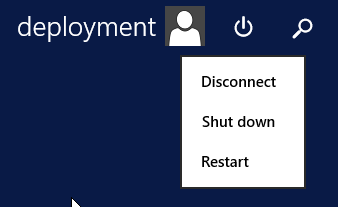
1. Click **Advanced** tab and click **Settings** Button on Performance section.



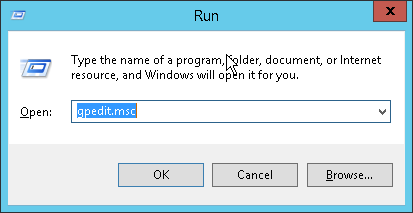
1. Select **Adjust to best performance** option.
2. After you complete, click **Apply**.

# Disabling Access to Shut-down / Restart Power Menu

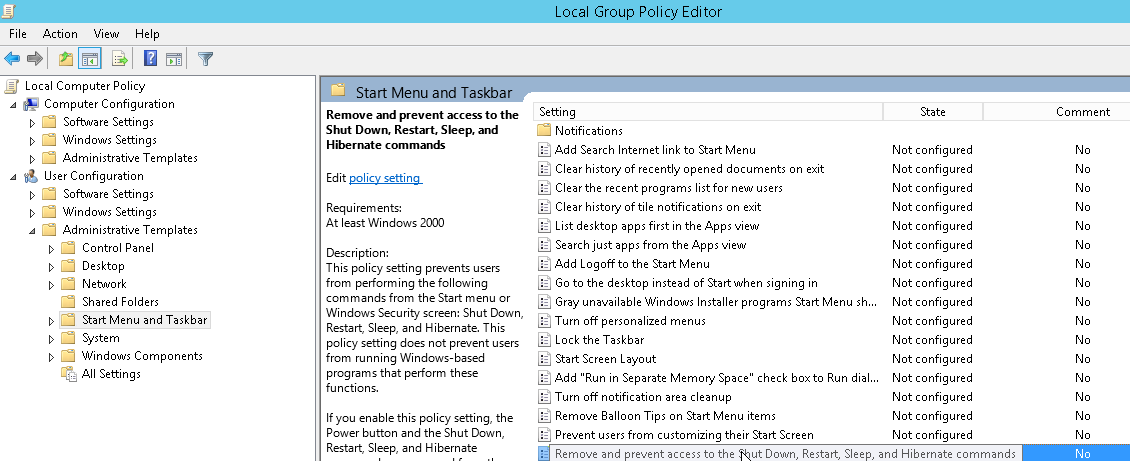
Follow the steps below to disable access to shut-down / restart power menu:



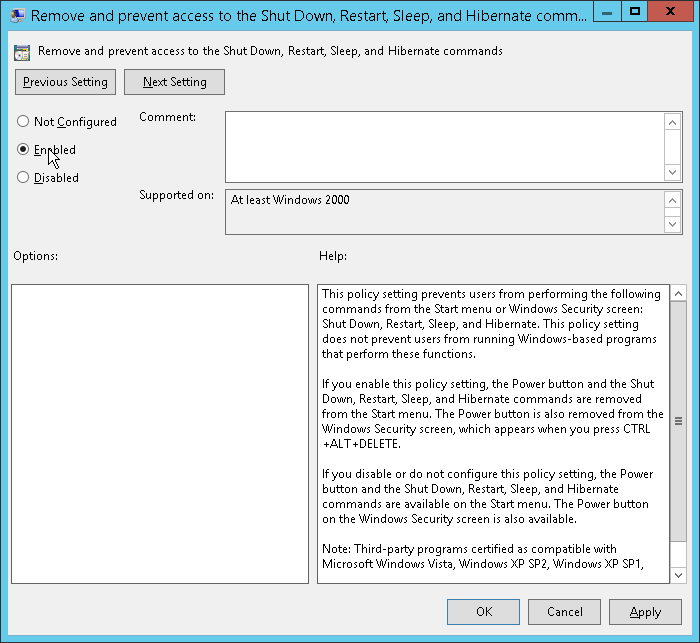
1. Click **Start Button** and Click **Power Menu** (We need to disable Shutdown & Restart Option).



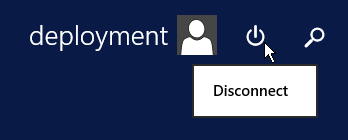
1. Click **Start** ->**Run** or “**Windows Button + R**” Type **gpedit.msc** (Group Policy Editor).



1. Under **User Configuration** Expand **Administrative Templates** -> Click on **Start Menu and Taskbar**.
2. On the **Right Pane** Select or Double-Click “**Remove and prevent access to the Shut Down, Restart, Sleep and Hibernate Commands**”.

