

Inhoudsopgave

Inhoudsopgave	1
System Center 2012 R2 Configuration Manager System Requirements	3
Installing Prerequisites for Configuration Manager 2012 R2	10
Installing SQL Server for System Center 2012 R2 Configuration Manager	32
Installing WSUS for Configuration Manager 2012 R2	46
Configuring Firewall Settings for Configuration Manager 2012 R2	54
Installing System Center 2012 R2 Configuration Manager	75
Installing Configuration Manager 2012 R2 Hotfixes	93
Configuring Discovery and Boundaries in Configuration Manager 2012 R2	113
Installing Site System Roles in Configuration Manager 2012 R2	124
Configuring Client Settings in Configuration Manager 2012 R2	137
Configuration Manager 2012 R2 Client Installation	148
Boot Images and Distribution Point Configuration For OSD In SCCM 2012 R2	161
Deploying Configuration Manager 2012 R2 Clients Using Group Policy	169
Capture Windows 7 Image Using SCCM 2012 R2	180
Deploying Windows 7 Using SCCM 2012 R2	193
How To Deploy Microsoft Office 2013 Using SCCM 2012 R2	221
System Center 2012 R2 Configuration Manager Toolkit	241
How To Deploy Software Updates Using SCCM 2012 R2	253
Installing And Configuring Endpoint Protection Role In SCCM 2012 R2	277
Managing Linux Computers Using System Center 2012 R2 Configuration Manager	307
How To Deploy Lync 2010 Client Using SCCM 2012 R2	323
Deploying Applications To Users Using SCCM 2012 R2	348
Deploying Endpoint Protection Updates Offline Using SCCM 2012 R2	364
How to Simulate an Application Deployment in SCCM 2012 R2	379
Deploying Adobe Reader Updates Using SCCM 2012 R2	385
Deploy .NET Framework 4.0 using SCCM 2012 R2	396
How To Backup SCCM 2012 R2 Server	407
SCCM 2012 Support Center Tool	416
How to Uninstall SCEP Client using SCCM 2012 R2	440
How to Setup Distribution Point in SCCM 2012 R2	452
How to increase SCCM client cache size	464
Create Automatic Deployment Rule in SCCM 2012 R2	470
Deploying Windows 7 Using MDT UDI	488

Import VMware drivers to your SCCM boot image	514
How to Deploy Office 2016 Using SCCM 2012 R2.....	523
How to Deploy Fonts Using SCCM 2012 R2.....	534
PKI requirements for SCCM 2012 R2.....	544
Deploying Web Server Certificate for Site Systems that Run IIS	547
Deploying the Client Certificate for Windows Computers	563
Deploying the Client Certificate for Distribution Points.....	571
PART 42	594

[System Center 2012 R2 Configuration Manager System Requirements](#)

Welcome to System Center 2012 R2 Configuration Manager deployment, I would like to start System Center 2012 R2 Configuration Manager deployment series with a little information about its basics and then we will look into its new features and design considerations. System Center 2012 R2 delivers unified management across on-premises, service provider and Windows Azure environments, in a manner that's simple and cost-effective, application focused, and enterprise-class. System Center 2012 R2 offers exciting new features and enhancements across infrastructure provisioning, infrastructure monitoring, application performance monitoring, automation & self-service, and IT service management. The Microsoft names it as Cloud OS, System Center enables the Microsoft Cloud OS by delivering unified management across on-premises, service provider, and Windows Azure environments. To know more on System Center 2012 R2 you can click [here](#).

With every deployment series of Configuration Manager I always want to put the information that is short, precise and that can be understood easily. In my upcoming posts I will also try to answer to few of the commonly asked questions in the [Technet Forum](#) related to System Center 2012 R2 Configuration Manager and discuss more on the troubleshooting part. We will first begin with the new features introduced in System Center 2012 R2 Configuration Manager, there are lot of new features added but we will see only the important ones here.



What's New In System Center 2012 R2 Configuration Manager

- 1) System Center 2012 R2 Configuration Manager now supports deployment of Windows 8.1 and Windows server 2012 R2. There is added support for boot images created by using the Windows Automated Installation Kit (Windows AIK) for Windows 7 SP1 and based on Windows PE 3.1.
- 2) System Center 2012 R2 Configuration Manager is now integrated with Windows Intune and this is named as **Unified Modern Device Management**. This means you can use System Center 2012 R2 Configuration Manager together with Windows Intune to manage a broad array of PCs and devices covering Windows, Windows RT, Macs, Windows Phone, Apple iOS and Android.
- 3) You can now select Resultant Client Settings (RSOP) from the Configuration Manager console to view the effective client settings that will be applied to the selected device. This is another great feature.
- 4) You can now reassign Configuration Manager clients, including managed mobile devices, to another primary site in the hierarchy. Clients can be reassigned individually or can be multi-selected and reassigned in bulk to a new site.
- 5) Compliance Settings – New mobile device settings and mobile device setting groups have been added.
- 6) Profiles – There are new Certificate Profiles, VPN Profiles and Wi-Fi Profiles introduced in System Center 2012 R2 Configuration Manager and the supported devices include those that run iOS, Windows 8.1 and Windows RT 8.1, and Android.
- 7) Software Updates – There is a new maintenance window dedicated for software updates installation. This lets you configure a general maintenance window and a different maintenance window for software updates. You can now change the deployment package for an existing automatic deployment rule. New software updates are added to the specified deployment package every time an automatic deployment rule is run. A new feature called **Software updates preview** lets you review the software updates before you create the deployment.
- 8) Application Management – Web applications in System Center 2012 R2 Configuration Manager are a new deployment type that allows you to deploy a shortcut to a web-based app on users devices.
- 9) Collections – A new management option allows you to configure maintenance windows to apply to task sequences only, software updates only, or to all deployments.
- 10) Reporting – Configuration Manager reports are now fully enabled for role-based administration. The data for all reports included with Configuration Manager is filtered based on the permissions of the administrative user who runs the report. Administrative users with specific roles can only view information defined for their roles.

System Center 2012 R2 Configuration Manager Design Considerations

Before we install the System Center 2012 R2 Configuration Manager it would be better to have an idea on System Center 2012 R2 Configuration Manager Site and System Roles and how are we going to install the roles and their limits. In most of the cases planning for hardware and software requirements for Configuration manager takes more time, so it is very important to understand about the site and system role scalability.

- 1) **Central Administration Site** – A central administration site can support up to 25 child primary sites. When you install a Central Administration Site and use an Enterprise or Datacenter edition of SQL Server, the hierarchy can support a combined total of up to 400,000 devices. So you must plan for CAS only when an organization has over 1,00,000 clients.
- 2) **Primary Site** – Each primary site can support up to 250 secondary sites and up to 1,00,000 clients.
- 3) **Secondary Site** – A secondary site supports a maximum of 5,000 clients. For secondary sites SQL Server must be installed on the site server computer and in a location if there are fewer than 500 clients, consider a distribution point instead of a secondary site.
- 4) **Management Point** – Each primary site supports up to 10 management points and each primary site management point can support up to 25,000 computer clients. Each secondary site supports a single management point which must be installed on the site server computer.
- 5) **Distribution Point** – With System Center 2012 R2 Configuration Manager each primary and secondary site supports up to 250 distribution points and each distribution point supports connections from up to 4,000 clients. Each primary site supports a combined total of up to 5,000 distribution points. This total includes all the distribution points at the primary site and all distribution points that belong to the primary site's child secondary sites. Each primary and secondary site supports up to 2000 additional distribution points configured as pull-distribution points. For example, a single primary site supports 2250 distribution points when 2000 of those distribution points are configured as pull-distribution points.
- 6) **Software Update Point** – A software update point that is installed on the site server can support up to 25,000 clients.
- 7) **Fallback status point** – Each fallback status point can support up to 100,000 clients.

Upgrade Paths For Configuration Manager

If you are planning to upgrade your existing Configuration Manager version to Configuration Manager 2012 R2 version then here is the information about it.

- 1) **Upgrading from Configuration Manager 2012 Prerelease Version** – If you have installed a prerelease version of System Center 2012 R2 Configuration Manager, uninstall the prerelease version before you install System Center 2012 R2 Configuration Manager. We recommend that you also uninstall and reinstall the operating system after you uninstall earlier versions of System Center 2012 R2 Configuration Manager and before you install the release version of System Center 2012 R2 Configuration Manager.
- 2) **Upgrading from Configuration Manager 2012 (without service pack or with SP1)** – If you have a release version of System Center 2012 Configuration Manager SP1, you can upgrade this to System Center 2012 R2 Configuration Manager. You do not have to be on the latest cumulative update to upgrade from System Center 2012 Configuration Manager SP1. If you are on System Center 2012 Configuration Manager with no service pack and want to upgrade to System Center 2012 R2 Configuration Manager, you must first upgrade to System Center 2012 Configuration Manager SP1 before you can upgrade to System Center 2012 R2 Configuration Manager.
- 3) **Upgrading from Configuration Manager 2007** -System Center 2012 R2 Configuration Manager does not support an in-place upgrade from Configuration Manager 2007, but does support a side-by-side installation of both products in the same environment.In such scenarios you can use System Center 2012 R2 Configuration Manager to create migration jobs that migrate objects and content from Configuration Manager 2007 to System Center 2012 R2 Configuration Manager.

System Center 2012 R2 Configuration Manager System Requirements

Now we will look at the system requirements for deploying System Center 2012 R2 Configuration Manager. If you have installed a prerelease version of System Center 2012 R2 Configuration Manager then uninstall the prerelease version before you install System Center 2012 R2 Configuration Manager. Microsoft recommends that you also uninstall and reinstall the operating system after you uninstall earlier versions of System Center 2012 R2 Configuration Manager and before you install the release version of System Center 2012 R2 Configuration Manager. This is to avoid errors that may occur due to change in versions of Configuration Manager. Here we will be looking at the system requirements for fresh install of System Center 2012 R2 Configuration Manager, there will be a separate post on upgrading System Center 2012 Configuration Manager SP1 to System Center 2012 R2 Configuration Manager.

Hardware Requirements For Site Systems :-

Please make sure you have the required hardware before installing System Center 2012 R2 Configuration Manager.

Processor – AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support. The minimum processor speed expected is 1.4 GHz.

RAM – A minimum of 2 GB RAM is required.

Disk Space – A minimum of 50 GB hard disk space is a must.

Operating System Support

The following table shows the operating systems that can support System Center 2012 Configuration Manager site servers, the database server, and the SMS Provider site system role.

SQL Server Support

Before you install the SQL server please go through this chart once, most of the times if the correct service pack or cumulative update is not installed then there are chances that you might encounter installation errors. Configuration Manager requires a 64-bit version of SQL Server to host the site database and site database must use the following collation **SQL_Latin1_General_CI_AS**. Microsoft recommends to reserve a minimum of 8GB of memory in the buffer pool used by an instance of SQL Server for the central administration site and primary site and a minimum of 4GB for the secondary site. We will discuss more on this while installing the SQL server for System Center 2012 R2 Configuration Manager.

Operating System Support Configuration Manager 2012 R2 Client Installation

The System Center 2012 R2 Configuration Manager clients can be installed on following Operating Systems :-

- 1) Windows XP Professional SP3 (x86), Windows XP Professional for 64-bit Systems (SP2).
- 2) Windows XP Tablet PC (SP3) (x86).
- 3) Windows Vista Business Edition (SP2), Enterprise Edition (SP2), Ultimate Edition (SP2) – (x86 and x64).
- 4) Windows 7 Professional (with no service pack, or with SP1), Enterprise Editions (with no service pack, or with SP1), Ultimate Editions (with no service pack, or with SP1) – (x86 and x64).
- 5) Windows 8, 8.1 Pro and Enterprise – (x86 and x64).

- 6) Windows Server 2003, Windows Server 2003 R2 SP2 Standard Edition (SP2), Enterprise Edition (SP2), Datacenter Edition1 (SP2) – (x86 and x64).
- 7) Windows Storage Server 2003 R2 SP2 – (x86 and x64).
- 8) Windows Server 2008 Standard Edition (SP2), Enterprise Edition (SP2), Datacenter Edition (SP2) – (x86 and x64).
- 9) Windows Storage Server 2008 R2 Workgroup, Standard, Enterprise – (x64).
- 10) Windows Server 2008 R2 Standard Edition (with no service pack, or with SP1), Enterprise Edition (with no service pack, or with SP1),Datacenter Edition (with no service pack, or with SP1) – (x64)
- 11) Windows Server 2008 (SP2) Server Core,Windows Server 2008 R2 Server Core(no service pack, or with SP1),Windows Server 2012 R2 Server Core,Windows Server 2012 R2 Server Core – (x64).
- 12) Windows Server 2012 Standard and Datacenter, Windows Server 2012 R2 Standard and Datacenter – (x64).
- 13) Red Hat Enterprise Linux – Version 4 x86,Version 4 x64,Version 5 x86,Version 5 x64,Version 6 x86,Version 6 x64.
- 14) CentOS – Version 5 x86,Version 5 x64,Version 6 x86,Version 6 x64.
- 15) Mac OS X 10.6 (Snow Leopard), Mac OS X 10.7 (Lion), Mac OS X 10.8 (Mountain Lion).

Active Directory Domains Support

Following are the Windows Active directory domain functional level that are supported by System Center 2012 R2 Configuration Manager. Please note that Configuration Manager does not support the change of domain membership, domain name, or computer name of a Configuration Manager site system after the site system is installed.

Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.

Operating System Support For Installing System Center 2012 R2 Configuration Manager Console

Here is the list of operating systems that are supported to run the Configuration Manager console, each of the operating system must have minimum version of Microsoft .NET Framework installed on them.

- 1) Windows XP Professional (SP3), Windows Vista Business Edition (SP2), Enterprise Edition (SP2), Ultimate Edition (SP2) – (x86 and x64) with minimum .NET Framework 4.

- 2) Windows 7 Professional, Enterprise, Ultimate – (with no service pack, or with SP1) – (x86 and x64) with minimum .NET Framework 4.
- 3) Windows 8, 8.1 Pro and Enterprise – (x86 and x64) with minimum .NET Framework 4.5
- 4) Windows Server 2008 Standard Edition (SP2),Enterprise Edition (SP2),Datacenter Edition (SP2) – (x86 and x64) with minimum .NET Framework 4.
- 5) Windows Server 2008 R2 Standard Edition, Enterprise Edition, Datacenter Edition (with no service pack, or with SP1) – (x64) with minimum .NET Framework 4.
- 6) Windows Server 2012, 2012 R2 (Standard Edition and Datacenter Edition) – (x64) with minimum .NET Framework 4.5.

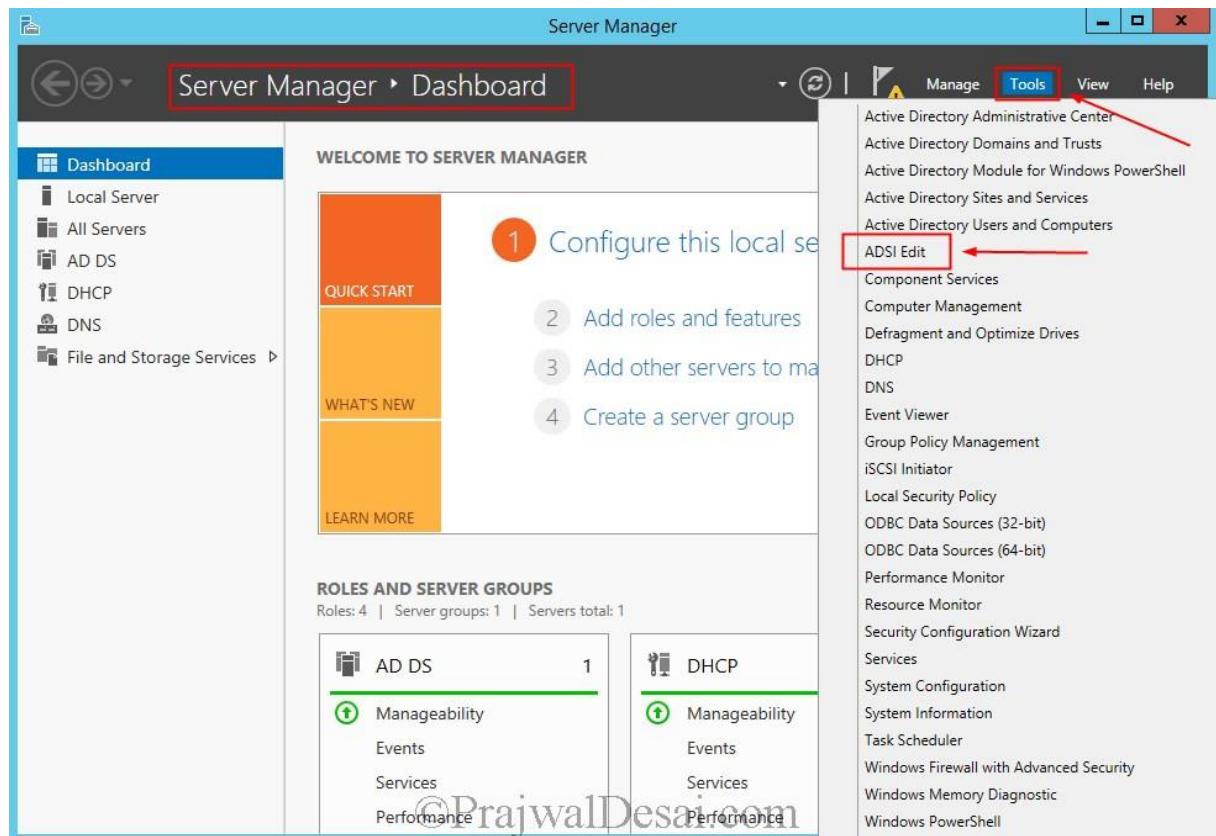
[Installing Prerequisites for Configuration Manager 2012 R2](#)

Installing Prerequisites for Configuration Manager 2012 R2 In this post we will see the steps for Installing Prerequisites for Configuration Manager 2012 R2 and we will also see the steps to create a system container, assign permissions for SCCM server on the container and extend the active directory schema. In my previous post I talked about the new features of [system center 2012 R2 configuration manager](#) and the system requirements for installing configuration manager 2012 R2. Before you can install Configuration Manager you should extend your Active Directory and give your SCCM server rights to create objects under the system container in AD.

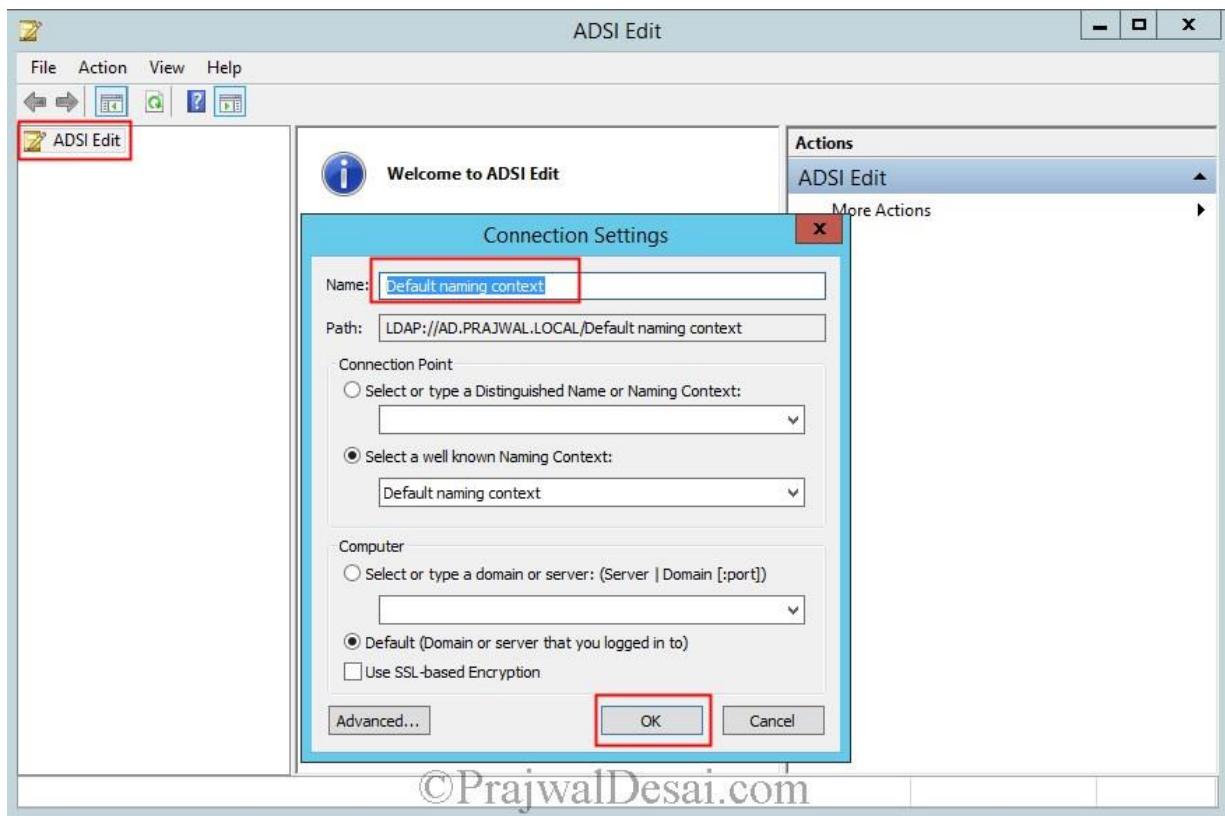
Does Configuration Manager creates System Container automatically ? – Configuration Manager does not automatically create the System Management container in Active Directory Domain Services when the schema is extended. The container must be created one time for each domain that includes a Configuration Manager primary site server or secondary site server that publishes site information to Active Directory Domain Services.

Creating the System Management Container

We will first create the system management container and we will assign the SCCM server permissions to create objects under the system container. The domain controller is running on windows server 2012 R2 Datacenter edition operating system. To create a container log on to the Domain controller with administrator account, click on **Server Manager**, **Tools**, click on **ADSI Edit**.

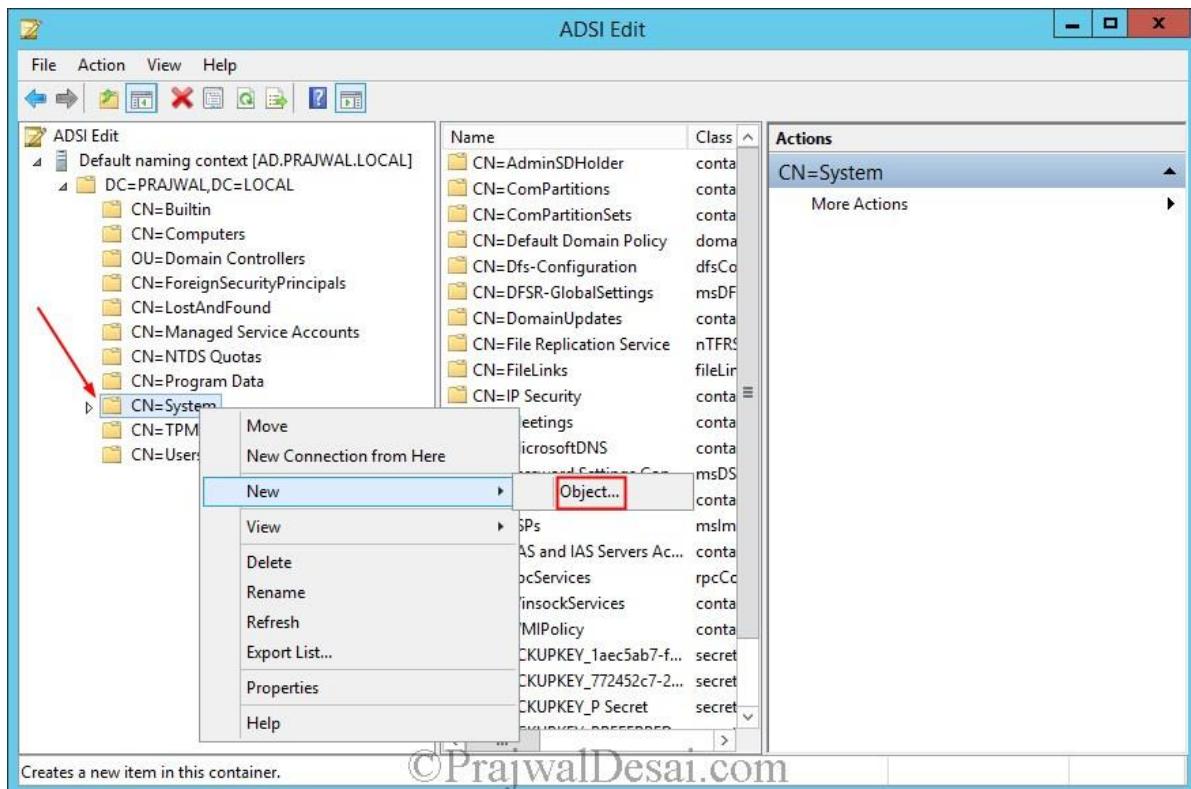


Right click **ADSI Edit** and click on **Connect to**. On the **Connection Settings** window, the naming context should be **Default naming context**. Do not change anything here, click on **OK**.

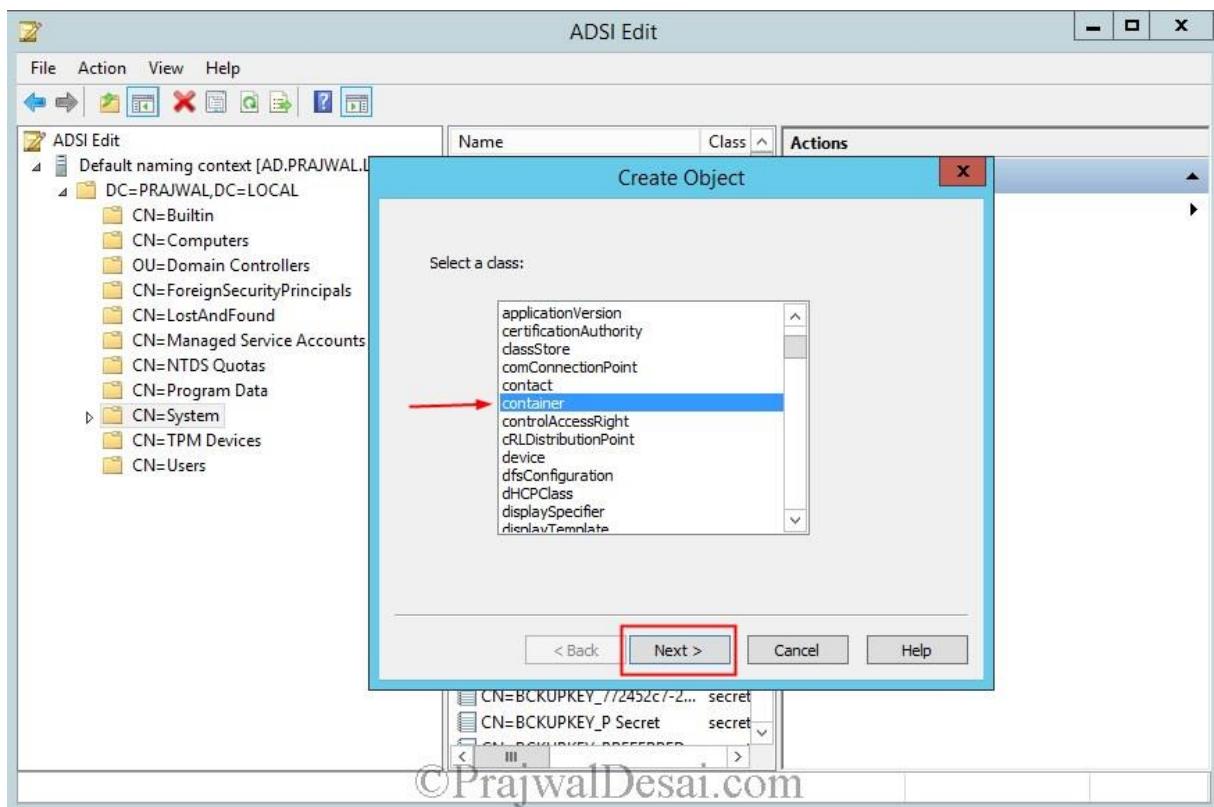


©PrajwalDesai.com

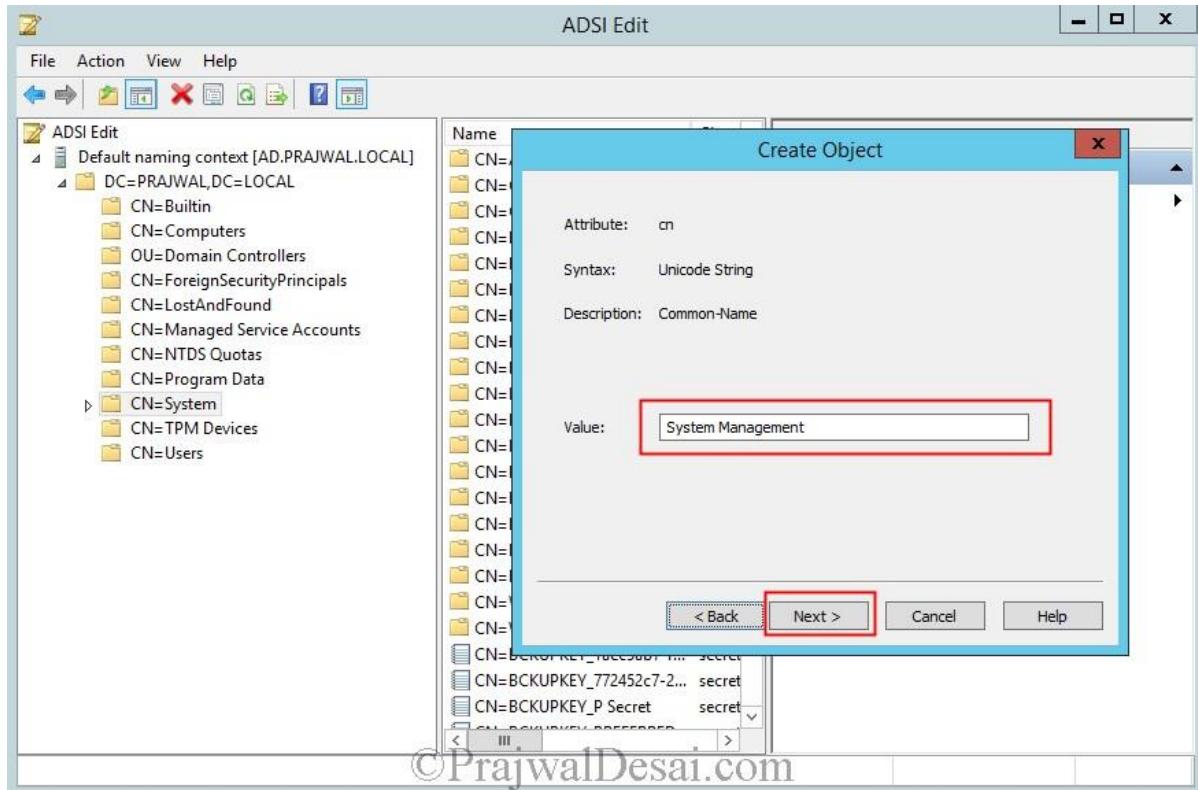
In the **ADSI Edit** Console, expand the **Default Naming Context**, right click **CN=System**, click on **New** and create an **Object**.



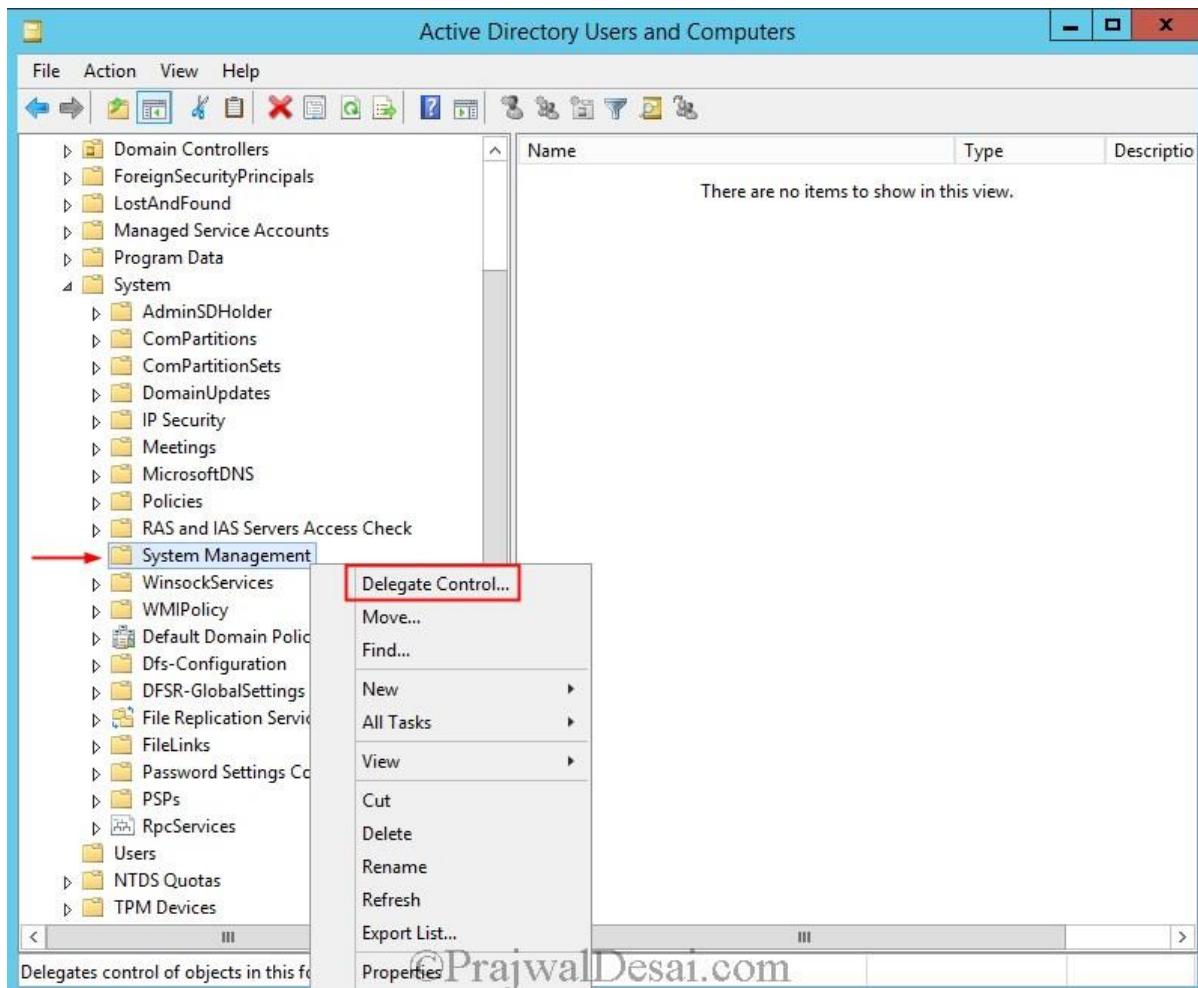
On the **Create Object** windows, select the class as **container** and click on **Next**.



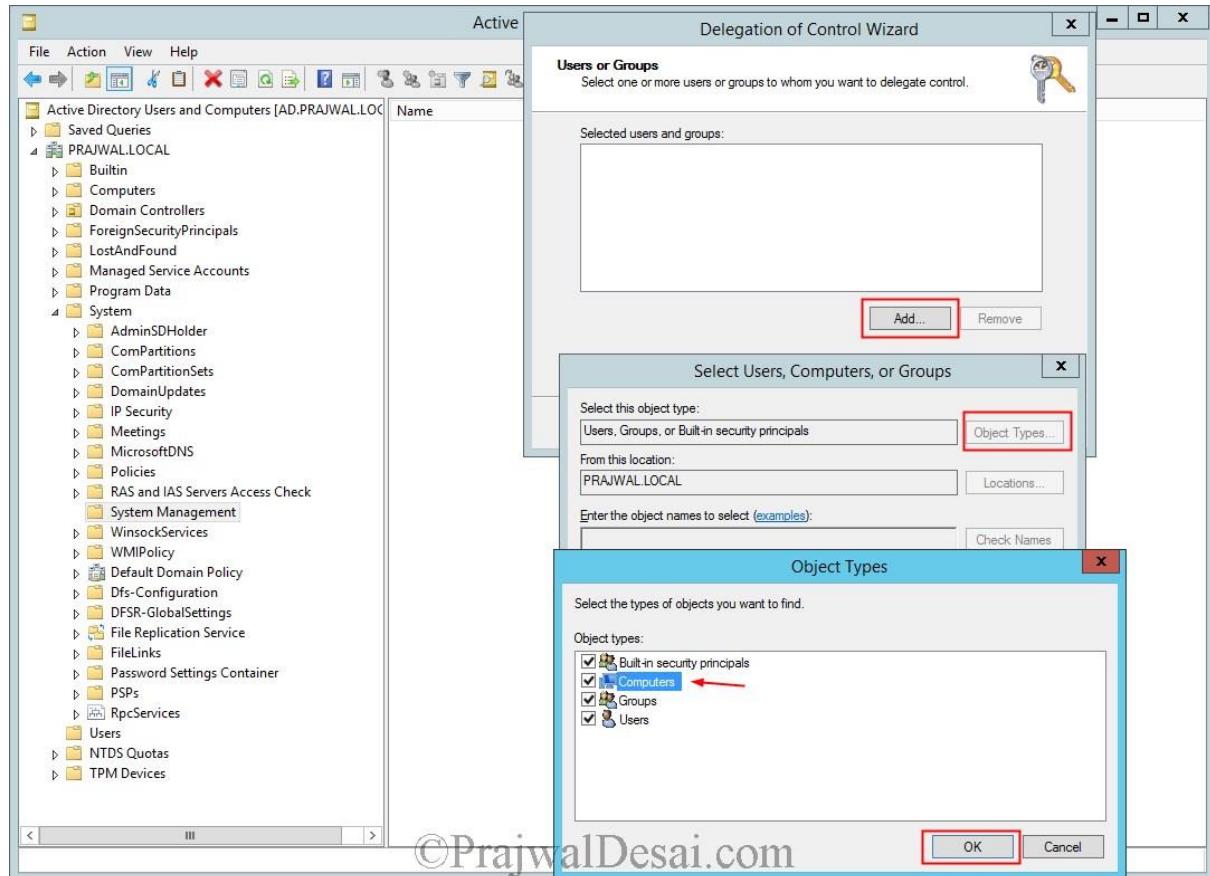
Provide the value as **System Management**. Click on **Next** and click on **Finish** to close the wizard.



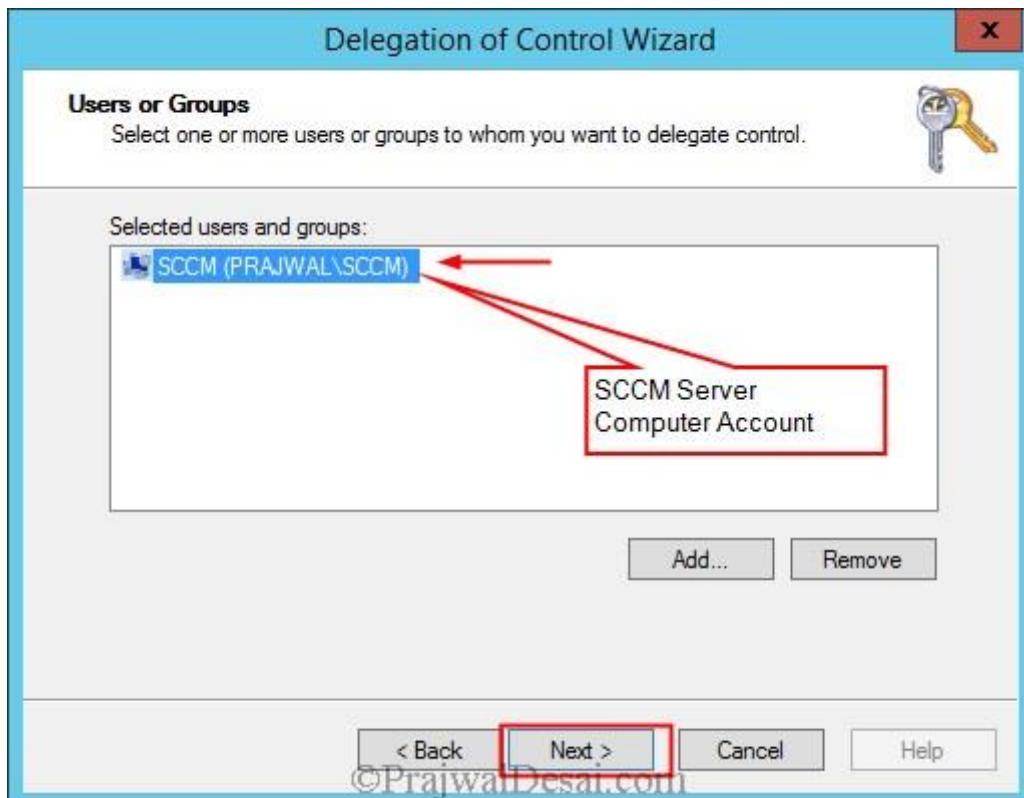
Now that we have created the system management container, we must grant the site server's computer account the permissions that are required to publish site information to the container. The primary site server computer account must be granted **Full Control** permissions to the System Management container and all its child objects. Click on **Server Manager**, click on **Tools**, click on **Active Directory Users and Computers**. Click on **View** and click **Advanced Features**. Expand **System**, right click **System Management** and click on **Delegate Control**.



The primary site server computer account must be granted Full Control permissions to the System Management container. Click on **Add**, on **select users,computers or groups** window click on **Object Types** and check for **Computers** as object types. Click on **OK**. Type the name of the primary site server computer account and click on **OK**.



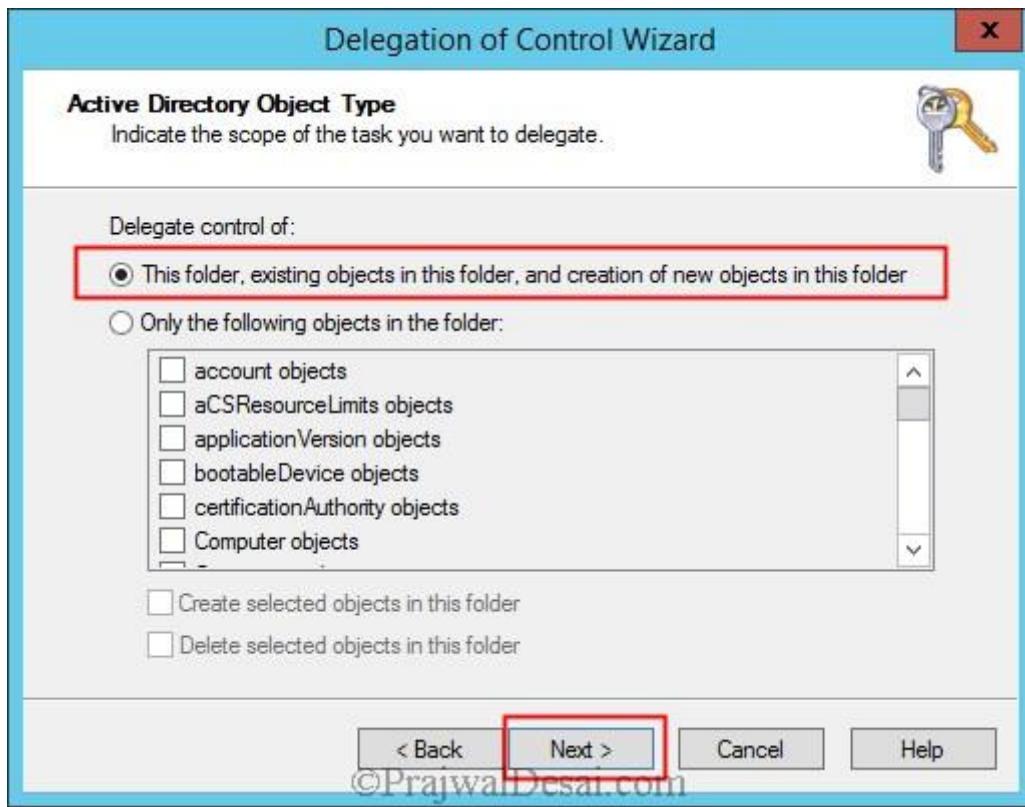
You must see the primary site server computer account listed under the users or groups. Click on **Next**.



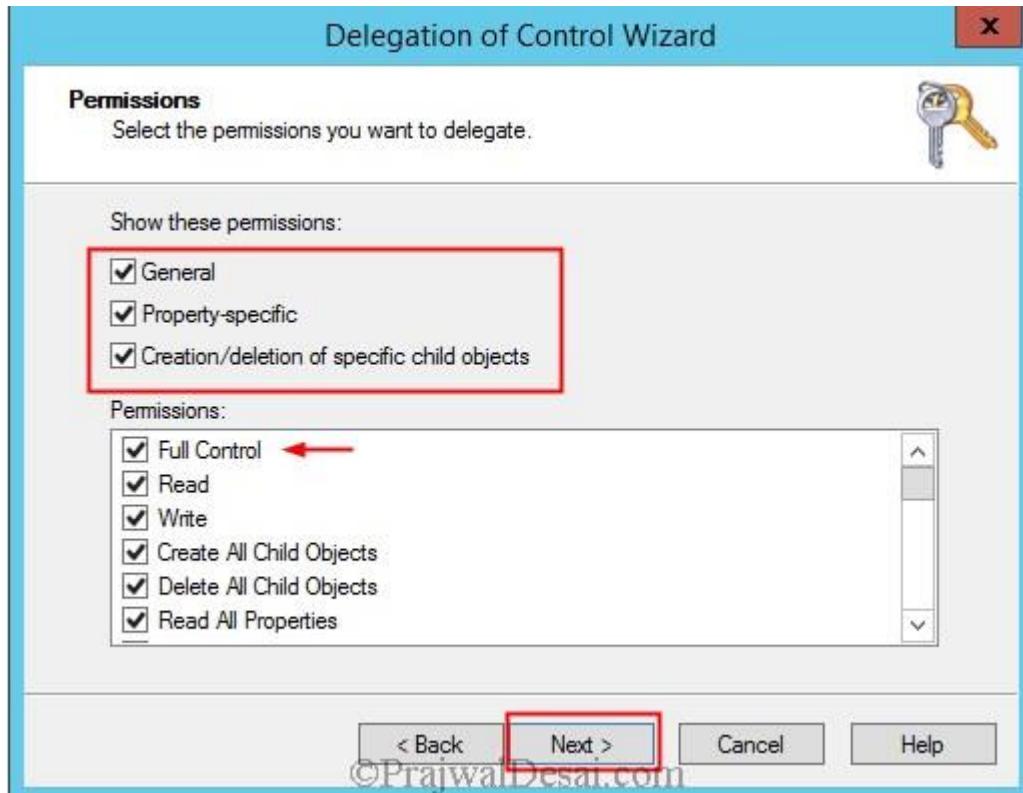
On the **Tasks to Delegate** page, click on **Create a custom task to delegate**. Click on **Next**.



On the **Active Directory Object Type** window, select the option **This folder, existing objects in this folder and creation of new objects in this folder**. Click on **Next**.

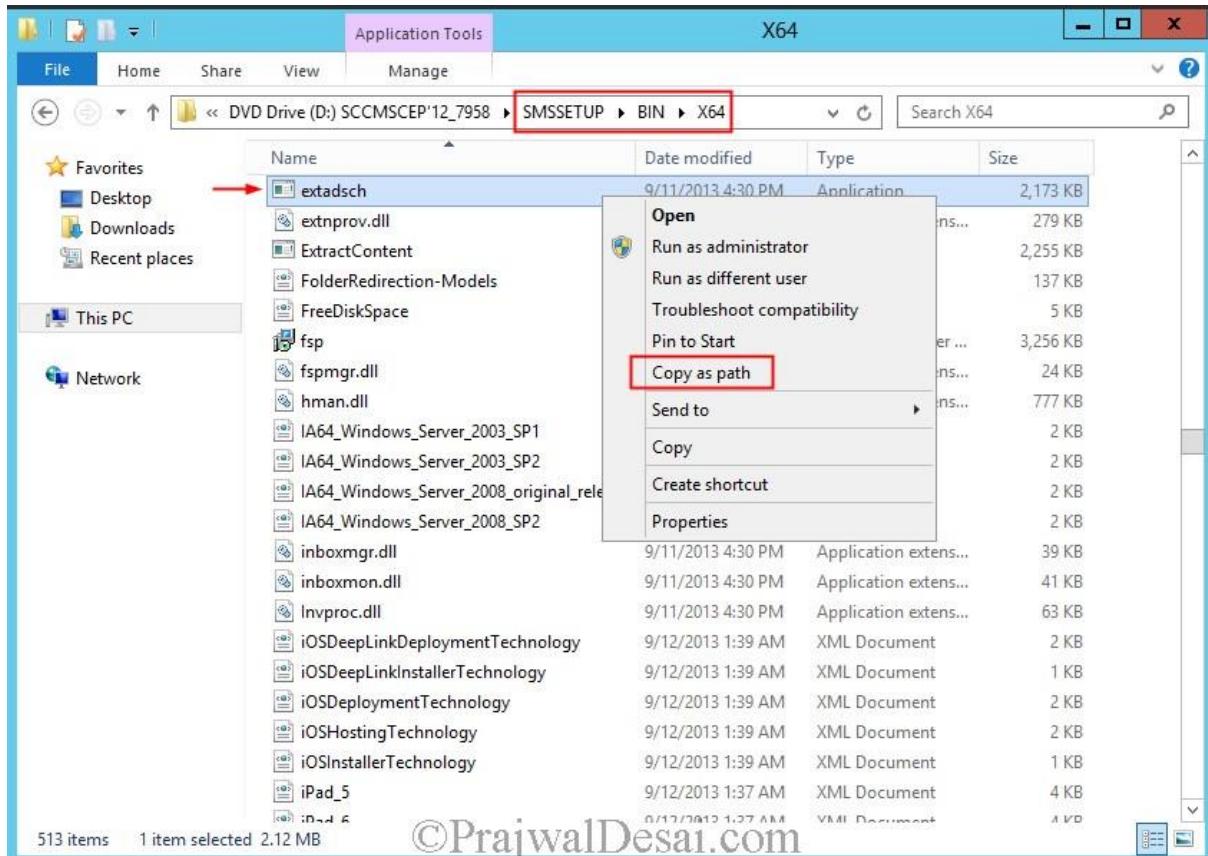


We need to select the **permissions to delegate**, choose **General, Property Specific** and **Creation/deletion of specific child objects**. Under the **permissions**, click on **Full Control**. when you check the box for Full Control all the other permissions gets checked automatically. Click on **Next** and click on **Finish** to close the wizard. We have delegated full permissions to primary site server computer account on **System Management** container.



Extending Active Directory Schema

To extend the Active Directory Schema using extadsh.exe utility, locate the **extadsh.exe** which can be found in **\SMSSETUP\BIN\X64** of the configuration manager setup DVD. Hold the shift key on your keyboard and right click **extadsh.exe** and click on **Copy as Path**.



Launch the **command prompt**. Right click and click paste and hit enter. You should see the line **Successfully extended the Active Directory Schema**.

```
Administrator: Select Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>"D:\SMSSETUP\BIN\X64\extadsh.exe"

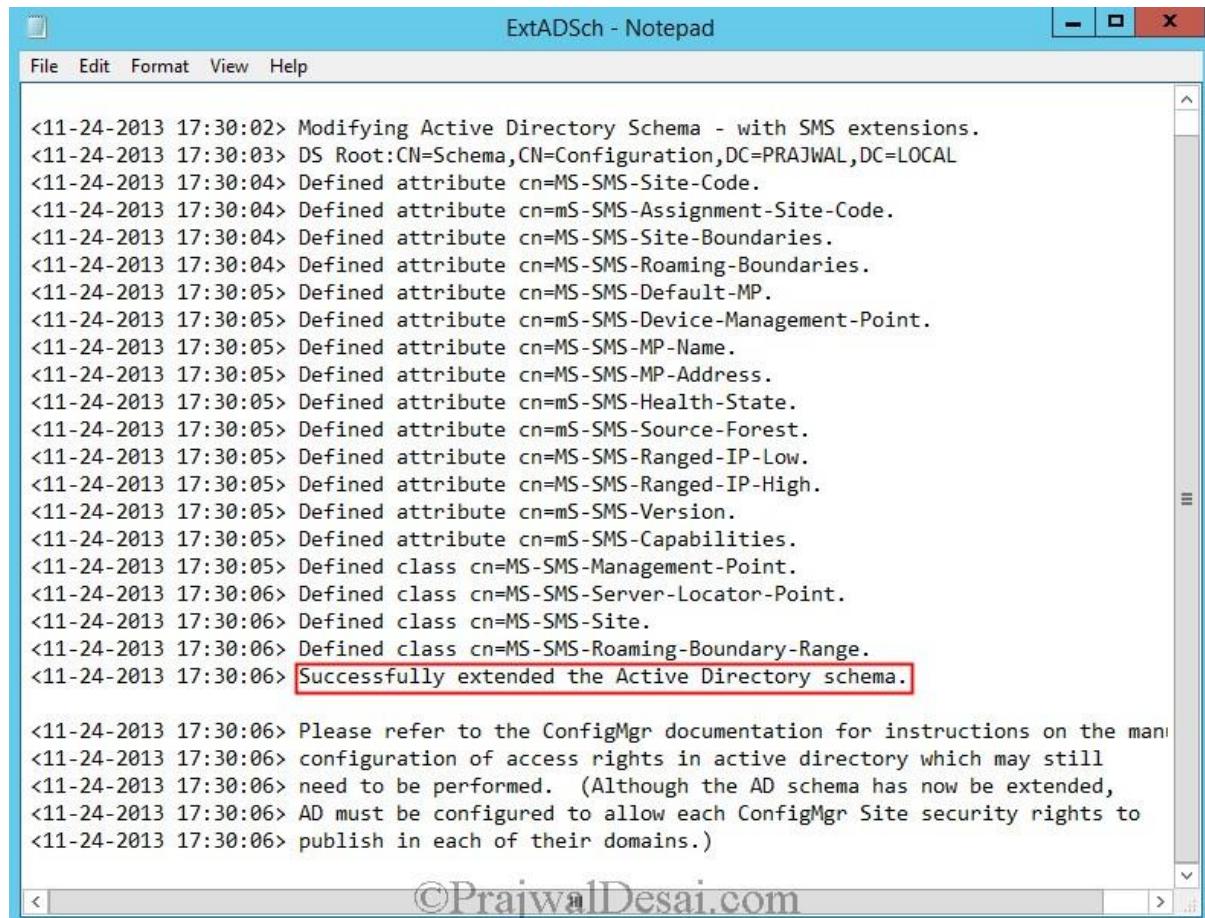
Microsoft System Center 2012 Configuration Manager v5.00 <Build 7958>
Copyright (C) 2011 Microsoft Corp.

Successfully extended the Active Directory schema.

Please refer to the ConfigMgr documentation for instructions on the manual configuration of access rights in active directory which may still need to be performed. (Although the AD schema has now been extended, AD must be configured to allow each ConfigMgr Site security rights to publish in each of their domains.)

C:\Users\Administrator>
```

To verify whether schema extension was successful, open the log file **extadsch.log** located in the root of the system drive. You should see the line “**Successfully extended the Active Directory Schema**”.



The screenshot shows a Windows Notepad window titled "ExtADSCh - Notepad". The window contains a log file with the following content:

```
<11-24-2013 17:30:02> Modifying Active Directory Schema - with SMS extensions.
<11-24-2013 17:30:03> DS Root:CN=Schema,CN=Configuration,DC=PRAJWAL,DC=LOCAL
<11-24-2013 17:30:04> Defined attribute cn=MS-SMS-Site-Code.
<11-24-2013 17:30:04> Defined attribute cn=mS-SMS-Assignment-Site-Code.
<11-24-2013 17:30:04> Defined attribute cn=MS-SMS-Site-Boundaries.
<11-24-2013 17:30:04> Defined attribute cn=MS-SMS-Roaming-Boundaries.
<11-24-2013 17:30:05> Defined attribute cn=MS-SMS-Default-MP.
<11-24-2013 17:30:05> Defined attribute cn=mS-SMS-Device-Management-Point.
<11-24-2013 17:30:05> Defined attribute cn=MS-SMS-MP-Name.
<11-24-2013 17:30:05> Defined attribute cn=MS-SMS-MP-Address.
<11-24-2013 17:30:05> Defined attribute cn=mS-SMS-Health-State.
<11-24-2013 17:30:05> Defined attribute cn=mS-SMS-Source-Forest.
<11-24-2013 17:30:05> Defined attribute cn=MS-SMS-Ranged-IP-Low.
<11-24-2013 17:30:05> Defined attribute cn=MS-SMS-Ranged-IP-High.
<11-24-2013 17:30:05> Defined attribute cn=mS-SMS-Version.
<11-24-2013 17:30:05> Defined attribute cn=mS-SMS-Capabilities.
<11-24-2013 17:30:05> Defined class cn=MS-SMS-Management-Point.
<11-24-2013 17:30:06> Defined class cn=MS-SMS-Server-Locator-Point.
<11-24-2013 17:30:06> Defined class cn=MS-SMS-Site.
<11-24-2013 17:30:06> Defined class cn=MS-SMS-Roaming-Boundary-Range.
<11-24-2013 17:30:06> Successfully extended the Active Directory schema.

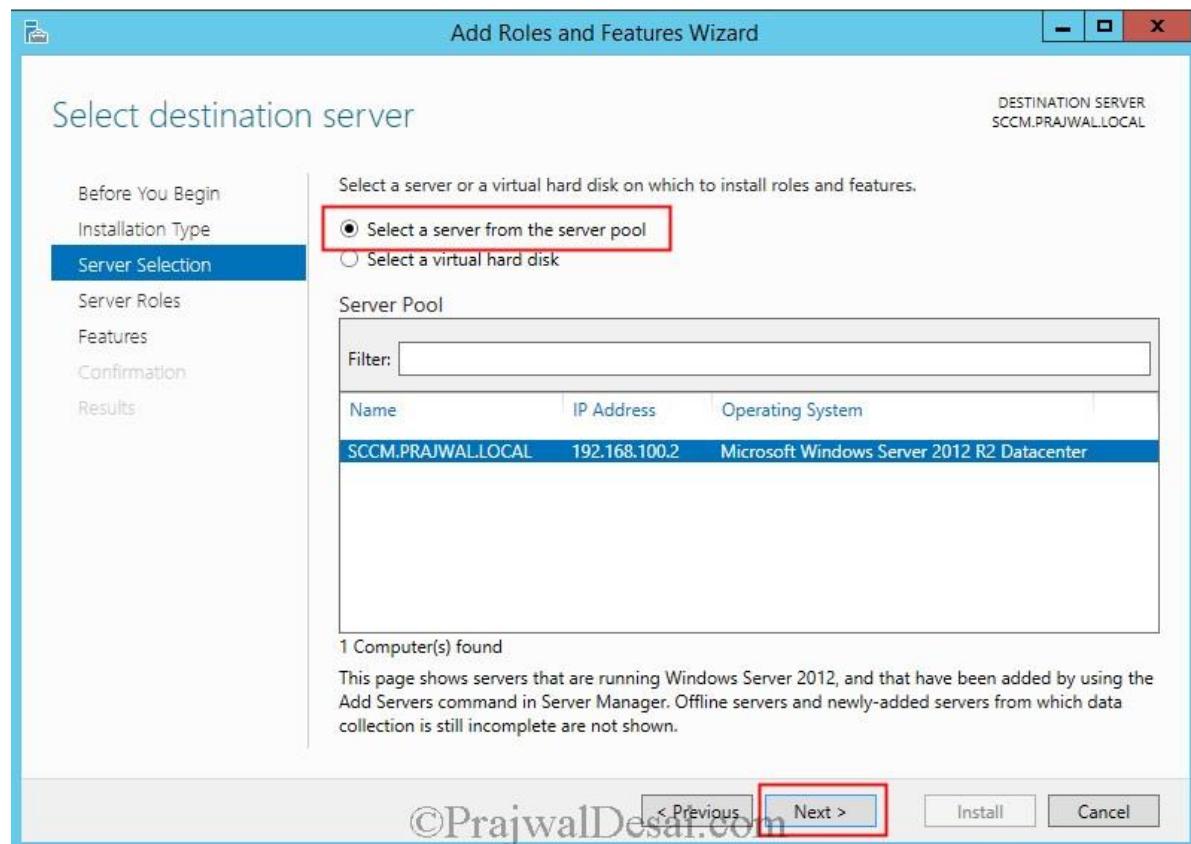
<11-24-2013 17:30:06> Please refer to the ConfigMgr documentation for instructions on the mani
<11-24-2013 17:30:06> configuration of access rights in active directory which may still
<11-24-2013 17:30:06> need to be performed. (Although the AD schema has now been extended,
<11-24-2013 17:30:06> AD must be configured to allow each ConfigMgr Site security rights to
<11-24-2013 17:30:06> publish in each of their domains.)
```

The line "Successfully extended the Active Directory schema." is highlighted with a red rectangular box.

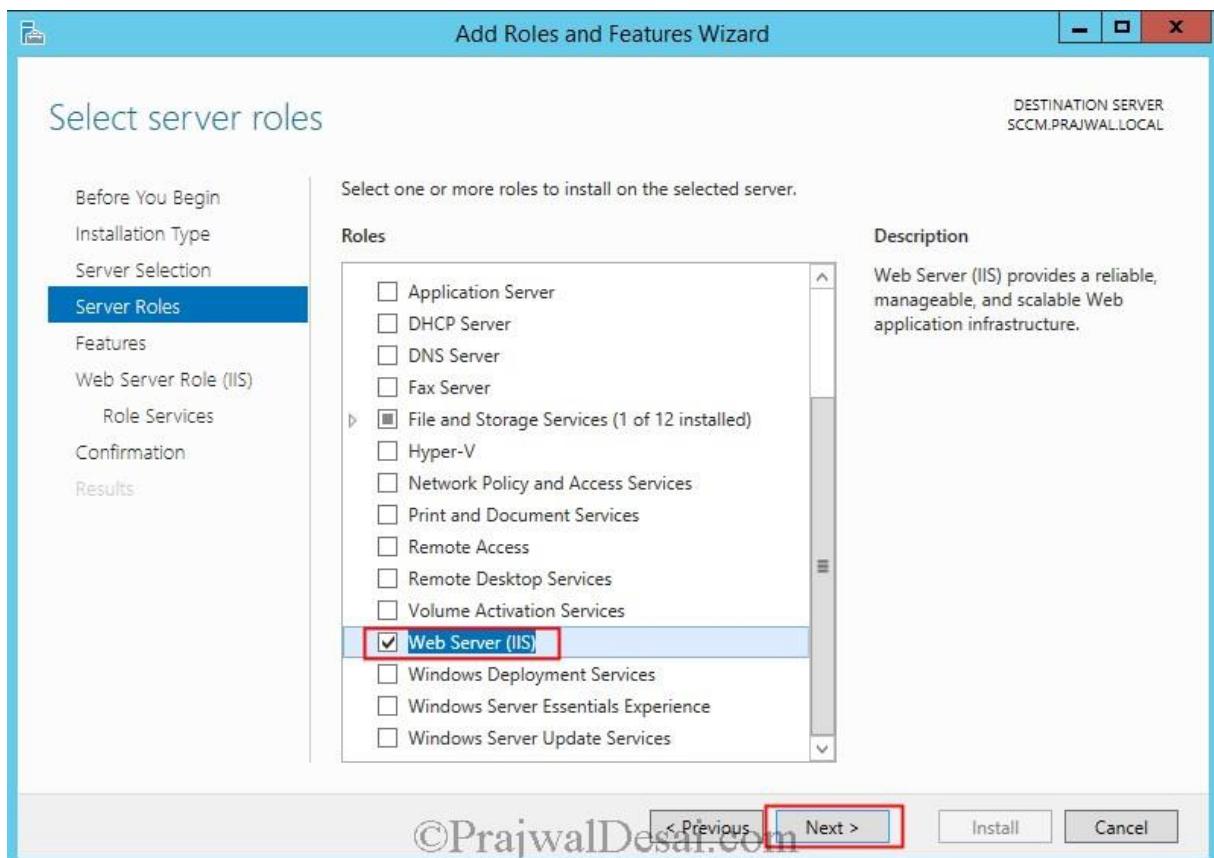
Installing Prerequisites for Configuration Manager 2012 R2

After creating system management container, assigning site server computer permissions on container, extending active directory schema we will now start installing prerequisites for configuration manager 2012 R2. I will be listing out the download links for all the prerequisites at the end of this post.

On the SCCM server, click on **Server Manager**, click on **Manage**, click on **Add Roles and Features**. Click on **Select a server from the server pool** and click on **Next**.



Select **Web Server (IIS)** as the server role and click on **Next**.



You need to enable the following features for installing configuration manager 2012 R2 on Windows server 2012 R2

1) .Net Framework 3.5 Features [Install all sub features]

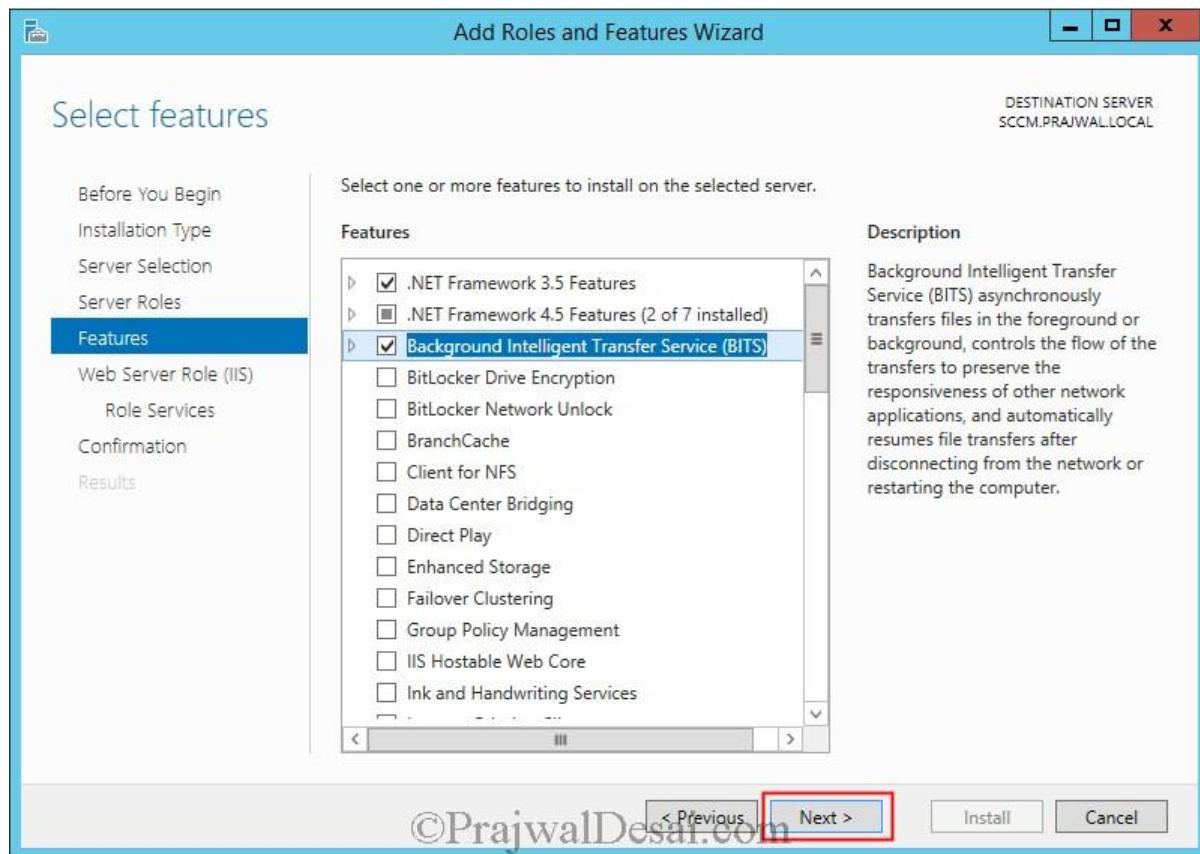
2) .Net Framework 4.5 Features [Install all sub features]

3) BITS

4) Remote Differential Compression

Note :- Microsoft lists the prerequisites that are required by Configuration Manager for each site system role on supported operating systems prior to Windows Server 2012 and for Windows Server 2012.

Once you select the features listed above, click on **Next**.



©PrajwallDesai.com

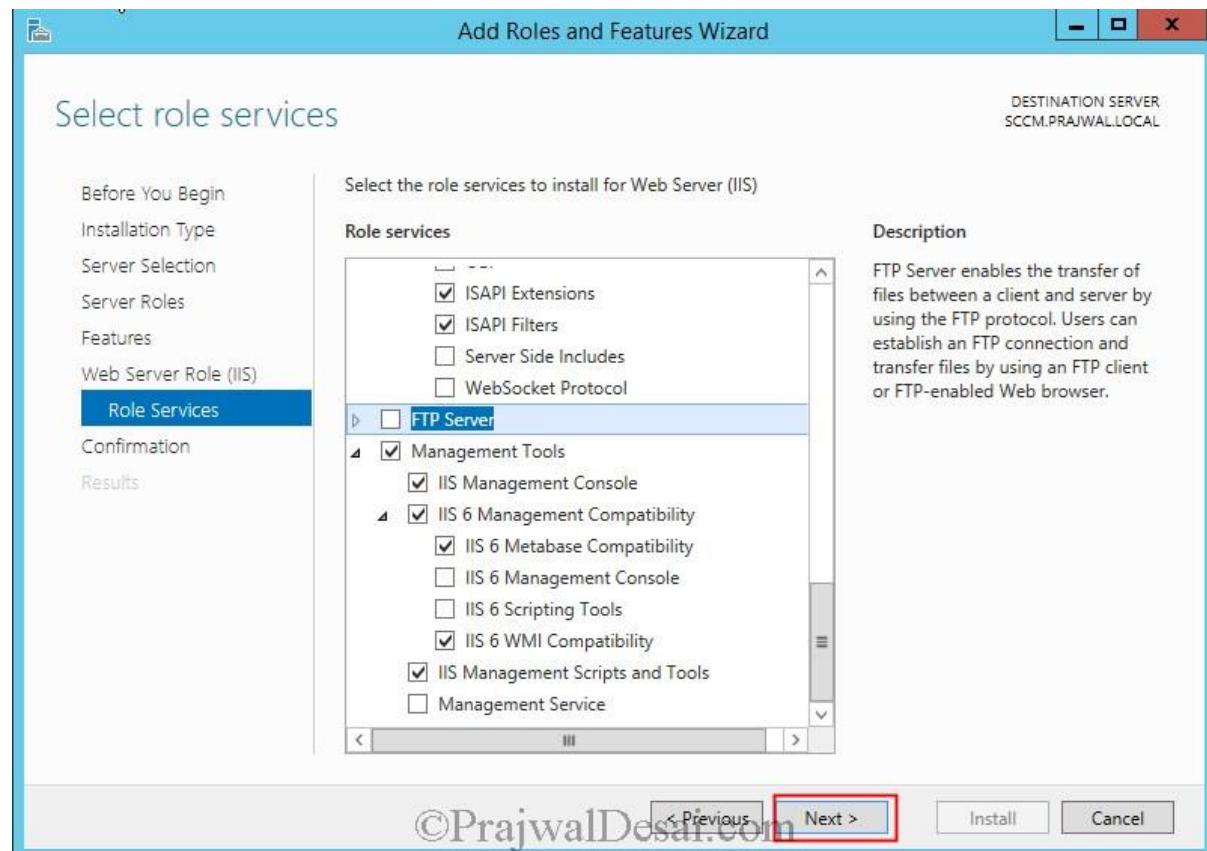
Install the following Roles Services

Common HTTP Features – Default Document, Static Content.

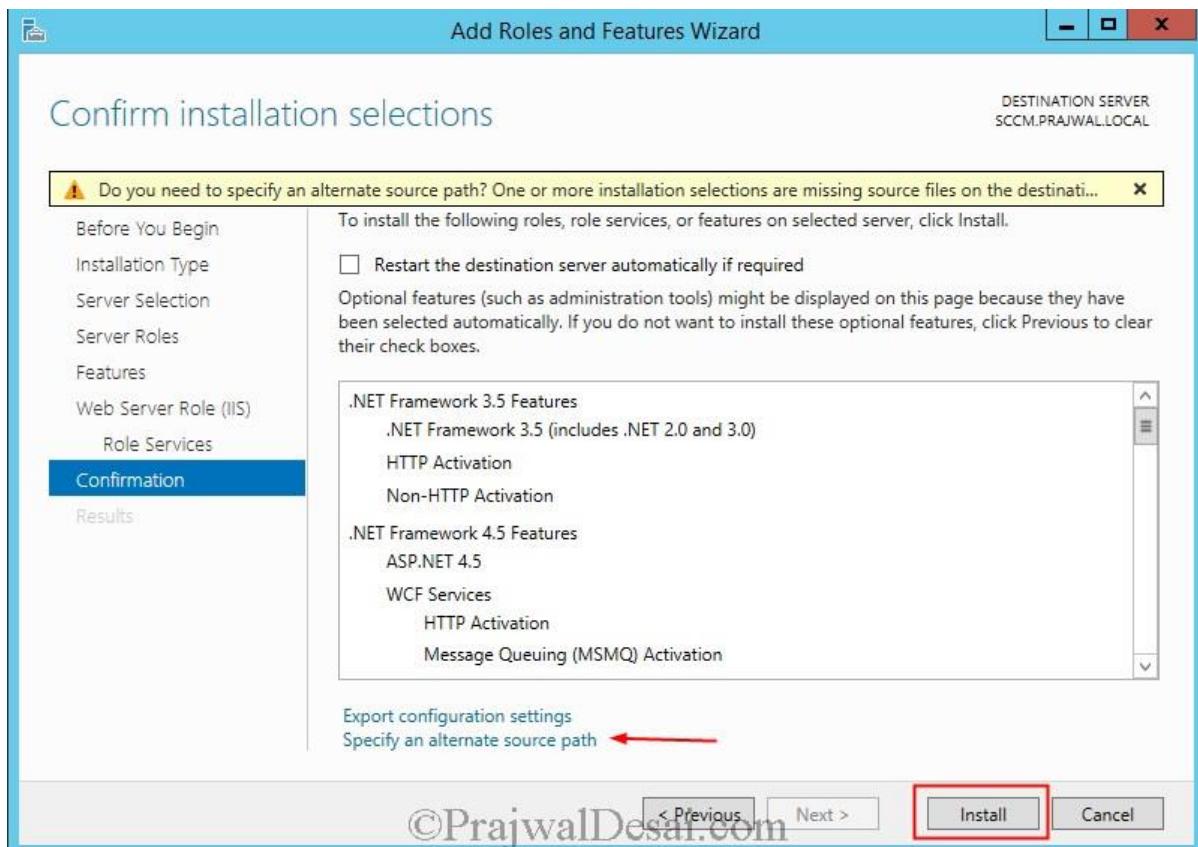
Application Development – ASP.NET 3.5, .NET Extensibility 3.5, ASP.NET 4.5, .NET Extensibility 4.5, ISAPI extensions.

Security – Windows Authentication.

IIS 6 Management Compatibility – IIS Management Console, IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS Management Scripts and Tools.



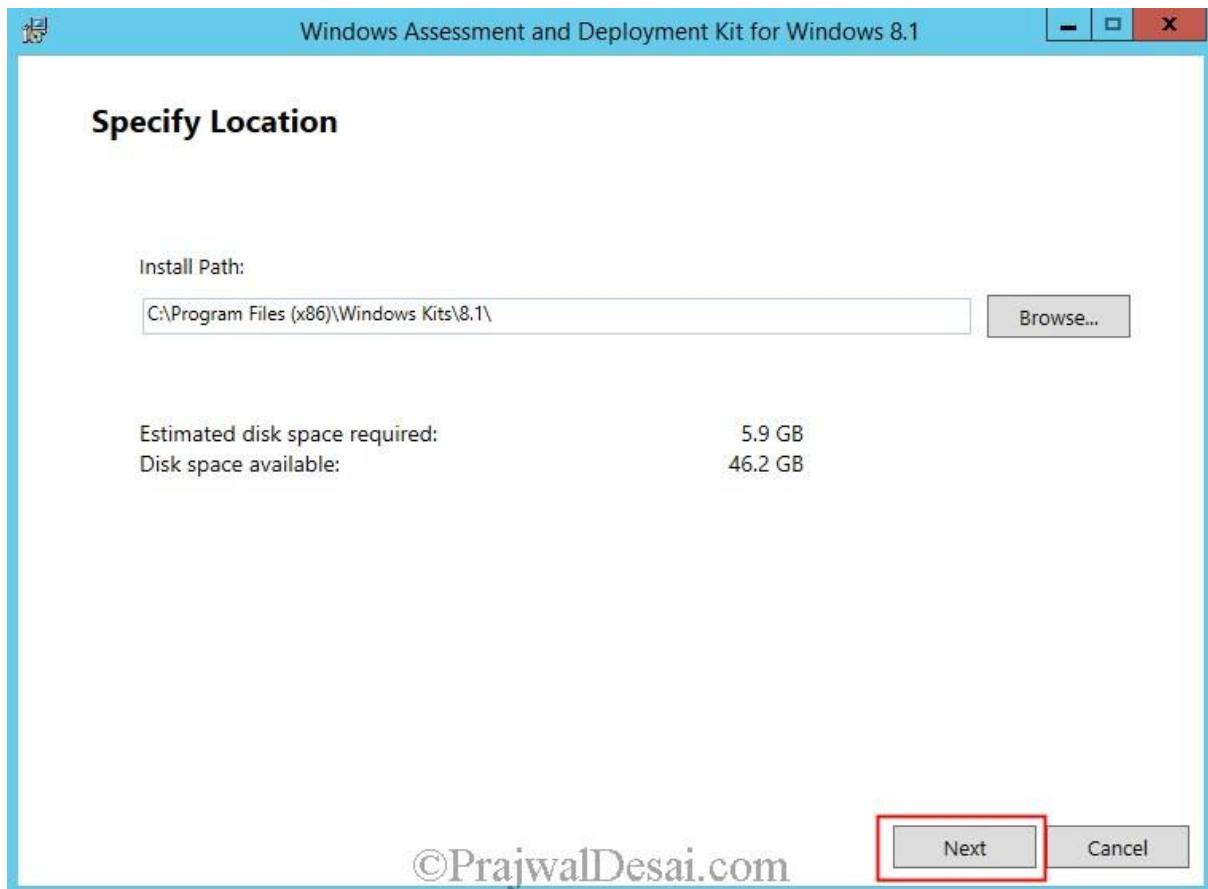
If the installation of roles services needs the windows server 2012 installation media click on **Specify an alternate source path** and provide the path as **D:\Sources\sxs** (where D is the drive letter where the Windows Server 2012 R2 media is mounted).



Windows Assessment and Deployment Kit (Windows ADK) for Windows 8.1

The Windows Assessment and Deployment Kit (Windows ADK) is a collection of tools that you can use to customize, assess, and deploy Windows operating systems to new computers. The latest version out there is ADK 8.1 and you can find the download links at the end of the post.

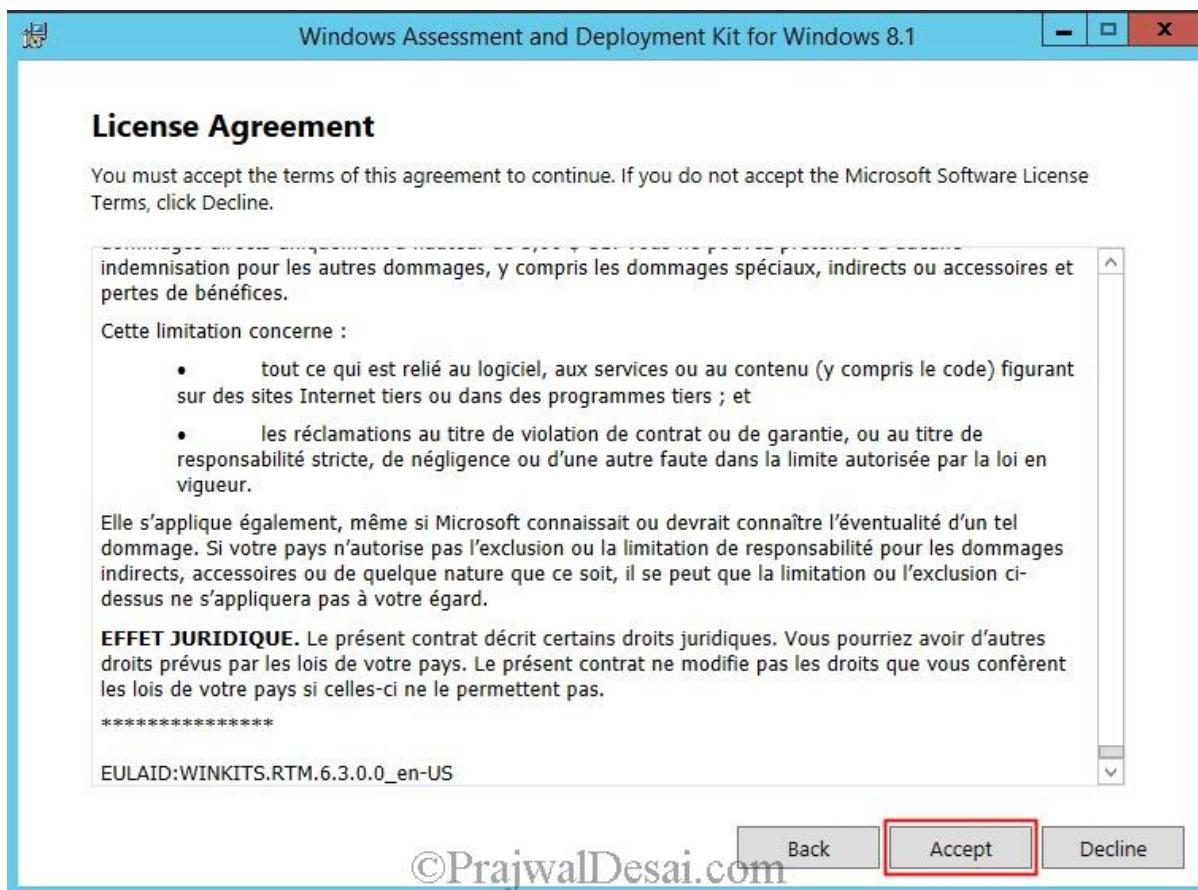
Download the **adksetup.exe**, right click on the file and click on **Run as Administrator**. On the **Specify Location** page, choose the install path. Click on **Next**.



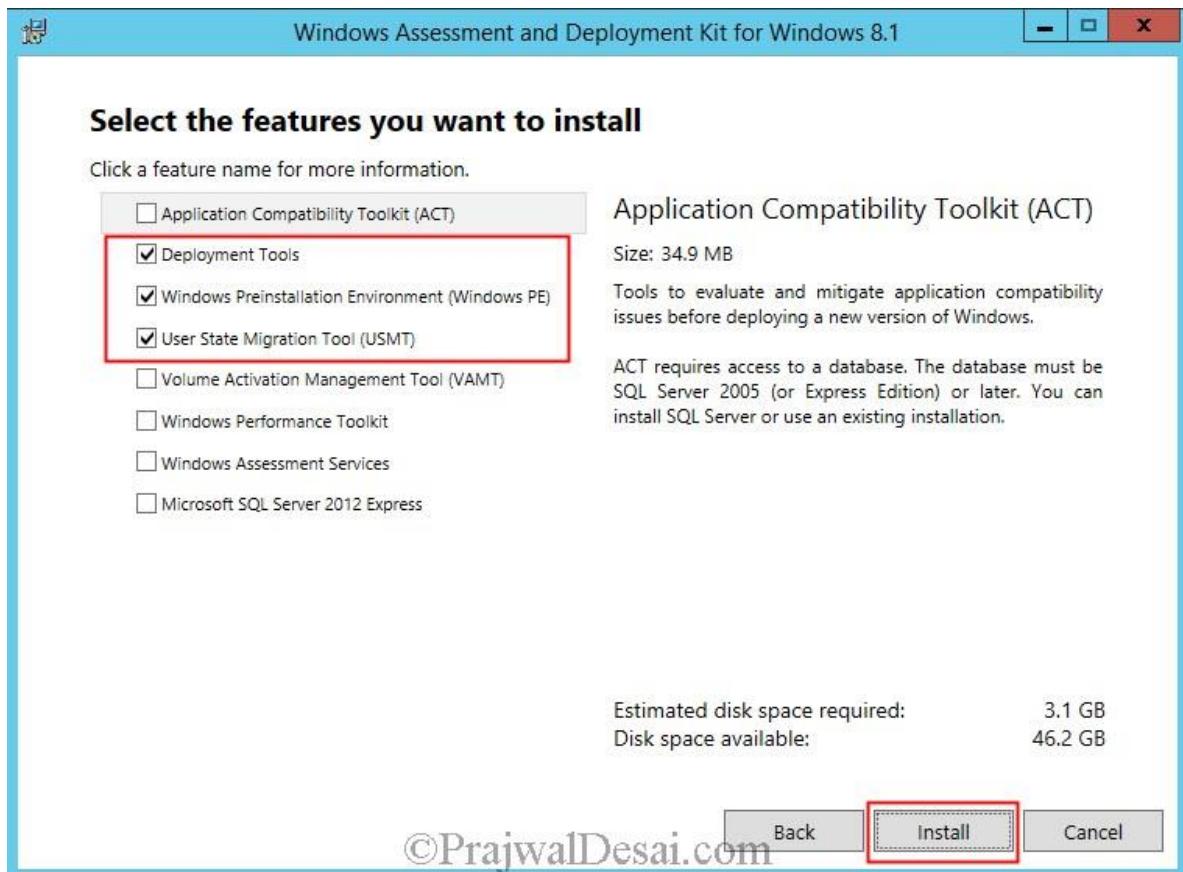
Click **No** for **Join the Customer Experience Improvement Program**. Click on **Next**.



On the License Agreement page, Click on Accept.



Select **Deployment Tools**, **Windows Preinstallation Environment** and **User State Migration Tool**. Click on **Install**.



We have installed the Windows Assessment and Deployment kit for Windows 8.1. Click on **Close**.



Installing SQL Server for System Center 2012 R2 Configuration Manager

In this post we will be looking at the steps for Installing SQL Server 2012 for Configuration Manager 2012 R2. In this deployment series of Configuration Manager 2012 R2 we started with [system center 2012 R2 Configuration Manager system requirements](#) which tells more about the new features of SCCM 2012 R2 and system requirements for Configuration Manager 2012 R2, in the next post we saw the steps for [installing prerequisites for SCCM 2012 R2](#). After installing prerequisites the next step is to install SQL server. Most of the users have a question on where should the SQL server be installed, should it be installed locally on the server where SCCM is installed or on a remote server ?. The answer is you can install it on local server or host the database on remote server. I would prefer to install SQL locally because this it requires less administrative overhead, the license for SQL is included with System Center so no additional license needs to be purchased and with local SQL you can achieve better performance than remote. In this post we will be installing SQL server 2012 with SP1 on windows server 2012 R2, if you have only SQL server 2012 iso copy, you can download the SQL server 2012 service pack 1 and install it.

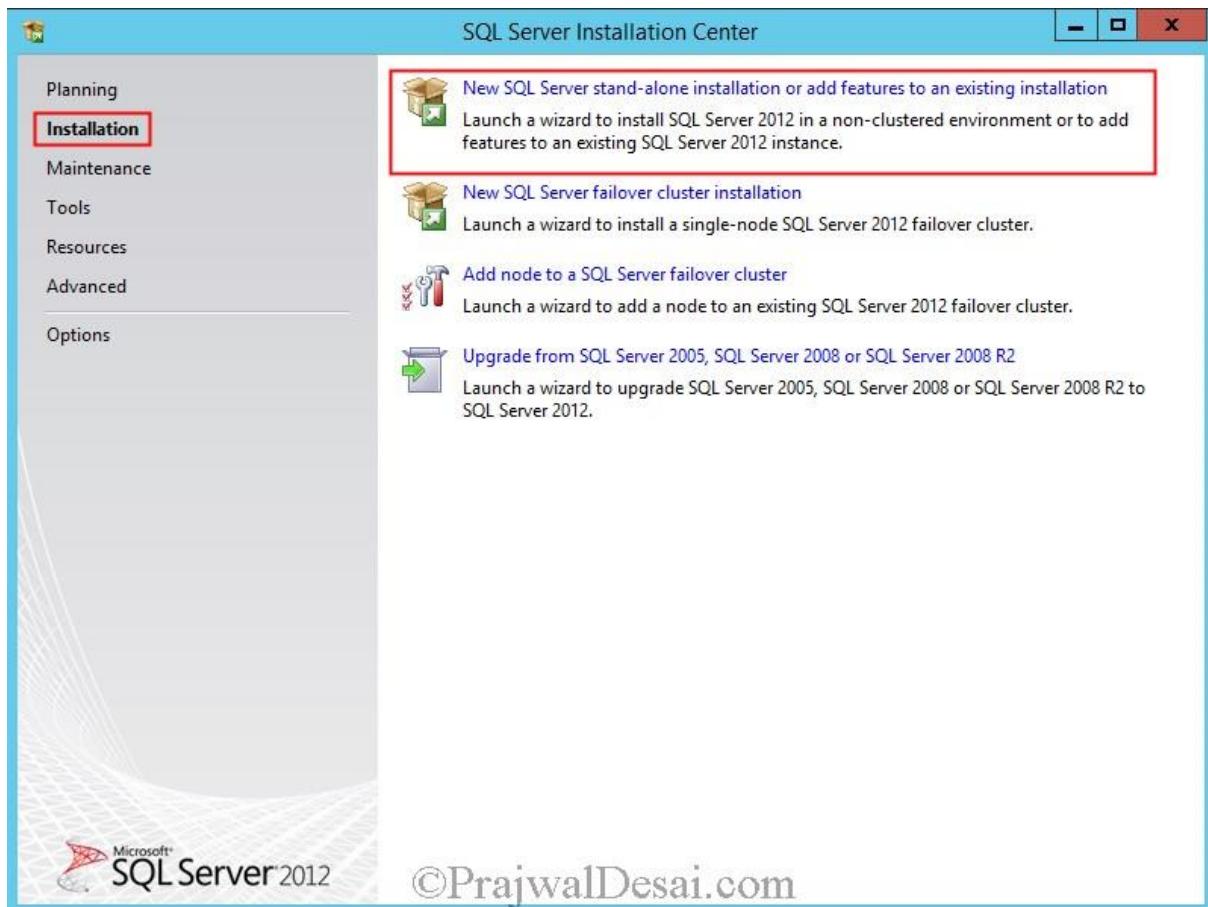
For System Center 2012 R2 Configuration Manager you can install the SQL server with combinations :-

- 1) **Install SQL Server 2012 + Min Cumulative Update 2**
- 2) **Install SQL Server 2012 + Service Pack 1 [no cumulative update required]**
- 3) **Install SQL Server 2012 with Service Pack 1 [no cumulative update required]**

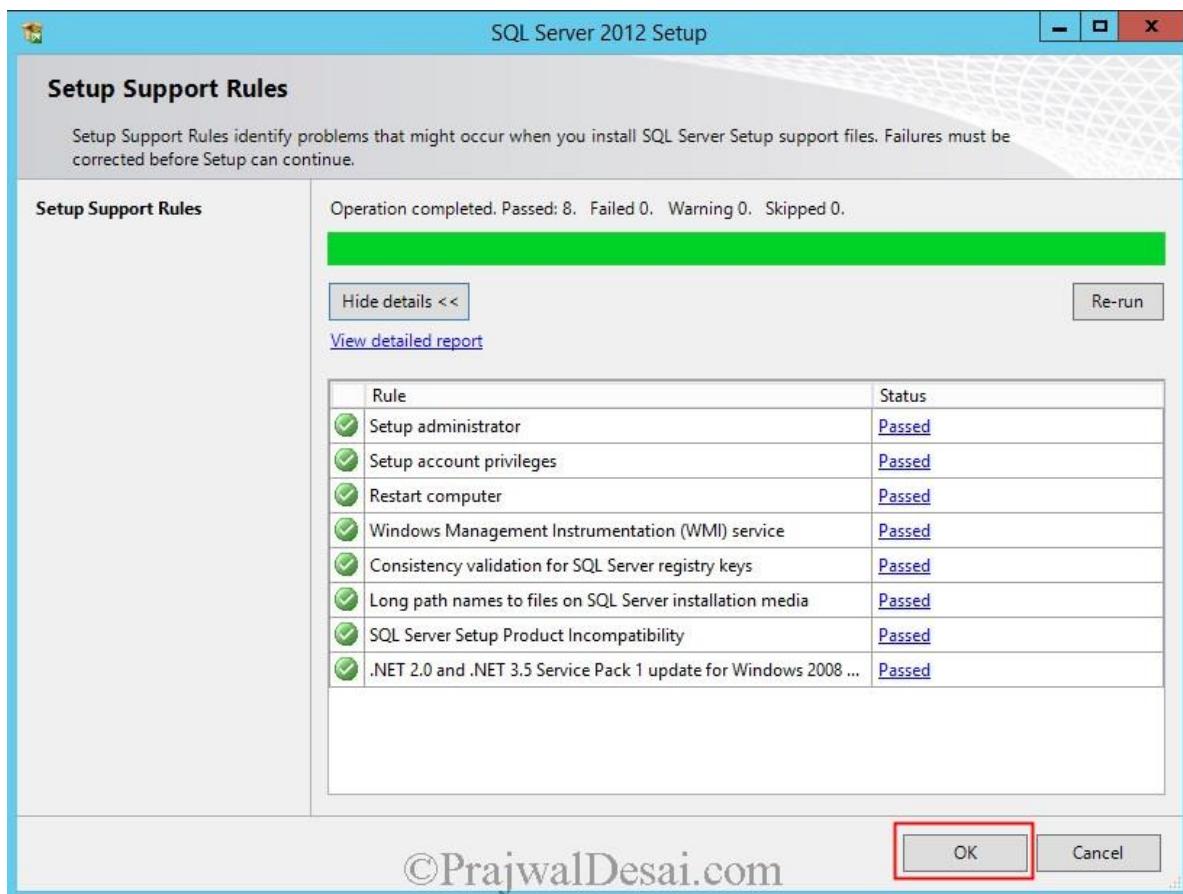
If you are planning to use SQL server other than 2012 then click here to see the [SQL Server Requirements for Configuration Manager 2012 R2](#).

Installing SQL Server 2012 for Configuration Manager 2012 R2

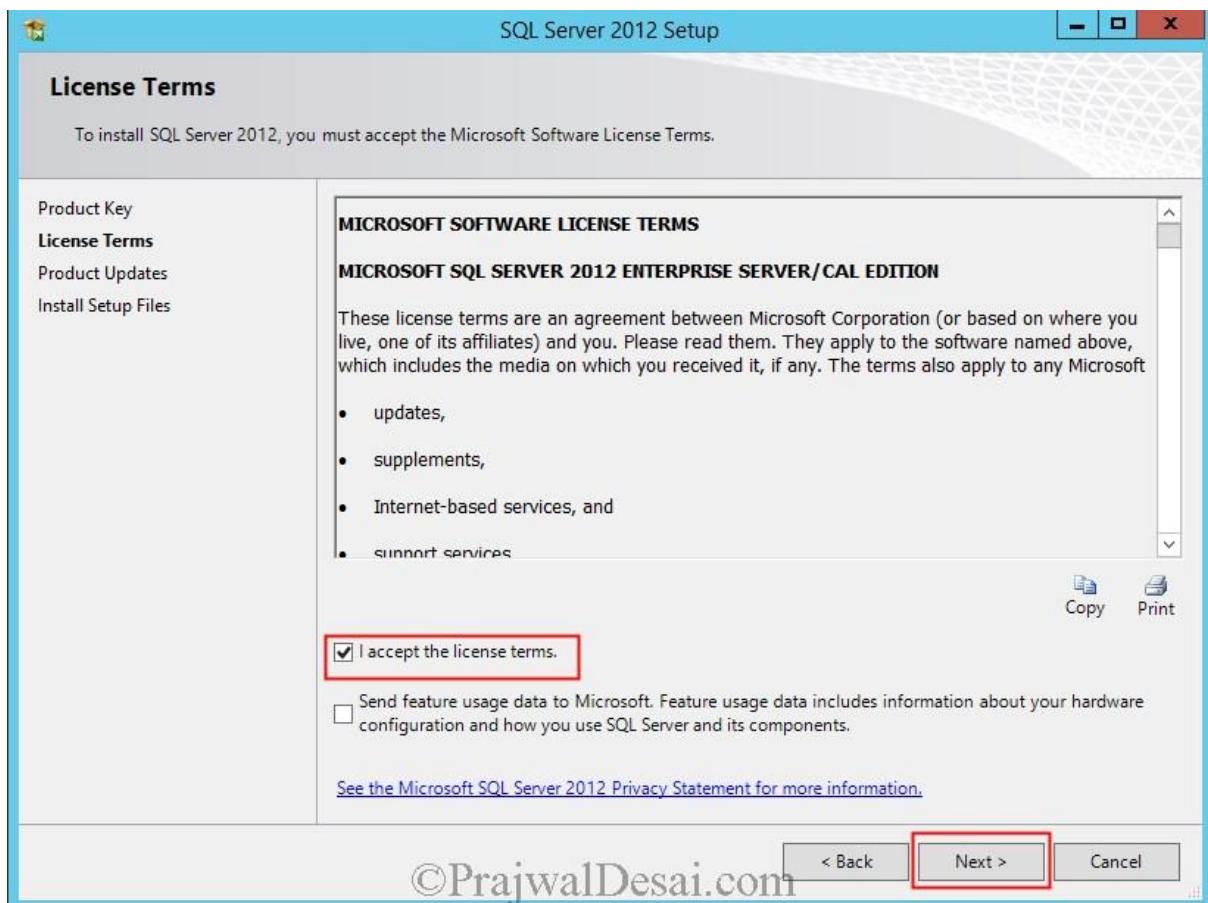
So lets look at the steps to install SQL Server 2012 with SP1 (x64 Bit). I have mounted the DVD on to the Windows Server 2012 R2, open the SQL server folder, run the setup as **administrator**. Click on **Installation** and click on **New SQL server standalone installation**.



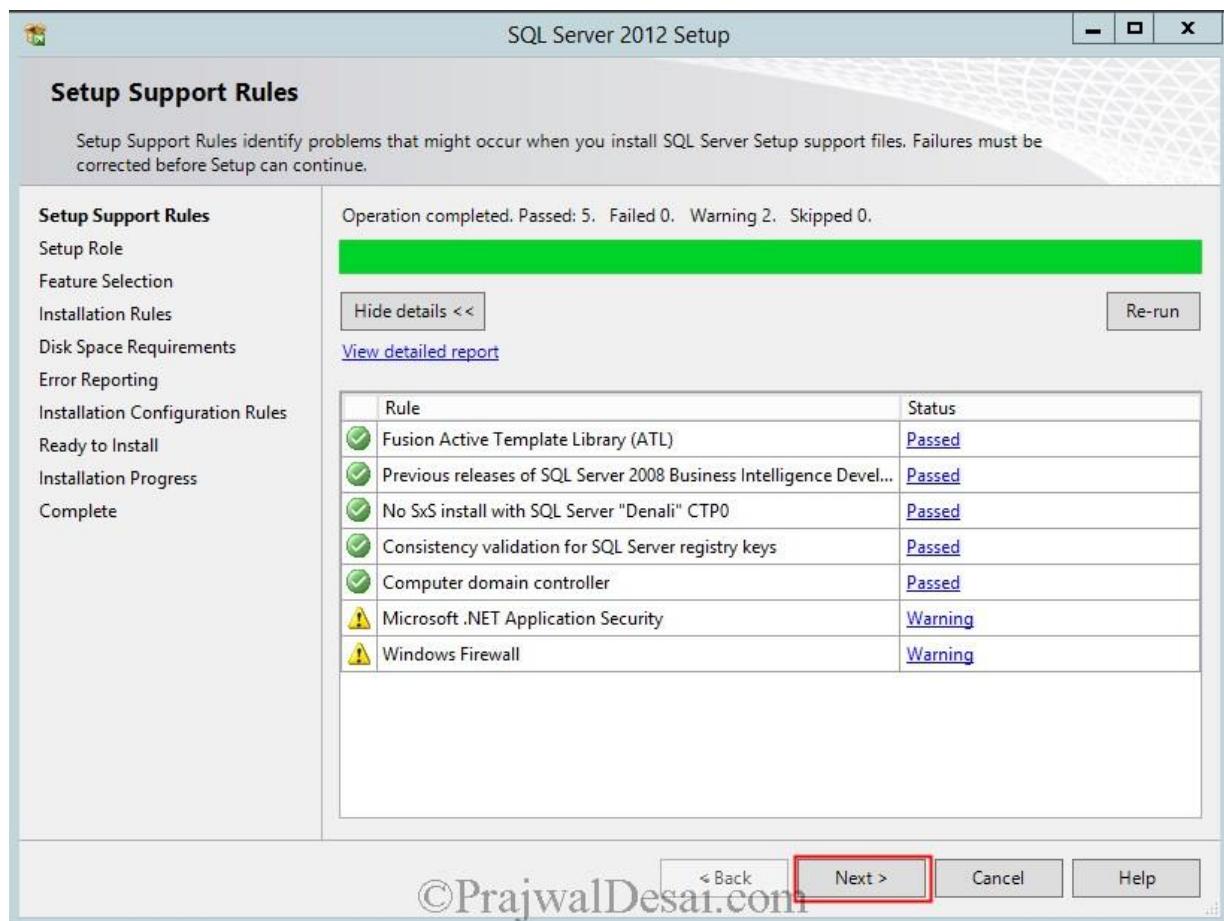
Click **OK** once the Setup support rules are run and verified.



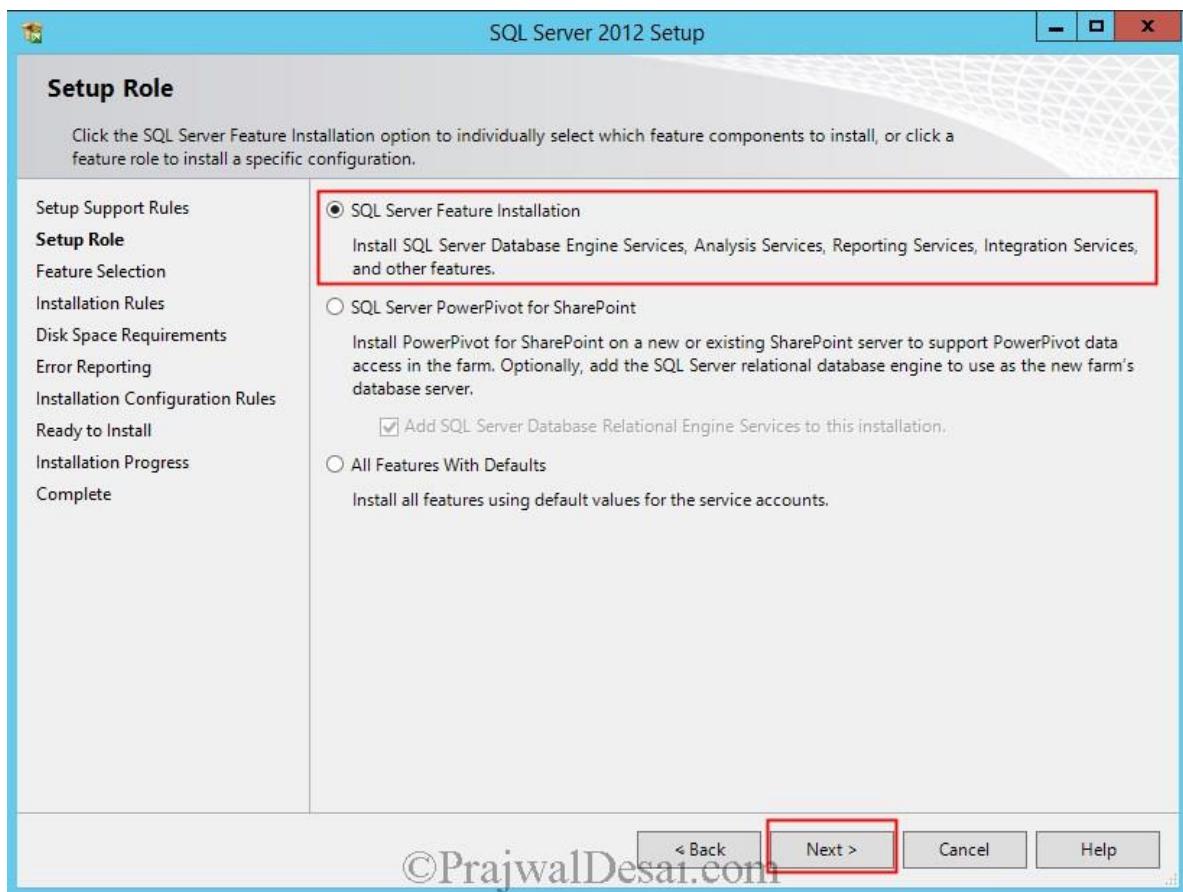
Check the box for **I accept the license terms** and click on **Next**.



After the Setup Support Rules are completed click on **Next**.

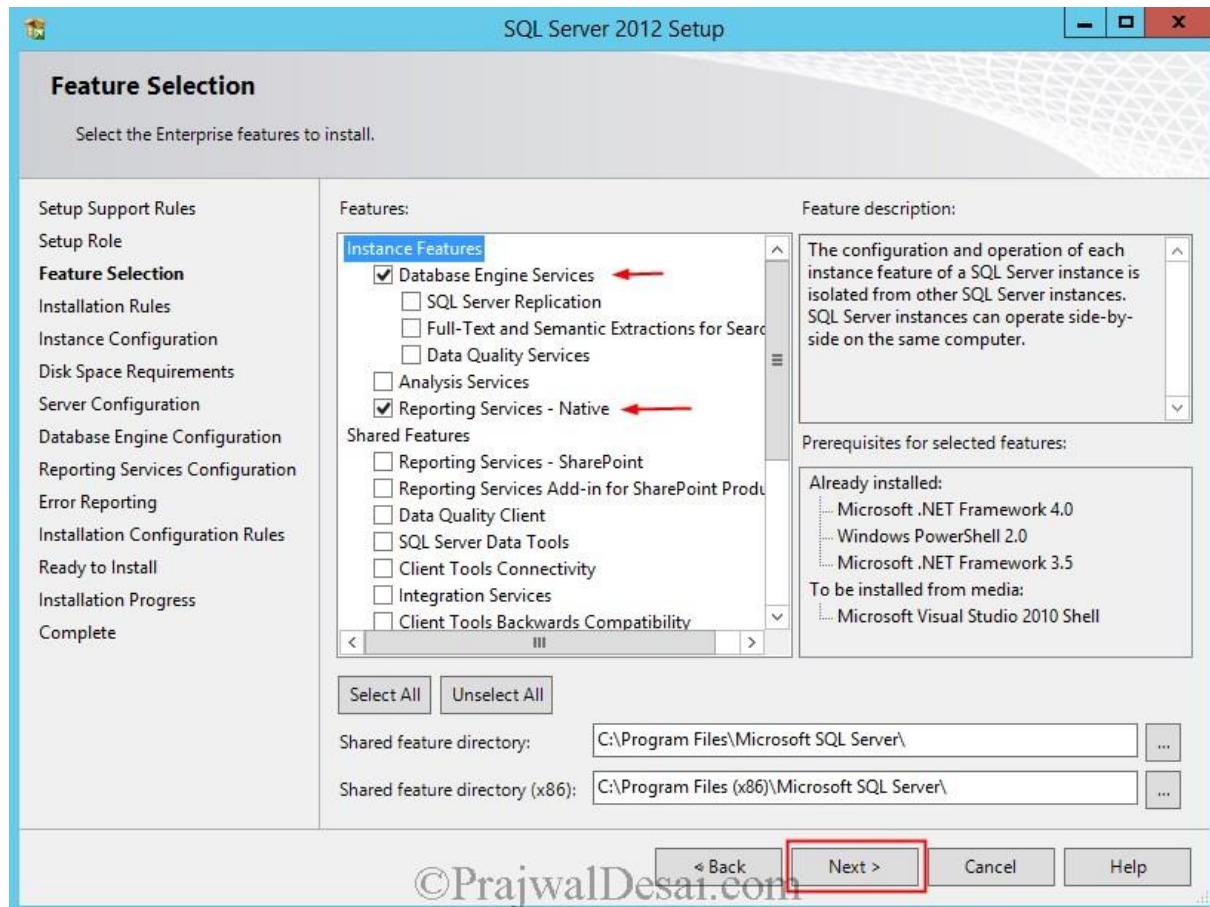


Select the **Setup Role** as **SQL Server Feature Installation** and click **Next**.



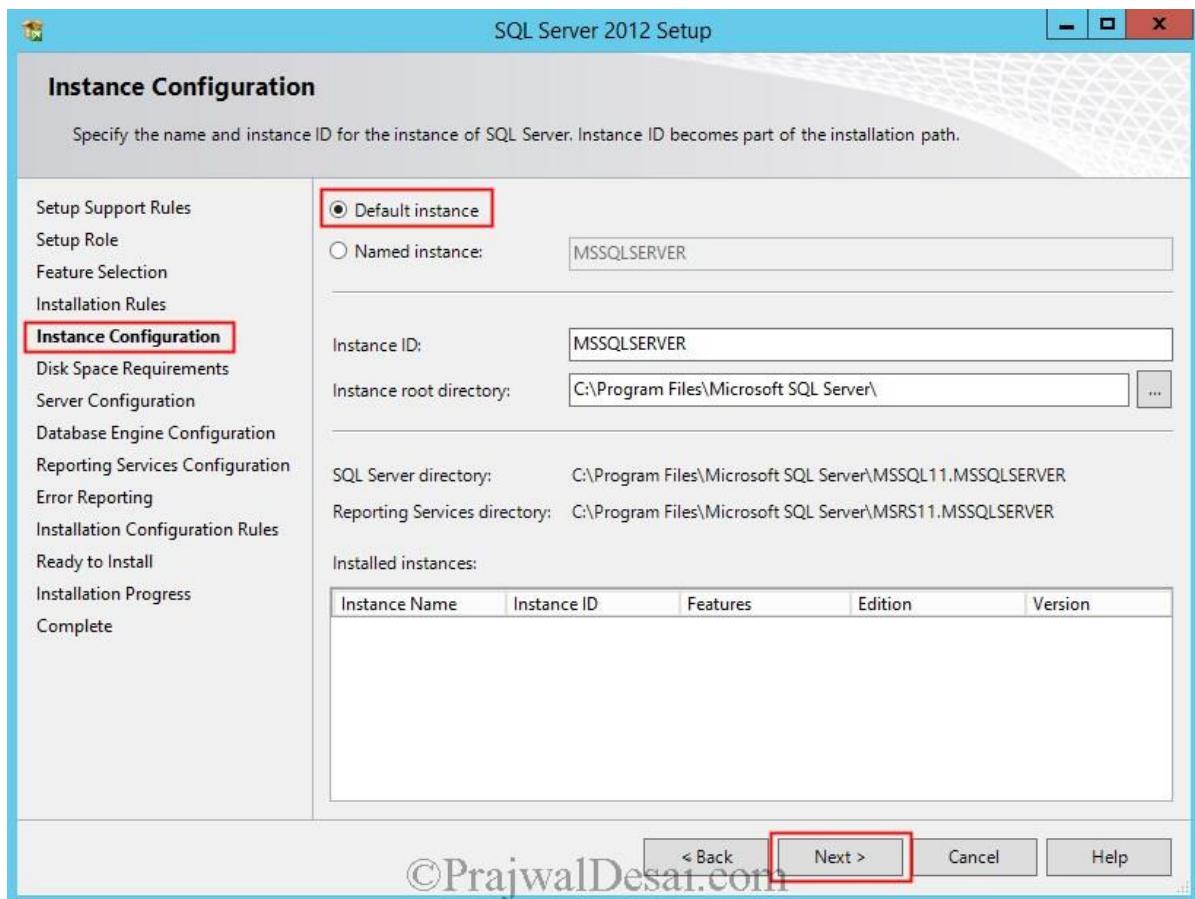
On the **Feature Selection** window, select **Database Engine Services, Reporting Services-Native and Management Tools – Complete**.

Note – The features that we have selected are the ones which are required for deploying Configuration Manager 2012 R2. However you can select all features and install them if you want to.



For **Instance Configuration** click on **Default Instance**, the instance ID **MSSQLSERVER** would be created.

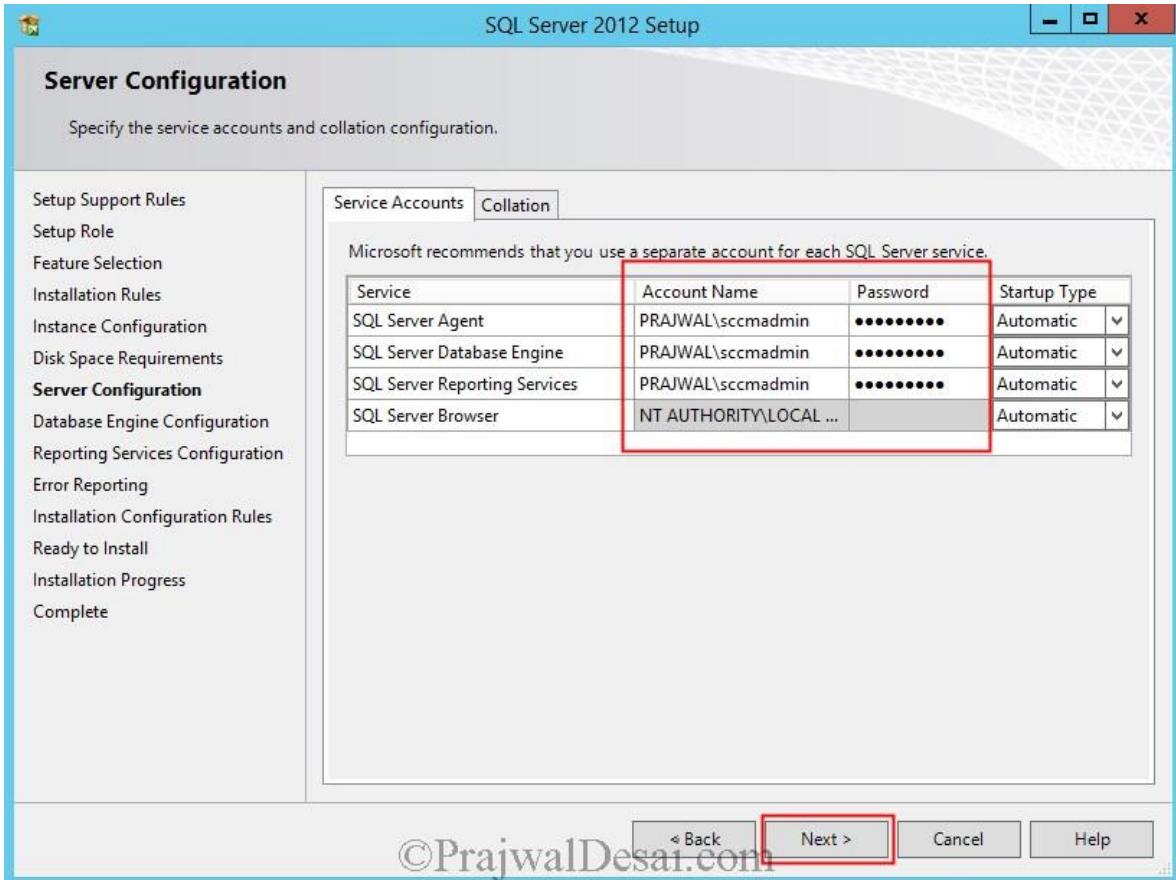
If you are creating a **Named Instance**, then during the SCCM 2012 R2 setup you might come across this error “**The specified SQL Server instance is not configured to use dynamic ports**” unless you have not configured dynamic ports for SQL server instance. To fix this error launch the **SQL Server Configuration Manager**, expand **SQL Server Network Configuration**. Click on **Protocols** for Instance (Instance is your Named Instance). On the right side pane, right click on the **TCP/IP** and click on **Properties**. Click on **IP Addresses** tab and scroll down to the bottom and under the **IPALL**, set **TCP Port** value to **1433**. Click on **Apply** and after this change you must restart **SQL Server Service**.



For Service Accounts, Microsoft recommends you to use domain service accounts and not the local system accounts. We will be using the account named sccmadmin which is a member of domain admins group. This account will be also used for installing and managing Configuration Manager 2012 R2. You can also create a separate user accounts for each of the SQL server services.

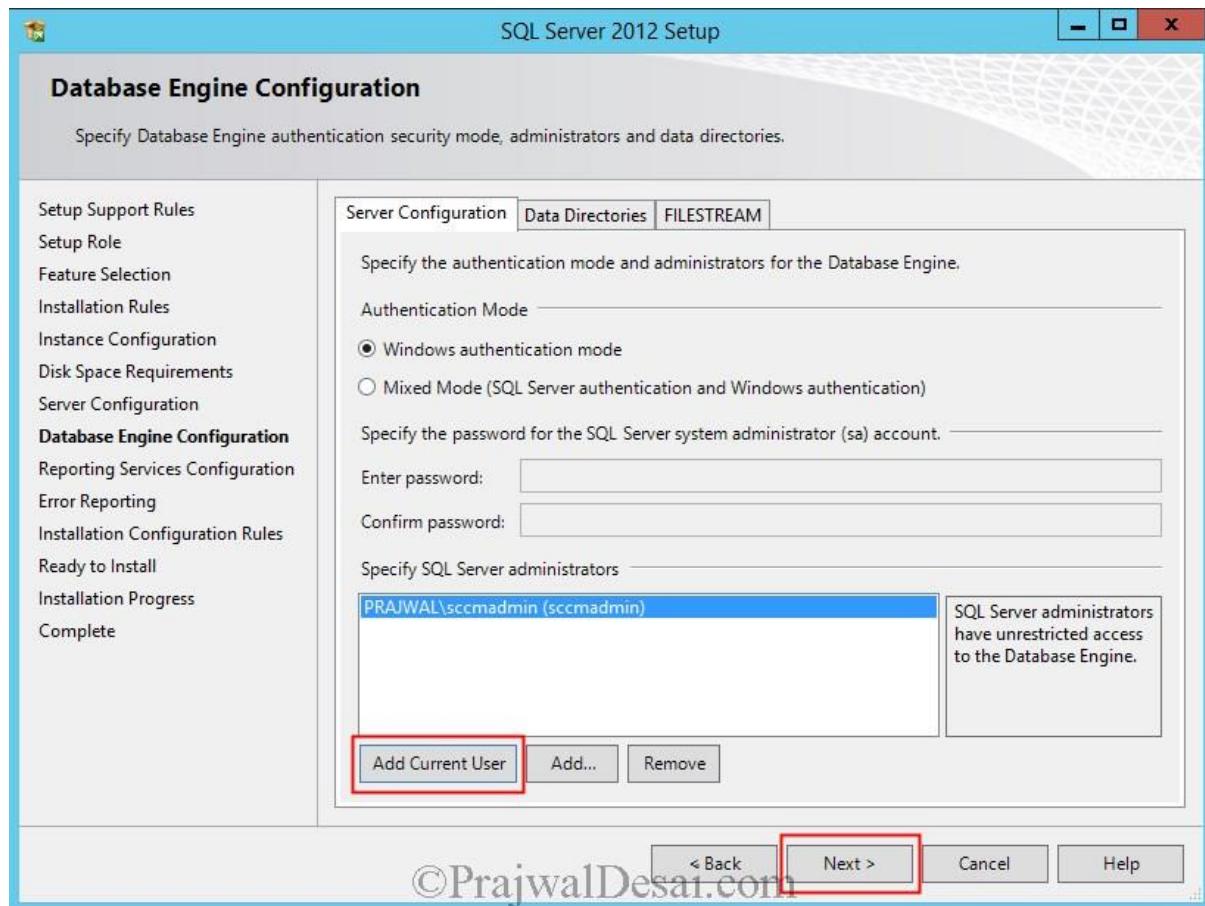
Specify the account name and password and click on **Next**.

Important – During the SQL install, the collation should be SQL_Latin1_General_CI_AS.

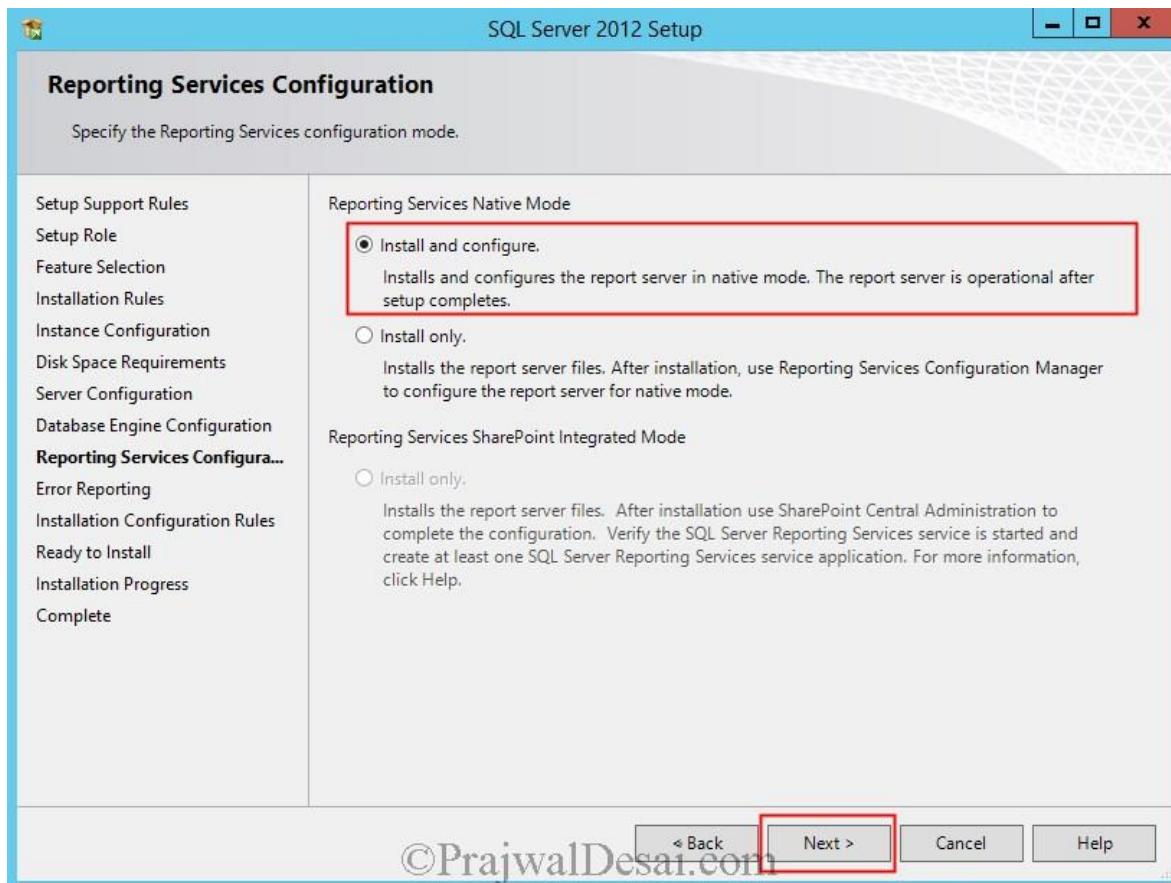


©PrajwalDesai.com

Click **Add Current User**, this will add the current user to SQL server administrators. Choose the **Authentication Mode** as **Windows authentication mode**. Click **Next**.

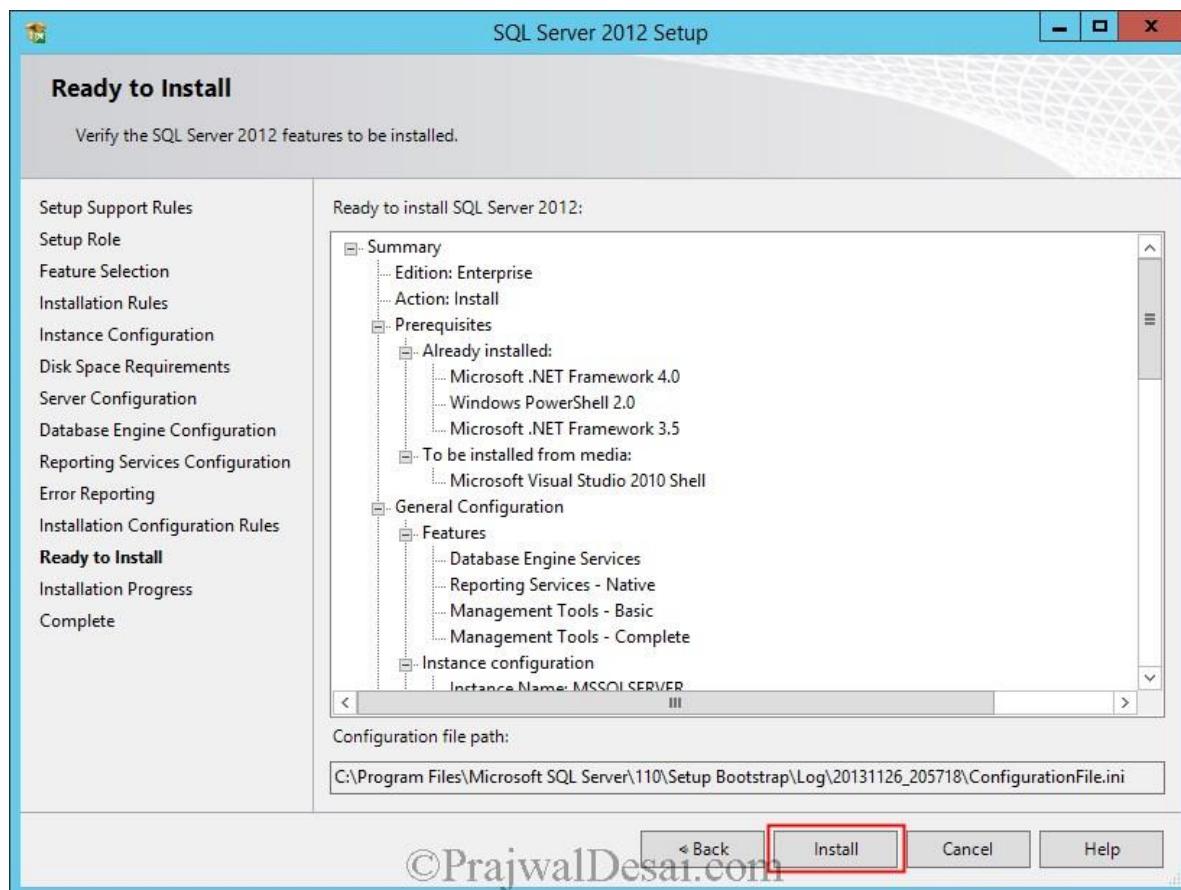


Choose **Reporting Services Native Mode** and click on **Install and Configure**. Click on **Next**.



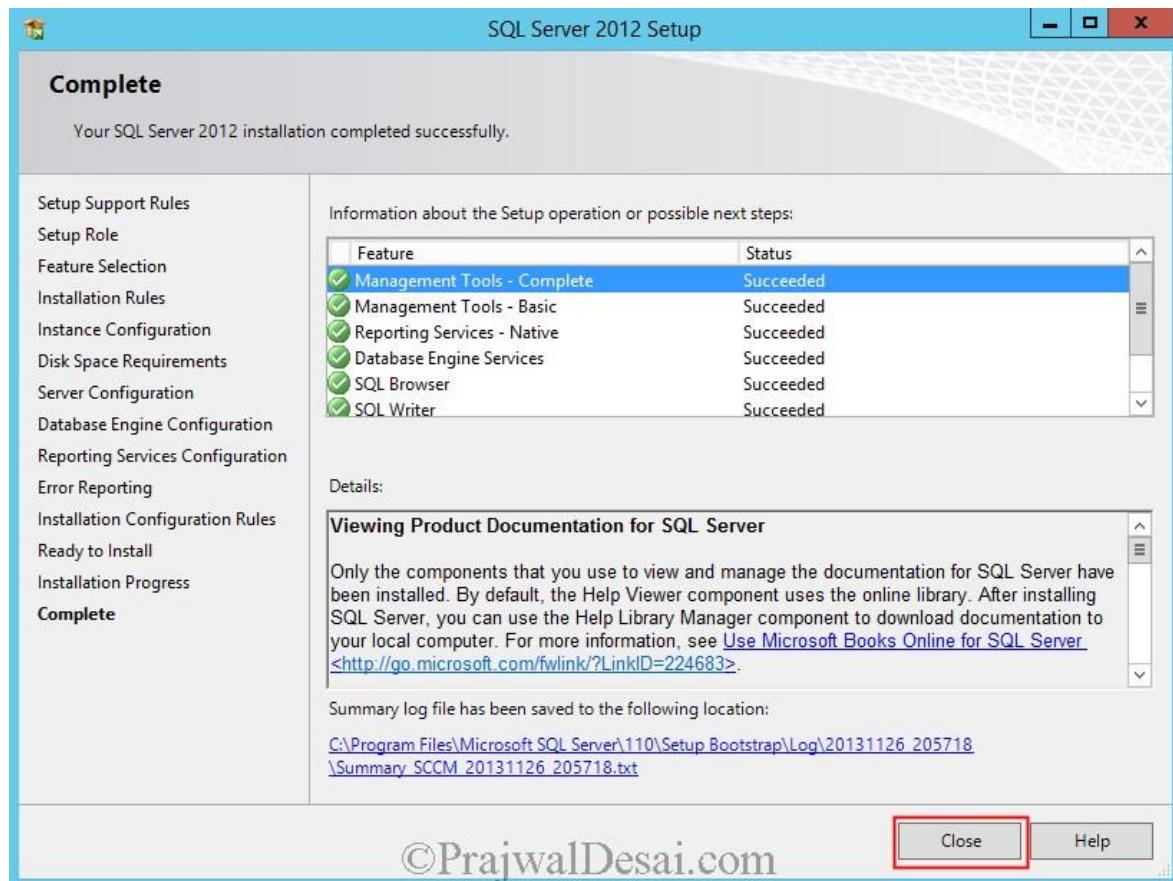
©PrajwalDesai.com

Click on **Install** to start the installation.

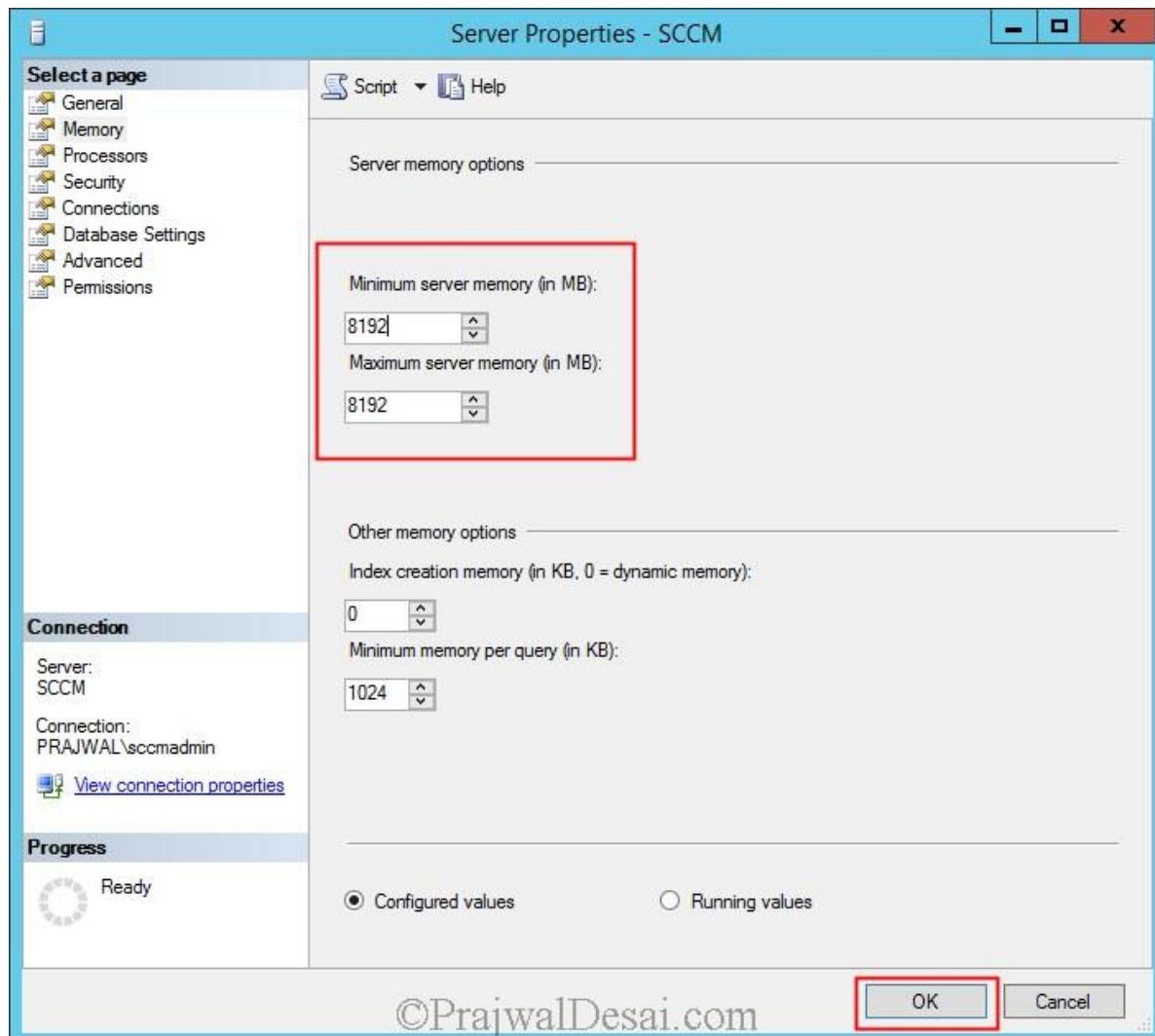


©PrajwalDesai.com

We have installed SQL server 2012 with SP1 on Windows Server 2012 R2 Datacenter Edition. Click on **Close**.



During the installation of Configuration Manager 2012 R2, the configuration manager checks if the SQL server memory limit is limited. If the memory is not limited, then a warning is displayed. To avoid that lets limit our server with a memory limit. Launch the **SQL Server Management Studio**. Login to the server and right click the Server and click on **Properties**. Click on **Memory**, set **Minimum server memory** value to **8192 MB** (The minimum value can be less than 8192 MB) and set **Maximum server memory** as **8192 MB**. Click on OK and close the SQL management studio.

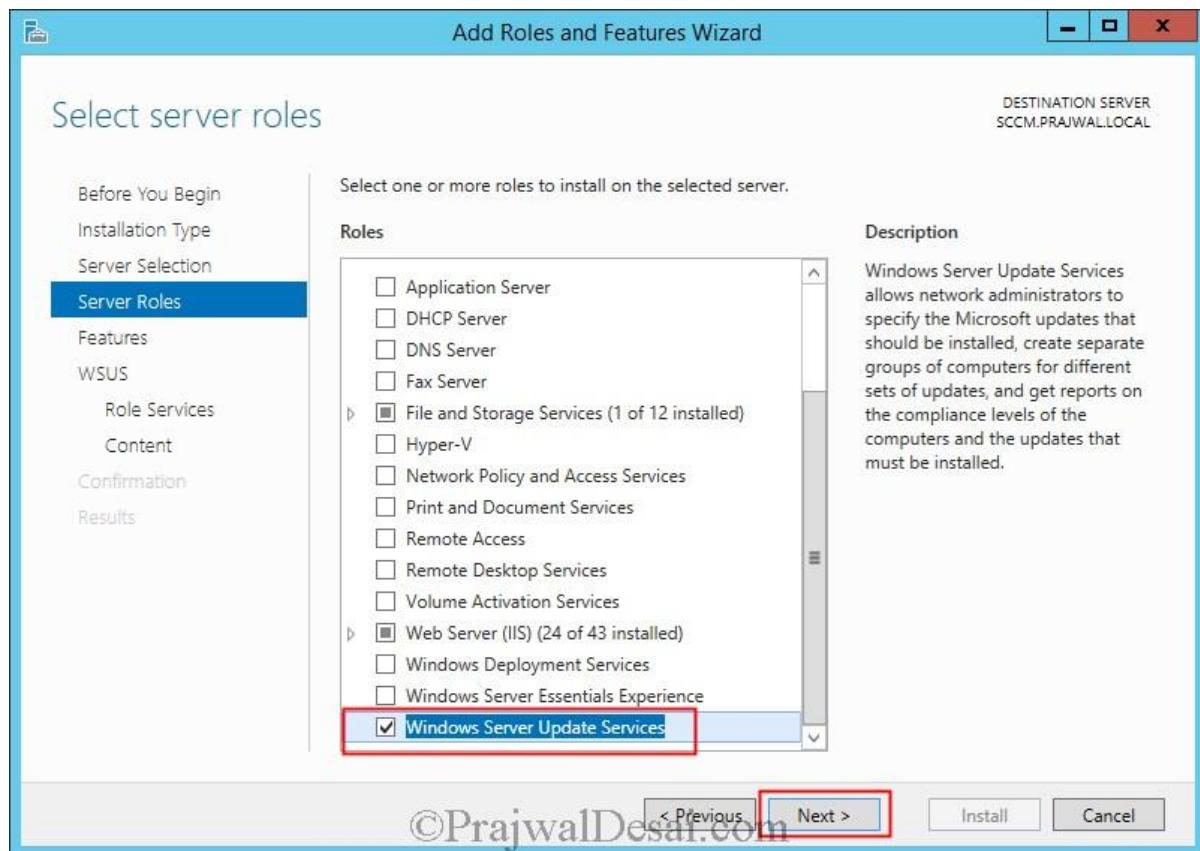


Installing WSUS for Configuration Manager 2012 R2

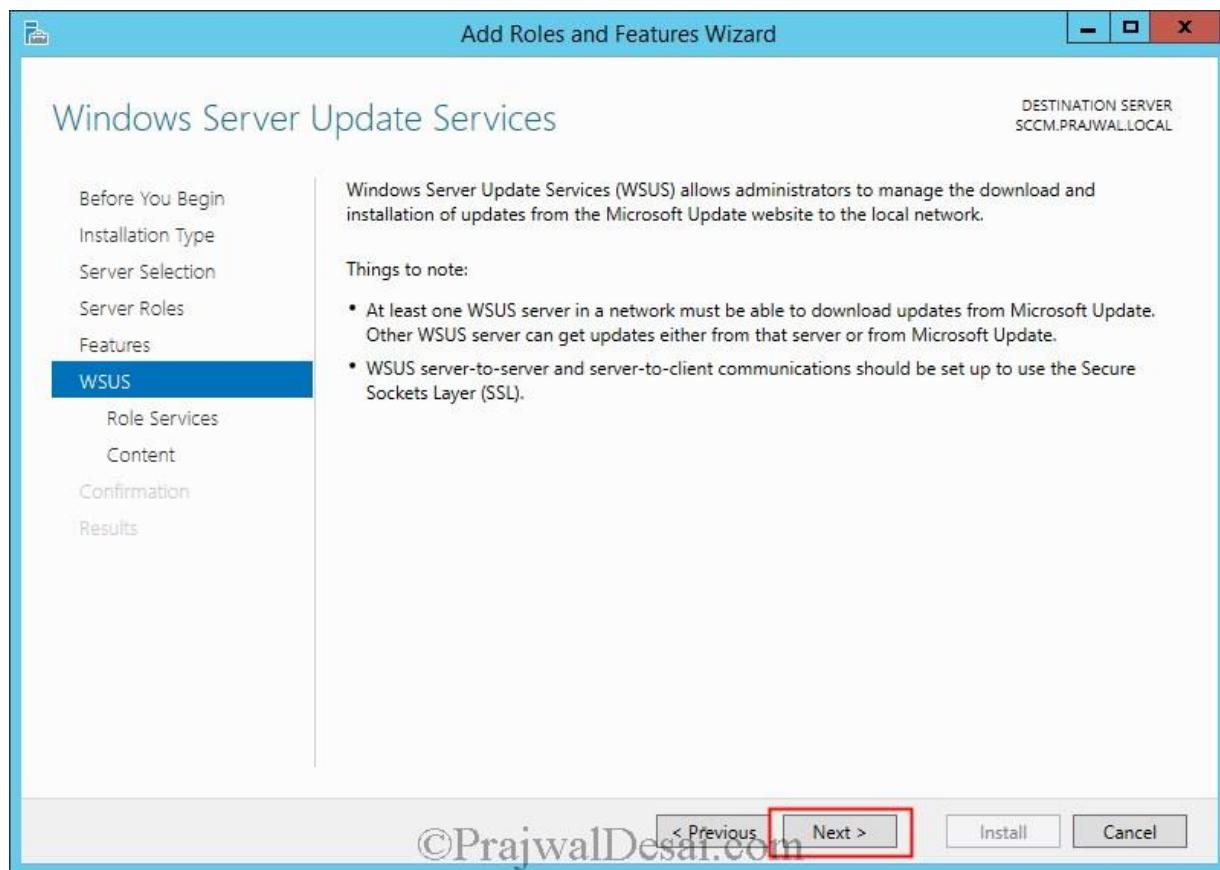
Installing WSUS for Configuration Manager 2012 R2 After installing [SQL server for Configuration Manager 2012 R2](#), we will now see the steps for Installing WSUS for Configuration Manager 2012 R2. WSUS is Microsoft's separate, stand-alone server-based product for distributing updates to Windows systems. WSUS also uses the WUA to scan for patch applicability and subsequently install updates delivered by WSUS. WSUS 3.0 Service Pack 2 is required for System Center 2012 R2 Configuration Manager. SCCM 2012 R2 supports only 64-bit site systems, you must use the 64-bit version of WSUS on one of the supported 64-bit editions of Windows Server. The WSUS 3.0 SP2 is available here:- <http://www.microsoft.com/en-us/download/details.aspx?id=5216>

Installing WSUS for Configuration Manager 2012 R2

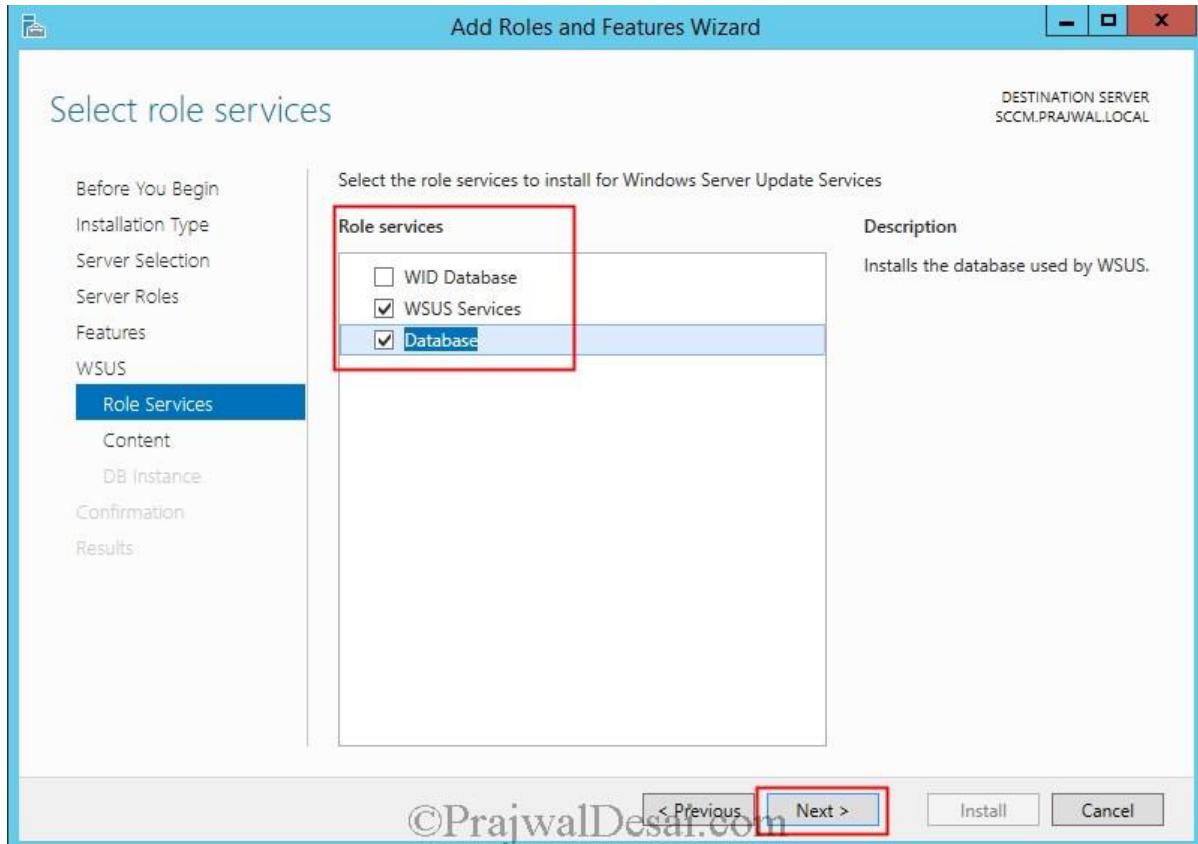
To install WSUS on Windows Server 2012 R2, click on **Server Manager**, click on **Manage**, click **Add Roles and Features**, select **Windows Server Update Services** and click on **Next**.



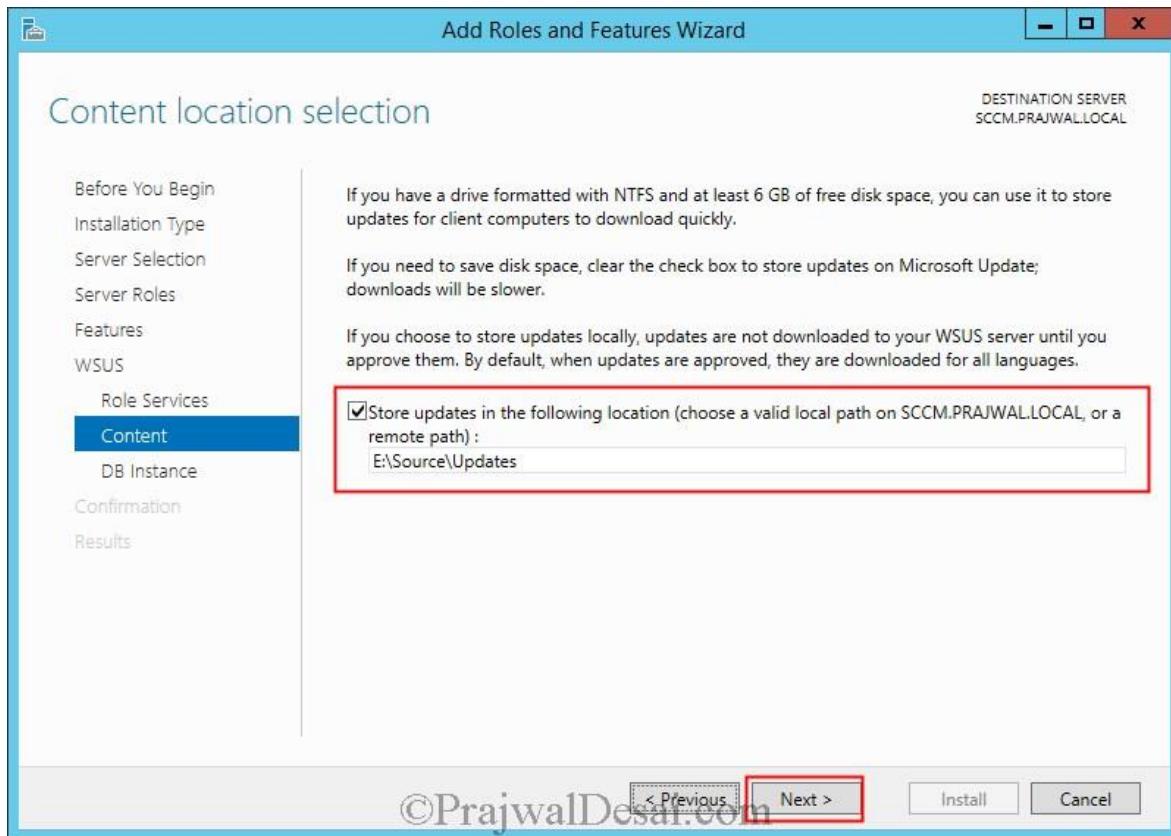
Click Next.



Choose **WSUS Services** and **Database** as these are the ones that are actually required. We will not select WID Database here. Click on **Next**.

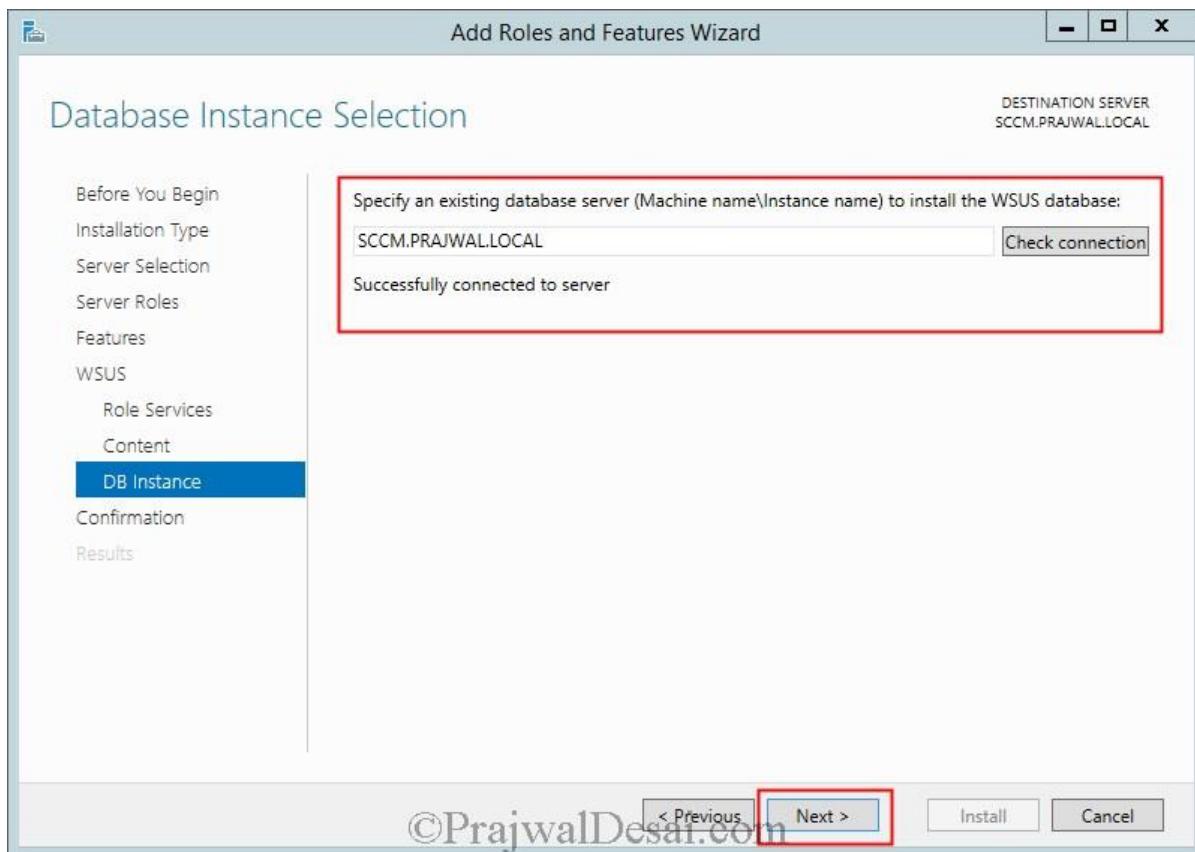


Content Location Selection – In this folder the WSUS downloads and stores license terms for specific software updates in the update content folder. During the update synchronization process, Configuration Manager looks for applicable license terms in the content folder. If it cannot find the license terms, it will not synchronize the update. Provide a folder path and click on **Next**.

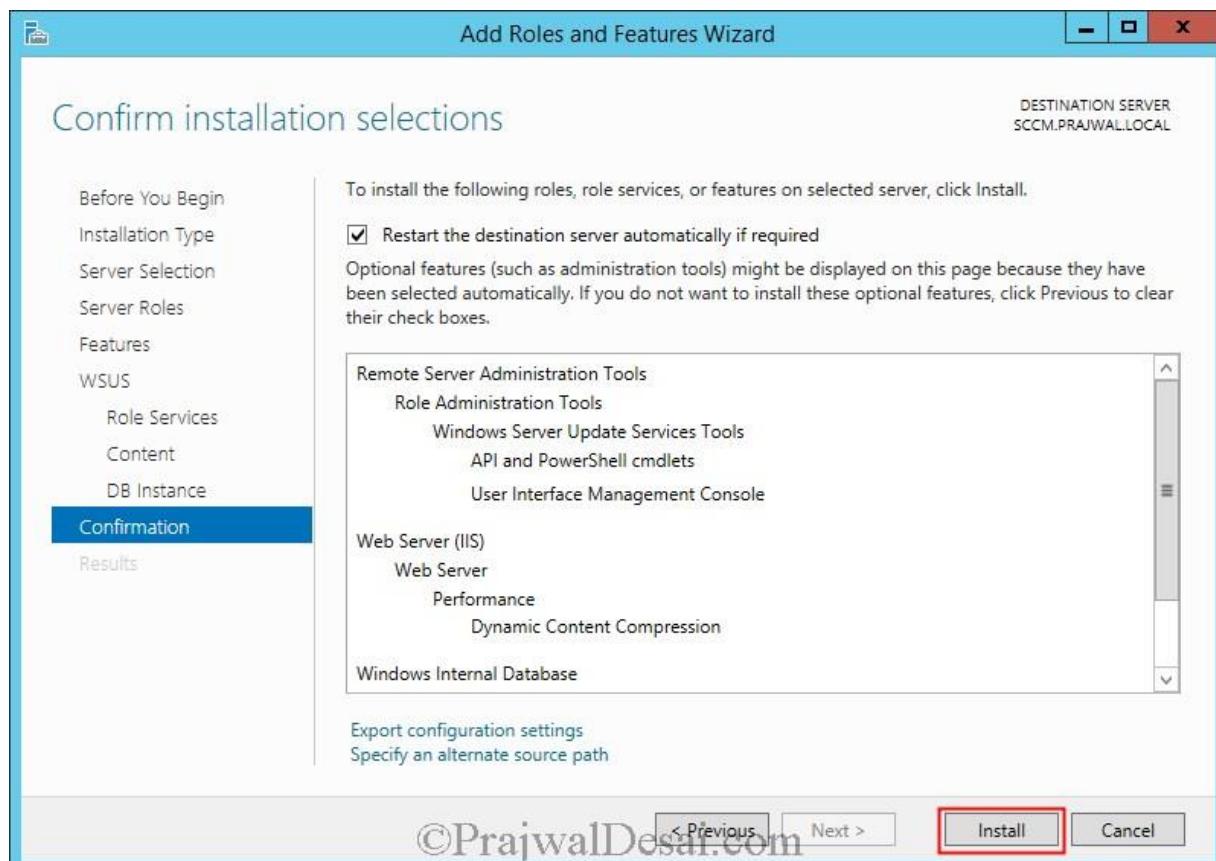


©PrajwalDesai.com

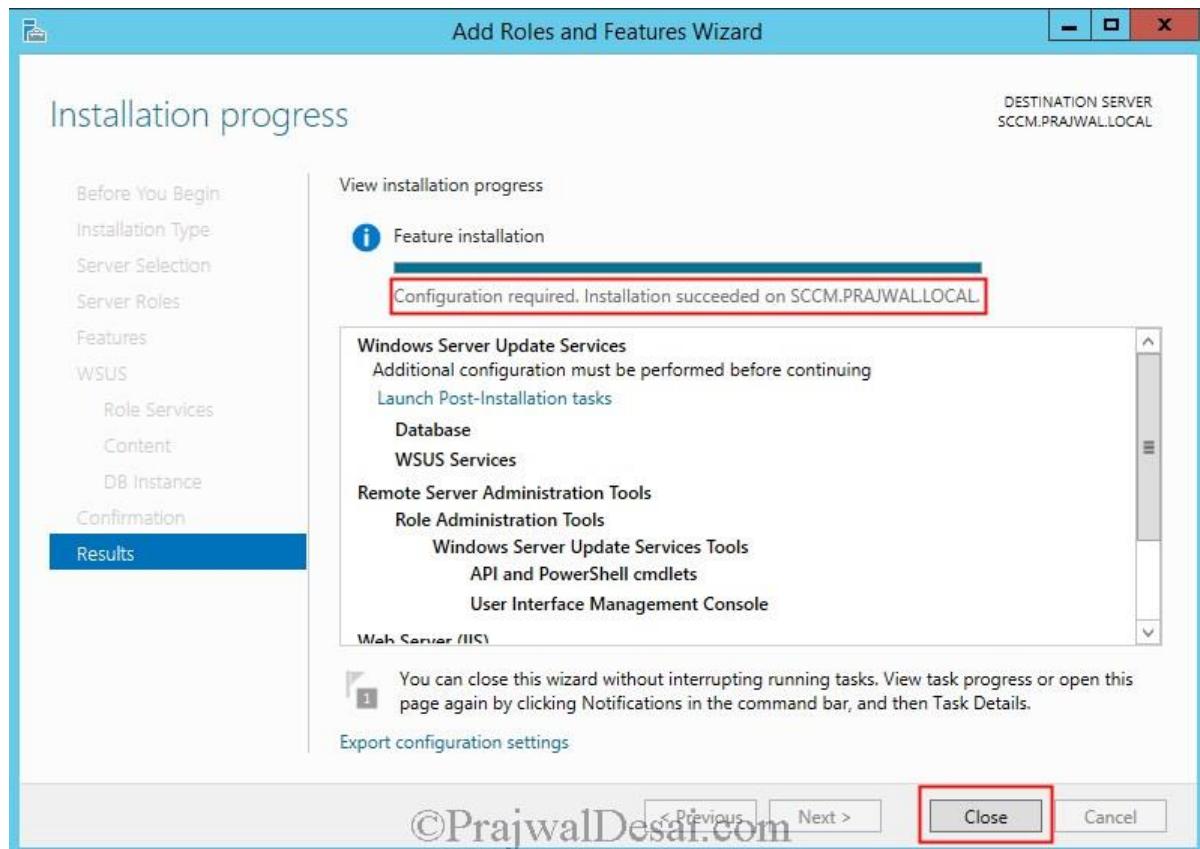
Database Instance Selection – Specify the database server where you want to store the WSUS database. Click on **Check connection** and you must see the message **Successfully connected to server**. Click on **Next**.



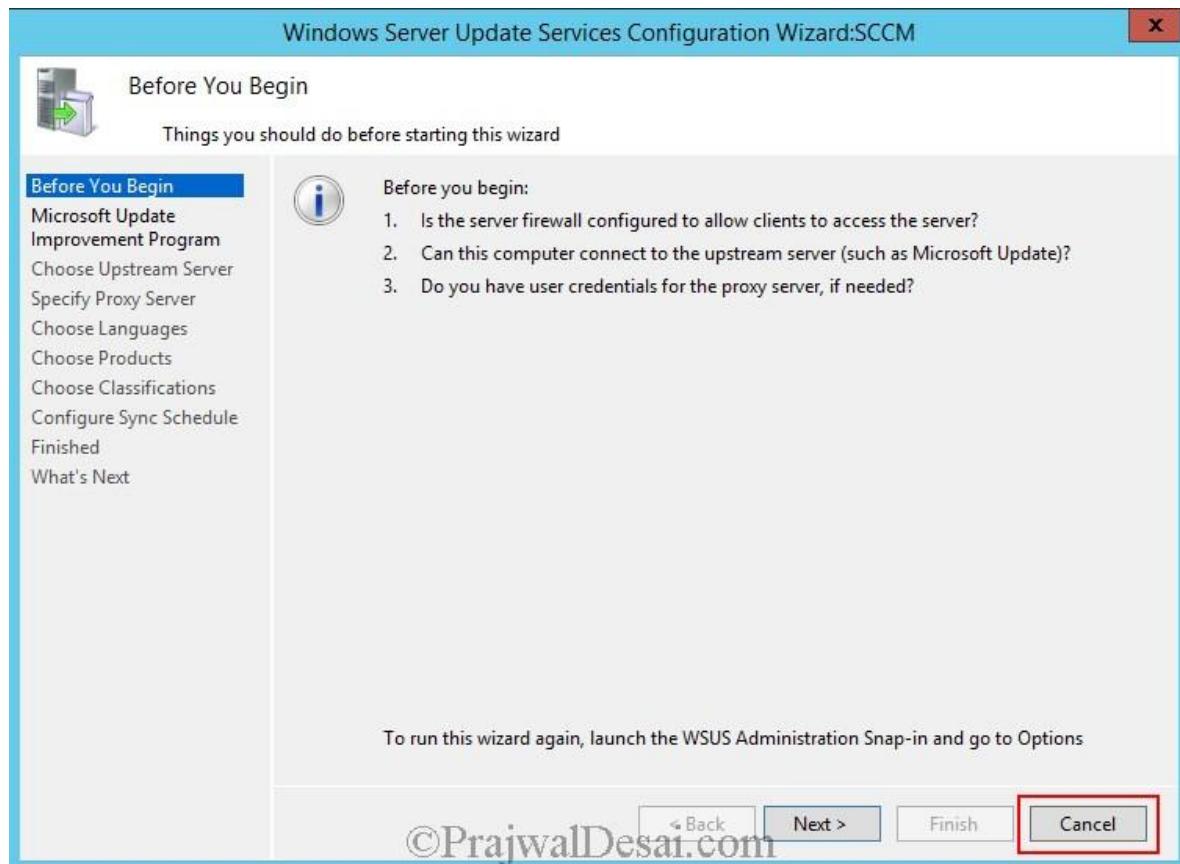
Click on **Install**.



Once the installation is complete **DO NOT** click on **Launch Post-Installation tasks**. Click on **Close**.



We should not configure the WSUS configuration wizard, going forward Configuration Manager must be used to synchronize updates, download updates and deploy updates. It is okay to go into the WSUS console to review updates or the synchronization status, but you should not perform tasks such as approving or declining updates because it can adversely affect Configuration Manager's software update management capabilities. Click on **Cancel** to close the wizard. With this the installation of WSUS for Configuration Manager 2012 R2 is complete.



Configuring Firewall Settings for Configuration Manager 2012 R2

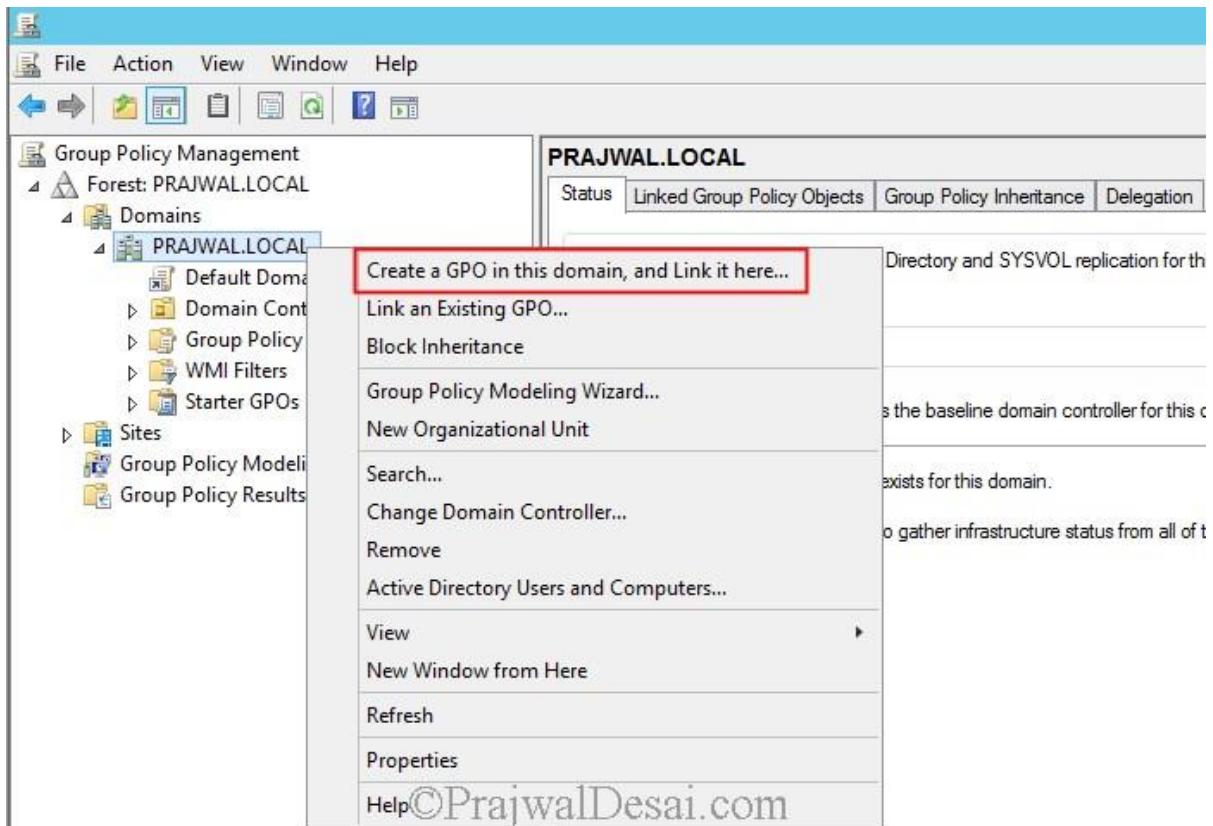
Configuring Firewall Settings For Configuration Manager 2012 R2 In this post we will look at the steps for configuring firewall settings for configuration manager 2012 R2.

System Center 2012 R2 Configuration Manager is a distributed client/server system. The distributed nature of Configuration Manager means that connections can be established between site servers, site systems, and clients. Some connections use ports that are not configurable, and some support custom ports you specify. You must verify that the required ports are available if you use any port filtering technology such as firewalls, routers, proxy servers, and IPsec. To know more about ports used by configuration manager 2012 R2 click [here](#).

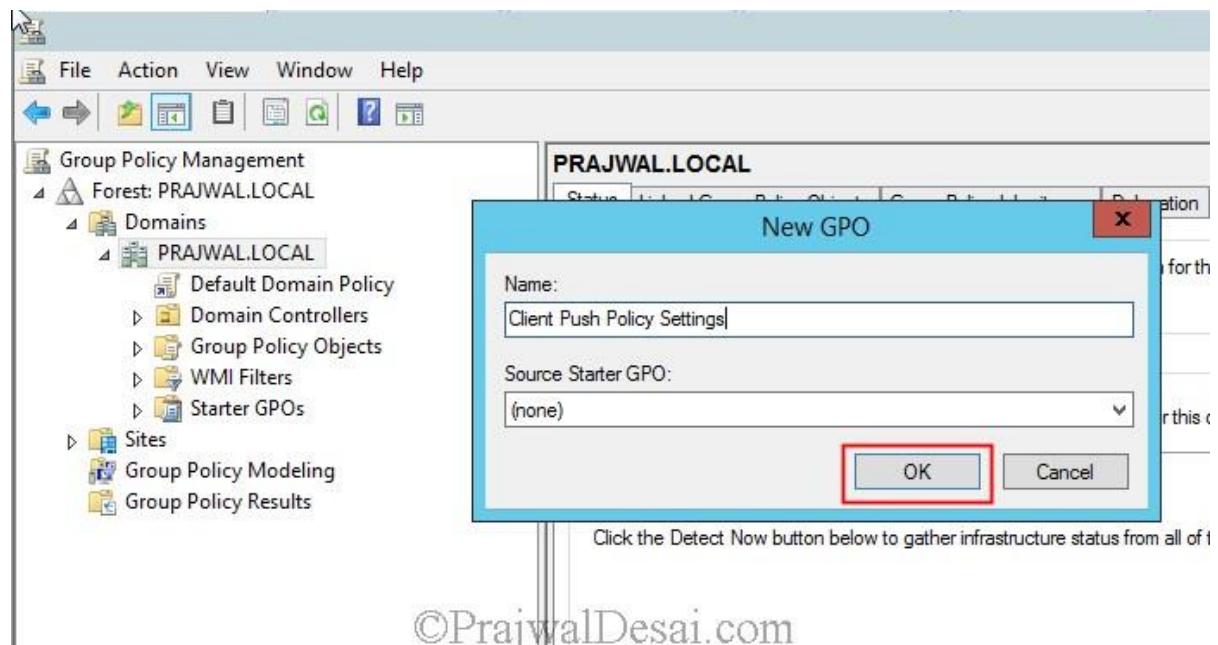
Note – In order to successfully use client push to install the Configuration Manager 2012 R2 client, you must add the following as exceptions to the Windows Firewall. If there is a firewall between the site system servers and the client computer, confirm whether the firewall permits traffic for the ports that are required for the client installation. 1) File and Printer Sharing 2) Windows Management Instrumentation (WMI).

Configuring Firewall Settings For Configuration Manager 2012 R2

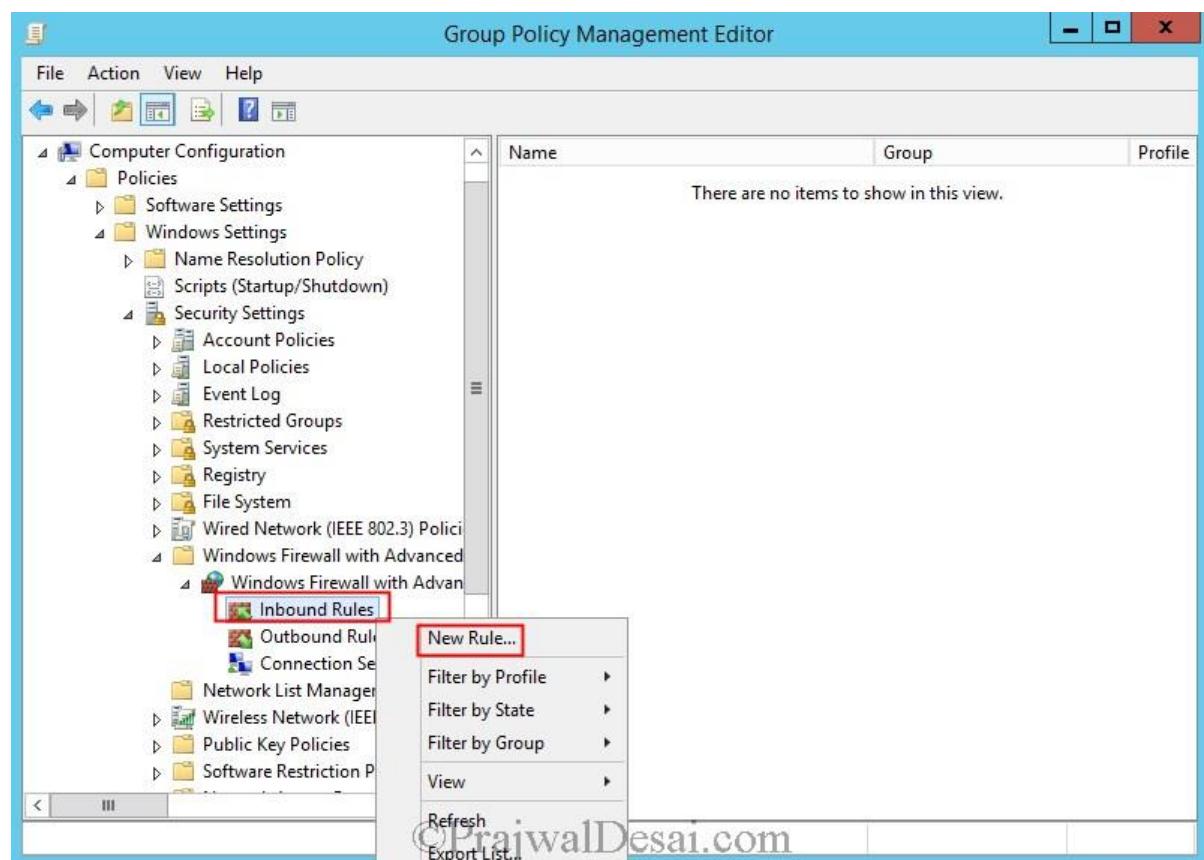
We will create an **inbound** and **outbound** rule, add **File and Printer sharing service** as exception to firewall and an **Inbound rule** to allow WMI. We will perform this activity on the Domain Controller. Click on **Server Manager**, click on **Tools**, open **Group policy management console**. Right Click on the domain and Create a **GPO**.



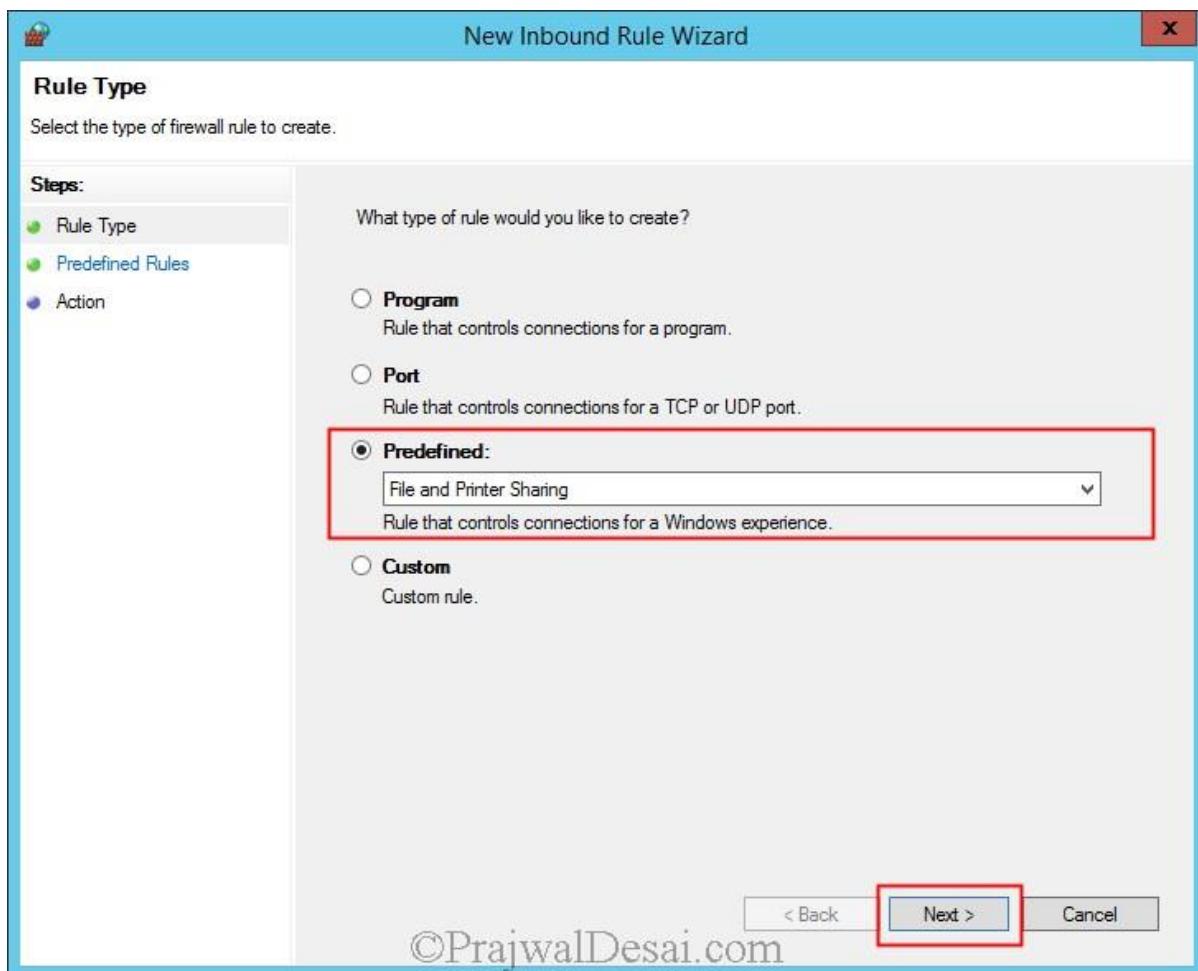
Provide a name to the GPO and click on **OK**.



Right click on the policy that you created and click on **Edit**. **Expand computer configuration, Windows settings, Security settings, Windows Firewall with advanced security**. Right click on **Inbound rules** and click on **New Rule...**

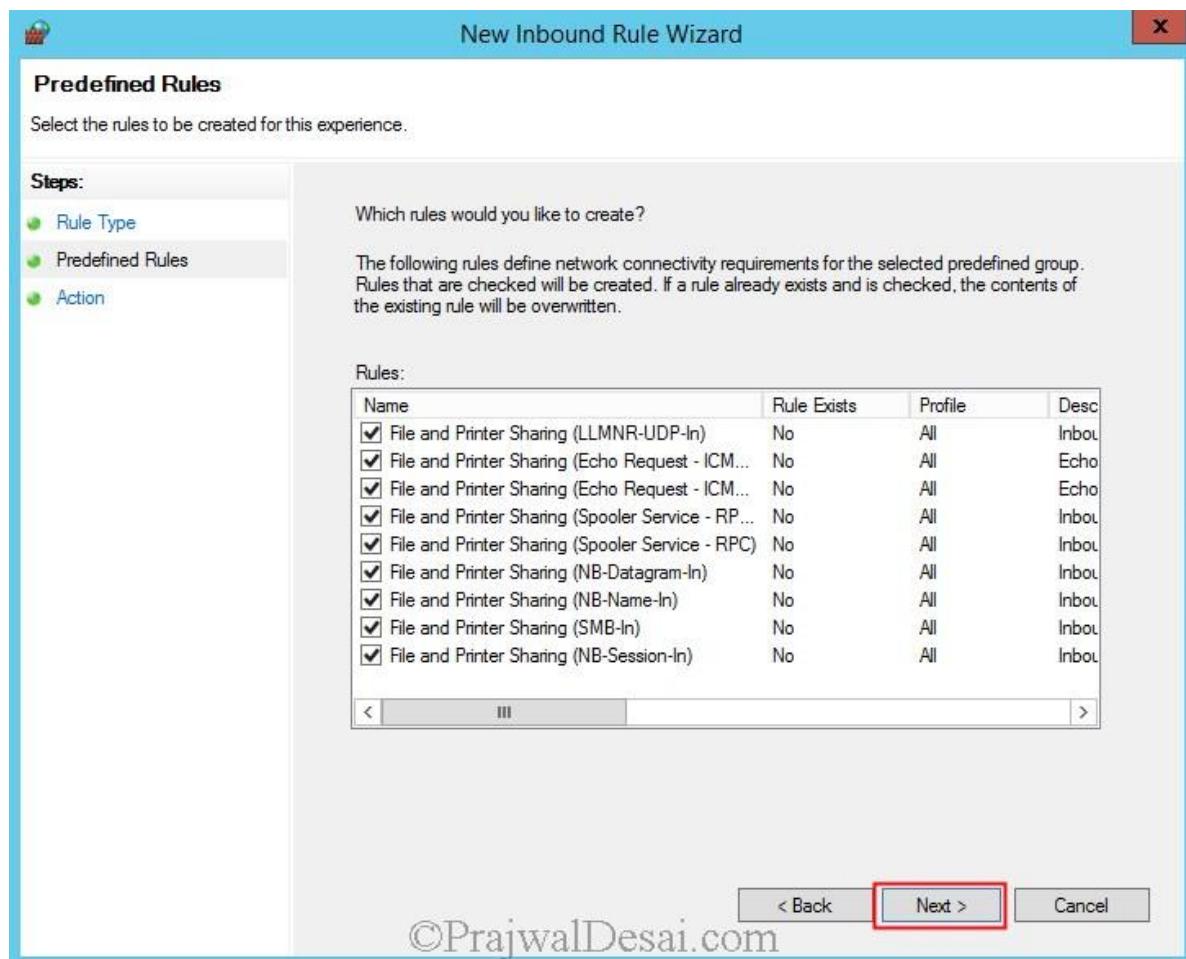


Click on **Predefined** and select **File and Printer Sharing**. Click on **Next**.



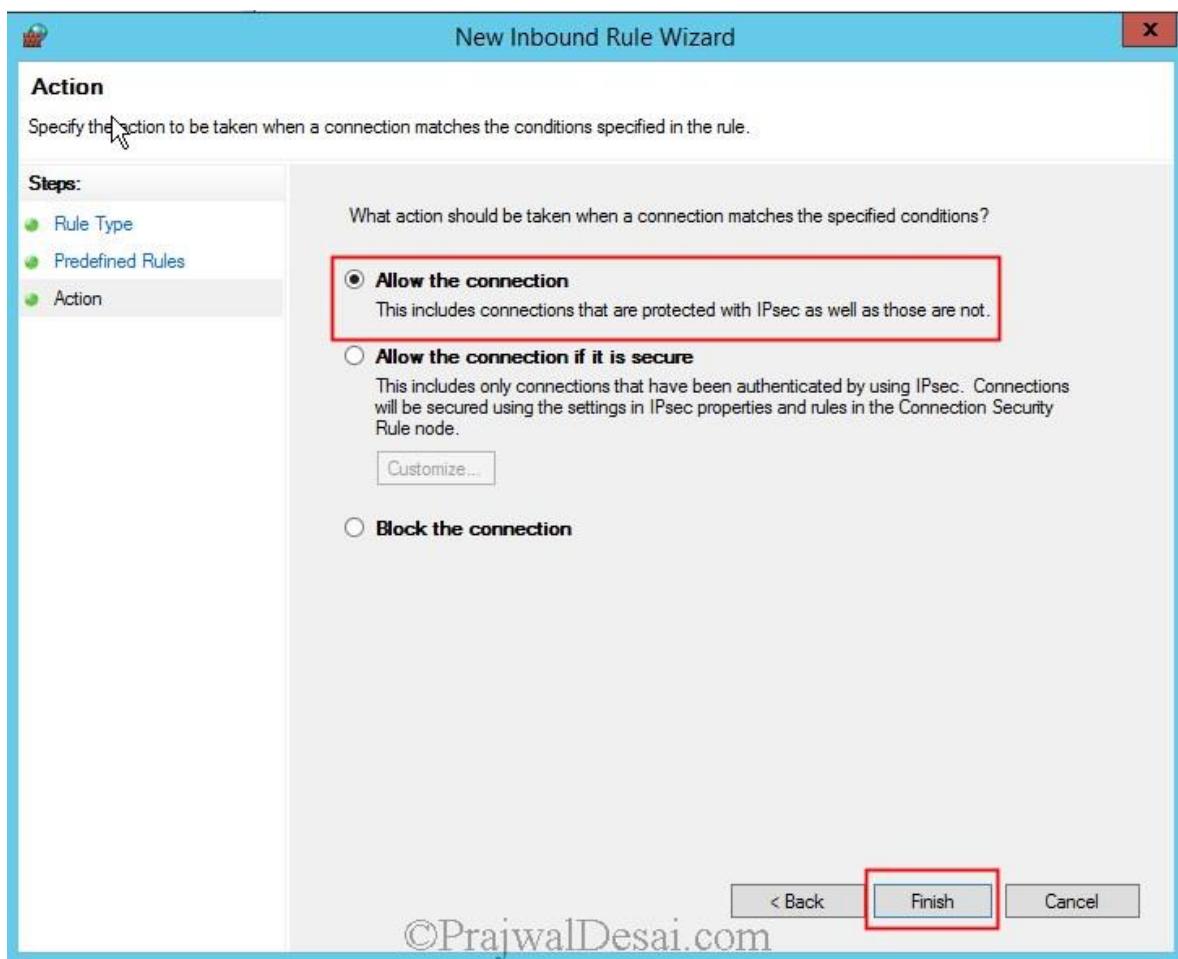
©PrajwalDesai.com

Don't change anything here, click on **Next**.



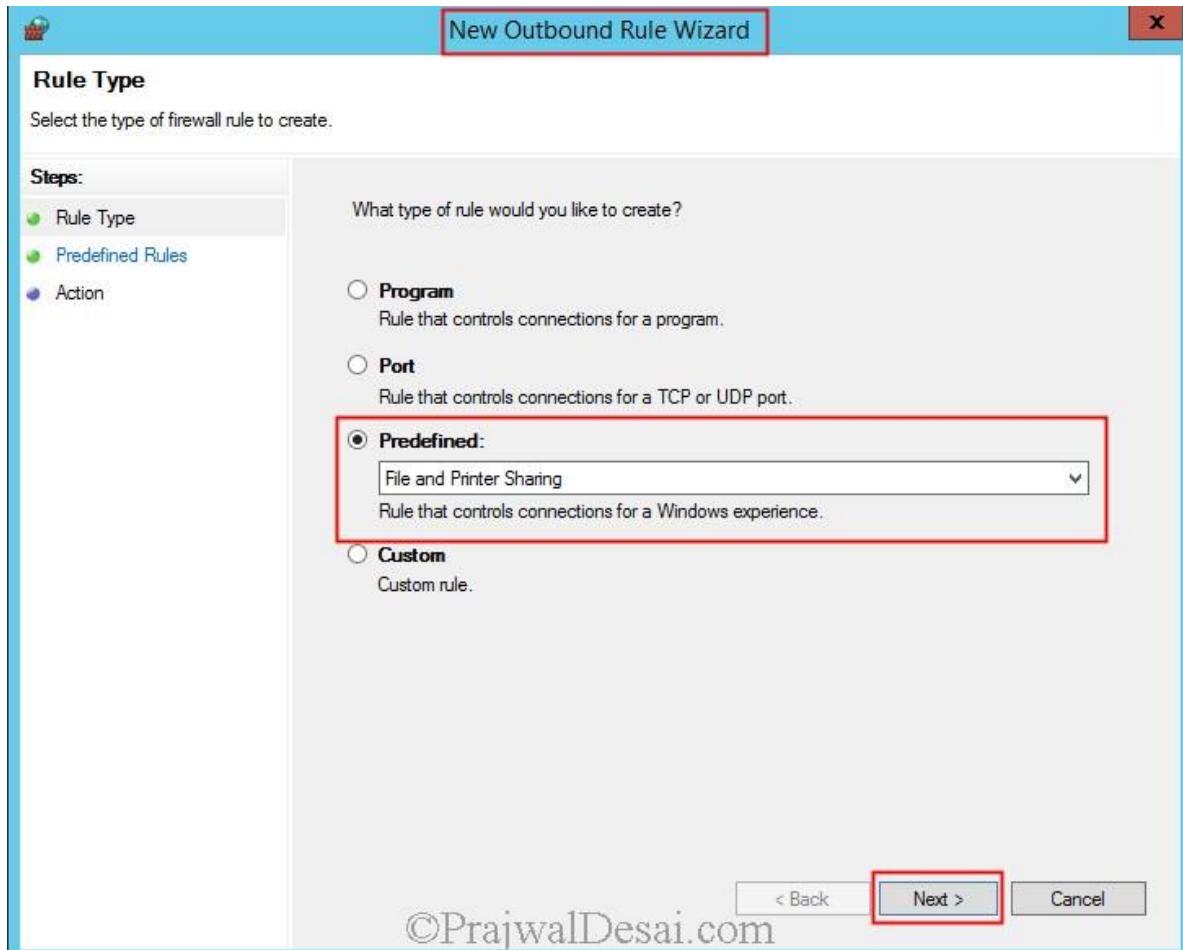
©PrajwalDesai.com

Click on **Allow the connection**. Click **Finish**.



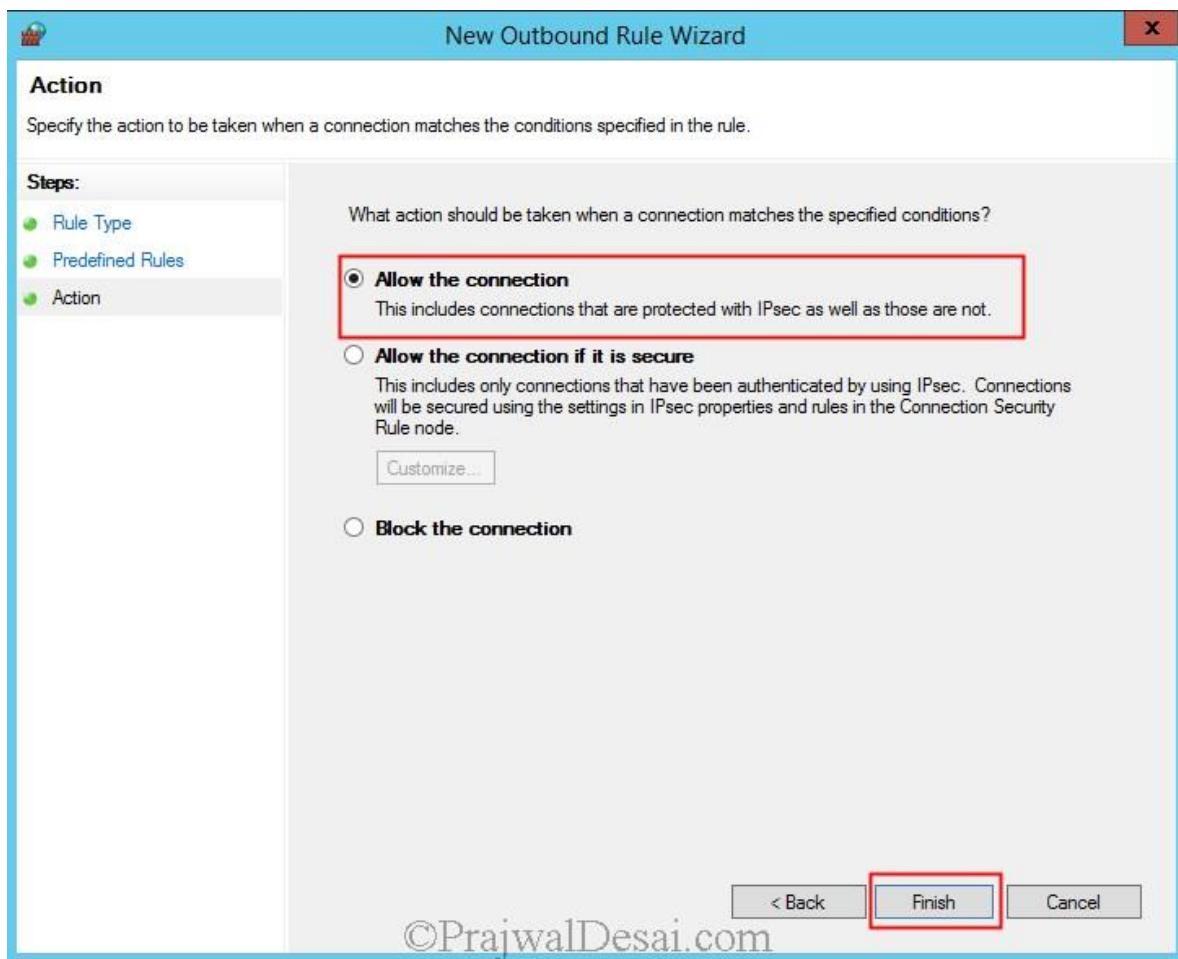
©PrajwalDesai.com

Now we will create an outbound rule to allow **File and Printer sharing**. Right click on the **Outbound Rule** and click on **New Rule**. Choose **Predefined** and select **File and Printer Sharing**. Click on **Next**.



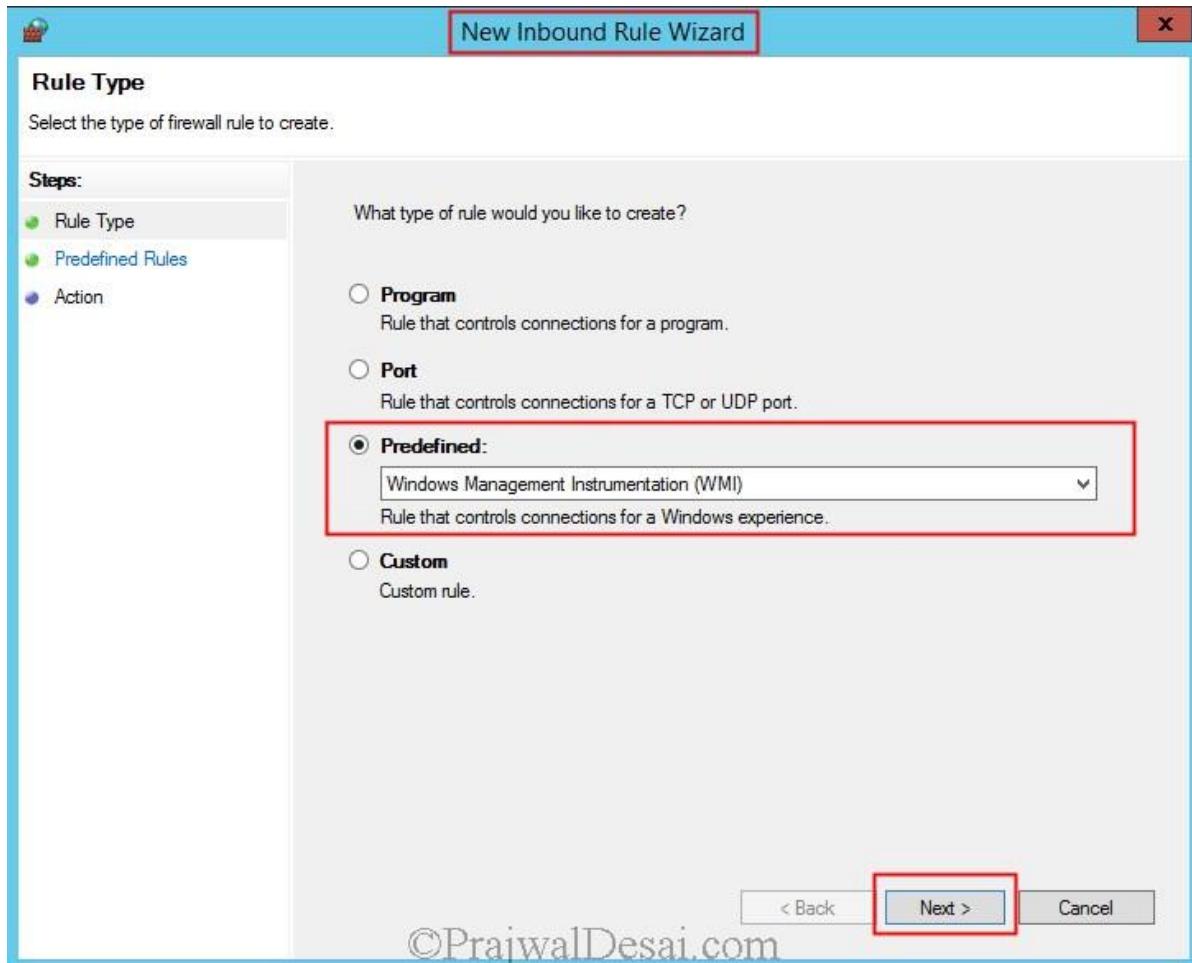
©PrajwalDesai.com

Click on **Allow the connection**. Click **Finish**.

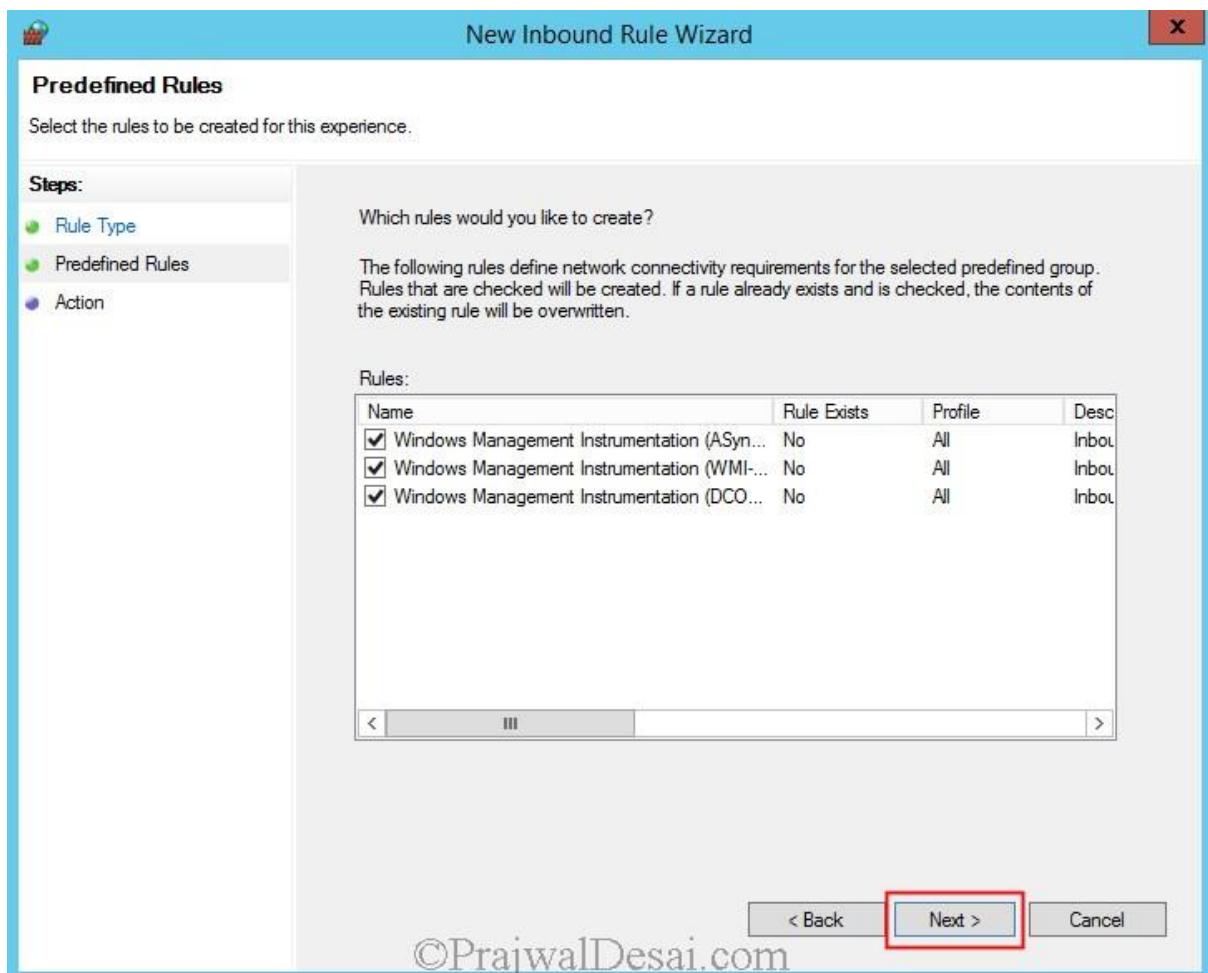


©PrajwalDesai.com

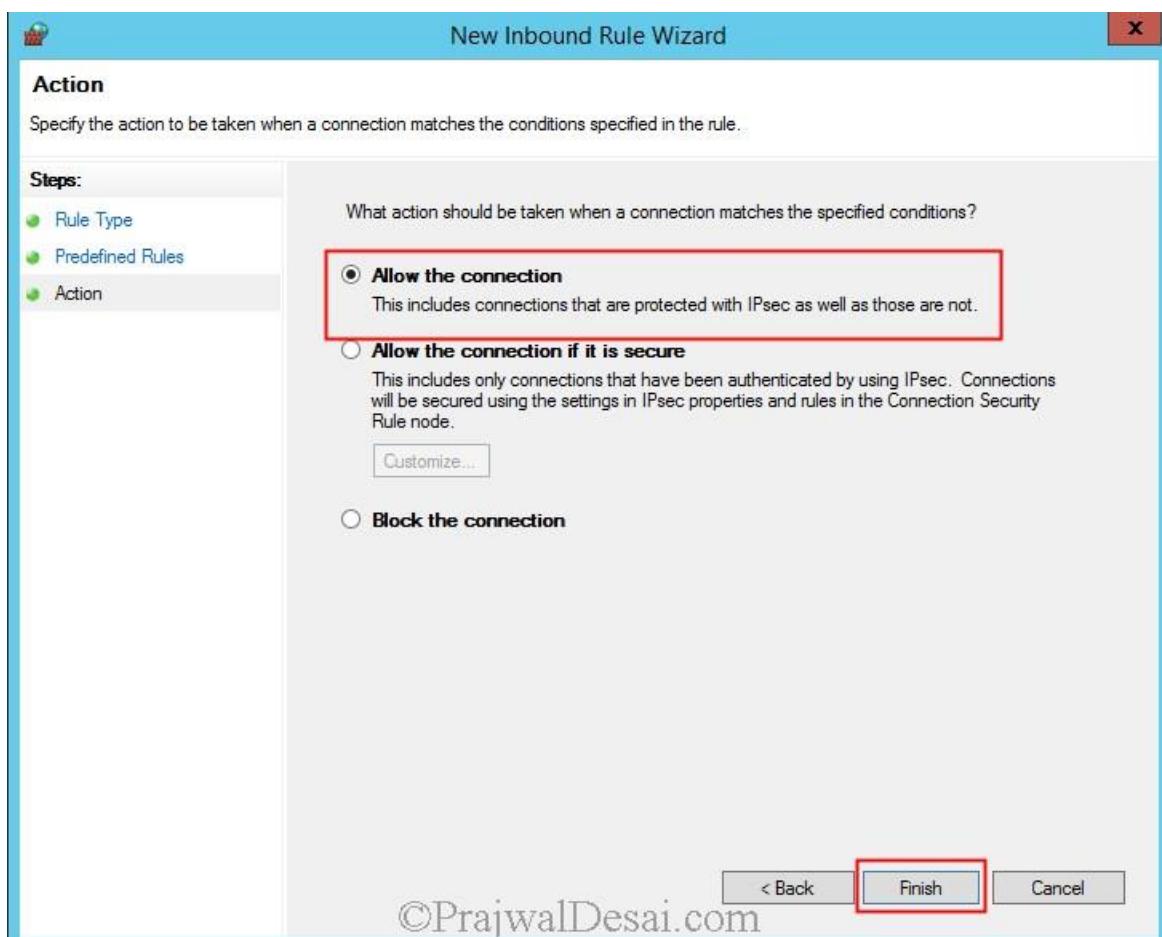
Now we will create an **Inbound Rule** to allow the **WMI** service on our Firewall. So right click on **Inbound Rule** and click on **New Rule**. Click on **Predefined** and select **Windows Management Instrumentation (WMI)**. Click on **Next**.



Click Next.



Choose **Allow the connection** and click **Finish**.



Opening Ports for SQL Replication

We will now see the steps to open the ports for SQL Replication. **Please note that Configuration Manager does not support dynamic ports.** Because SQL Server named instances by default use dynamic ports for connections to the database engine, when you use a named instance, you must manually configure the static port that you want to use for intrasite communication. This point has been discussed while [installing SQL server for configuration manager 2012 R2](#).

Why should the ports 1433 and 4022 opened on Firewall ??

Port 1433 – SQL Server listens for incoming connections on a particular port. The default port for SQL Server is 1433. It applies to routine connections to the default installation of the Database Engine, or a named instance that is the only instance running on the computer.

Port 4022 – This is SQL Service Broker, though there is no default port for SQL Server Service Broker, but this is the port that we allow inbound on our firewall.

Site System roles that communicate directly with the SQL Server database

Application Catalog web service point

Certificate registration point role

Enrollment point role

Management point

Site server

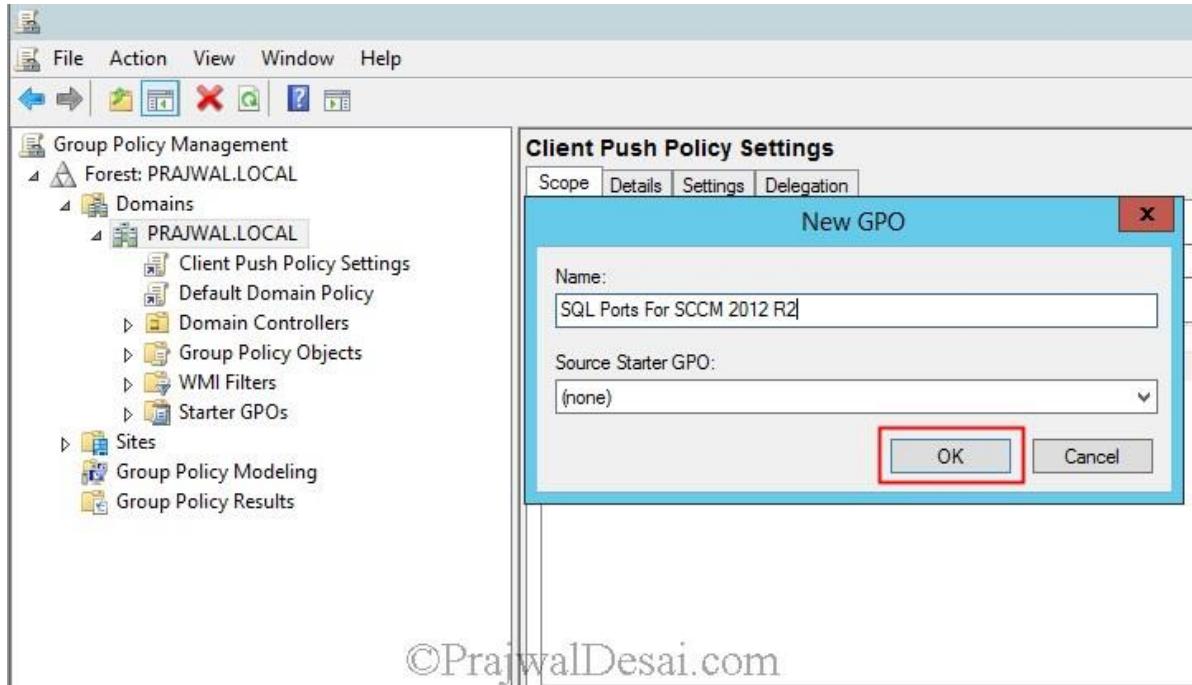
Reporting services point

SMS Provider

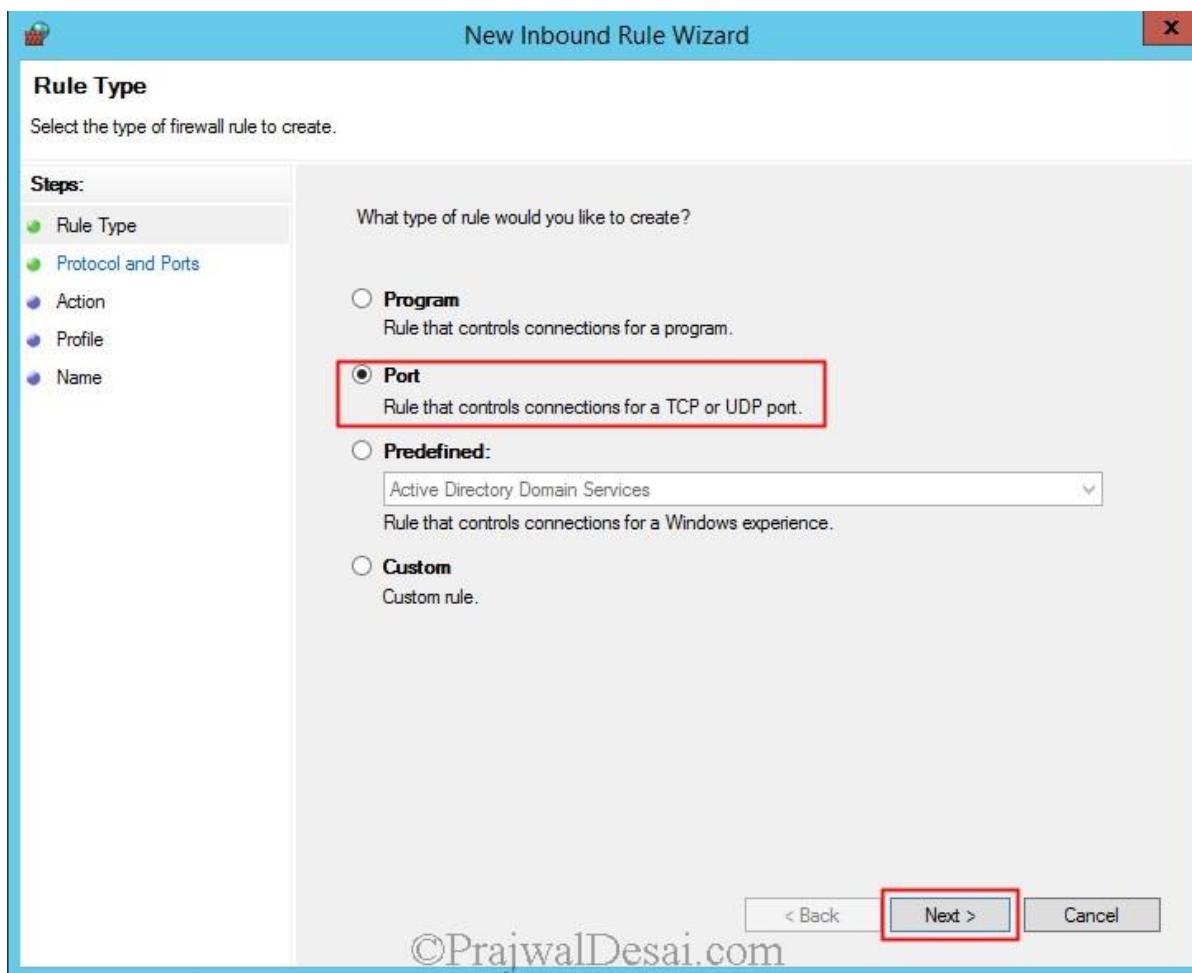
SQL Server to SQL Server

By default, Microsoft Windows enables the Windows Firewall, which closes port 1433 to prevent Internet computers from connecting to a default instance of SQL Server on your computer. Connections to the default instance using TCP/IP are not possible unless you reopen port 1433. We will now create a group policy to open TCP ports **1433** and **4022**.