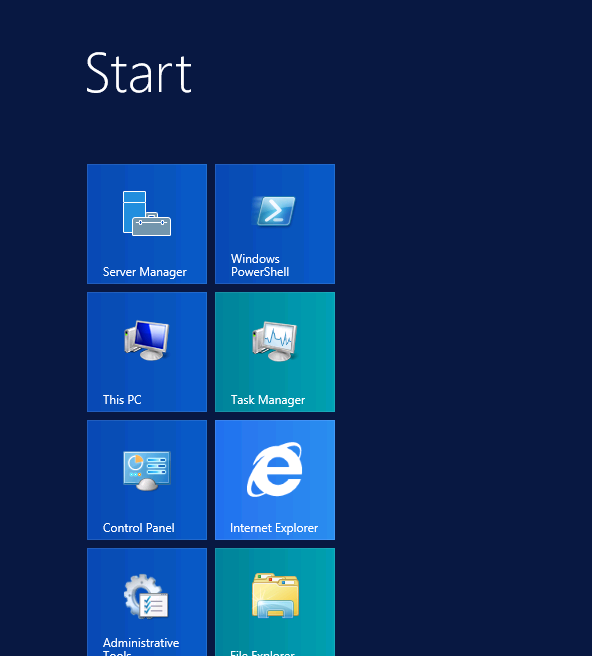


1. Select **Enabled** option to Disable shutdown & restart from Power Menu.

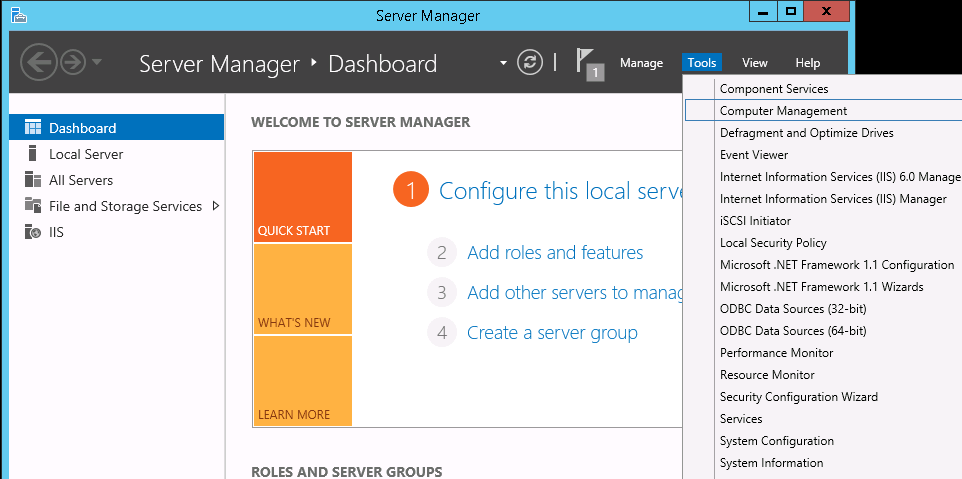


1. To verify, click **Start Button** and Click **Power Menu** (We have disabled Shutdown & Restart Option).

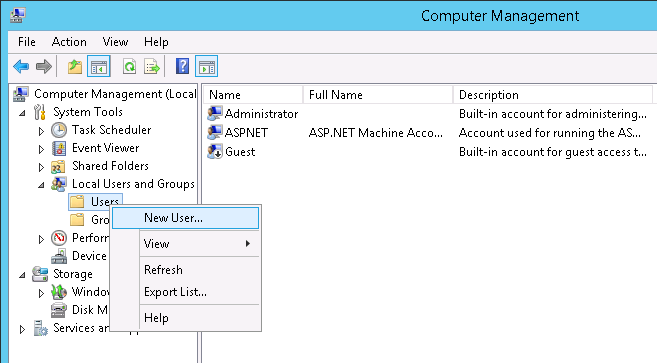
# Impersonate account creation



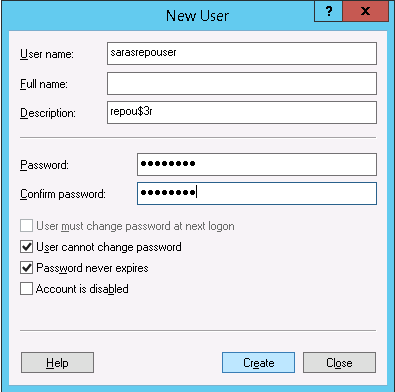
1. Goto Start and Click on Server Manager to Open the same.



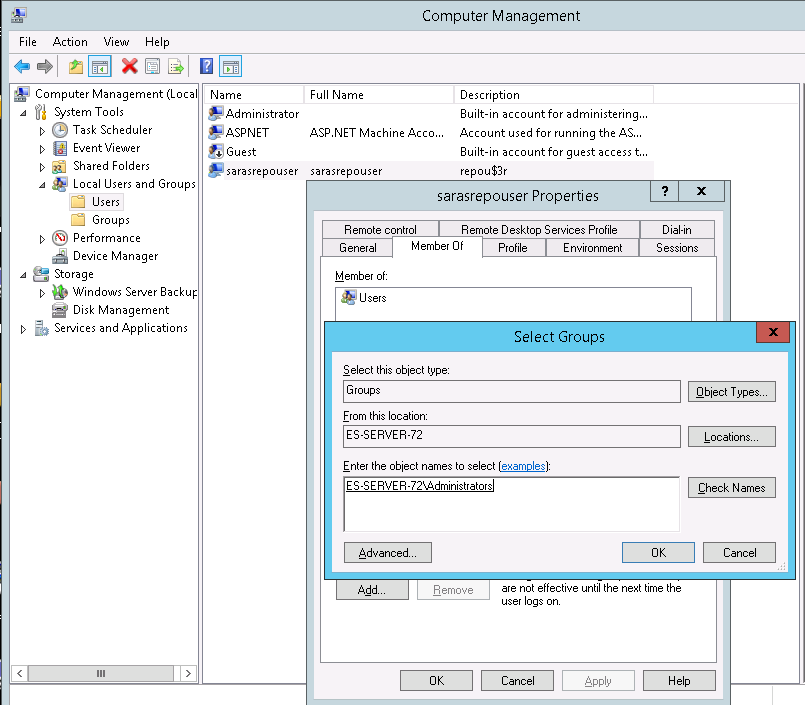
1. Go to **Computer Management.**



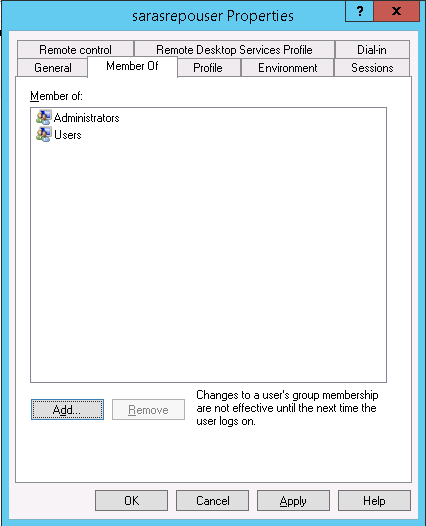
1. Expand Local Users and Groups -> Right Click on Users on left pane and click **New User** to create new Login Account.



1. Type the Credentials for below mentioned (**User Name & Password**) and select check boxes as mentioned below and Click on **OK.**



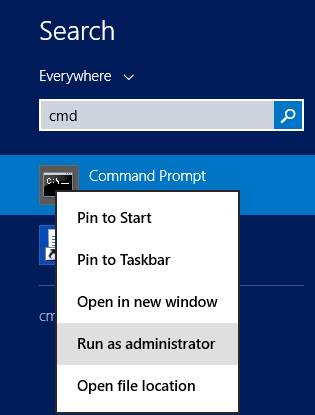
1. Right click on **SarasRepouser -> Goto Properties - > Goto Member of Tab ->** Type the word **‘Administrators’** and click **check Names ->** Click **OK.**



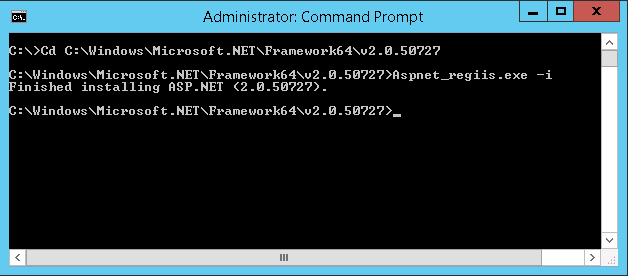
1. Click on **Apply** and **OK.**

**Note: Repeat the Step No. 5 (1, 2, 3, 4, 5, 6) to create the SarasRepousr Account in Database Server or in Repository Server Where the Repository Folder is Placed.**

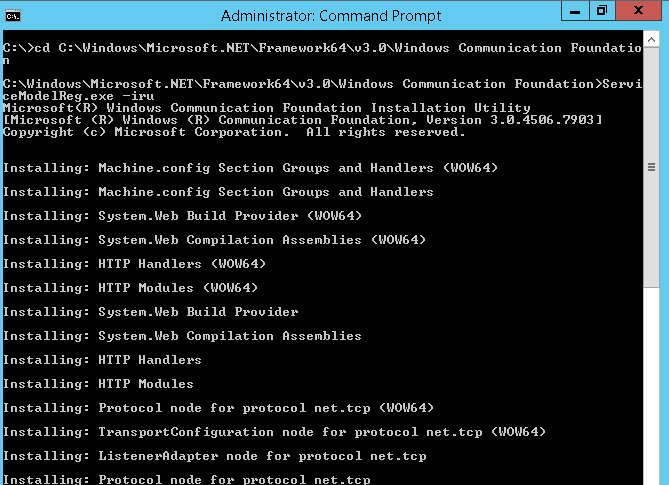
# Registering Dot Net Frameworks with IIS



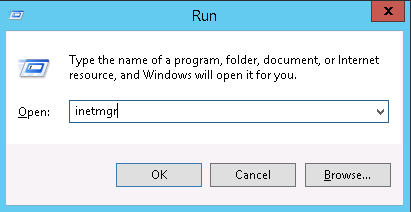
1. Goto ‘**Run’** or Search and type ‘**cmd’**(make sure this is opened with Run as Administrator) command as shown above and click **OK**.



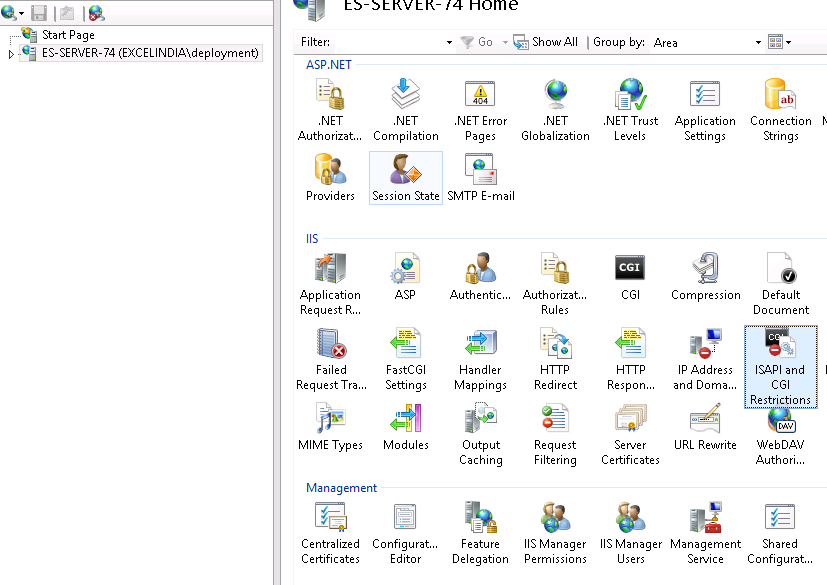
1. To Register 2.0 Framework with IIS, Type command (**Cd C:\Windows\Microsoft.NET\Framework64\v2.0.50727)**
2. Once the path is navigated type the command “**Aspnet\_regiis.exe -i”** and hit Enter, which should show the Finished installing message as above.