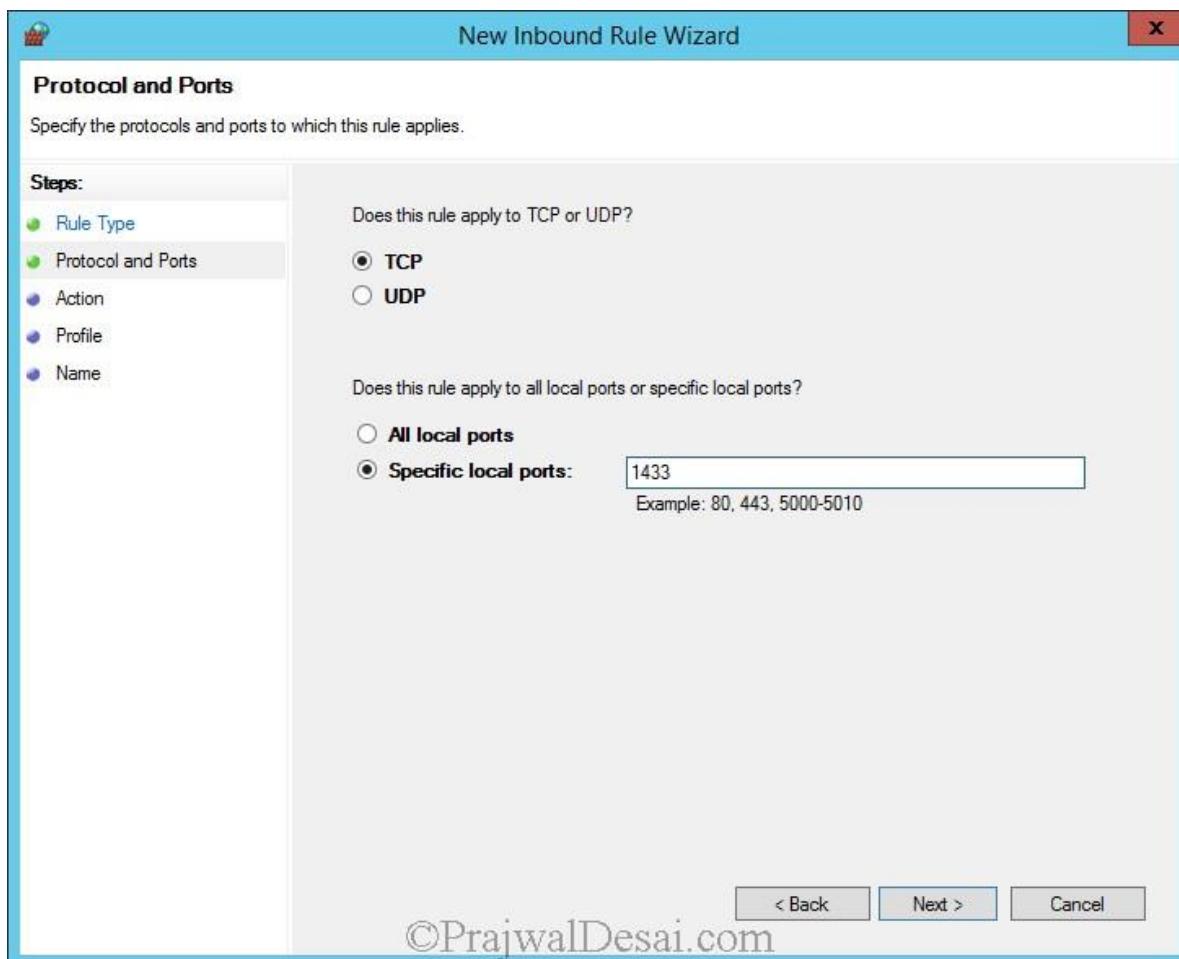
Open the **Group Policy Management console**. Create a new policy and provide a name for the policy. Right Click the policy and edit it.



In the Windows GP management console, expand **computer configuration**, **Windows settings**, **Security settings**, **Windows firewall with advanced security**. Right click on **Inbound Rule** and create an **Inbound Rule** and select **Port**. Click on **Next**.

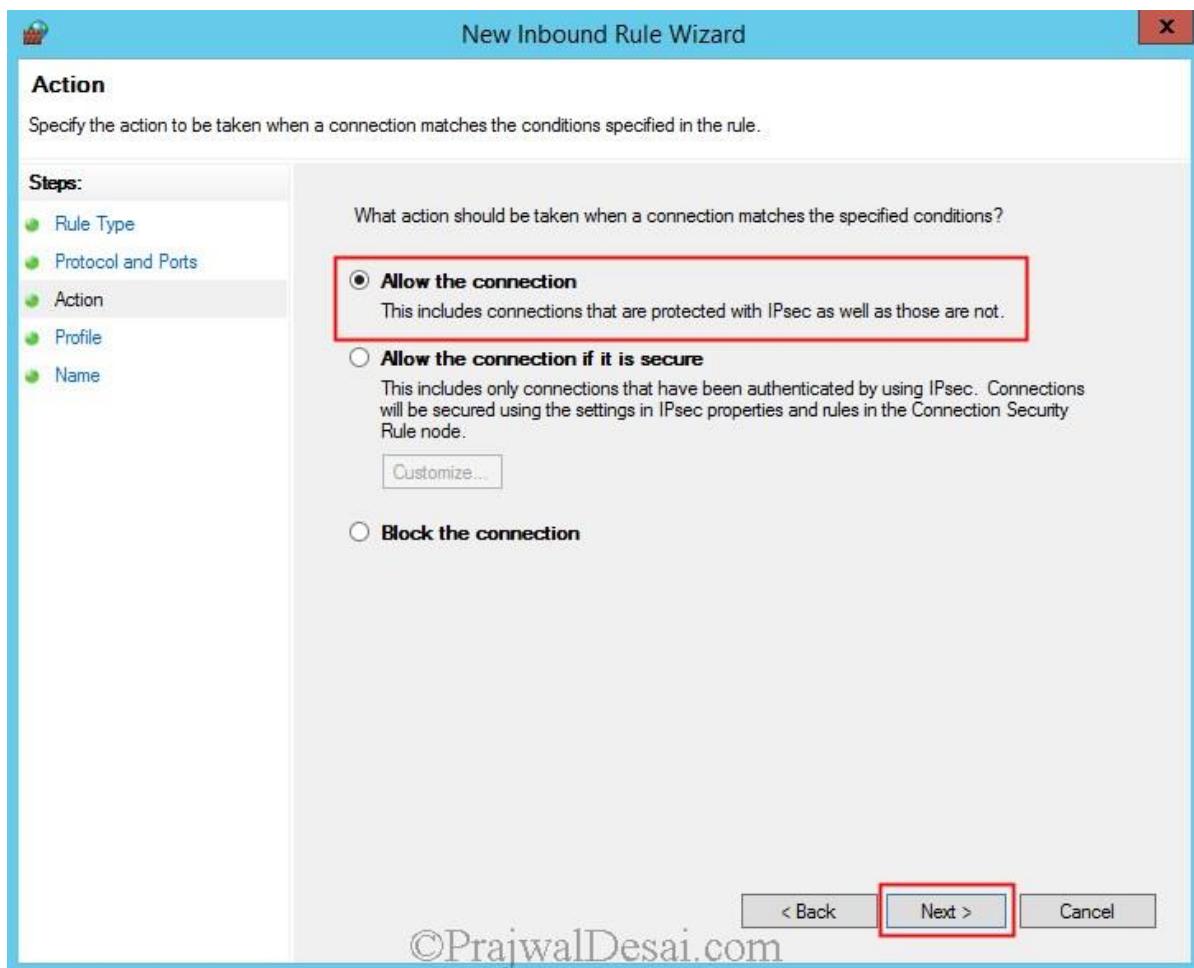


Select **TCP**, and specify port **1433** in **specific local ports**. Click **Next**.



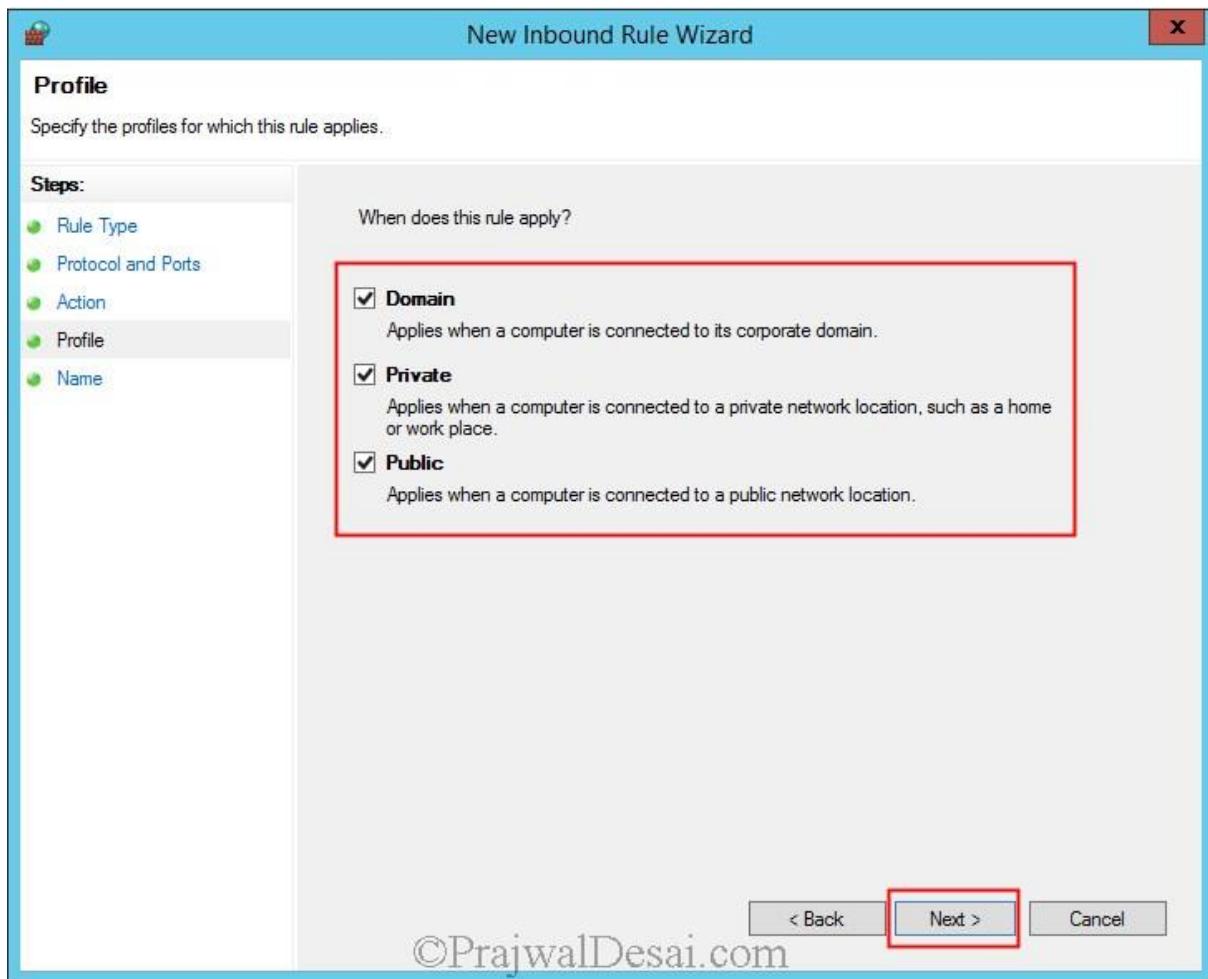
©PrajwalDesai.com

Click on **Allow connection** and click on **Next**.

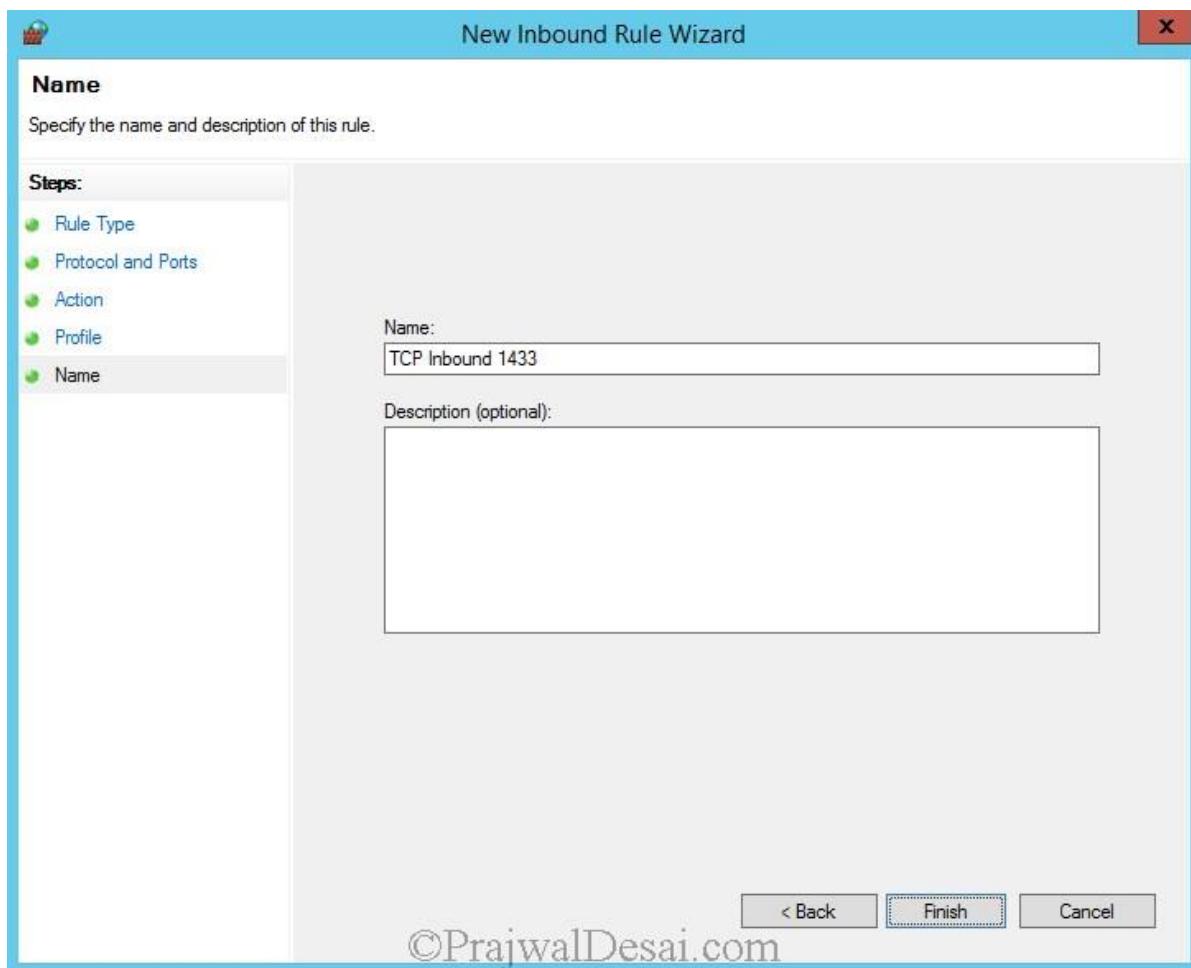


©PrajwalDesai.com

The firewall rule will be applied for all the 3 profiles. Click on **Next**.

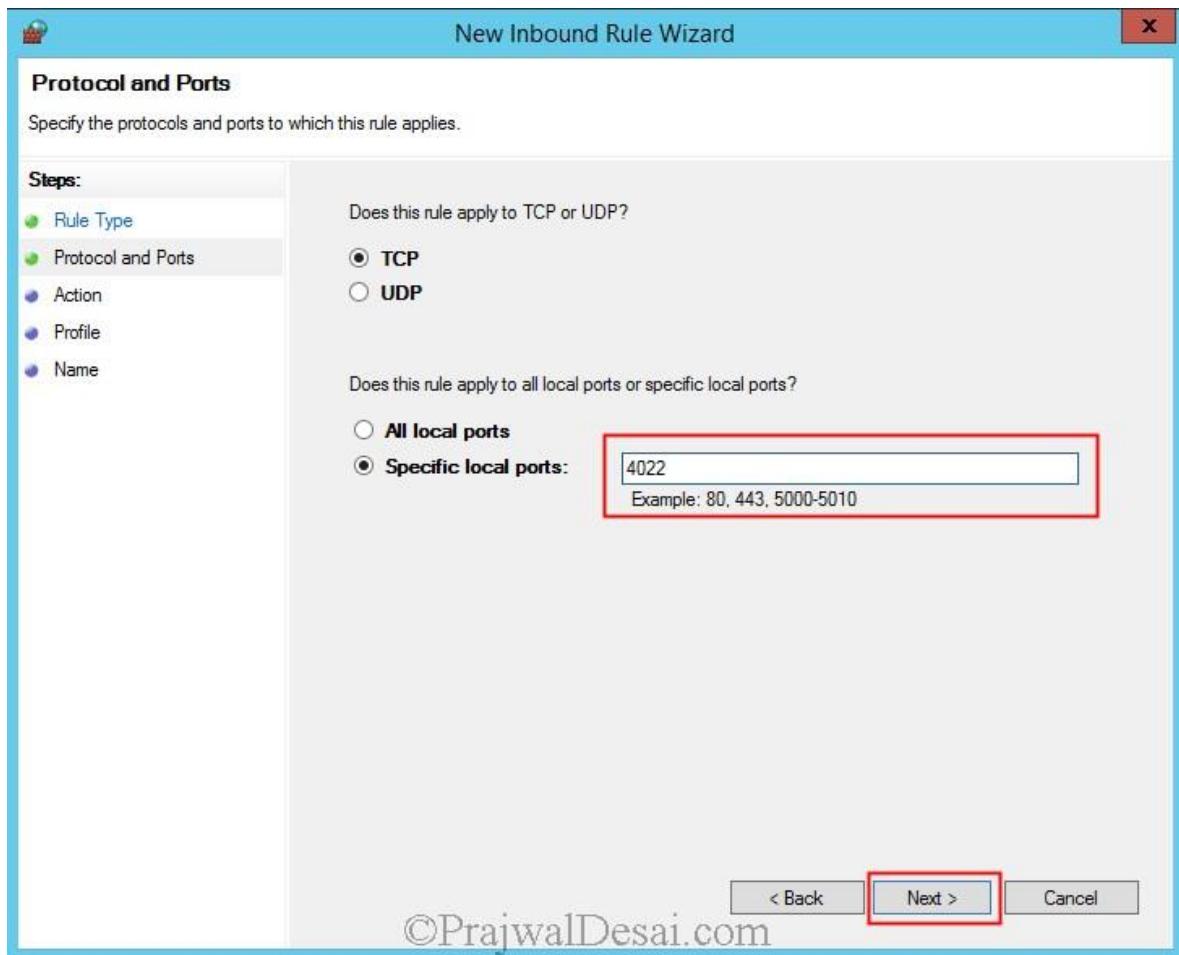


Name the rule as **TCP Inbound 1433**. Click on **Finish**.



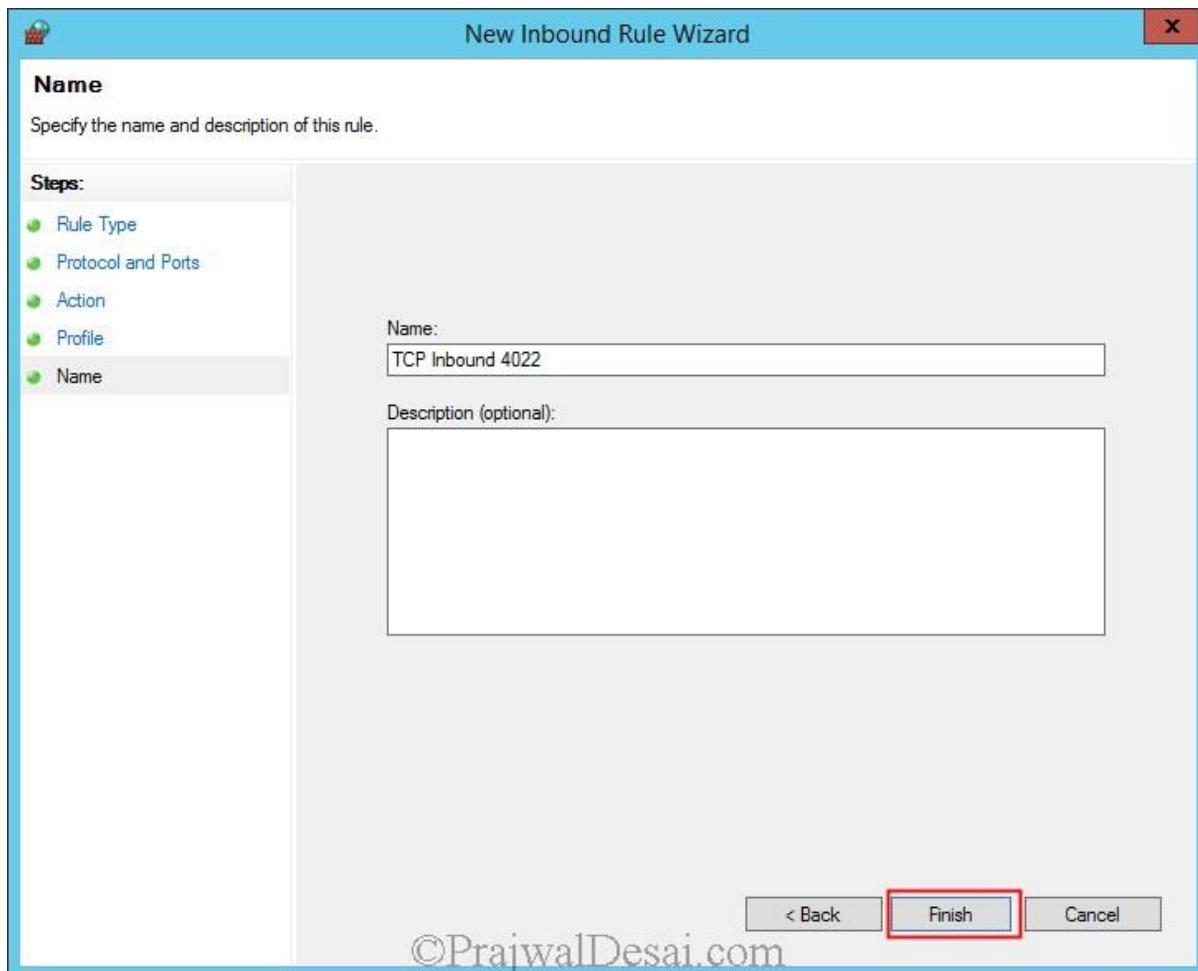
©PrajwalDesai.com

Similarly create an **Inbound Rule** to allow port **4022**. choose **TCP** and specify the port number as **4022**. Click on **Next**.



©PrajwalDesai.com

Click on **Allow the connection**. Click on **Next**. Select **Domain, Private and Public** and click on **Next**. Provide the name as **TCP Inbound 4022** to identify the rule. Click on **Finish**.



©PrajwalDesai.com

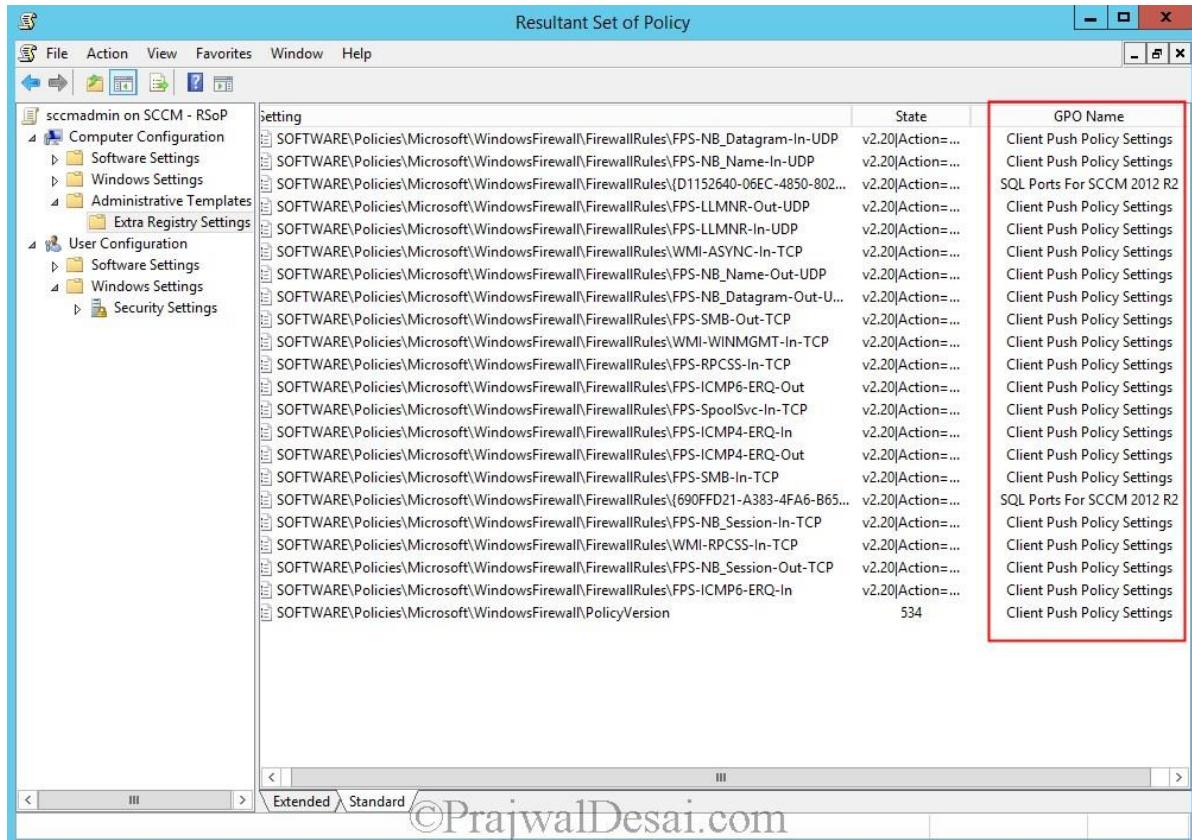
We have allowed TCP inbound ports 1433 and 4022 on our firewall.

The screenshot shows the Group Policy Management Editor window. The left pane displays a navigation tree for a policy named "SQL Ports For SCCM 2012 R2 [AD.PRAJWAL.LOC]". Under the "Windows Settings" section, the "Security Settings" node is expanded, showing "Account Policies", "Local Policies", "Event Log", "Restricted Groups", "System Services", "Registry", "File System", "Wired Network (IEEE 802.3) Policies", "Windows Firewall with Advanced Security", and "Network List Manager Policies". The "Windows Firewall with Advanced Security" node is selected and expanded, revealing "Inbound Rules", "Outbound Rules", and "Connection Security Rules". The "Inbound Rules" node is highlighted with a red box. The right pane is a table titled "Group Policy Management Editor" with columns: Name, Group, Local Port, Profile, and Enabled. It lists two entries: "TCP Inbound 1433" (Local Port 1433, Profile All, Enabled Yes) and "TCP Inbound 4022" (Local Port 4022, Profile All, Enabled Yes). The entire table area is also highlighted with a red box.

Name	Group	Local Port	Profile	Enabled
TCP Inbound 1433		1433	All	Yes
TCP Inbound 4022		4022	All	Yes

©PrajwalDesai.com

Run the **gpupdate /force** command on the domain controller and on any of the client machine, launch the command prompt and type the command **gpupdate /force** and hit enter. In the same command prompt, type the command **rsop.msc**. This will show the resultant set of policies, group policies that are applied to this client. Expand **Administrative Templates** and click on **Extra Registry Settings**. On the right side pane you will find that the policies that we created are applied on the machine.



[Installing System Center 2012 R2 Configuration Manager](#)

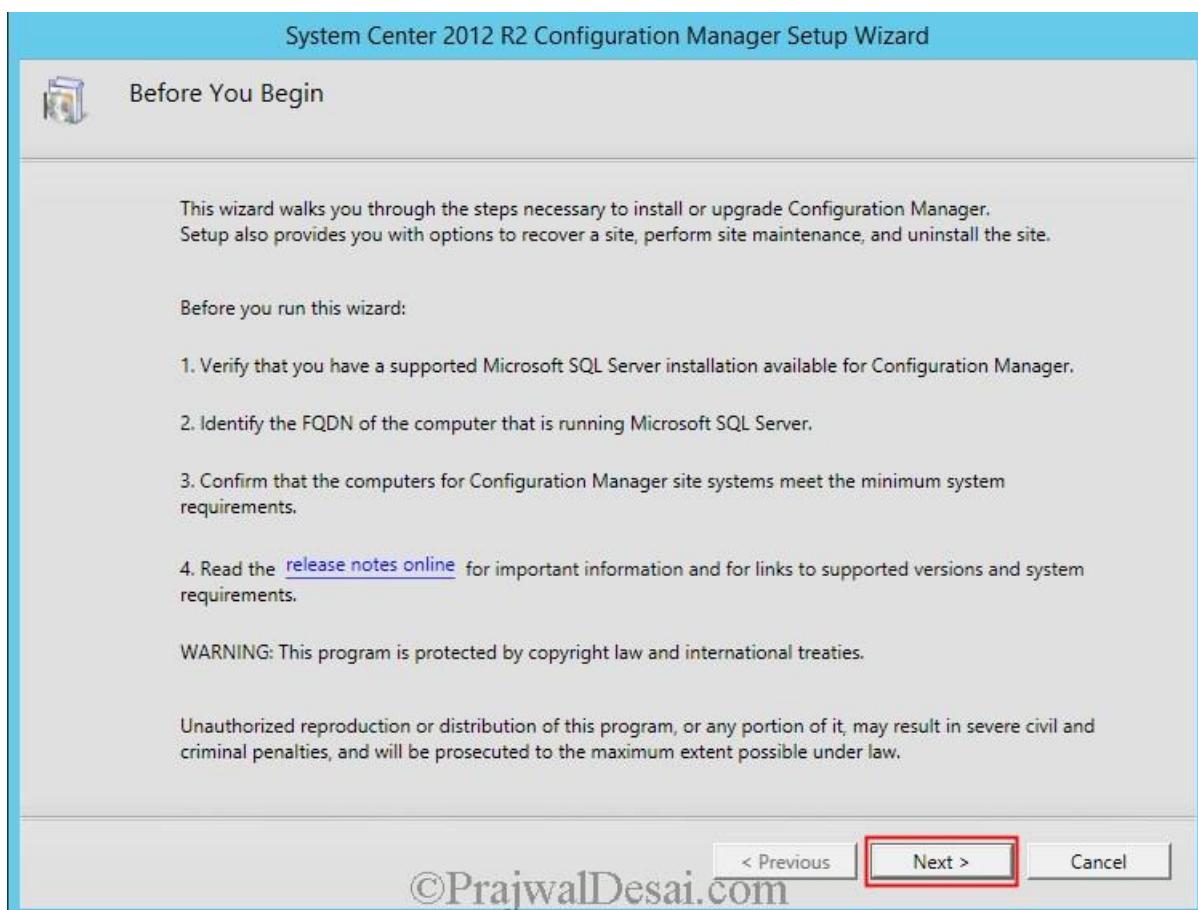
Installing System Center 2012 R2 Configuration Manager In this post we will see the steps for Installing System Center 2012 R2 Configuration Manager. So far in this deployment series of System Center 2012 R2 Configuration Manager we started with [Configuration Manager 2012 R2 System requirements](#), [Installing prerequisites for SCCM 2012 R2](#), [Installing SQL Server for Configuration Manager 2012 R2](#), [Installing WSUS for Configuration Manager 2012 R2](#), [Configuring Firewall for SCCM 2012 R2](#). The next step is to install System Center 2012 R2 Configuration Manager and the evaluation copy is available [here](#). The System Center 2012 R2 Configuration Manager and System Center 2012 R2 Endpoint Protection are provided as a single installation package.

Installing System Center 2012 R2 Configuration Manager

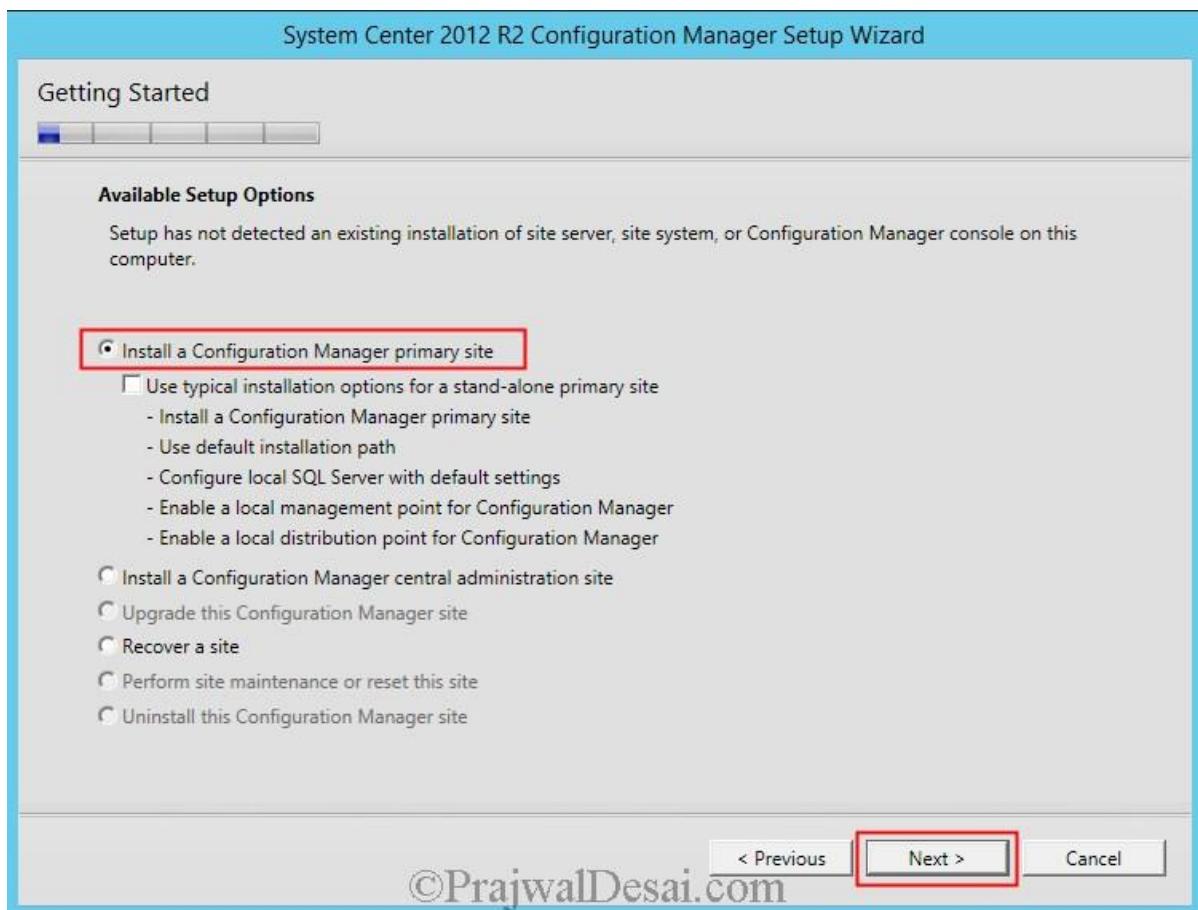
Once you have downloaded the configuration Manager 2012 R2 iso file, extract the iso file to a folder on the machine where you are going to install the SCCM. Run the file **splash** to launch the Setup screen. Click on **Install** to the begin the Installation.



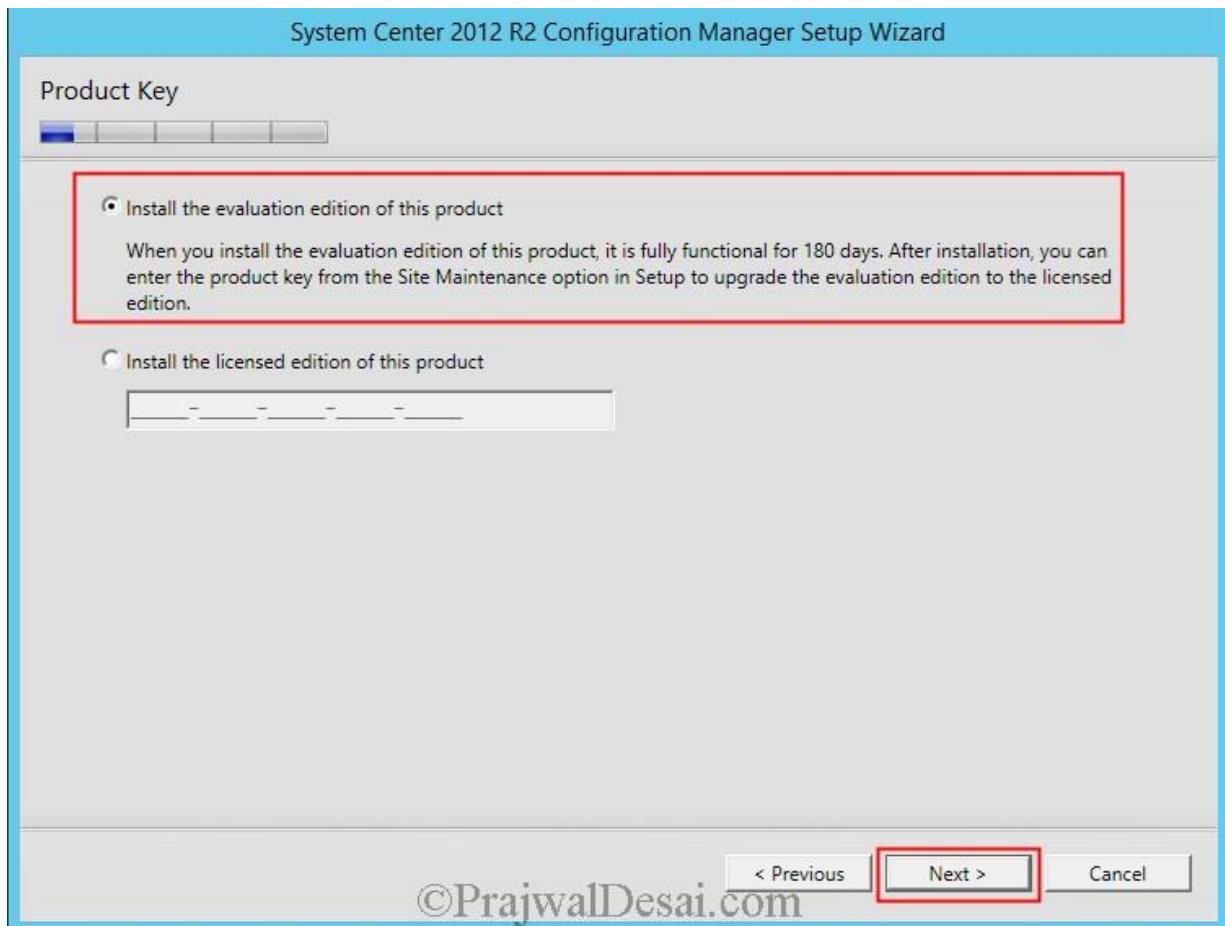
Click on **Next**.



Click on **Install a Configuration Manager Primary Site** and click **Next**.

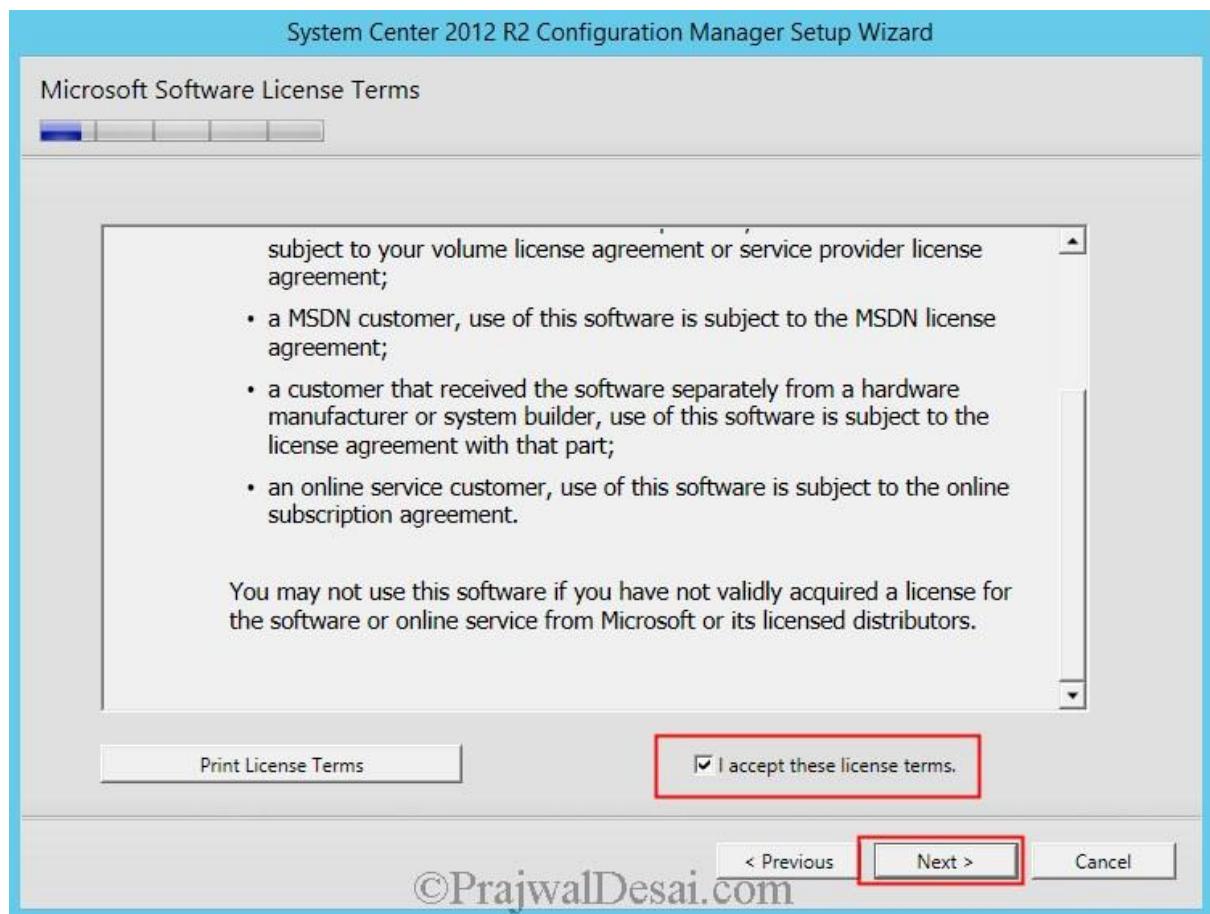


Enter the product key if you have purchased the copy of system center 2012 R2 configuration manager. Else choose **Install the evaluation edition** and click on **Next**.

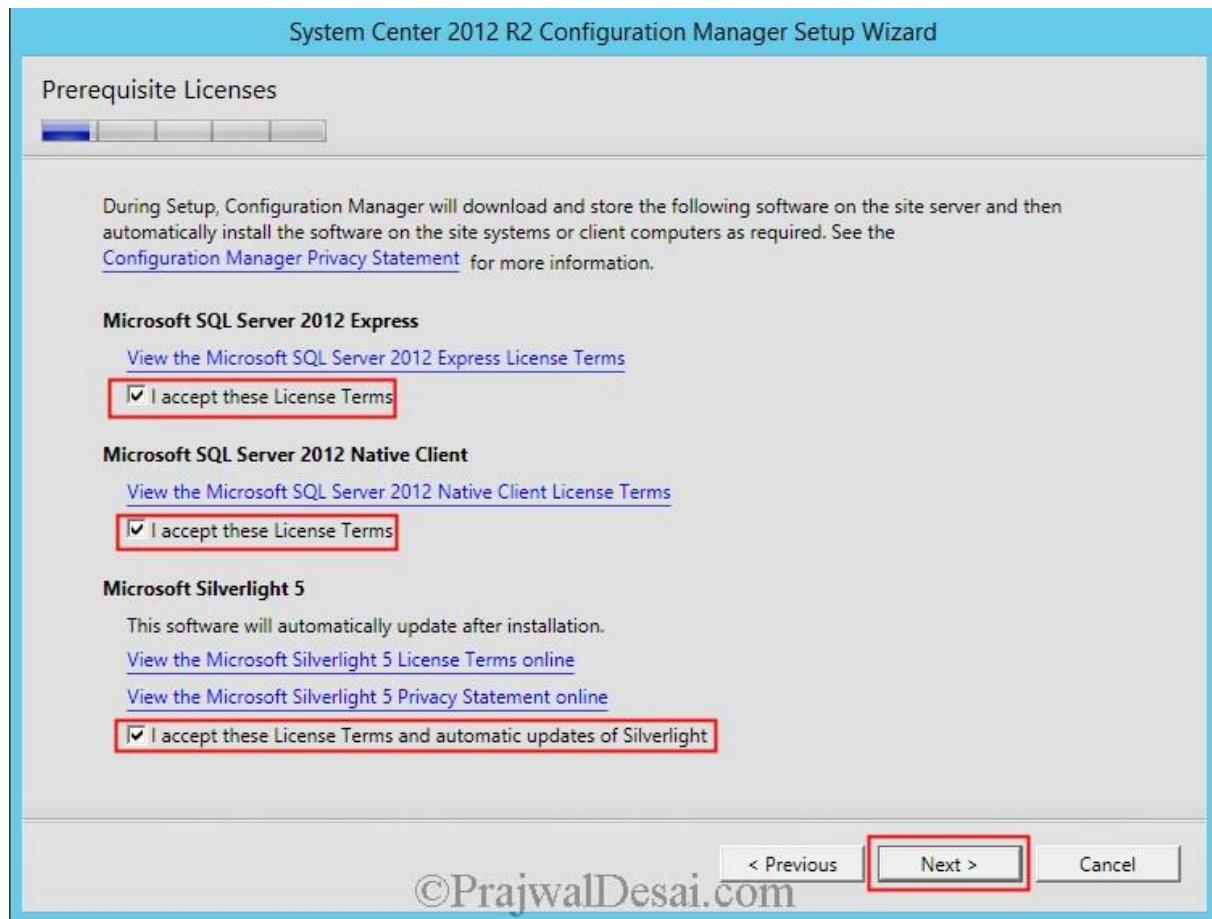


©PrajwalDesai.com

Click **I accept the license terms** and click on **Next**.



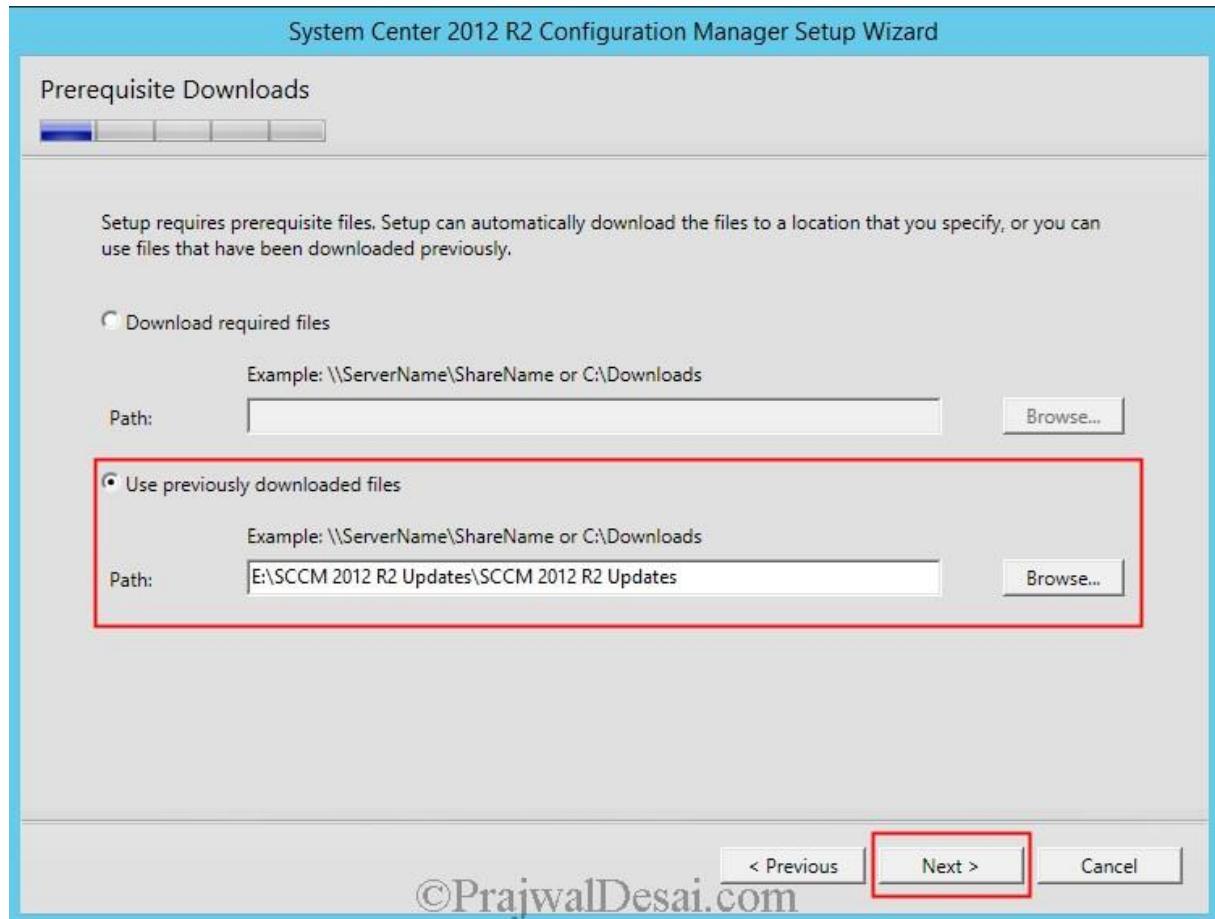
Accept the license terms for **Microsoft SQL Server 2012 Express**, **SQL 2012 Native Client** and **Silverlight 5** and click on **Next**.



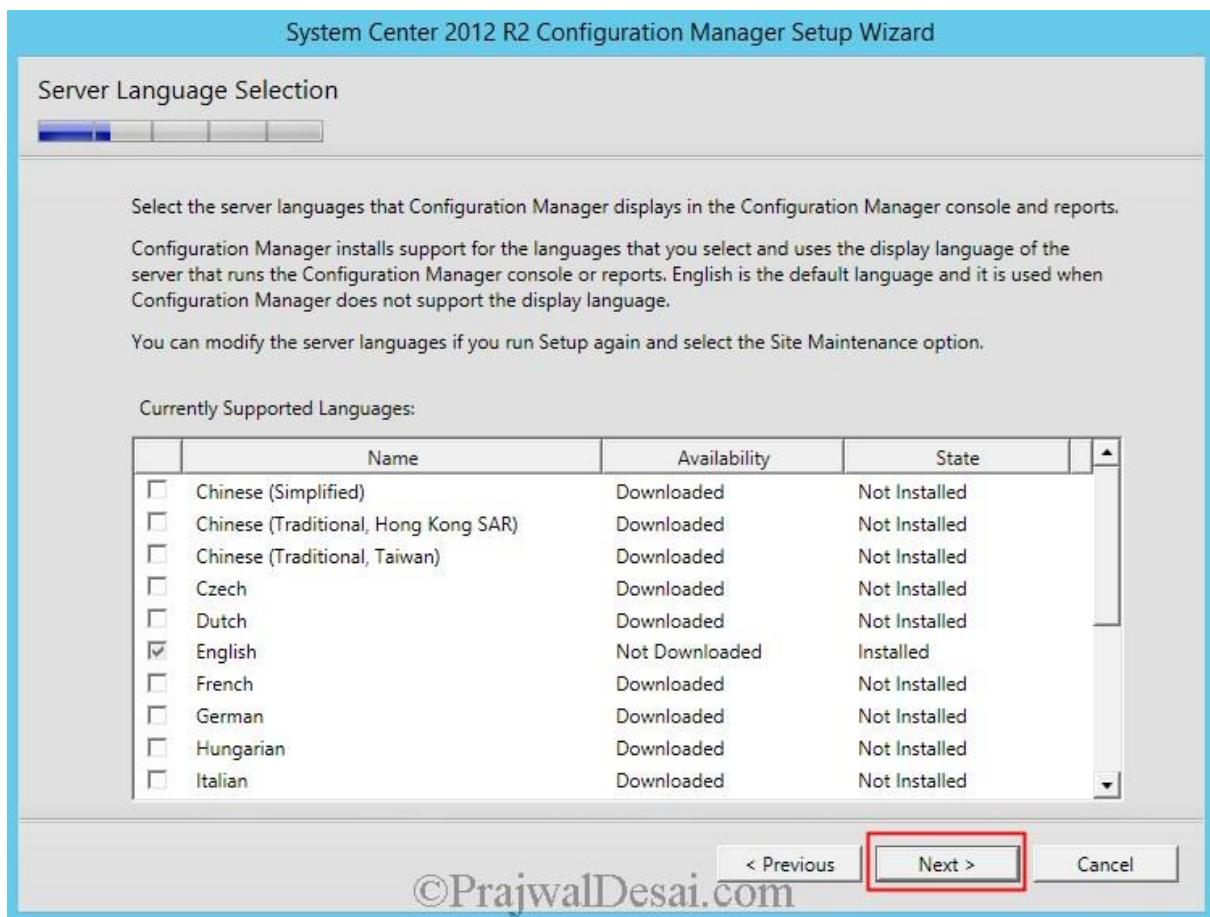
Prerequisite Downloads – There are 2 options that we see here.

1) **Download required files** – Select this option to download the setup prerequisites from Microsoft and you can store them in a folder or shared path.

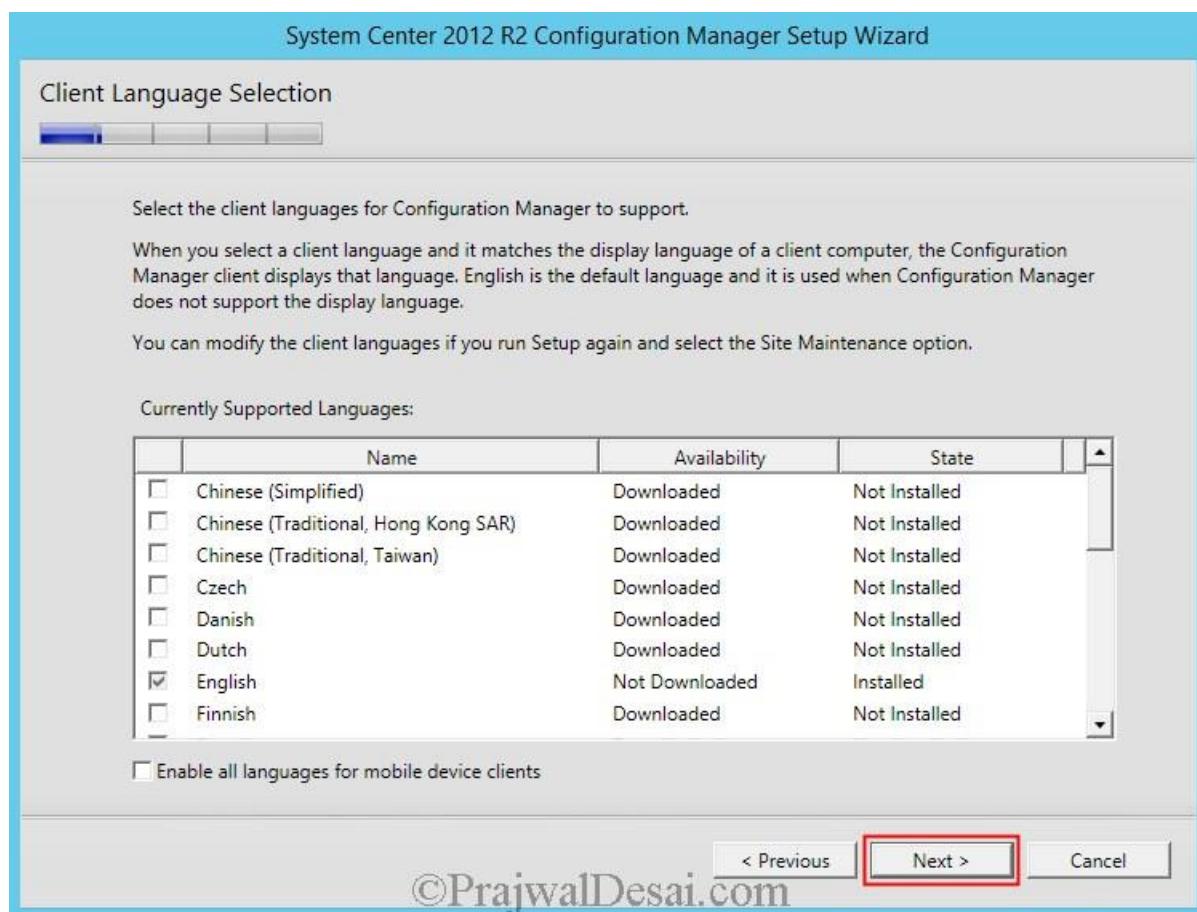
2) **Use previously downloaded files** – Select this option if you have downloaded the prerequisites. Browse to the folder where the prerequisites are stored and click on **Next**.



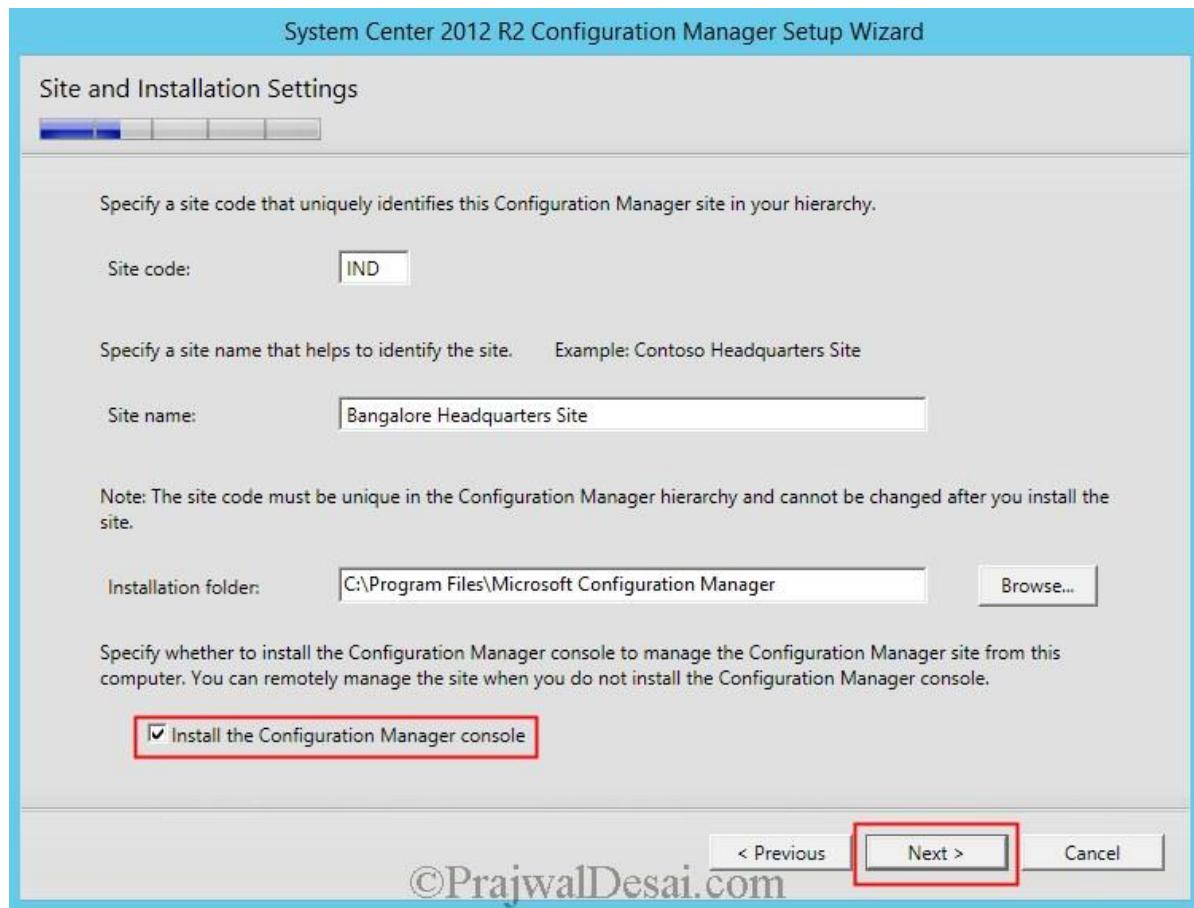
Click on **Next**.



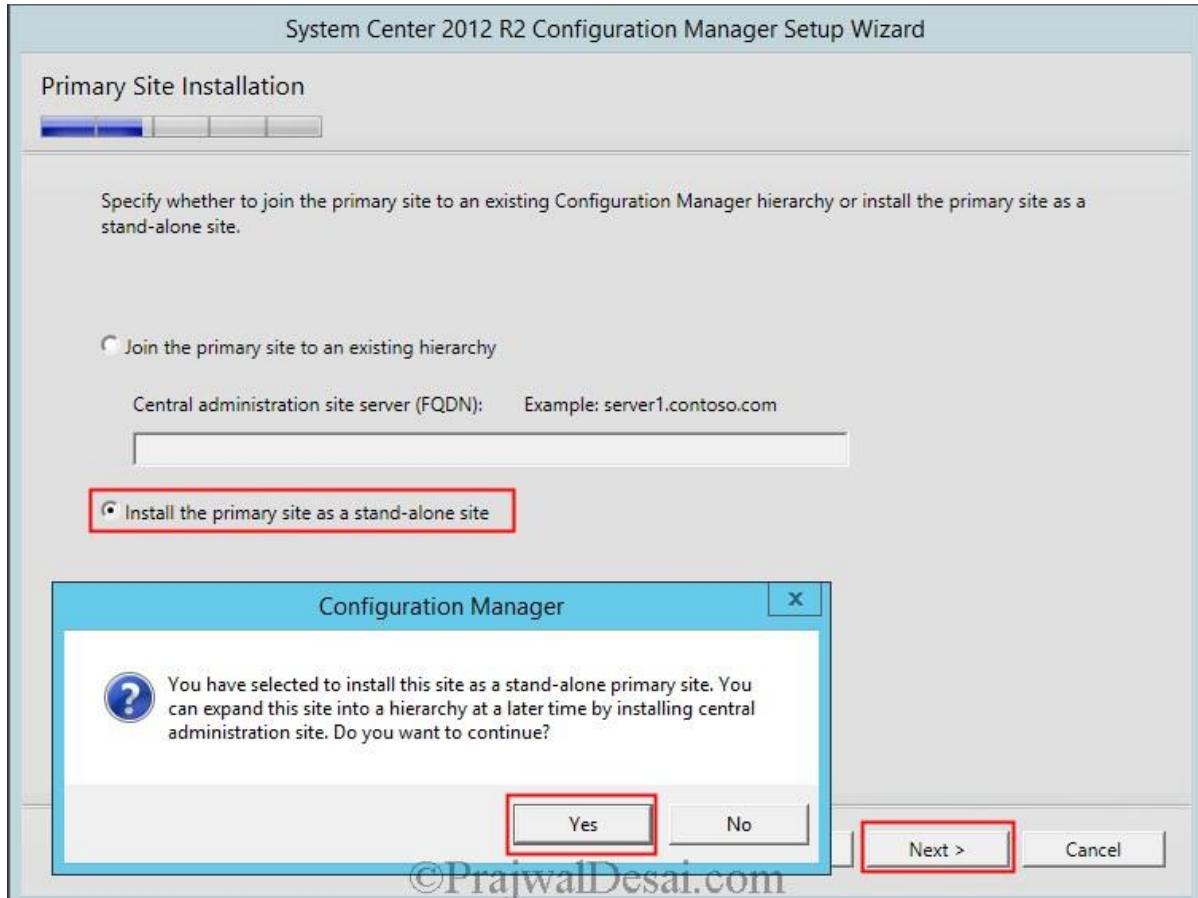
Click on **Next**.



Specify a **Site Code**, **Site name** and check the box **Install the Configuration Manager Console**. Click on **Next**.

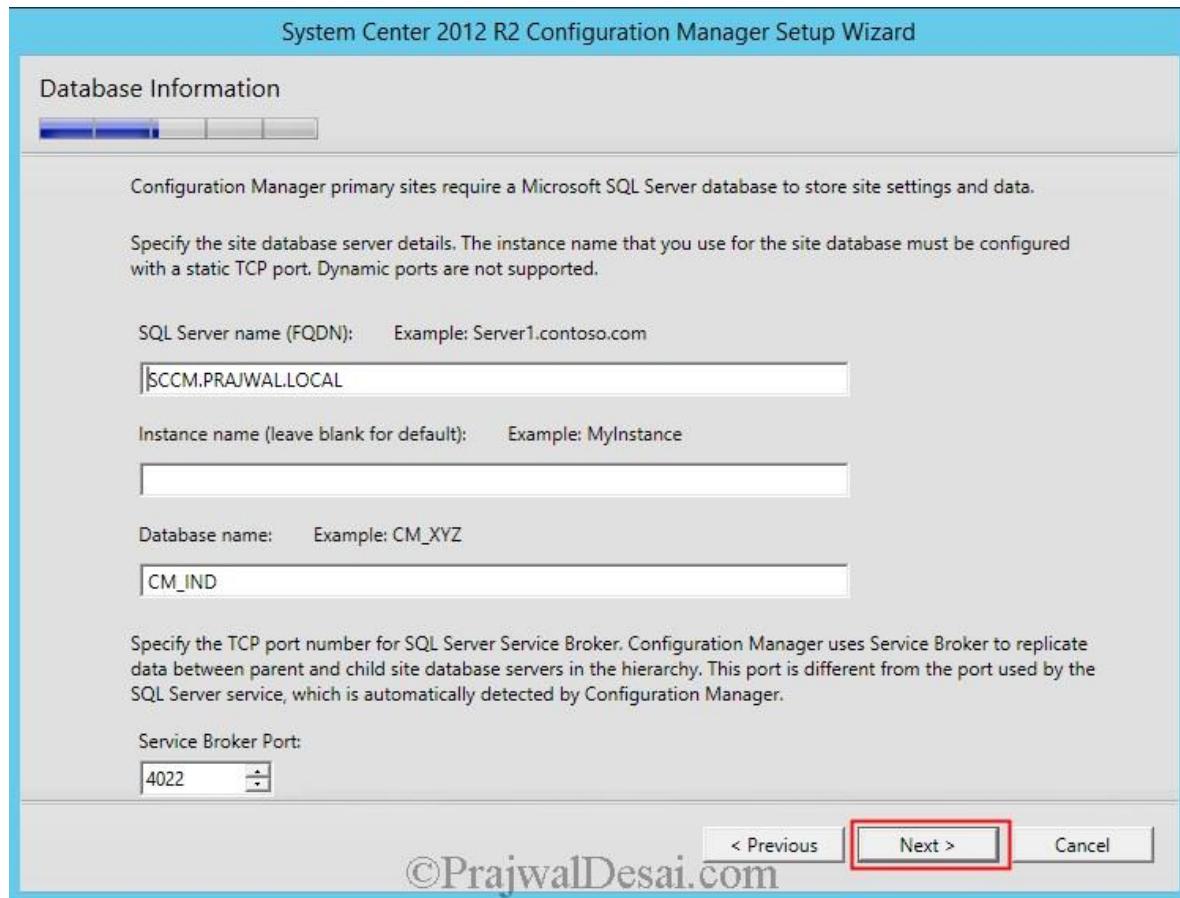


If you plan to join this primary site to CAS then choose **Join the primary site to an existing hierarchy**, you must provide the CAS server FQDN to join the hierarchy. If you plan to build hierarchy with more than one primary site, you must install CAS first. Else if you are installing primary site as a standalone site then choose the second option. Click **Yes** on the message box and click on **Next**.



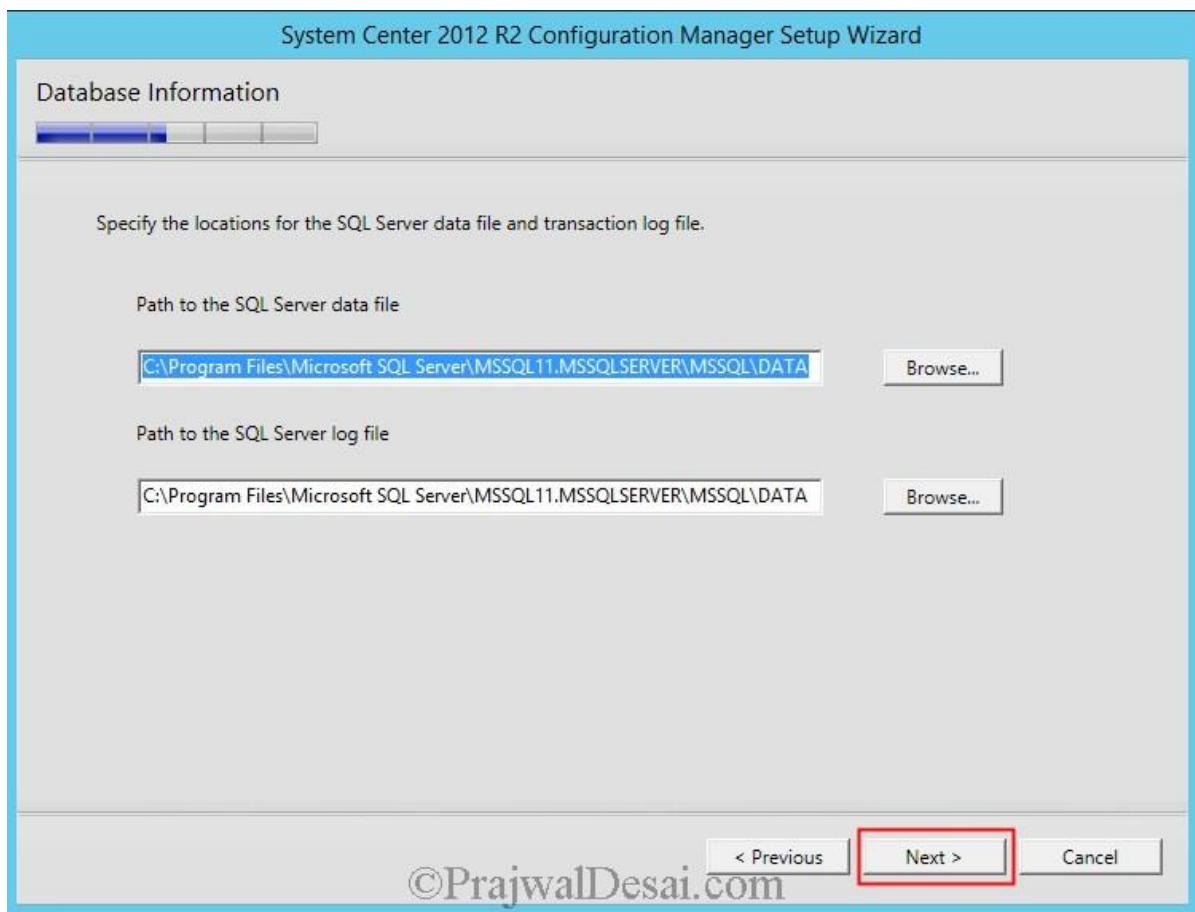
©PrajwallDesai.com

Do not change anything here, click on **Next**.

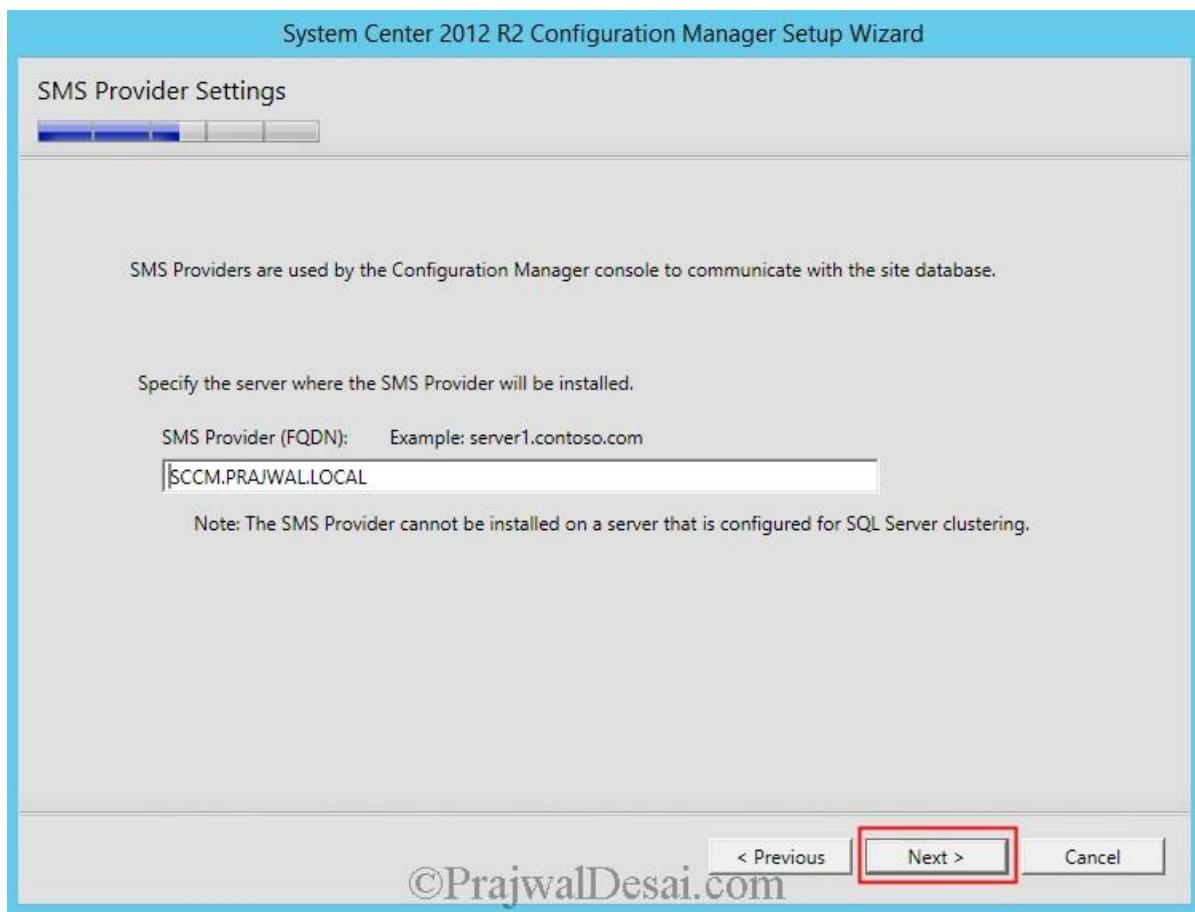


©PrajwalDesai.com

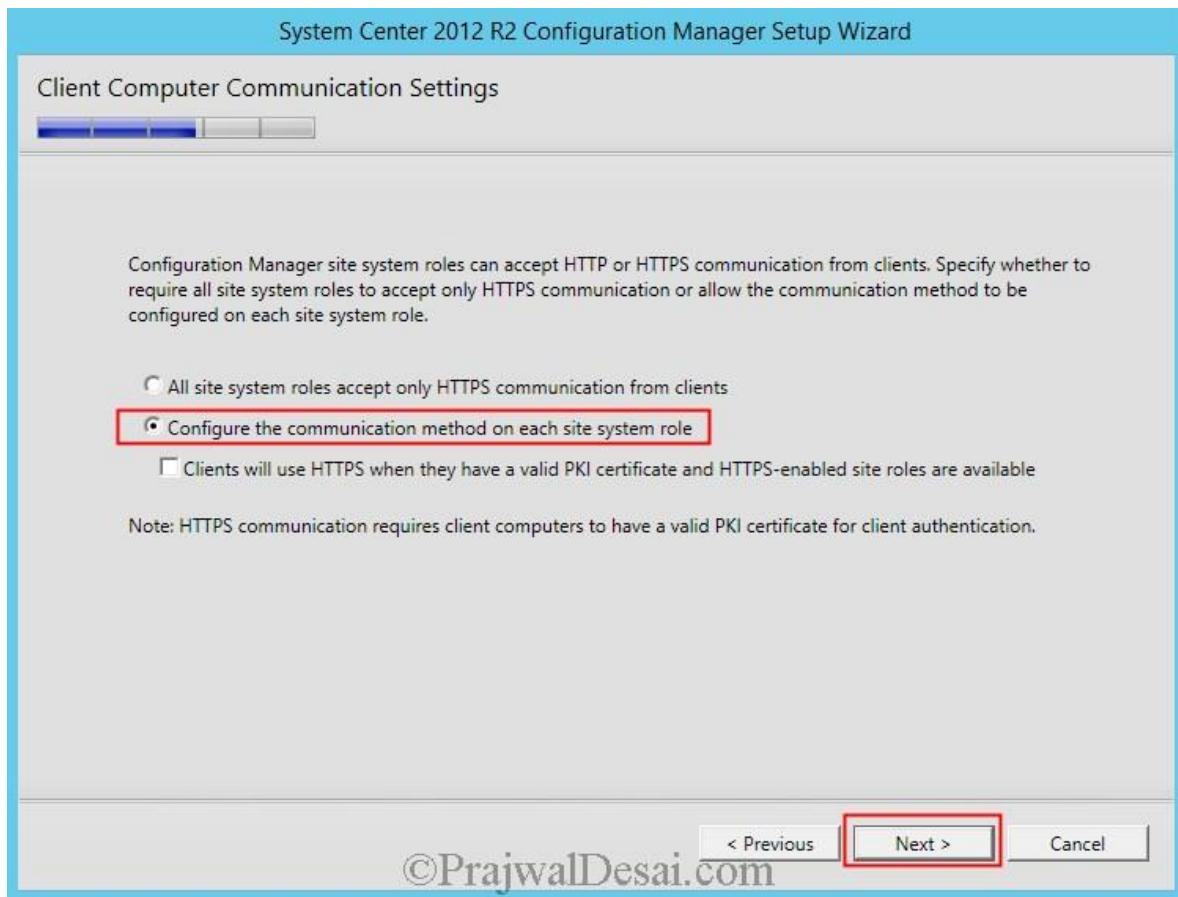
Click on **Next**.



Click on **Next**.

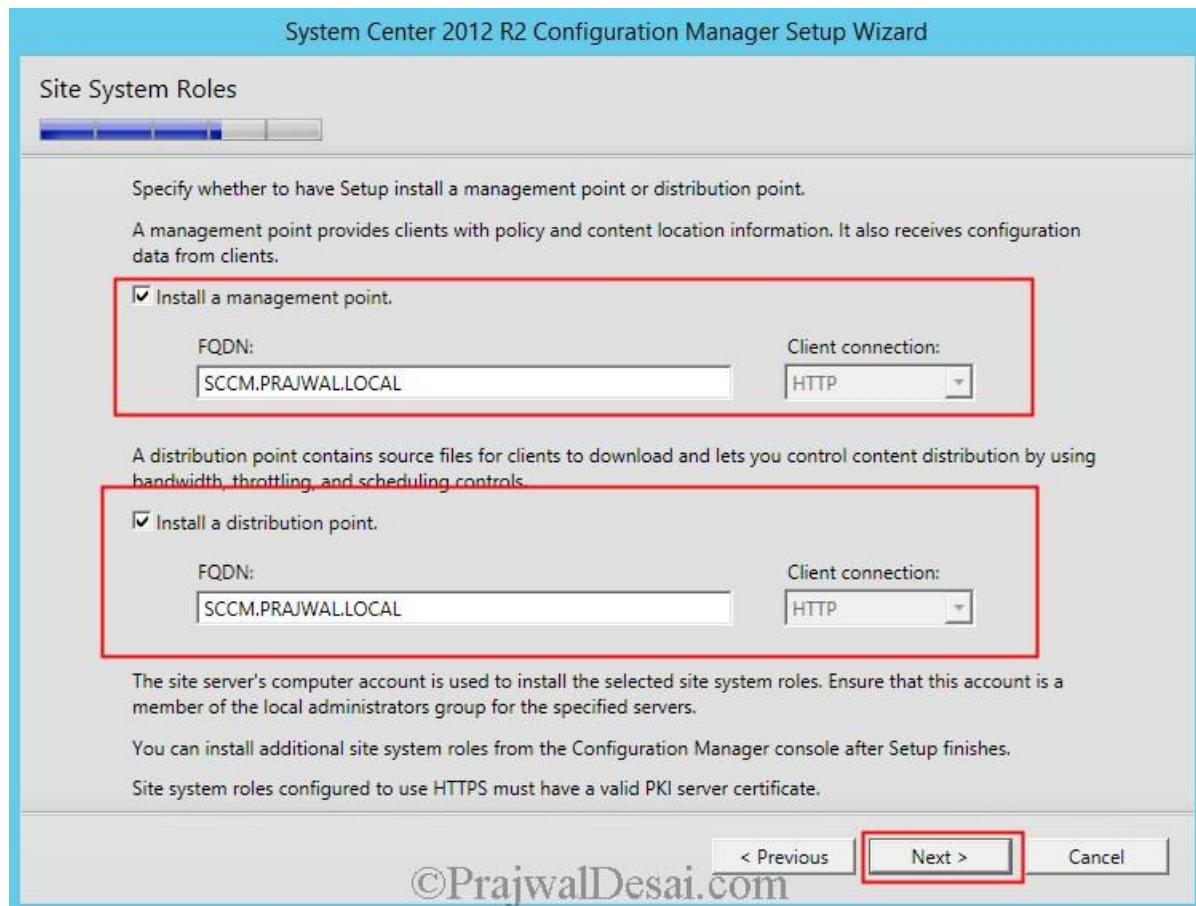


Client Computer Communication Settings – Choose Configure the communication method on each site system role and click Next.

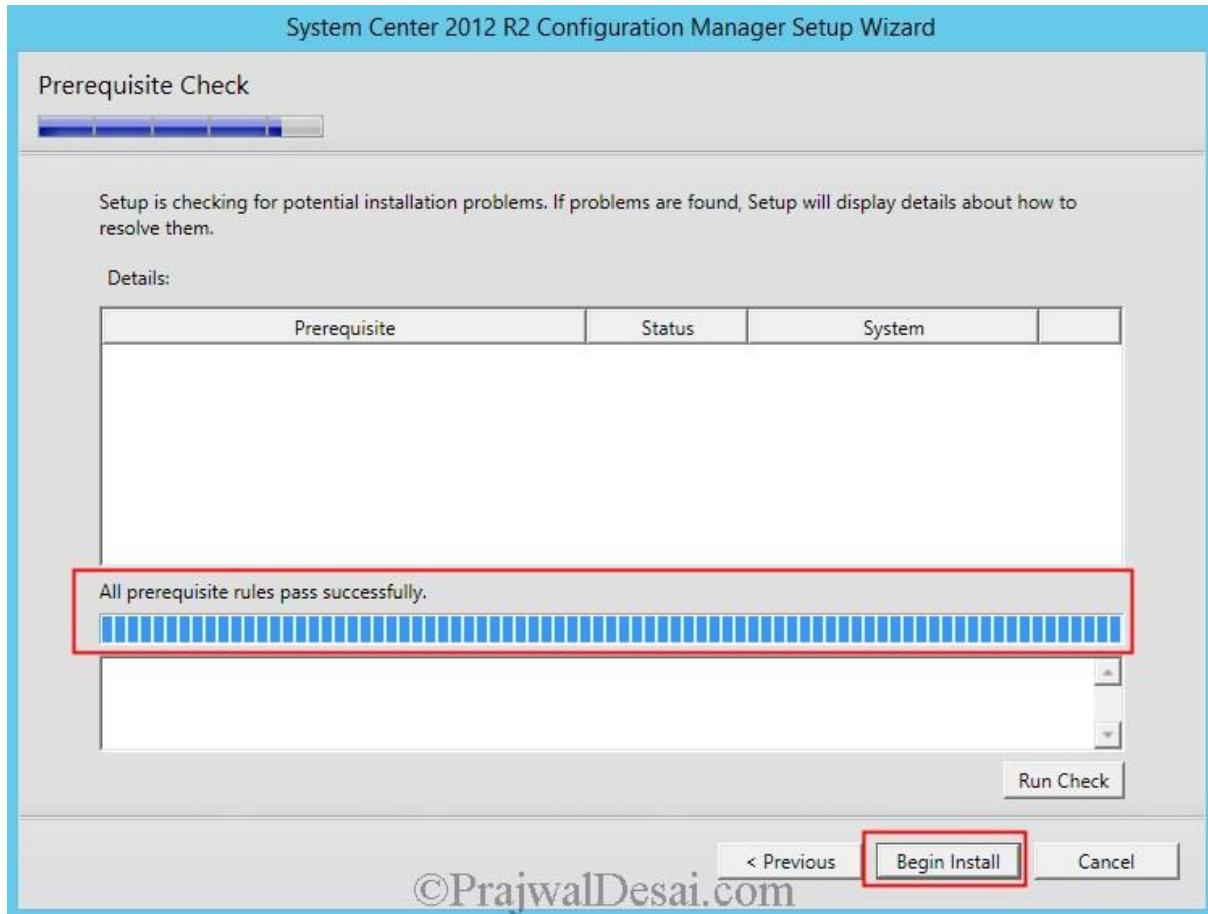


©PrajwalDesai.com

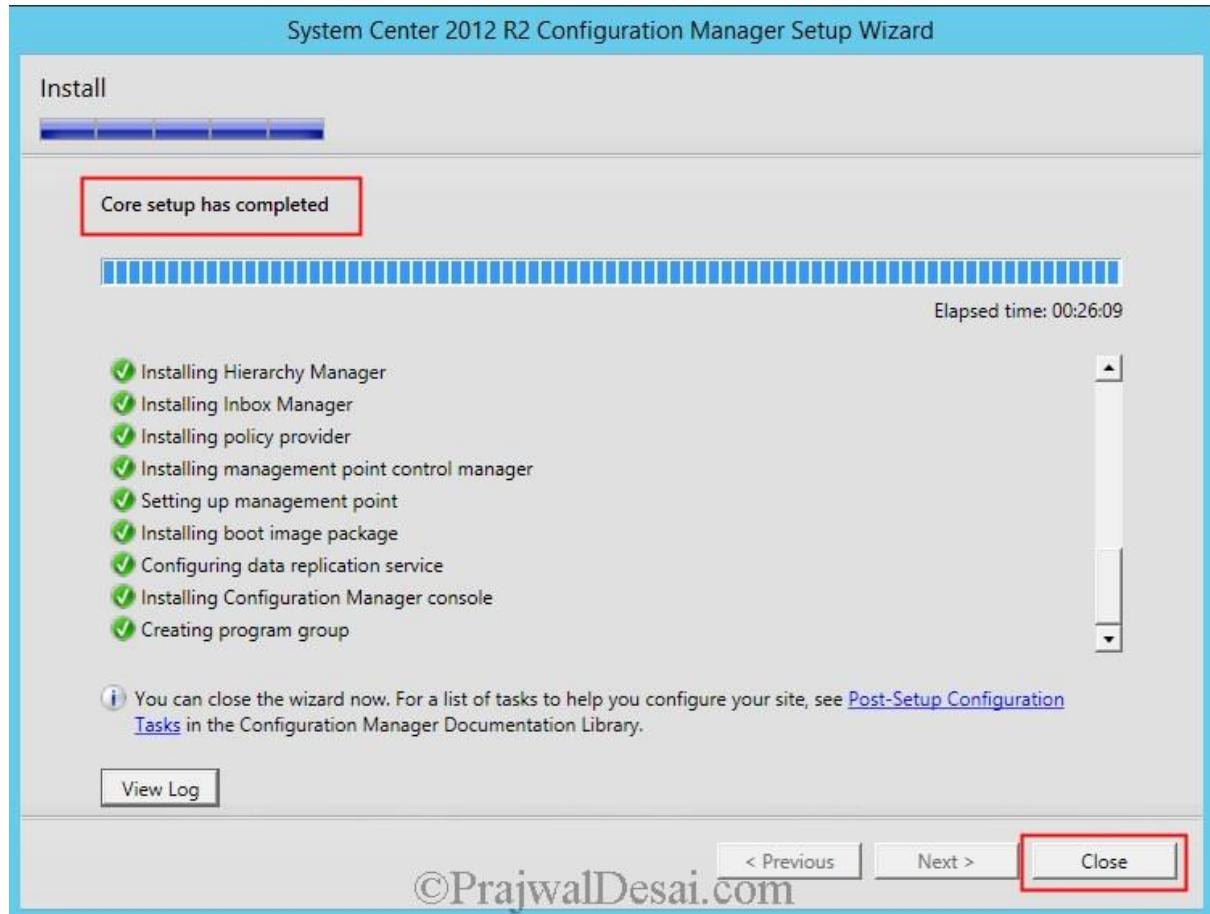
Check the box for **Install a management point** and **Install a distribution point** and click on **Next**.



Prerequisite Check – Here the Configuration Manager setup checks whether all prerequisites are installed correctly, if any of the prerequisite is not installed it would be displayed. If all the prerequisites are installed correctly then you will see the message “**All prerequisites rules pass successfully**“. Click on **Begin Install**.



The installation takes sometime to get completed. Once the installation is complete you can click on **Close**. You can view the setup log file with a tool called **CMTrace**. The tool is located in SCCM 2012 R2 source DVD under **\SMSSETUP\TOOLS**. Launch the **CMTrace** tool, open the log file **ConfigMgrSetup.log** located in C drive.



Installing Configuration Manager 2012 R2 Hotfixes

Configuration Manager 2012 R2 Hotfixes Soon after the release of Microsoft System Center 2012 R2 Configuration Manager, Microsoft released Configuration Manager 2012 R2 hotfixes that addressed some of the major issues in Configuration Manager 2012 R2. Lets look at what issues do these hotfixes resolve and we will also install them on SCCM 2012 R2.

Configuration Manager 2012 R2 Hotfixes

An update is available for the “Operating System Deployment” feature of System Center 2012 R2 Configuration Manager

This update resolves the following issues in Microsoft System Center 2012 R2 Configuration Manager.

Issue 1 – After you enable the PXE Service Point role on an instance of a specific distribution point, or you select the Deploy this boot image from the PXE-enabled distribution point property of a boot image, the Windows Deployment Service (WDS) stops running.

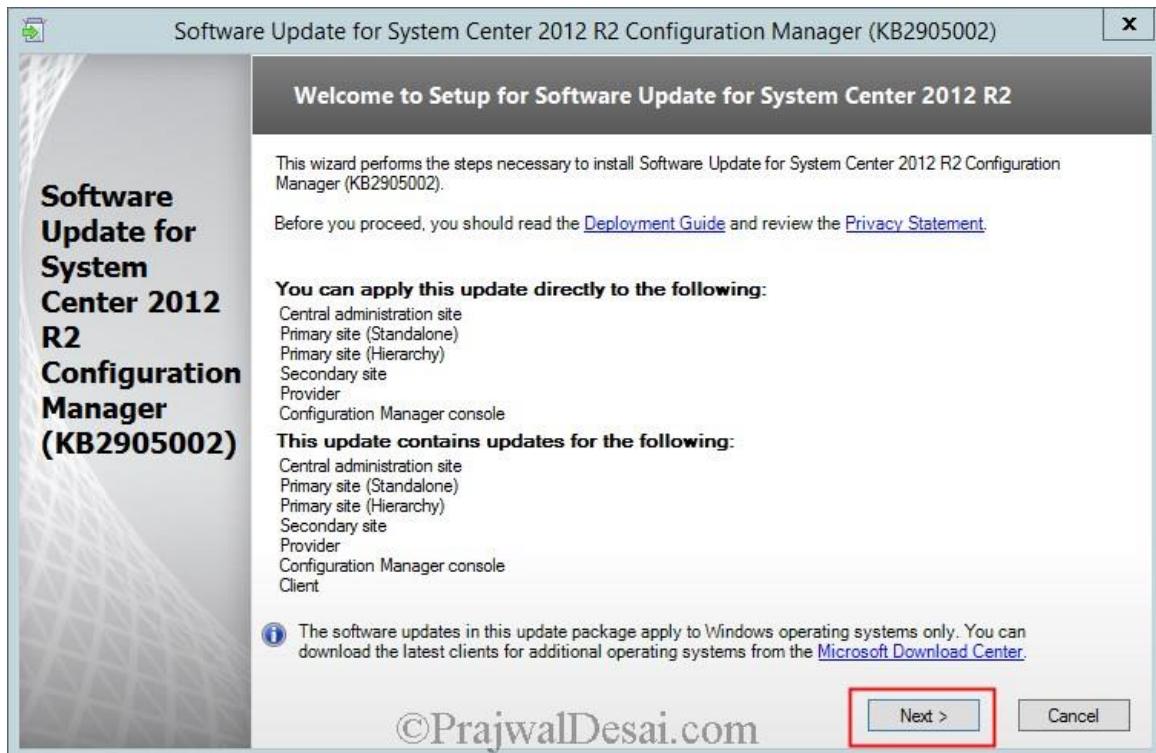
Following are the lines from Windows Application log: (**Note:- This problem affects only distribution points that are installed on site servers**)

Faulting application name: svchost.exe_WDSServer, version: 6.3.9600.16384, time stamp: 0x5215dfe3
Faulting module name: MSVCR100.dll, version: 10.0.40219.1, time stamp: 0x4d5f034a
Exception code: 0xc0000005
Fault offset: 0x000000000005f61a
Faulting process id: 0xae4
Faulting application start time: 0x01cec5d767184634
Faulting application path: C:\Windows\system32\svchost.exe
Faulting module path: C:\Program Files\Microsoft Configuration Manager\bin\x64\MSVCR100.dll

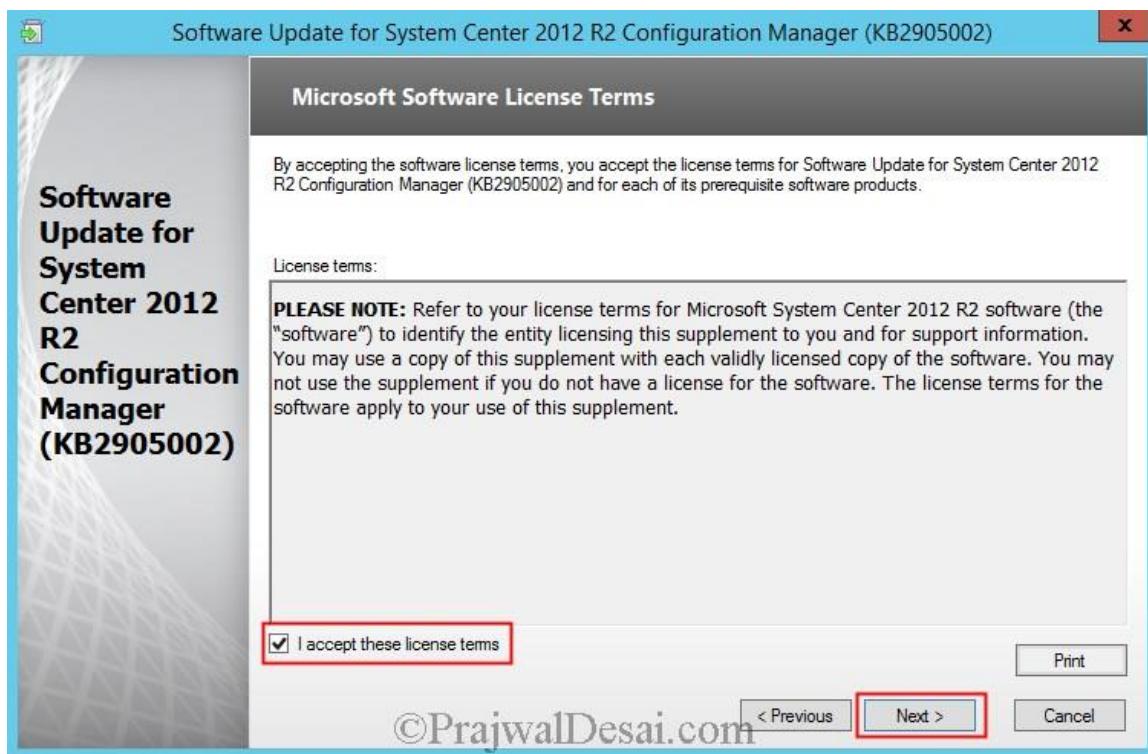
Issue 2 – When operating system image files are downloaded to Configuration Manager 2012 R2 clients, you may find that the download takes longer than it did in previous versions of Configuration Manager 2012 clients. You may see this behavior when the target client is running Windows PE or a full Windows operating system [Download Hotfix](#)

Installing Hotfix (KB2905002)

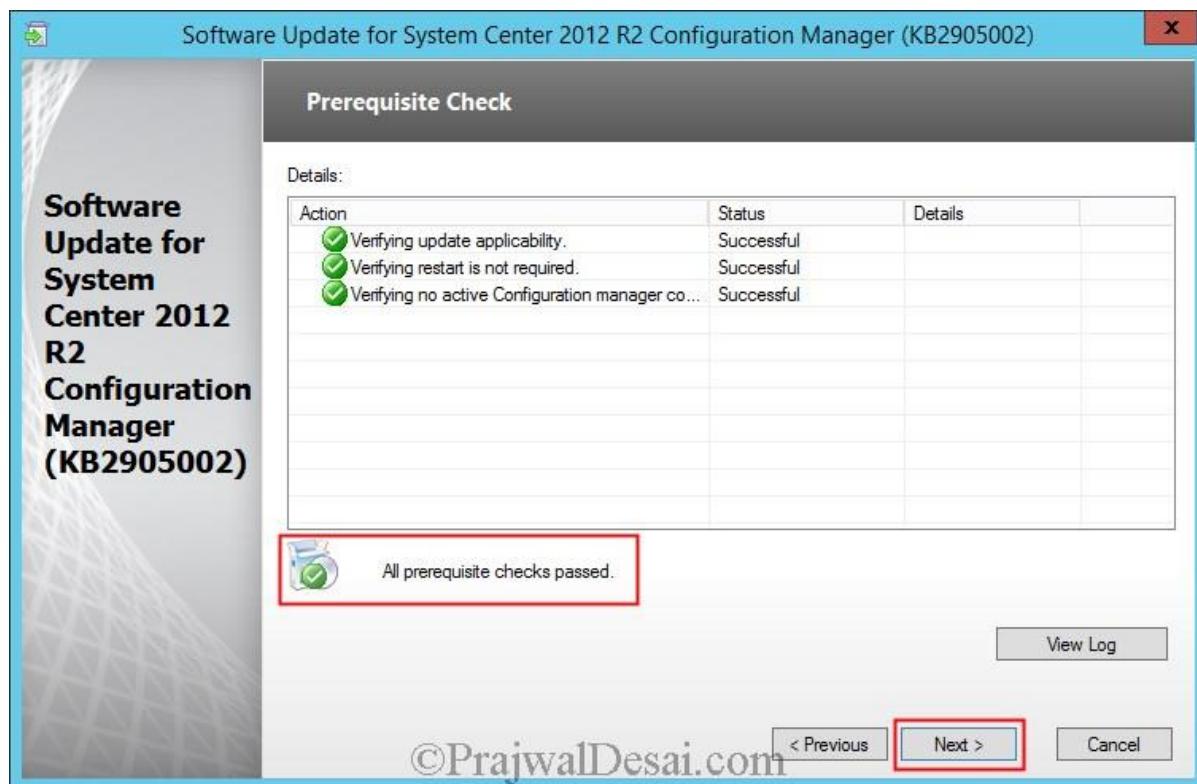
Log in to the machine where the Configuration Manager 2012 R2 is installed, extract the hotfix (**CM12-R2RTM-QFE-KB2905002-X64-ENU**) that you have downloaded and run the hotfix file. You will see the setup wizard **Software Update for System Center 2012 R2 Configuration Manager**. Click on **Next**.



Click I accept these license terms and click on Next.

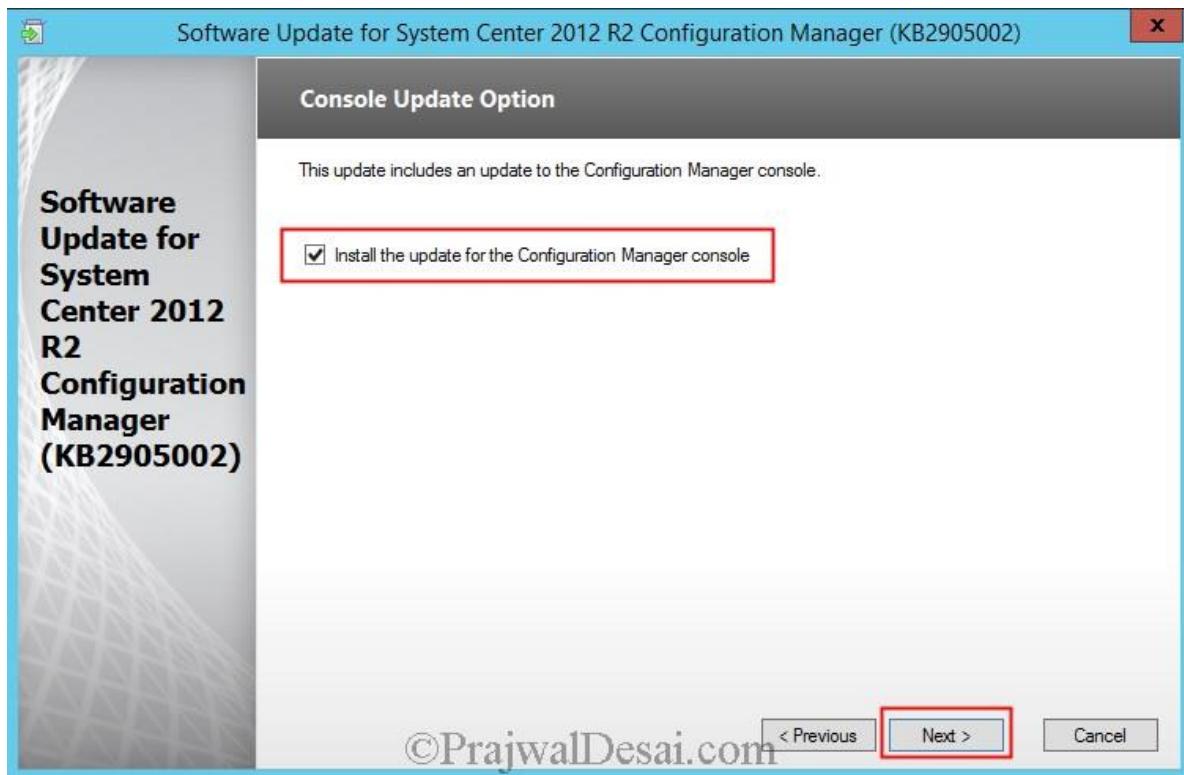


After the prerequisite check is done click **Next**.



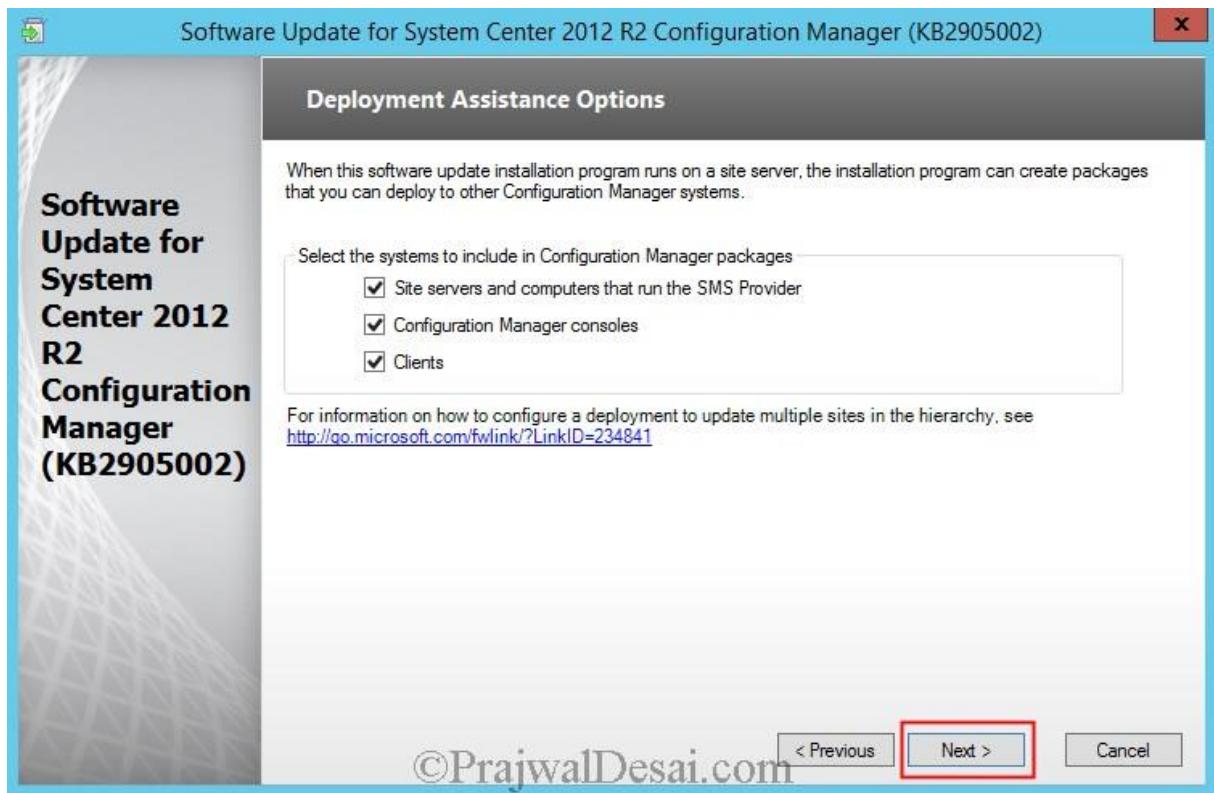
©PrajwalDesai.com

This hotfix will install the update for the Configuration Manager 2012 R2 console. Click on **Next**.

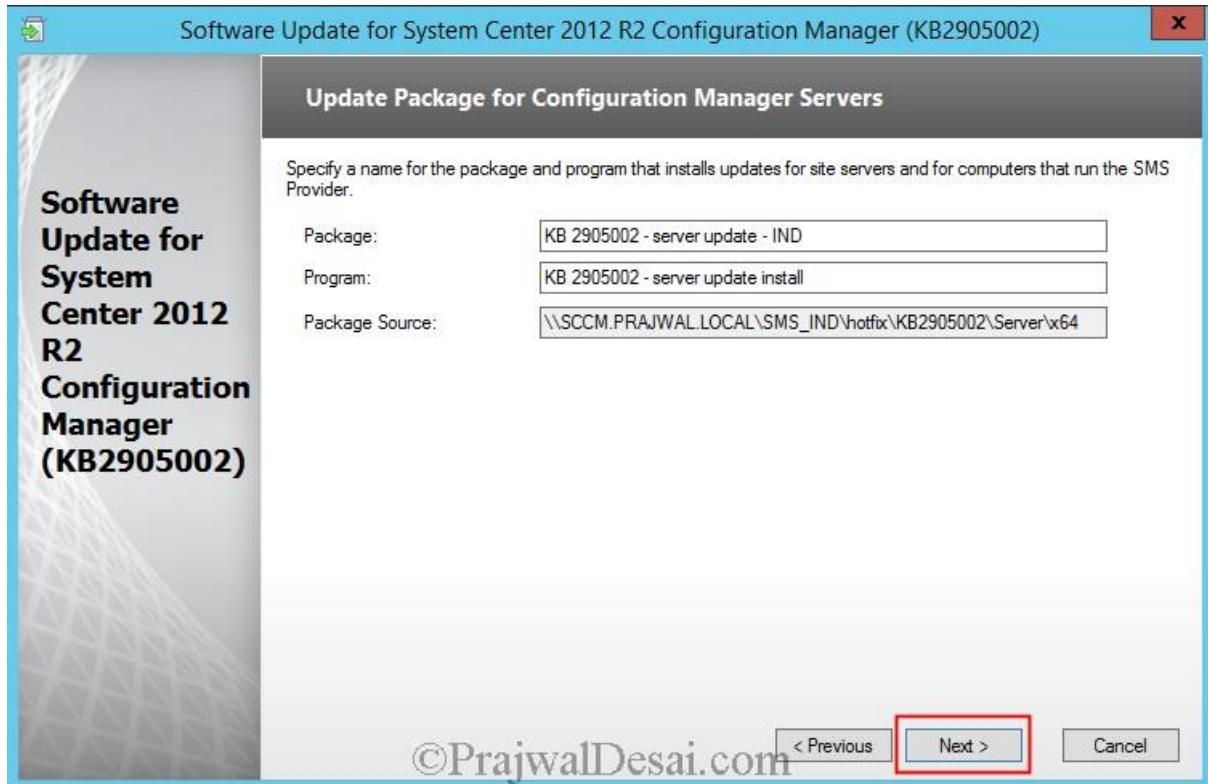


©PrajwalDesai.com

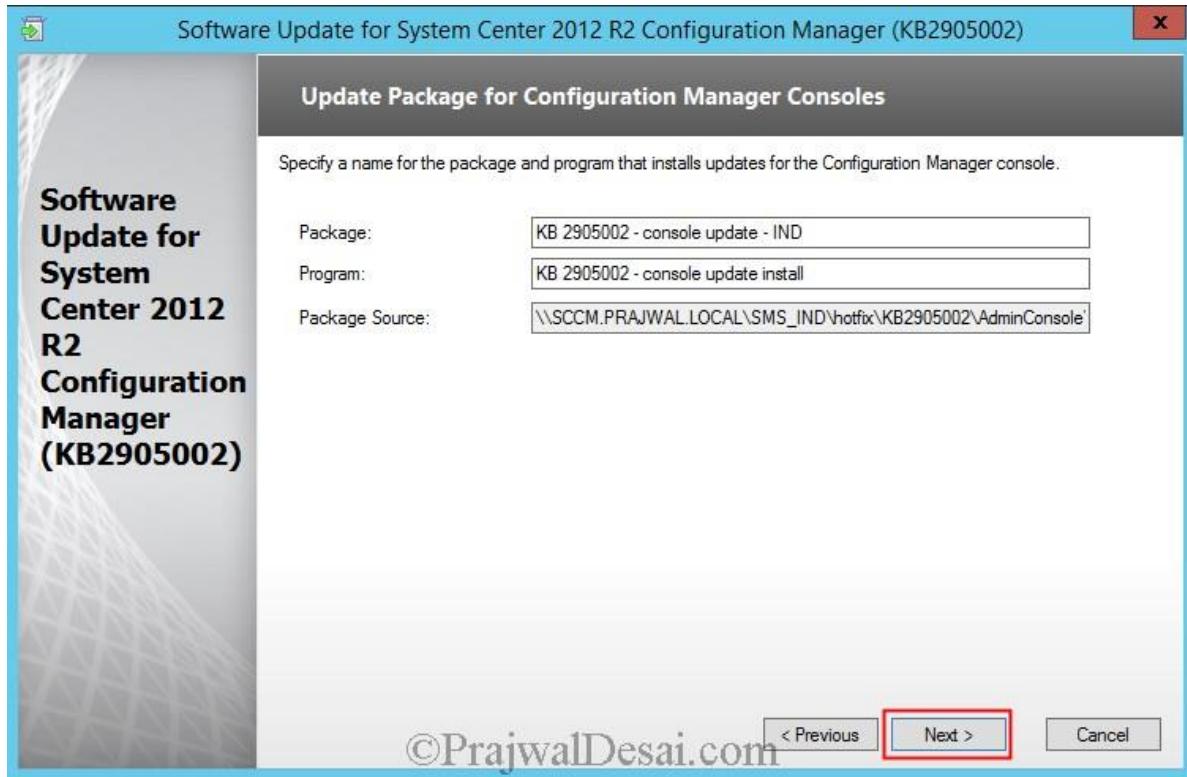
The hotfix also creates packages which can be deployed to other configuration manager systems, click on **Next**.



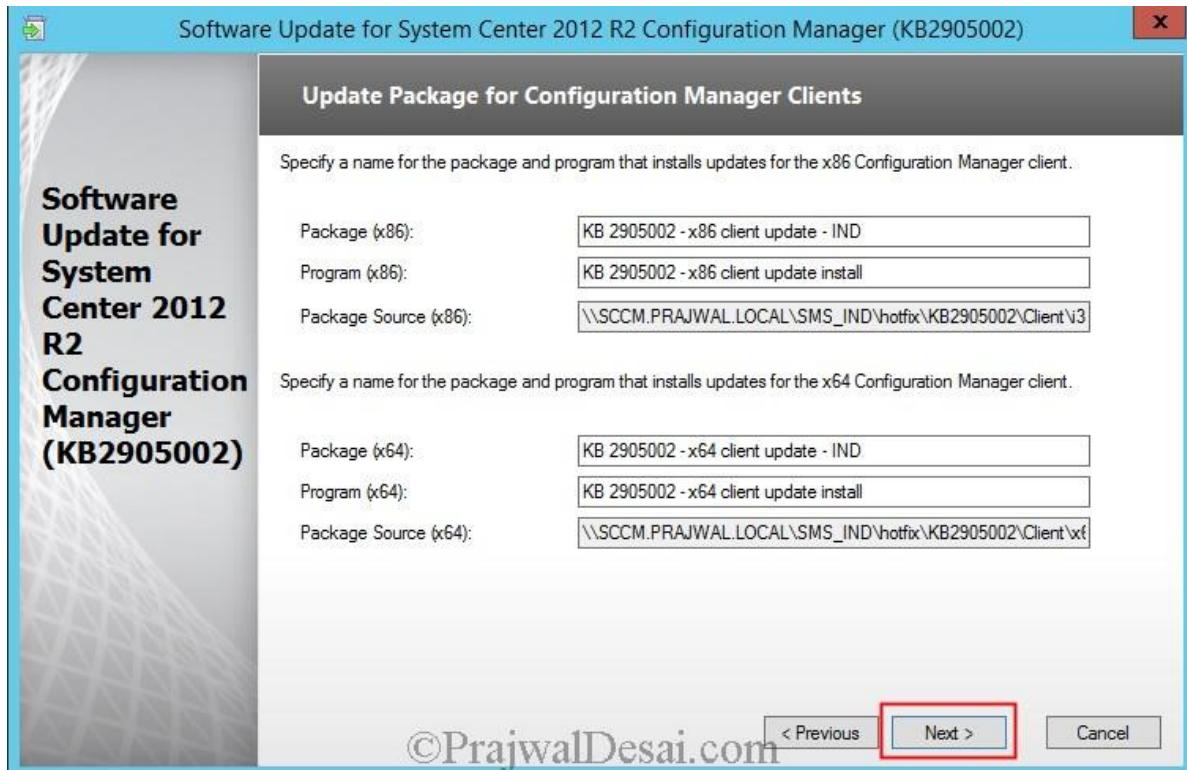
The name of the package for CM servers would be **KB 2905002-server update-Site Code**. Click on **Next**.



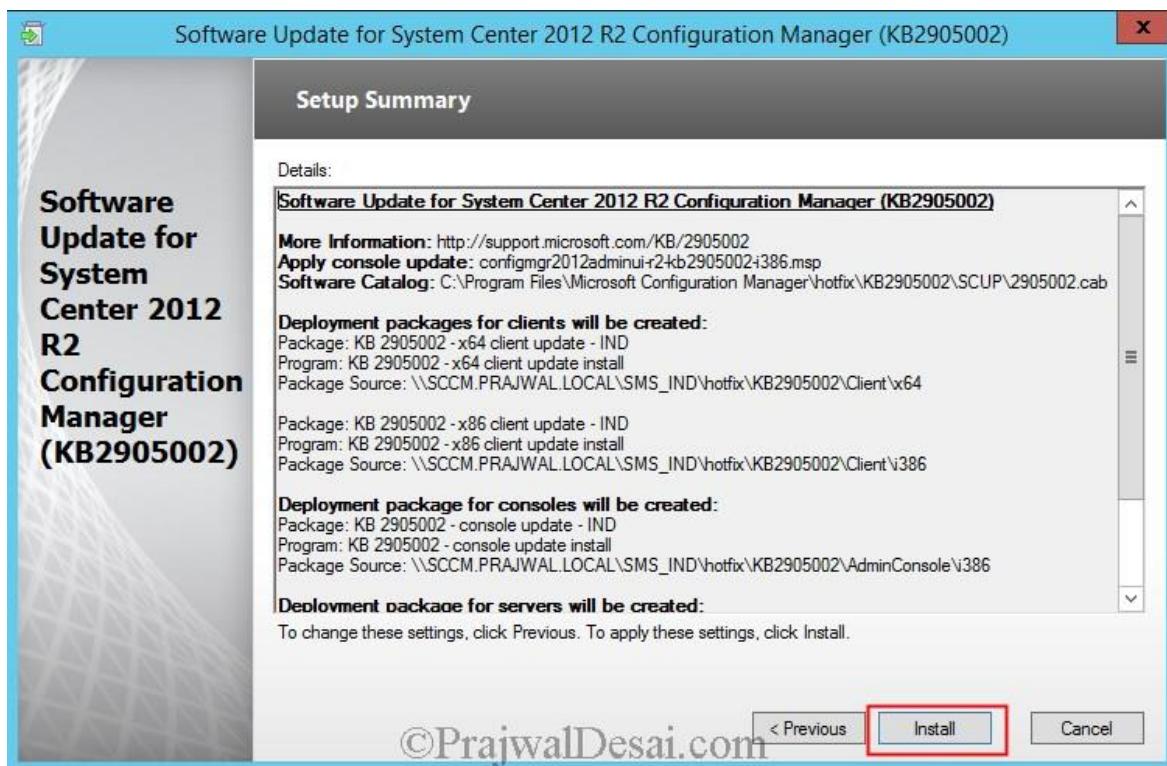
The name of the package for CM consoles would be **KB 2905002-console update-Site Code**. Click on **Next**.



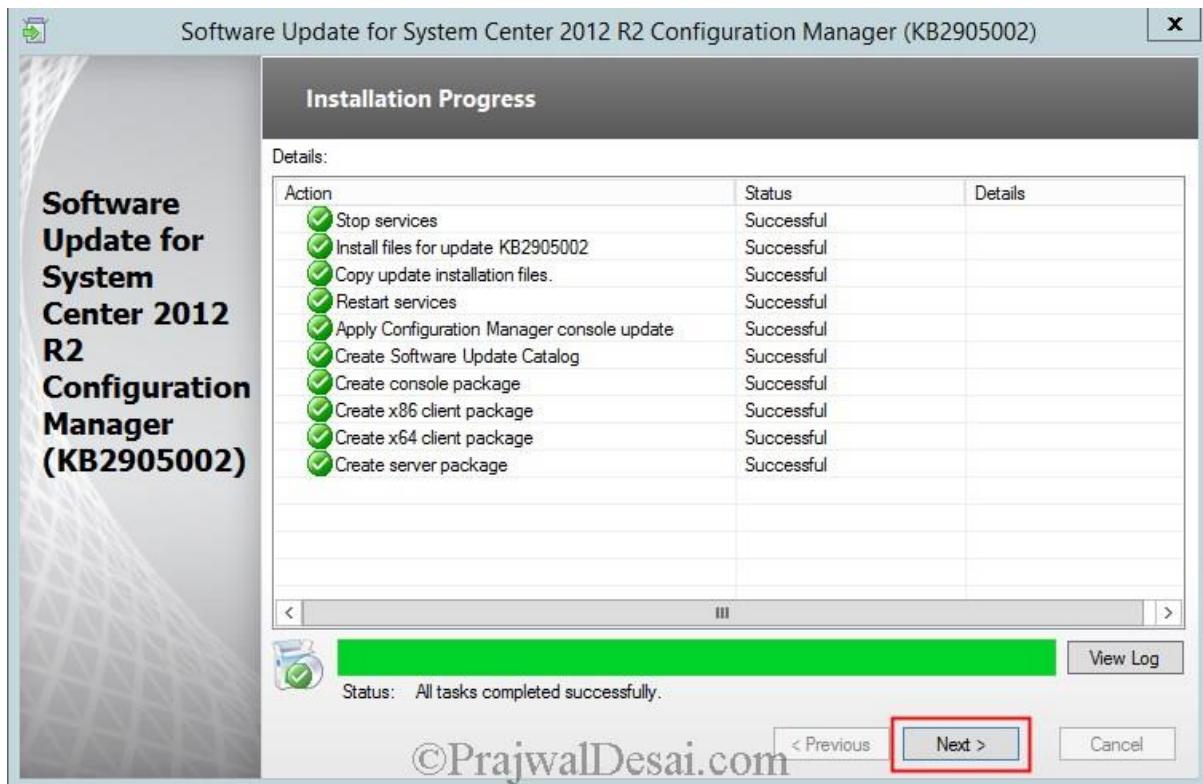
The name of the update package for CM clients(x86 and x64 respectively) would be **KB 2905002- x86 client update-Site Code** and **KB 2905002- x64 client update-Site Code**. Click on **Next**.



On Setup Summary page click on **Install**.



The hotfix is installed successfully. You can view the setup log file by clicking on **View Log**. Click on **Next**.



©PrajwalDesai.com

Click on **Finish**.



The hotfix setup log file.

The screenshot shows the Configuration Manager Trace Log Tool window. The title bar reads "Configuration Manager Trace Log Tool - [C:\...\cm12-r2rtm-qfe-kb2905002-x64-enu.log]". The menu bar includes File, Tools, Window, Help, and several icons for file operations like Open, Save, Print, and Copy/Paste. The main area is a table with columns: Log Text, Component, Date/Time, and Thread. The log text contains messages from the "Update Setup" component. Key entries include:

Log Text	Component	Date/Time	Thread
Creating program...	Update Setup	11/30/2013 6:36:07 PM	5788 (0x169C)
Created program 'KB 2905002 - server update install', program id is IND00009.	Update Setup	11/30/2013 6:36:07 PM	5788 (0x169C)
Adding program comment KB 2905002 - server update install	Update Setup	11/30/2013 6:36:07 PM	5788 (0x169C)
Task 'Create server package' completed, state is 'passed'	Update Setup	11/30/2013 6:36:08 PM	1660 (0x67C)
Installation tasks completed.	Update Setup	11/30/2013 6:36:08 PM	1660 (0x67C)
Update Setup has completed successfully.	Update Setup	11/30/2013 6:36:08 PM	1660 (0x67C)
Displaying wizard page: 'Installation Complete'.	Update Setup	11/30/2013 6:38:57 PM	1660 (0x67C)
Setup exit status: 0 (Task State: Success)	Update Setup	11/30/2013 6:39:20 PM	1660 (0x67C)
Update installer has completed, exit code is 0	Update Setup	11/30/2013 6:39:20 PM	1660 (0x67C)

Below the table, there are two status lines: "Date/Time: 11/30/2013 6:36:08 PM Component: Update Setup" and "Thread: 1660 (0x67C) Source:". At the bottom of the log area, it says "Update Setup has completed successfully." and shows scroll bars. The footer of the window displays "Elapsed time is 0h 5m 29s 547ms (329.547 seconds)" and the watermark "©PrajwalDesai.com".

Launch the **Configuration Manager 2012 R2 console**, click on **Software Library**, expand **Overview**, expand **Application Management**, expand **Packages** and click on **Configuration Manager Updates**. On the right hand side of console you will see the packages that were created by this hotfix.

The screenshot shows the System Center 2012 R2 Configuration Manager console. The navigation path is: Software Library > Overview > Application Management > Packages > Configuration Manager Updates. A red box highlights the 'Configuration Manager Updates' folder under the 'Packages' section. To the right, a table lists four packages:

Icon	Name
[Icon]	KB 2905002 - console update - IND
[Icon]	KB 2905002 - server update - IND
[Icon]	KB 2905002 - x64 client update - IND
[Icon]	KB 2905002 - x86 client update - IND

©PrajwalDesai.com

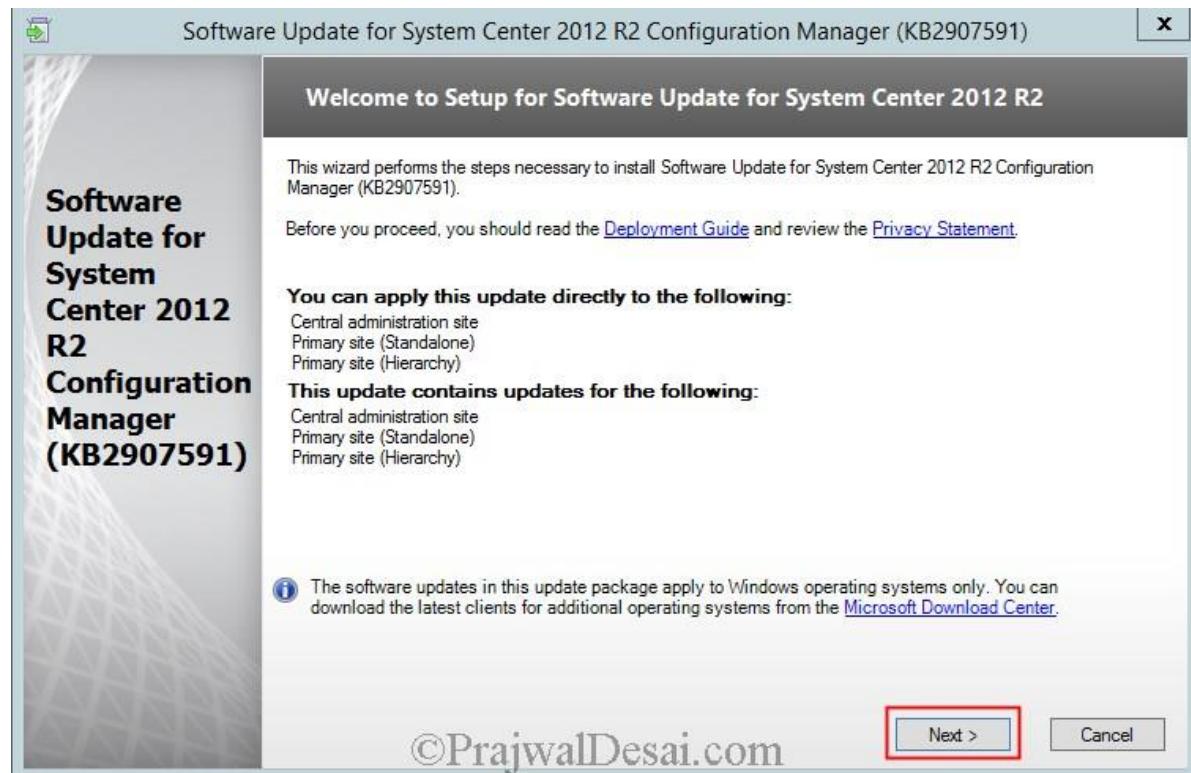
Per-computer variables for imported computers are not read in System Center 2012 R2 Configuration Manager

Per-computer task sequence variables that are defined for imported computers are filtered out of client policies. This prevents the variables from being read during task sequence execution. This problem does not affect per-computer variables that are defined for existing clients. **This update applies only to Primary sites.**

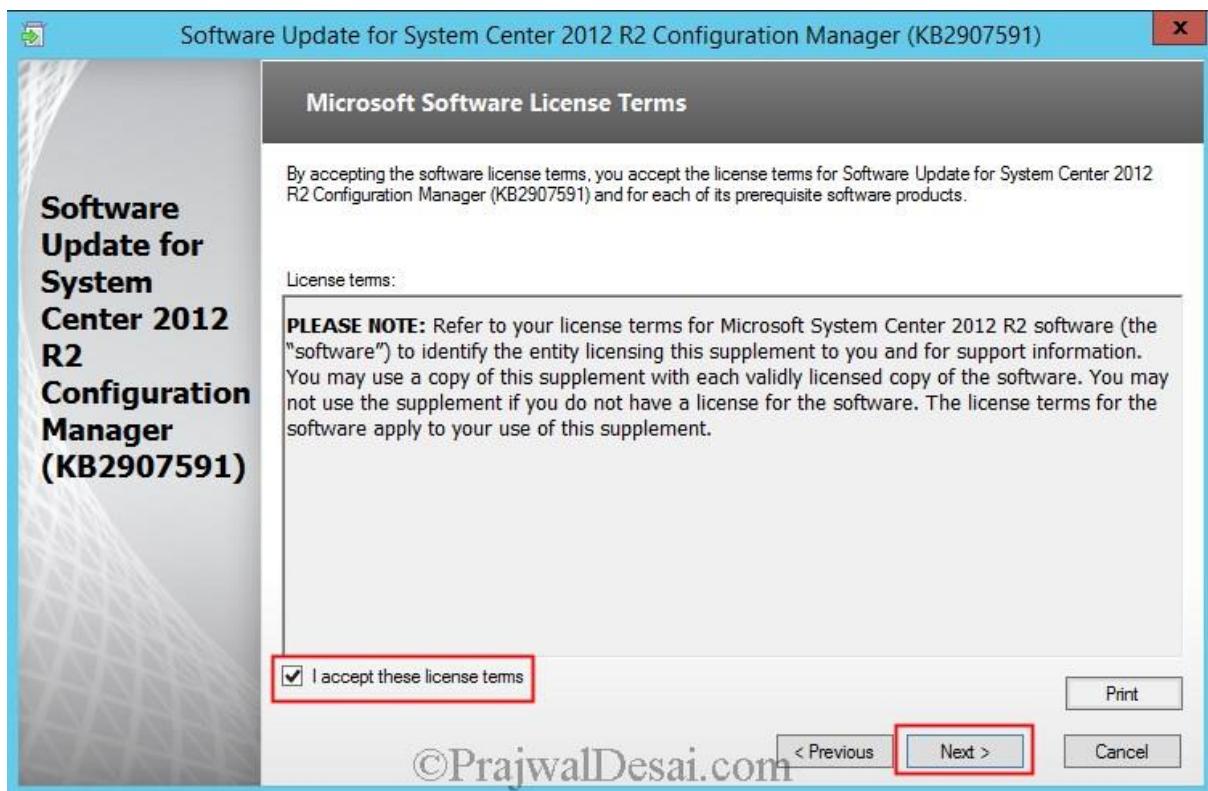
[Download Hotfix](#)

Installing Hotfix (KB2907591)

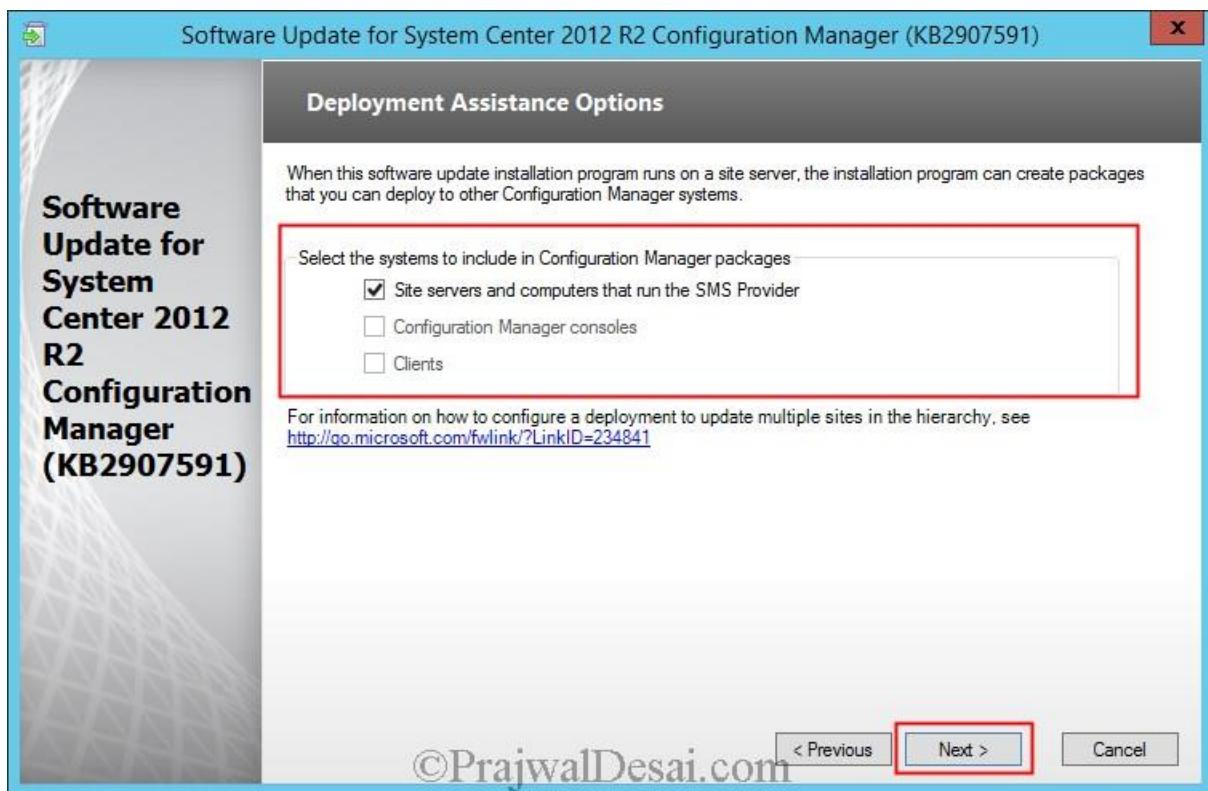
Log in to the machine where the Configuration Manager 2012 R2 is installed, extract the hotfix (**CM12-R2RTM-QFE-KB2907591-X64-ENU**) that you have downloaded and run the hotfix file. You will see the setup wizard **Software Update for System Center 2012 R2 Configuration Manager**. Click on **Next**.



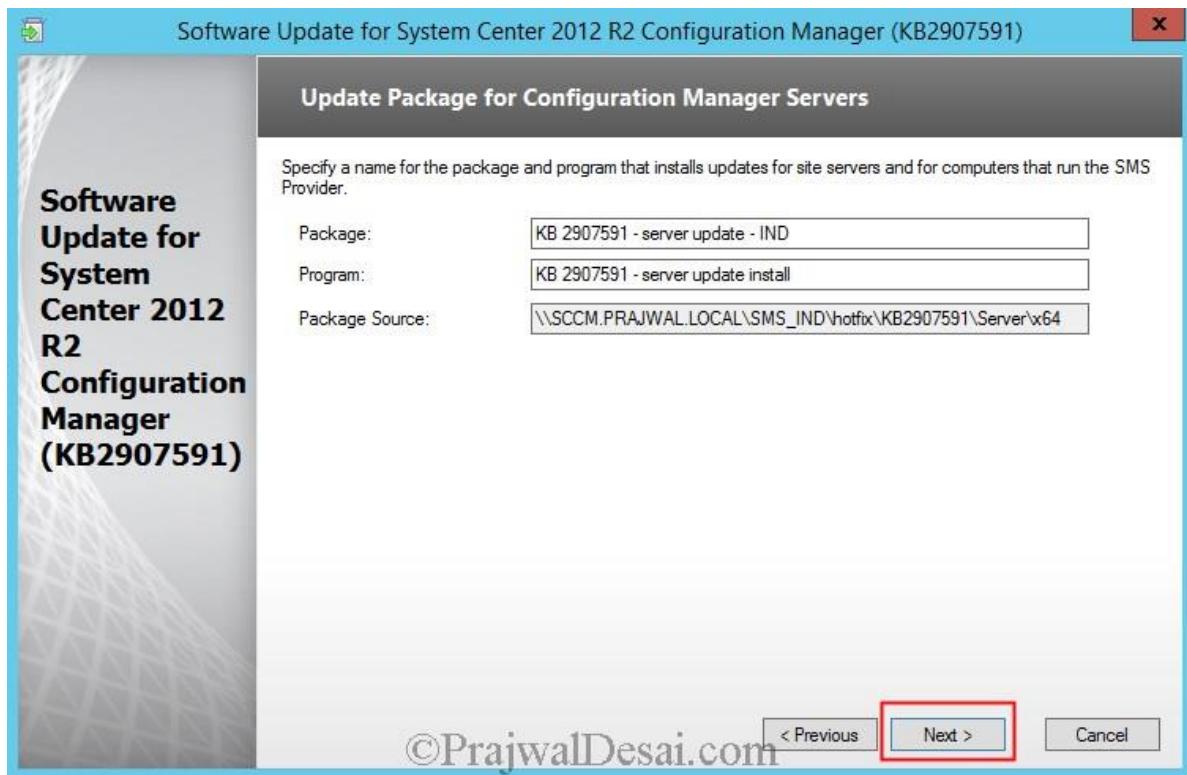
Click I accept these license terms and click on **Next**.



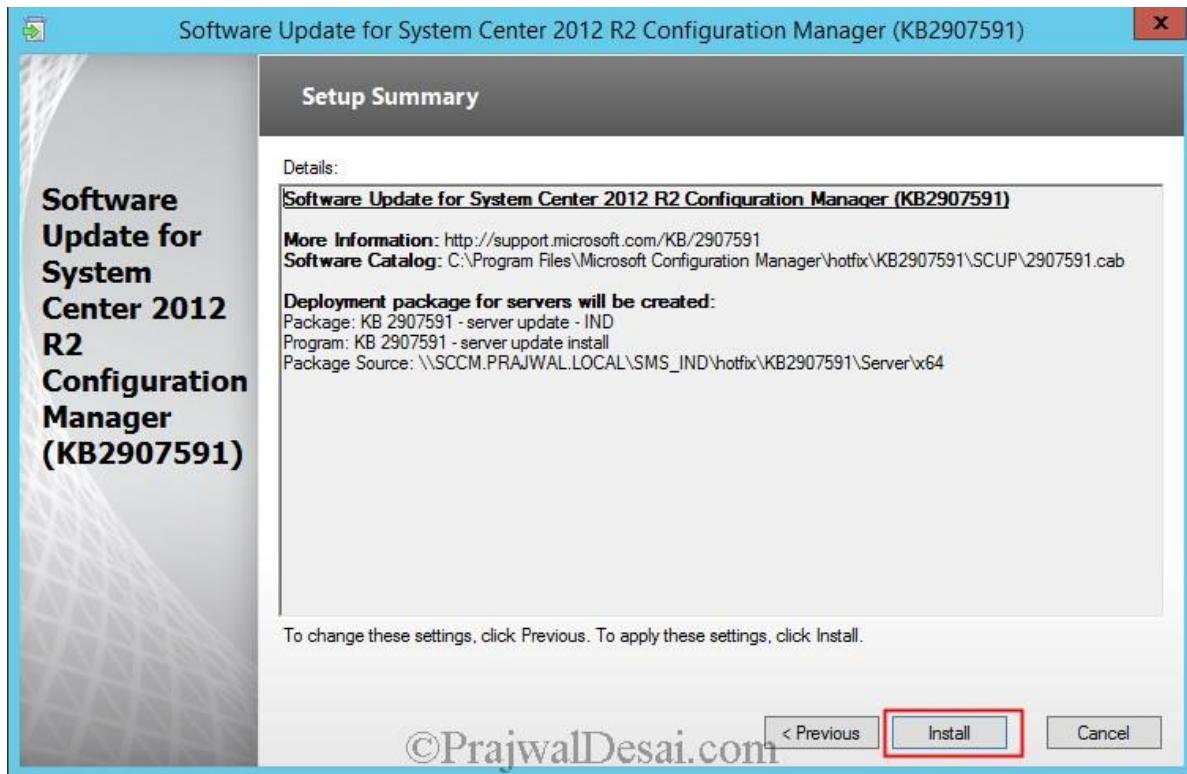
This hotfix updates only for Site servers that run SMS provider. Click **Next**.



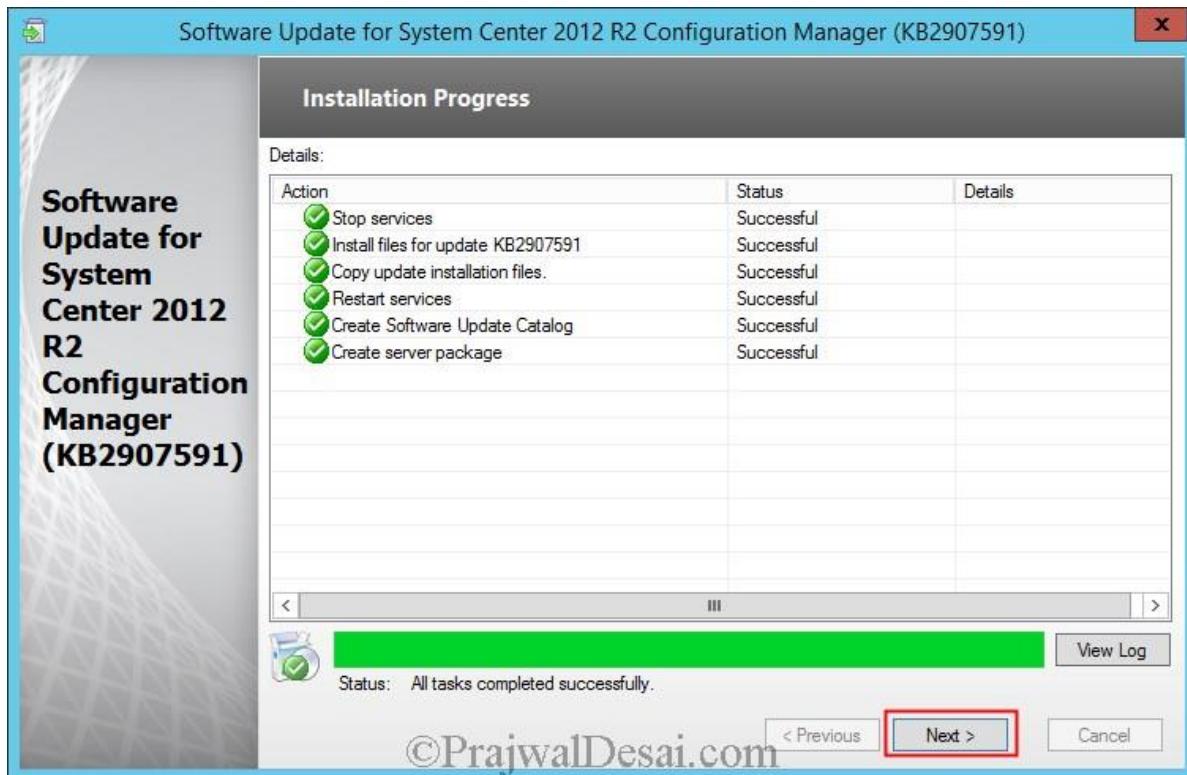
The name of the package for CM servers would be **KB 2907591-server update-Site Code**. Click on **Next**.



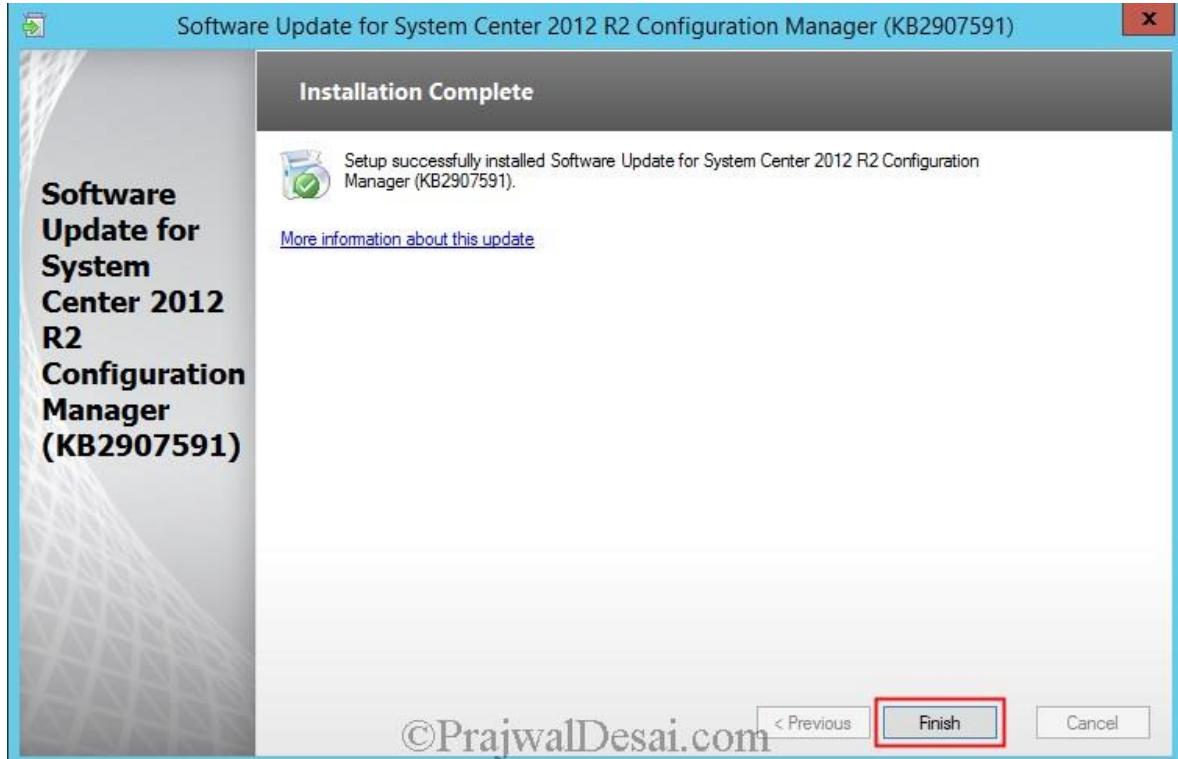
Click on **Install**.



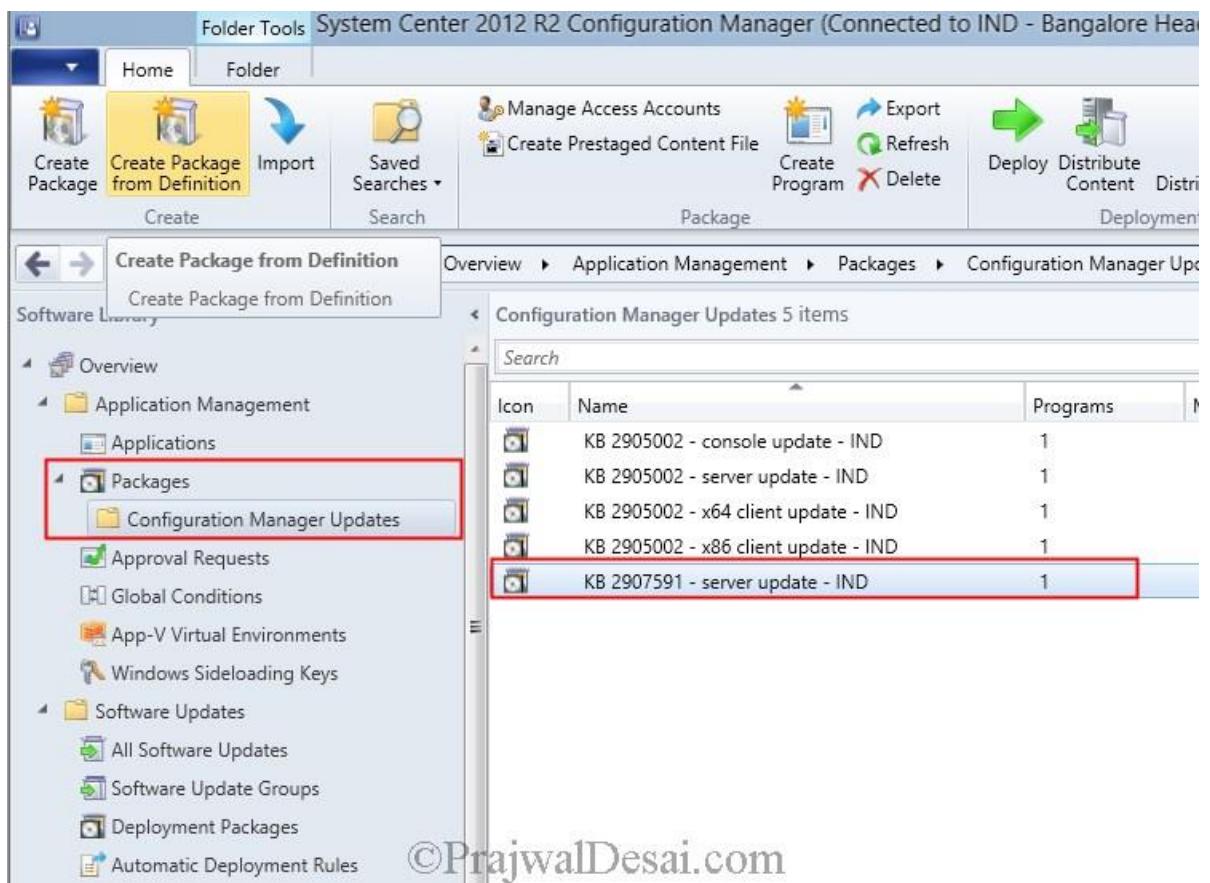
Click **Next**.



Click on **Finish**.



Launch the **Configuration Manager 2012 R2 console**, click on **Software Library**, expand **Overview**, expand **Application Management**, expand **Packages** and click on **Configuration Manager Updates**. On the right hand side of console you will see the packages that were created by this hotfix. In the below screenshot we see a new package **KB 2907591 – server update-IND** has been created.



After the update is installed on site servers, any operating system boot images should be updated. To update boot images after the hotfix is applied, open the Configuration Manager console, click **Software Library**, expand **Operating Systems**, and then click **Boot Images**, select the boot image that you want to update, right-click, and then select the **Update Distribution Points** action.

Configuring Discovery and Boundaries in Configuration Manager 2012 R2

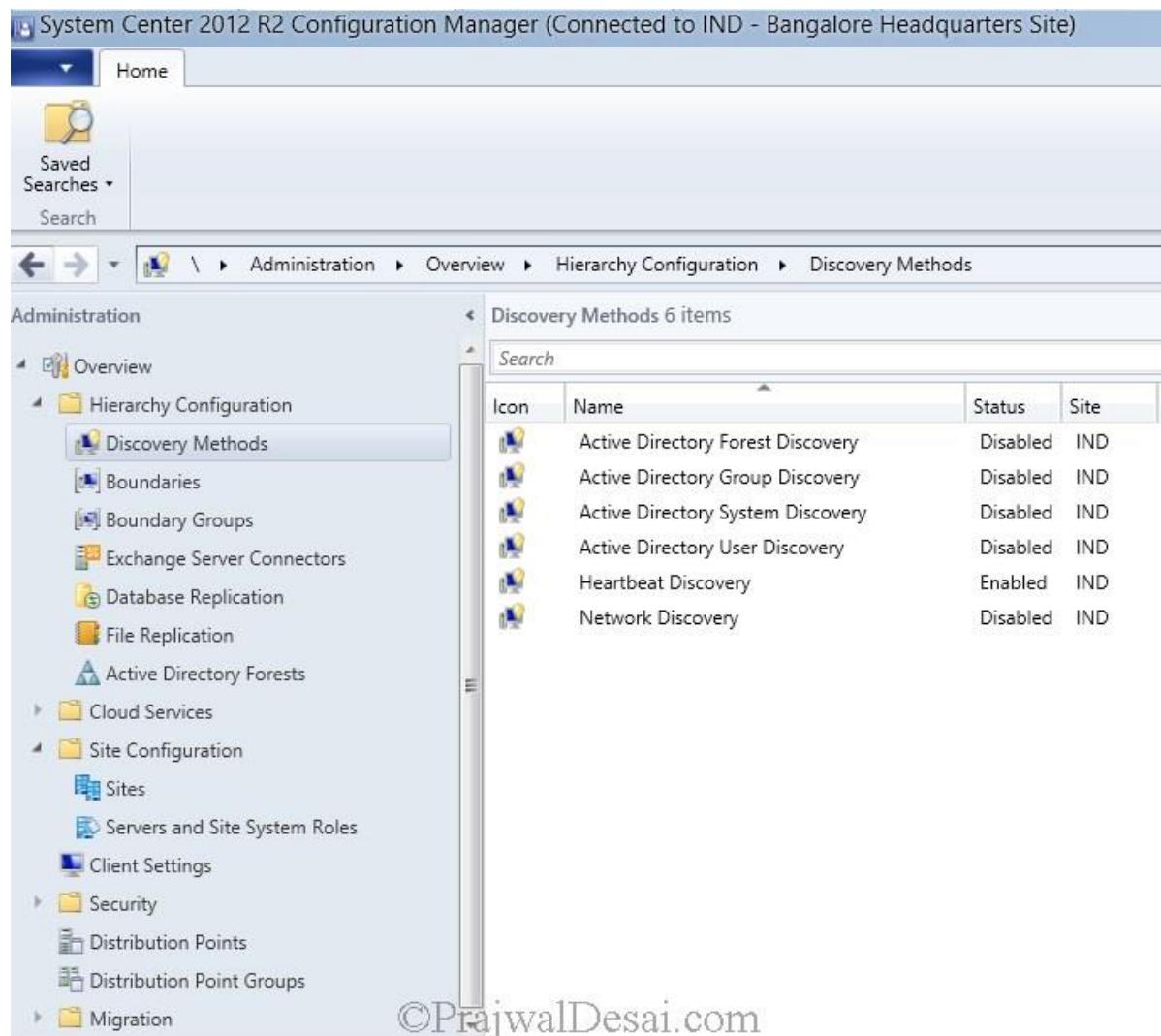
Configuring Discovery and Boundaries in Configuration Manager 2012 R2 In this post we will see the steps for configuring discovery and boundaries in configuration manager 2012 R2. In my previous deployment series of [SCCM 2012](#) and [SCCM 2012 SP1](#) we have seen much about the discovery methods and boundaries, this post is no different when it comes to configuring discovery and boundaries in configuration manager 2012 R2. We will begin with discovery methods available in configuration manager 2012 R2.

So what are discovery methods in configuration manager 2012 ? In simple terms when you have resources in your company and to gather the resource information, configuration manager 2012 R2 makes use of methods called discovery methods. Configuration Manager 2012 R2 uses a variety of discovery methods to gather resource information and each of the discovery methods gathers information about different objects. Lets see one by one..

Configuring Discovery and Boundaries in Configuration Manager 2012 R2

Active Directory Forest Discovery – As the name suggests it discovers Active Directory sites and subnets, and then creates Configuration Manager boundaries for each site and subnet from the forests which have been configured for discovery. With this discovery method you are able to automatically create the Active Directory or IP subnet boundaries that are within the discovered Active Directory Forests.

You can see in the below screenshot that except Heartbeat Discovery all the other discovery methods are disabled (not configured) by default.

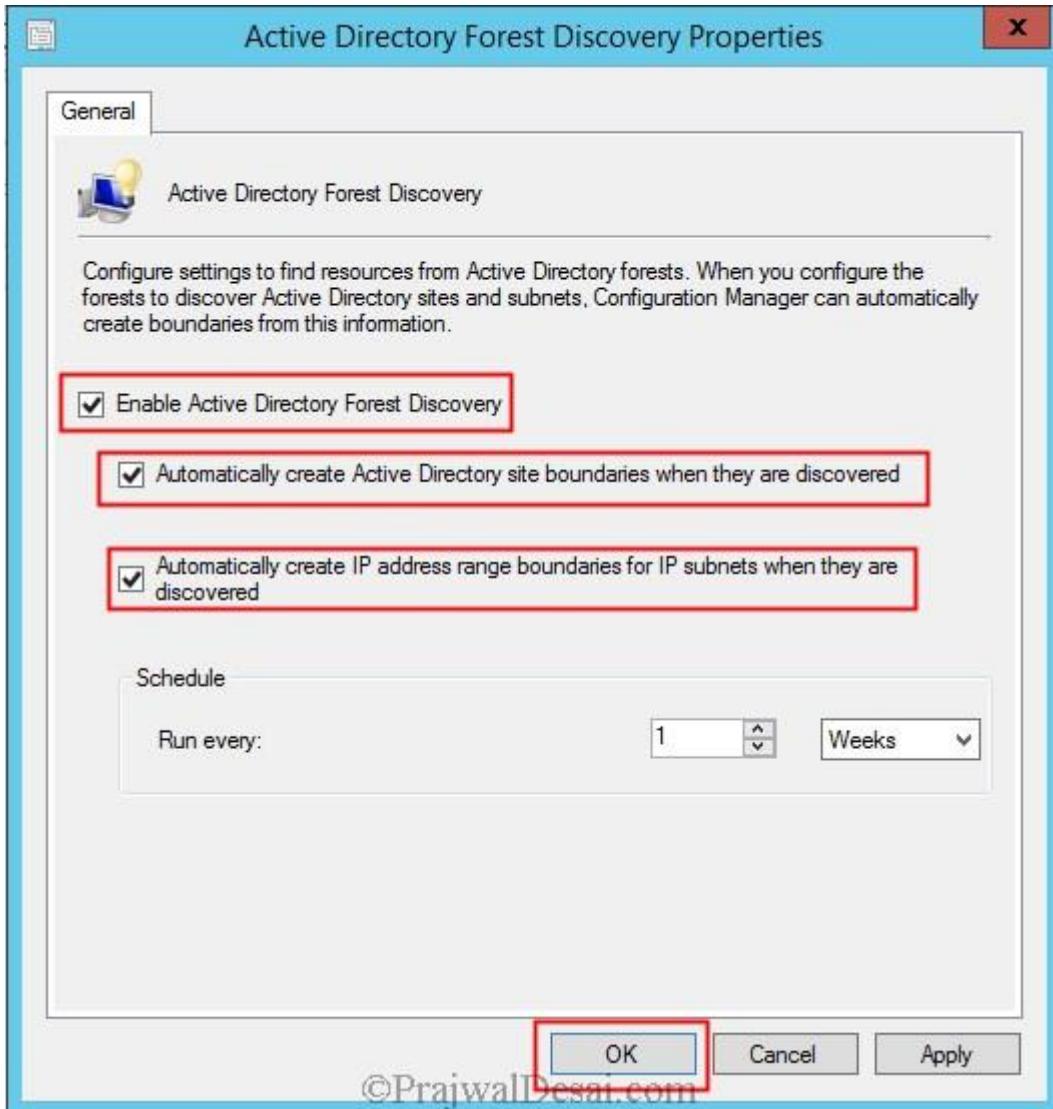


The screenshot shows the 'Discovery Methods' list in the Configuration Manager console. The left navigation pane is under 'Administration' > 'Hierarchy Configuration' > 'Discovery Methods'. The right pane displays a table titled 'Discovery Methods 6 items' with the following data:

Icon	Name	Status	Site
[Icon]	Active Directory Forest Discovery	Disabled	IND
[Icon]	Active Directory Group Discovery	Disabled	IND
[Icon]	Active Directory System Discovery	Disabled	IND
[Icon]	Active Directory User Discovery	Disabled	IND
[Icon]	Heartbeat Discovery	Enabled	IND
[Icon]	Network Discovery	Disabled	IND

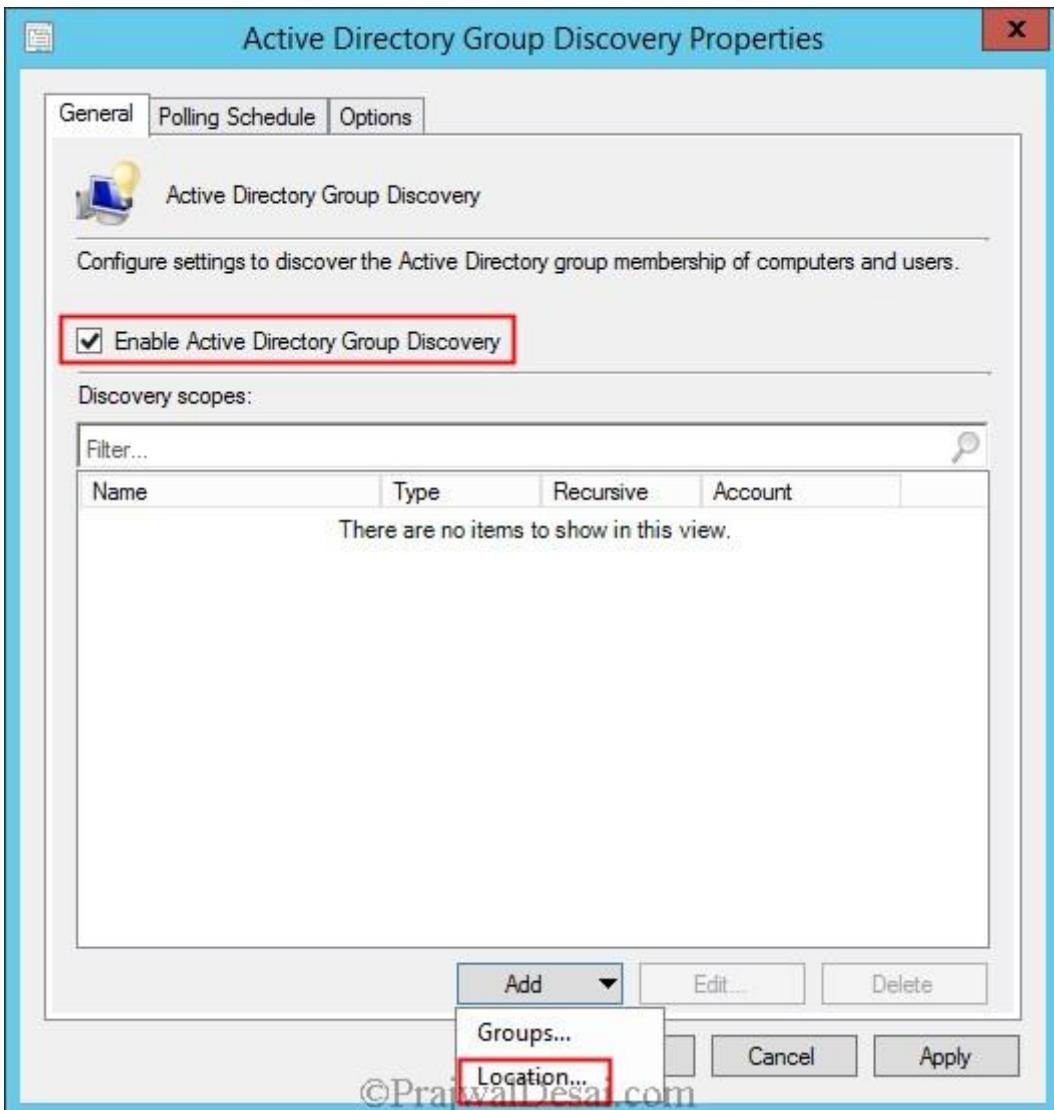
©PrajwalDesai.com

Launch the System Center 2012 Configuration Manager R2 Console. On the left pane select the **Administration**, expand **Hierarchy Configuration**, Select **Discovery Methods**. On the right pane double click “**Active Directory Forest Discovery**”. Check all the boxes to enable the **AD Forest Discovery**. With this all the Active Directory site boundaries are created automatically along with IP address boundaries. Click on **Apply**. When you click on **Apply**, it asks you to **run the full discovery as soon as possible**. Click on **Yes**. Click on **OK**.

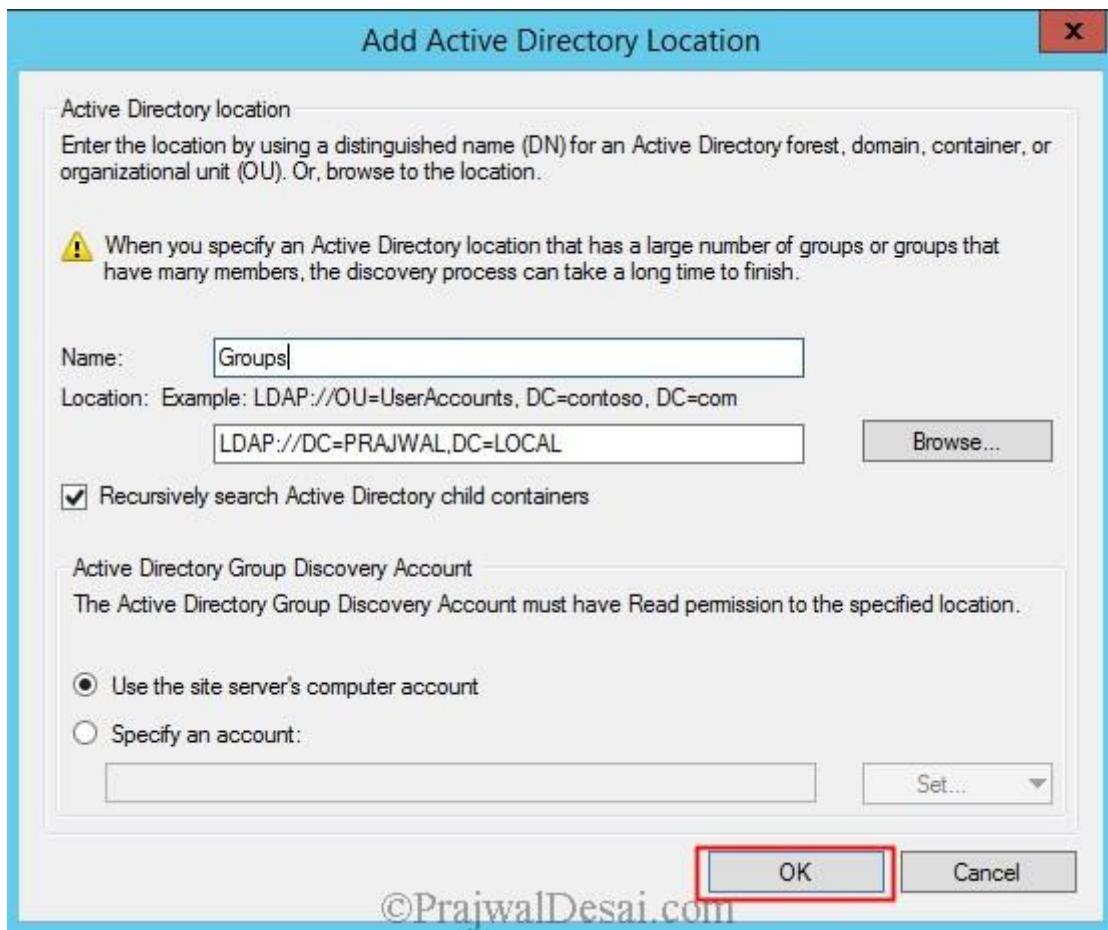


Active Directory Group Discovery – The Active Directory Group Discovery discovers the groups from the defined location in the Active Directory. The Discovery Process discovers local, global, and universal security groups, the membership within these groups. When you configure the Group discovery you have the option to discover the membership of distribution groups. With the Active Directory Group Discovery you can also discover the computers that have logged in to the domain in a given period of time.

To enable the **Active Directory Group Discovery**, Double click the **Active Directory Group Discovery** and check the box which says “**Enable Active Directory Group Discovery**“. Once you do that at the bottom you must add the Groups or the Location. Click on **Add** and click on **Location**.



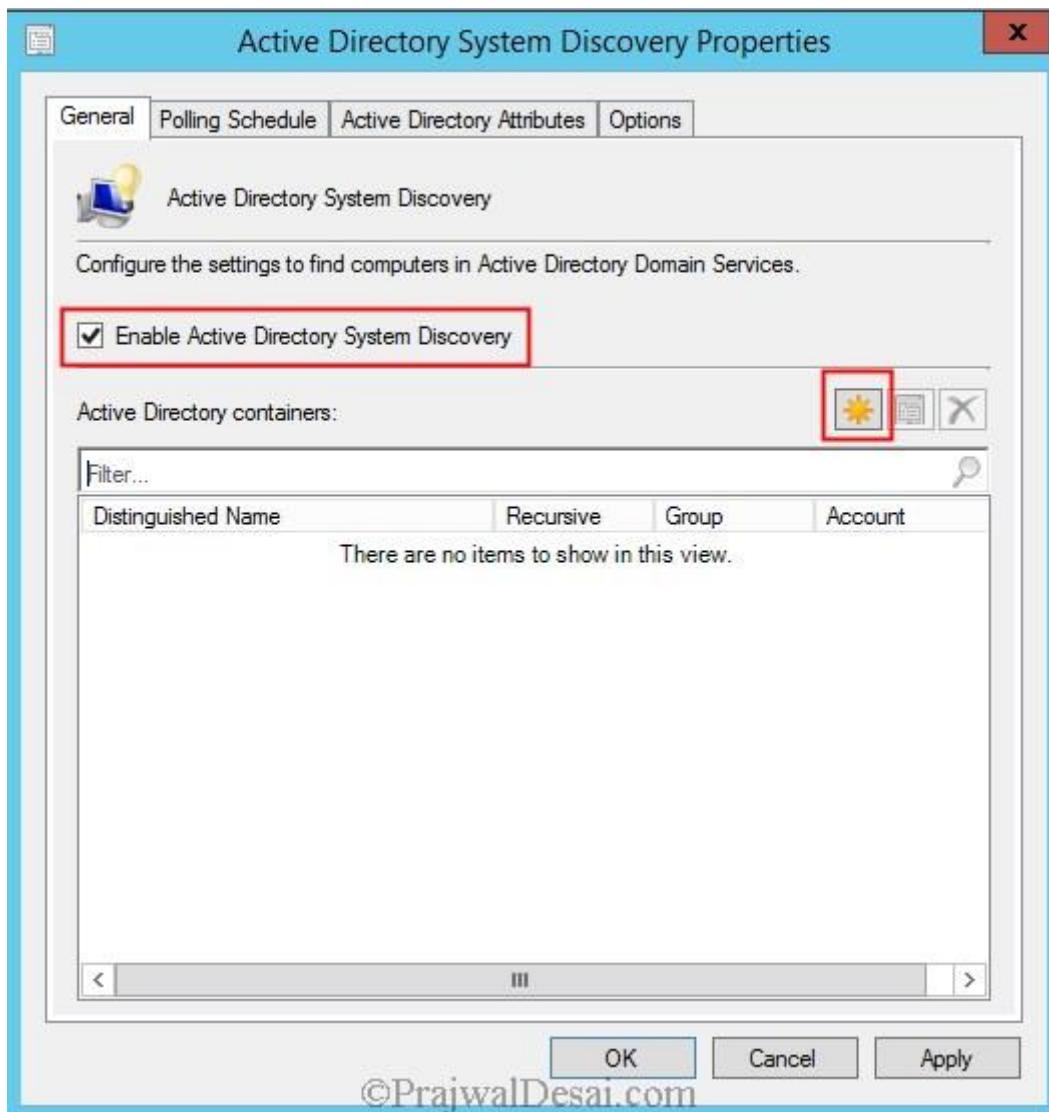
Click Browse to specify the location. Select the **Active Directory Container**. In this example I have selected the Domain **PRAJWAL.LOCAL**. Click on **Apply**. When you click on **Apply**, it asks you to **run the full discovery as soon as possible**. Click on **Yes**. Click on **OK**.



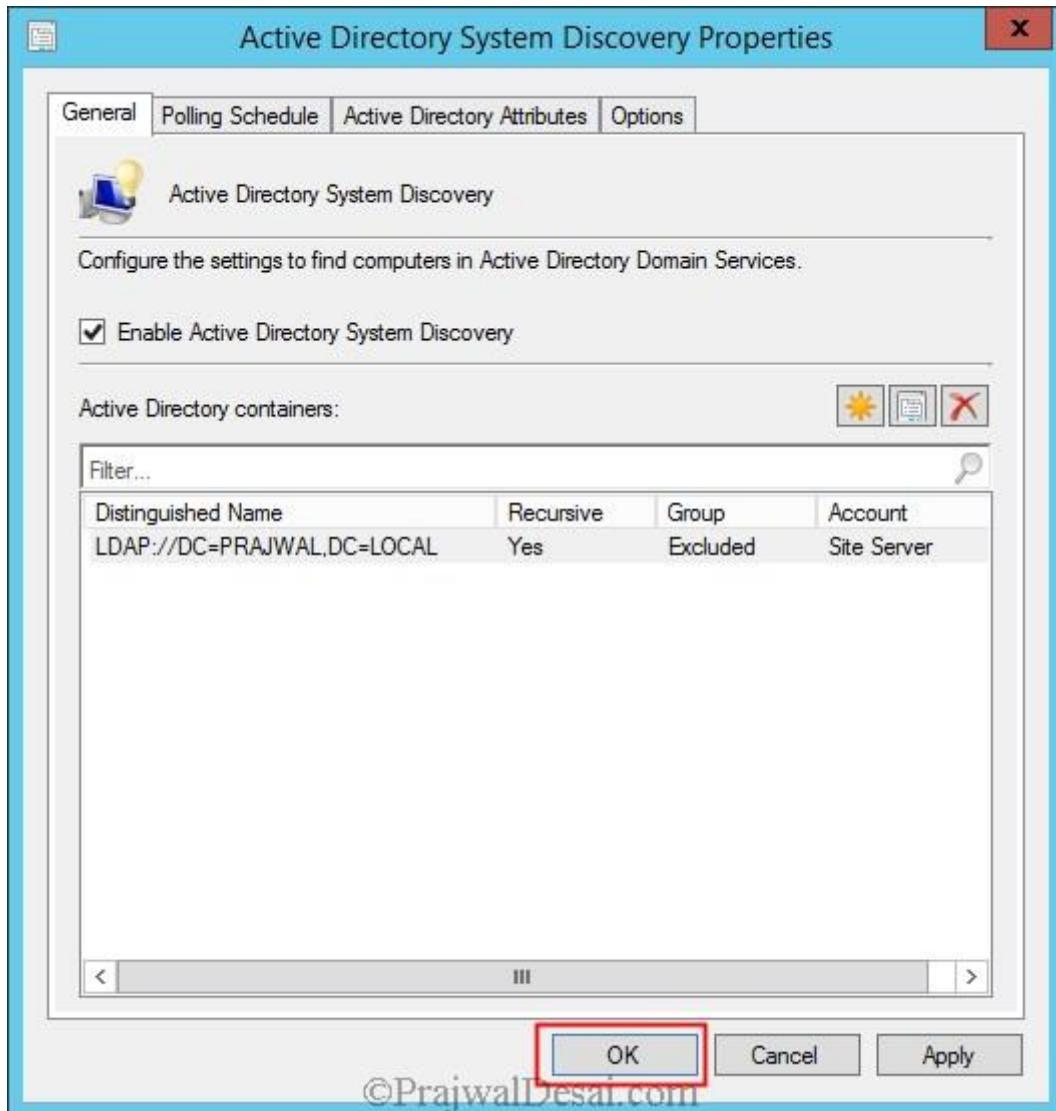
©PrajwalDesai.com

Active Directory System Discovery – If you want to discover the computers in your organization from specified locations in Active Directory Domain Services then we use Active Directory System Discovery. In order to push the SCCM clients into the computers, the resources must be discovered first. There is an option to discover the computers that have logged on to a domain in given period of time, this way you won't discover obsolete computer accounts from the Active Directory.

Right Click Active Directory System Discovery and click on properties. Click on **Enable Active Directory System Discovery**.

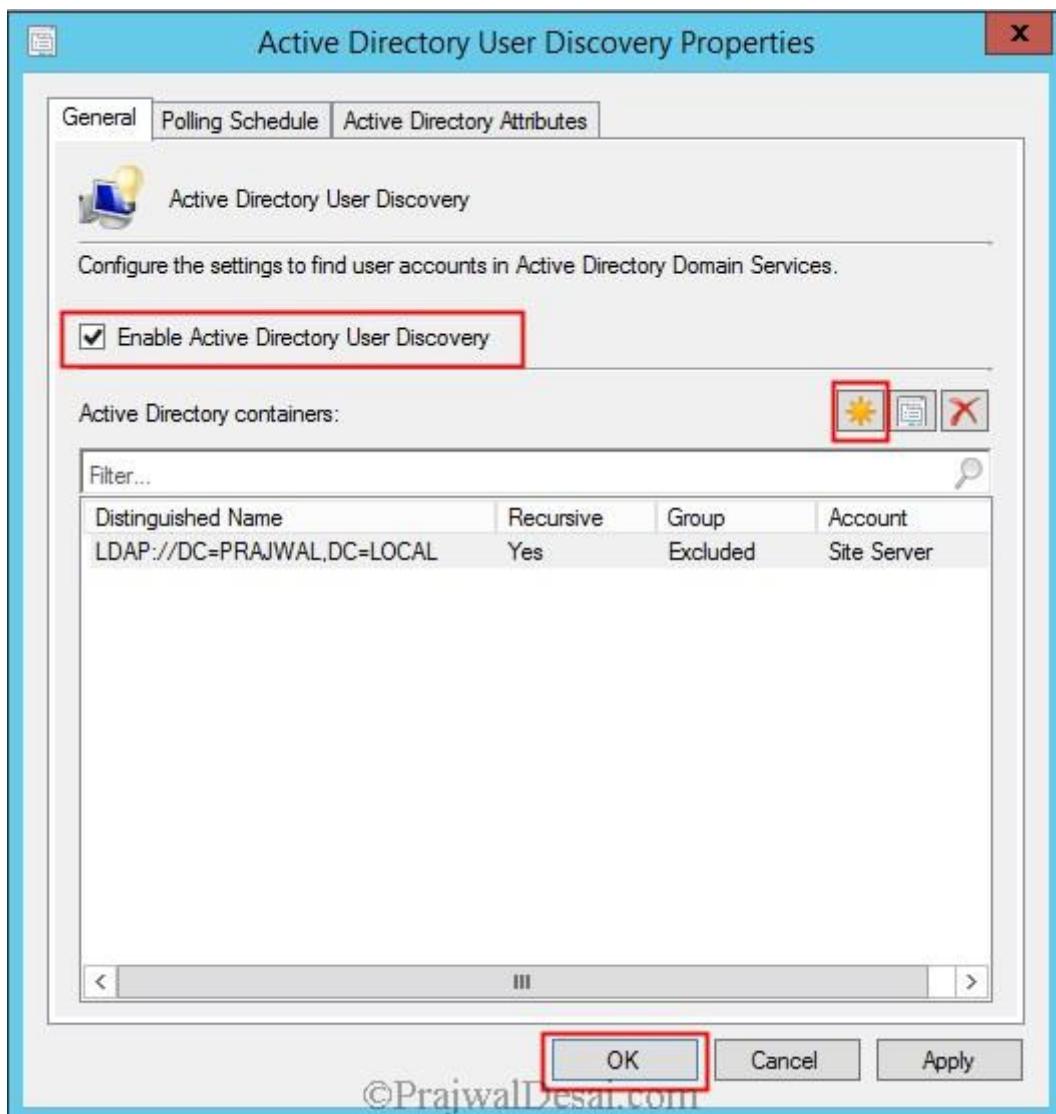


To add the Active Directory Containers click on the Orange color icon. Click on **Browse** and select the **domain**. click **OK**. Click on **Apply**. Run the **full discovery** by clicking **Yes**. Click on **OK** and close the properties page.



Active Directory User Discovery – This Discovery process discovers the user accounts from your Active Directory domain. You will have to specify the Active Directory container to search for the user accounts. There are some good options to discover the user accounts like the option to discover the user objects based on the attributes, recursively search AD child containers, discover objects within the AD groups.

Double click the **Active Directory User Discovery**, Enable the **Active Directory User Discovery**. select the **Active Directory Container**. Click on **OK**.



HeartBeat Discovery – The HeartBeat Discovery runs on every Configuration Manager client and is used by Active Configuration Manager clients to update their discovery records in the database. The records (Discovery Data Records) are sent to the management point in specified duration of time. Heartbeat Discovery can force discovery of a computer as a new resource record, or can repopulate the database record of a computer that was deleted from the database. Note that the HeartBeat Discovery is enabled by default and is scheduled to run every 7 days.

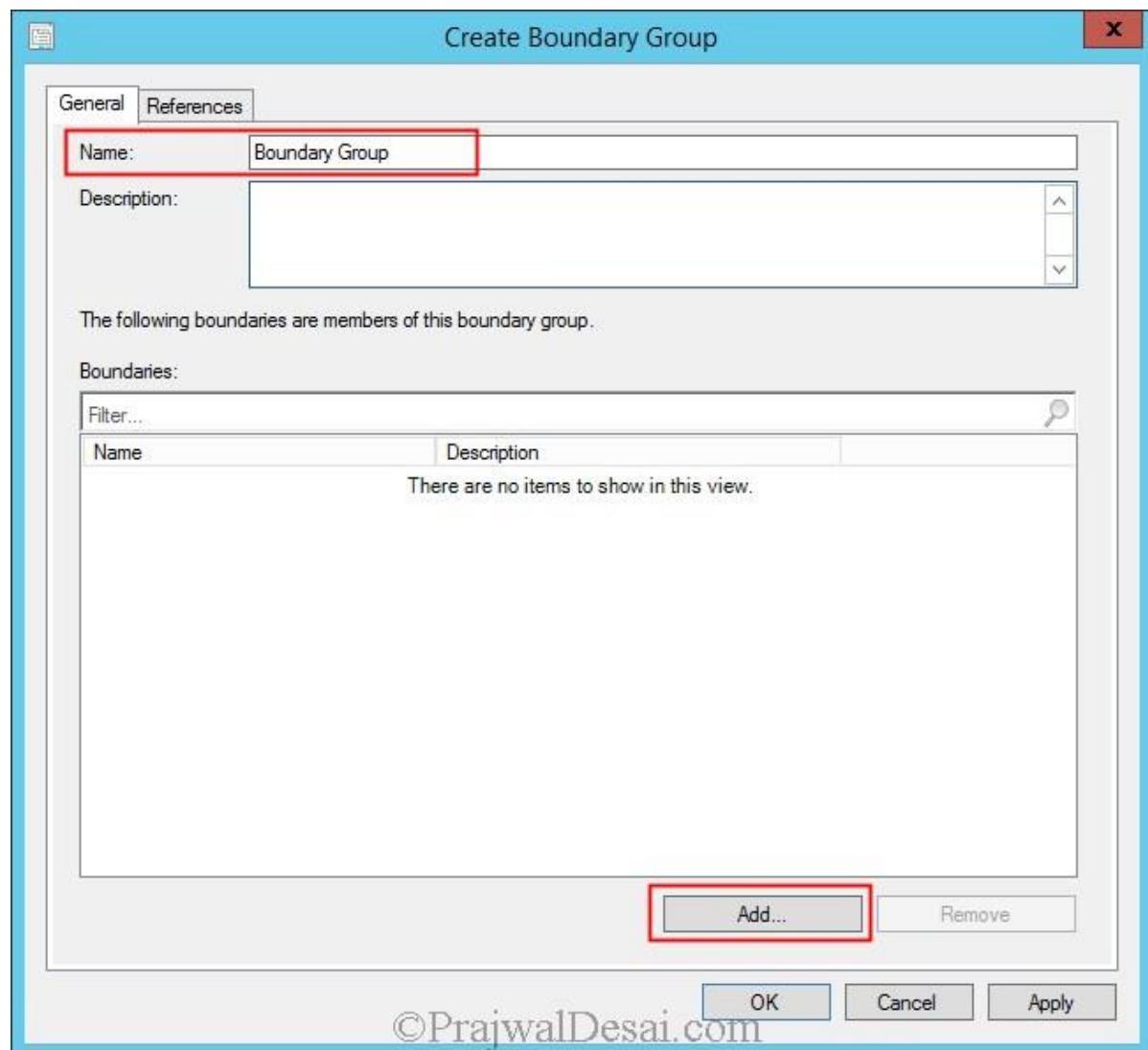
Network Discovery – The Network Discovery searches your network infrastructure for network devices that have an IP address. It can search the domains, SNMP devices and DHCP servers to find the resources. It also discovers devices that might not be found by other discovery methods. This includes printers, routers, and bridges. In this post we will not configure the Network Discovery method as its not required here.

Concept Of Boundaries – A boundary is a network location on the intranet that can contain one or more devices that you want to manage. Boundaries can be an IP subnet, Active Directory site name, IPv6 Prefix, or an IP address range, and the hierarchy can include any combination of these boundary types. To use a boundary, you must add the boundary to one or more boundary groups. Boundary groups are collections of boundaries. By using boundary

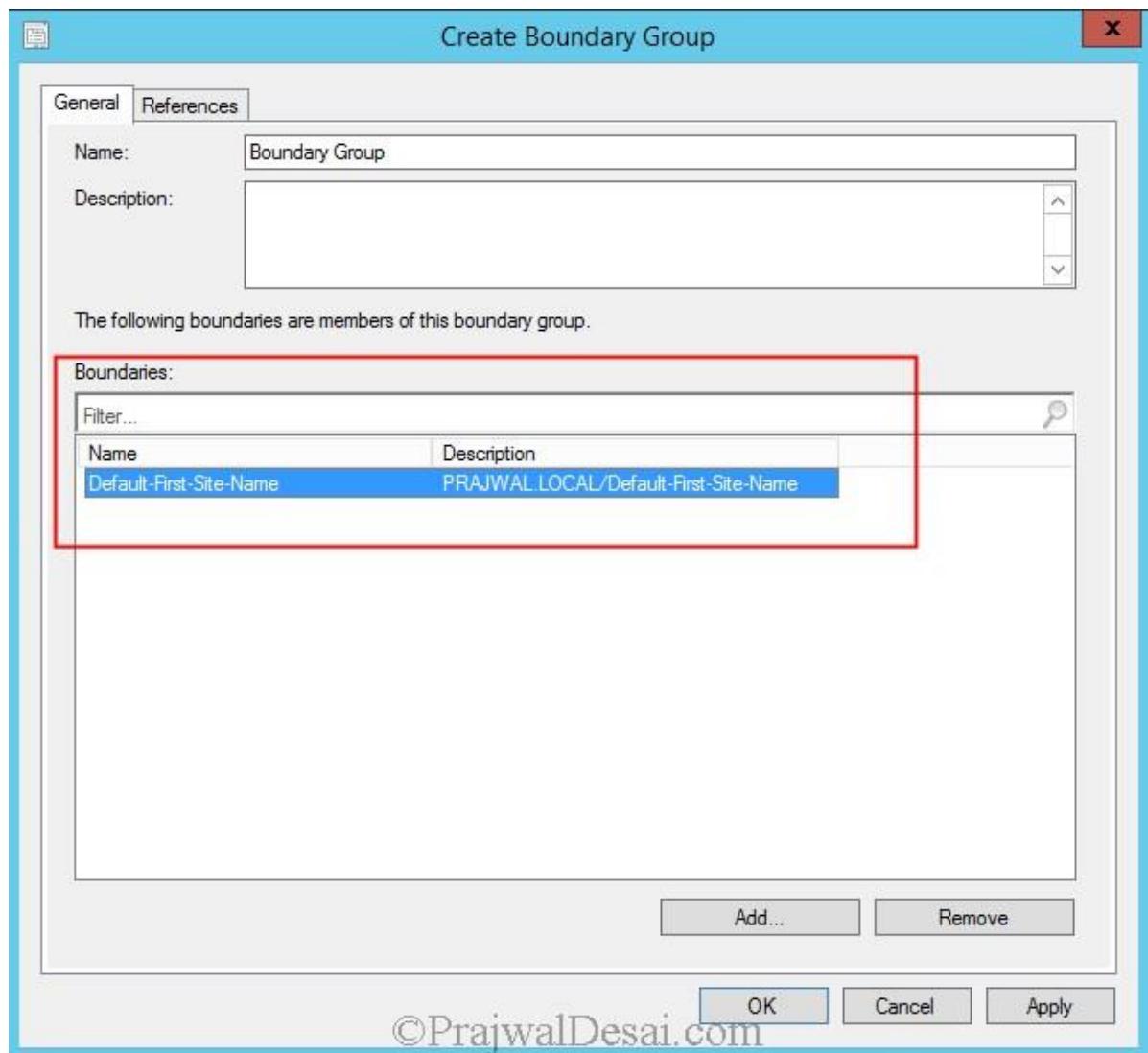
groups, clients on the intranet can find an assigned site and locate content when they have to install software, such as applications, software updates, and operating system images.

Note – When we run the Active Directory Forest Discovery, the boundaries are discovered automatically.

Since we have run the Active Directory Forest Discovery method we need not create a boundary here, we will create a Boundary Group. Now we need to add the Boundary to the **Boundary groups**. In the Configuration Manager console, select **Boundary Groups**, right click and click on **create a boundary group**. Provide a name to the boundary group and click on **Add**.

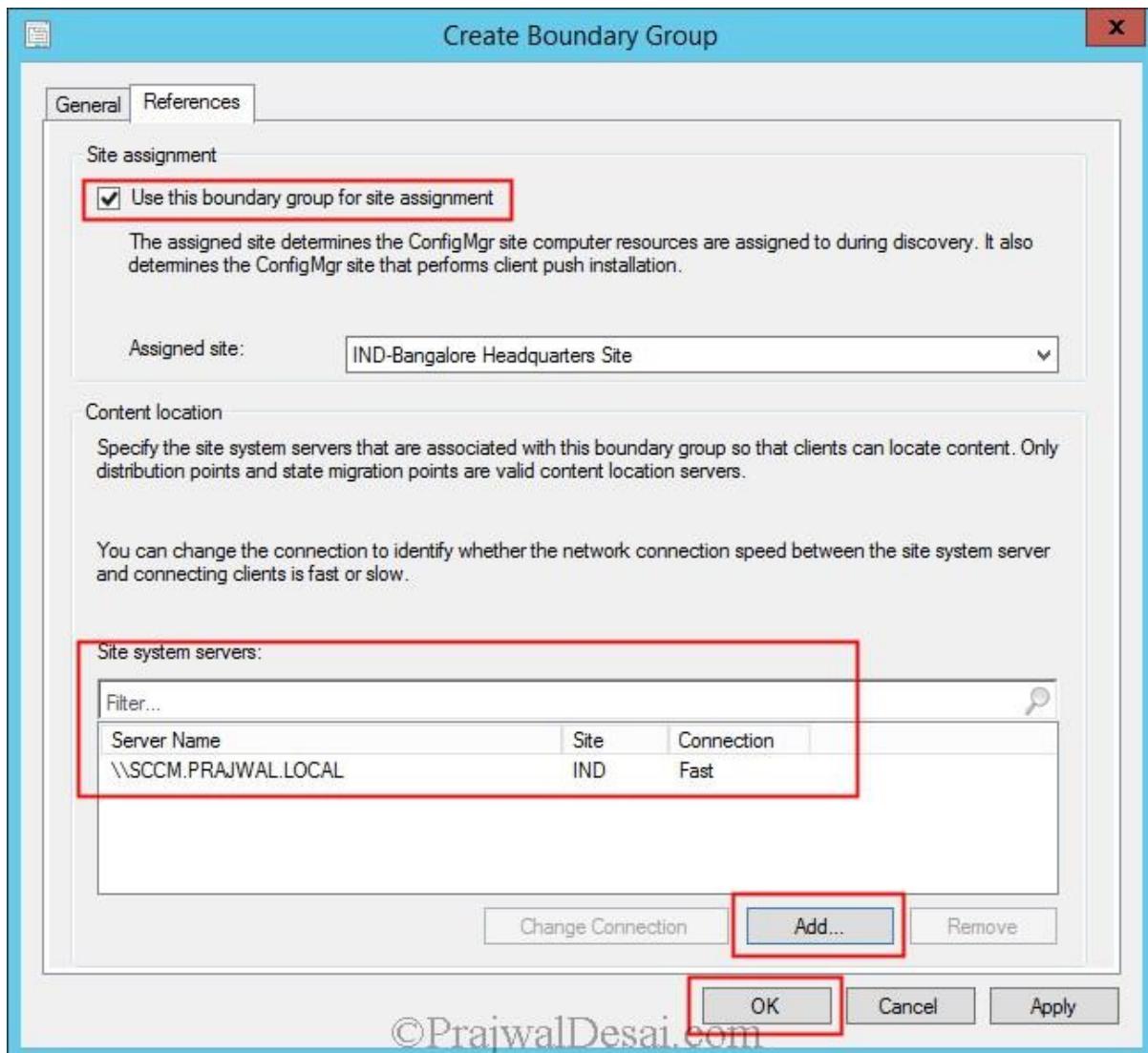


On the **Add Boundaries** window select the boundary, in our case there is only one discovered boundary and that is the **Default-First-Site-Name**. Click on **Apply**.



©PrajwalDesai.com

Click on **References tab**, check **Use this Boundary group for site assignment**. To add the site system servers, click **Add** and select the **Site System Server**. Click on **OK**.



©PrajwalDesai.com

Installing Site System Roles in Configuration Manager 2012 R2

In this post we see the steps for installing site system roles in configuration manager 2012 R2. These roles are added to extend the management functionality of the site. In this post we will be installing the Application catalog website point, Application catalog web service point and Fallback status point. There are many sites system roles available in configuration manager 2012 R2, we shall install them when it is required. You can find the step-by-step guide for SCCM 2012 R2 [here](#).

Before we start installing site system roles in configuration manager 2012 R2 we will see a brief description about each and every site system role.

Site System Roles

Site System Role – A computer on which you run the Configuration Manager setup program and which provides the core functionality for the site. Any computer, either server or workstation, hosting a site system role is referred to as a site system server.

Site Database Server – Site Database Server hosts the SQL Server database, which stores information about Configuration Manager assets and site data.

Component server – This is any server running the ConfigMgr Executive service.

Management point – Provides policy and service location information to clients and receives configuration data from clients. The Management Point facilitates communication between a client and site server by storing and providing policy and content location information to the client, and receiving data from the client such as status messages and inventory.

Distribution point – Contains source files for clients to download, such as application content, software packages, software updates, operating system images, and boot images.

Reporting services point – This role is used to integrate reporting through SQL Server Reporting Services and is required if using reports.

State migration point – Stores user state data when a computer is migrated to a new operating system during OSD.

Software update point – Integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients.

System Health Validator point – Validates Configuration Manager Network Access Protection (NAP) policies. This role must be installed only on a NAP health policy server.

Endpoint Protection point – This is an optional site system role that Configuration Manager uses to accept the Endpoint Protection license terms and to configure the default membership for Microsoft Active Protection Service.

Fallback status point – The FSP provides an alternative location for clients to send up status messages during installation when they cannot communicate with

their management point. This role helps you monitor client installation and identify the clients that are unmanaged because they cannot communicate with their management point.

Out of band service point – Provisions and configures Intel AMT-based computers for out of band management.

Asset Intelligence synchronization point – Connects to System Center Online to download Asset Intelligence catalog information and upload uncategorized titles so that they can be considered for future inclusion in the catalog.

Application Catalog web service point – Provides software information to the Application Catalog website from the Software Library.

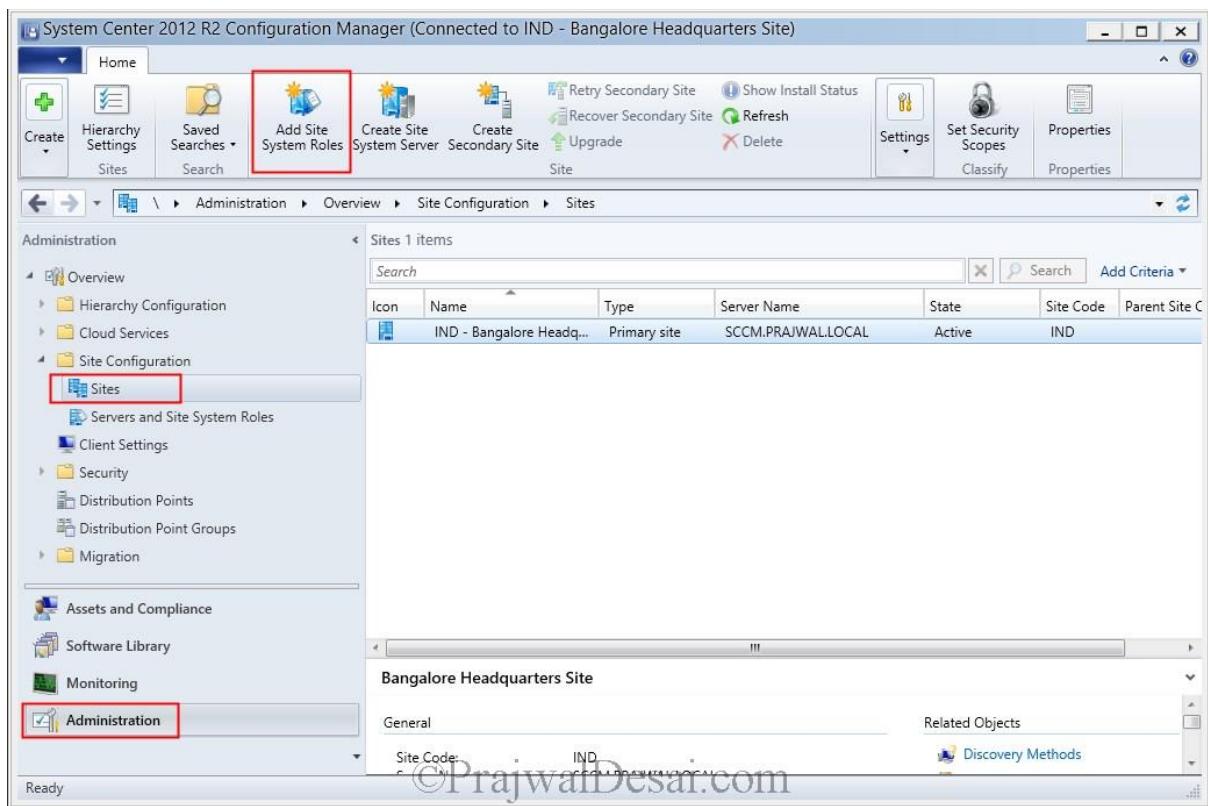
Application Catalog website point – Provides users with a list of available software from the Application Catalog.

Enrollment proxy point – Manages enrollment requests from mobile devices so that they can be managed by Configuration Manager.

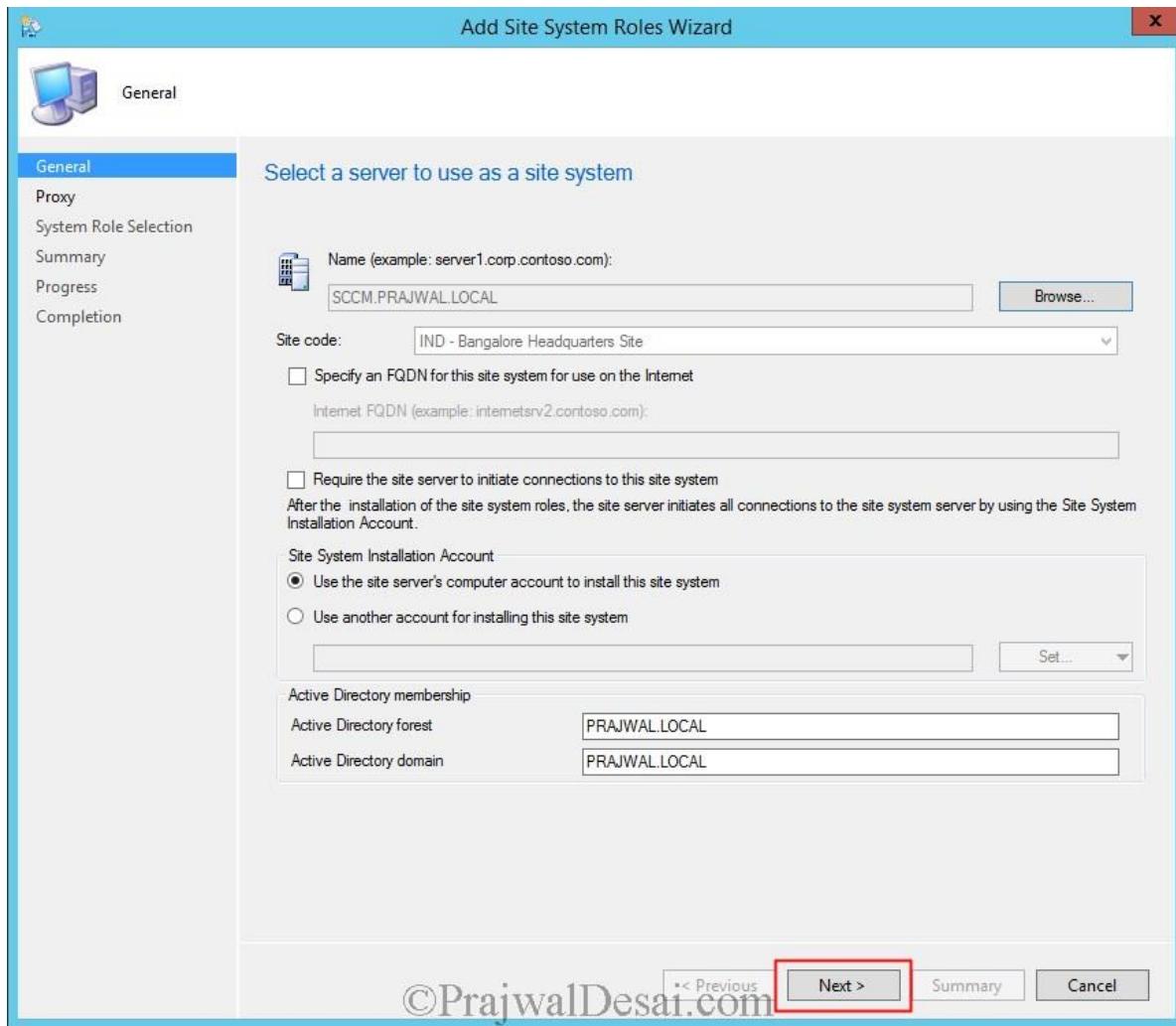
Enrollment point – Uses PKI certificates to complete mobile device enrollment and to provision Intel AMT-based computers.

Installing Site System Roles In Configuration Manager 2012 R2 is pretty simple but you must check if the role is really required. In this post we will be installing **Application Catalog web service point**, **Application Catalog website point** and **Fallback status point**. Application Catalog Website Point system role provides users with a list of available software. When the SCCM client is installed on a computer, the software center includes a link to Application Catalog. The Application Catalog shows the users, list of available softwares. This will be possible only when you install the roles. The Application Catalog Web Service Point system role provides information about available software from the Software Library to the Application Catalog website.

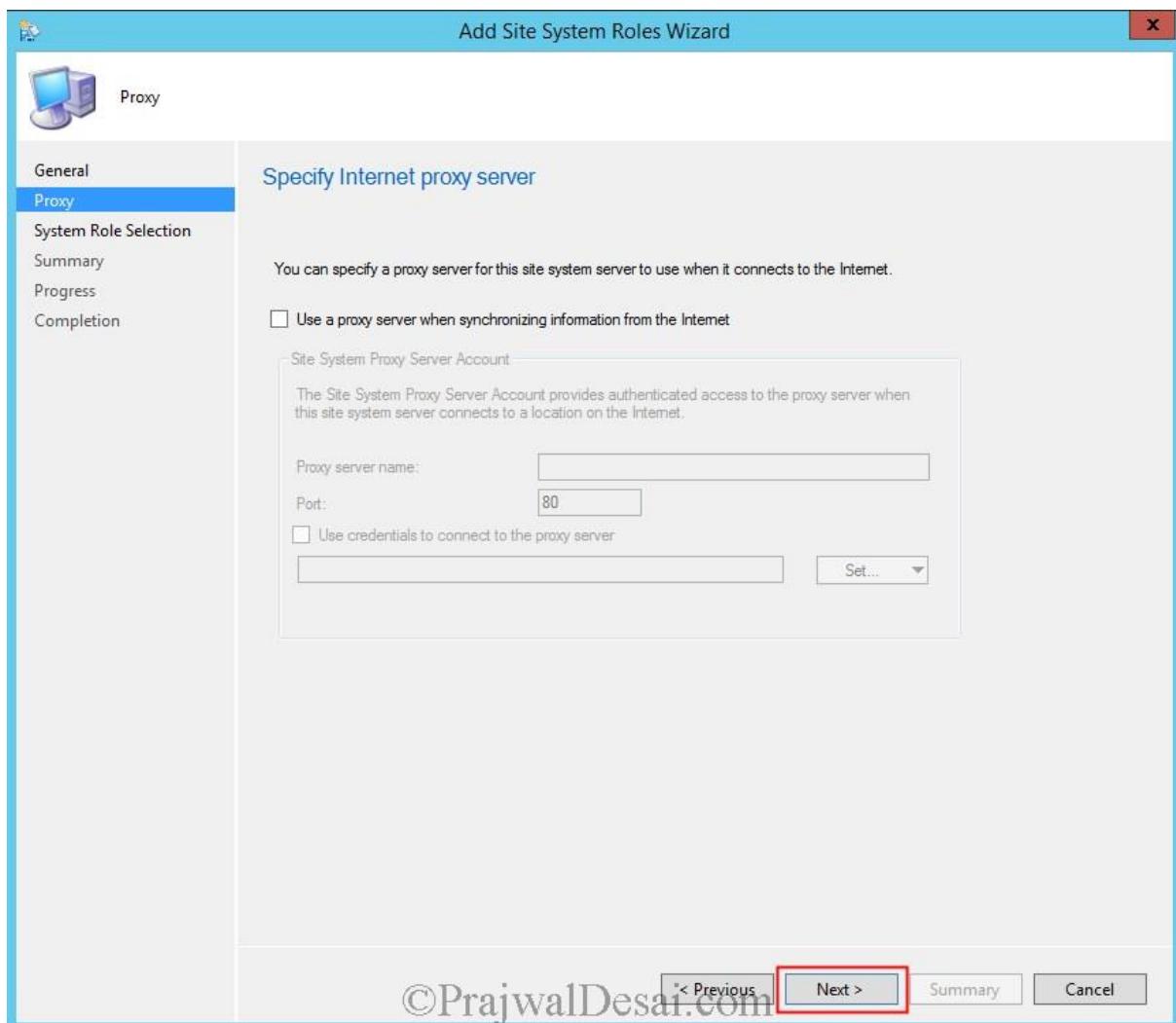
Open the **Configuration Manager console**, Select **Administration**, Under **Site Configuration** select **Sites**. Click on **Add Site System Roles**.