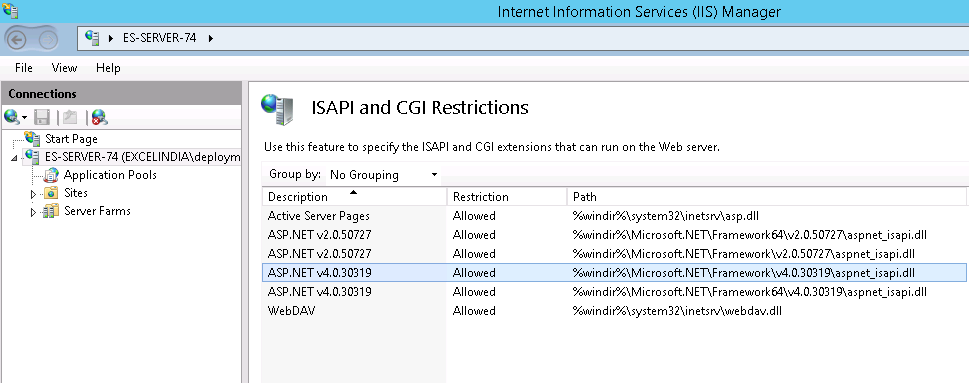
1. To Register 3.0 Communication Foundation framework with IIS Type Command (**Cd C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication Foundation)**
2. Once the path is navigated type the command “**ServiceModelReg.exe -iru”** and hit Enter, which should show the Finished installing message as above.



1. Goto ‘**Run**’ and type ‘**Inetmgr**’ command as shown above and click **OK**.



1. Click on server Name and double click on **ISAPI and CGI Restriction** on Right Pane.



1. Right-click and Select ‘**Allow’** option for both the ASP.NET version which are displaying as ‘**Not Allowed**’.

# Disabling Unsecure SSL/TLS on Registry

## Disable SSL 2.0 Protocols

Below is the set of steps to ensure SSL2.0 is disabled on the Server.

**Step 1 -** Disable SSL 2.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

1. Check if we already have client key, if yes ignore this step,
2. If no add key and Name it Client - Right Click on SSL 2.0 -> New -> Key and Name it Client
3. Right Click on SSL 2.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000001

1. Add key and Name it Server - Right Click on SSL 2.0 -> New -> Key and Name it Server
2. Right Click on SSL 2.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000

## Disable SSL 3.0 Protocols

Below is the set of steps to ensure SSL3.0 is disabled on the Server.

**Step 2 -** Disable SSL 3.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

1. Add key and Name it SSL 3.0 - Right Click on Protocols -> New -> Key and Name it SSL 3.0
2. Add key and Name it Client - Right Click on SSL 3.0 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on SSL 3.0 -> New -> Key and Name it Server
4. Right Click on SSL 3.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000001

1. Right Click on SSL 3.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

## Disable TLS 1.0 Protocols

Below is the set of steps to ensure TLS1.1 is disabled on the Server.

**Step 3 -** Disable TLS 1.0 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

1. Add key and Name it TLS 1.1 - Right Click on Protocols -> New -> Key and Name it TLS 1.0
2. Add key and Name it Client - Right Click on TLS 1.0 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.0 -> New -> Key and Name it Server
4. Right Click on TLS 1.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.0 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

1. Right Click on TLS 1.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.0 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

## Disable TLS 1.1 Protocols

Below is the set of steps to ensure TLS1.1 is disabled on the Server.

**Step 4 -** Disable TLS 1.1 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

1. Add key and Name it TLS 1.1 - Right Click on Protocols -> New -> Key and Name it TLS 1.1
2. Add key and Name it Client - Right Click on TLS 1.1 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.1 -> New -> Key and Name it Server
4. Right Click on TLS 1.1 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.1 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

1. Right Click on TLS 1.1 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

1. Right Click on TLS 1.1 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 1

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

## Enable TLS 1.2 Protocols

Below is the set of steps to ensure TLS1.2 is enabled on the Server.

**Step 5 -** Enable TLS 1.2 Protocols

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

1. Add key and Name it TLS 1.2 - Right Click on Protocols -> New -> Key and Name it TLS 1.2
2. Add key and Name it Client - Right Click on TLS 1.2 -> New -> Key and Name it Client
3. Add key and Name it Server - Right Click on TLS 1.2 -> New -> Key and Name it Server
4. Right Click on TLS 1.2 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 1

1. Right Click on TLS 1.2 -> Client -> Right Click on Client and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"Enabled"=dword:00000001

"DisabledByDefault"=dword:00000000

1. Right Click on TLS 1.2 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 1

1. Right Click on TLS 1.2 -> Server -> Right Click on Server and Select New -> DWORD (32-Bit) Value

Name: DisabledByDefault

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"Enabled"=dword:00000001

"DisabledByDefault"=dword:00000000

# Ciphers

## Key Exchange Algorithms

Below is the steps to Set Key Exchange Algorithms on the Server.

**Step 6 -** Disable Ciphers

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]

1. Add key and Name it Diffie-Hellman Right Click on KeyExchangeAlgorithms -> New -> Key and Name it Diffie-Hellman
2. Right Click on Diffie-Hellman and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

"Enabled"=dword: 00000000

## Disable TLS/SSL support for static key cipher suites

1. Right Click on KeyExchangeAlgorithms -> New -> Key and Name it PKCS

Right Click on PKCS and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

"Enabled"=dword: 00000000

## Disable RC4 Ciphers

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 128/128 Right Click on Ciphers -> New -> Key and Name it RC4 128/128

Right Click on RC4 128/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 40/128 Right Click on Ciphers -> New -> Key and Name it RC4 40/128

Right Click on RC4 40/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

1. Add key and Name it RC4 56/128 Right Click on Ciphers -> New -> Key and Name it RC4 56/128

Right Click on RC4 56/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

1. Navigate to the below mentioned Path in registry

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

Add key and Name it RC4 128/128 - Right Click on Ciphers -> New -> Key and Name it RC4 128/128

Right Click on RC4 128/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

1. Add key and Name it RC4 64/128 Right Click on Ciphers -> New -> Key and Name it RC4 64/128

Right Click on RC4 64/128 and Select New -> DWORD (32-Bit) Value

Name: Enabled

Value Data: 0

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]

"Enabled"=dword:00000000

## To Prevent Poodle Attack

Solution: Disable SSL3

## To Prevent BEAST Attack

## Solution: Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled.”

## To Prevent Birthday attacks on 64-bit block ciphers (SWEET32)

Solution: Disable TLS/SSL support for 3DES cipher suite

**Actual solution**: Add this registry key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168\Enabled (DWORD: 0)

## To Remove Weak Cipher Suites from TLS

**Solution 1:**

Step 1: Query the TLS Cipher Suites supported from the machine in Power Shell using below command

Command: Get-TlsCipherSuite | Format-Table Name

Step 2: Identify the Weak Cipher Suites name to remove and use the below command to remove the Cipher Suite.

**Example**: In below command we are just removing weak cipher suite “TLS\_RSA\_WITH\_RC4\_128\_SHA”

Similarly you can use other weak cipher suite **name** to remove in below command.

Command: Disable-TlsCipherSuite -Name “TLS\_RSA\_WITH\_RC4\_128\_SHA“

Step 3: Again query the TLS Cipher suites supported from machine using **Step 1 command** and check the weak cipher is removed from the results.

Step 4: Restart the server to apply the config changes.

**If Solution 1 not works then try Solution 2 to fix.**

**Solution 2:**

Steps 1: Download IISCrypto and install in machine where TLS need to be configured

Steps 2: Launch IISCrypto

Step 3: Click on **Cipher Suites icon** from left menu

Step 4: **Uncheck the checkbox** of the weak ciphers suites shown in window and click on apply button

Step 5: IISCrypto will show **reboot** **prompt** to apply changes and click on **OK** button.

Step 6: Again launch the IISCrypto, select the Cipher Suite menu and we can see that unchecked weak cipher suites are not shown in that window.

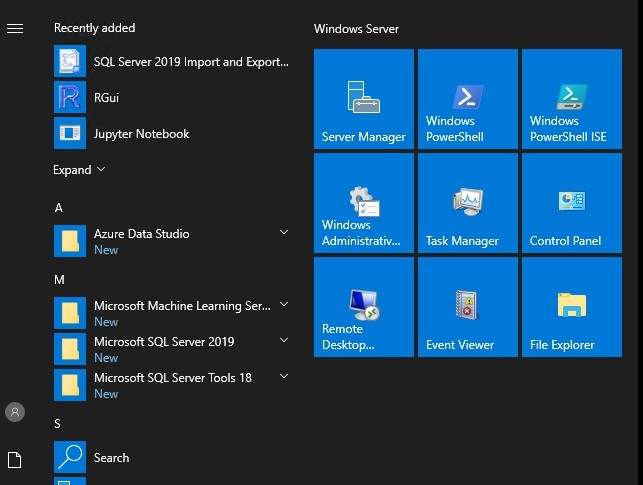
## Ensuring the Changes reflects on Server

**Step 7 -** Restart the Server

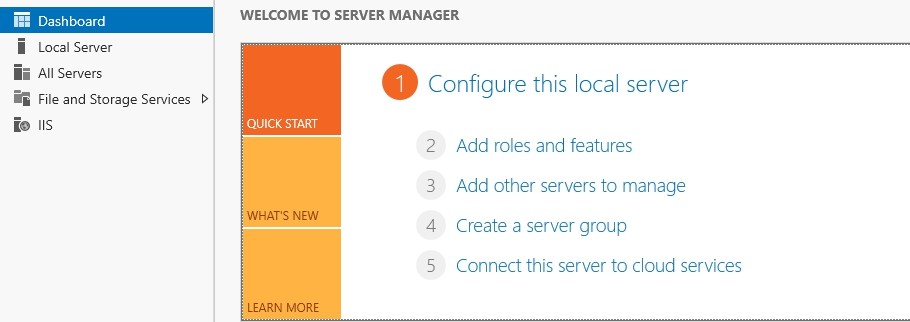
**IIS installation and best practices**

# IIS intallation

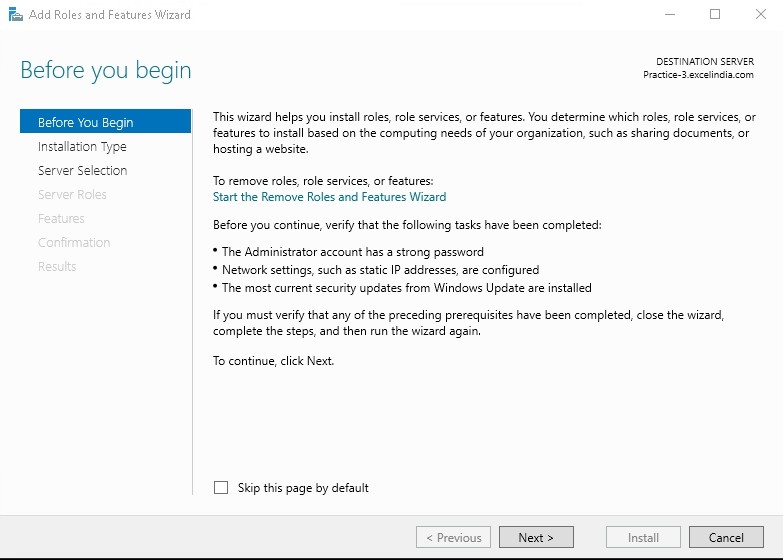
* Press the [Windows] key and select Server Manager.