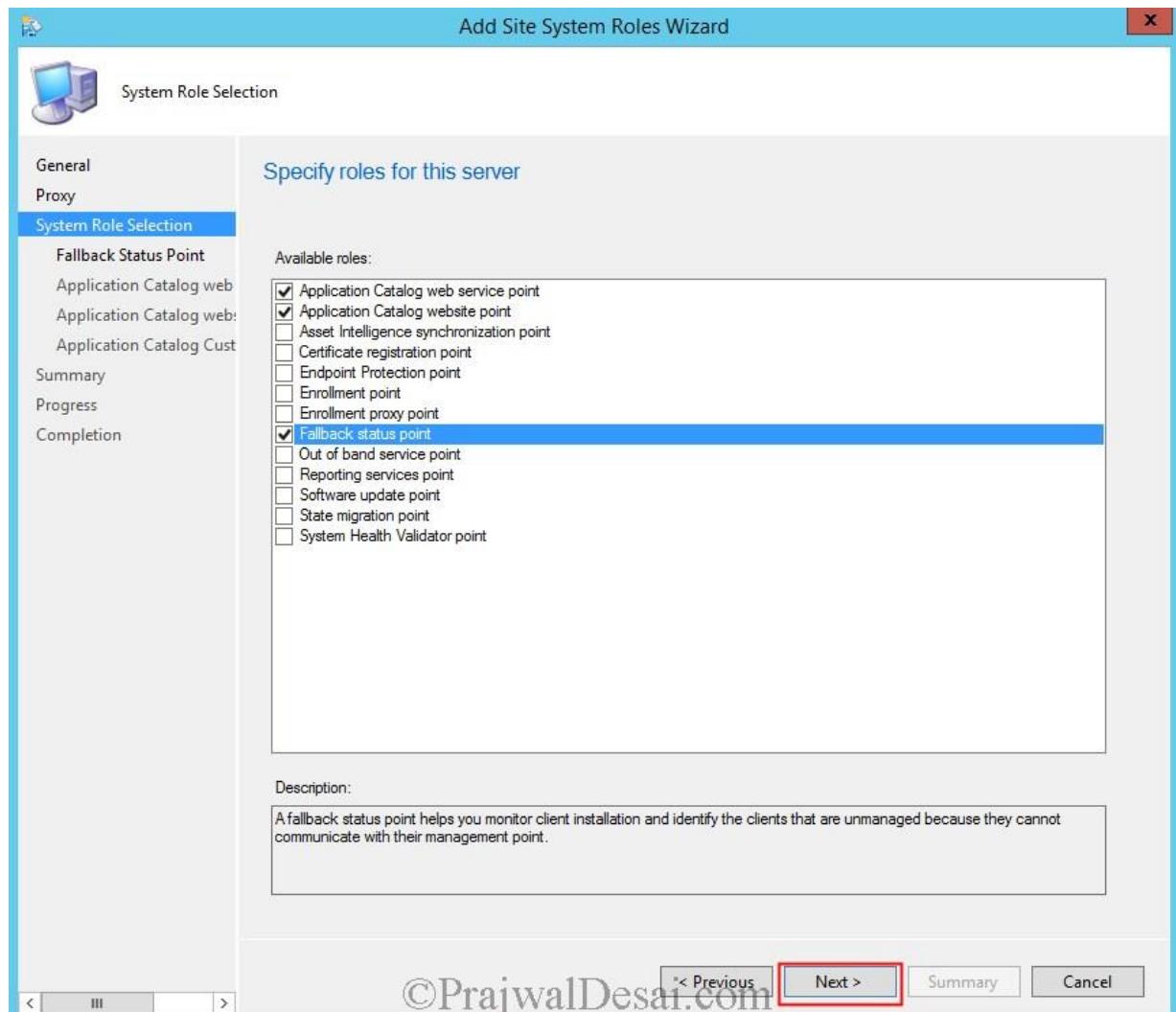
Leave this page to default and click on **Next**.



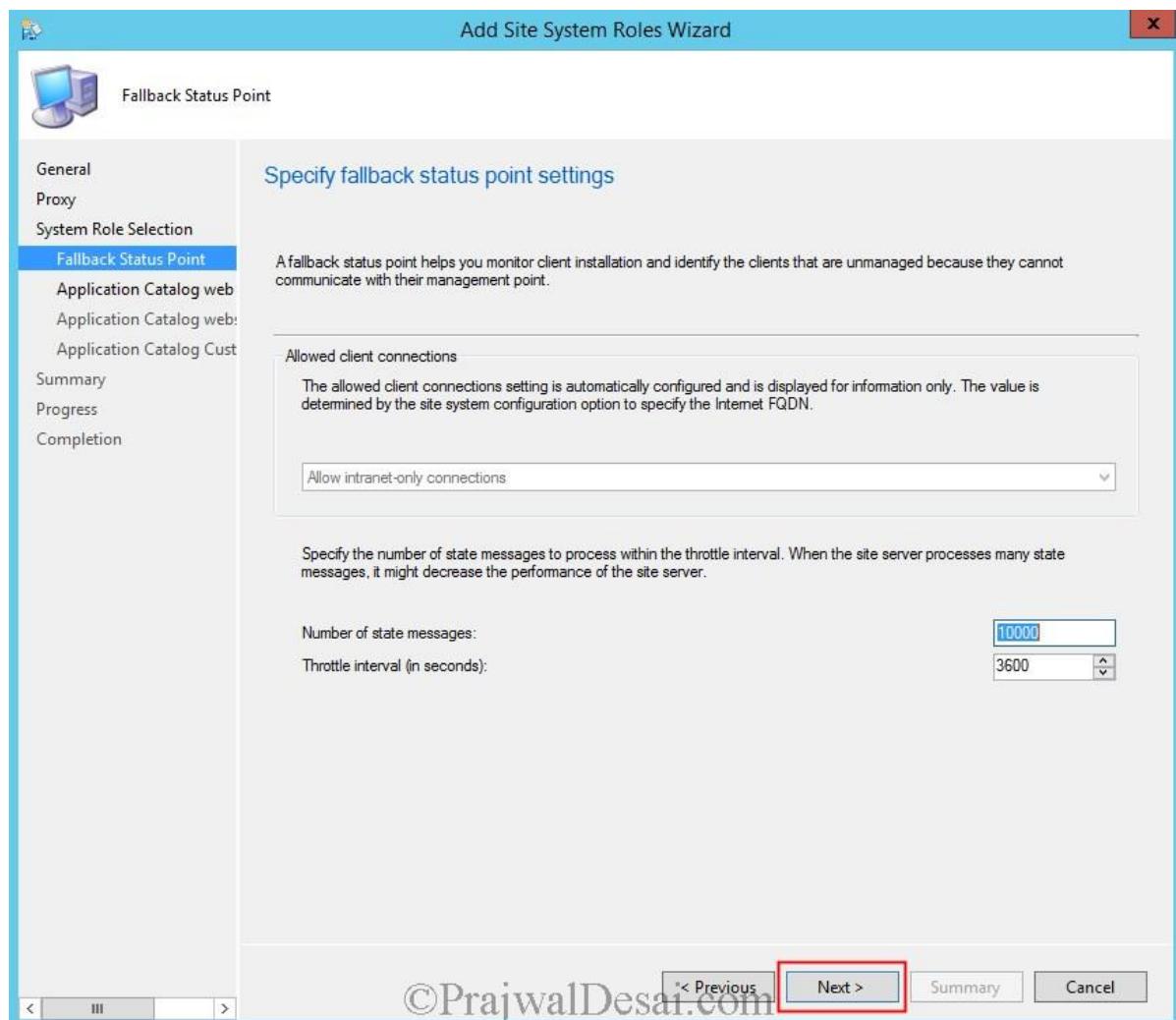
If you have an Internet proxy server please specify the details here, else click **Next**.



Select Application Catalog Web Service Point, Application Catalog Website Point, Fallback status point. Click Next.

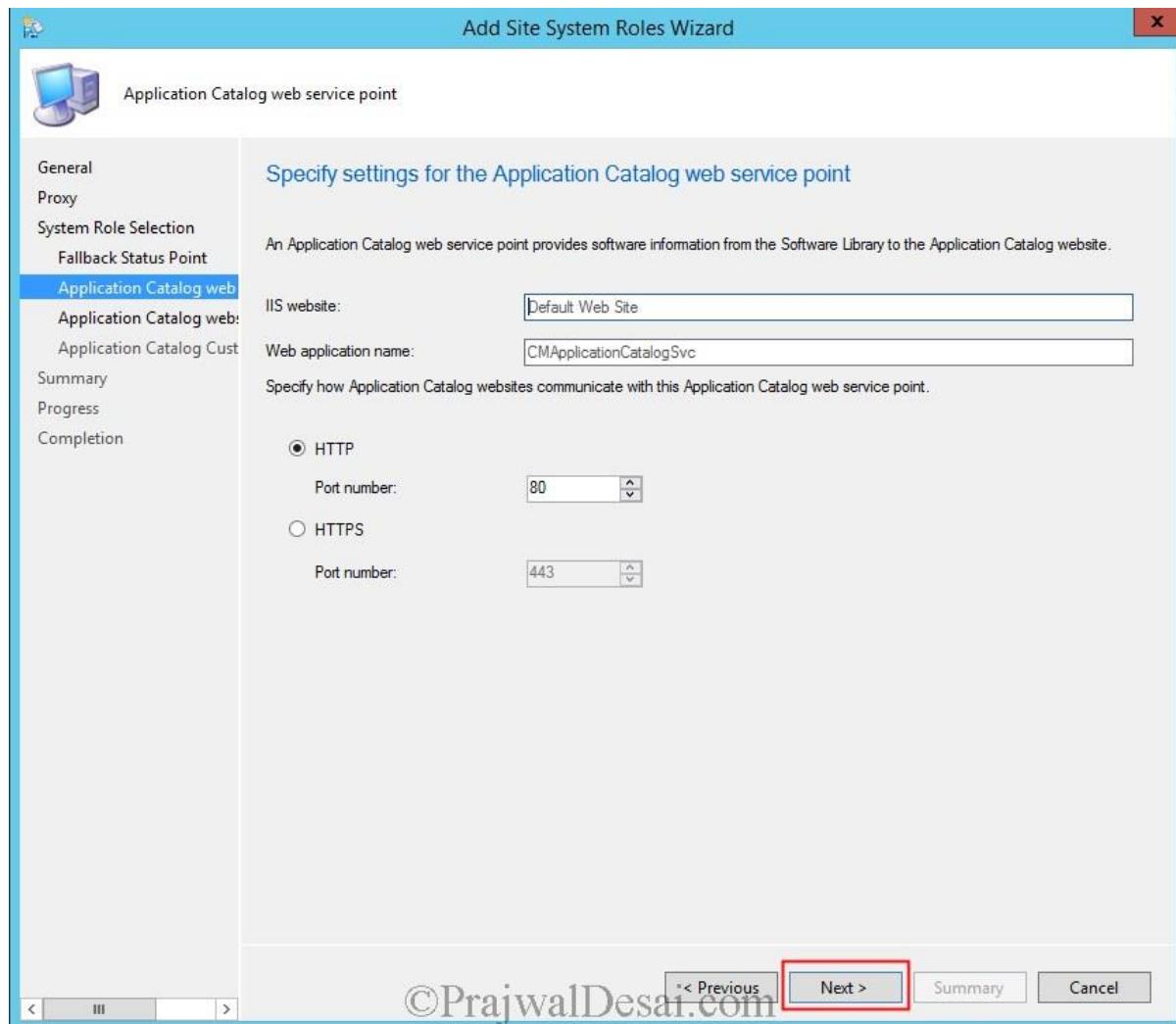


Leave the **fallback status point settings** to default and click **Next**.

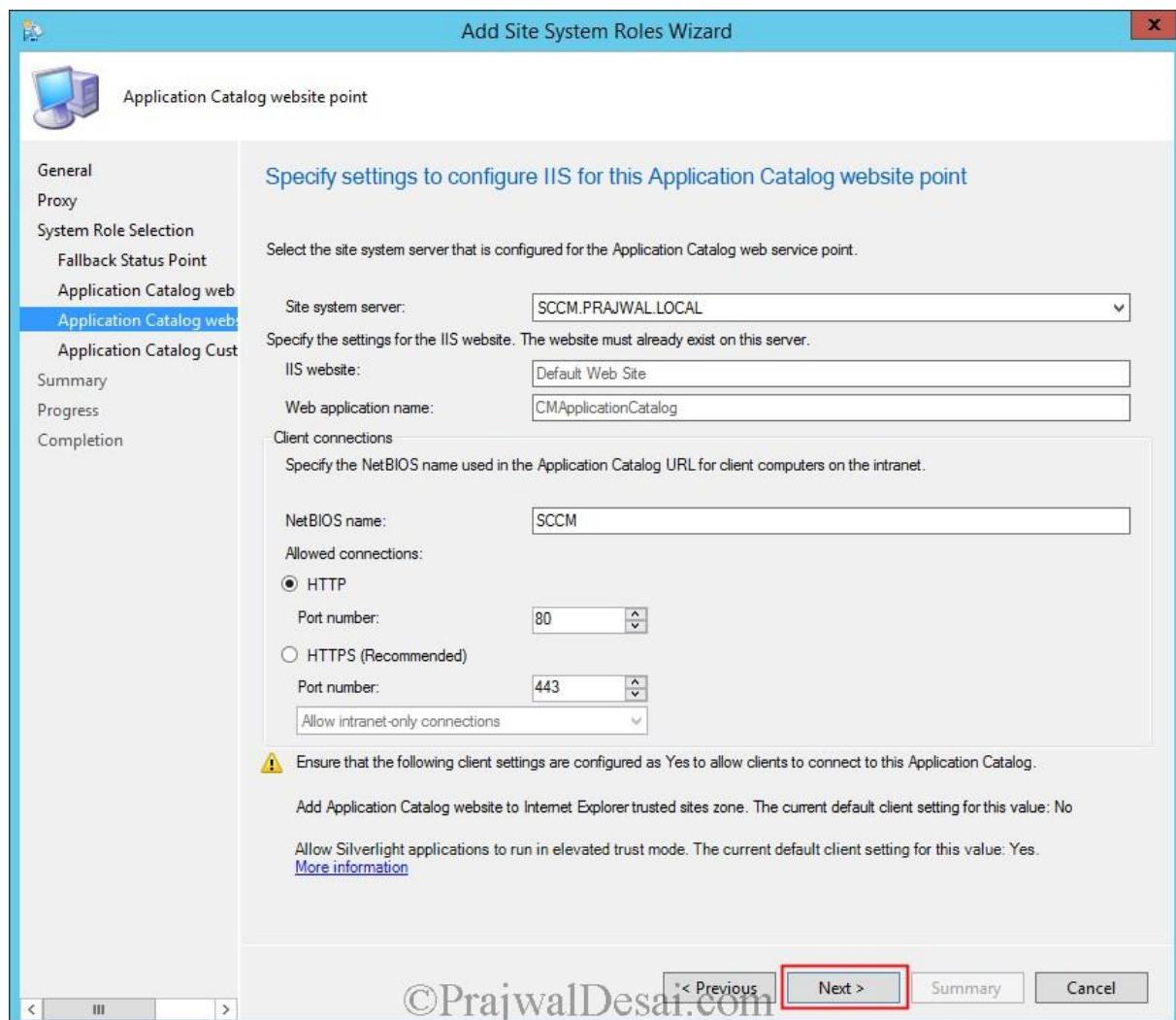


©PrajwalDesai.com

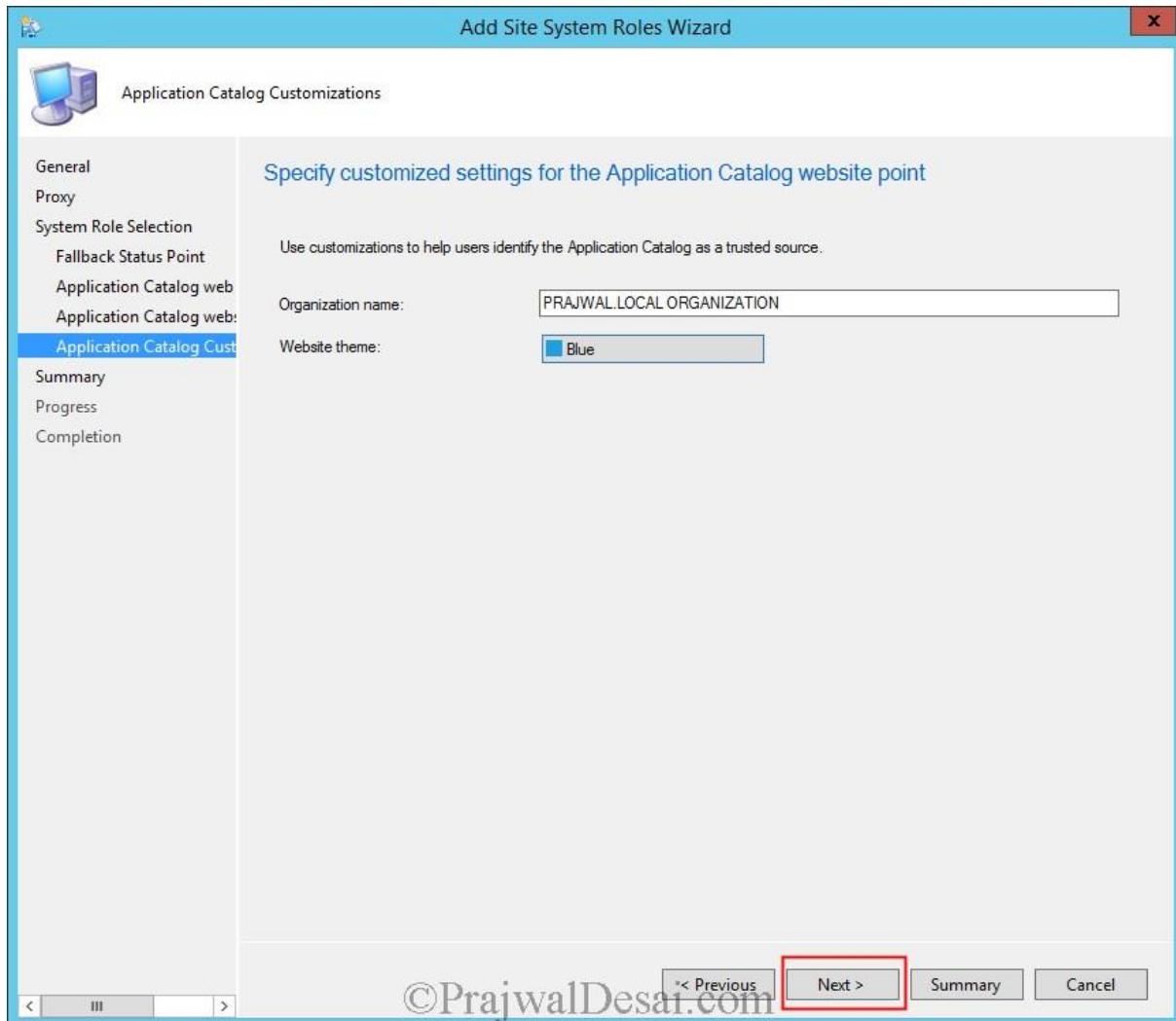
Application catalog website communicates with Application catalog web service point using port 80. Do not change anything here, Click **Next**.



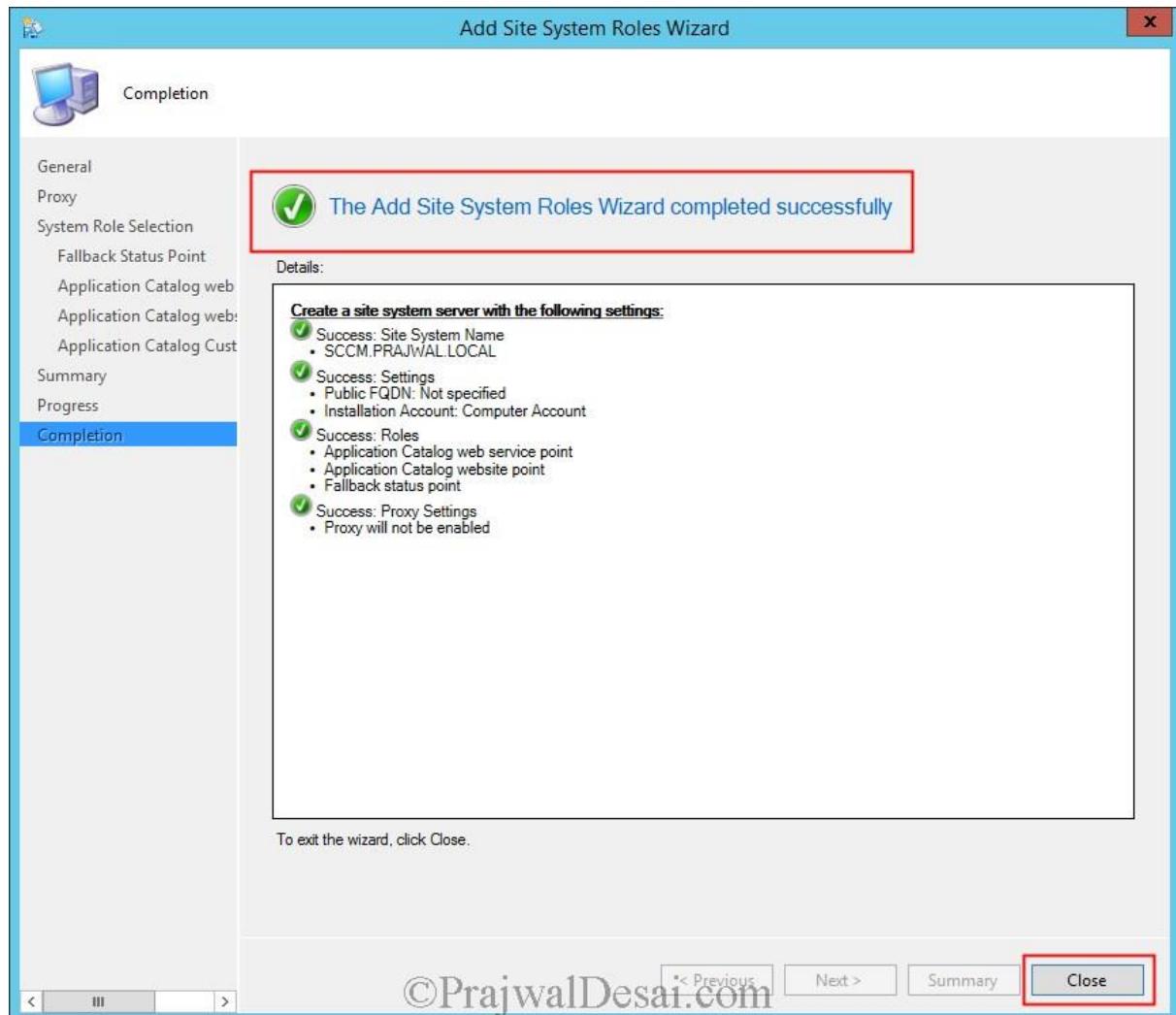
Click on **Next**.



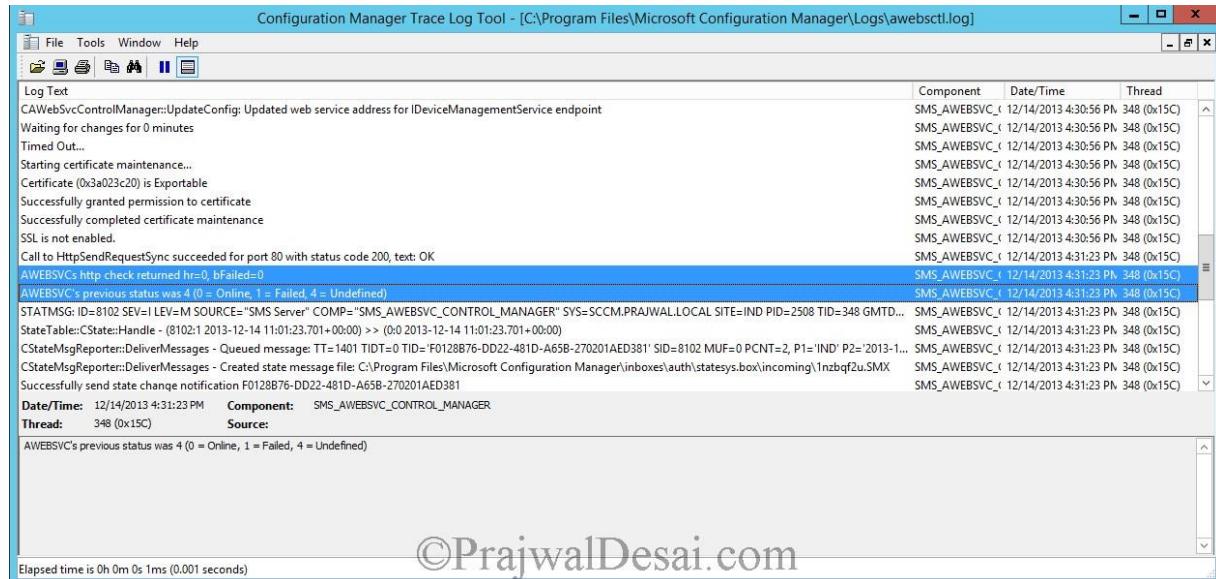
Provide the **Organization Name** and choose the **color**. With the below customization when an user opens the Application Catalog link from his computer, user would see that website theme color is Blue and organization name is what we have entered. Click **Next**.



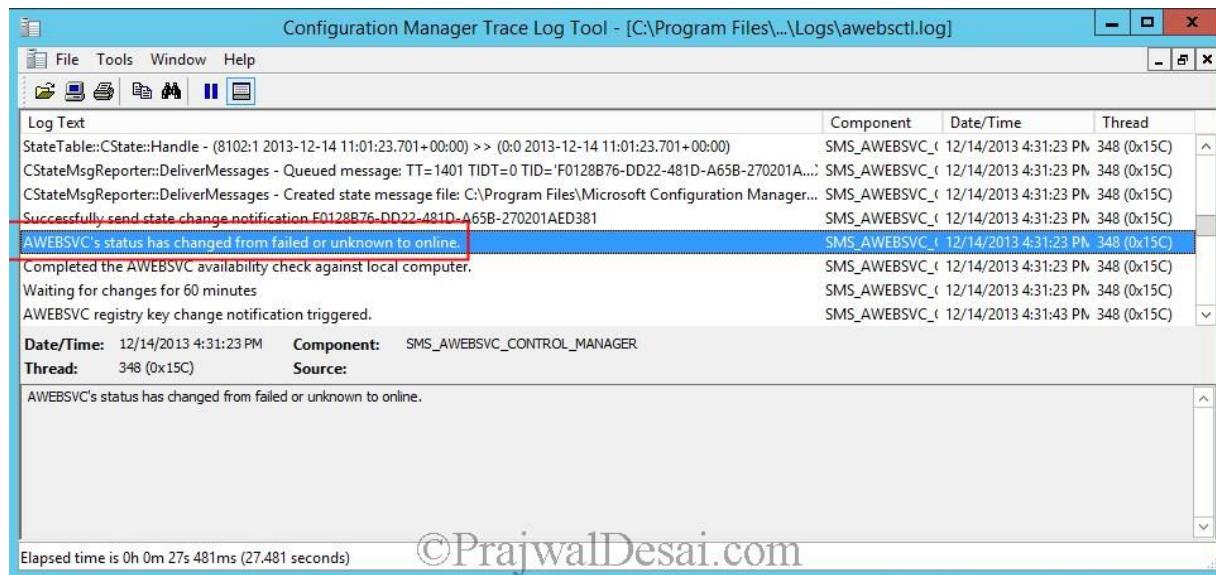
Alright, we have added the site system roles. Lets check if they are installed correctly.



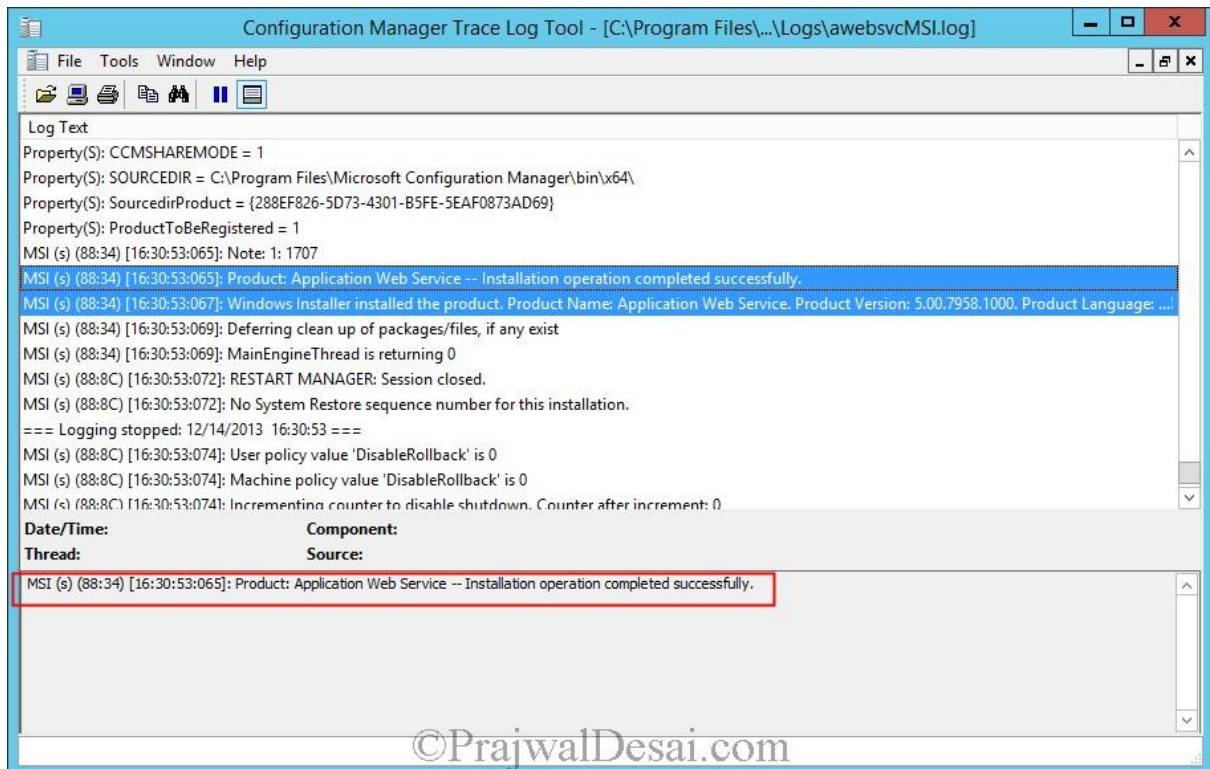
You can check logs of Application catalog website point by opening the log file named **awebsctl.log**. The log file is located in **C:\Program Files\Microsoft Configuration Manager\Logs**. Look for the line AWEBSVC's http check returned **hr=0, bFailed=0**. Wait for few minutes while we see the change in the status.



We see that the AWEBSVC's status is changed from failed or unknown to **online**.



To check Application catalog Web service point log role installation details, open the log file **awebsvcMSI.log** with CMtrace log viewer and look for the line **Application Web Service — Installation Operation Completed Successfully.**



©PrajwalDesai.com

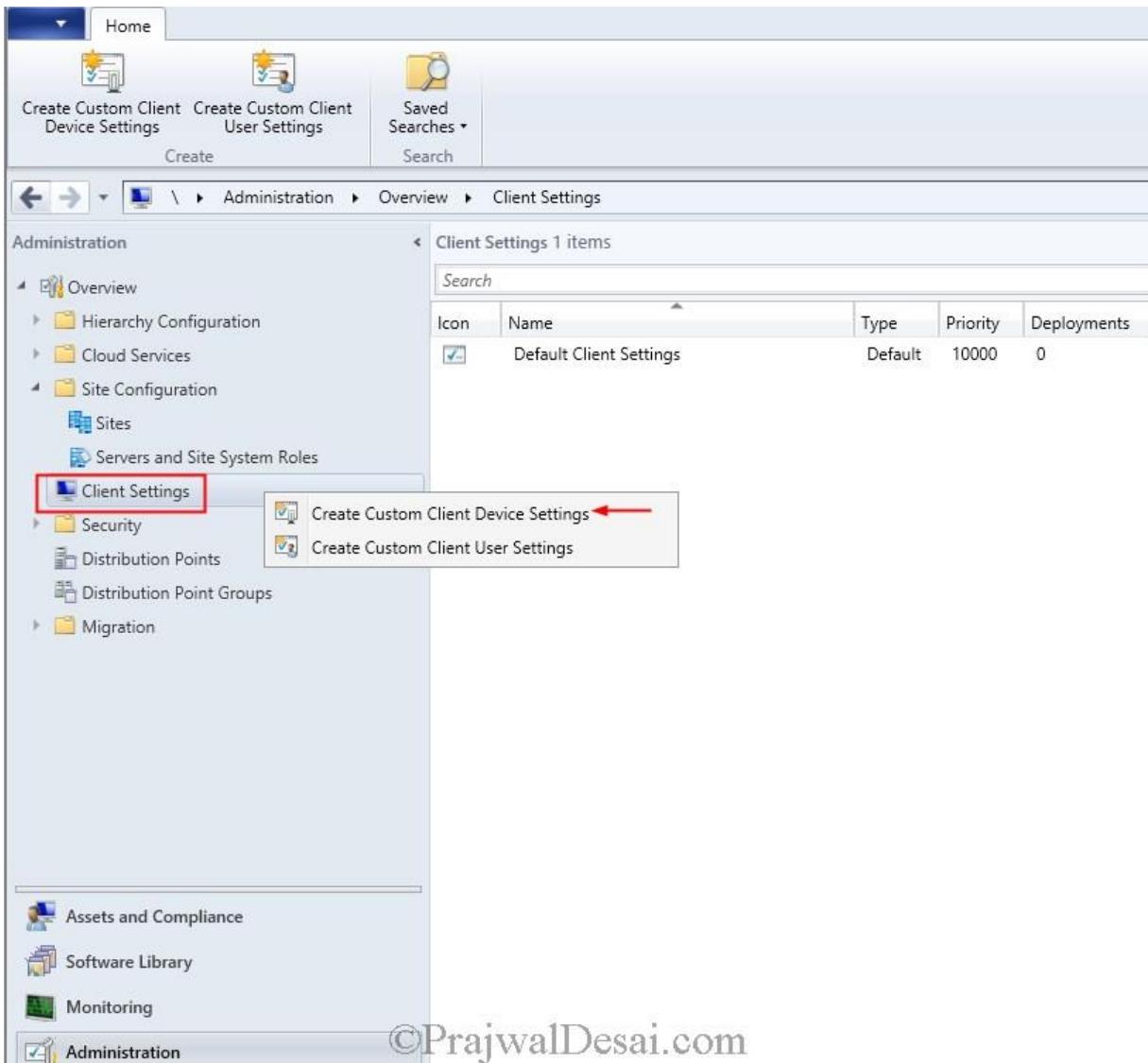
Configuring Client Settings in Configuration Manager 2012 R2

In this post we will be taking a look at steps on configuring client settings in configuration manager 2012 R2. In System Center 2012 R2 Configuration Manager, you can specify client settings at a collection level, allowing you to define different settings as necessary. We have the flexibility to create multiple client device or client user settings and apply it to different collections as per our requirement. When you create a client setting a priority is assigned to it, those with a higher priority win over settings with a lower priority. Note that the default client settings has the priority of 10000, which means you can have 9999 client settings that would have higher priority over the default client settings.

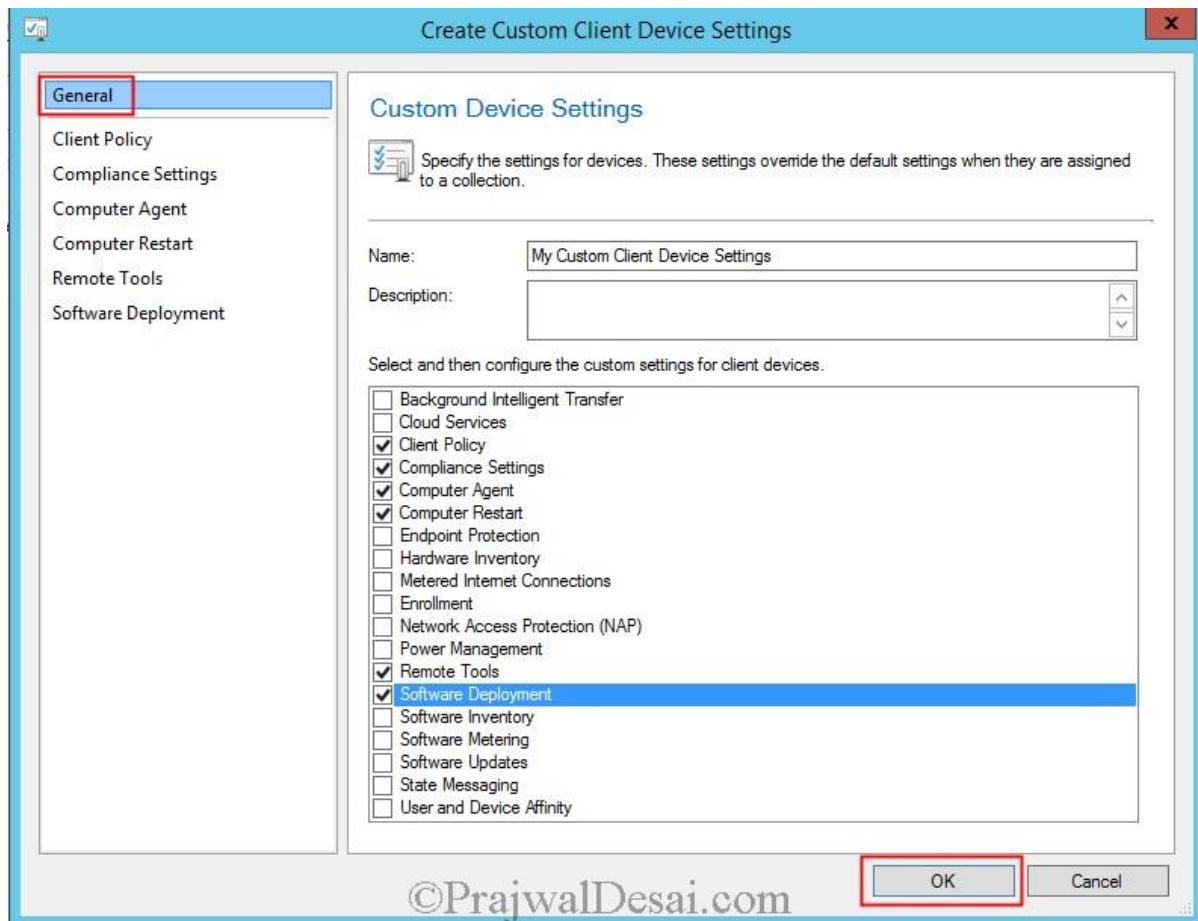
All client settings in System Center 2012 R2 Configuration Manager are managed in the Configuration Manager console from the **Client Settings** node in the **Administration** workspace. A set of default settings is supplied with Configuration Manager 2012. When you modify the default client settings, these settings are applied to all clients in the hierarchy. You can also configure custom client settings, which override the default client settings when you assign these to collections. We will configure few of the [client settings](#) in this post. If you are looking for default client settings information you can go through this [post](#).

Configuring Client Settings in Configuration Manager 2012 R2

Launch the **Configuration Manager 2012 R2** console, click on **Administration**. Right click Client Settings and click **Create Custom Client Device Settings**.

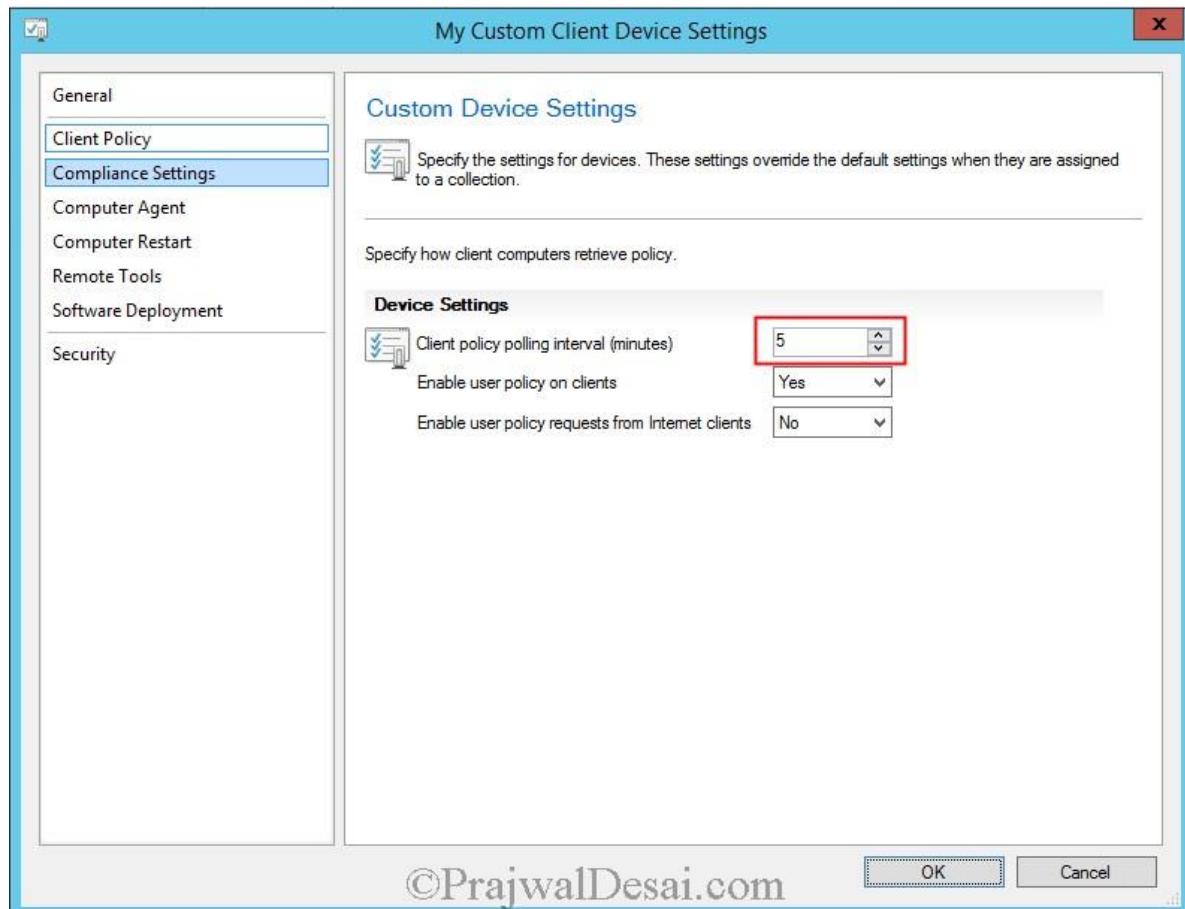


In this example we will select **Client Policy, Compliance Settings, Computer Agent, Computer Restart, Remote Tools and Software Deployment**.

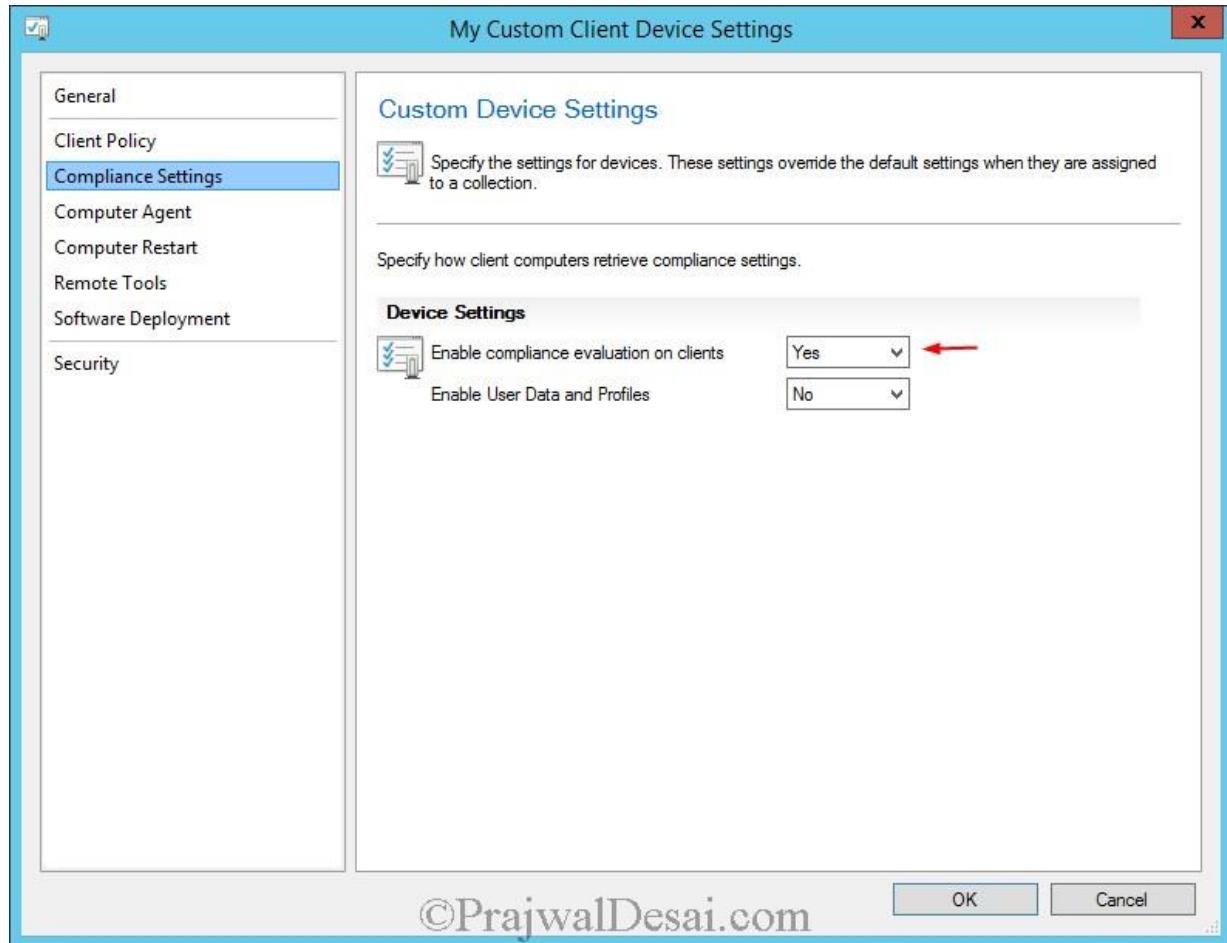


©PrajwalDesai.com

Client Policy – Client Policy polling interval specifies how frequently client computers download client policy from management point. Select **Client Policy** from the left pane, Set **Client Policy Polling to interval to 5 minutes**.

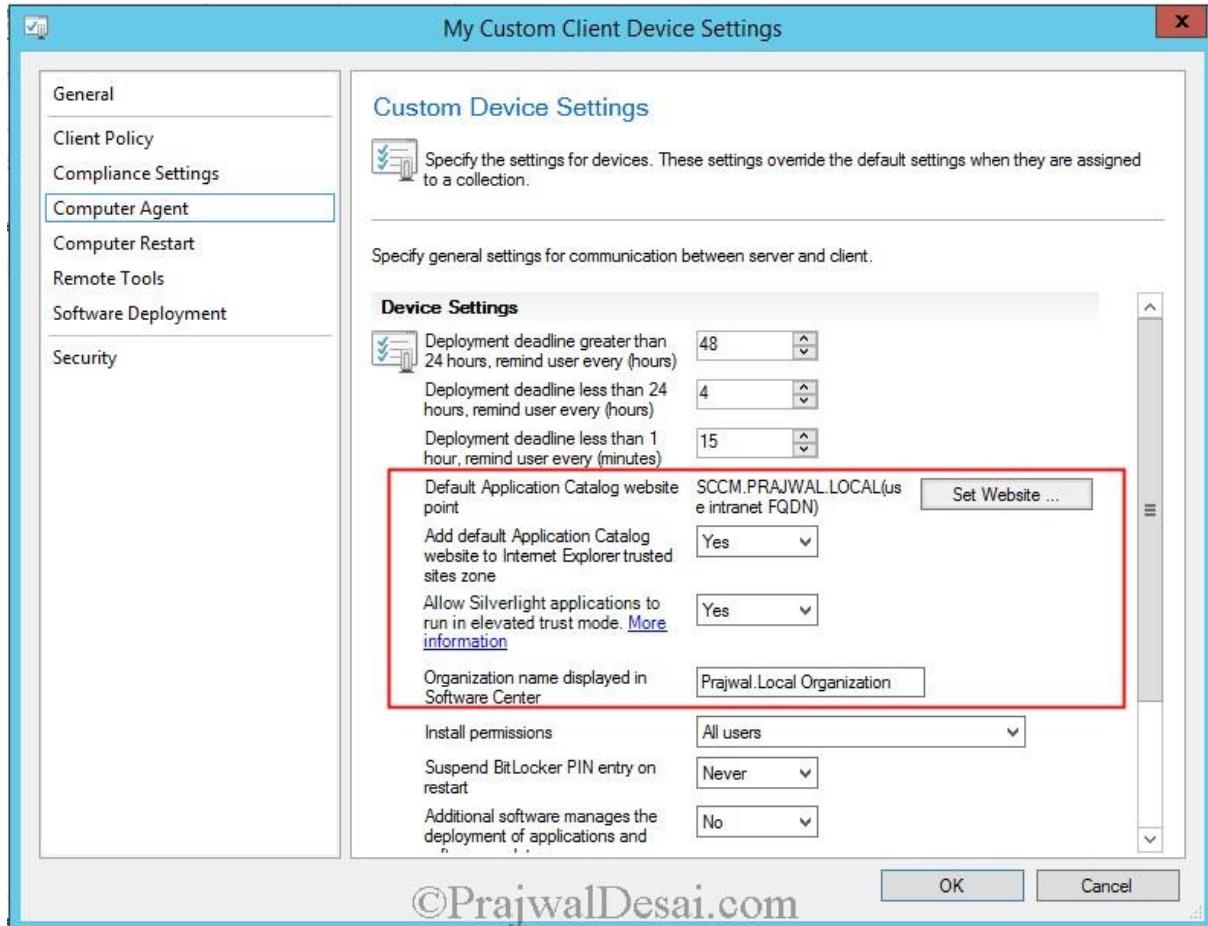


Compliance Settings – If compliance settings are enabled or compliance evaluation on client is set to yes, then compliance evaluation happens on clients.

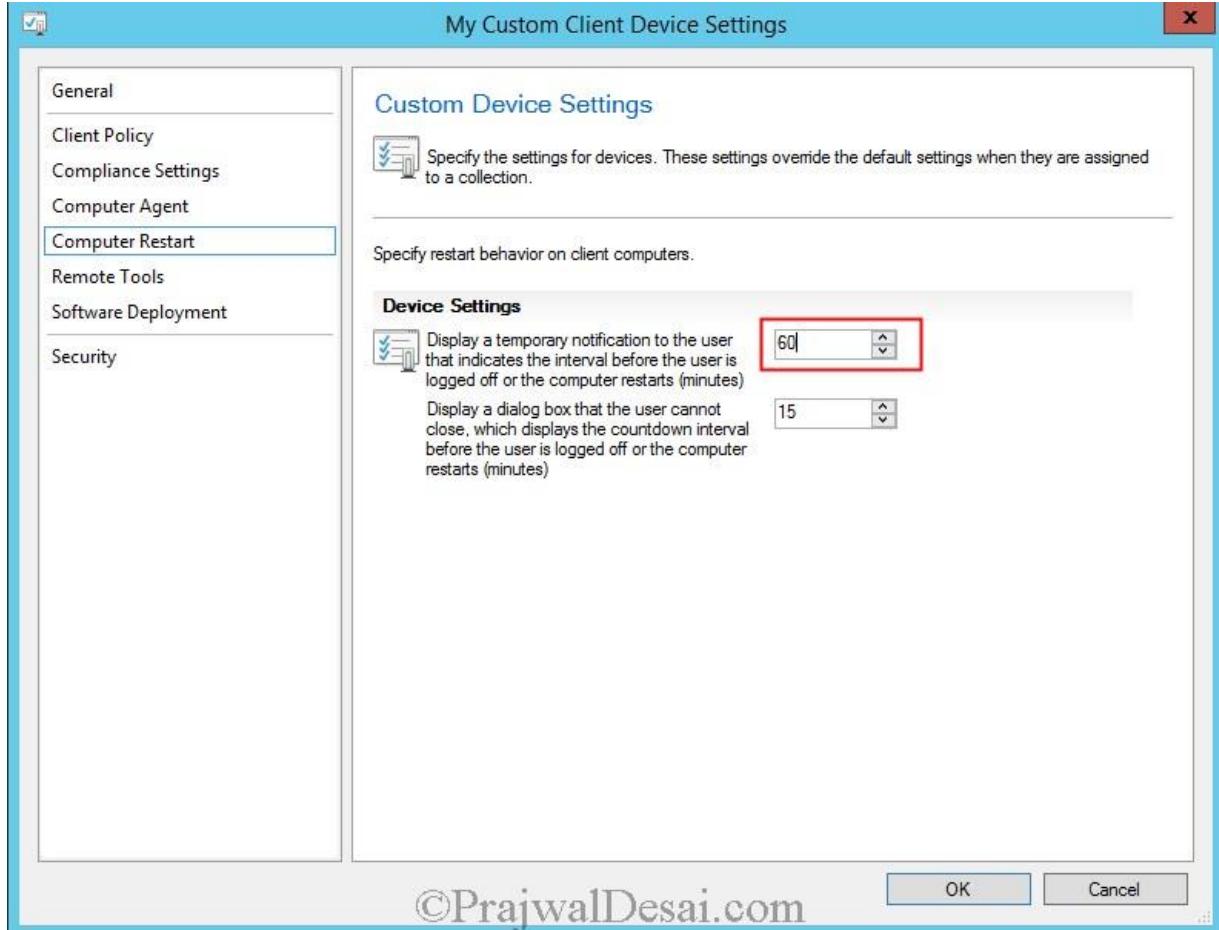


Computer Agent – Computer Agent allows you to define settings related to software distribution on the Configuration Manager client. These include specifying the notification interval for deployments, the default Application Catalog website point, Organization name that will be displayed in software center, displaying notifications for new deployments and more.

Select **Computer Agent**, to set the **default Application Catalog website point** click “**Set Website**”. Select use **Intranet FQDN**. click OK. Set “**Add Default Application catalog website to IE trusted site zones**” to **Yes**. Specify the Organization Name to be displayed in Software center. Rest of the settings remain unchanged.



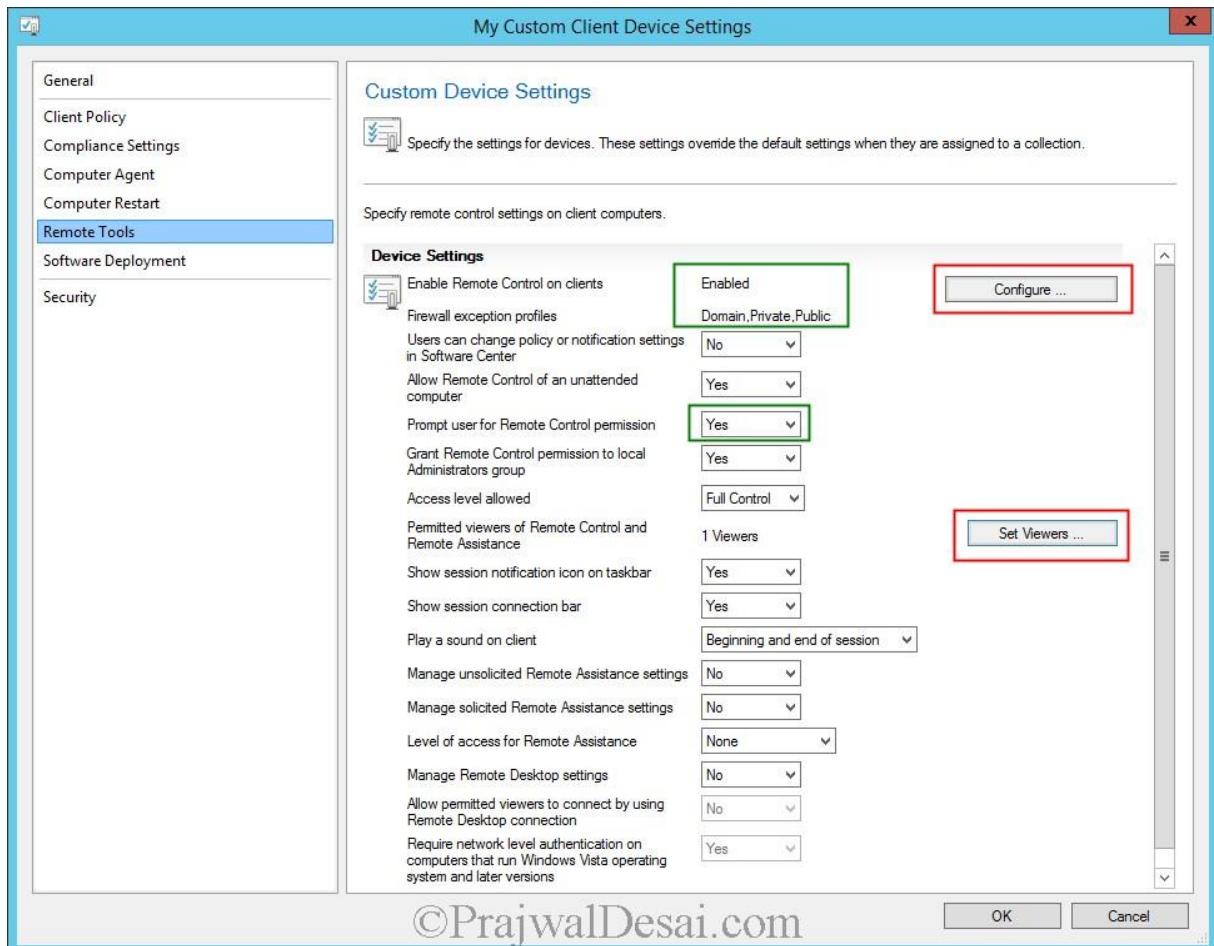
Computer Restart – Computer restart device settings allow you to specify the countdown interval for ConfigMgr-initiated restarts. Ensure that the intervals specified are shorter in duration than the shortest maintenance window applied to your client, so the computer restarts during the window. We will change the temporary notification that's displayed to user to 60 minutes.



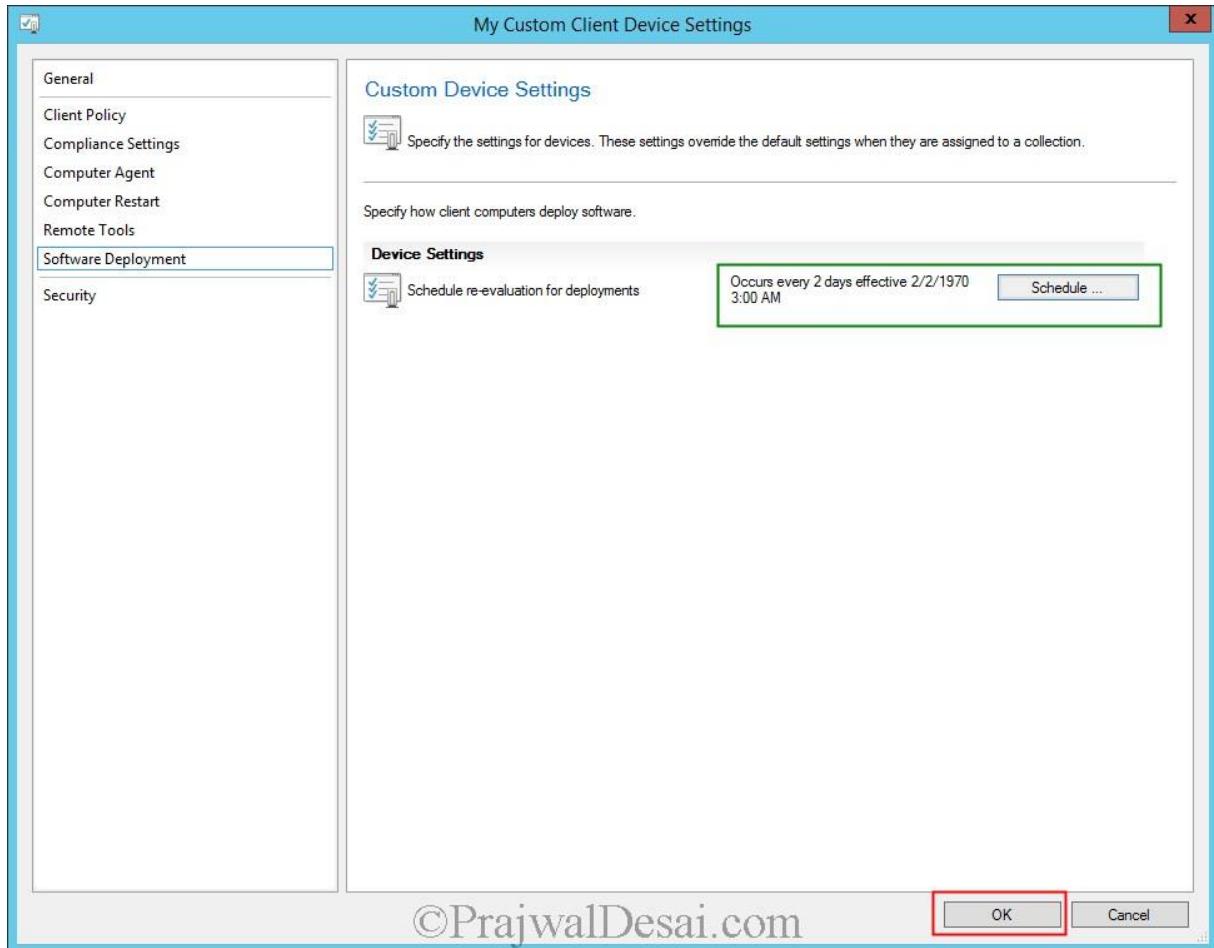
Remote Tools – You can use Remote Tools for remote management of client desktops for troubleshooting purposes, **Remote Tools** uses the RDP functionality provided by the Windows OS and you can use this feature to take over desktop using Remote Desktop or assisting the end user using the Remote Assistance functionality, where both the end user and help desk look at the same desktop.

Click on **Remote Tools** on the left Pane, we will enable **Remote Control** on clients. To do so click on configure. check **Enable Remote Control on Client Computers**. Choose **Domain, Private and Public**. Click OK.

To set **Permitted Viewers** for remote connection and remote assistance click “**Set Viewers**”. For example you can add a group which consists of users from IT team who would take a remote control for troubleshooting purpose.

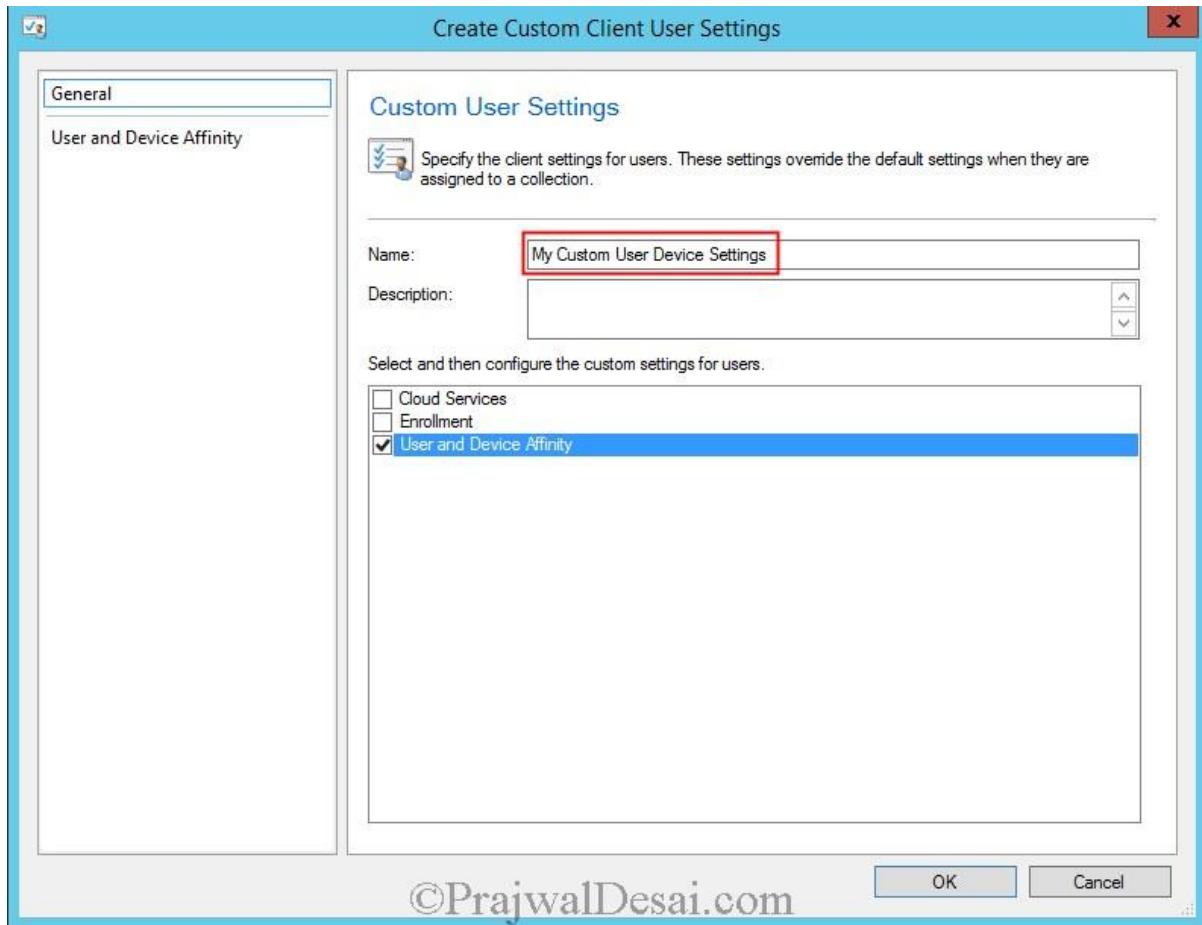


Software Deployment – Software Deployment settings allow you to specify when software deployments are re-evaluated. By default re-evaluation for deployments occurs every 7 days, you can change the default value by clicking on Schedule and set it to your requirement. In this example I have set it for evaluate for every 2 days. Click OK.



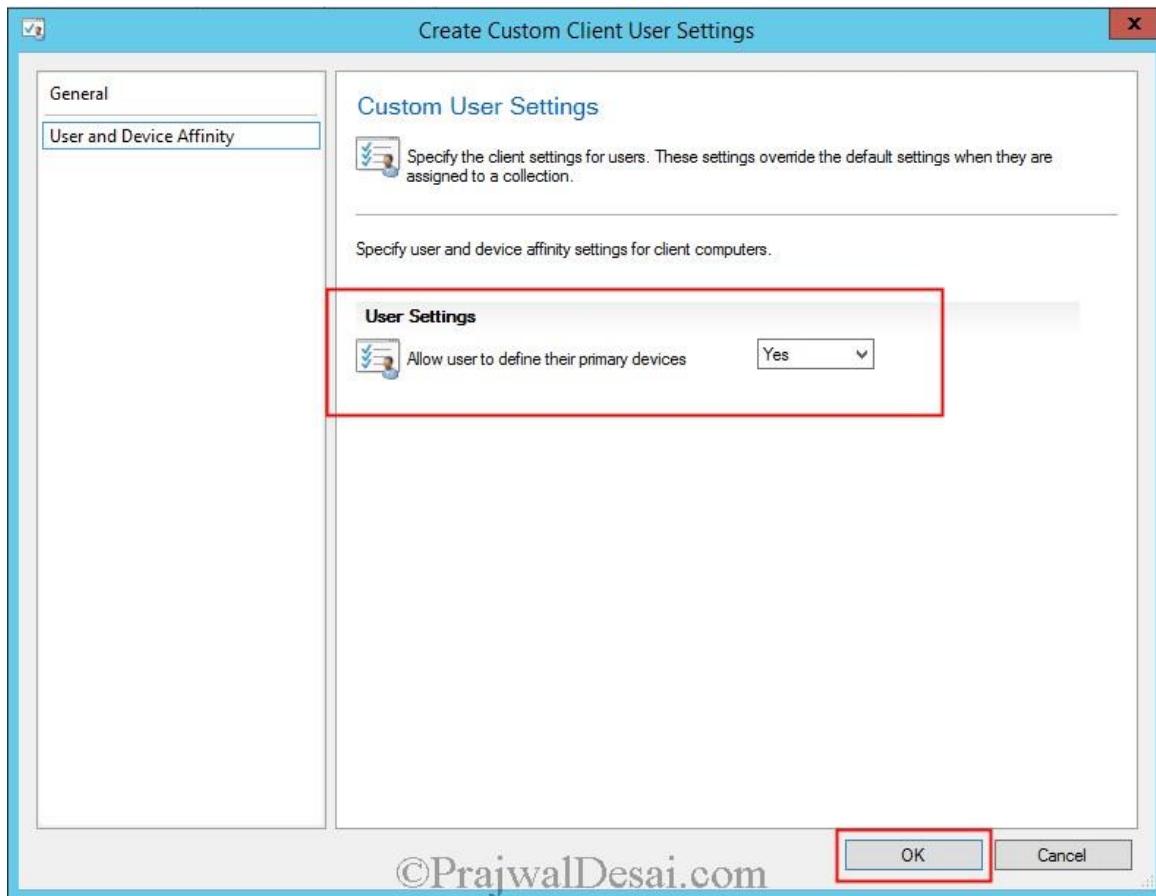
©PrajwalDesai.com

You can also create Custom User Settings as we did for Device settings in the above steps. We will create Custom user device settings and allow users to define their primary device. Right click **Client Settings** and click **Create Custom Client User Settings**.



©PrajwallDesai.com

User and Device Affinity – The User and Device Affinity settings for users allow you to specify whether you want to enable a user to define their primary device. You can see this setting when you create custom client device settings and custom client user settings.



We have got the client device and client user settings ready, we can apply these once we deploy the configuration manager client to the machines. You create separate client device settings and apply it for different collections as per your requirement.

Configuration Manager 2012 R2 Client Installation

Configuration Manager 2012 R2 Client Installation In this post we will discuss about the Configuration Manager 2012 R2 Client Installation methods, we will also configure the network access account that is a must before you perform Configuration Manager 2012 R2 Client Installation. Configuration Manager 2012 R2 Client Installation can be done in various ways, before you can use Configuration Manager to manage a system, you must discover the system and install the client. In my previous posts we have seen how to configure [Configuration Manager 2012 R2 Boundaries and Discoveries](#), so once the systems are discovered you can proceed with Configuration Manager 2012 R2 Client Installation. At any point of time you can jump to [configuration manager 2012 R2 step by step guide](#) for my previous posts.

Configuration Manager 2012 R2 Client Installation

Lets look at the methods available for Configuration Manager 2012 R2 Client Installation, we will be deploying the clients using client push installation in this post.

- 1) **Client Push Installation** – Client Push Installation happens when an the SCCM server makes a network connection to the client (a machine where configuration manager client is to be installed) and then begins the client installation process. For this the system must be discovered and the administrator should have [configured the firewall exceptions](#). This method requires the administrator to start the client push installation on selected computers.
- 2) **Automatic Sitewide Client Push Installation** – In Automatic sitewide Client Push Installation method you can configure client push installation for a site, and client installation will automatically run on the computers that are discovered within the site's configured boundaries when those boundaries are configured as a boundary group.
- 3) **Software update point installation** – This method installs the client by using the Configuration Manager software updates feature. No prior discovery of system is required in this method.
- 4) **Manual Installation** – This method allows you to install the configuration manager clients manually. The installation can be initiated by copying the CCMSetup.exe file on the system and running it with an user account which has enough permissions to install the software. This program and its supporting files can be found in the **Client** folder of the System Center 2012 Configuration Manager installation folder on the site server and on management points in your site.
- 5) **Group Policy based Installation** – As the name says you can install the Configuration Manager client using group policy. When you assign the Configuration Manager client to computers by using Group Policy, the client installs when the computer first starts. When you publish the System Center 2012 R2 Configuration Manager client to users by using Group Policy, the client displays in the Control Panel **Add or Remove Programs** for the computer for the user to install.

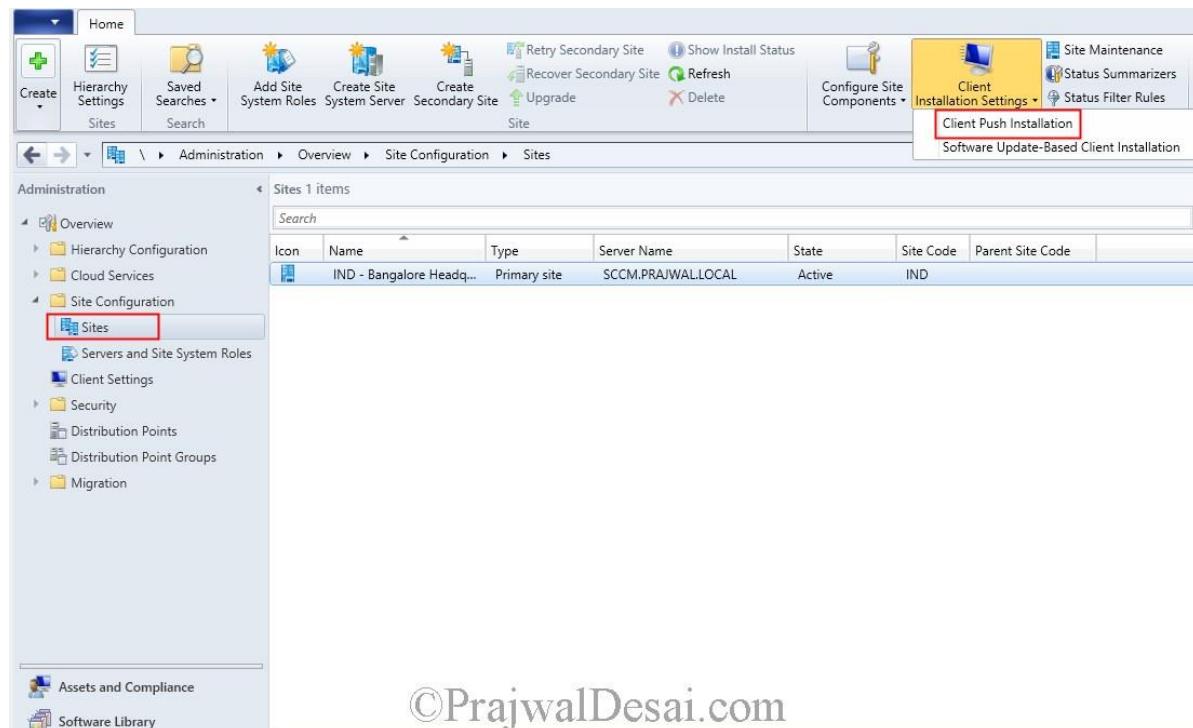
6) **Using Logon Scripts** – Configuration Manager 2012 R2 supports logon scripts to install the System Center 2012 R2 Configuration Manager client software. You can use the program file **CCMSetup.exe** in a logon script to trigger the client installation.

7) **Using Computer Imaging** – You can preinstall the Configuration Manager 2012 R2 client software on a master image computer that will be used to build computers in your enterprise. When computers are imaged from this master image, they will contain the Configuration Manager 2012 R2 client and must complete site assignment when installation is complete.

8) **Upgrade Installation** – This method uses your existing software distribution infrastructure to upgrade the client. Upgrade installation requires prior discovery and site assignment of the system.

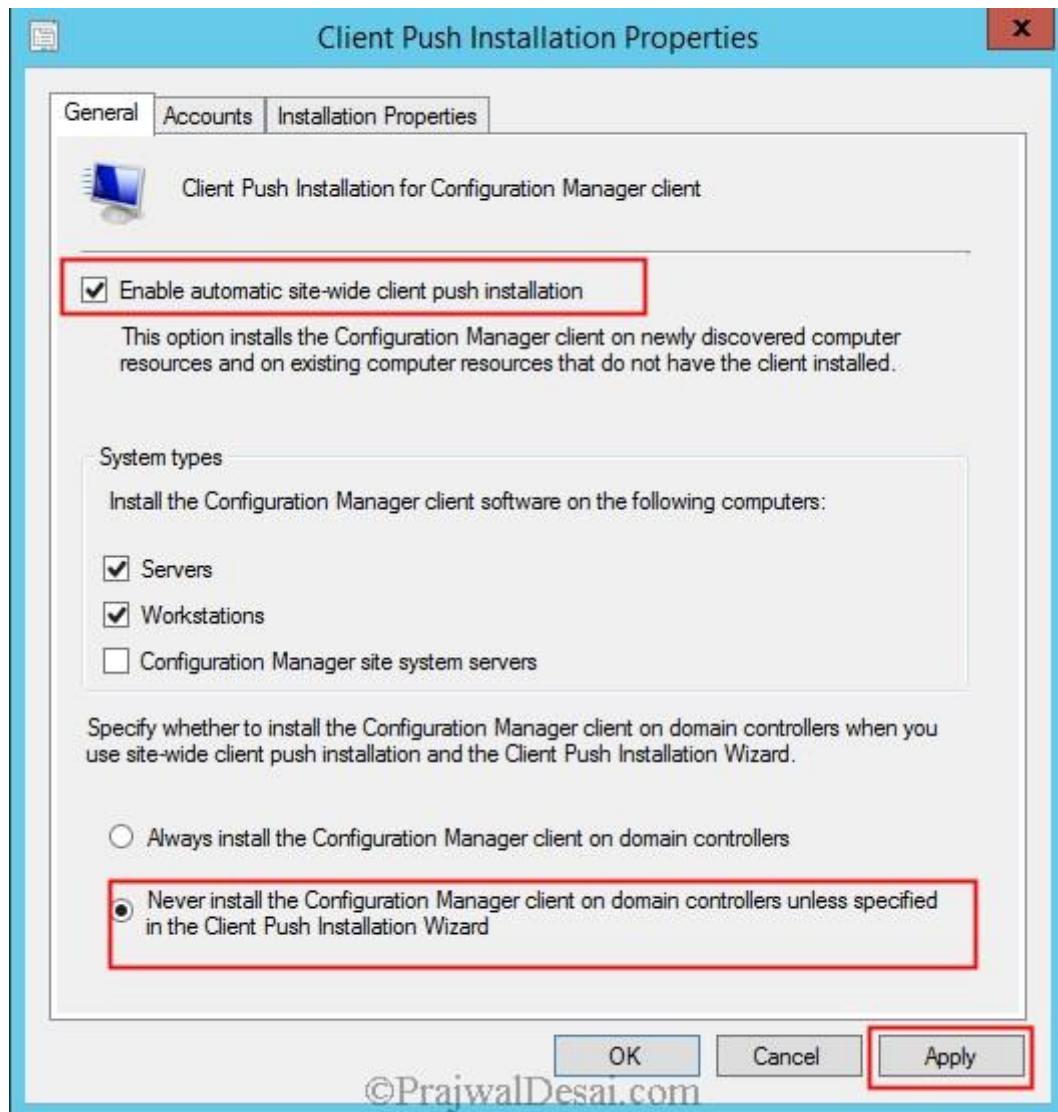
The above methods are some of the ways where the SCCM admin can use for Configuration Manager 2012 R2 Client Installation. In this post we will install the Configuration Manager 2012 R2 Client by enabling the automatic sitewide client push installation method. For Client push installation you can check this [post](#).

From the Configuration Manager Console Click **Administration**, Under **Site Configuration**, Click **Sites**, at the top ribbon under **Client Installation Settings**, click **Client Push Installation**.

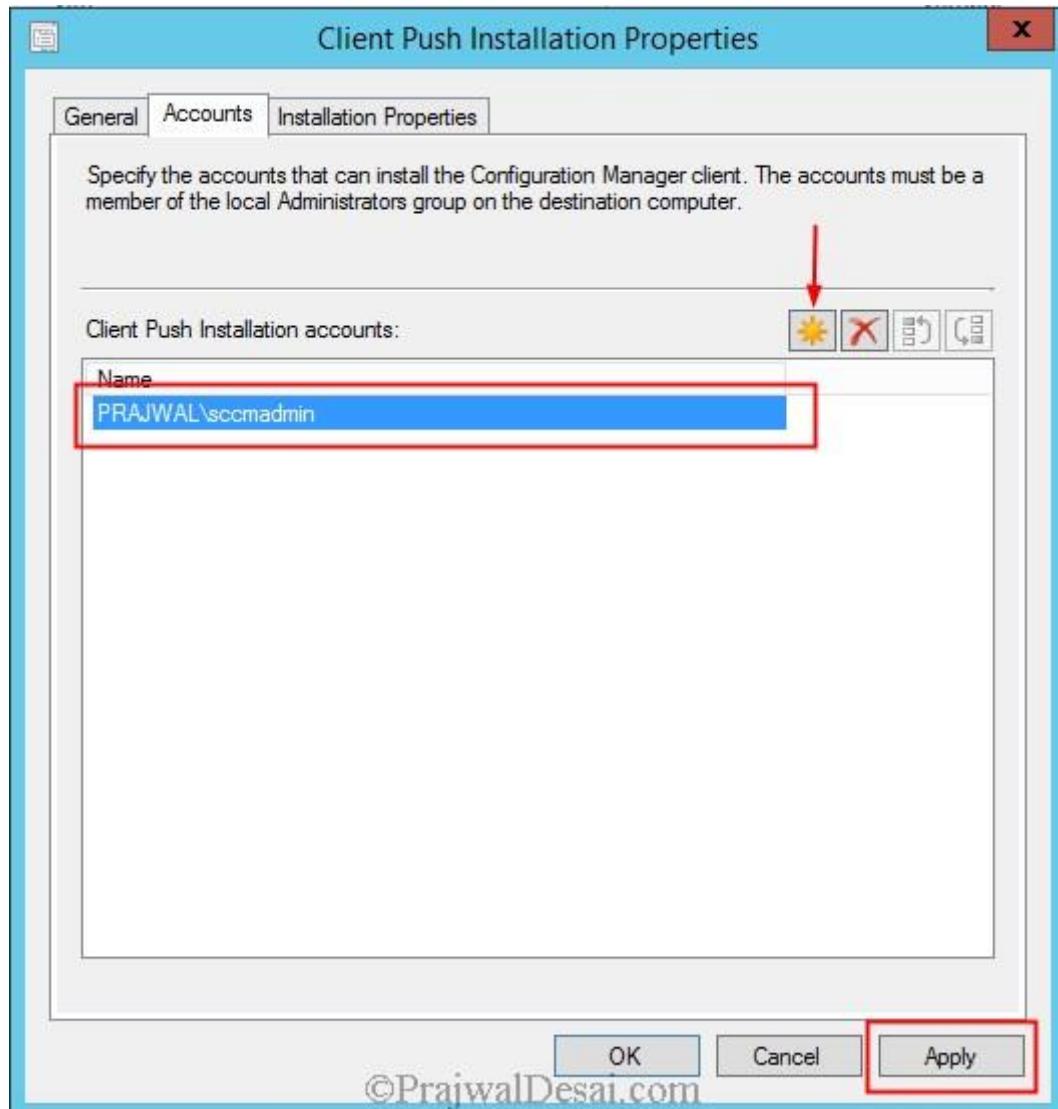


In the **General** tab check the box for **Enable Automatic site wide client push installation**. Under **System types** select **Servers** and **Workstations**. If you want to install the client agent on domain controllers choose the option “**Always Install configuration Manager Client on Domain Controllers**”, with this the client agents will be installed on all the newly discovered Domain controllers. If you want to have an option of pushing the client agent to domain controllers during client installation wizard then choose the option “**Never Install**

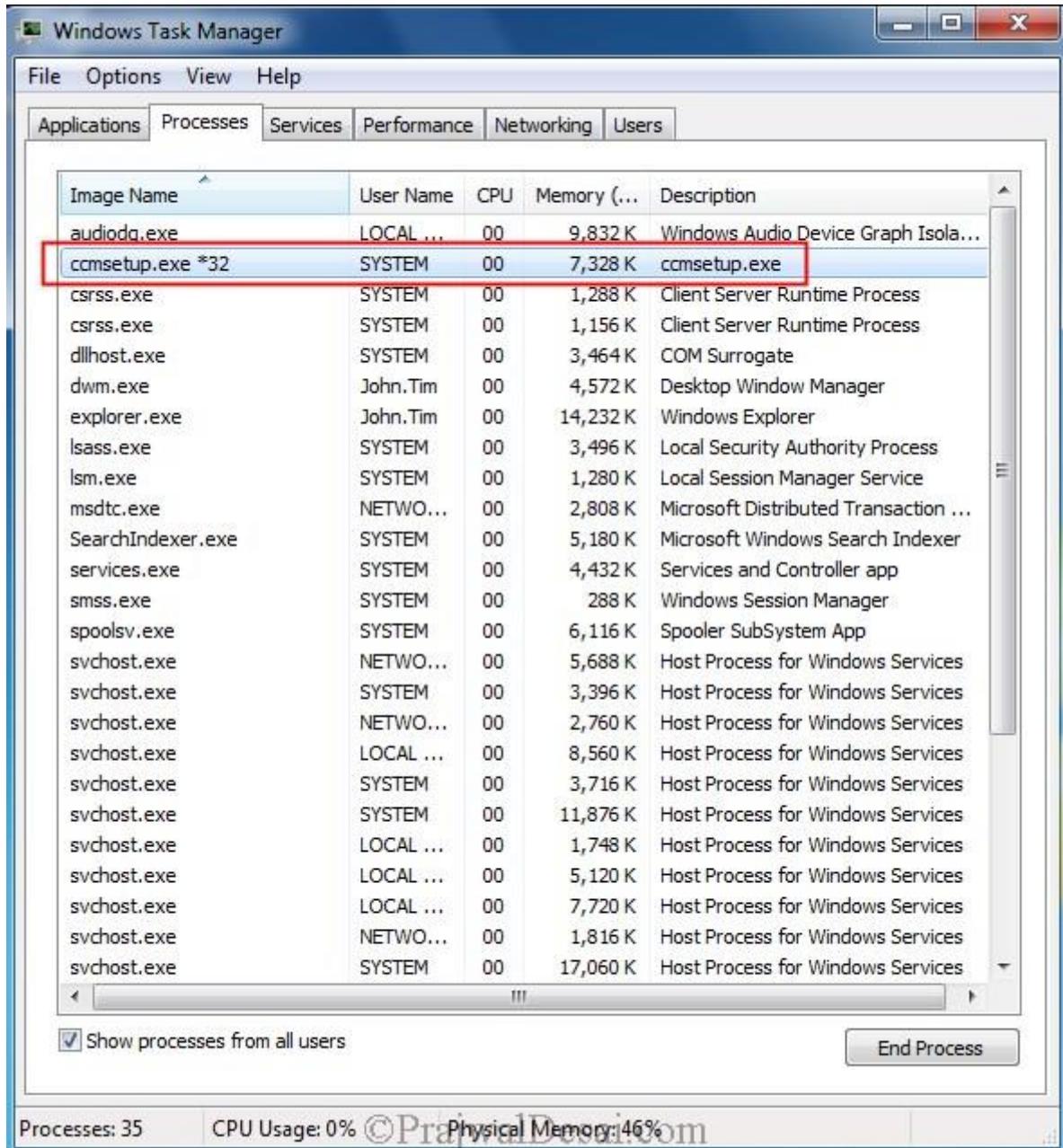
Configuration Manager Client on Domain Controller unless specified in Client Push Installation Wizard". Click on Apply.



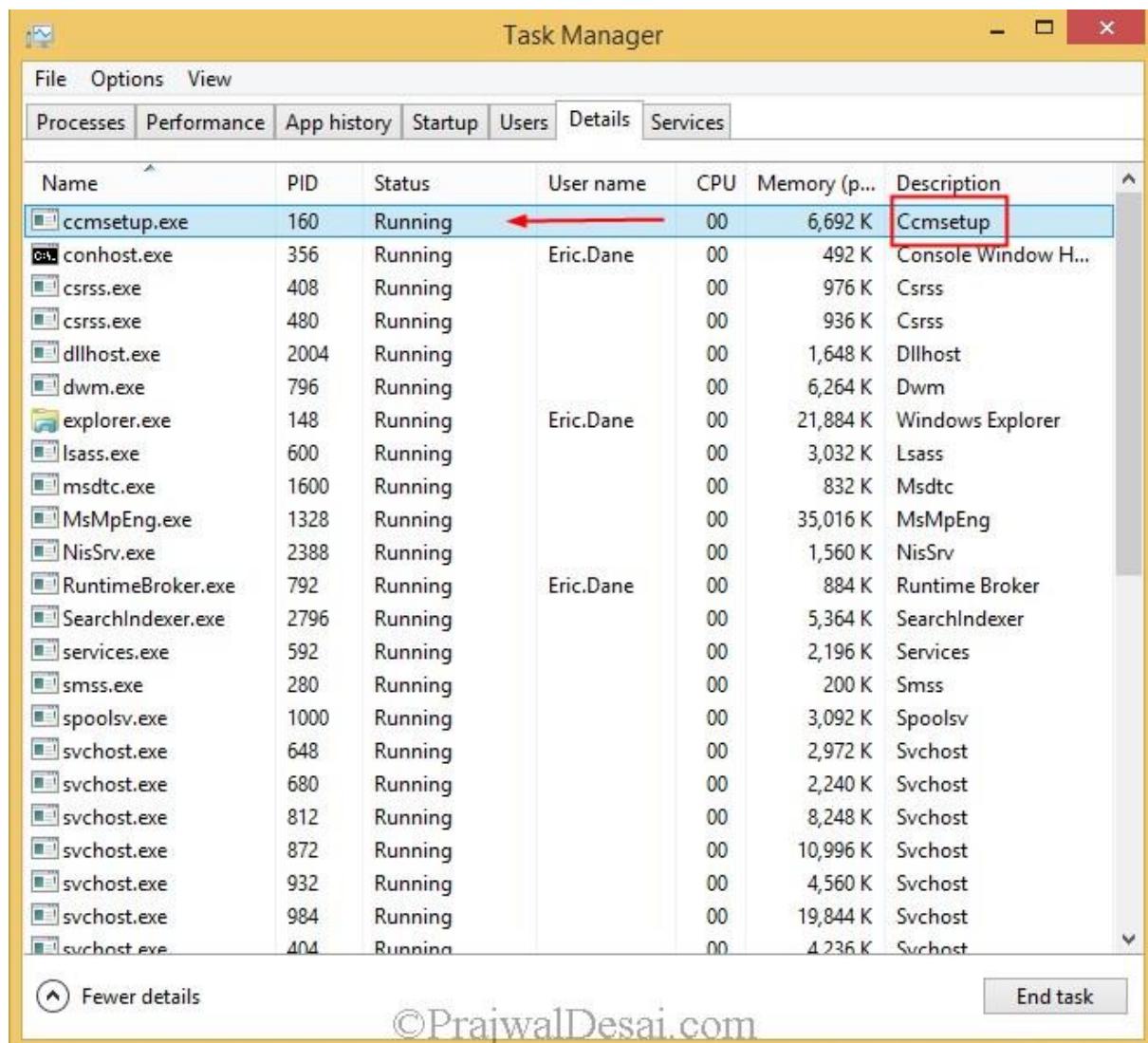
Select the **Accounts** tab, the account that you will add here must have local administrator rights on every computer on which you want to install the client.. I will choose “**PRAJWAL\scmadmin**” as the user account for deploying client agent on systems. Once you have added the account, Click **Apply** and **OK** to close the properties page.



After few minutes we see that **ccmsetup.exe *32** process is seen on the systems. The below screenshot is from one of the machine named WIN7.PRAJWAL.LOCAL.



milar screenshot from one of the machine named WIN8.PRAJWAL.LOCAL.



The screenshot shows the Windows Task Manager window with the 'Details' tab selected. The table lists various processes running on the system, including system services like csrss.exe, svchost.exe, and explorer.exe, along with other application processes. A red arrow points to the 'PID' column header, and a red box highlights the 'Description' column header. The 'Name' column contains the executable names, 'PID' shows the process ID, 'Status' indicates if it's running or not, 'User name' shows the logged-in user, 'CPU' usage is minimal, 'Memory (p...)' shows memory usage in kilobytes, and 'Description' provides a brief description of the process.

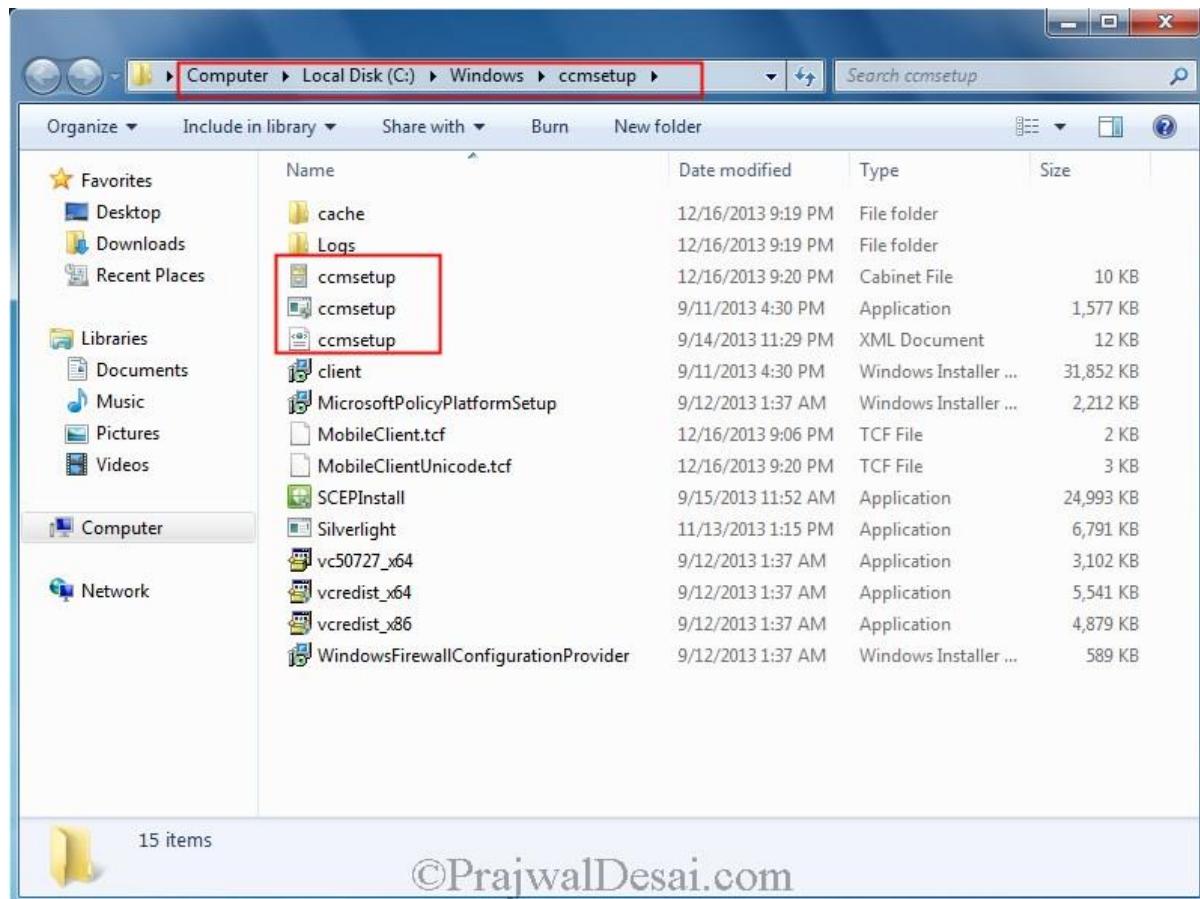
Name	PID	Status	User name	CPU	Memory (p...)	Description
ccmsetup.exe	160	Running		00	6,692 K	Ccmsetup
conhost.exe	356	Running	Eric.Dane	00	492 K	Console Window H...
csrss.exe	408	Running		00	976 K	Csrss
csrss.exe	480	Running		00	936 K	Csrss
dllhost.exe	2004	Running		00	1,648 K	Dllhost
dwm.exe	796	Running		00	6,264 K	Dwm
explorer.exe	148	Running	Eric.Dane	00	21,884 K	Windows Explorer
lsass.exe	600	Running		00	3,032 K	Lsass
msdtc.exe	1600	Running		00	832 K	Msdtc
MsMpEng.exe	1328	Running		00	35,016 K	MsMpEng
NisSrv.exe	2388	Running		00	1,560 K	NisSrv
RuntimeBroker.exe	792	Running	Eric.Dane	00	884 K	Runtime Broker
SearchIndexer.exe	2796	Running		00	5,364 K	SearchIndexer
services.exe	592	Running		00	2,196 K	Services
smss.exe	280	Running		00	200 K	Smss
spoolsv.exe	1000	Running		00	3,092 K	Spoolsv
svchost.exe	648	Running		00	2,972 K	Svchost
svchost.exe	680	Running		00	2,240 K	Svchost
svchost.exe	812	Running		00	8,248 K	Svchost
svchost.exe	872	Running		00	10,996 K	Svchost
svchost.exe	932	Running		00	4,560 K	Svchost
svchost.exe	984	Running		00	19,844 K	Svchost
svchost.exe	404	Running		00	4,236 K	Svchost

 Fewer details

End task

©PrajwalDesai.com

Before the client agent is installed, the files required for installation is first copied to the system under the path **\windows\ccmsetup**.



After few minutes we see that the configuration manager 2012 R2 client has been installed on 2 machines (WIN7 and WIN8) and the **Client Activity** status is **Active**.

The screenshot shows the Configuration Manager 2012 R2 interface. The top navigation bar includes Home, Collection, Close, Add Selected Items, Install Client, Manage Affinity Requests, Manage Out of Band, Update Membership, Export, Add Resources, Copy, Clear Required PXE Deployments, Endpoint Protection, Delete, Deploy (with a green arrow icon), and Properties. Below the navigation bar, the breadcrumb path is Assets and Compliance > Overview > Devices > All Systems. The left sidebar under Assets and Compliance shows Overview, Users, Devices (with All Systems selected), User Collections, Device Collections, User State Migration, Asset Intelligence, Software Metering, Compliance Settings, and Endpoint Protection. The main content area displays a table titled 'All Systems 8 items' with columns: Icon, Name, Client Type, Client, Site Code, and Client Activity. The table lists the following items:

Icon	Name	Client Type	Client	Site Code	Client Activity
AD	None	No	IND		
EXCH	None	No	IND		
SCCM	None	No	IND		
SCOM	None	No	IND		
WIN7	Computer	Yes	IND	Active	
WIN8	Computer	Yes	IND	Active	
x64 Unknown Computer...	None	No	IND		
x86 Unknown Computer...	None	No	IND		

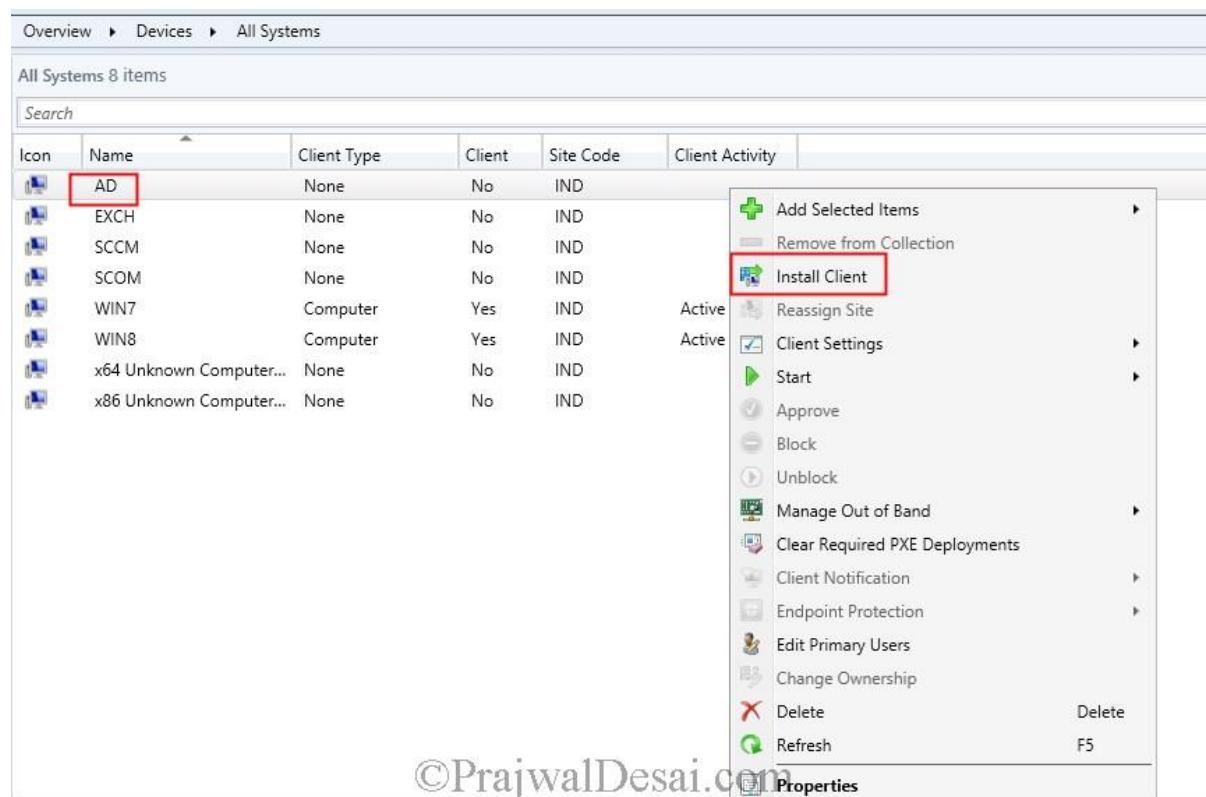
The last two rows (x64 and x86 Unknown Computers) are listed but have no activity status shown.

©PrajwalDesai.com

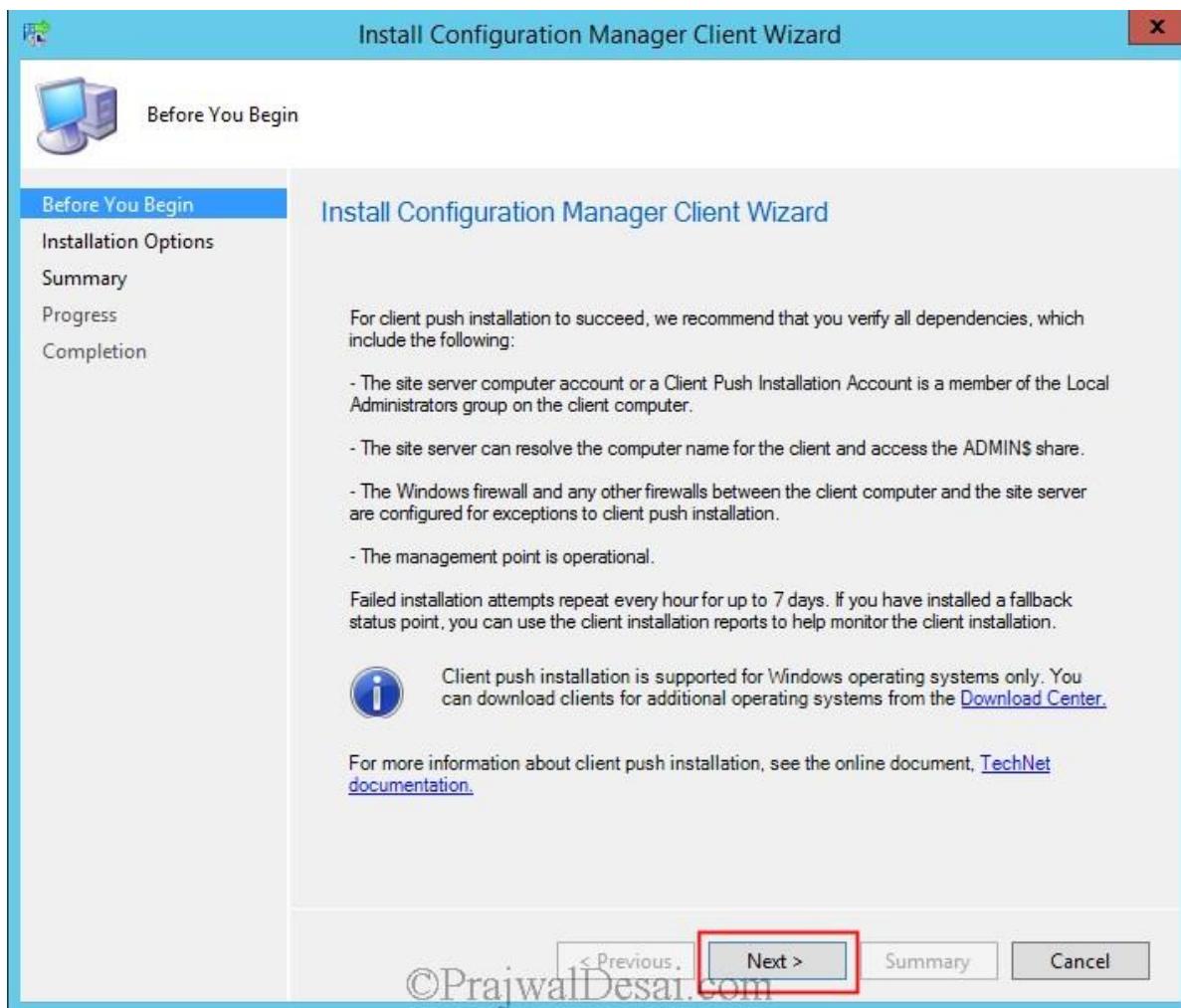
Installing the Configuration Manager Client through Client Push Wizard

In the above example we enabled automatic sitewide client push installation and the client were installed on few systems. While configuring client push installation we had specified not to install the configuration manager clients on domain controllers automatically when discovered, however the client could be installed through client push installation. In this example we will install the configuration manager client to one machine Named **AD (Domain controller)**.

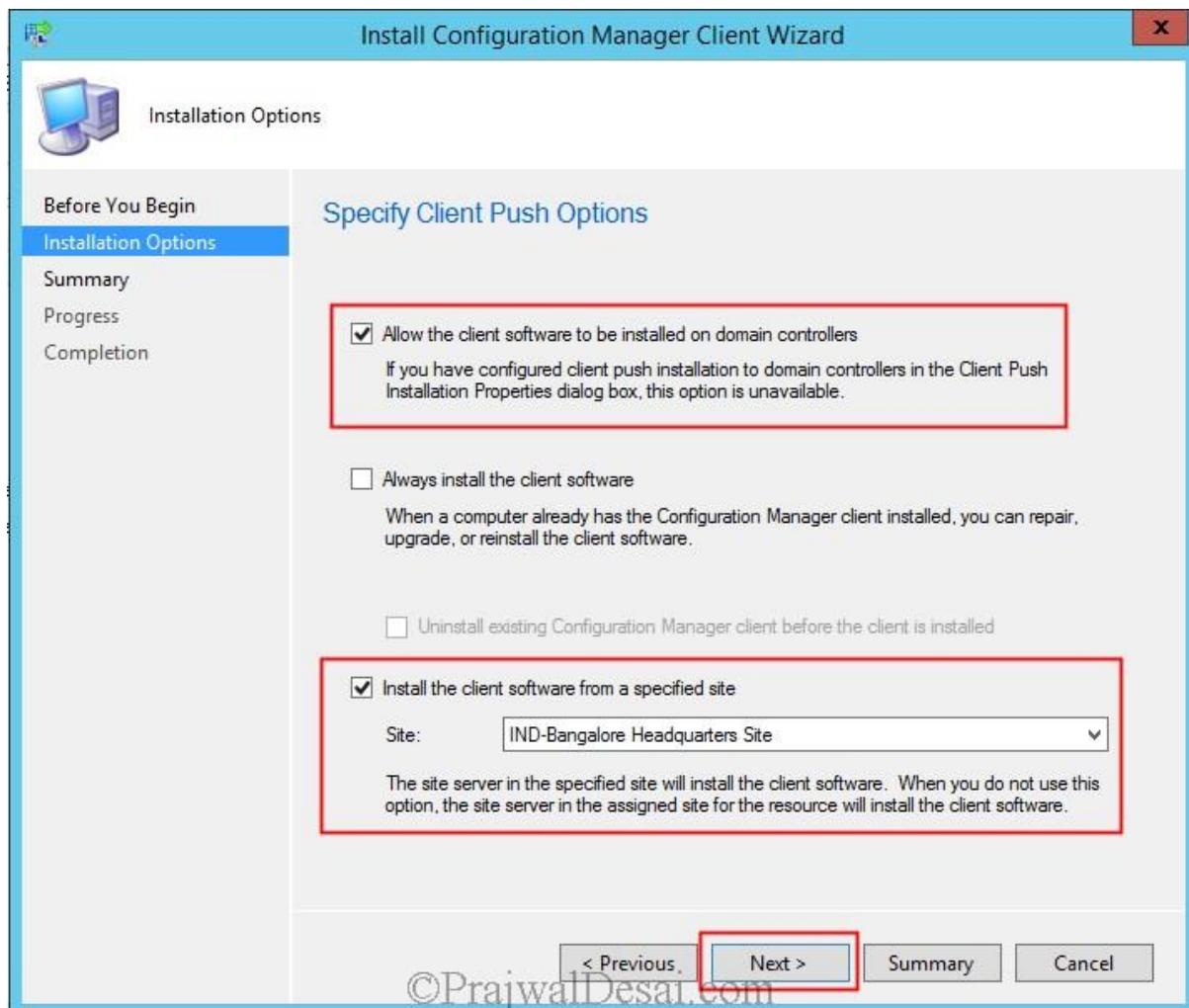
From the **Configuration Console**, Click **Assets and Compliance**, Under **Devices** Select **All Systems**. Right Click on the system where the client has to be pushed. Click **Install Client**.



Click Next.

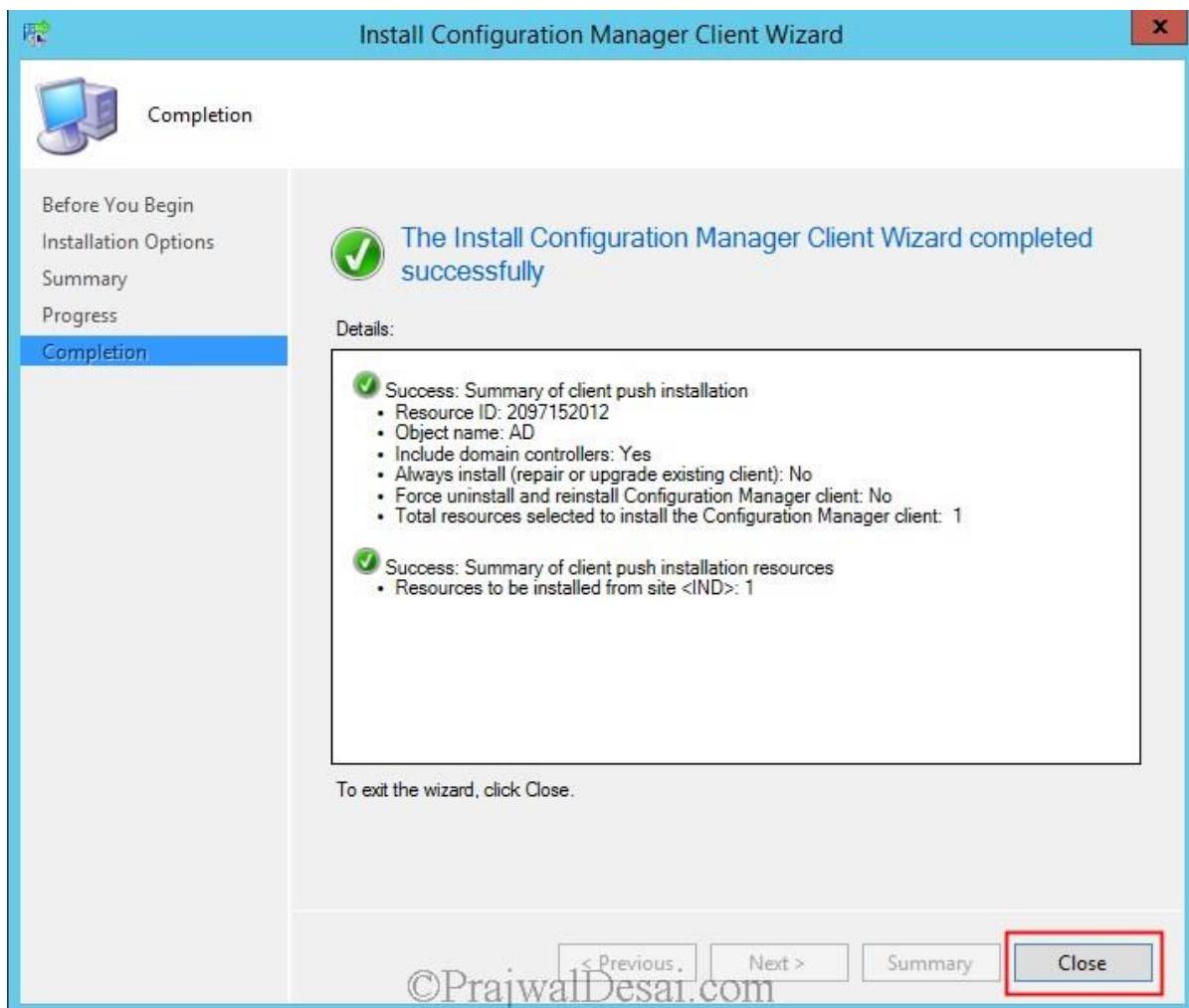


Specify Client Push Options – Since we are installed the client on the system which is a domain controller, check the box for **Allow the client software to be installed on domain controllers**. Also check **Install the client software from a specified site** and click **Next**.



©PrajwallDesai.com

Click **Close**.



If we take a look at **ccm.log** file on the SCCM server, we see the complete process right from how the request is sent to server and how the client is installed.



Boot Images and Distribution Point Configuration For OSD In SCCM 2012 R2

Boot Images and Distribution Point Configuration For OSD In SCCM 2012 R2 In this post we will look at the steps for boot images and Distribution Point configuration for OSD In SCCM 2012 R2. We will enable the PXE support and note that the steps shown in the post needs to be done before you use system center 2012 R2 configuration manager to deploy operating systems. One of the biggest advantage of using SCCM 2012 R2 is support for Windows Server 2012 R2 and Windows 8.1 and support for boot images created by using the Windows Automated Installation Kit (Windows AIK) for Windows 7 SP1 and based on Windows PE 3.1. You can refer to SCCM 2012 R2 step by step guide [here](#).

Ways to deploy operating systems

There are several methods that you can use to deploy operating systems to Configuration Manager client computers.

PXE initiated deployments: PXE-initiated deployments let client computers request a deployment over the network. The operating system image and a Windows PE boot image are sent to a distribution point that is configured to accept PXE boot requests.

Multicast deployments: In this method the operating system image is sent to a distribution point, which in turn simultaneously deploys the image when client computers request the deployment.

Bootable Media Deployments: Bootable media deployments let you deploy the operating system when the destination computer starts. When the destination computer starts, it retrieves the task sequence, the operating system image, and any other required content from the network. Because that content is not on the media, you can update the content without having to recreate the media.

Stand-alone Media Deployments: Stand-alone media deployments let you deploy operating systems in environments where it is not practical to copy an operating system image or other large packages over the network and in environments without network connectivity or low bandwidth network connectivity.

Prestaged Media deployments: Prestaged media deployments let you deploy an operating system to a computer that is not fully provisioned. The prestaged media is a Windows Imaging Format (WIM) file that can be installed on a bare-metal computer by the manufacturer or at an enterprise staging center that is not connected to the Configuration Manager environment.

We will first enable the **PXE support** for the clients. Launch the Configuration Manager 2012 R2 console, click on **Administration, Servers and Site system roles**, right click **Distribution point** and click **properties**. Click on **PXE** tab, check the box “**Enable PXE support for clients**“. There is warning box that appears, click on **Yes**. This will enable the PXE support for clients. When you enable the PXE support for clients the Windows Deployment Services will be installed in the background. You will see the WDS service running when you open services.msc.

Enable the option **Allow this DP to respond to incoming PXE requests**, this will allow DP to respond to the incoming PXE requests.

Enable the option **Enable unknown computer support**, an unknown computer may be a computer where the Configuration Manager client is not installed or it can be a computer that is not imported into Configuration Manager or that has not been discovered by Configuration Manager. To deploy operating systems to any of the computers you must enable this option.

Enable the option **Require a password when computers use PXE**, it is recommended to provide a strong password for any computers that use PXE. This is more of an additional security for your PXE deployments.

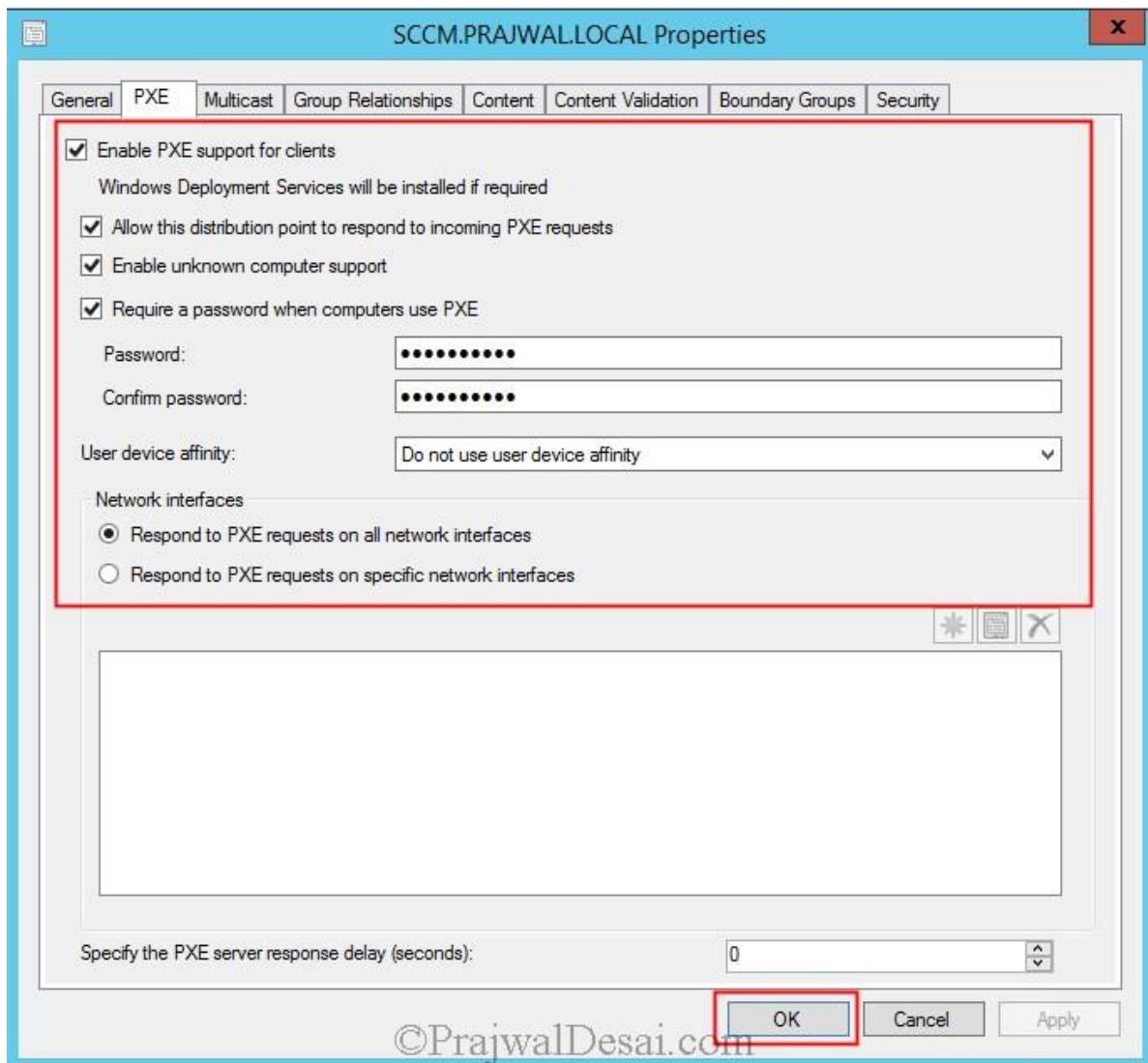
User Device Affinity – This is to specify how you want the distribution point to associate users with the destination computer for PXE deployments. You have 3 options for user device affinity,

- a) **Do not use user device affinity** – Select this if you do not want to associate users with the destination computer.
- b) **Allow user device affinity with manual approval** – Select this option to wait for approval from an administrative user before users are associated with the destination computer.
- c) **Allow user device affinity with automatic approval** – Select this option to automatically associate users with the destination computer without waiting for approval.

For the option **Network Interfaces**, select **Respond to PXE requests on all network interfaces**. Here you basically specify whether the distribution point responds to PXE requests from all network interfaces or from specific network interfaces. If you want a specific network interface to respond to PXE request select **Respond to PXE requests on specific network interfaces**.

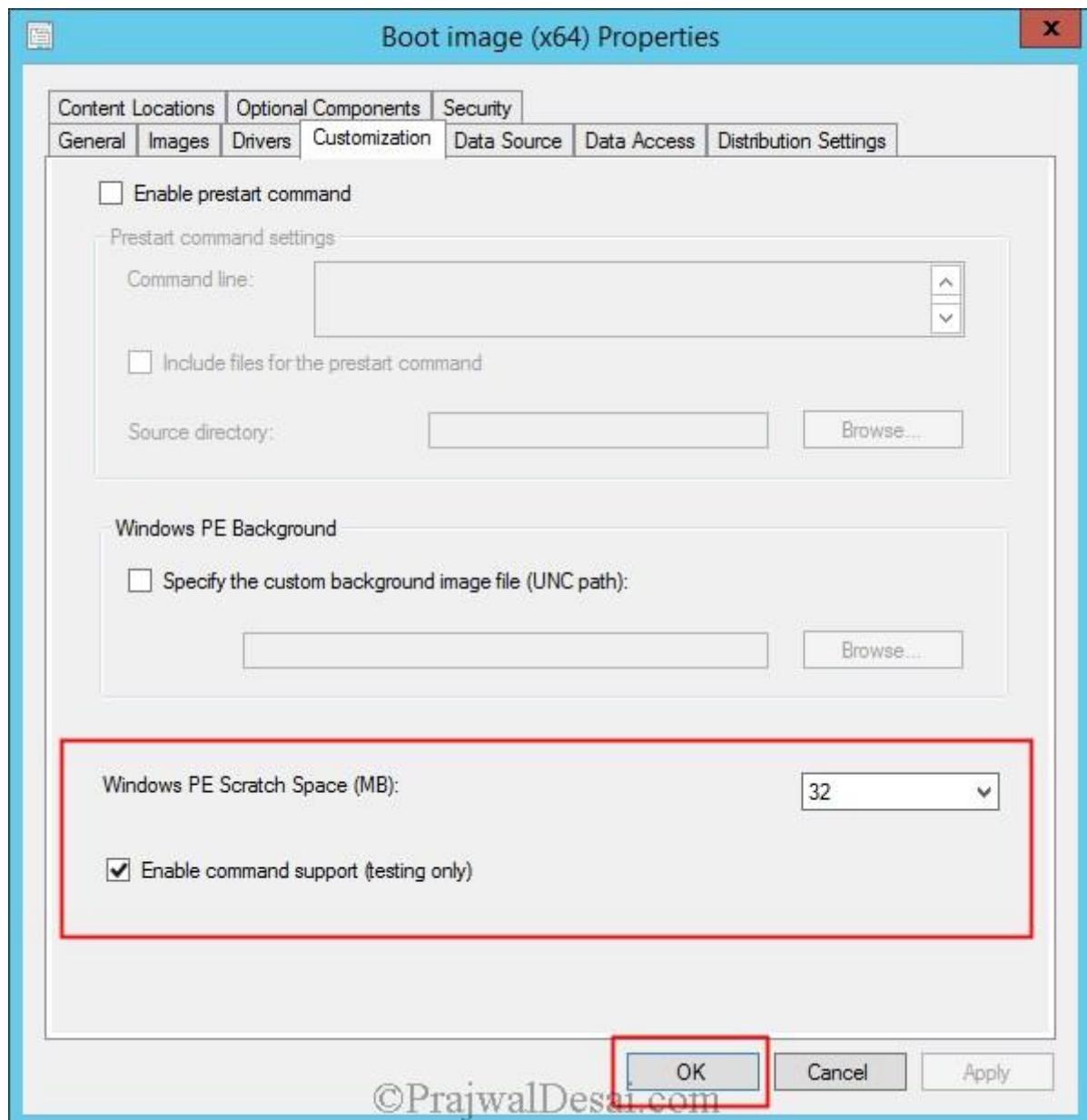
PXE server response delay – This option is to specify delay (in seconds) for the distribution point before it responds to computer requests when multiple PXE-enabled distribution points are used. By default, the Configuration Manager PXE service point responds first to network PXE requests.

Once you have configured these options click on **Apply** and click on **OK**.



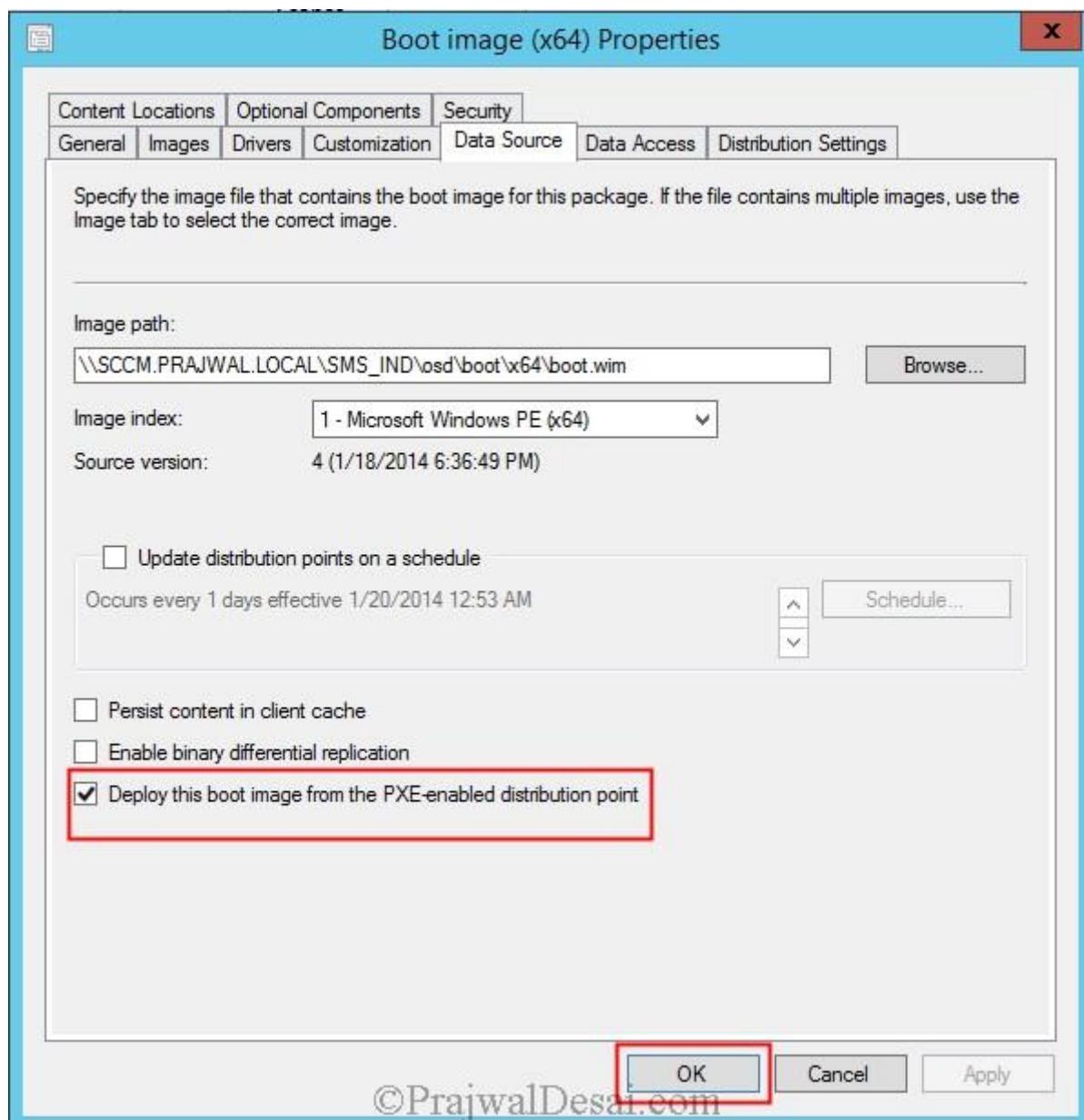
Boot Images – Before you proceed for OSD, you need to make few changes to the Boot Images too. When you install SCCM 2012 R2, you will find that there are 2 images that are installed by SCCM. **Boot Image (x64)** – used when you deploy 64 bit OS, **Boot Image (x86)** – used when you deploy 32 bit OS.

The first step is to enable the command support on both the boot images. Enabling this option helps in troubleshooting OS deployment issues. To enable the command support, in the CM console, click **Software Library**, expand **Operating system**, Click **Boot Images**. Right click **Boot Image (X64)** and click on **Properties**. Click on **Customization** tab and check the box **Enable Command Support (testing only)**. Click on **Apply**.



After you enable the command support, on the same window click on **Data Source** tab and make sure the option **Deploy this boot image from the PXE-enabled DP**. This is option is enabled by default, if its not enabled please enable it. Click on **Apply** and click **OK**.

The changes that you made to **Boot Image (x64)**, repeat the same for **Boot Image (x86)**.



©PrajwalDesai.com

After you make the changes to the Boot Images you must distribute the content to DP. If you had distributed the boot images to DP previously and in case if you make changes to it post that then you can **Update Distribution Points**. To distribute the boot images to DP, right click on the boot image and click **Distribute Content**. Distribute content of both the boot images.

The screenshot shows the Software Library interface with the following details:

- Software Library Tree:** Packages, Global Conditions, App-V Virtual Environments, Windows Sideloading Keys, Software Updates, All Software Updates, Software Update Groups, Deployment Packages, Automatic Deployment Rules, Operating Systems, Drivers, Driver Packages, Operating System Images, Operating System Installers, Boot Images (selected), Task Sequences, Virtual Hard Disks.
- Search Bar:** Search term: "Boot Images 2 items".
- Table View:**

Icon	Name	Version	Comment	Image ID	OS Version
Boot image (x64)	6.3.9600.16384			IND00005	6.3.9600.1...
Boot image (x86)	6.3.9600.16384				6.3.9600.1...
- Context Menu (Open for Boot image (x64)):**
 - Refresh (F5)
 - Delete
 - Distribute Content
 - Update Distribution Points
 - Create Prestaged Content File
 - Manage Access Accounts
 - Move
 - Set Security Scopes
 - Properties
- Bottom Navigation:** Assets and Compliance, ©PrajwalDesai.com, Summary, Content Status.

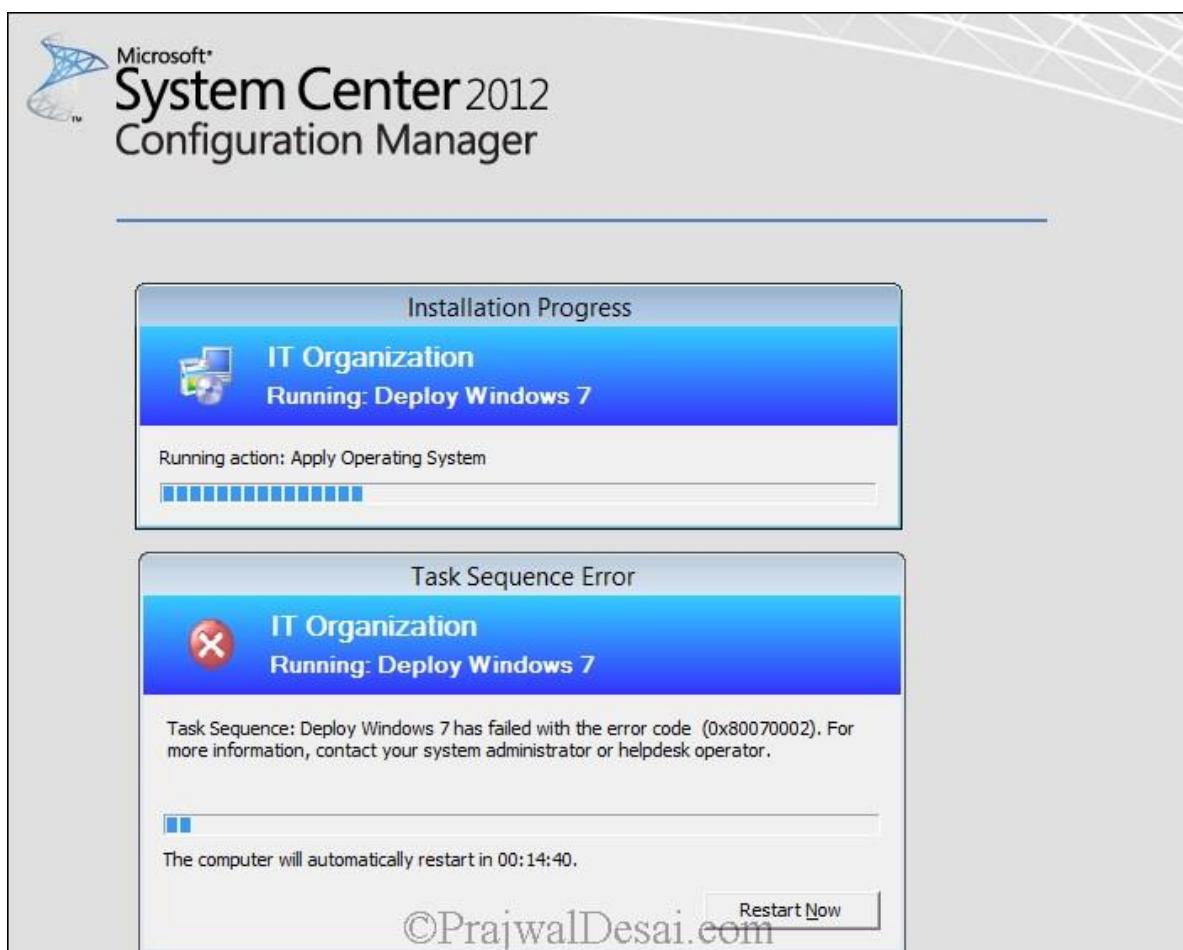
You can check if these boot images are available to DP by checking the **Content Status** of each boot image. Under **Completion Statistics** you should see a green circle that indicates that the content is distributed successfully and is available with DP.

The screenshot shows the Monitoring interface with the following details:

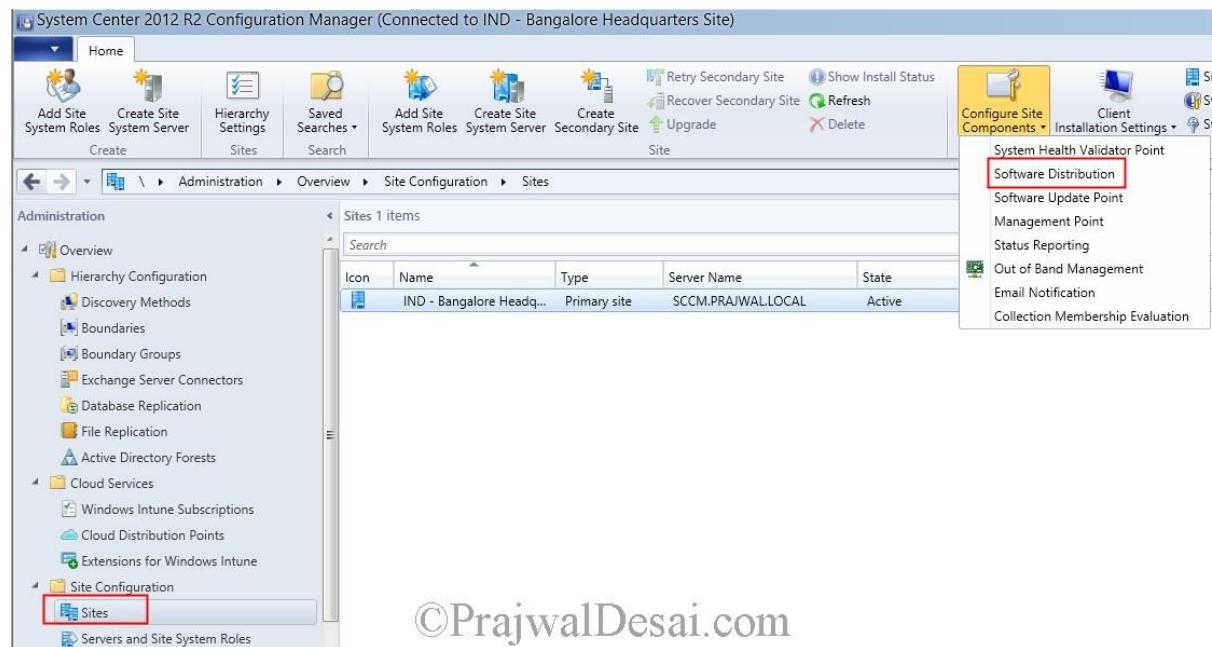
- Monitoring Tree:** Overview, Alerts, Queries, Reporting, Site Hierarchy, System Status, Deployments, Client Operations, Client Status, Database Replication, Distribution Status (Content Status selected), Distribution Point Group Status, Distribution Point Configuration, Software Update Point Synchronization, Endpoint Protection Status.
- Content Status Table:**

Icon	Software	Type	Targeted	Size (MB)	Compliance %	Date Cre
Boot image (x64)	Boot Image	1	209.67	100.0	1/18/20	
Boot image (x86)	Boot Image	1	171.02	100.0	1/9/201	
Configuration Manager Client Package	Package	1	173.37	100.0	1/9/201	
Configuration Manager Client Upgrade Package	Package	1	1.54	100.0	1/9/201	
KB 2905002 - console update - IND	Package	1	2.07	100.0	1/9/201	
KB 2905002 - server update - IND	Package	1	28.96	100.0	1/9/201	
KB 2905002 - x64 client update - IND	Package	1	0.97	100.0	1/9/201	
KB 2905002 - x86 client update - IND	Package	1	0.81	100.0	1/9/201	
Microsoft Corporation User State Migration Tool f...	Package	0	48.66		1/9/201	
Microsoft Office Professional Plus 2010	Application	1	1,402.03	100.0	1/18/20	
Windows 7 Professional	Operating System Image	1	2,816.18	100.0	1/18/20	
- Content Status Details for Boot image (x64):**
 - General:** Software: Boot image (x64), Type: Boot Image, Date Created: 1/18/2014 6:36 PM, Package ID: IND00005.
 - Completion Statistics:** Success: 1, In Progress: 0, Failed: 0, Unknown: 0. A large green circle icon is displayed.
 - Bottom Navigation:** Assets and Compliance, Software Library, Monitoring, Administration.

Network Access Account – In the SCCM Technet forums I have seen users posting questions on OSD error “**Task Sequence Failed with the Error Code 0x80070002**“. We see this error during the operating system deployment using SCCM 2012 R2. When you deploy the task sequence to a collection and when you boot the computer from the network, during the step “**Applying Operating System**” you encounter the Error Code 0x80070002. To fix the issue **Error Code 0x80070002**, we have to define the network access account. The Network Access account is used only for accessing the content and not for running the task sequence. This account should have the minimum appropriate permissions on operating system deployment content it needs to access. This account is important because the computer receiving the operating system does not have a security context it can use to access content on the network.

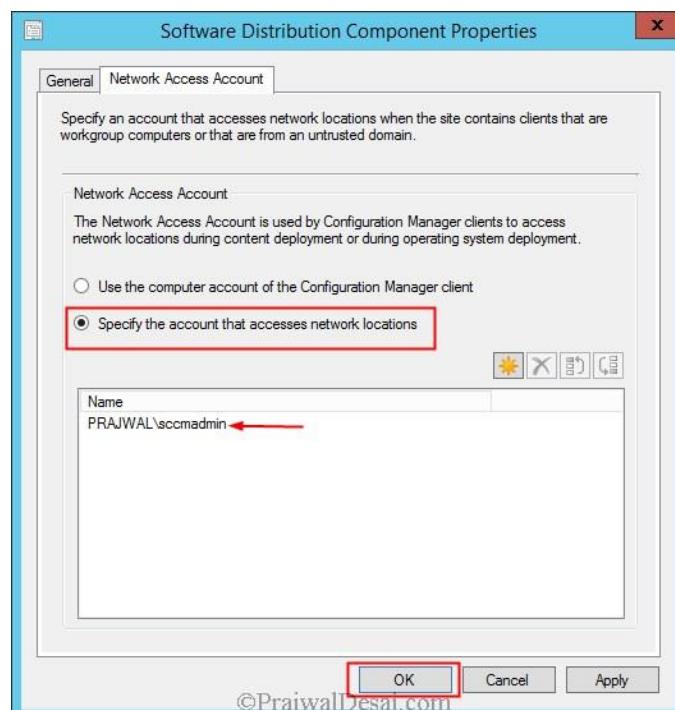


To configure the Network Access Account, open the CM2012 R2 console, click on **Administration**, expand Overview, expand **Site Configuration**, click **Sites**, on the top ribbon click **Configure Site Components**, click **Software Distribution**.



©PrajwalDesai.com

Click on the tab **Network Access Account**, choose **Specify the account that accesses network locations** (by default the option is set to **Use the computer account of Configuration Manager client**). Click on the orange icon and add the user account that has enough permissions to access the content which is required while deploying Operating System. Click on **Apply** and click on **OK**.



©PrajwalDesai.com

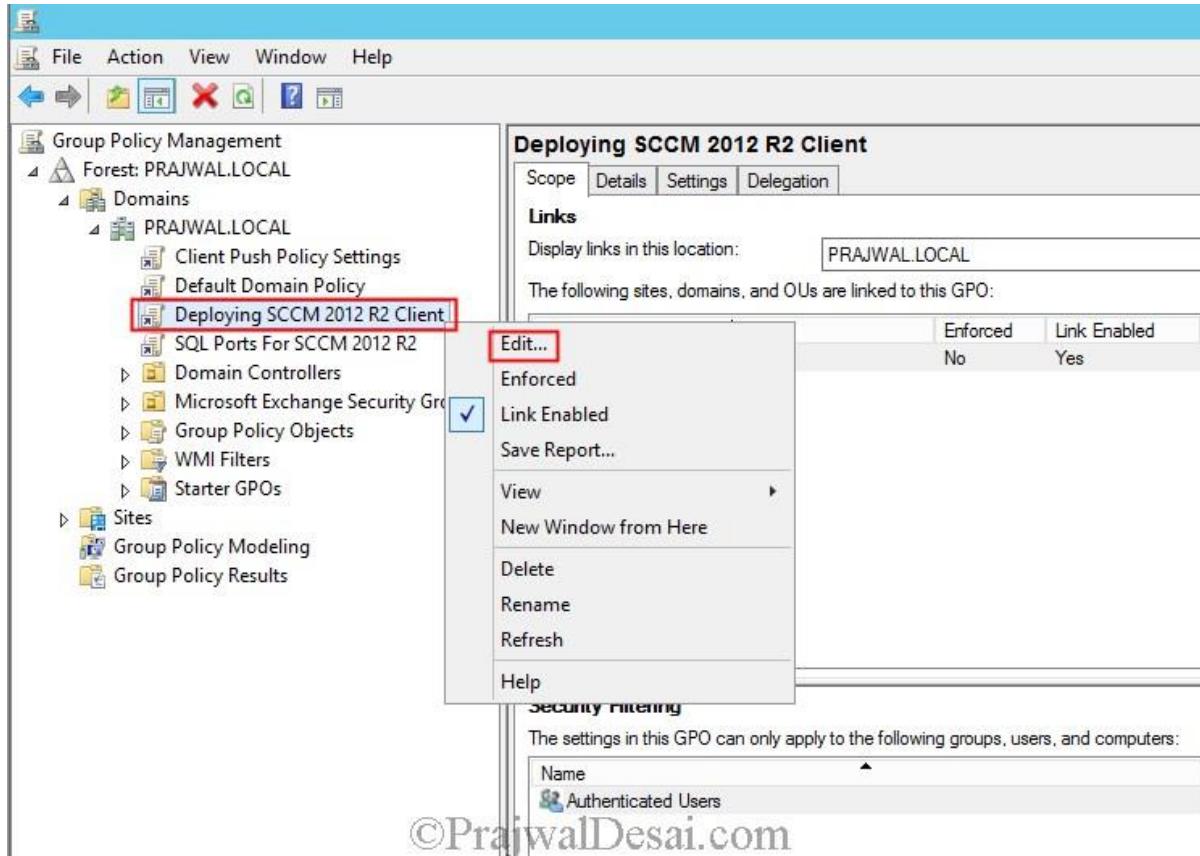
[Deploying Configuration Manager 2012 R2 Clients Using Group Policy](#)

Deploying Configuration Manager 2012 R2 Clients Using Group Policy In this post we will see the steps for Deploying Configuration Manager 2012 R2 Clients Using Group Policy. This is the post that I wanted to add to when I was working on SCCM 2012 SP1, however the same steps will still work if you want to deploy configuration manager clients using group policy using SCCM 2012 or SCCM 2012 SP1. In my previous post we saw the configuration manager 2012 R2 client installation using [automatic site wide client push installation method](#) and [client push installation method](#). In this post we will see the steps for Deploying Configuration Manager 2012 R2 Clients Using Group Policy. At any point of time you can jump to [configuration manager 2012 R2 step by step guide](#) for my previous posts.

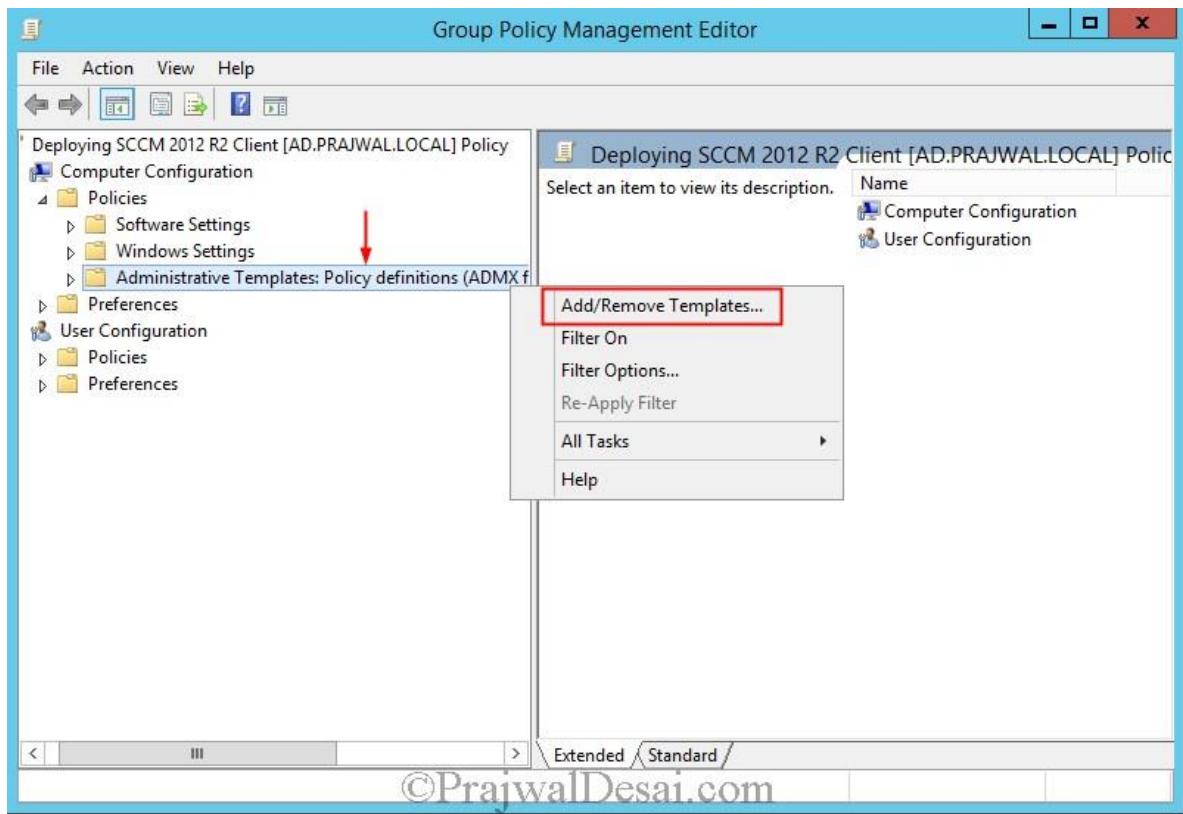
If you are planning to deploy SCCM 2012 R2 clients using group policy then you must make sure that in the client push installation properties, **Enable Automatic site wide client push installation** is not checked. If this is checked then the client would get installed on all the systems after its discovery. So first uncheck the option **Enable Automatic site wide client push installation** and proceed. In this post my domain controller is running on Windows Server 2012 R2 Datacenter edition, SCCM 2012 R2 running on Windows Server 2012 R2 Datacenter edition and the client machines are running windows 7 professional SP1 x64 and Windows 8.1.

Deploying Configuration Manager 2012 R2 Clients Using Group Policy

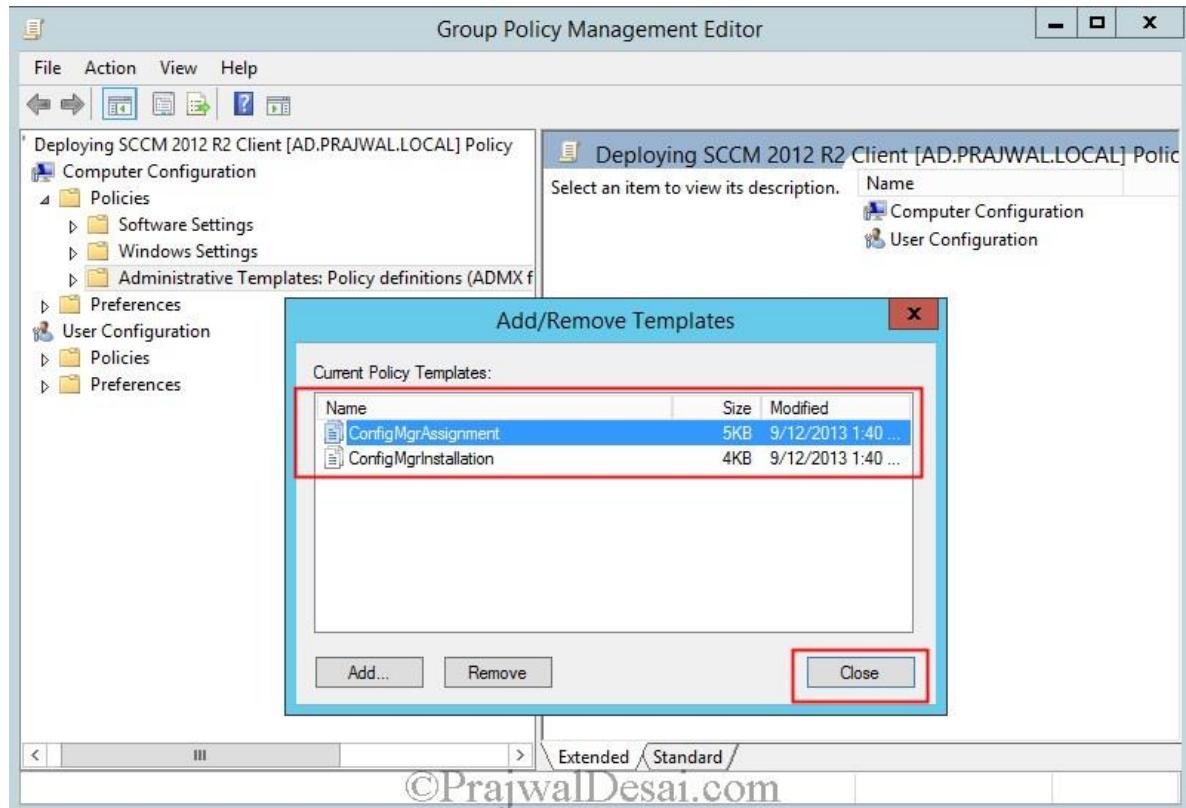
We will create a new policy first, click on **Server Manager**, click on **Tools**, click **Group Policy Management**. Right click on domain and create a new policy, we will name it as **Deploying SCCM 2012 R2 Client**. Right click on the policy that is created and click **Edit**.



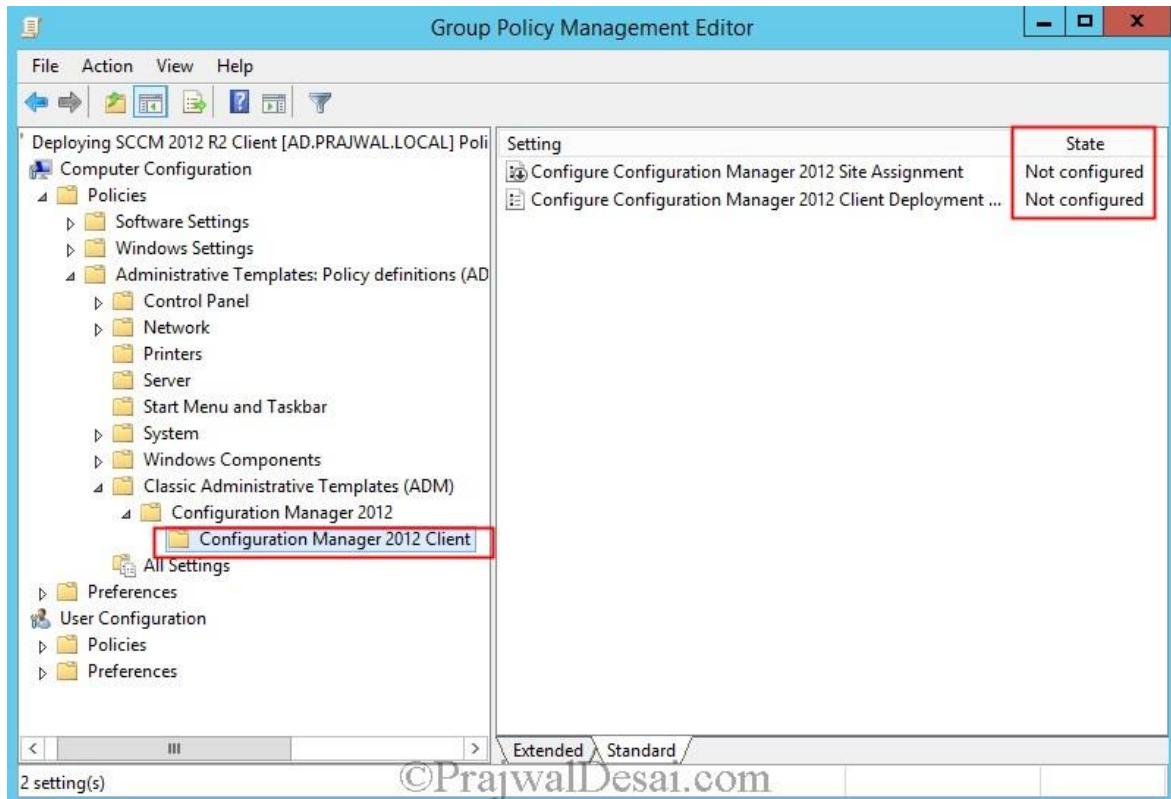
Expand **Computer Configuration**, **Policies** and right click on **Administrative Templates** and click on **Add/Remove Templates**.



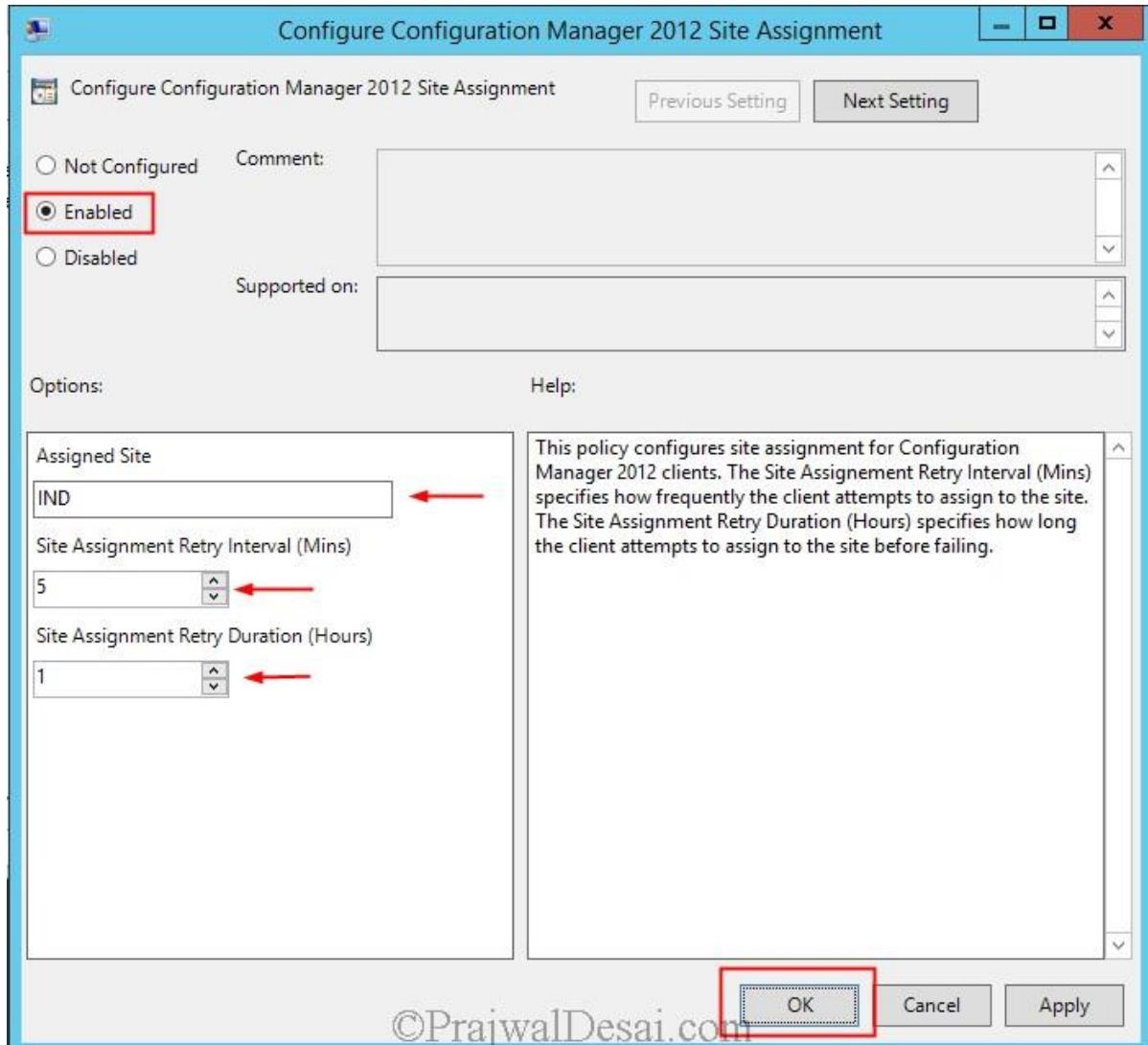
You can add the templates by clicking on **ADD**. The Configuration Manager templates can be found in **SourceDVD\SMSSETUP\TOOLS\ConfigMgrADMTemplates** or you can also add it from **<Drive>:\Program Files\Microsoft Configuration Manager\tools\ConfigMgrADMTemplates**. You need to add 2 templates **ConfigMgrAssignment** and **ConfigMgrInstallation**. Click on **Close**.



Expand **Administrative Templates**, **Classic Administrative Templates**, **Configuration Manager 2012**, **Configuration Manager 2012 Client**. We see on the right pane that both the templates have been added but they not configured yet.



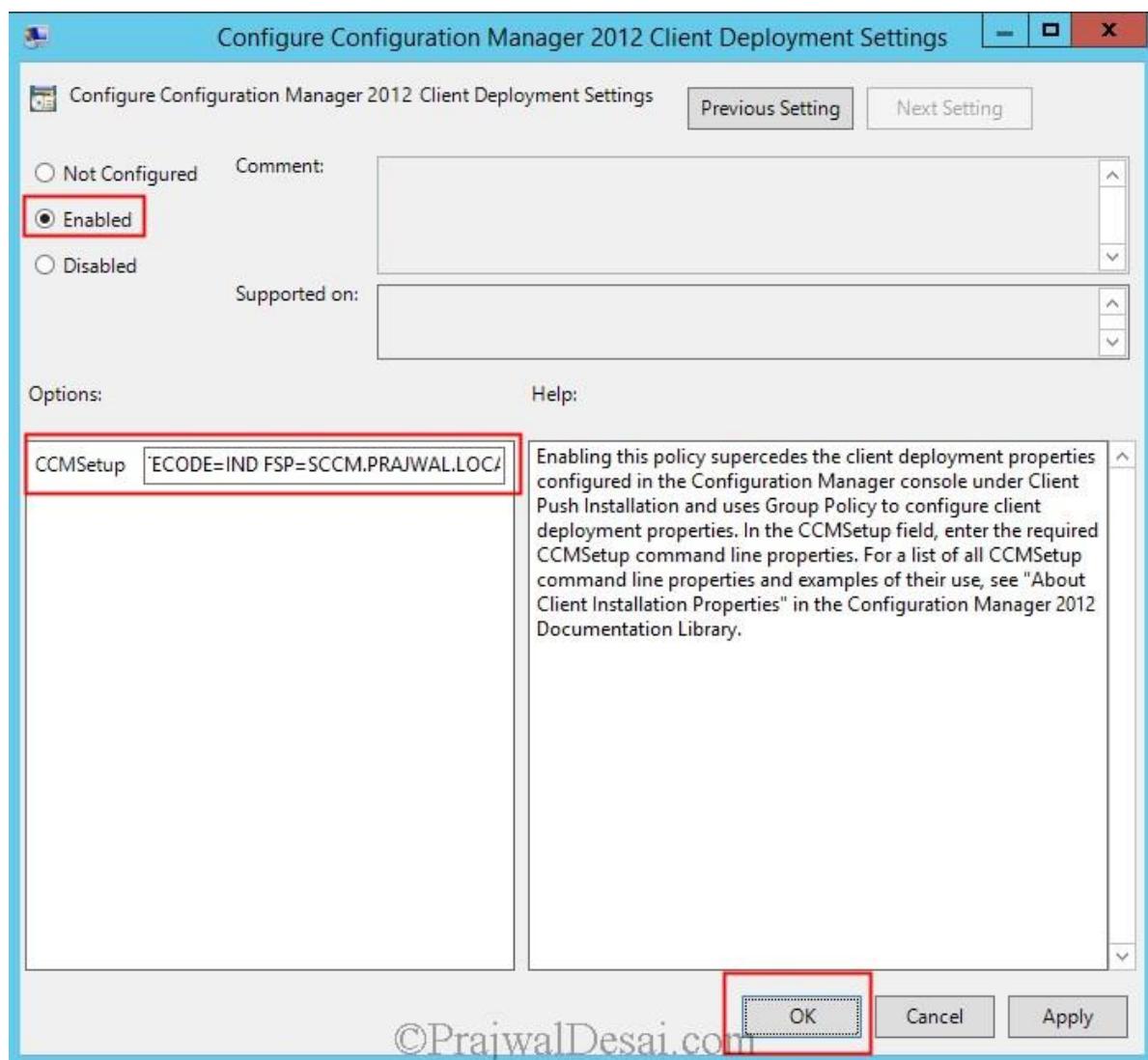
Right click on **Configure Configuration Manager 2012 Site Assignment** template and click **edit**. Click **Enabled** to enable the policy, under Options specify **Assigned Site code**, **Site Assignment Retry Interval** to **5 minutes**, **Site Assignment Retry Duration** to **1 hour** (You can also choose to leave the options to default except site code). Click **OK**.



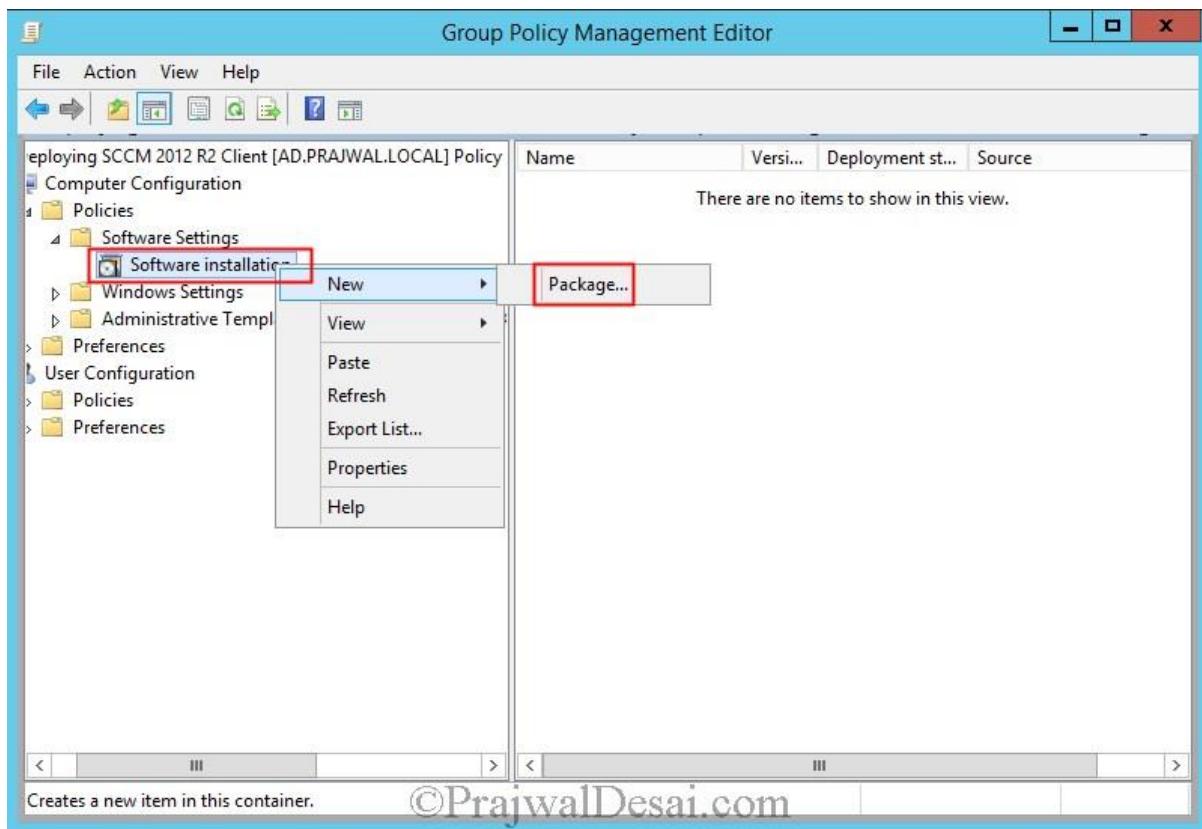
Right click **Configure Configuration Manager 2012 Client Deployment Settings** and click on **Enabled**. Under options specify the installation properties for CCMSetup file. You can specify lots of installation properties for installation of configuration manager client, click the button below for knowing more on CCMSetup command line properties. In our case I have used following installation command **CCMSetup.exe SMSSITECODE=IND FSP=SCCM.PRAJWAL.LOCAL MP=SCCM.PRAJWAL.LOCAL**

[CCMSetup Command Line Properties](#)

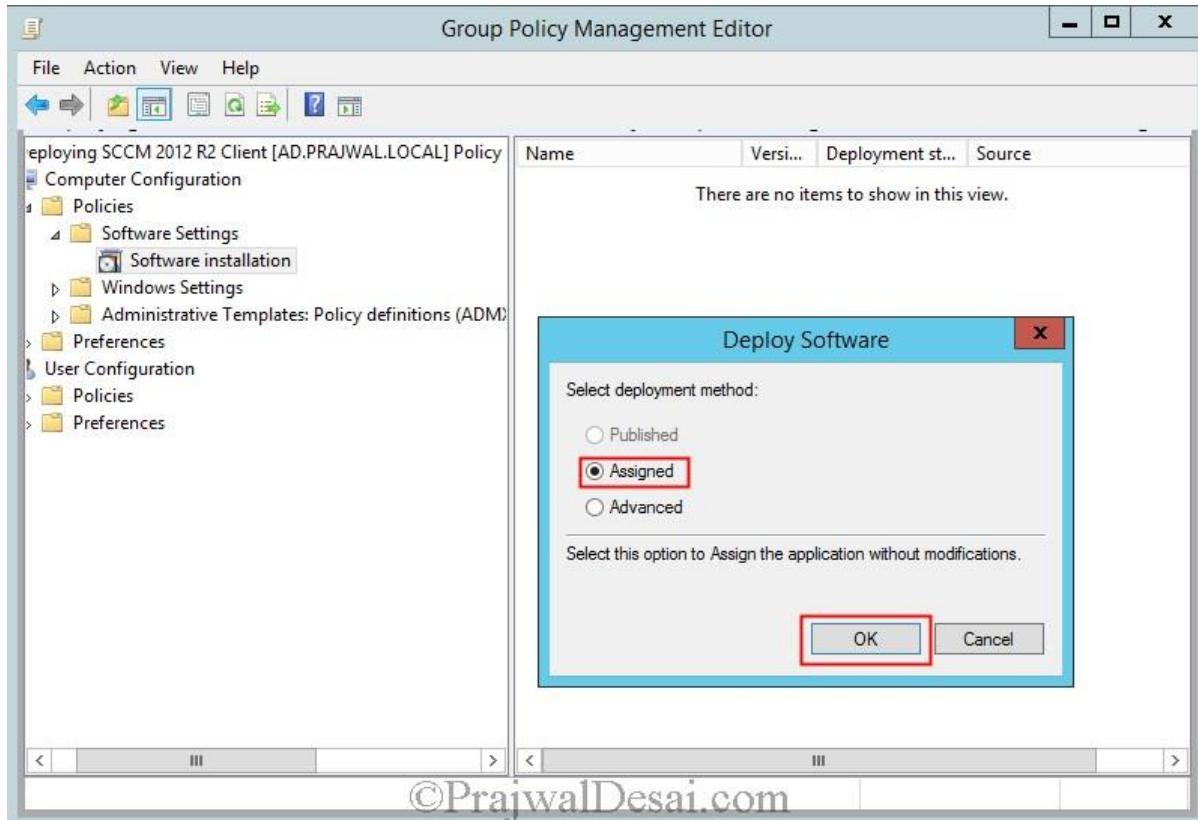
Click on **OK**.



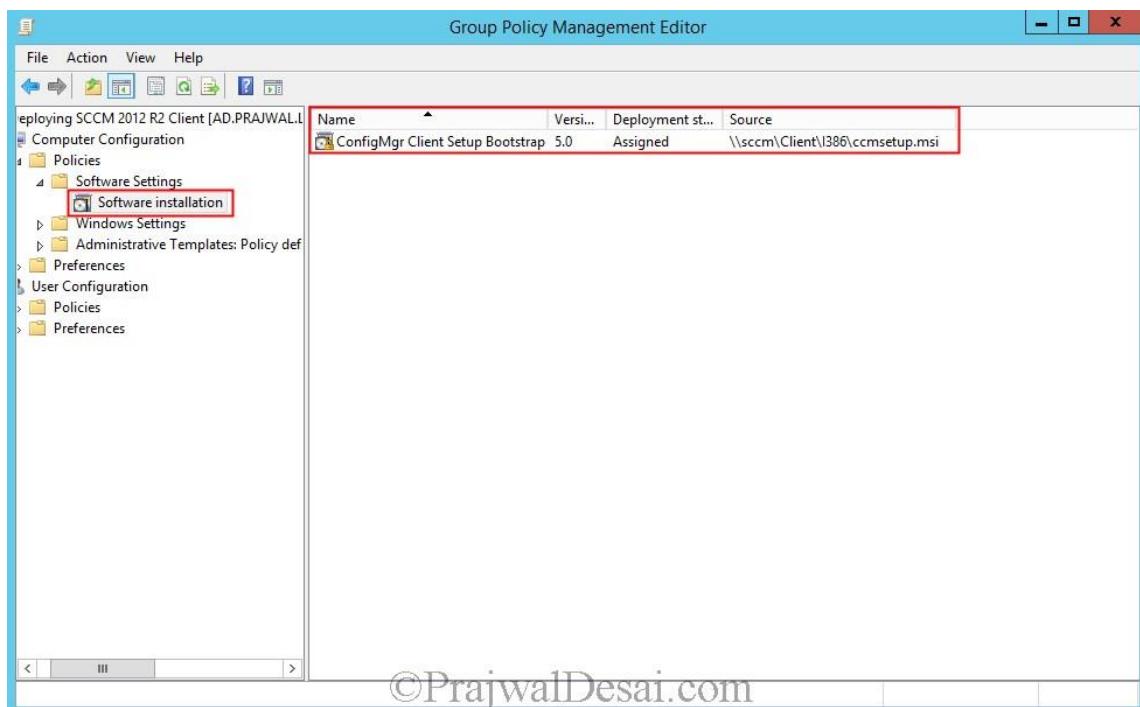
Under **Computer Configuration** expand **Policies, Software Settings**. Right click **Software Installation** and click **New -> Package**.



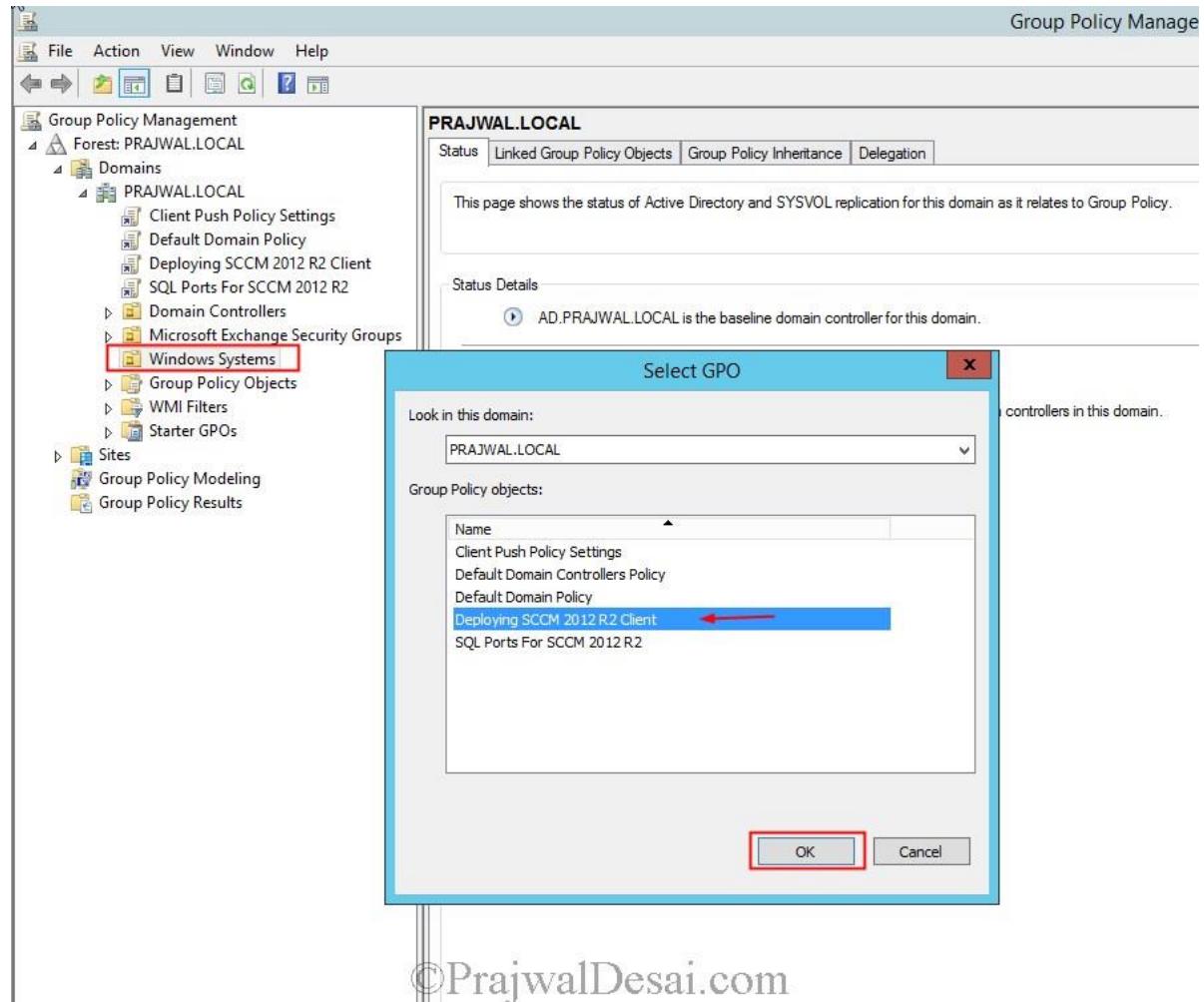
The **ccmsetup.msi** can be found in **SOURCEDVD\SMSSETUP\BIN\I386** (SourceDVD Is the SCCM 2012 .ISO file). Copy the ccmsetup.msi in a folder (Create a new folder on SCCM Server) and share it with permissions Read-only for **Everyone**. Browse the file ccmsetup.msi to the folder that you created and Select the **deployment method** as **Assigned**. Click **OK**.



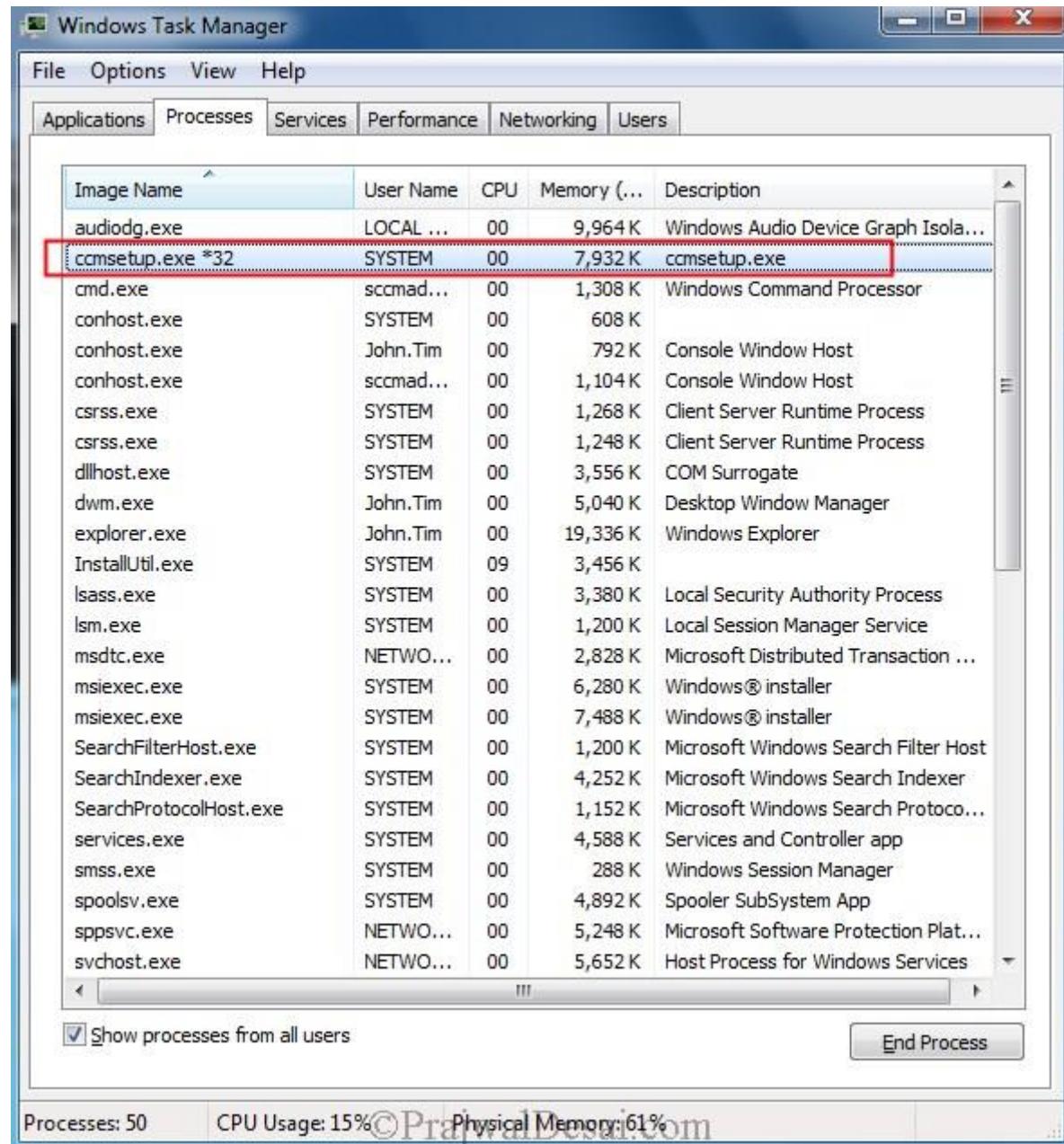
When you click on Software installation you should see the name of the **Package**, its **Version**, **Deployment Status** and **Source**. You can now close the GPMC.



You can choose to apply this policy at domain level or at OU level. If you apply it at domain level then every computer in your domain will get the SCCM 2012 R2 client installation on next reboot. I have created a OU called **Windows Systems** which consists of client computers. To link the policy to this OU, right click on OU **Windows Systems**, click **Link an existing GPO**, choose the GPO **Deploying SCCM 2012 R2 Client** and click **OK**.



You need to perform gpupdate on domain controller first and then on client machines. Reboot the client machine and after you login to client machine the configuration manager 2012 R2 client installation begins. You can see the cmmsetup.exe *32 on one the client machines in the below screenshot.



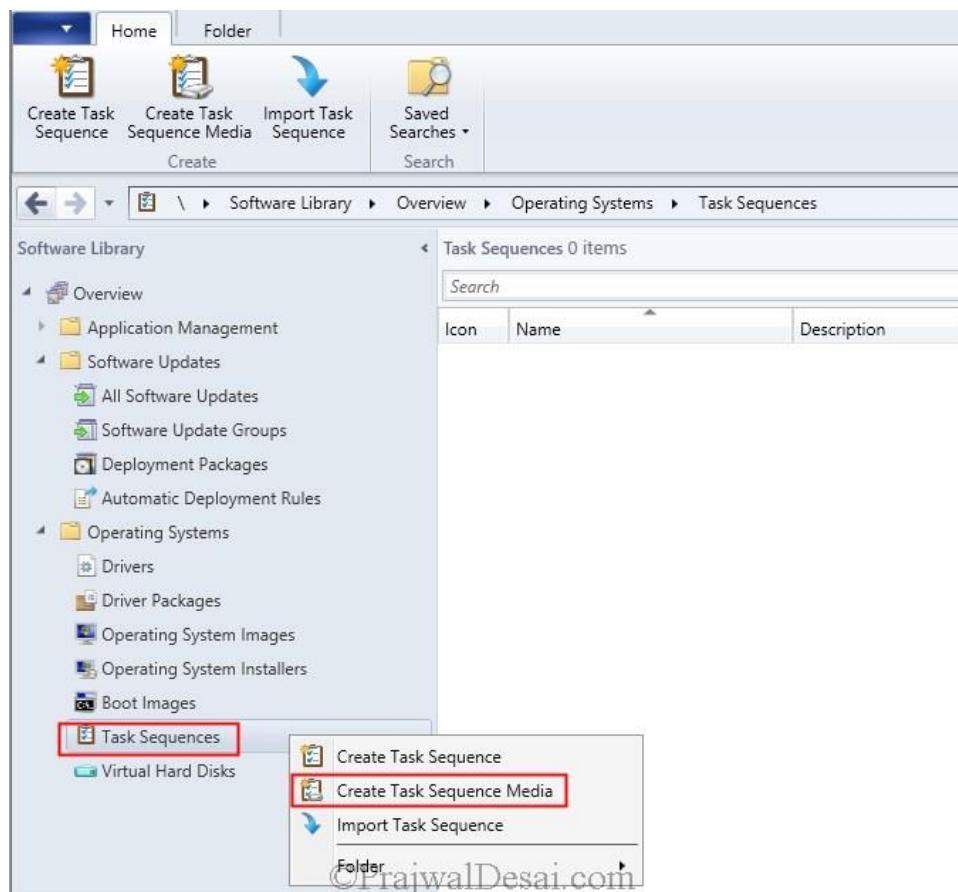
[Capture Windows 7 Image Using SCCM 2012 R2](#)

In this post we will see the steps to capture windows 7 using SCCM 2012 R2. This post is different from the one which shows the steps to [build and capture the operating systems using SCCM 2012 R2](#). We will not be using build and capture approach here rather we will capture a reference operating system, i.e. capture windows 7 using SCCM 2012 R2 and we will also see how to deploy the same using SCCM 2012 R2 in the next post. Please note that the computer operating system that we are going to capture should not be part of domain, else the sysprep fails during this process. So you capture a computer that has windows 7 installed (along with softwares like office, adobe reader etc) which is not joined to the domain. At any point of time you can check the [step by step guide for SCCM 2012 R2](#) which contains all the posts related to SCCM 2012 R2.

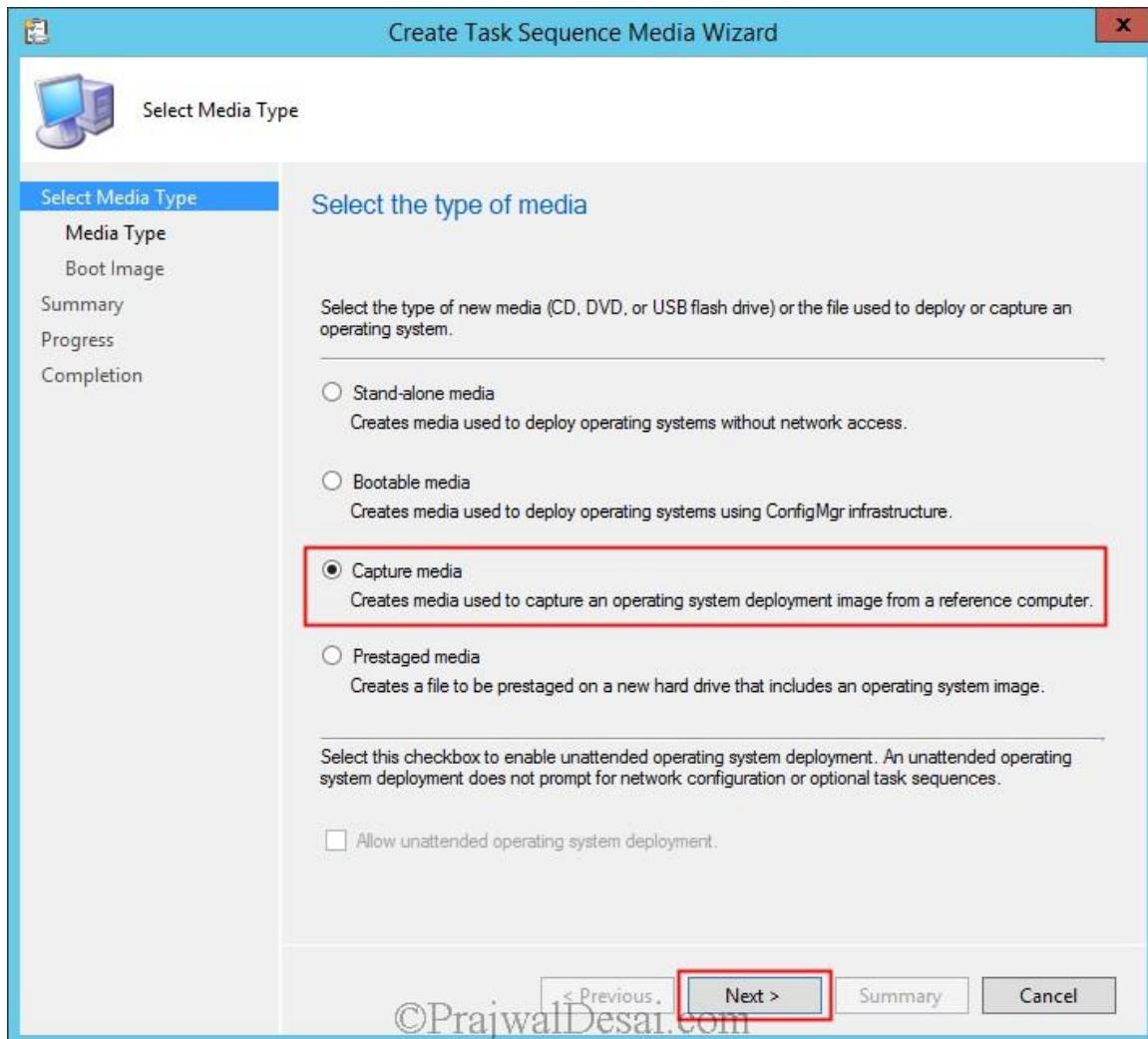
Capture Windows 7 Using SCCM 2012 R2

We will first create a task sequence media and create a capture media which is in saved .iso format. This .iso file contains the necessary files and instructions to capture a reference operating system. The same .iso file captures the operating system and stores the captured OS in .wim format. Once we get the .wim file we will import the file to SCCM 2012 R2 and we can use this .wim to deploy this OS to another computer either by using SCCM or WDS.

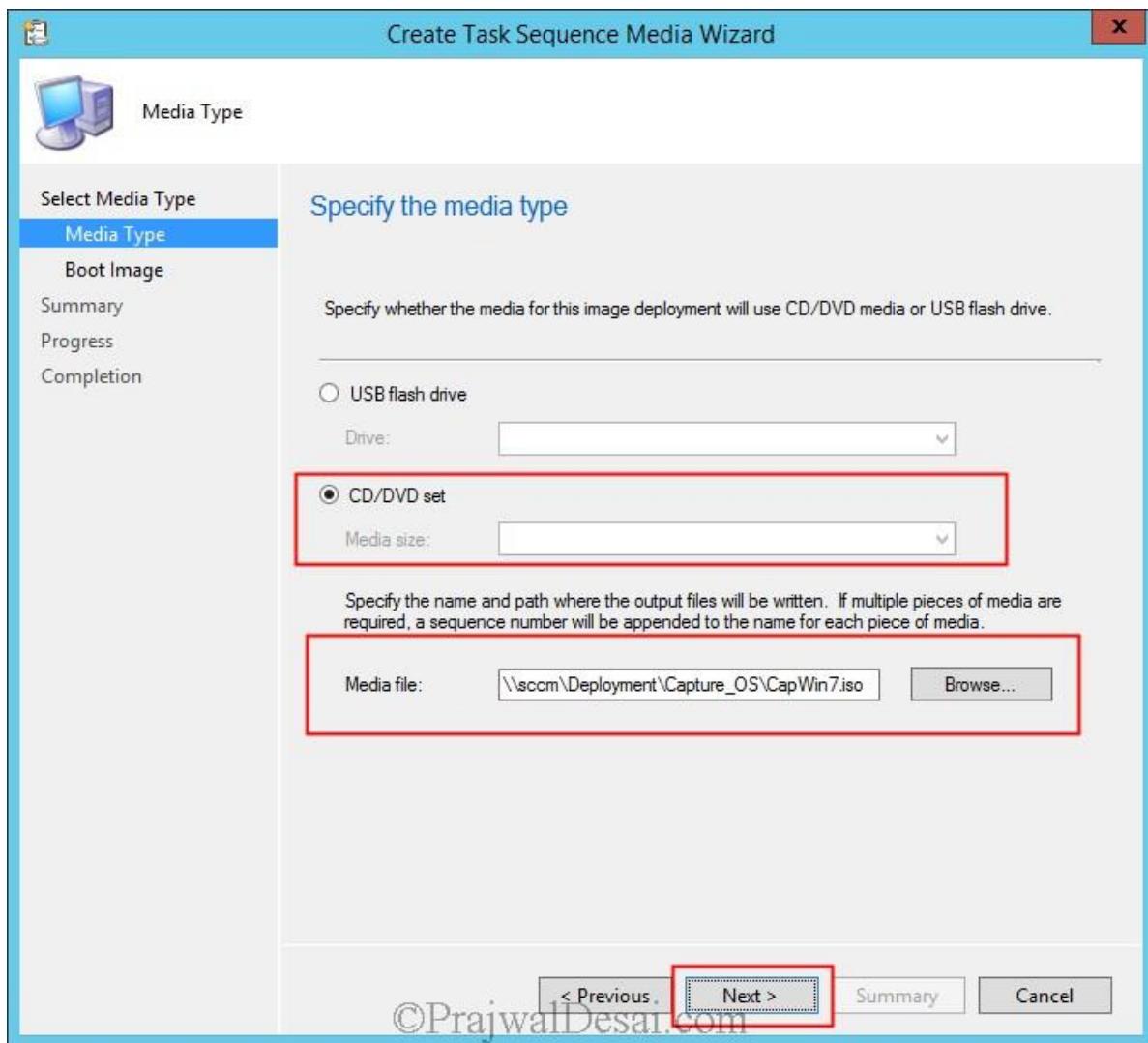
The first step involves creating a capture media which is in .iso file. Launch the **ConfigMgr** console, click on **Software Library**, expand **Overview**, expand **Operating Systems**, right click **Task Sequences** and click on **Create Task Sequence Media**.



Type of Media – Select the type of media as **Capture Media**. Click **Next**.

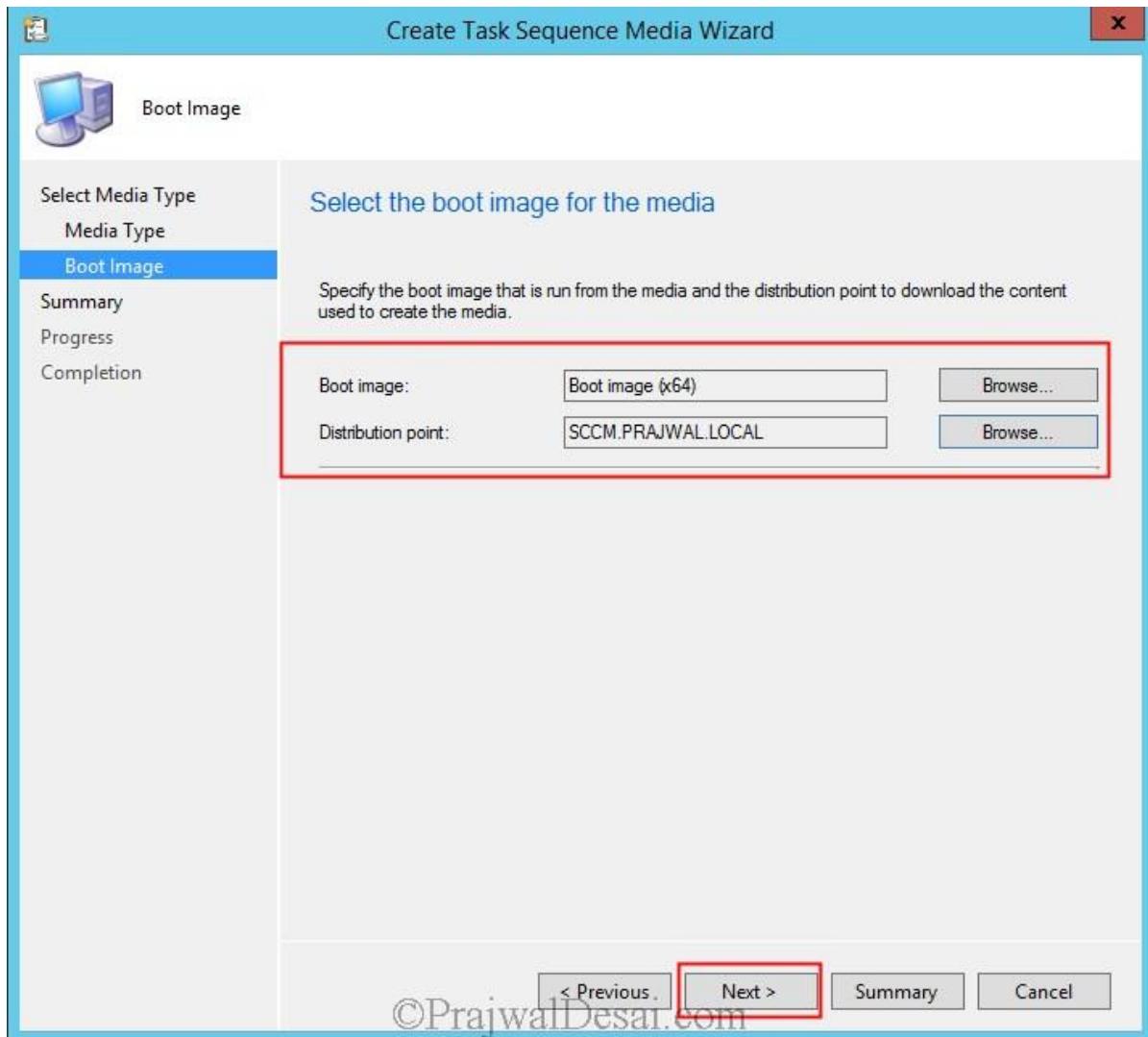


Media Type – You can select either **USB flash drive** or **CD/DVD**. I have tried using USB flash drive and even that works. In this example we will choose **CD/DVD**, and we will store the media file in one of the shared location on SCCM server. You can choose to store the capture media on any shared location, it may not be necessarily SCCM server. One important thing here you must save the capture media with **.iso** extension. Click on **Next**.

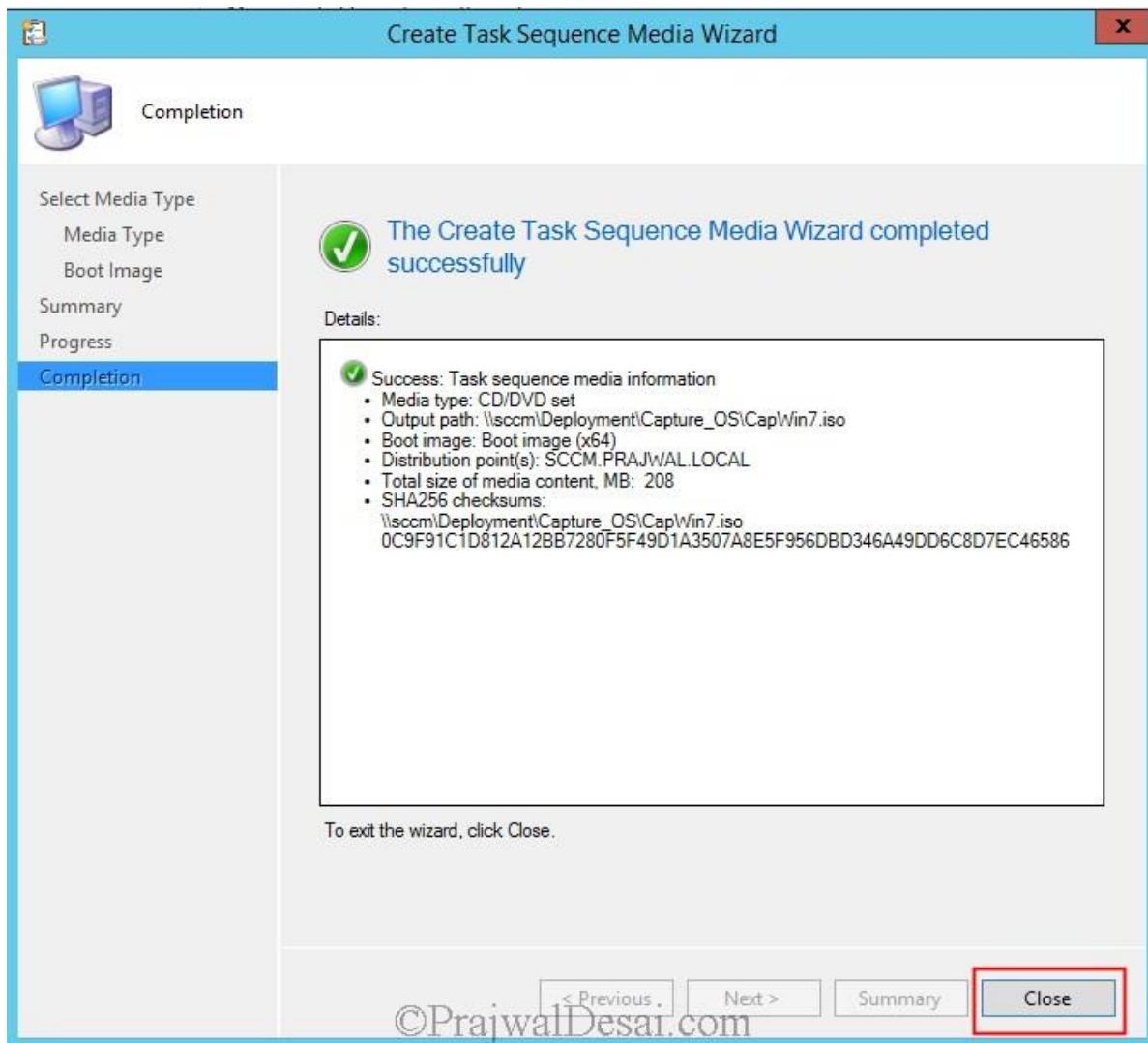


Selecting Boot Image – This is very important step. Select the **Boot Image** by clicking on **Browse**. Select **Boot Image (x64)** and for DP click on **Browse** and select the desired DP. Click **Next**.

NOTE – You must first enable the command support on both the boot images(x64 and x86) and then distribute it to the distribution point. To enable the command support right click on each of the boot image, click on properties and under Customization tab check the box Enable Command Support (testing only). Enable command support for both the boot images. By default the boot images are not distributed to DP and if you don't distribute the boot images you will not be able to select the DP in the below step. To distribute the boot images to DP, right click on each boot image and click Distribute Content.



The capture media has been created by the wizard. Click on **Close**.



After creating the capture media we will now mount the capture media (.iso file) on the windows 7 machine and run the image capture wizard. In this example I have a virtual machine which has been installed with windows 7 professional SP1 x64 OS and we will be capturing this computer OS image. If its a physical machine you can burn the capture media .iso to a CD and insert it in the CD tray and run the image capture wizard. If its a virtual machine you can mount the .iso file by providing the path where the capture media .iso file exists. On a virtual machine when you mount the .iso file by providing a shared location, it asks for a user account to access the .iso file, provide a domain user account which has enough permissions to access the folder where the .iso file exists.

Once you mount the capture media on a windows 7 machine you will see the autorun box. Click **Run TSMBAutorun.exe**, you will see the Image Capture Wizard. Click on **Next**.



Image Destination – Provide a folder path where the captured image should be stored. The name of the captured image should have **.wim** as extension. Also provide a user account that has enough permissions to store the captured file to the shared folder. Click **Next**.

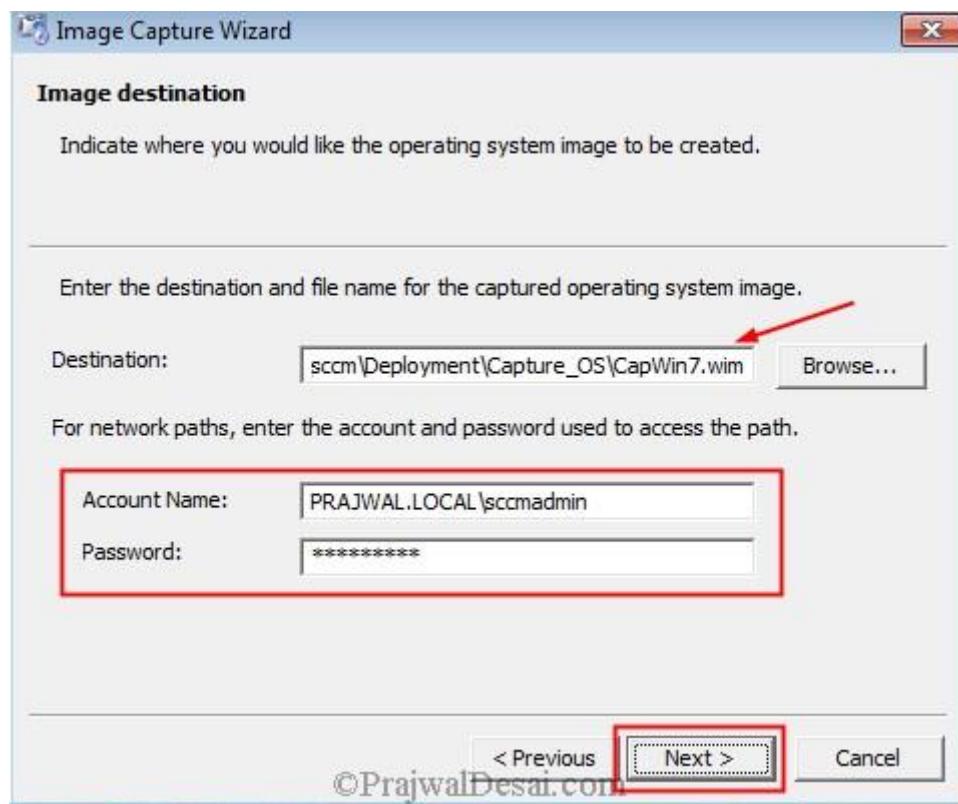
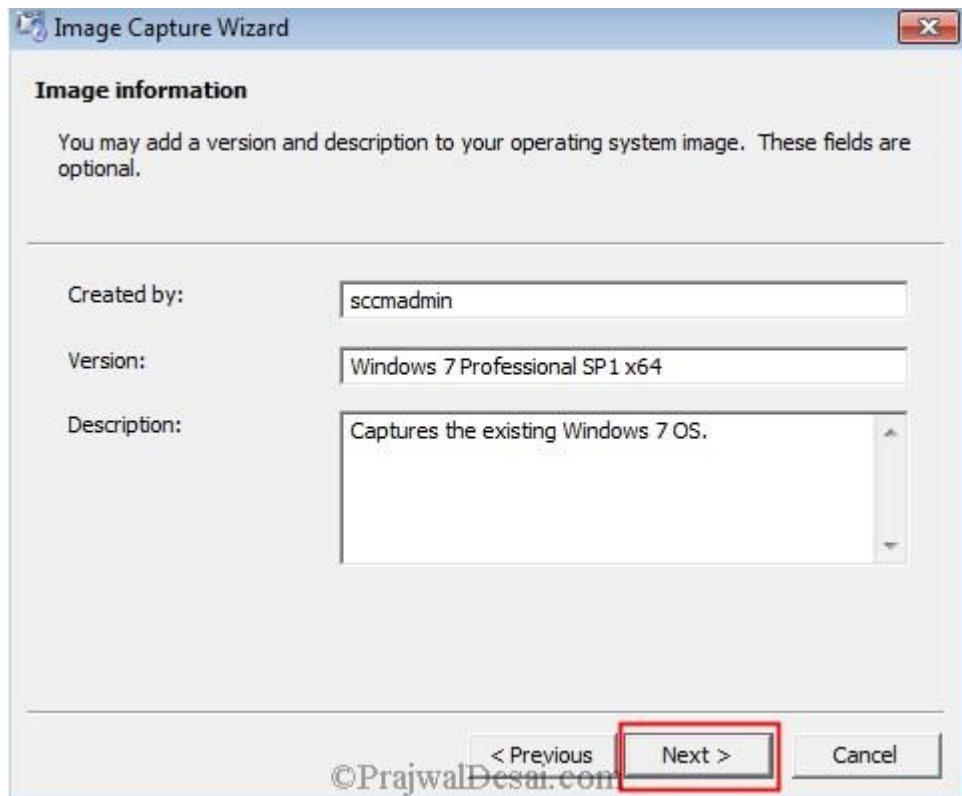
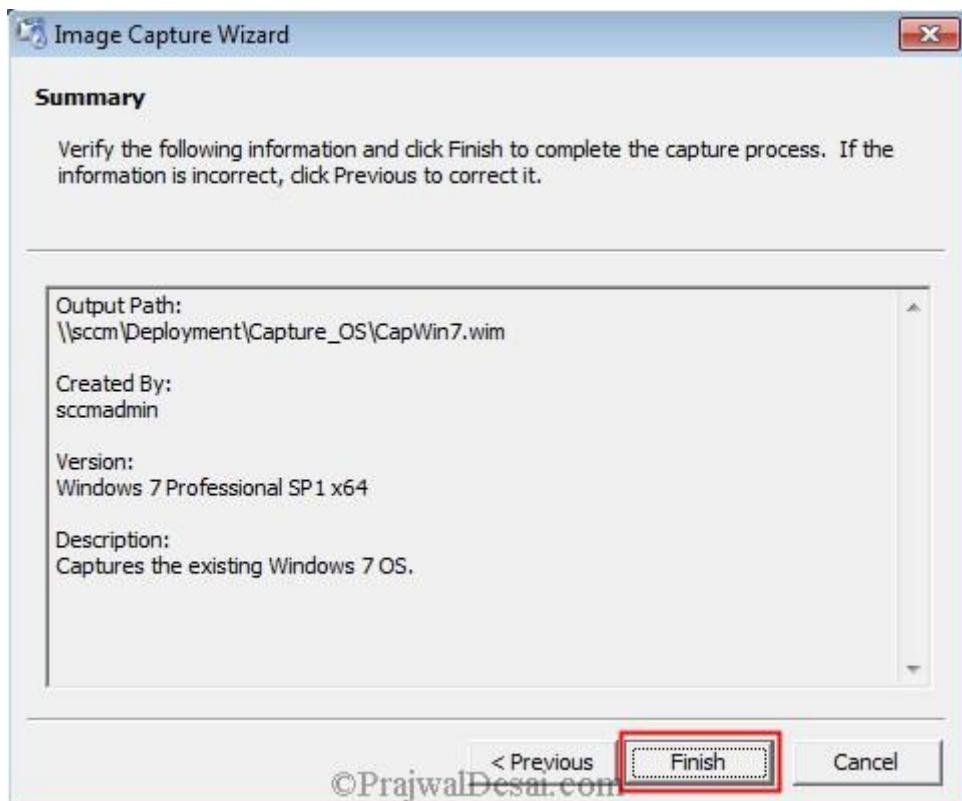


Image Information – Provide the image information such as **Created by, Version and Description**. Click on **Next**.



Click on **Finish** to complete the Image Capture Wizard. Note that we have just run the image capture wizard, in the next step **sysprep** captures the OS.



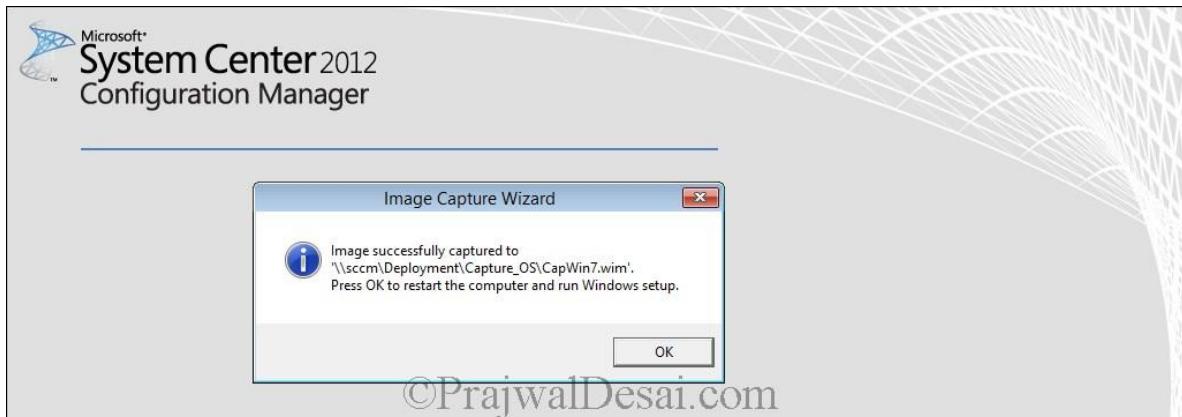
In the below screenshot we can see that the sysprep command is running. Wait for the computer to restart automatically where the actual capture process begins.



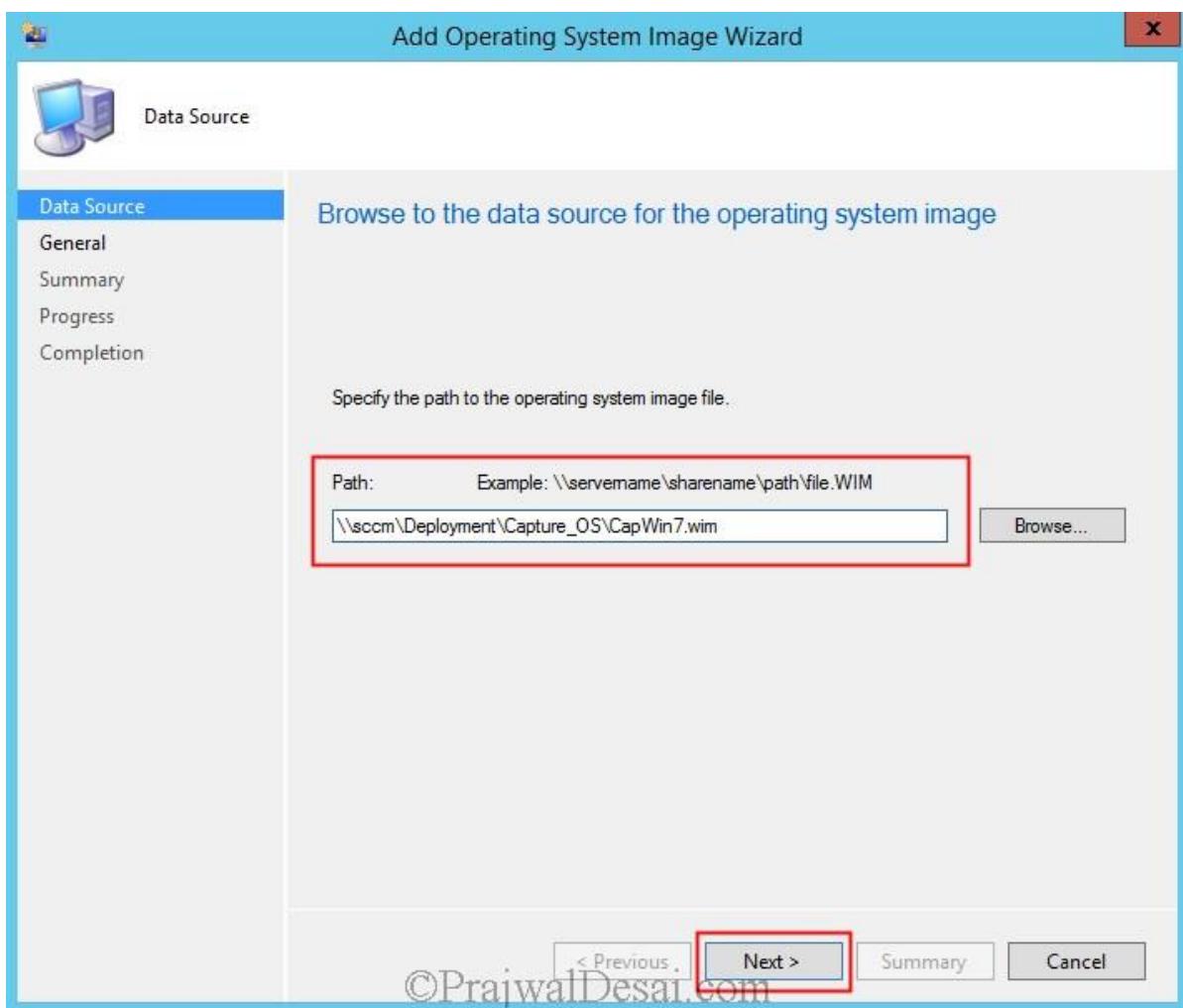
The computer restarts and we see that the wizard now starts capturing volume and the OS. This process took around 25 minutes to complete in my lab setup.



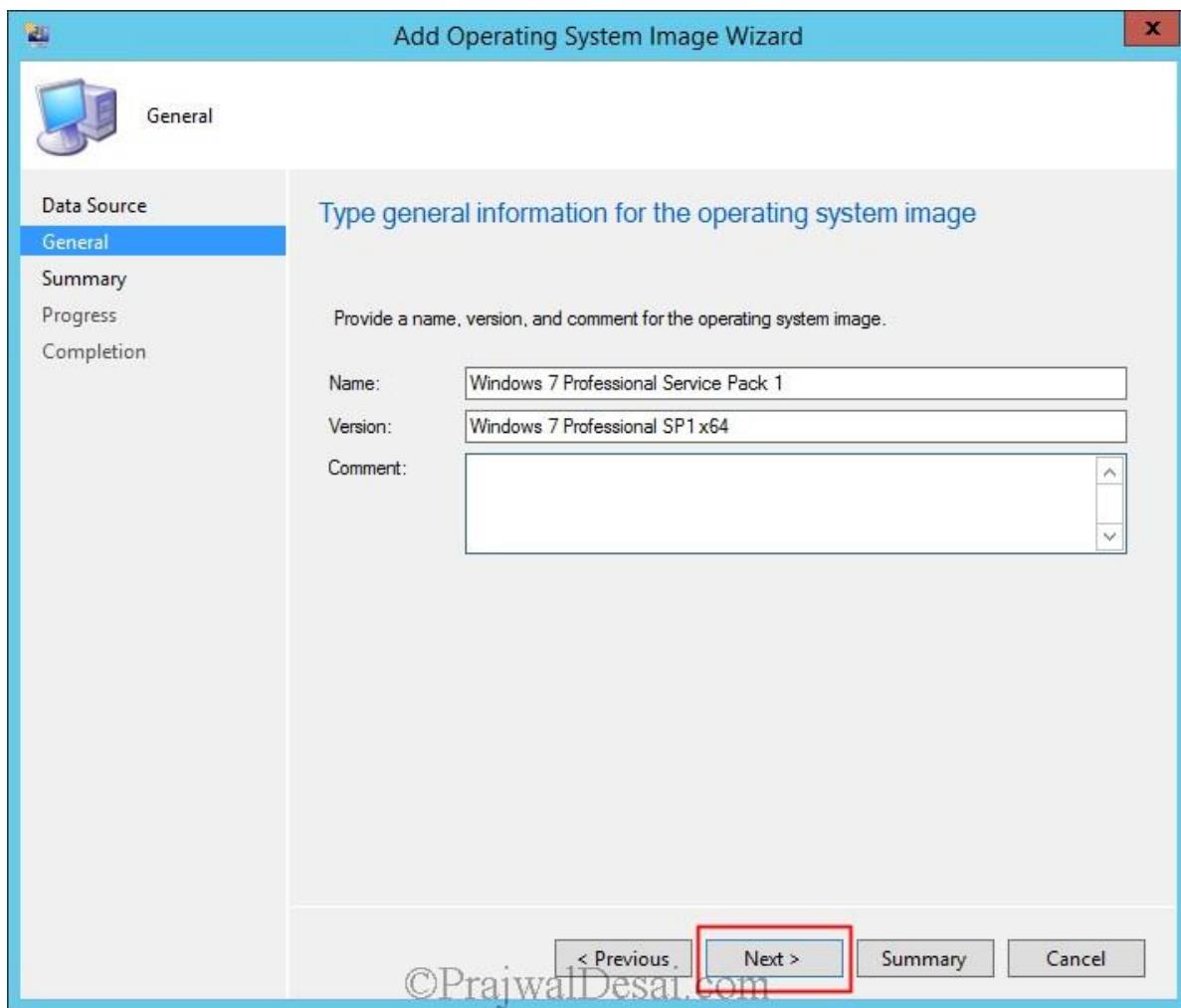
Alright, we now see that the windows 7 OS image has been captured and saved to the destination folder. Click on **OK**. The computer now restarts and enters Out of Box experience (**OOBE**).



Once we have got the .wim file, we can import the .wim as operating system image in SCCM 2012 R2. To import the operating system image, right click **Operating System Images**, click on Add **Operating System Image**. Enter the path where the captured .wim file is present. Click on **Next**.

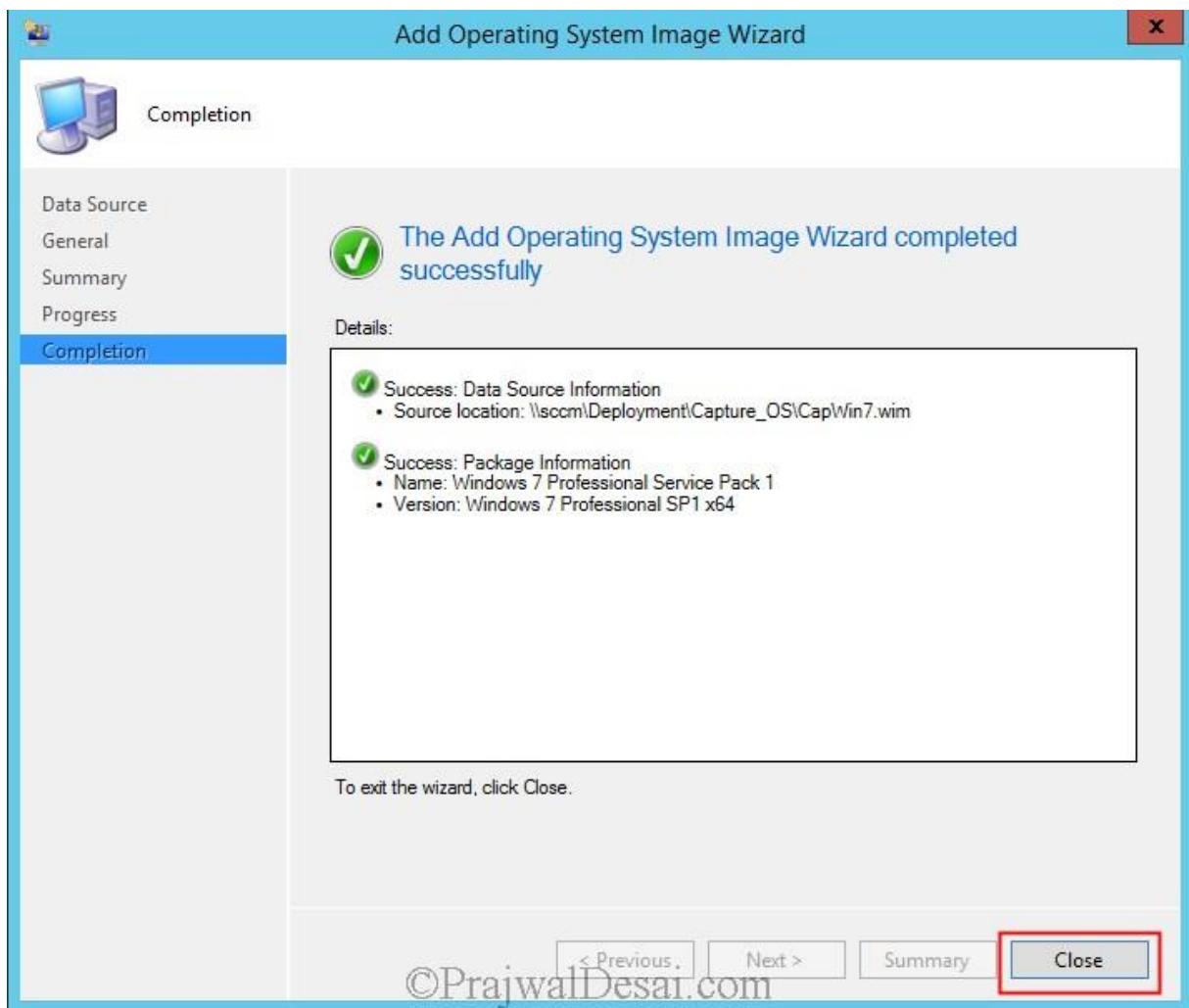


The name and version is picked up automatically, click on **Next**.

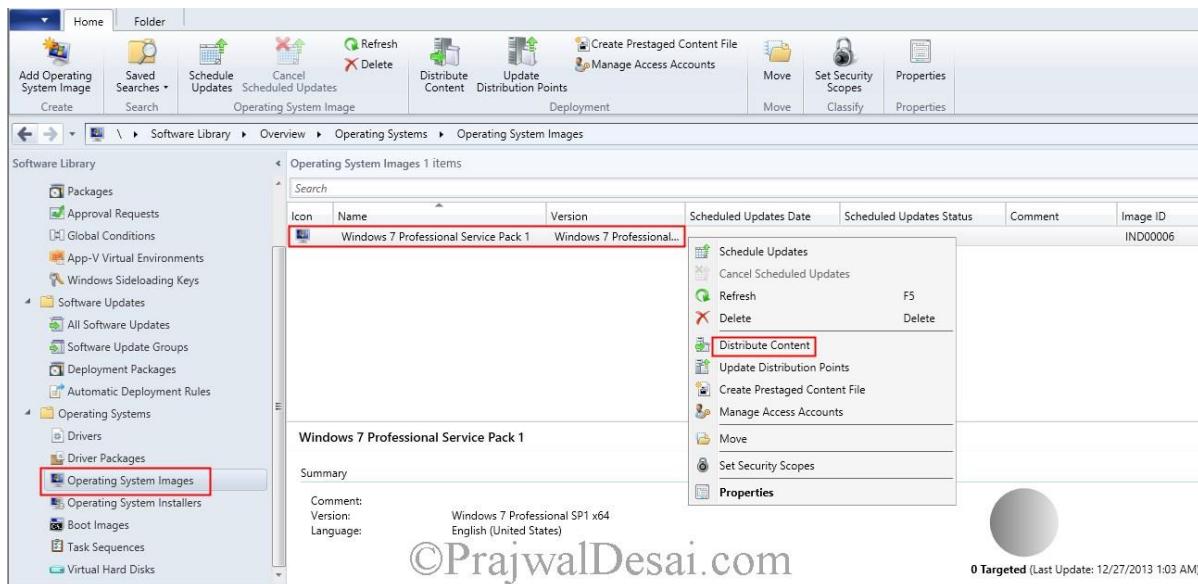


©PrajwalDesai.com

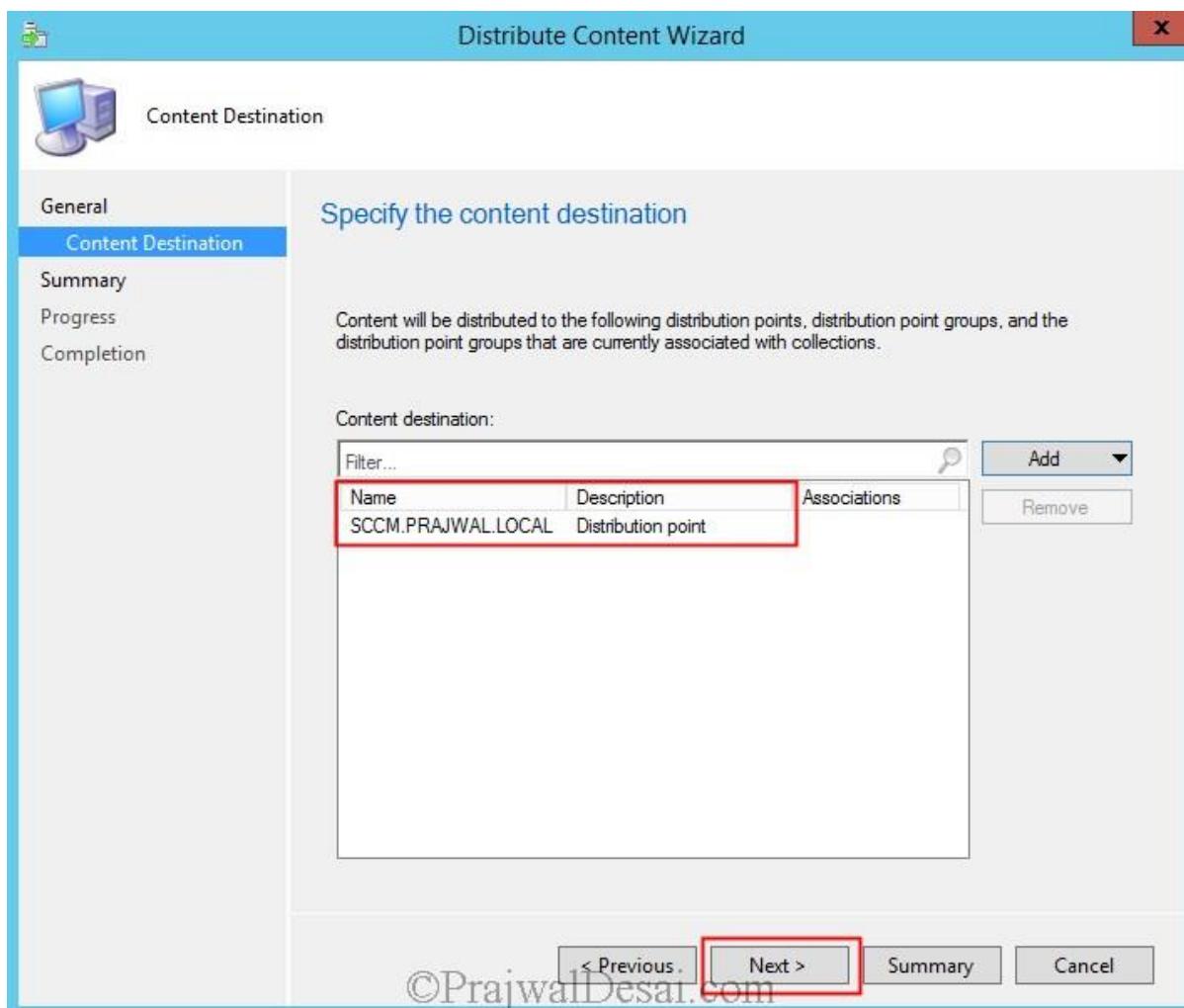
The operating system image has been imported successfully. Click on **Close**.



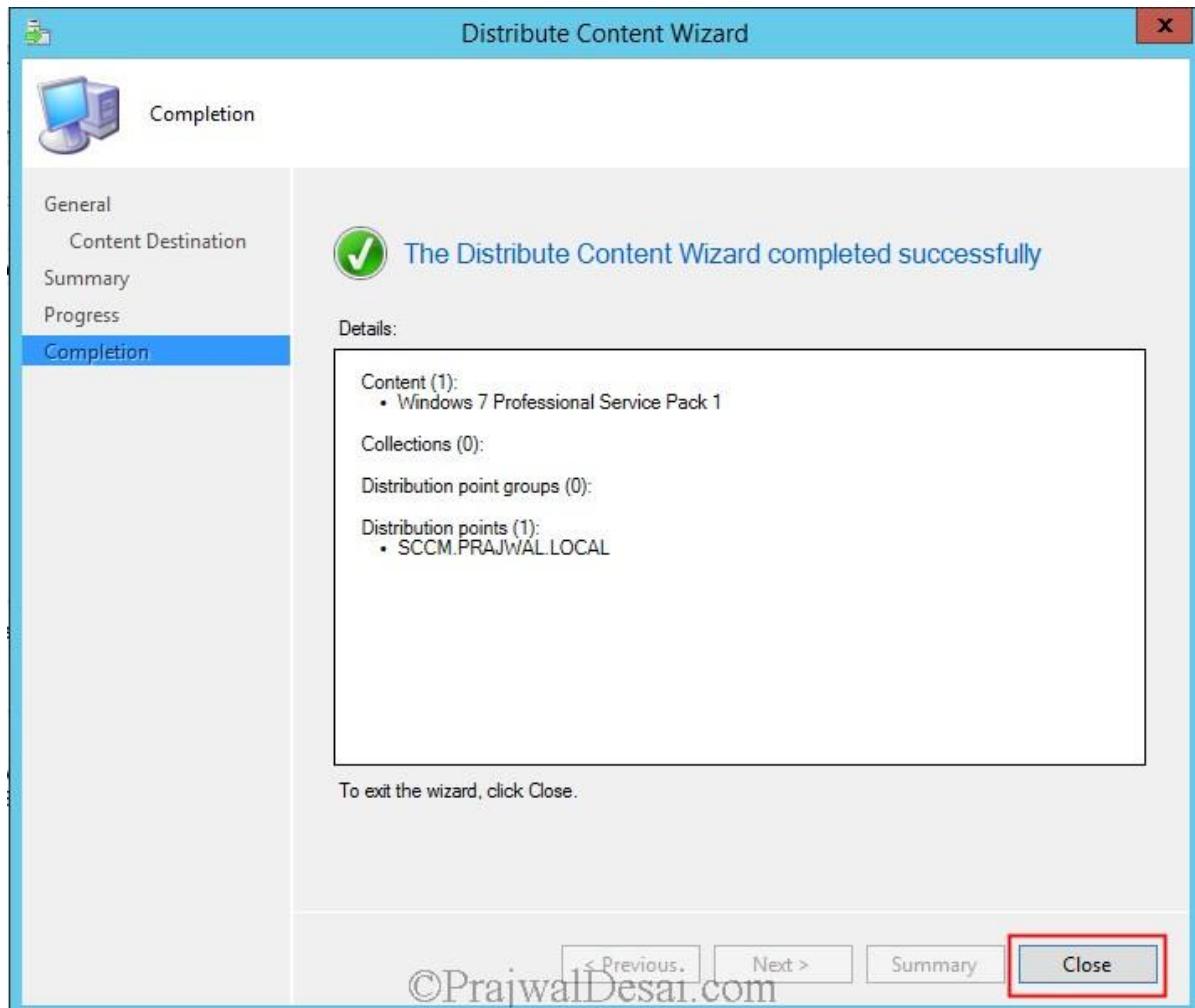
After importing the image the next step is to distribute the image to the DP. Right click on the windows 7 image and click on **Distribute Content**.



Add the DP and click **Next**.



The image file has been distributed to the DP. Click on **Close**. Wait for sometime while the DP updates the content, check the content status and you must see a green circle which means that content is now available with DP.

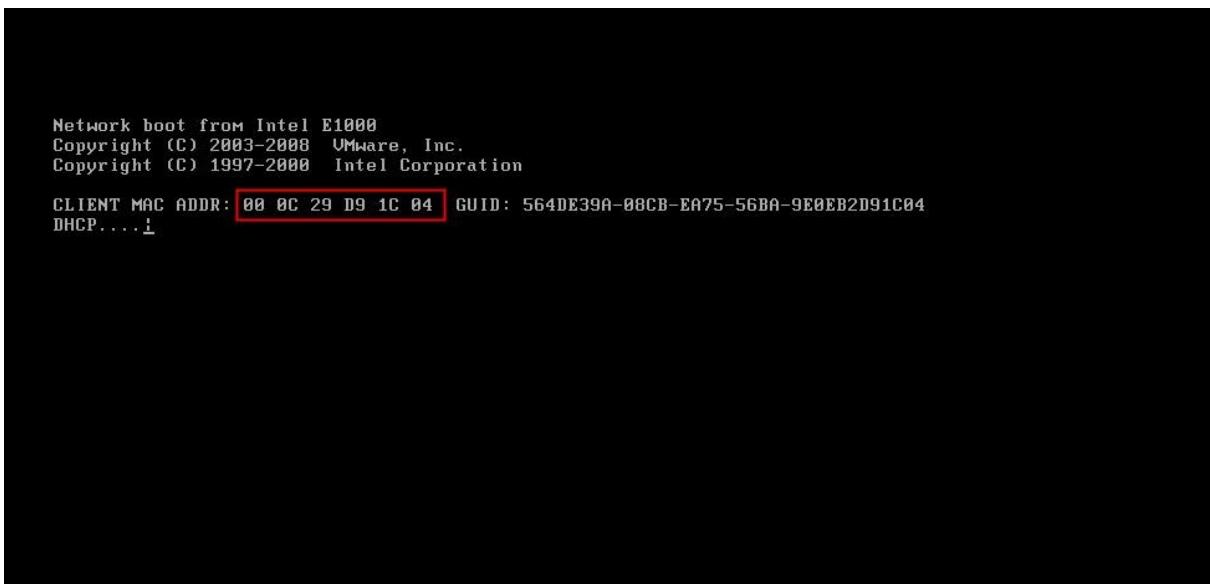


Deploying Windows 7 Using SCCM 2012 R2

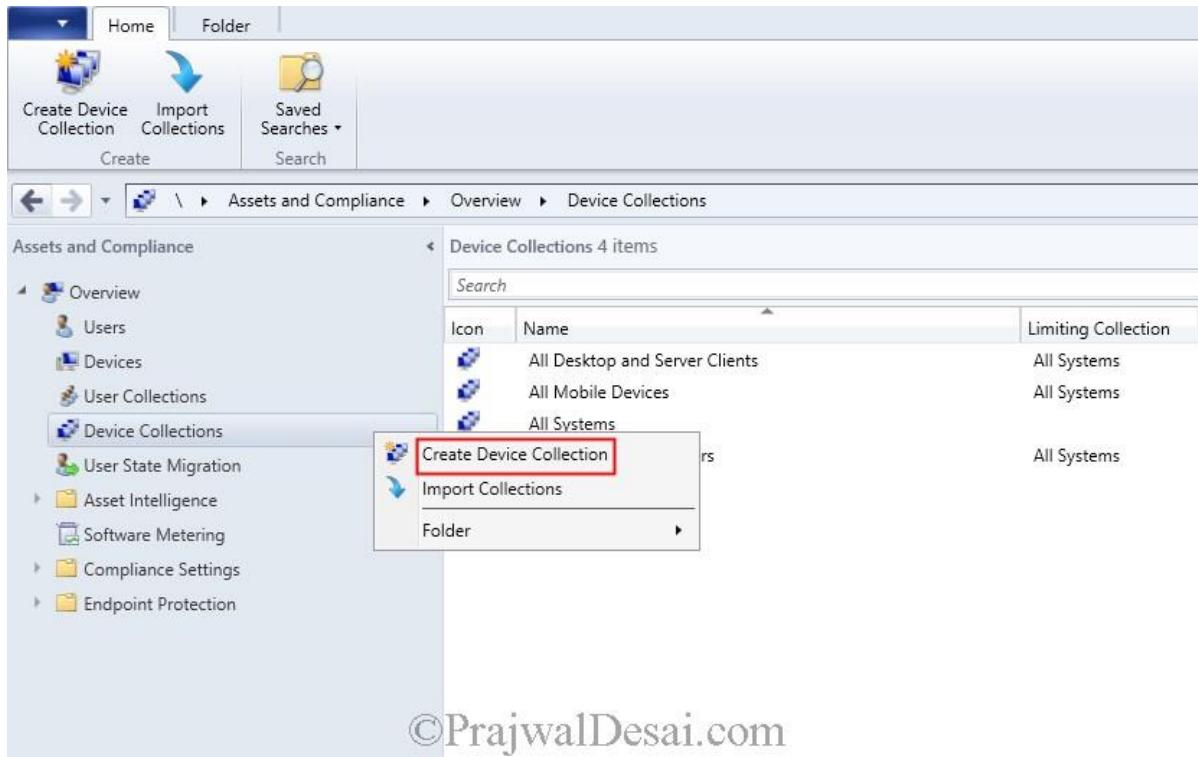
Deploying Windows 7 Using SCCM 2012 R2 n this post we will see the steps for deploying windows 7 using SCCM 2012 R2. In my previous post we saw the steps to [capture a reference operating system \(Windows 7\) using SCCM 2012 R2](#). Note that this post is different from the one which shows the steps to [build and capture the operating systems using SCCM 2012](#), we will not be using build and capture approach here rather we will capture a reference operating system, i.e. capture windows 7 using SCCM 2012 R2 and we will deploy the same using SCCM 2012 R2 in the this post. We will be creating a device collection first and then we will import the computer information to this device collection. Once the computer is added to the collection we will create task sequence, configure it and deploy it the device collection.

Deploying Windows 7 Using SCCM 2012 R2

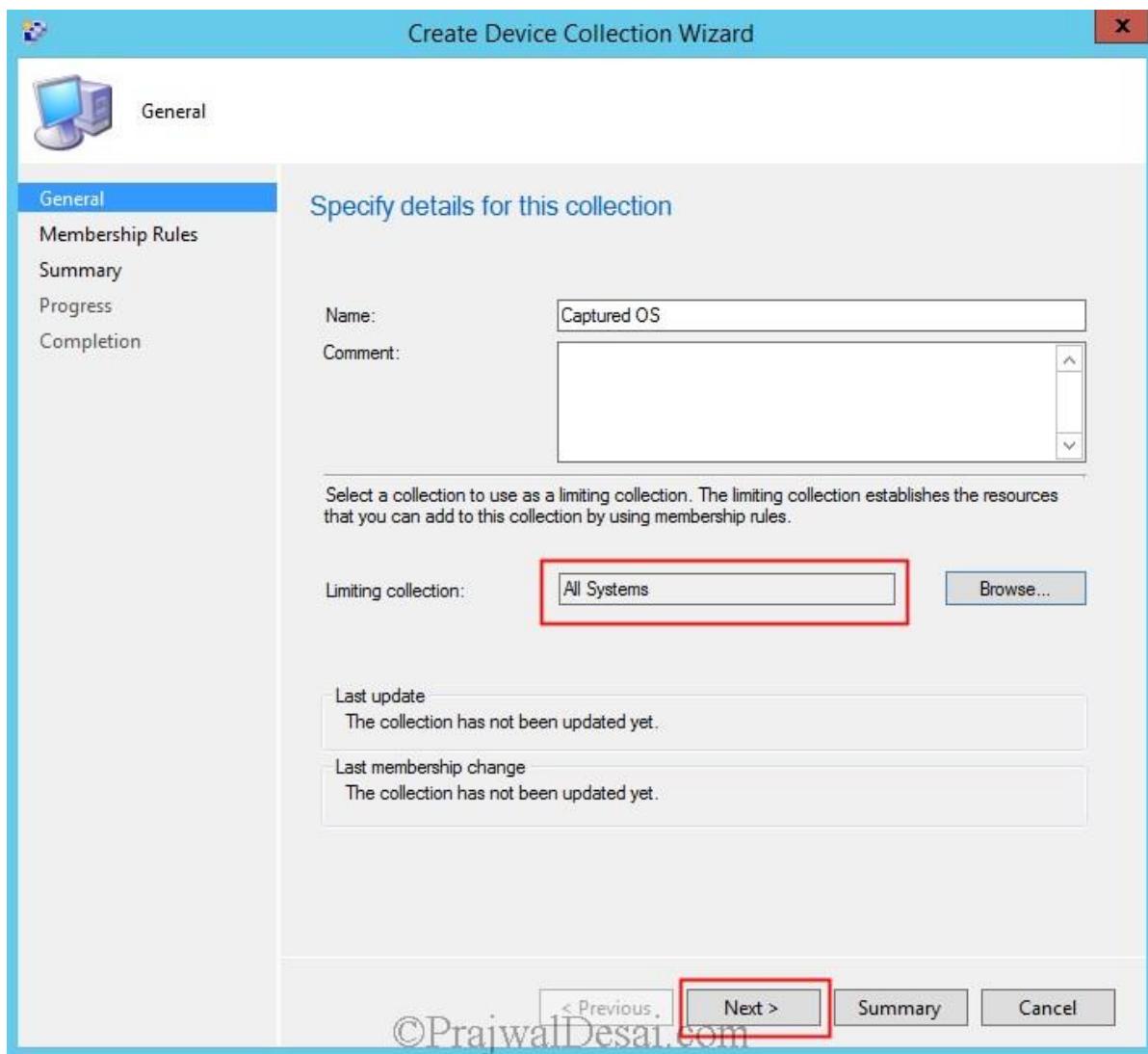
So in my previous post we had successfully captured the windows 7 operating system and now we will be deploying the captured image using SCCM 2012 R2. To do that lets create a blank virtual machine without any operating system installed on it. Note down the MAC address of the virtual machine (the same applies to a physical box too).



Lets create a new device collection. This is to add the computer to this collection for which the operating system is going to be deployed. Right click on **Device Collections**, click **Create Device Collection**.

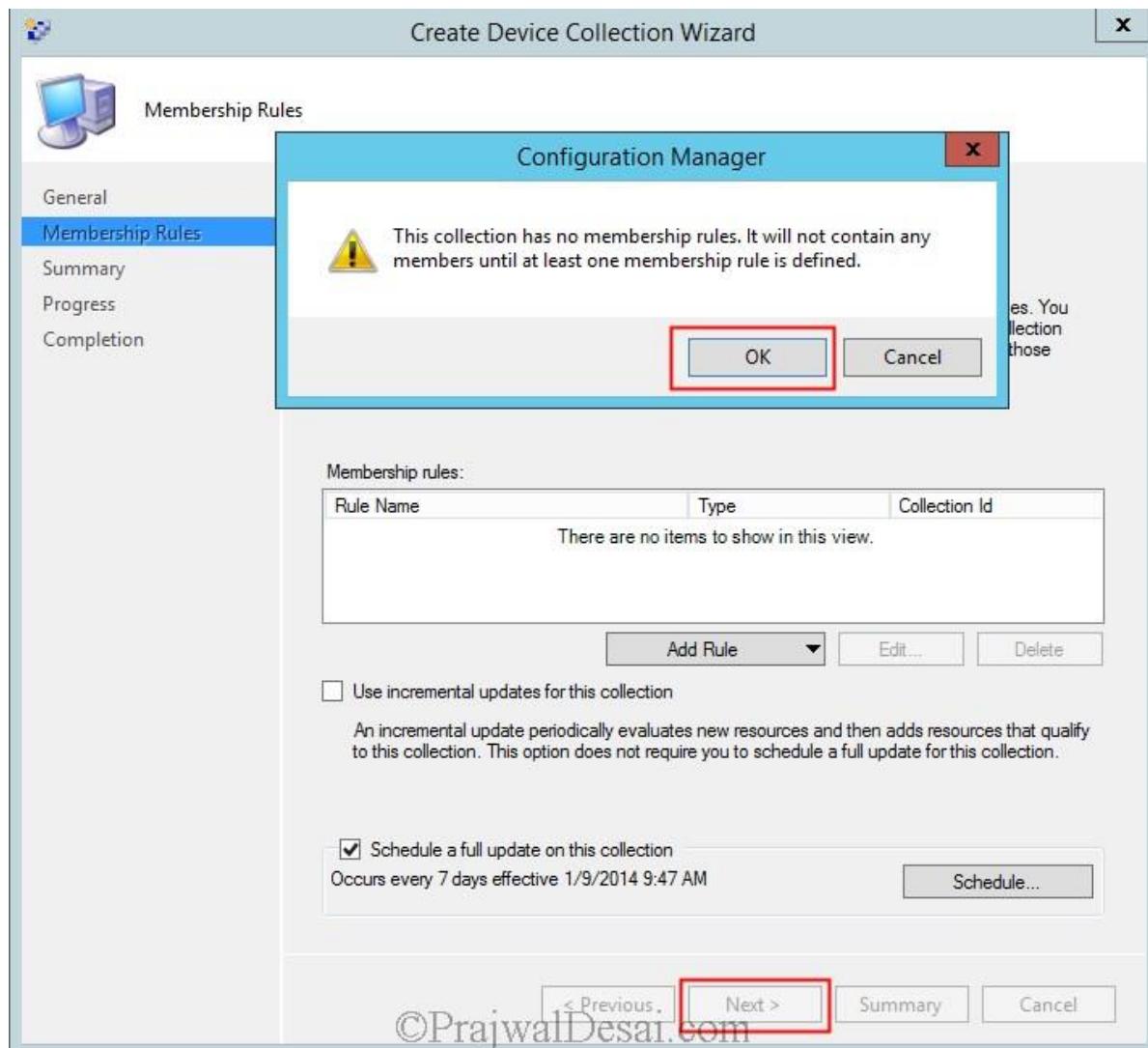


Provide the name for this **collection** , set the **Limiting collection** to **All Systems**. Click **Next**.



©PrajwallDesai.com

We will not define any rules for this collection. Click on **Next**. Since we will be creating a collection without defining any rule, the wizard prompts that the collection will not contain any members until we define a membership rule. On the pop up box click on **OK**.



©PrajwallDesai.com

The device collection has been created. Now we will import the computer information to add the new computer object to this collection. Click on **Devices**, click on **Import Computer Information**.

The screenshot shows the Configuration Manager console under the 'Assets and Compliance' category. In the left navigation pane, 'Devices' is selected. On the top ribbon, the 'Import Computer Information' button is highlighted with a red box. The main pane displays a table titled 'Devices 5 items' with columns for Icon, Name, Client, Site Code, and Client Activity. The data is as follows:

Icon	Name	Client	Site Code	Client Activity
AD	Yes	IND	Active	
SCCM	Yes	IND	Active	
WIN7	Yes	IND	Active	
x64 Unknown Computer...	No	IND		
x86 Unknown Computer...	No	IND		

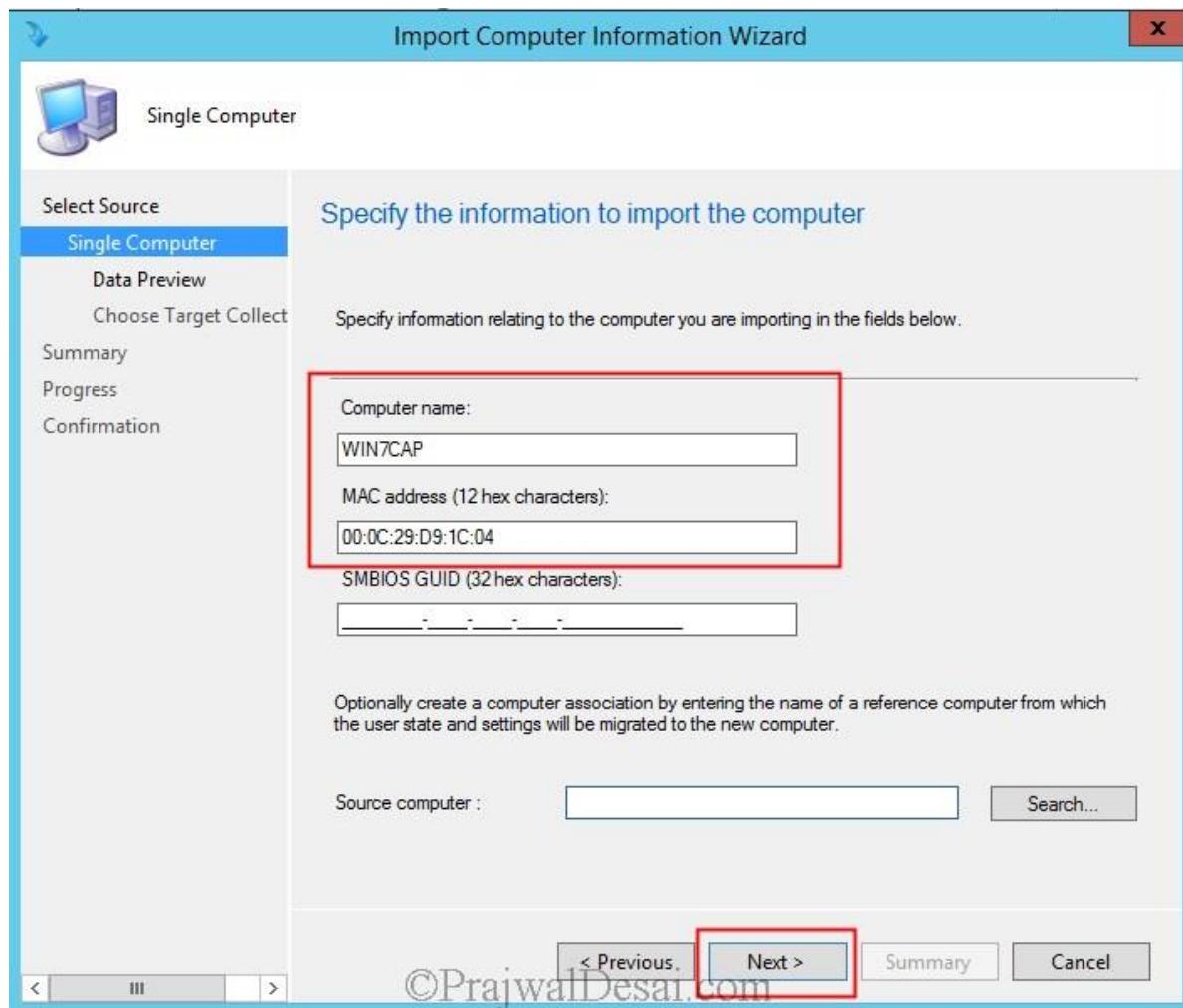
©PrajwalDesai.com

Choose **Import single computer** and click **Next**.

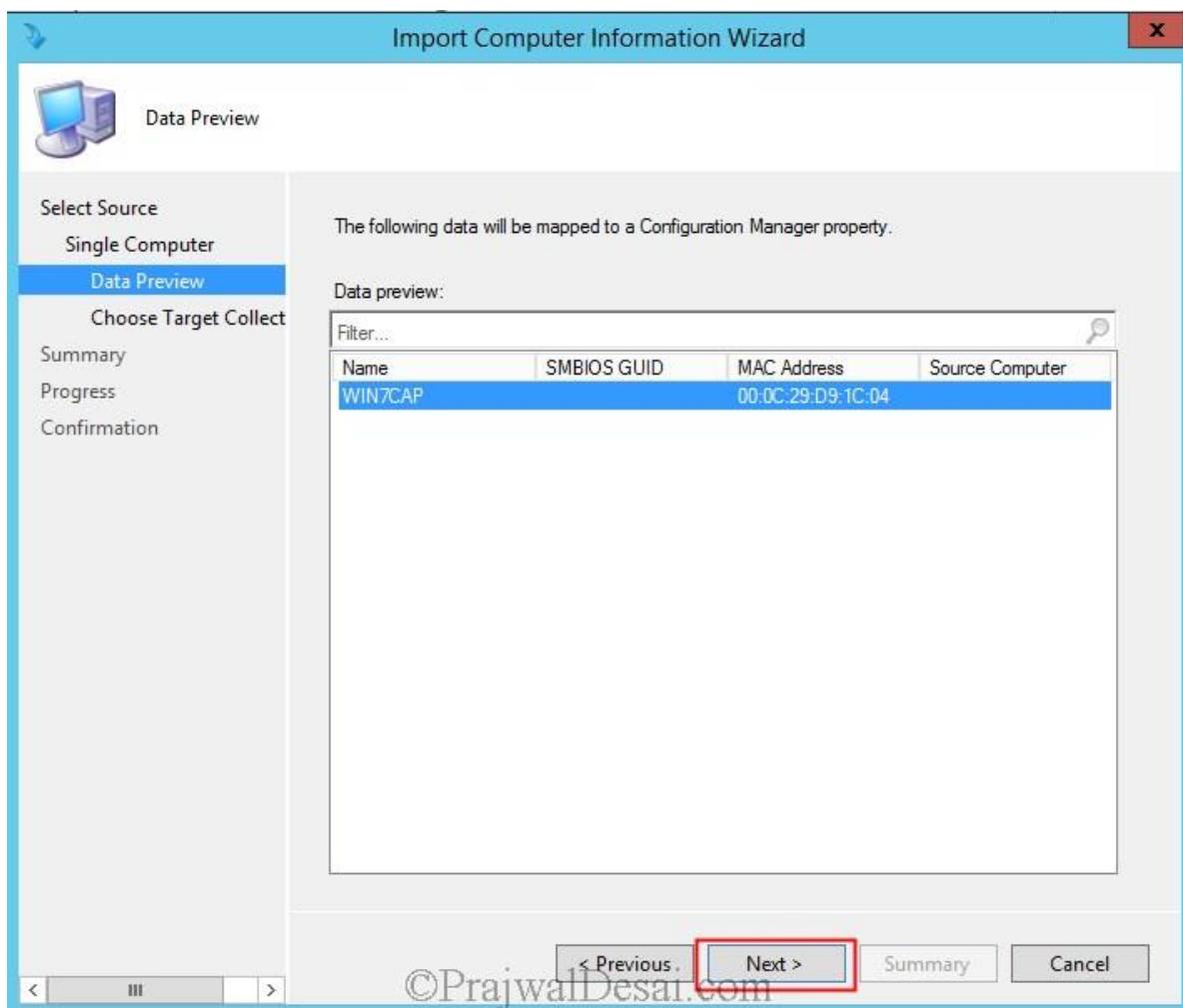
The screenshot shows the 'Import Computer Information Wizard' dialog box. The left sidebar shows steps: 'Select Source', 'Single Computer', 'Summary', 'Progress', and 'Confirmation'. The main panel is titled 'Select Computer Information Source' and contains the following text: 'This wizard imports new computer information into the Configuration Manager database. Select Import computers using a file to specify a file that contains the computer information to import. Select Import a single computer to specify information relating to that one computer.' Below this is a radio button group with two options: 'Import computers using a file' and 'Import single computer', with the latter being selected and highlighted with a red box. At the bottom are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

©PrajwalDesai.com

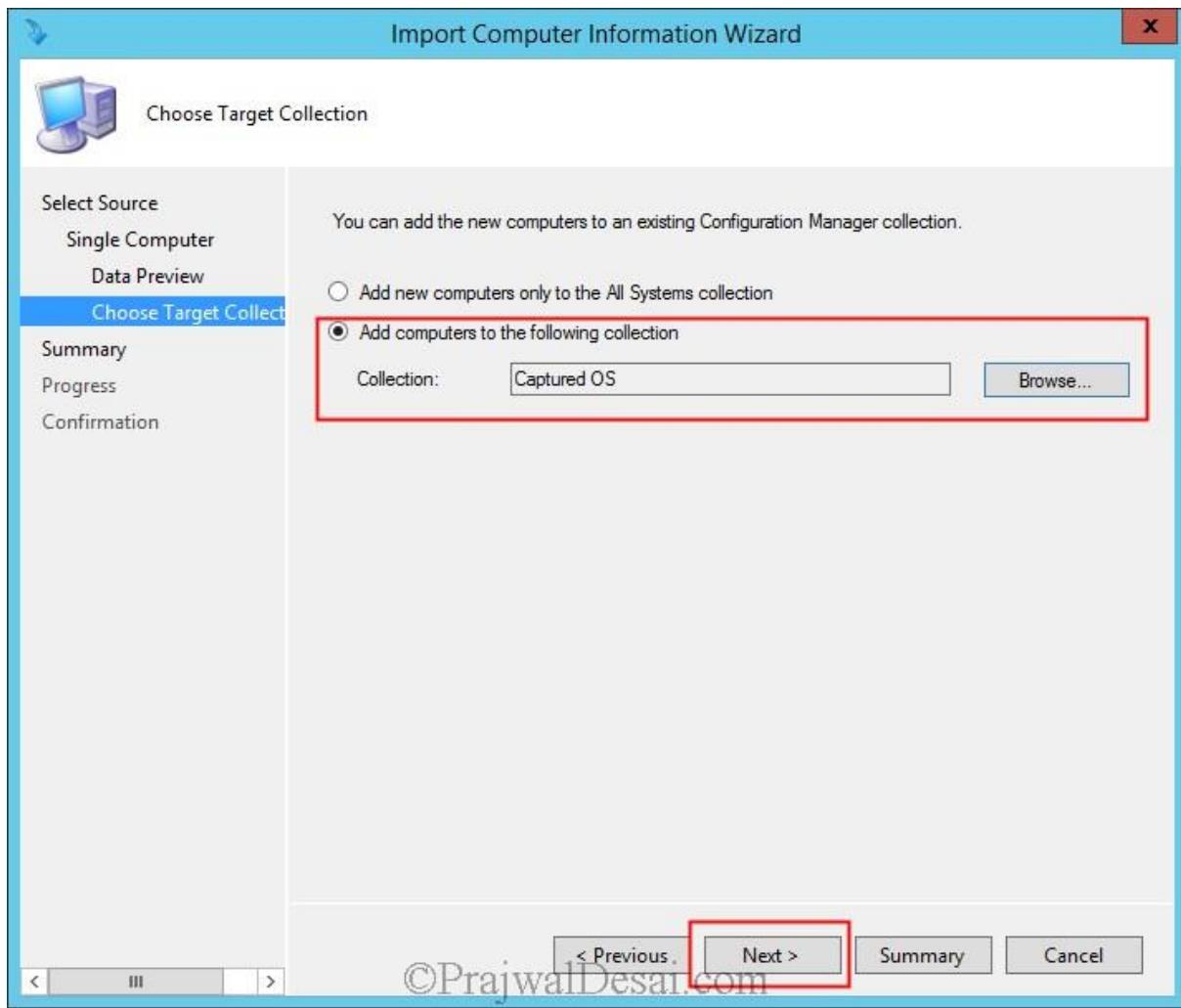
Specify the **Computer name**, **MAC Address** of the computer (MAC address of the computer where the OS is going to be deployed) and click **Next**.



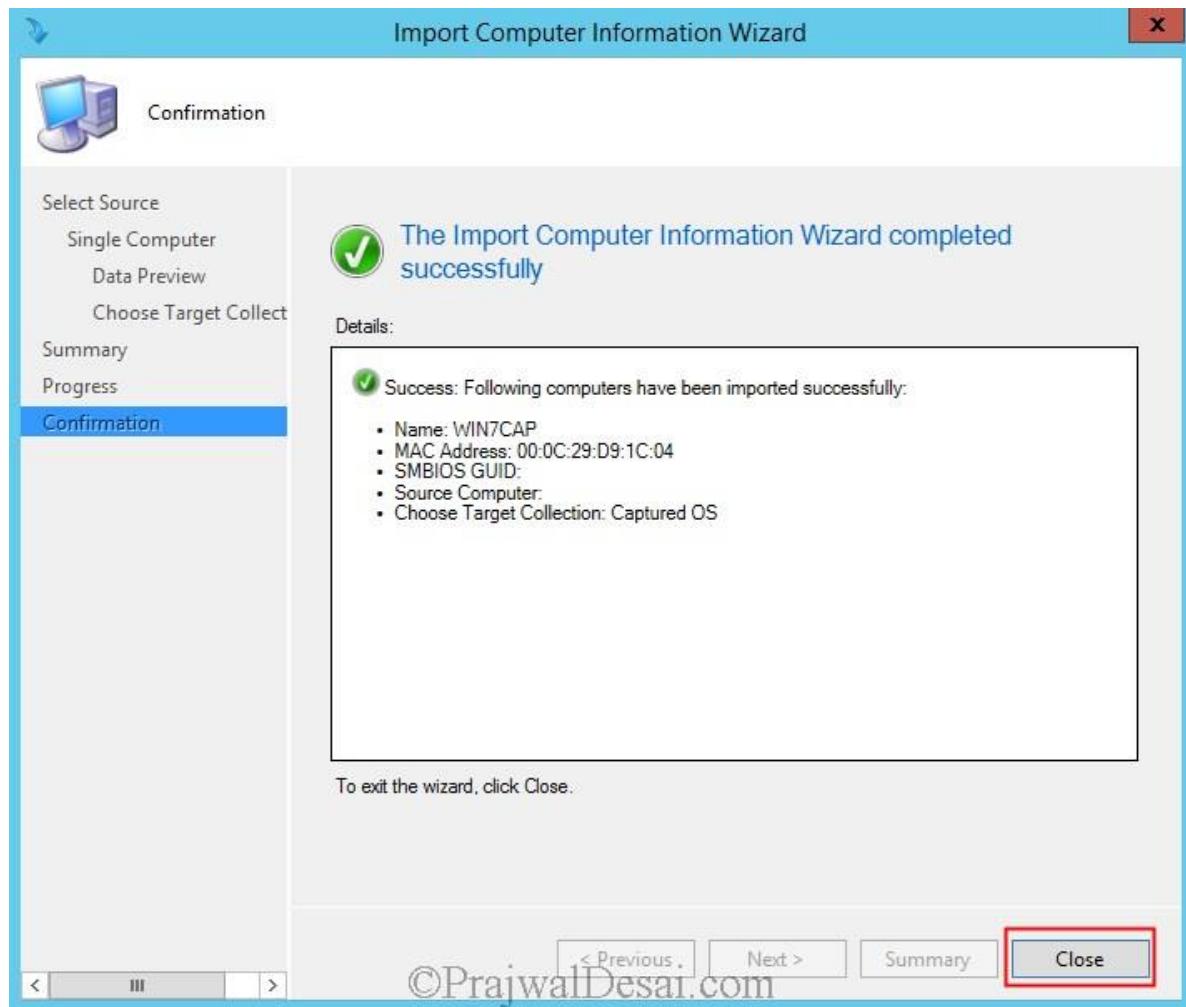
Click Next.



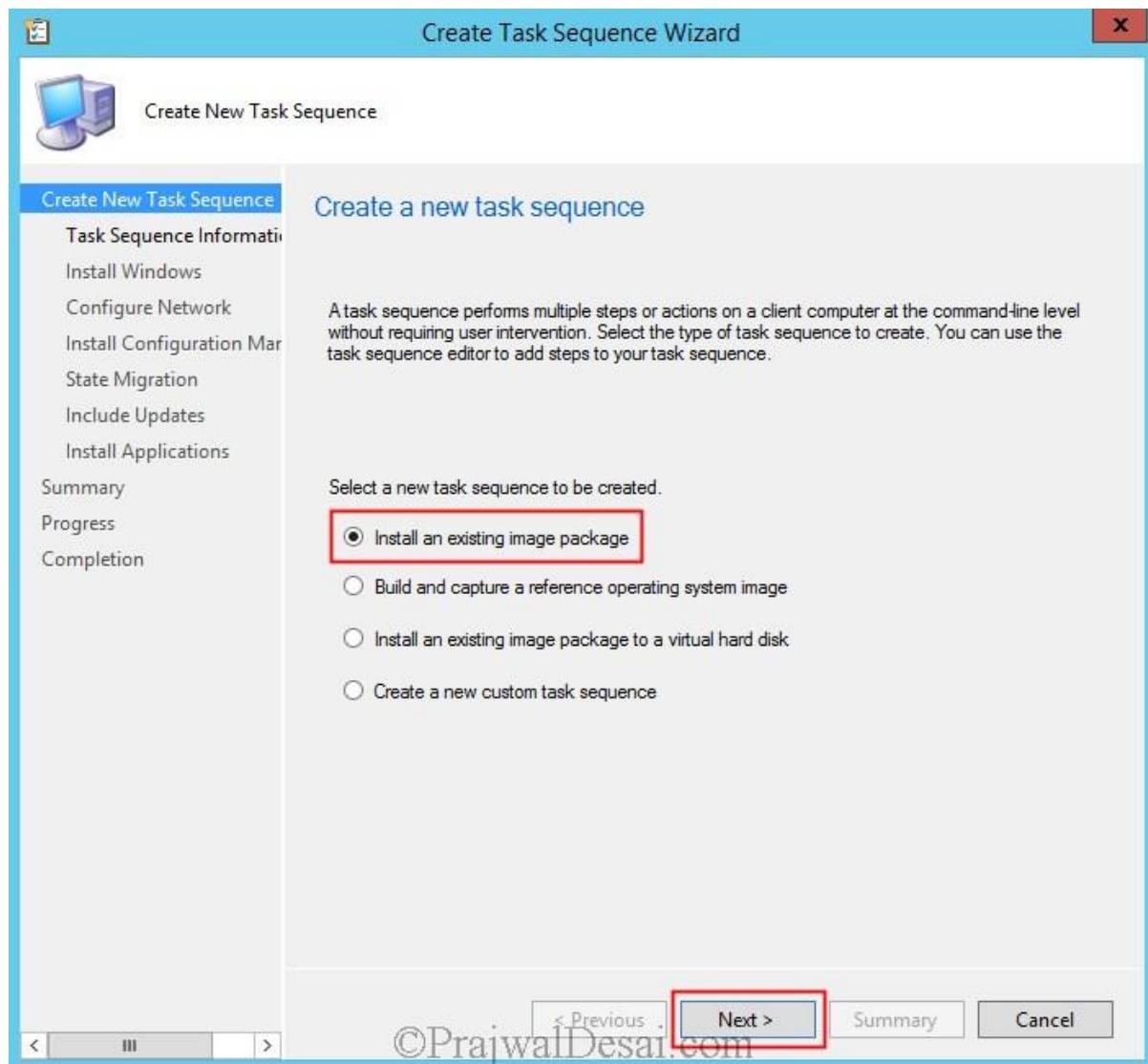
Choose **Add computers to the following collection**, click on **Browse** and choose the new device collection that we created. Click **Next**.



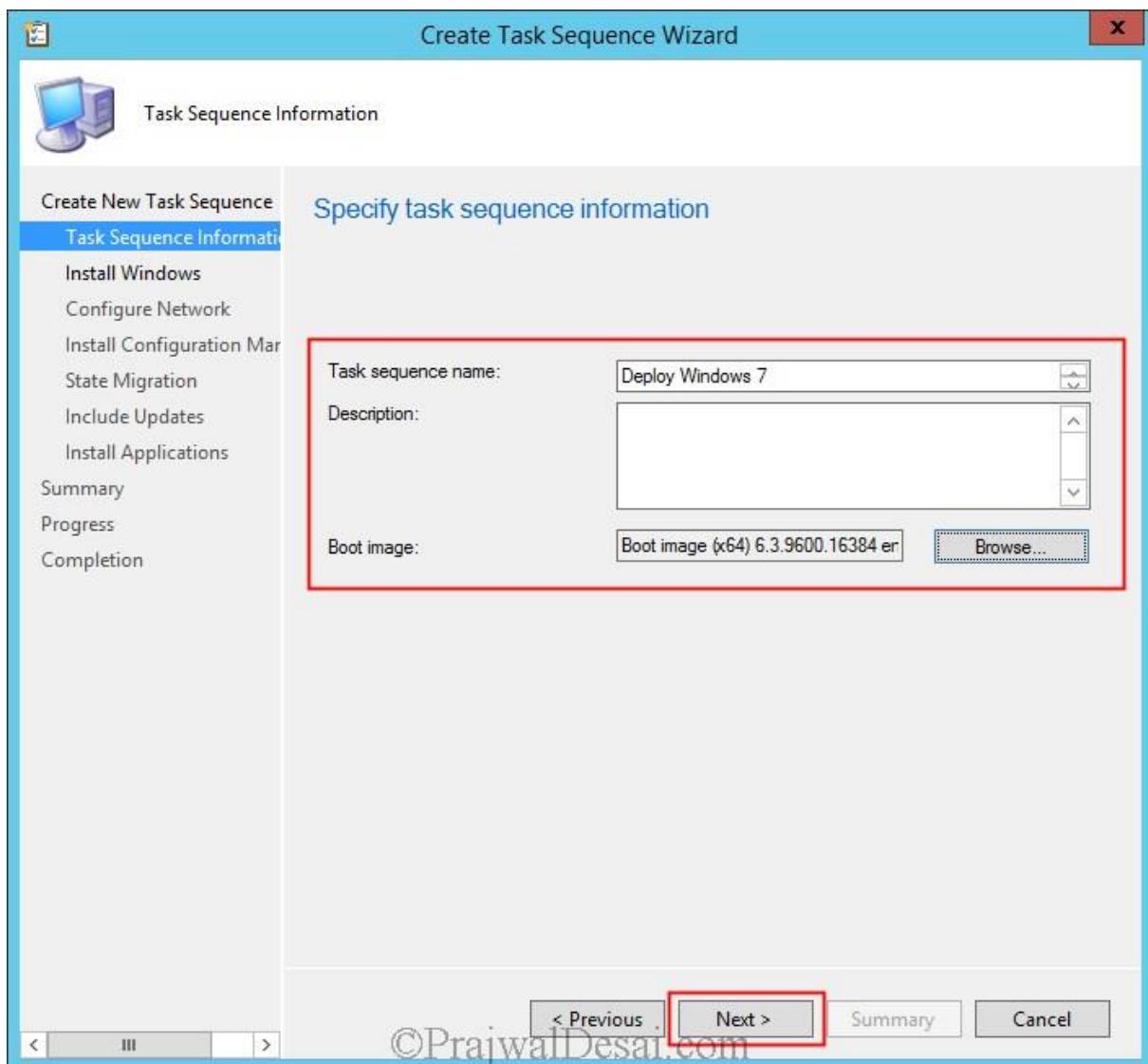
Once the computer information is imported, click on **Close**. The process of importing this new computer to a new device collection will take few minutes.



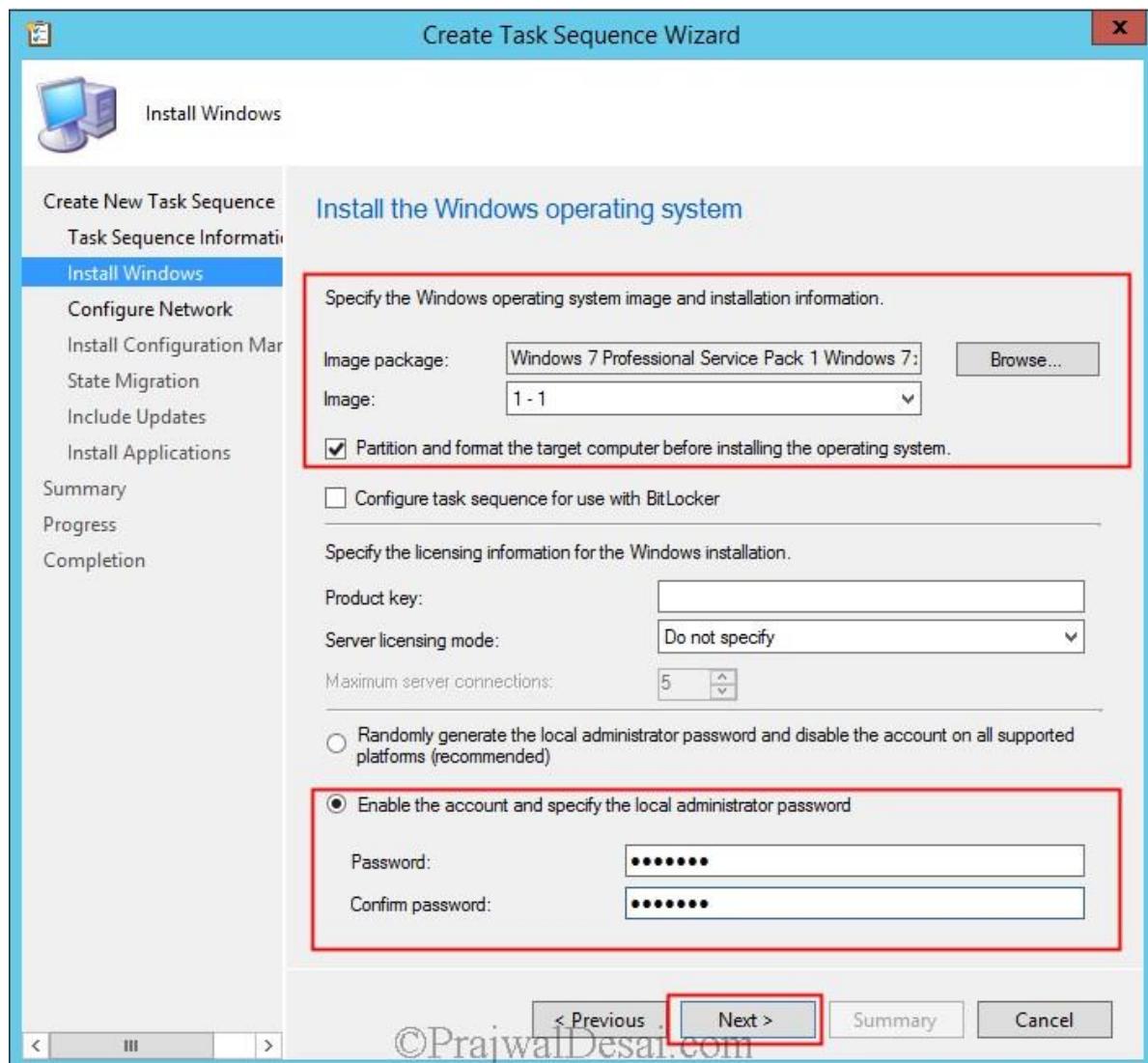
After we create a device collection and import the computer information, the next step is to deploy the captured operating system. Right **Task Sequences** and click **Create Task Sequence**. Choose **Install an existing image package**. Click **Next**.



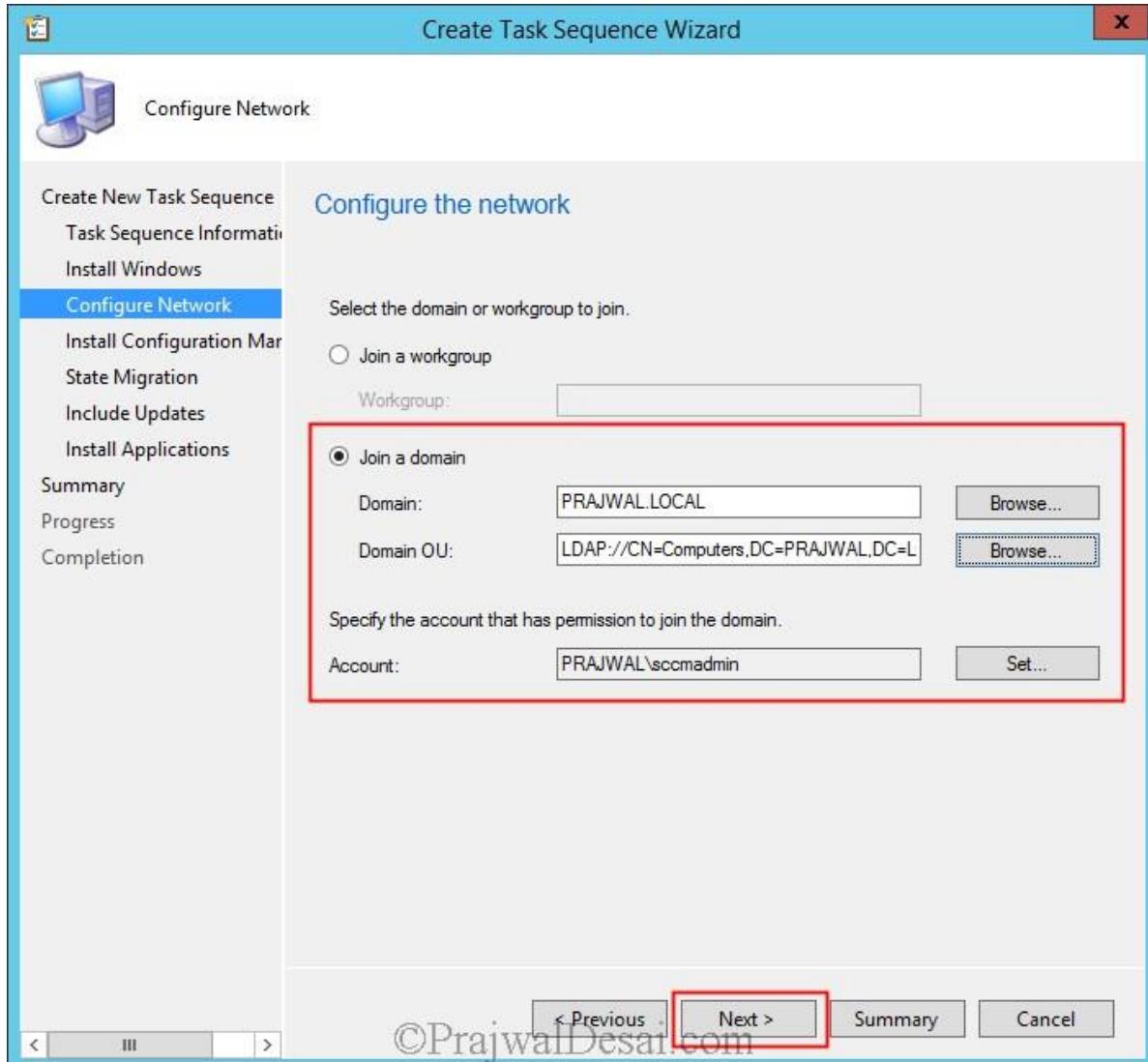
Provide the **Task sequence name**, click on **Browse** and specify the **Boot Image**. Click **Next**.



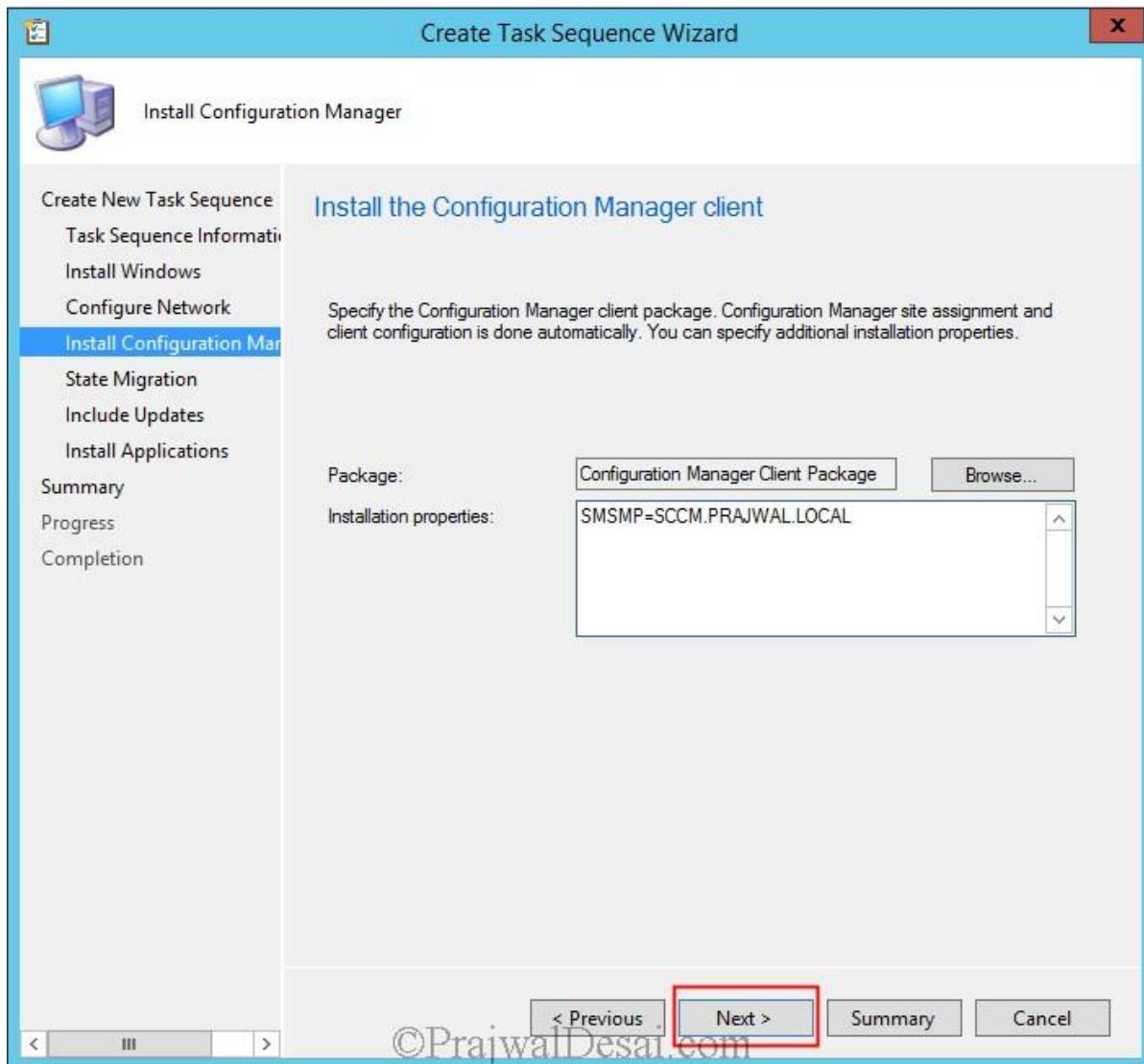
Click on **Browse** and specify the **Image Package**. Choose **Enable the local admin account** and set the desired password. Click **Next**.



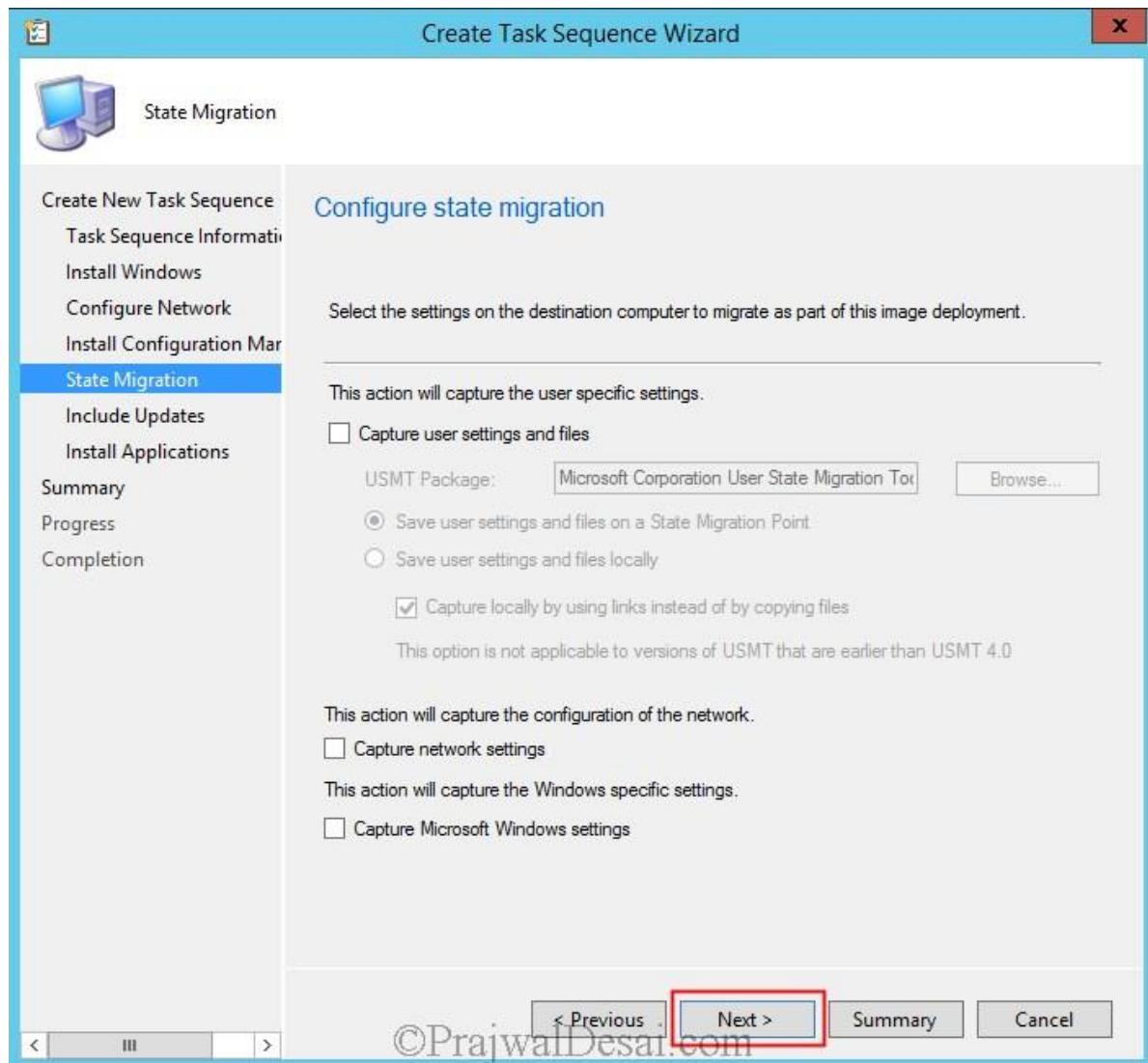
You can choose to add this computer to the domain or join a workgroup. In this example we will choose the computer to **Join a domain**, click on **Browse** and select **Domain, Domain OU** and specify an account that has permissions to join the computer to the domain. In this example we will be using an user account named **sccmadmin** which is a member of Domain Admins group. Click **Next**.



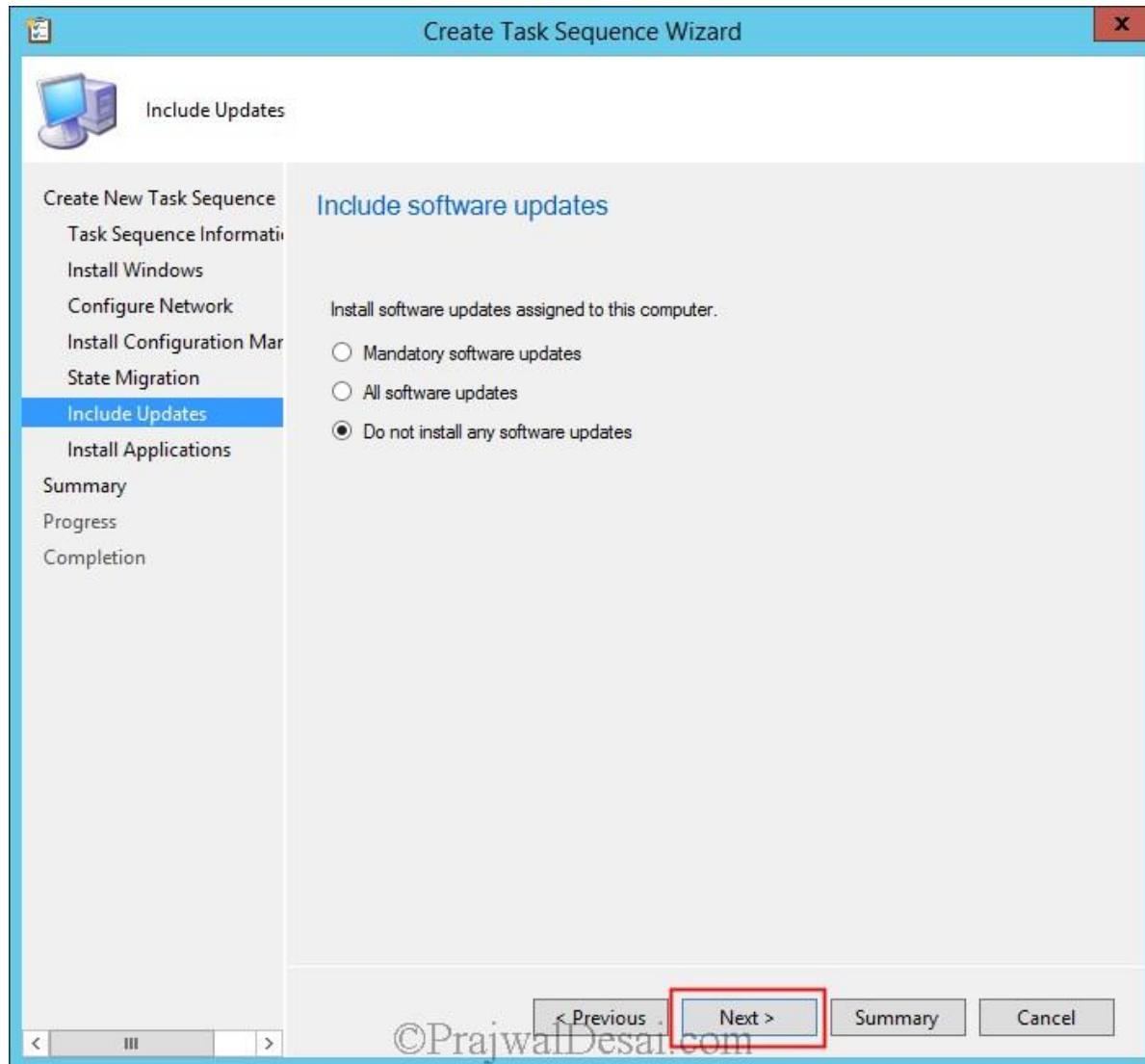
The Configuration manager client package is automatically selected, you can specify additional information in Installation properties such as Management Point, Fallback status point etc. Click on **Next**.



We will not configure **Configuration state migration** in this post so uncheck all the checkboxes and click on **Next**.

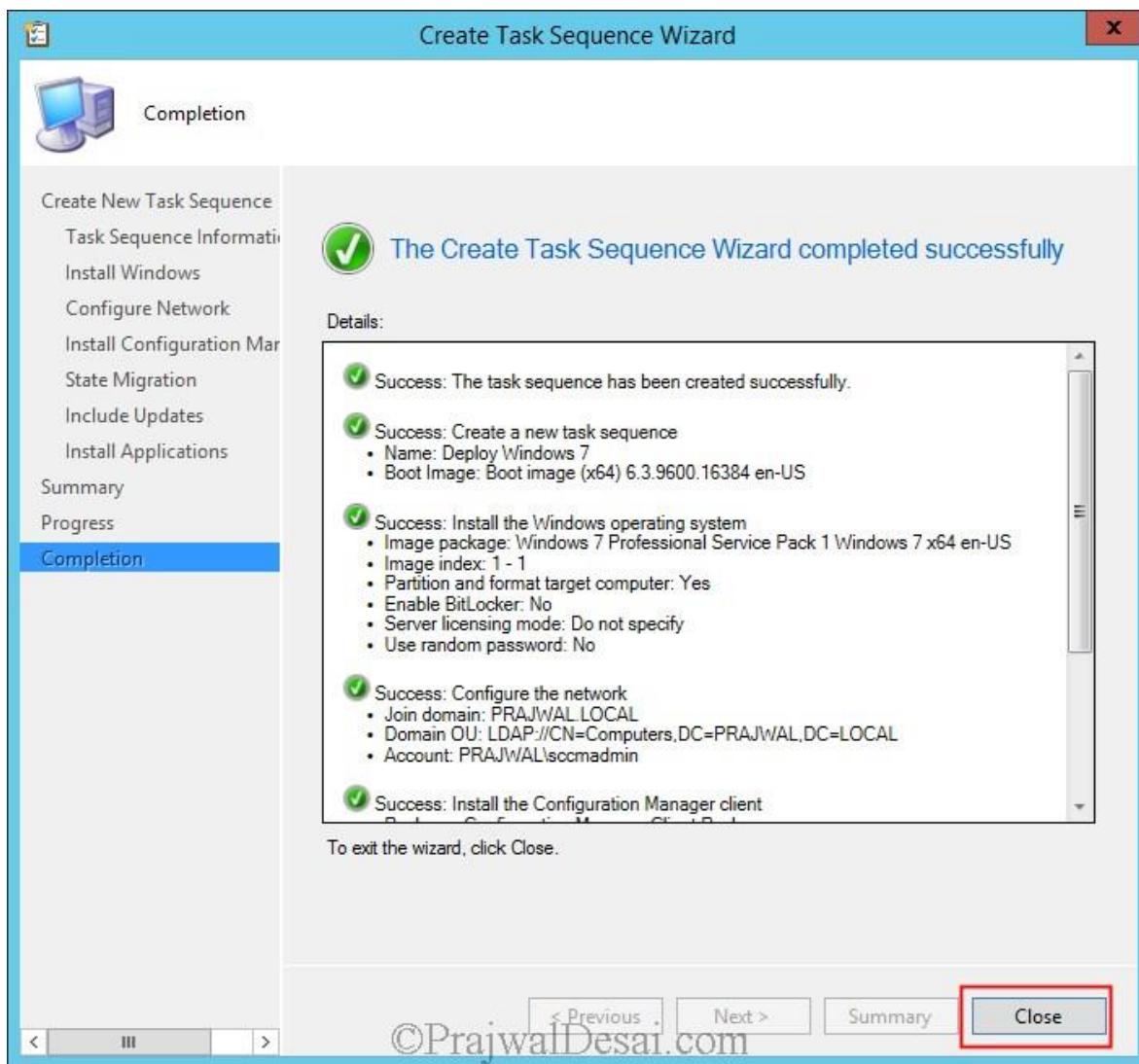


You can choose to include the windows updates which will be installed after the OS deployment. We will see the deployment of software updates in a different post, choose **Do not install any software updates**. Click **Next**.

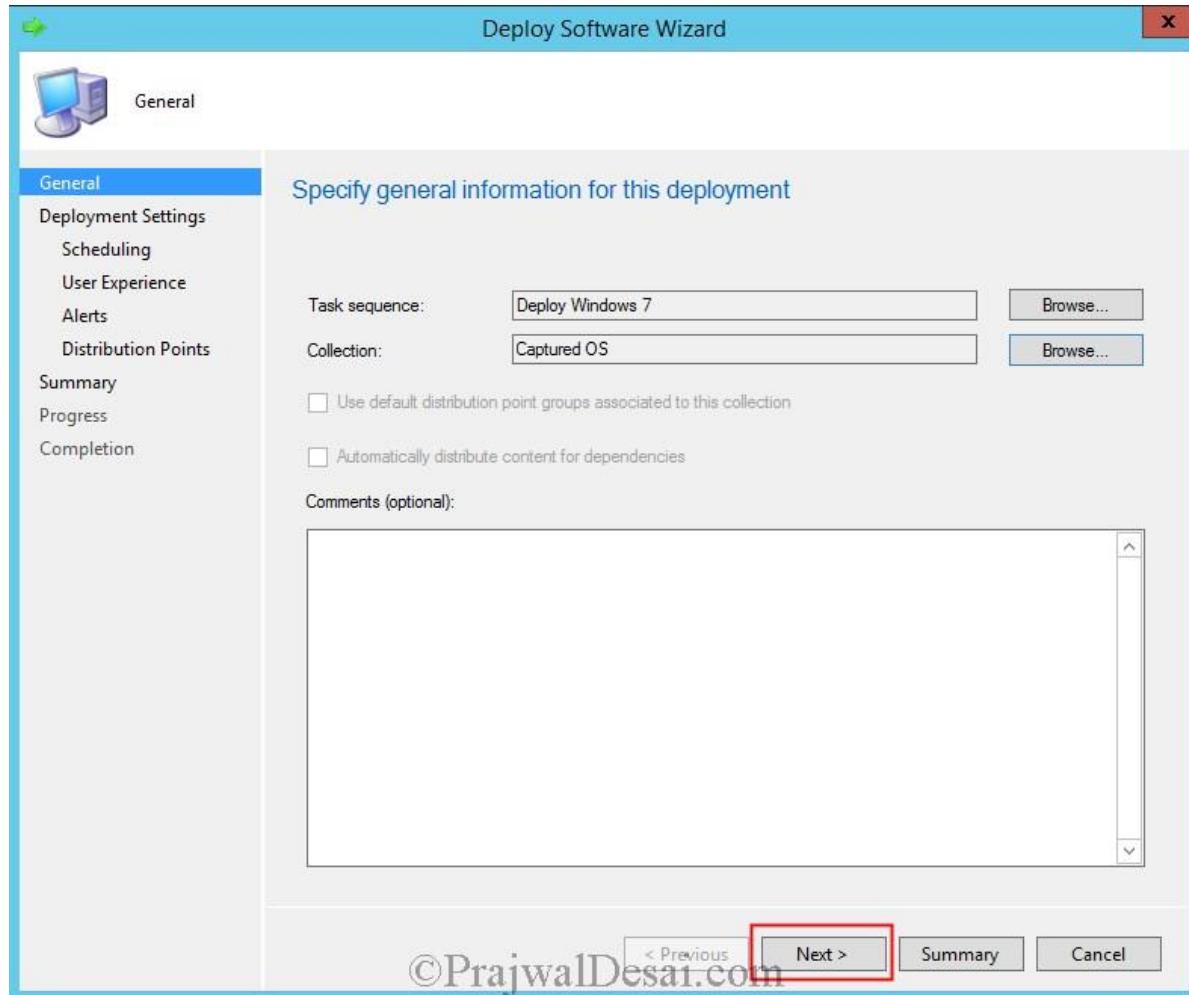


©PrajwallDesai.com

Click **Close**.

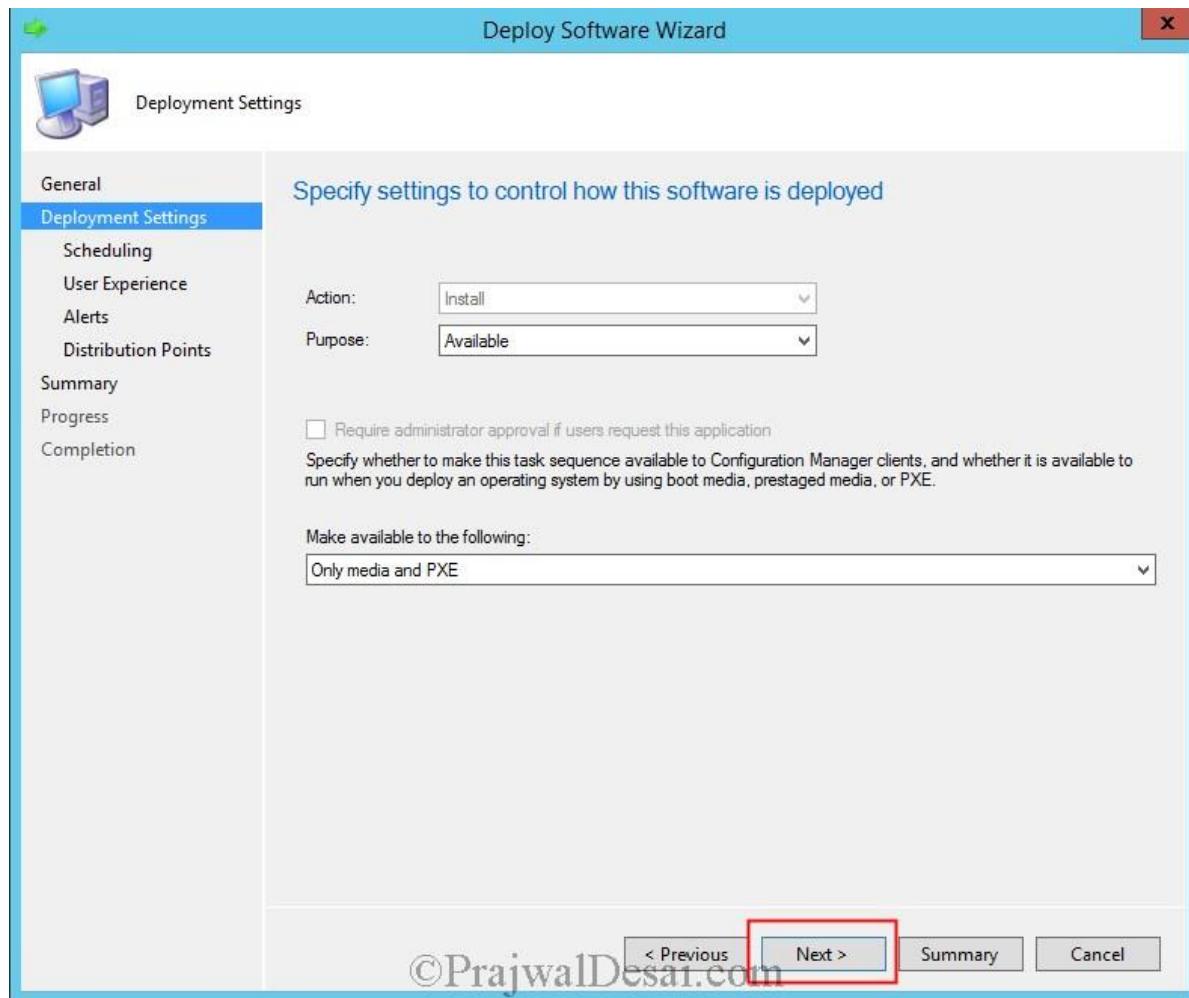


Once the task sequence is created the next step is to deploy it to the device collection. Click on **Task Sequences**, right click the task sequence that you have created for deploying OS and click on **Deploy**. In the Deploy Software Wizard, click on **Browse** and choose the **task sequence** and **Collection**. Click **Next**.



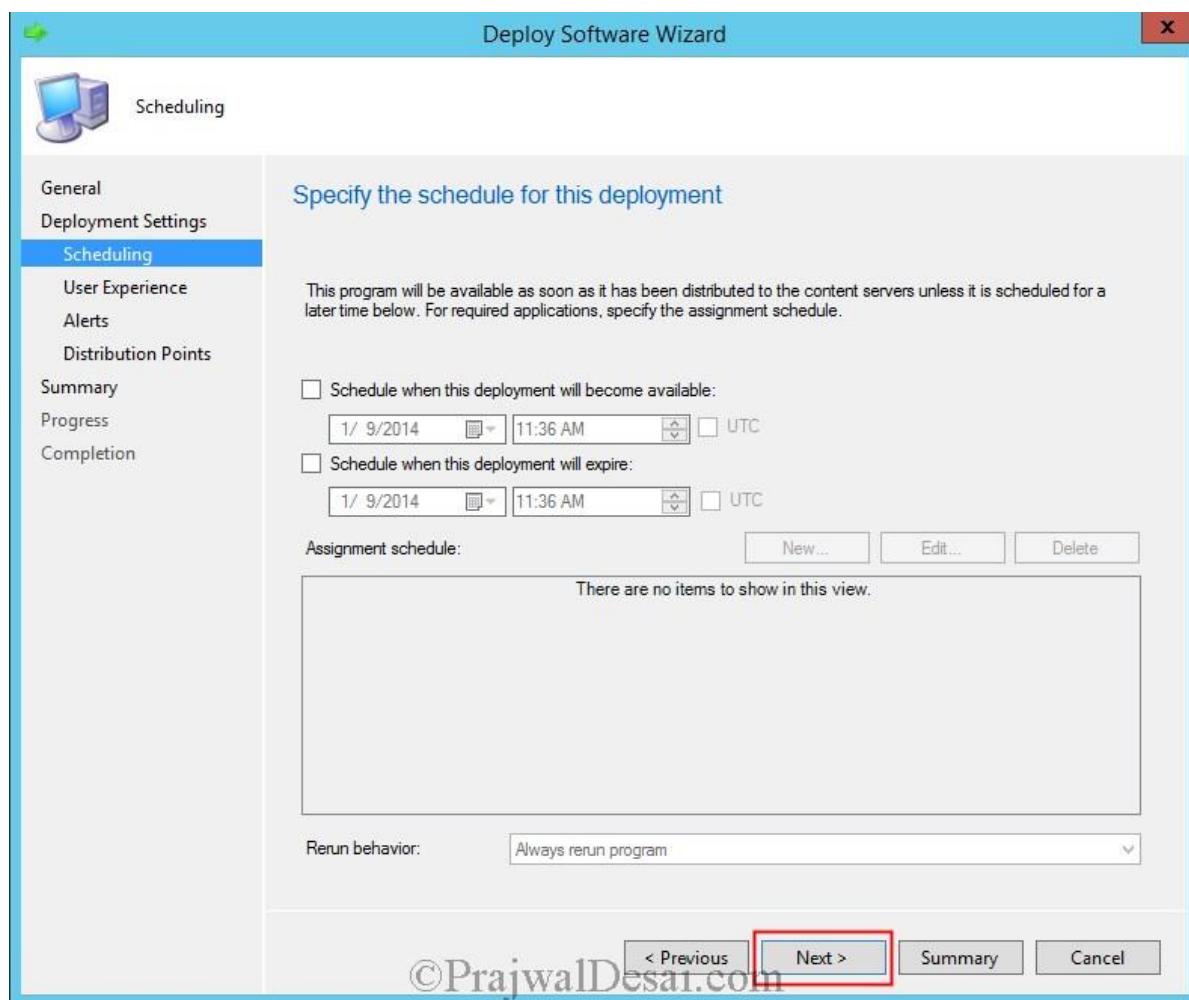
©PrajwalDesai.com

Set the purpose as **Available** and let this task sequence be available to only **media and PXE**. Click **Next**.



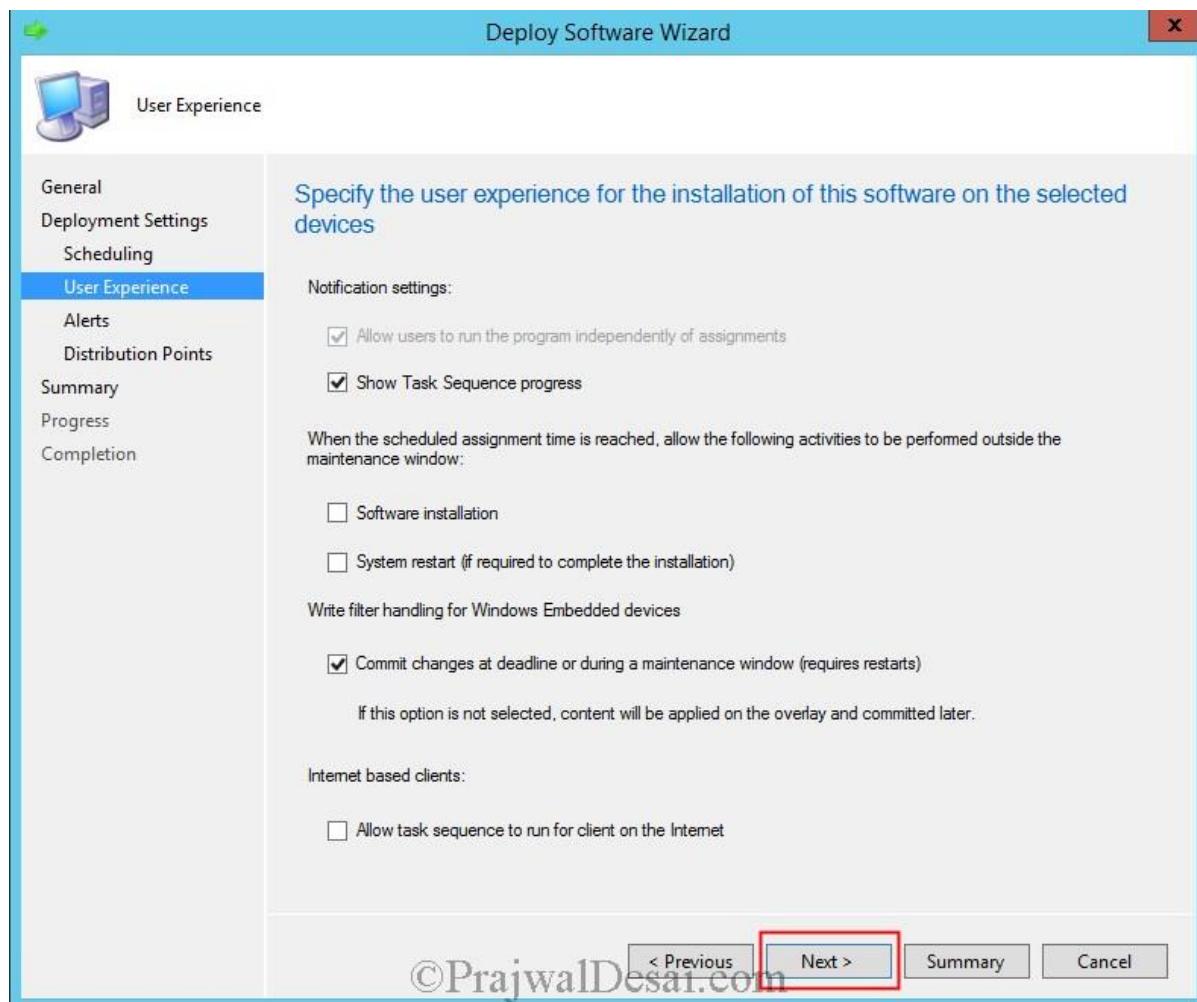
©PrajwalDesai.com

Leave this to default and click **Next**.

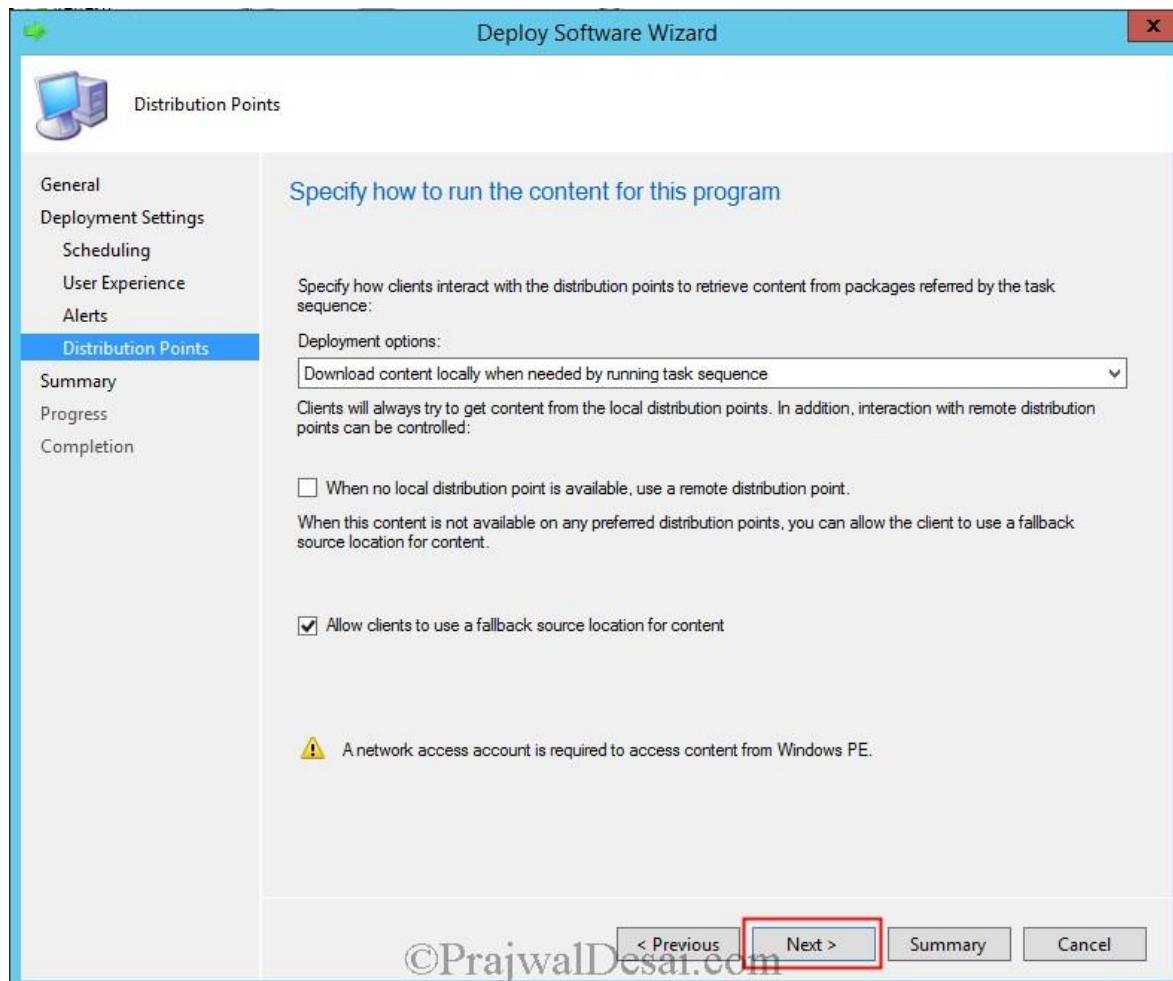


©PrajwalDesai.com

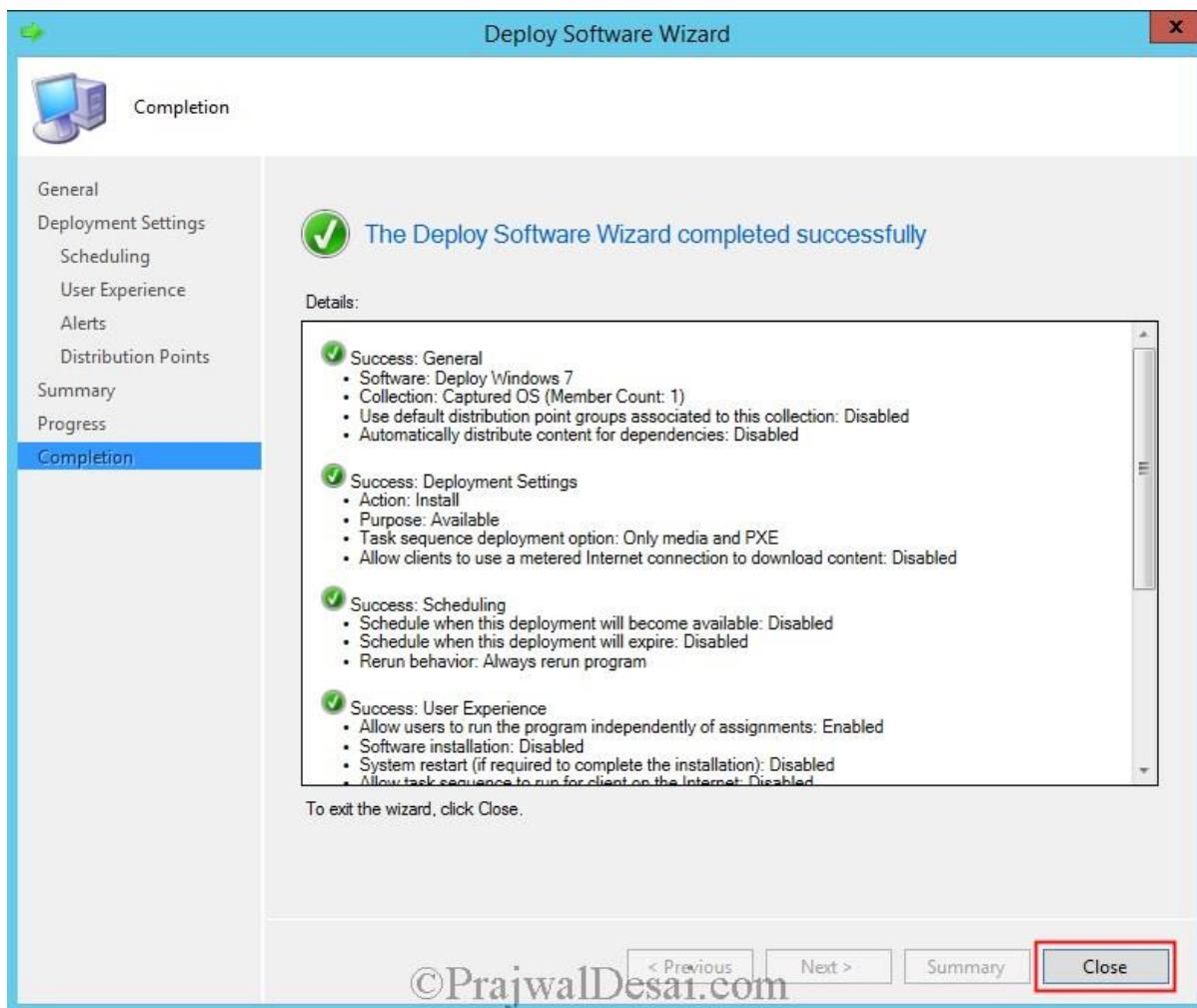
Leave the **User Experience** options to default and click **Next**.



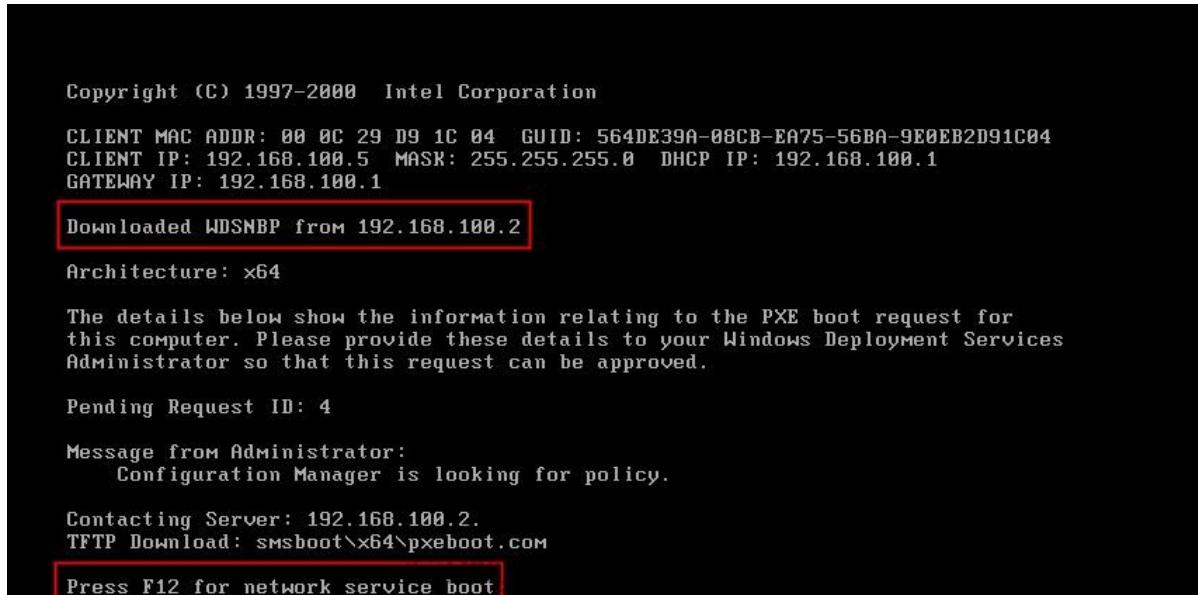
On this screen please read the warning line at the bottom. “**A network account is required to access content from Windows PE**“. You must define a network access account in order for this deployment to run smoothly. To define a network access account, on the CM2012 R2 console click **Administration**, under **Site Configuration** click **Sites**, in the top ribbon click **Configure Site Components**, click **Software Distribution**. Click **Network Access Account** and add specify the account which has enough permissions to access the network locations. Click **Next**.



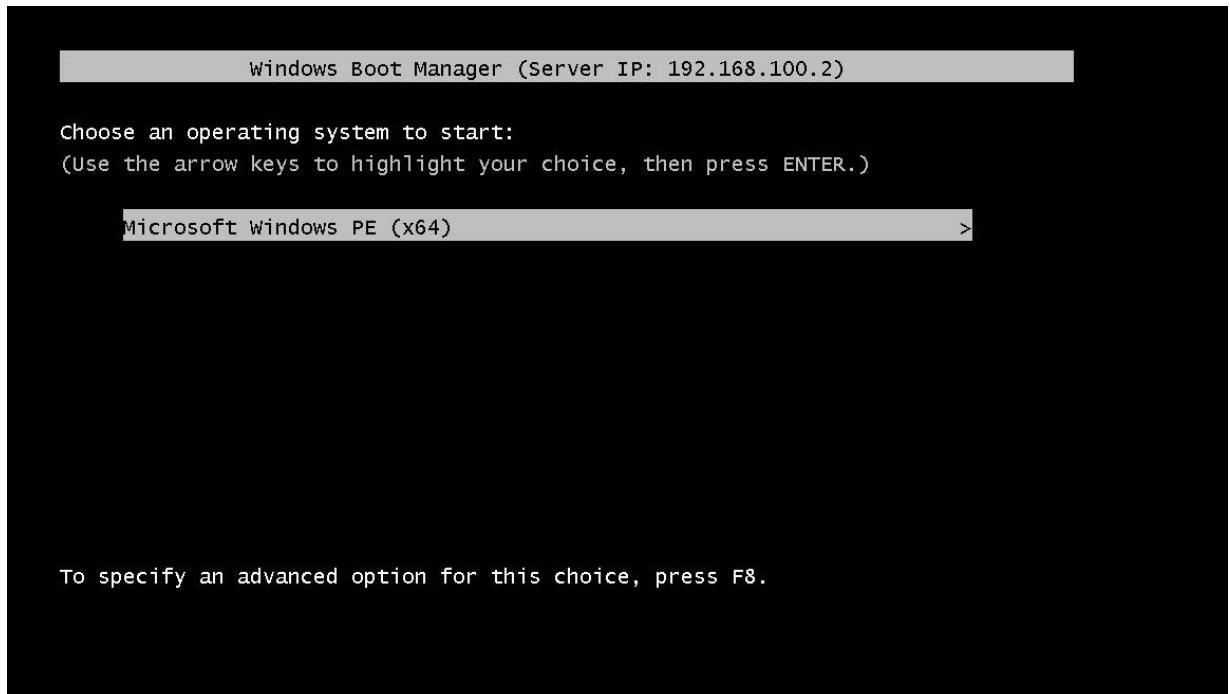
Click **Close** to close the Deploy software wizard.



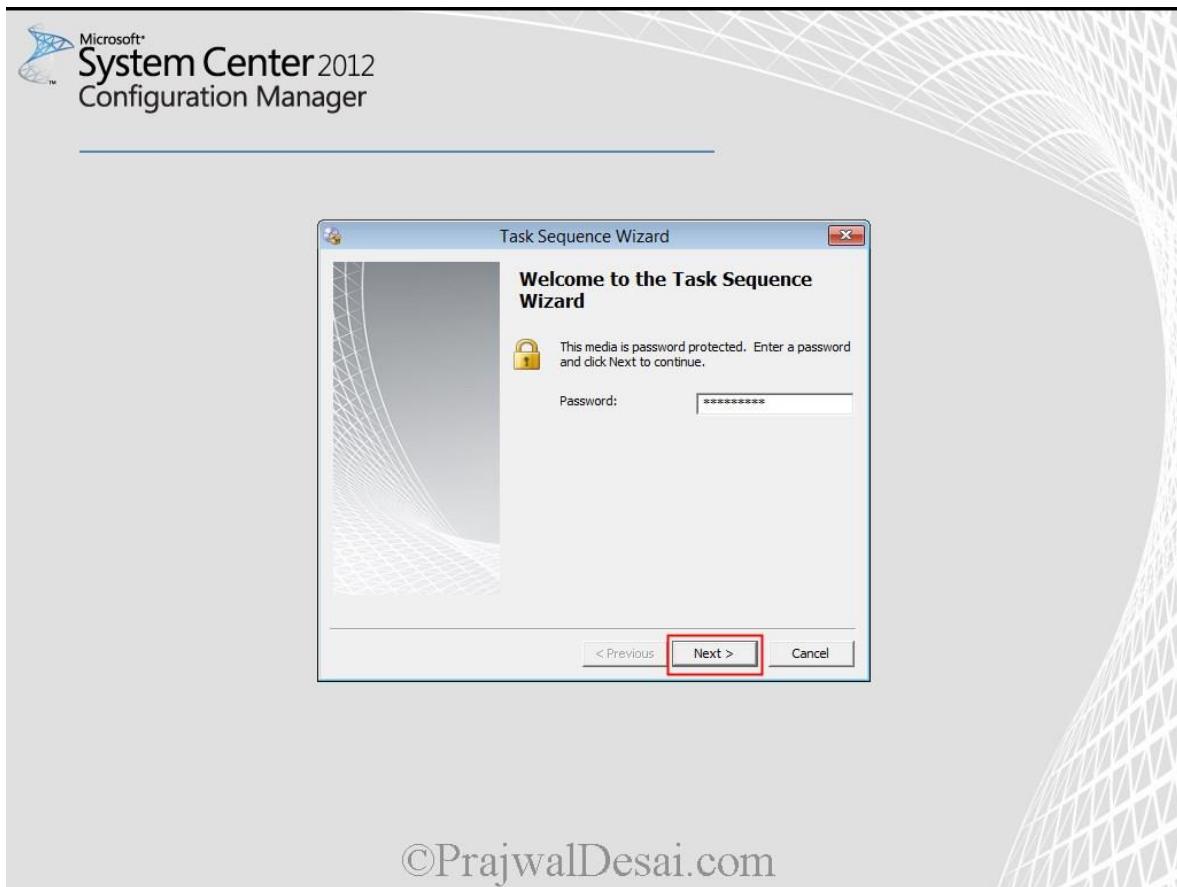
So far in this post we have created a device collection, imported the computer information to the collection, created a task sequence for deploying the captured OS and deployed it to the collection. Now we are ready for deploying the operating system, power on the VM / Physical box where the OS is to be deployed, set the device to boot from the network. On the screen press **F12** key for network service boot.



Hit **Enter** key when you see this screen.

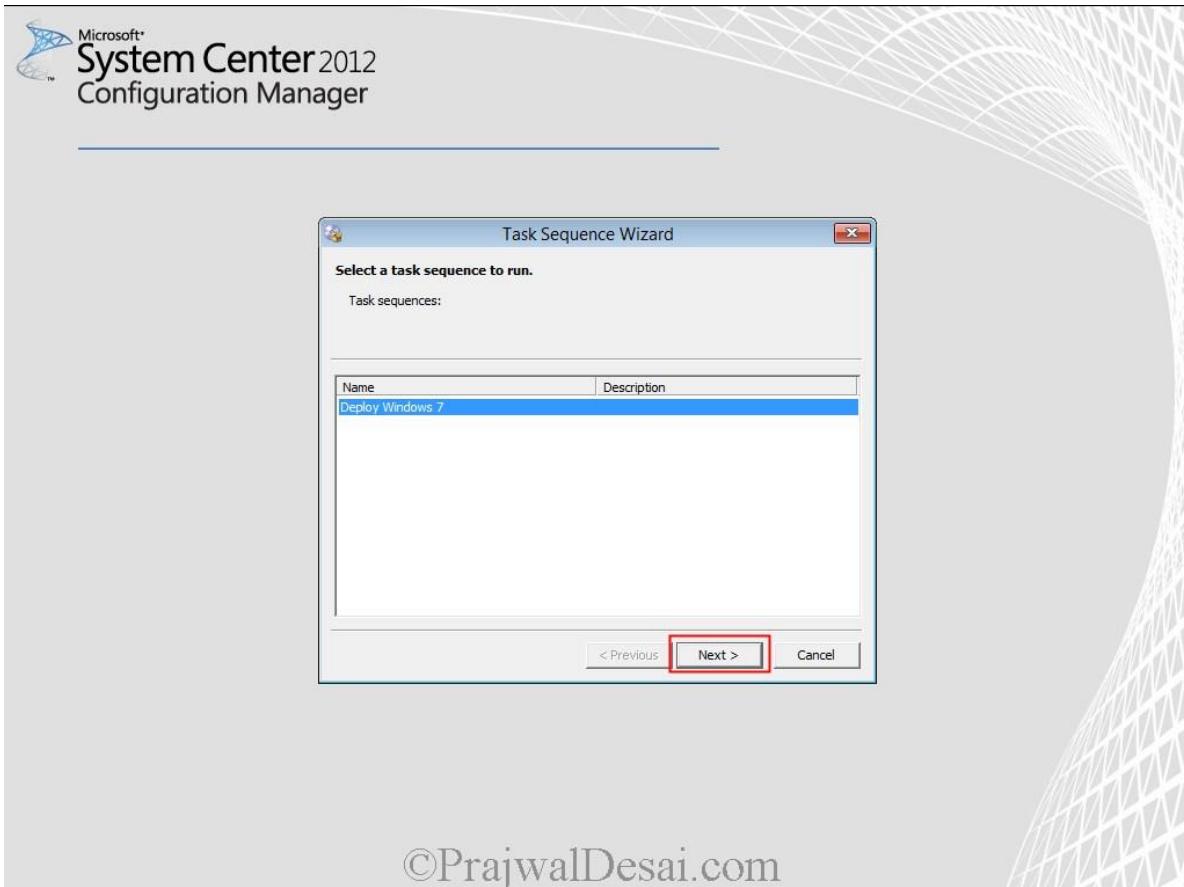


On the **Task Sequence Wizard**, provide the password and click on **Next**.



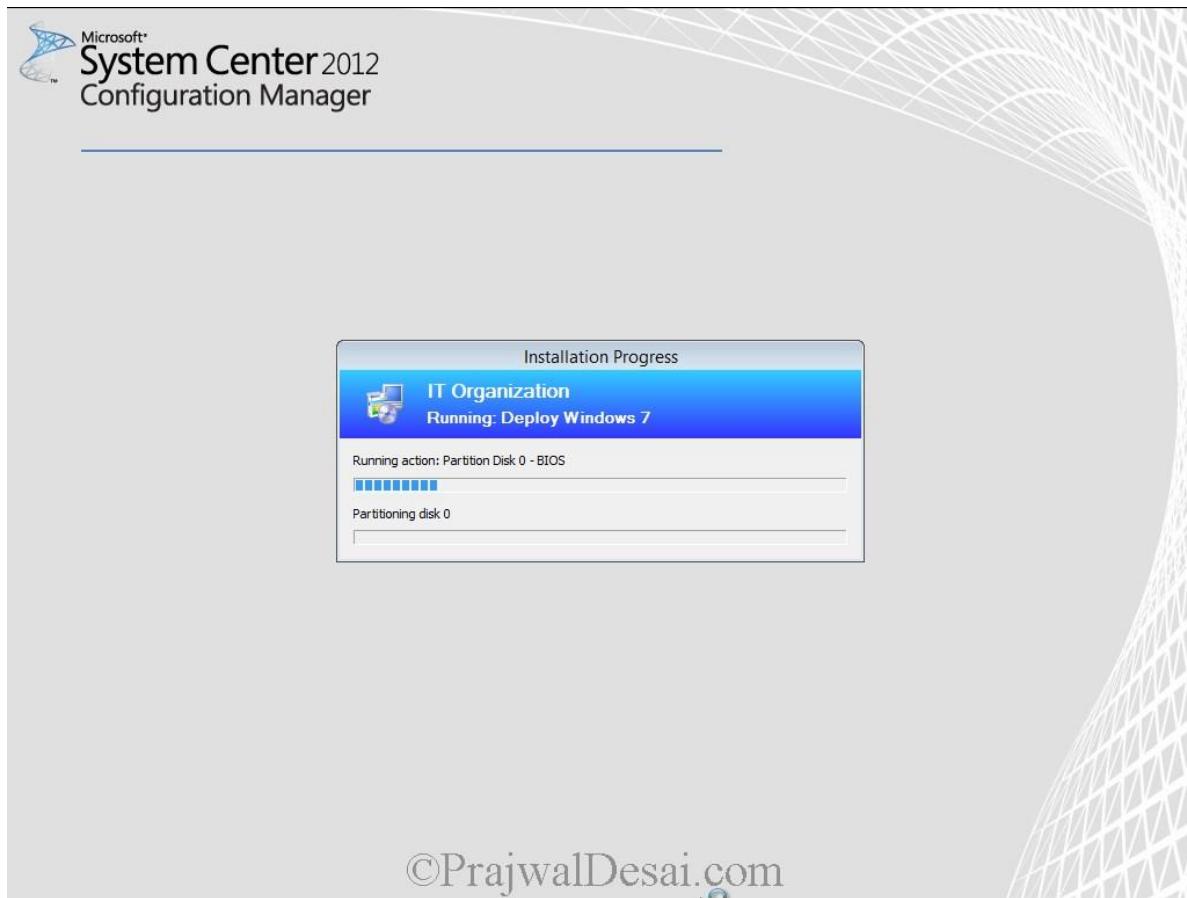
©PrajwalDesai.com

You should see the task sequence for deploying OS under the list of Task Sequences. Choose the task sequence and click **Next**.



©PrajwalDesai.com

The hard disk is being partitioned.



©PrajwalDesai.com

We see that the captured image is being applied to the new computer.



Final screenshot of the windows 7 OS deployment.

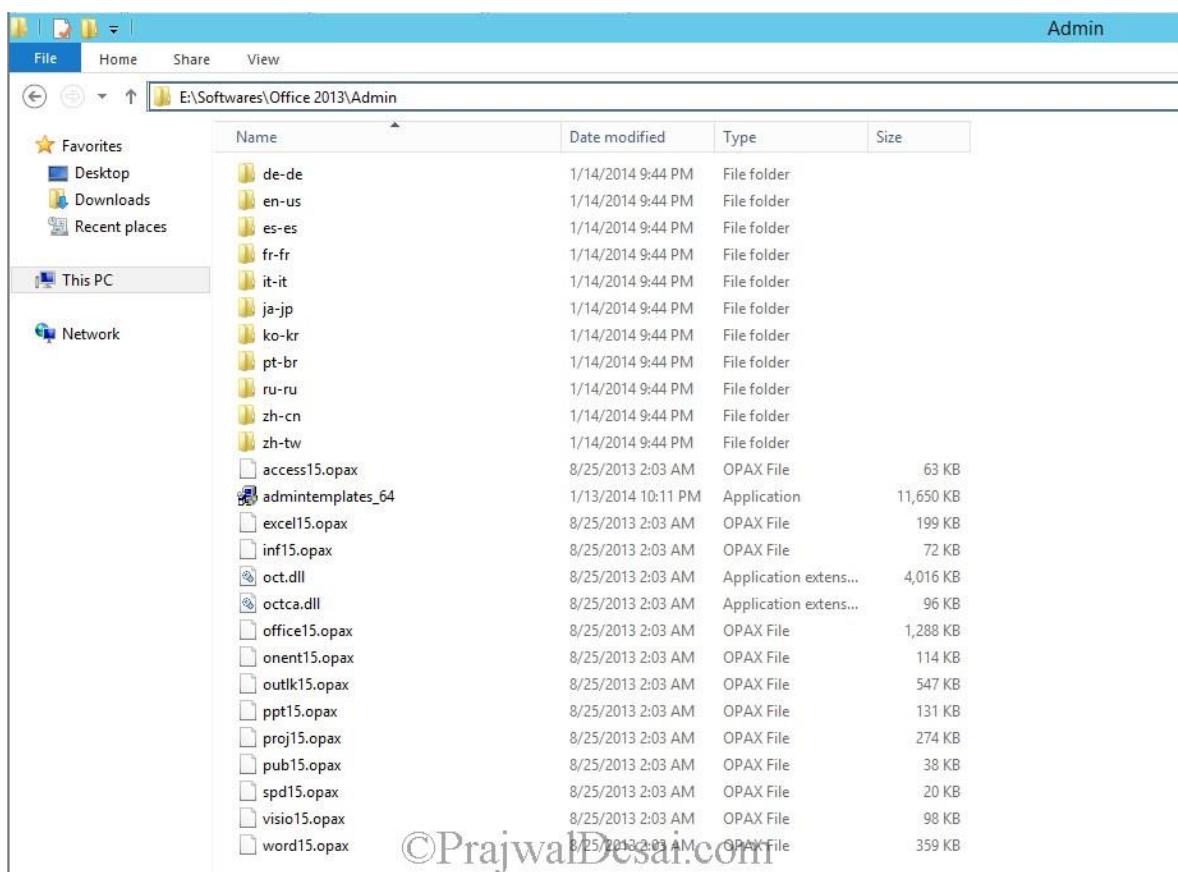


How To Deploy Microsoft Office 2013 Using SCCM 2012 R2

How To Deploy Microsoft Office 2013 Using SCCM 2012 R2 In this post we will see how to deploy Microsoft Office 2013 using SCCM 2012 R2. If you are planning to deploy Microsoft Office 2010 using SCCM 2012 then you can click on this [link](#). In this post we will be deploying Microsoft Office Professional Plus 2013 64 bit edition and the copy of office that I have is an MSDN copy. We know that the OCT (Office Customization Tool) is available only with volume licensed versions of Windows Installer-based Office 2013, Office 2010, and the 2007 Office system. To determine whether an Office 2013 installation is a volume licensed version, check the Office 2013 installation disk to see whether it contains a folder named **Admin**. If the Admin folder exists, the disk is a **volume license edition**. If the Admin folder does not exist, the disk is a **retail edition**. As there is no admin folder with MSDN copy we will first download **Office Customization Tool** 2013 from [here](#). We are basically looking for an unattended setup of Microsoft Office 2013 and this can be achieved only when you customize the installation using office customization tool. You can refer to SCCM 2012 R2 step by step guide [here](#).

How To Deploy Microsoft Office 2013 Using SCCM 2012 R2

Once you download the OCT 2013 setup file you need to install the software. Run the OCT 2013 executable file and extract the files to a folder inside Office installation files. In the below screenshot I have manually created the Admin folder and copied the OCT 2013 setup file inside it. The files are extracted to Admin folder, you can also skip creating a folder manually because the OCT 2013 setup file creates a folder named Admin by itself and extracts the files in it. The office 2013 setup files are stored on a drive in SCCM server in a folder named **Office 2013**.



On the SCCM server run the command prompt as administrator, change the path where office 2013 setup files are located. Run the command **setup.exe /admin**.

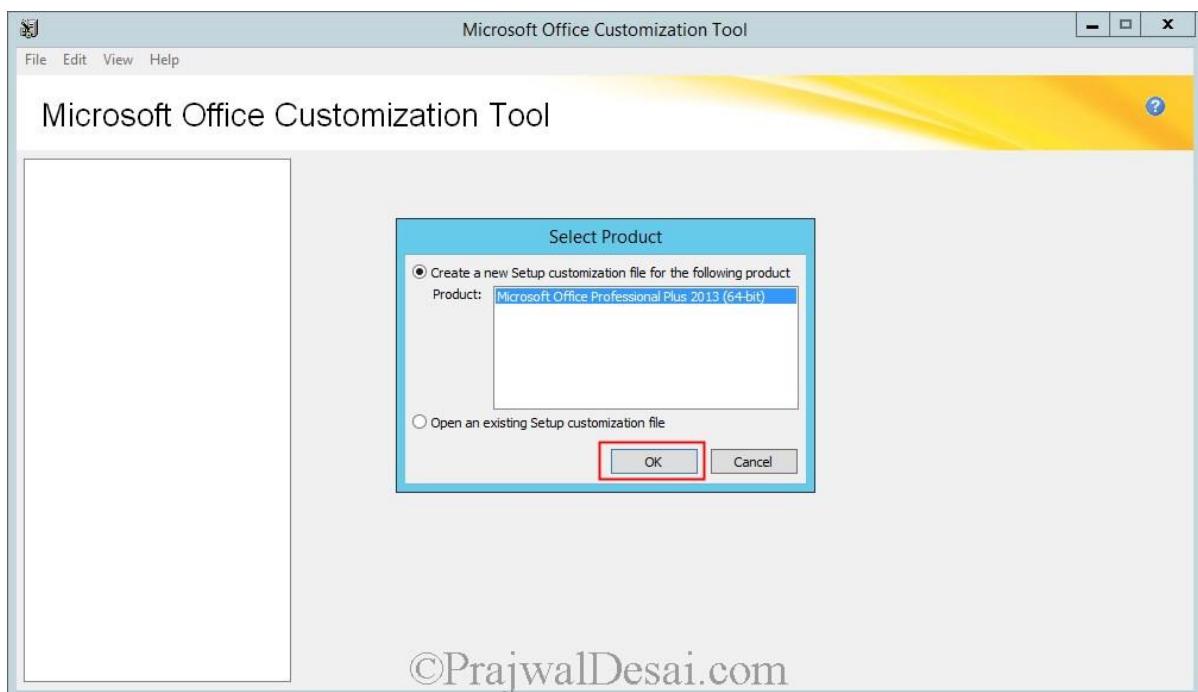


The screenshot shows an Administrator Command Prompt window. The title bar reads "Administrator: Command Prompt". The window content shows the following command being run:

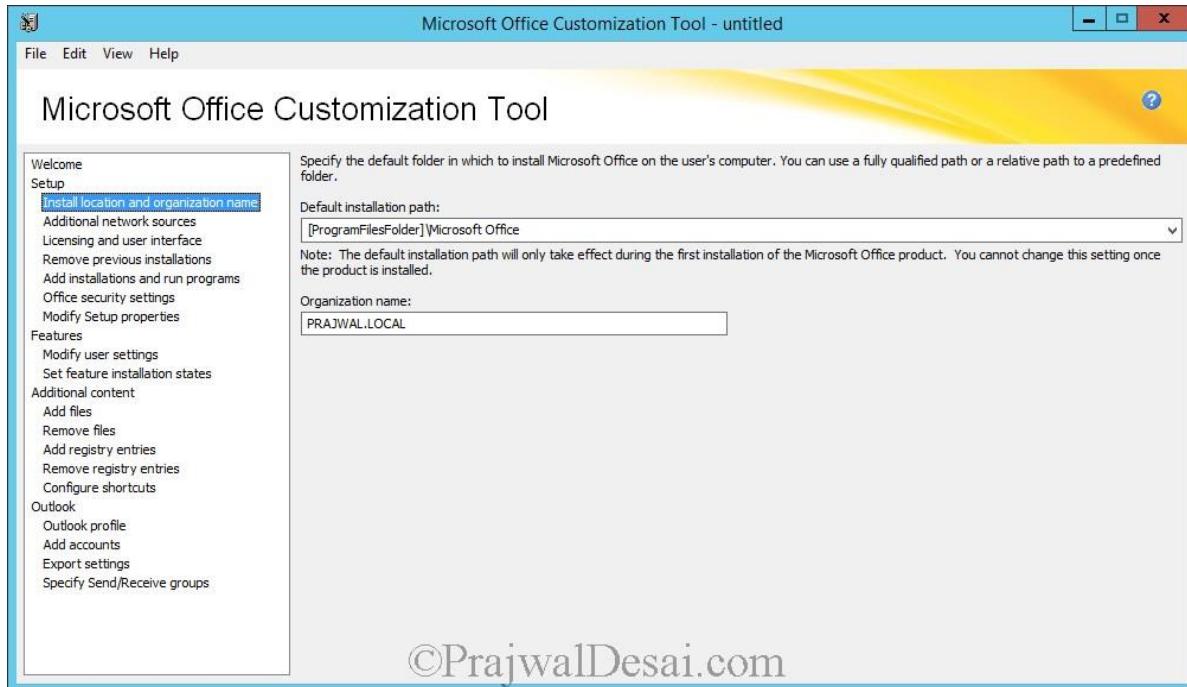
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>E:
E:>cd "Softwares\Office 2013"
E:\Softwares\Office 2013>setup.exe /admin
```

You will now see **Microsoft Office Customization Tool**, Choose **Create a new setup customization file for following product**, verify that correct product is selected. Click on **OK**.

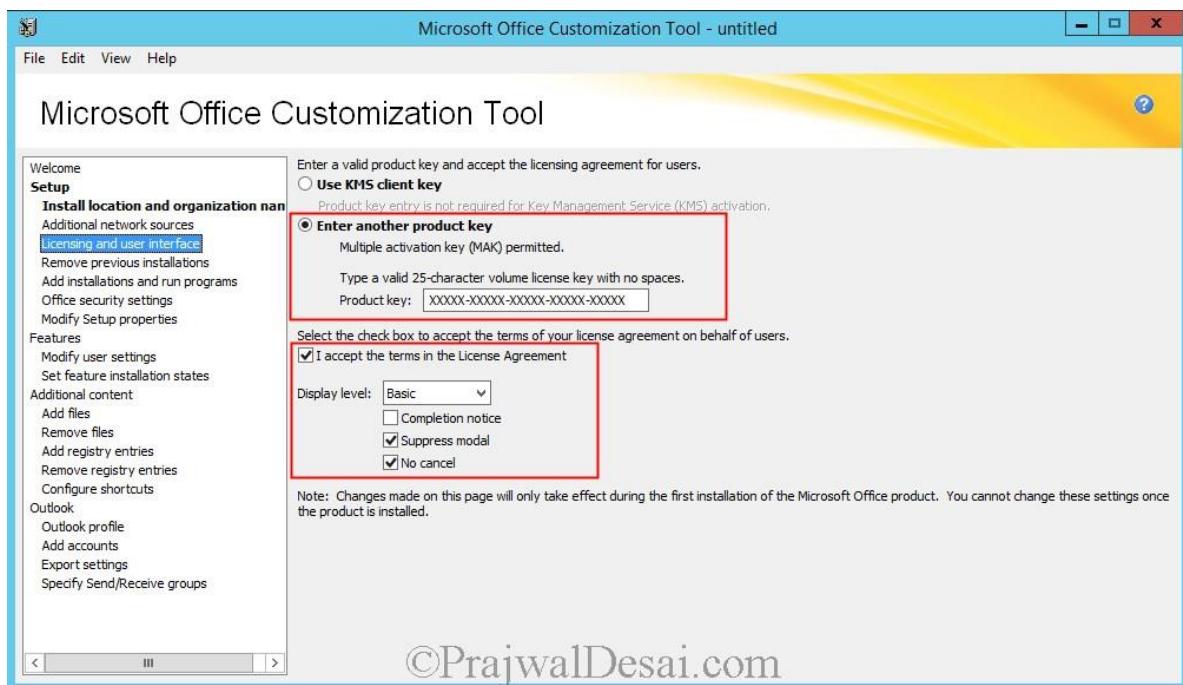


Select **Install location and organization name**, in the text box provide the **Organization Name**.



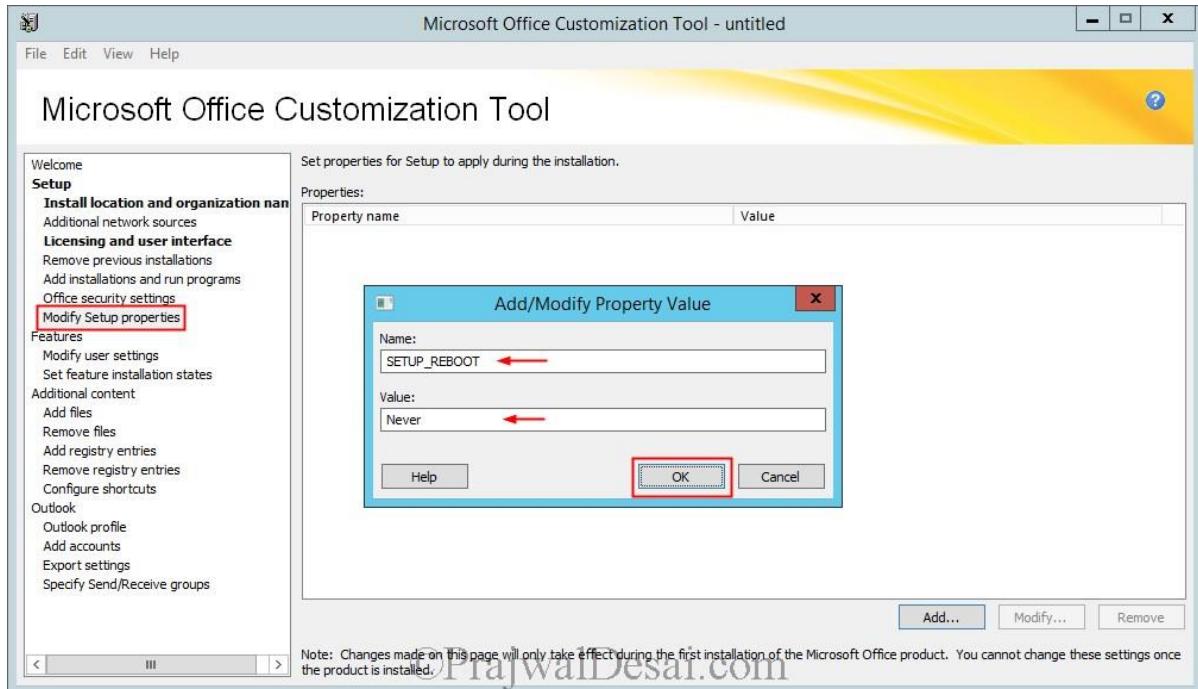
©PrajwalDesai.com

Click on **Licensing and user interface**, choose the option **Use KMS client key** if you have KMS server in your organization for activating office 2013 suite, else choose **Enter another product key** and enter the office 2013 key. Click on **I accept the terms in the license agreement**. Select the **Display level** as **Basic**, check the box for **Suppress modal** and **No cancel**.

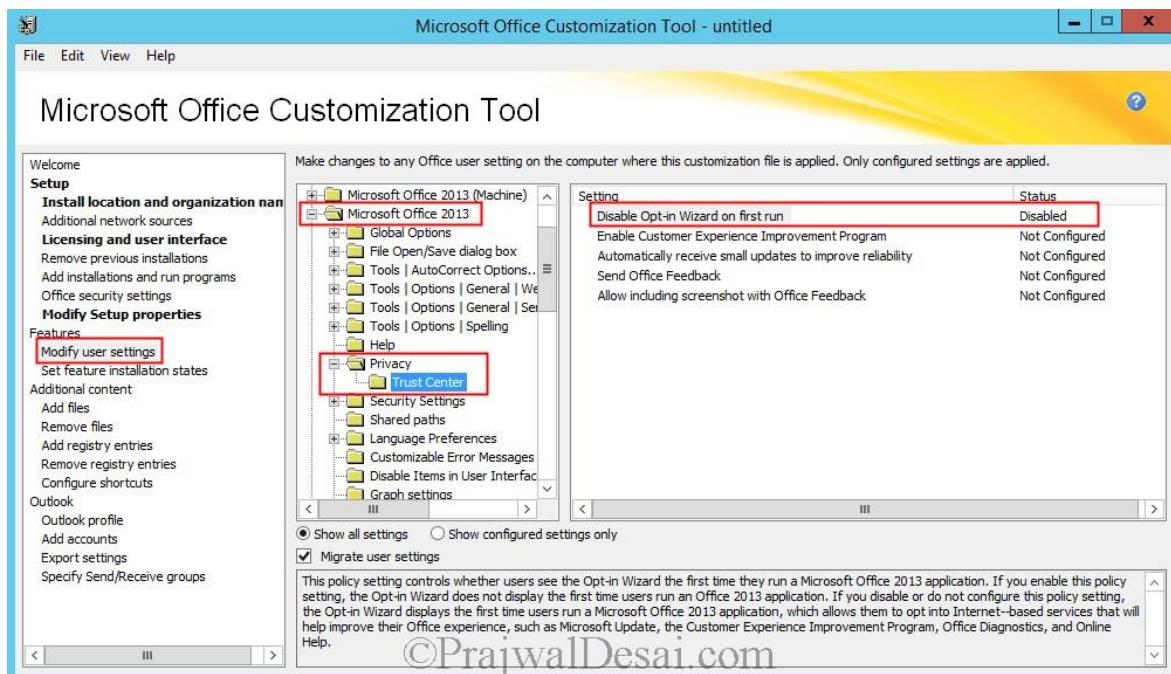


©PrajwalDesai.com

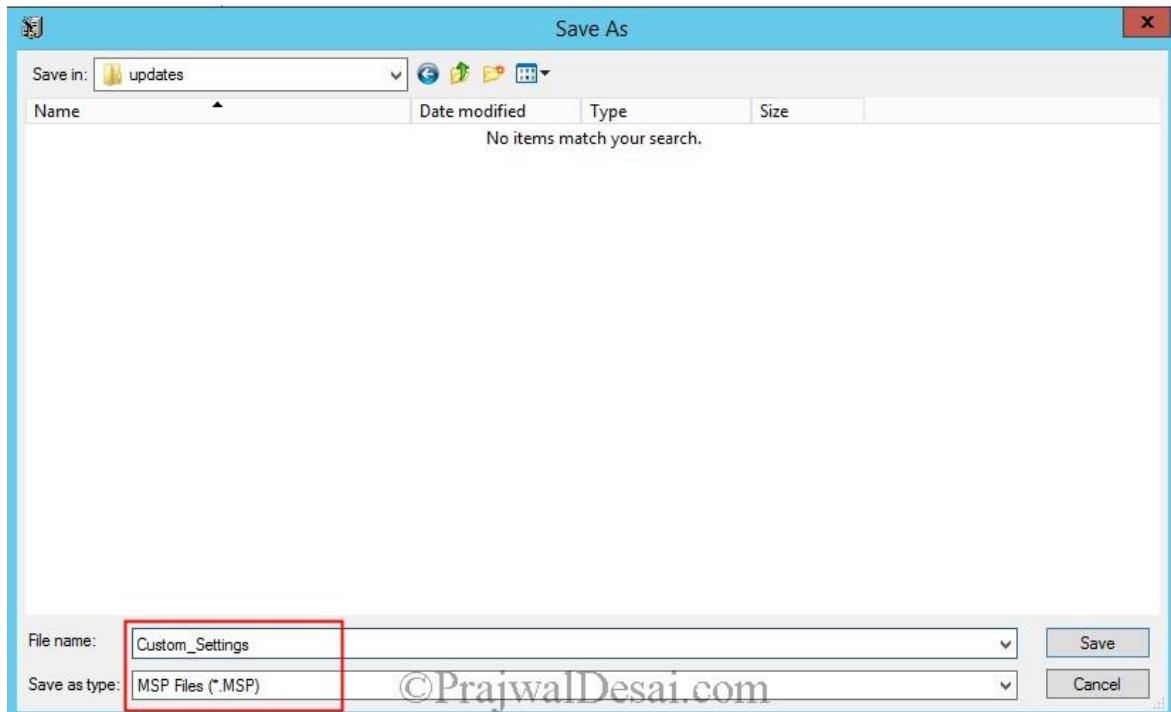
Now click on **Modify Setup properties**. Click **Add**, provide the **Name** as **SETUP_REBOOT** and **Value** as **Never**. Click **OK**.



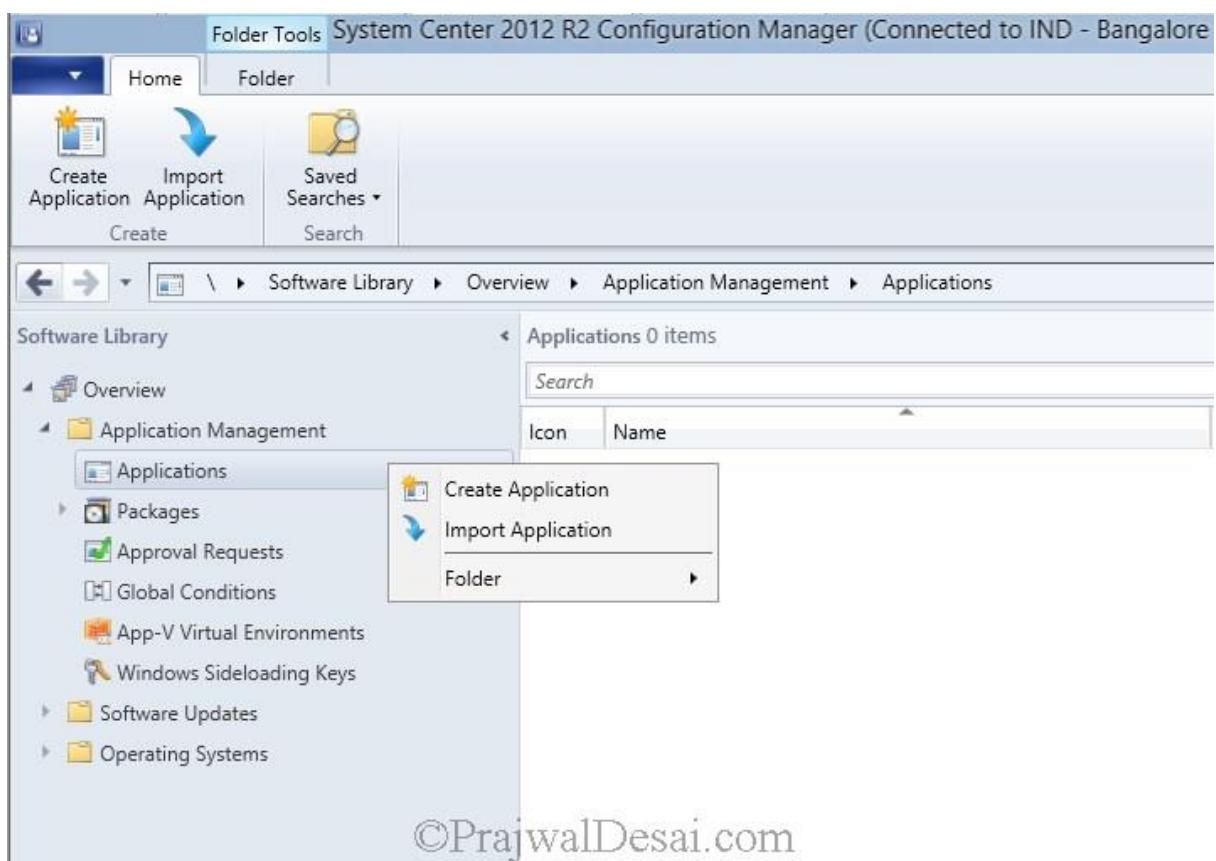
Select **Modify user settings**, **Microsoft Office 2013**, **Privacy**, **Trust Center**. Double click the setting **Disable Opt-in Wizard on first run** and set the status as **Enabled**.



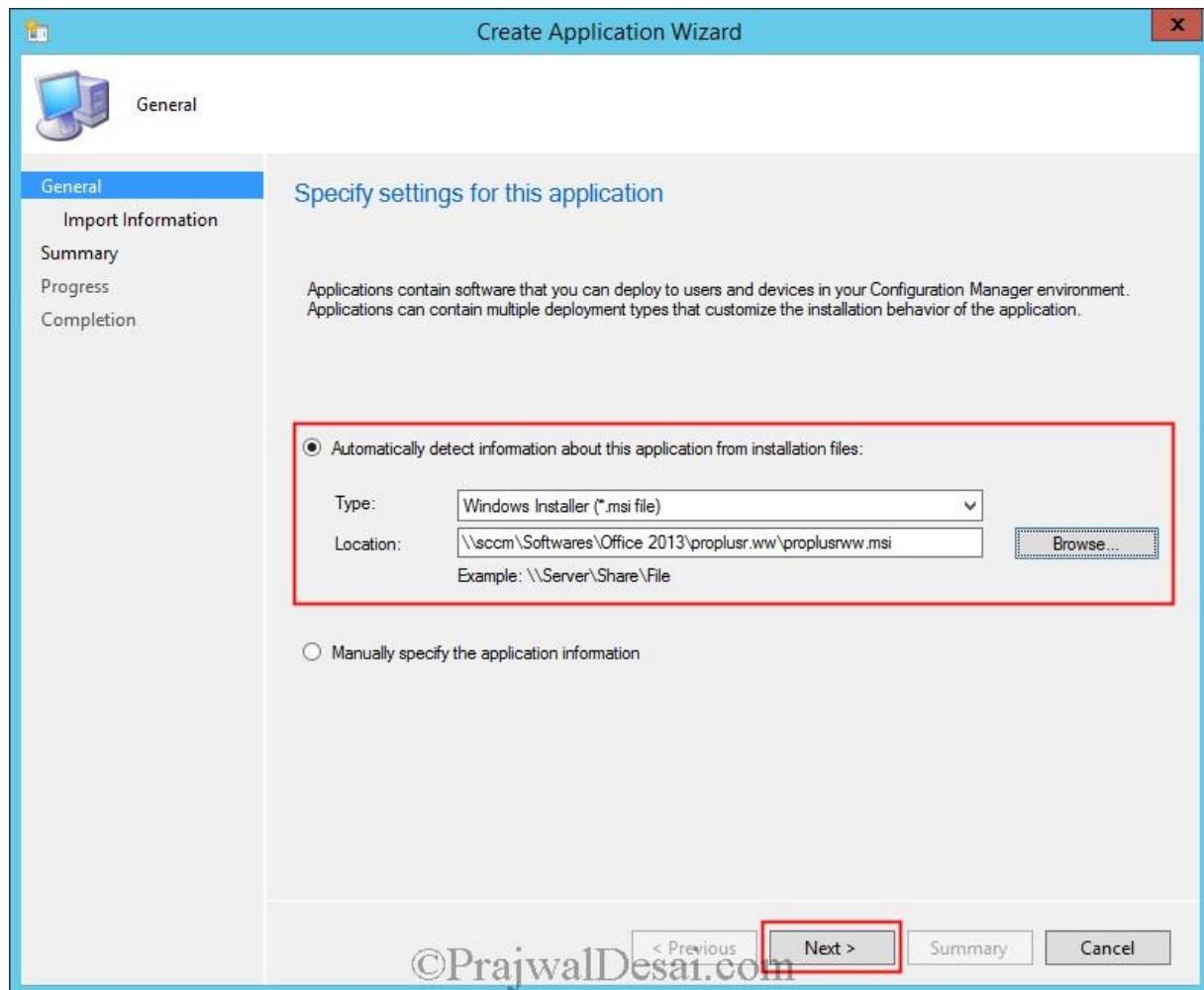
Now click on **File -> Save As** -> save the customization file inside **Updates** folder. Close the OCT tool.



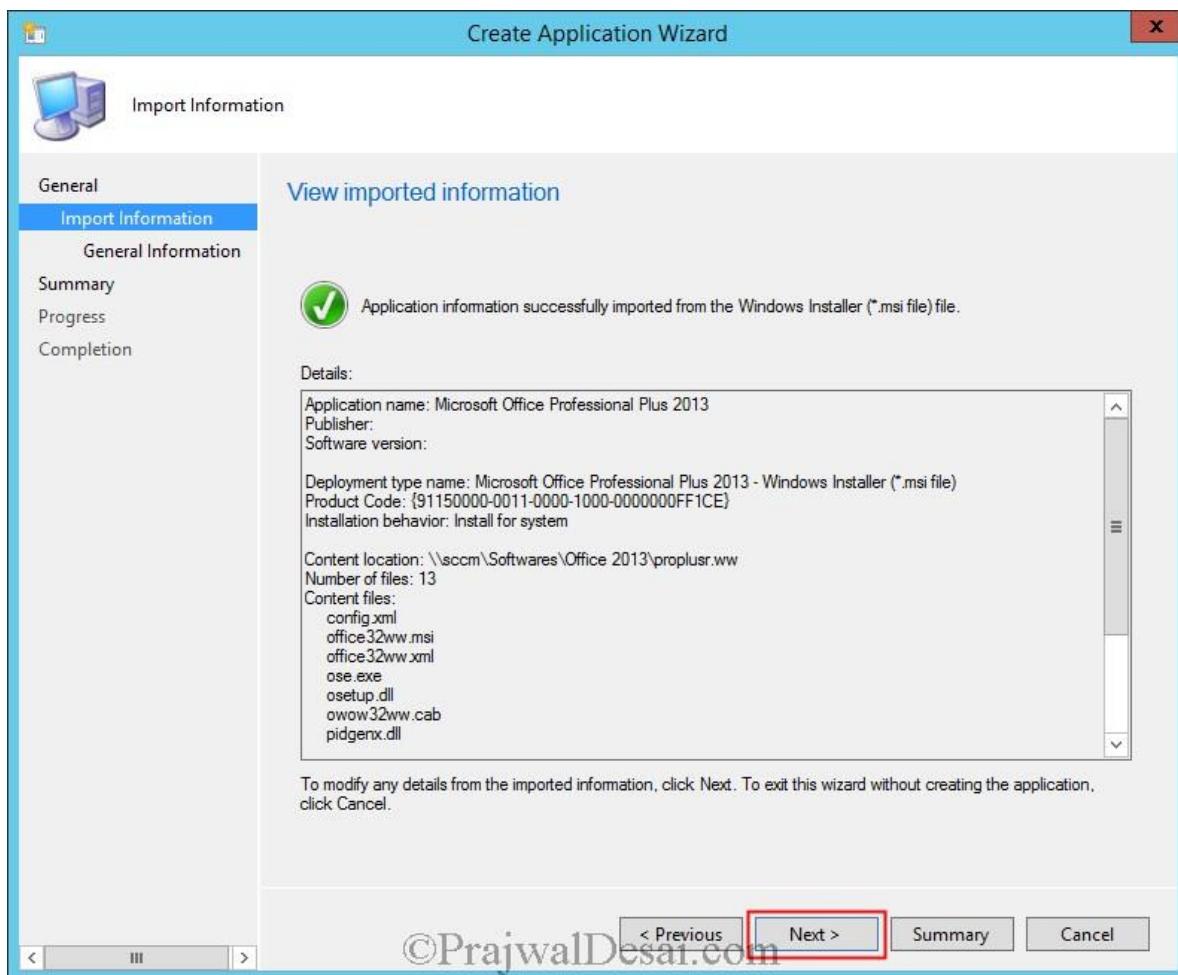
Open the SCCM 2012 R2 console, under the **Application Management**, right click **Applications** and click **Create Application**.



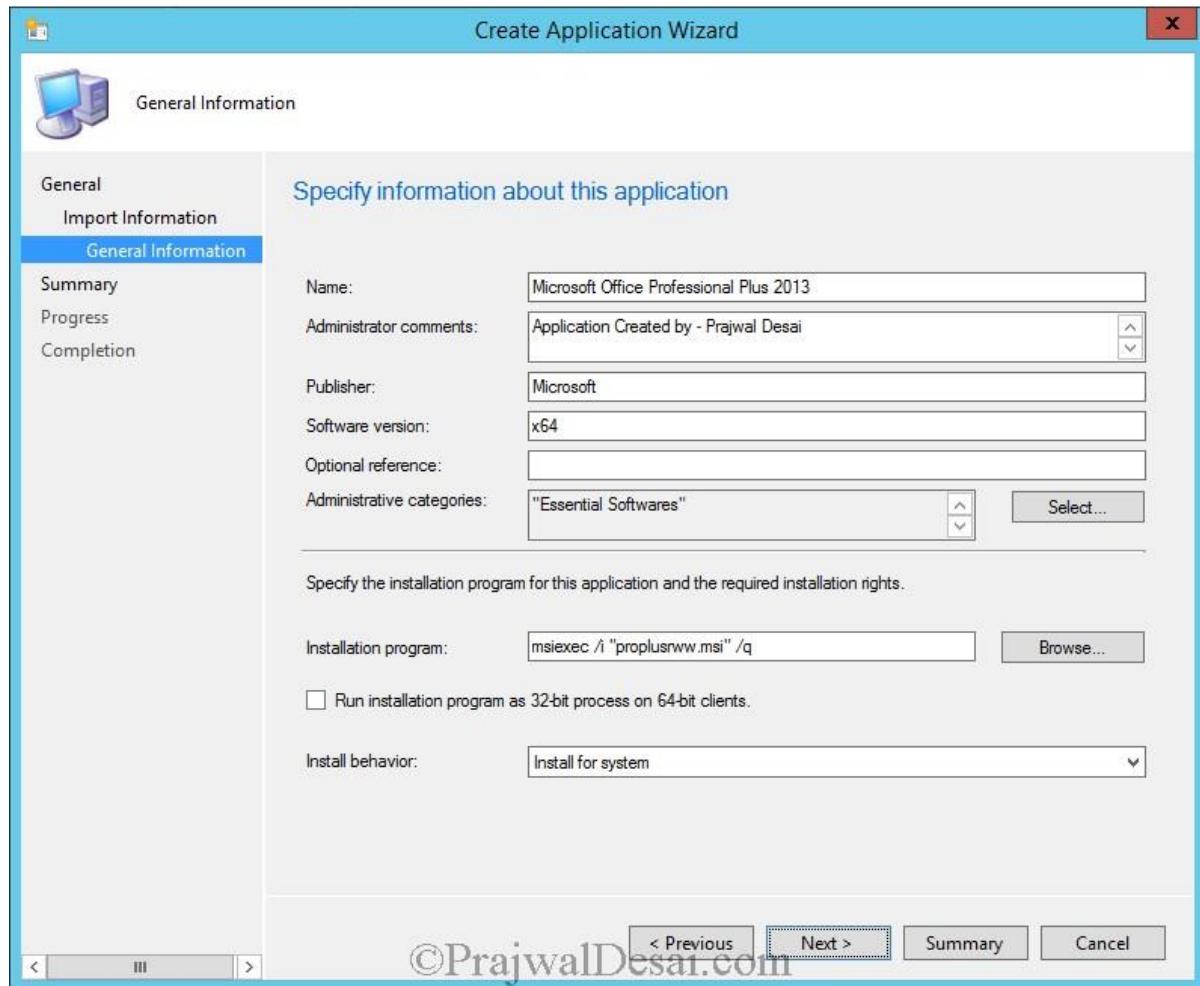
Choose **Automatically detect information** and provide the path to file **proplusrww.msi**. Click **Next**.



The application information has been imported from .msi file. Click **Next**.

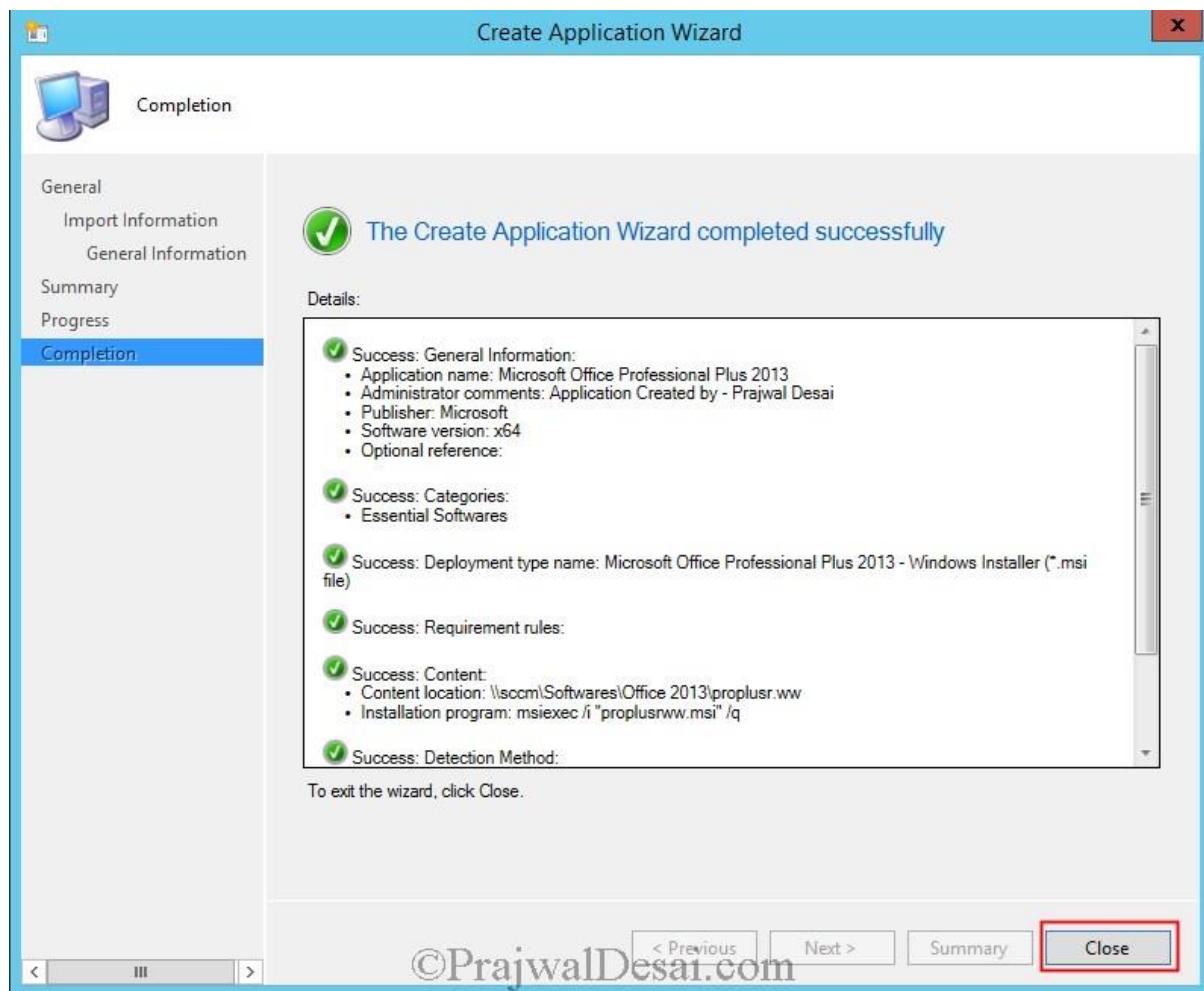


You can specify a little information about this application. We will change the **Installation program** command later. Choose the **Install behavior** as **Install for system**. Click **Next**.

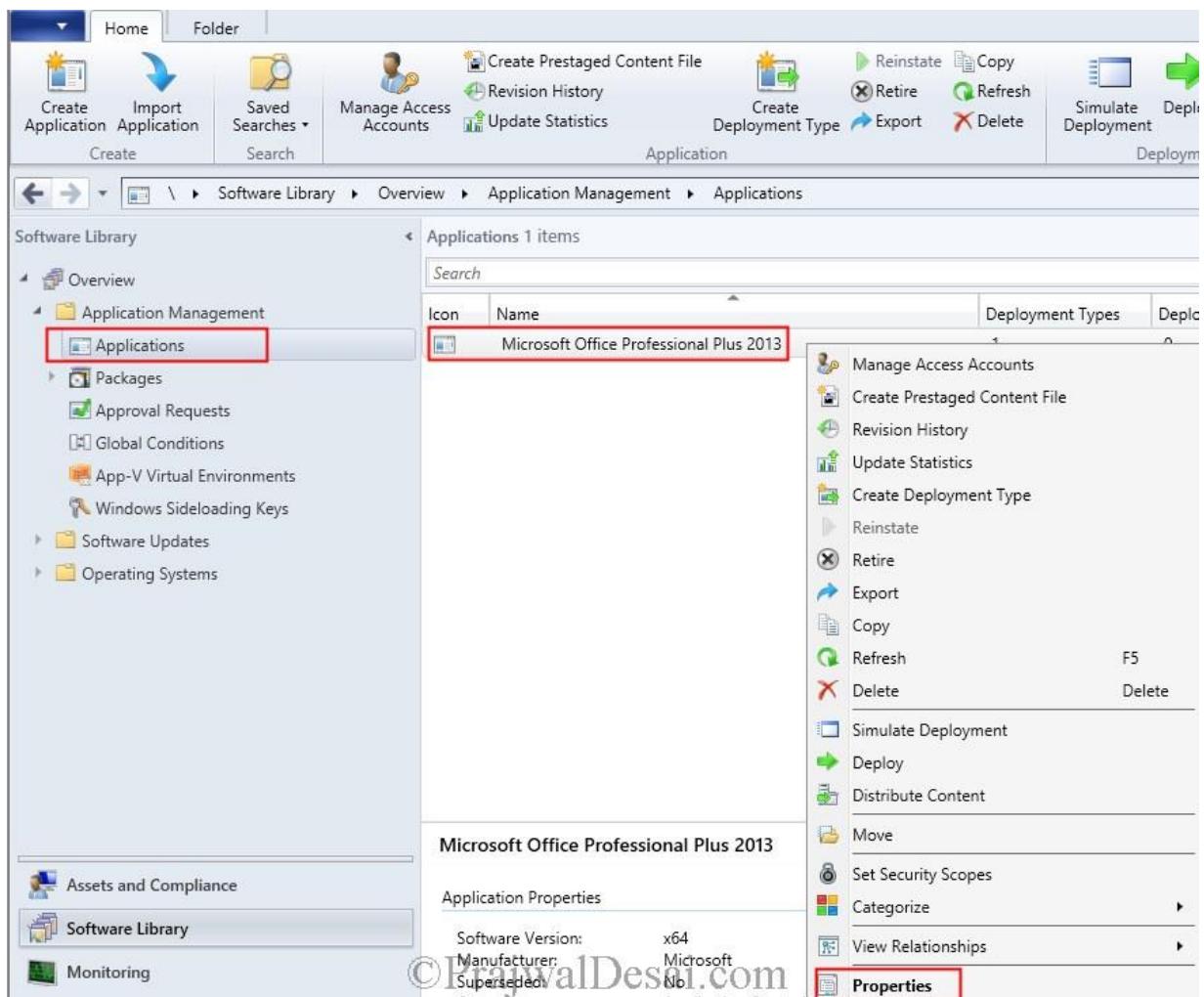


©PrajwalDesai.com

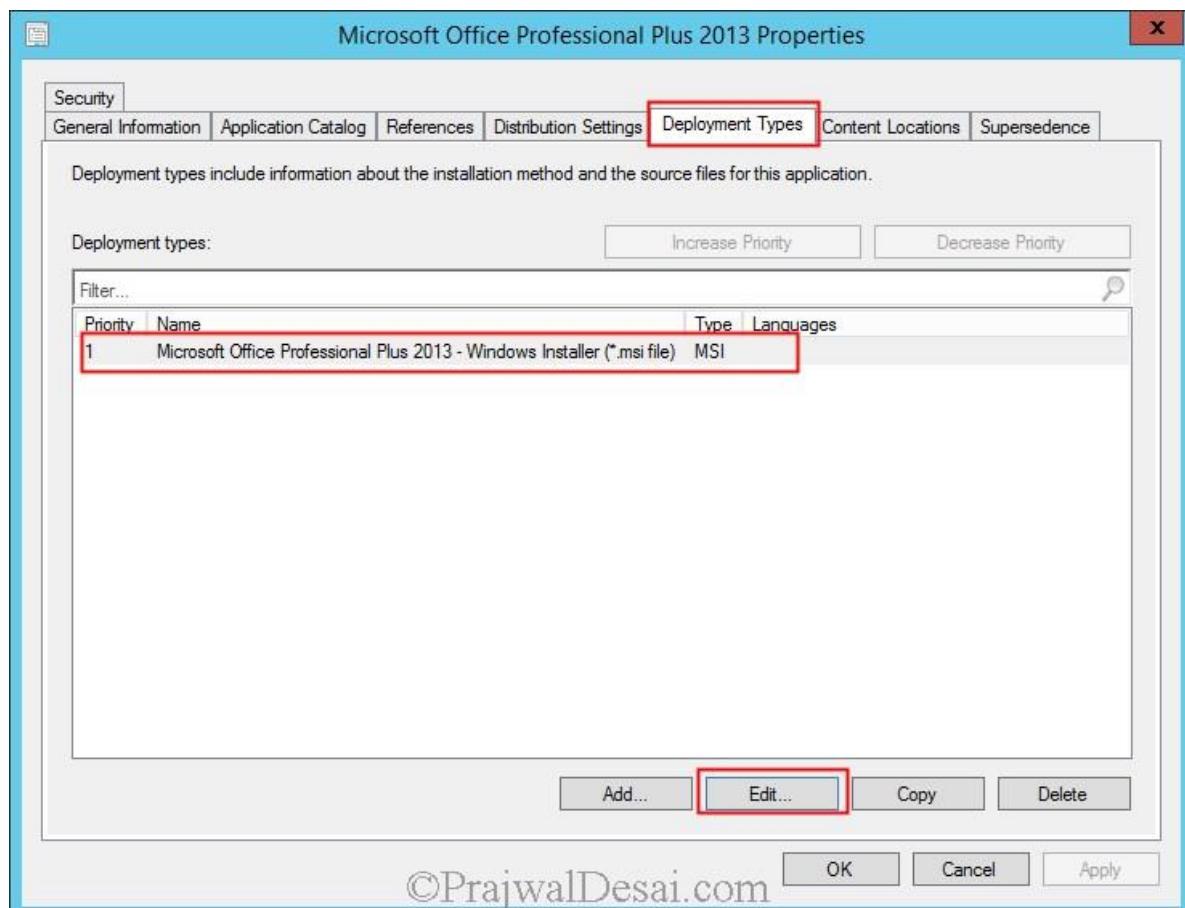
The Application has been created successfully. Click **Close**.



Right click the Office 2013 application, click on **Properties**.

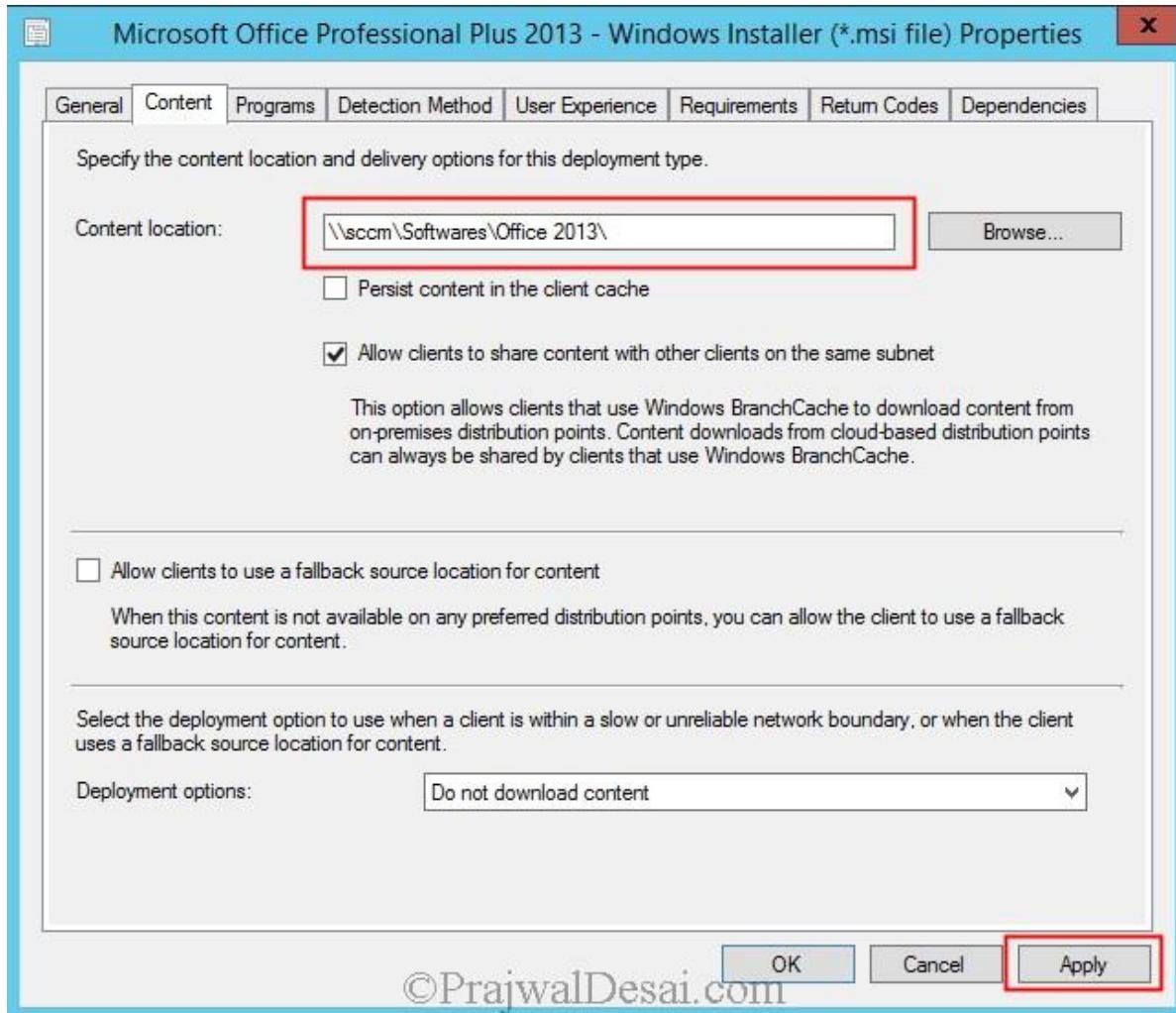


Click on **Deployment Types** tab, click on the msi file and click **Edit**.



©PrajwalDesai.com

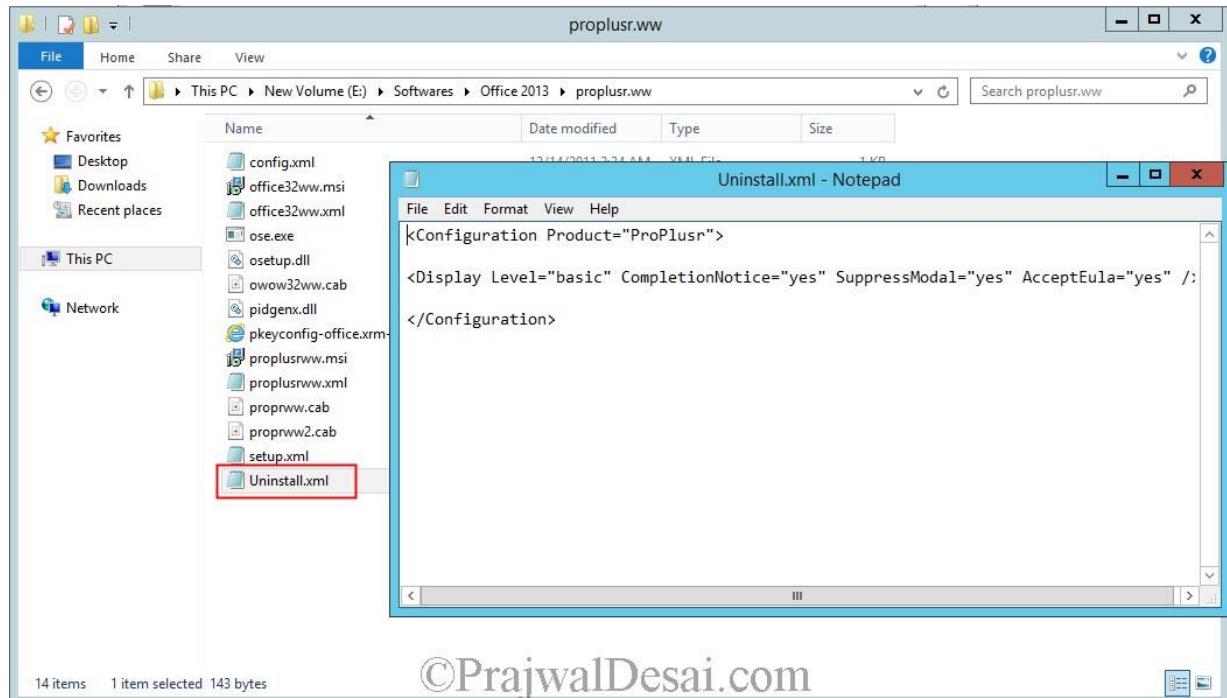
Click on **Content** tab, set the Content location to Office 2013 folder (or a folder where Office 2013 installation files are present, remove **proplusr.ww** after **Office 2013**). Click on **Apply**.



We will also create a .xml file that will help us in uninstalling the Office 2013. Open Notepad and paste the below lines.

```
<Configuration Product="ProPlusr">  
<Display Level="basic" CompletionNotice="yes" SuppressModal="yes"  
AcceptEula="yes" />  
</Configuration>
```

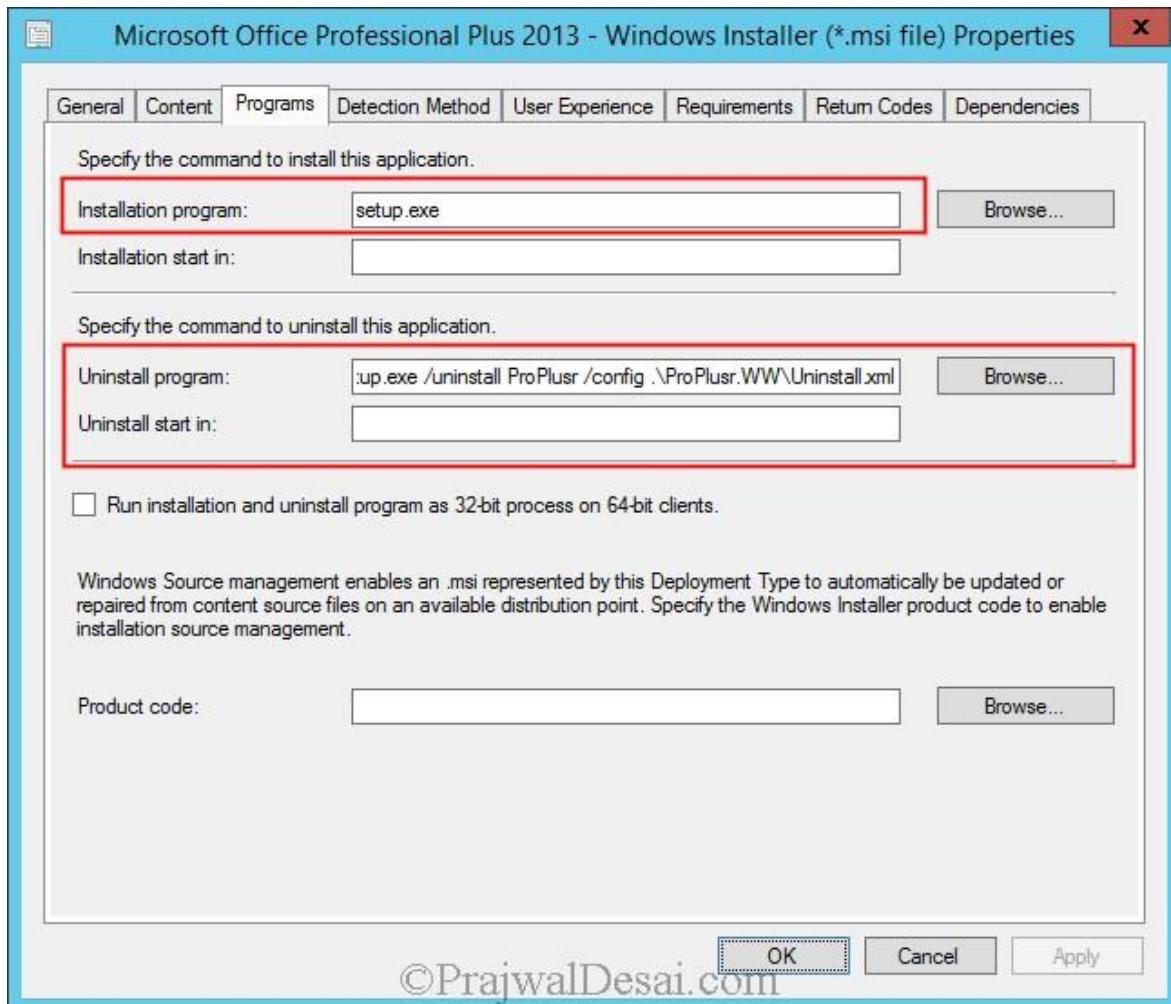
Save the file as **Uninstall.xml** in the folder **proplusr.ww** (you can choose any filename, only the extension should be .xml)



©PrajwalDesai.com

Click on **Programs** tab, change the **Installation Program** command to **setup.exe**, change the **Uninstall program** command to **setup.exe /uninstall ProPlusr /config .ProPlusr.WWUninstall.xml**

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



The next step is to make the application available to DP. Right click the Office 2013 application, click on **Distribute Content**, choose you **DP** and wait until the application is available with DP. You can verify this by checking the **Content Status** of the Office 2013 application under **Distribution Status**.

Deploy the Office 2013 application to the collection. Right click on the Office 2013 application and click on **Deploy**. Choose the **Device Collection** and choose the **Action as Install** and **Purpose as Available**. (I haven't covered the screenshots of deploying application as it's simple to deploy an application to collection).

The screenshot shows the Configuration Manager interface under 'Monitoring > Overview > Content Status'. A red box highlights the 'Content Status' link in the left navigation. The main pane displays a table titled 'Content Status 11 items' with columns for Icon, Software, Type, Targeted, Size (MB), Compliance, Date Created, Package ID, and Source. The row for 'Microsoft Office Professional Plus 2013' is highlighted with a red arrow pointing to the 'Targeted' column, which contains the value '2'. Below the table, a summary for 'Microsoft Office Professional Plus 2013' shows its details: Software: Microsoft Office Professional Plus 2013, Type: Application, Date Created: 1/14/2014 10:50 PM, and Package ID: IND00008. To the right, there is a completion statistics chart with a green circle and a red border, indicating 1 Targeted. The status bar at the bottom right shows 'Last Update: 1/14/2014 10:56 PM'.

After few minutes, on the client computer we see that the application is available. Select the software and click on **Install Selected**.

The screenshot shows the Software Center interface with tabs for Available Software, Installation Status, Installed Software, and Options. The Available Software tab is selected. A red box highlights the 'NAME' column header in the table below. The table lists one item: Microsoft Office Professional P... (Application, Microsoft, Available, 1/14/2014). Below the table, a detailed view for 'Microsoft Office Professional Plus 2013' is shown with sections for OVERVIEW, REQUIREMENTS, and DESCRIPTION. The 'DESCRIPTION' section notes 'Application Created by - Prajwal Desai'. At the bottom right of this view, a red box highlights the 'INSTALL SELECTED' button.

The application is first downloaded to the client computer and then installed. We now see that the application is installed successfully.

The screenshot shows a software management interface titled "Software Center" under "IT Organization". The "Installation Status" tab is selected. A search bar at the top right contains the placeholder "Find additional applications from the Application Catalog". Below the tabs, there's a dropdown menu set to "All" and a "SEARCH" button with a magnifying glass icon. The main area displays a table with columns: NAME, TYPE, PUBLISHER, AVAILABL..., and STATUS. One row is highlighted with a red border, representing Microsoft Office Professional Plus... which is listed as an Application published by Microsoft, available since 1/14/2014, and in the Installed status. At the bottom of the table, there's a section for "Microsoft Office Professional Plus 2013" with three tabs: OVERVIEW, REQUIREMENTS, and DESCRIPTION. The OVERVIEW tab shows details like Status: Installed, Version: x64, Date published: Not specified, Help document: None, and Date Modified: 1/14/2014. The REQUIREMENTS tab lists requirements such as Restart required: Might be required, Download size: 825 MB, Estimated time: Not specified, and Total components: 1. The DESCRIPTION tab notes the application was created by Prajwal Desai. A blue "UNINSTALL" button is located at the bottom right of this section. The watermark "©PrajwallDesai.com" is visible across the bottom of the interface.

NAME	TYPE	PUBLISHER	AVAILABL...	STATUS
Microsoft Office Professional Plus...	Application	Microsoft	1/14/2014	Installed

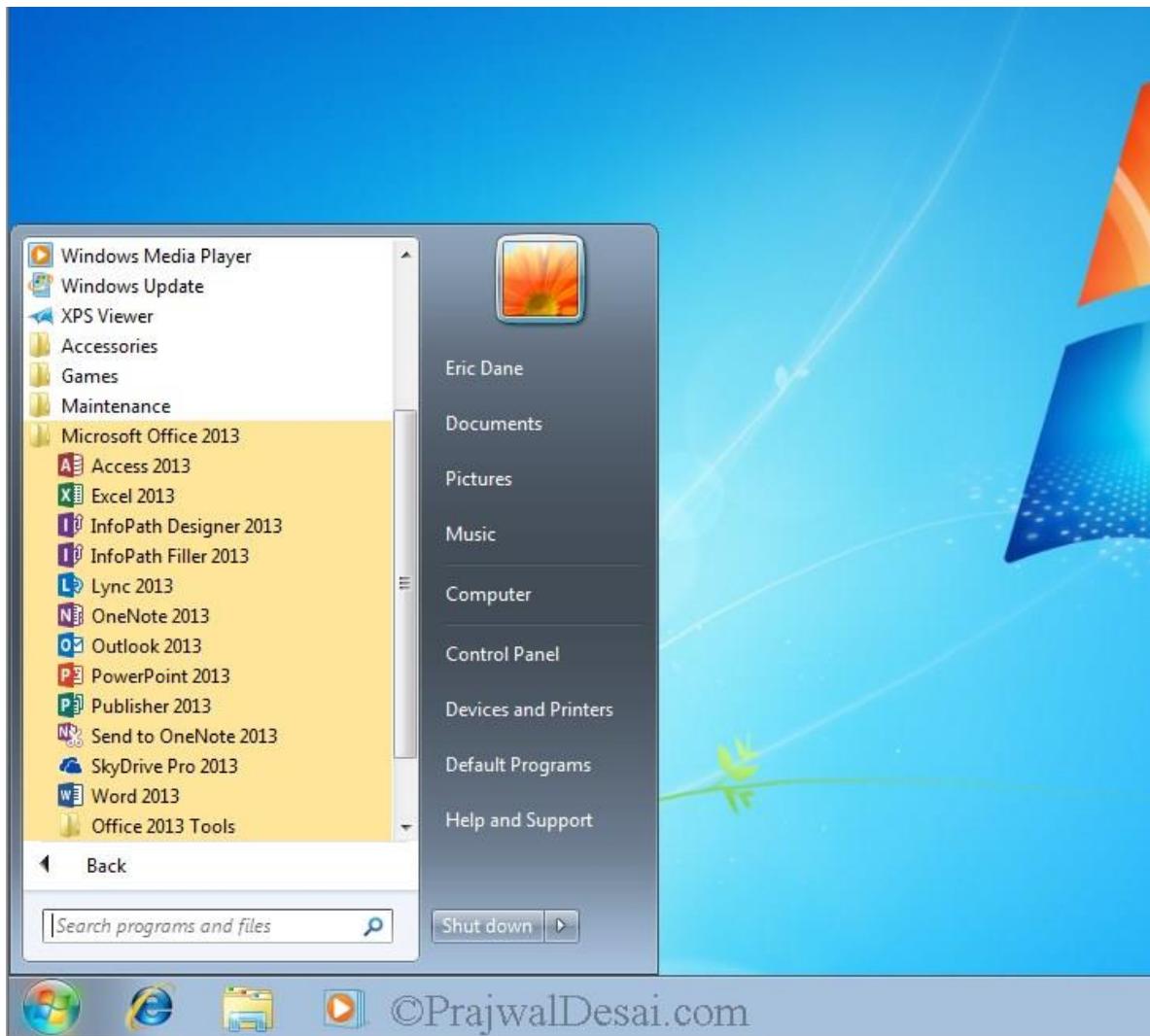
Microsoft Office Professional Plus 2013

OVERVIEW		REQUIREMENTS		DESCRIPTION
Status:	Installed	Restart required:	Might be required	Application Created by - Prajwal Desai
Version:	x64	Download size:	825 MB	
Date published:	Not specified	Estimated time:	Not specified	
Help document:	None	Total components:	1	
Date Modified:	1/14/2014			

UNINSTALL

©PrajwallDesai.com

On the client machine we see **Microsoft Office 2013** as installed program.



Lets try uninstalling the Office 2013 suite, to uninstall the app click on **Uninstall**. You will see the status as **Removing**. Since we had configured the uninstall command for this application, the uninstall process goes smoothly.

Software Center

Available Software Installation Status Installed Software Options

SHOW All Find additional applications

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
Microsoft Office Professional Plus 2013	Application		1/15/2014	Removing

Microsoft Office Professional Plus 2013

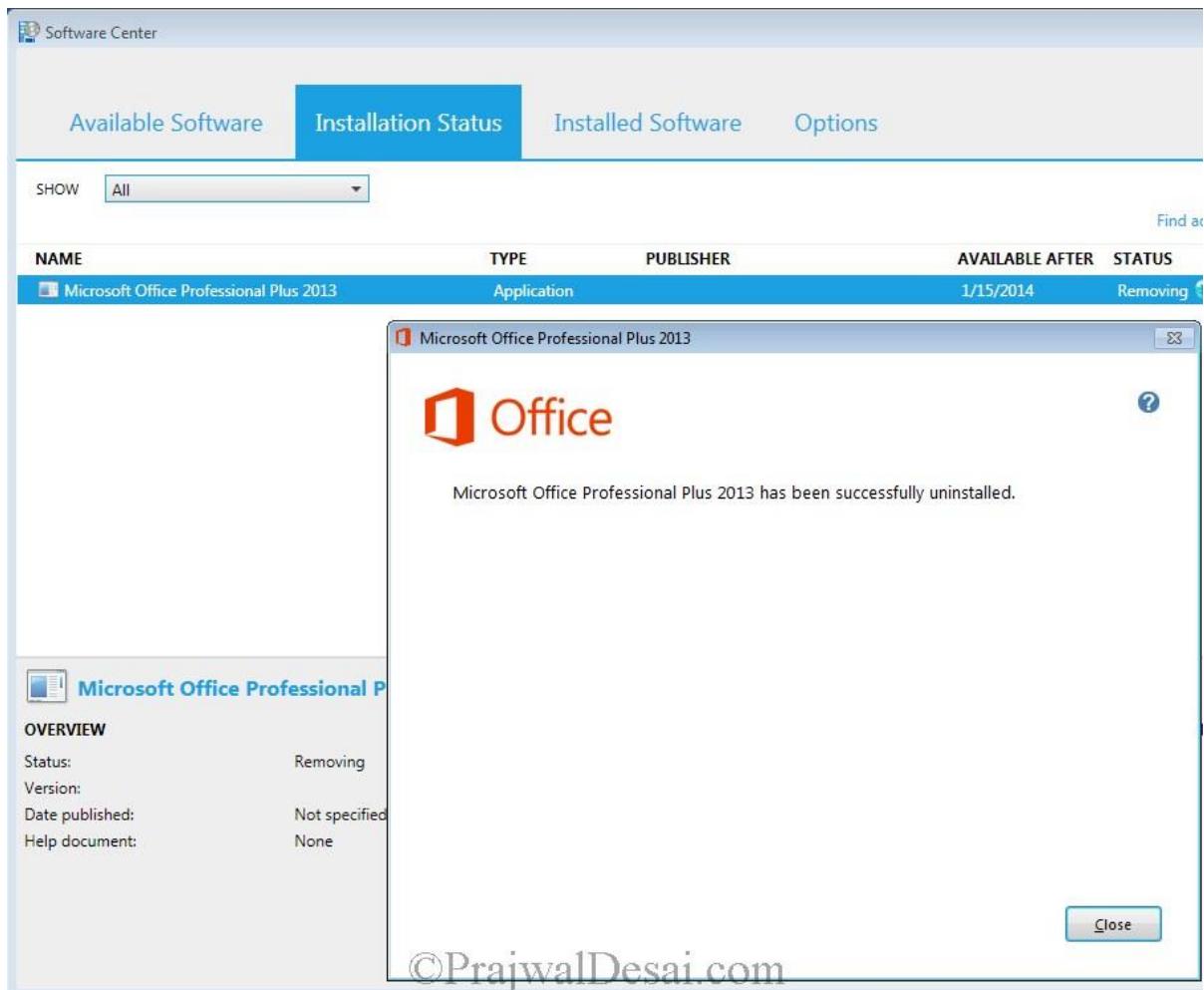
Uninstall Progress

Uninstalling Microsoft Office Professional Plus 2013...

OVERVIEW

Status:	Removing
Version:	
Date published:	Not specified
Help document:	None

Finally we see that Microsoft Office Professional Plus 2013 has been successfully uninstalled. You can again install the application if you need it.

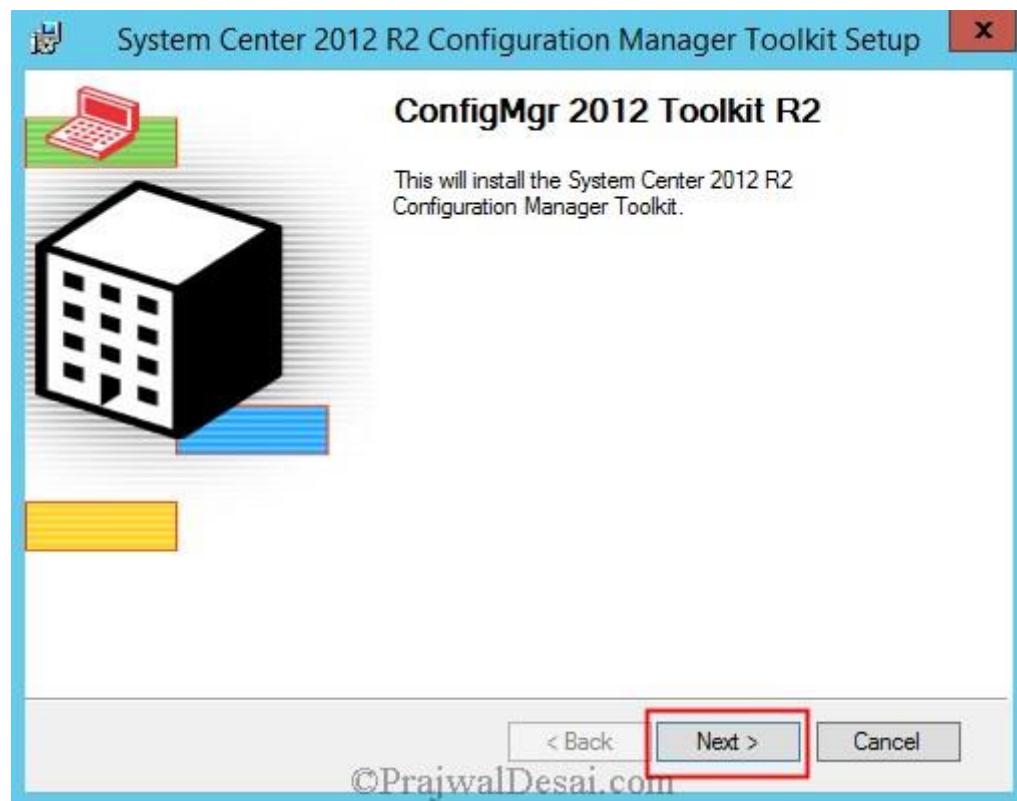


[System Center 2012 R2 Configuration Manager Toolkit](#)

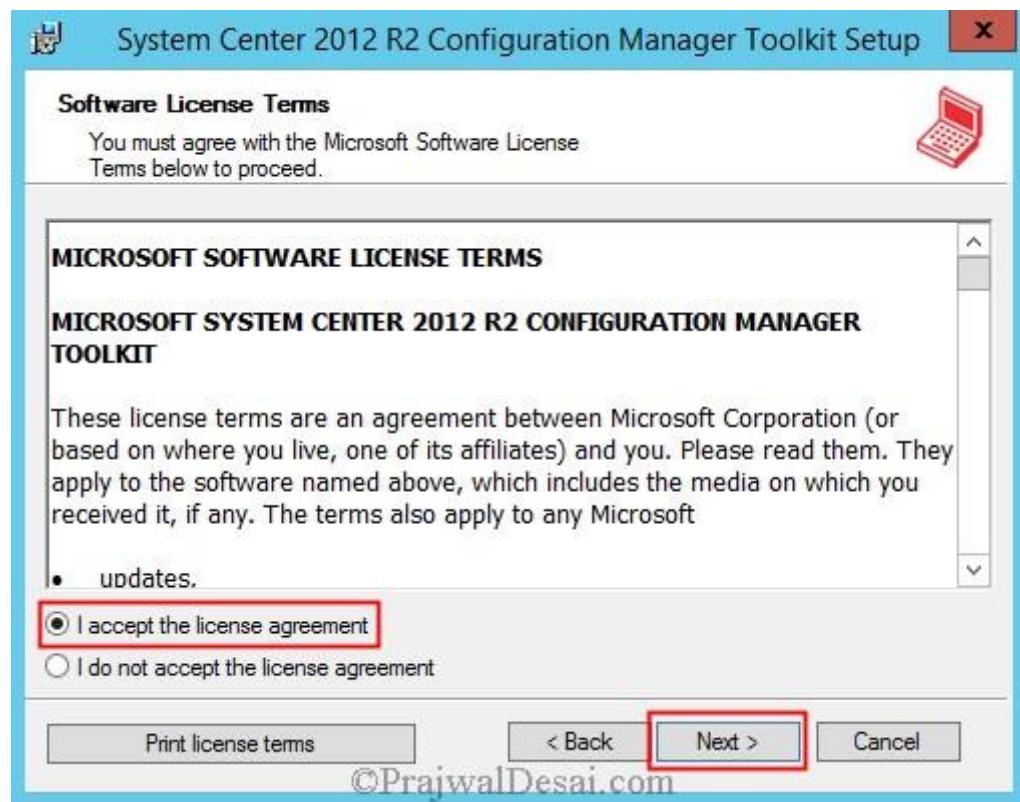
System Center 2012 R2 Configuration Manager toolkit was most awaited software and this time toolkit contains fifteen downloadable tools to help you manage and troubleshoot Microsoft System Center 2012 R2 Configuration Manager. It's not mandatory to install these tools however these tools are very good for troubleshooting issues related to SCCM 2012 R2. The tools are classified into two types- **Server Based Tools** and **Client Based Tools**. In this post we will be taking a look at all these tools briefly and understand what each tool does, we will see the details about all the tools in my coming posts. You can also refer to my SCCM 2012 R2 step by step guides [here](#). Click on the below button to download System Center 2012 R2 Configuration Manager Toolkit.

System Center 2012 R2 Configuration Manager Toolkit

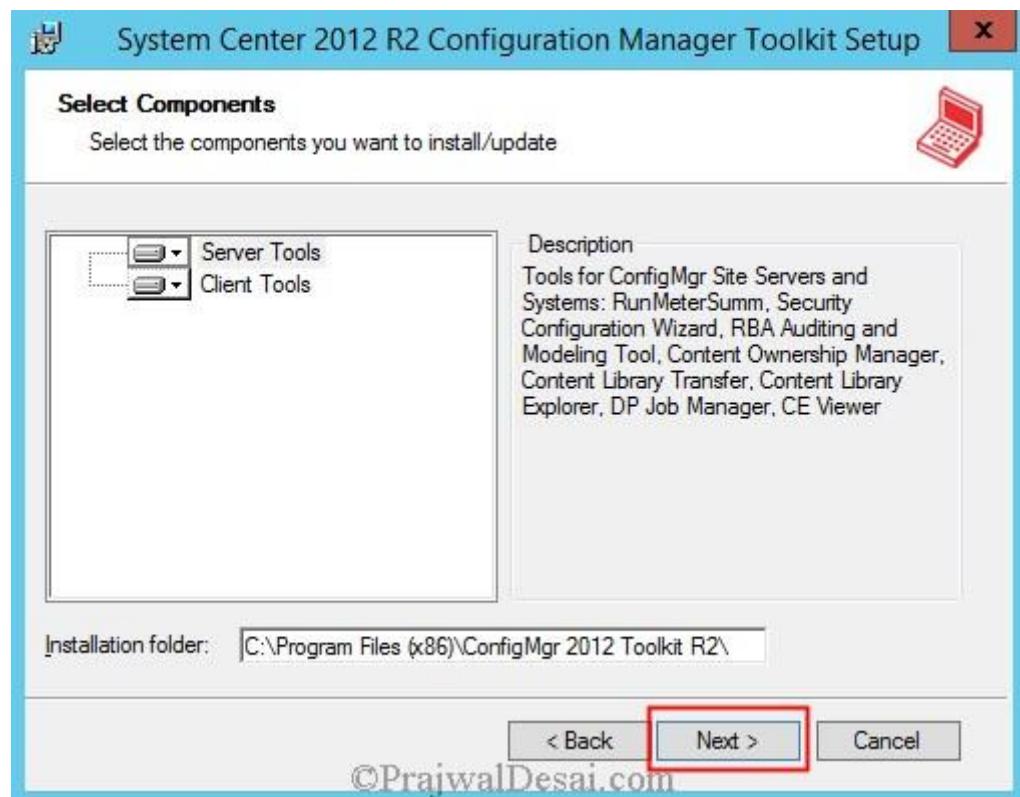
To install the System Center 2012 R2 Configuration Manager Toolkit (I am installing the System Center 2012 R2 Configuration Manager Toolkit on my SCCM box), click the Download button, and download **ConfigMgrTools.msi**. Run **ConfigMgrTools.msi** to install the System Center 2012 R2 Configuration Manager Toolkit. Click **Next**.



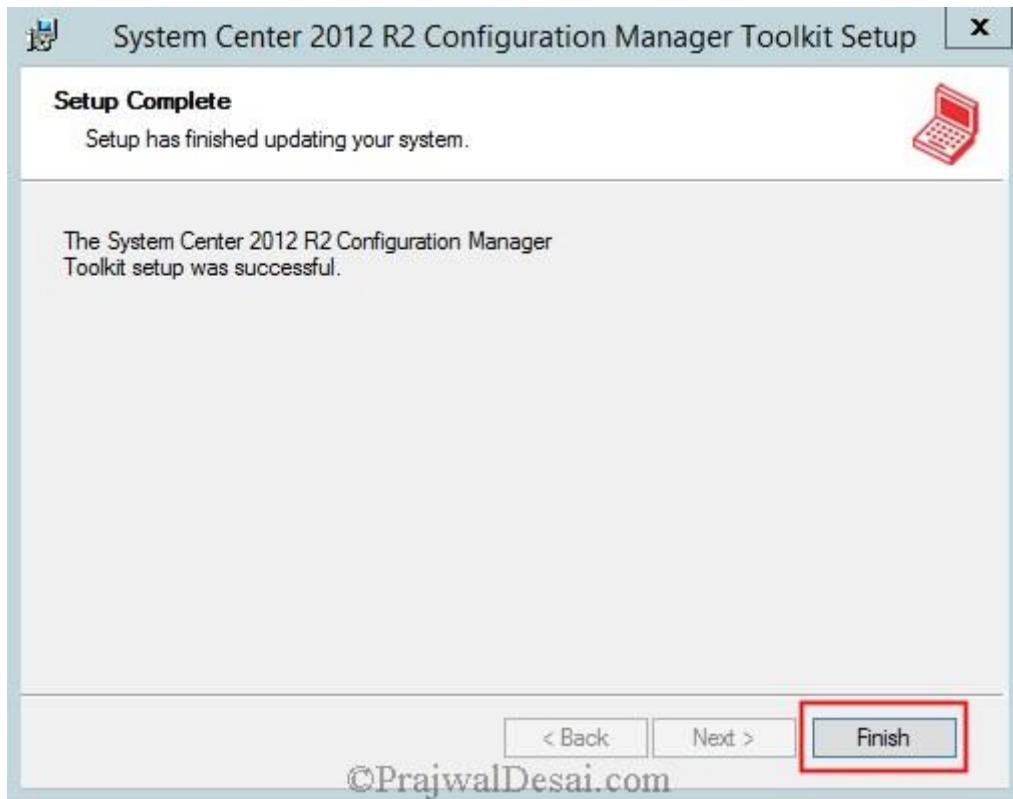
Accept the license agreement and click **Next**.



Make a note of the installation folder and click **Next**.

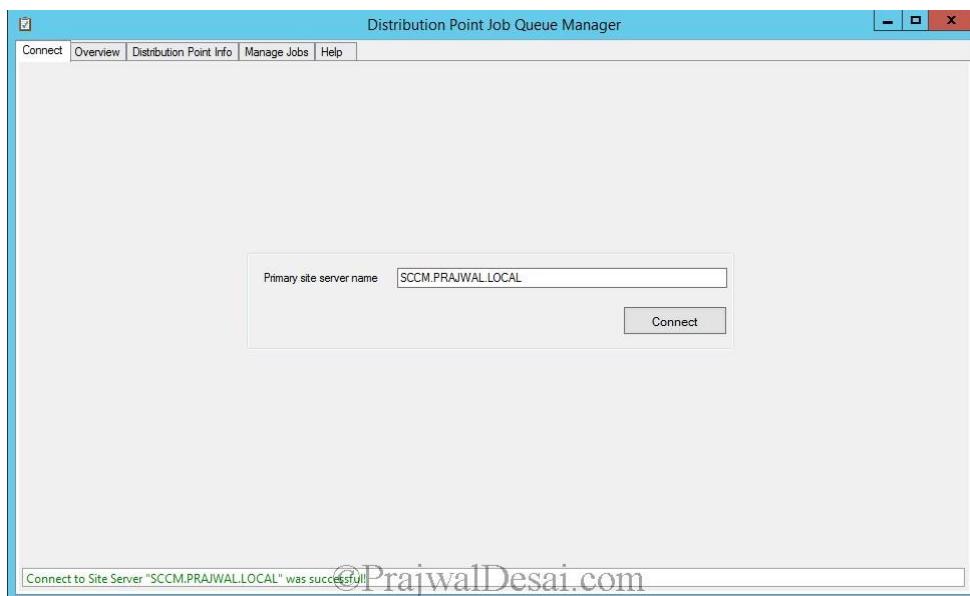


System Center 2012 R2 Configuration Manager Toolkit has been installed now. Click **Finish**.

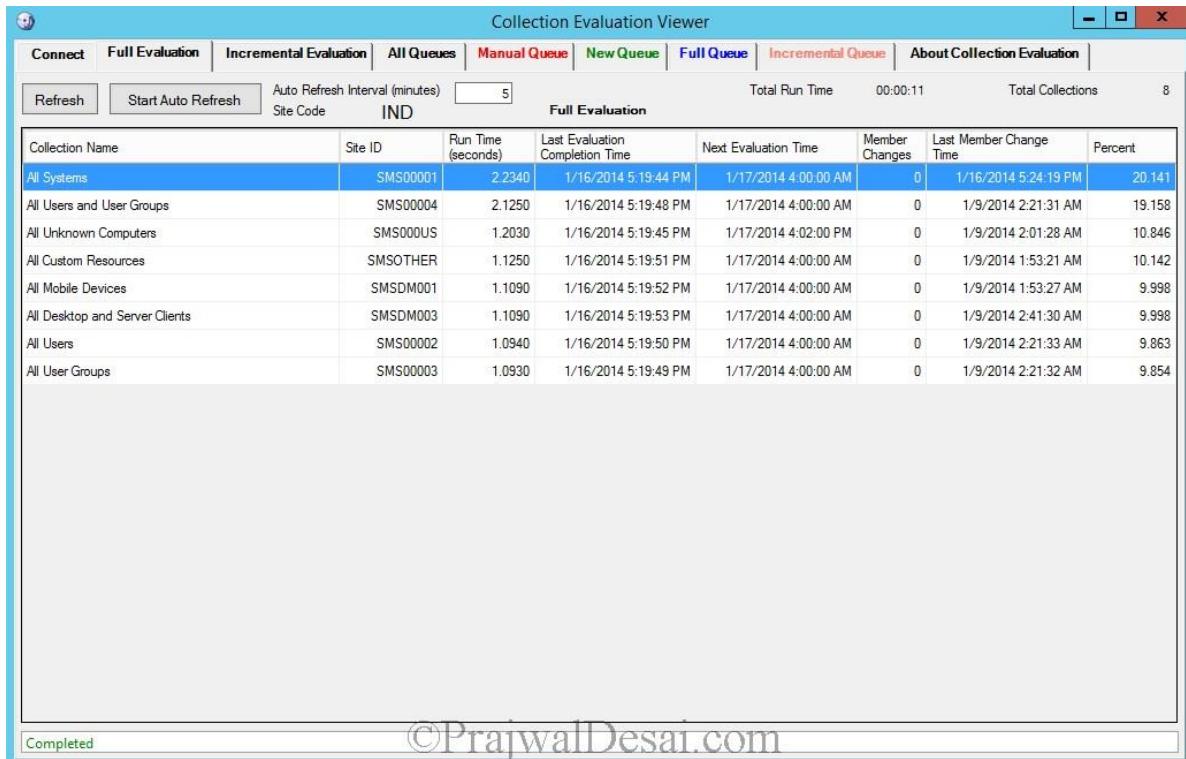


Server Based Tools

DP Job Manager – A tool that helps troubleshoot and manage ongoing content distribution jobs to Configuration Manager distribution points. (Requires Microsoft System Center 2012 R2 Configuration Manager for full functionality). The tool displays the list of jobs that the package transfer manager component has in its queue as well as the status of the jobs (ready to be executed, running or retrying). The tool also allows manipulation of the jobs in the queue, moving jobs higher on the list, cancelling or even kick start running a job manually.



Collection Evaluation Viewer – A tool that assists in troubleshooting collection evaluation related issues by viewing collection evaluation details (Requires Microsoft System Center 2012 R2 Configuration Manager for full functionality). The collection evaluation process runs by evaluating the membership rules of a collection to update its members. The tool displays both historic and live information for full and incremental collection evaluations and the evaluation queue status. It will provide information on the time for collection evaluations to complete, which collections are currently being evaluated, and the estimated time that a collection evaluation will start and complete.



The screenshot shows the 'Collection Evaluation Viewer' window. At the top, there's a menu bar with 'Connect', 'Full Evaluation', 'Incremental Evaluation', 'All Queues', 'Manual Queue' (which is selected), 'New Queue', 'Full Queue', 'Incremental Queue', and 'About Collection Evaluation'. Below the menu is a toolbar with 'Refresh', 'Start Auto Refresh', 'Auto Refresh Interval (minutes)' set to 5, and a 'Site Code' dropdown set to 'IND'. The main area is titled 'Full Evaluation' and contains a table with the following data:

Collection Name	Site ID	Run Time (seconds)	Last Evaluation Completion Time	Next Evaluation Time	Member Changes	Last Member Change Time	Percent
All Systems	SMS00001	2.2340	1/16/2014 5:19:44 PM	1/17/2014 4:00:00 AM	0	1/16/2014 5:24:19 PM	20.141
All Users and User Groups	SMS00004	2.1250	1/16/2014 5:19:48 PM	1/17/2014 4:00:00 AM	0	1/9/2014 2:21:31 AM	19.158
All Unknown Computers	SMS000US	1.2030	1/16/2014 5:19:45 PM	1/17/2014 4:02:00 PM	0	1/9/2014 2:01:28 AM	10.846
All Custom Resources	SMSOTHER	1.1250	1/16/2014 5:19:51 PM	1/17/2014 4:00:00 AM	0	1/9/2014 1:53:21 AM	10.142
All Mobile Devices	SMSDM001	1.1090	1/16/2014 5:19:52 PM	1/17/2014 4:00:00 AM	0	1/9/2014 1:53:27 AM	9.998
All Desktop and Server Clients	SMSDM003	1.1090	1/16/2014 5:19:53 PM	1/17/2014 4:00:00 AM	0	1/9/2014 2:41:30 AM	9.998
All Users	SMS00002	1.0940	1/16/2014 5:19:50 PM	1/17/2014 4:00:00 AM	0	1/9/2014 2:21:33 AM	9.863
All User Groups	SMS00003	1.0930	1/16/2014 5:19:49 PM	1/17/2014 4:00:00 AM	0	1/9/2014 2:21:32 AM	9.854

At the bottom left, there's a 'Completed' button, and at the bottom right, the text '©PrajwallDesai.com'.

Content Library Explorer – A tool that assists in troubleshooting issues with and viewing the contents of the content library (Requires Microsoft System Center 2012 R2 Configuration Manager for full functionality). This tool can be used to troubleshoot issues with the content library, as well as explore its contents. Using the tool, packages, contents, folders, and files can all be copied out of the content library. Packages can be redistributed to the distribution point, and on remote distribution points, packages can be validated. This tool must be run using an account that has administrative access to the target distribution point, as well as access to the WMI provider on the site server and the Configuration Manager provider.

The screenshot shows the SCCM Content Library Explorer window. The left pane displays a hierarchical tree of content libraries, with one library expanded to show its contents. The right pane is a grid view showing a list of files with columns for Name, Size (bytes), Drive, Time Modified, and Shared With.

File	Size (bytes)	Drive	Time Modified	Shared With
ABCPY.INI	625	E:	9/24/2012 9:13:40 AM	
AcroRead.msi	2,385,920	E:	9/24/2012 9:17:27 AM	
Data1.cab	129,304,692	E:	9/24/2012 9:17:54 AM	
setup.exe	364,224	E:	9/24/2012 9:17:39 AM	
Setup.ini	292	E:	9/24/2012 9:13:38 AM	

Security Configuration Wizard Template for Microsoft System Center 2012 R2

Configuration Manager – The Security Configuration Wizard (SCW) is an attack-surface reduction tool for the Microsoft Windows Server 2008 R2 operating system. Security Configuration Wizard determines the minimum functionality required for a server's role or roles, and disables functionality that is not required.

Content Library Transfer – A tool that transfers content from one disk drive to another. The tool is useful for the scenario when the disk drive hosting the content library becomes full.

After a hard disk is installed with sufficient space to host the content library,

ContentLibraryTransfer.exe is used transfer content from the old filled hard disk to the new (empty) drive. Once the transfer is complete, content is now accessible to client computers from the new location without admin intervention.

The syntax of the command is **ContentLibraryTransfer.exe –SourceDrive <drive letter of source drive> –TargetDrive <drive letter of destination drive>**

```
Windows - Select Administrator: Command Prompt
CLT:01/16/2014 22:28:20 Deleting Old Content
CLT:01/16/2014 22:28:20 ****
CLT:01/16/2014 22:28:20 WARN: Deleting Old Content. This change cannot be reversed.
CLT:01/16/2014 22:28:20 ****
CLT:01/16/2014 22:28:20 Deleting C:\SMSSIG$
CLT:01/16/2014 22:28:20 Deleting C:\SMSPKG$C
CLT:01/16/2014 22:28:20 Deleting C:\SMSPKG$SIG
CLT:01/16/2014 22:28:20 Deleting C:\SMSPKG
CLT:01/16/2014 22:28:20 Deleting C:\SCCMContentLib
CLT:01/16/2014 22:28:20 Deleting Old Content Complete
CLT:01/16/2014 22:28:20
CLT:01/16/2014 22:28:20 Updating Virtual Directories
CLT:01/16/2014 22:28:21 Virtual Directories Update Complete
CLT:01/16/2014 22:28:21 Executing Transfer: Completed Successfully
CLT:01/16/2014 22:28:21 Verifying Transfer: Check if the transfer was successful
CLT:01/16/2014 22:28:21 Verifying Transfer: Completed Successfully
CLT:01/16/2014 22:28:21 ****
CLT:01/16/2014 22:28:21
CLT:01/16/2014 22:28:21 Content Library Transfer is now complete !!
CLT:01/16/2014 22:28:21 ****
C:\Program Files (x86)\ConfigMgr_2012 Toolkit_R2\ServerTools>
```

Content Ownership Tool – A tool that changes ownership of orphaned packages (packages without an owner site server). Orphaned packages are packages without an owner site server. Packages that are created at a site can become orphaned by removing the site server while they are still owned by this site server. You can select the package and change the site ownership of the package.

ContentOwnership Tool

Content Ownership Manager

Select one or more packages that you want to assign to a new site. After this tool transfers ownership of a package to a new site, the new site is responsible for monitoring the package source files. A change of site ownership for a package does not cause the package to update on distribution points and does not cause clients to re-evaluate policy for deployments of the package.

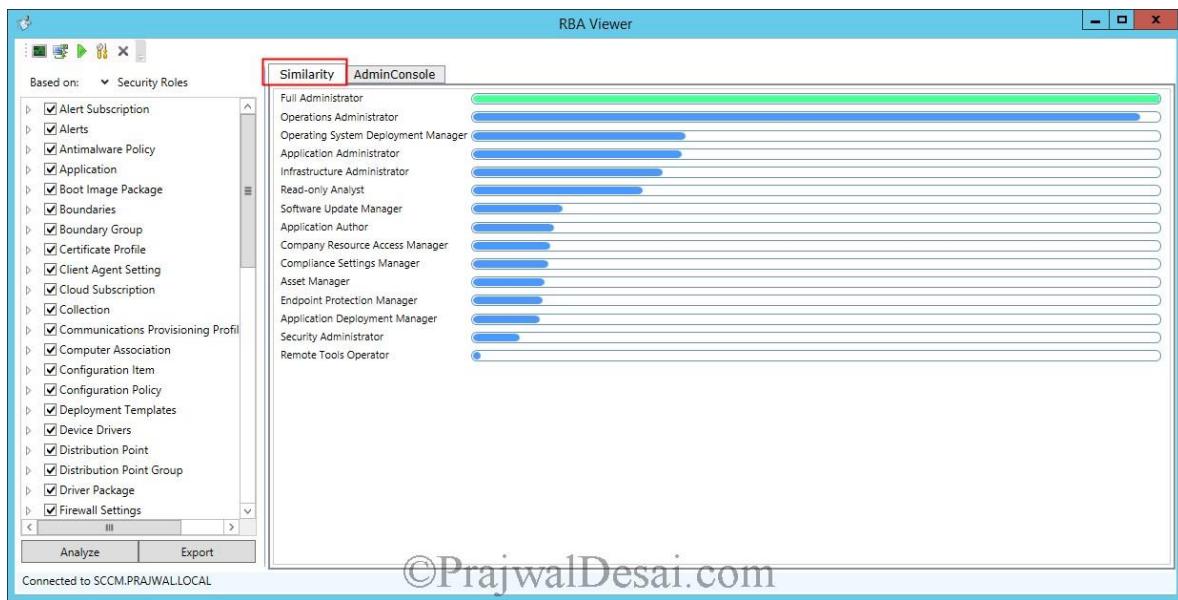
Package Name	Site Code	Type			
Search by:	AND IND	AND All			
<input type="radio"/> Only orphaned packages <input checked="" type="radio"/> All Packages					
Package Name	Site Code	Package ID	Type	Size (MB)	
User State Migration Tool for Windows 8	IND	IND00001	SMS_Package	48.66	C:\Program Files (x86)\Windows\
KB 2905002 - console update - IND	IND	IND00006	SMS_Package	2.07	\SSCCM.PRAJWAL.LOCAL\SMS_IN
KB 2905002 - x86 client update - IND	IND	IND00007	SMS_Package	0.81	\SSCCM.PRAJWAL.LOCAL\SMS_IN
KB 2905002 - x64 client update - IND	IND	IND00008	SMS_Package	0.97	\SSCCM.PRAJWAL.LOCAL\SMS_IN
KB 2905002 - server update - IND	IND	IND00009	SMS_Package	28.96	\SSCCM.PRAJWAL.LOCAL\SMS_IN
Winrar	IND	IND0000D	SMS_Package	0	\sccm\Deployment\Winrar v4.20
Windows 7 Professional Service Pack 1	IND	IND0000A	SMS_ImagePackage	2729.81	\sccm\Deployment\Capture_OS\
Boot image (x86)	IND	IND00002	SMS_BootImagePackage	171.02	\SSCCM.PRAJWAL.LOCAL\SMS_IN
Boot image (x64)	IND	IND00005	SMS_BootImagePackage	208.92	\SSCCM.PRAJWAL.LOCAL\SMS_IN
<input checked="" type="checkbox"/> Adobe Reader XI	IND	IND0000C	SMS_ContentPackage	125.94	\sccm\Deployment\Adobe

Specify site ownership to assign a new site that will manage the packages that you have selected. The site server computer of the site you specify must be able to access the source files for each package, and requires Read permission to the source files of each package.

Change Site ownership to: IND - Bangalore Headquarters Site View Log

Connected to Site IND ©PrajwalDesai.com

Role-based Administration Modeling and Auditing Tool – This tool helps administrators to model and audit RBA configurations. With this tool you can select the **Run As** button in toolbar tray. You can input the specific user name to check the permissions for that user account. You will see the security roles assigned to the user or the security group the user belongs to.



©PrajwalDesai.com

Run Metering Summarization Tool – The purpose of this tool is to run the metering summarization task to analyze raw metering data. The **RunMeterSumm** tool is used to trigger Metering Summarization immediately on Primary Sites, by default it's running as scheduled in Site Maintenance tasks, which start after 12:00AM every day. These tasks summarize the data in table MeterData, and write the summary result into the tables **FileUsageSummary** and **MonthlyUsageSummary**, so the user can see the summarized result in metering reports. The administrator who can connect to the primary site database can use this tool to run summarization.