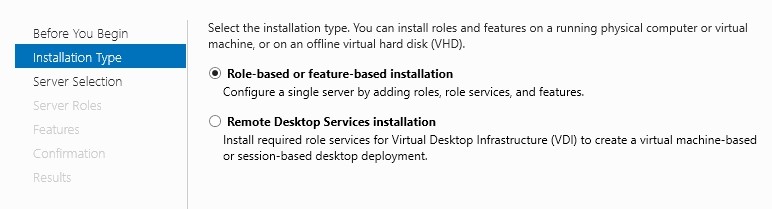
* In the Server Manager dashboard, click manage > add roles and features.



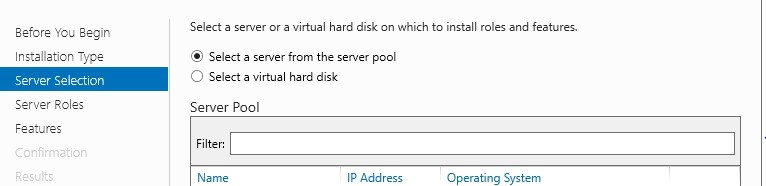
* Click installation type and click next.



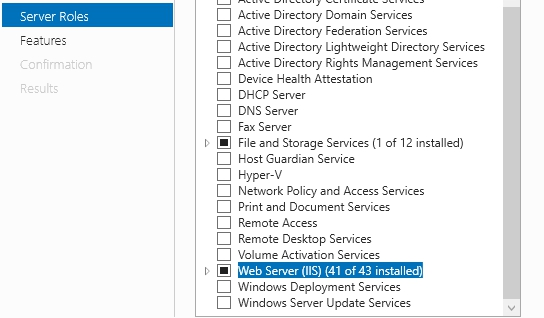
* Select the role-based or feature-based installation option and click Next.



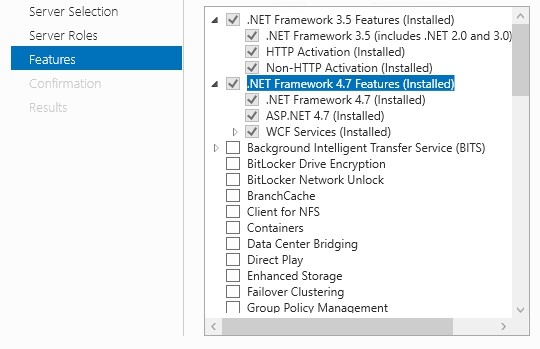
* Select the server on which IIS will be installed and click Next.



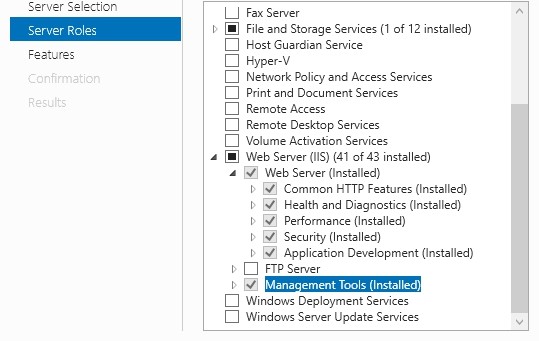
* Activate the Web Server (IIS) Role in server roles and click next.



* Select required features.

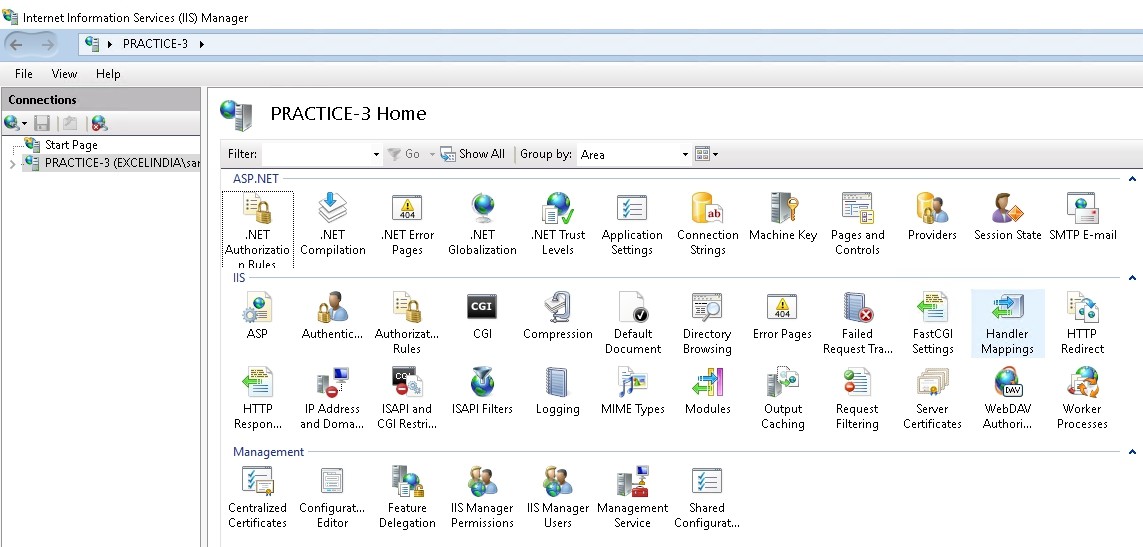


* Select required Web Server Role (IIS)

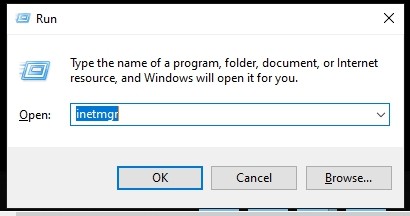


* Click Install to install the selected roles, role services and features.
* Click Close to complete the installation.

# IIS Logs File Settings



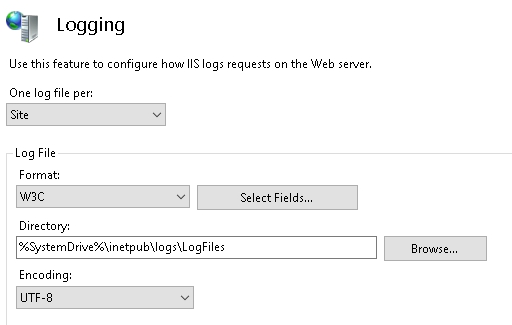
1. Click Start and select Run or “**Windows Button + R**” Type “**inetmgr**” (Internet Information Services Manager) and select ok.

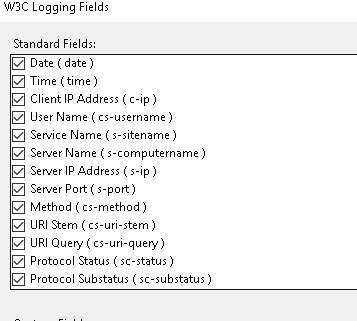


1. After launching the IIS Manger on the **Feature View** Select **Logging**

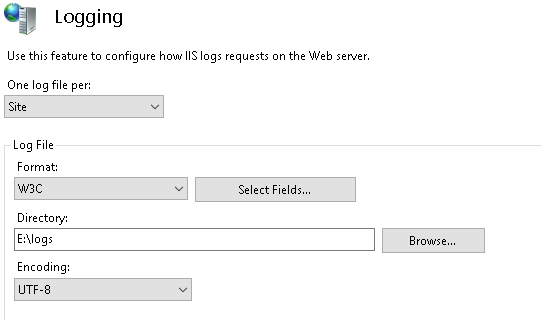
Option.

1. Click on Select fields and select all the Fields in the logging option.

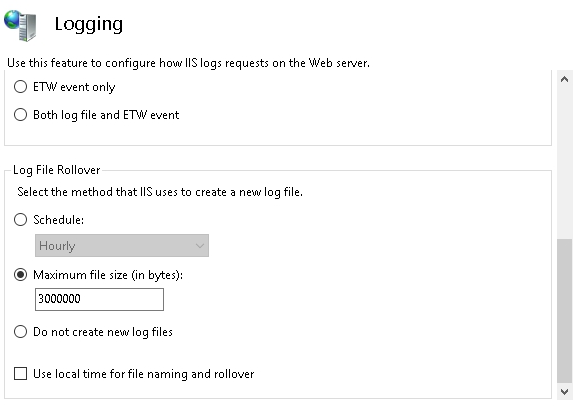




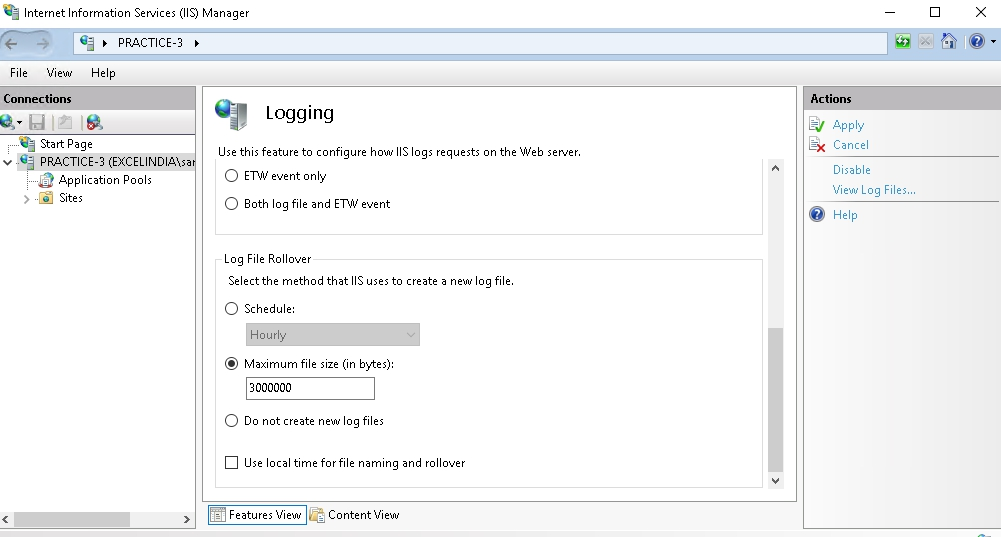
1. Change the IIS logs Directory to move to other drive.



1. Select **Maximum Files size** and Provide **Maximum Files size (in bytes)** 3MB - 3000000 in bytes.



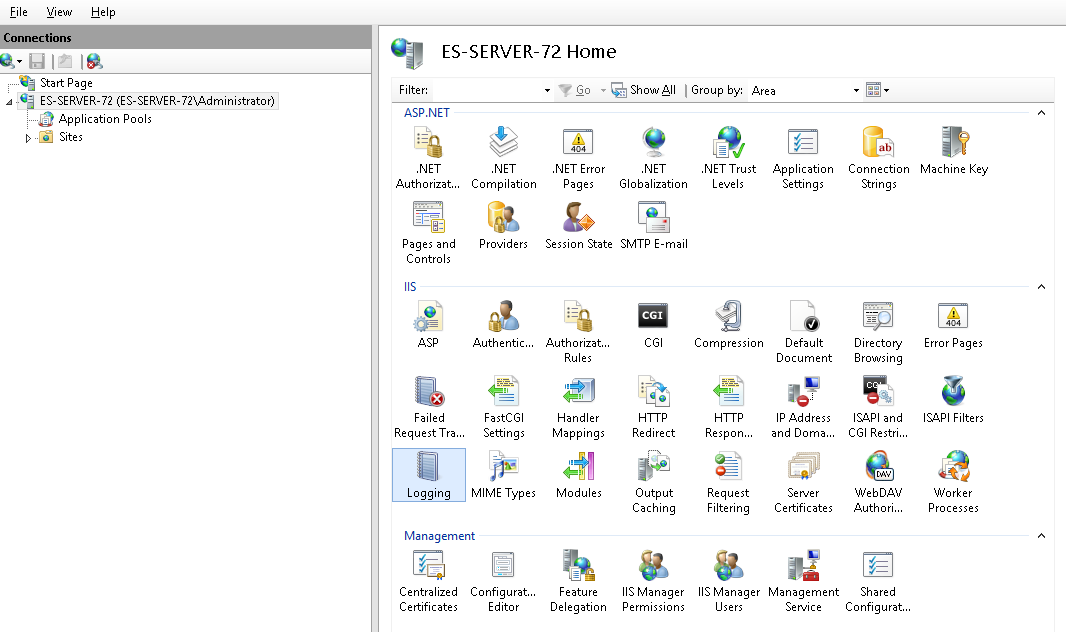
1. Click **Apply** button to save.