```

Administrator: Tools Command Prompt

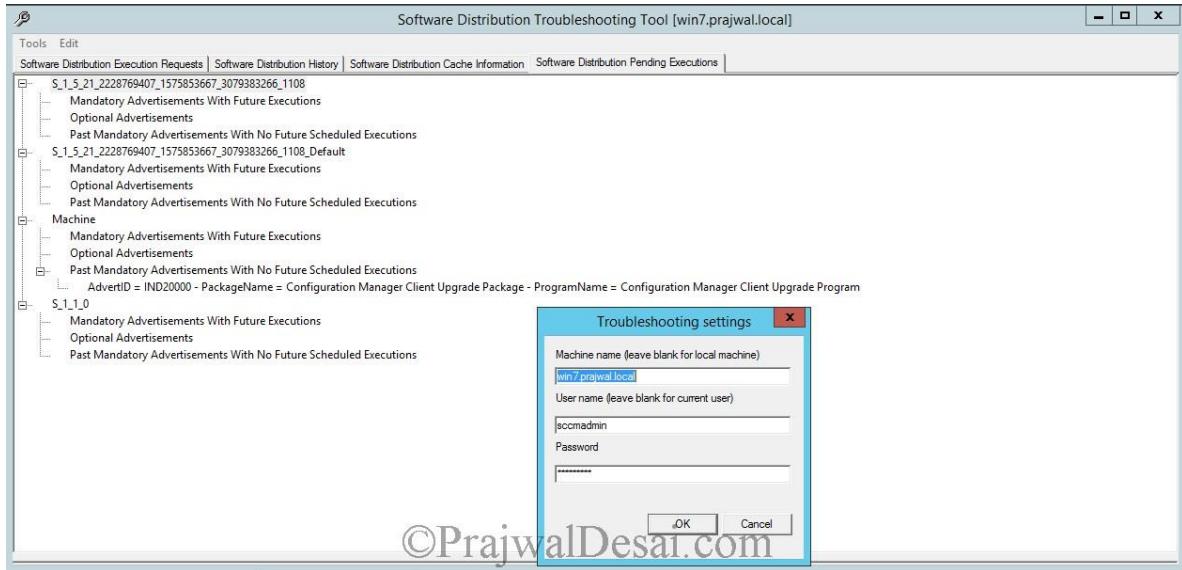
C:\Program Files (x86)\ConfigMgr 2012 Toolkit R2\ServerTools>runmetersumm.exe CM_LND
Logging is turned off, turn on logging for the SMS_SQL_MONITOR component for more detail.
Summarizing data up to 0 hours old.
File Usage Summary added 0 rows in 0 seconds.
Monthly Usage Summary added 0 rows in 0 seconds.

C:\Program Files (x86)\ConfigMgr 2012 Toolkit R2\ServerTools>

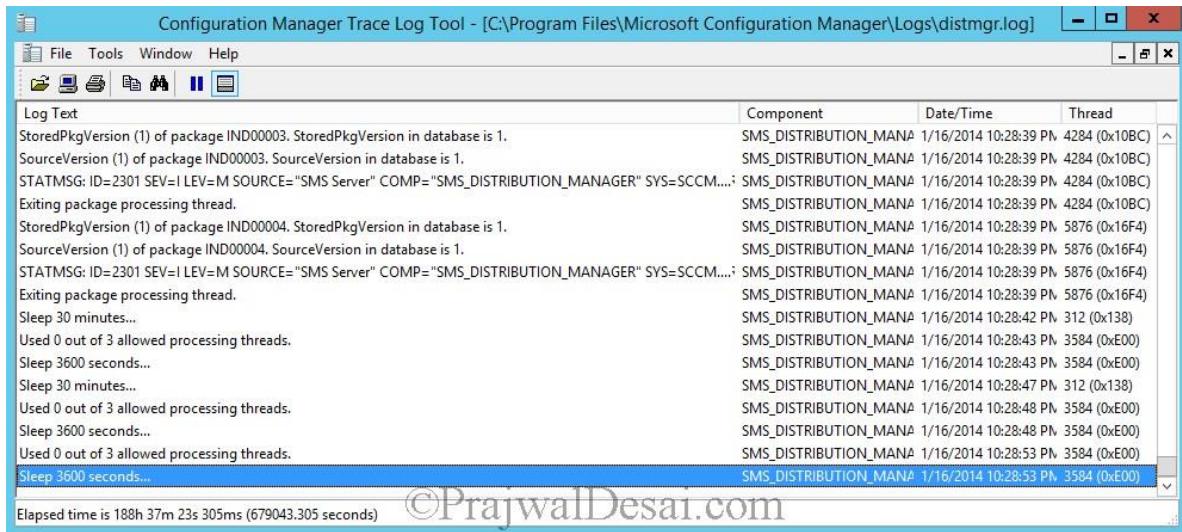
```

Client Based Tools

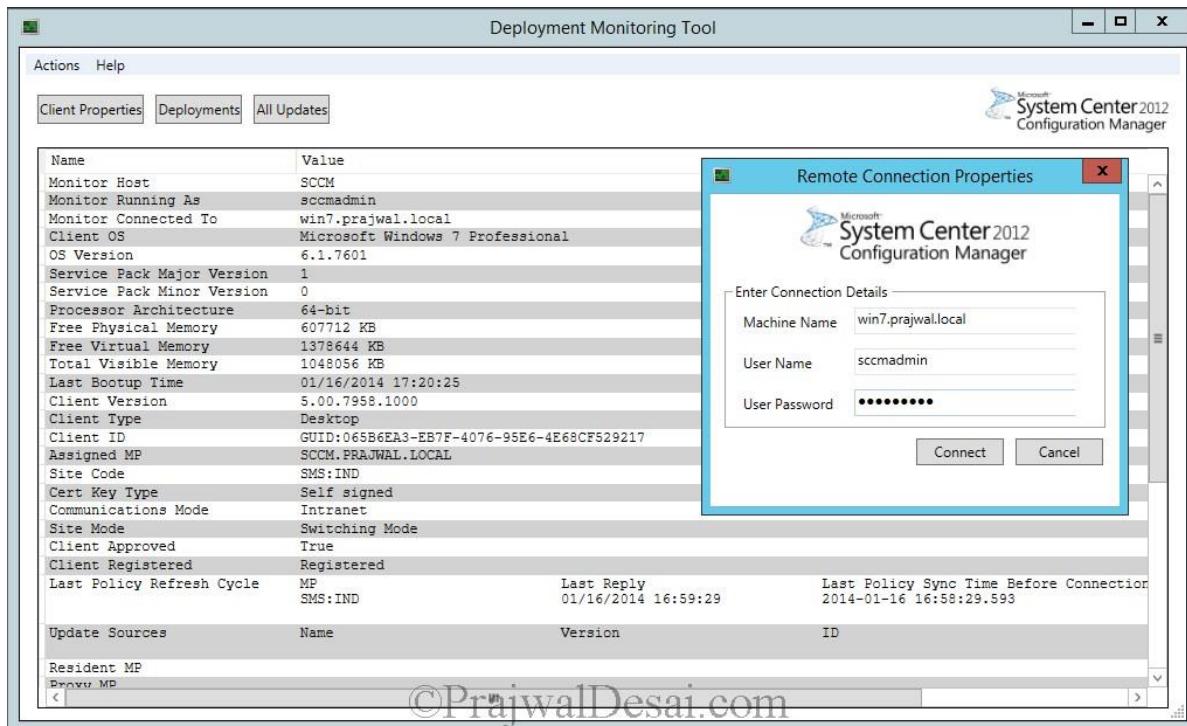
Client Spy – A tool that helps you troubleshoot issues related to software distribution, inventory, and software metering on System Center 2012 Configuration Manager clients. Click on **Tools** and click **connect**. You can connect it to a remote machine and troubleshoot issues related to software distribution, inventory, and software metering.



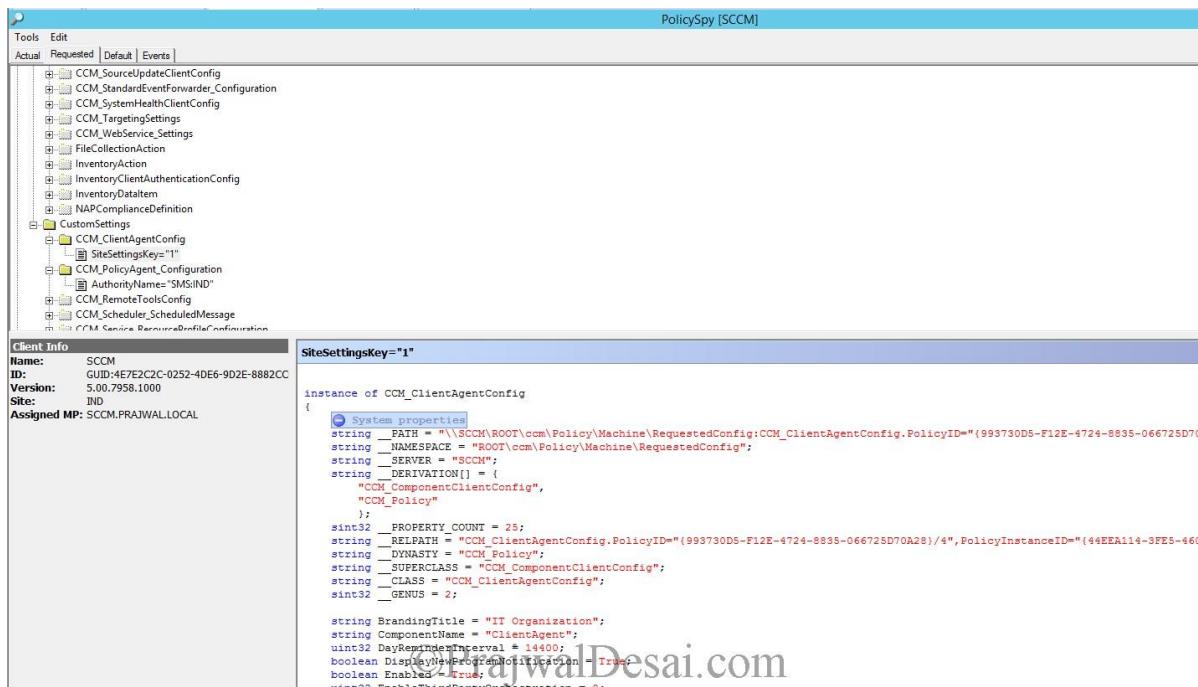
Configuration Manager Trace Log Viewer – A tool used to view log files created by Configuration Manager components and agents. Most of you would have used this tool and I must say its an excellent log file viewer till date.



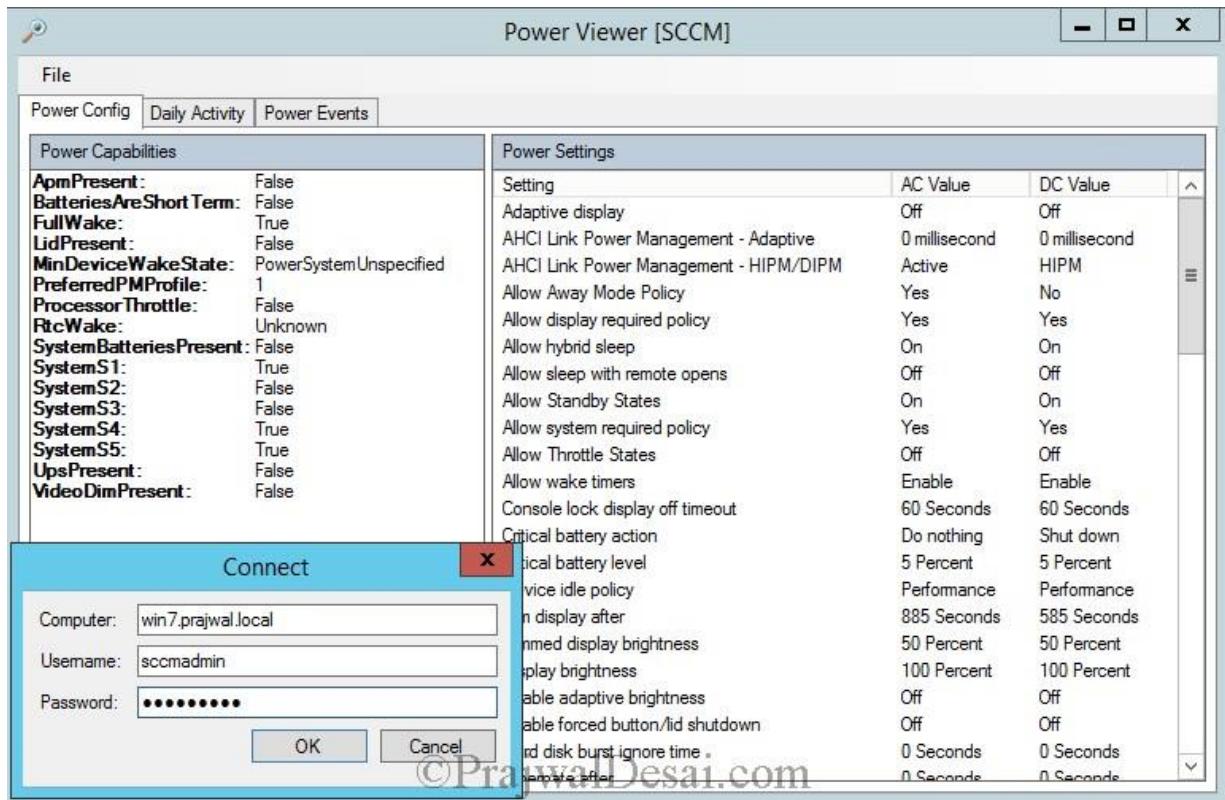
Deployment Monitoring Tool – The Deployment Monitoring Tool is a graphical user interface designed help troubleshoot Applications, Updates, and Baseline deployments on System Center 2012 Configuration Manager clients. To connect to remote machine, click on **Actions** and click on **Connect to Remote Machine**, type the machine name, user name and password. The tool is **read only** it does not change any state on the client and can be safely used to diagnose common deployment scenarios.



Policy Spy – A policy viewer that helps you review and troubleshoot the policy system on System Center 2012 Configuration Manager clients. This tool must be run as administrator.



Power Viewer Tool – A tool to view the status of power management feature on System Center 2012 Configuration Manager clients. You must run this tool as administrator, when you launch this tool it will display the power settings and capabilities data of local computer. You can connect to a remote computer and view the power management data.



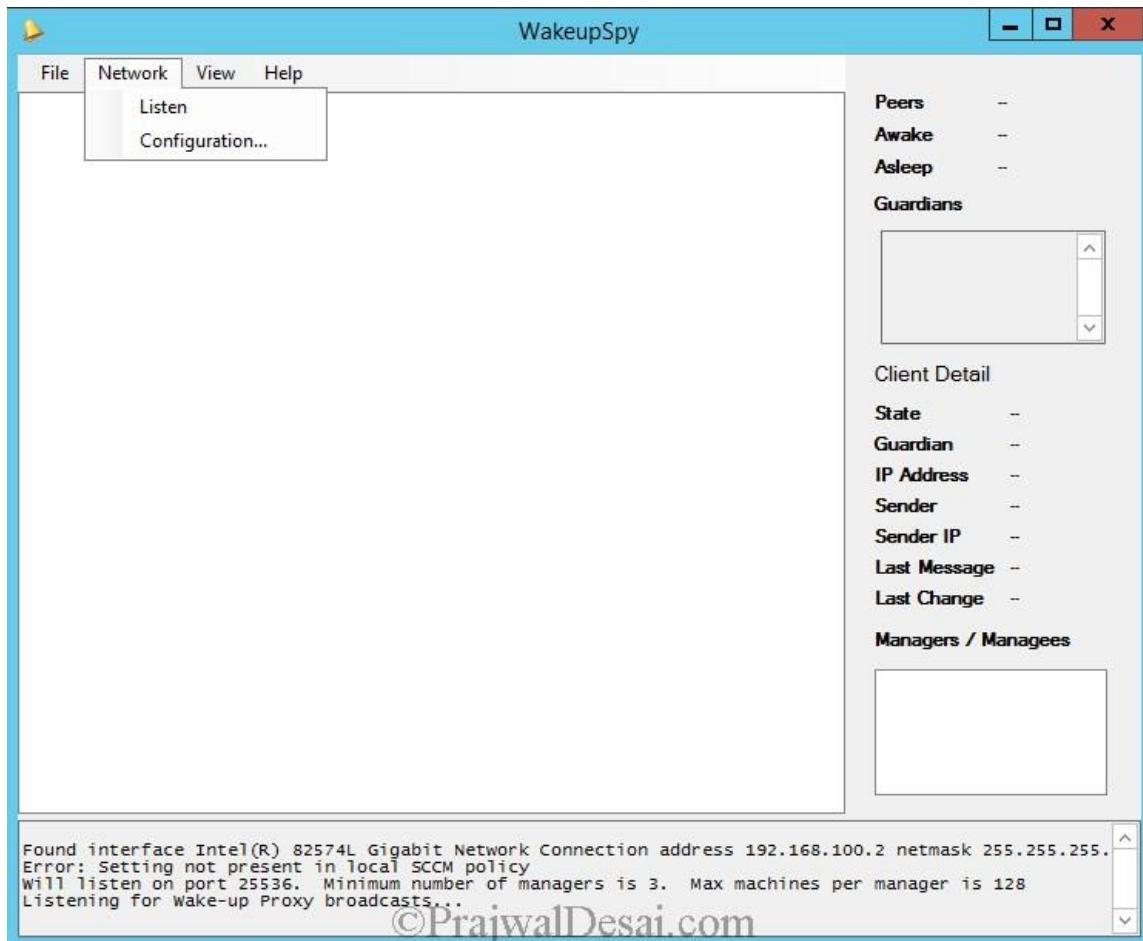
Send Schedule Tool – A tool used to trigger a schedule on a client or trigger the evaluation of a specified DCM Baseline. You can trigger a schedule either locally or remotely. This tool must be run as administrator.

```

Administrator: Command Prompt
C:\>Program Files (<x86>)\ConfigMgr 2012 Toolkit R2\ClientTools>SendSchedule.exe /L
SCCM.PRAJWAL.LOCAL
*****
Show Available Message GUID:
Message GUID: {ND20000-0000-0000-0000-000000000001} DisplayName: Hardware Inventory
Message GUID: {00000000-0000-0000-0000-000000000002} DisplayName: Software Inventory
Message GUID: {00000000-0000-0000-0000-000000000003} DisplayName: Discovery Inventory
Message GUID: {00000000-0000-0000-0000-000000000010} DisplayName: File Collection
Message GUID: {00000000-0000-0000-0000-000000000021} DisplayName: Request Machine Assignments
Message GUID: {00000000-0000-0000-0000-000000000022} DisplayName: Evaluate Machine Policies
Message GUID: {00000000-0000-0000-0000-000000000023} DisplayName: Refresh Default MP Task
Message GUID: {00000000-0000-0000-0000-000000000024} DisplayName: LS <Location> Refresh Locations Task
Message GUID: {00000000-0000-0000-0000-000000000025} DisplayName: LS <Location> Timeout Refresh Task
Message GUID: {00000000-0000-0000-0000-000000000031} DisplayName: Software Metering Generating Usage Report
Message GUID: {00000000-0000-0000-0000-000000000032} DisplayName: Source Update Message
Message GUID: {00000000-0000-0000-0000-000000000040} DisplayName: Machine Policy Agent Cleanup
Message GUID: {00000000-0000-0000-0000-000000000042} DisplayName: Policy Agent Validate Machine Policy / Assignment
Message GUID: {00000000-0000-0000-0000-000000000051} DisplayName: Retrying/Refreshing certificates in AD on MP
Message GUID: {00000000-0000-0000-0000-0000000000108} DisplayName: Software Updates Assignments Evaluation Cycle
Message GUID: {00000000-0000-0000-0000-0000000000111} DisplayName: Send Unseen

```

Wakeup Spy – A tool that provides a view of the power state of Configuration Manager client computers and which operate as managers or managed. The tool is useful to get an understanding of wake up traffic being generated and the current power status of client computers. It cannot be used to control the power state of computers.



How To Deploy Software Updates Using SCCM 2012 R2

How To Deploy Software Updates Using SCCM 2012 R2 In this post we will look at the steps on how to deploy software updates using SCCM 2012 R2. Deploying the software updates for the computers is essential, the software updates are released by major software vendors to address security vulnerabilities in their existing products. To stay protected against cyber-attacks and malicious threats it is very important that you keep the computers patched with latest software updates. Software updates in System Center 2012 R2 Configuration Manager provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to client computers in the enterprise. Talking about software updates, in SCCM 2012 R2 there are few new features added which includes a new maintenance window dedicated for software updates installation. This lets you configure a general maintenance window and a different maintenance window for software updates. When a general maintenance window and software updates maintenance window are both configured, clients install software updates only during the software updates maintenance window. A new feature called Software updates preview lets you review the software updates before you create the deployment.

How To Deploy Software Updates Using SCCM 2012 R2

In this post we will see the steps on how to deploy software updates using SCCM 2012 R2, if you are looking for SCCM 2012 R2 step by step guides click [here](#). There are 2 ways to deploy software updates using SCCM 2012 R2, **Manual** and **Automatic**. In Manual software updates deployment, a set of software updates is selected the Configuration Manager console and these updates are deployed to the target collection whereas Automatic software updates deployment is configured by using automatic deployment rules. This method is used for deploying monthly software updates and for managing definition updates. When the rule runs, the software updates that meet a specified criteria (for example, all security software updates released in the last week) are added to a software update group, the content files for the software updates are downloaded and copied to distribution points, and the software updates are deployed to client computers in the target collection. In this post we will see the steps to deploy the software updates manually and for automatic software updates deployment, there will be a separate post.

To start with, install the **Software Update Point** role first. Launch the **Configuration Manager** Console, click on **Administration**, expand **Overview**, click **Site Configuration**, click on **Sites**. At the top ribbon click on **Add Site System Roles**.

System Center 2012 R2 Configuration Manager (Connected to IND - Bangalore Headquarters Site)

Home

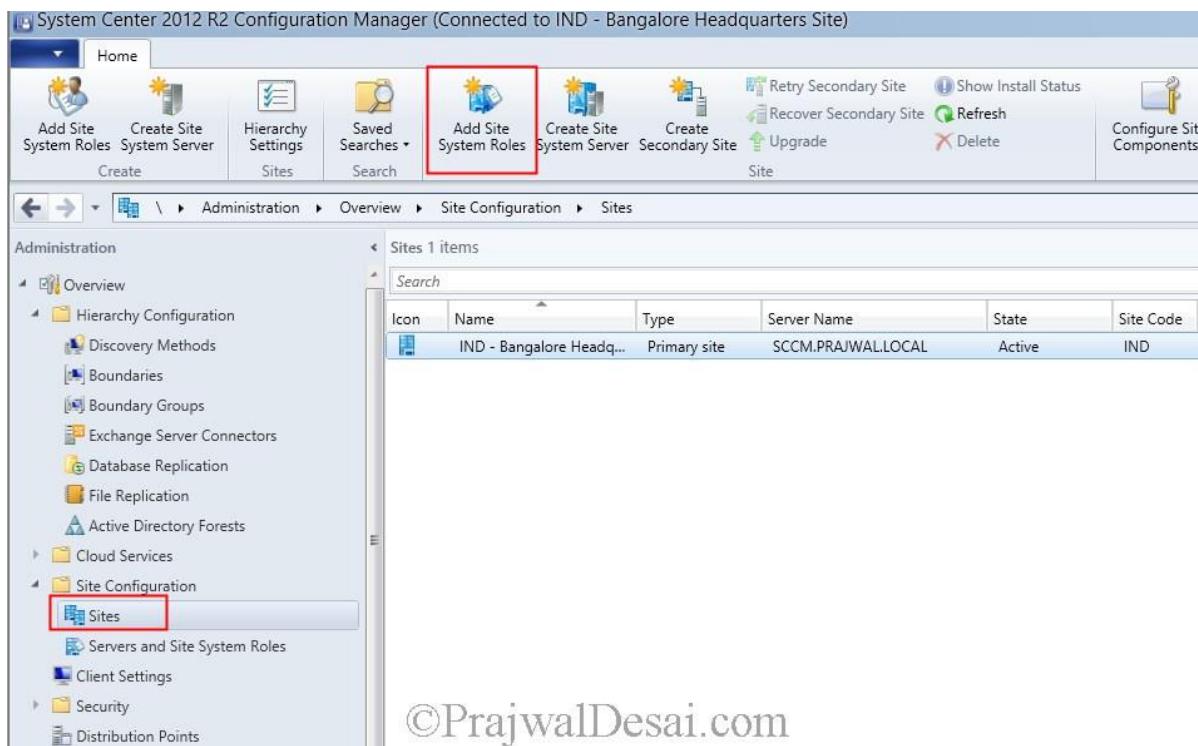
Add Site System Roles Create Site System Server Hierarchy Settings Saved Searches Add Site System Roles Create Site System Server Create Secondary Site Retry Secondary Site Show Install Status Refresh Configure Site Components

Administration \ Administration Overview Hierarchy Configuration Discovery Methods Boundaries Boundary Groups Exchange Server Connectors Database Replication File Replication Active Directory Forests Cloud Services Site Configuration Sites Servers and Site System Roles Client Settings Security Distribution Points

Sites 1 items

Icon	Name	Type	Server Name	State	Site Code
IND - Bangalore Headq...	Primary site	SCCM.PRAJWALLOCAL	Active	IND	

©PrajwalDesai.com



From the **Add Site System Roles Wizard**, click on **Software Update Point** and click **Next**.

Add Site System Roles Wizard

System Role Selection

General Proxy System Role Selection Software Update Point

Proxy and Account Settings Synchronization Source Synchronization Schedule Supersedence Rules Classifications Products Languages

Summary Progress Completion

Specify roles for this server

Available roles:

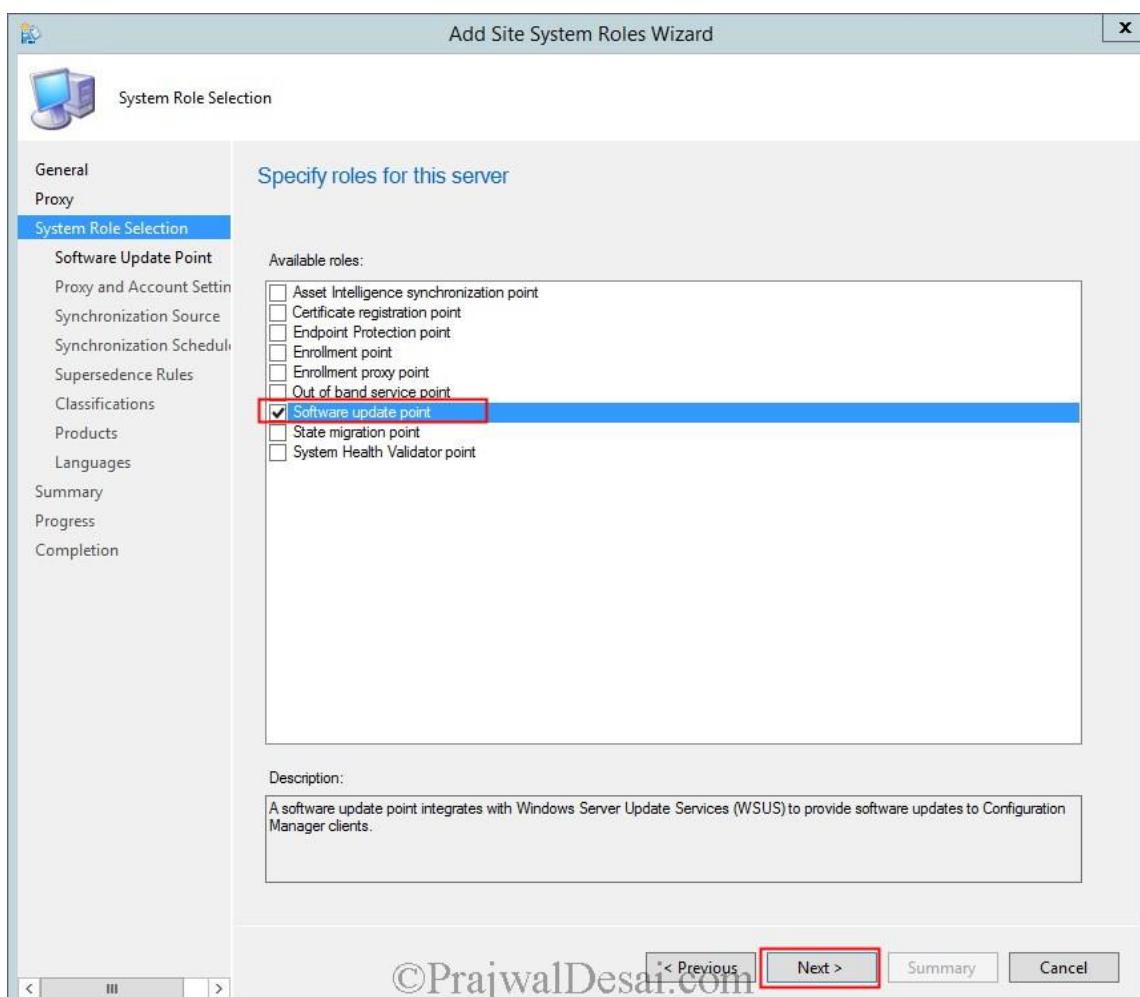
- Asset Intelligence synchronization point
- Certificate registration point
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Out of band service point
- Software update point
- State migration point
- System Health Validator point

Description:

A software update point integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients.

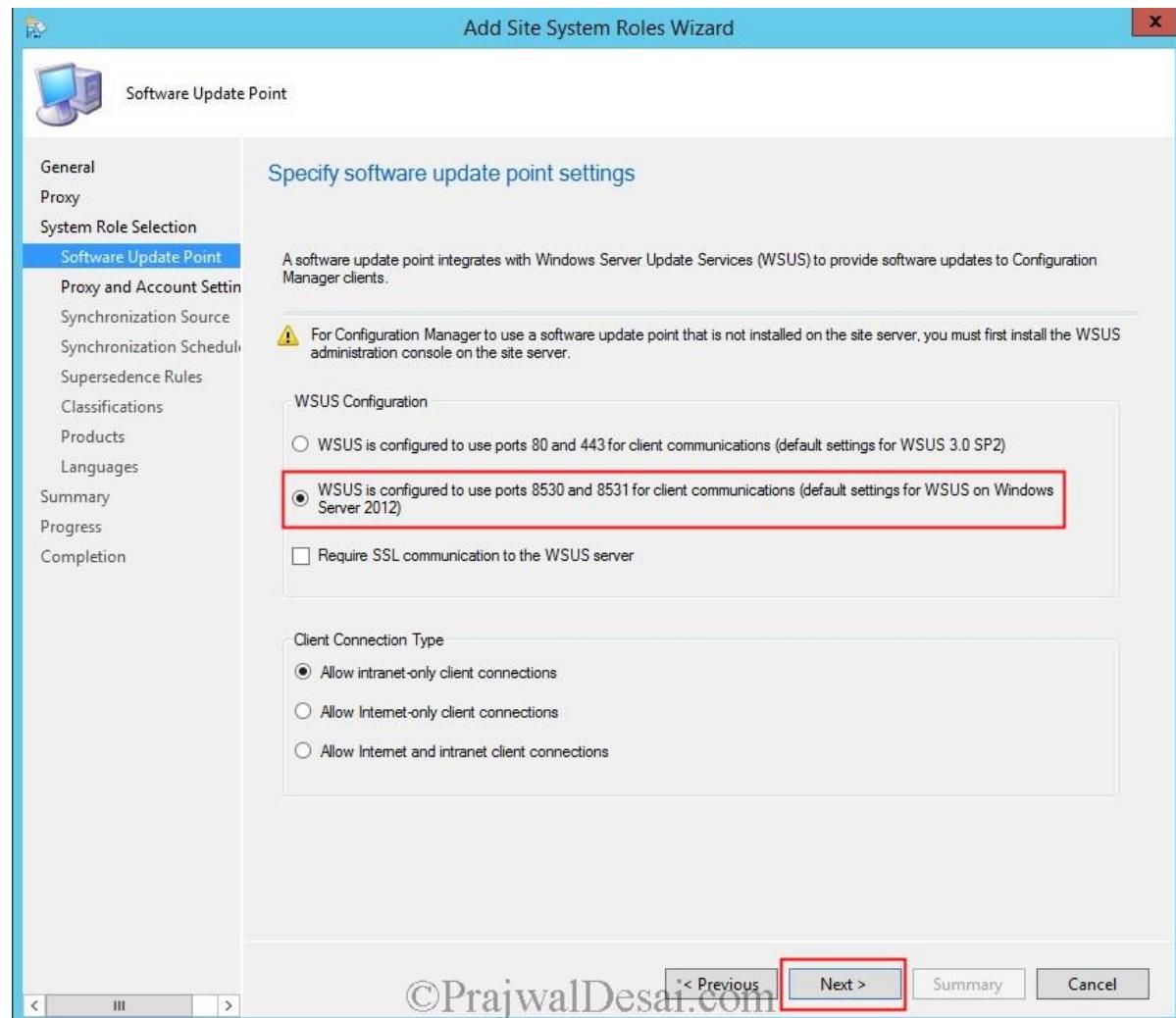
< Previous Next > Summary Cancel

©PrajwalDesai.com

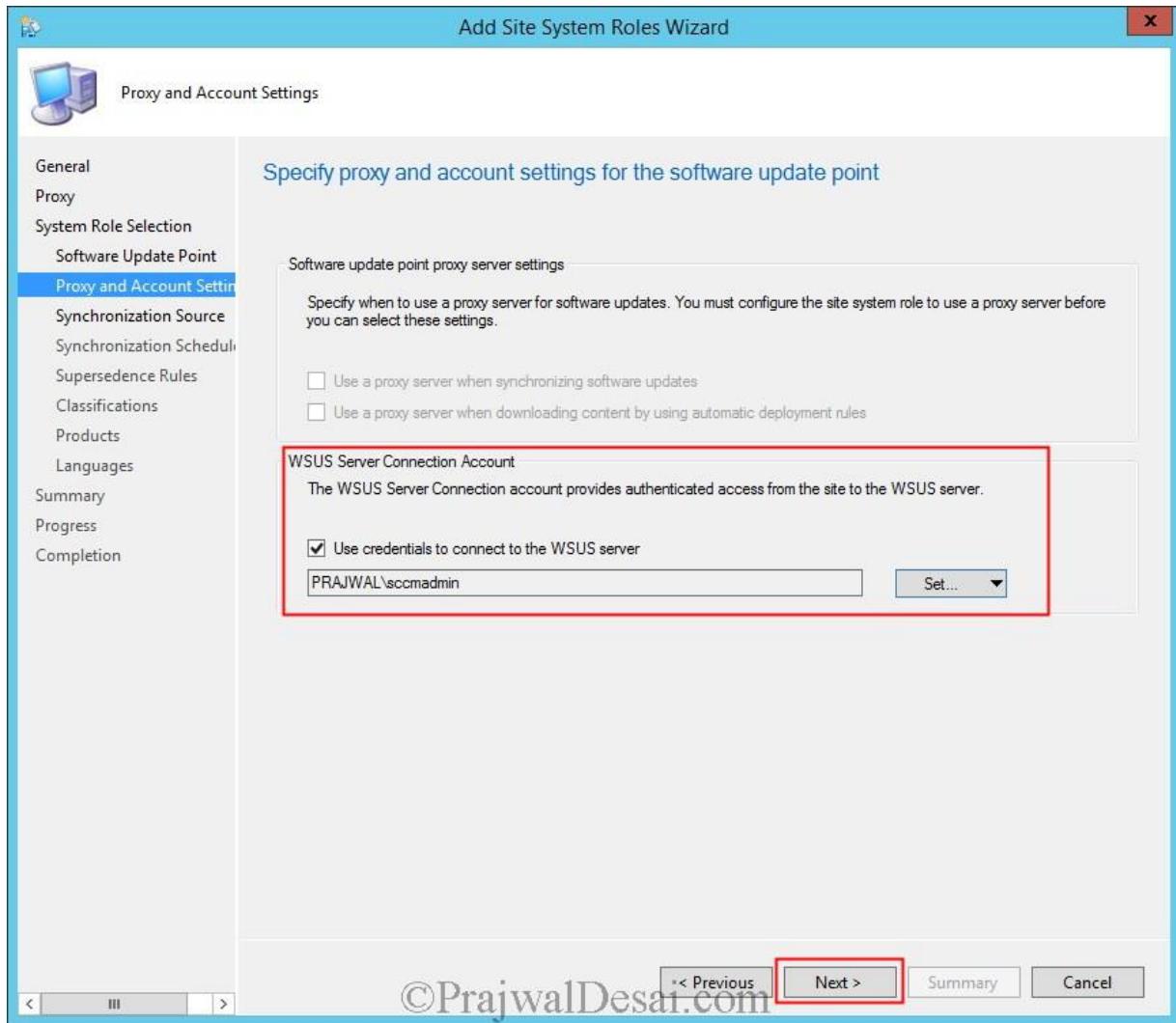


For **WSUS Configuration**, select **WSUS is configured to use ports 8530 and 8531 for client communications** and click **Next**.

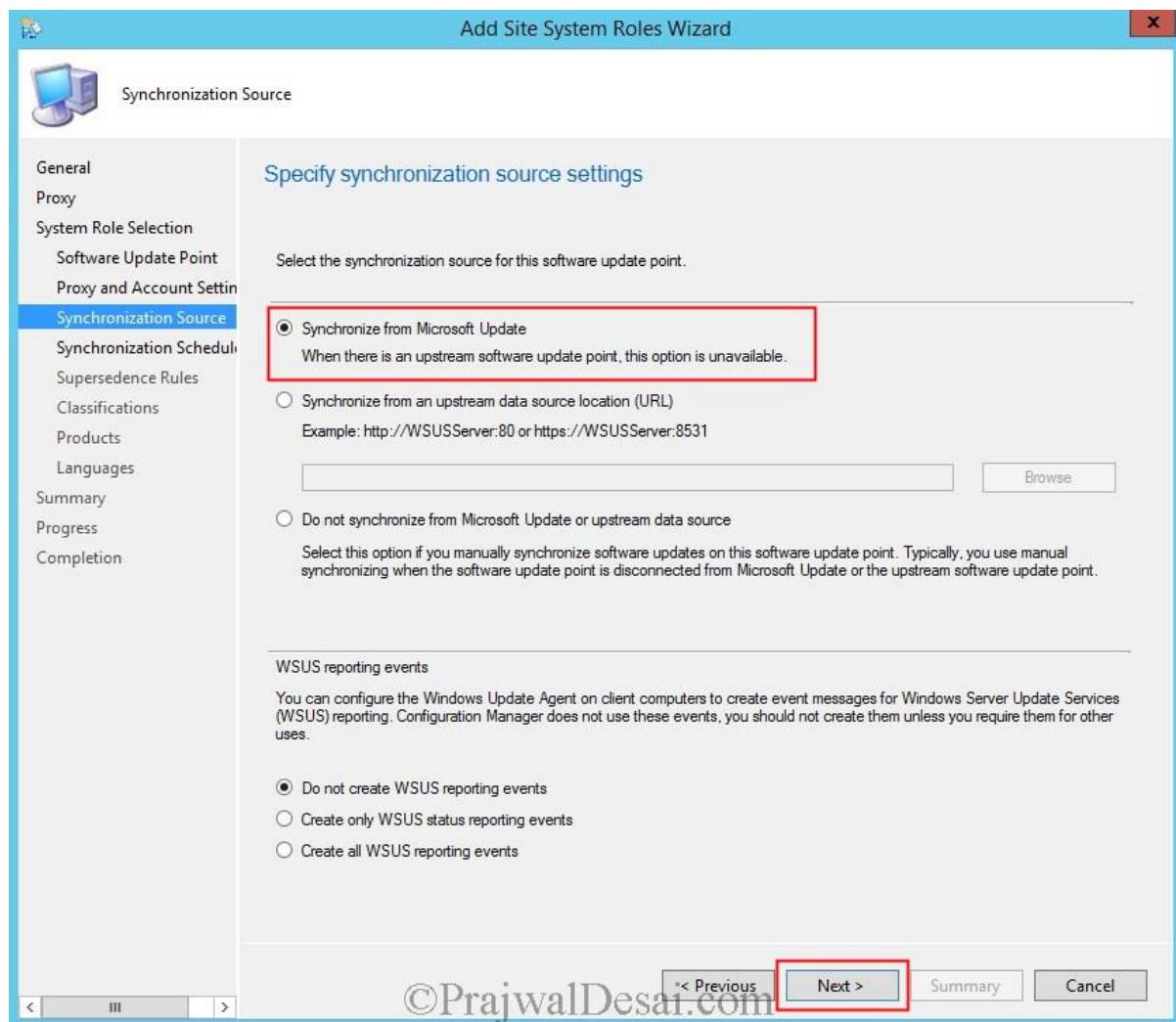
When you install WSUS, you can specify whether to use the default Internet Information Services (IIS) website or create a new custom WSUS website. As a best practice, select **Create a Windows Server Update Services 3.0 Web site** so that IIS hosts the WSUS 3.0 services in a dedicated website instead of sharing the same website with other Configuration Manager site systems or other software applications. When you use a custom website for WSUS 3.0, WSUS configures port 8530 for HTTP and port 8531 for HTTPS. You must specify these port settings when you create the software update point for the site.



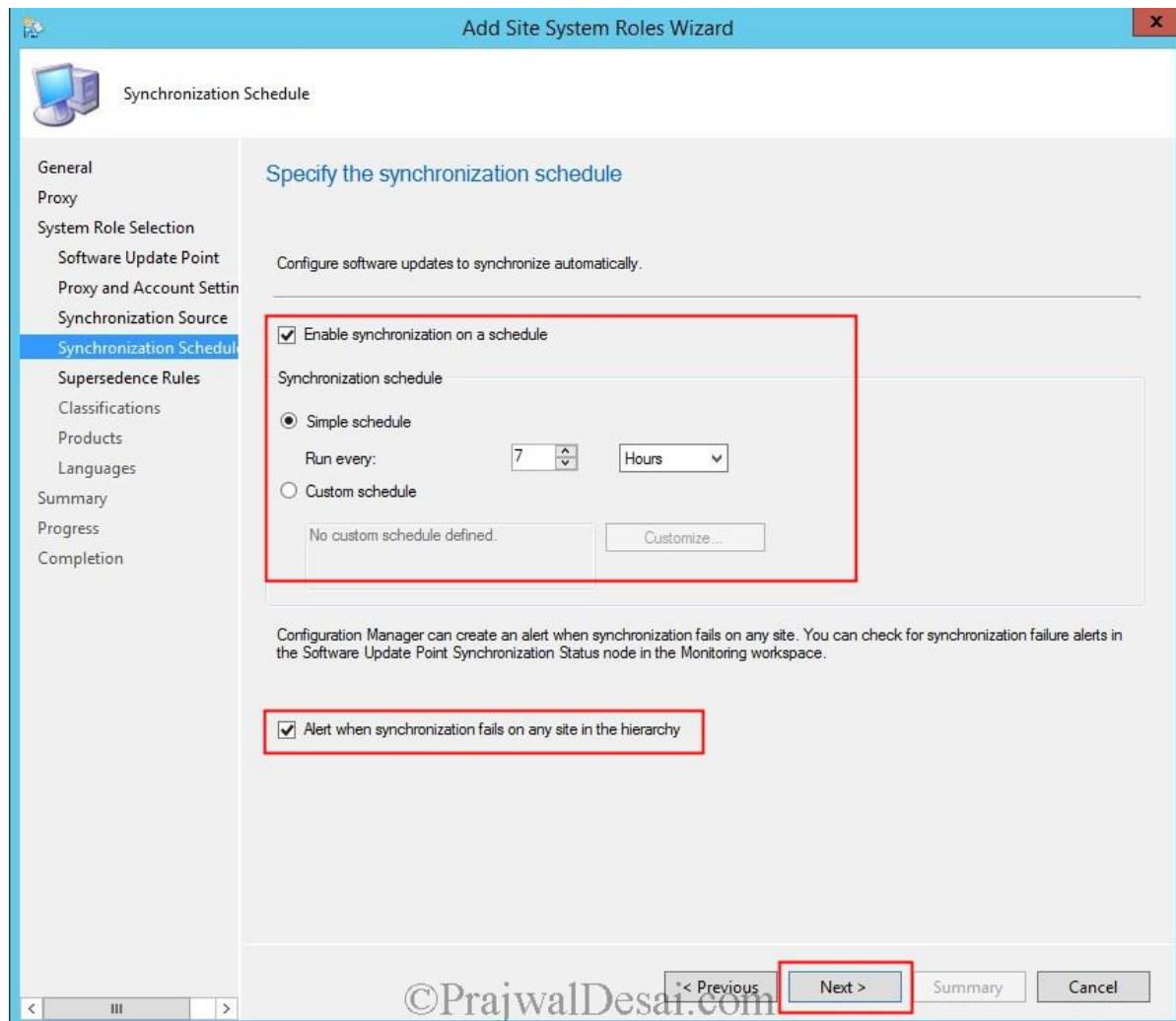
For **WSUS Server Connection Account**, click **Use credentials to connect to the WSUS server**, click on **Set** and choose the account. The account provides authenticated access from the site to WSUS server. Click **Next**.



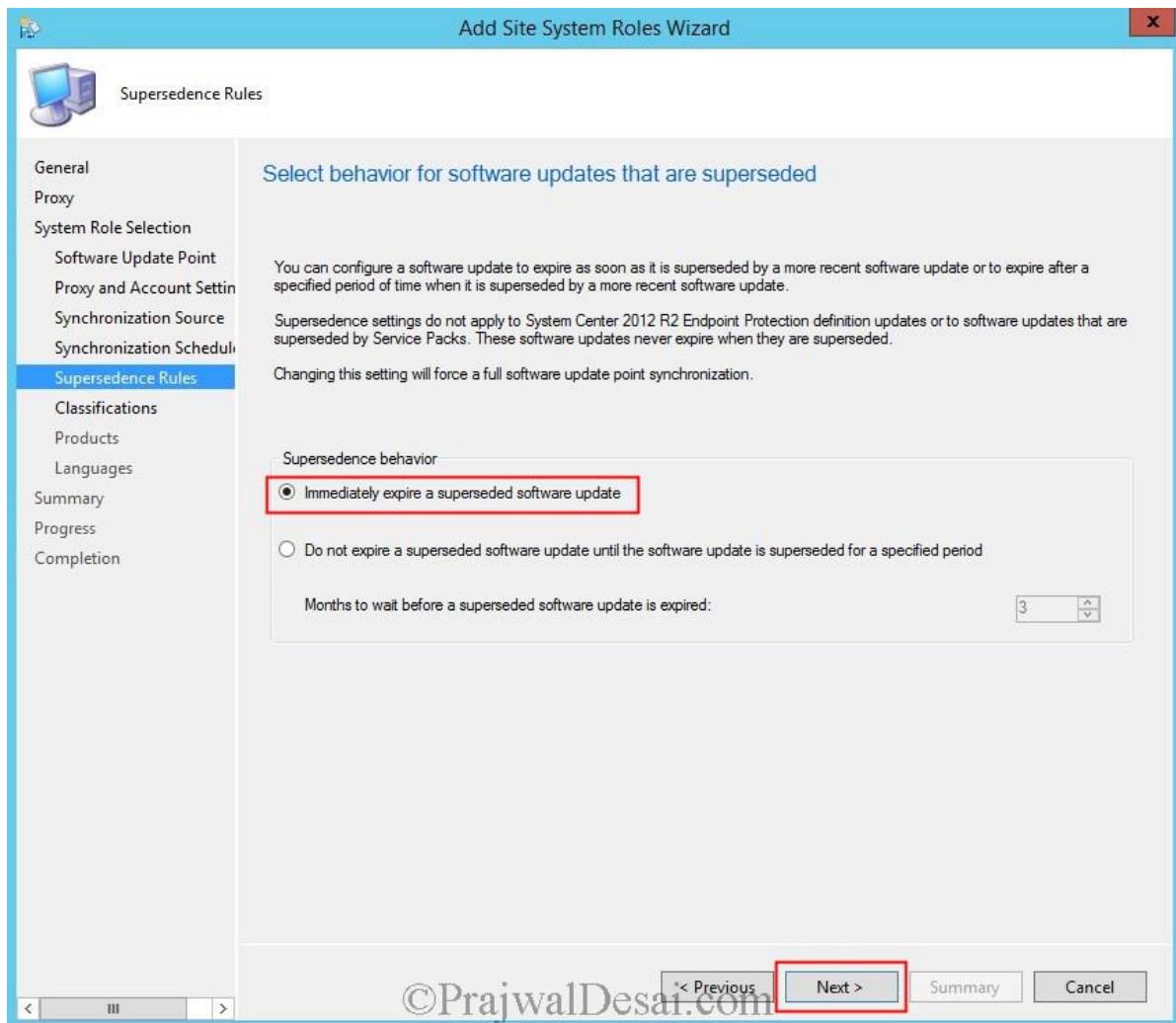
Click **Synchronize from Microsoft Update** and click **Next**.



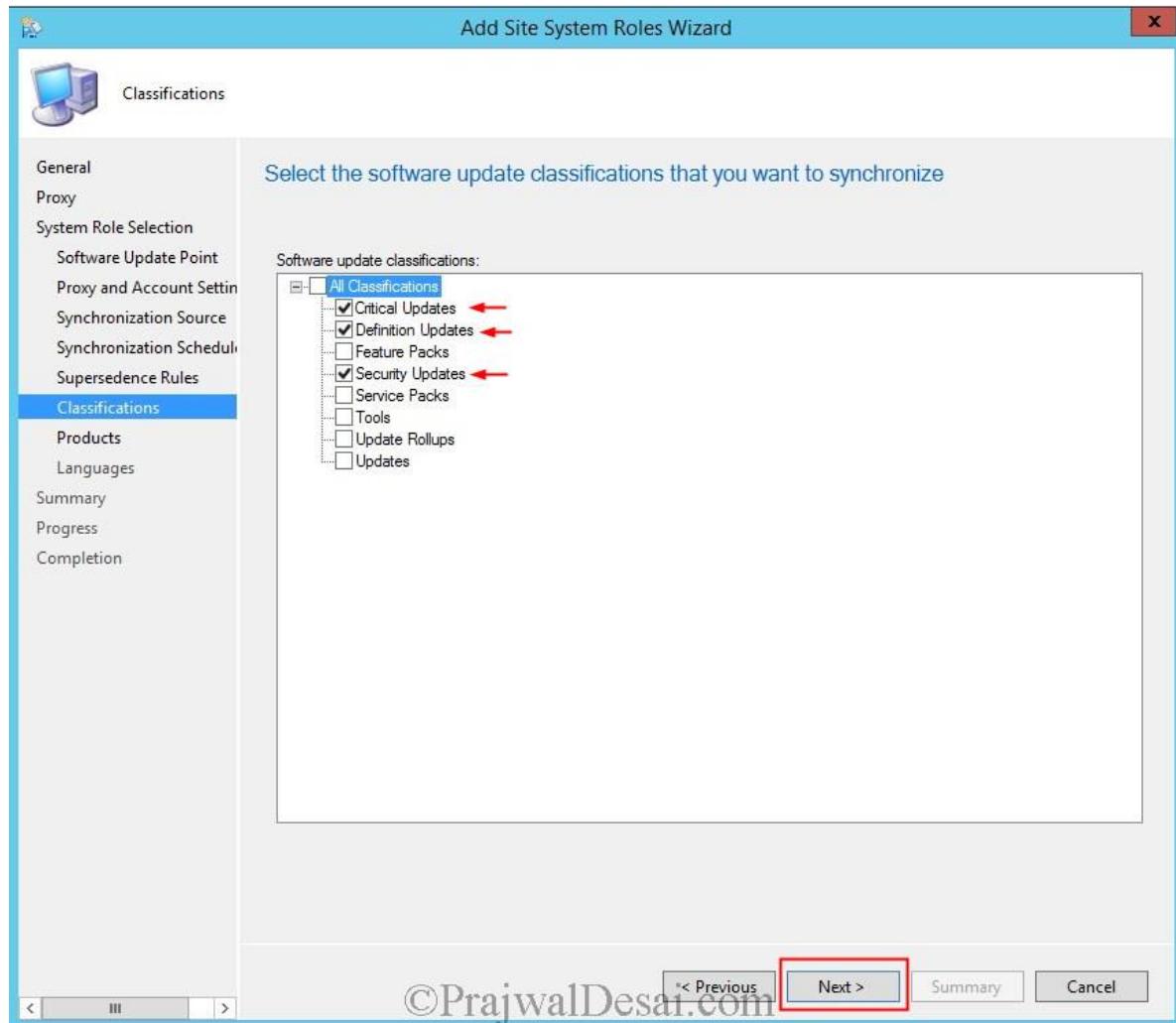
Click **Enable synchronization on a schedule** and let the schedule be set to default (simple schedule). You may also click **Alert when sync fails on any site in hierarchy**. Click **Next**.



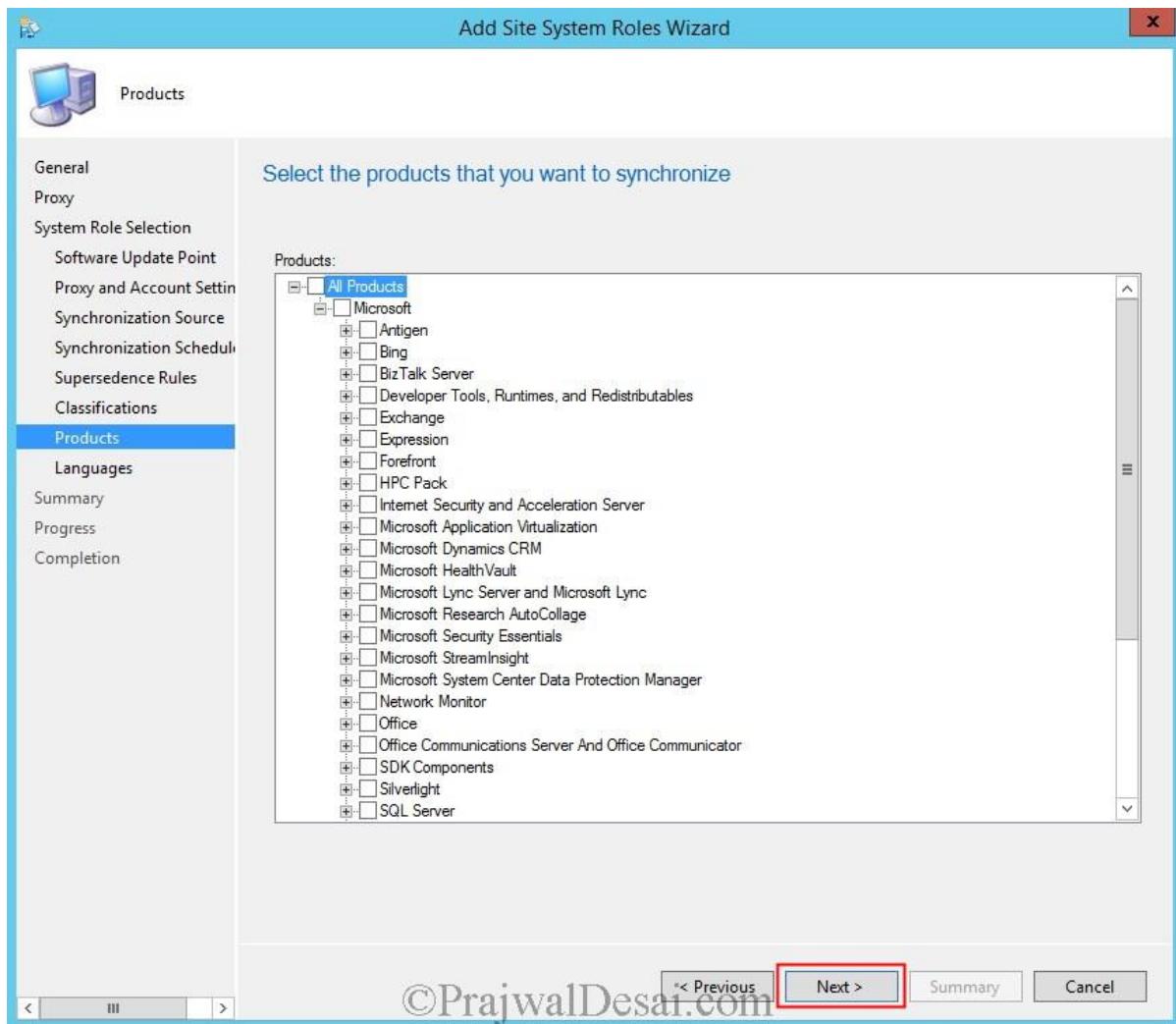
For **Supersedence behavior**, select **Immediately expire a superseded software update**. Click **Next**.



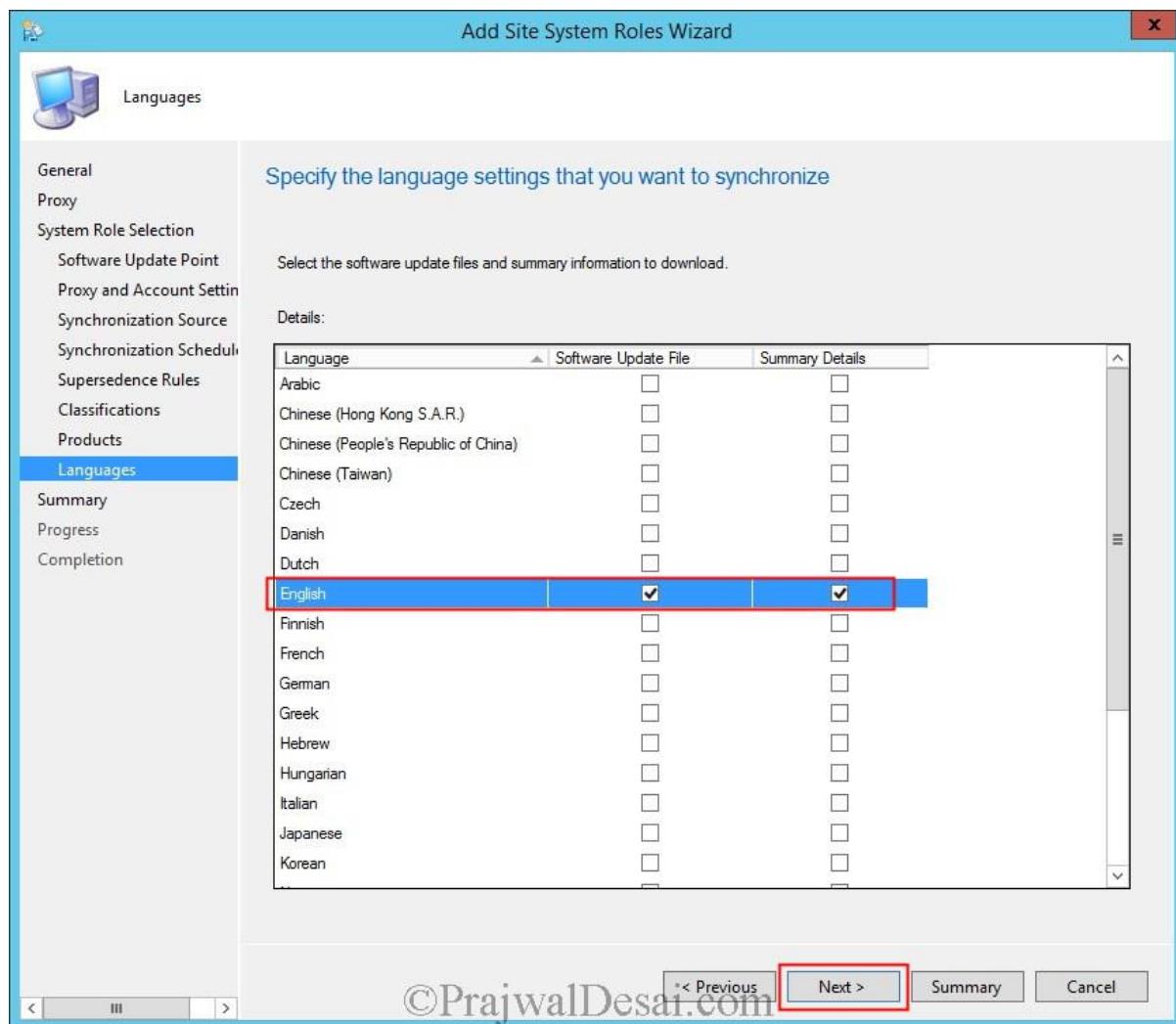
Select **Critical Updates, Definition Updates and Security Updates**. Note that you can do this after installation of SUP. Click **Next**.



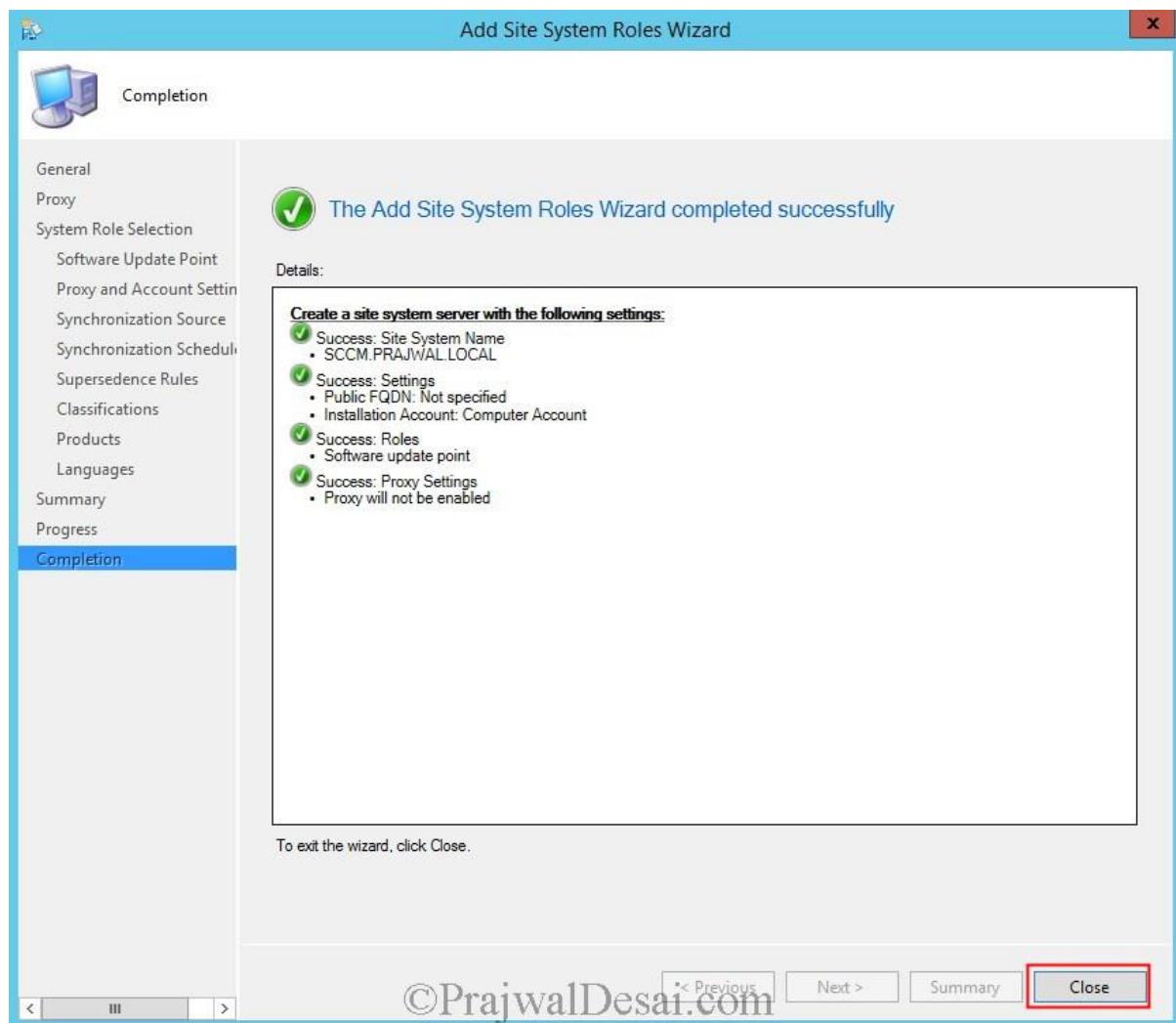
Choose the **products** that you want to synchronize, in this step I have selected **Windows 7, Forefront Endpoint Protection 2010**. Click **Next**.



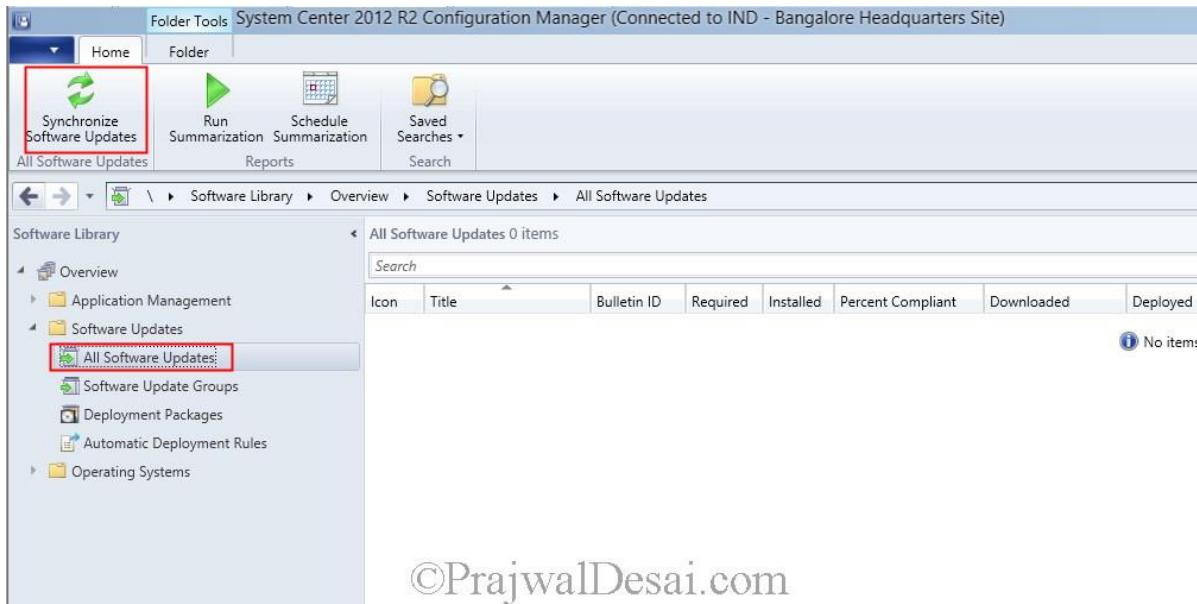
Choose the desired **language**, click **Next**.



The Software Update Point role has been installed. Click **Close**.

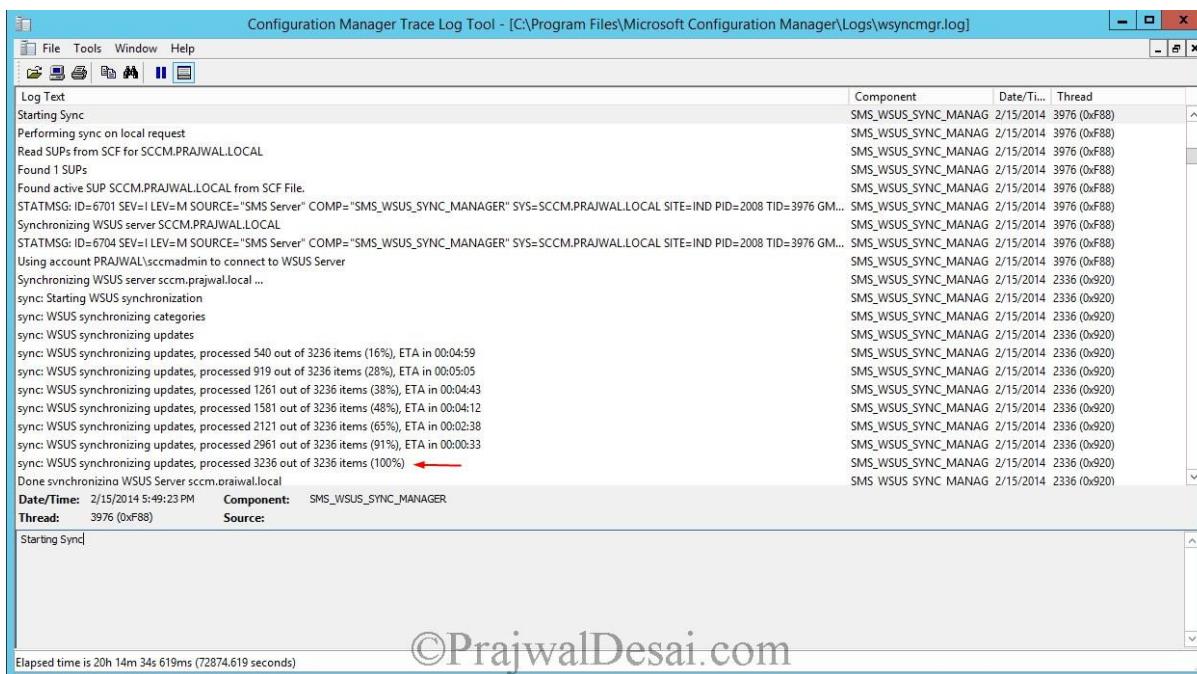


In the configuration manager console, click **Software Library**, expand **Overview**, click **Software Updates**, click **All Software Updates** and at the top ribbon click **Synchronize Software Updates**.

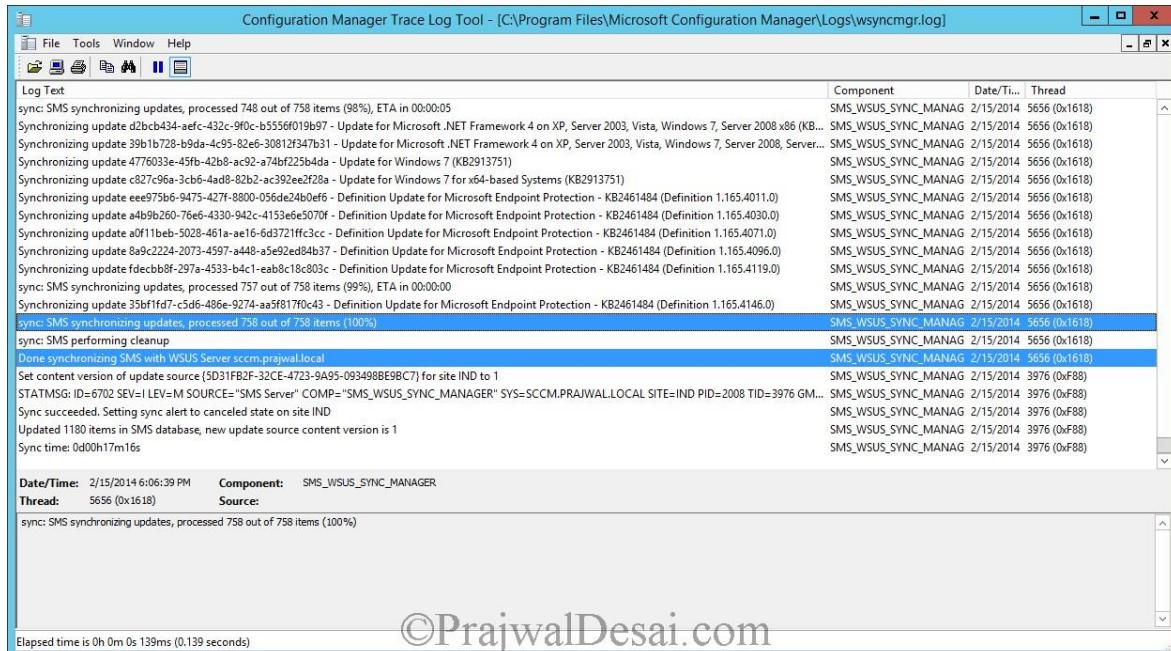


©PrajwalDesai.com

To see what's happening at the background, you need to have 2 files opened **wsyncmgr.log** and **WCM.log** file. Below is the screenshot of the **wsyncmgr.log** file and we can see that the WSUS is synchronizing the **categories** and **updates**.



The synchronization is completed. The software updates can now be seen when you click **All Software Updates option** in CM Console. Note that the updates are yet to be downloaded.



Out of all the updates we will not deploy all of them rather we will filter the updates by adding criteria. Click on **Add criteria**. Select **Expired**, **Product**, **Superseded**, **Bulletin ID**. Click **Add**. Choose the **product** as **Windows 7**, **Bulletin ID** as **MS**, **Expired** as **NO**, **Superseded** as **NO**.

The screenshot shows the CM console's "All Software Updates Search Results" page. The search bar at the top contains the following criteria:

- AND Expired No
- AND Product Windows 7
- AND Superseded No
- AND Bulletin ID contains MS

The main table lists 316 software updates. The columns are:

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed	Expired	Superseded
[Icon]	Cumulative Security Update for ActiveX Killbits for Windows 7 (KB290...	MS13-090	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for ActiveX Killbits for Windows 7 for x64...	MS13-090	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 10 for Windows 7 S...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 10 for Windows 7 S...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 11 for Windows 7 (K...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 11 for Windows 7 (...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 11 for Windows 7 (...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 8 for Windows 7 (K...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 8 for Windows 7 for...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 9 for Windows 7 (K...	MS14-010	0	0	0	No	No	No	No
[Icon]	Cumulative Security Update for Internet Explorer 9 for Windows 7 for...	MS14-010	0	0	0	No	No	No	No
[Icon]	Security Update for Internet Explorer 10 for Windows 7 (KB2909210)	MS14-011	0	0	0	No	No	No	No
[Icon]	Security Update for Internet Explorer 10 for Windows 7 for x64-based...	MS14-011	0	0	0	No	No	No	No

Below the table, there are two tabs: "Detail" and "Statistics". The "Detail" tab shows the following details for the first update:

- Severity: Critical
- Bulletin ID: MS13-090
- Article ID: 2900986
- Date Released: 11/12/2013 11:30 PM
- Date Released or Revised: 11/12/2013 11:30 PM
- Superseded: No

The "Statistics" tab shows the following counts:

- Compliant: 0
- Required: 0
- Not Required: 0
- Unknown: 3

Total Asset Count: 3 (Last Update: 2/15/2014 6:07:29 PM)

Now select all the updates (hold Shift+page Down), right click on the updates and click **Create Software Update Group**.

All Software Updates Search Results - 316 items shown

Search

AND Expired No ×
AND Product Windows 7 ×
AND Superseded No ×
AND Bulletin ID contains MS

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed	Expired	Superseded
[Icon]	Security Update for Windows 7 for x64-based Systems (KB2887069)	MS13-101	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB2892074)	MS13-099	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KR2893294)	MS13-098	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Download]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Create Software Update Group]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Edit Membership]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Review License]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Deploy]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Move]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (K)	[Properties]	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB978542)	MS10-030	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB979309)	MS10-019	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB979482)	MS10-033	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB979687)	MS10-083	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB979688)	MS10-083	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB982132)	MS10-076	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB982665)	MS10-055	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB982666)	MS10-040	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB982799)	MS10-059	0	0	0	No	No	No	No

Provide the name to the software update group as **Windows 7 Update group**. Click **Create**.

All Software Updates Search Results - 316 items shown

Search

AND Expired No ×
AND Product Windows 7 ×
AND Superseded No ×
AND Bulletin ID contains MS

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed	Expired	Superseded
[Icon]	Security Update for Windows 7 for x64-based Systems (KB2910030)	MS14-003	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB972270)	MS10-001	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB974571)	MS09-056	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB975467)	MS09-059	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB975560)	MS10-013	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KB979309)	MS10-080	0	0	0	No	No	No	No
[Icon]	Security Update for Windows 7 for x64-based Systems (KR979309)	MS10-019	0	0	0	No	No	No	No

Click on **Software Update Group** and you will find the software update group that was created in the previous step. Right click on the **Windows 7 Update Group** and click **Deploy**.

The screenshot shows a Windows interface for managing software update groups. A context menu is open over the 'Windows 7 Update Group'. The 'Deploy' option is highlighted with a red box. Other options in the menu include 'Show Members', 'Download', 'Run Summarization', 'Refresh', 'Delete', 'Set Security Scopes', and 'Properties'.

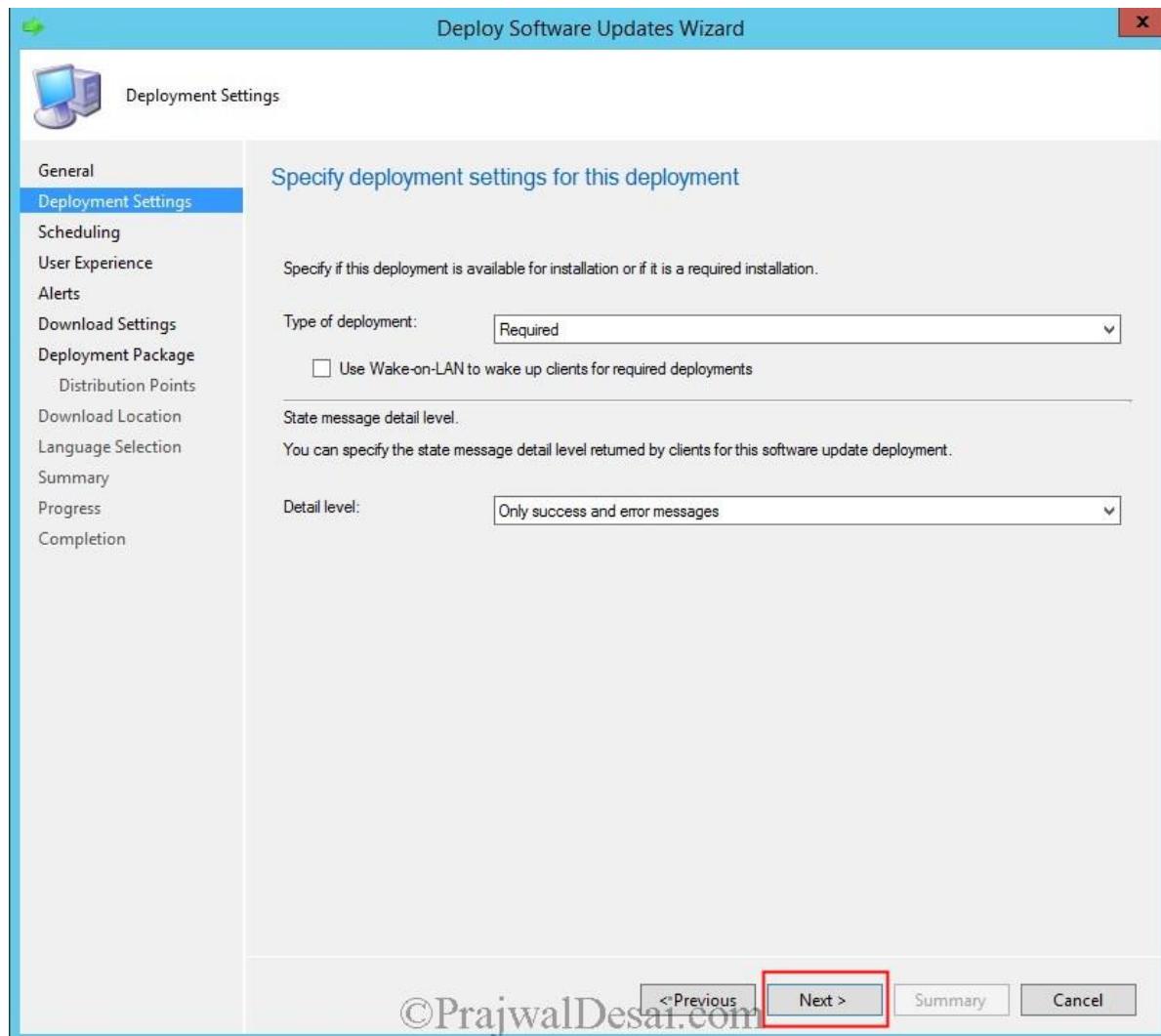
©PrajwalDesai.com

On the **Deploy Software Updates Wizard**, provide a **Deployment Name**, **description** and choose the **collection** for which this software update deployment must be deployed. Click **Next**.

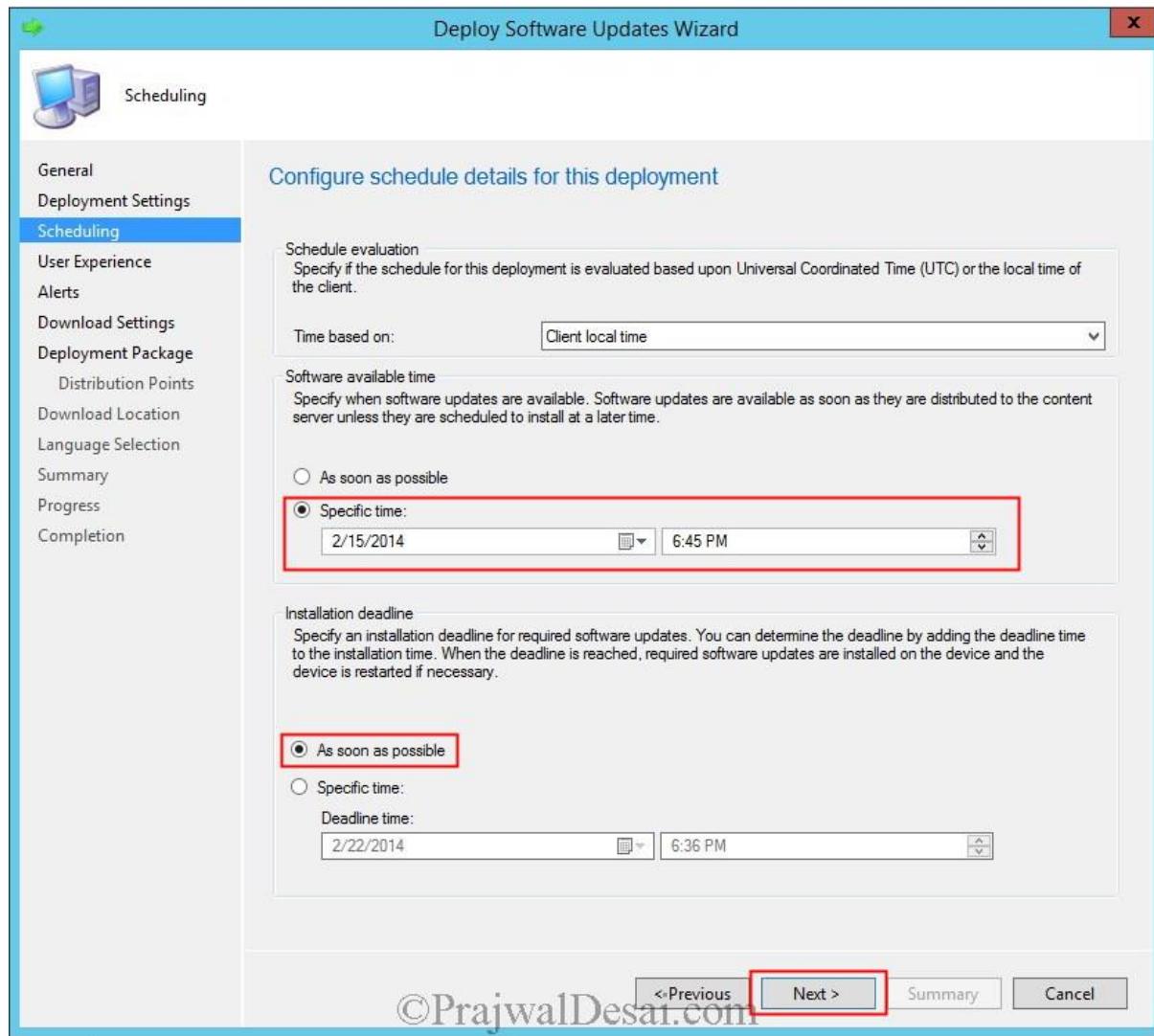
The screenshot shows the 'General' step of the 'Deploy Software Updates Wizard'. The left sidebar lists various deployment settings. The main area is titled 'Specify general information for this deployment'. It includes fields for 'Deployment Name' (set to 'Windows 7 Updates Deployment'), 'Description' (containing 'Deploying Windows 7 Critical, Security Updates Date - 15-Feb-2015'), and 'Software Update/Software Update Group' (set to 'Windows 7 Update Group'). Below these, there's a section for selecting a deployment template and a collection. The 'Collection' field is highlighted with a red box and contains 'Windows 7 Computers'. At the bottom, there are buttons for '<*Previous', 'Next >', 'Summary', and 'Cancel'.

©PrajwalDesai.com

Set the **Type of deployment** as **Required** and detail level can be set to **Only success and error messages**. Click **Next**.

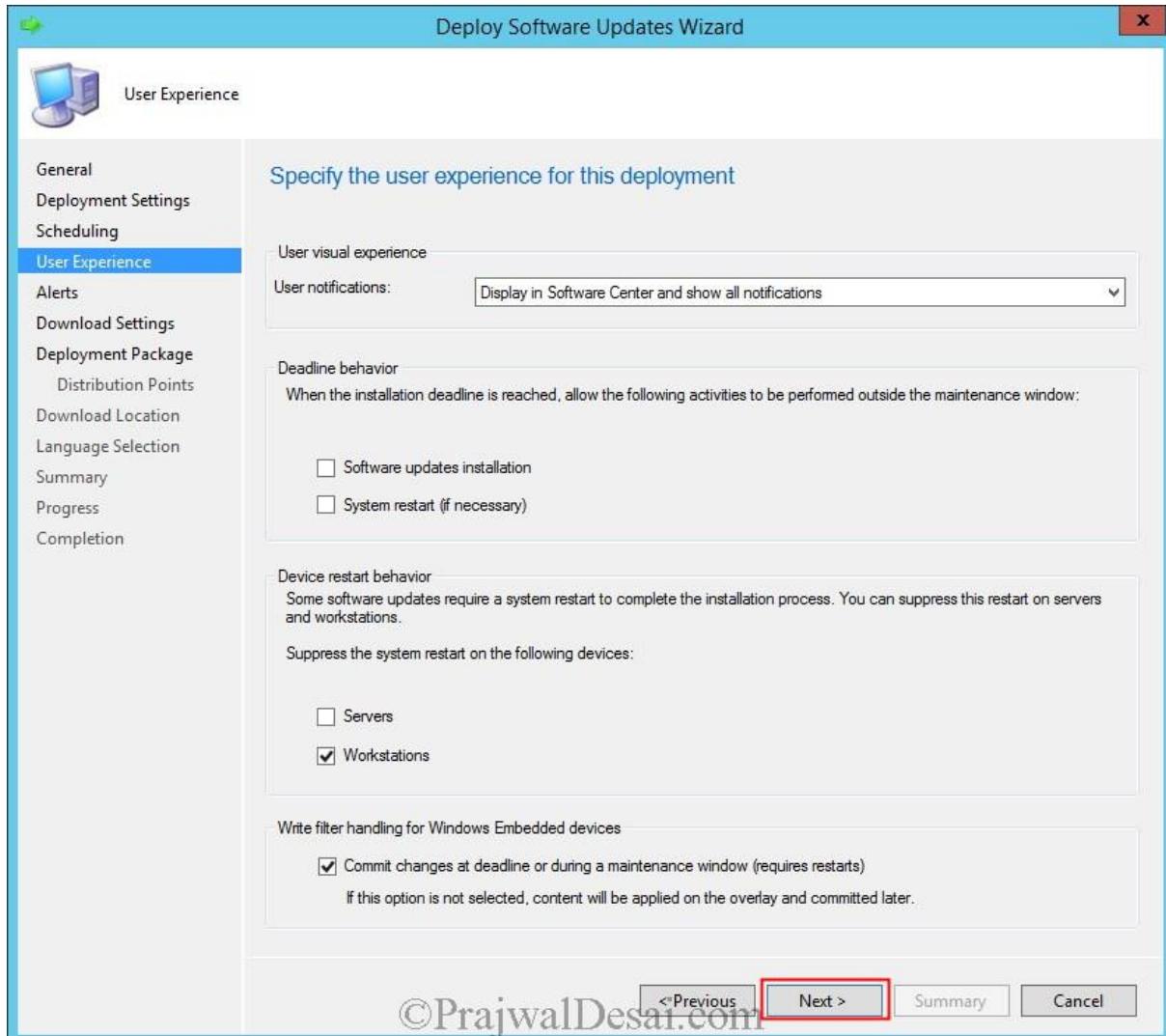


Configure the schedule for this deployment, set the **Time based on** to **Client local time**. Choose **Software available time** to **specific time** and set the **Installation deadline** to **as soon as possible**. Click **Next**.



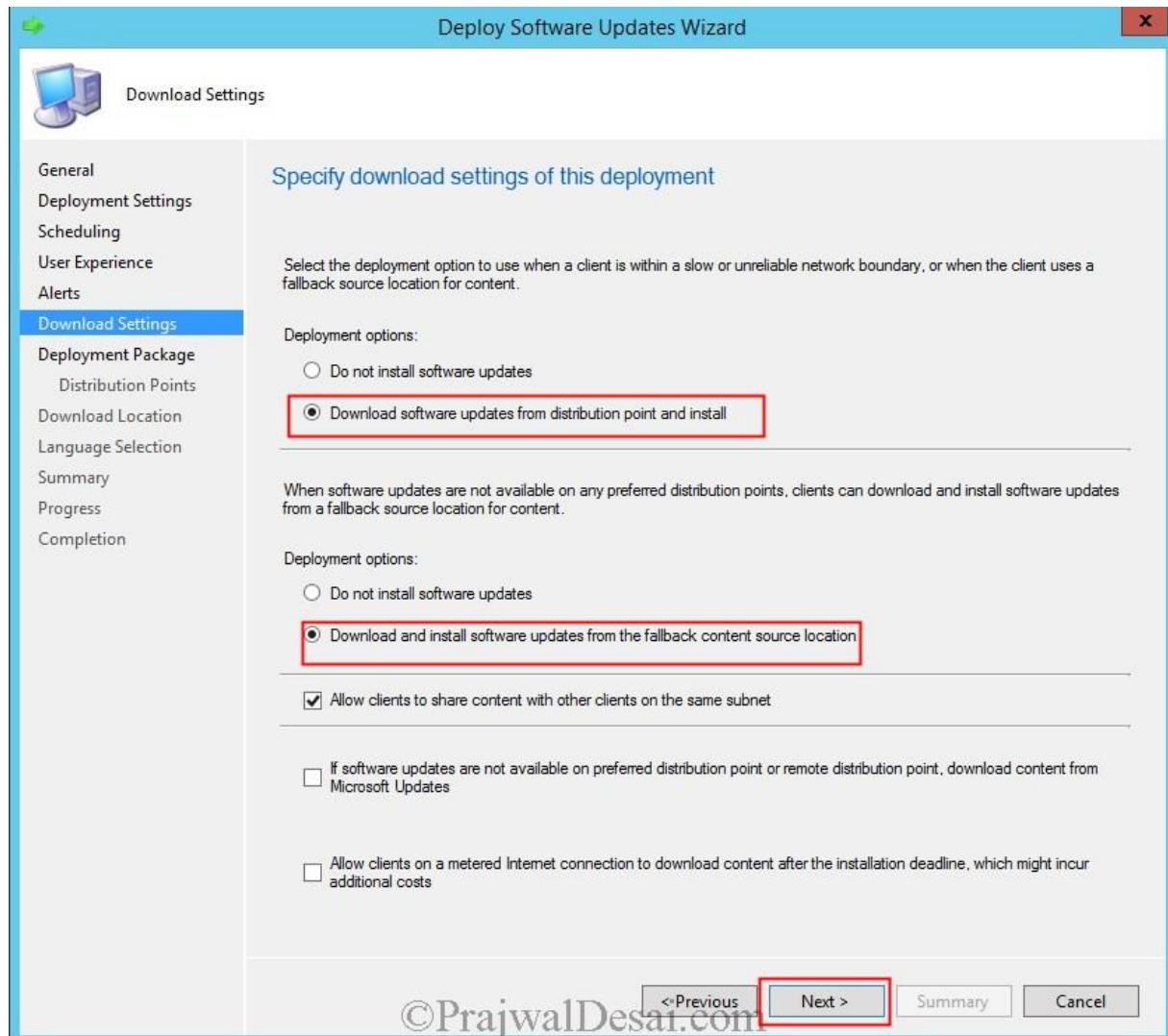
©PrajwalDesai.com

On the **User Experience** page, you can choose to suppress the restart for Server or Workstations. Click **Next**.

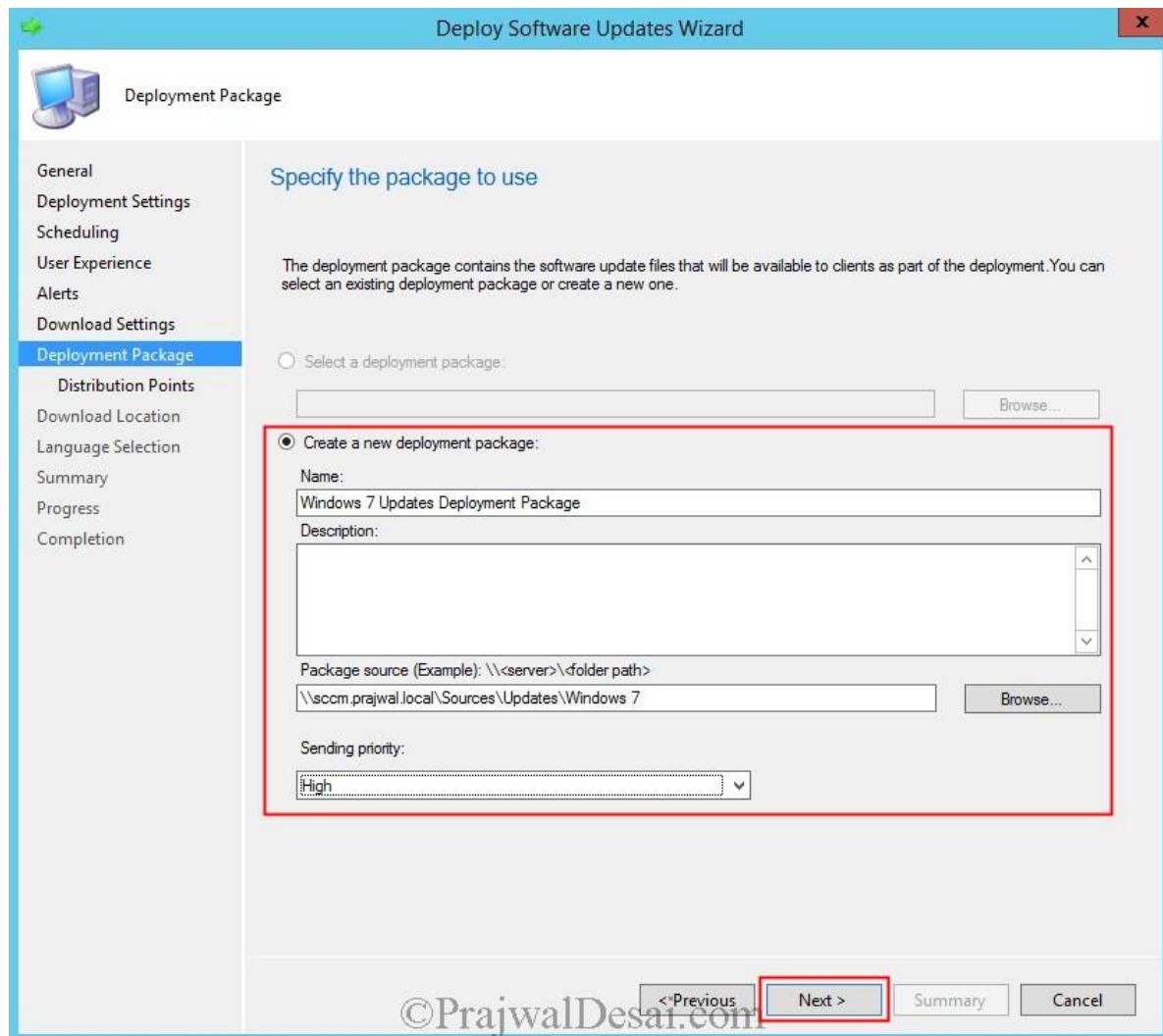


©PrajwalDesai.com

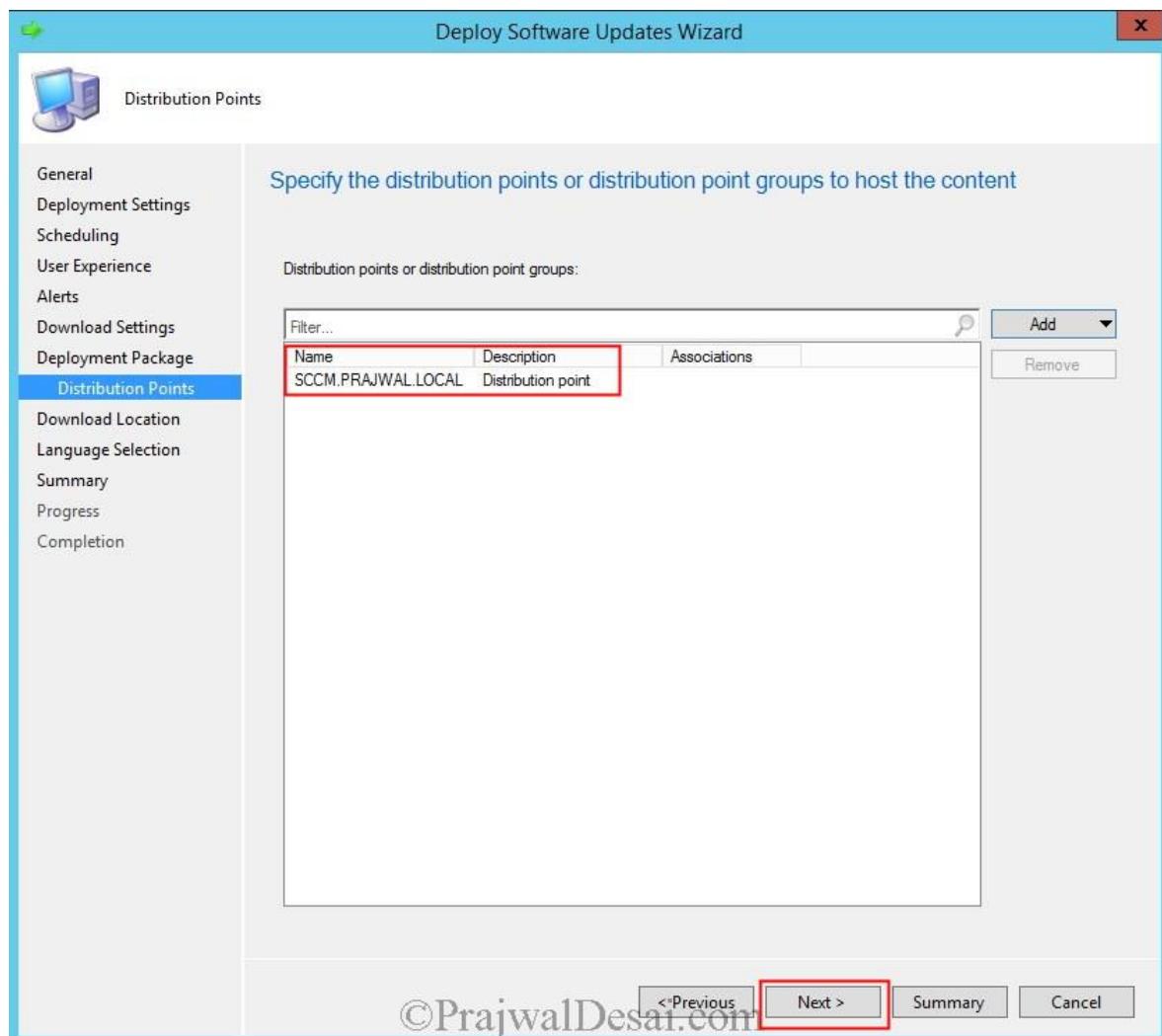
For **Deployment options**, if a client is within a slow or unreliable network boundary then select **Download software updates from distribution point and install**. If the updates are not available with preferred DPs then select **Download and install software updates from the fallback content source location**. Click Next.



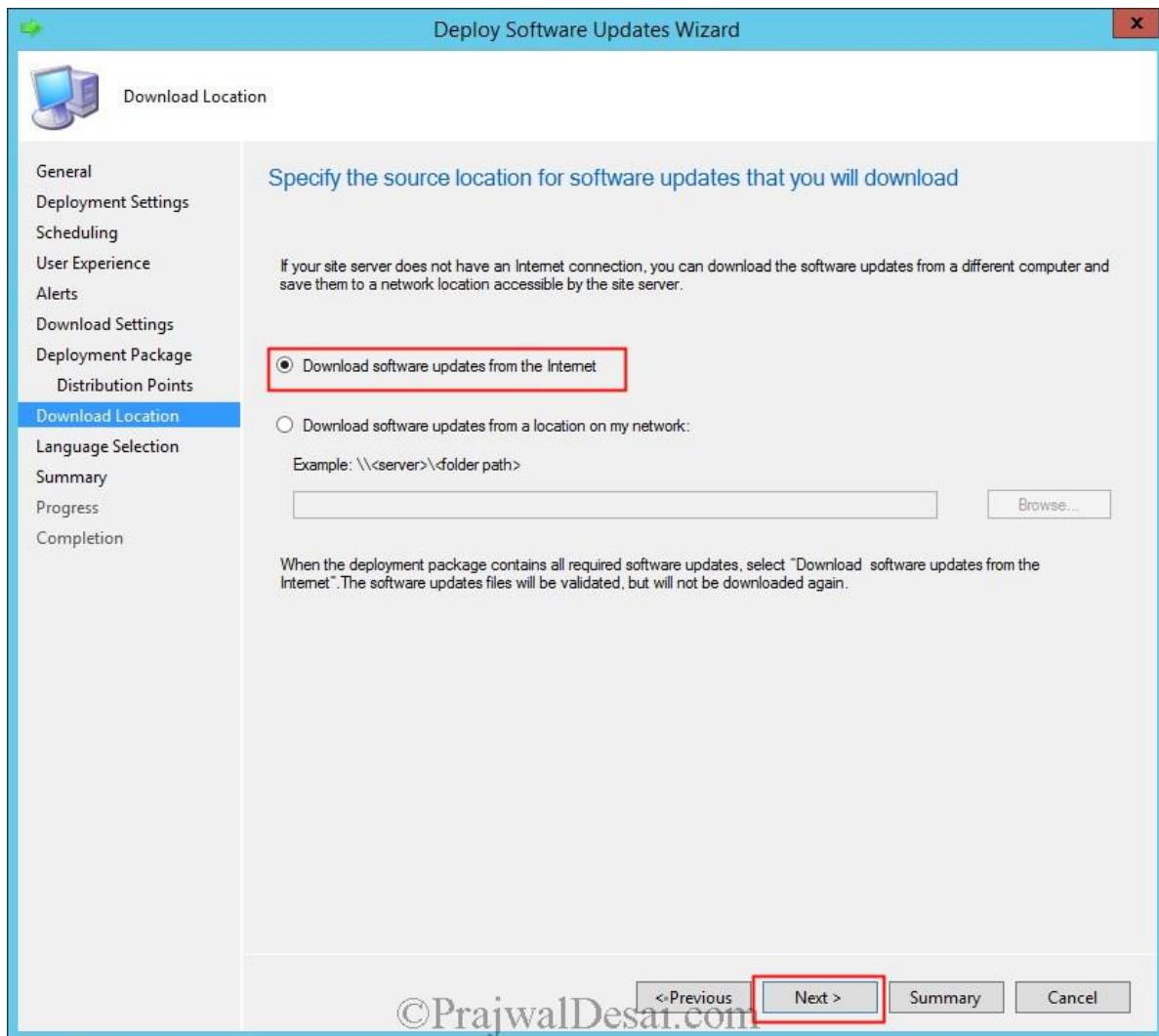
Create a new deployment package by providing a name, location for the **Package source** and **Sending priority**. Click **Next**.



Add the **Distribution Point** and click **Next**.

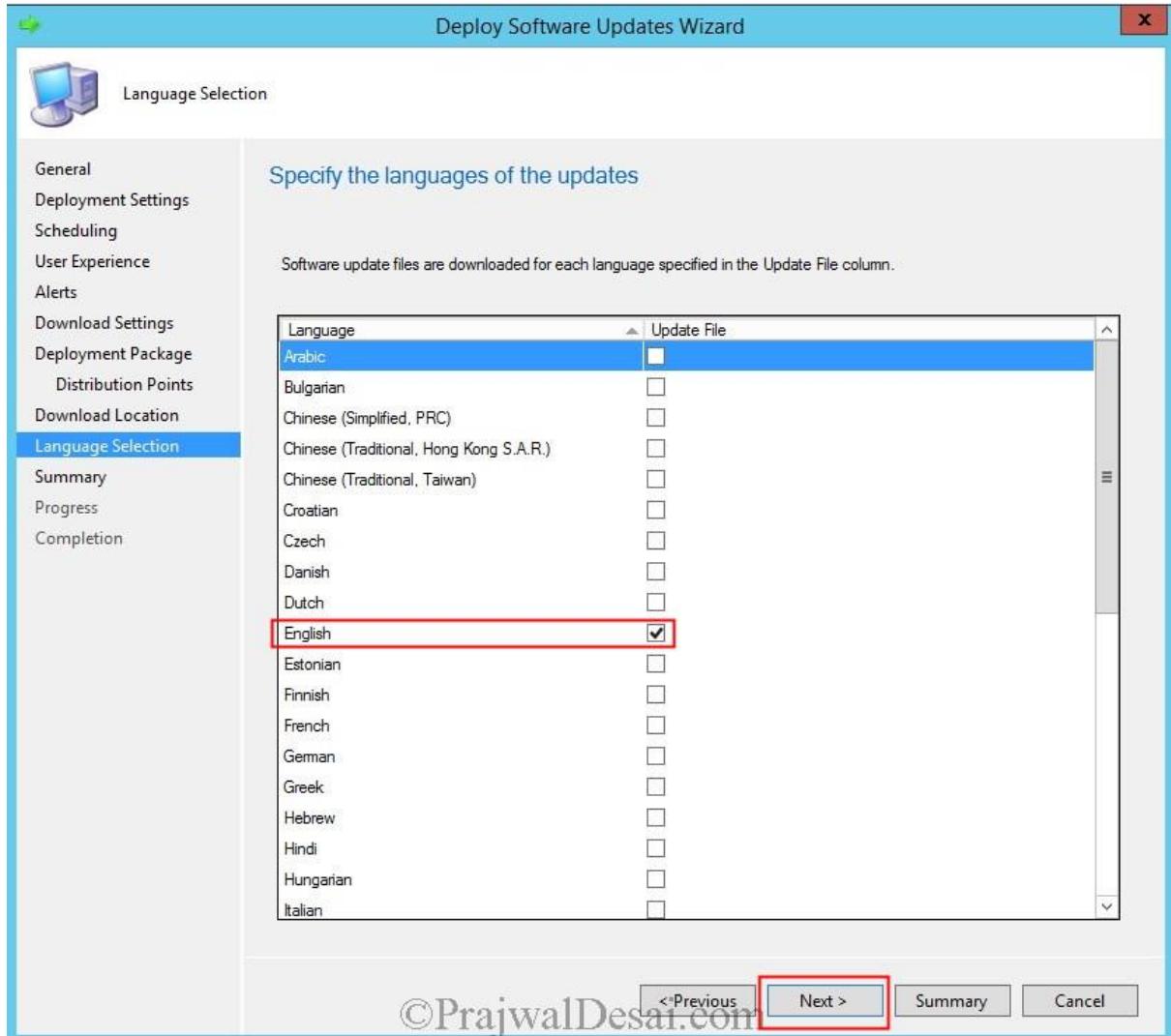


For **Download Location** choose **Download software updates from the Internet**. Click **Next**.

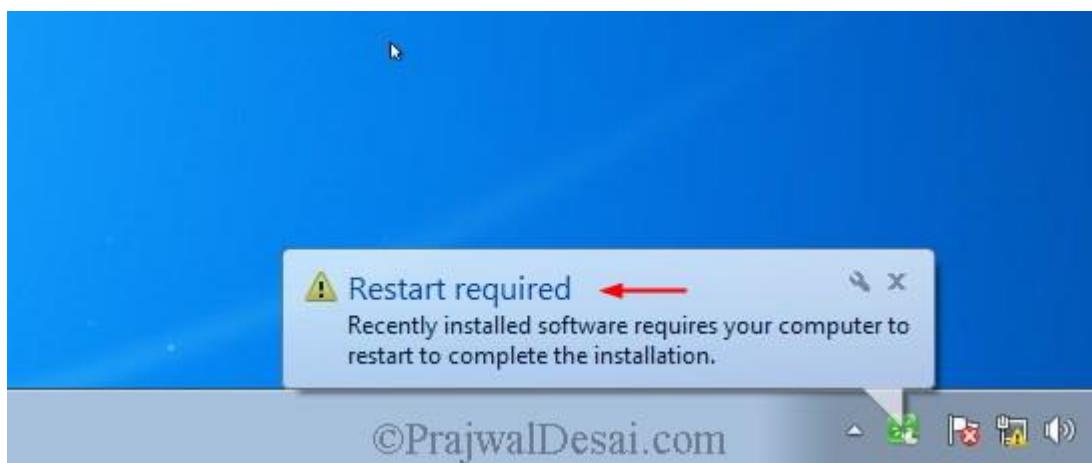


©PrajwalDesai.com

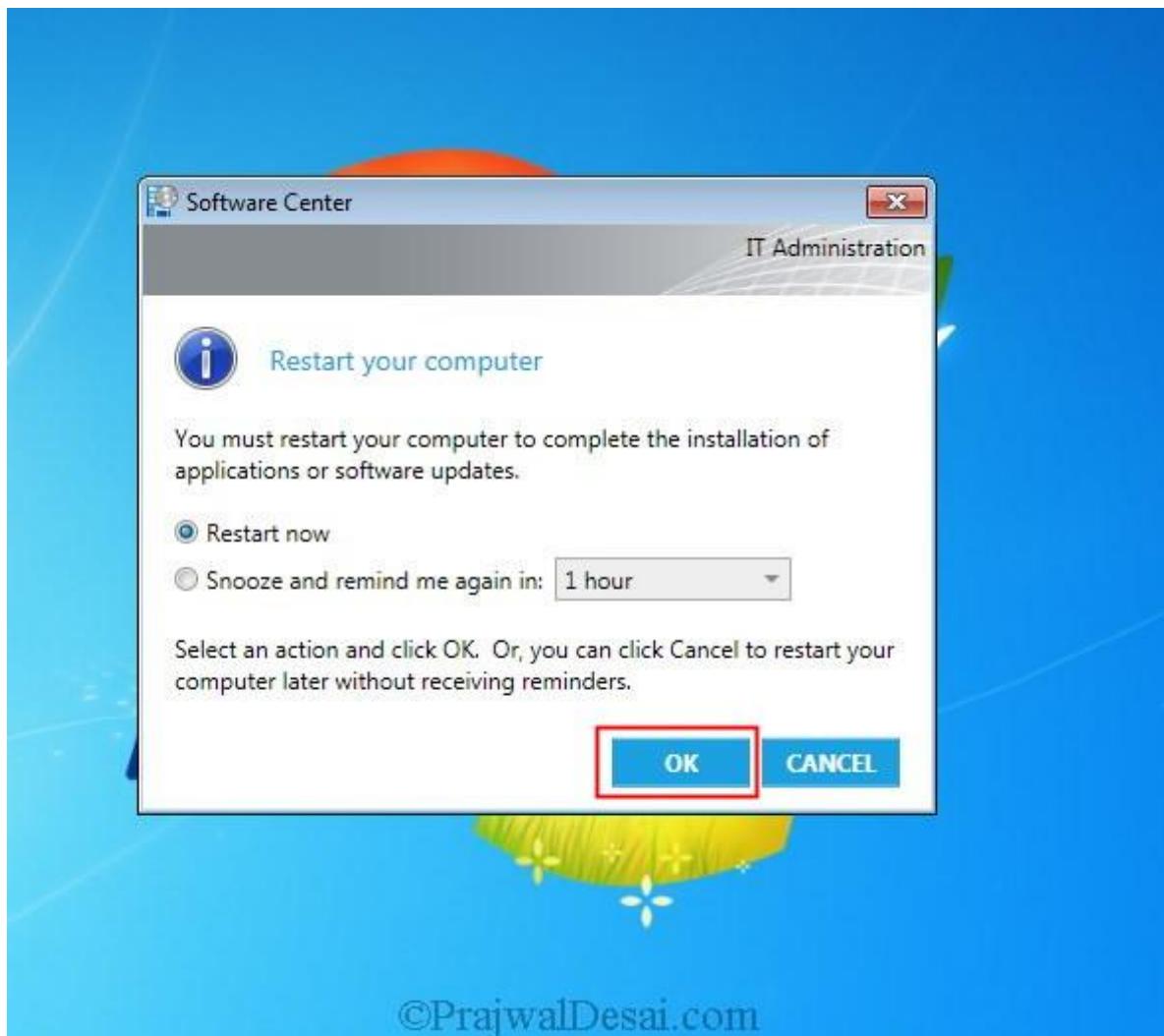
Choose the **language** and click **Next**. The wizard will now download the updates and deploy them to the collection as per the schedule defined. Click on **Close** to close the wizard.



After few minutes we see that the updates are installed on one the client machines in the collection and there is a notification that system needs to be restarted.



You can choose to restart the computer by choosing **Restart now** or you can choose **Snooze and remind me again** in hours.



Installing And Configuring Endpoint Protection Role In SCCM 2012 R2

In this post we will look at the steps for installing and configuring Endpoint protection role in SCCM 2012 R2. Endpoint Protection in System Center 2012 R2 Configuration Manager allows you to manage antimalware policies and Windows Firewall security for client computers in your Configuration Manager hierarchy. Endpoint Protection helps protect your PC from malicious software (malware) such as viruses, spyware, and other potentially harmful software. Before you install the Endpoint protection role you need to install the prerequisites. Windows Server Update Services (WSUS) must be installed and configured for software updates synchronization if you want to use Configuration Manager software updates to deliver definition and engine updates.

For SCCM 2012 R2 Step by Step Guides click [here](#).

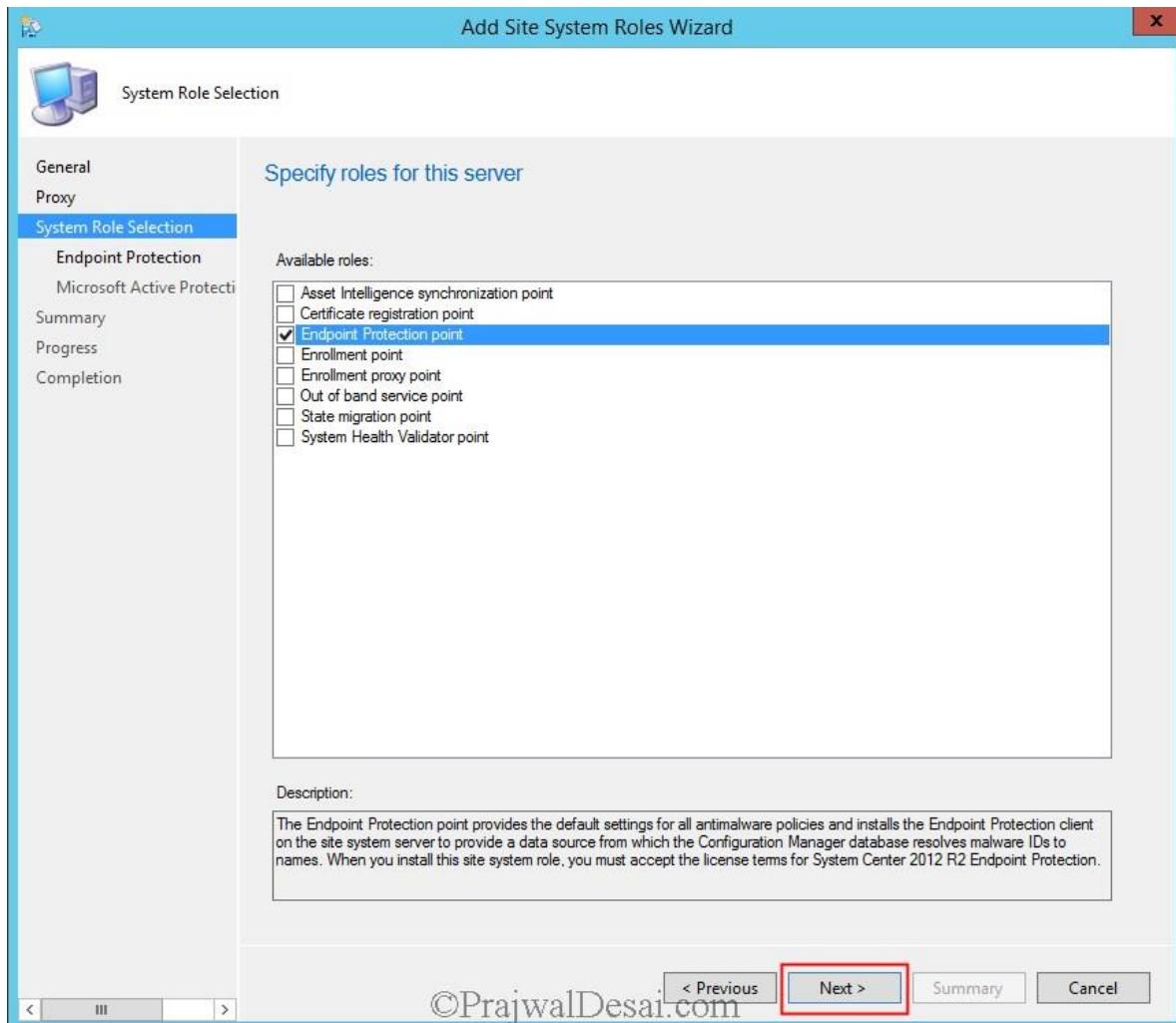
When you install the Endpoint Protection with Configuration Manager you get following advantages :-

1. Endpoint Protection in Configuration Manager allows you to manage Windows Firewall settings in the Configuration Manager console. You can also configure antimalware policies and apply that to selected groups of computers, by using custom antimalware policies and client settings.
2. Configuration Manager software updates can be used to download the latest antimalware definition files to keep client computers up-to-date.
3. You can send email notifications, use in-console monitoring, and view reports to keep administrative users informed when malware is detected on client computers.

Where Should I Install the Endpoint Protection Role ? – The Endpoint Protection point site system role must be installed on one site system server only, and it must be installed at the top of the hierarchy on a central administration site or a stand-alone primary site.

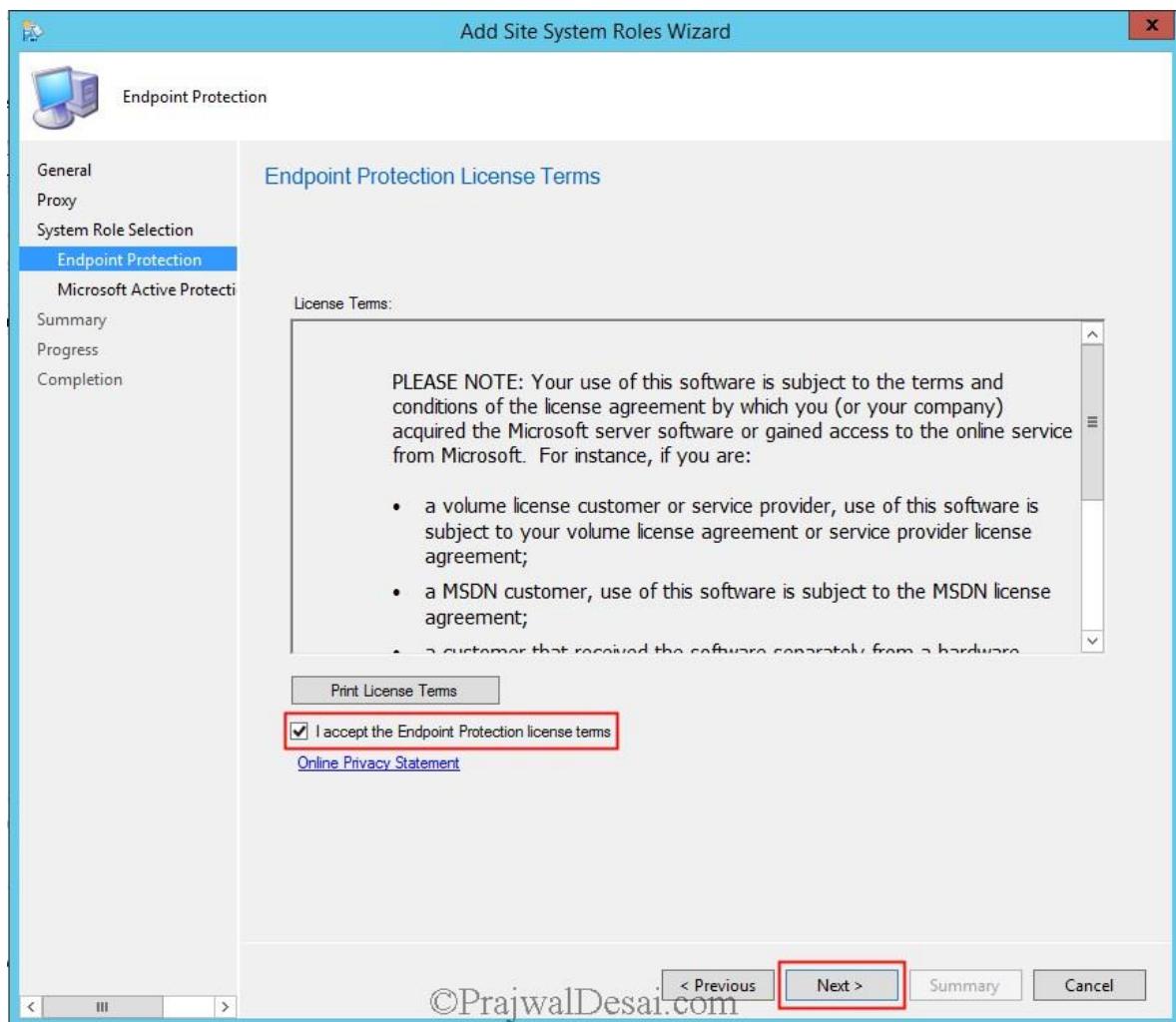
Before you begin installing the endpoint protection role, you must have the WSUS installed and configured for software updates synchronization. A software update point site system role must be installed and configured to deliver definition updates if you want to use Configuration Manager software updates to deliver definition and engine updates.

To install the Endpoint Protection Role, launch the Configuration Manager console, click **Administration**. In the Administration workspace, expand **Site Configuration**, click **Servers and Site System Roles**, right click the server and click **Add site system roles**. Check the role **Endpoint Protection Point**. Click **Next**.

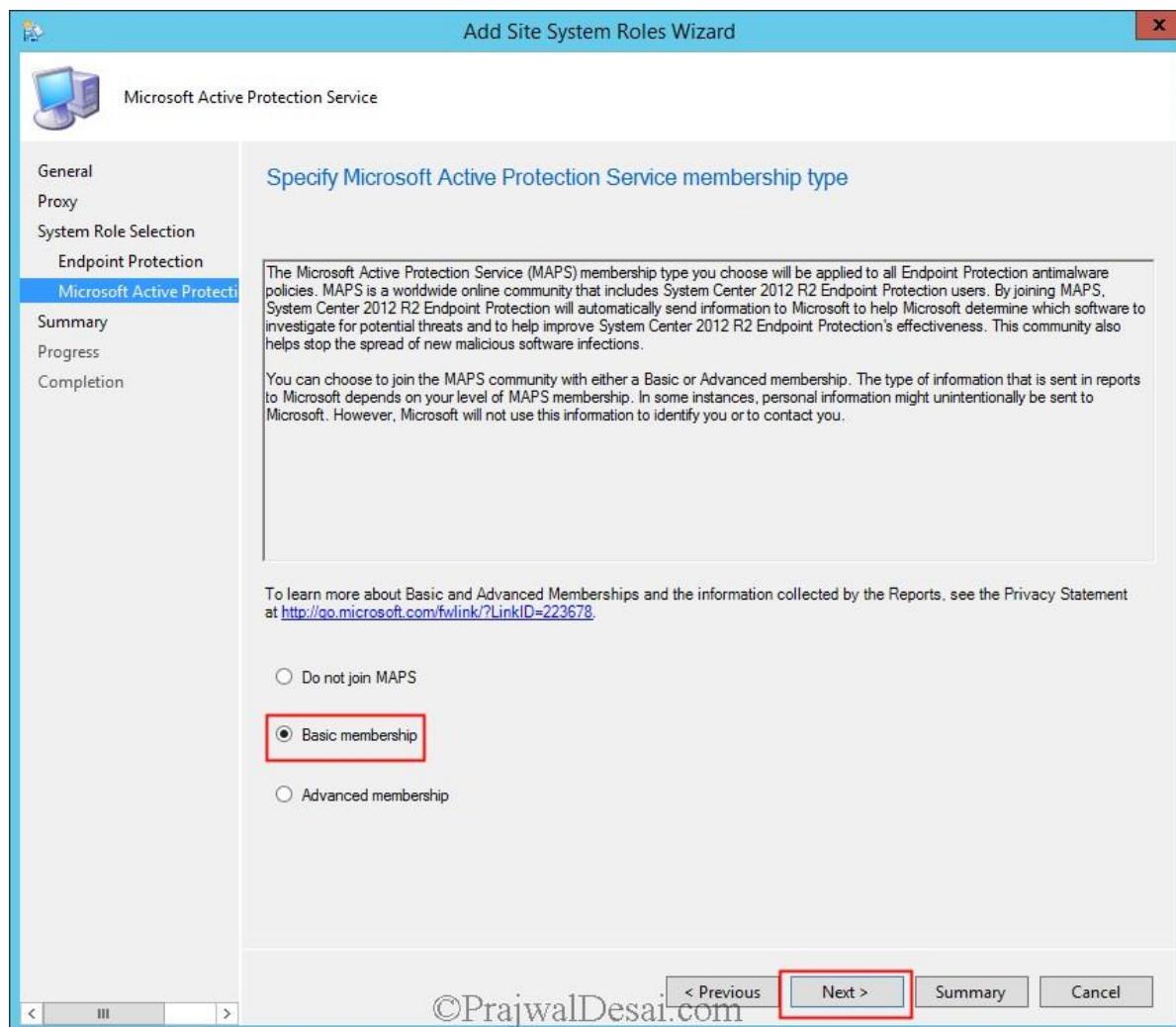


©PrajwalDesai.com

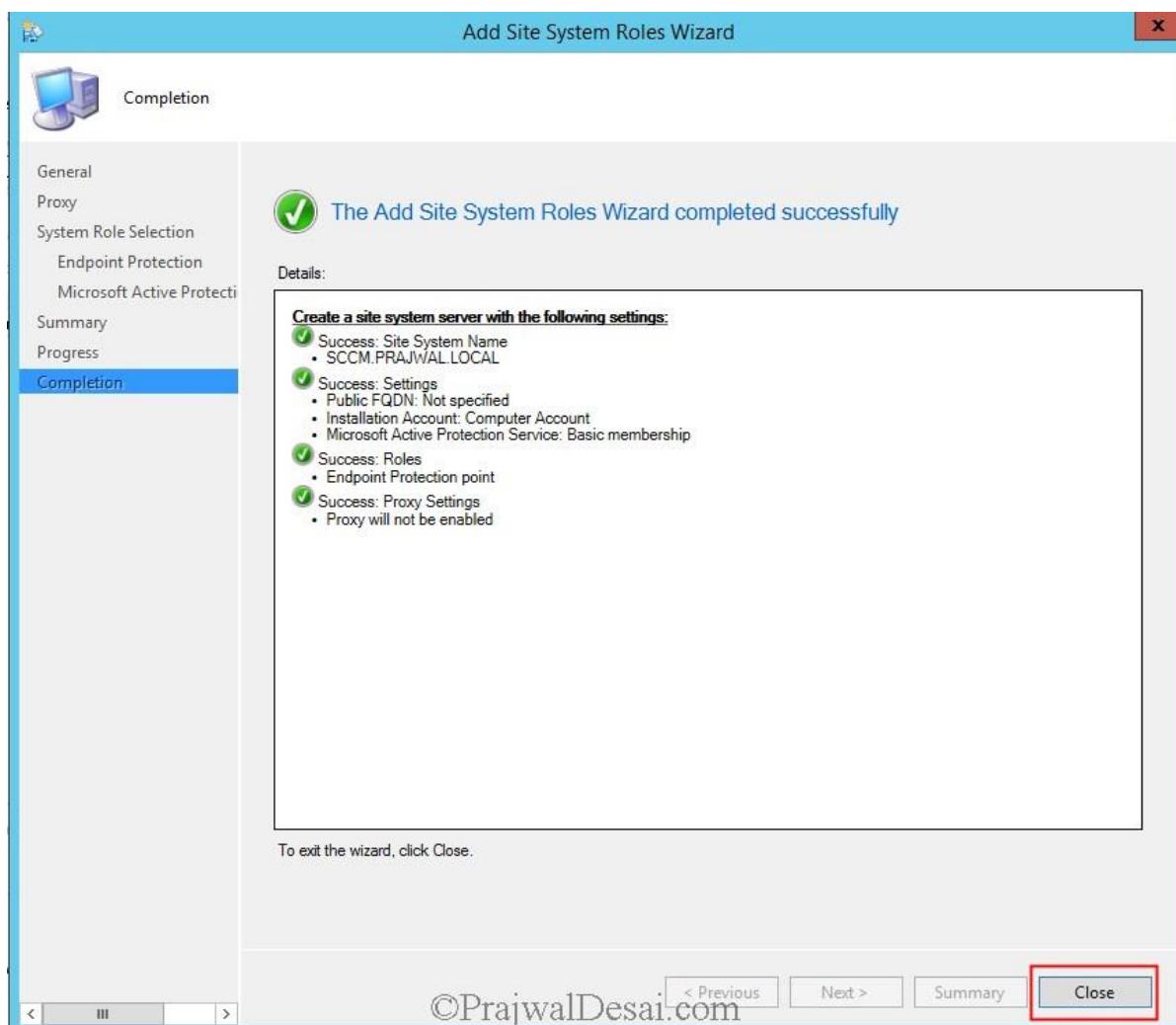
Click on **I accept the EP license terms** and click **Next**.



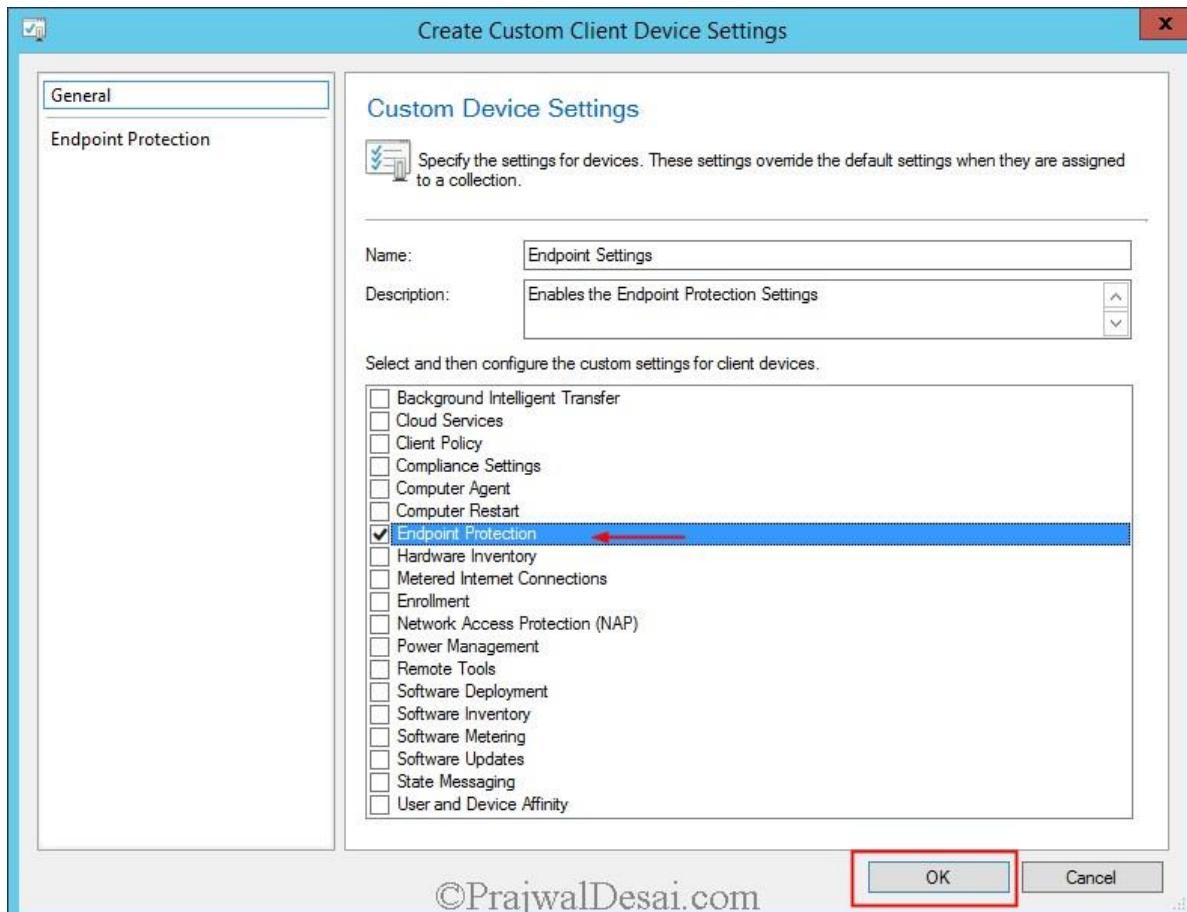
For MAPS membership type select **Basic Membership**, click **Next**.



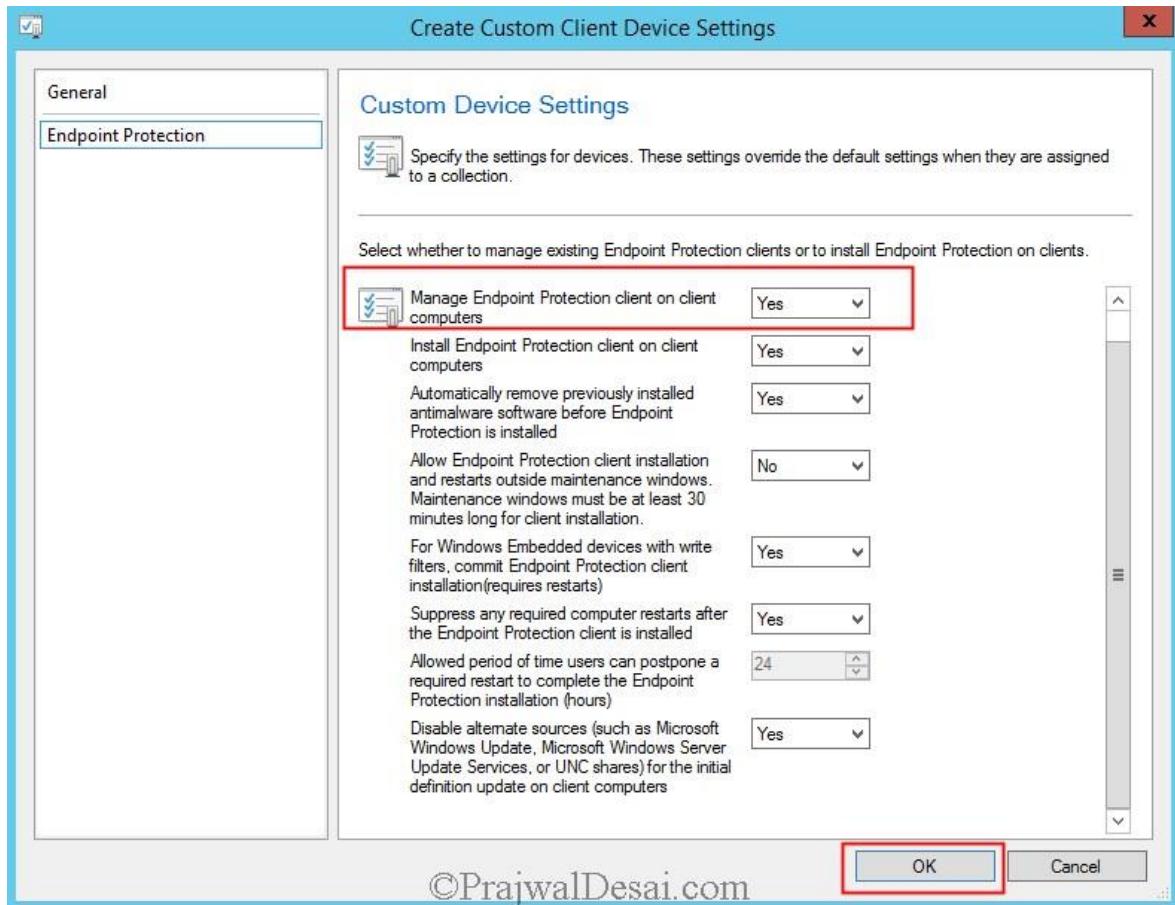
The Endpoint Protection role has been installed successfully. Click **Close**.



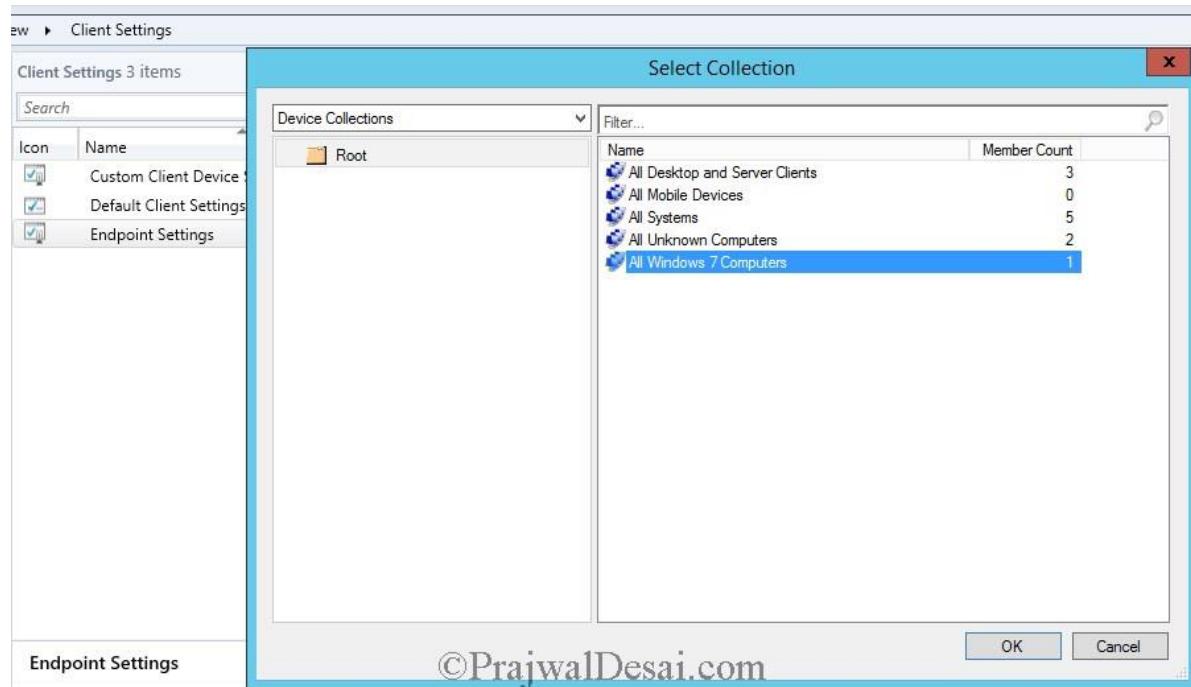
After the installation of Endpoint Protection role, we will now create a **Custom client device settings** for Endpoint protection. You need to enable this setting to install Endpoint Protection client on systems. In the Configuration Manager console click **Administration**, under **Site Configuration**, right click **Client Device settings** and click on **Create Custom Client Device Settings**. Specify a name for the custom client device settings and check **Endpoint Protection** and click **OK**.



On the left pane click **Endpoint Protection** setting, on the right side set **Manage Endpoint Protection client on client computers** to **Yes**. When you enable this setting the Configuration Manager can be used to manage the endpoint protection clients on the client computers. Below it there is another setting **Install Endpoint Protection client on client computers**, when you enable this setting and if this device settings is deployed to the target collection, the endpoint protection client is installed on all the computers present inside the target collection. Likewise you can configure the remaining settings as per your requirement. Click on **OK**.

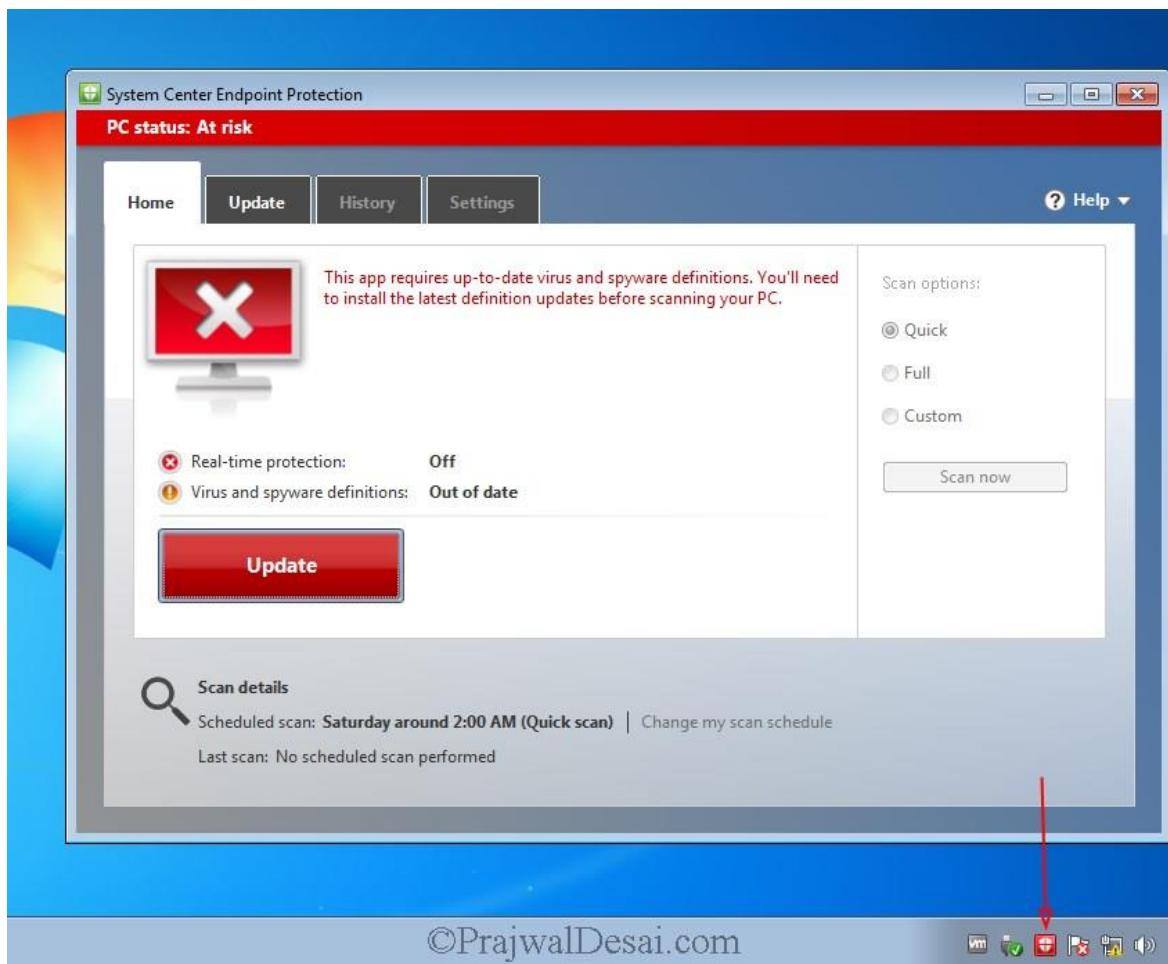


The EP client device settings that we created in above step is deployed to the target collection named **All Windows 7 Computers**.



After few minutes when you log in to one of the machines which was a part of target collection to which the EP client device settings was applied, we see that the EP client has been installed but it needs to be updated (Status color is RED) as the definition updates are missing.

When you install an Endpoint Protection point, an Endpoint Protection client is installed on the server hosting the Endpoint Protection point.



Next we will create an Antimalware policy. Antimalware policies when deployed to the collections specify how Endpoint Protection protects them from malware and other threats. These antimalware policies include information about the scan schedule, the types of files and folders to scan, and the actions to take when malware is detected. When you enable Endpoint Protection, a default antimalware policy is applied to client computers. You can also use additional policy templates that are supplied or create your own custom antimalware policies to meet the specific needs of your environment. It's recommended to create your own antimalware policy.

To create a antimalware policy, in Configuration Manager console, click **Assets and Compliance** expand **Endpoint Protection**, right click **Antimalware Policies** and click **Create Antimalware Policy**.

System Center 2012 R2 Configuration Manager (Connected to IND - Bangalore Headquarters Site)

Home

Create Antimalware Policy Import Saved Searches Search

Assets and Compliance Overview Endpoint Protection Antimalware Policies

Assets and Compliance Overview Devices All Systems User Collections Device Collections User State Migration Asset Intelligence Software Metering Compliance Settings Endpoint Protection Antimalware Policies Windows Firewall Policies Create Antimalware Policy Import

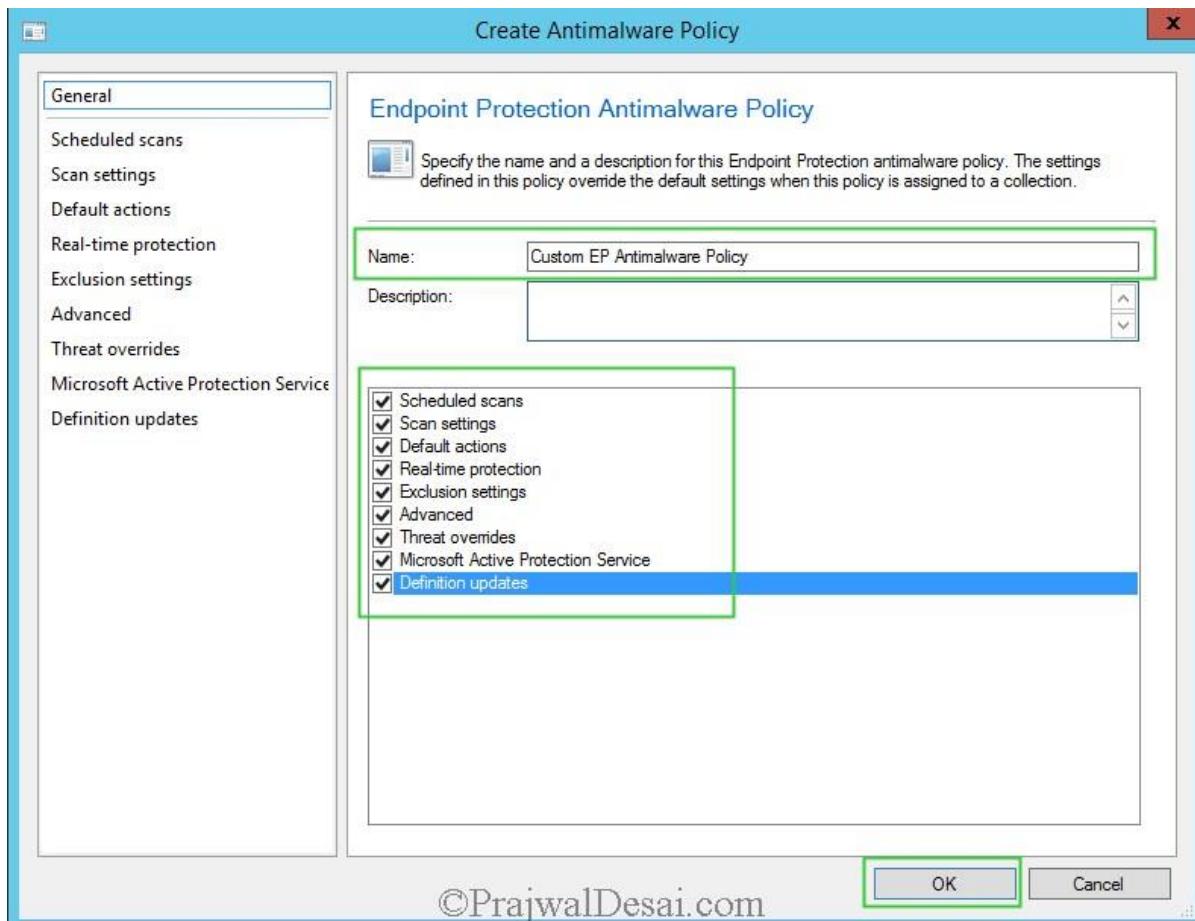
Antimalware Policies 1 items

Icon	Name	Type	Order	Deployments
<input checked="" type="checkbox"/>	Default Client Antimalware Policy	Default	10000	0

Assets and Compliance ©PrajwalDesai.com

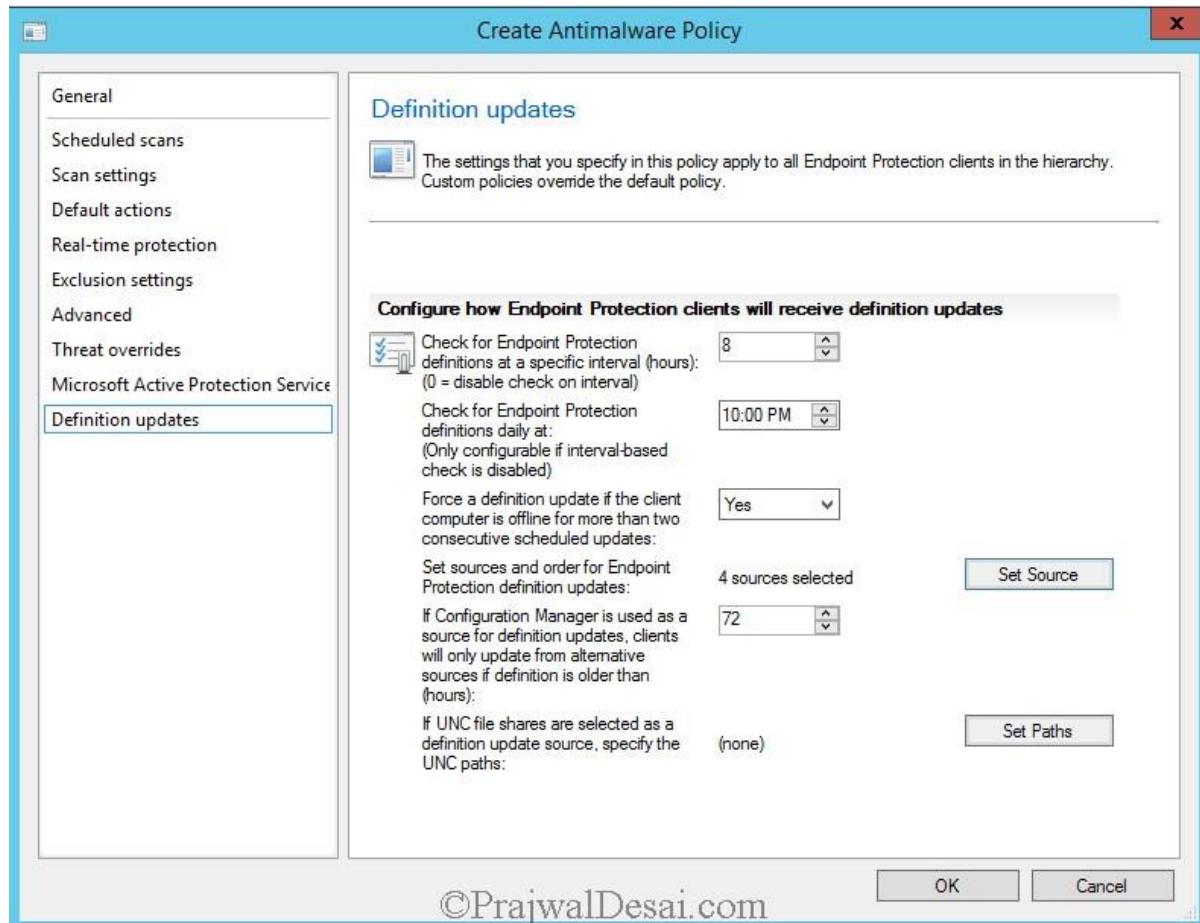
The screenshot shows the System Center 2012 R2 Configuration Manager interface. The left navigation pane is expanded to show the 'Endpoint Protection' section, specifically the 'Antimalware Policies' item. A red box highlights the 'Create Antimalware Policy' button in the toolbar at the bottom of the main content area. The right side displays a table of existing Antimalware Policies, with one entry named 'Default Client Antimalware Policy'. The bottom status bar shows 'Assets and Compliance' and the copyright information '©PrajwalDesai.com'.

Specify a name for the new antimalware policy and enable all the settings as shown in the below screenshot. Click **OK**.

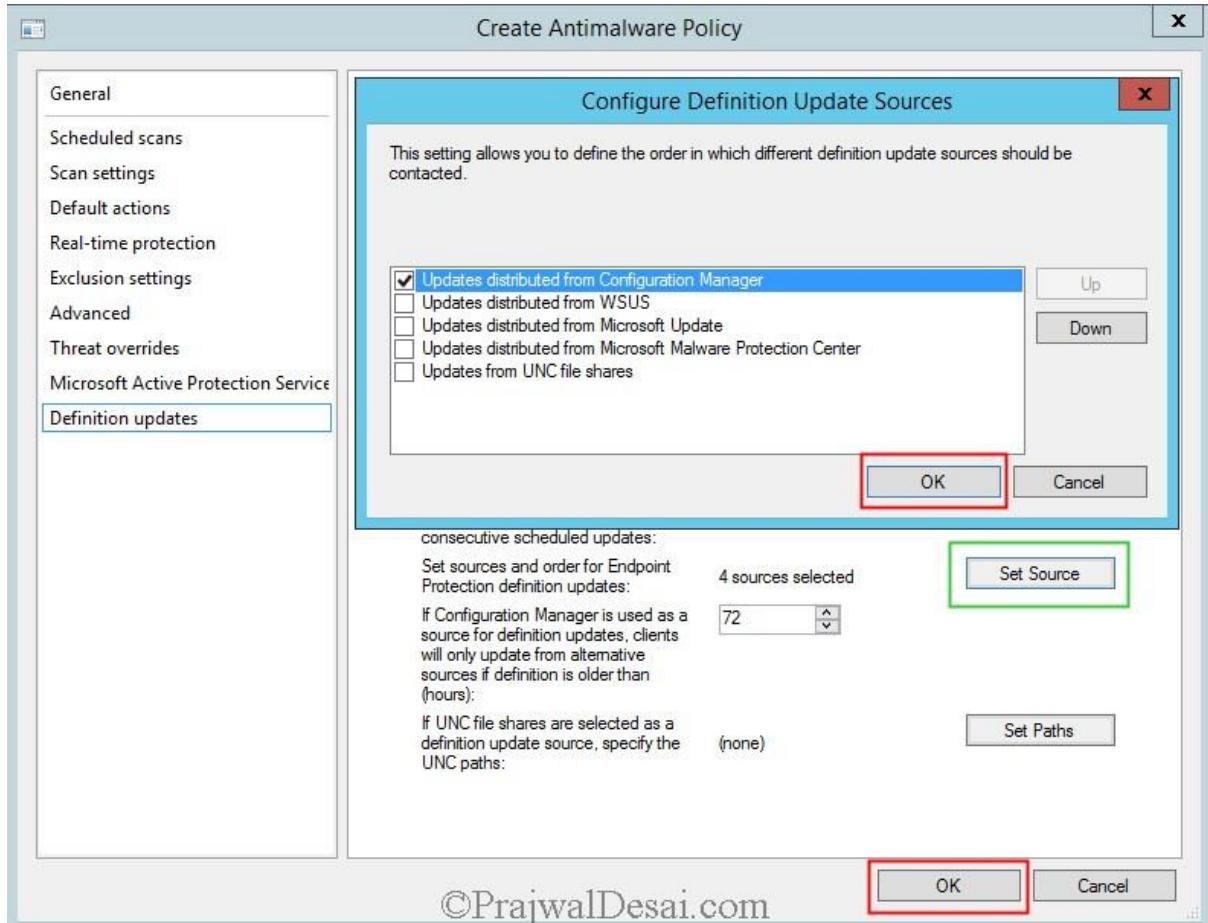


©PrajwalDesai.com

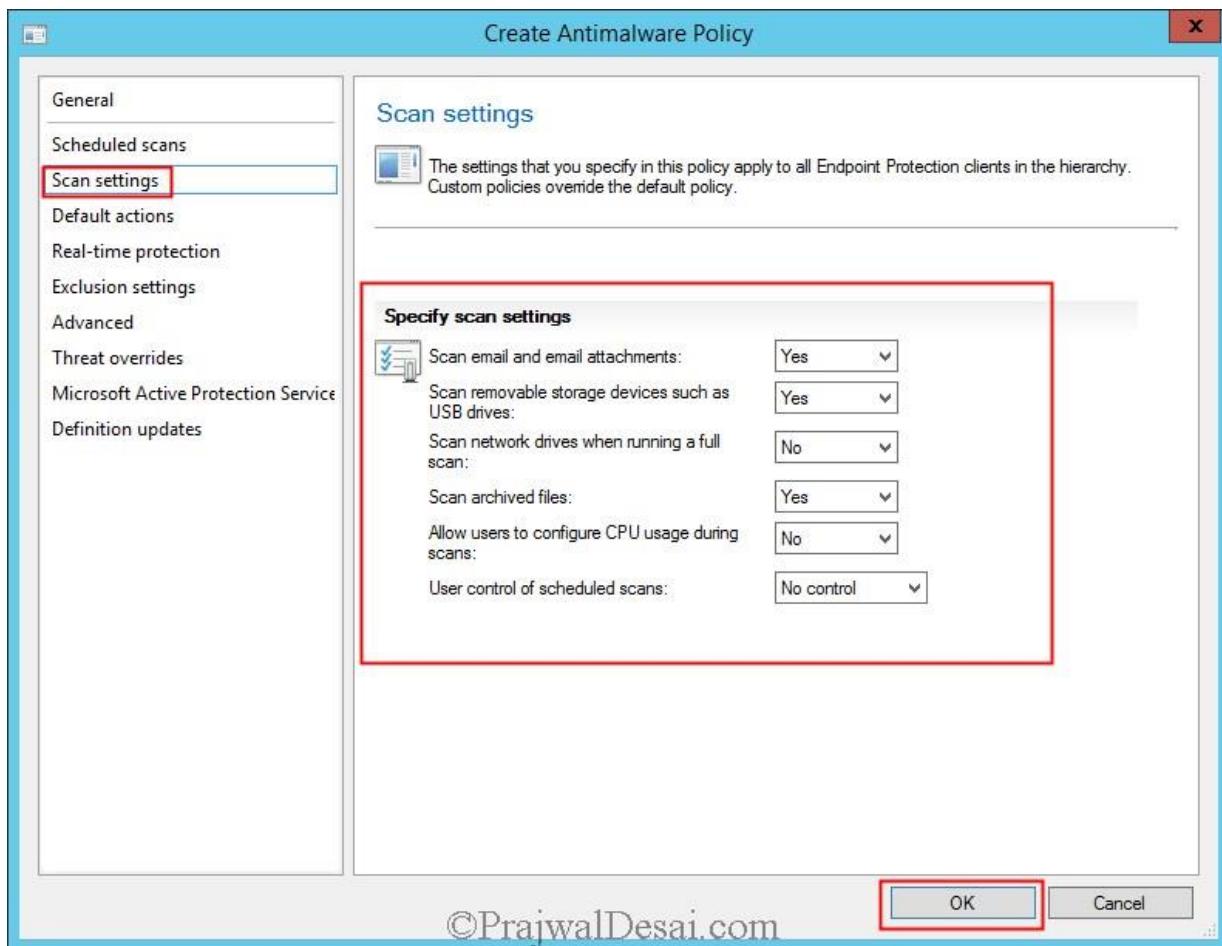
On the left pane, click **Definition updates**, on the right pane we see the settings on how EP clients will receive definition updates.



Click on **Set Source**, we see a new window showing the options using which we can deploy the definition updates to the EP clients. Uncheck all the sources and select **Updates distributed from Configuration Manager** and click **OK**. This option uses Configuration Manager software updates to deliver definition and engine updates to computers in your hierarchy.



On the left pane select **Scan Settings**, on the right pane you will find the scan settings such as scan email and attachments, scan removable drives etc. Configure these settings as per your requirements and click **OK**.



The next step is to deploy the custom antimalware policy to a collection. Right click on the antimalware policy and click **Deploy**. Choose the target collection and click **OK**.

Overview ► Endpoint Protection ► Antimalware Policies

Antimalware Policies 2 items

Search

Icon	Name	Type	Order	Deployments	Description
<input checked="" type="checkbox"/>	Custom EP Antimalware Policy	Custom	1	0	
<input checked="" type="checkbox"/>	Default Client Antimalware Policy	Default	10000	0	Settings that apply to all clients in the hierarchy

Select Collection

Device Collections

Root

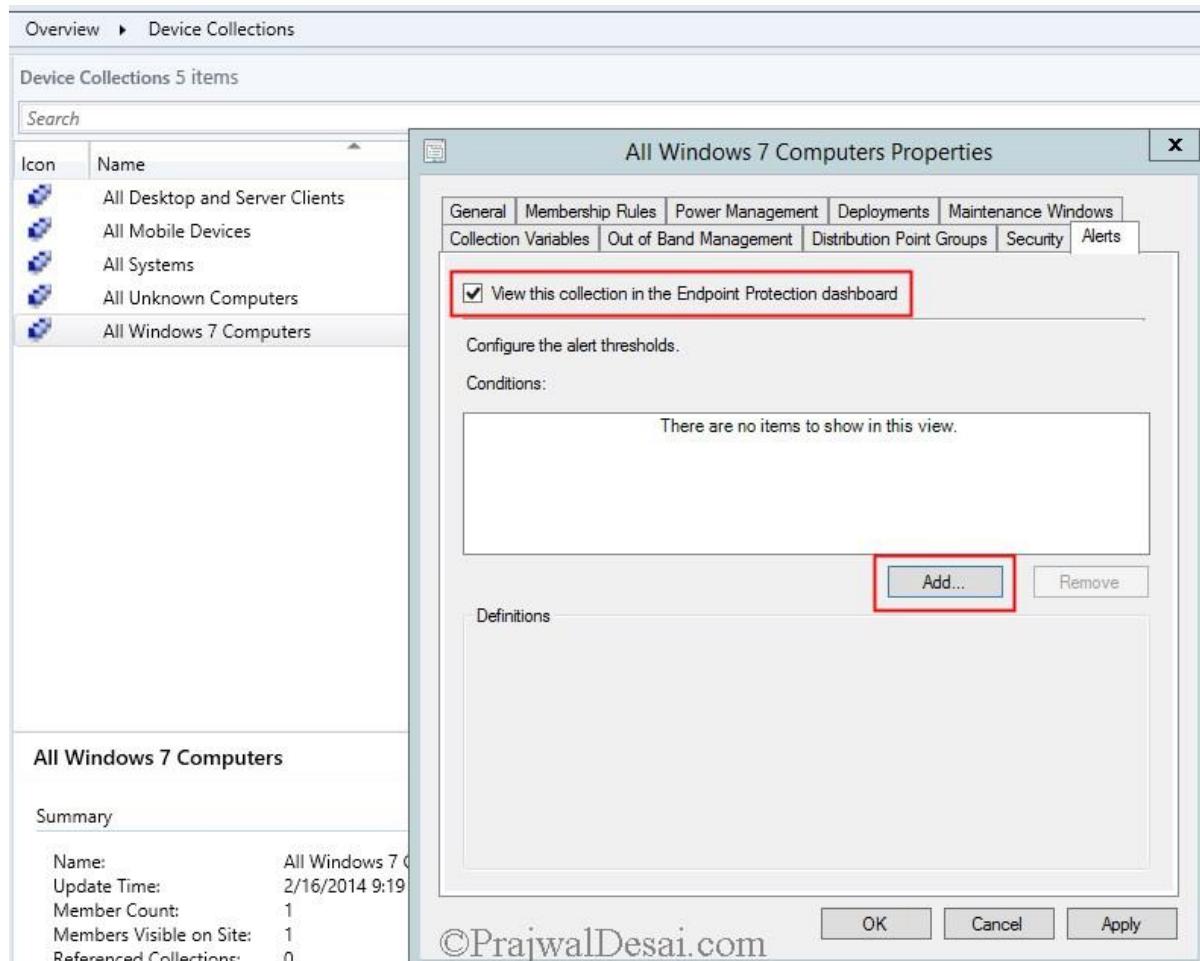
Name	Member Count
All Desktop and Server Clients	3
All Mobile Devices	0
All Systems	5
All Unknown Computers	2
All Windows 7 Computers	1

©PrajwalDesai.com

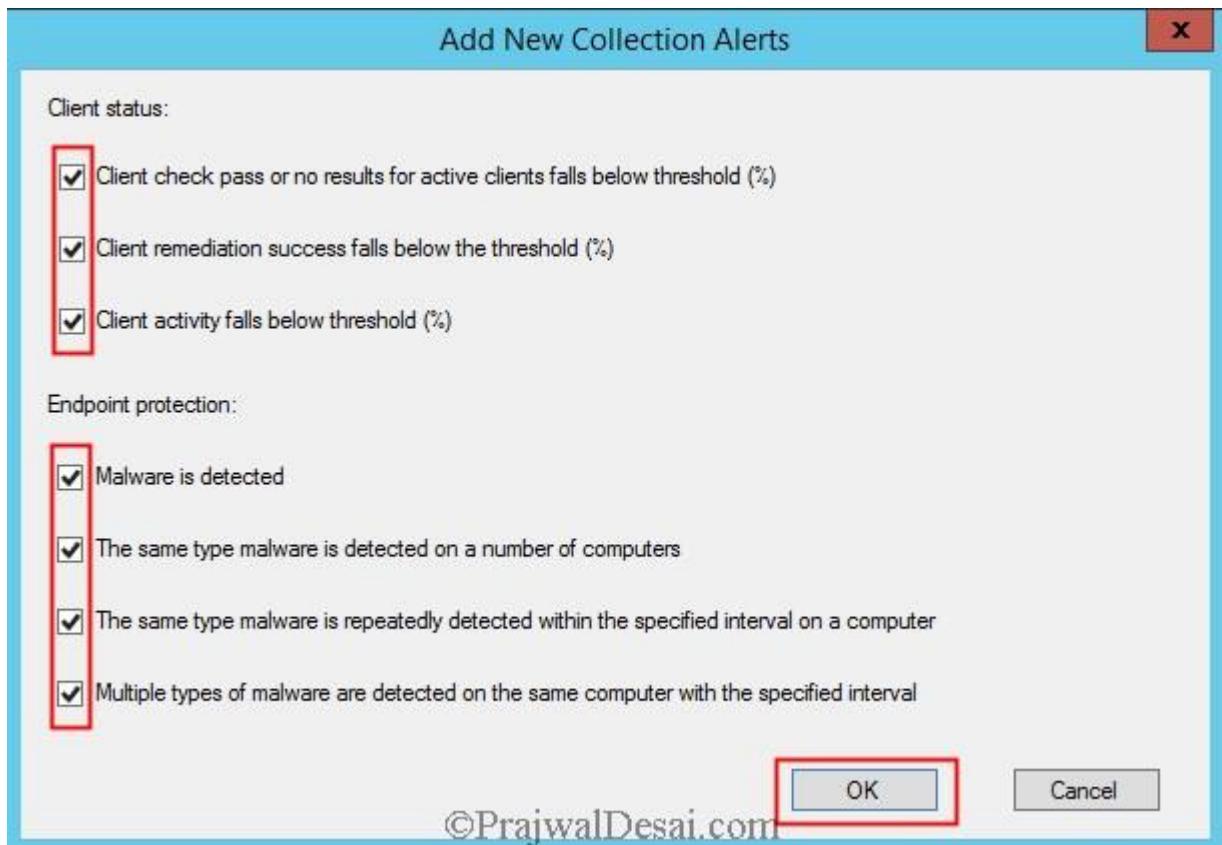
OK Cancel

Detailed description: This screenshot shows a 'Select Collection' dialog box overlaid on a main interface. The dialog has a title bar 'Select Collection'. On the left, there's a dropdown menu set to 'Device Collections' and a tree view showing 'Root'. The main area is a table with columns 'Name' and 'Member Count'. It lists several collections: 'All Desktop and Server Clients' (3 members), 'All Mobile Devices' (0 members), 'All Systems' (5 members), 'All Unknown Computers' (2 members), and 'All Windows 7 Computers' (1 member). A red arrow points to the 'Member Count' column for the 'All Windows 7 Computers' row. At the bottom right of the dialog are 'OK' and 'Cancel' buttons, with 'OK' being highlighted by a red box.

In the Configuration Manager console, click on **Assets and Compliance** select **Devices** and choose **Device Collections**, right click target collection on which you deployed the antimalware policy and click on **properties**. Click on **Alerts**, check the box **View this collection in the Endpoint Protection Dashboard**. Click **Add**.

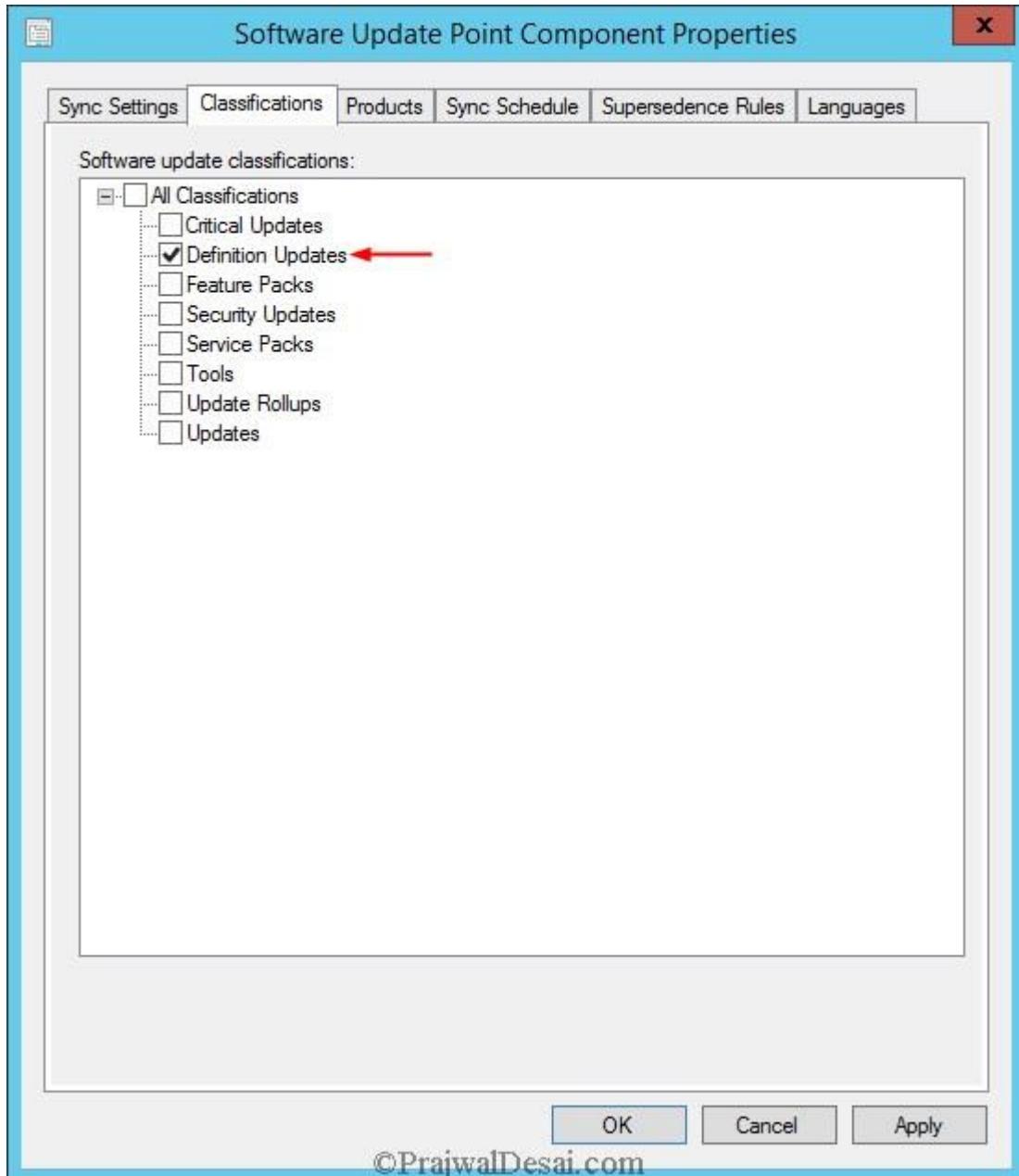


In **Add New Collection Alerts** window, check **all the boxes** and click **OK**. Click **OK** again to close the Computer properties window.

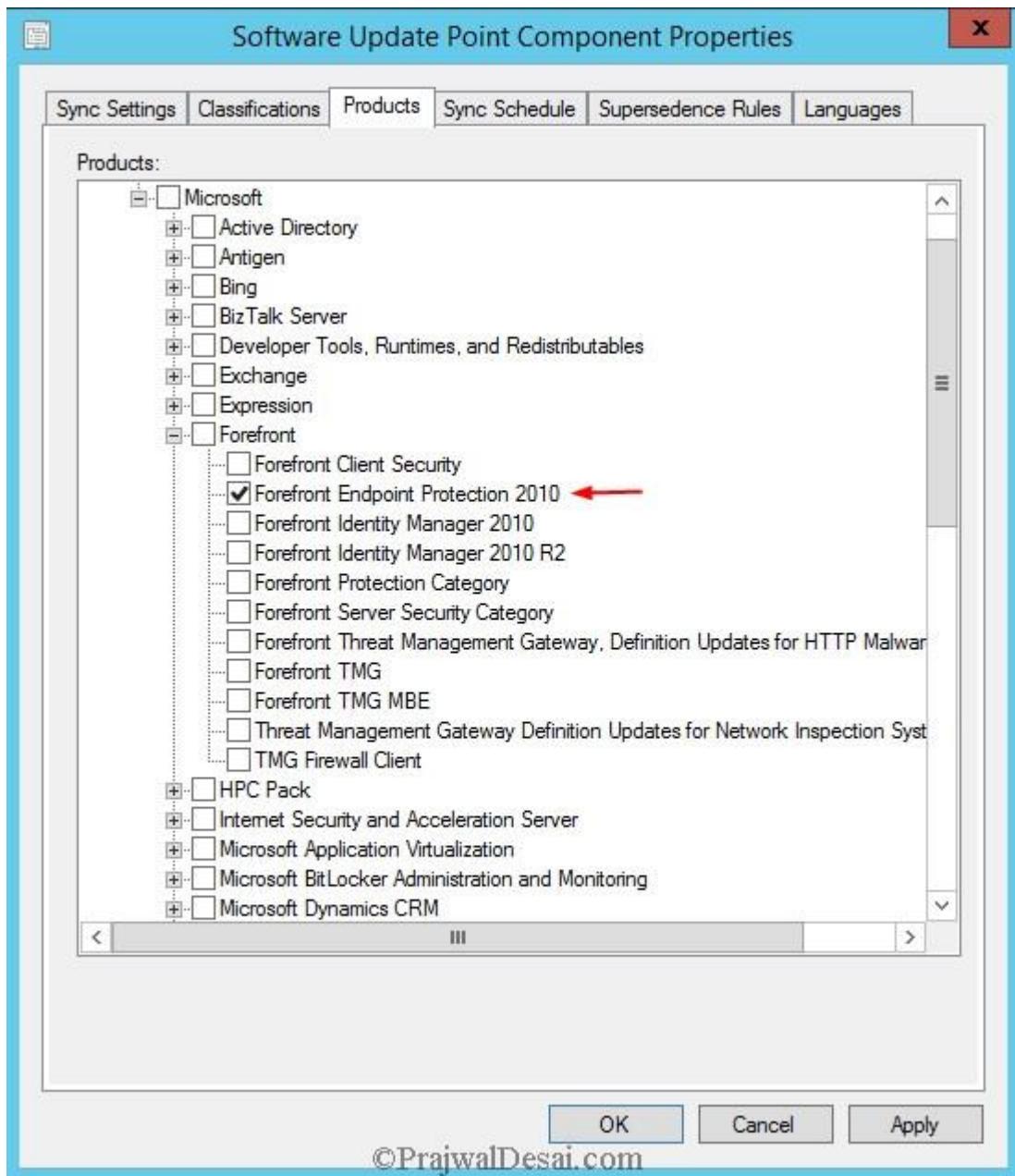


©PrajwalDesai.com

We will now configure the **Software Update Point** to download the EP definition updates. In the **Configuration Manager** console, click on **Administration**, under **Site Configuration** click **Sites**, under **Configure Site Components**, click **Software Update Point**. In the **Classifications** tab you must select **Definition Updates**. Click on **Apply**.



In the **Products** tab, select **Forefront Endpoint Protection 2010** as the product and click **Apply** and then click **OK**.



©PrajwalDesai.com

In the Configuration Manager console, Click on **Software Library**, expand **Software Updates**, right click on **All Software Updates** and choose **Synchronize Software Updates**. After the synchronization process is over you should see the list of definition updates under **All Software Updates**.

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed	Expired
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4096.0)	0	0	0	0	No	No	No
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4119.0)	0	0	0	0	No	No	No
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4146.0)	0	0	0	0	No	No	No
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4160.0)	0	0	0	0	No	No	No
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4171.0)	0	0	0	0	No	No	No
	Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4181.0)	0	0	0	0	No	No	No

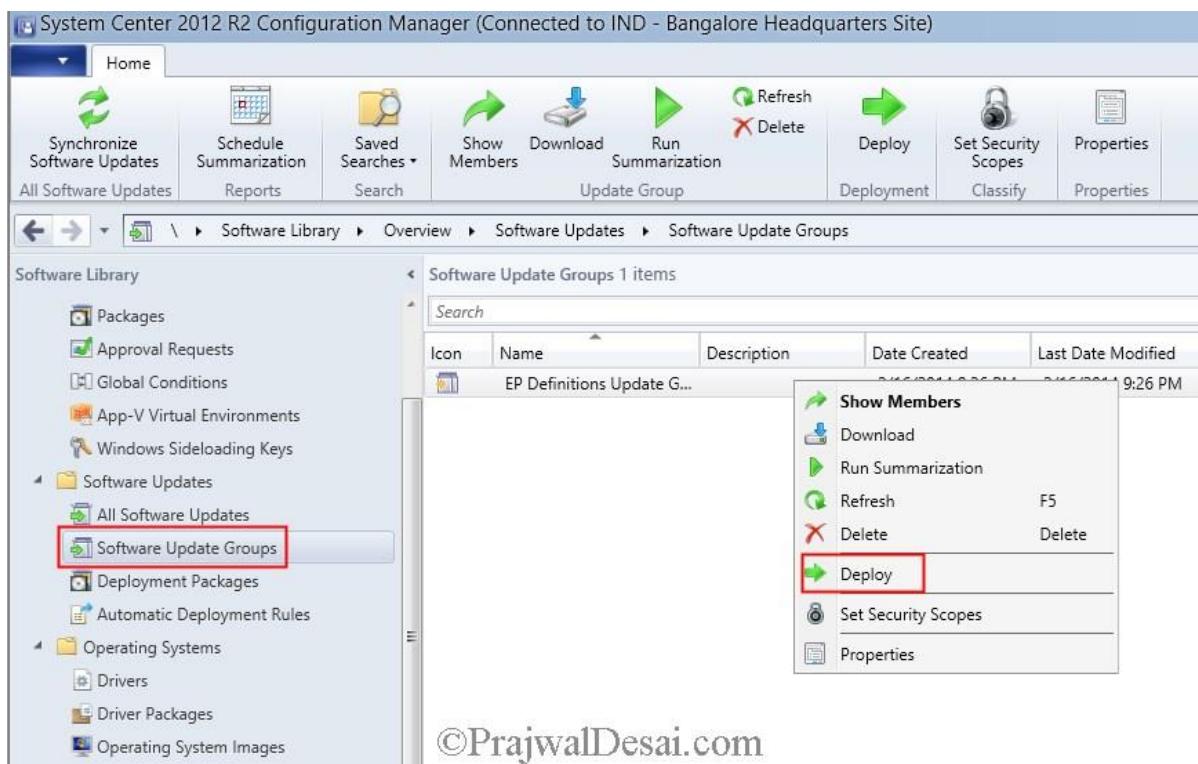
©PrajwalDesai.com

We will now select all the definition updates and put them inside a **Software Update Group**. To create a SUG, select the updates and right click and click on **Create Software Update Group**. Provide a name to SUG and click **Create**.

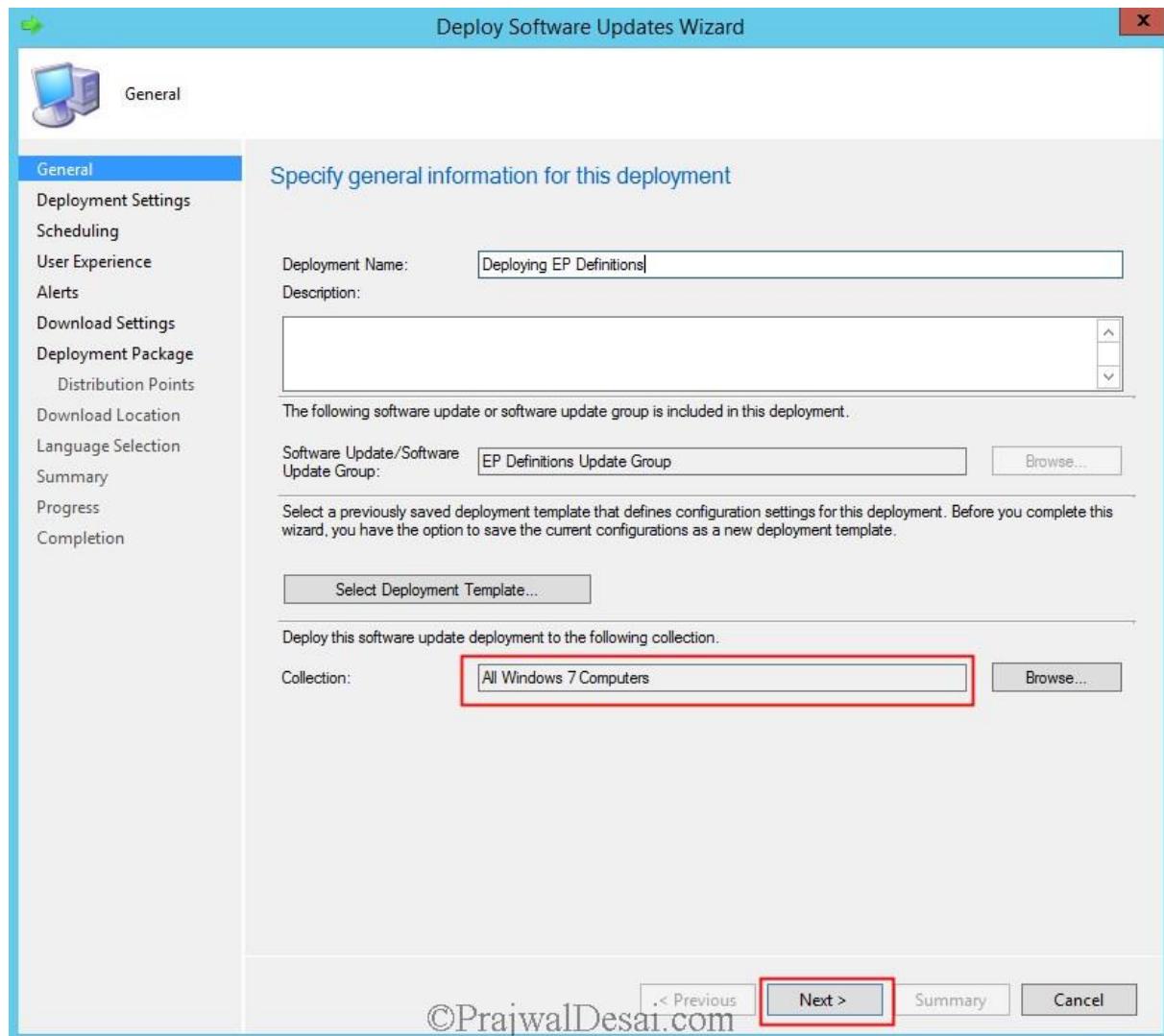
©PrajwalDesai.com

Click on **Software Update Groups**, right click on the Software Update Group that we created and click on **Deploy**.

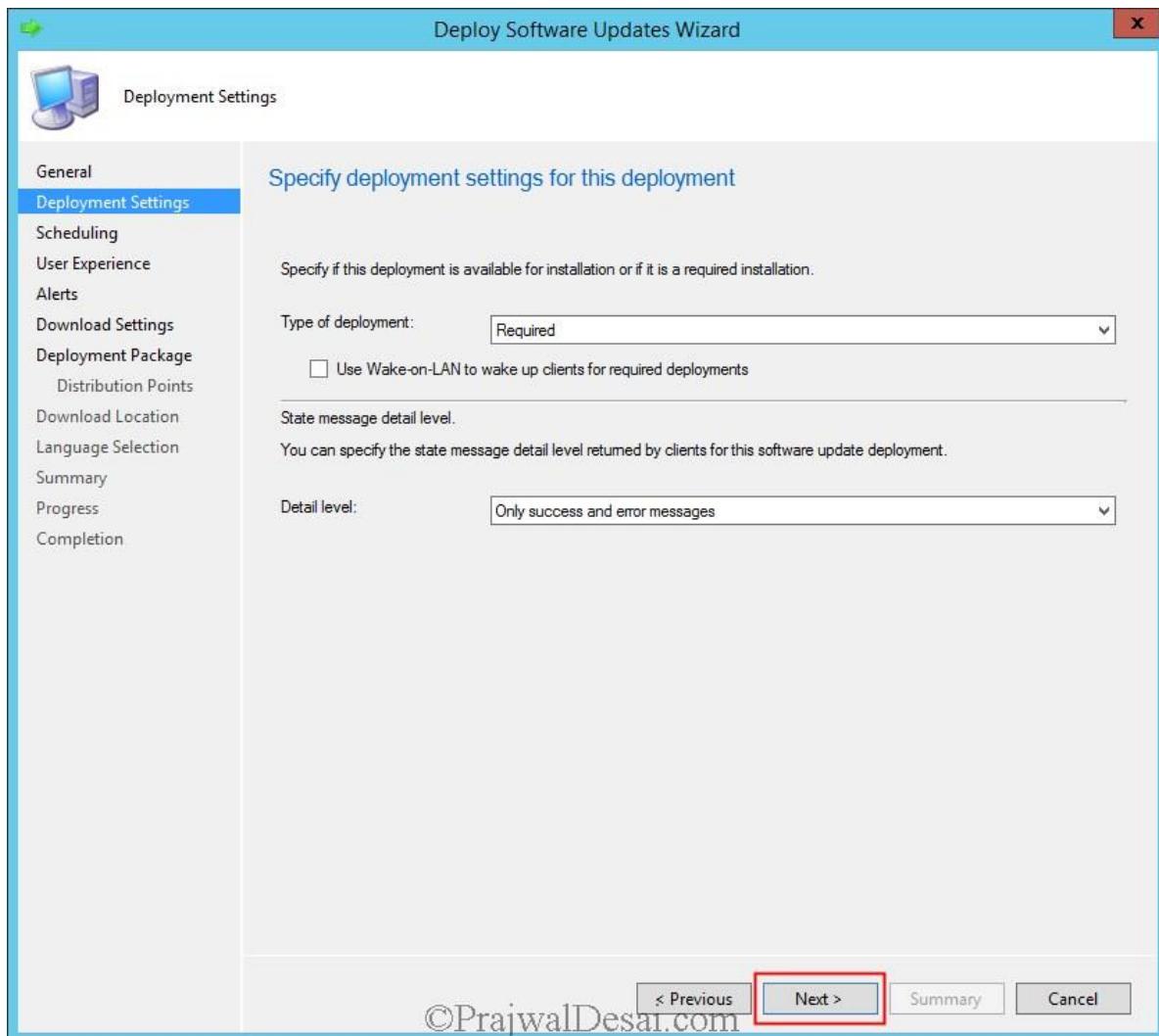
There are 2 ways to deploy the definitions – Manual and Automatic. In this example we will be deploying the EP definitions manually. If you want to deploy definition updates using Automatic method then you can create an Automatic Deployment Rule.



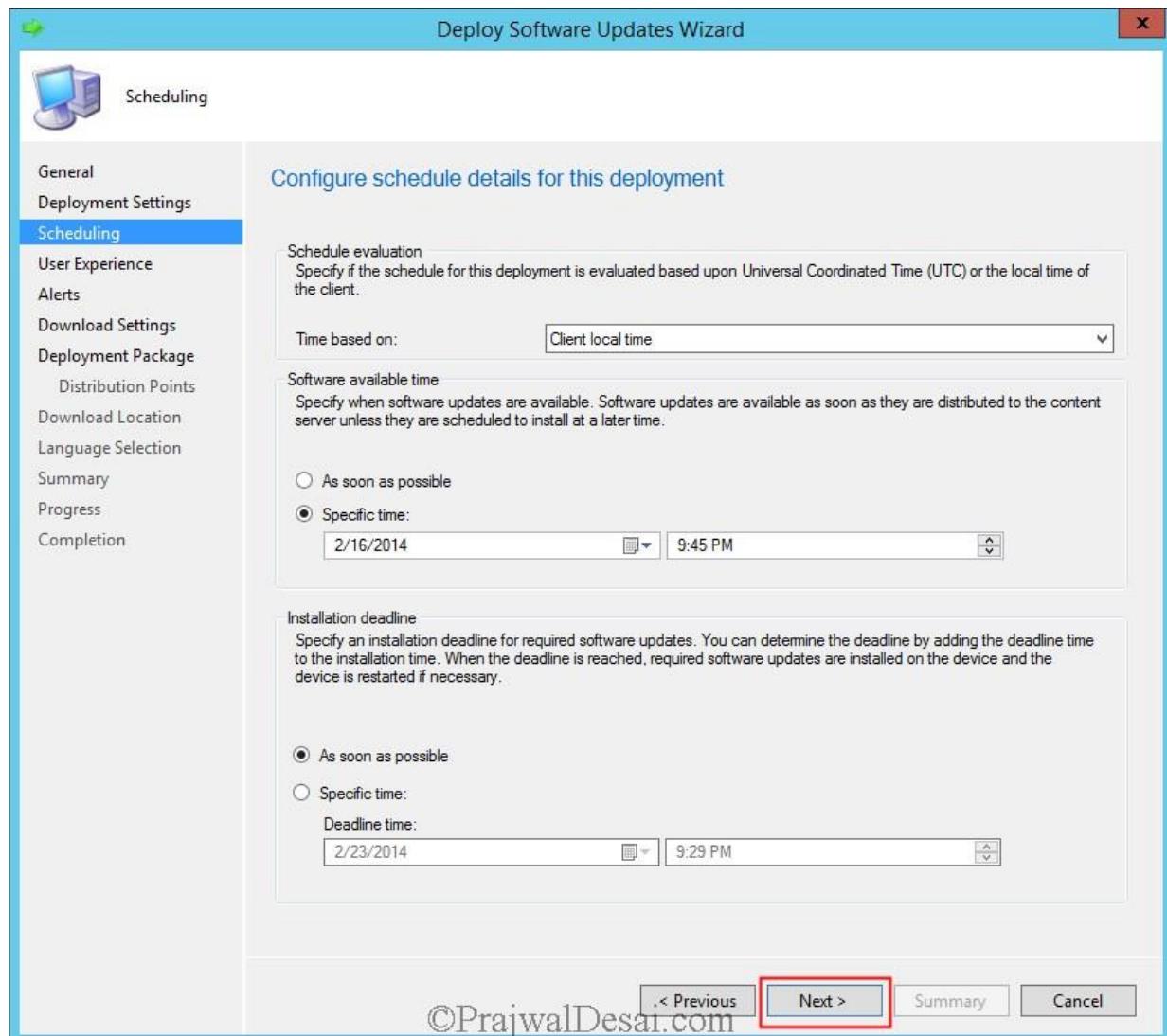
Specify the **Deployment Name**, choose the collection to which you want to deploy this software update deployment. Click **Next**.



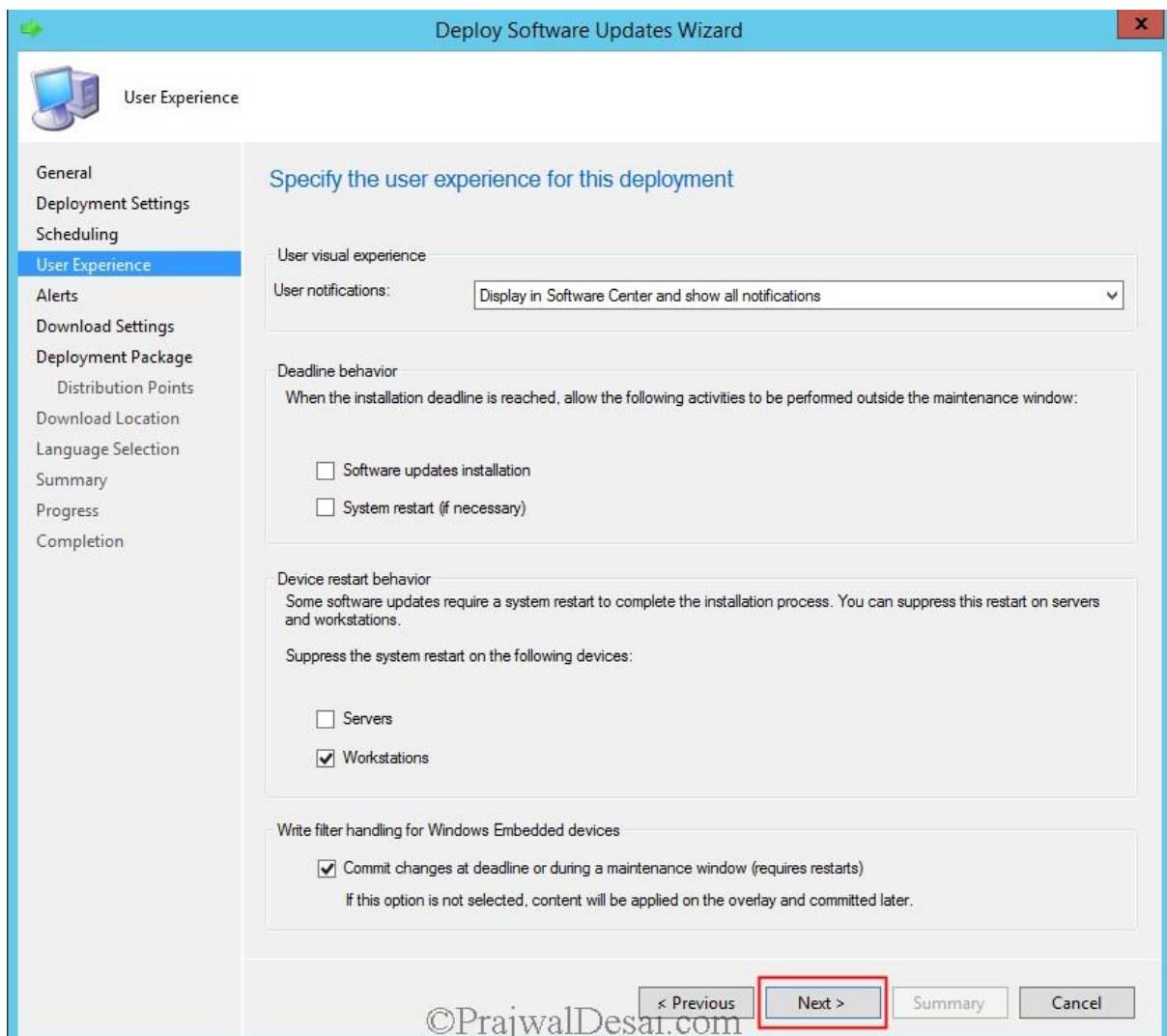
Set the **Type of Deployment** to **Required** and set the **Detail Level** to **Only success and error messages**. Click **Next**.



Choose the **Time based on** to **Client local time**, **Software available time** to **specific time**, **Installation deadline** to **As soon as possible**. Click **Next**.

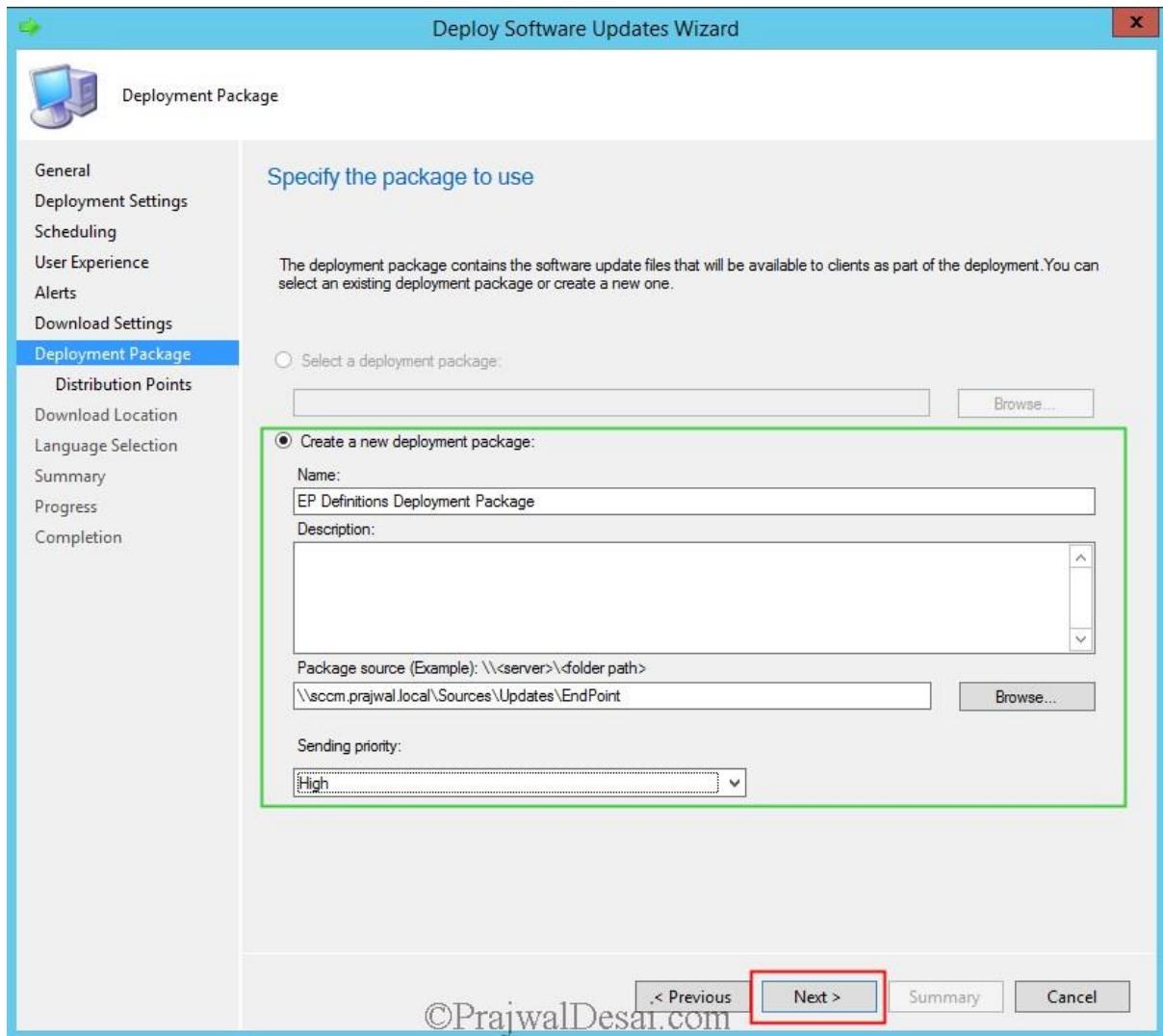


Click **Next**.

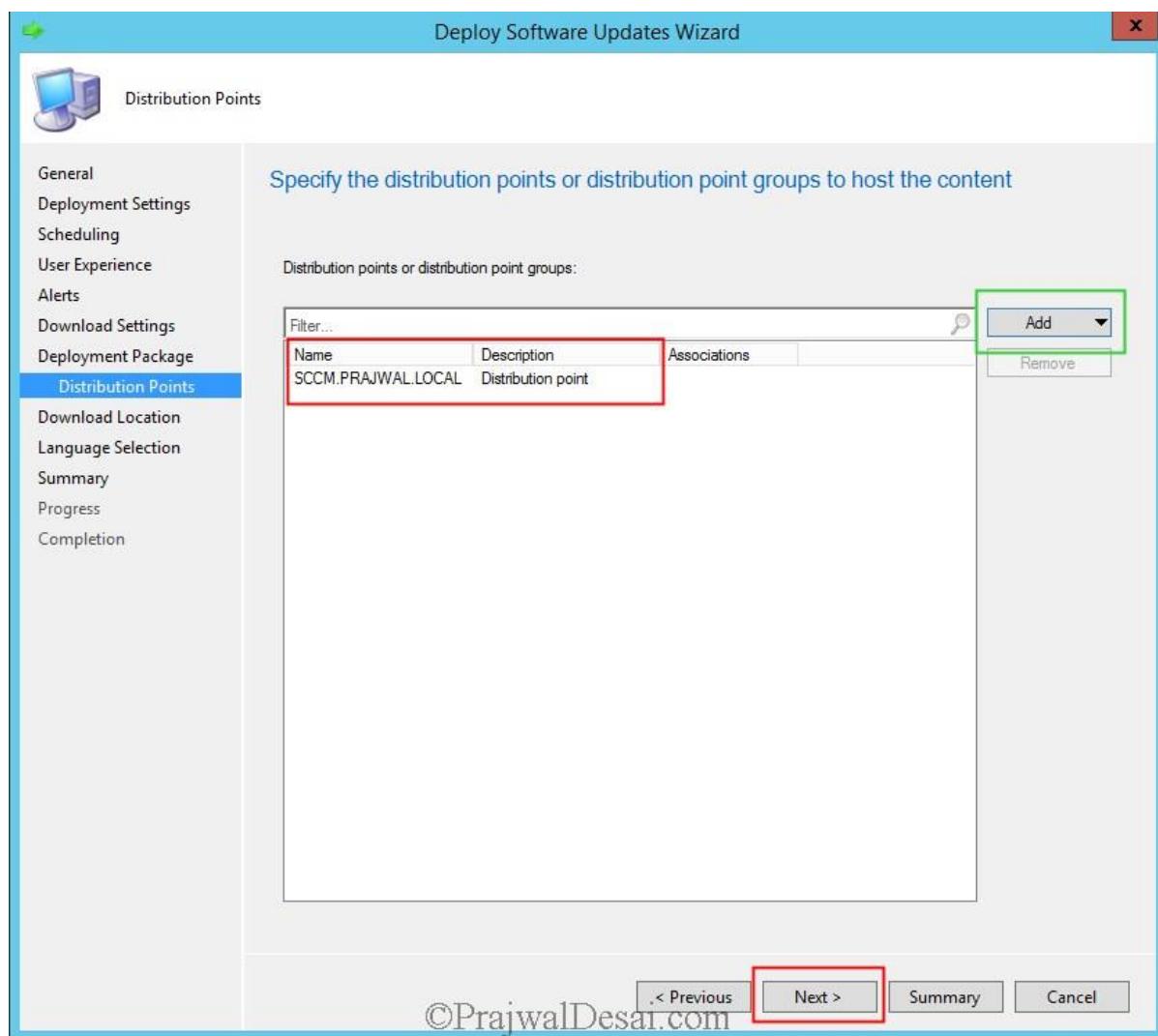


If you are using Configuration Manager software updates to distribute definition updates, consider placing definition updates in a package that does not contain other software updates. This keeps the size of the definition update package smaller which allows it to replicate to distribution points more quickly.

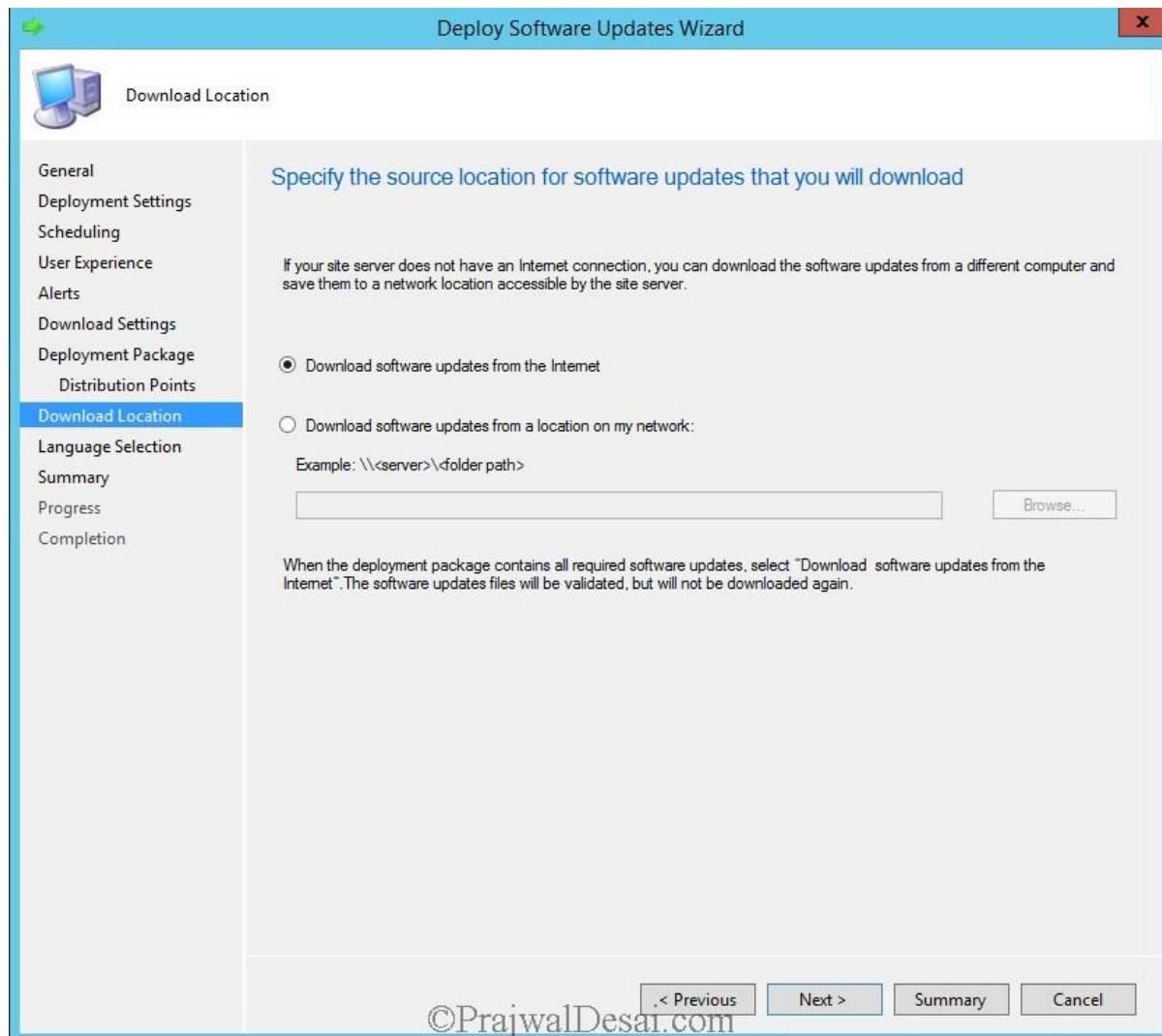
We will create a new deployment package to deploy the definition updates. Specify the **Name** and **Package source** and click **Next**.



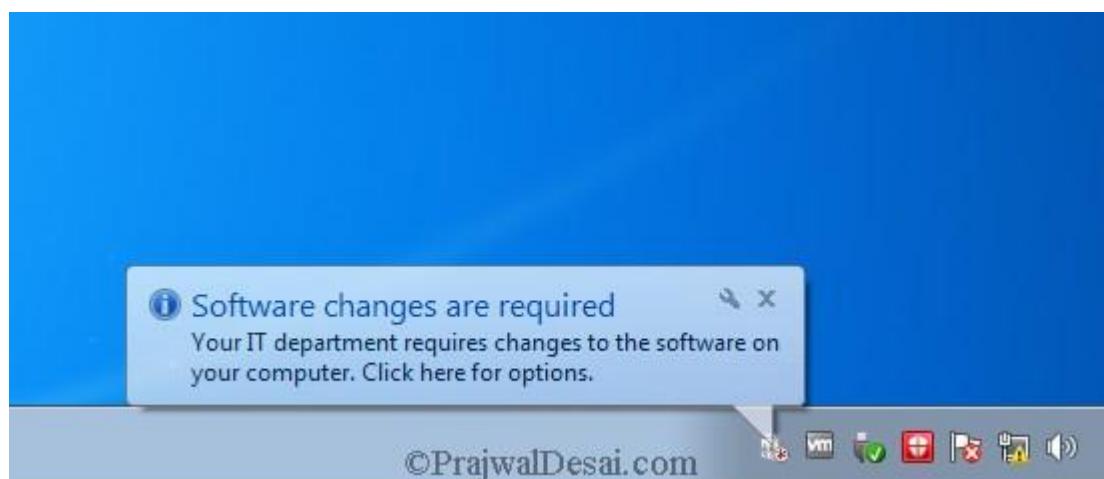
Add the DP and click **Next**.



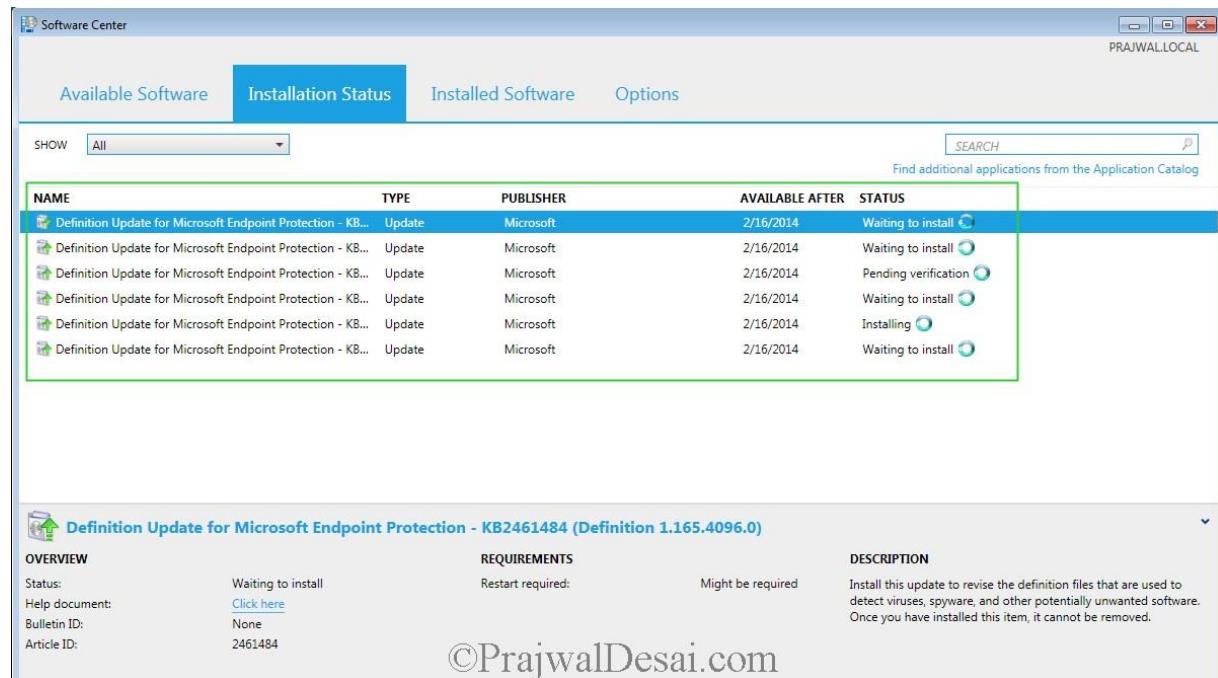
Choose **Download software updates from the Internet**. Click **Next** and click **Close** to close the wizard.



On the client machine we see a notification that **Software changes are required**.



The definition updates are downloaded from the DP and then installed on the client systems.



This screenshot shows the Software Center interface on a Windows system named PRAJWAL.LOCAL. The 'Installation Status' tab is selected. A green box highlights a row in the table where the status is 'Waiting to install'. Below the table, a detailed view of the update 'Definition Update for Microsoft Endpoint Protection - KB2461484' is shown, indicating it is waiting to be installed.

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Waiting to install
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Waiting to install
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Pending verification
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Waiting to install
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installing
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Waiting to install

Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4096.0)

OVERVIEW

Status: Waiting to install
Help document: [Click here](#)
Bulletin ID: None
Article ID: 2461484

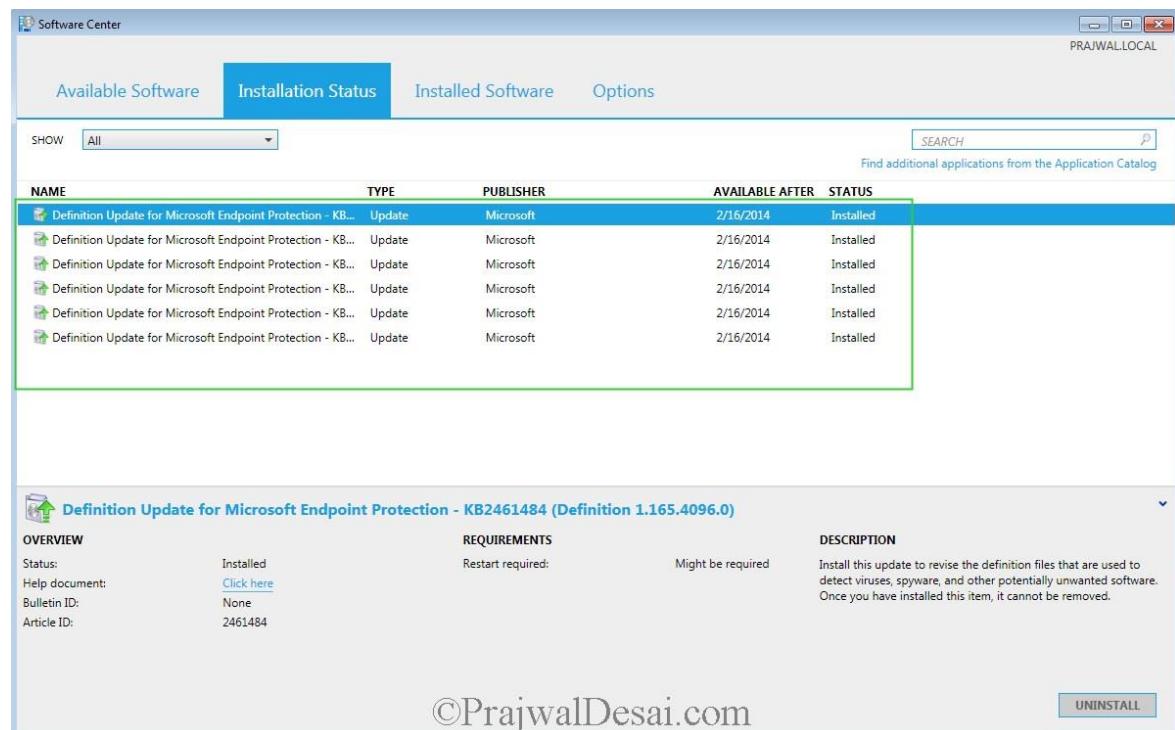
REQUIREMENTS

Restart required: Might be required

DESCRIPTION

Install this update to revise the definition files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

The definition updates are installed successfully.



This screenshot shows the Software Center interface on the same Windows system. The 'Installation Status' tab is selected. A green box highlights a row in the table where the status is 'Installed'. Below the table, a detailed view of the same update is shown, now with an 'Installed' status. An 'UNINSTALL' button is visible at the bottom right of the update details.

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installed
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installed
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installed
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installed
Definition Update for Microsoft Endpoint Protection - KB...	Update	Microsoft	2/16/2014	Installed

Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.165.4096.0)

OVERVIEW

Status: Installed
Help document: [Click here](#)
Bulletin ID: None
Article ID: 2461484

REQUIREMENTS

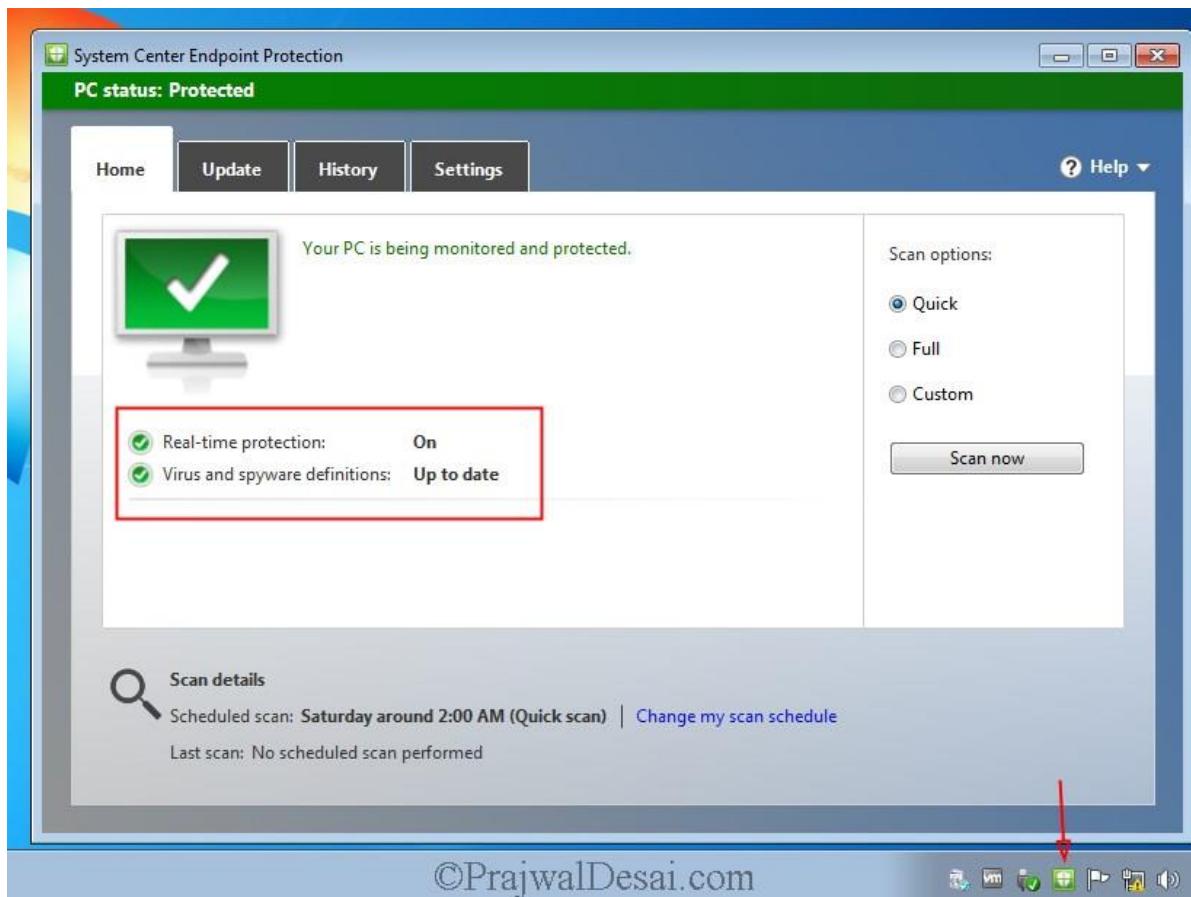
Restart required: Might be required

DESCRIPTION

Install this update to revise the definition files that are used to detect viruses, spyware, and other potentially unwanted software. Once you have installed this item, it cannot be removed.

UNINSTALL

Now see the change, the status of EP client is Green and virus and spyware definitions are up to date.



Managing Linux Computers Using System Center 2012 R2 Configuration Manager

Managing Linux Computers Using System Center 2012 R2 Configuration Manager

In this post we will take a look at steps for managing linux computers using System Center 2012 R2 Configuration manager (SCCM 2012 R2). If I look back at my post on [Installing SCCM 2012 SP1 client agents on linux computers](#) it was just about the installation of SCCM client agents on the linux machine. In this post we will not only install the SCCM 2012 R2 client on linux machine but we will learn more on managing the linux computers using SCCM 2012 R2. We will install the client agent, create a collection for [linux based computers](#), create and deploy the custom client device settings enabling hardware inventory settings, we will see examples of hardware inventory reports and lastly we will see how to uninstall the sccm client out of the linux machines. The System Center 2012 R2 Configuration manager clients for UNIX and Linux extends the scope of your Configuration Manager environment to collect inventory, deploy software, and run reports about UNIX and Linux servers in your enterprise. The client operates as a workgroup client that is managed by Configuration Manager.

When we install SCCM 2012 R2 client agents on linux machine, you can use some of the management capabilities on Linux and UNIX computers while some of them cannot be used.

Supported	Not Supported
Collections, queries, and maintenance windows	Client push installation
Hardware inventory	Operating system deployment
Software deployment	Application deployment
Monitoring	Software inventory
Reporting	Software updates, Compliance settings
Deploy custom client settings	Internet-based client management
Deploy software by using packages and programs	Remote control, Power management
	Client status client check and remediation

Now we will download the SCCM 2012 R2 client agents for linux based computers. You can download the client agent for linux computers by clicking on below button. The following UNIX and Linux versions are supported.

1. AIX Version 7.1, 6.1, 5.3
2. Solaris Version 11, 10, 9
3. HP-UX Version 11iv2 , 11iv3
4. RHEL Version 6 , 5, 4
5. SLES Version 11, 10, 9
6. CentOS Version 6, 5
7. Debian Version 6, 5
8. Ubuntu Version 12.4 LTS, 10.4 LTS
9. Oracle Linux 6, 5

[**SCCM 2012 R2 Clients for Additional Operating Systems**](#)

Download the **ConfigMgr Clients for Linux.exe** and click **Next**.

Choose the download you want 

<input type="checkbox"/> File Name	Size
<input checked="" type="checkbox"/> ConfigMgr Clients for Linux.exe	46.7 MB
<input type="checkbox"/> ConfigMgr Clients for AIX.exe	115.7 MB
<input type="checkbox"/> ConfigMgr Clients for HP-UX.exe	49.0 MB
<input type="checkbox"/> ConfigMgr Clients for Solaris.exe	57.2 MB
<input type="checkbox"/> ConfigmgrMacClient.msi	5.4 MB

Download Summary:
1. ConfigMgr Clients for Linux.exe

Total Size: 46.7 MB

©PrajwalDesai.com

[Next](#)

Once you have downloaded the ConfigMgr clients for linux, extract it to a folder and copy the folder to your Linux machine, copy the files to a directory **/opt/client** (client is a new folder that has been created under /opt) . In this example I am using RedHat 6.2 server on which the SCCM 2012 R2 client agent will be installed.



Before you proceed and install the client agent on linux machine make sure that your linux machine is properly communicating with SCCM server. Use **Ping** to check the connectivity to the SCCM server. To resolve the hostname, open the **terminal** on linux machine and type the command **vi /etc/resolv.conf**. Set the IP address for nameserver (set to DNS Server IP), provide the domain name and search name and save the file.

```
root@localhost:~# File Edit View Search Terminal Help
[root@localhost ~]#
[root@localhost ~]# cd ..
[root@localhost /]# cat /etc/resolv.conf
# Generated by NetworkManager
domain PRAJWAL.LOCAL
search PRAJWAL.LOCAL
nameserver 192.168.100.1
[root@localhost /]# ping sccm.prajwal.local
PING sccm.prajwal.local (192.168.100.4) 56(84) bytes of data.
64 bytes from sccm.prajwal.local (192.168.100.4): icmp_seq=1 ttl=128 time=1.55 ms
64 bytes from sccm.prajwal.local (192.168.100.4): icmp_seq=2 ttl=128 time=0.191 ms
64 bytes from sccm.prajwal.local (192.168.100.4): icmp_seq=3 ttl=128 time=0.196 ms
^C
--- sccm.prajwal.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2603ms
rtt min/avg/max/mdev = 0.191/0.645/1.550/0.640 ms
[root@localhost /]#
```

On the linux computer, use root credentials to run the following command to enable the script to run as a program, **chmod +x install**.

execute the command **./install -mp sccm.prajwal.local -sitecode IND ccm-UniversalX64.1.0.0.4580.tar**

The syntax of the command is **./install -mp <Management point server FQDN> -sitecode <code> ccm-Universal-x64.<build>.tar**

Additionally, Configuration Manager client for Linux and UNIX supports the use of fallback status points. You can specify the FSP by adding **-fsp <FSP server FQDN>** to the command.



The screenshot shows a terminal window titled "root@localhost:/opt/client". The terminal session starts with the command "cd /opt/client/", followed by "ls" which lists several tar files: "ccm-RHEL4x64.1.0.0.4580.tar", "ccm-SLES9x86.1.0.0.4580.tar", "ccm-Universalx86.1.0.0.4580.tar", "install", "ccm-RHEL4x86.1.0.0.4580.tar", "ccm-Universalx64.1.0.0.4580.tar", "ConfigMgr Clients for Linux", and "License.rtf". The next command is "chmod +x install". The final command shown is "../install -mp sccm.prajwal.local -sitecode IND ccm-Universalx64.1.0.0.4580.tar", which is highlighted with a red rectangle. The terminal window has a standard Linux-style interface with a title bar, menu bar, and scroll bars.

©PrajwalDesai.com

From the below screenshot we see that the client agent has been installed successfully on the linux machine. If you are looking for a log file to validate the install process you can check **/var/opt/microsoft/scxcm.log**. In case you change the hostname of linux machine after the installation of client agent, then you must reboot the linux machine once.

/var/opt/microsoft/scxcm.log – This log file contains information about the installation and ongoing operations of ccmexec.bin. If you are looking for troubleshooting UNIX/Linux client operations then you must use this log file.

/opt/microsoft/omi/scxcmprovider.log – This is the CIM service log file which captures the CIM service operations. The CIM server installs as part of the client for Linux and UNIX. If you are using SCCM 2012 SP1 (without CU1) you will see that the client used **nanowbem** as its CIM server.

I would recommend to restart the linux machine once the client agent has been installed on it. If you don't want to restart the server you can stop and start the **ccmexecd** process.

To **STOP** the ccmexecd you can use the command
To **START** the ccmexecd you can use the command

/etc/init.d/ccmexecd stop
/etc/init.d/ccmexecd start

```
root@localhost:~# cd /opt/client/
[root@localhost client]# ls
ccm-RHEL4x64.1.0.0.4580.tar  ccm-SLES9x86.1.0.0.4580.tar      ccm-Universalx86.1.0.0.4580.tar  install
ccm-RHEL4x86.1.0.0.4580.tar  ccm-Universalx64.1.0.0.4580.tar  [ccm-Universalx64.1.0.0.4580.log]  License.rtf
[root@localhost client]#
[root@localhost client]# chmod +x install
[root@localhost client]#
[root@localhost client]# ./install -mp sccm.prajwal.local -sitecode IND ccm-Universalx64.1.0.0.4580.tar
./install -mp sccm.prajwal.local -sitecode IND ccm-Universalx64.1.0.0.4580.tar

Checking Prerequisites...
Running preinstall validator
All pre-install tests succeeded!
Beginning installation of Config Manager in /opt/microsoft/configmgr
Creating install directory...
Extracting archive file to /opt/microsoft/configmgr...
Installing OMI
Generating a 2048 bit RSA private key
...+++
.....+-----+-----+
writing new private key to '/opt/microsoft/omi/etc/ssl/certs/omikey.pem'
-----
omi already configured
Successfully installed OMI under: /opt/microsoft/omi/.
Setting CM_HOME in omiserver...
Disabling HTTP Ports...
Modifying install scripts for OMI
Registering Providers...
Created /opt/microsoft/omi/.etc/omiregister/root-cimv2/scxcmprovider.reg
Performing post installation cleanup...
Linking startup script...
Initializing data store. This may take a few minutes...
Installing boot-time scripts...
Starting Configuration Manager...
Installation complete.
[root@localhost client]#
```

©PrajwalDesai.com

As mentioned earlier **scxcm.log** file records both installation and operational information. This log file is useful when you want to troubleshoot client operations. There might be a situation where you are troubleshooting the client installation issues and you want verbose information to be logged in scxcm.log. There are four different log levels each one having a unique setting.

- 1) ERROR: Indicates problems that require attention.
- 2) WARNING: Indicates possible problems for the client operations.
- 3) INFO: More detailed logging that indicates the status of various events on the client.
- 4) TRACE: Verbose logging that is typically used to diagnose problems.

```
root@localhost:/opt/microsoft/configmgr/etc
File Edit View Search Terminal Help
[root@localhost ~]# cd ..
[root@localhost /]# cd opt/microsoft/configmgr/etc/
[root@localhost etc]#
[root@localhost etc]# ls
buildarch scxcm.conf scx-release
[root@localhost etc]# cat scx
scxcm.conf scx-release
[root@localhost etc]# cat scxcm.conf
FILE (
PATH: /var/opt/microsoft/scxcm.log
MODULE: WARNING
MODULE: scx.client WARNING
)

[root@localhost etc]#
```

©PrajwalDesai.com

To change the log level, edit **/opt/microsoft/configmgr/etc/scxcm.conf** and change each instance of the tag **MODULE** to the desired log level.

```
root@localhost:/opt/microsoft/configmgr/etc
File Edit View Search Terminal Help
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]# ls
buildarch scxcm.conf scx-release
[root@localhost etc]# cat scxcm.conf
FILE (
PATH: /var/opt/microsoft/scxcm.log
MODULE: TRACE
MODULE: scx.client TRACE
)

[root@localhost etc]#
```

©PrajwalDesai.com

After the SCCM client has been installed on linux machine, in the Configuration Manager console, under **All Systems** you will find the linux machine name. Right click on the linux computer and click **Approve**.

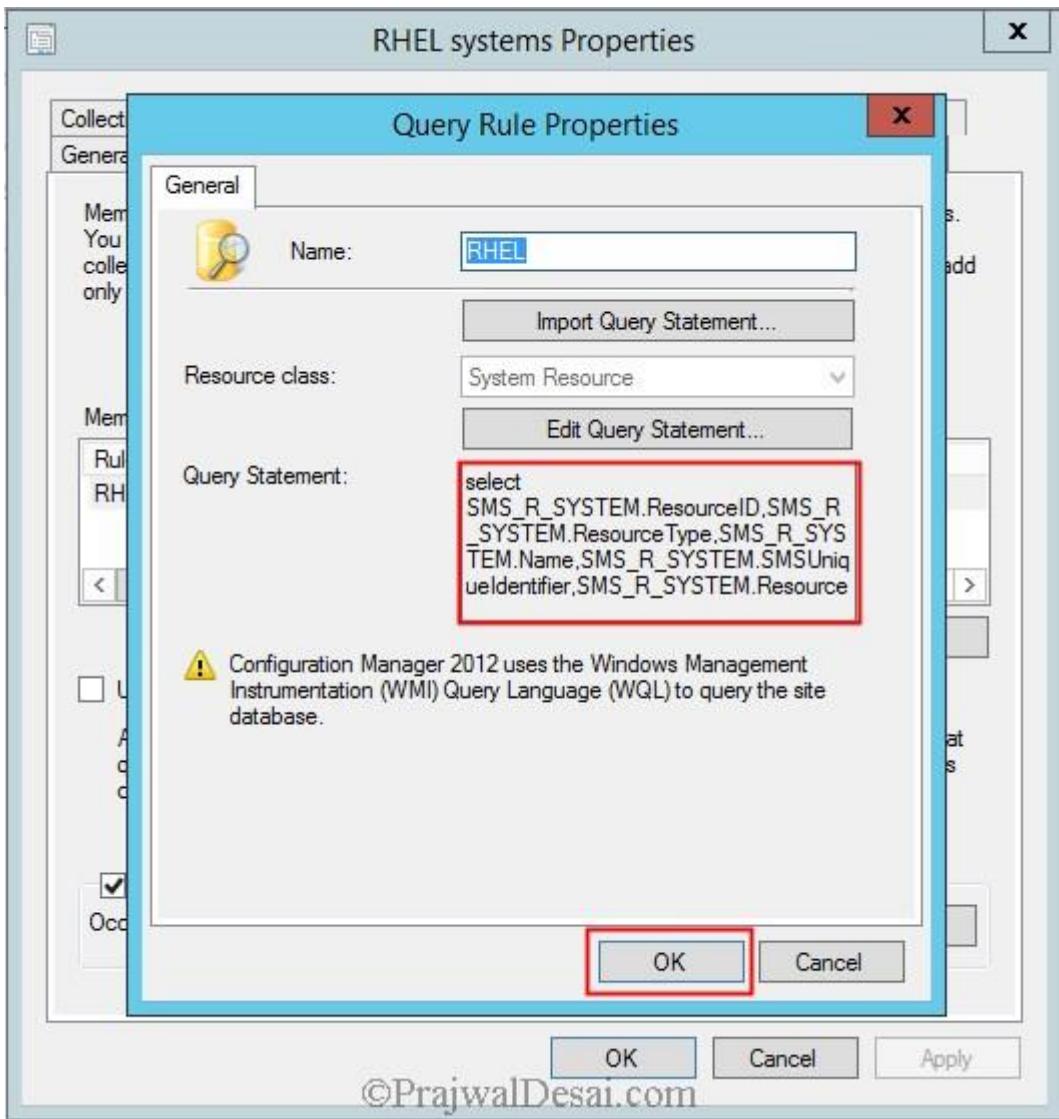
The screenshot shows the SCCM console interface. The top navigation bar includes 'Home', 'Collection', 'Close', 'Manage Affinity Requests', 'Update Membership', 'Export', 'Add Resources', 'Copy', 'Deploy', 'Properties', 'Selected Items', 'Install Client', 'Manage Out of Band', 'Clear Required PXE Deployments', and 'Endpoint Protection'. Below the navigation is a breadcrumb trail: 'Assets and Compliance > Overview > Devices > All Systems'. On the left, a tree view shows 'Overview', 'Devices' (selected), 'All Systems' (highlighted with a red border), 'User Collections', 'Device Collections', 'User State Migration', 'Asset Intelligence', 'Software Metering', 'Compliance Settings', and 'Endpoint Protection'. The main pane displays a table titled 'All Systems 7 items' with columns: Icon, Name, Client Type, Client, Site Code, and Client Activity. The table lists the following items:

Icon	Name	Client Type	Client	Site Code	Client Activity
AD	AD	Computer	Yes	IND	Active
EXC	EXC	Computer	Yes	IND	Active
linux.prajwal.local	linux.prajwal.local	Computer	Yes	IND	Active
SCCM	SCCM	Computer	Yes	IND	Active
WIN7	WIN7	Computer	Yes	IND	Active
x64 Unknown Computer (x64 Unknown Computer)	x64 Unknown Computer (x64 Unknown Computer)	None	No	IND	
x86 Unknown Computer (x86 Unknown Computer)	x86 Unknown Computer (x86 Unknown Computer)	None	No	IND	

©PrajwalDesai.com

Now lets create a collection to group the linux computers. Microsoft recommends to use the **Caption** value for the **Operating System** class to identify different Linux and UNIX operating systems in queries and collections. In this example I will be using the **Attribute Class as Operating System and Attribute as Manufacturer**. You can use the below query to add the redhat machines to collection.

```
select SMS_R_System.ResourceId, SMS_R_System.ResourceType,
SMS_R_System.Name, SMS_R_System.SMSUniqueIdentifier,
SMS_R_System.ResourceDomainORWorkgroup, SMS_R_System.Client
from SMS_R_System inner join SMS_G_System_OPERATING_SYSTEM on
SMS_G_System_OPERATING_SYSTEM.ResourceID = SMS_R_System.ResourceId
where SMS_G_System_OPERATING_SYSTEM.Manufacturer = "Red Hat, Inc."
```



©PrajwalDesai.com

We have now created a collection named RHEL systems and our linux machine has been added to the collection.

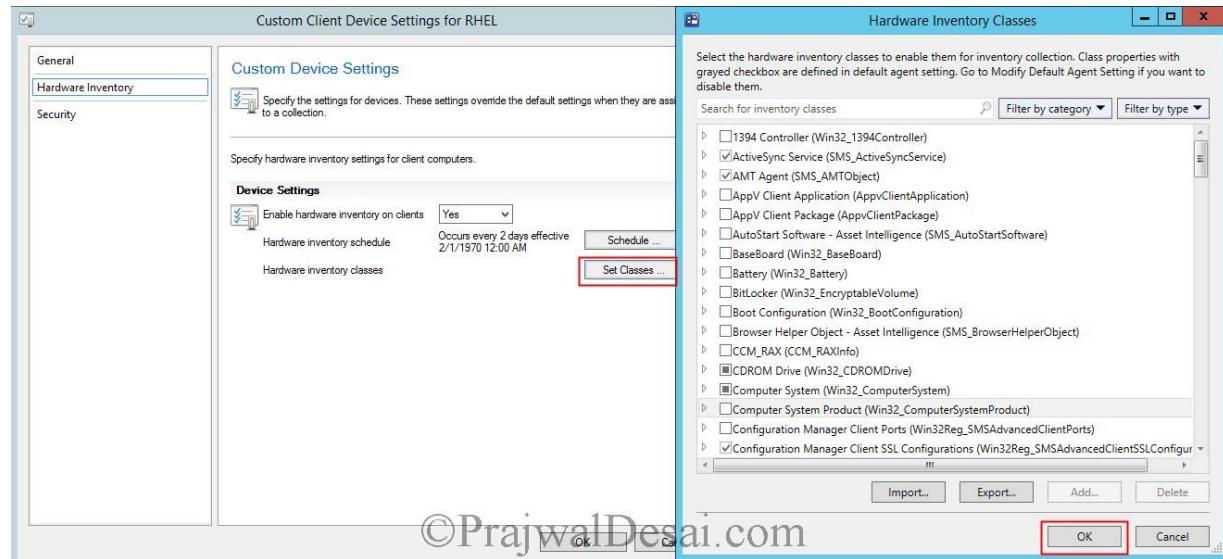
The screenshot shows the System Center 2012 R2 Configuration Manager interface. The top navigation bar includes 'Selected Object' (Collection), 'Folder Tools', and the title 'System Center 2012 R2 Configuration Manager (Connected to IND - Bangalore Headquarters Site)'. Below the toolbar, there are buttons for 'Home', 'Collection', 'Close', 'Manage Affinity Requests', 'Manage Out of Band', 'Update Membership', 'Export', 'Add Resources', 'Copy', 'Deploy', 'Properties', 'Clear Required PXE Deployments', 'Endpoint Protection', and 'Delete'. The main pane displays the 'Assets and Compliance' section with 'Overview', 'Devices', and 'All Systems'. Under 'All Systems', the 'RHEL systems' collection is selected and highlighted with a red box. The right pane shows a table titled 'RHEL systems 1 items' with one entry: 'Icon' (blue square), 'Name' (linux.prajwal.local), 'Client Type' (Computer), 'Client' (Yes), 'Site Code' (IND), and 'Client Activity' (Active). A watermark '©PrajwalDesai.com' is visible across the center of the screen.

We will now create a custom client device settings for the RHEL systems collection and enable the Hardware Inventory.

The screenshot shows the 'Custom Client Device Settings for RHEL' dialog box. The title bar is 'Custom Client Device Settings for RHEL'. On the left, a sidebar lists 'General', 'Hardware Inventory' (which is selected and highlighted with a red box), and 'Security'. The main pane is titled 'Custom Device Settings' and contains the following text: 'Specify the settings for devices. These settings override the default settings when they are assigned to a collection.' Below this is a section titled 'Device Settings' with the following options: 'Enable hardware inventory on clients' (set to 'Yes'), 'Hardware inventory schedule' (set to 'Occurs every 2 days effective 2/1/1970 12:00 AM'), and 'Schedule ...' (button highlighted with a red box). There is also a 'Set Classes ...' button. At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box. A watermark '©PrajwalDesai.com' is visible at the bottom center.

The client for Linux and UNIX supports the following hardware inventory classes that are available on Linux and UNIX servers:

- Win32_BIOS
- Win32_ComputerSystem
- Win32_DiskDrive
- Win32_DiskPartition
- Win32_NetworkAdapter
- Win32_NetworkAdapterConfiguration
- Win32_OperatingSystem
- Win32_Process
- Win32_Service
- Win32Reg_AddRemovePrograms
- SMS_LogicalDisk
- SMS_Processor



To perform a Machine Policy Refresh action on clients execute the following command :-
/opt/microsoft/configmgr/bin/ccmexec -rs policy



A terminal window titled "root@linux:/". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command "/opt/microsoft/configmgr/bin/ccmexec -rs policy" is entered and highlighted with a red box. The output shows the logging configuration file path: "/opt/microsoft/configmgr/etc/scxcm.conf".

```
[root@linux /]# 
[root@linux /]# 
[root@linux /]# /opt/microsoft/configmgr/bin/ccmexec -rs policy
[root@linux /]# Logging Configuration File for SCX CM:::/opt/microsoft/configmgr/etc/scxcm.conf

[root@linux /]#
```

©PrajwalDesai.com

To trigger an inventory scan from a client run the following command :-
/opt/microsoft/configmgr/bin/ccmexec -rs hinv



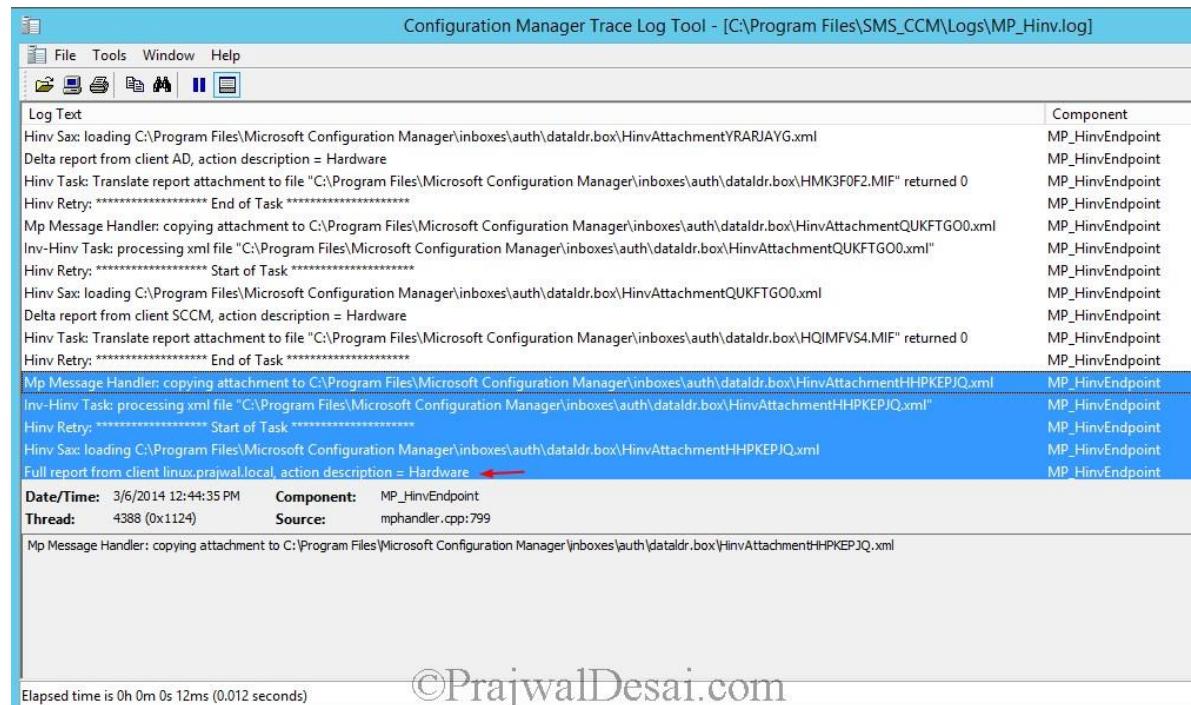
A terminal window titled "root@linux:/". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command "/opt/microsoft/configmgr/bin/ccmexec -rs hinv" is entered and highlighted with a red box. The output shows the logging configuration file path: "/opt/microsoft/configmgr/etc/scxcm.conf".

```
[root@linux /]# 
[root@linux /]# 
[root@linux /]# /opt/microsoft/configmgr/bin/ccmexec -rs hinv
[root@linux /]# Logging Configuration File for SCX CM:::/opt/microsoft/configmgr/etc/scxcm.conf

[root@linux /]#
```

©PrajwalDesai.com

Once you trigger the hardware inventory scan cycle, open the **MP_Hinv.log** file located on the SCCM server. Look for the line **Full report from client linux.prajwal.local, action description = hardware.**



```
Configuration Manager Trace Log Tool - [C:\Program Files\SMS_CCM\Logs\MP_Hinv.log]
File Tools Window Help
Log Text Component
Hinv Sax: loading C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentYRARJAYG.xml MP_HinvEndpoint
Delta report from client AD, action description = Hardware MP_HinvEndpoint
Hinv Task: Translate report attachment to file "C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HMK3F0F2.MIF" returned 0 MP_HinvEndpoint
Hinv Retry: ***** End of Task *****
Mp Message Handler: copying attachment to C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentQUKFTGO0.xml MP_HinvEndpoint
Inv-Hinv Task: processing xml file "C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentQUKFTGO0.xml" MP_HinvEndpoint
Hinv Retry: ***** Start of Task *****
Hinv Sax: loading C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentQUKFTGO0.xml MP_HinvEndpoint
Delta report from client SCCM, action description = Hardware MP_HinvEndpoint
Hinv Task: Translate report attachment to file "C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HQJMFVS4.MIF" returned 0 MP_HinvEndpoint
Hinv Retry: ***** End of Task *****
Mp Message Handler: copying attachment to C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentHHPKEPJQ.xml MP_HinvEndpoint
Inv-Hinv Task: processing xml file "C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentHHPKEPJQ.xml" MP_HinvEndpoint
Hinv Retry: ***** Start of Task *****
Hinv Sax: loading C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentHHPKEPJQ.xml MP_HinvEndpoint
Full report from client linux.prajwal.local, action description = Hardware → MP_HinvEndpoint
Date/Time: 3/6/2014 12:44:35 PM Component: MP_HinvEndpoint
Thread: 4388 (0x1124) Source: mpandler.cpp:799
Mp Message Handler: copying attachment to C:\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\HinvAttachmentHHPKEPJQ.xml
Elapsed time is 0h 0m 0s 12ms (0.012 seconds)
```

©PrajwalDesai.com

In the CM console right click the linux machine and click **Start > Resource Explorer**. Under **Hardware**, click **Services** to see the list of services.

System Center 2012 R2 Configuration Manager - Resource Explorer

Name	Display Name	Path Name	Start Name	Status
gnome-terminal(3557)	gnome-terminal	/usr/bin/gnome-terminal	root	OK
ccmexec.bin(3228)	ccmexec.bin	/opt/microsoft/configmgr/bin/ccmexec.bin	root	OK
omiserver.bin(3227)	omiserver.bin	/opt/microsoft/omi/bin/omiserver.bin	root	OK
gvfsd-metadata(2713)	gvfsd-metadata	/usr/libexec/gvfsd-metadata	root	OK
gvfsd-burn(2711)	gvfsd-burn	/usr/libexec/gvfsd-burn	root	OK
clock-applet(2685)	clock-applet	/usr/libexec/clock-applet	root	OK
gdm-user-switch(2684)	gdm-user-switch	/usr/libexec/gdm-user-switch-applet	root	OK
notification-ar(2683)	notification-ar	/usr/libexec/notification-area-applet	root	OK
gnote(2682)	gnote	/usr/bin/gnote	root	OK
gnome-screensav(2665)	gnome-screensav	/usr/bin/gnome-screensaver	root	OK
restorecond(2661)	restorecond	/usr/sbin/restorecond	root	OK
gvfs-trash(2659)	gvfs-trash	/usr/libexec/gvfsd-trash	root	OK
gvfs-photov(2657)	gvfs-photov	/usr/libexec/gvfs-photov-volume-monitor	root	OK
gvfs-afc-volume(2653)	gvfs-afc-volume	/usr/libexec/gvfs-afc-volume-monitor	root	OK
pulseaudio(2642)	pulseaudio	/usr/bin/pulseaudio	root	OK
udisks-daemon(2616)	udisks-daemon	/usr/libexec/udisks-daemon	root	OK
vmtoolsd(2613)	vmtoolsd	/usr/lib/vmware-tools/sbin64/vmtoolsd	root	OK
trashapplet(2610)	trashapplet	/usr/libexec/trashapplet	root	OK
wnck-applet(2609)	wnck-applet	/usr/libexec/wnck-applet	root	OK
gvfs-gdu-volume(2608)	gvfs-gdu-volume	/usr/libexec/gvfs-gdu-volume-monitor	root	OK
bonobo-activati(2598)	bonobo-activati	/usr/libexec/bonobo-activation-server	root	OK
gvfs-fuse-daemo(2577)	gvfs-fuse-daemo	/usr/libexec/gvfs-fuse-daemon	root	OK
gvfsd(2572)	gvfsd	/usr/libexec/gvfsd	root	OK
seahorse-daemon(2567)	seahorse-daemon	/usr/bin/seahorse-daemon	root	OK
gnome-settings-(2564)	gnome-settings-	/usr/libexec/gnome-settings-daemon	root	OK
gconfd-2(2557)	gconfd-2	/usr/libexec/gconfd-2	root	OK
dbus-daemon(2543)	dbus-daemon	/bin/dbus-daemon	root	OK
dbus-launch(2542)	dbus-launch	/usr/bin/dbus-launch	root	OK
gnome-keyring-d(2525)	gnome-keyring-d	/usr/bin/gnome-keyring-daemon	root	OK
auditd(2460)	auditd	/sbin/auditd	root	OK
rkit-daemon(2432)	rkit-daemon	/usr/libexec/rkit-daemon	rkit	OK
polkitd(2423)	polkitd	/usr/libexec/polkit-1/polkitd	root	OK
polkitd-powerd(2201)	polkitd-powerd	/usr/libexec/polkit-powerd	root	OK

You can also find the **Installed Applications** on the linux machine.

The screenshot shows the System Center 2012 R2 Configuration Manager - Resource Explorer interface. On the left, a tree view shows a connection to a Linux machine named "linux.prajwal.local". Under "Hardware", the "Installed Applications" node is selected. On the right, a grid displays a list of installed packages. The columns are "Display Name" and "Product ID". The "Display Name" column lists package names like "libpciaccess-0.12.1-1.el6.x86_64", "foomatic-4.0.4-1.el6_1.1.x86_64", and "festival-1.96-18.el6.x86_64". The "Product ID" column provides detailed information for each package, including version numbers and checksums. The bottom status bar indicates the URL "©PrajwalDesai.com".

Display Name	Product ID
libpciaccess-0.12.1-1.el6.x86_64 (32804165)	libpciaccess-0.12.1-1.el6.x86_64 (32804165)
foomatic-4.0.4-1.el6_1.1.x86_64 (373295528)	foomatic-4.0.4-1.el6_1.1.x86_64 (373295528)
festival-1.96-18.el6.x86_64 (2018701164)	festival-1.96-18.el6.x86_64 (2018701164)
pam-1.1.1-10.el6.x86_64 (2684792761)	pam-1.1.1-10.el6.x86_64 (2684792761)
gnome-utils-2.28.1-10.el6.x86_64 (39692043)	gnome-utils-2.28.1-10.el6.x86_64 (39692043)
libprint-0.1.0-19.pre2.el6.x86_64 (287691611)	libprint-0.1.0-19.pre2.el6.x86_64 (287691611)
ncurses-5.7-3.20090208.el6.x86_64 (354991)	ncurses-5.7-3.20090208.el6.x86_64 (354991)
rhythmbox-0.12.8-1.el6.x86_64 (471260444)	rhythmbox-0.12.8-1.el6.x86_64 (471260444)
gtk2-engines-2.18.4-5.el6.x86_64 (28540133)	gtk2-engines-2.18.4-5.el6.x86_64 (28540133)
liberation-sans-fonts-1.05.1.20090721-4.el6.noarch (28540133)	liberation-sans-fonts-1.05.1.20090721-4.el6.noarch (28540133)
evince-2.28.2-14.el6_0.1.x86_64 (20974449)	evince-2.28.2-14.el6_0.1.x86_64 (20974449)
gnome-media-libs-2.29.91-6.el6.x86_64 (7721)	gnome-media-libs-2.29.91-6.el6.x86_64 (7721)
diffutils-2.8.1-28.el6.x86_64 (4120956974)	diffutils-2.8.1-28.el6.x86_64 (4120956974)
cjkuni-uming-fonts-0.2.20080216.1-35.el6.noarch (28540133)	cjkuni-uming-fonts-0.2.20080216.1-35.el6.noarch (28540133)
xorg-x11-xkb-utils-7.4-6.el6.x86_64 (4655349)	xorg-x11-xkb-utils-7.4-6.el6.x86_64 (4655349)
net-tools-1.60-109.el6.x86_64 (3965752299)	net-tools-1.60-109.el6.x86_64 (3965752299)
alsa-plugins-pulseaudio-1.0.21-3.el6.x86_64 (22128)	alsa-plugins-pulseaudio-1.0.21-3.el6.x86_64 (22128)
evince-libs-2.28.2-14.el6_0.1.x86_64 (22128)	evince-libs-2.28.2-14.el6_0.1.x86_64 (22128)
polkit-desktop-policy-0.96-2.el6_0.1.noarch (175799885)	polkit-desktop-policy-0.96-2.el6_0.1.noarch (175799885)
compiz-0.8.2-24.el6.x86_64 (175799885)	compiz-0.8.2-24.el6.x86_64 (175799885)
gtkmm24-2.18.2-1.el6.x86_64 (2574796435)	gtkmm24-2.18.2-1.el6.x86_64 (2574796435)
cpp-4.4.6-3.el6.x86_64 (3691260115)	cpp-4.4.6-3.el6.x86_64 (3691260115)
plymouth-utils-0.8.3-24.el6.x86_64 (14092600)	plymouth-utils-0.8.3-24.el6.x86_64 (14092600)
at-spi-1.28.1-2.el6.x86_64 (4246177963)	at-spi-1.28.1-2.el6.x86_64 (4246177963)
libiec61883-1.2.0-4.el6.x86_64 (3430298736)	libiec61883-1.2.0-4.el6.x86_64 (3430298736)
xorg-x11-drv-mach64-6.9.0-1.el6.x86_64 (321)	xorg-x11-drv-mach64-6.9.0-1.el6.x86_64 (321)
libgnomecanvas-2.26.0-4.el6.x86_64 (32593)	libgnomecanvas-2.26.0-4.el6.x86_64 (32593)
xorg-x11-font-utils-7.2-11.el6.x86_64 (227758)	xorg-x11-font-utils-7.2-11.el6.x86_64 (227758)
xorg-x11-drv-vmmouse-12.7.0-1.el6.x86_64 (32593)	xorg-x11-drv-vmmouse-12.7.0-1.el6.x86_64 (32593)
libXft-2.1.13-4.1.el6.x86_64 (631471954)	libXft-2.1.13-4.1.el6.x86_64 (631471954)
sysvinit-tools-2.87-4.ds1.el6.x86_64 (3440276)	sysvinit-tools-2.87-4.ds1.el6.x86_64 (3440276)
xorg-x11-drv-glx-1.2.5-1.el6.x86_64 (989965)	xorg-x11-drv-glx-1.2.5-1.el6.x86_64 (989965)
libXvbe-1.0.5-1.el6.x86_64 (3440276)	libXvbe-1.0.5-1.el6.x86_64 (3440276)

You can also generate the report for the linux machine.

Computer information for a specific computer

Description Displays summary information for a single computer.

NetBIOS Name	User Name	User Domain	Computer Domain	Operating System	Version	Total Physical Memory (KBytes)	IP Addresses	Manufacturer
linux.prajwal.local				Red Hat Enterprise Linux 6.2 (x86_64)	6.2	6.2 GB	192.168.100.5, 192.168.100.3 192.168.100.5, fe80::20c:29ff:fed0:79e 192.168.100.3, fe80::30c:29ff:fed0:79e	AuthenticAMD

©PrajwalDesai.com

In case of Windows we typically query WMI for inventory data, whereas the UNIX/Linux client stores its inventory data in a series of XML files. You can view the default classes by directory listing **/opt/microsoft/configmgr/root/cimv**.

```
[root@linux root]# ls
ccm_ccmvdi_cimv2_invagt_microsoft __namespace.xml
[root@linux root]# cd cimv2/
[root@linux cimv2]# ls
ccm_antimalwarepolicyclientconfig.xml
ccm_antimalwarepolicygroupconfig.xml
ccm_antimalwarepolicyplaceholder.xml
ccm_applicationciassignment.xml
ccm_applicationmanagementclientconfig.xml
ccm_bgbclientconfig.xml
ccm_ciassociations.xml
ccm_civersioninfo.xml
ccm_cloudclientconfig.xml
ccm_configurationmanagementclientconfig.xml
ccm_endpointprotectionclientconfig.xml
ccm_externaleventconfig.xml
ccm_networksettings.xml
ccm_outofbandmanagementclientconfig.xml
ccm_softwareupdatesclientconfig.xml
ccm_systemhealthclientconfig.xml
ccm_targetingsettings.xml
ClassNameMap.xml
napcompliancedefinition.xml
sms
win32_bios.xml
win32_computerSystem.xml
win32_diskDrive.xml
win32_diskPartition.xml
win32_networkAdapterConfiguration.xml
win32_networkAdapter.xml
win32_operatingSystem.xml
win32_processor.xml
win32Reg_addRemovePrograms.xml
win32Reg_smsAdvancedClientPorts.xml
win32Reg_smsAdvancedClientsSSLConfiguration.xml
win32Reg_smssGuestVirtualMachine64.xml
win32Reg_smssGuestVirtualMachine.xml
win32_service.xml
[root@linux cimv2]#
```

©PrajwalDesai.com

Lastly to uninstall the SCCM client agent from the linux machine you can use the command :-
/opt/microsoft/configmgr/bin/uninstall



```
root@linux:/#
File Edit View Search Terminal Help
[root@linux /]#
[root@linux /]#
[root@linux /]# /opt/microsoft/configmgr/bin/uninstall
Uninstalling System Center Configuration Manager
Do you wish to continue y/n [n]: y
```

©PrajwalDesai.com

To completely uninstall ConfigMgr and OMI press C and hit enter. The client has been uninstalled.



```
root@linux:/#
File Edit View Search Terminal Help
Please choose your desired uninstall option.

Do you want to:
Completely Uninstall: ConfigMgr and OMI      [C]
Partial Uninstall: Remove ConfigMgr, Keep OMI  [P]
Exit Uninstaller                                [X]

Which method do you want? [C]: C
Shutting down configmgr...
2090,/opt/microsoft/configmgr/bin/ccmexec.bin
Waiting for configmgr to exit...
Uninstall complete...
[root@linux /]#
```

©PrajwalDesai.com

[How To Deploy Lync 2010 Client Using SCCM 2012 R2](#)

How To Deploy Lync 2010 Client Using SCCM 2012 R2

In this post we will see how to deploy Lync 2010 client using SCCM 2012 R2. The Lync server 2010 client is a single unified communication client that replaces previously released Office Communicator and Live meeting client, single client performs all the functions of the previous clients including instant messaging (IM), web conferencing, white boarding, desktop sharing, and enterprise voice. I have seen most of the users asking questions in Technet on how to deploy Lync 2010 client using SCCM 2012 R2, since the Lync Communicator comes as an executable file you cannot deploy it like the way you do for a .msi file. We will see step by step method on how to deploy Lync 2010 client using SCCM 2012 R2 and also we will see the uninstallation of Lync 2010 client.

You can deploy Lync 2010 in a managed-desktop environment by using the following methods:

SCCM – You can use Microsoft System Center Configuration Manager to deploy the Lync 2010 Client to the systems.

Group Policy – You can create a Group Policy object to deploy Lync 2010 to specific users or computers based on group memberships.

Logon Script – To deploy Lync 2010 client you can use a logon script that performs an unattended installation of Lync 2010 when a user logs on.

As mentioned earlier, in this post we will see the deployment of Lync 2010 client using SCCM 2012 R2. You can download the Lync 2010 client by clicking on below buttons.

[Microsoft Lync 2010 Trial \(64 Bit\)](#)

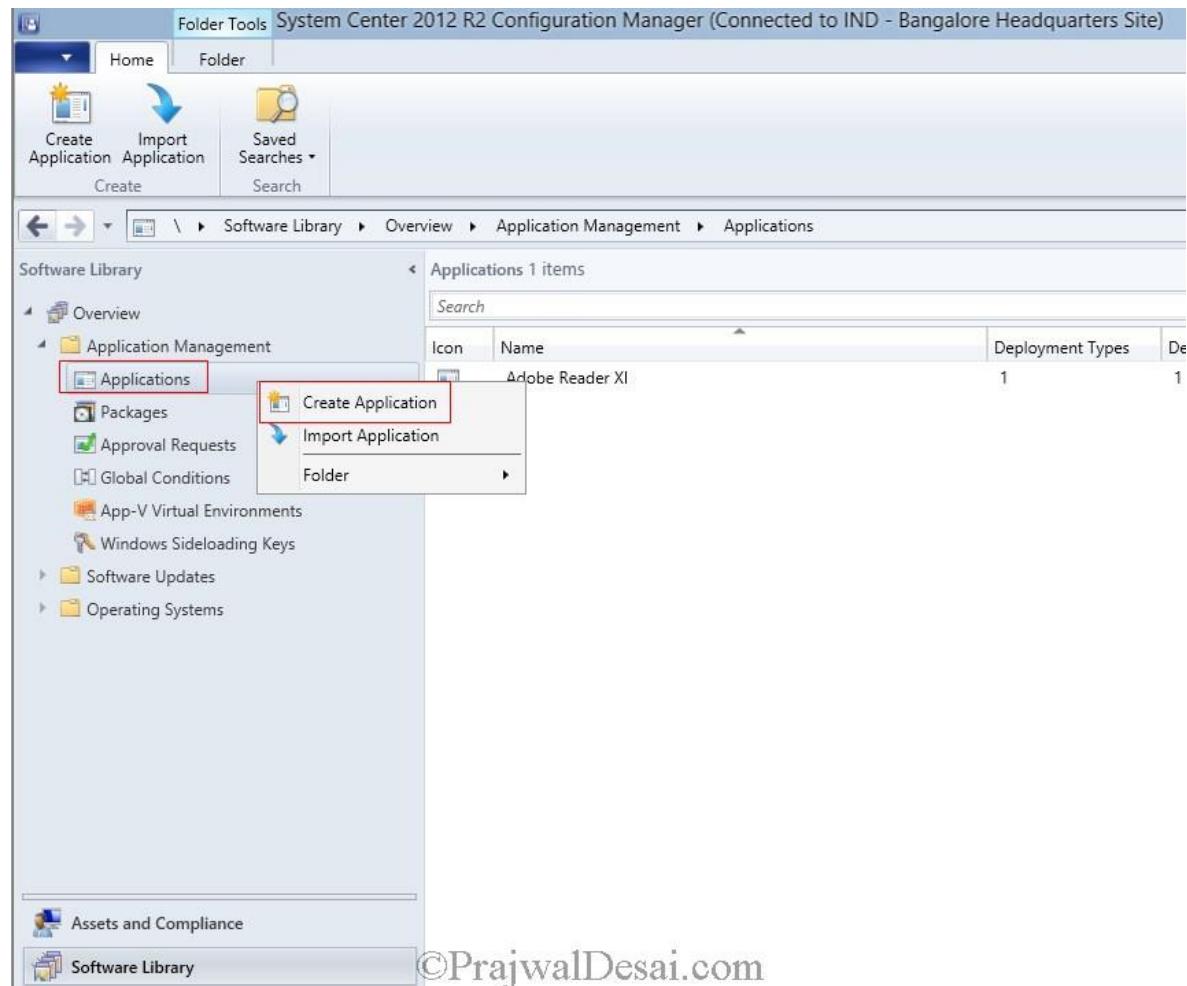
[Microsoft Lync 2010 Trial \(32 Bit\)](#)

When you deploy Lync 2010, you can use the Lync 2010 setup program command-line arguments listed in the following table.

Command Line Argument	Description
/Silent	Suppresses the installation user interface
/Install	Installs the client
/Uninstall	Removes previous versions of Office Communicator and add-ins
/Repair	Reinstalls the client to repair any installation issues
/InstallDir	Specifies the installation directory

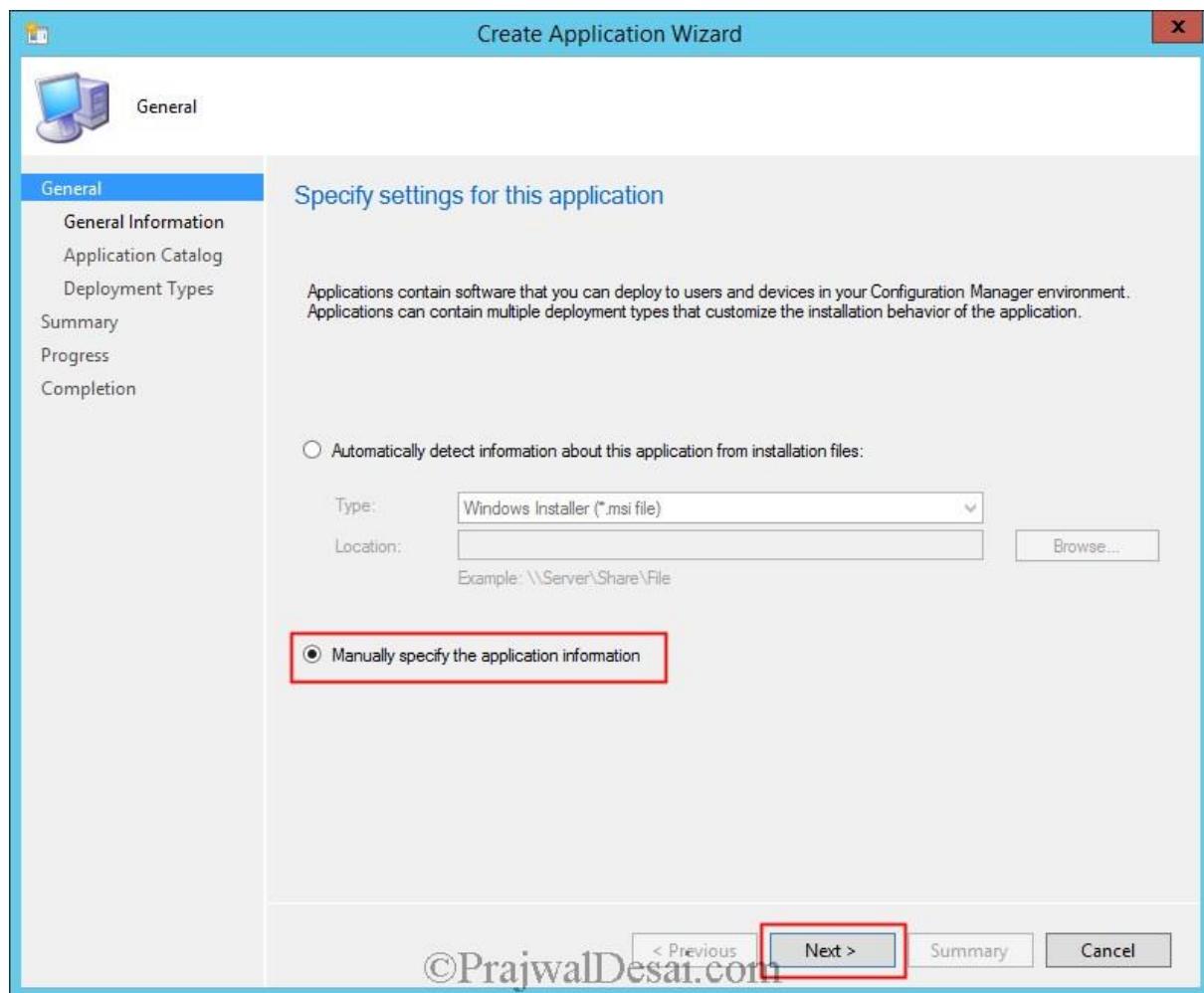
Command Line Argument	Description
/fulluisuppression	Enables Lync 2010 to run in user interface suppression mode

Once you have downloaded the Lync 2010 client setup file, you can copy it to a folder on the ConfigMgr server. Launch the Configuration Manager console, click **Software Library**, under **Application Management** right click **Applications** and click **Create Application**.



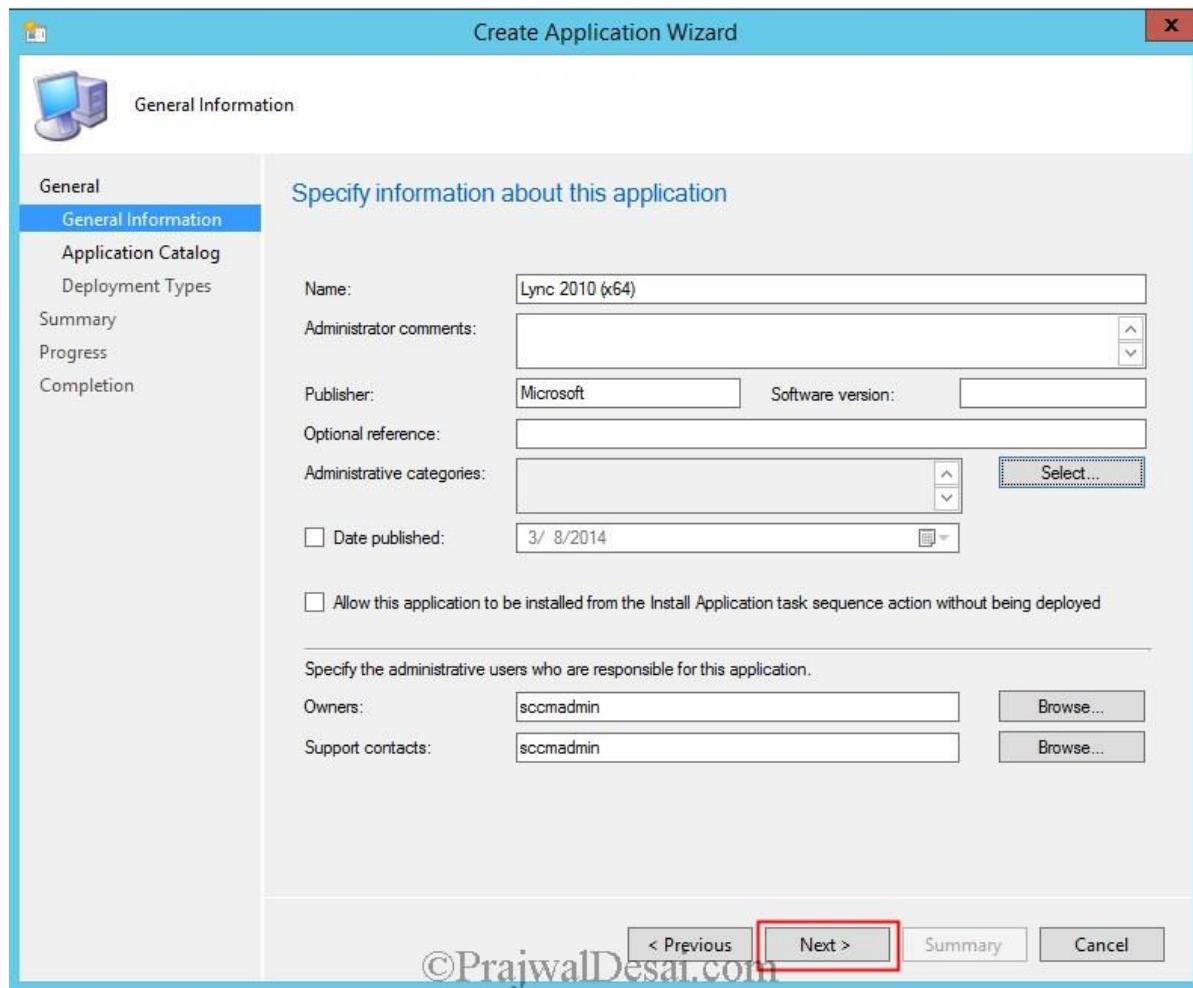
©PrajwalDesai.com

Choose **Manually specify the application information** and click **Next**.

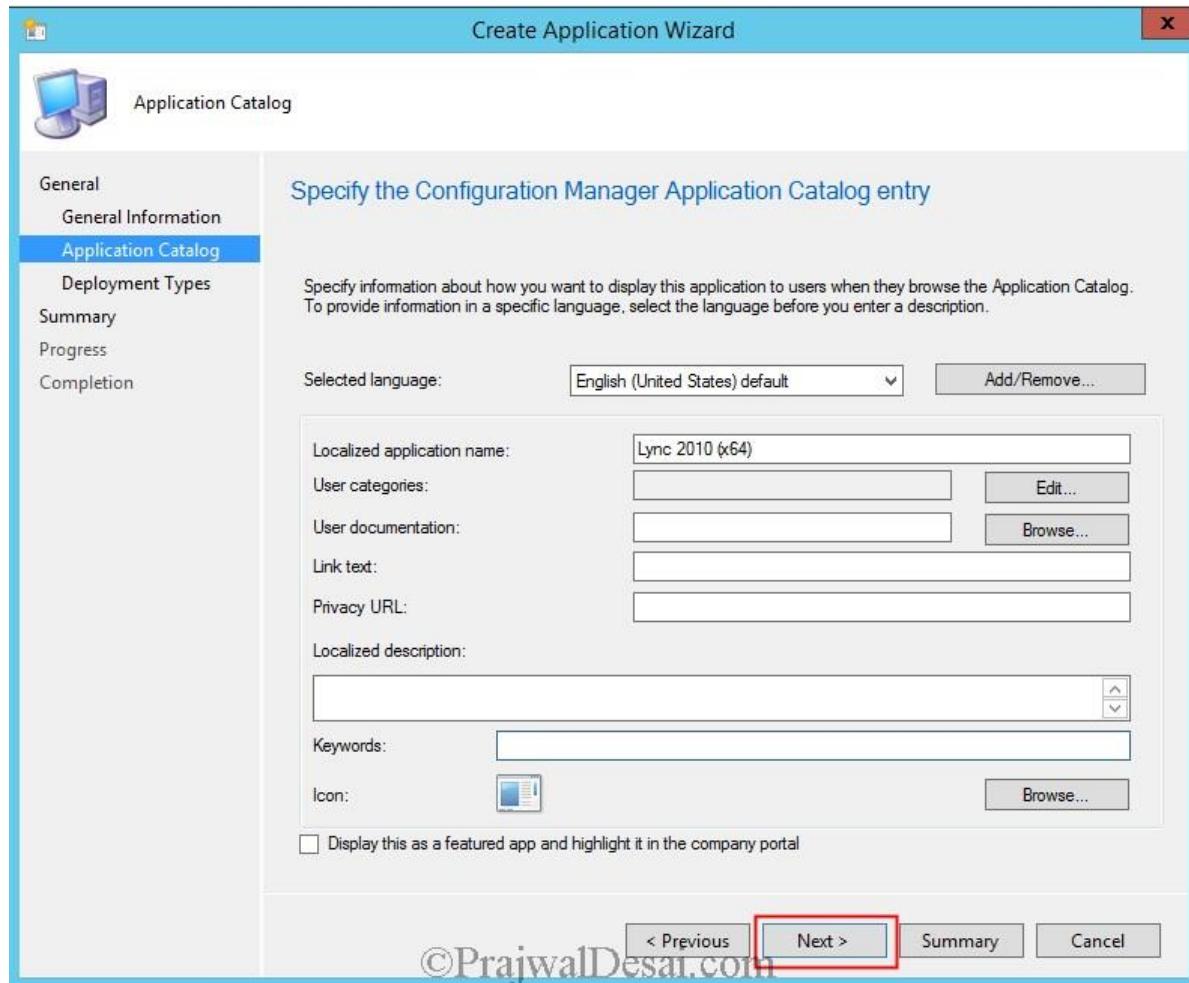


©PrajwalDesai.com

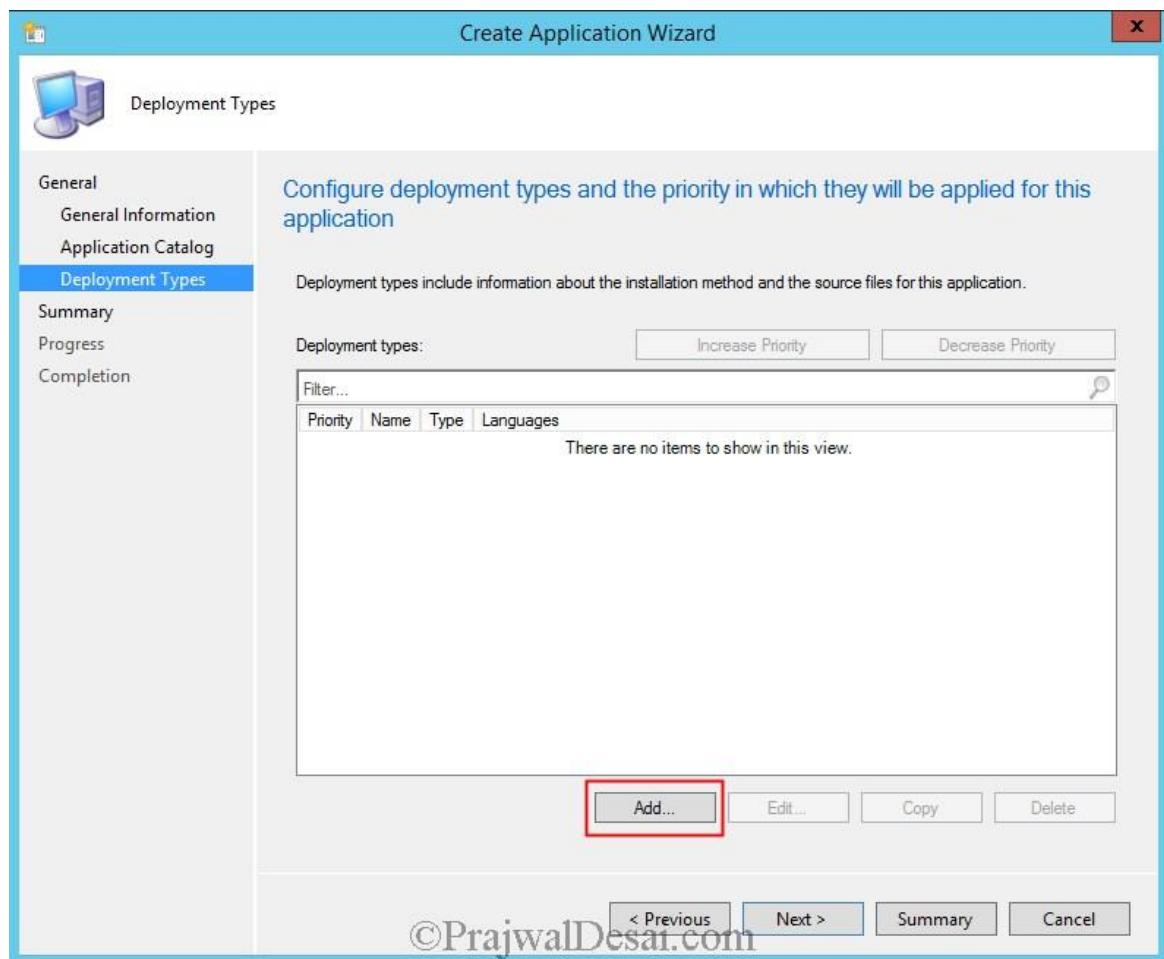
Specify some information about the application such as **Name**, **Publisher** etc. Click **Next**.



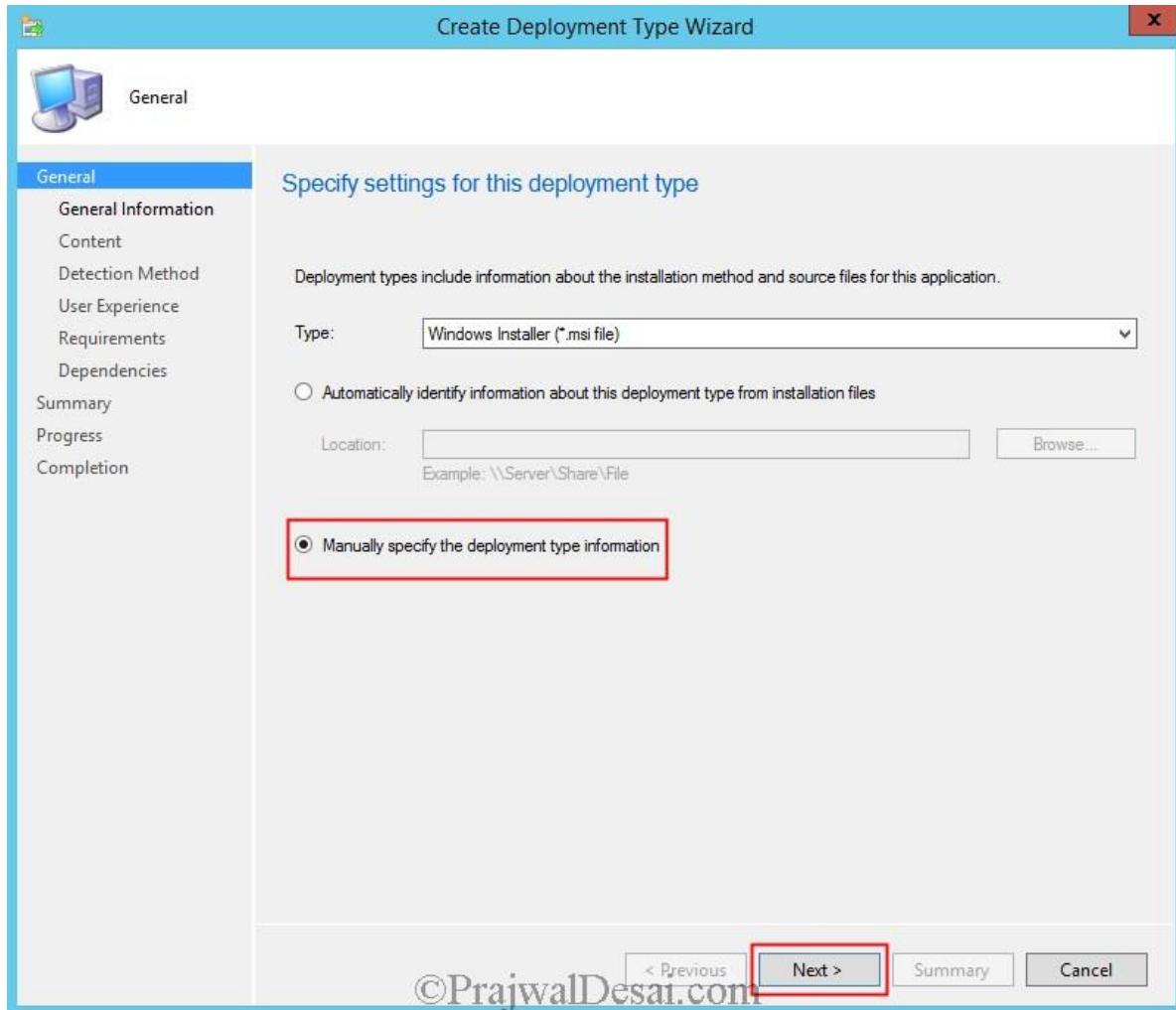
You can specify more information about the application here, the information specified here will be seen by user in the Application Catalog. Click **Next**.



Yes, we will configure the Deployment Type for Lync 2010 client setup. Click on **Add**.

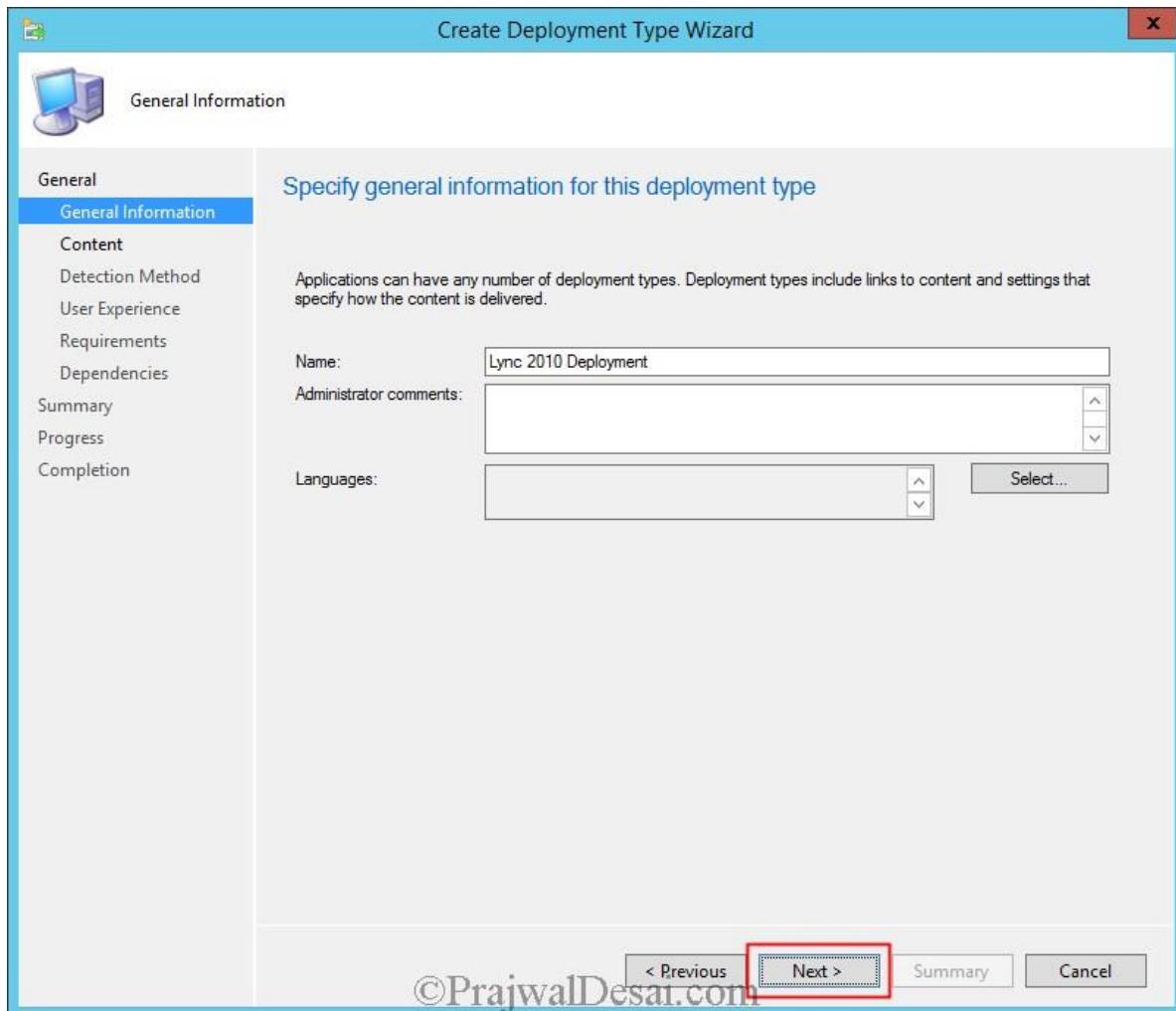


Let the deployment type be a **Windows Installer (*.msi)**, choose **Manually specify the deployment type information**. Click **Next**.



©PrajwalDesai.com

Specify some information about this deployment type and click **Next**.

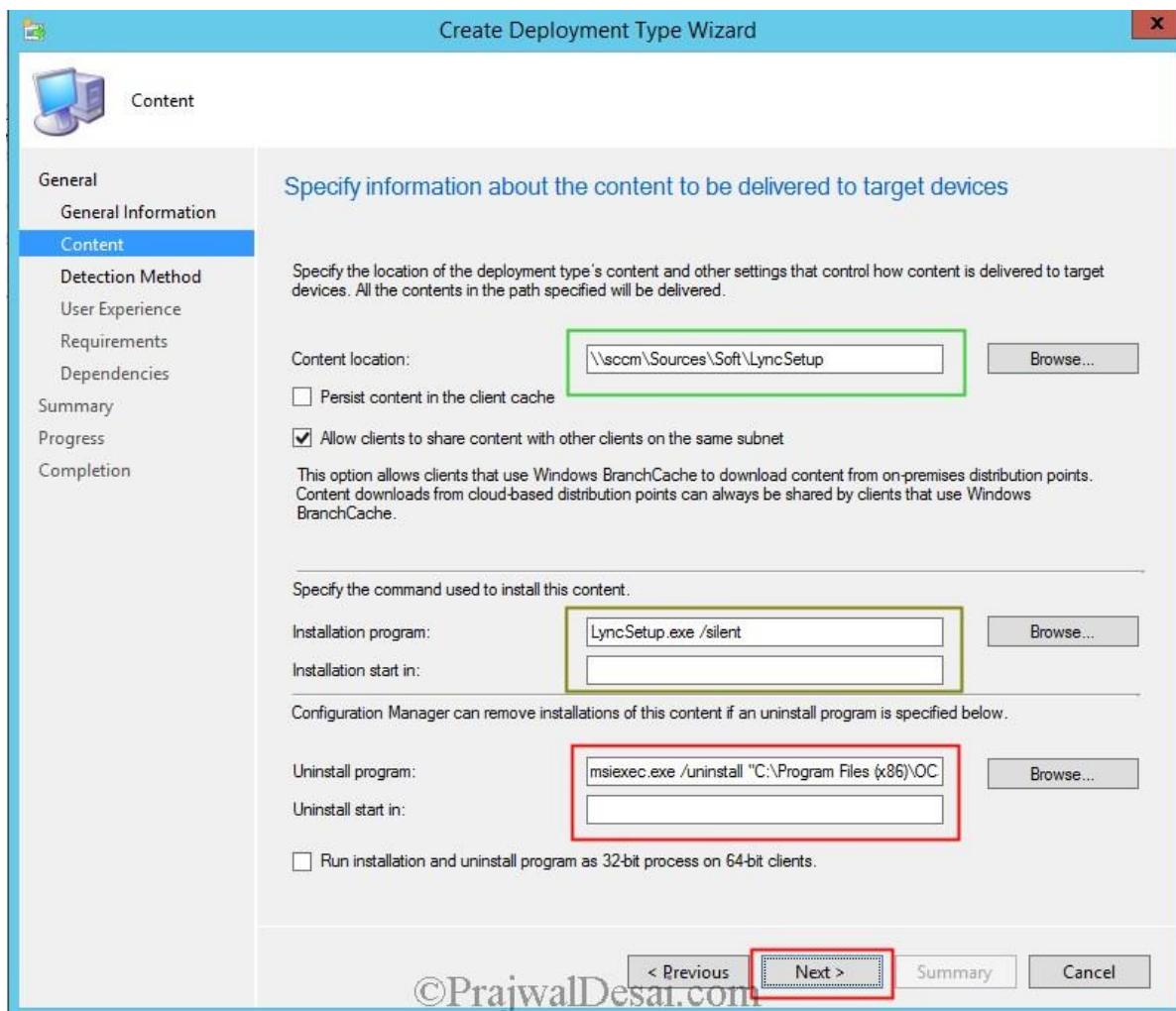


For the **Content Location**, provide the path where the Lync 2010 setup file is present, in my case I have copied the setup file to a folder named **LyncSetup** on SCCM server. The next step is to specify install and uninstall command.

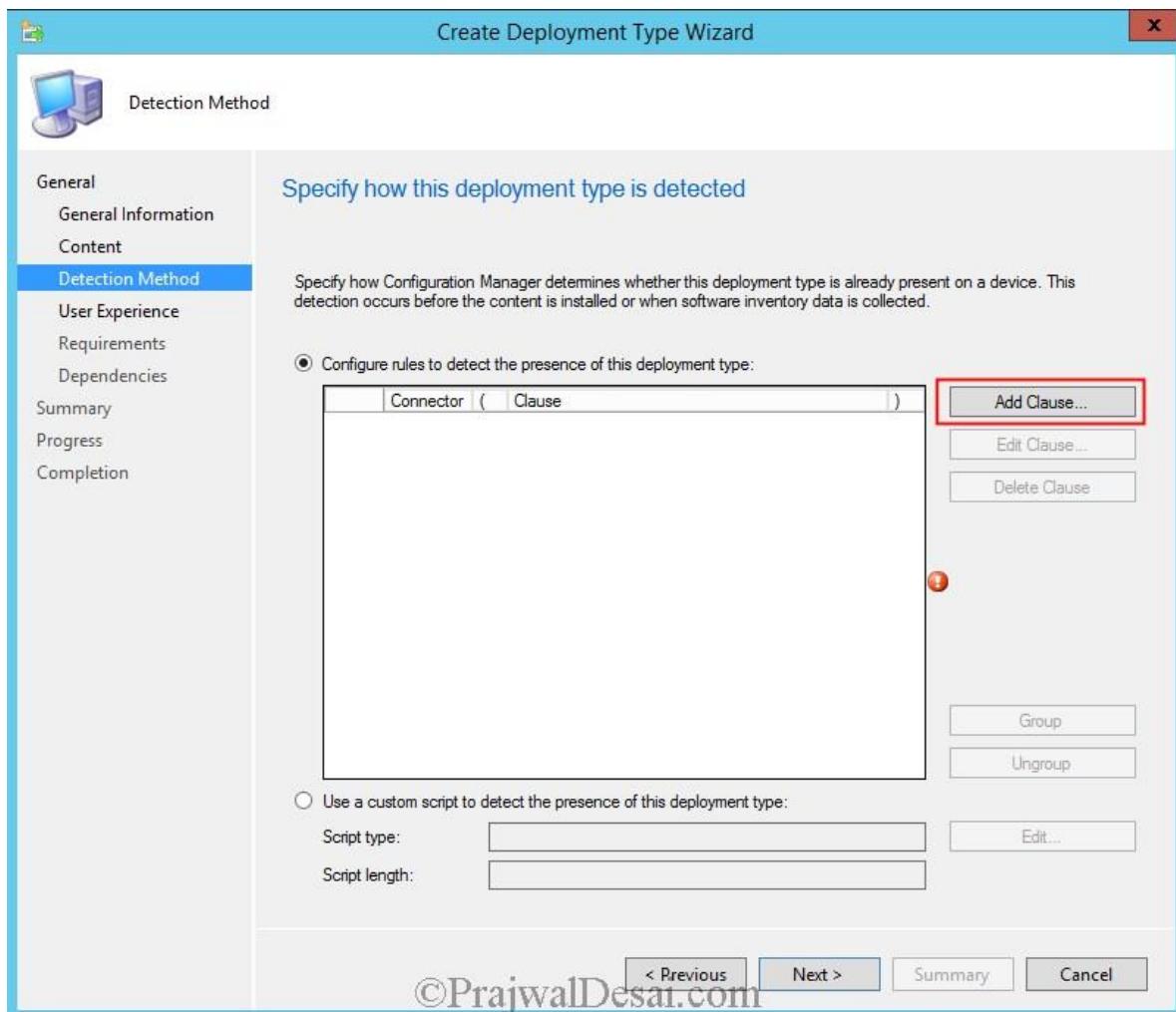
Specify the **Installation Program** as **LyncSetup.exe /silent**

Specify the **Uninstall Program** as **msiexec.exe /uninstall "C:\Program Files (x86)\OCSetupLync.msi"**

Click Next.



Detection Method – Detection methods allow the administrator to check if application is already installed. It can also prevent an install of an application if it conflicts with another application that is already installed. In this step you configure the rules to detect whether the application already exists on the client machine. Click **Configure rules to detect the presence of this deployment type** and click on **Add Clause**.



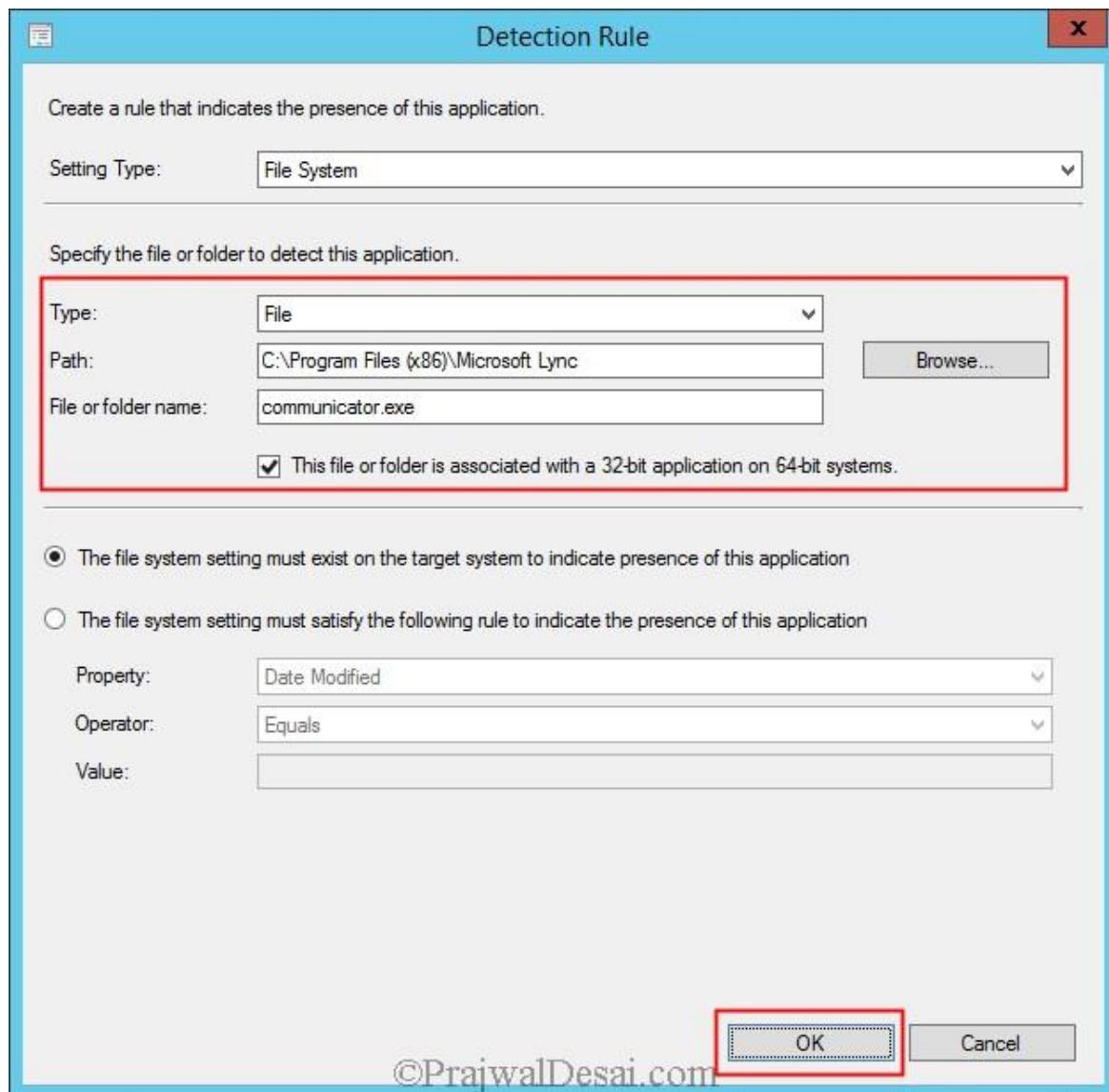
On the **Detection Rule** window, choose **Setting Type** as **File System**. Under **Specify the file or folder to detect the app**, set the following

Type – File

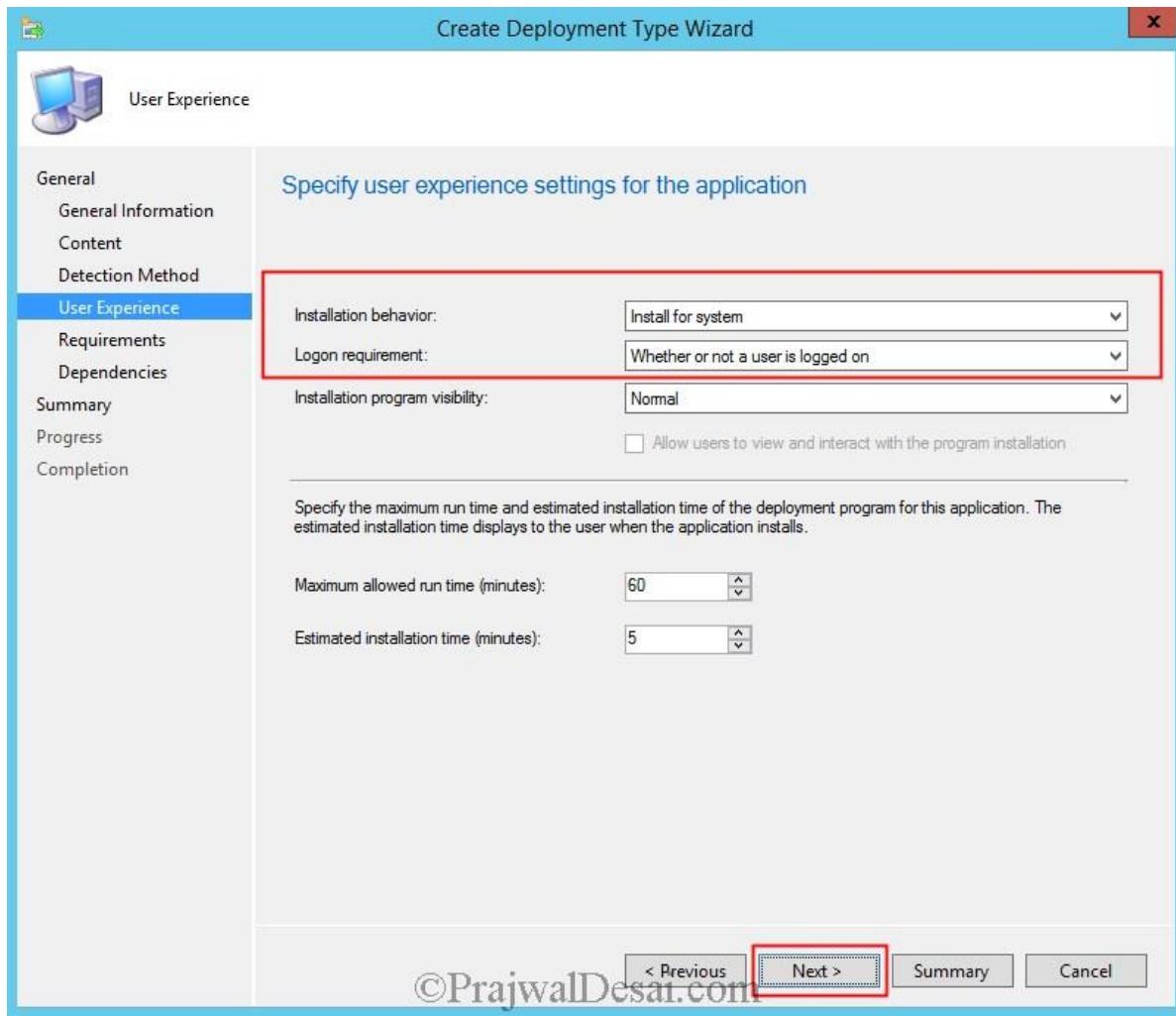
Path – C:\Program Files (x86)\Microsoft Lync

File or Folder name – communicator.exe

Click **OK** and then **Next**.

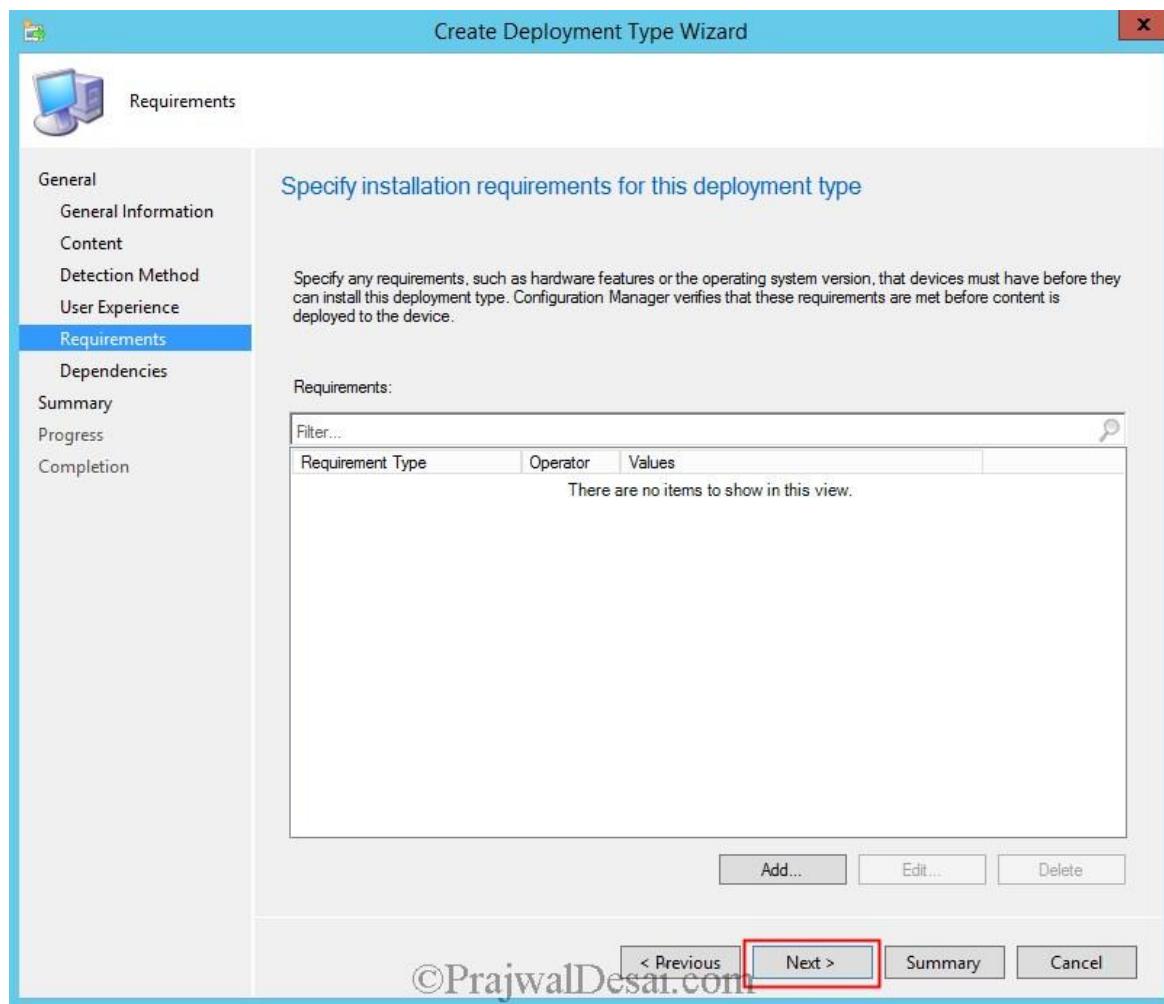


Selection the **Installation behavior** as **Install for system**, **Logon requirement** as **Whether or not a user is logged on** and **Installation program visibility** to **Normal**. Click **Next**.

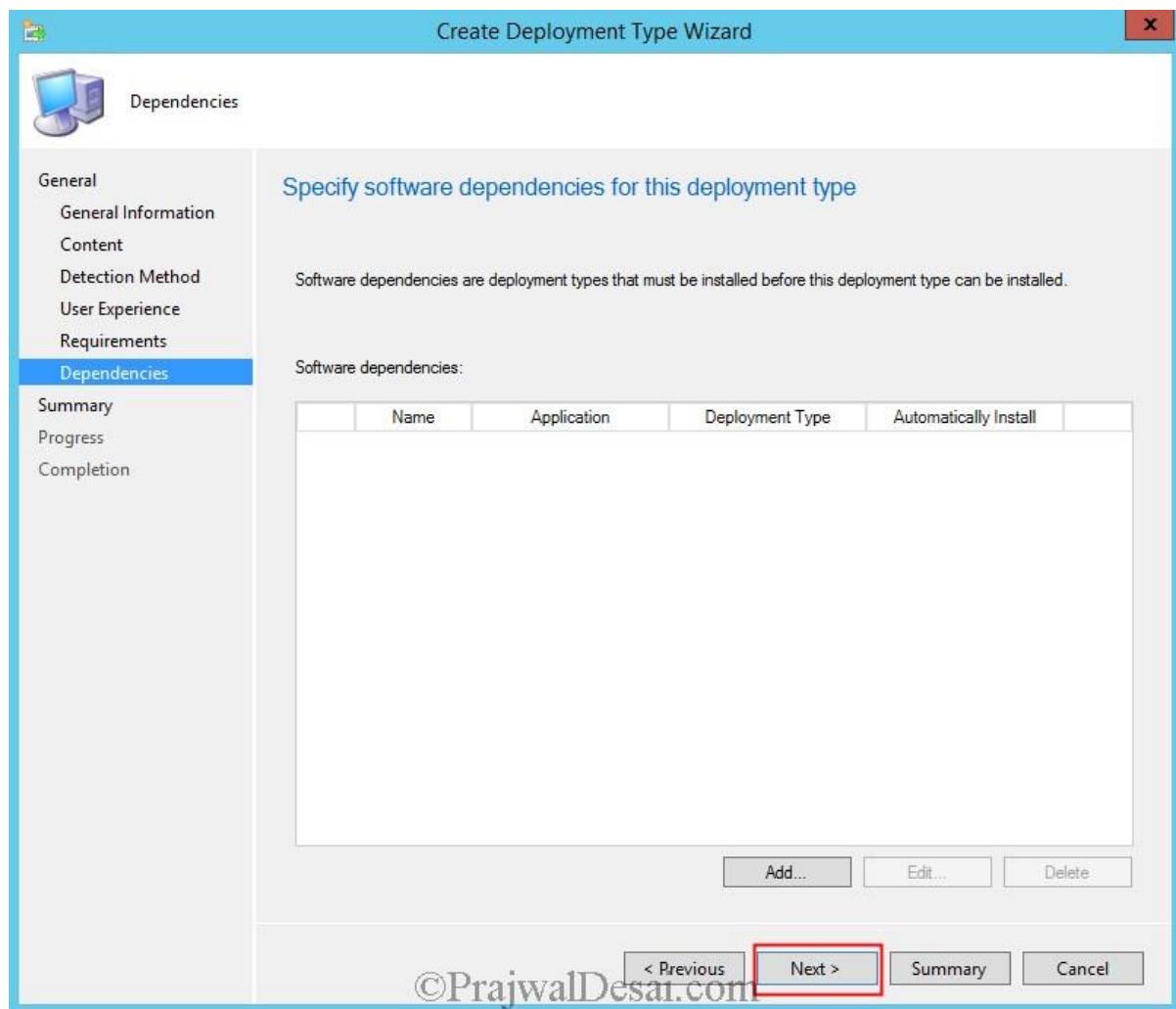


©PrajwalDesai.com

We will not specify any installation requirements for this deployment type so click **Next**.

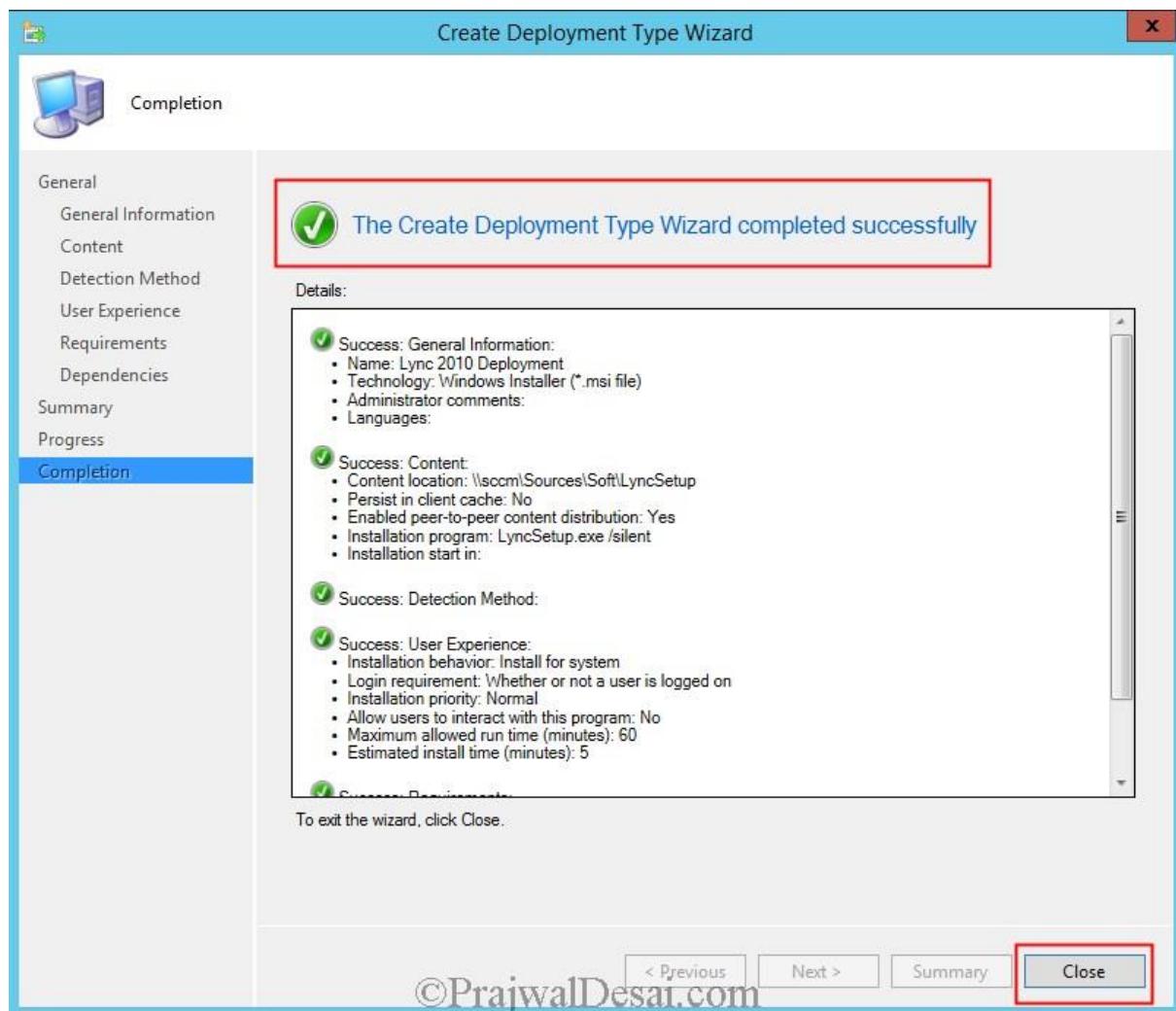


We will not specify any software dependencies for this deployment type so click **Next**.

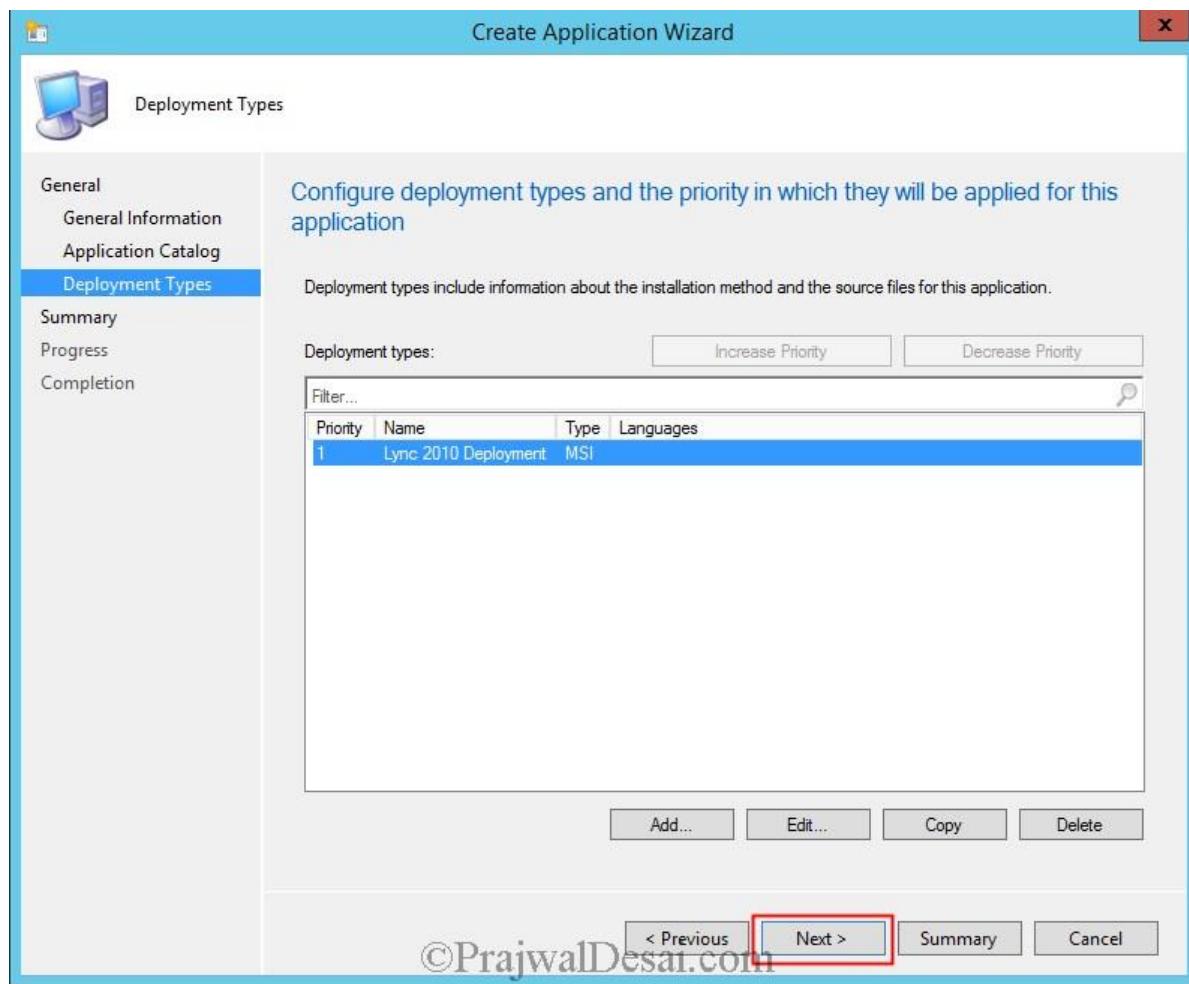


©PrajwalDesai.com

Click **Close**.

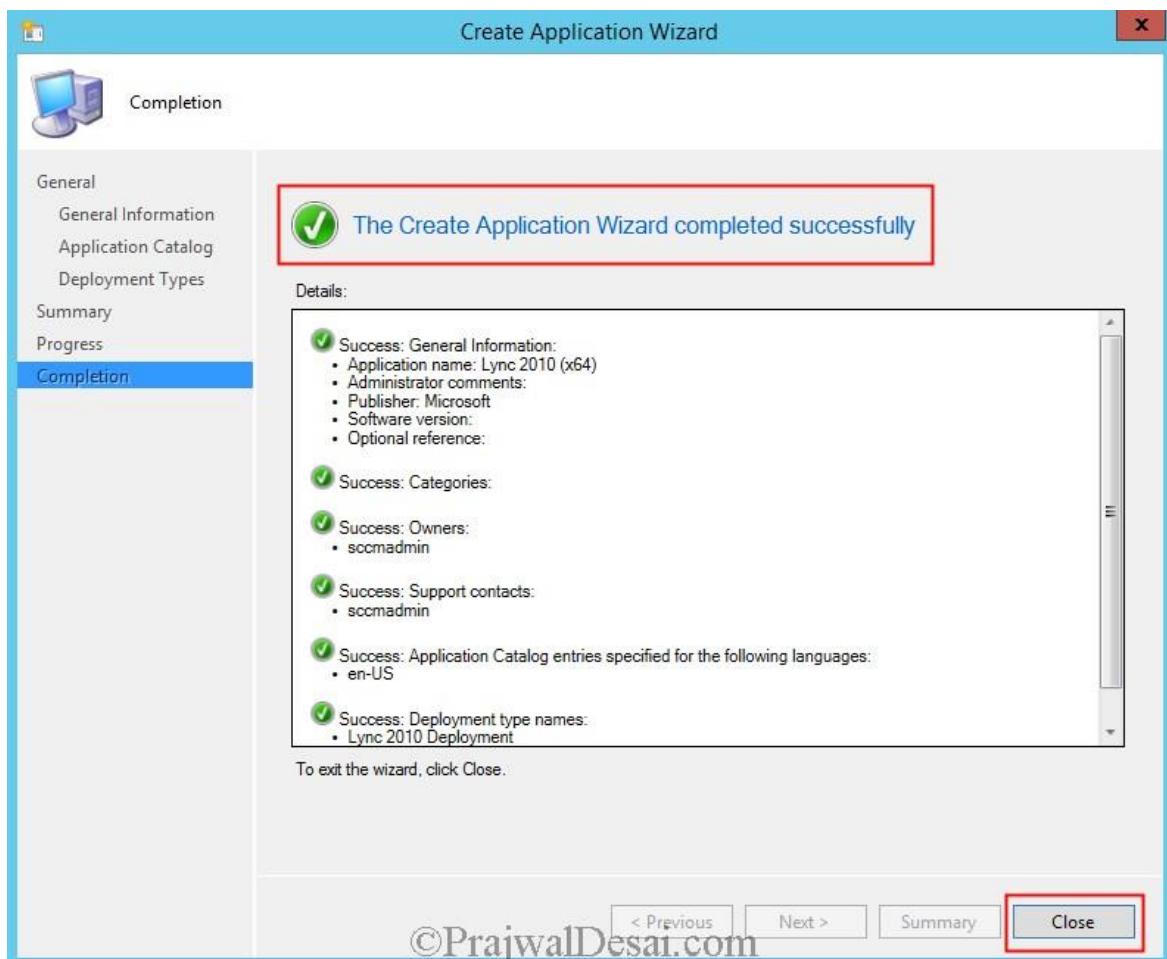


Under the Deployment types we see the Lync 2010 application. Click **Next**.



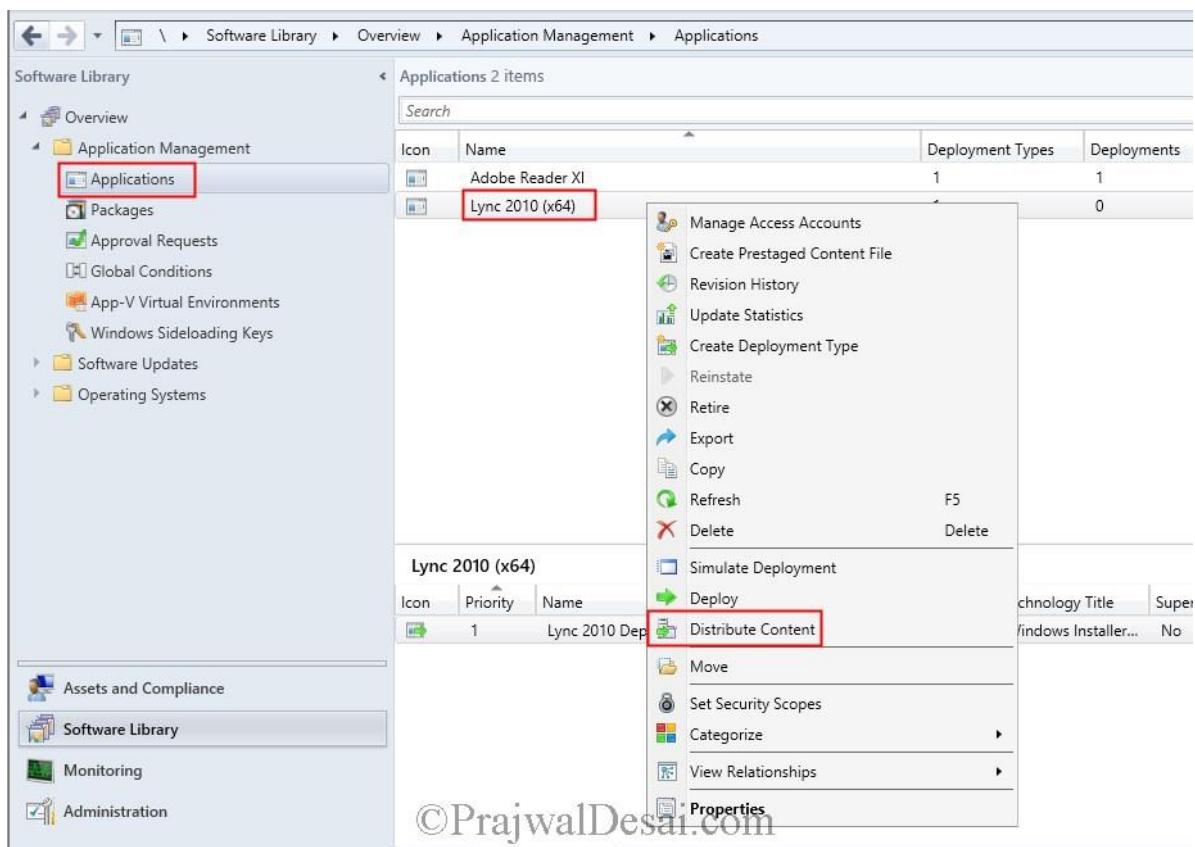
©PrajwalDesai.com

Click on **Close**.

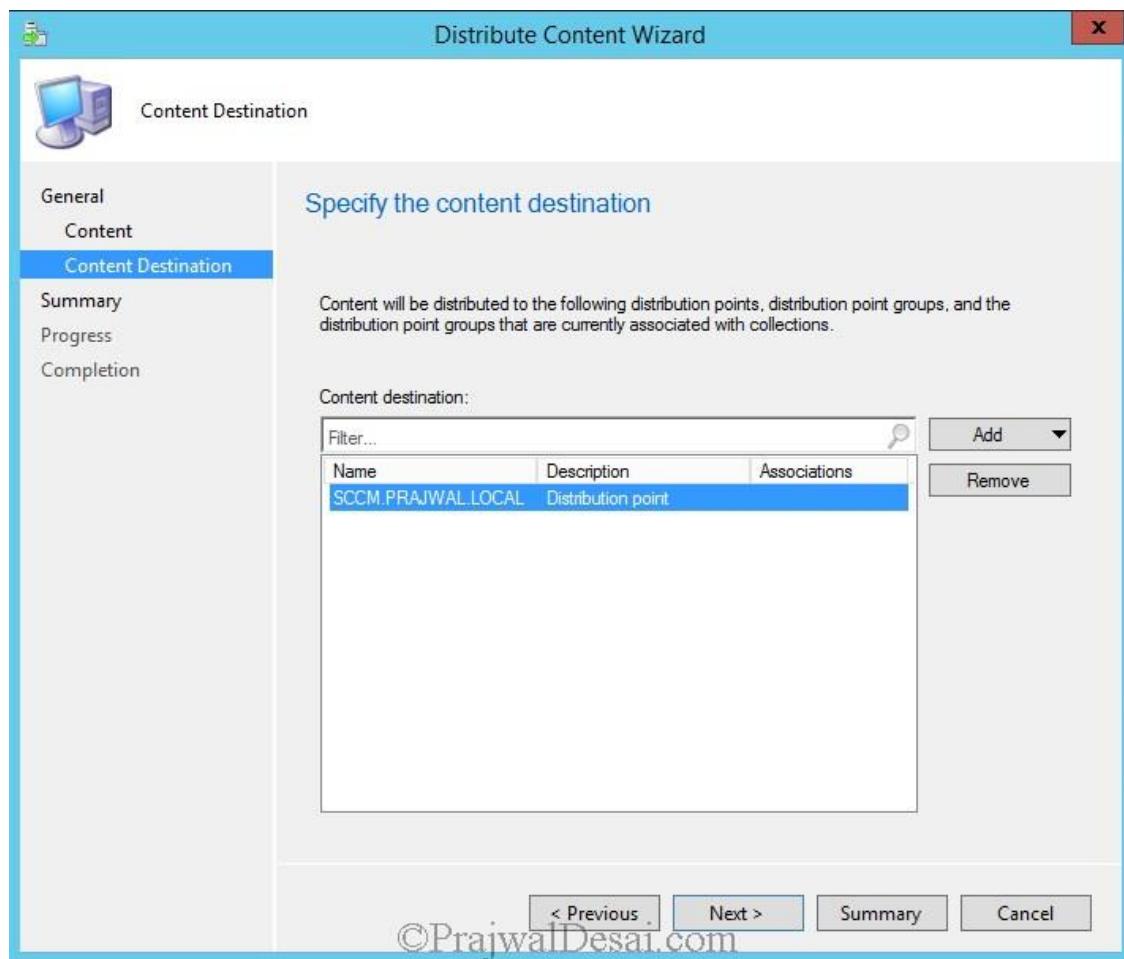


©PrajwalDesai.com

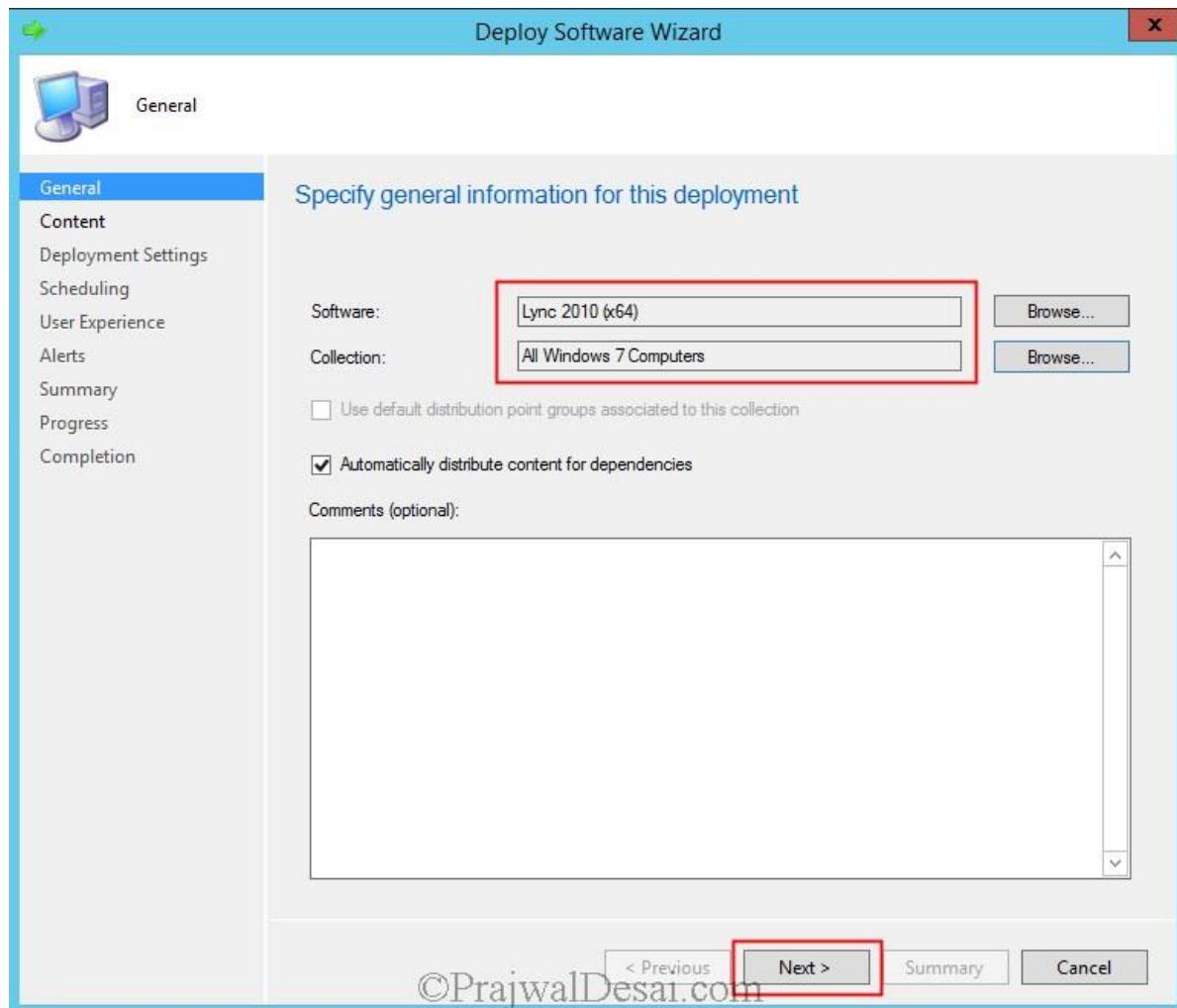
Right click the Lync application (**Lync 2010 (x64)**) and click on **Distribute Content**.



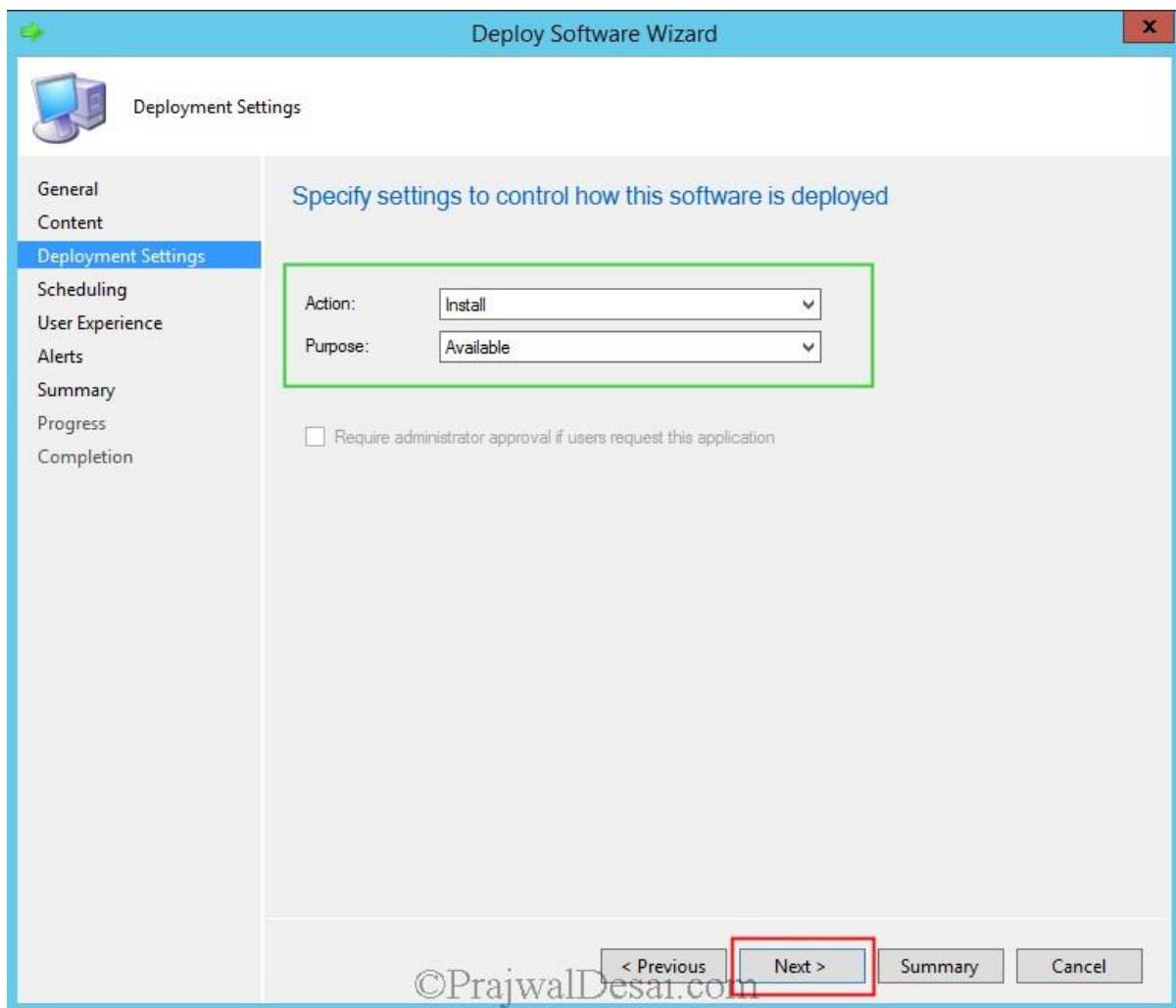
Add the Distribution Point and complete the wizard.



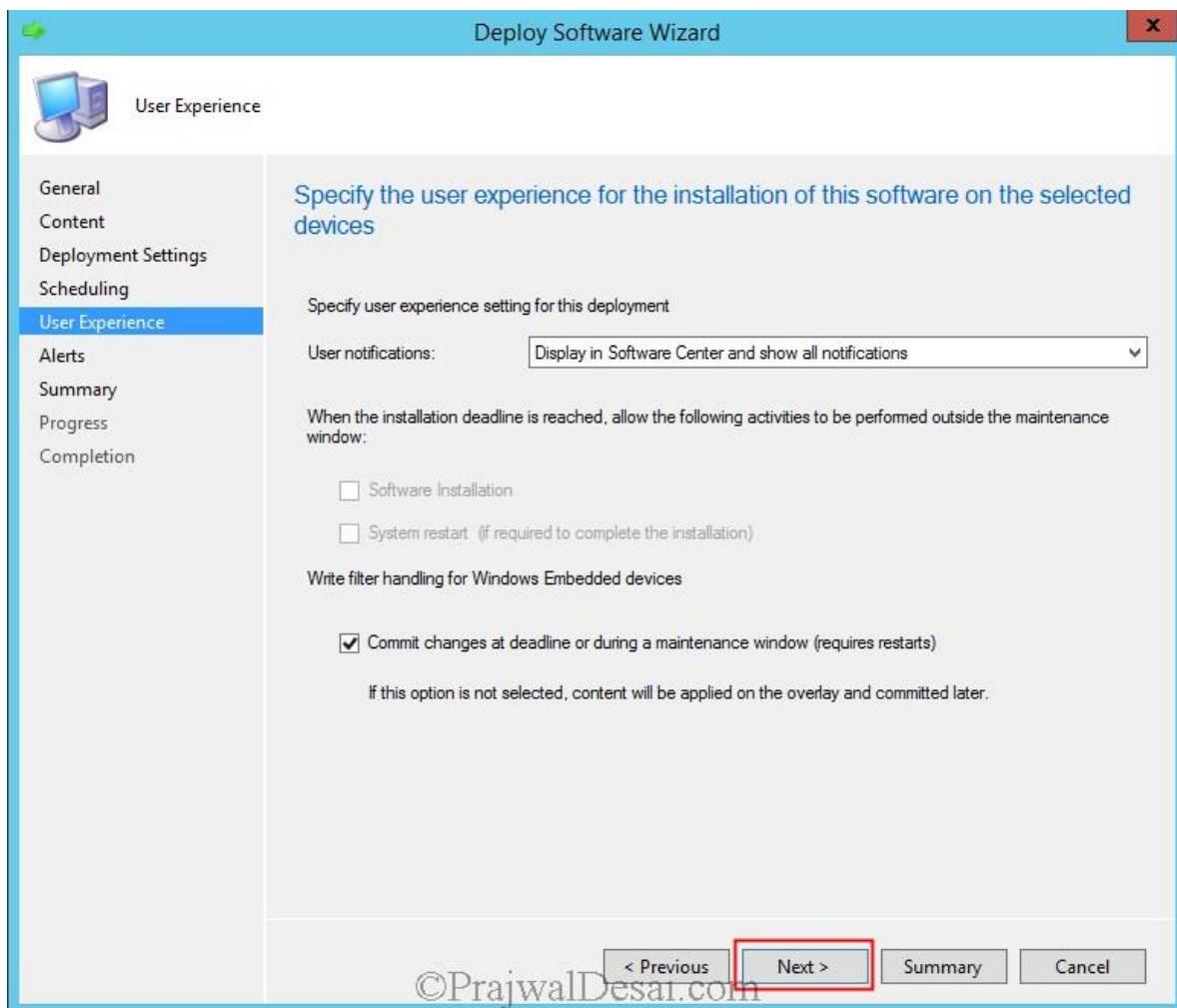
After you distribute the application to DP, right click on the Lync application and click on **Deploy**. Choose the **Collection** where this application is to be deployed and click **Next**.



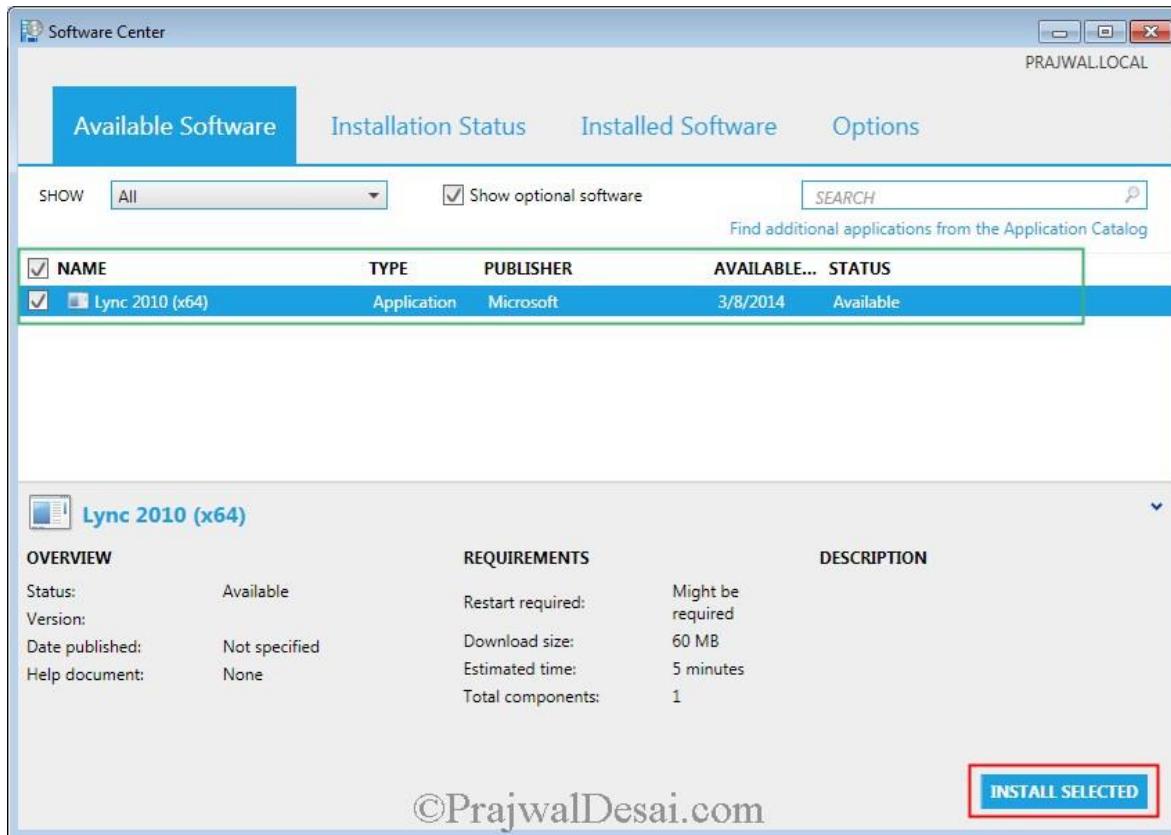
Deployment Settings – Set the Action as **Install** and Purpose as **Available**. Click on **Next**.



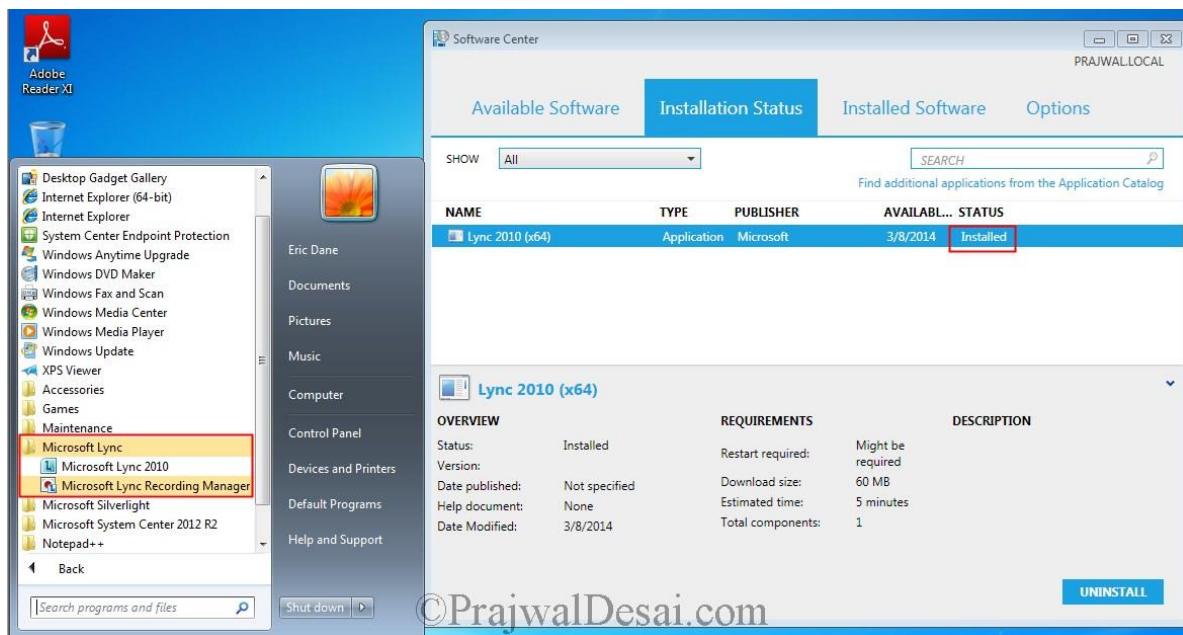
Click on **Next** and complete the wizard.



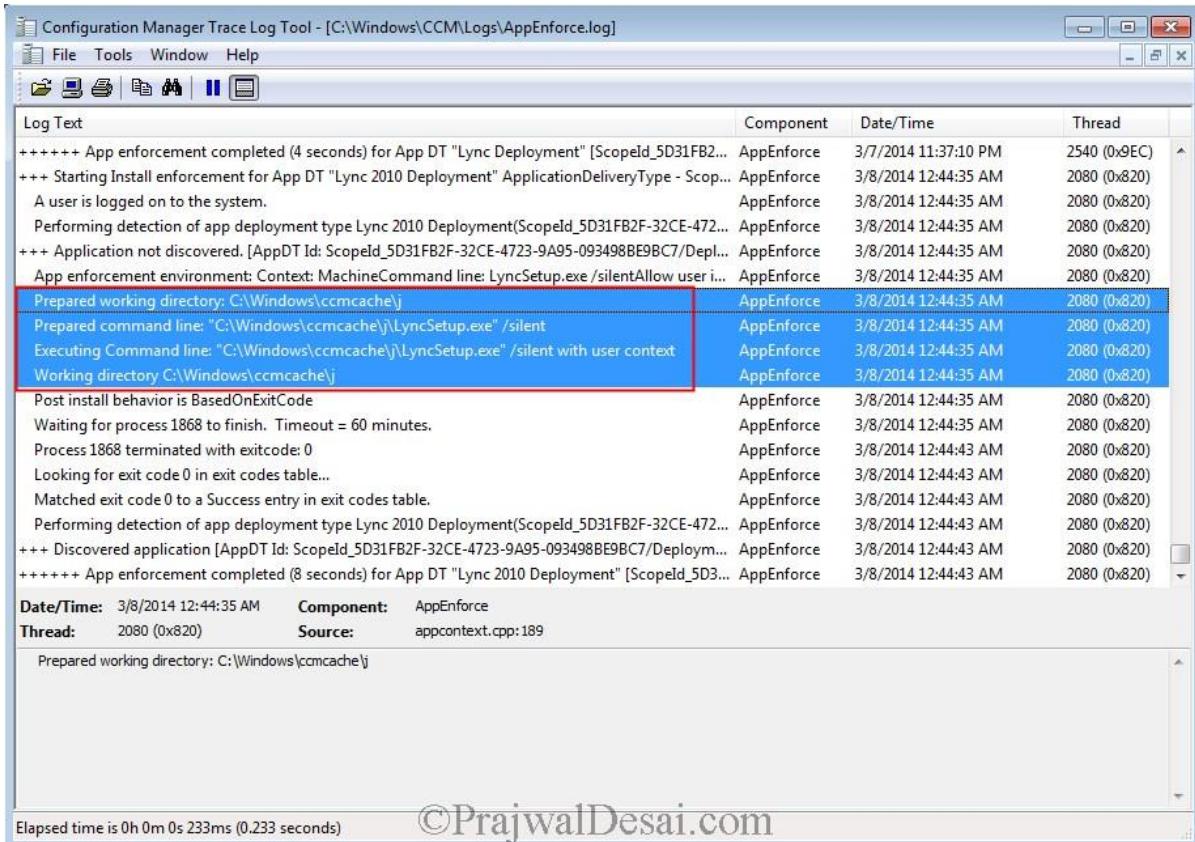
After few minutes the Lync 2010 app can be seen in the **Software Center** under **Available Software**. Select the app and click on **Install Selected**. The app is downloaded from the DP and installed.



The Lync 2010 client has been installed on the computer.



If you want to what's going in the background during the client installation, you can open the **AppEnforce.log** file on the client computer using **CM Trace** tool. If the app fails to install you can check this file for troubleshooting purpose.



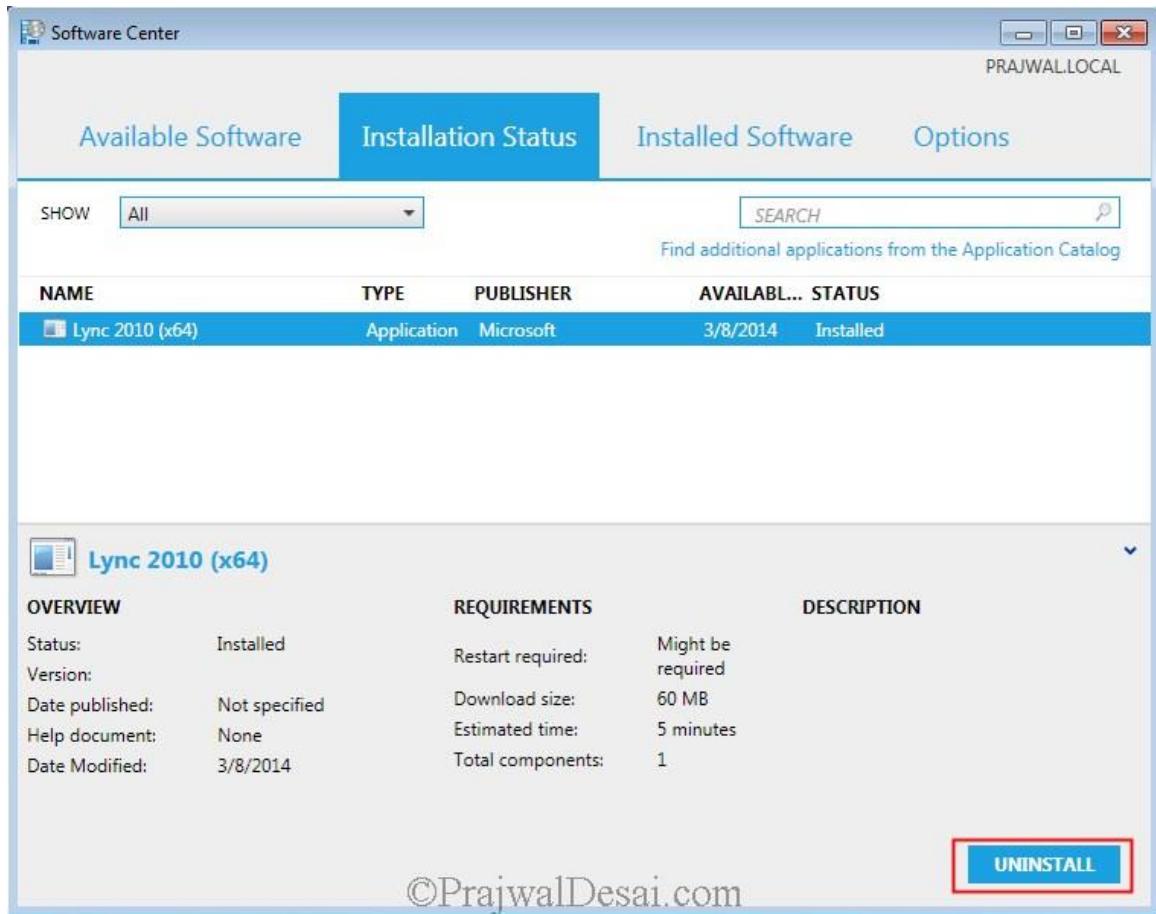
The screenshot shows the Configuration Manager Trace Log Tool interface. The window title is "Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\AppEnforce.log]". The menu bar includes File, Tools, Window, Help, and several icons. The main area is a table with columns: Component, Date/Time, and Thread. The log text section contains several entries related to the Lync 2010 deployment process. A red box highlights a group of four log entries from the "Prepared working directory" section. The bottom of the window displays the copyright information "©PrajwalDesai.com" and the elapsed time "Elapsed time is 0h 0m 0s 233ms (0.233 seconds)".

Log Text	Component	Date/Time	Thread
+++++ App enforcement completed (4 seconds) for App DT "Lync Deployment" [ScopeId_5D31FB2...	AppEnforce	3/7/2014 11:37:10 PM	2540 (0x9EC)
+++ Starting Install enforcement for App DT "Lync 2010 Deployment" ApplicationDeliveryType - Scop...	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
A user is logged on to the system.	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Performing detection of app deployment type Lync 2010 Deployment(ScopeId_5D31FB2F-32CE-472...	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
+++ Application not discovered. [AppDT Id: ScopeId_5D31FB2F-32CE-4723-9A95-093498BE9BC7/Depl...	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
App enforcement environment: Context: MachineCommand line: LyncSetup.exe /silentAllow user i...	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Prepared working directory: C:\Windows\ccmcache\j	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Prepared command line: "C:\Windows\ccmcache\j\lyncsetup.exe" /silent	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Executing Command line: "C:\Windows\ccmcache\j\lyncsetup.exe" /silent with user context	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Working directory C:\Windows\ccmcache\j	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Post install behavior is BasedOnExitCode	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Waiting for process 1868 to finish. Timeout = 60 minutes.	AppEnforce	3/8/2014 12:44:35 AM	2080 (0x820)
Process 1868 terminated with exitcode: 0	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
Looking for exit code 0 in exit codes table...	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
Matched exit code 0 to a Success entry in exit codes table.	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
Performing detection of app deployment type Lync 2010 Deployment(ScopeId_5D31FB2F-32CE-472...	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
+++ Discovered application [AppDT Id: ScopeId_5D31FB2F-32CE-4723-9A95-093498BE9BC7/Depl...	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
+++++ App enforcement completed (8 seconds) for App DT "Lync 2010 Deployment" [ScopeId_5D3...	AppEnforce	3/8/2014 12:44:43 AM	2080 (0x820)
Date/Time: 3/8/2014 12:44:35 Component: AppEnforce			
Thread: 2080 (0x820) Source: appcontext.cpp:189			
Prepared working directory: C:\Windows\ccmcache\j			

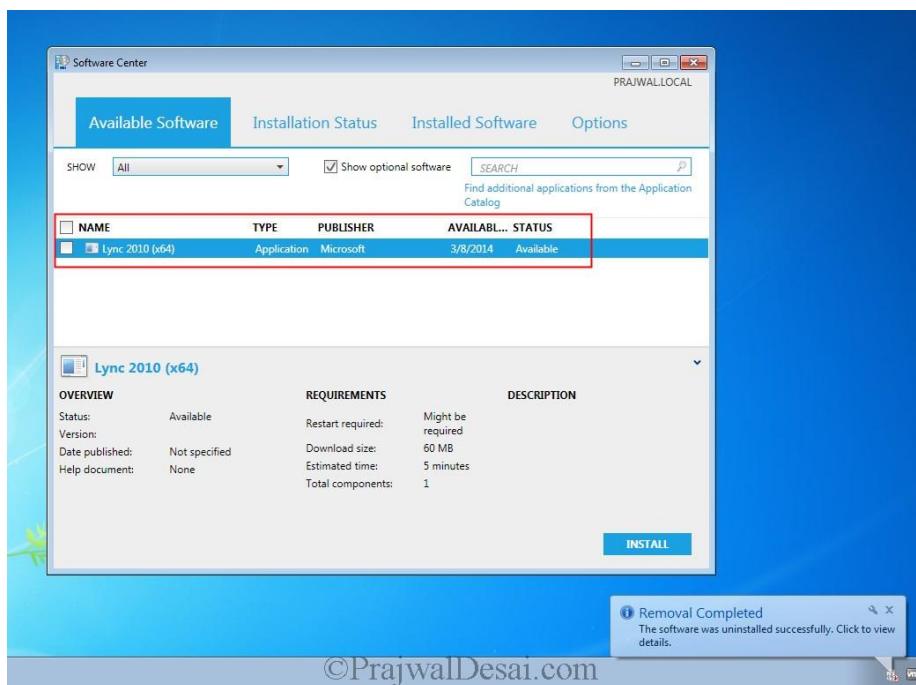
Elapsed time is 0h 0m 0s 233ms (0.233 seconds)

©PrajwalDesai.com

While we were creating the deployment type for this app we had specified the Uninstall Program command. Let's see if the app gets uninstalled without any issues, click on **Uninstall**.



We have uninstalled the Lync Client 2010 successfully. 😊



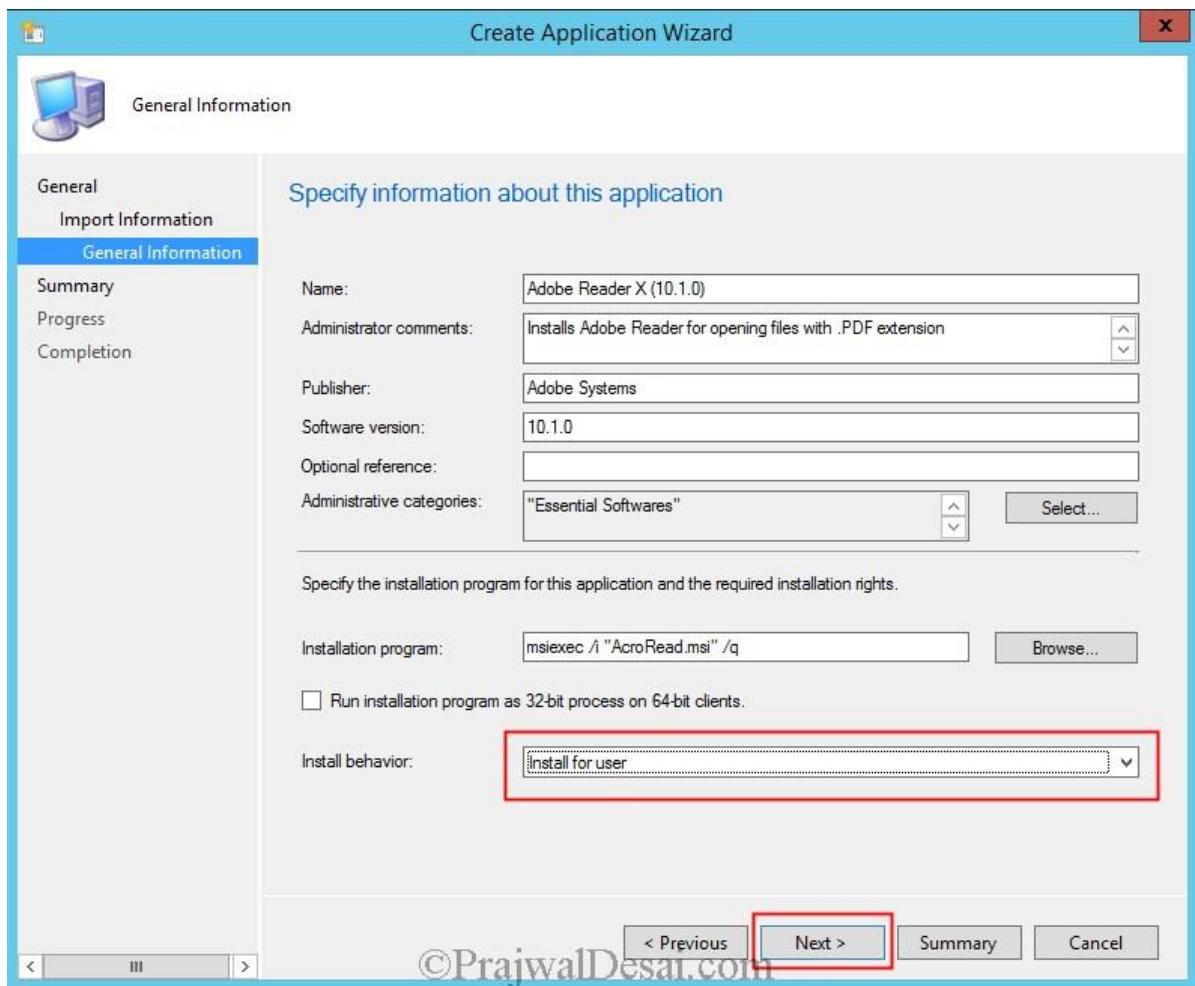
[Deploying Applications To Users Using SCCM 2012 R2](#)

In this post we will look at the steps for deploying applications to users using SCCM 2012 R2. In SCCM 2012 R2, an application basically contains the files and information that are required to deploy software to a device. In one of my post that I had posted when I was deploying SCCM 2012 we had seen the steps for [deploying applications to devices using SCCM 2012](#). Applications in Configuration Manager support user-centric management so that you can associate specific users with specific devices. Instead of having to remember the name of a user's device, you can now deploy software to the user and to the device. This functionality can help you make sure that the most important software is always available on each device that a specific user accesses. If a user acquires a new computer, you can automatically install the user's applications on the device before the user logs on.

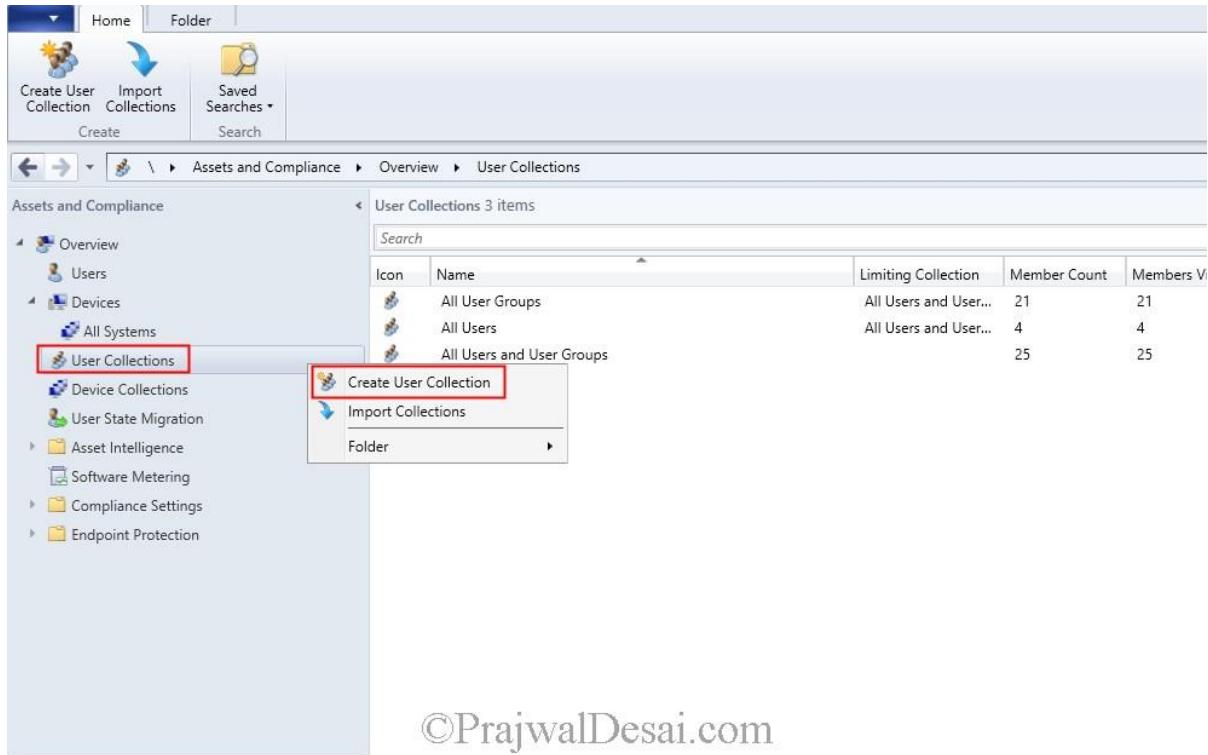
If an application is deployed by SCCM 2012 R2 and has been installed on a device, the Configuration Manager always checks whether the application is present on the device or not. Let's say if the application was uninstalled by the user then at the next evaluation cycle, Configuration Manager detects that the application is not present and reinstalls it. This is one of the good feature I liked about Configuration Manager.

The re-evaluation interval for application deployments can be configured by using the **Schedule re-evaluation for deployments** client setting. The default value is every 7 days. You can also initiate this action from a Configuration Manager client computer by selecting the action **Application Deployment Evaluation Cycle** from the **Actions** tab of **Configuration Manager** in Control Panel.

In this post we will be deploying a simple application to the user and this application won't install unless the SCCM administrator/approver approves it. In the below example I am creating a application for Adobe Reader and this will be deployed to the user group. You can take any application of your choice and follow the below screenshots. Enter the information about the application and choose the **Install behavior** as **Install for User** and click **Next** and complete the App creation wizard.

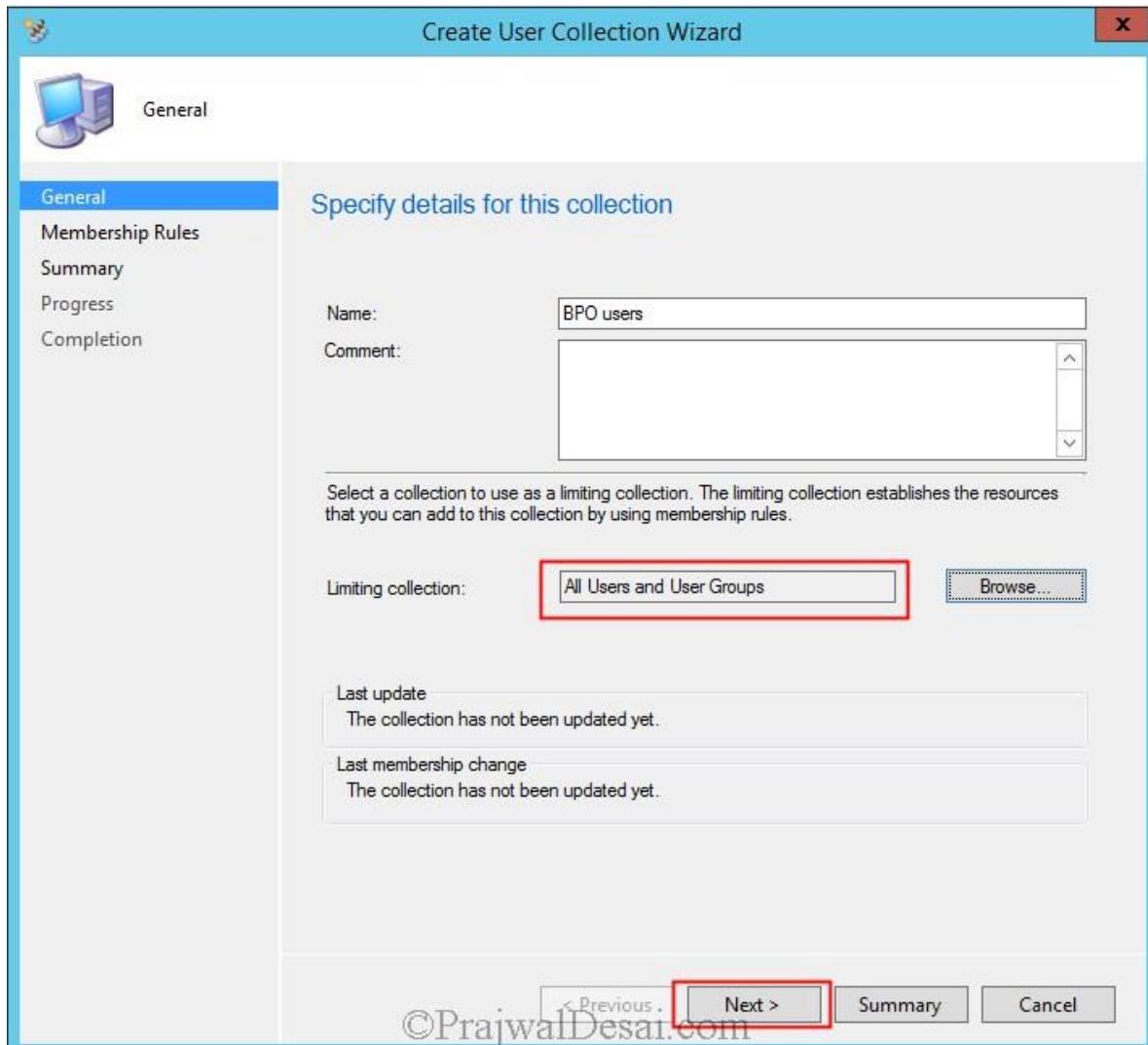


Since we will be deploying the application to the users, we will first create a group in active directory and add the user to that group. I have skipped the screenshots as it's fairly simple to create a group and add user to it. Once you have done that, right click the **User Collections** and click **Create User Collection**.

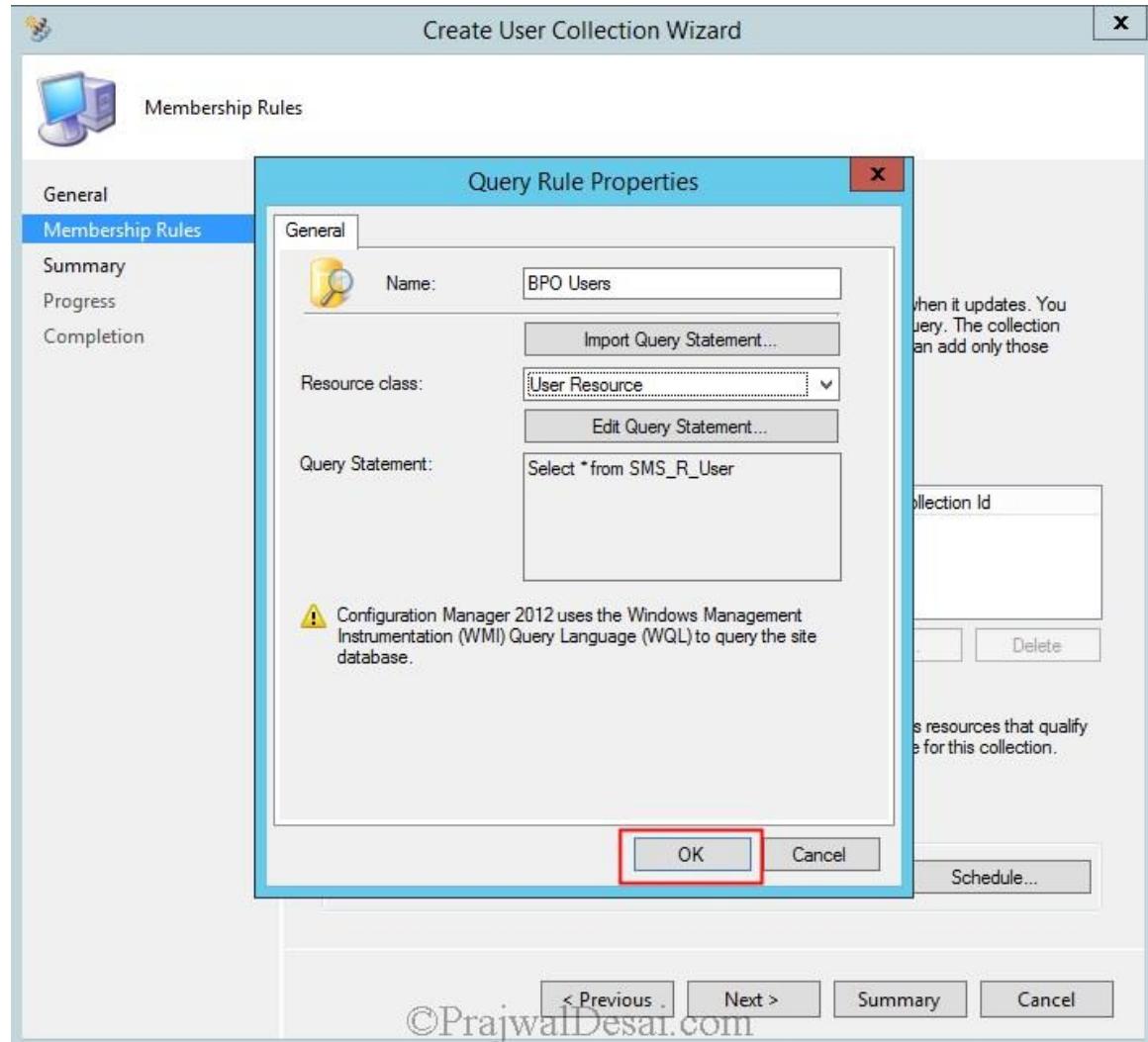


©PrajwalDesai.com

Specify a name to the user collection and set the **Limiting collection** to **All Users and User Groups**. Click **Next**.

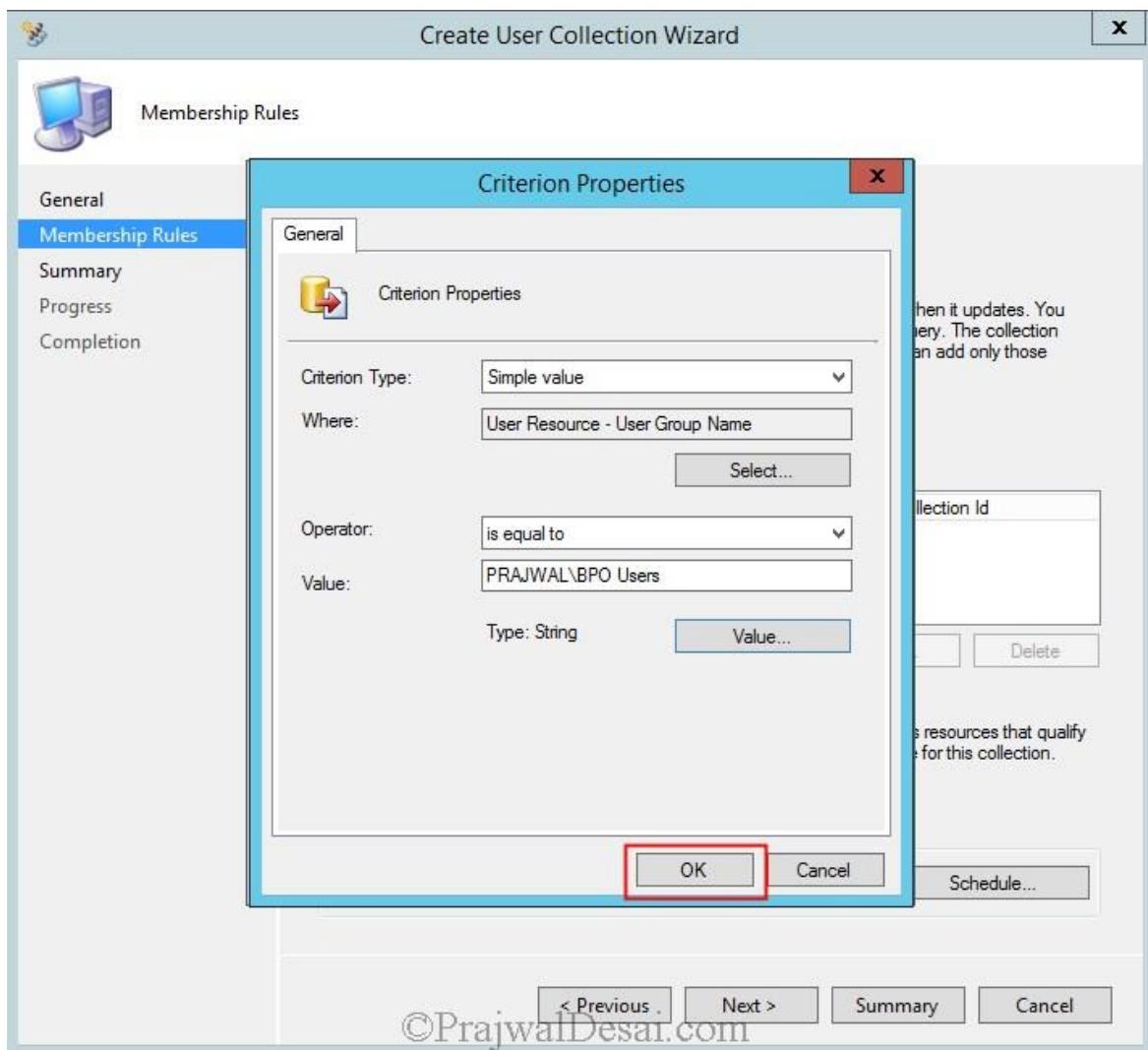


Now let's create a query which will add the user group to the collection. Click **Add Rule** and select **Query Rule**. Specify a name for the query and Click **Edit Query Statement**.



On the **Query Statement Properties** window click on tab named **Criteria** and click on yellow icon. On the **Criterion Properties** window, set **Attribute Class** to **User Resource**, set **Attribute** to **User Group Name**. Set the **Value** as the name of the group that you created in your active directory. In this example BPO Users is the group that is created in active directory that contains user named Eric.

Click **OK** and then click **Next** and complete the **User Collection wizard**.



©PrajwallDesai.com

In the Configuration Manager console, when we click **User Collections**, we see that the user collection **BPO Users** has been created.

The screenshot shows the Configuration Manager console under the 'Assets and Compliance' category. In the left navigation pane, 'User Collections' is selected. The main area displays a table titled 'User Collections 4 items'. The table includes columns for Icon, Name, Limiting Collection, Member Count, Members Visible on Site, and Referenced Collections. A new entry, 'BPO users', is listed at the bottom of the table, highlighted with a red box. The table data is as follows:

Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
User Group	All User Groups	All Users and User Groups	22	22	0
User	All Users	All Users and User Groups	4	4	0
User Group	All Users and User Groups		26	26	0
User	BPO users	All Users and User Groups	1	1	0

©PrajwalDesai.com

Next we will deploy the application to the user collection. Right click the Adobe application and click **Deploy**.

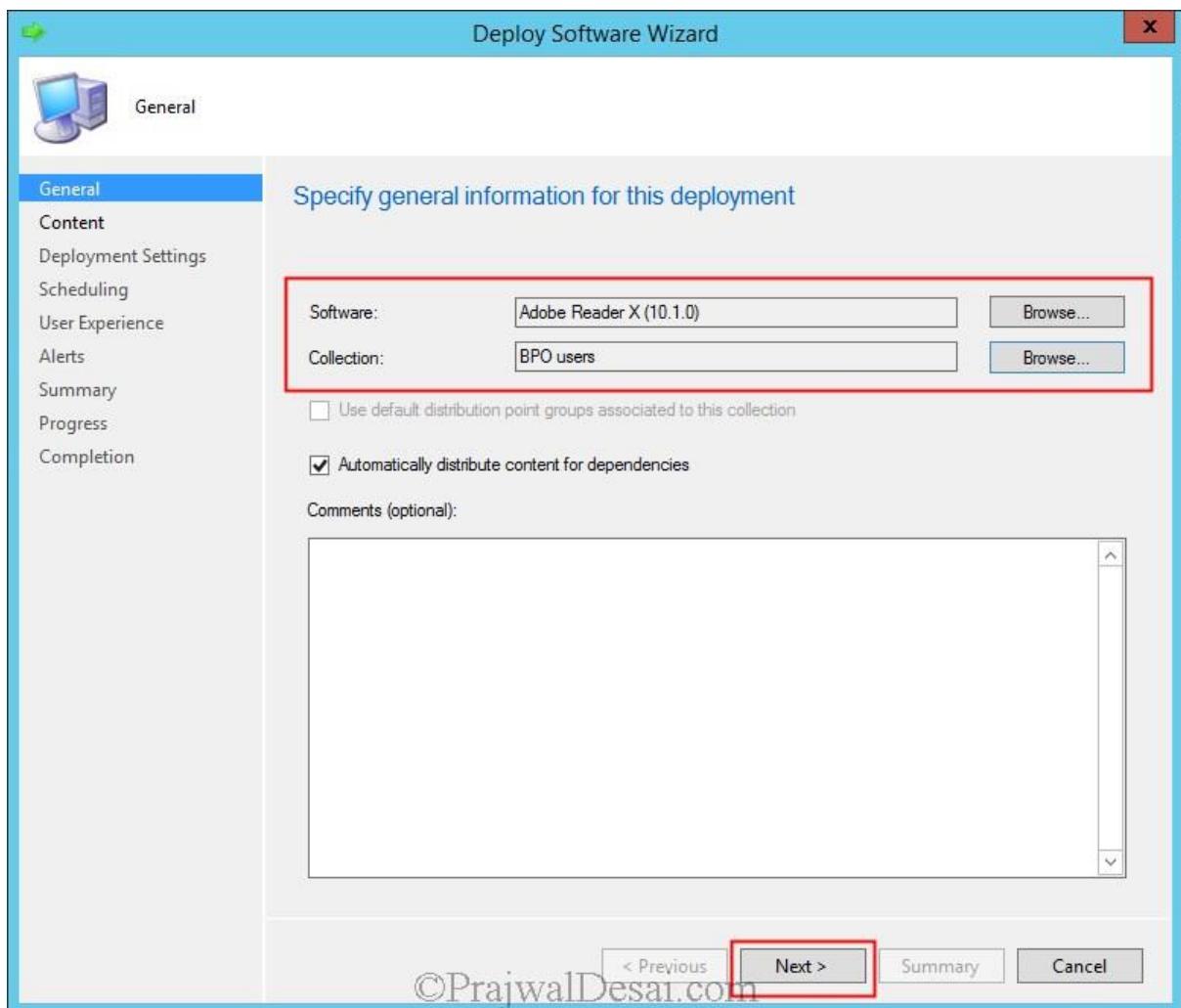
The screenshot shows the Configuration Manager console under the 'Software Library' category. In the left navigation pane, 'Application Management' is selected, and 'Applications' is highlighted with a red box. The main area displays a table titled 'Applications 1 items'. The table includes columns for Icon, Name, Deployment Types, Deployments, and Status. One item, 'Adobe Reader X (10.1.0)', is listed with a status of 'Active'. The table data is as follows:

Icon	Name	Deployment Types	Deployments	Status
File	Adobe Reader X (10.1.0)	1	0	Active

A context menu is open for the 'Adobe Reader X (10.1.0)' application. The menu items are: Manage Access Accounts, Create Prestaged Content File, Revision History, Update Statistics, Create Deployment Type, Reinstate, Retire, Export, Copy, Refresh, Delete, Simulate Deployment, Deploy (highlighted with a red box), Distribute Content, Move, Set Security Scopes, Categorize, View Relationships, and Properties.

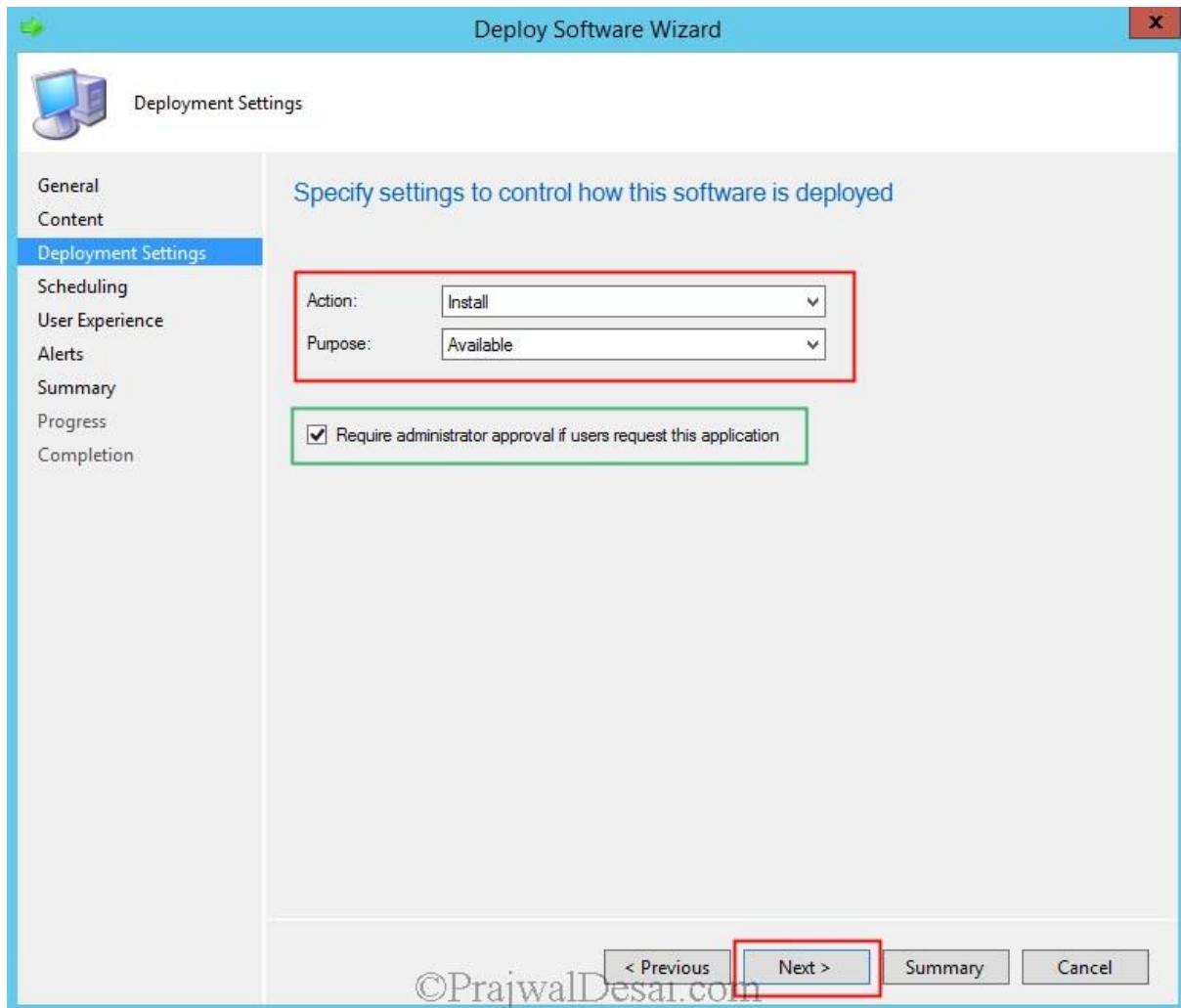
©PrajwalDesai.com

Click **Browse** and choose the collection as **BPO Users**. Click **Next**.

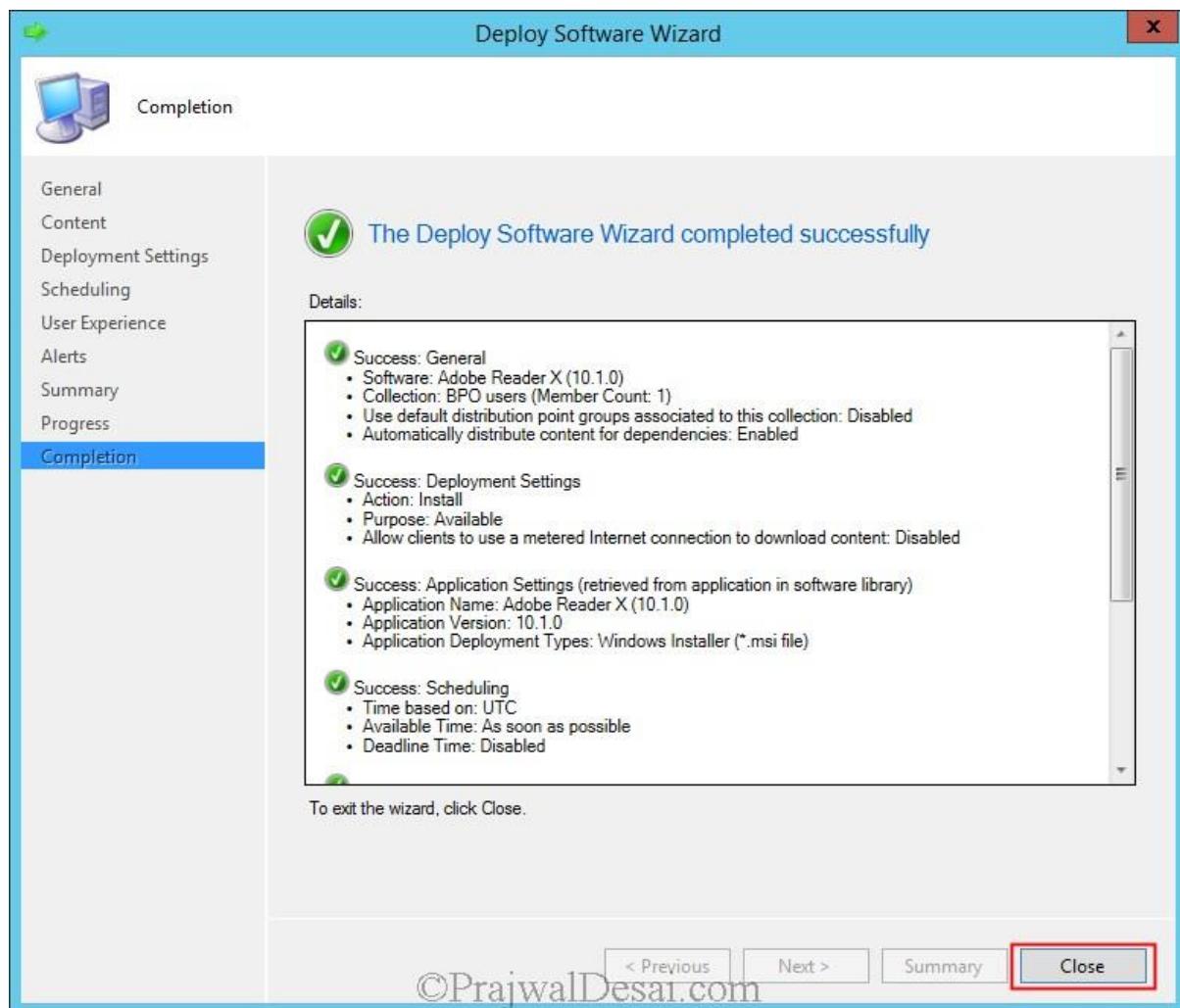


©PrajwalDesai.com

Specify the **Deployment Settings**, choose **Action** as **Install** and **Purpose** as **Available**. Check box “**Require administrator approval if users request this application**“. When you check this option, the application will be available to the user but it cannot be installed without SCCM administrator/approver approving it. Click **Next** and complete the wizard.



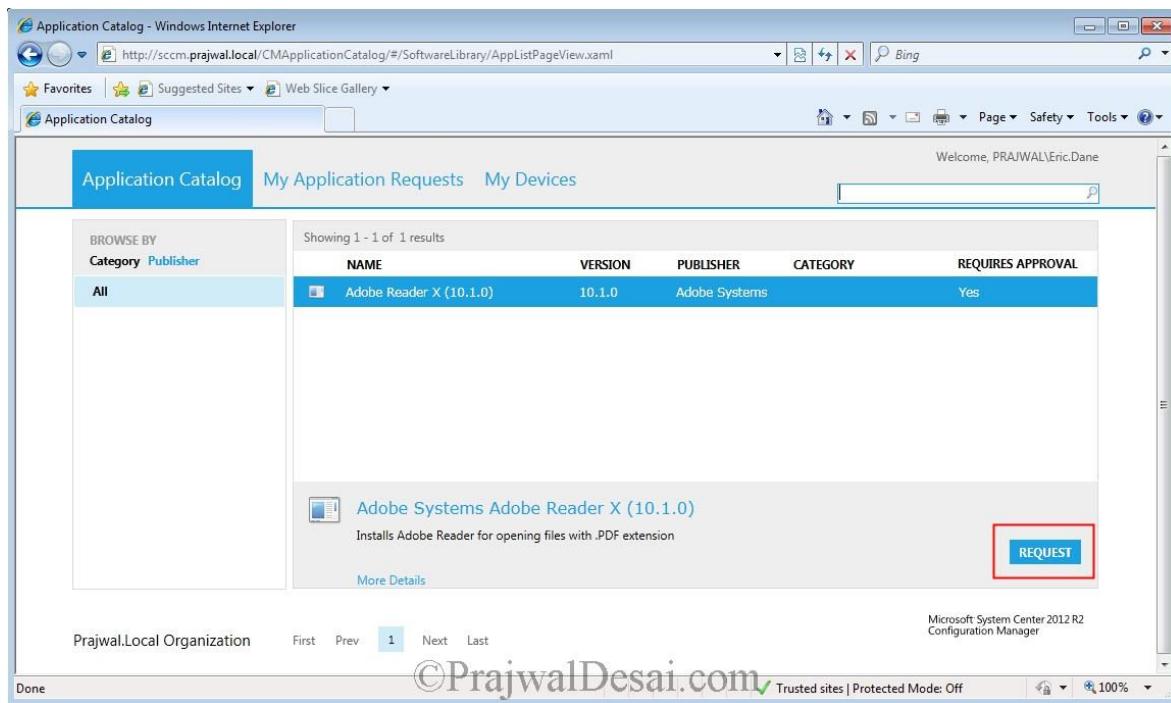
We have deployed the application to the user. Click **Close**.



The software has been deployed to the user group. Let's login with the user account that is member of **BPO Users** group. Launch the **Software Center** and click on **Find additional applications from the Application Catalog**. When you click the link you will be prompted for user authentication, provide the username and password of logged in user account.



When you click **Application Catalog**, we see the Adobe application over there. There is no **Install** option seen because during our application deployment we have defined that the user must first request the SCCM administrator/approver for installing the software. So click on **REQUEST**.



You can send the reason for application request so that administrator/approver can know why exactly you need the software. Click on **SUBMIT**.

The screenshot shows a Windows Internet Explorer window titled "Request approval - Windows Internet Explorer". The URL is <http://sccm.prajwal.local/CMApplicationCatalog/#/SoftwareCatalog/RequestWizard/RequestWizardForSoftware>. The page is part of the "Application Catalog" section, with tabs for "My Application Requests" and "My Devices". The user is logged in as "PRAJWAL\Eric.Dane".

The main content area displays a software item: "Adobe Systems Adobe Reader X (10.1.0)". Below it, under "REQUEST APPROVAL", is a text input field for the "Reason for application request (required)". The input field contains the following text:

```
Hi Prajwal,  
I need this software for opening .pdf files. Request you to approve the  
same.  
Thanks,  
Eric Dane
```

Below the input field, it says "Characters remaining: 1891". At the bottom right of the form are two buttons: "SUBMIT" (highlighted with a red box) and "CANCEL".

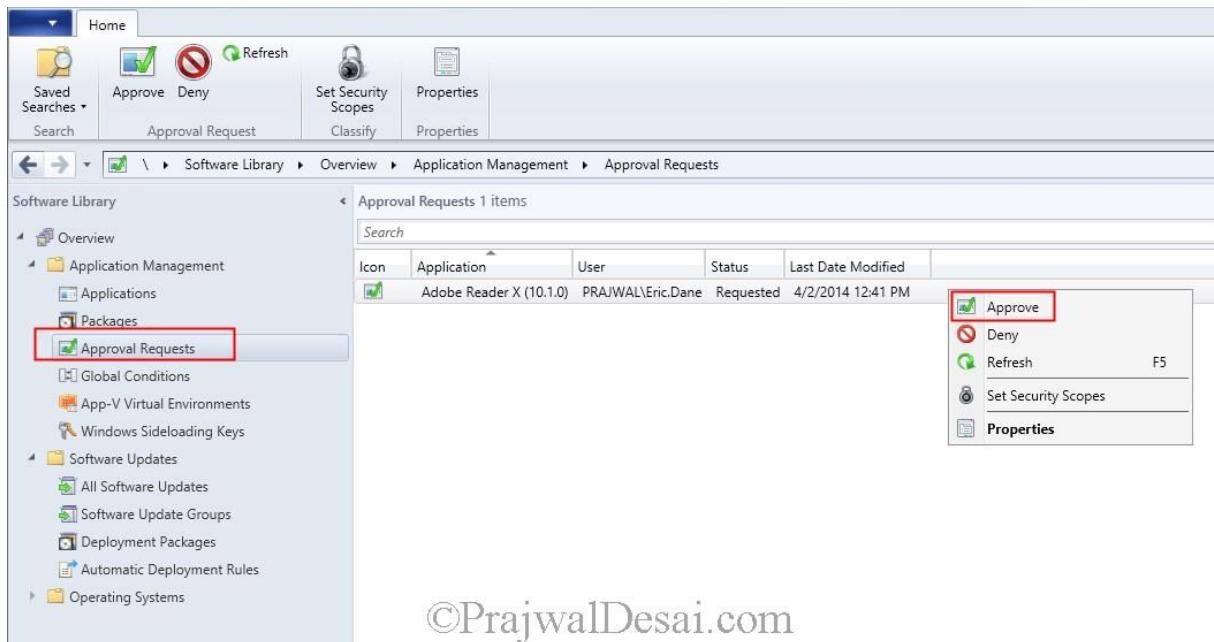
The status bar at the bottom of the browser window shows "Prajwal.Local Organization" and "Microsoft System Center 2012 R2 Configuration Manager". The address bar shows "Done" and the URL.

The approval request has now been sent to the administrator/approver. Let's go back to Configuration Manager console and check it.

The screenshot shows a Microsoft Internet Explorer window with the title "Request submitted - Windows Internet Explorer". The URL is <http://sccm.prajwal.local/CMAApplicationCatalog/#/SoftwareCatalog/RequestWizard/RequestWizardFor>. The page displays the "Application Catalog" interface. On the left, there is a sidebar titled "BROWSE BY" with "Category" and "Publisher" options, and a "All" link which is highlighted. In the main content area, there is a section titled "Adobe Systems Adobe Reader X (10.1.0)" with a small icon. Below this, under "REQUEST APPROVAL", there is a green checkmark icon followed by the text "Your request has been submitted." A note below it says "You can track the status of this request from the My Application Requests tab." At the bottom of the main content area, there are two links: "View My Application Requests" and "Back to Application Catalog". The status bar at the bottom of the browser window shows "Prajwal.Local Organization" on the left and "Microsoft System Center 2012 R2 Configuration Manager" on the right. The address bar shows "Done" and the URL again. The search bar contains "©PrajwalDesai.com". The bottom right corner of the browser window shows "Trusted sites | Protected Mode: Off" and "100%".

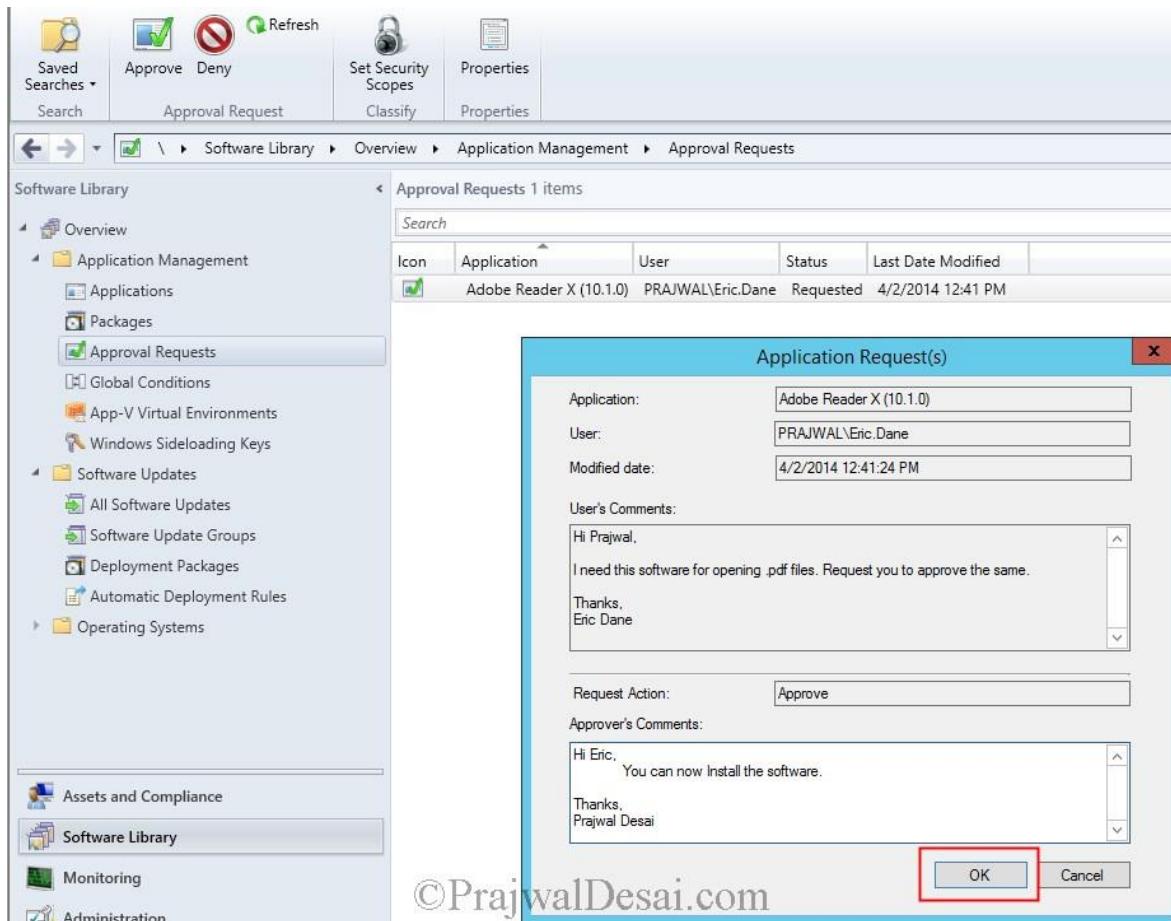
In the **Configuration Manager** console, under **Application Management**, click **Approval Requests**. We see that there is one request from the user Eric.

To approve the application, right click the application and click **Approve**.



©PrajwalDesai.com

On the **Application Request** window the administrator/approver can see user comments and even add the comments. Click on **OK**.



©PrajwalDesai.com

On the client machine refresh the link once and we see the **INSTALL** option. Also under **REQUIRES APPROVAL** we see its **No**, that means the application has been approved for installation. Click on **Install** to install the application.

The screenshot shows a Microsoft Internet Explorer window displaying the Microsoft System Center 2012 R2 Configuration Manager Application Catalog. The URL in the address bar is <http://sccm.prajwal.local/CMAApplicationCatalog/#/SoftwareCatalog/FullRefresh/true>. The page title is "Application Catalog". The main content area shows a table of results:

NAME	VERSION	PUBLISHER	CATEGORY	REQUIRES APPROVAL
Adobe Reader X (10.1.0)	10.1.0	Adobe...		No

Below the table, there is a summary for the "Adobe Systems Adobe Reader X (10.1.0)" entry:

Installs Adobe Reader for opening files with .PDF extension

[More Details](#) INSTALL

At the bottom of the page, there are navigation links for "Prajwal.Local Organization", "First", "Prev", "1", "Next", and "Last". On the right side, there is a note: "Microsoft System Center 2012 R2 Configuration Manager". The status bar at the bottom shows "Done", "©PrajwalDesai.com", "Trusted sites | Protected Mode: Off", and "100%".

The application installation has started and it will be installed.

A screenshot of a Microsoft System Center 2012 R2 Configuration Manager interface. The browser title bar says "Application installation result - Windows Internet Explorer". The URL is "http://sccm.prajwal.local/CMApplicationCatalog/#/SoftwareCatalog/FastInstall/Fast". The page shows the "Application Catalog" tab selected. A message box with a green checkmark says "Your application installation has started. The application will install on your computer and you will be notified when the application installation finishes." Below the message is a link "Back to Application Catalog". The left sidebar shows "BROWSE BY Category Publisher" with "All" selected. The right sidebar shows "Microsoft System Center 2012 R2 Configuration Manager". The footer includes "Prajwal.Local Organization", "©PrajwalDesai.com", "Trusted sites | Protected Mode: Off", and "100%".

You can always check your application requests by clicking on **My Application Requests**.

A screenshot of the "My application requests" page. The browser title bar says "My application requests - Windows Internet Explorer". The URL is "http://sccm.prajwal.local/CMApplicationCatalog/#/MySoftwareRequests". The page shows the "My Application Requests" tab selected. It displays a table of results:

NAME	PUBLISHER	CATEGORY	STATUS	LAST UPDATED
Adobe Reader X (10.1.0)	Adobe Systems		Approved	4/2/2014 12:43 PM

Below the table, there is a detailed view of the "Adobe Reader X (10.1.0)" entry. It shows "LATEST STATUS" (Approved on: 4/2/2014 12:43 PM) and "COMMENTS" (Hi Eric, You can now Install the software.). There is a "VIEW HISTORY" button. The footer includes "Prajwal.Local Organization", "©PrajwalDesai.com", "Trusted sites | Protected Mode: Off", and "100%".

Deploying Endpoint Protection Updates Offline Using SCCM 2012 R2

Deploying Endpoint Protection Updates Offline Using SCCM 2012 R2 In this post we will look at the steps for Deploying [Endpoint Protection](#) Updates Offline Using SCCM 2012 R2. We know that with Endpoint Protection in Microsoft System Center 2012 Configuration Manager, you can use any of several available methods mentioned below to keep antimalware definitions up to date on client computers in your hierarchy. To update antimalware definitions, you can use one or more of the following methods:

Updates distributed from Configuration Manager – This method uses Configuration Manager software updates to deliver definition and engine updates to computers in your hierarchy.

Updates distributed from Windows Server Update Services (WSUS) – This method uses your WSUS infrastructure to deliver definition and engine updates to computers.

Updates distributed from Microsoft Update – This method allows computers to connect directly to Microsoft Update in order to download definition and engine updates. This method can be useful for computers that are not often connected to the business network.

Updates distributed from Microsoft Malware Protection Center – This method will download definition updates from the Microsoft Malware Protection Center.

Updates from UNC file shares – With this method, you can save the latest definition and engine updates to a share on the network. Clients can then access the network to install the updates.

I will not be covering the installation and configuration of [Endpoint Protection role](#). If you are looking for the [Endpoint Protection role](#) deployment then please check the below links.

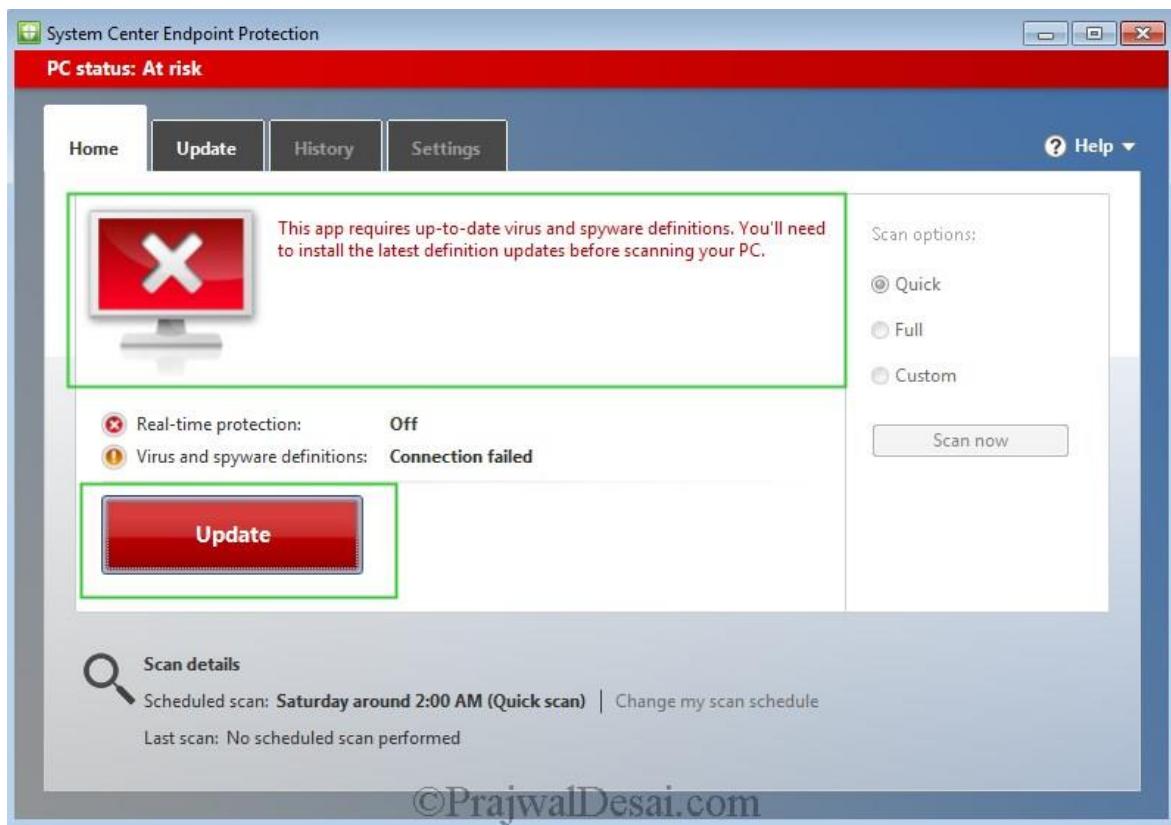
In this post we will download the Antivirus and Antispyware updates for [Endpoint Protection](#) from [Malware Protection Center](#) and deploy it using SCCM 2012 R2. Antivirus and Antispyware updates for Endpoint Protection are available for 32 bit and 64 bit versions. Depending upon the OS version (32 / 64 bit) download the update file, the update file will have either of these names ***mpam-fe.exe, mpas-fe.exe, or mpam-feX64.exe.***

Deploying Endpoint Protection Updates Offline Using SCCM 2012 R2

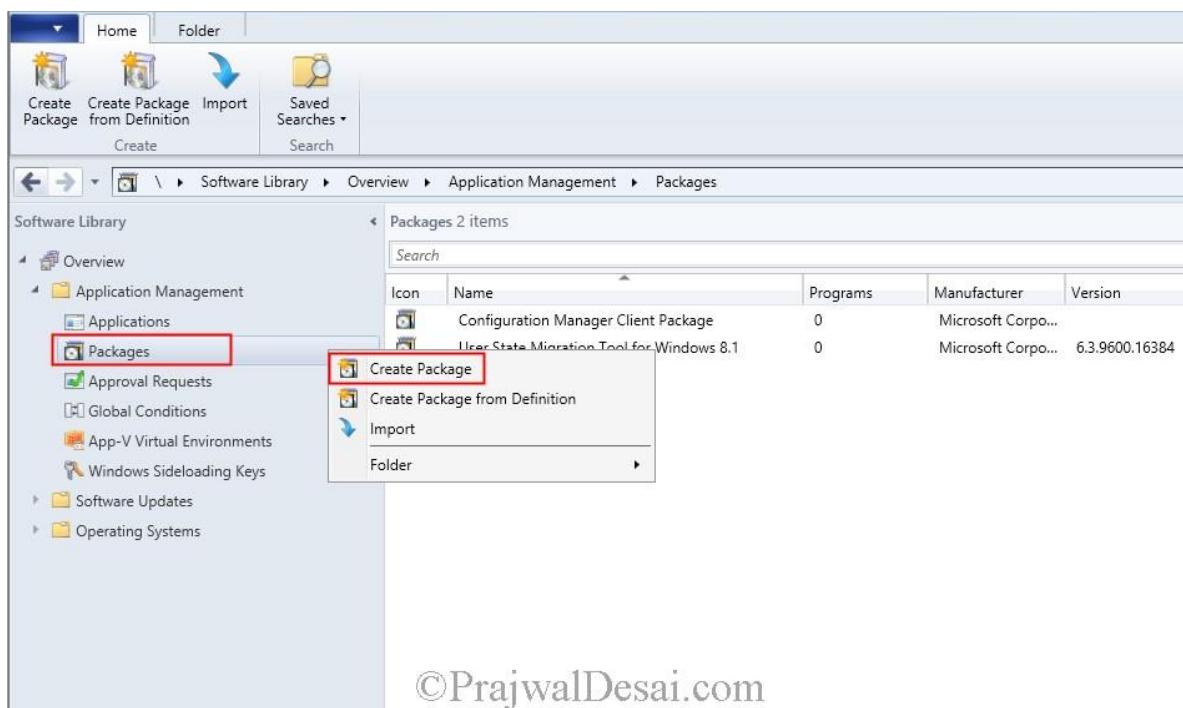
In this post we will be deploying [Endpoint Protection](#) updates offline using SCCM 2012 R2 for a Windows 7 computers device collection. So I have downloaded the update file ***mpam-feX64.exe*** and the update file is copied to a shared folder on SCCM server.

Antivirus and antispyware definitions (choose either 32-bit or 64-bit depending on your computer)	
Microsoft Security Essentials	32-bit 64-bit
Windows Defender in Windows 8.1	32-bit 64-bit ARM
Windows Defender in Windows 7 and Windows Vista	32-bit 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)	32-bit 64-bit
Forefront Client Security	32-bit 64-bit
Forefront Server Security	32-bit 64-bit
Forefront Endpoint Protection	32-bit 64-bit
System Center 2012 Configuration Manager	32-bit 64-bit
System Center 2012 Endpoint Protection	32-bit 64-bit
Windows Intune	32-bit 64-bit

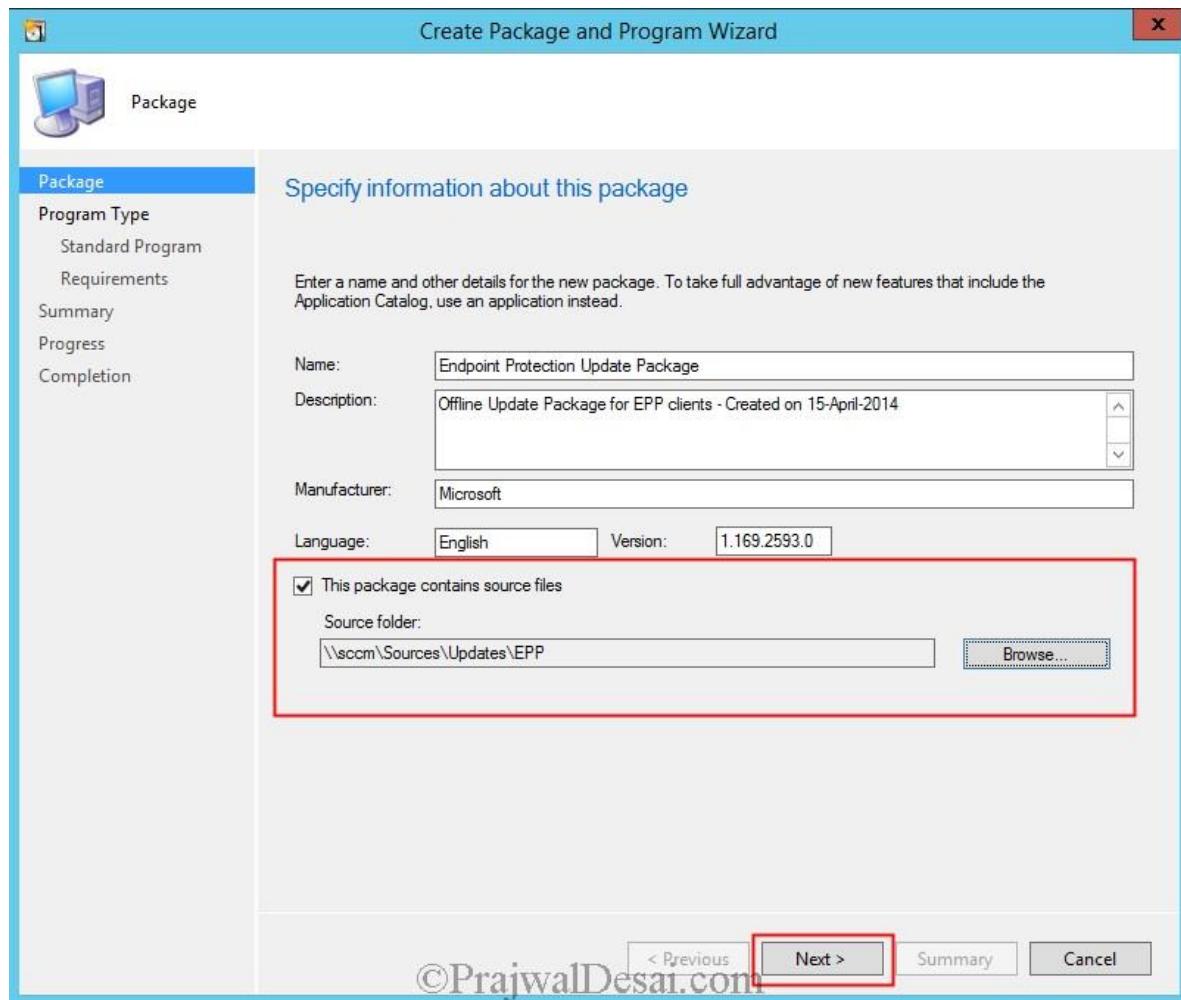
Let's take a look at one of the computer which is installed with Endpoint Protection client. Note that the antivirus updates are not yet deployed so the **PC status** shows **At Risk** and is **RED** color.



In the Configuration Manager console, click **Software Library**, expand **Application Management**, right click **Packages** and click **Create Package**.

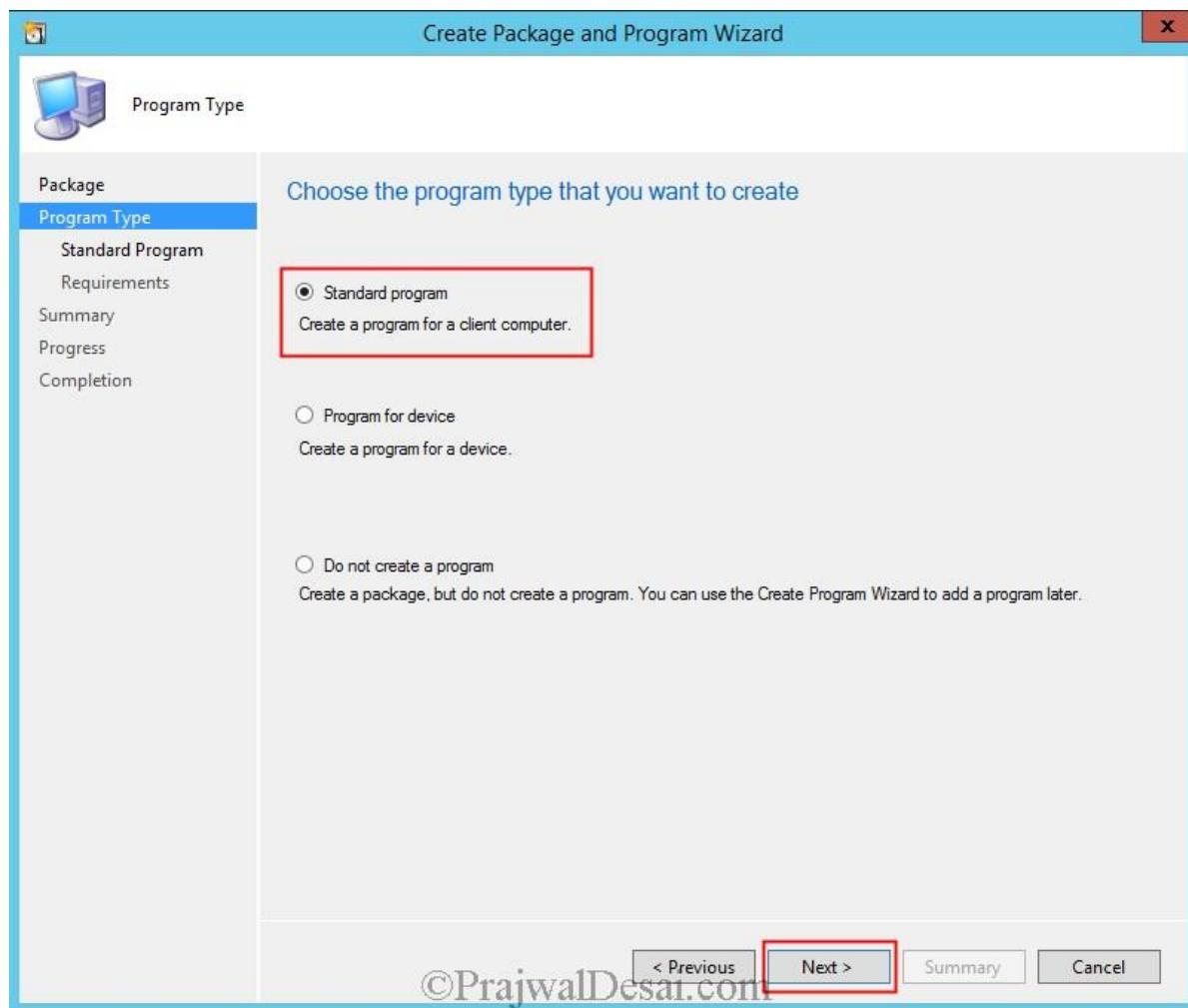


Specify details about the package. Choose the **Source Folder** where the update file is located and click **Next**.



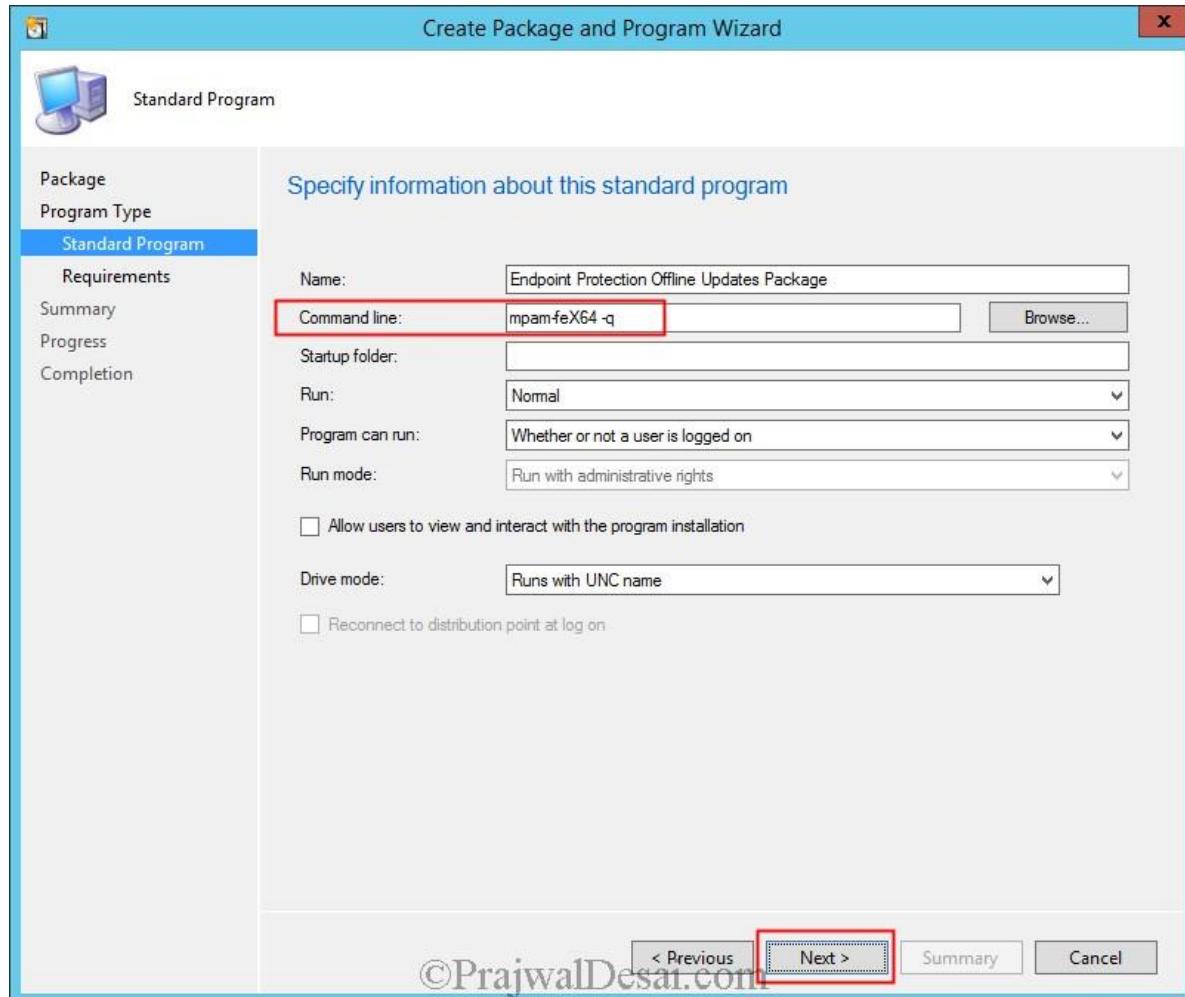
©PrajwalDesai.com

Select the **Program Type** as **Standard Program** and click **Next**.

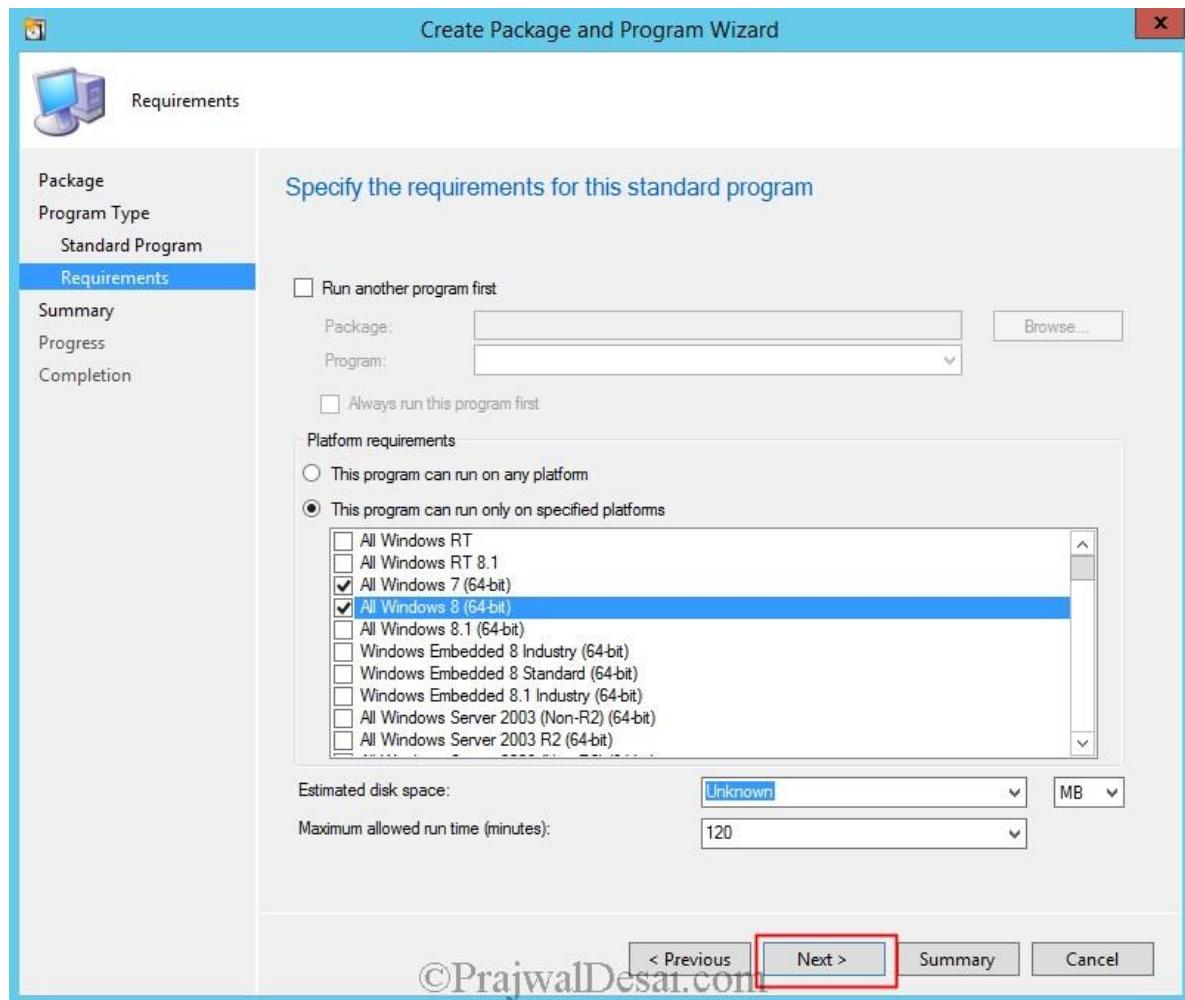


Specify information for the standard program, specify the command line as **mpam-feX64 -q**. Click **Next**

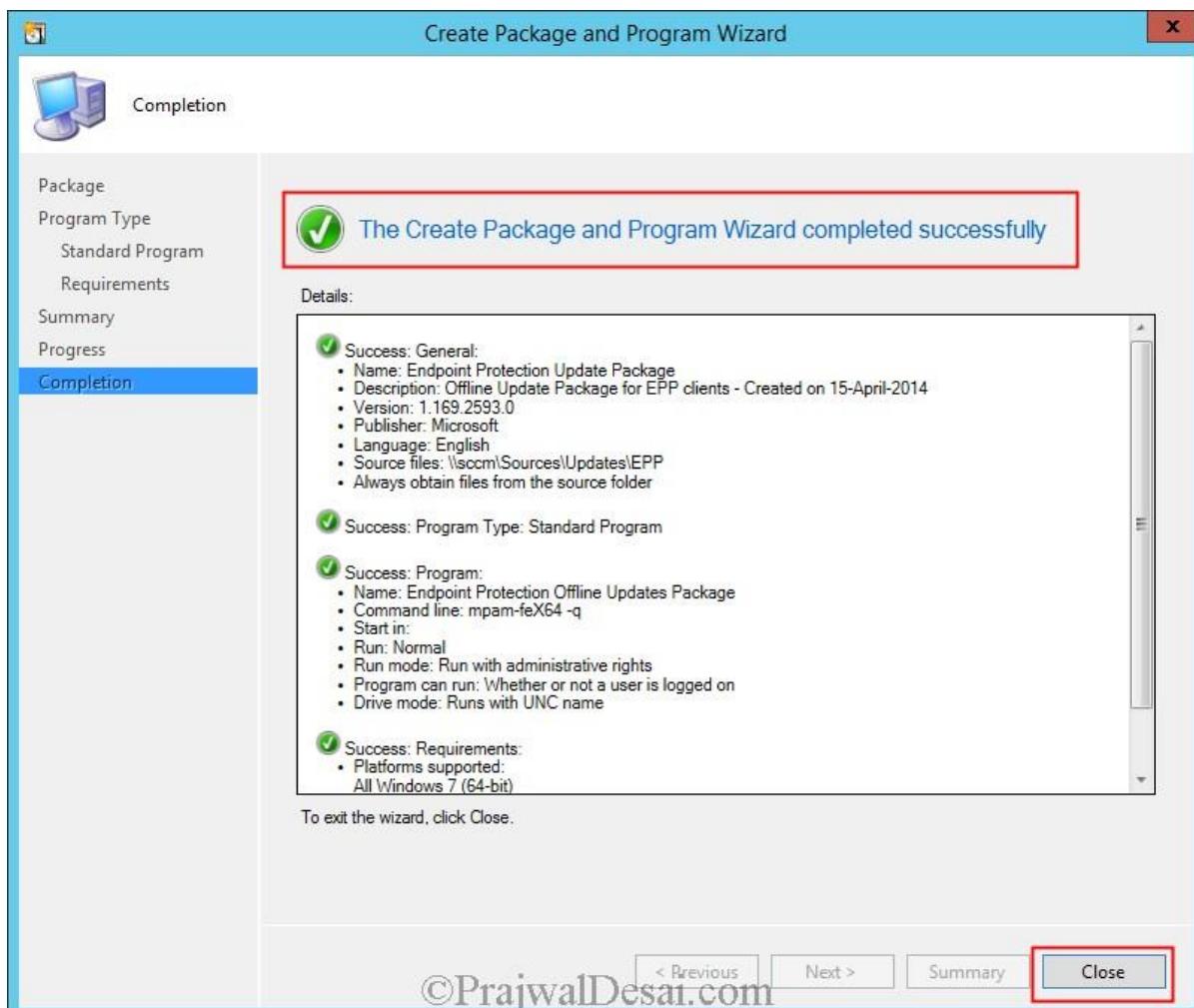
-q switch installs the definition update in quiet mode. Quiet mode suppresses the file extraction dialog box.



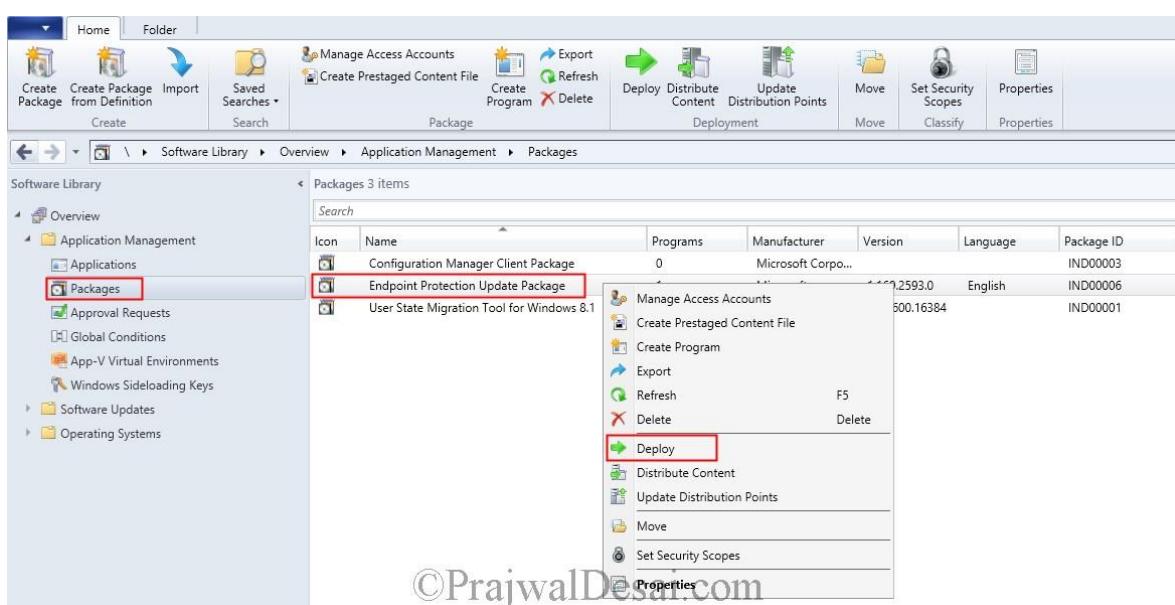
You may choose to specify the requirements for the program or you can leave it unchanged. Click **Next**.



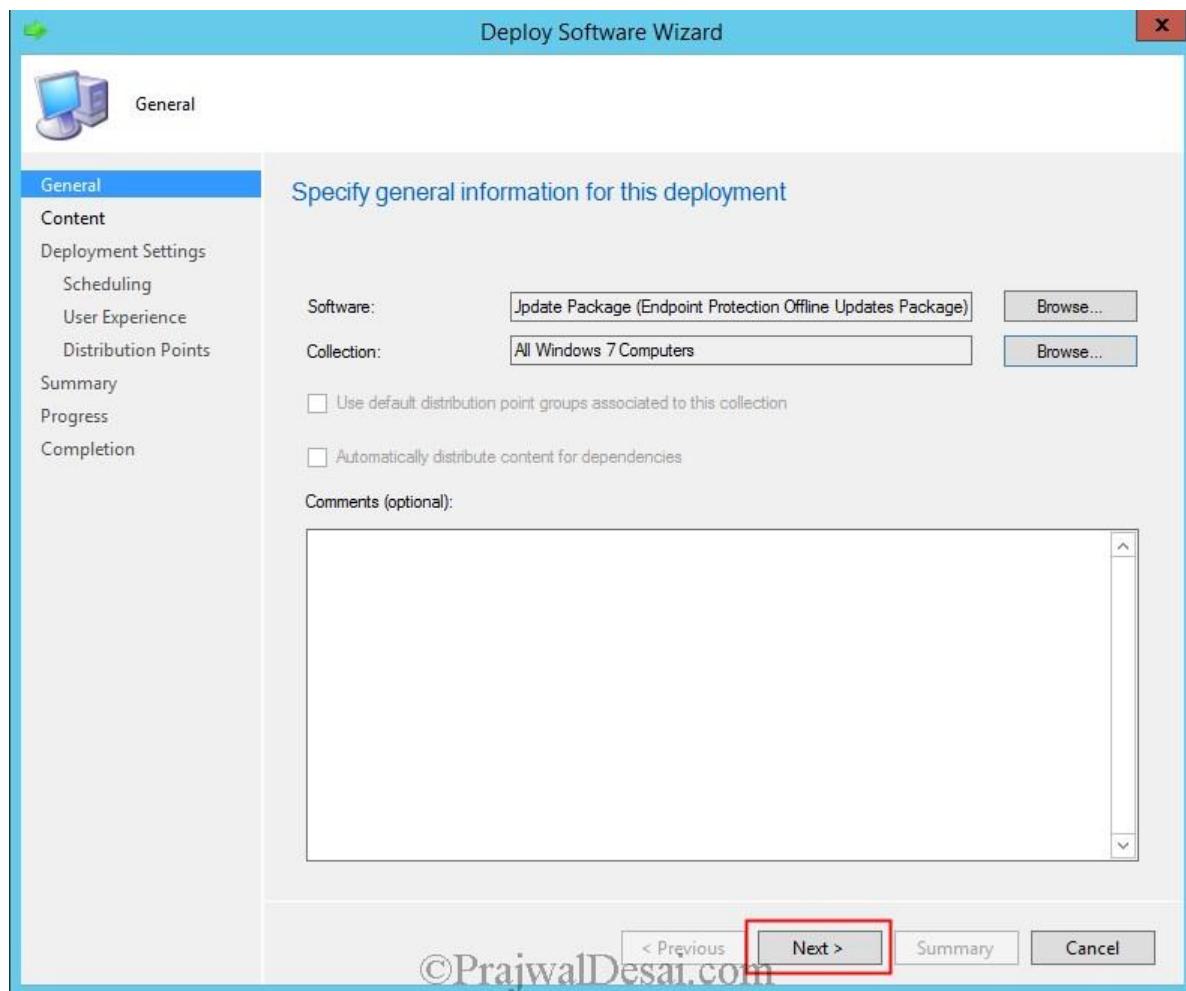
Click **Close**.



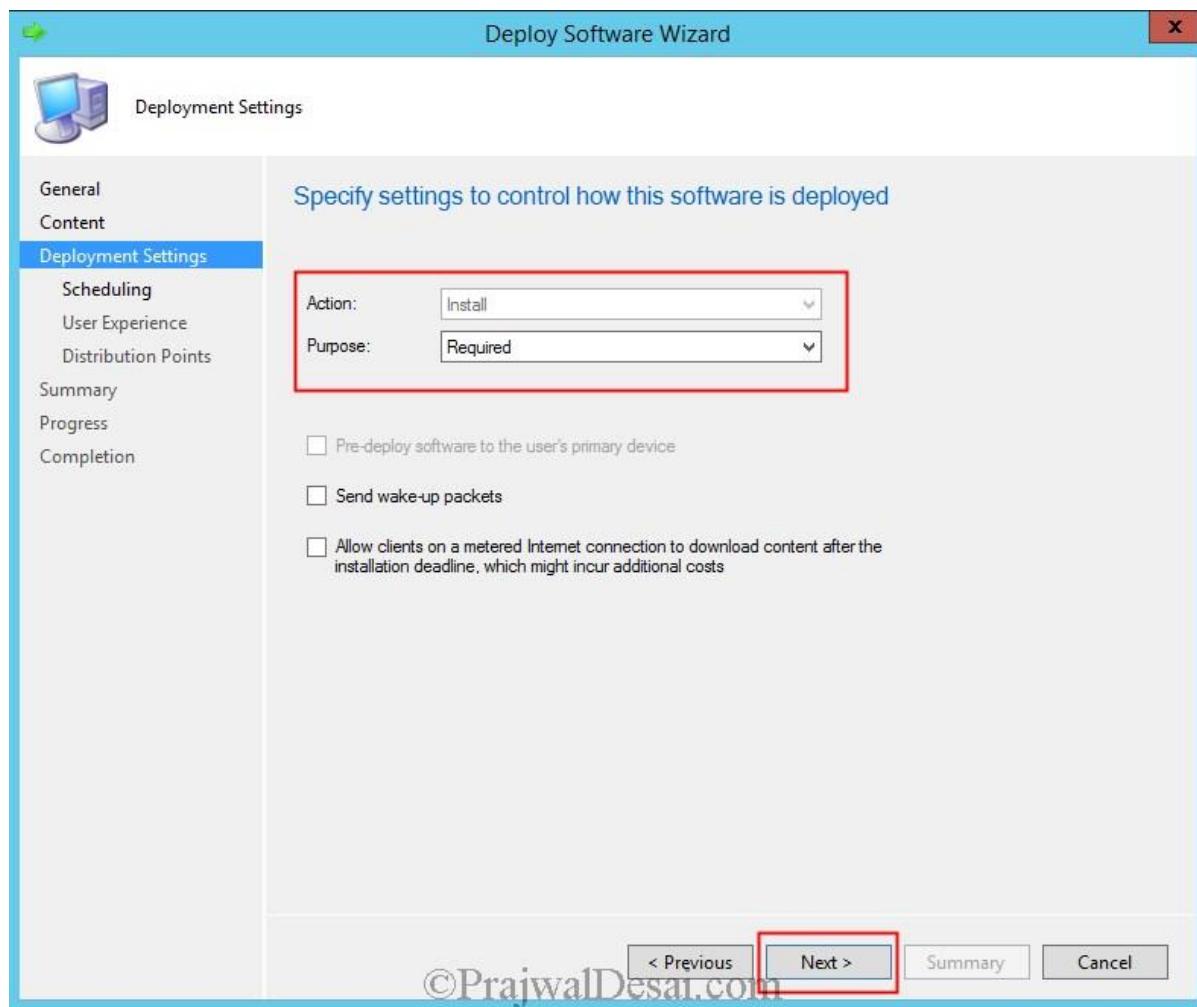
Before you deploy the package distribute the content to the DP. To deploy the package, right click the package and click **Deploy**.



Choose the device collection to which you want to deploy the update package. Click **Next**.

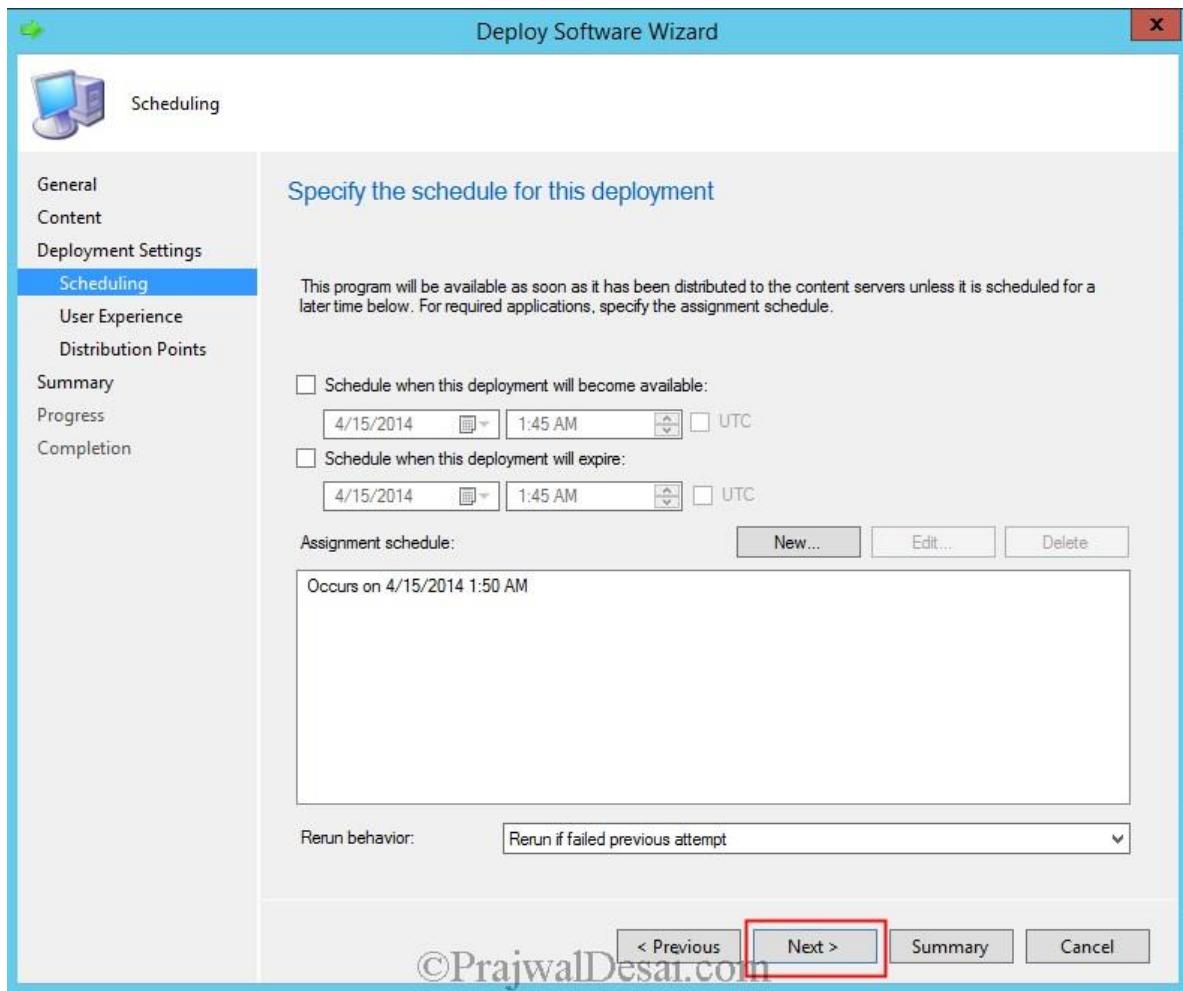


Set the **Purpose** as **Required** and click **Next**.



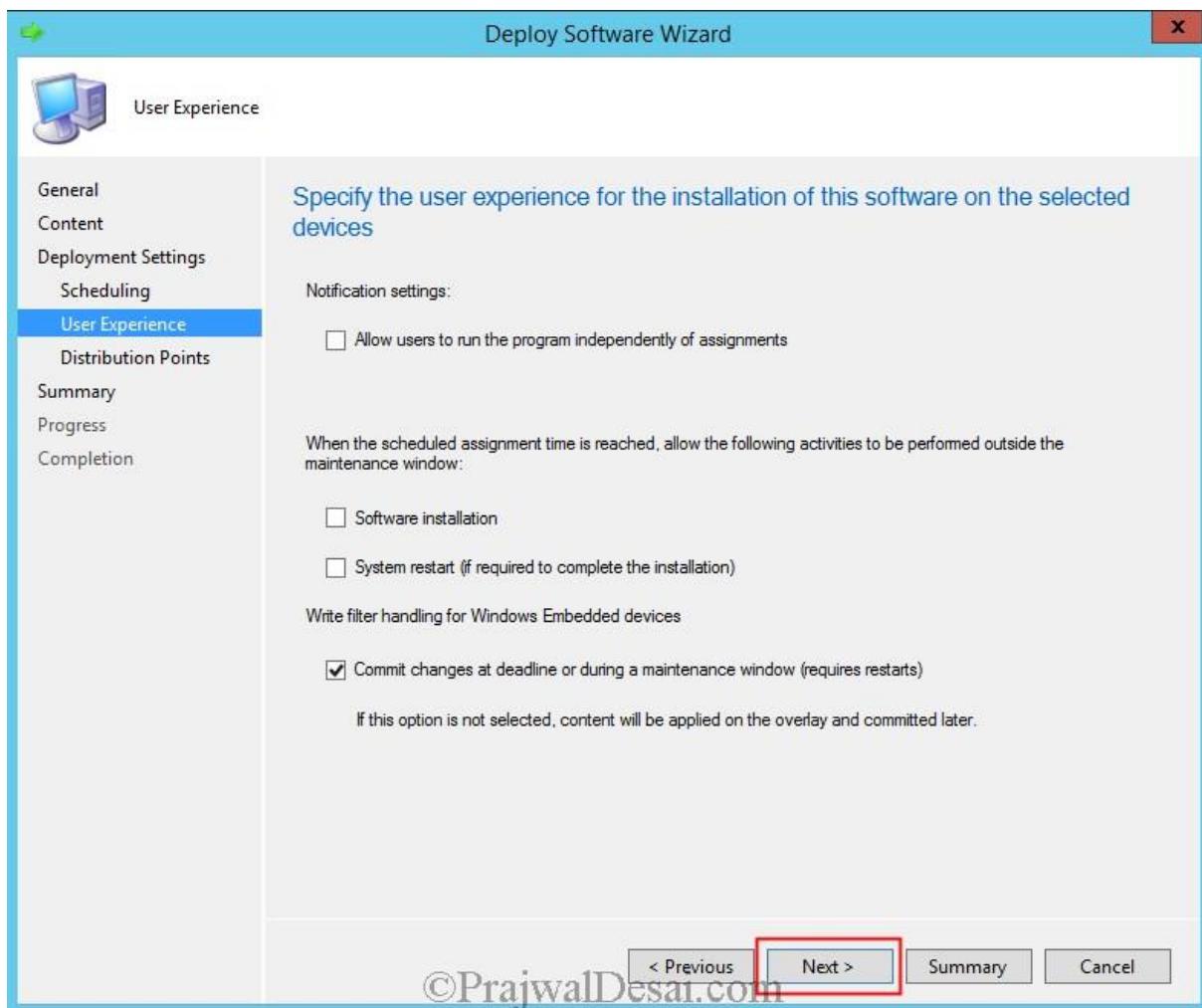
©PrajwallDesai.com

To schedule the deployment of the package click on **New** and schedule it to specific time or you can choose to make it available as soon as possible. Click **Next**.

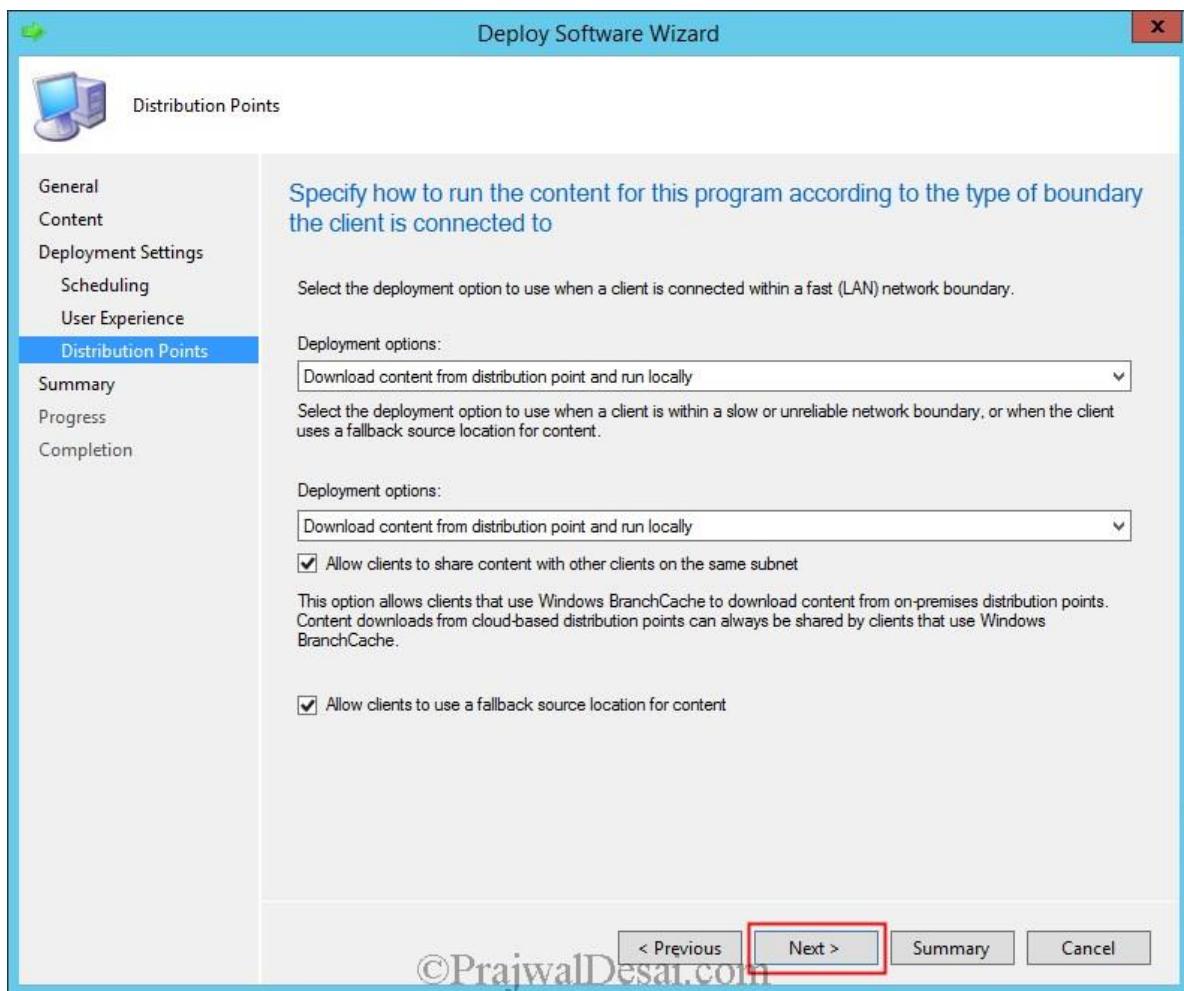


©PrajwallDesai.com

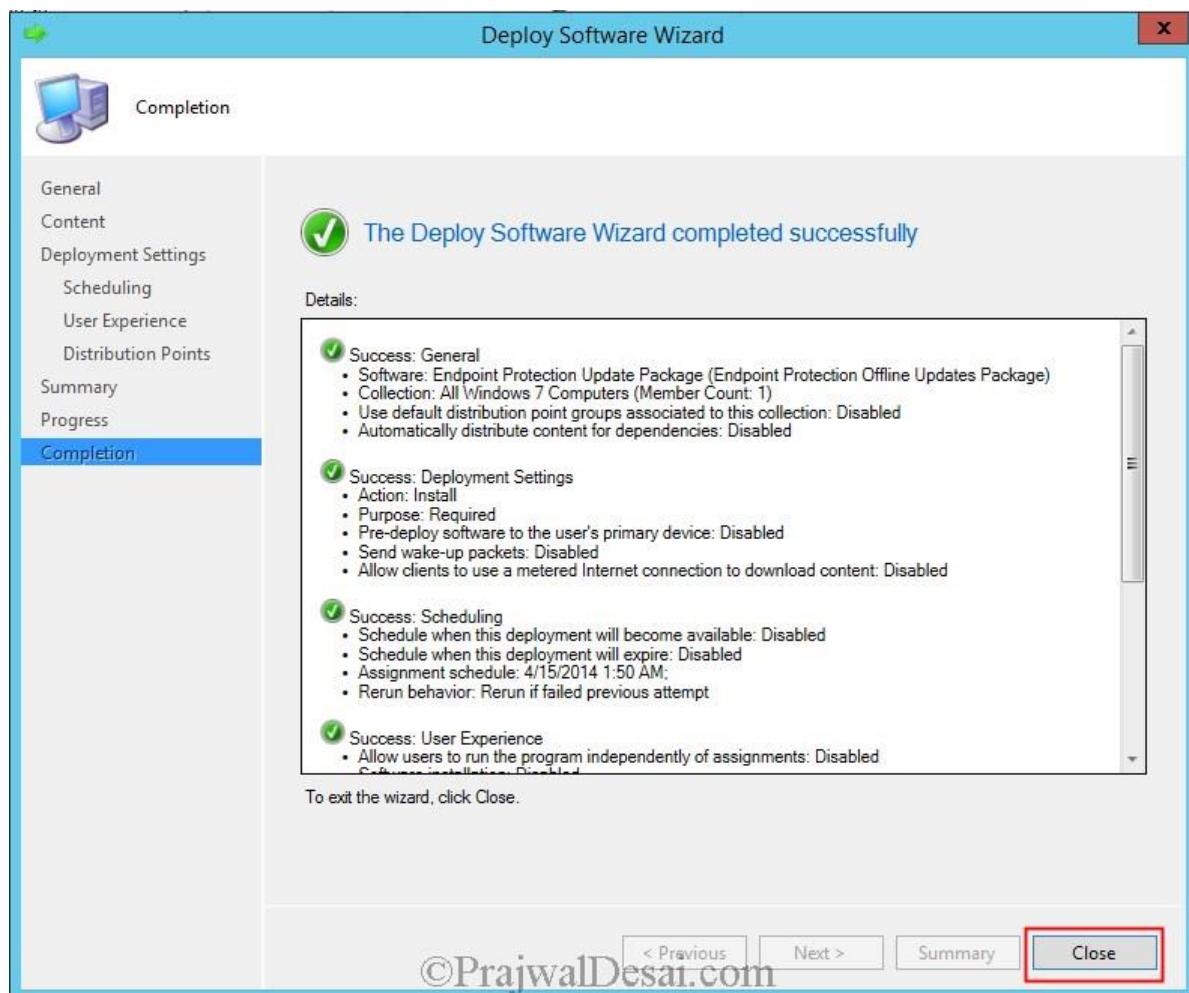
Leave the options unchanged here and click **Next**.



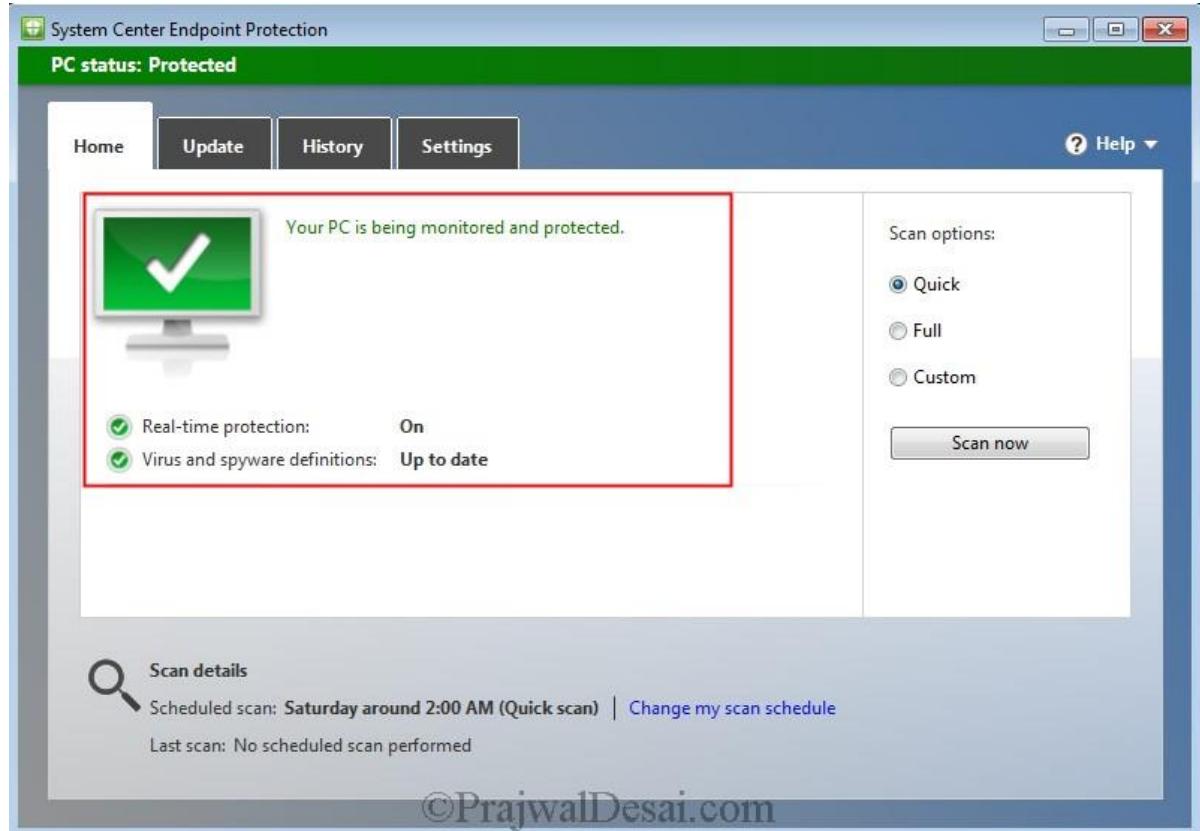
Click Next.



We have deployed the update package to the device collection. Click **Close**.



After sometime we see the update package is downloaded and installed on the client machine. We now see that **PC status** as **Protected** and it is **GREEN** color.



If the updates don't get installed or if you want to know whether the package has been download to client machine or not, look for log file named **execmgr.log** located in client machine under **C:\Windows\CCM\Logs** folder path.

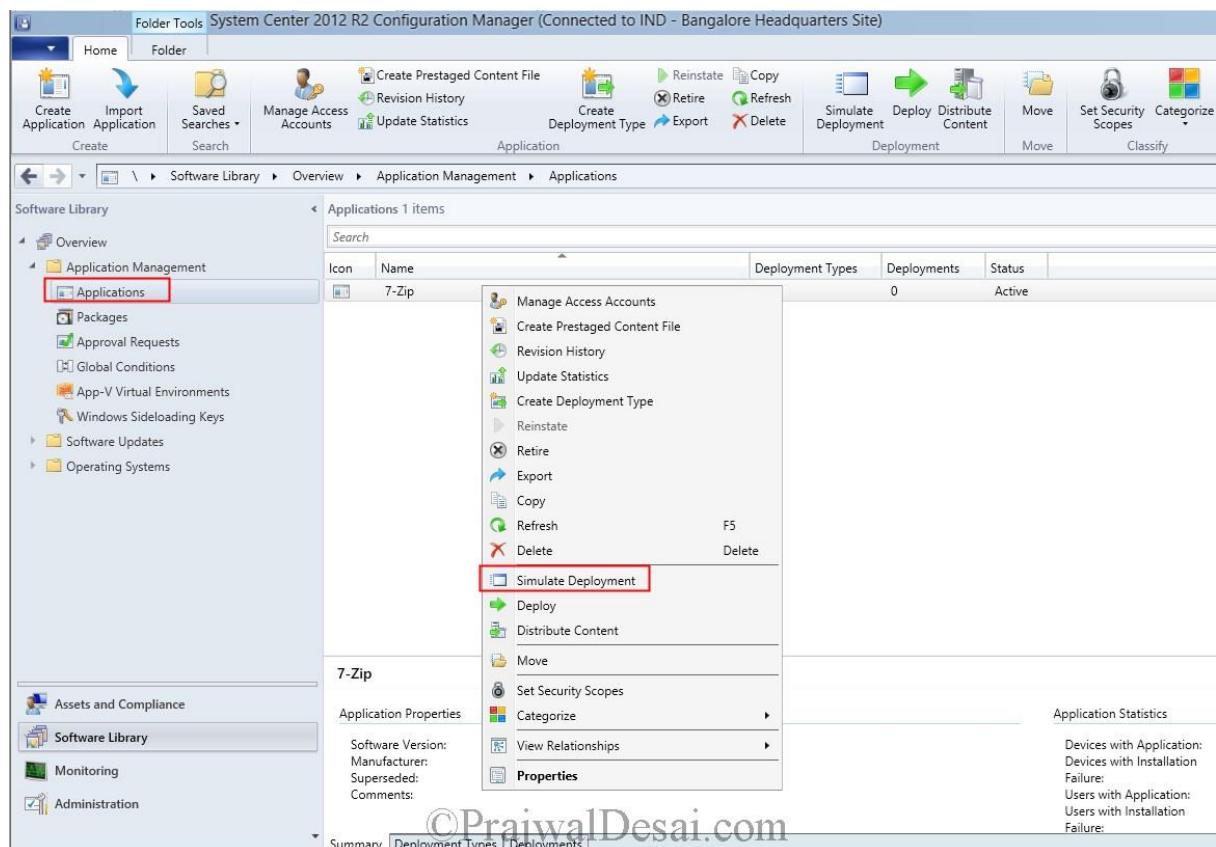
Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\execmgr.log]			
	Component	Date/Time	Thread
Checking content location C:\Windows\ccmcache\1 for use	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Successfully selected content location C:\Windows\ccmcache\1	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Executing program as a script	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Successfully prepared command line "C:\Windows\ccmcache\1\mpam-feX64.exe" -q	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Command line = "C:\Windows\ccmcache\1\mpam-feX64.exe" -q. Working Directory = C:\Windows\ccmcache\1	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Running "C:\Windows\ccmcache\1\mpam-feX64.exe" -q with 32bit.launcher	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Created Process for the passed command line	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent[AdvertisementId = "IND20001";ClientID ...	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Raised Program Started Event for Ad:IND20001, Package:IND00006, Program: Endpoint Protection Offline Updates Package	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00006",ProgramID="Endpoint Protection Offline..."	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00006",ProgramID="Endpoint Protection Offline..."	execmgr	4/15/2014 1:50:00 AM	2088 (0x828)
MTC task with id {B4ACCFE-7819-498F-90B3-68D7CBEB2BCA}, changed state from 4 to 5	execmgr	4/15/2014 1:50:00 AM	2660 (0xA64)
Program exit code 0	execmgr	4/15/2014 1:50:08 AM	1744 (0x6D0)
Looking for MIF file to get program status	execmgr	4/15/2014 1:50:08 AM	1744 (0x6D0)
Script for Package:IND00006, Program: Endpoint Protection Offline Updates Package succeeded with exit code 0	execmgr	4/15/2014 1:50:08 AM	1744 (0x6D0)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessfullyEvent[AdvertisementId = "IN...]	execmgr	4/15/2014 1:50:09 AM	1744 (0x6D0)
Raised Program Success Event for Ad:IND20001, Package:IND00006, Program: Endpoint Protection Offline Updates Package	execmgr	4/15/2014 1:50:09 AM	1744 (0x6D0)
Execution is complete for program Endpoint Protection Offline Updates Package. The exit code is 0, the execution status is Success	execmgr	4/15/2014 1:50:09 AM	1744 (0x6D0)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00006",ProgramID="Endpoint Protection Offline..."	execmgr	4/15/2014 1:50:09 AM	1744 (0x6D0)
Date/Time: 4/15/2014 1:50:00 AM Component: execmgr			
Thread: 2088 (0x828) Source: executioncontext.cpp:459			
Raised Program Started Event for Ad:IND20001, Package:IND00006, Program: Endpoint Protection Offline Updates Package			
Elapsed time is 0h 0m 8s 876ms (8.876 seconds)			

[How to Simulate an Application Deployment in SCCM 2012 R2](#)

In this post we will look at steps on how to simulate an application deployment in SCCM 2012 R2. So what is this **Simulate Deployment** feature in SCCM 2012 R2 ? . Typically you use simulated deployments if you want to test the applicability of an application deployment to computers without installing or uninstalling the application. A simulated deployment evaluates the detection method, requirements and dependencies for a deployment type. Let's assume that you want to deploy an application to a device collection and you want to know if it deploys correctly, in this case you would make use **Simulate Deployment** feature. The simulation will evaluate the dependencies, requirement and detection methods of a deployment and report the results in the **deployments** node of the monitoring workspace.

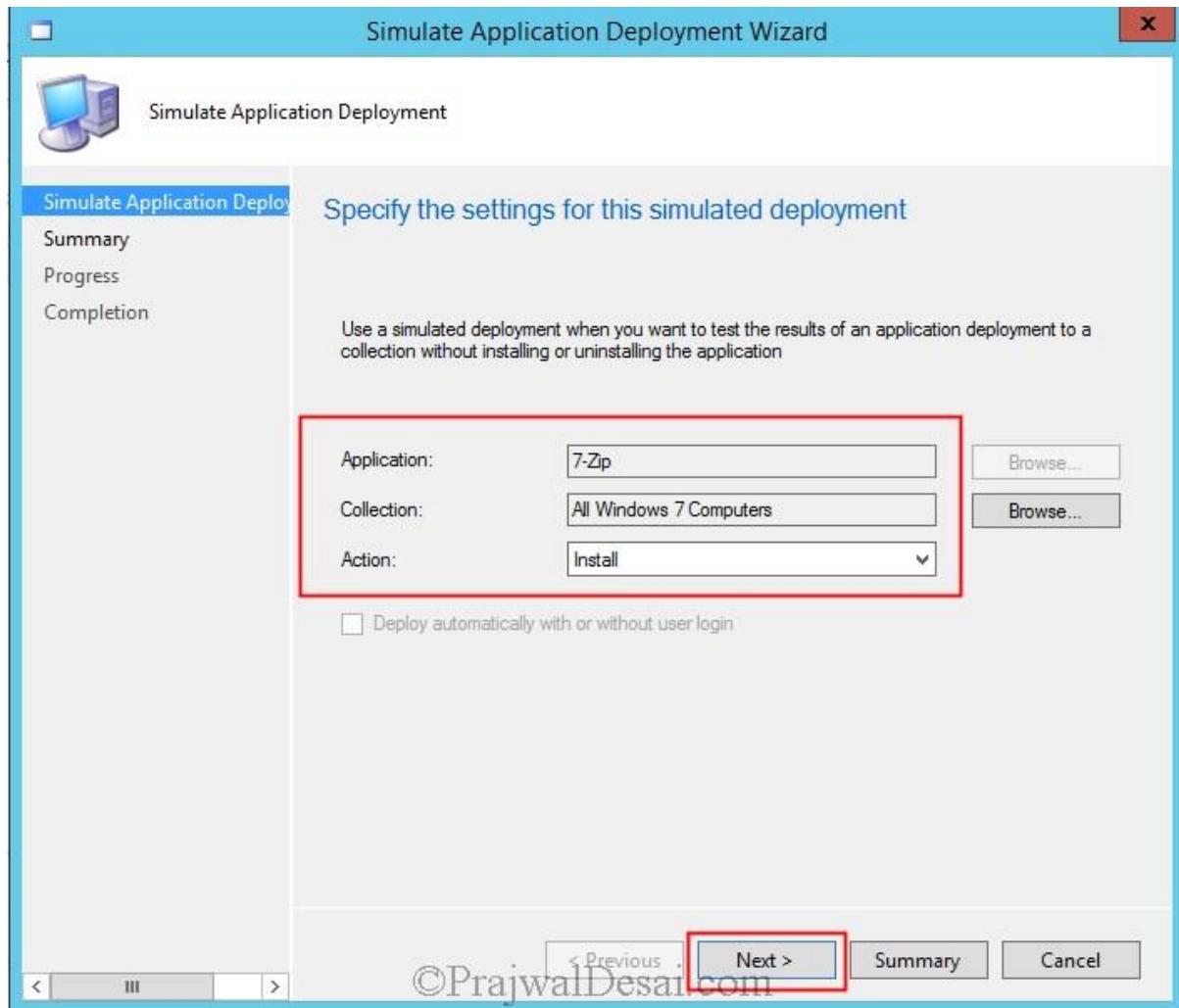
How to Simulate an Application Deployment in SCCM 2012 R2

In this post we will use a simple application named [7-zip](#) x64 bit, and we will use the simulate deployment feature and see how it works. You can choose your own application for trying out simulated deployment. In the **Configuration Manager** console, click **Software Library**, under **Application Management** click **Applications**. On the right hand side you will find the list of applications (The application has been already created, to create application from scratch you can check [Deploying Applications Using SCCM 2012](#)). Right click the application and click **Simulate Deployment**.

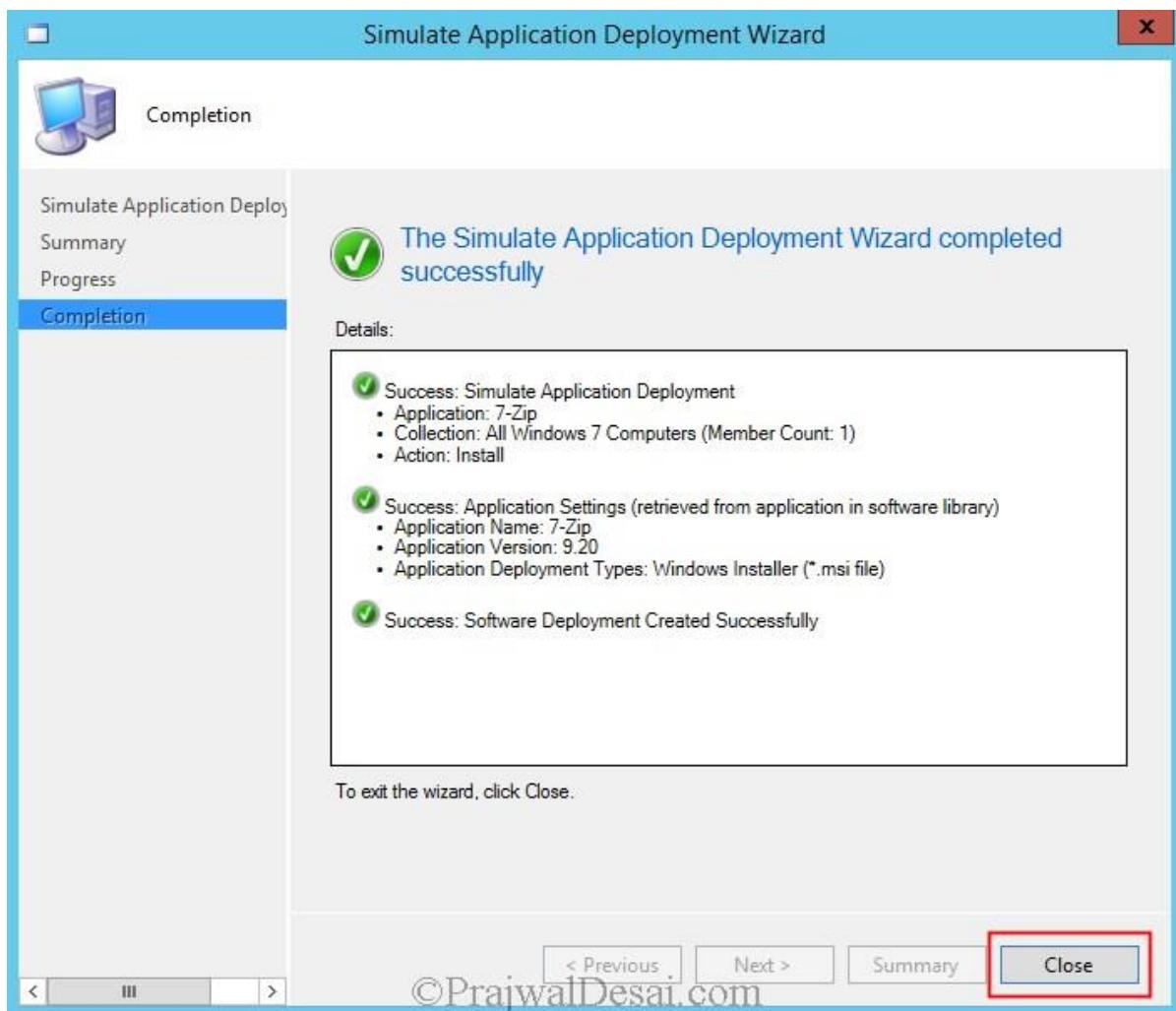


In the **Simulate Application Deployment Wizard**, choose the collection and choose the Action as **Install**.

Note – You cannot deploy an application with a deployment purpose of **Uninstall** if a simulated deployment of the same application is active.



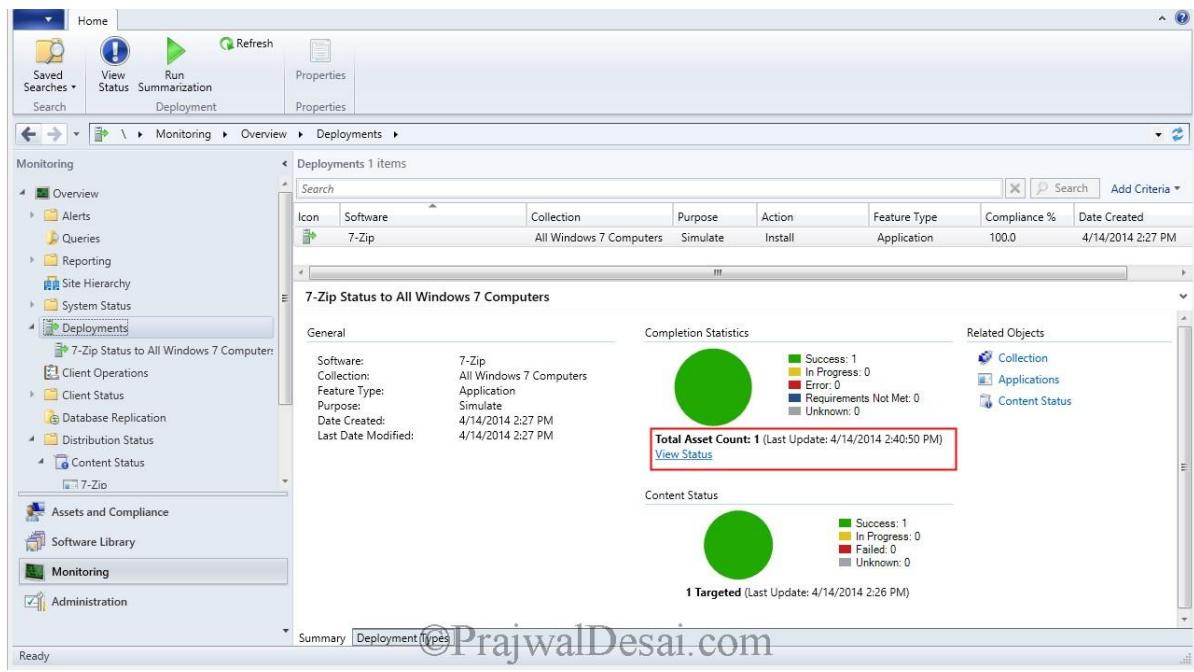
Click **Next** and close the wizard.



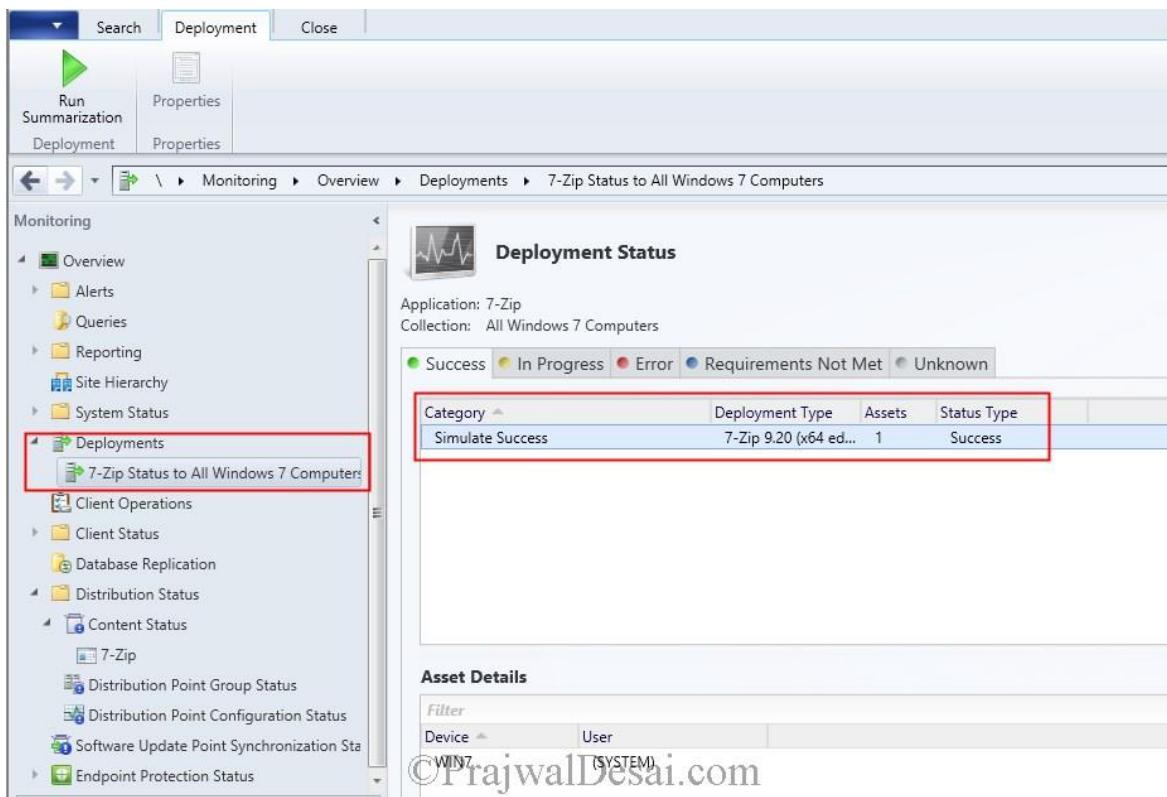
Let's see some of the things related to **Simulated Deployment** of an application.

1. Simulated applications appear in the **Deployments** node of the **Monitoring** workspace with a purpose of **Simulate**.
2. As said earlier, you cannot deploy an application with a deployment purpose of **Uninstall** if a simulated deployment of the same application is active.
3. You cannot use simulated deployments for collections of mobile devices.

Click **Monitoring**, under **Deployments** choose the **application**. We see that the **Purpose** is **Simulate** and if you look at the **Completion Statistics** we see its successful. What happened in the background was the Configuration Manager 2012 R2 clients have processed the application and evaluated the dependencies, requirement and detection methods and have reported back the information to Configuration Manager 2012 Primary Site.



When you right click on the application and click **View Status**, you will see that the simulated deployment of application is successful.



In this post we have used 7zip 64 bit software for deploying to the **Windows 7 computers** device collection. Now I have another collection named **All Windows XP computers** which consists of Windows XP 32 bit OS, since the 7zip 64 bit version is not compatible or cannot be installed on 32 bit Windows XP OS, I have performed Simulate Deployment of 7zip 64 bit application to Windows XP device collection just to see what would happen.

If you look at the Completion Statistics of the 7zip x64 application which was deployed to Windows 7 device collection, we see that it was successful.

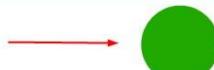
Deployments 0 items							
Search							
Icon	Software	Collection	Purpose	Action	Feature Type	Compliance %	Date Created
7-Zip	All Windows XP Computers	Simulate	Install	Application	0.0	4/14/2014 3:47 PM	
7-Zip	All Windows 7 Computers	Simulate	Install	Application	100.0	4/14/2014 2:27 PM	←

7-Zip Status to All Windows 7 Computers

General

Software: 7-Zip
 Collection: All Windows 7 Computers
 Feature Type: Application
 Purpose: Simulate
 Date Created: 4/14/2014 2:27 PM
 Last Date Modified: 4/14/2014 2:27 PM

Completion Statistics



Total Asset Count: 1 (Last Update: 4/14/2014 4:05:32 PM) [View Status](#)

- Success: 1
- In Progress: 0
- Error: 0
- Requirements Not Met: 0
- Unknown: 0

Content Status



1 Targeted (Last Update: 4/14/2014 2:26 PM)

- Success: 1
- In Progress: 0
- Failed: 0
- Unknown: 0

©PrajwalDesai.com

If you look at the **Completion Statistics** of the 7zip x64 application which was deployed to Windows XP device collection, we see it is **Unknown**.

Deployments 0 items							
Search							
Icon	Software	Collection	Purpose	Action	Feature Type	Compliance %	Date Created
7-Zip	All Windows XP Computers	Simulate	Install	Application	0.0	4/14/2014 3:47 PM	←
7-Zip	All Windows 7 Computers	Simulate	Install	Application	100.0	4/14/2014 2:27 PM	

7-Zip Status to All Windows XP Computers

General

Software: 7-Zip
 Collection: All Windows XP Computers
 Feature Type: Application
 Purpose: Simulate
 Date Created: 4/14/2014 3:47 PM
 Last Date Modified: 4/14/2014 3:47 PM

Completion Statistics



Total Asset Count: 1 (Last Update: 4/14/2014 4:03:36 PM) [View Status](#)

- Success: 0
- In Progress: 0
- Error: 0
- Requirements Not Met: 0
- Unknown: 1

Content Status



1 Targeted (Last Update: 4/14/2014 2:26 PM)

- Success: 1
- In Progress: 0
- Failed: 0
- Unknown: 0

©PrajwalDesai.com

To look for more information, on the device which is a part of Windows 7 device collection, under **Push Information** check the **Last Status** and it shows **Complete**.

The screenshot shows the 'Assets and Compliance' interface. In the left navigation pane, under 'Devices', there is a red box around the link 'Success status devices from deploying "7-'. The main content area displays a table with one item: WIN7, Computer, Client Type: Yes, Site Code: IND, Client Activity: Active. Below this is a section titled 'WIN7' with 'General Information' showing Name: WIN7 and Client Type: Computer. On the right, 'Client Check Information' shows Client Check Result: No Results. At the bottom right, a red box highlights the 'Push Information' section which shows Last Installation Error: 0, Last Request Attempt: 4/14/2014 1:53 PM, and Last Status: Complete.

On the device which is a part of Windows XP device collection, under **Push Information** check the **Last Status** and it shows **Retry**.

The screenshot shows the 'Assets and Compliance' interface. In the left navigation pane, under 'Devices', there are two red boxes around the links 'Success status devices from deploying "7-' and 'Success status devices from deploying "7-'. The main content area displays a table with one item: TEST, Computer, Client Type: Yes, Site Code: IND, Client Activity: Active. Below this is a section titled 'TEST' with 'General Information' showing Name: TEST and Client Type: Computer. On the right, 'Client Check Information' shows Client Check Result: No Results. At the bottom right, a red box highlights the 'Push Information' section which shows Last Installation Error: 67, Last Request Attempt: 4/14/2014 3:25 PM, and Last Status: Retry.

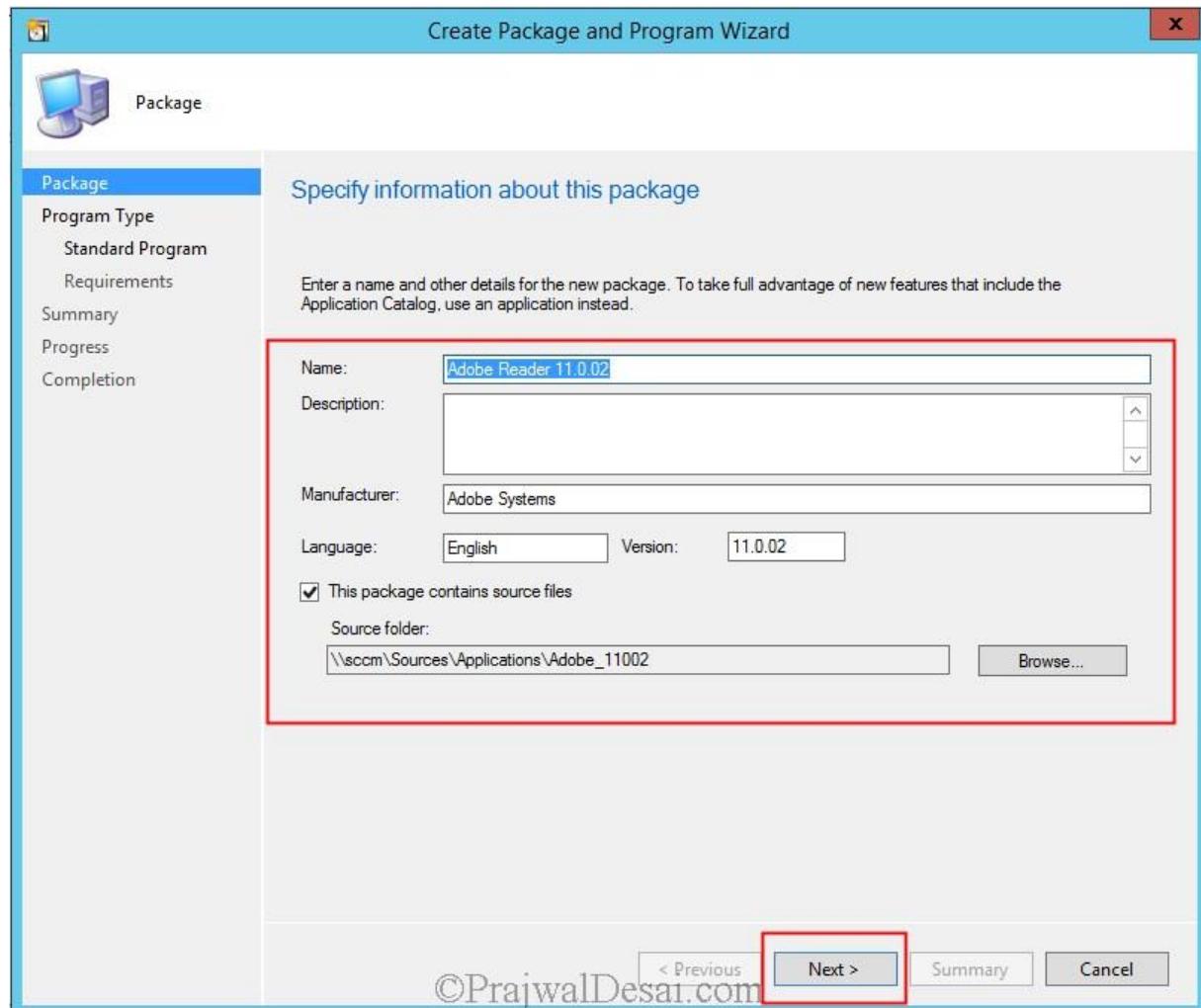
Once you complete the above steps you should delete the Simulation Deployment and create a real deployment to a collection with users or devices.

[Deploying Adobe Reader Updates Using SCCM 2012 R2](#)

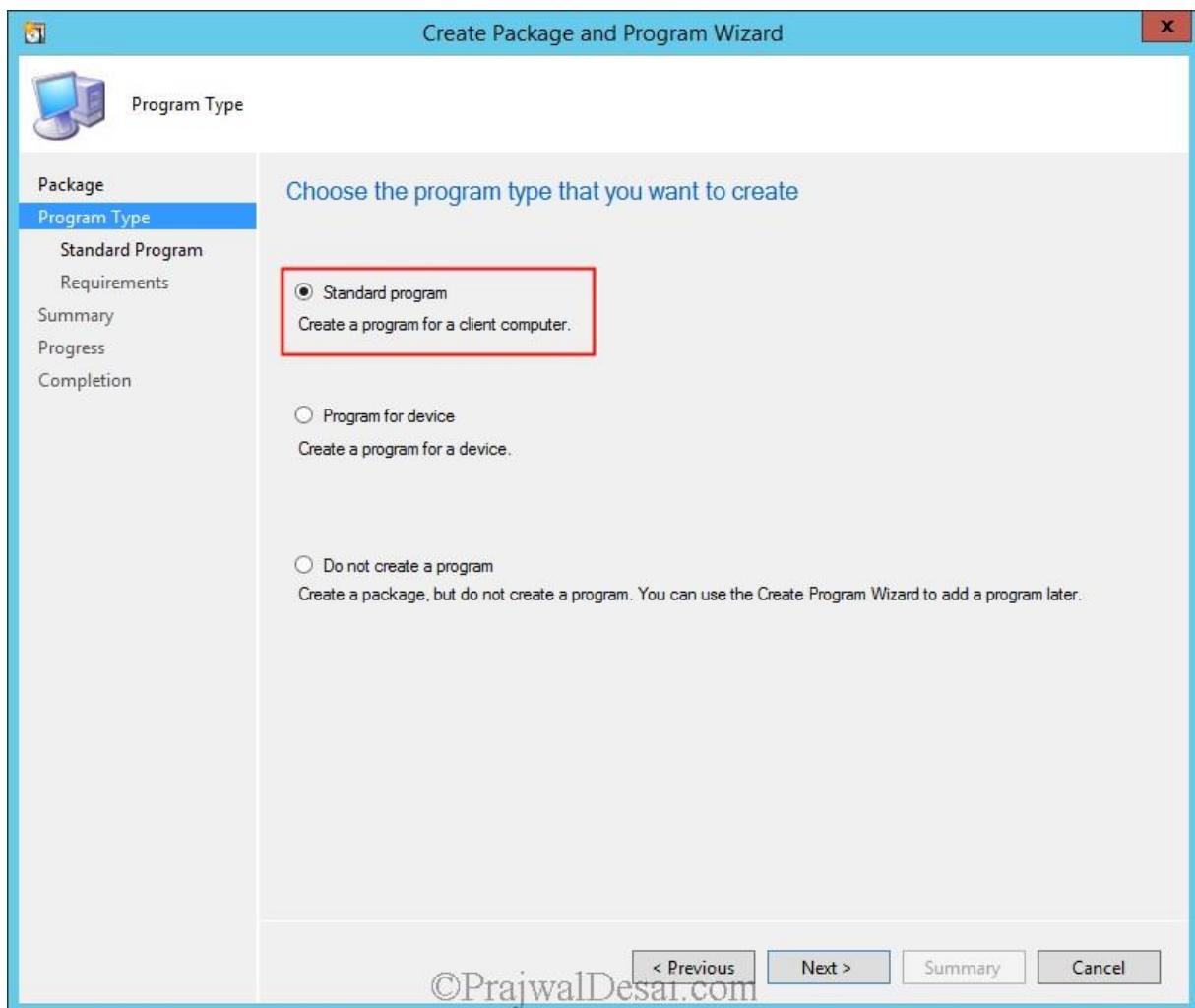
In this post we will look at the steps for deploying adobe reader updates using SCCM 2012 R2. Adobe reader updates are available as .msp files and we will learn how to deploy the same using SCCM 2012 R2. One of the recommended ways to deploy third-party software updates is by using [System Center Updates Publisher \(SCUP\)](#). System Center Updates Publisher (SCUP) is a stand-alone tool that is used in conjunction with Microsoft's System Center Configuration Manager to allow administrators to more accurately and efficiently install and update software. However in this post we will do it in simpler way i.e. by creating an update package and deploying it to the collections which already have the software installed.

Deploying Adobe Reader Updates Using SCCM 2012 R2

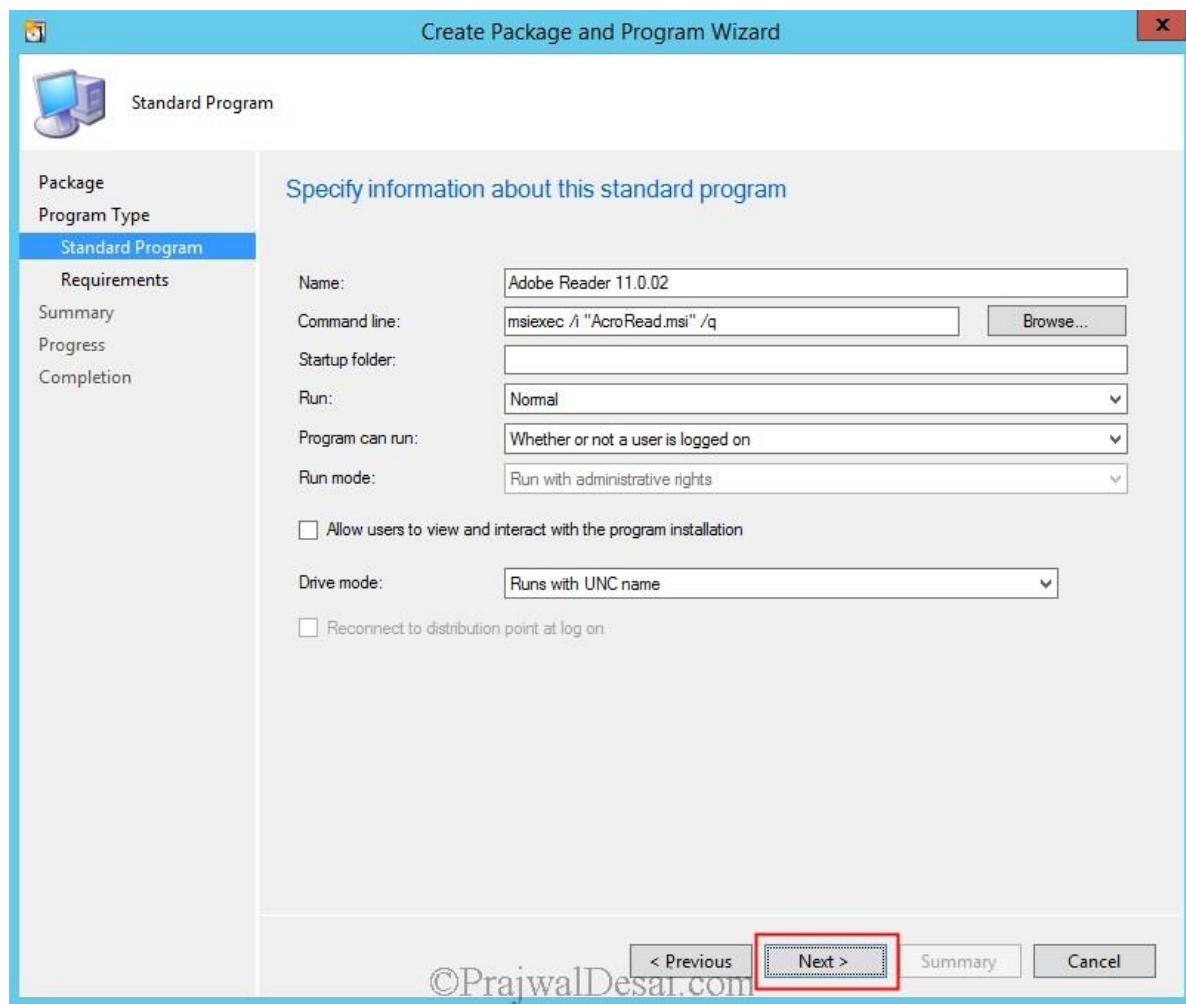
First we will create a package for Adobe Reader 11.0.02 and deploy it to a collection. If you know how to create a package and deploy you can skip the below step. In the SCCM console, click on **Software Library**, click **Application Management**. Right click on **Packages** and click **Create Package**. Provide the **Name**, **Source Folder** for the package and click **Next**.



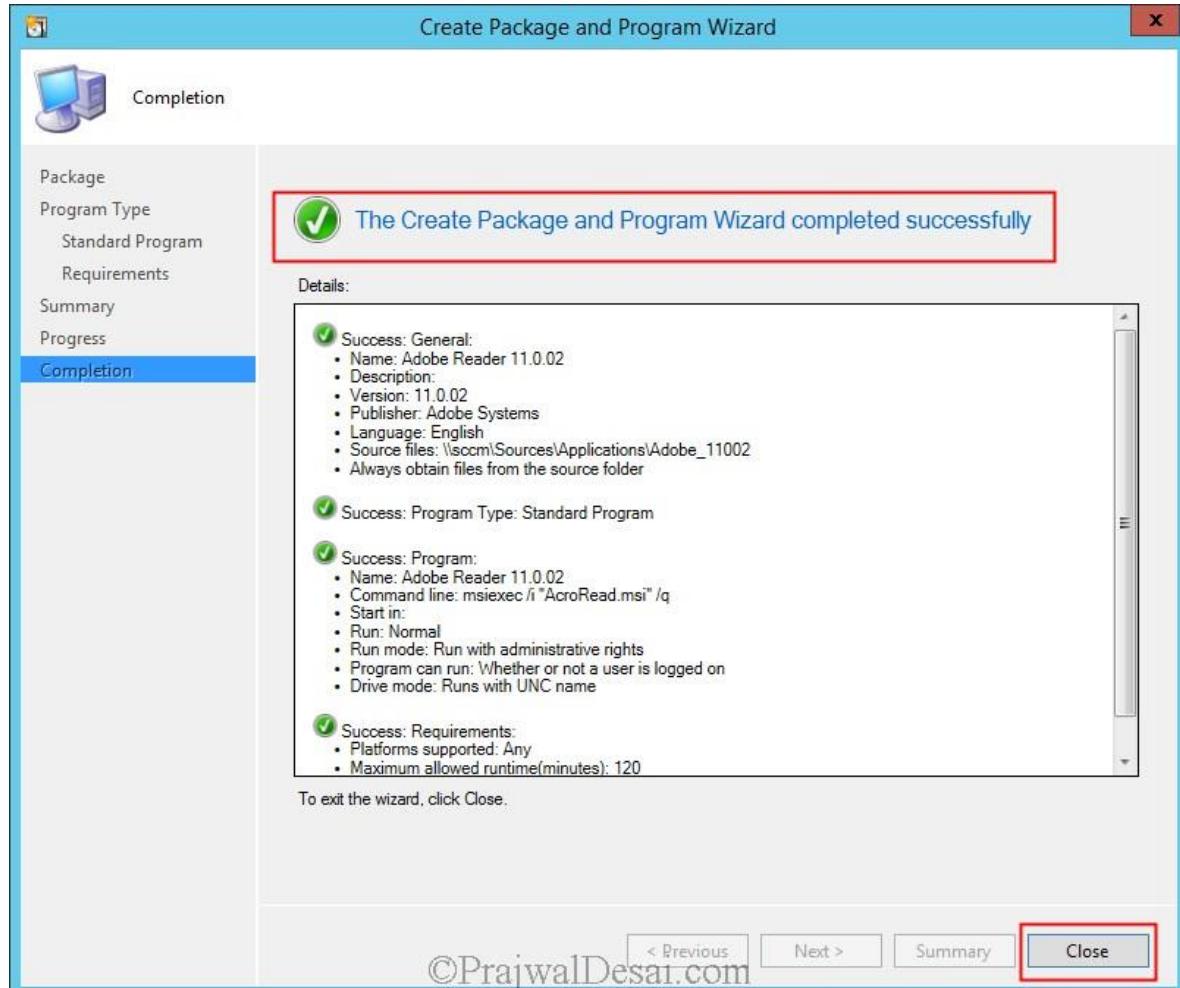
Choose the **Program Type** as **Standard program**. Click **Next**.



Specify the information about the program as shown in the below screenshot. Click **Next**.



Complete the **Create Package and Program Wizard** and click **Close**. The next step is to distribute the Adobe Reader Program to the distribution point and deploy it to the collection. To distribute the program, right click on the program and click **Distribute Content**, follow the wizard and wait till the content status color shows green. After that right click the program and deploy it to the collection.

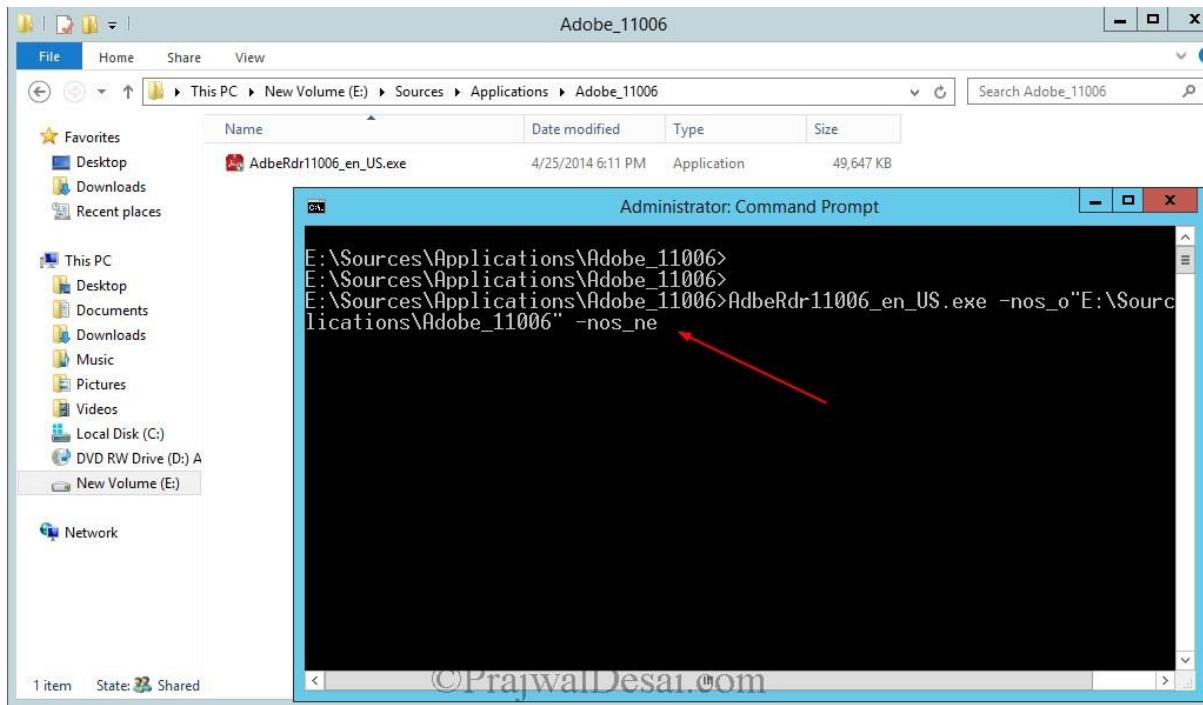


After you have deployed the Adobe Reader software to the collections, the next step is deploying adobe reader updates using SCCM 2012 R2. In the above example we had deployed Adobe Reader 11.0.02 to client systems, now what if there is a new version of Adobe Reader?.

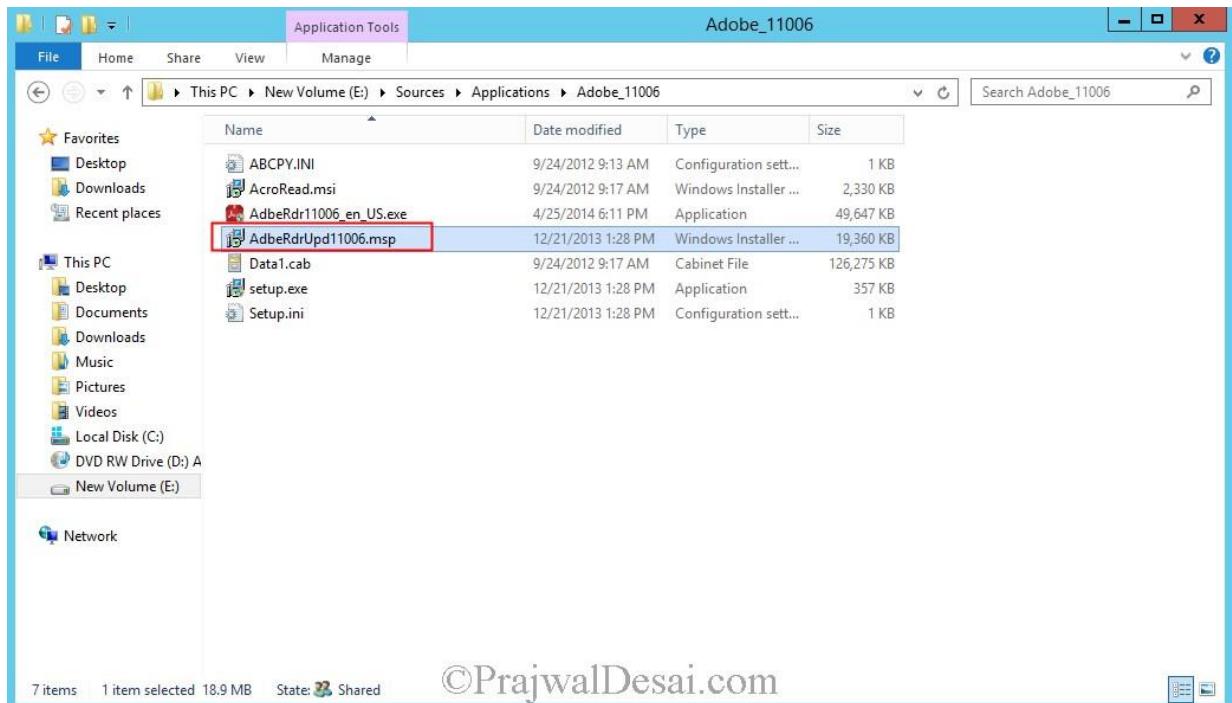
We have the latest version of **Adobe reader 11.0.06** which can be downloaded from [here](#). But since you have already deployed Adobe Reader 11.0.02 to the client systems it makes no sense to deploy 11.0.06 over it again. So we will now deploy only the update patch which will update Adobe Reader 11.0.02 to 11.0.06.

Download the latest version of Adobe Reader from [here](#) and extract the executable using the command line **AdbeRdr11006_en_US.exe -nos_o"E:\\Sources\\Applications\\Adobe_11" -nos_ne** (where **AdbeRdr11006_en_US.exe** is the executable name, **E:\\Sources\\Applications\\Adobe_11** is the path where the executable is stored).

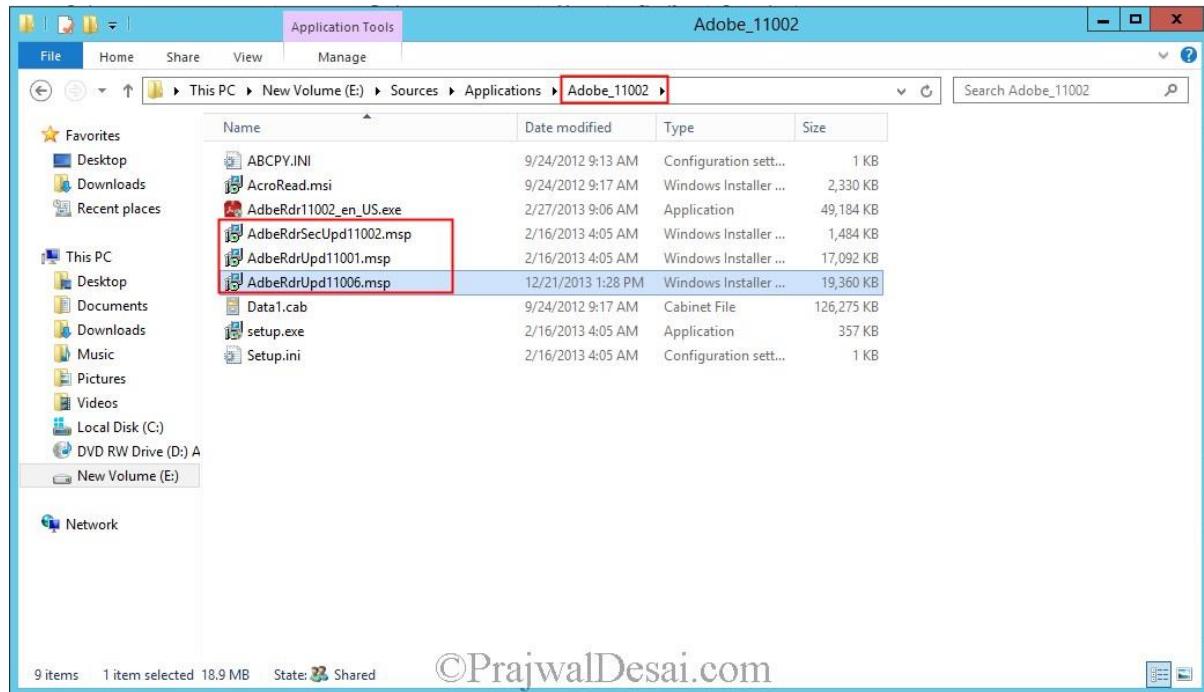
Note – If you extract the Adobe Reader executable using winrar or any third party software you will not see .msp files. You have to extract it using a command line.



After we extract the setup file we see that it contains the update .msp file named **AdbeRdrUpd11006.msp**. This is the update file that we will be deploying using SCCM and this will update the existing adobe reader 11.0.02 version to 11.0.06 version.

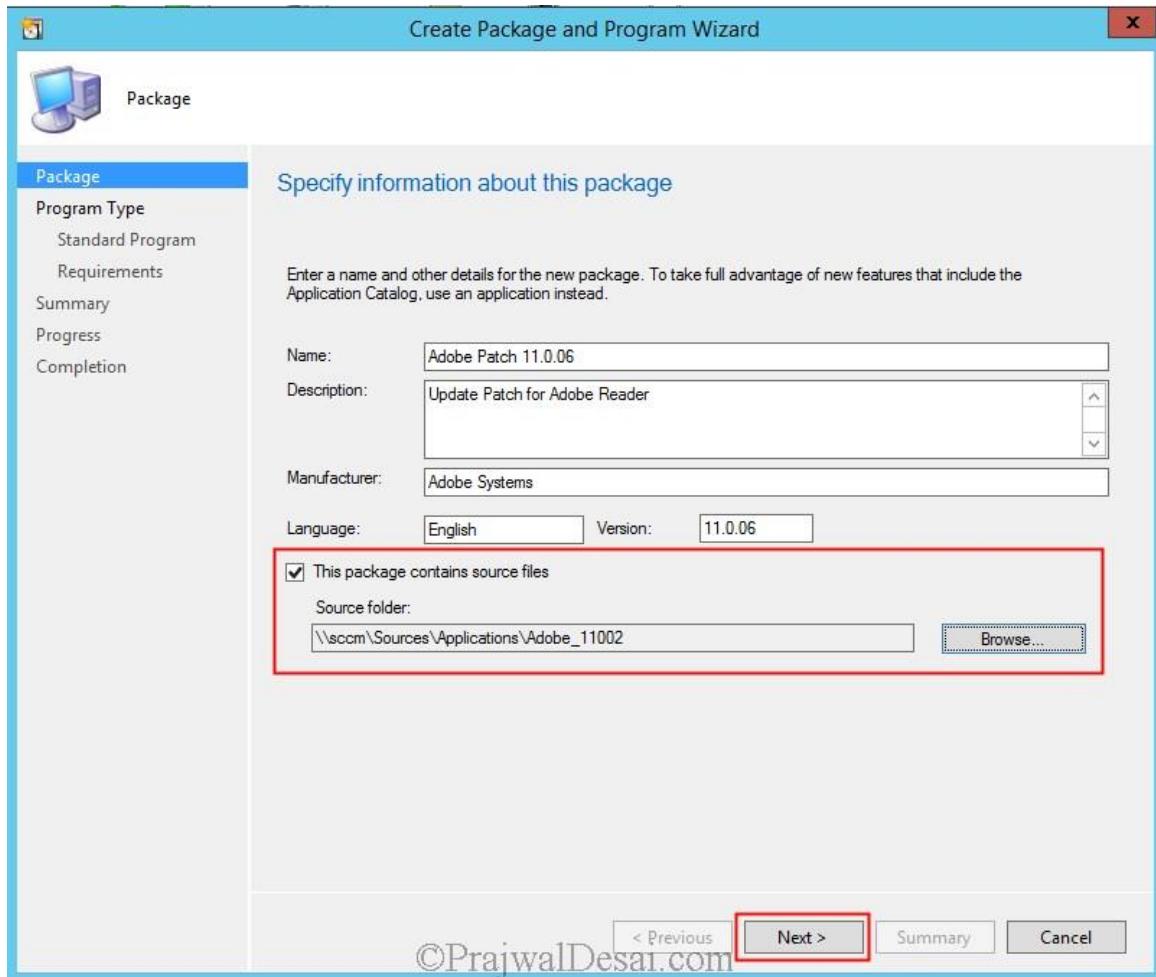


Copy the **AdbeRdrUpd110006.msp** to the folder where Adobe 11.0.02 files exists.

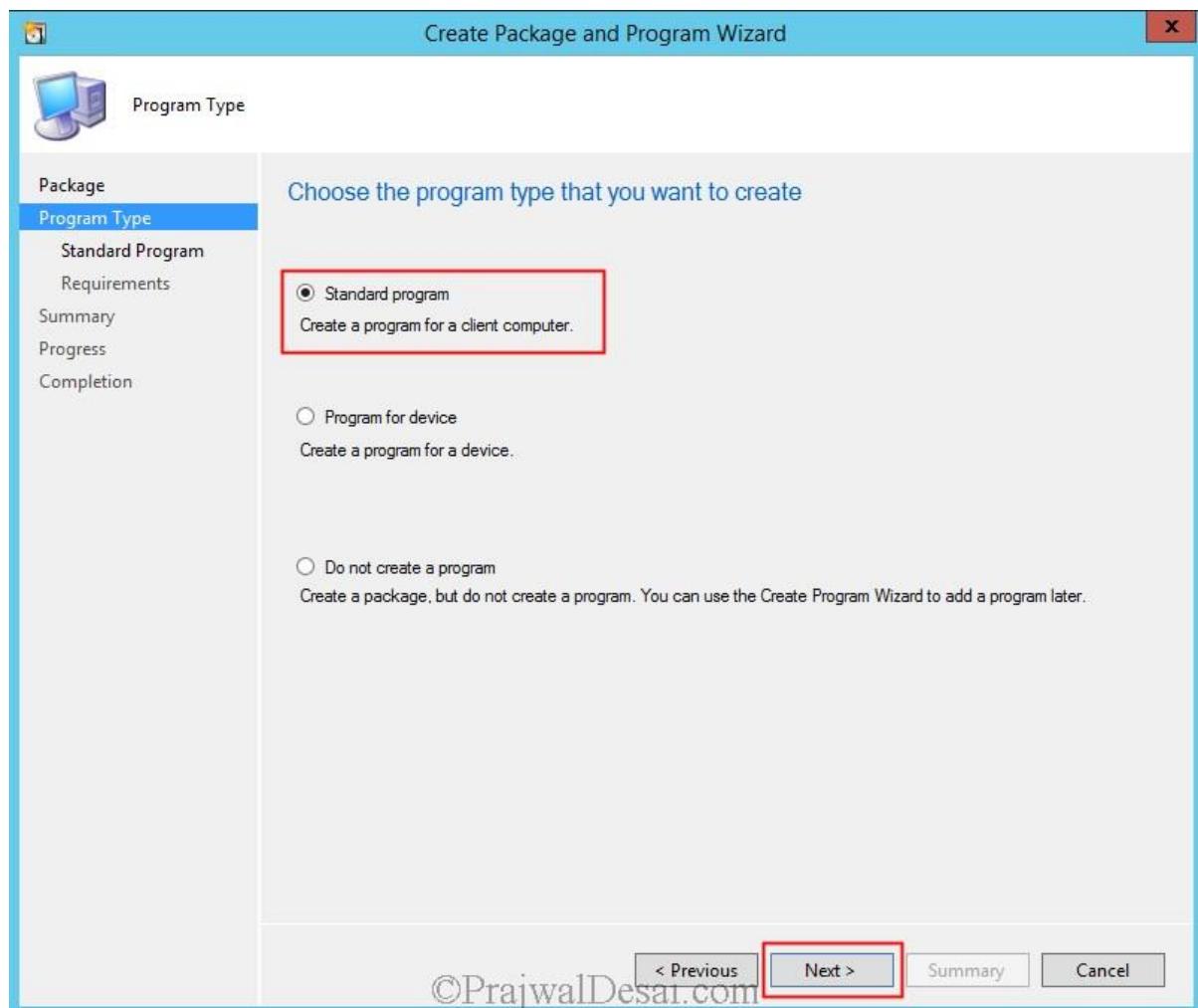


©PrajwalDesai.com

Right click on **Packages** and click **Create Package**. Provide the **Name, Source Folder** for the package and click **Next**.

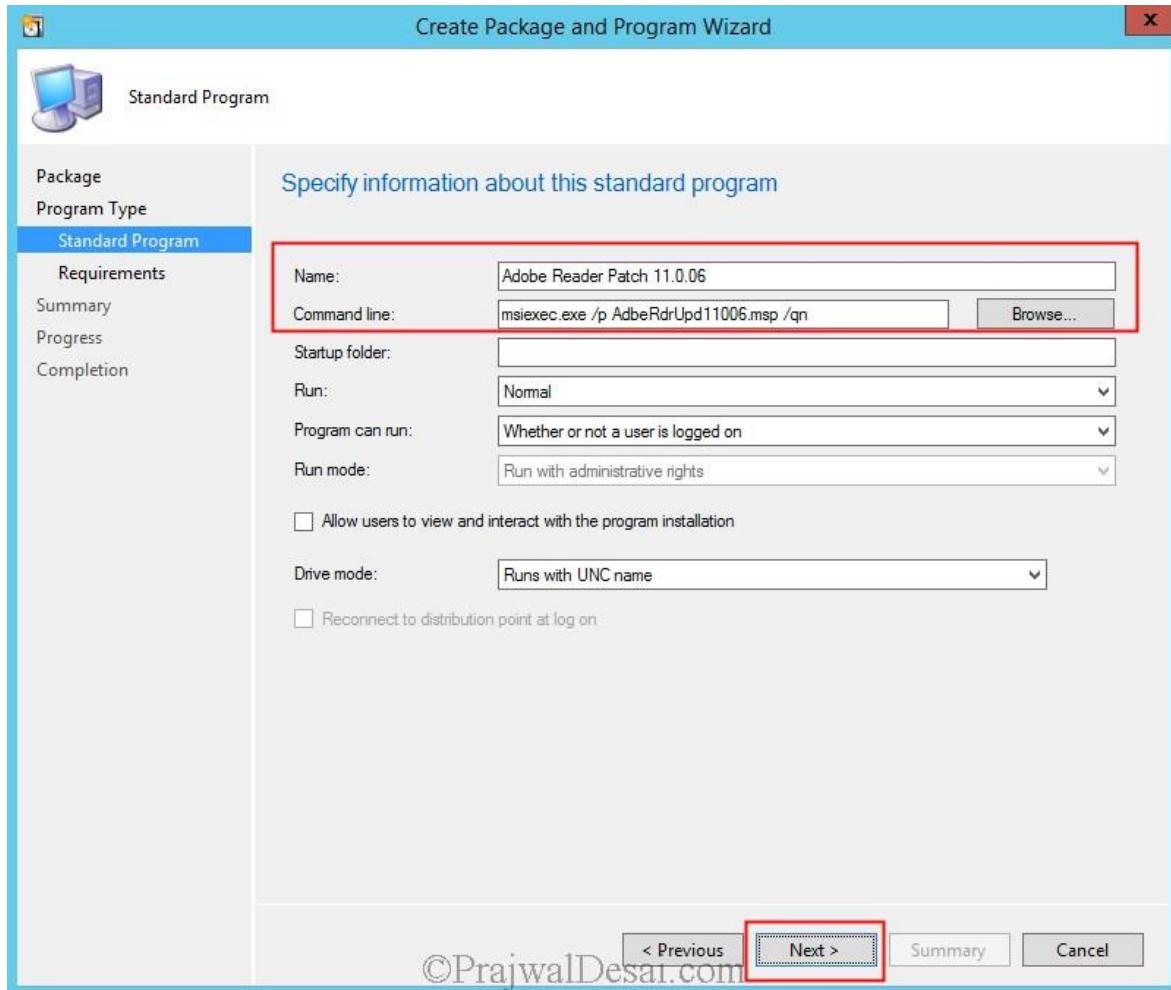


Choose the **Program Type** as **Standard program**. Click **Next**.



Syntax – “**msiexec /update msipatchname.msp /qn (OR) msiexec /p msipatchname.msp /qn**

Specify the name for the program, enter the command line **msiexec /p AdbeRdrUpd11006.msp /qn** and click **Next**.



We now see that the Adobe Patch package is created. Right the package and distribute the content to the DP. Once the content status of the package shows green deploy it the collections.

Icon	Name	Programs	Manufacturer	Version	Language	Package ID
	Adobe Patch 11.0.06	1	Adobe Systems	11.0.06	English	IND0008
	Adobe Reader 11.0.02	1	Adobe Systems	11.0.02	English	IND0007
	Configuration Manager Client Package	0	Microsoft Corp...			IND0003
	User State Migration Tool for Windows 8.1	0	Microsoft Corp...	6.3.9600.16384		IND0001

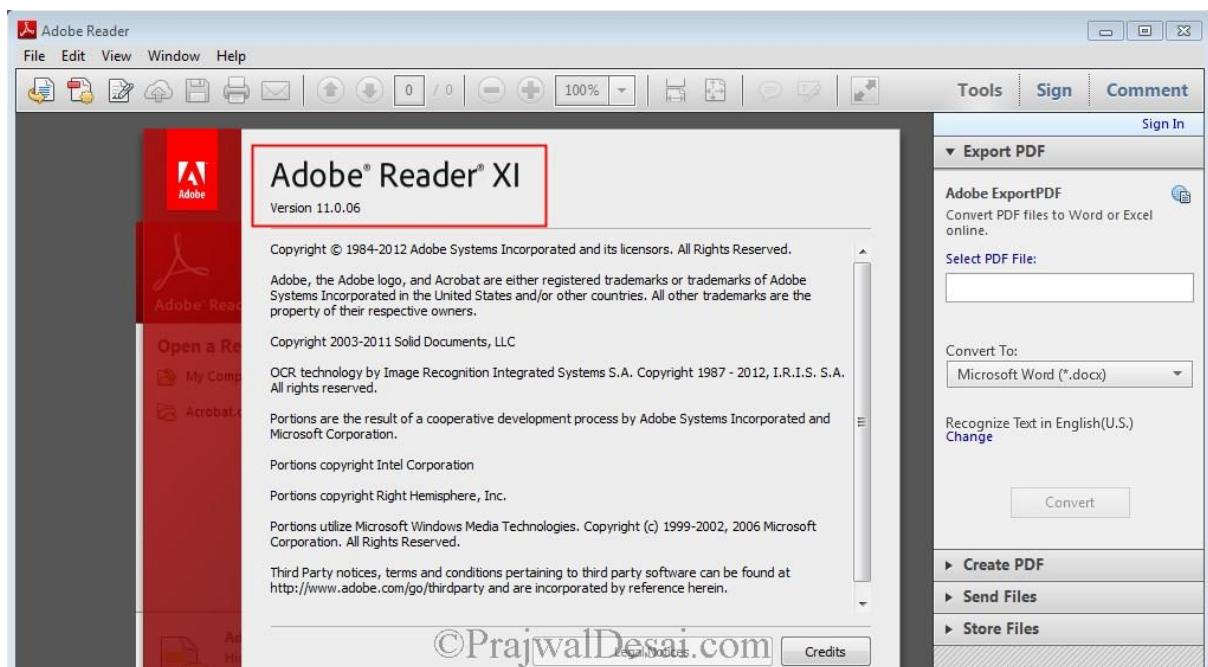
On one the client machine we open the **execmgr.log** file and we see that the patch file is being downloaded and installed.