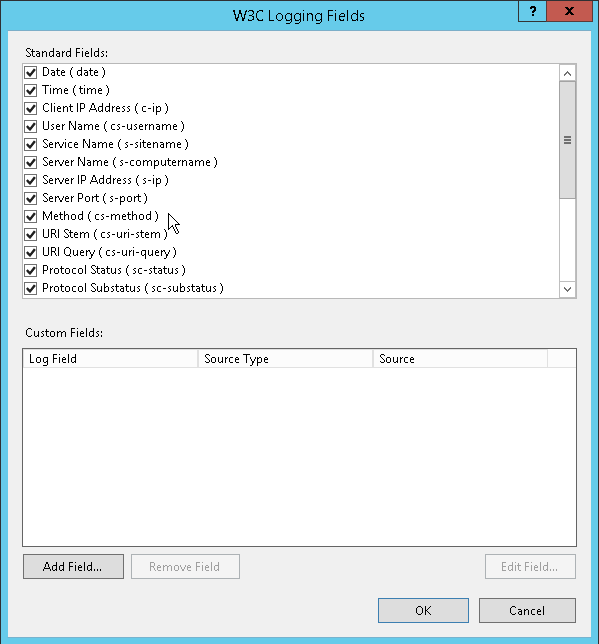
# IIS Logs File Settings

Follow the steps below to set IIS log files:

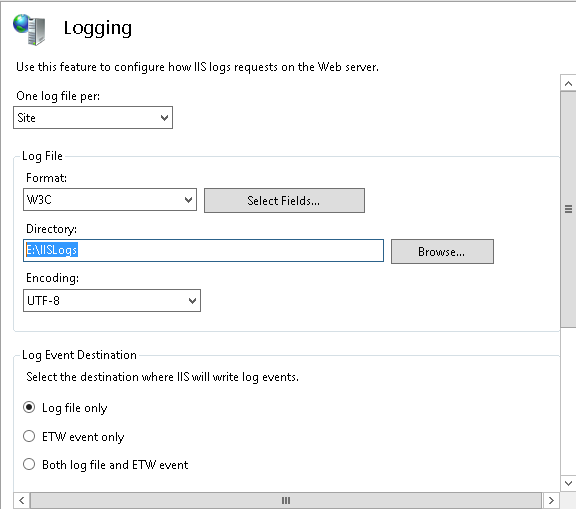
1. Click Start -> Run or “**Windows Button + R**” Type “**inetmgr”** (Internet Information Services Manager) and hit Enter.



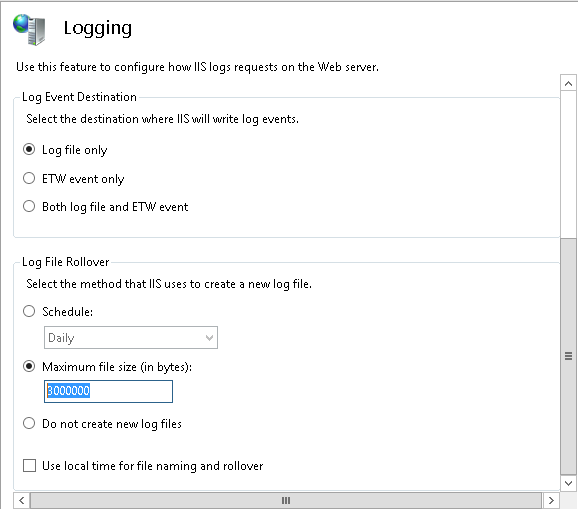
1. After launching the IIS Manger on the **Feature View** Select **Logging** Option.



1. **Select all the Fields** in the logging option.



1. Change the **IISLogs Directory** to move to other drive.

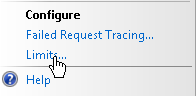


1. Select **Maximum Files size** and Provide **Maximum Files size (in bytes)** 3MB - 3000000 in bytes.
2. Scroll down to view Apply button Click **Apply** button to complete.

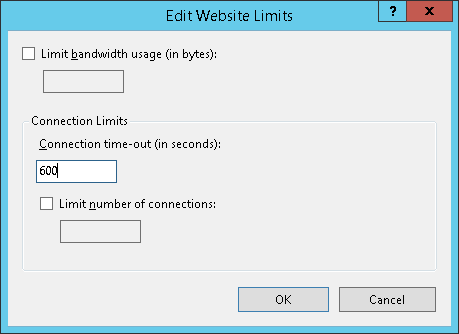
# IIS Limits Setting

Follow the steps below to set IIS limits:

1. Click Start -> Run or “**Windows Button + R**” Type “**inetmgr”** (Internet Information Services Manager).



1. After launching the IIS Manger **Navigate** to **Default Web Site** on the Feature View **Select Limits** Option on Right pane.



1. In Connection Limits **change** the value from “**120**” to “**600**”.
2. Click **OK** to complete.