```

Log Text
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent[AdvertisementId = "IND2003";Cli...
Raised Program Started Event for Ad:IND2003, Package:IND0008, Program: Adobe Reader Patch 11.0.06
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND0008",ProgramID="Adobe Reader Patch ...
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND0008",ProgramID="Adobe Reader Patch ...
MTC task with id {0CE91D2-23F5-4B0C-9B68-36F85641B4CE}, changed state from 4 to 5
Program exit code 3010
Looking for MIF file to get program status
Script for Package:IND0008, Program: Adobe Reader Patch 11.0.06 succeeded with exit code 3010
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramPrelimSuccessEvent[AdvertisementId = "IND20...
Raised Program Prelim Success Event for Ad:IND2003, Package:IND0008, Program: Adobe Reader Patch 11.0.06
Execution is complete for program Adobe Reader Patch 11.0.06. The exit code is 3010, the execution status is SuccessRebootRequired
Requesting MTC to delete task with id: {0CE91D2-23F5-4B0C-9B68-36F85641B4CE}
MTC task with id: {0CE91D2-23F5-4B0C-9B68-36F85641B4CE} deleted successfully.
Execution Request for advert IND2003 package IND0008 program Adobe Reader Patch 11.0.06 state change from Running to Repor...
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND0008",ProgramID="Adobe Reader Patch ...
Program exited expecting reboot, delaying execution of other programs for 60000 ms
Date/Time: 4/26/2014 12:31:07 PM Component: execmgr Thread: 3936 (0xF60)
Source: executioncontext.cpp:792
Elapsed time is 0h 0m 0s 0ms (0.000 seconds)

```

After few minutes we see that the Adobe Reader is updated to version 11.0.06.

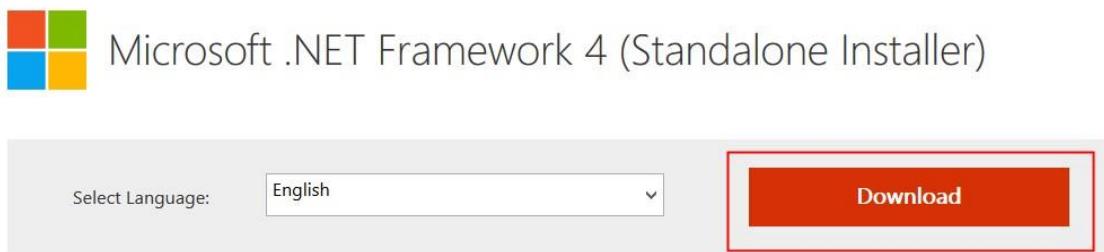


Deploy .NET Framework 4.0 using SCCM 2012 R2

This step-by-step post describes how a system administrator can deploy .NET Framework 4.0 using SCCM 2012 R2. The .NET Framework is a managed execution environment that provides a variety of services to its running applications. It consists of two major components: the common language runtime (CLR), which is the execution engine that handles running applications; and the .NET Framework Class Library, which provides a library of tested, reusable code that developers can call from their own applications. In this post we will deploy .NET Framework 4.0 using SCCM 2012 R2 to a collection which consists of Windows 7 computers. The overall deployment of .NET Framework 4.0 is easy however if you follow screenshots it will be pretty easy.

Download the .NET Framework 4.0 standalone installer by clicking below button.

[Download Microsoft .NET Framework 4.0](#)



The Microsoft .NET Framework 4 redistributable package installs the .NET Framework runtime and associated files that are required to run and develop applications to target the .NET Framework 4.

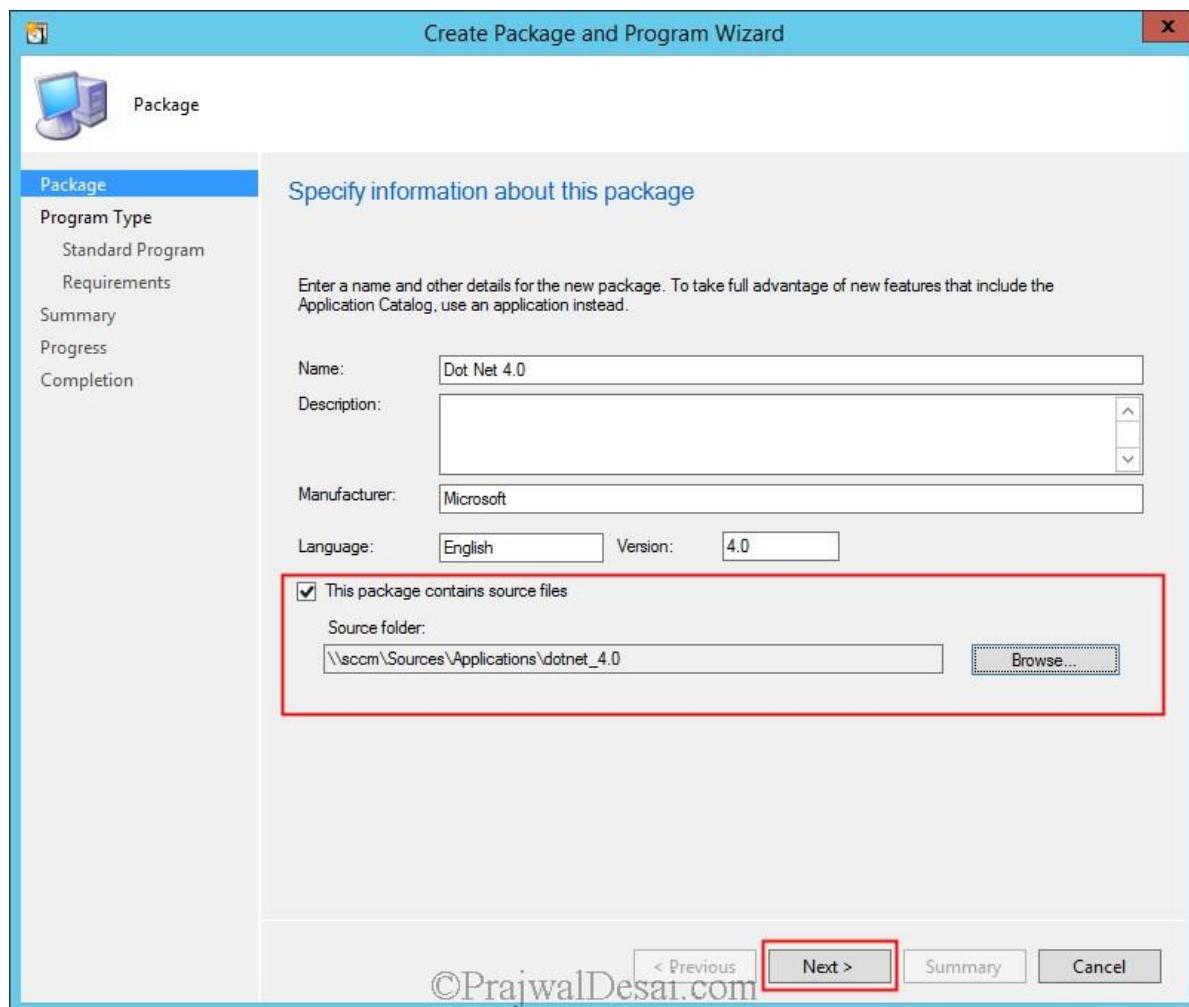
Details

System Requirements

©PrajwalDesai.com

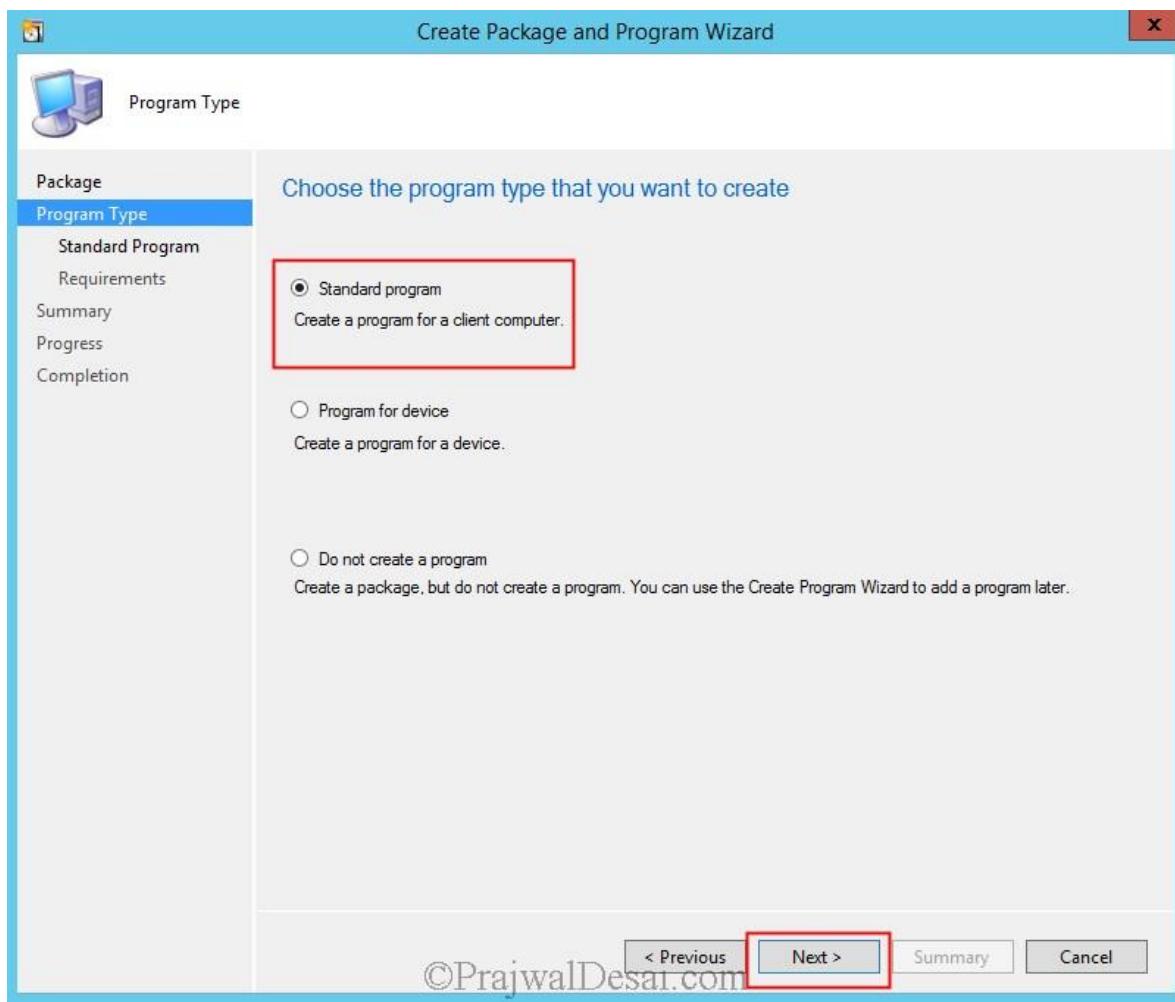
After you download .NET Framework 4.0 installer, copy it to a folder on the SCCM server. In the Configuration Manager console, choose **Software Library**. In the **Software Library** workspace, expand **Application Management**, and then choose **Packages**. Right click **Packages** and click **Create Package**.

Specify the **Name**, **Source folder** and click **Next**.

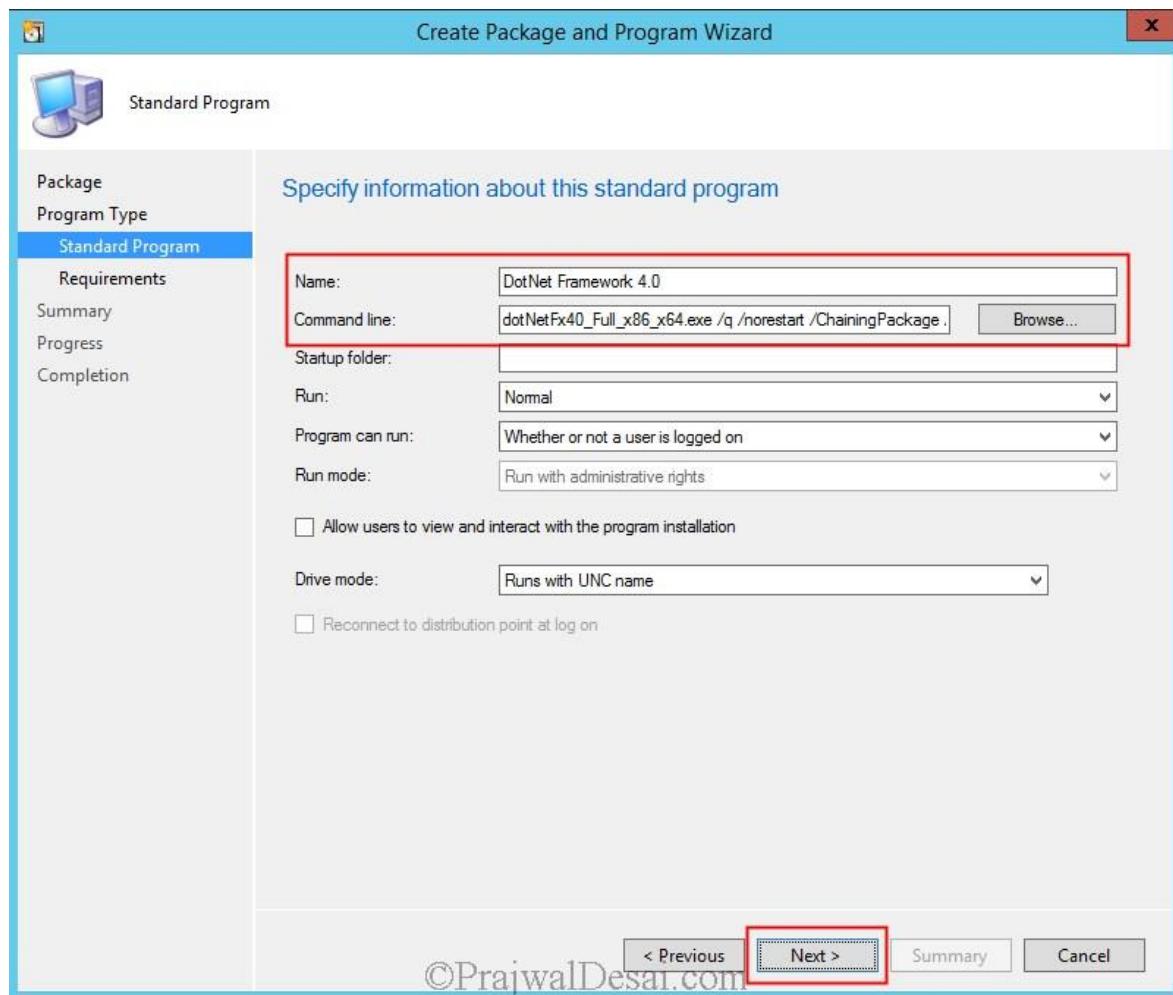


©PrajwalDesai.com

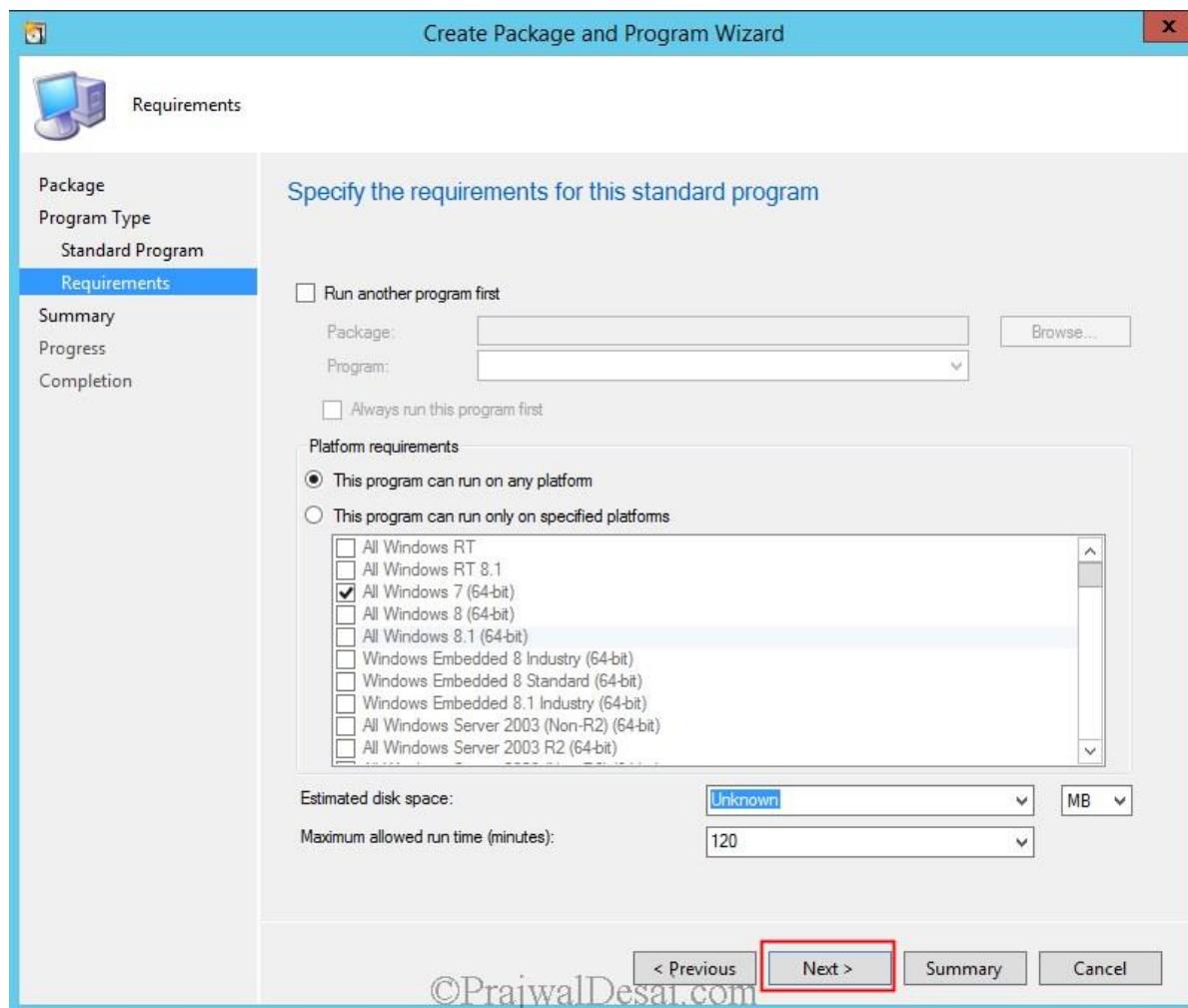
Choose the **Program Type** as **Standard Program**. Click **Next**.



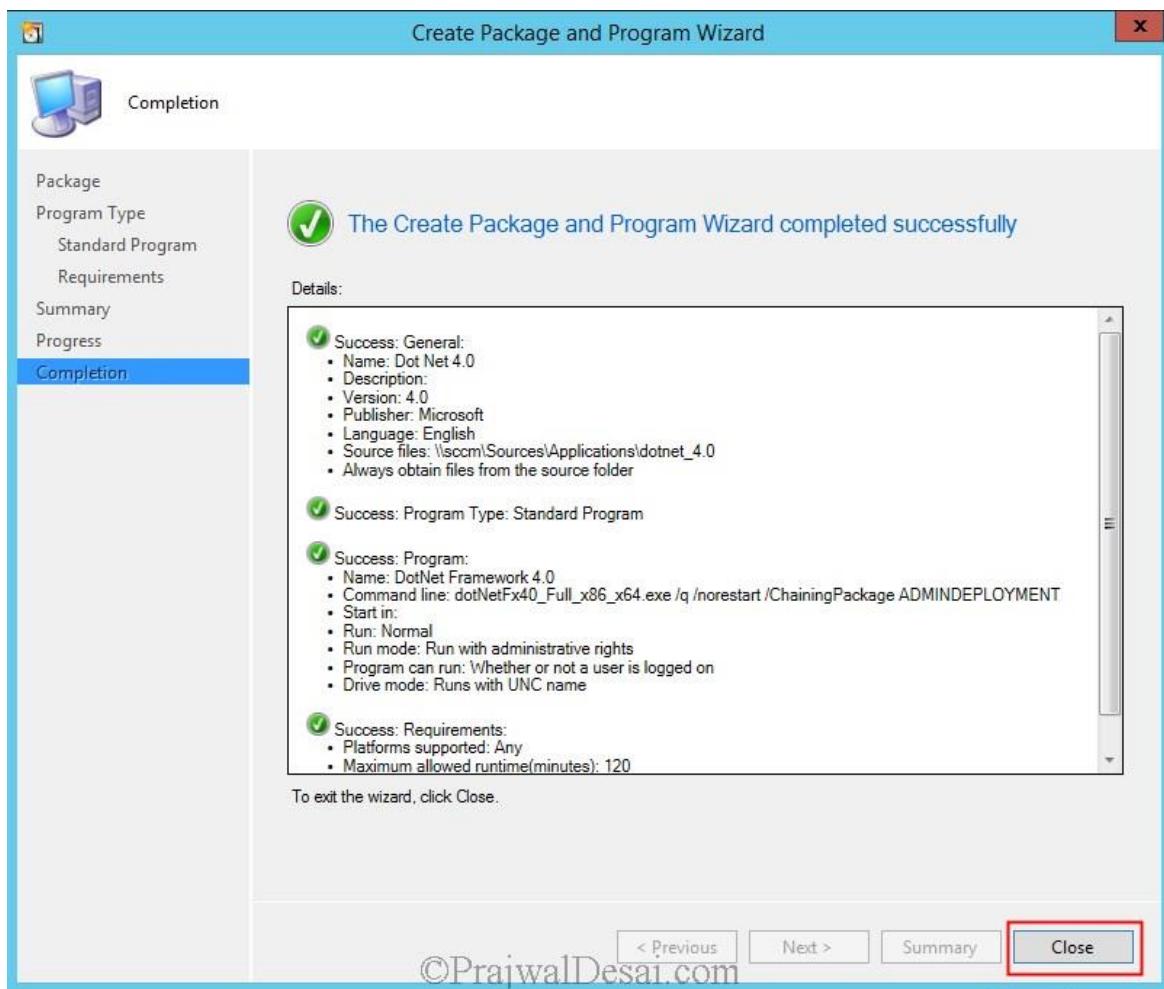
Specify the **Name** for the standard program, enter the Command line as
dotNetFx40_Full_x86_x64.exe /q /norestart /ChainingPackage
ADMINDEPLOYMENT and click **Next**.



Click **Next**.

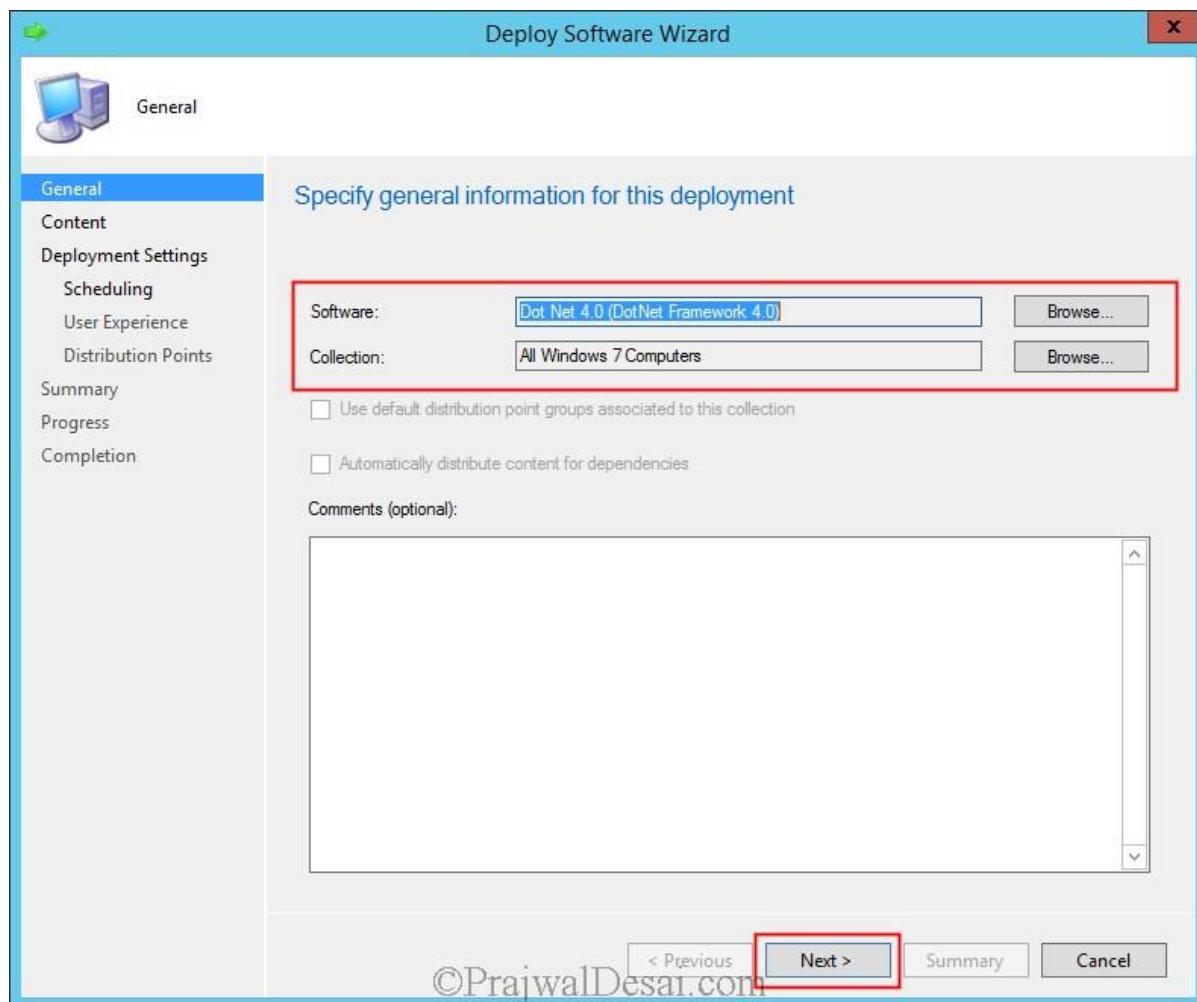


Click on **Close**.

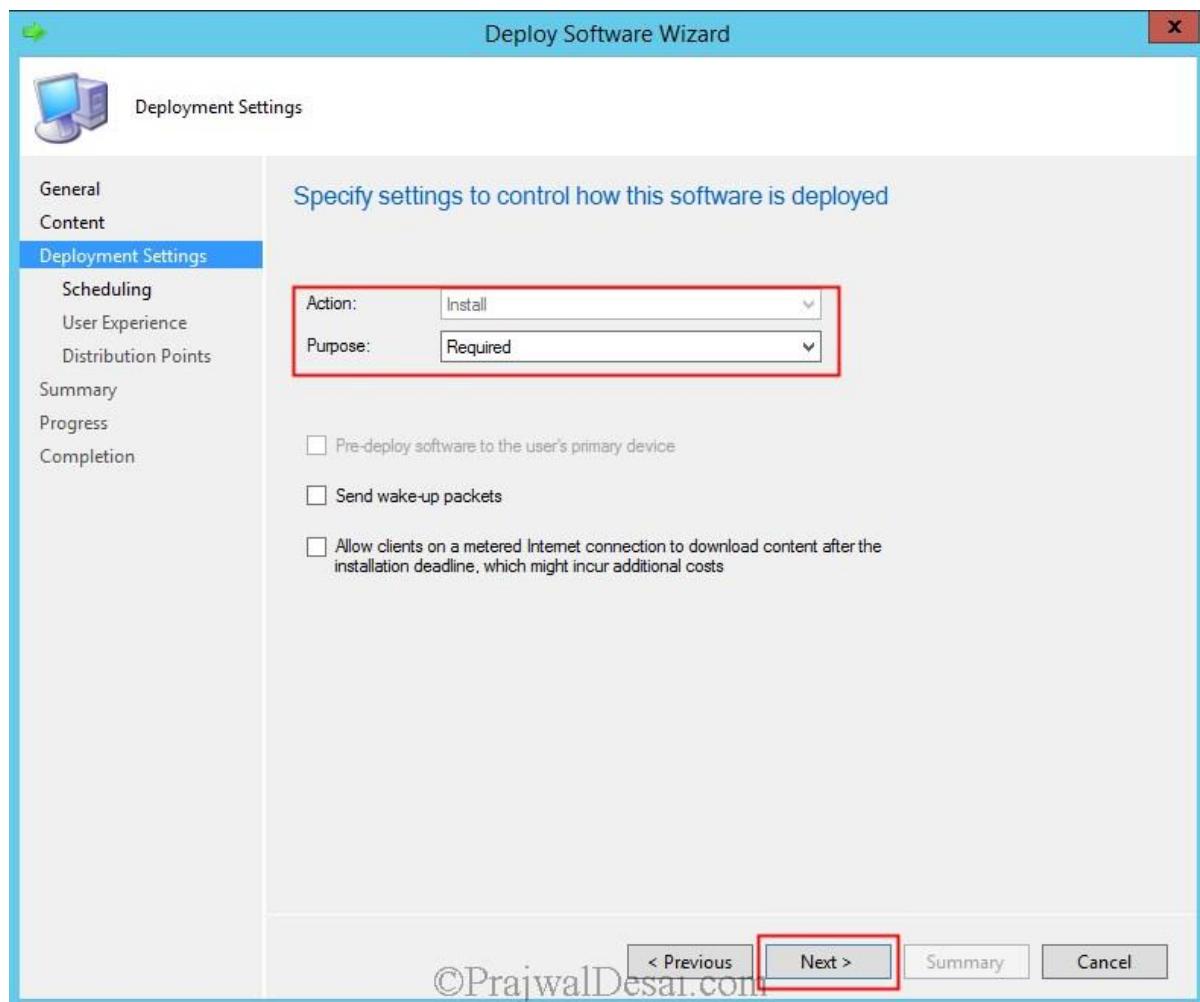


The next step to distribute the program to DP and deploy it to the collection. To distribute the package, right click the package and click **Distribute Content**. Follow the wizard, add your DP and close the wizard. Once the package has distributed the next step is to deploy the package. Right click the package and click **Deploy**. Click on **Browse** and add the collection to which this package is to be deployed.

Click **Next**.

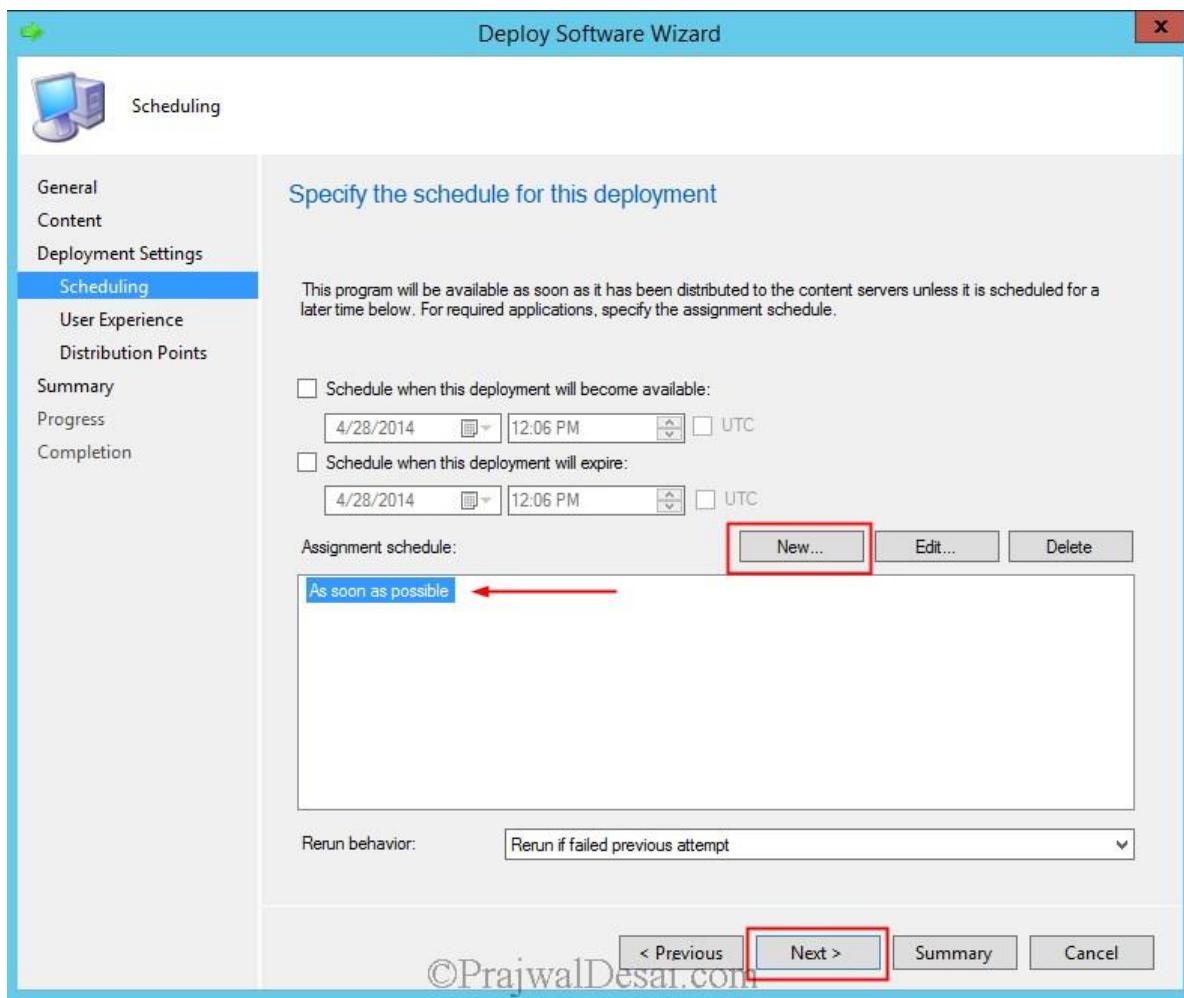


Set the purpose as **Required** and click **Next**.

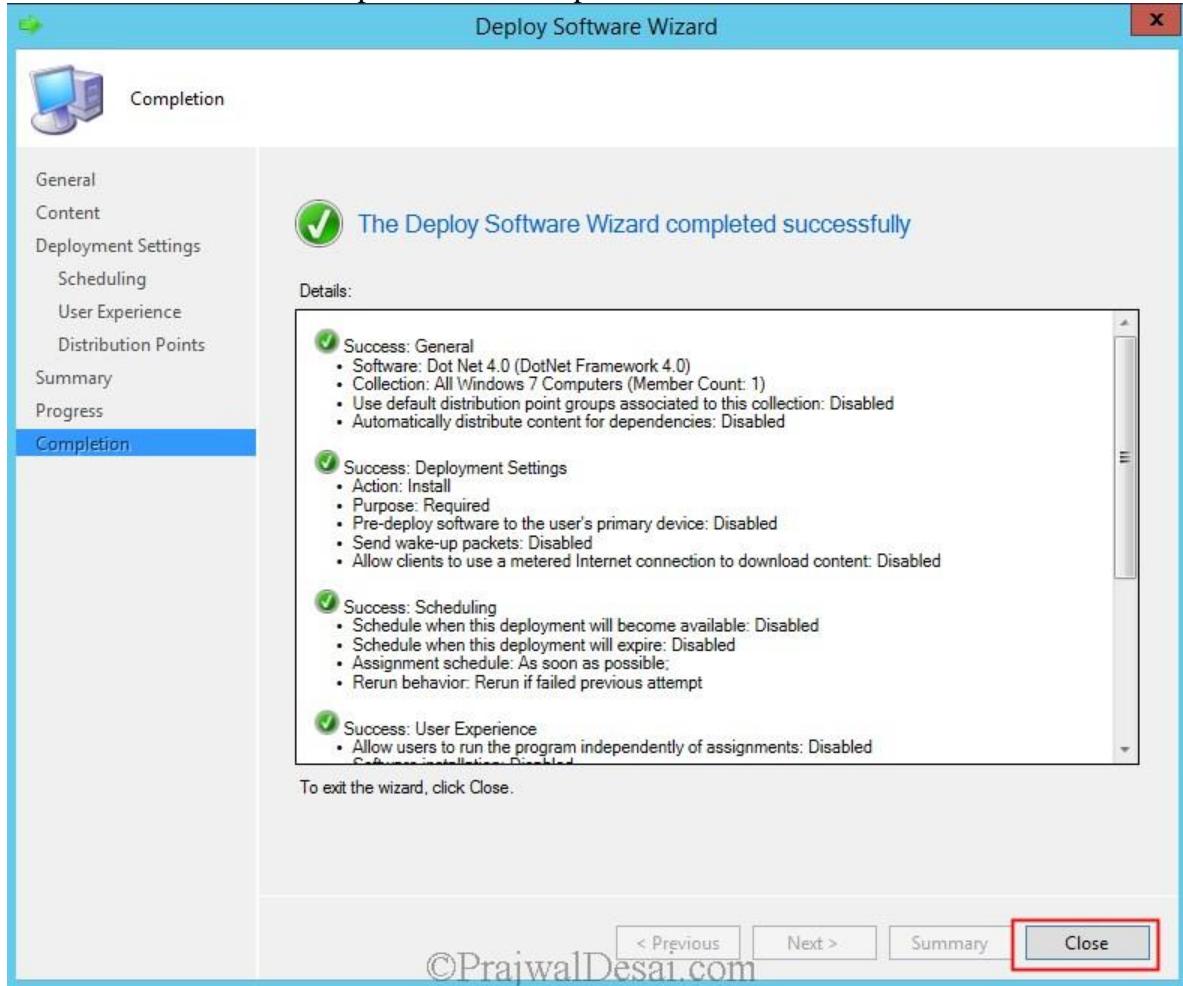


Specify the schedule for this deployment. Specify when you want the .NET Framework 4.0 to be installed. Click **New** and set the assignment schedule to **As soon as possible**.

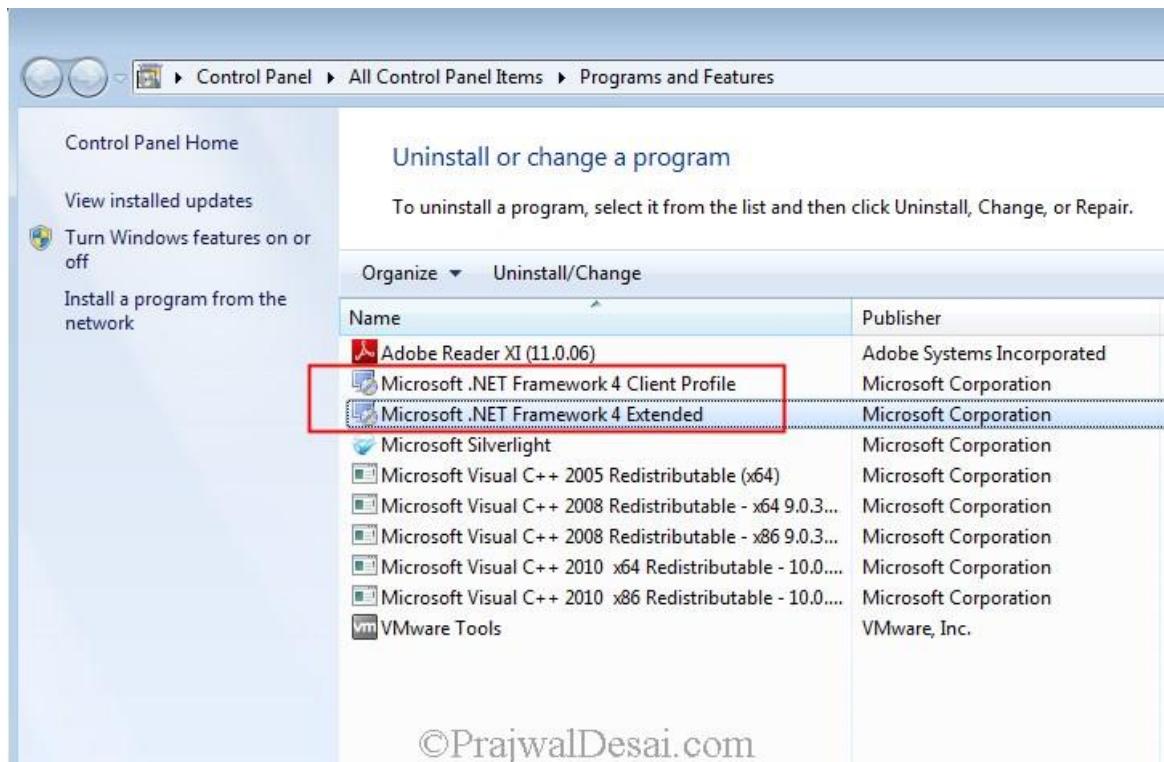
Click Next.



Follow the wizard and complete the next steps. Click **Close**.



On one the client machine, under **Program and Features** we see that .NET Framework 4.0 has been installed.



Open the **execmgr.log** file on the client machine, we see that the execution is complete for .Net Framework 4.0. In case the installation fails check the log file for any errors.

The screenshot shows the Configuration Manager Trace Log Tool window with the title bar "Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\execmgr.log]". The menu bar includes File, Tools, Window, Help. The toolbar has icons for Open, Save, Print, and Stop. The main pane displays a table of log entries:

Log Text	Component	Date/Time	Thread
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent[AdvertisementId = ...]	execmgr	4/28/2014 12:08:53 PM	3724 (0xE8C)
Raised Program Started Event for Ad:IND20004, Package:IND00009, Program: DotNet Framework 4.0	execmgr	4/28/2014 12:08:53 PM	3724 (0xE8C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00009",ProgramID="DotNet..."	execmgr	4/28/2014 12:08:53 PM	3724 (0xE8C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00009",ProgramID="DotNet..."	execmgr	4/28/2014 12:08:53 PM	3724 (0xE8C)
MTC task with id {7A956FE1-C75A-4029-A4A9-5E35AFD01658}, changed state from 4 to 5	execmgr	4/28/2014 12:08:53 PM	2052 (0x804)
Program exit code 0	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Looking for MIF file to get program status	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Script for Package:IND00009, Program: DotNet Framework 4.0 succeeded with exit code 0	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessfullyEvent[Advertis...	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Raised Program Success Event for Ad:IND20004, Package:IND00009, Program: DotNet Framework 4.0	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Execution is complete for program DotNet Framework 4.0. The exit code is 0, the execution status is Success	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00009",ProgramID="DotNet..."	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Requesting MTC to delete task with id:{7A956FE1-C75A-4029-A4A9-5E35AFD01658}	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
MTC task with id: {7A956FE1-C75A-4029-A4A9-5E35AFD01658} deleted successfully.	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00009",ProgramID="DotNet..."	execmgr	4/28/2014 12:12:01 PM	1148 (0x47C)

At the bottom, it says "Elapsed time is 334h 13m 2s 94ms (1203182.094 seconds)".

©PrajwalDesai.com

How To Backup SCCM 2012 R2 Server

How To Backup SCCM 2012 R2 Server In this post we will see **How To Backup SCCM 2012 R2 Server**. If you have deployed SCCM 2012 R2 in your organization then you must know how to backup SCCM 2012 R2 server because backing up avoids loss of critical data. For Configuration Manager sites, this preparation ensures that sites and hierarchies are recovered with the least data loss and in the quickest possible time. System Center 2012 R2 Configuration Manager provides a [backup](#) maintenance task that runs on a schedule and backs up the site database, specific registry keys, and specific folders and files. You can also create the **AfterBackup.bat** file to perform post-backup actions automatically after the backup maintenance task runs successfully.

Before you perform the backup of SCCM server few things to keep in mind.

1. The SMS Writer service must be running for the Configuration Manager site back up to successfully complete.
2. The SMS Writer service must run under the Local System account.
3. You can automate backup for Configuration Manager sites by scheduling the predefined Backup Site Server maintenance task.
4. The Local System account on the site server must have **Write** NTFS file system permissions to the local folder for the site server backup. The Local System account on the computer that is running SQL Server must have **Write** NTFS permissions to the folder for the site database backup.

1. What is the recommended schedule to take a backup of SCCM Server ?

You must configure an appropriate schedule for the site backup task. As a best practice, consider a backup schedule that is outside active working hours. If you have a hierarchy, consider a schedule that runs at least two times a week to ensure maximum data retention in the event of site failure.

2. What Gets Backed Up ?

3. Can I use the same technique to backup my secondary site ?

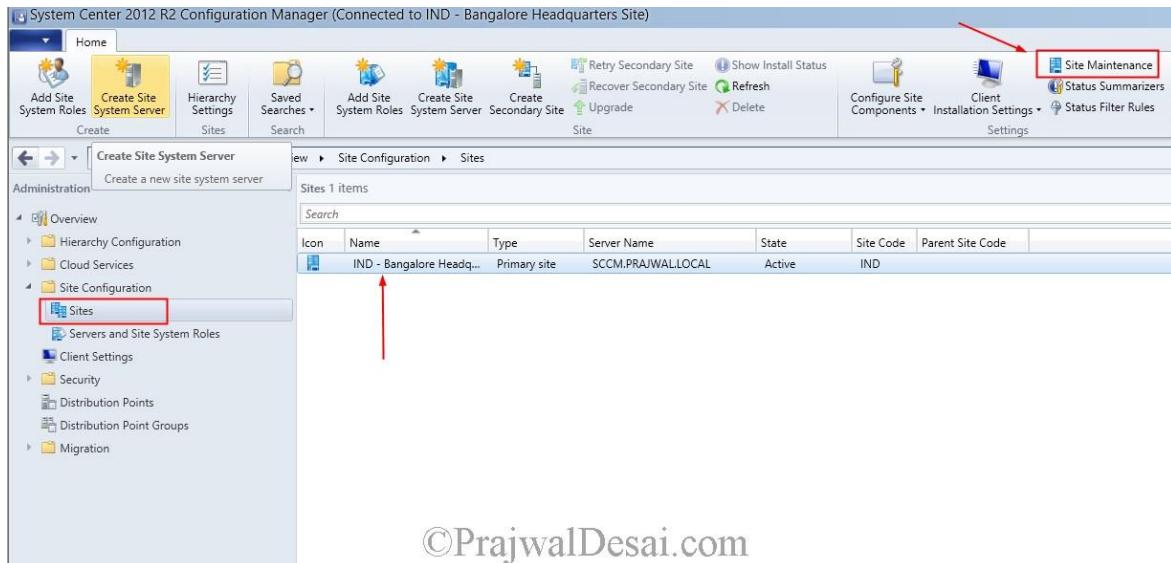
4. Can I use Data Protection Manager to Backup Site Database ?

5. What does not get backed up ?

6. When can I use option Recover the site database using a backup set ?

How To Backup SCCM 2012 R2 Server

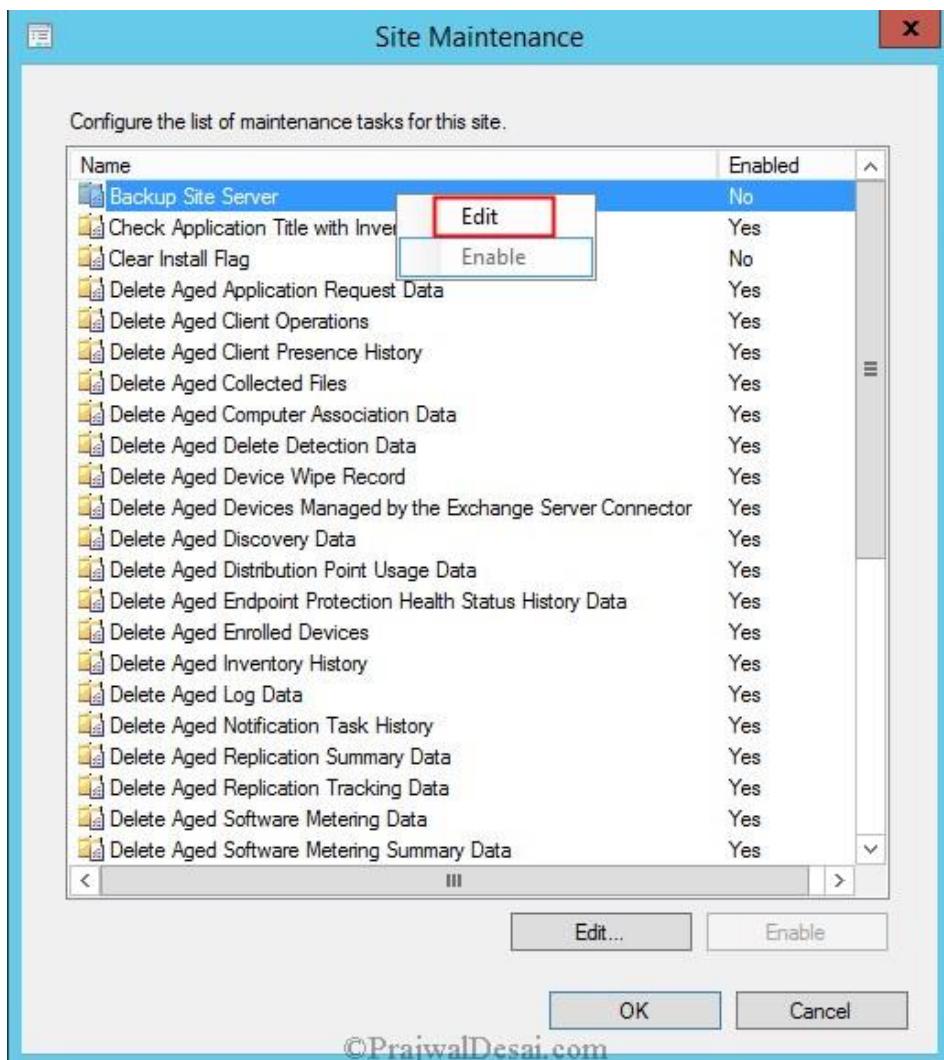
Launch the SCCM 2012 R2 console, click on **Administration**, expand **Overview**, expand **Site Configuration**, click on **Sites** and on the right pane click on your primary site. On the top ribbon click **Site Maintenance**.



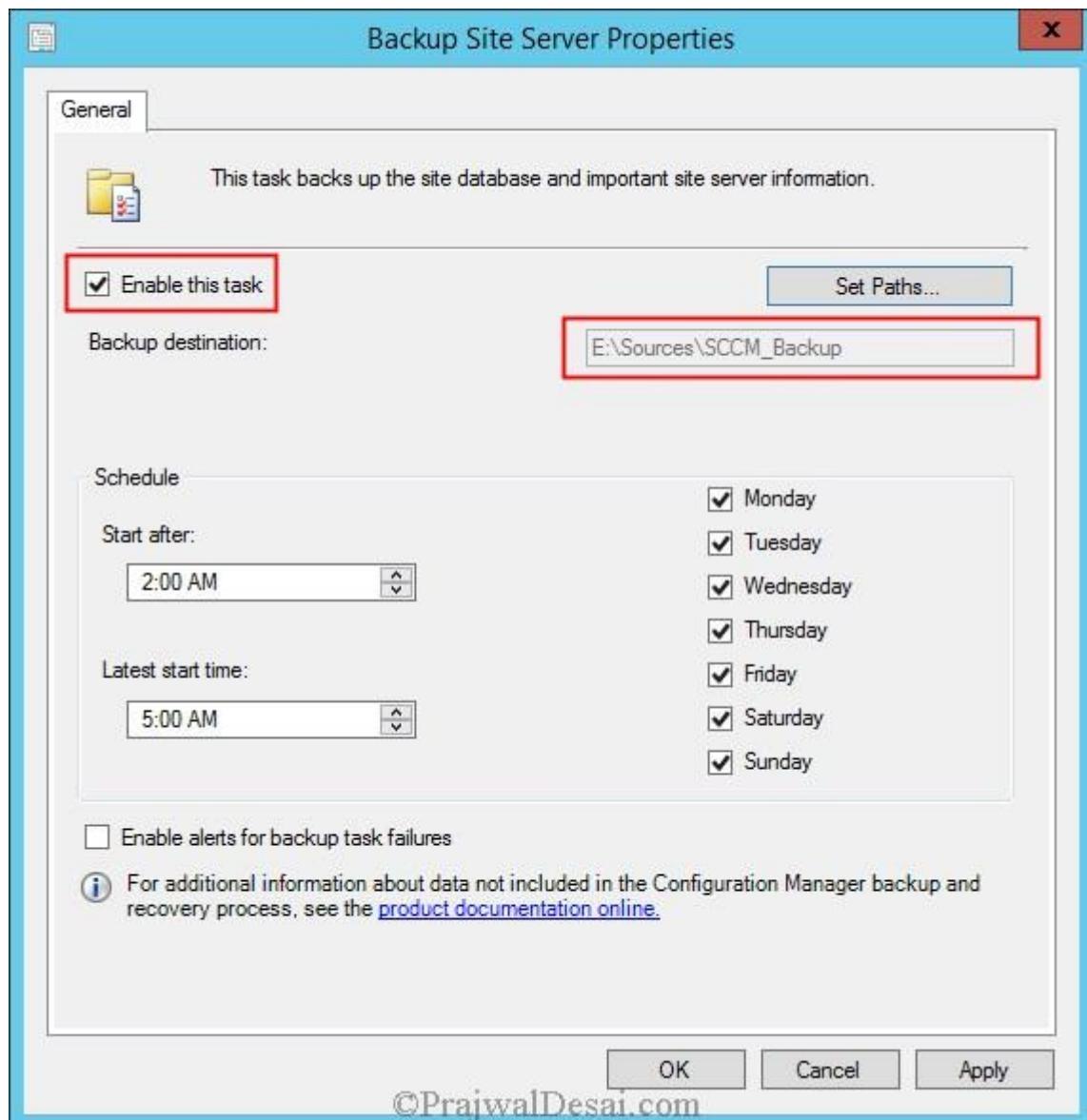
©PrajwalDesai.com

This will bring up **Site Maintenance** window. You can see there are list of tasks, few of them are enabled and running. Look for task named “**Backup Site Server**“.

This task is **not enabled** by default, right click on the task and click **Edit**.

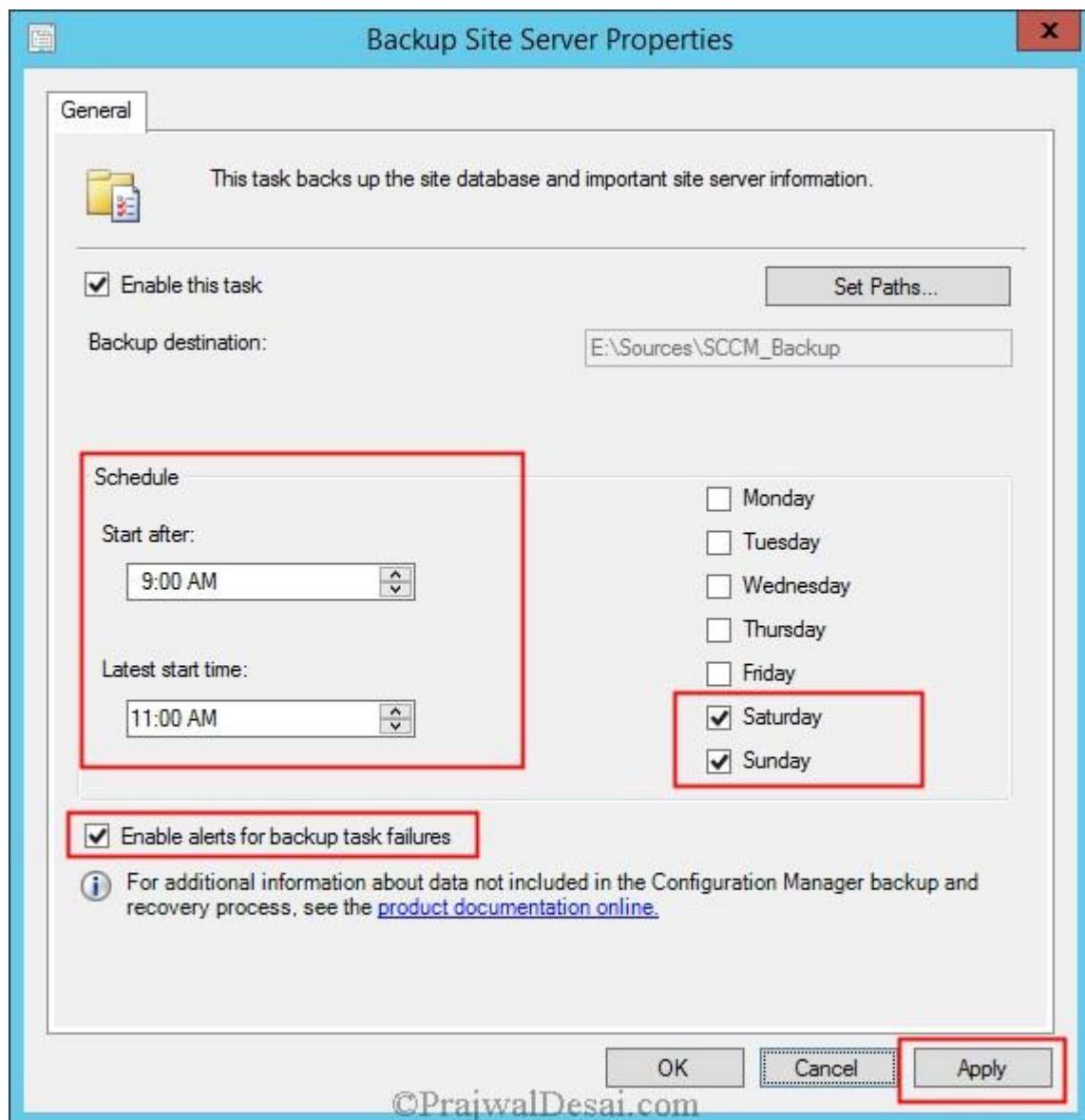


When you edit the task it brings **Backup Site Server Properties** window, click **Enable this task**, click **Set Paths** and set the path where you want to place the backup files of SCCM 2012 R2 server.

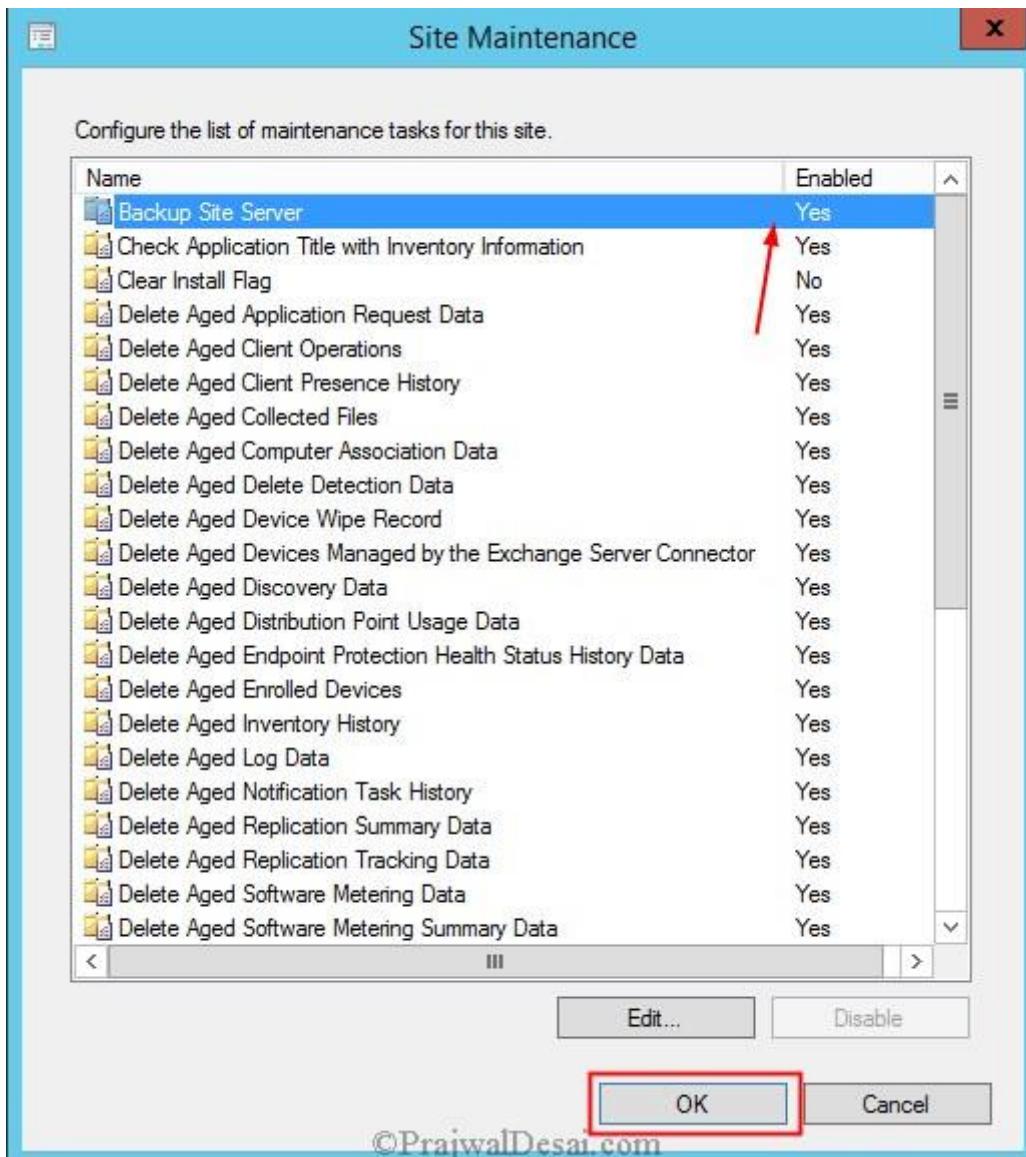


Set the **Schedule** for the backup. In this example we will schedule the backup on weekends. Set the start time as per your requirements. Check the box **Enable alerts for backup task failures**.

Click **Apply** and **OK**.

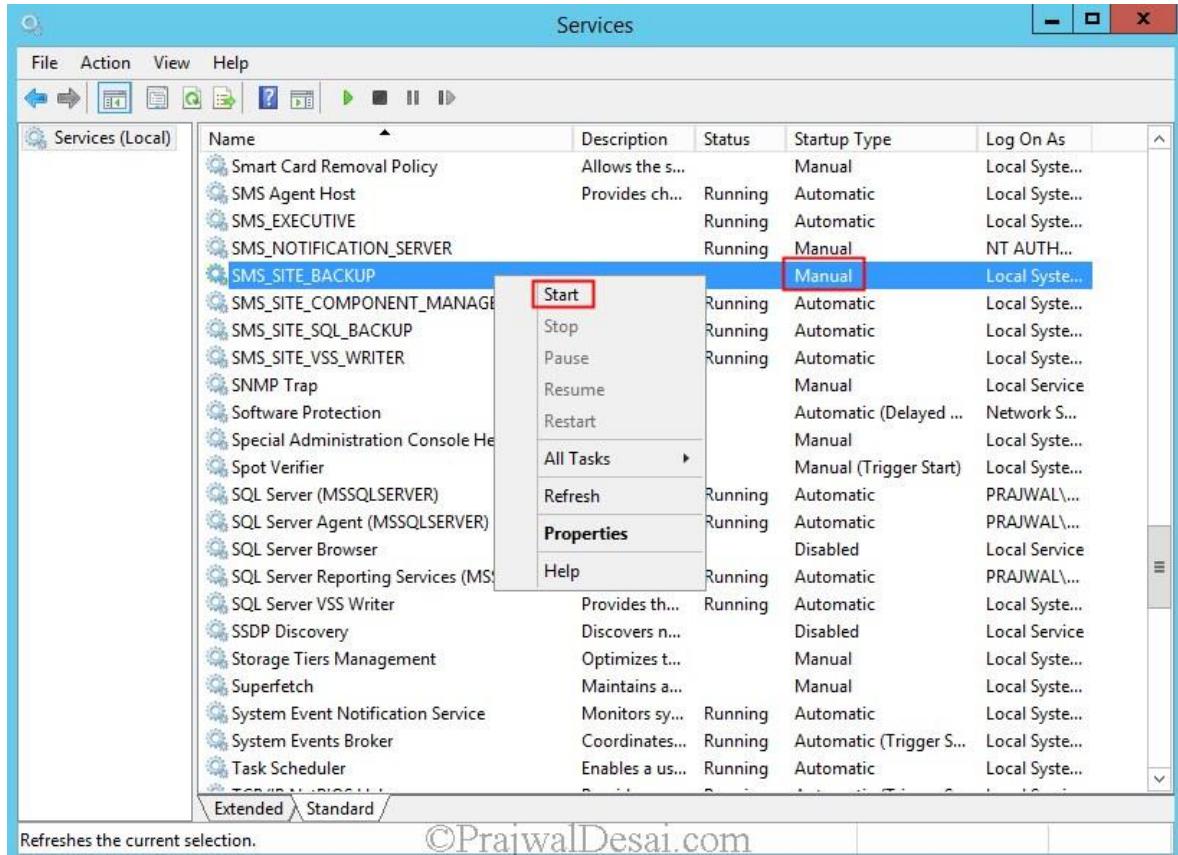


We now see that Backup Site Server task is enabled and scheduled to run with configured settings.

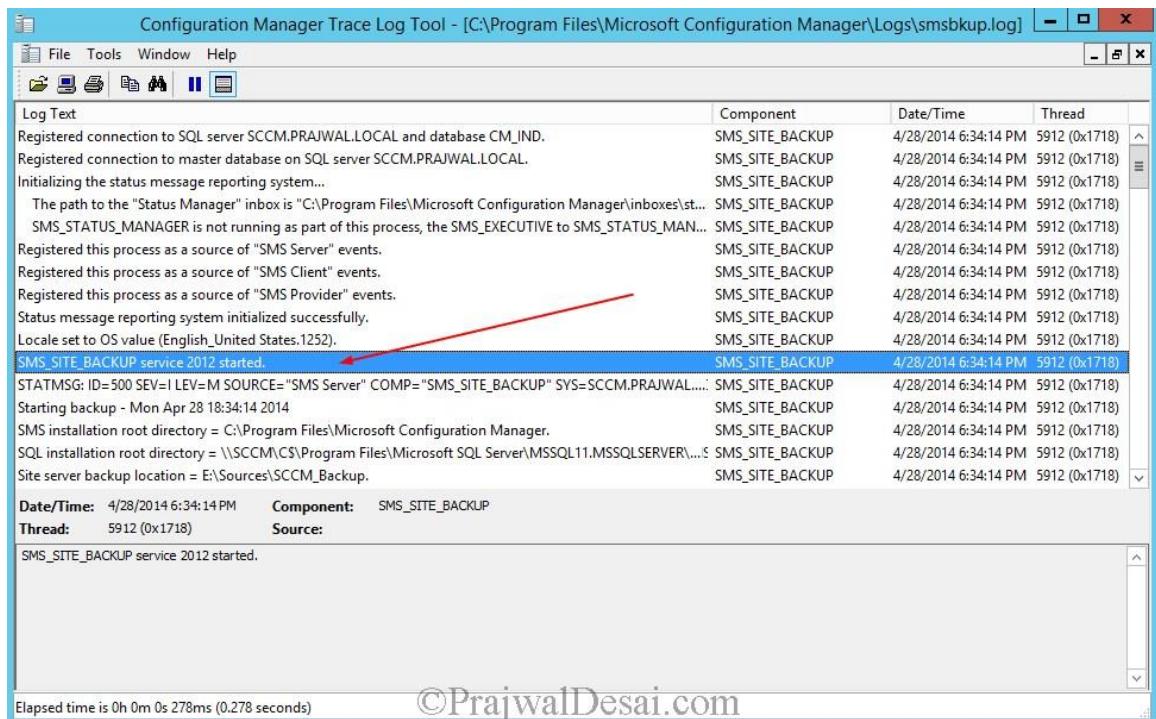


This was all about scheduling the backup task automatically. The next section will show how to backup SCCM 2012 R2 server manually.

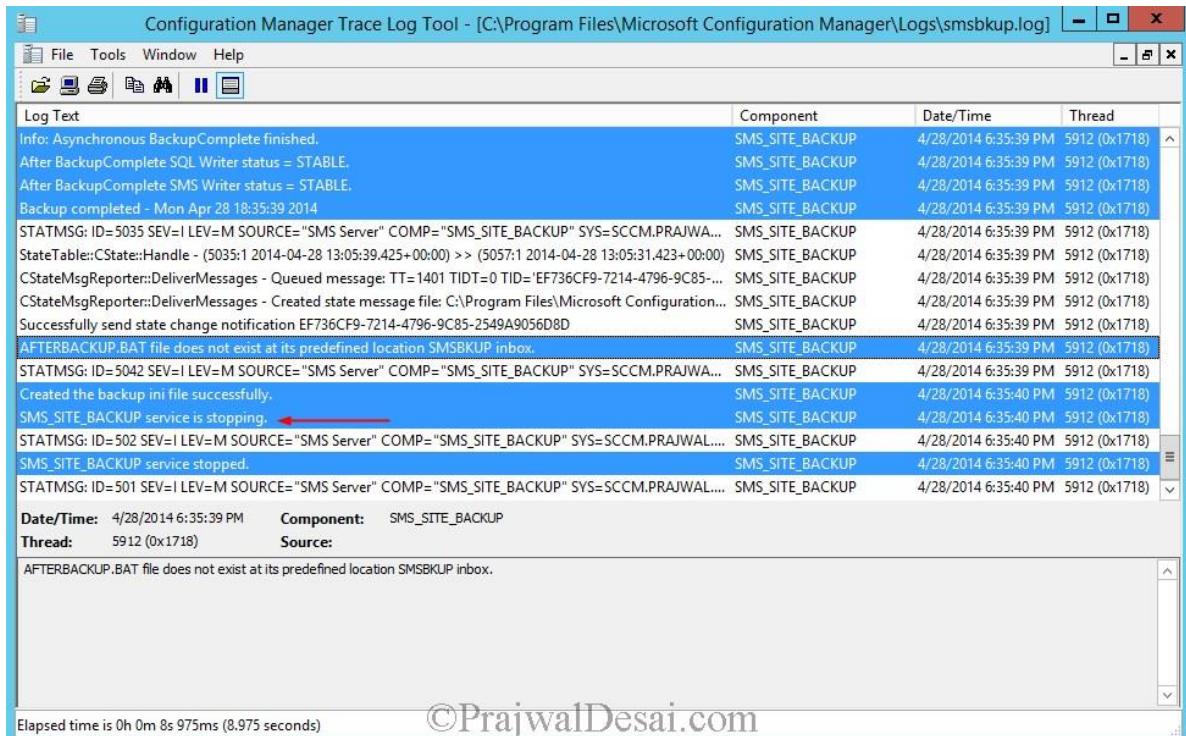
How To Backup SCCM 2012 R2 Server Manually – Consider a scenario where administrator needs to backup the SCCM 2012 R2 server immediately ? In such cases we can manually backup SCCM server. On the SCCM server, click on run and click **services.msc**, look for the service named **SMS_SITE_BACKUP (C:\Program Files\Microsoft Configuration Manager\bin\x64\smsbkup.exe)**, right click the service and click **Start**.



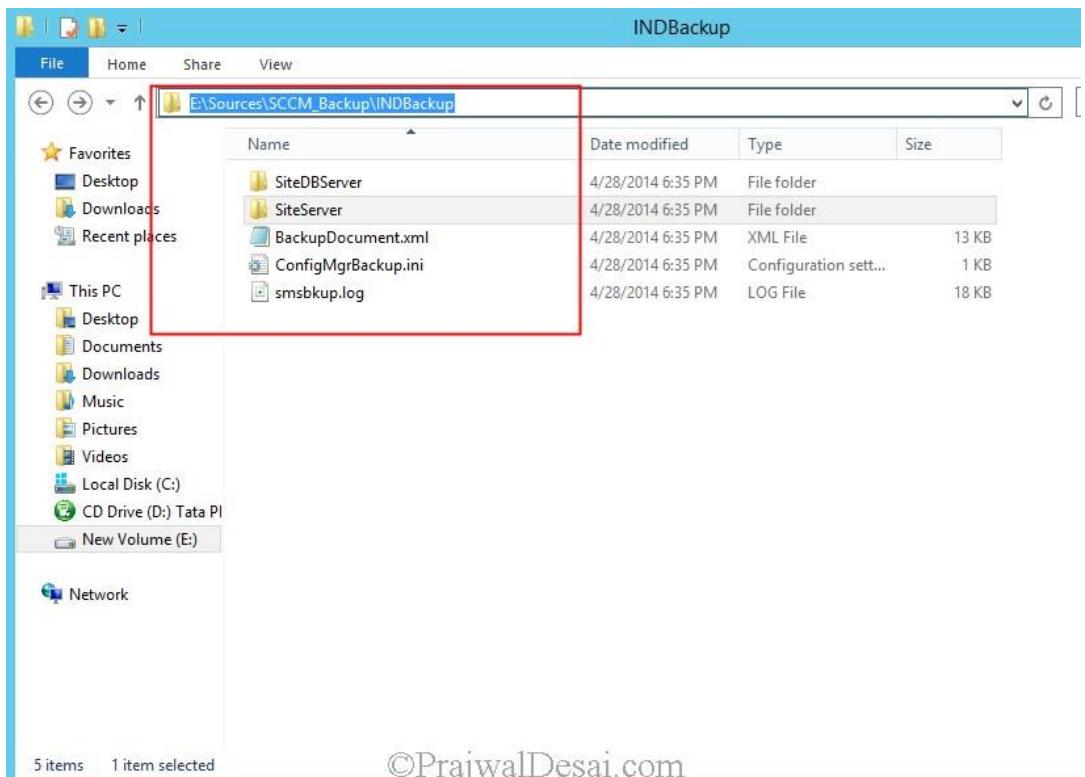
The backup task has started and it is being done in the background. In <ConfigMgrInstallationFolder>\Logs, review **Smsbkup.log** for warnings and errors. To see the backup process open the log file **smsbkup.log** located under the path **C:\Program Files\Microsoft Configuration Manager\Logs**. From the log file we see that **SMS SITE BACKUP** service 2012 has been started.



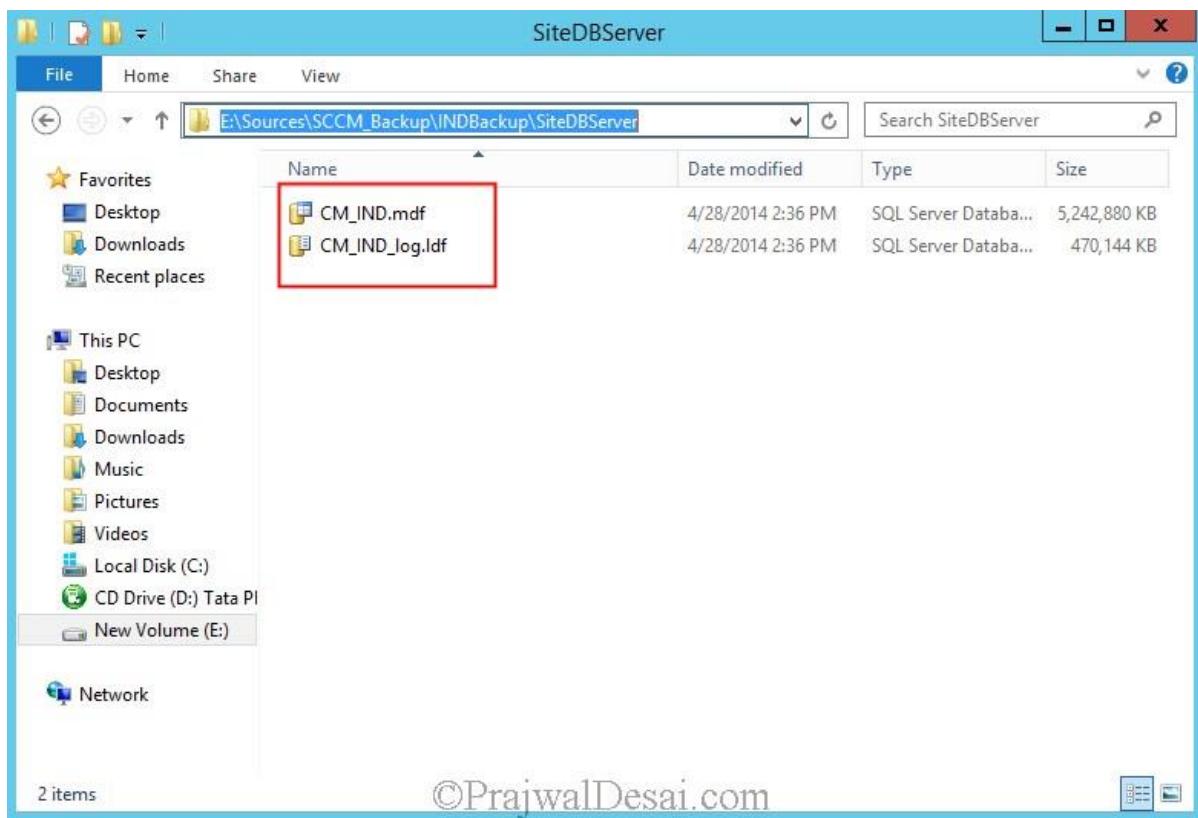
After few seconds we see that the backup has been completed successfully. Look for the line **Backup completed – Day Month Date HH:MM:SS YY**. After the backup task is completed the **SMS_SITE_BACKUP** service is stopped automatically.



Let's open the backup folder and see what's inside it. We see 2 folders **SiteDBServer** and **SiteServer** which contains database files and SCCM folders (Inboxes, Logs, Data etc) respectively.



Under **SiteDBServer** folder we see **CM_sitecode.mdf** and **CM_sitecode_log.ldf** files.



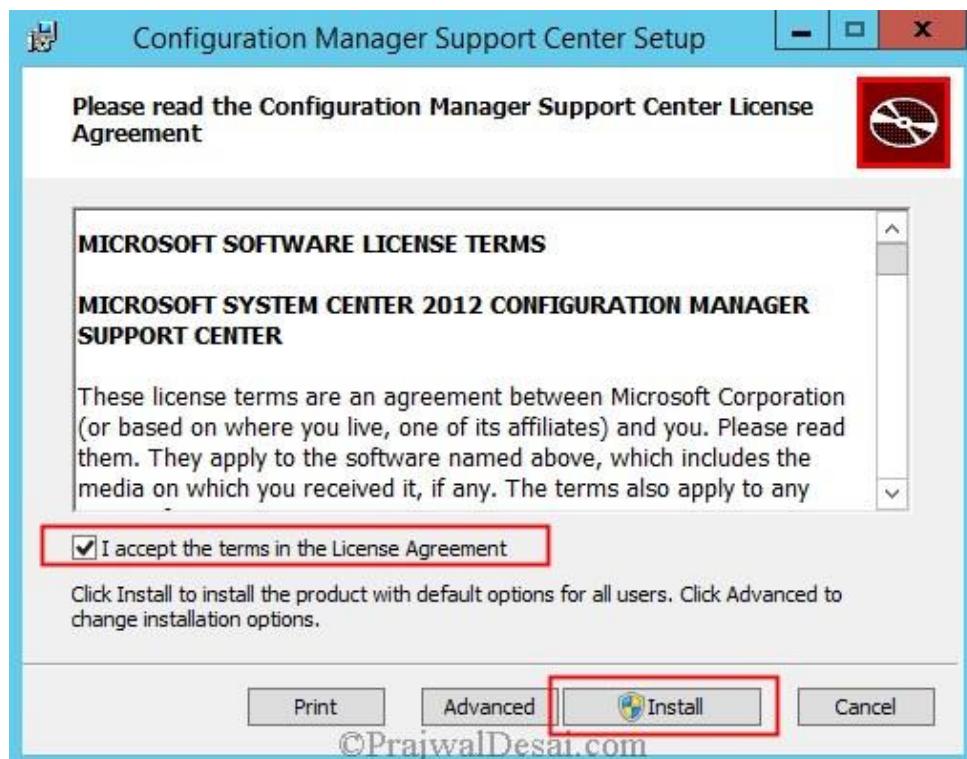
SCCM 2012 Support Center Tool

Microsoft has come up with a new tool called SCCM 2012 Support Center Tool. You might wonder why this tool ?. The reason is when you call up Microsoft Technical Support to address an issue with Configuration Manager clients, you would sometimes need to manually collect log files and other information to help support personnel to diagnose and address the issue. This tool will collect all the necessary files so that you need not do it manually. The System Center 2012 Configuration Manager Support Center helps you to gather information about System Center 2012 Configuration Manager clients, so that you can more easily address issues with those clients when working with product support specialists. SCCM 2012 Support Center tool gathers a bundle of log files which will help product support specialists to examine log files and other client data for in-depth analysis of issues with Configuration Manager clients.

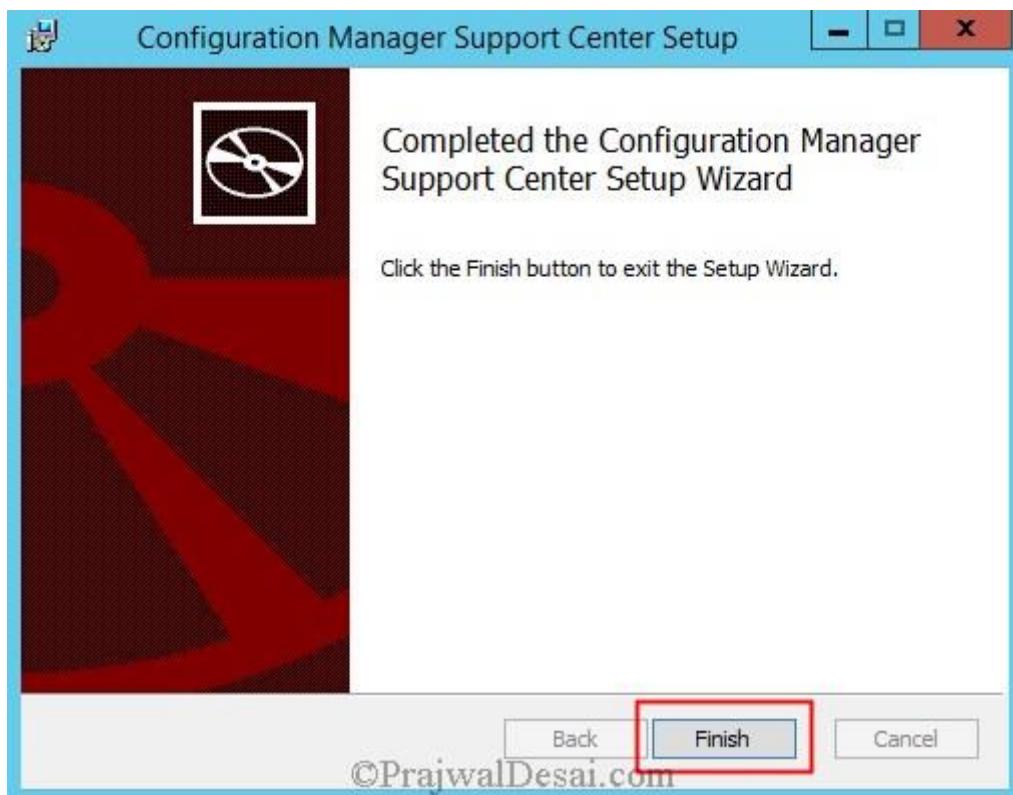
Download SCCM 2012 Support Center Tool

SCCM 2012 Support Center Tool also includes Configuration Manager Support Center Viewer, a tool that support personnel can use to open the bundle of files that you create using Configuration Manager Support Center. SCCM 2012 Support Center tool also includes PowerShell cmdlets that can be used to create a remote connection to another Configuration Manager client, to configure the data collection options provided on the Data Collection tab, and to start data collection. So this tool will create a zip file as output that contains all of the relevant log files on your Configuration Manager client that you can send to support personnel.

The installation is very simple, you need to check the [system requirements](#) before installing this tool. In this post I will be installing the support center tool on my SCCM Primary site server. Run the installer and accept the license terms and click **Install**.



Click **Finish** to complete the installation.



Launch the **Configuration Manager Support Center**, the first thing that you see is that of **Data Collection**. This window allows you to select the various kinds of tasks that are very useful for troubleshooting client related issues. You can click on **Collect Selected Data** and choose to collect only the data for enabled tasks or collect data for all the items.

A screenshot of the Configuration Manager Support Center Data Collection window. The title bar says "Configuration Manager Support Center". The menu bar includes "Data Collection", "Client Details", "Client Policy", "Content", "Inventory", "Troubleshooting", and "Logs", with "Data Collection" being the active tab. On the left, there's a "Collect Selected Data" button with a red arrow pointing to it. Below it is a "Main data collection status" section with a checked checkbox and a progress bar. The main area is a table of data collection tasks:

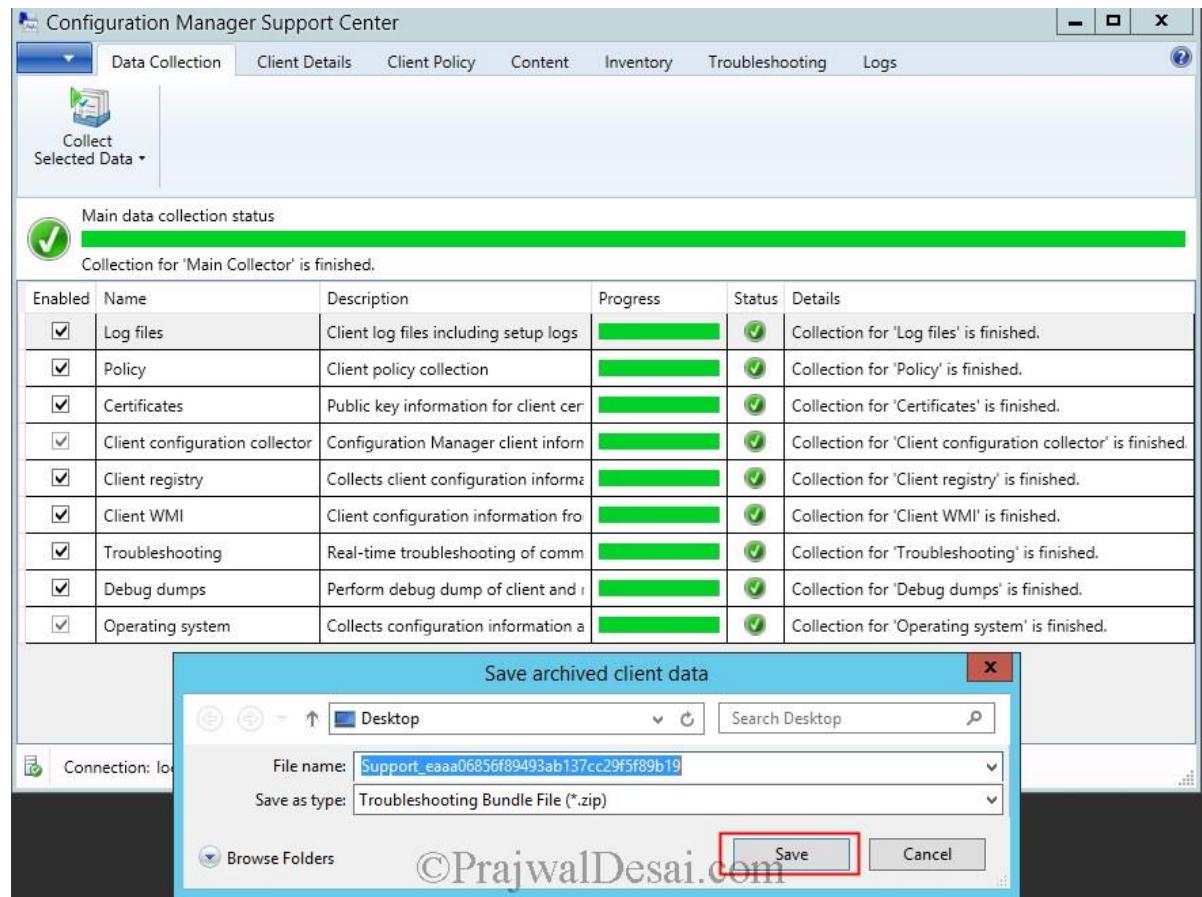
Enabled	Name	Description	Progress	Status	Details
<input checked="" type="checkbox"/>	Log files	Client log files including setup logs	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Policy	Client policy collection	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Certificates	Public key information for client certificates. Private keys are not col	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Client configuration collector	Configuration Manager client information	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Client registry	Collects client configuration information from the registry. Only Cor	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Client WMI	Client configuration information from WMI. This does not collect cli	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Troubleshooting	Real-time troubleshooting of common client problems	<div style="width: 20%;"></div>		
<input checked="" type="checkbox"/>	Debug dumps	Perform debug dump of client and related processes. Debug dump:	<div style="width: 100%; background-color: #0072bc; color: white;"></div>		
<input checked="" type="checkbox"/>	Operating system	Collects configuration information about the local machine. This inc	<div style="width: 20%;"></div>		



Connection: localhost (Connected)

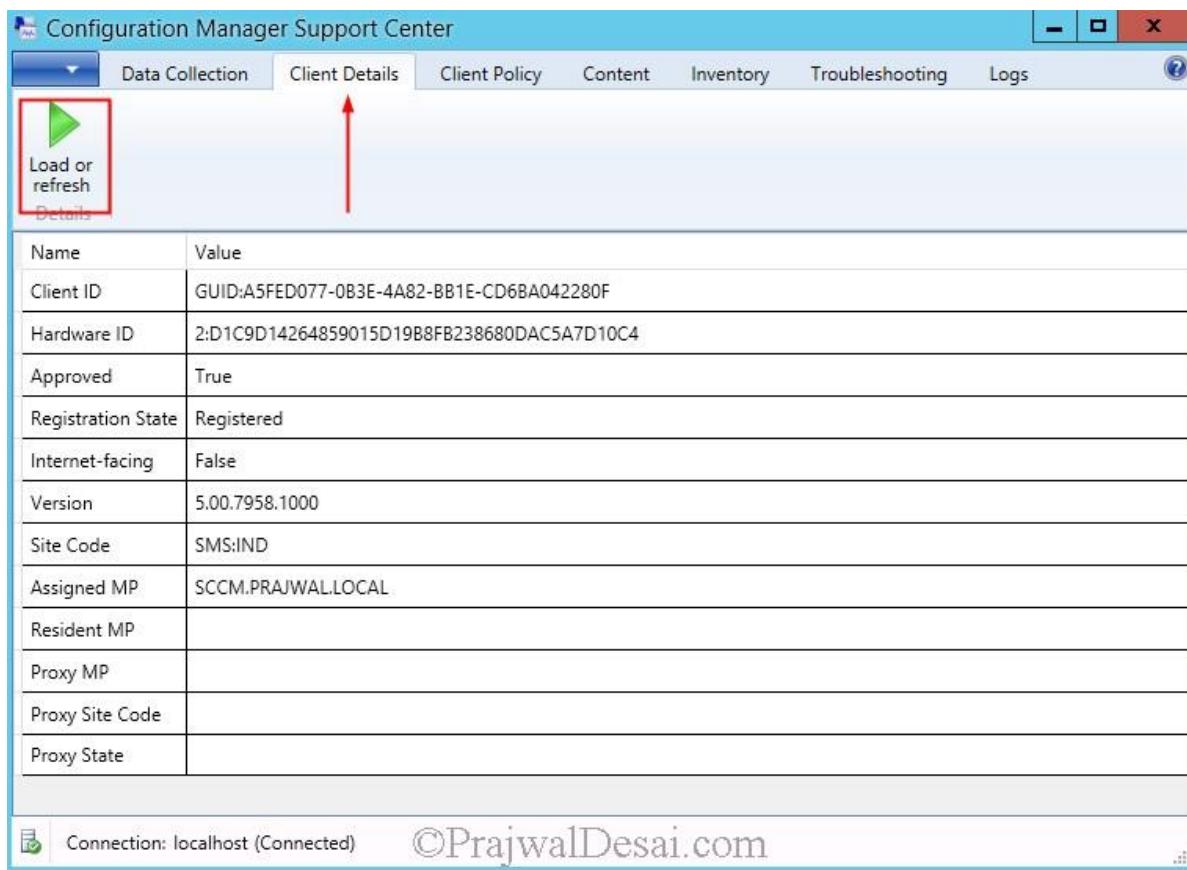
©PrajwalDesai.com

When you run the **Data Collection** step for the selected items all the relevant data is collected and stored in a .zip file.



In the next tab we see **Client Details** feature. Click on **Load or refresh** to get the information about the configuration manager client properties such as Client ID, Hardware ID, client version, Site Code etc.

You can also connect to a remote machine and check the client properties.



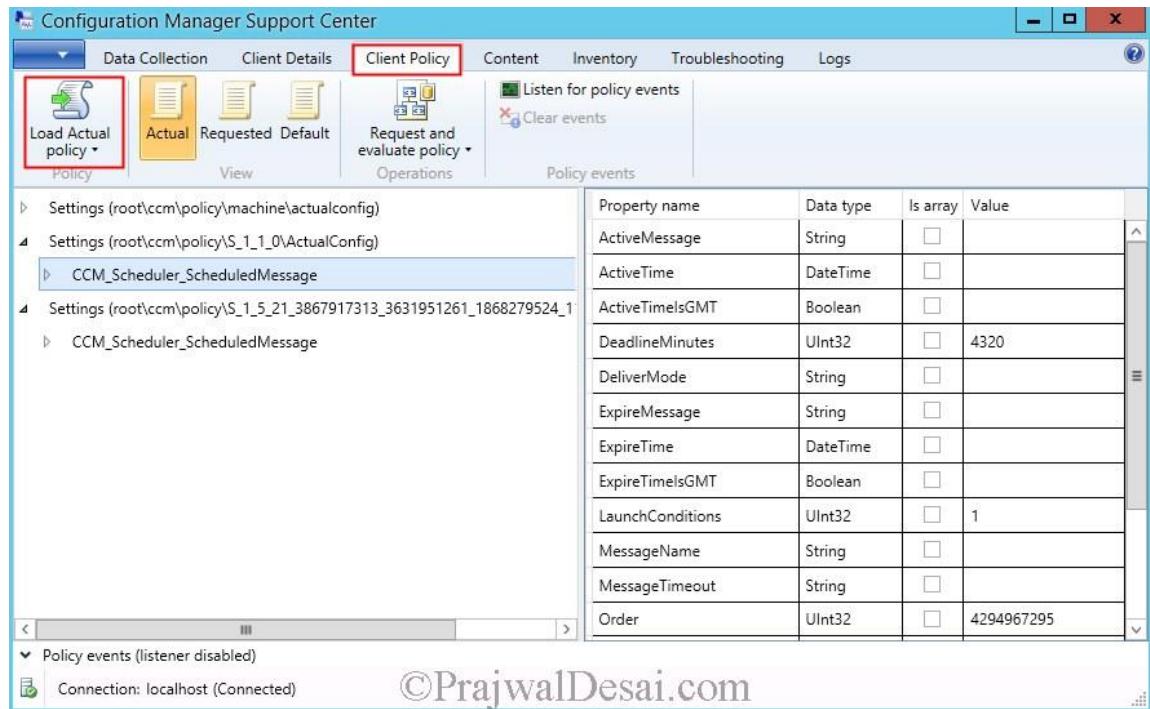
The screenshot shows the Configuration Manager Support Center window. The title bar reads "Configuration Manager Support Center". The menu bar includes "File", "Data Collection", "Client Details" (which is selected), "Client Policy", "Content", "Inventory", "Troubleshooting", and "Logs". A red box highlights the "Load or refresh" button in the top-left corner of the main content area. A red arrow points upwards from the bottom of the "Load or refresh" button towards the "Client Details" tab in the menu bar. The main content area displays a table of client details:

Name	Value
Client ID	GUID:A5FED077-0B3E-4A82-BB1E-CD6BA042280F
Hardware ID	2:D1C9D14264859015D19B8FB238680DAC5A7D10C4
Approved	True
Registration State	Registered
Internet-facing	False
Version	5.00.7958.1000
Site Code	SMS:IND
Assigned MP	SCCM.PRAJWAL.LOCAL
Resident MP	
Proxy MP	
Proxy Site Code	
Proxy State	

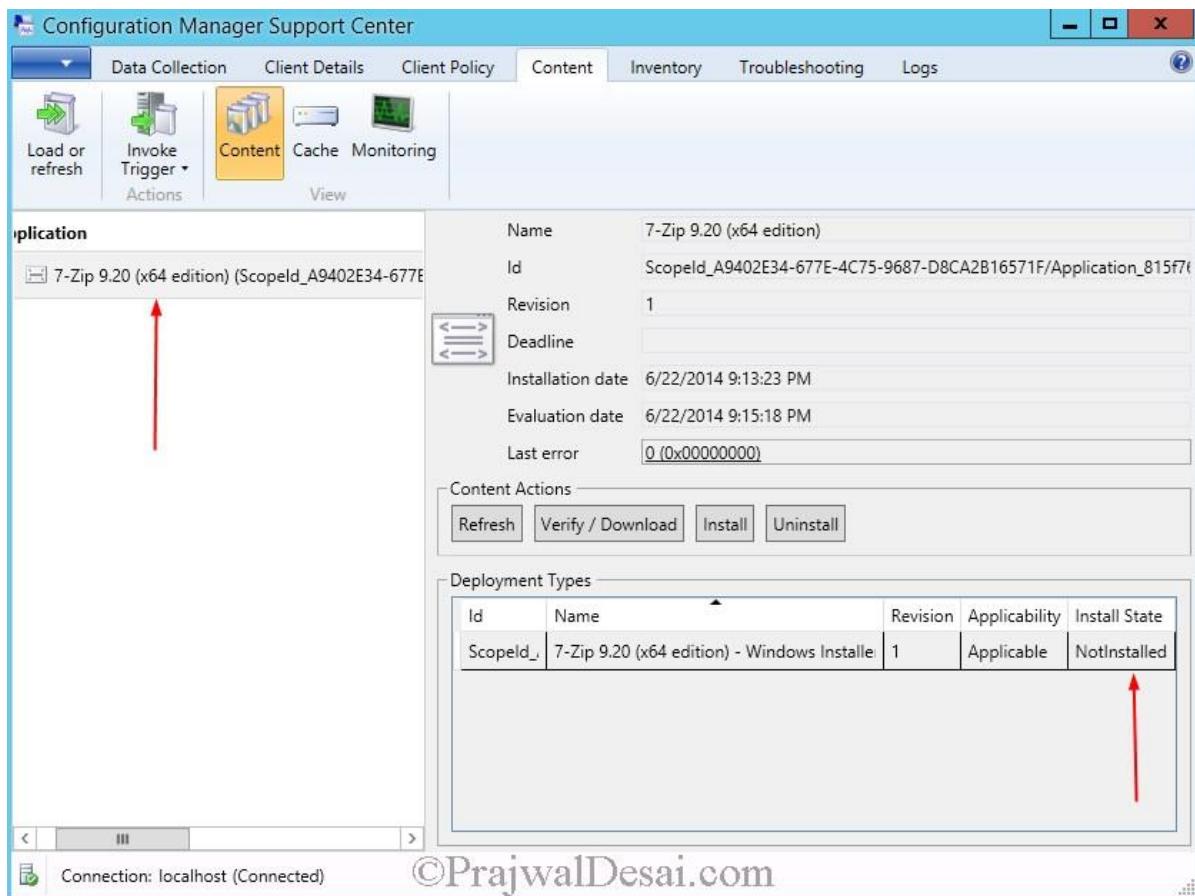
At the bottom left, there is a connection status icon and the text "Connection: localhost (Connected)". At the bottom right, there is a copyright notice "©PrajwalDesai.com".

The next feature that we see is the **Client Policy**. There are lot of things to know here, when you click on **Load Actual Policy** you see the set of policies that are applicable to the configuration manager client.

You also have got an option to request policy and evaluate policy.



In the **Content** tab, when you click **Content** you get to know what applications, packages and updates have been deployed or assigned to the client. You get to know about the application name, whether its installed or not and many other properties. If you click on **Invoke Trigger** it allows you to run the actions such as **Application deployment evaluation**, **Software updates deployment evaluation**, **Software update source scan**, **Windows installer source list update**. You can also monitor the progress of application deployment and software update deployment by clicking on **Monitoring**. The **Cache** option gives you the information on client cache configuration and details about cache contents.



When you click on **Inventory** tab, you can **Load** the inventory data for that client. The **Invoke Trigger** invokes inventory related client actions such as File collection cycle, Discovery data collection cycle, Hardware inventory cycle, IDMIF collection cycle, Software inventory cycle and Software metering report cycle.

Configuration Manager Support Center

Data Collection Client Details Client Policy Content Inventory Troubleshooting Logs

Load Invoke Trigger Actions Status DDR File Collection HINV IDMIF SINV Metering View

Name	ID	Major Version	Minor Version	Last Collection Date	Last Report Date
Device Discovery Record	{00000000-0000-0000-0000-000000000003}	3	0	6/22/2014 1:08:04 PM	6/22/2014 1:08:04 PM
Software Inventory	{00000000-0000-0000-0000-000000000002}	0	0	6/22/2014 3:22:46 PM	1/1/1970 12:00:00 AM
File Collection	{00000000-0000-0000-0000-000000000010}	0	0	6/22/2014 3:18:43 PM	1/1/1970 12:00:00 AM
Hardware Inventory	{00000000-0000-0000-0000-000000000001}	1	1	6/22/2014 3:18:15 PM	6/22/2014 3:18:15 PM

Connection: localhost (Connected) ©PrajwalDesai.com

On the **Troubleshooting** tab, you can click on **Start troubleshooting**. This executes troubleshooting tasks listed in the left column of the below screenshot and displays the state of each task.

The screenshot shows the Configuration Manager Support Center window with the 'Troubleshooting' tab selected. On the left, there's a toolbar with icons for 'Start troubleshooting' (highlighted with a red box), 'View selected log', and 'Keep previous results'. Below the toolbar is a table listing troubleshooting tasks:

Name	Description	State
Active Directory	Active Directory queries for Configuration Manager schema items	✓
MPCERTIFICATE	Gets management point certificates	✓
MPKEYINFORMATION	Gets management point cryptographic key information	✓
MPLIST	Gets list of management points	✓
Networking	Network troubleshooter	✓
Policy Assignments	Verifies policy assignment retrieval	✓
Registration	Verifies client registration	✓

At the bottom left, it says 'Connection: localhost (Connected)'. The bottom right corner has a copyright notice: ©PrajwalDesai.com.

The last one is **Logs**. We normally use CMTrace tool to view the configuration manager log files. With this feature you can open the log file right in the same window and use filters to include or exclude the entries from the log file.

Configuration Manager Support Center

Logs (highlighted)

Log Files (highlighted)

Show details (highlighted)

Message	Date/Time	Component	Thread
BEGIN ExecuteSystemTasks('PowerChangedEx')	6/22/2014 8:56 PM	CcmExec	272 (0x110)
Invoking system task 'PwrMgmtPowerChangedEx' via ICcmSystemTask2 interface.	6/22/2014 8:56 PM	CcmExec	1916 (0x77c)
END ExecuteSystemTasks('PowerChangedEx')	6/22/2014 8:56 PM	CcmExec	272 (0x110)
SystemTaskProcessor::QueueEvent(PowerChanged, 0)	6/22/2014 8:59 PM	CCMEXEC	2004 (0x7d4)
>>> User is present	6/22/2014 8:59 PM	CCMEXEC	2004 (0x7d4)
SystemTaskProcessor::QueueEvent(PowerChanged, 0)	6/22/2014 8:59 PM	CcmExec	4416 (0x1140)
BEGIN ExecuteSystemTasks('PowerChanged')	6/22/2014 8:59 PM	CcmExec	4076 (0xfc)
Invoking system task 'PowerStateManager_PowerChanged' via ICcmSystemTask2 interface.	6/22/2014 8:59 PM	CcmExec	4076 (0xfc)
Invoking system task 'PwrMgmtPowerChanged' via ICcmSystemTask2 interface.	6/22/2014 8:59 PM	CcmExec	4076 (0xfc)
END ExecuteSystemTasks('PowerChanged')	6/22/2014 8:59 PM	CcmExec	4416 (0x1140)
BEGIN ExecuteSystemTasks('PowerChangedEx')	6/22/2014 8:59 PM	CcmExec	4076 (0xfc)
Invoking system task 'PwrMgmtPowerChangedEx' via ICcmSystemTask2 interface.	6/22/2014 8:59 PM	CcmExec	4416 (0x1140)
END ExecuteSystemTasks('PowerChangedEx')	6/22/2014 8:59 PM	CcmExec	4076 (0xfc)
Executing Task LSRefreshLocationsTask	6/22/2014 9:01 PM	LocationSe...	4416 (0x1140)
*** Keep the system awake	6/22/2014 9:11 PM	CcmExec	2968 (0xb98)
*** System is now free to go to sleep	6/22/2014 9:11 PM	CcmExec	2968 (0xb98)
Executing Task LSRefreshLocationsTask	6/22/2014 9:13 PM	LocationSe...	2732 (0xaac)

Executing Task LSRefreshLocationsTask

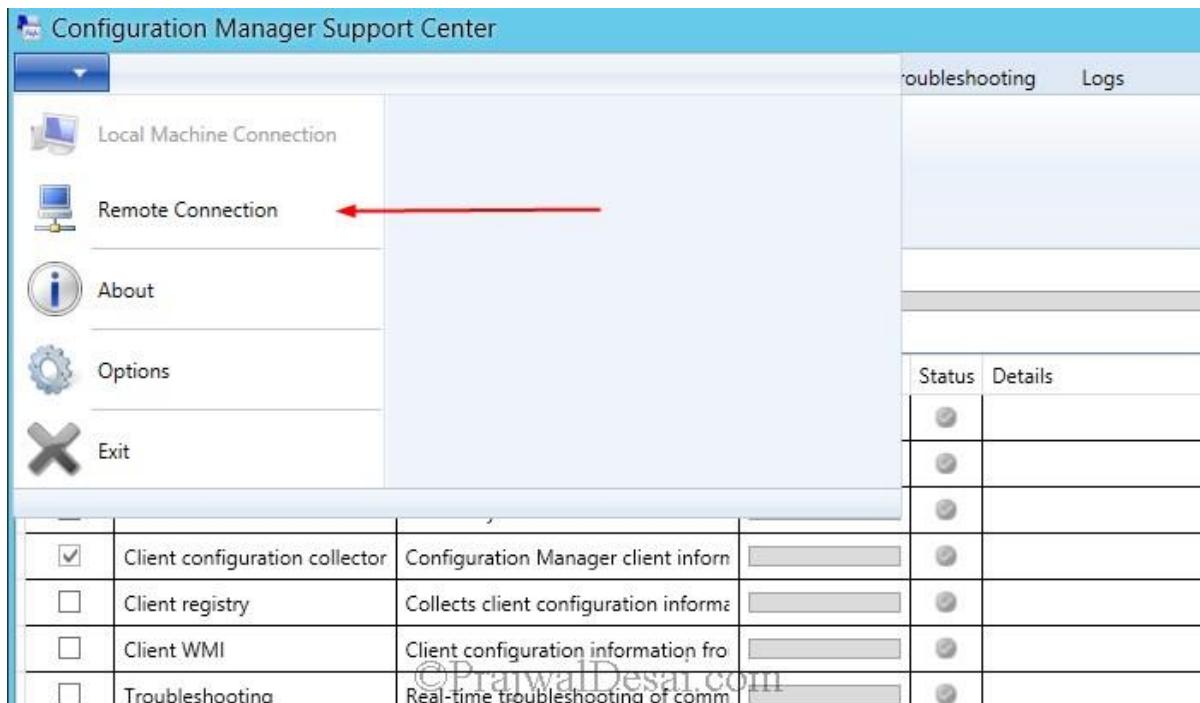
Timestamp: 6/22/2014 9:13 PM **Component:** LocationServices
Thread: 2732 (0xaac) **Level:** Info
Source: scheduledcleanupendpoint.cpp:116 **Context:**
Filename: C:\Program Files\SMS_CCM\Logs\LocationServices.log:747

Entry 2489 of 2489

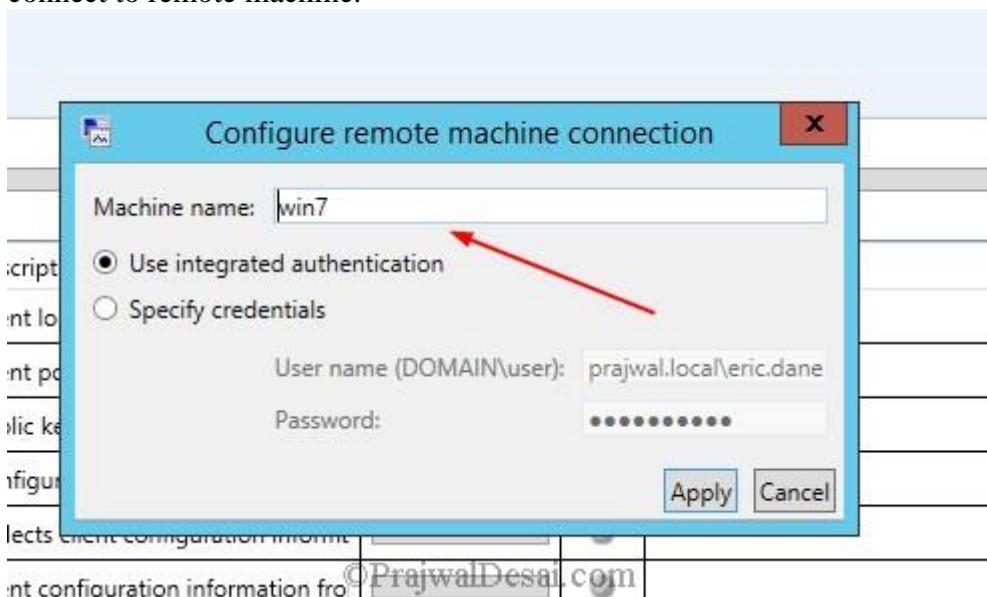
Connection: localhost (Connected)

©PrajwalDesai.com

One of the cool feature of this tool is you can connect to remote machine using an option called **Remote Connection**.



Provide the remote machine name (IP address also works here). Specify the credentials to connect to remote machine and click **Apply**. You can also use Integrated Authentication to connect to remote machine.



Overall this is a very good tool and I can say it's a All in One tool that can be used for troubleshooting sccm client related issues.

How to deploy Internet Explorer 11 using SCCM 2012 R2

Deploy Internet Explorer 11 using SCCM 2012 R2 In this post we will see how to deploy internet explorer 11 using SCCM 2012 R2. Internet Explorer is installed when you install the windows operating system and is the default browser for any windows OS. Today most of the companies use Windows 7 as the OS and IE 10 as the browser, with the release of Internet Explorer 11, the companies might be looking to upgrade their browser version from IE10 to IE11. The internet Explorer 11 offers better features than IE10 and is more faster and smoother when compared to IE10. Note that the Internet Explorer 11 is available for a number of systems and languages. Internet Explorer 11 is pre-installed on Windows 8.1 and Windows Server 2012 R2. There are multiple ways on deploying internet explorer 11 and they are listed below.

System Center R2 2012 Configuration Manager – Deploy and install Internet Explorer 11 on your user's computers through a software distribution package.

Windows Server Update Services (WSUS) – Download a single copy of the Internet Explorer 11 updates, caching them to local servers so your users' computers can receive the updates directly from the WSUS servers, instead of through Windows Update.

Group Policy Software Installation – Deploy and install Internet Explorer 11 on your user's computers through a combination of Group Policy and Active Directory.

Microsoft Deployment Toolkit (MDT) – Add the Internet Explorer 11 update to your deployment share, using MDT to update your previously-deployed Windows image.

In this post we will see the steps to deploy the IE11 using SCCM 2012 R2 on a Windows 7 computer. We will download the [Internet Explorer Administration Kit 11](#) first. Internet Explorer Administration Kit 11 (IEAK 11) simplifies the creation, deployment, and management of customized Internet Explorer 11 packages. It can be used to configure the out-of-box Internet Explorer 11 experience, and to manage user settings after deployment.



Internet Explorer Administration Kit 11

Language: English

[Download](#)

Internet Explorer Administration Kit 11 (IEAK 11) simplifies the creation, deployment, and management of customized Internet Explorer 11 packages. It can be used to configure the out-of-box Internet Explorer 11 experience, and to manage user settings after deployment.

[Details](#)

[System Requirements](#)

[Install Instructions](#)

[Additional Information](#)

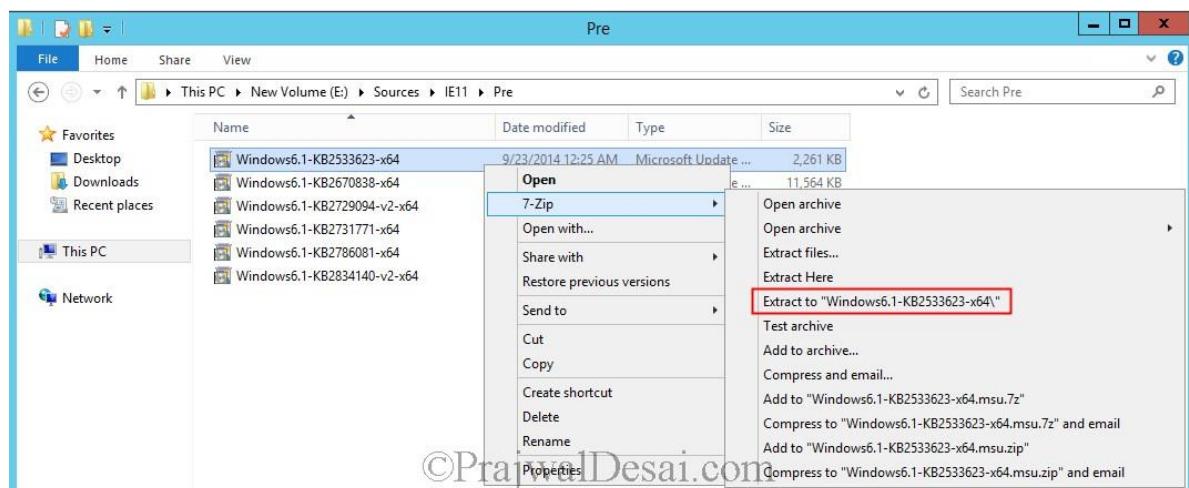
[Related Resources](#)

©PrajwalDesai.com

When you install Internet Explorer 11 for Windows 7, the installer program tries to automatically install some prerequisite components. If this part of the installation fails, Internet Explorer stops the installation process. We will download the prerequisites first and then install IEAK 11. To download the IE 11 prerequisites click on the below button.

[Prerequisite updates for Internet Explorer 11](#)

The prerequisites are available for both 32 bit and 64 bit OS, download the appropriate files depending on whether you are running a 32-bit or 64-bit edition of the operating system. Download the files and extract each update to a folder using 7zip.



The below screenshot shows the updates extracted to each folder.

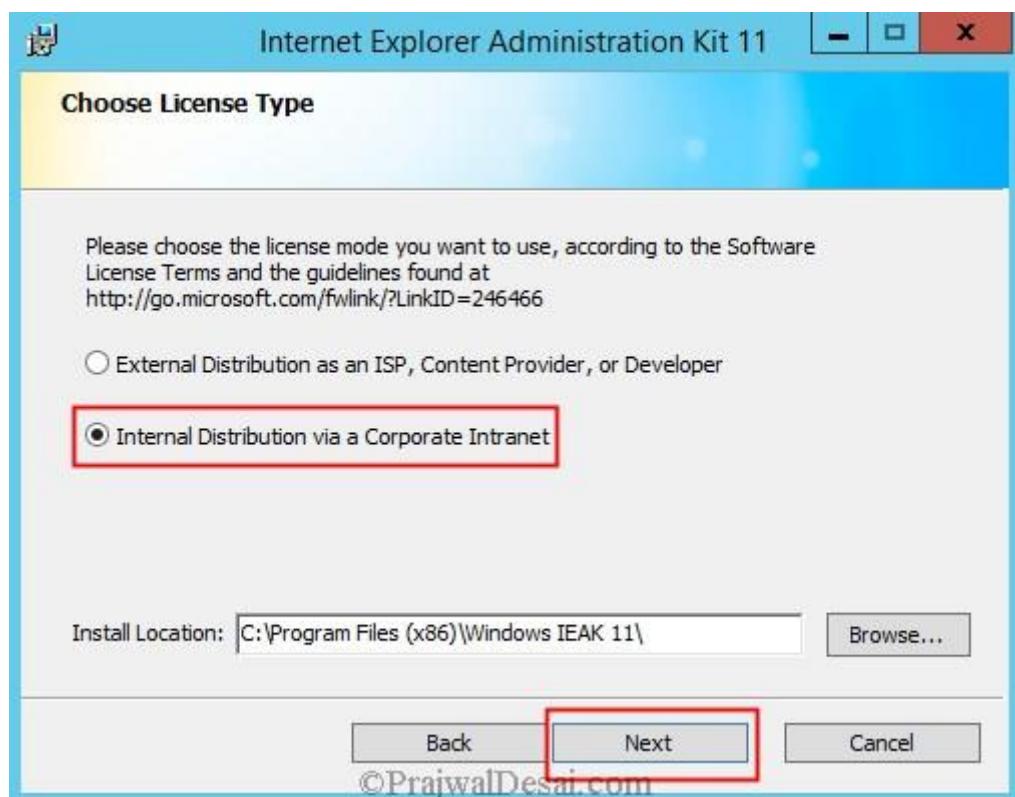
©PrajwalDesai.com

	Name	Date modified	Type	Size
	Windows6.1-KB2533623-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2670838-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2729094-v2-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2731771-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2786081-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2834140-v2-x64	9/23/2014 12:36 AM	File folder	
	Windows6.1-KB2533623-x64	9/23/2014 12:25 AM	Microsoft Update ...	2,261 KB
	Windows6.1-KB2670838-x64	9/23/2014 12:26 AM	Microsoft Update ...	11,564 KB
	Windows6.1-KB2729094-v2-x64	9/23/2014 12:25 AM	Microsoft Update ...	1,625 KB
	Windows6.1-KB2731771-x64	9/23/2014 12:25 AM	Microsoft Update ...	6,427 KB
	Windows6.1-KB2786081-x64	9/23/2014 12:25 AM	Microsoft Update ...	231 KB
	Windows6.1-KB2834140-v2-x64	9/23/2014 12:25 AM	Microsoft Update ...	981 KB

Install the Internet Explorer Administration Kit 11 on SCCM server or any computer you want. The below listed screenshots shows the installation of IEAK 11, you can skip these if you are familiar with the installation. Click **Next**.



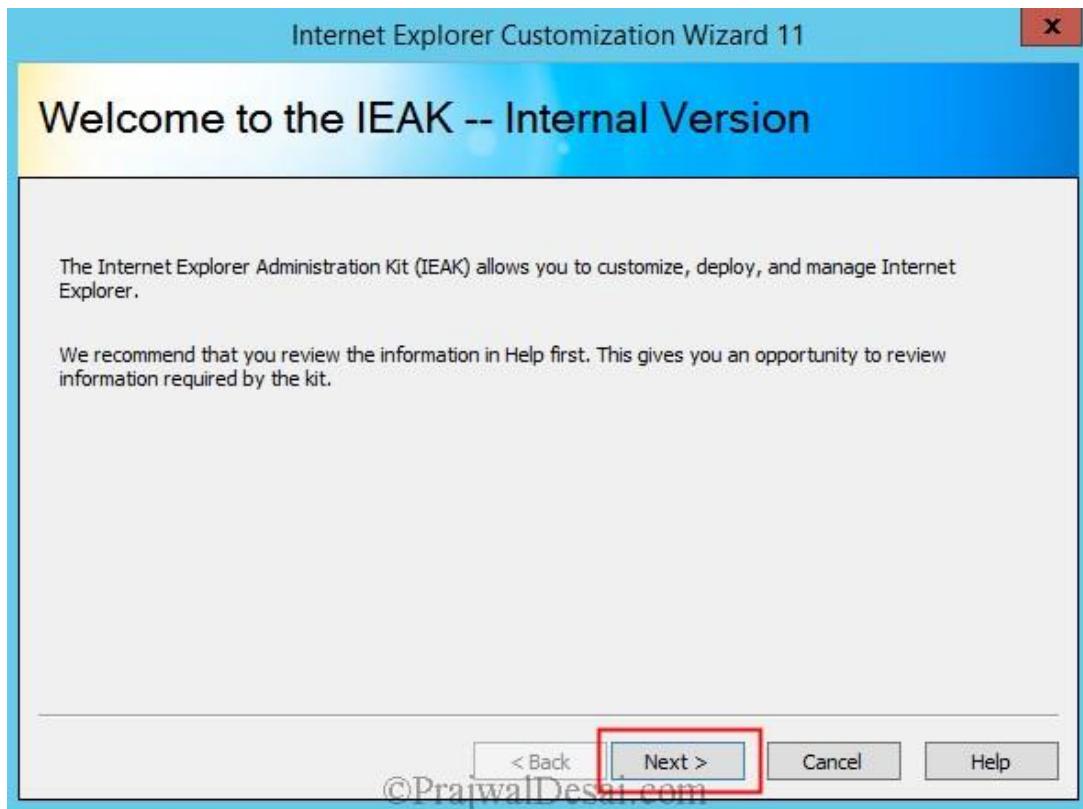
Choose **Internal Distribution via a Corporate Intranet**. Click **Next**.



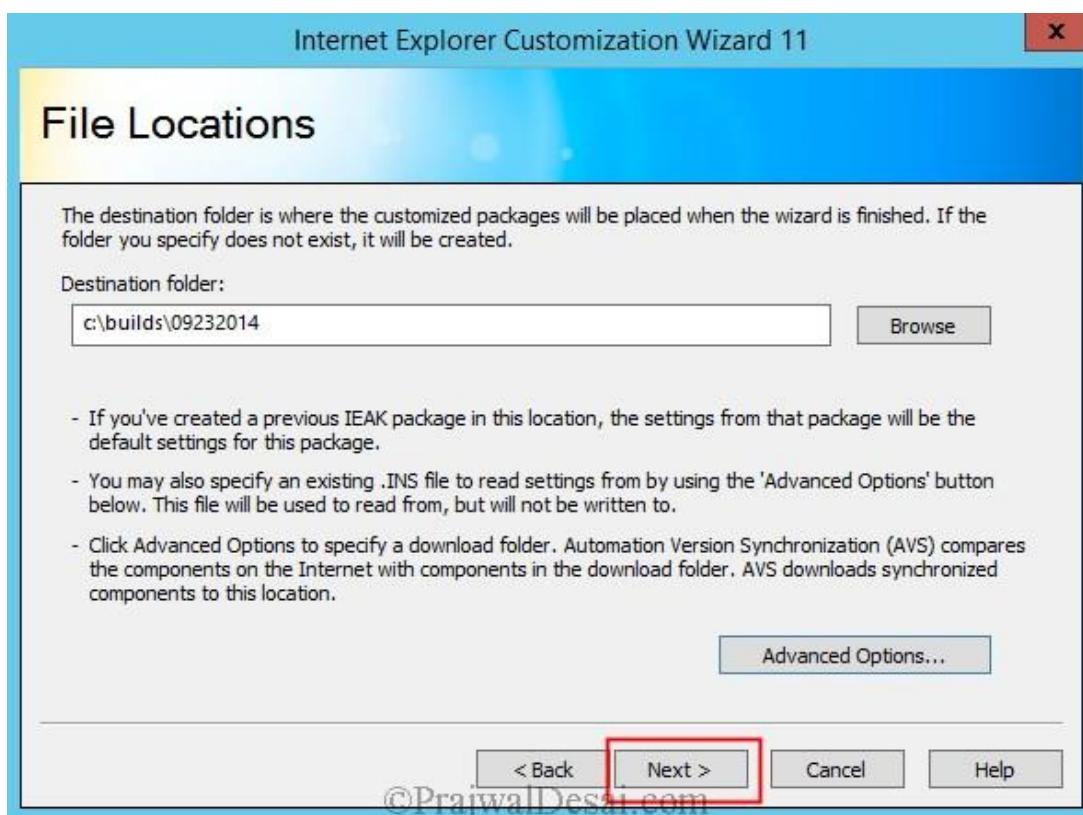
Complete the installation and click **Finish**.



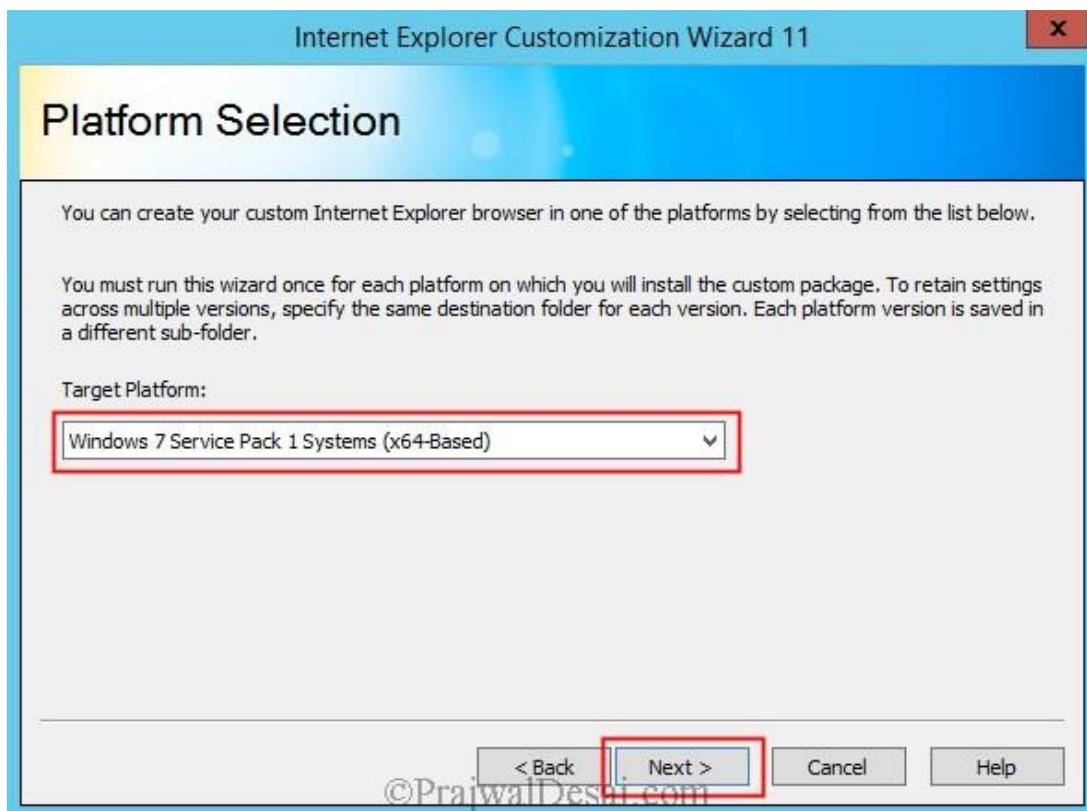
Now the IEAK 11 customization wizard pops up, this wizard will help you to customize, deploy and manage IE. Click **Next**.



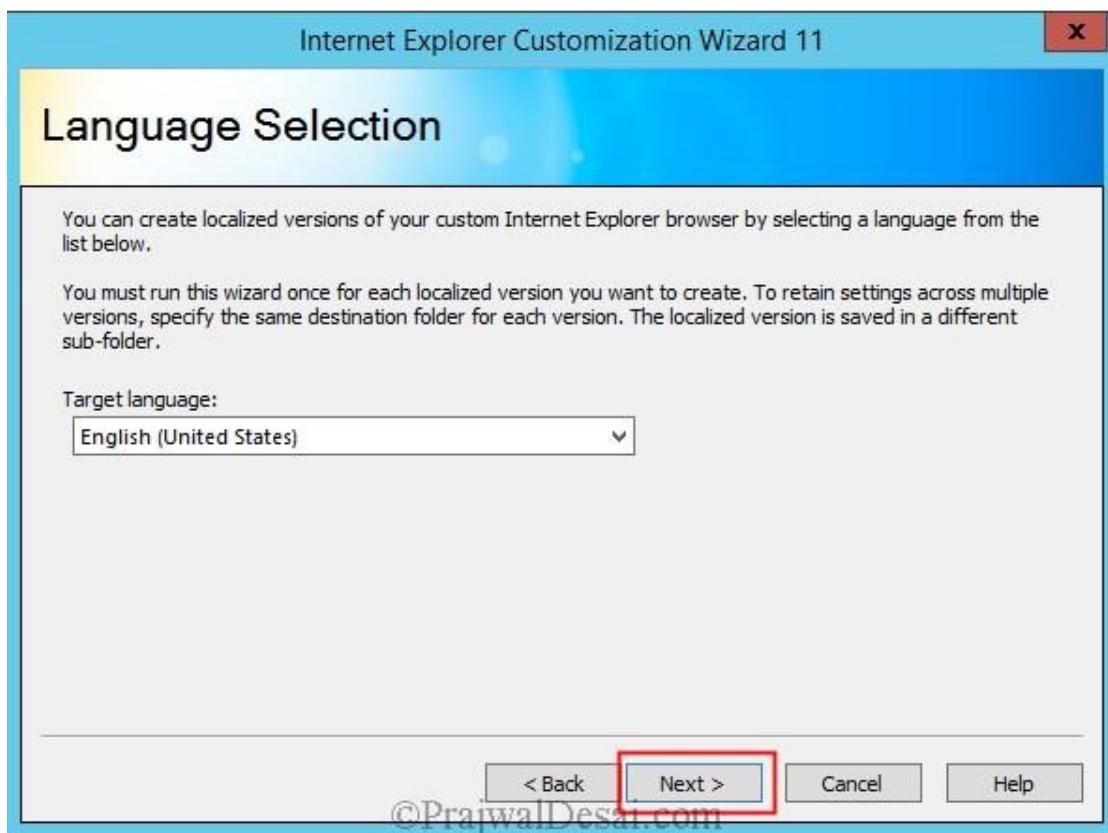
Choose the location where you want to store the package. Click **Next**.



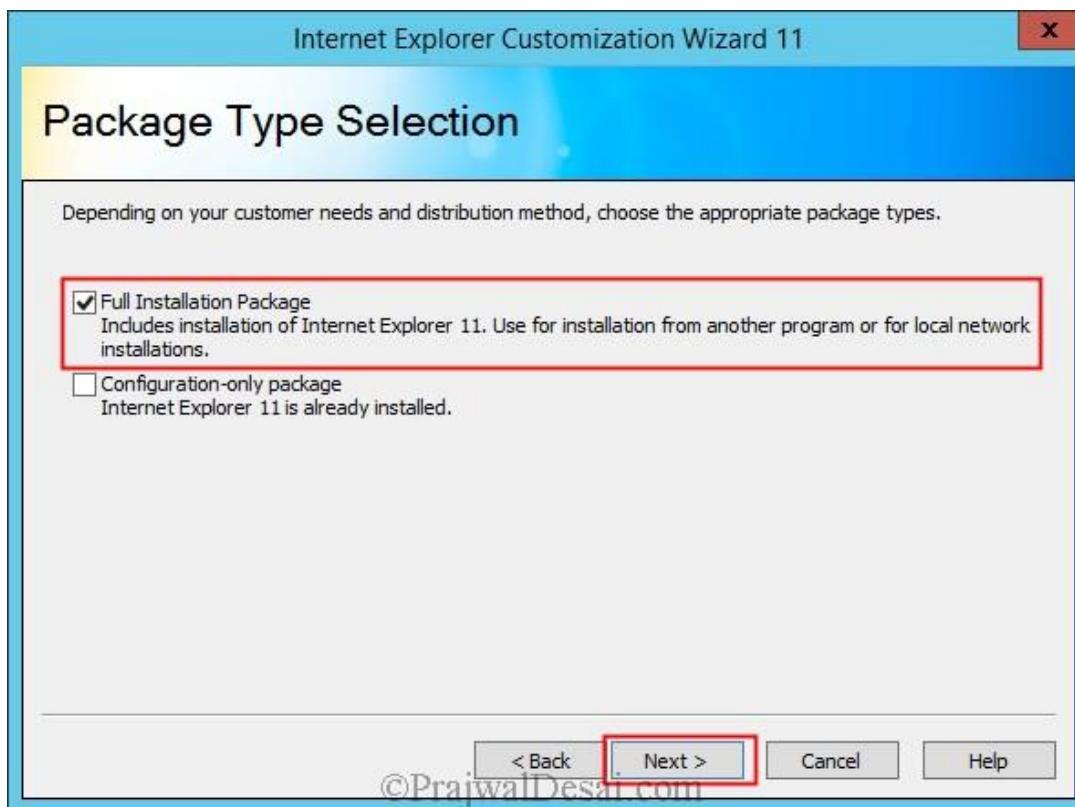
Choose the **Target Platform** and click **Next**.



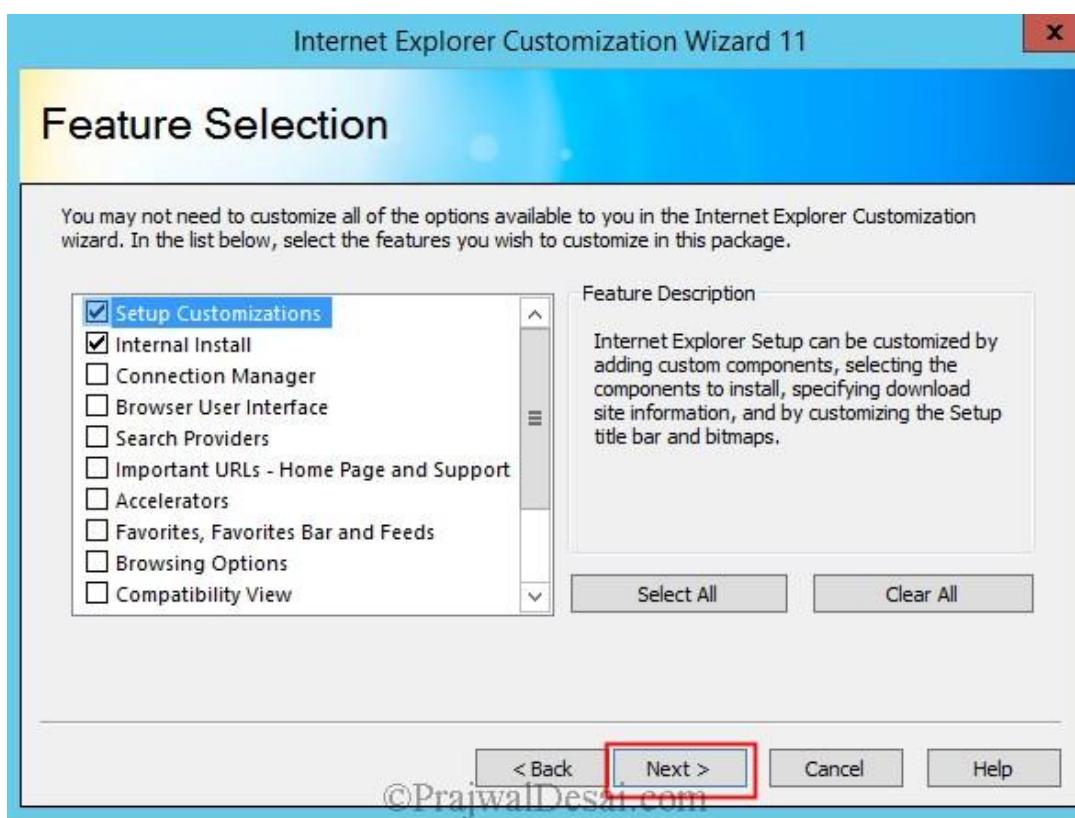
Choose the **Target Language** and click **Next**.



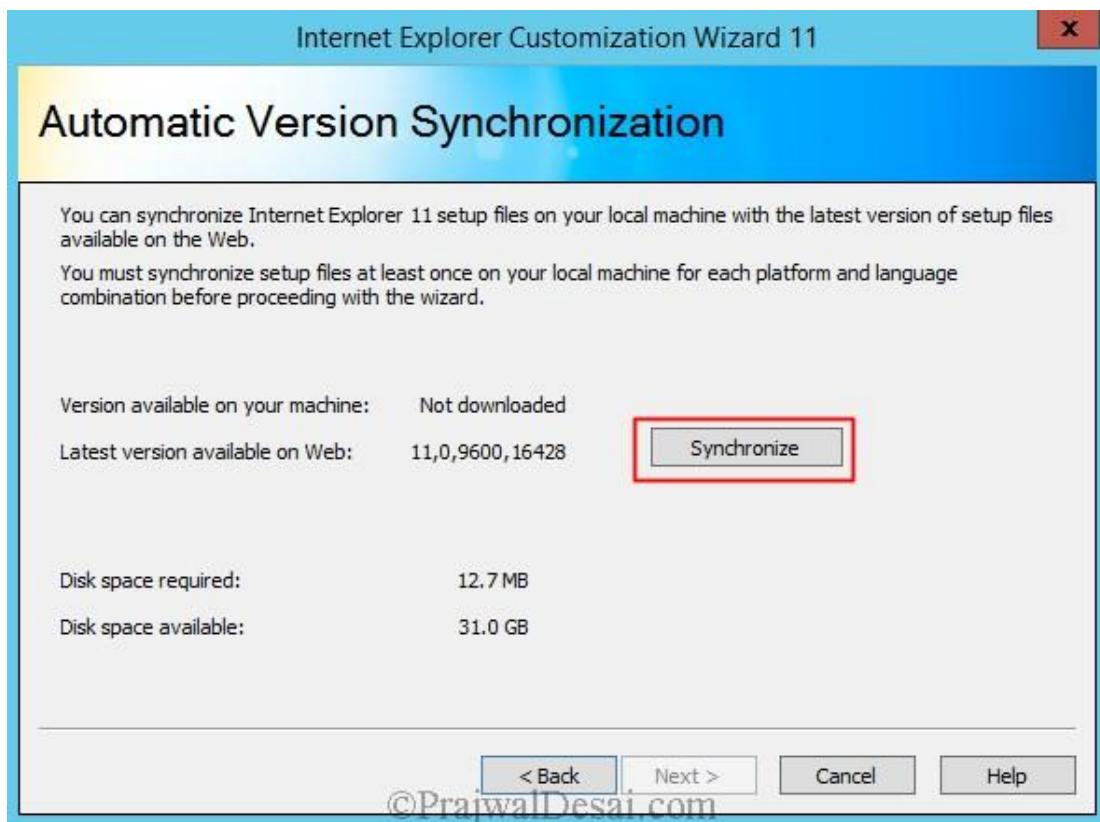
Package Type Selection – Click Full Installation Package. Click Next.



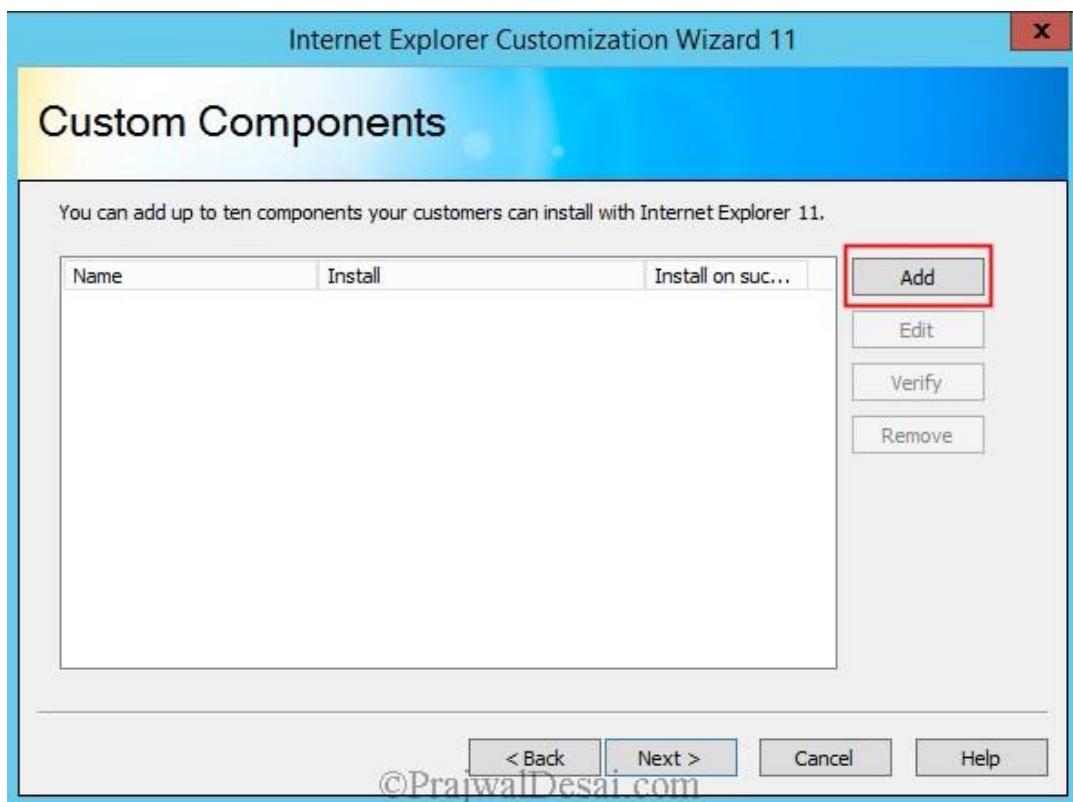
You can choose all the features and customize them as per your requirement. Select the IE11 features that you wish to customize and click **Next**.



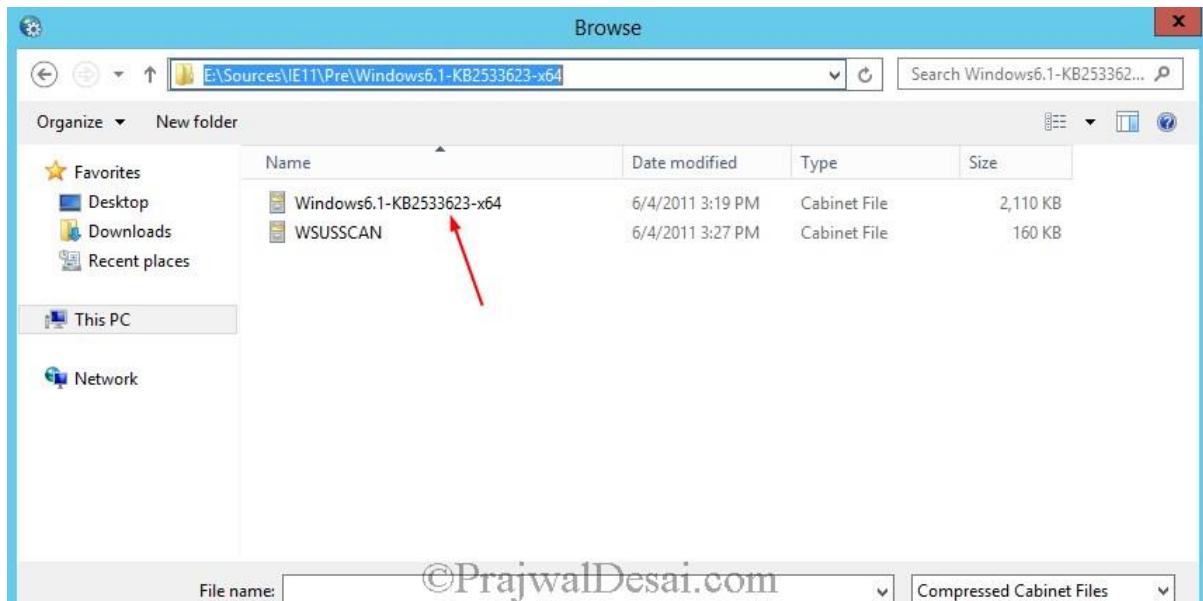
Click on **Synchronize**.



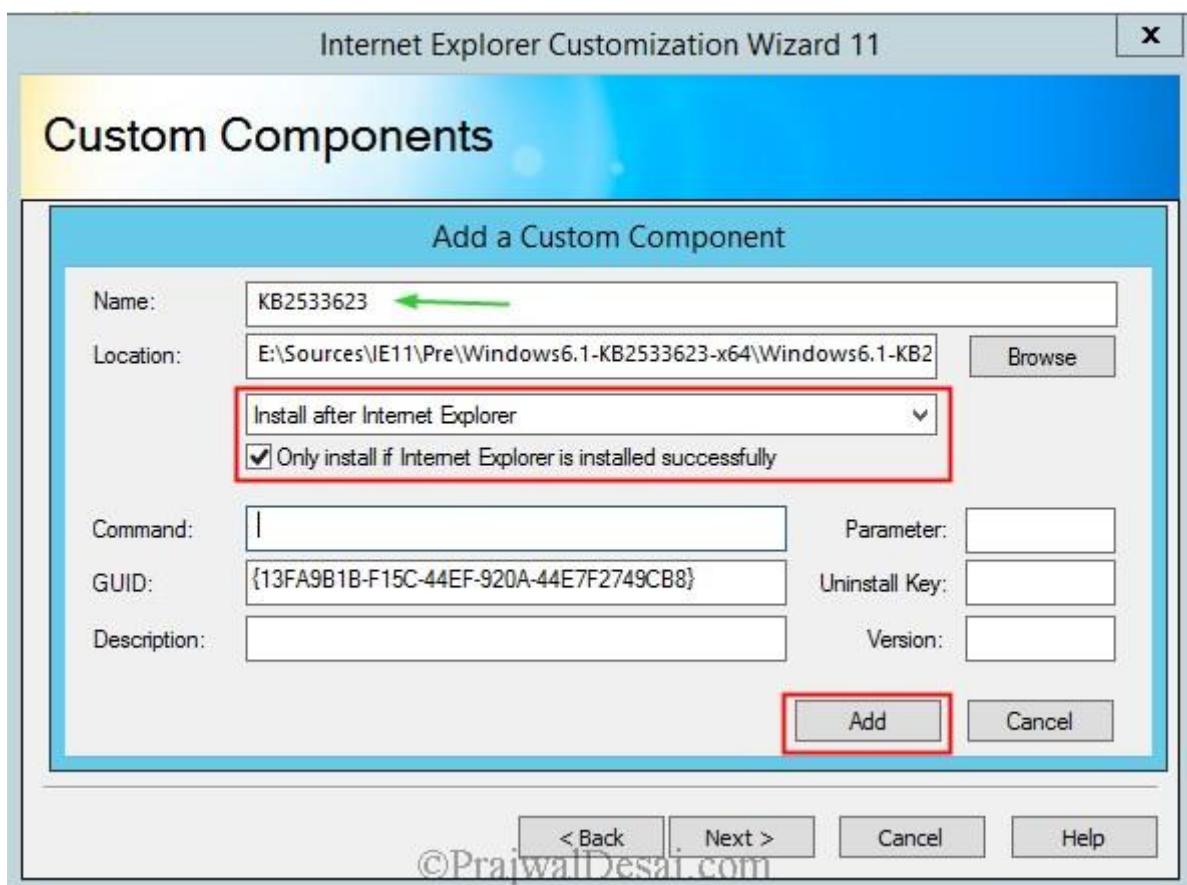
Now we know that IE11 requires certain prerequisites which we have download already. Let's add them to custom components. Click on **Add**.



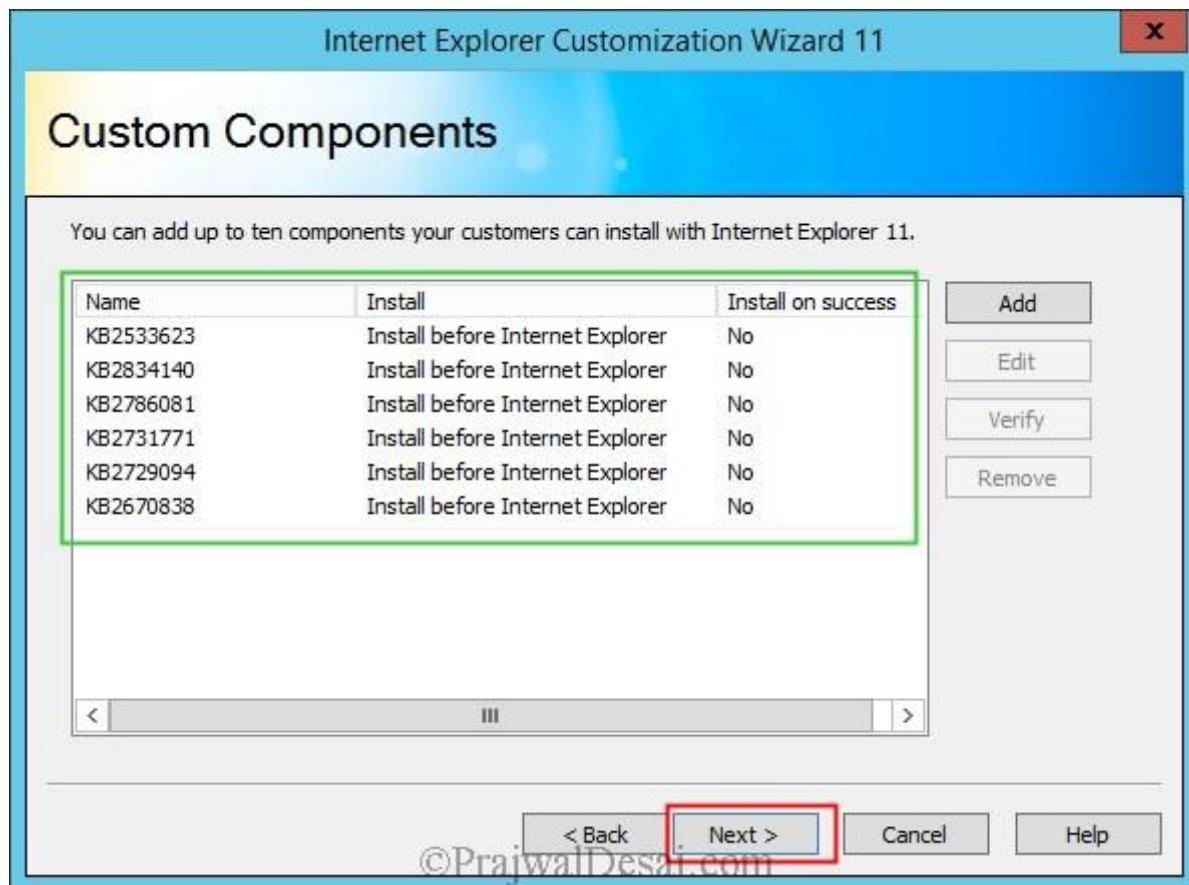
For every KB update go to the individual update folder and select the cabinet file.



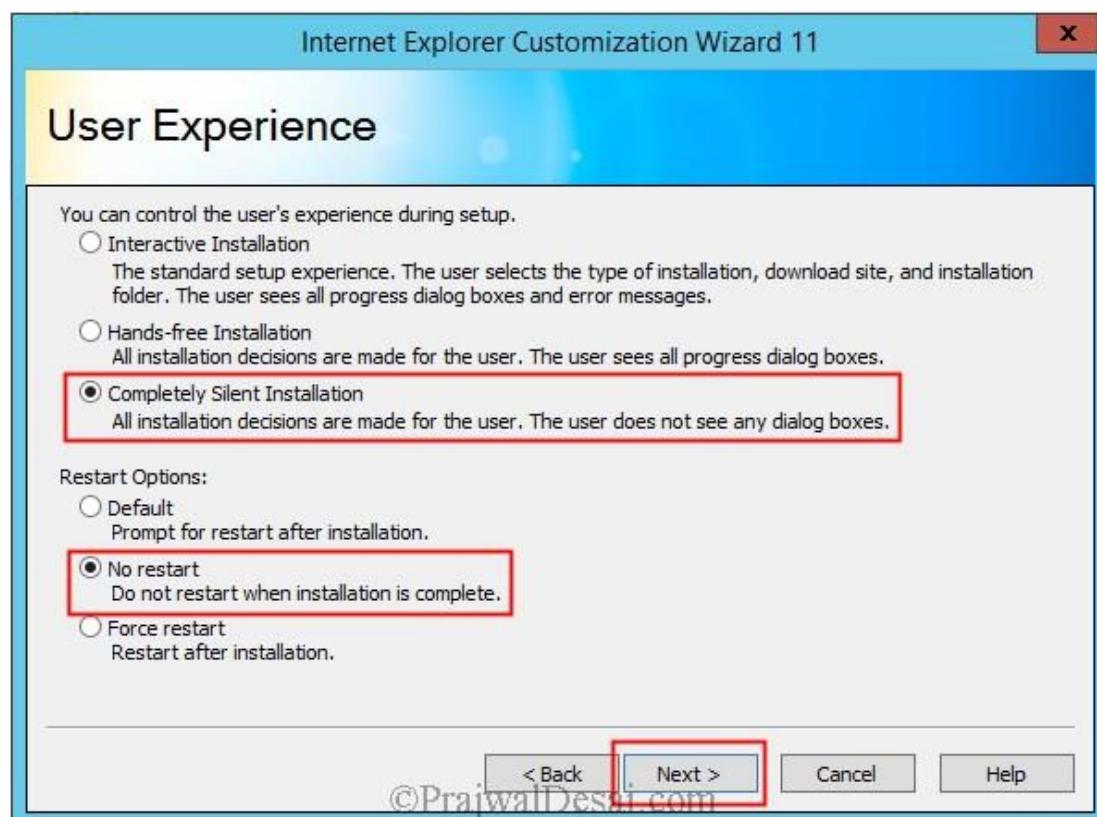
Provide the name for that component (provide KB number as its easy to identify the update), choose **Install before Internet Explorer** (we want the updates to be installed before IE11 is installed) and click **Add**.



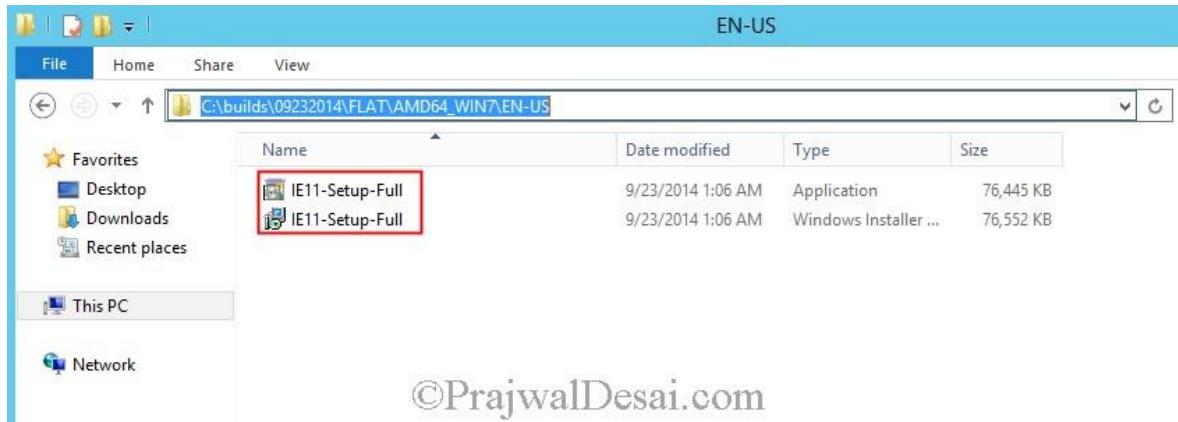
When you have added all the components, it should resemble the below screenshot. Click **Next**.



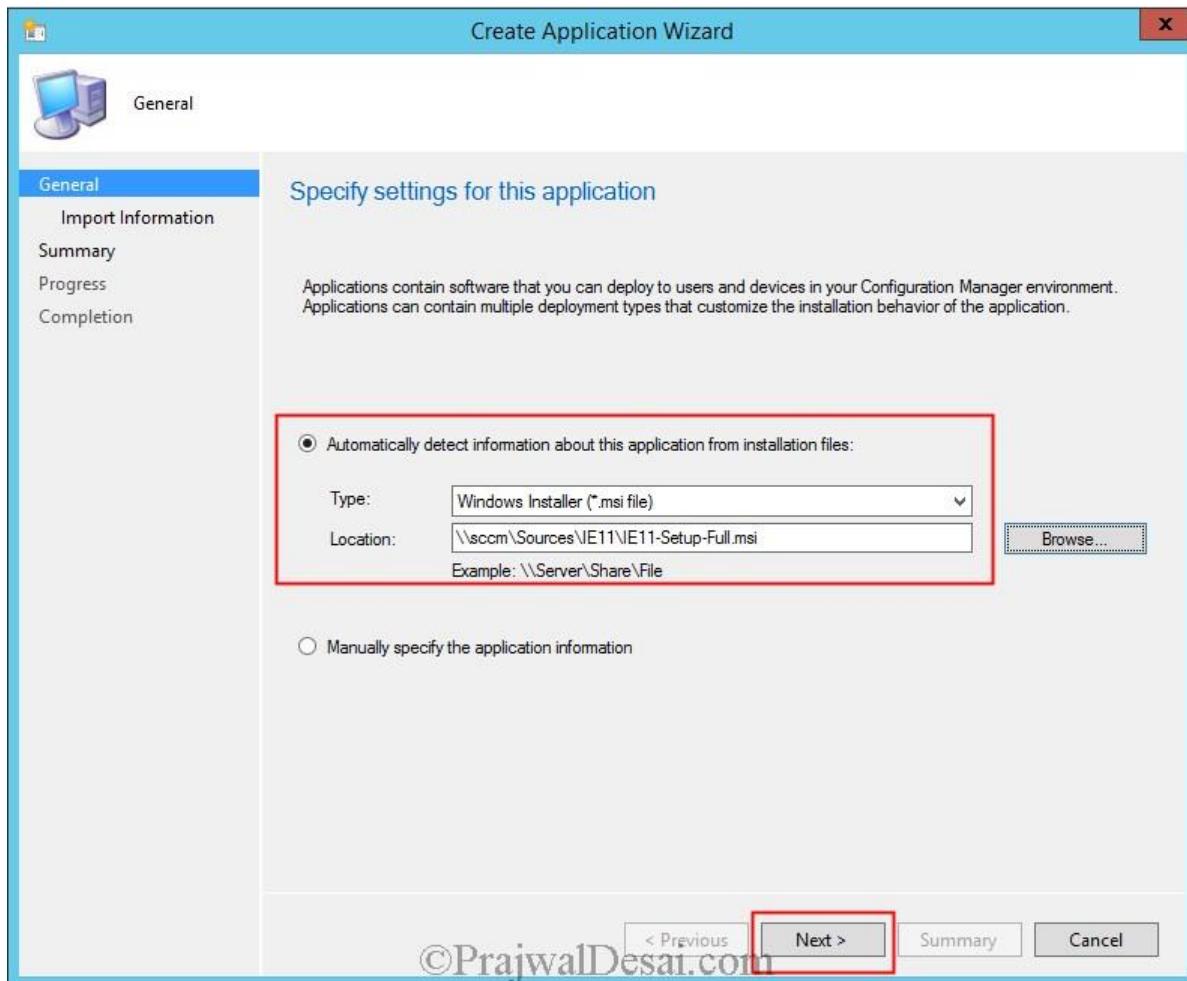
User Experience – Choose Completely Silent Installation and No restart. Click Next and complete the wizard.



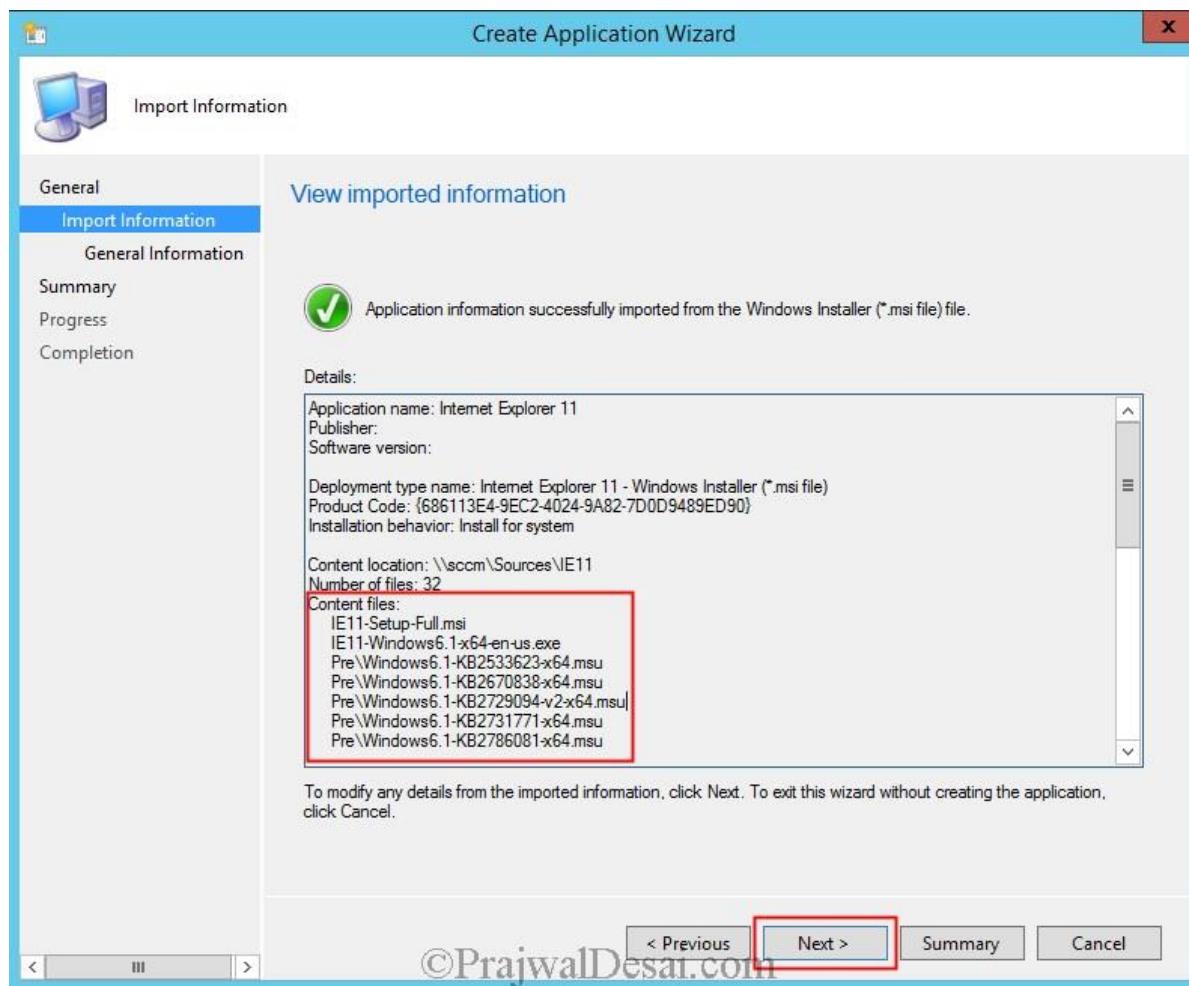
When you open the destination folder you will see the IE11 package. One of them is an app and other one is windows installer package (.msi).



In the above step we have got the .msi file, we will now create an application and choose the IE11 msi file and click **Next**.



Click **Next**. Deploy the app to the device collection.



Now on the client computer we see that the app is available. Click on **Install**.

The screenshot shows the Software Center interface. The title bar says "Software Center" and "IT Organization". The tabs at the top are "Available Software" (selected), "Installation Status", "Installed Software", and "Options". Below the tabs are filters: "SHOW All" dropdown, "Show optional software" checkbox checked, and a "SEARCH" input field with a magnifying glass icon. A link "Find additional applications from the Application Catalog" is also present. The main table has columns: NAME, TYPE, PUBLISHER, AVAILABL..., and STATUS. One item is listed: "Internet Explorer 11" (Application, Microsoft, Available). The details for "Internet Explorer 11" are shown in a modal window. The "OVERVIEW" section includes: Status: Available, Version: Not specified, Date published: Not specified, Help document: None. The "REQUIREMENTS" section includes: Restart required: Might be required, Download size: 173 MB, Estimated time: Not specified, Total components: 1. The "DESCRIPTION" section states: Deployed by sccmadmin. At the bottom right of the modal is a red-bordered "INSTALL" button.

©PrajwalDesai.com

Wait for some time while the installation is completed. Check the **AppEnforce.log** file on client computer for troubleshooting. We see that the IE11 is installed successfully. Though we had suppressed the reboot during the creation of package,

I would recommend to reboot the client computer once.

The screenshot shows two windows. The top window is titled "Software Center" and has tabs for "Available Software", "Installation Status" (which is selected), "Installed Software", and "Options". It displays a table of software packages with columns for Name, Type, Publisher, Availability Date, and Status. Two entries are shown: "7-Zip 9.20 (x64 edition)" and "Internet Explorer 11". Red arrows point from the status column to the "Installed" status of both entries. The bottom window is titled "Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\AppEnforce.log]" and shows a log of events. The log text includes messages about MSI application discovery, command line execution, working directory preparation, executable file finding, command line preparation, package validation, advertising, command execution, working directory setting, post-install behavior, process waiting, process termination, exit code matching, success entry detection, and finally the completion of app enforcement. A red arrow points to the first line of the log: "+++ MSI application not discovered [MSI Product Code: {686113E4-.... AppEnforce".

NAME	TYPE	PUBLISHER	AVAILABL...	STATUS
7-Zip 9.20 (x64 edition)	Application	7-Zip	9/23/2014	Installed
Internet Explorer 11	Application	Microsoft	9/23/2014	Installed

Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\AppEnforce.log]

Log Text	Component	Date/Time	Thread
+++ MSI application not discovered [MSI Product Code: {686113E4-.... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
App enforcement environment: Context: MachineCommand line:... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Prepared working directory: C:\Windows\ccmcache\2 AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Found executable file msiexec with complete path C:\Windows\syst... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Prepared command line: "C:\Windows\system32\msiexec.exe" /i ... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Valid MSI Package path = C:\Windows\ccmcache\2\IE11-Setup-Full... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Advertising MSI package [C:\Windows\ccmcache\2\IE11-Setup-F... AppEnforce	AppEnforce	9/23/2014 1:22:21 AM	2368 (0x940)
Executing Command line: "C:\Windows\system32\msiexec.exe" /i... AppEnforce	AppEnforce	9/23/2014 1:22:24 AM	2368 (0x940)
Working directory C:\Windows\ccmcache\2 AppEnforce	AppEnforce	9/23/2014 1:22:24 AM	2368 (0x940)
Post install behavior is BasedOnExitCode AppEnforce	AppEnforce	9/23/2014 1:22:24 AM	2368 (0x940)
Waiting for process 2988 to finish. Timeout = 120 minutes. AppEnforce	AppEnforce	9/23/2014 1:22:24 AM	2368 (0x940)
Process 2988 terminated with exitcode: 0 AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)
Looking for exit code 0 in exit codes table... AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)
Matched exit code 0 to a Success entry in exit codes table. AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)
Performing detection of app deployment type Internet Explorer 1.... AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)
+++ Discovered MSI application [AppDT Id: ScopeId_57E4FF17-3A2... AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)
***** App enforcement completed (154 seconds) for App DT in... AppEnforce	AppEnforce	9/23/2014 1:24:56 AM	2368 (0x940)

How to Uninstall SCEP Client using SCCM 2012 R2

How to Uninstall SCEP Client using SCCM 2012 R2 In this post we will see how to uninstall SCEP client using SCCM 2012 R2. I have been asked most of the times in my [ticketing tool](#) on what is the easiest way to uninstall the System center Endpoint protection client from windows computer. Most of the admins prefer to uninstall the SCEP client using group policy or a logon script. Well, I believe that method works fine however I wanted to uninstall the SCEP client using SCCM. We will now create a script that uninstalls the SCEP client from Windows computers. We will basically create a package and add the script to that package and then deploy it to computers.

Create a new text document and rename it to “**Uninstall MEP.bat**“. Right click the batch file and edit with Notepad. Now add the below code to the batch file and save the file. Let me tell you this is a very simple code and works correctly.

Uninstall SCEP Client

```
1 @echo off  
2 C:\Windows\ccmsetup\scepinstall.exe /u /s
```

If you are looking for a script that cleans up all the files associated with SCEP client then use the below script. I have had less success with the below script :). In this post I will be using the first code for uninstalling SCEP Clients.

Uninstall SCEP Script

```
cd /d "%ProgramFiles%\Microsoft Security Client"  
TASKKILL /f /im MsMpEng.exe  
TASKKILL /f /im msseces.exe  
TASKKILL /f /im MpCmdRun.exe  
  
net stop MsMpSvc  
  
sc delete MsMpSvc  
  
REG DELETE "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MsMpSvc" /f  
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware" /f  
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Security Client" /f  
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Antimalware" /f  
REG DELETE "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\MSC" /f  
REG DELETE "HKEY_CLASSES_ROOT\Installer\Products\4C677A77F01DD614880F352F9DCD9D3B" /f  
REG DELETE "HKEY_CLASSES_ROOT\Installer\Products\4D880477777087D409D44E533B815F2D" /f
```

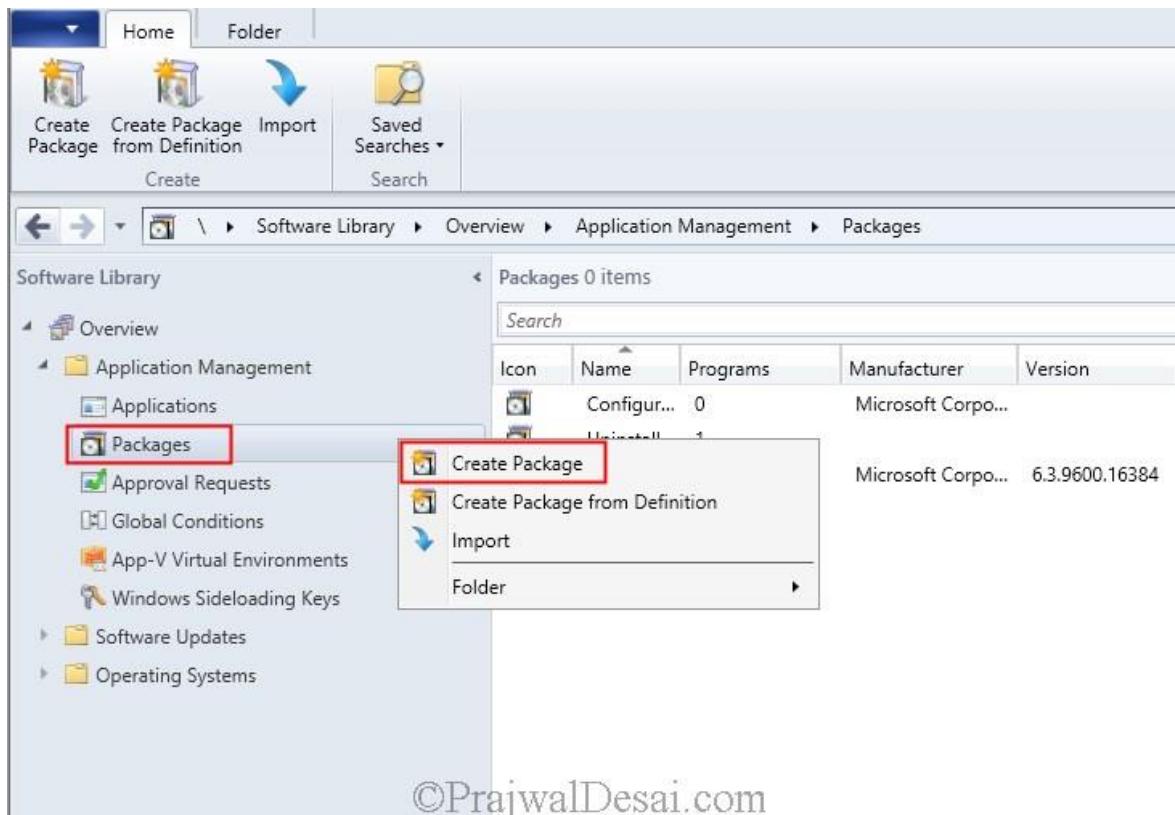
```
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Security Client" /f
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{774088D4-0777-4D78-904D-E435B318F5D2}" /f
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{77A776C4-D10F-416D-88F0-53F2D9DCD9B3}" /f
REG DELETE "HKEY_CLASSES_ROOT\Installer\UpgradeCodes\1F69ACF0D1CF2B7418F292F0E05EC20B" /f
REG DELETE "HKEY_CLASSES_ROOT\Installer\UpgradeCodes\11BB99F8B7FD53D4398442FBBAEF050F" /f
REG DELETE "HKEY_CLASSES_ROOT\Installer\UpgradeCodes\26D13F39948E1D546B0106B5539504D9" /f
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\4C677A77F01DD614880F352F9DCD9D3B" /f
REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\4D88047777087D409D44E533B815F2D" /f
REG DELETE
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UpgradeCodes\11BB99F8B7FD53D4398442FBBAEF050F" /f
REG DELETE
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UpgradeCodes\1F69ACF0D1CF2B7418F292F0E05EC20B" /f
takeown /f "%ProgramData%\Microsoft\Microsoft Antimalware" /a /r
takeown /f "%ProgramData%\Microsoft\Microsoft Security Client" /a /r
takeown /f "%ProgramFiles%\Microsoft Security Client" /a /r
REM Delete the MSE folders.
rmdir /s /q "%ProgramData%\Microsoft\Microsoft Antimalware"
rmdir /s /q "%ProgramData%\Microsoft\Microsoft Security Client"
rmdir /s /q "%ProgramFiles%\Microsoft Security Client"
REM Stop the WMI and its dependency services
sc stop sharedaccess
sc stop mpssvc
sc stop wscsvc
sc stop iphlpsvc
sc stop winmgmt
REM Delete the Repository folder.
rmdir /s /q "C:\Windows\System32\wbem\Repository"
```

```
sc stop
```

```
PAUSE
```

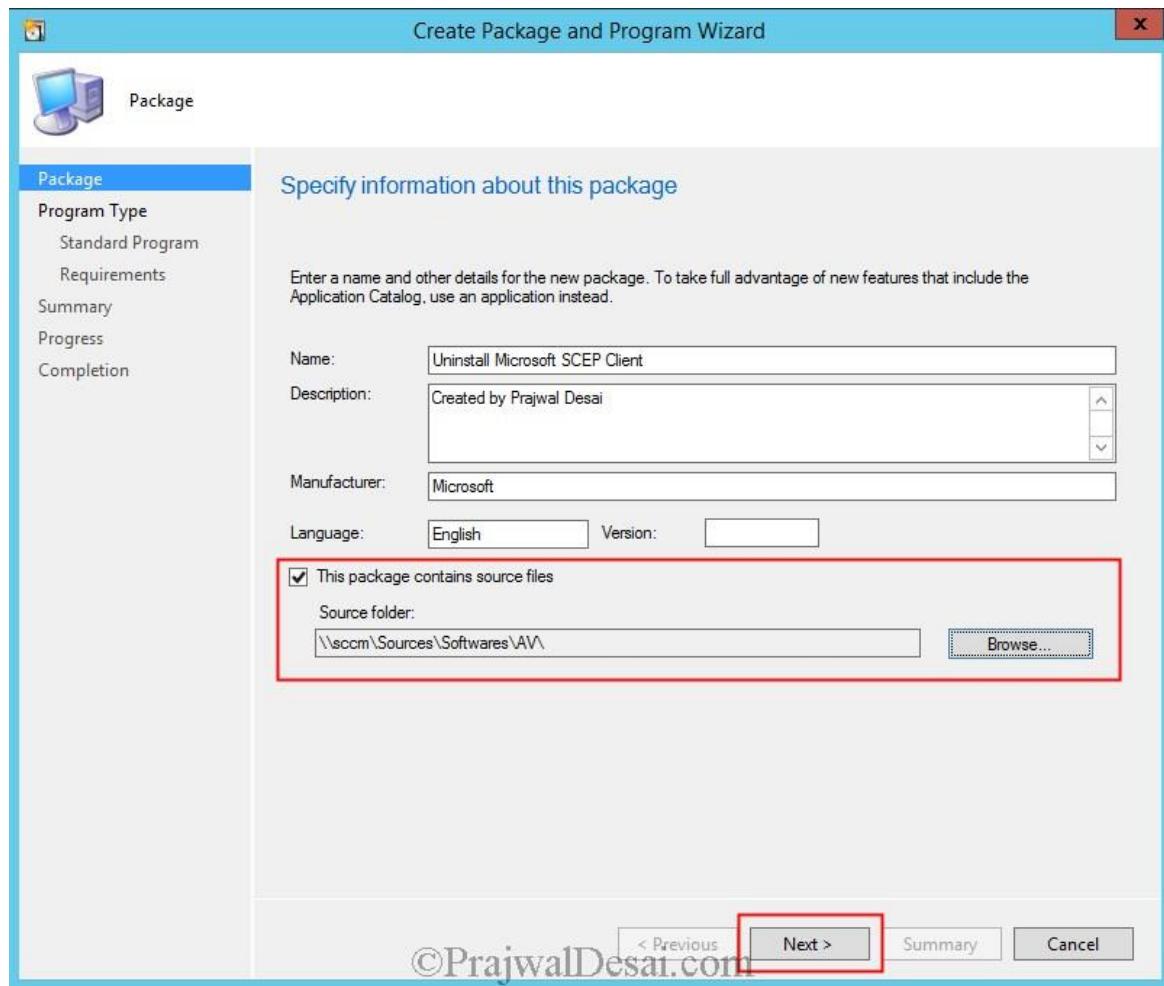
```
EXIT
```

After you are ready with the batch file, create a new package in SCCM. Right click **Packages** and click **Create Package**.

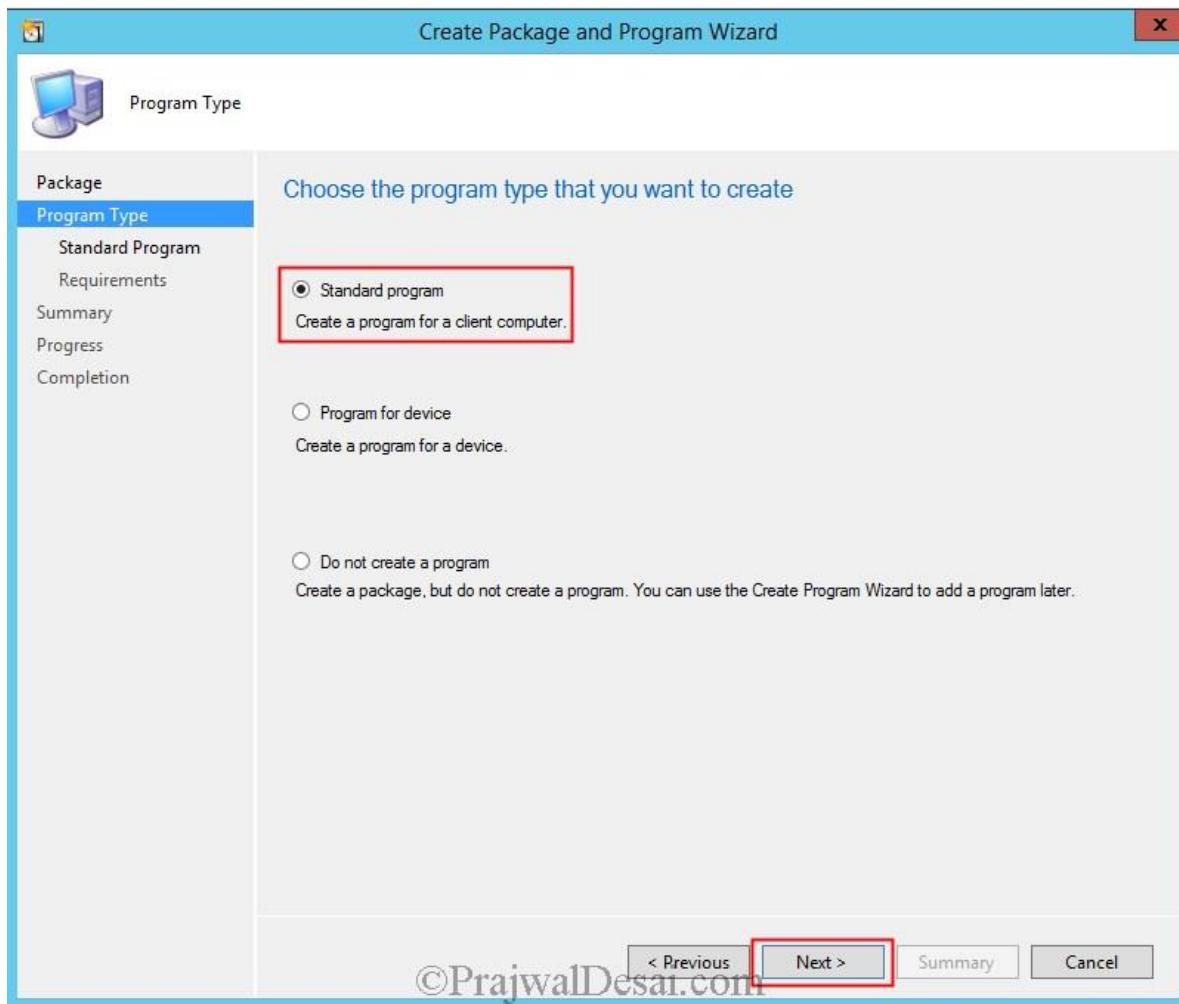


©PrajwalDesai.com

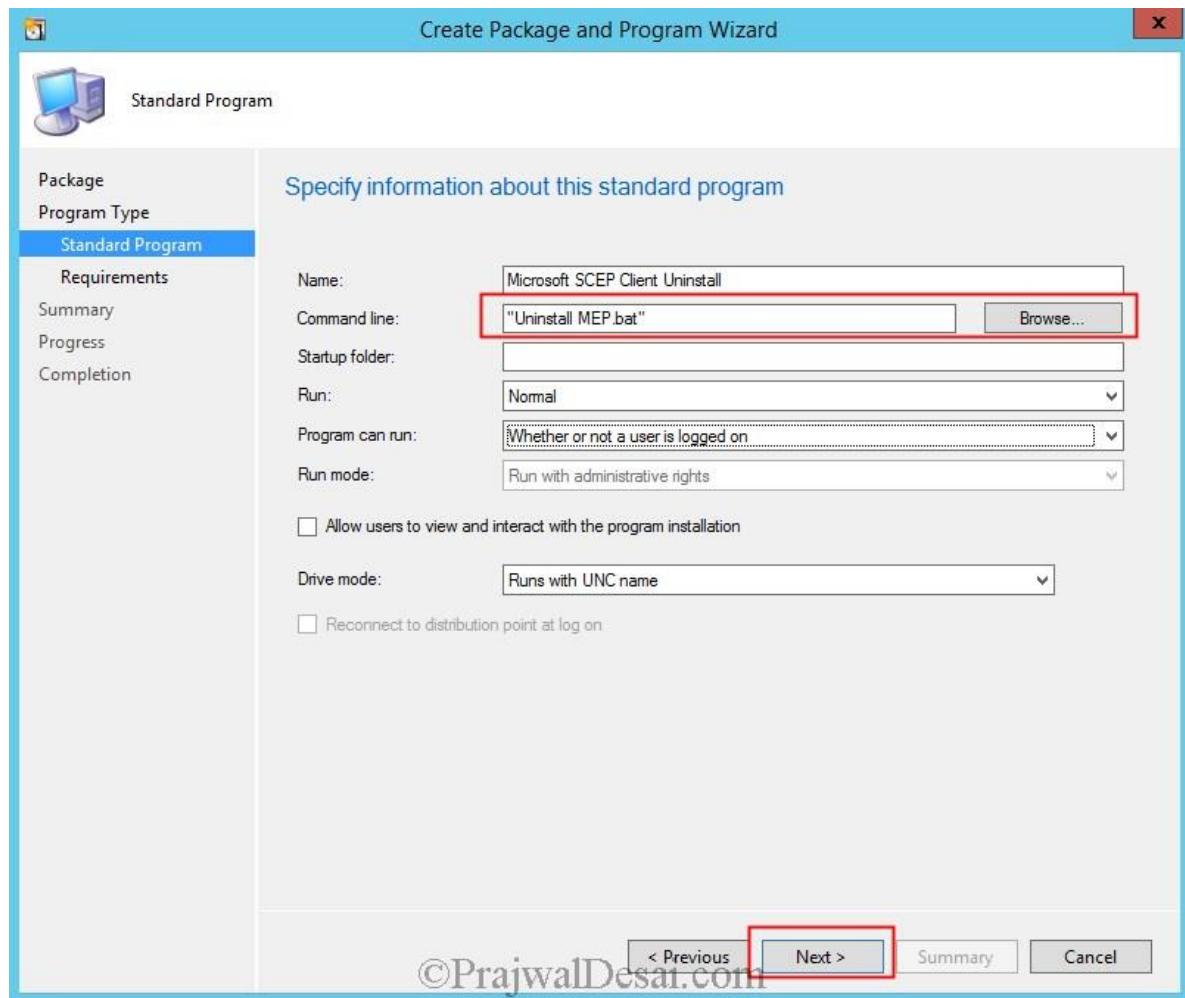
Specify the name for the package and browse to the folder where the script is located. Click **Next**.



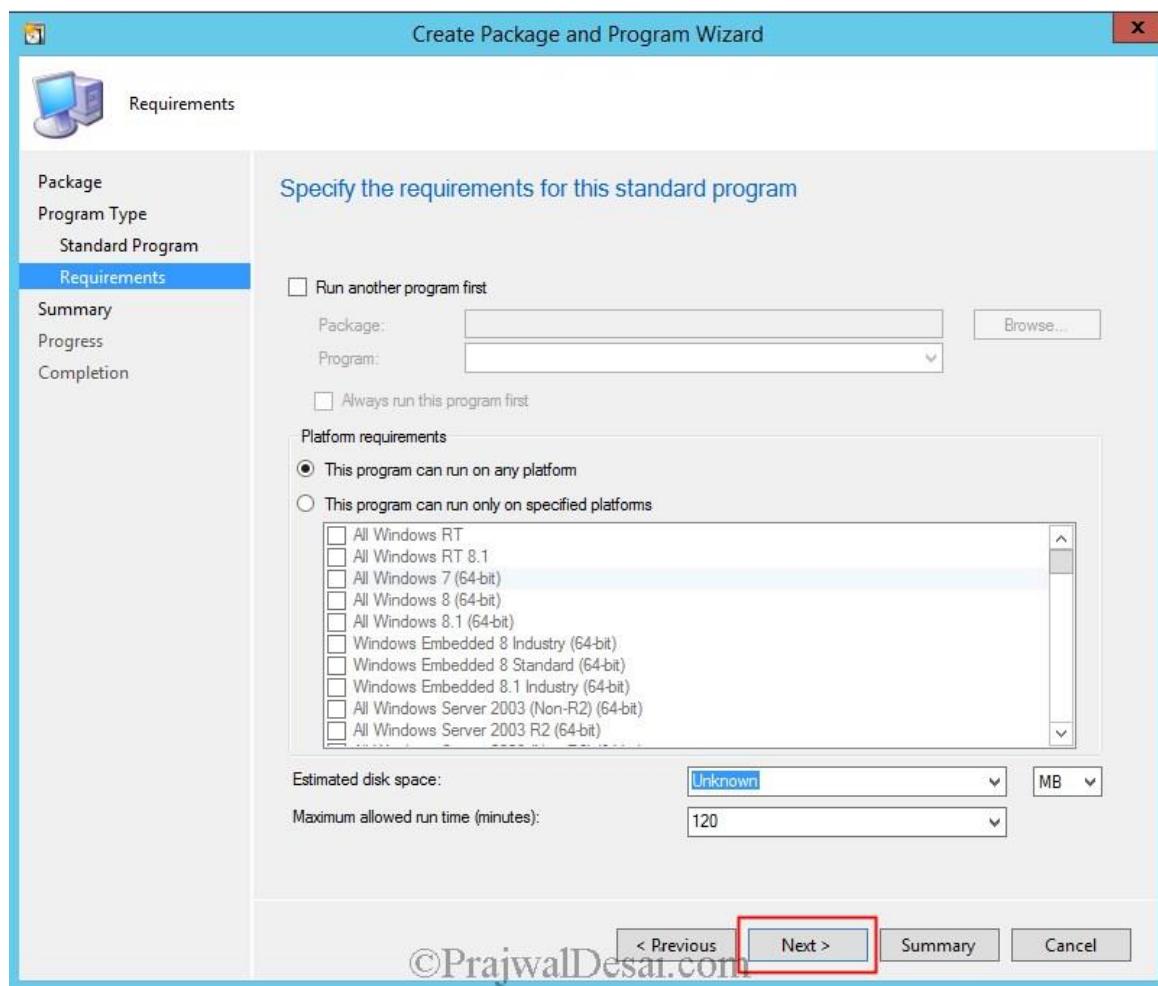
Choose the program type as **Standard Program**. Click **Next**.



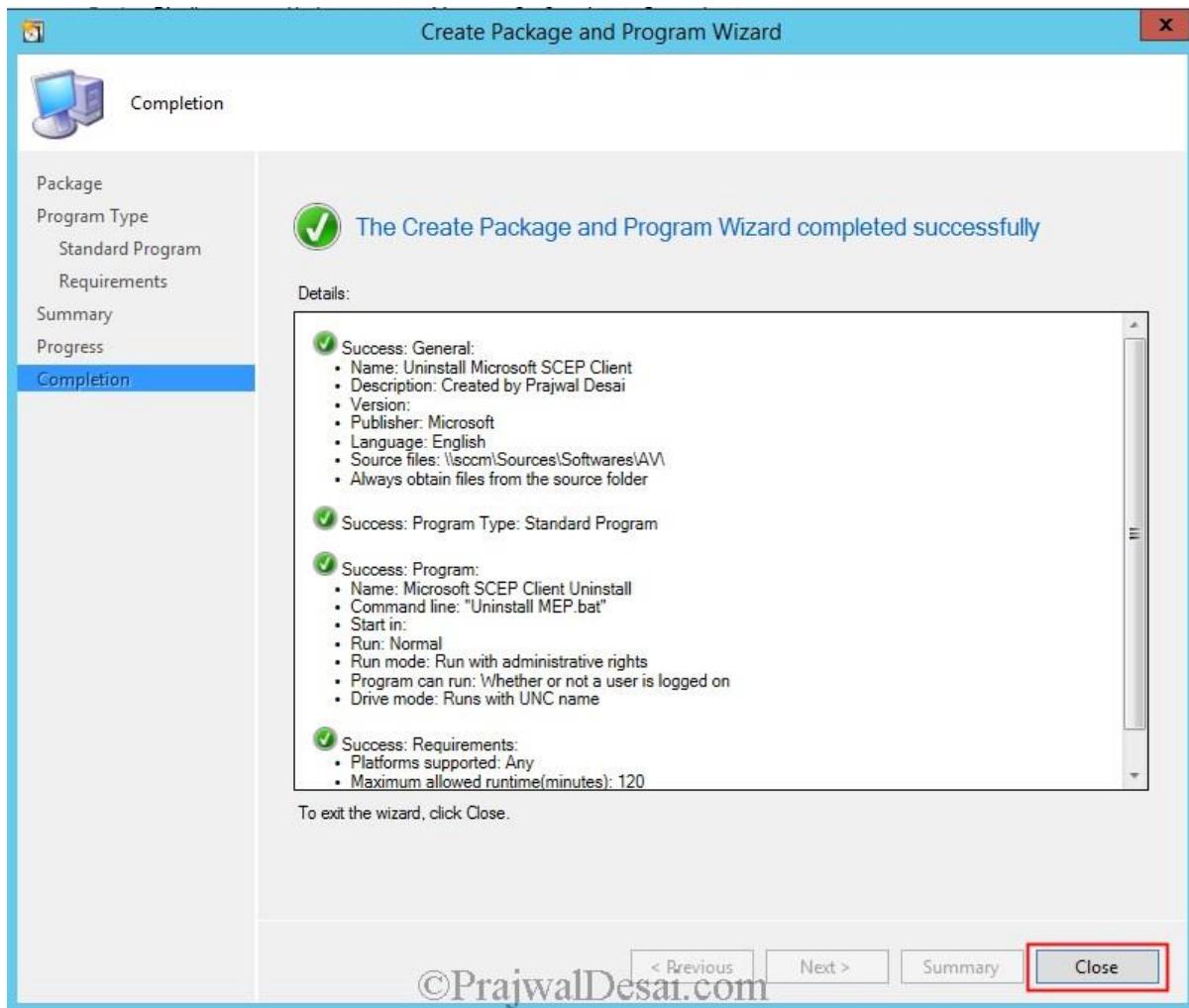
Specify the name of the standard program, in the command line text box click **Browse** and select the batch file and click **Next**.



No changes to be made here, click **Next**.



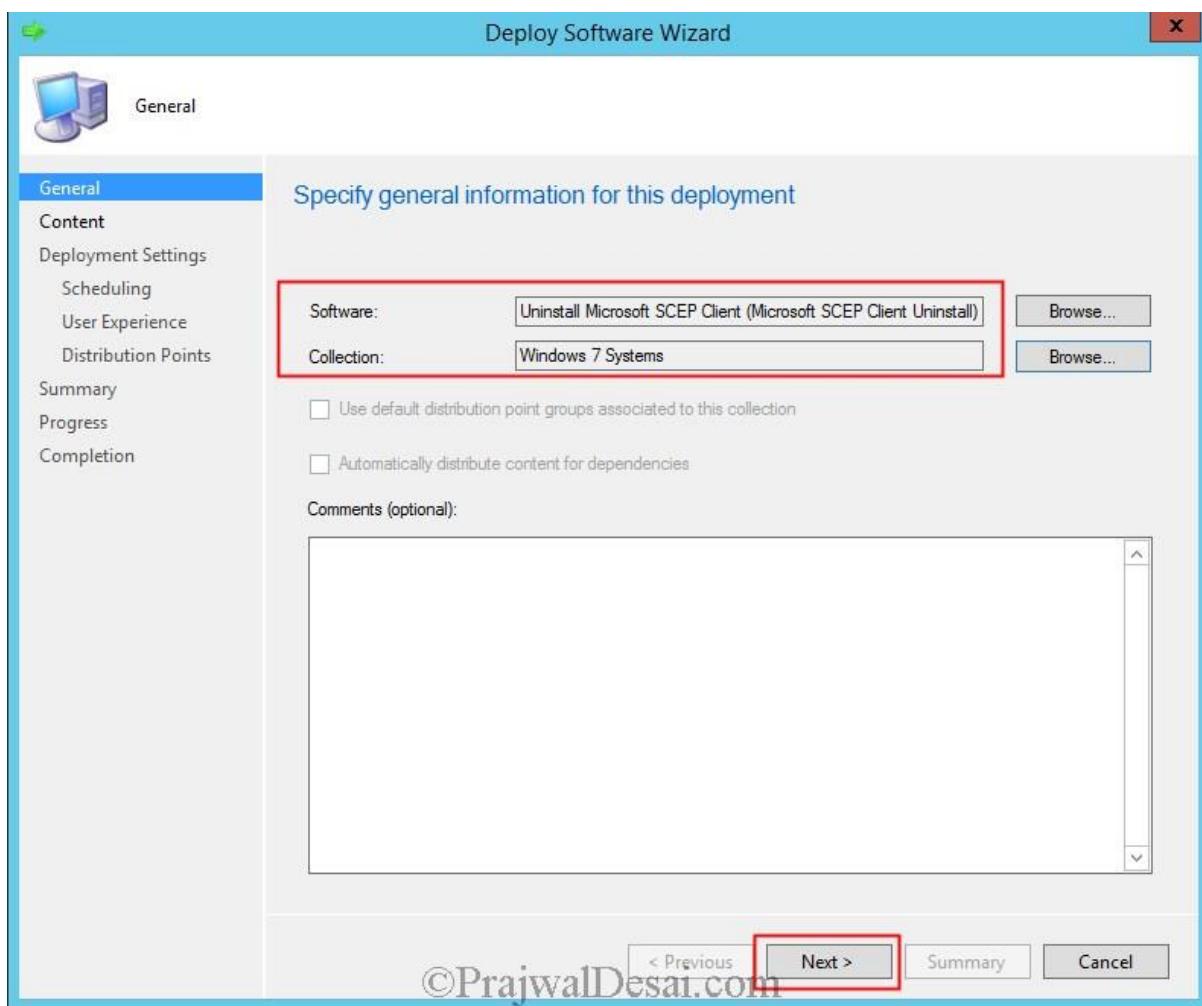
Click on **Close**.



Note – You need to distribute the content to the DP. Right click on the package and click **Distribute Content**. Proceed to the below steps only when the package is available with DP.

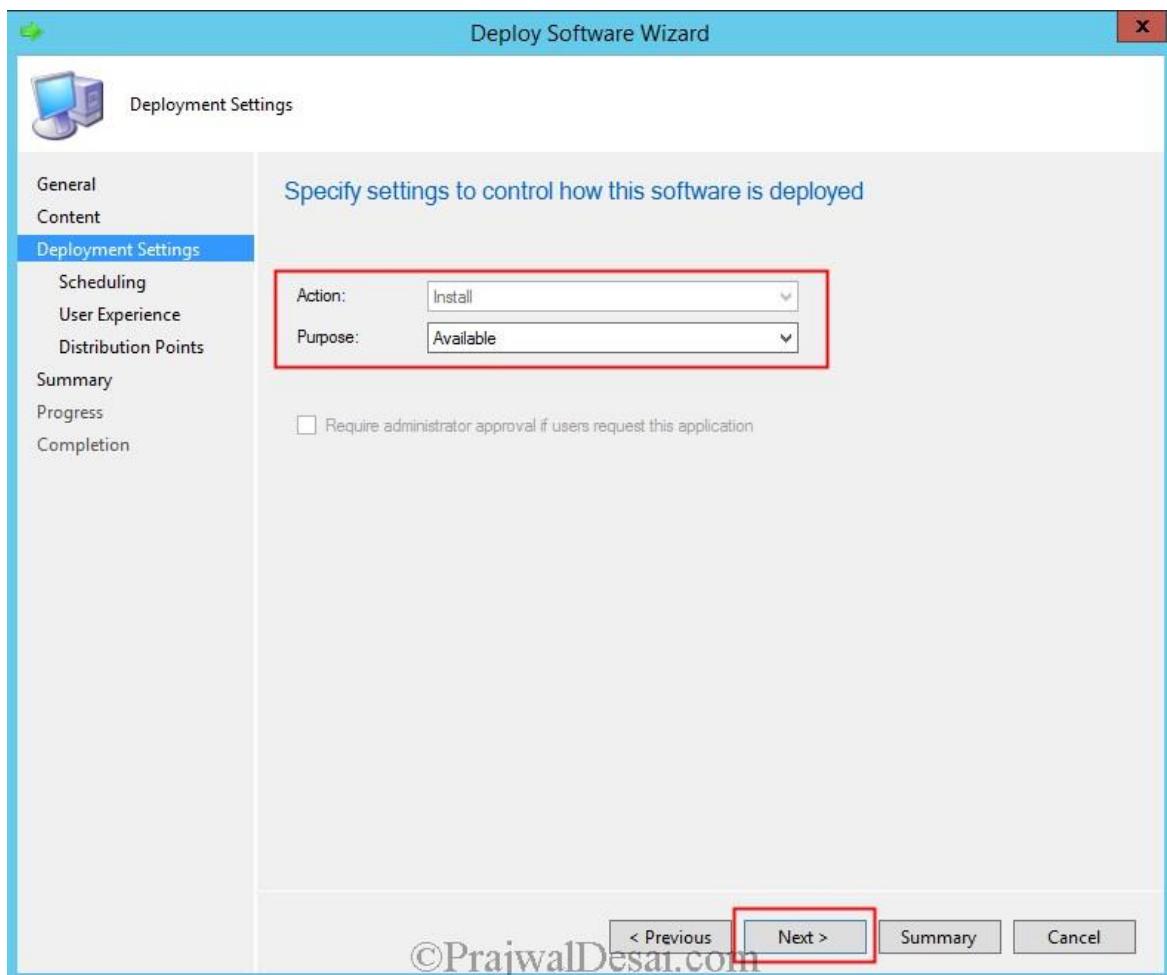
Right click on the package and click **Deploy**. Choose the Collection that you want to deploy.

Click Next.

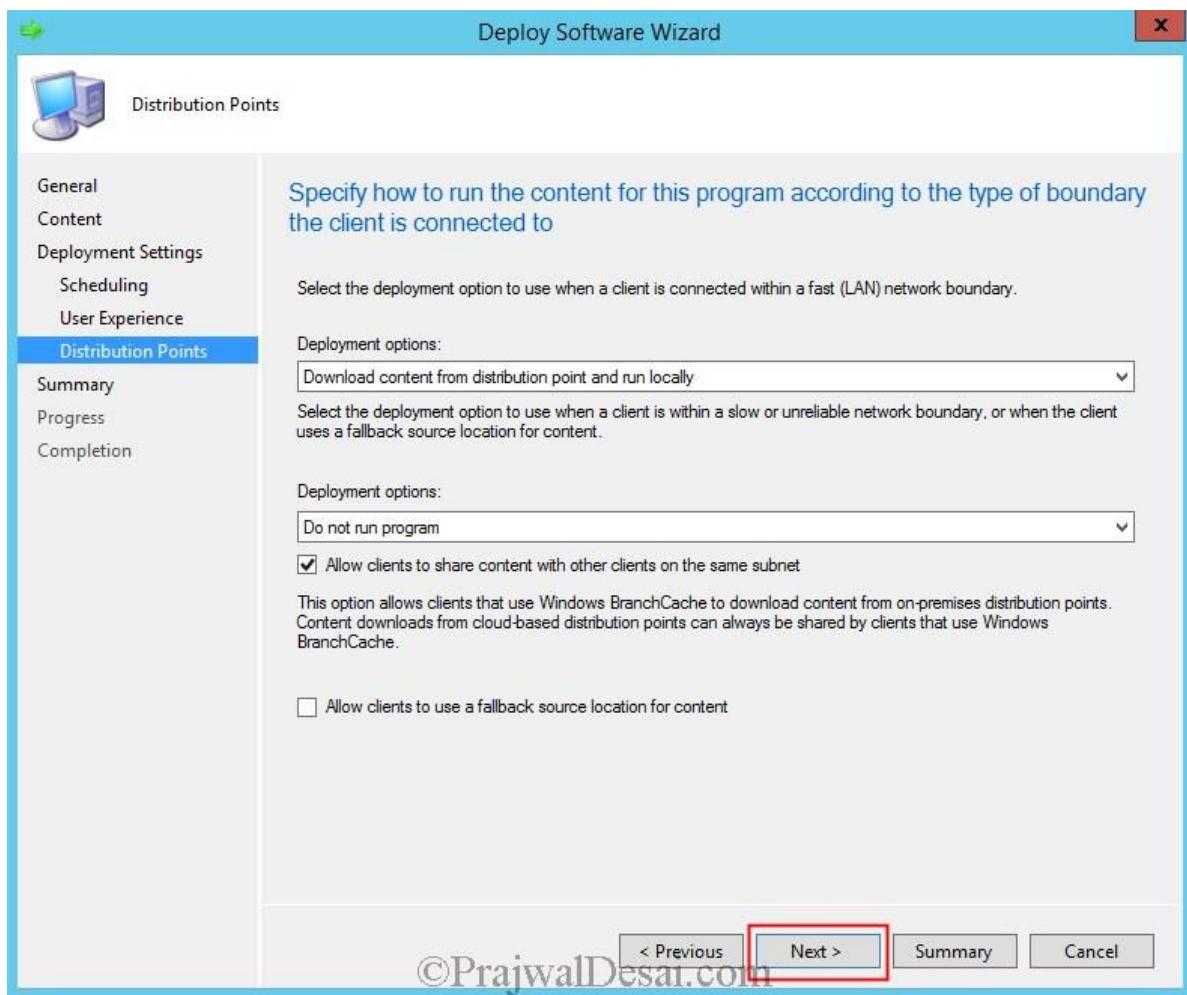


Set the Purpose as Available.

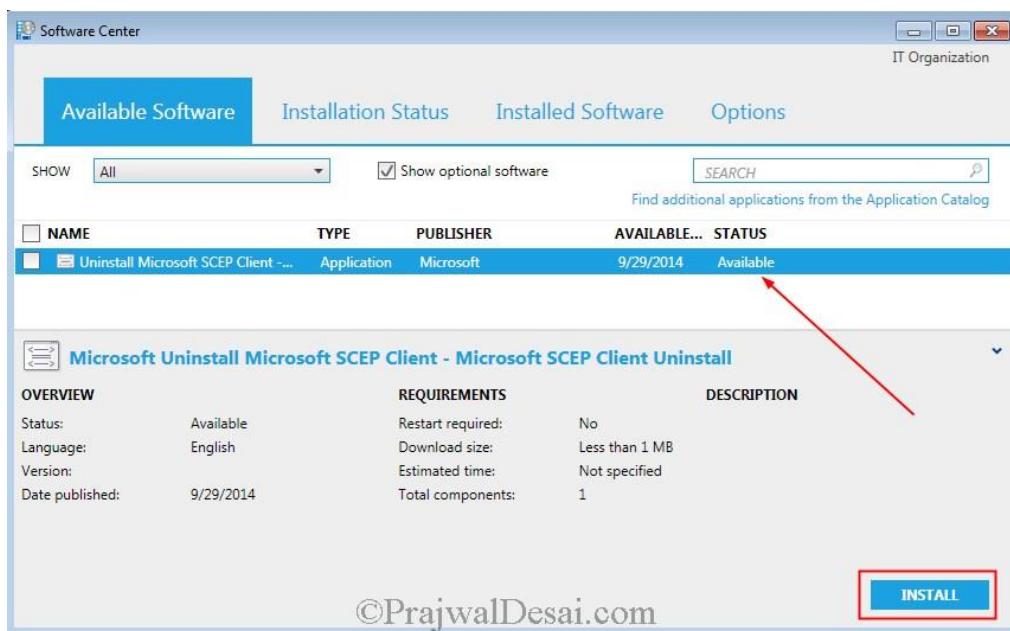
Click Next.



No changes to made here, click **Next** and complete the wizard.



After few minutes, on the client computer the package is available. Select the package and click on **Install**.



On the client computer open the **execmgr.log** file for troubleshooting purpose. We see that the script has been executed and the SCEP client has been uninstalled successfully from the computer.

The screenshot shows two windows side-by-side. The top window is the 'Software Center' interface, displaying a table of installed applications. One row for 'Uninstall Microsoft SCEP Client - Microsoft SCEP Client U...' has its 'STATUS' column highlighted with a red arrow pointing to it. The bottom window is the 'Configuration Manager Trace Log Tool' showing the contents of the 'execmgr.log' file. A red arrow points to a specific log entry: 'Execution is complete for program Microsoft SCEP Client Uninstall. The exit code is 0, the execution status is Success.'

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
7-Zip 9.20 (x64 edition)	Application		9/29/2014	Installed
Uninstall Microsoft SCEP Client - Microsoft SCEP Client U...	Application	Microsoft	9/29/2014	Installed

```

Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\execmgr.log]
File Tools Window Help
Log Text Component Date/Time Thread
Created Process for the passed command line execmgr 9/29/2014 4:06:14 PM 2412 (0x96C)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent[AdvertisementId = "IND20006";ClientID = "GUID:FCB... execmgr 9/29/2014 4:06:14 PM 2412 (0x96C)
Raised Program Started Event for Ad:IND20006, Package:IND0000A, Program: Microsoft SCEP Client Uninstall execmgr 9/29/2014 4:06:14 PM 2412 (0x96C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageId="IND0000A",ProgramId="Microsoft SCEP Client Uninstall", action... execmgr 9/29/2014 4:06:14 PM 2412 (0x96C)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageId="IND0000A",ProgramId="Microsoft SCEP Client Uninstall", action... execmgr 9/29/2014 4:06:14 PM 2412 (0x96C)
MTC task with id (7A0260E4-A773-46C5-9B77-A9E2705CBF37) changed state from 4 to 5 execmgr 9/29/2014 4:06:14 PM 3580 (0xDFC)
Program exit code 0 execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Looking for MIF file to get program status execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Script for Package:IND0000A, Program: Microsoft SCEP Client Uninstall succeeded with exit code 0 execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessfullyEvent[AdvertisementId = "IND20006";ClientID = "GUID:FCB... execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Raised Program Success Event for Ad:IND20006, Package:IND0000A, Program: Microsoft SCEP Client Uninstall execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Execution is complete for program Microsoft SCEP Client Uninstall. The exit code is 0, the execution status is Success. execmgr 9/29/2014 4:06:41 PM 1724 (0x6BC)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageId="IND0000A",ProgramId="Microsoft SCEP Client Uninstall", action... execmgr 9/29/2014 4:06:42 PM 1724 (0x6BC)
Requesting MTC to delete task with id: (7A0260E4-A773-46C5-9B77-A9E2705CBF37) execmgr 9/29/2014 4:06:42 PM 1724 (0x6BC)
|MTC task with id: (7A0260E4-A773-46C5-9B77-A9E2705CBF37) deleted successfully. execmgr 9/29/2014 4:06:42 PM 1724 (0x6BC)

```

How to Setup Distribution Point in SCCM 2012 R2

How to Setup Distribution Point in SCCM 2012 R2 In this post we will see the steps on how to setup [Distribution Point](#) in SCCM 2012 R2. Distribution points play a very important role in the delivery of packages, programs, endpoint protection updates, applications, software updates, and operating system deployment (OSD). When the site server is installed, it becomes a distribution point by default. However, you might want to assign other site systems as distribution points and remove the DP role from the site server to reduce its resource requirements and improve its performance as well as to load balance the potentially significant network traffic generated by clients downloading package source files. In Configuration Manager 2007, there were three basic types of distribution points **Standard**, **Server Share** and **Branch Distribution Points**. Starting with Configuration Manager 2012, Microsoft has updated the distribution point role to become one standard distribution point. In this post we will be installing the Distribution Point role on Windows Server 2012 R2 server.

How to Setup Distribution Point in SCCM 2012 R2

This is really important. Before you install DP role check whether the operating system supports the installation of DP role. For example if you are planning to install DP on Windows 7, distribution points on this operating system version do not support Multicast or PXE. Click the [link](#) to know more about it. When you install a distribution point, you see an option to “**Install and configure IIS if required by Configuration Manager**“. When you enable this option the Configuration Manager will install and configure IIS if it is not installed. In case you want to install the prerequisites manually then install the below listed IIS prerequisites.

Remote Differential Compression

IIS Configuration:

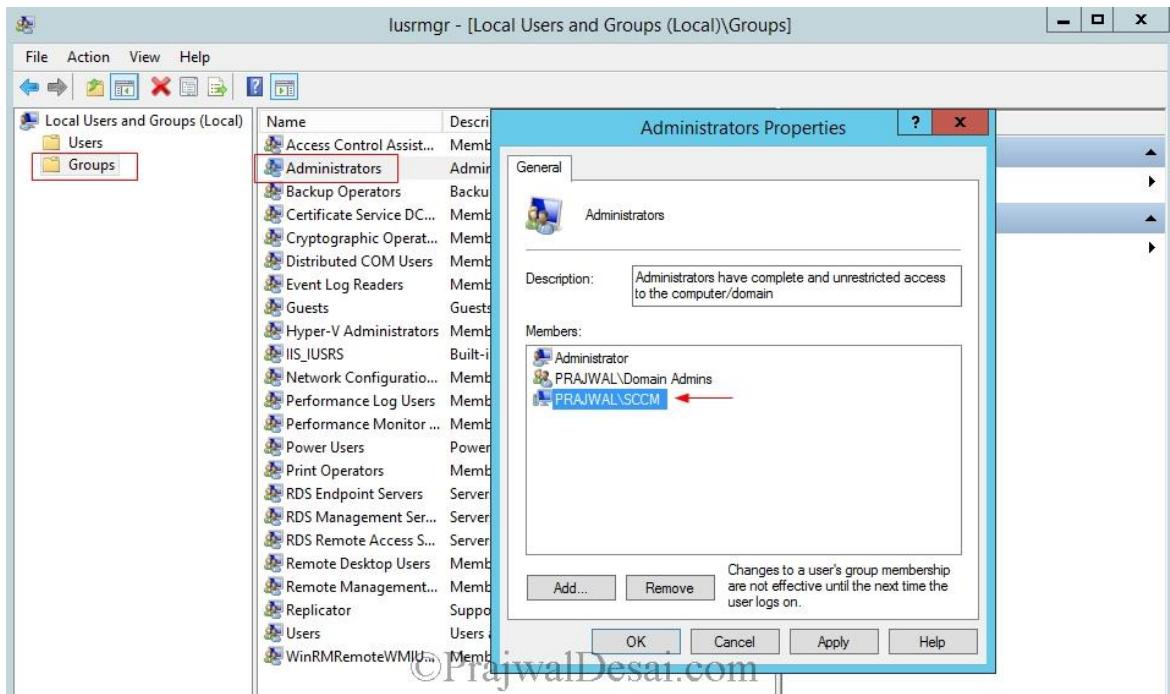
Application Development: ISAPI Extensions

Security: Windows Authentication

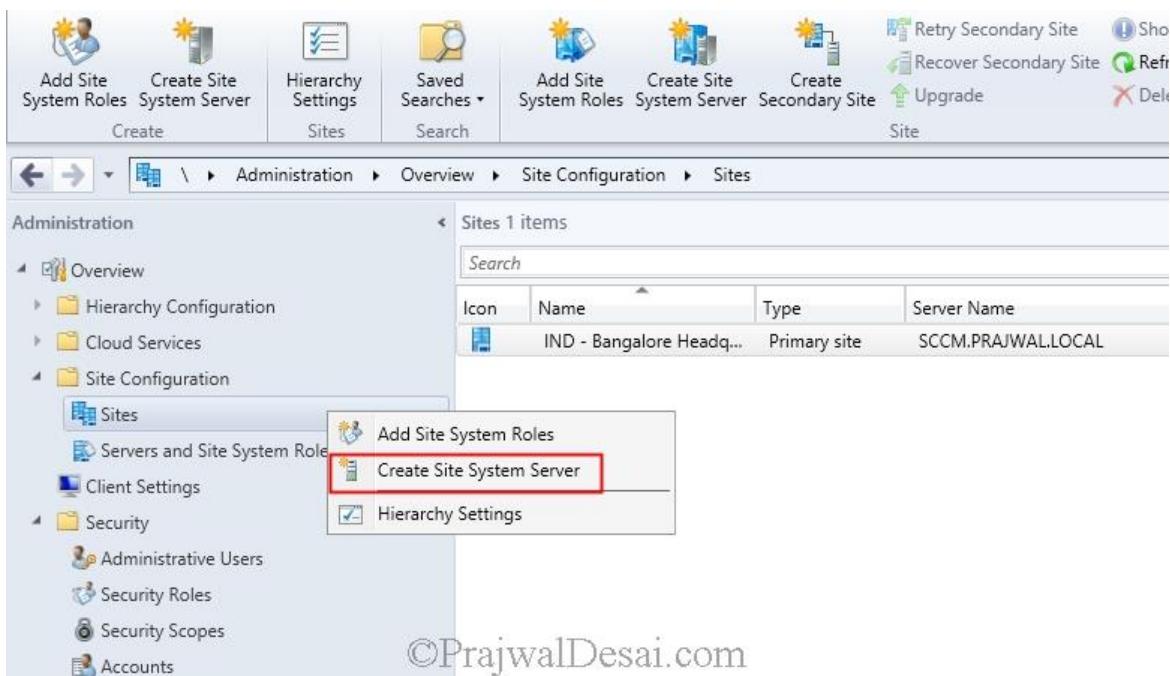
IIS 6 Management Compatibility: IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility.

To support PXE or multicast role on DP, the WDS role is required. WDS installs and configures automatically when you configure a distribution point to support PXE or Multicast on Windows Server 2012. Also **PowerShell 3.0** is required on Windows Server 2012 before you install the distribution point.

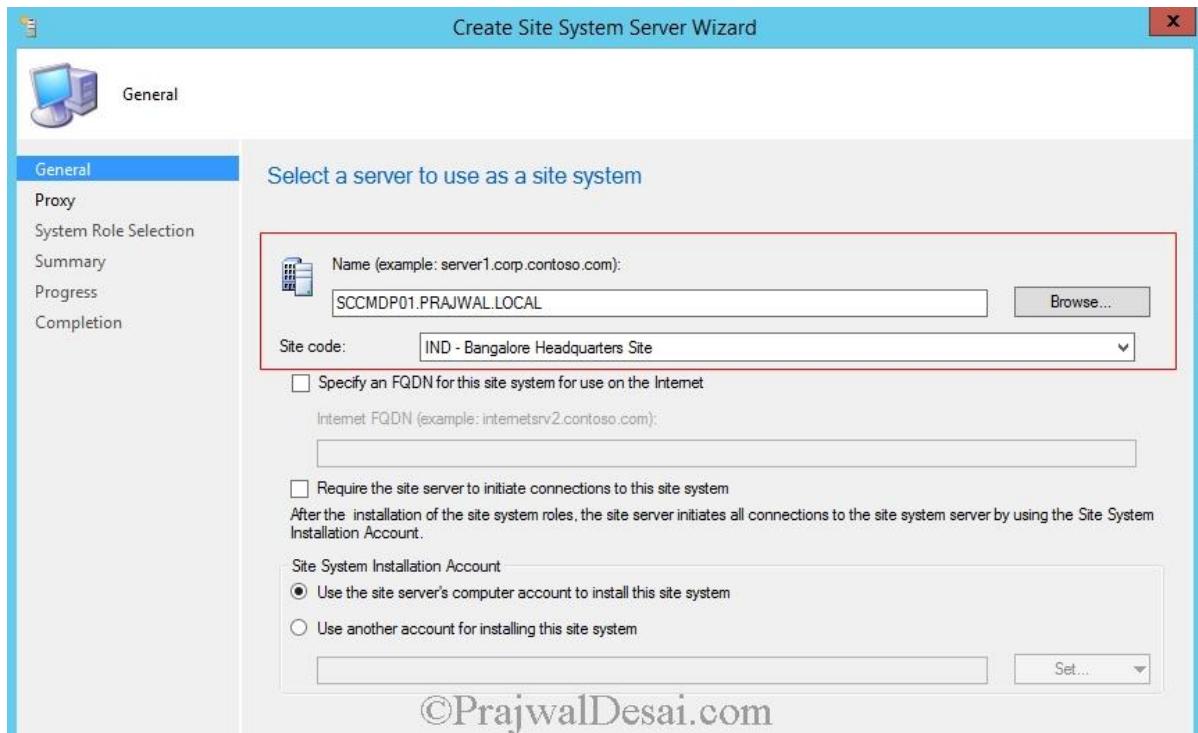
Next, you need to add the SCCM site server computer account to the Local **Administrators** group on the box where DP role is to be installed. In this example, **SCCM** is the name of the site server and **SCCMDP01** is my DP server where DP role shall be installed. So I add the **SCCM** site server computer account to the Local Administrators group on **SCCMDP01** computer.



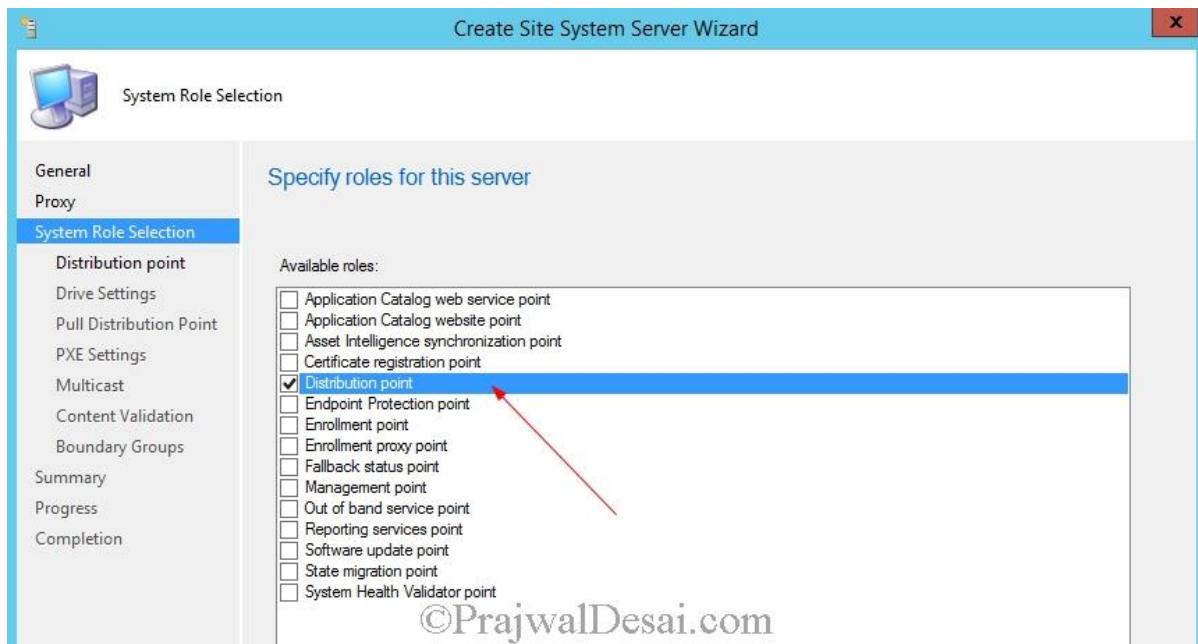
In the console, navigate to **Administration -> Overview -> Site Configuration**. Right click **Sites** and click **Create Site System Server**.



In the **Create Site System Server Wizard**, click **Browse** and select the computer on which DP role is to be installed. Select the **Site Code** and click **Next**.



On the **System Role Selection** page, select **Distribution Point**. Click **Next**.



On the **Distribution Point** page, configure the DP settings for your environment. Here is a brief description of each of the setting.

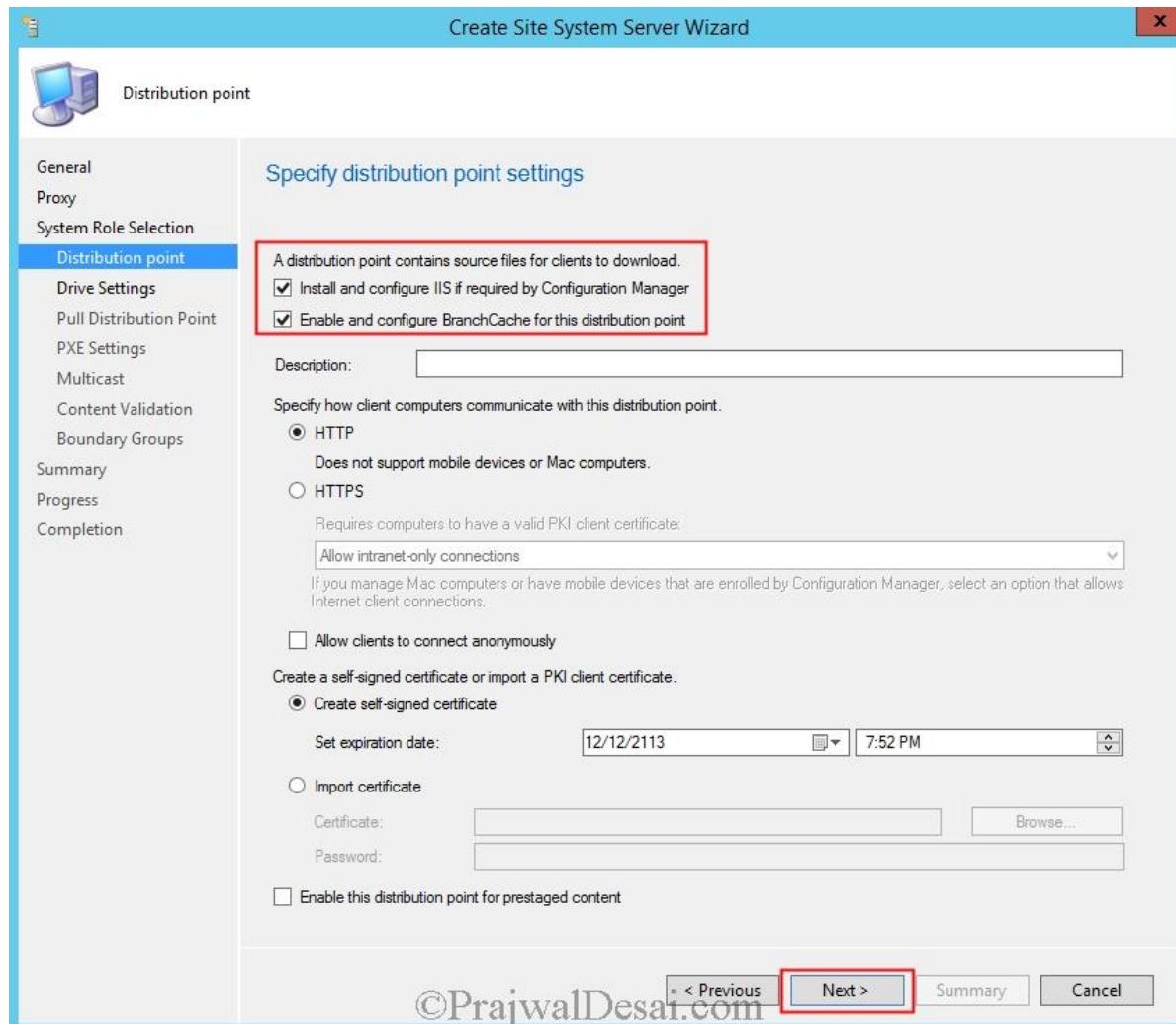
Install and configure IIS if required by Configuration Manager: Enable this setting to install Windows components required for a DP automatically.

Enable and configure BranchCache for this distribution point: Enable this setting to enable and configure BranchCache.

Specify how client computers communicate with the distribution point: Choose HTTP or HTTPS for client communication with the DP.

Allow clients to connect anonymously: Enable this check box only if you need anonymous connections to the DP. The ConfigMgr client uses the Local System account and the Network Access account to connect to the DP.

Click **Next**.

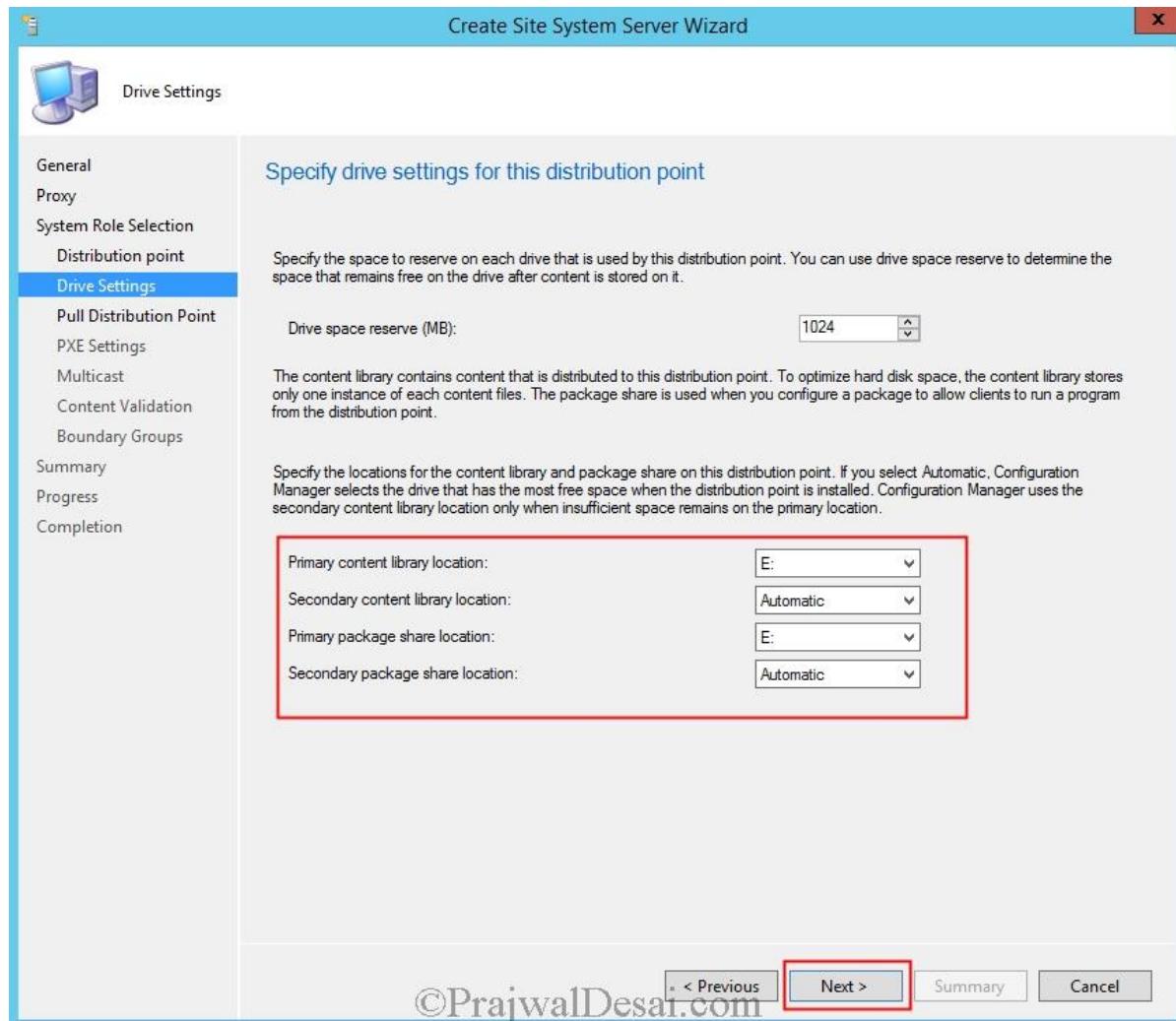


Specify the drive settings for the distribution point – You can configure up to two disk drives for the content library and two disk drives for the package share.

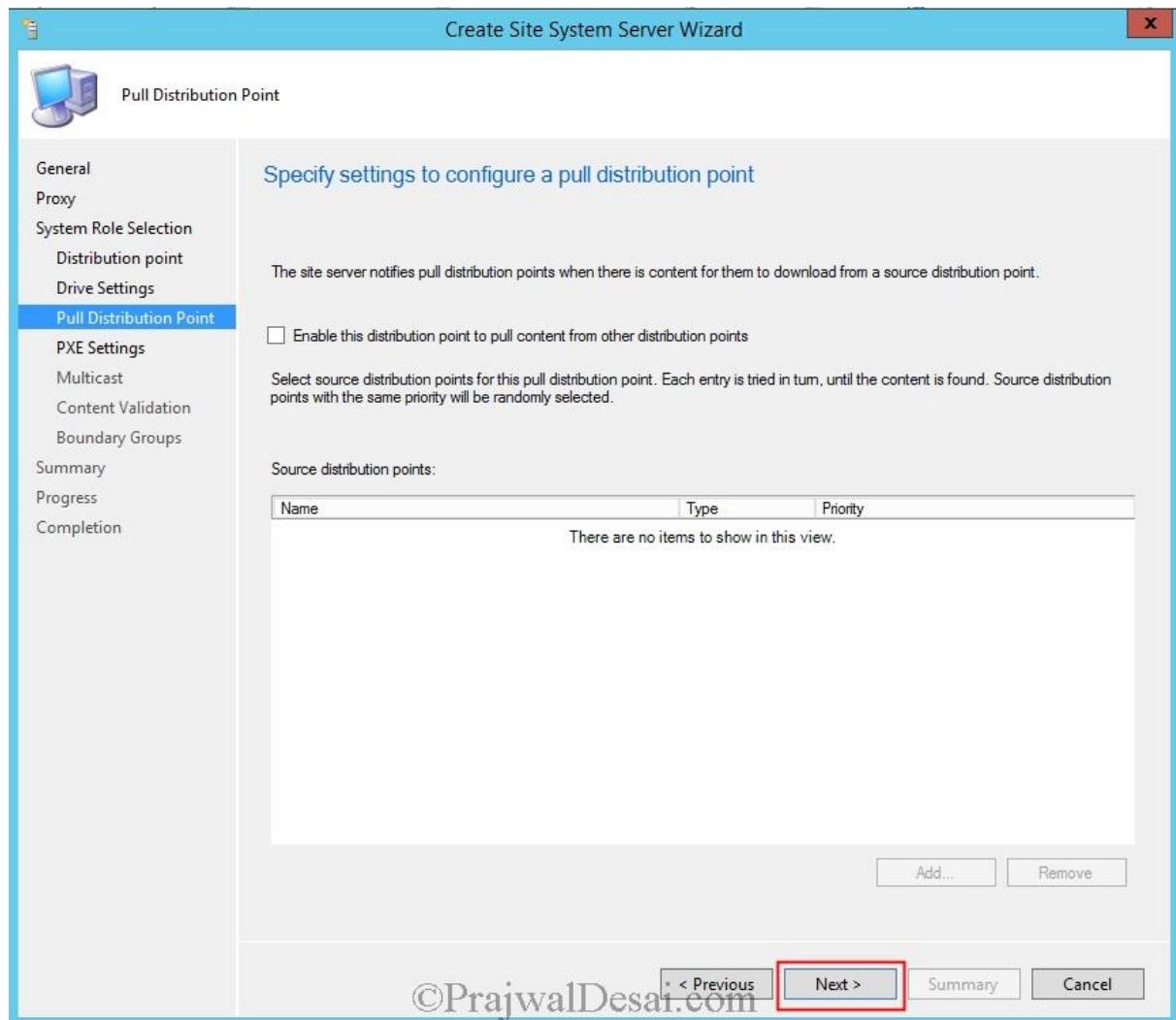
Drive space reserve (MB) – The value that you configure for this setting determines the amount of free space on a drive before Configuration Manager 2012 chooses a different drive and continues the copy process to that drive. By default the **Drive space reserve** is 50 MB, in this example I will setting it to 1024 MB.

Content Locations – Specify the content locations for the content library and package share. Configuration Manager 2012 will copy content to the primary content location until the amount of free space reaches the value specified for Drive space reserve (MB). By default the content locations are set to **Automatic** and the primary content location will be set to the disk

drive that has the most disk space at installation and the secondary location assigned the disk drive that has the second most free disk space. When the primary and secondary drives reach the drive space reserve, Configuration Manager will select another available drive with the most free disk space and continue the copy process.

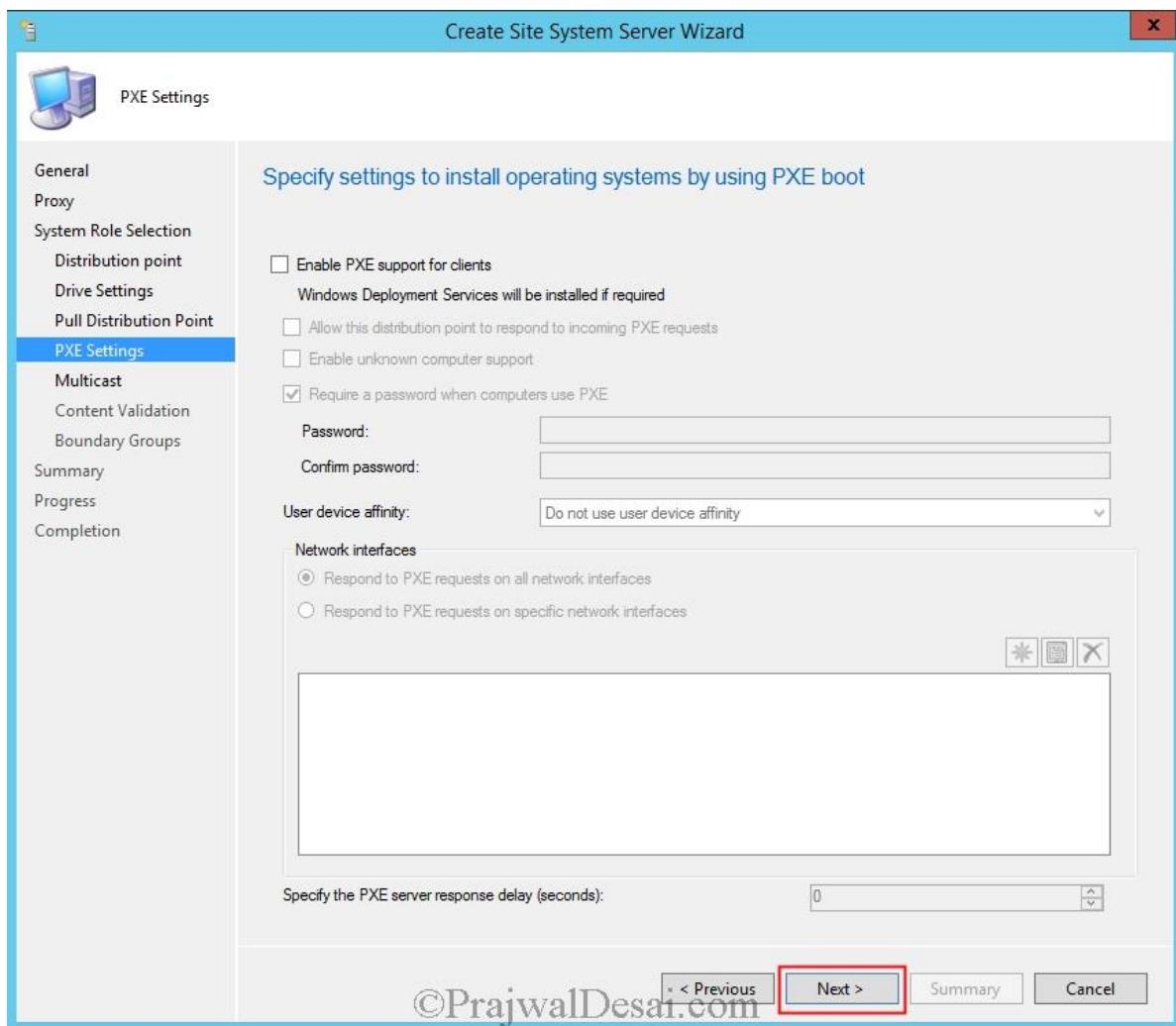


This option can be configured later. Click **Next**.

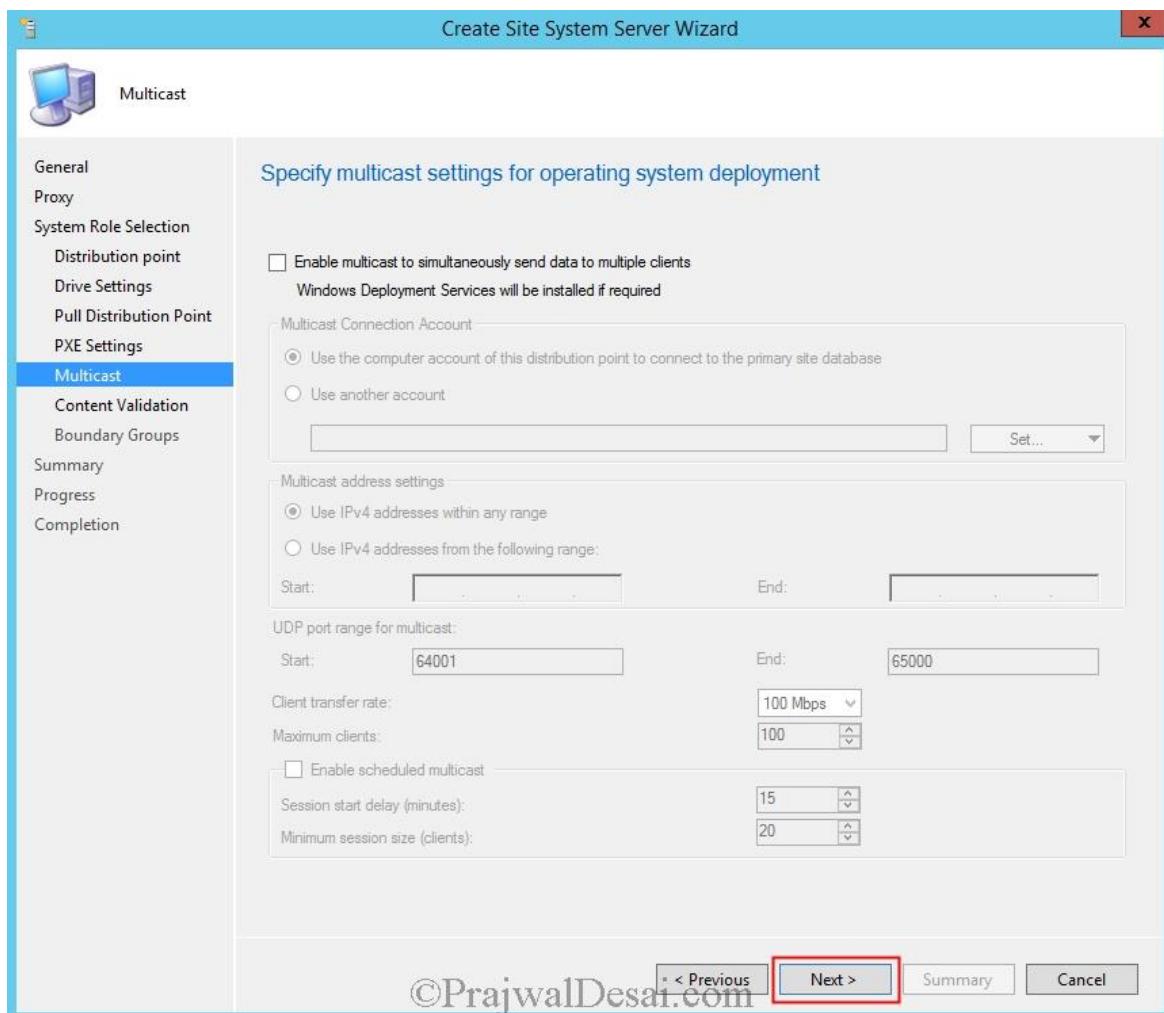


©PrajwallDesai.com

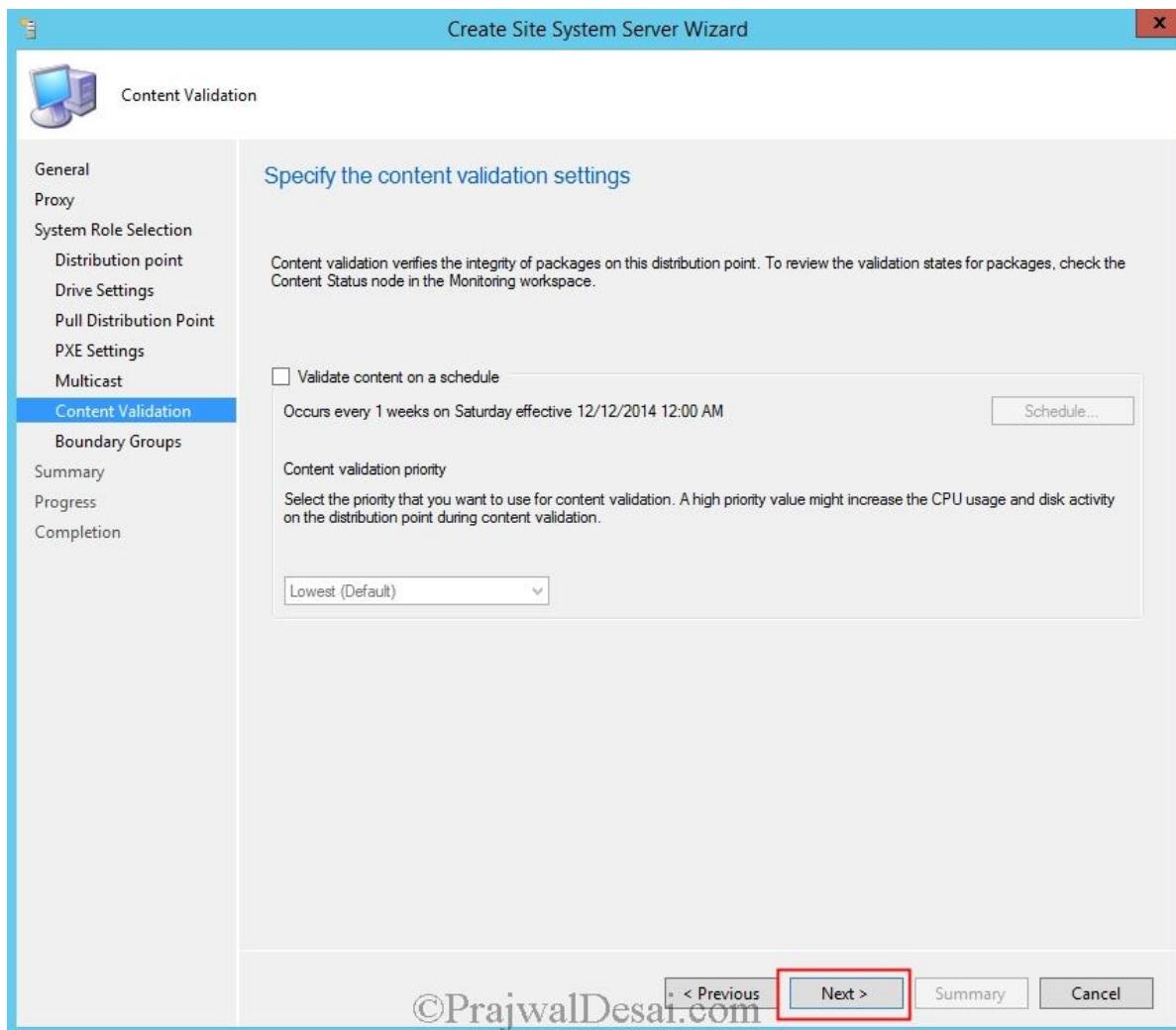
The PXE option can be enabled and configured later. Click **Next**.



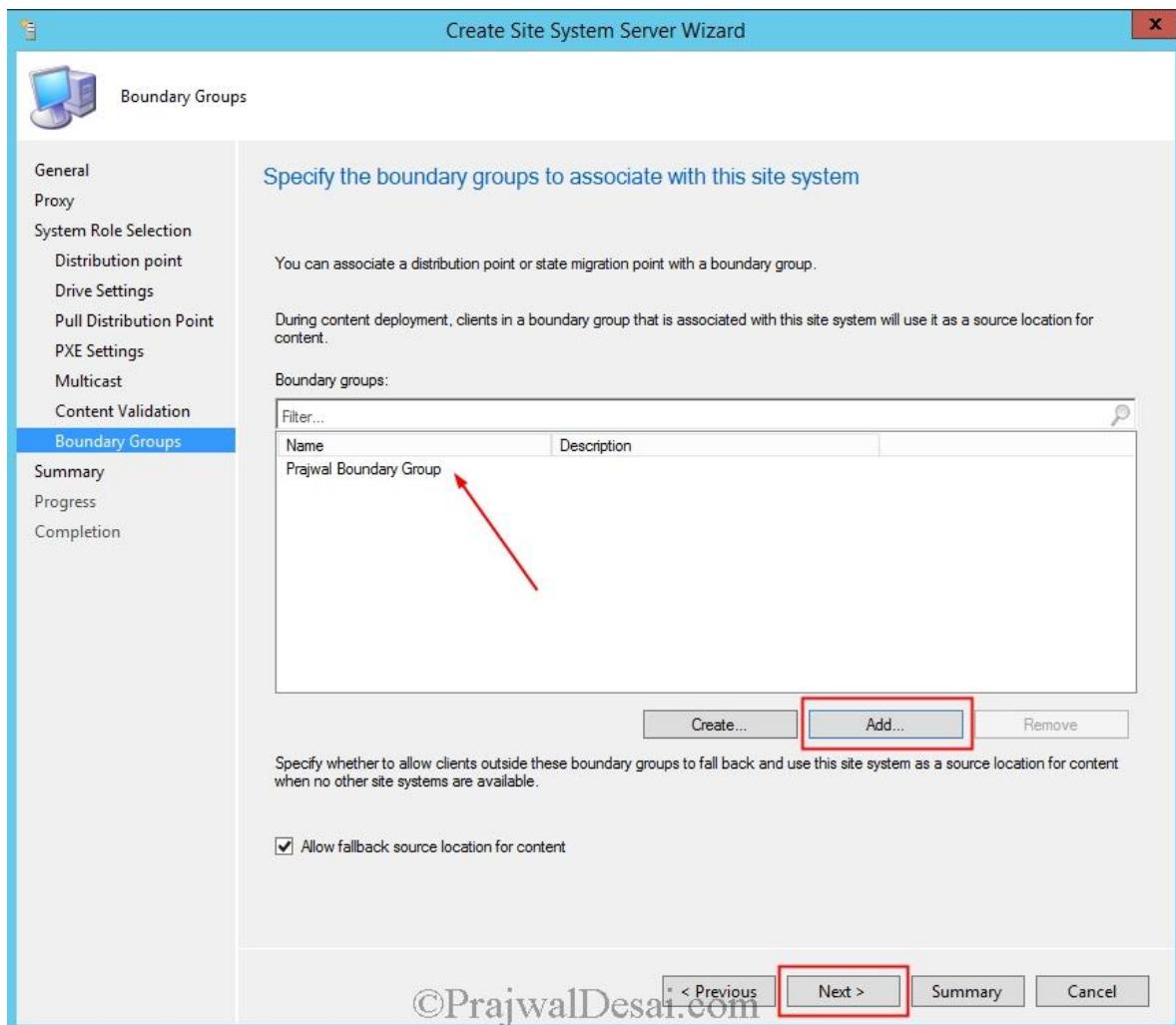
This Multicast option can be configured later. Click **Next**.



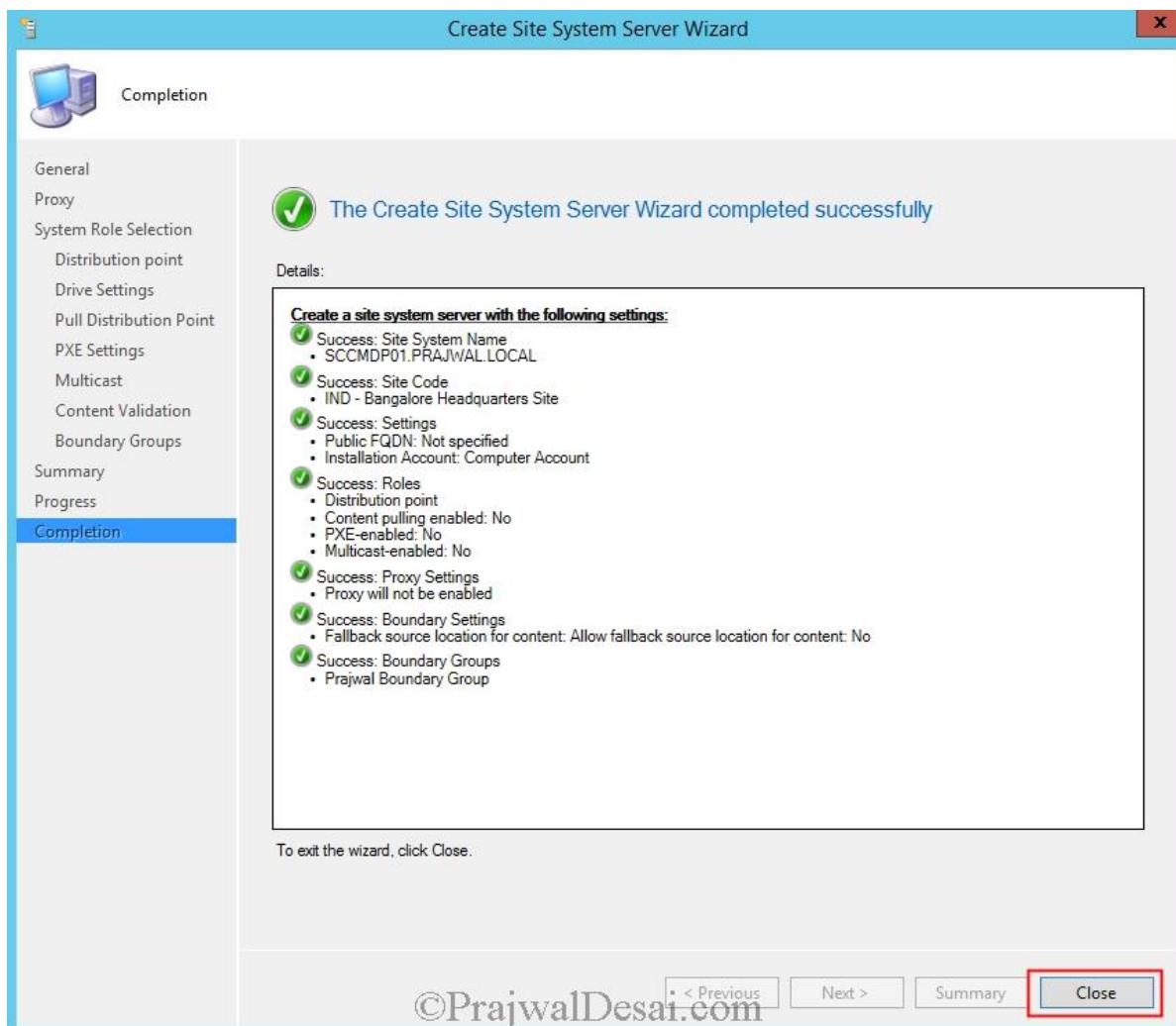
Specify whether to validate the integrity of content files on the distribution point. When you enable **content validation** on a schedule, Configuration Manager will initiate the process at the scheduled time, and all content on the distribution point is verified. We will not configure this option, click **Next**.



To specify the boundary group(s) with the site system, click on **Add** and choose the boundary group. The distribution point is considered protected for the clients that are within the boundaries associated with the boundary group. Click **Next**.



Click Close.



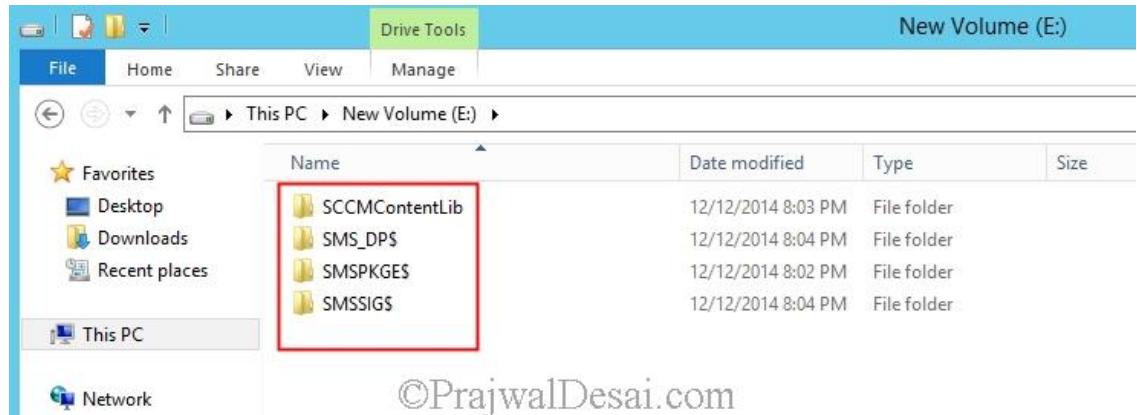
To check the DP status, click on **Monitoring** and click **Distribution Point Configuration Status**. Now you will see the list of DP's, click the DP server and you should see status of server as green .

The screenshot shows the SCCM Monitoring interface. The left navigation pane includes categories like Monitoring, Site Hierarchy, Status, Deployments, Client Operations, Client Status, Distribution Status, Content Status, Configuration Manager Client Package, Distribution Point Group Status, Distribution Point Configuration Status, Software Update Point Synchronization Status, and Endpoint Protection Status. The 'Distribution Point Configuration Status' link is selected. The main pane displays a table titled 'Distribution Point Configuration Status 2 items' with two entries:

Icon	Distribution Point Name	PXE	Content Validation	Multicast	Messages	Last Status Date
	SCCM.PRAJWAL.LOCAL	No	No	No	7	12/12/2014 12:4...
	SCCMDP01.PRAJWAL.LOC...	No	No	No	6	12/12/2014 8:03...

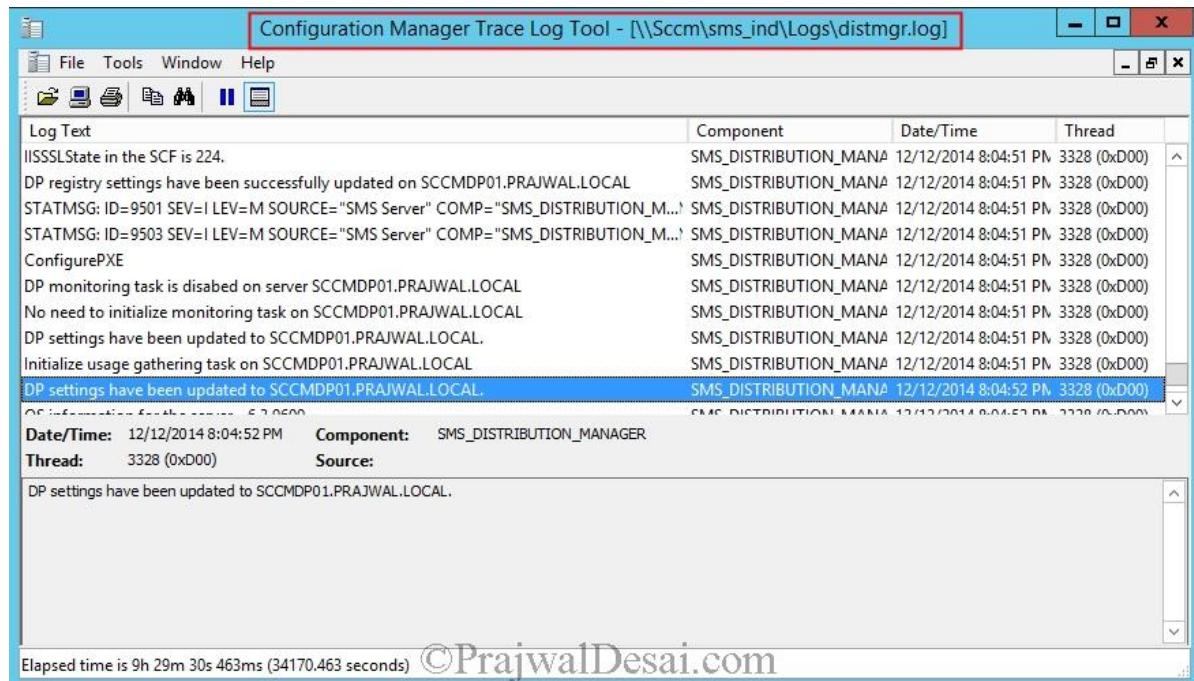
A red arrow points from the text 'server as green ' to the green checkmark icon next to the first distribution point entry. The bottom right corner of the screenshot has a watermark: ©PrajwalDesai.com.

After the DP is installed successfully, you can login to the DP server and check for the folders shown in the below screenshot.



©PrajwalDesai.com

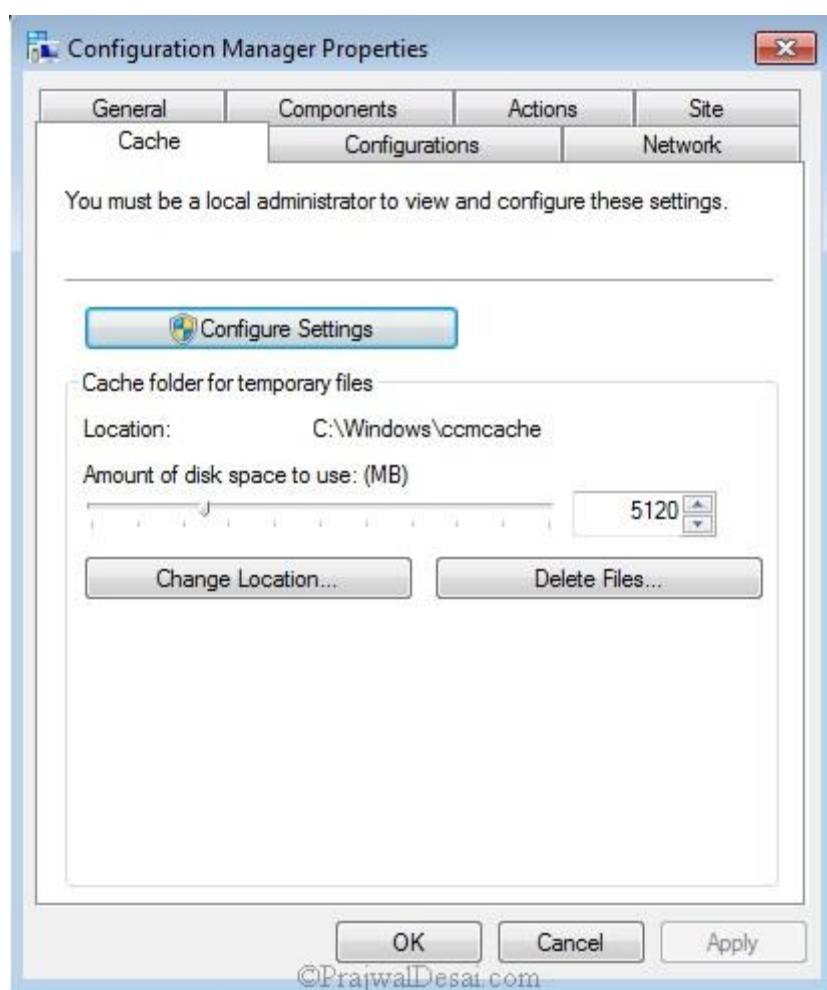
For DP troubleshooting you can see the **Distmgr.log** file which records content creation, compression, delta replication, and information updates.



©PrajwalDesai.com

[How to increase SCCM client cache size](#)

How to increase SCCM client cache size when you have large applications to deploy during an OSD, it will fail because the size of the [SCCM Client Cache](#) is not big enough to cache the application installation files. Software updates also use the client cache, but software updates are not restricted by the configured cache size and will always attempt to download to the cache. You can configure the client cache settings when you install the Configuration Manager client manually, when you use client push installation, or after the client is installed. When you distribute software, you can set the Advanced Client to download package source files from a distribution point to a cache on the Advanced Client computer before the program runs. When the program runs, it uses the source files in the cache instead of the source files on the distribution point. By default, the [SCCM 2012 Client Cache](#) is set to 5120MB and if you do not set this property while installing SCCM Client, the folder defaults to a maximum size of 5120 MB. The lowest value you can specify is 1 MB.



You could change the client cache size on a single machine by getting into **Control Panel > Configuration Manager Client Properties > Cache >** click on **Configure Settings** and change the value of cache size and click **OK**.

VB script to modify SCCM client cache size

```
On Error Resume Next
Dim UIResManager
Dim Cache
Dim CacheSize
CacheSize=20000
Set UIResManager = CreateObject("UIResource.UIResourceMgr")
Set Cache=UIResManager.GetCacheInfo()
Cache.TotalSize=CacheSize
```

Power shell script to increase SCCM client cache size

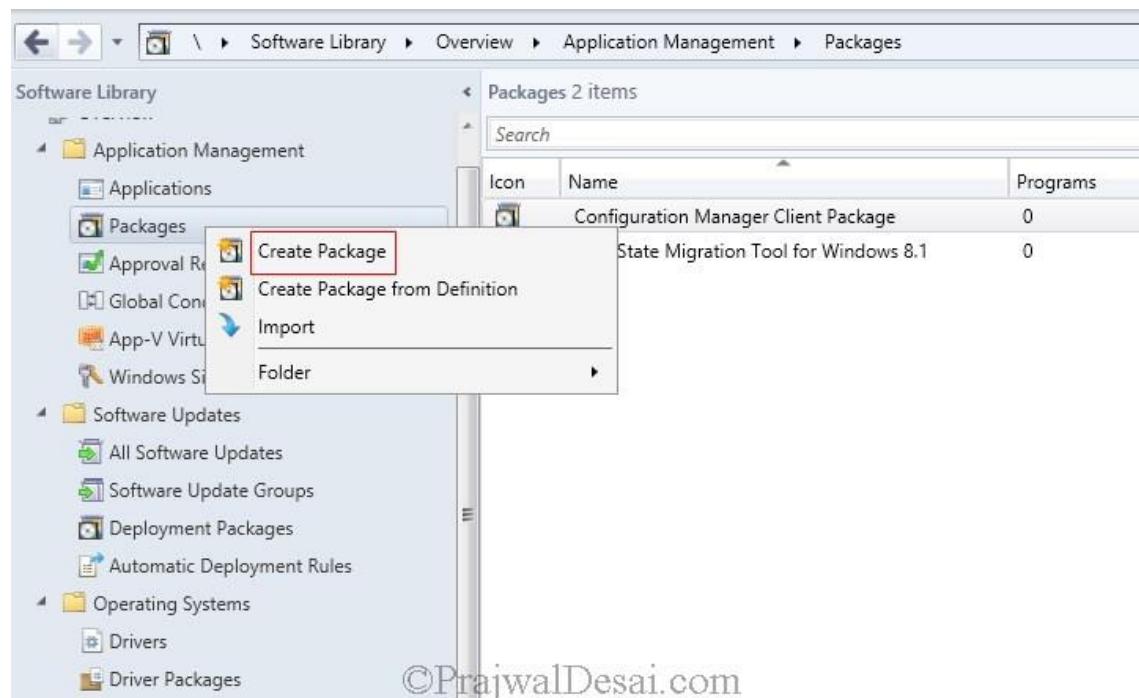
```
$Cache = Get-WmiObject -Namespace 'ROOT\CCM\SoftMgmtAgent' -Class CacheConfig
$Cache.Size = '10240'
$Cache.Put()
Restart-Service -Name CcmExec
```

[DOWNLOAD VB SCRIPT](#) [DOWNLOAD PS SCRIPT](#)

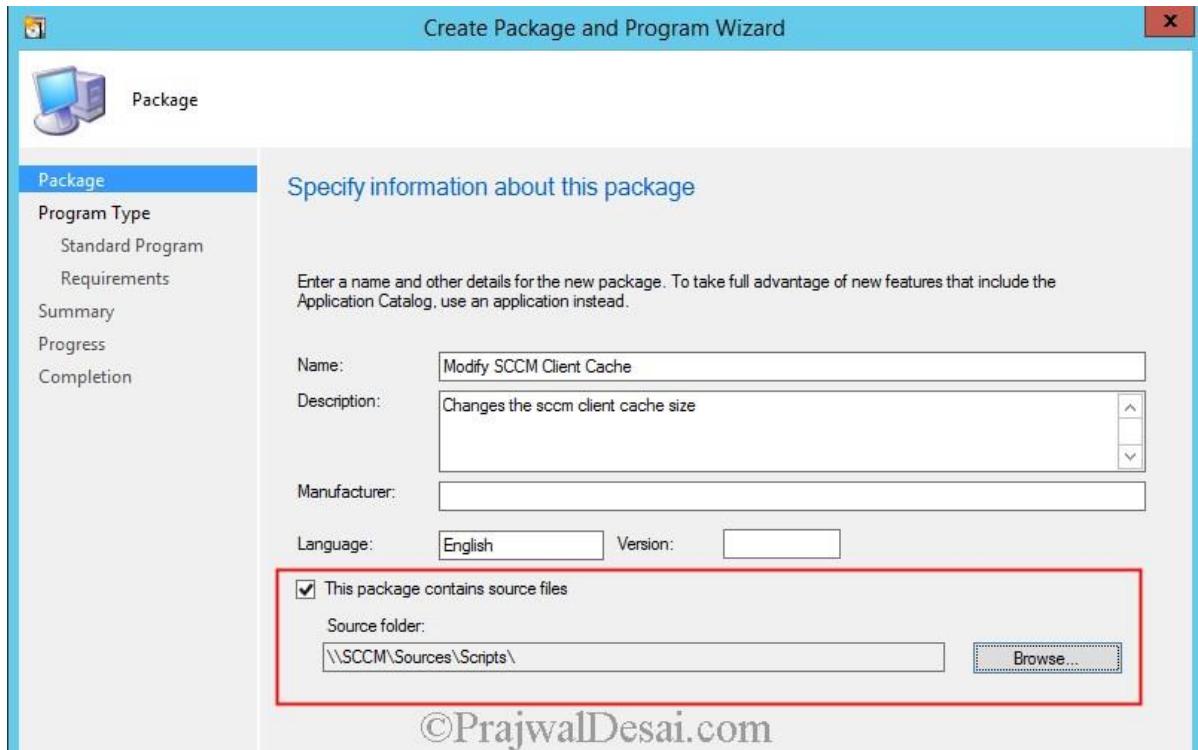
You could download the VB and PowerShell script by clicking on above button.

If you want to change SCCM client cache size on multiple computers then you could deploy the script to a device collection. Here are the steps to change the client cache size.

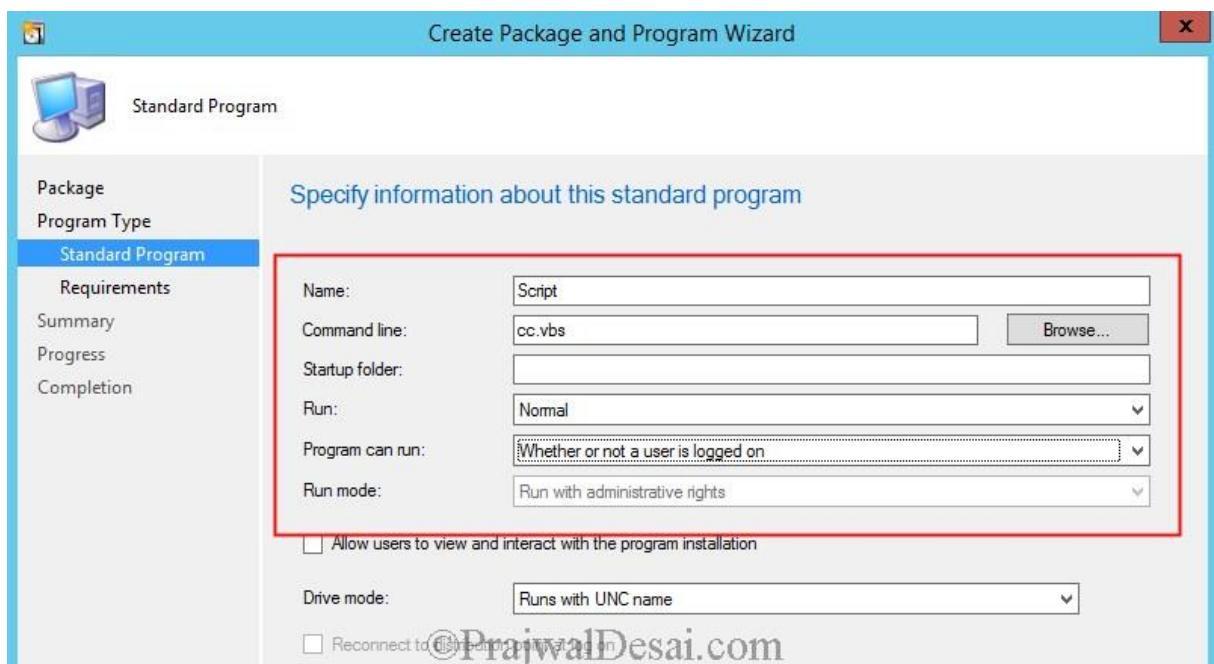
Launch the **Configuration Manager** console, click on **Software Library** and click on **Application Management**. Right click on **Packages** and click on **Create Package**.



Provide the **Name**, **Description** for this package. You need to specify the location where you have stored the script files so your **Source folder** should be the path where the script is located. Click **Next**.



We will be using the VB script to change the cache size, provide details for the standard program as shown in the below screenshot. cc.vbs is the name of the script file. Click **Next** and complete the wizard.



Before you deploy the package you need to distribute the package to the distribution point, so right click on the package and click **Distribute Content** and distribute the package to the

desired DP. The next step is to deploy the package to a device collection, right click the package and click on **Deploy**.

The screenshot shows the SCCM console's 'Packages' view with three items listed:

Icon	Name	Programs	Manufacturer	Version	Language	Package ID
Configuration Manager Client Package	0	Microsoft Corp...		IND00004		
Modify SCCM Client Cache			English	IND00008		
User State Migration Tool for Windo...		6.3.9600.16384		IND00001		

A context menu is open over the 'Modify SCCM Client Cache' package, showing options like Manage Access Accounts, Create Prestaged Content File, Create Program, Export, Refresh (F5), Delete, Deploy (which is highlighted with a red box), Distribute Content, Update Distribution Points, Move, Set Security Scopes, and Properties.

©PrajwalDesai.com

Choose the collection for which you want to deploy this package and click **Next**.

The screenshot shows the 'Deploy Software Wizard' dialog box, Step 1: General. The left sidebar shows tabs for General, Content, Deployment Settings, Scheduling, User Experience, Distribution Points, Summary, Progress, and Completion. The 'General' tab is selected.

The main area displays the following information:

Specify general information for this deployment

Software:

Collection:

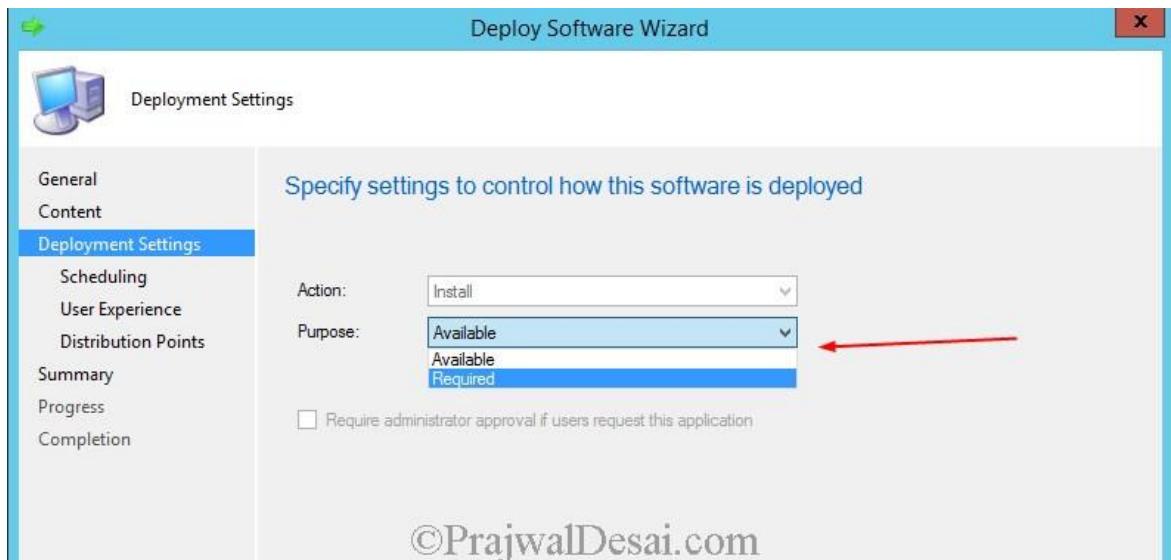
Use default distribution point groups associated to this collection

Automatically distribute content for dependencies

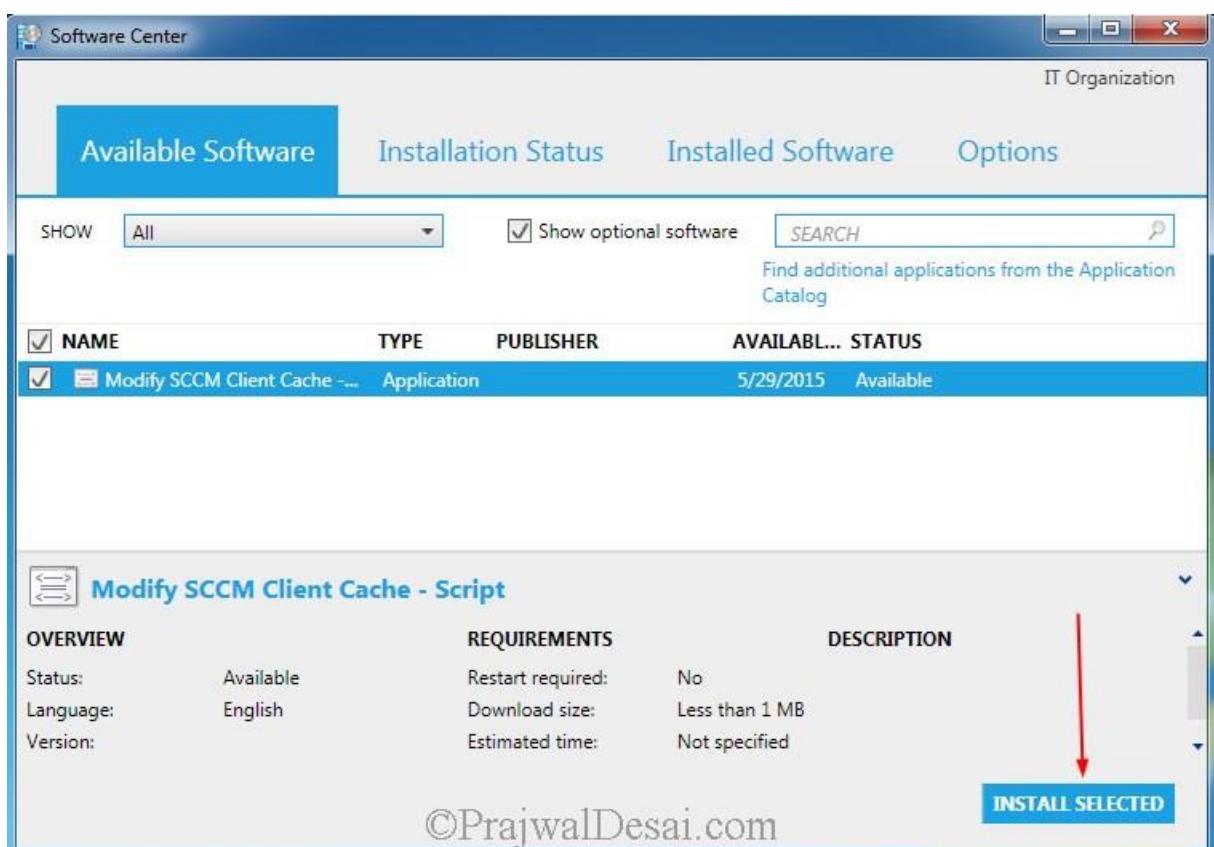
Comments (optional):

©PrajwalDesai.com

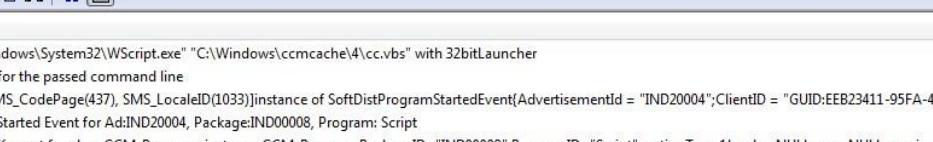
Set the **Purpose** to **Available** or **Required**. In this example I am setting it to **Available**. Click **Next** and complete the remaining steps by clicking **Next**.



On the client machine open the **Software Center** and select the package and click **Install Selected**.



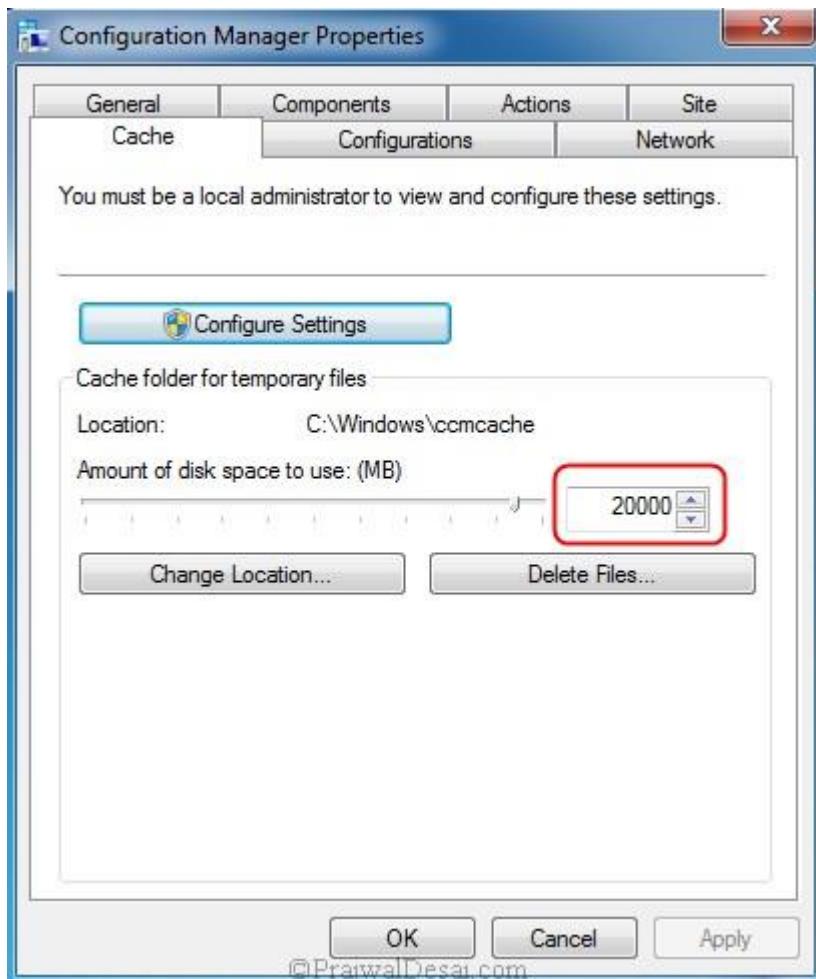
Open the **execmgr.log** file on the client machine to see more details on the program execution.



The screenshot shows the Configuration Manager Trace Log Tool interface. The main window displays a log of events from a trace log file. A red arrow points to a specific line in the log:

```
Running "C:\Windows\System32\WScript.exe" "C:\Windows\ccmcache\4\cc.vbs" with 32bitLauncher
Created Process for the passed command line
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramStartedEvent[AdvertisementId = "IND20004";ClientID = "GUID:EEB23411-95FA-44A0... execmgr
Raised Program Started Event for Ad:IND20004, Package:IND00008, Program: Script
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00008",ProgramID="Script", actionType 1, value NULL, user NULL, session 42...
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00008",ProgramID="Script", actionType 1, value , user NULL, session 4294967...
MTC task with id {8EF34734-ADA2-4BB1-BC82-2D0BC561A332}, changed state from 4 to 5
Program exit code 0
Looking for MIF file to get program status
Script for Package:IND00008, Program: Script succeeded with exit code 0
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessfullyEvent[AdvertisementId = "IND20004";ClientID = "GUID:EEB2... execmgr
Raised Program Success Event for Ad:IND20004, Package:IND00008, Program: Script
Execution is complete for program Script. The exit code is 0, the execution status is Success
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00008",ProgramID="Script", actionType 10, value Result:TRUE,SDKCallerId: u... execmgr
Requesting MTC to delete task with id: {8EF34734-ADA2-4BB1-BC82-2D0BC561A332}
MTC task with id: {8EF34734-ADA2-4BB1-BC82-2D0BC561A332} deleted successfully.
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00008",ProgramID="Script", actionType 11, value , user NULL, session 4294967... execmgr
```

After the script is run you can see the client cache size is increased.

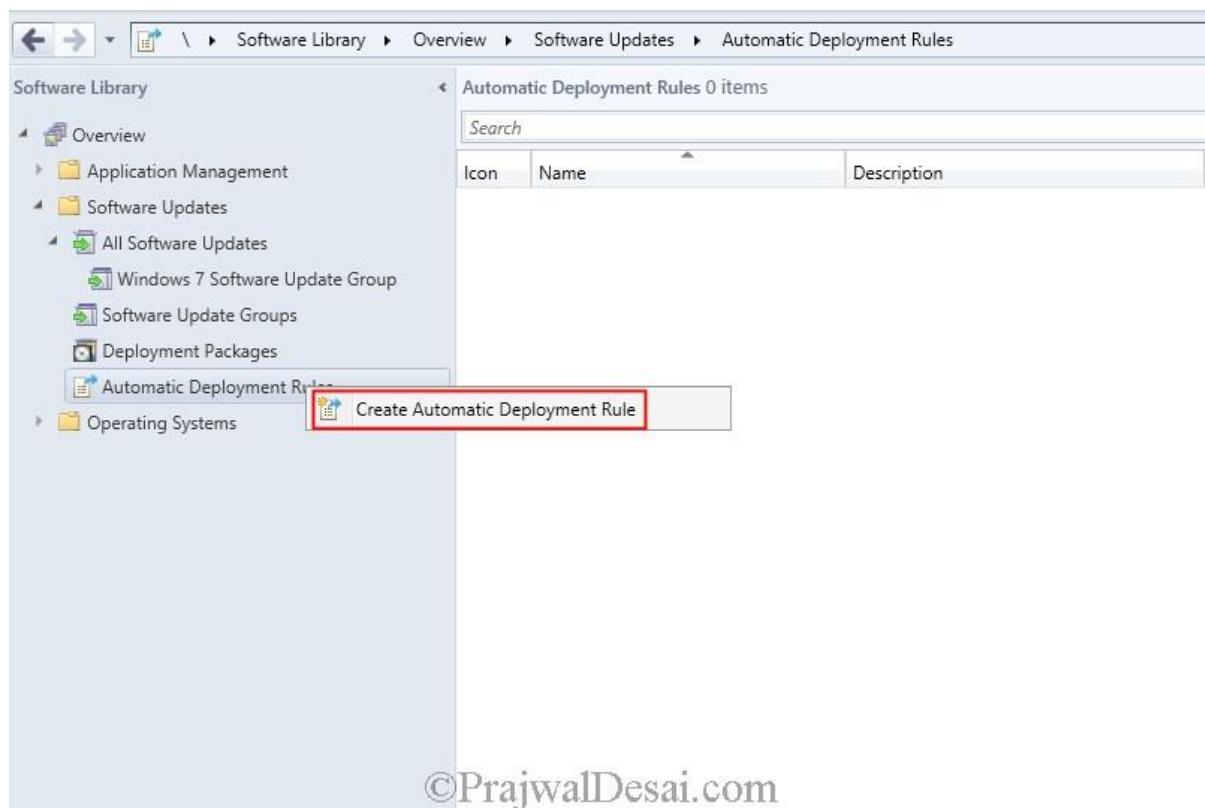


[Create Automatic Deployment Rule in SCCM 2012 R2](#)

In this post we will see how to Create Automatic Deployment Rule in SCCM 2012 R2. ADRs fill a large gap in software update functionality that existed in ConfigMgr 2007, as there was no way to automatically download and assign updates. Thanks to Microsoft for introducing the ADR's which have the ability to automatically approve updates and deploy them. You typically use this method of deployment for your monthly [software updates](#) (generally known as Patch Tuesday) and for managing definition updates. When the rule runs, software updates are removed from the software update group (if using an existing group), the [software updates](#) that meet a specified criteria (for example, all security software updates released in the last week) are added to a software update group, the content files for the software updates are downloaded and copied to distribution points, and the software updates are deployed to client computers in the target collection.

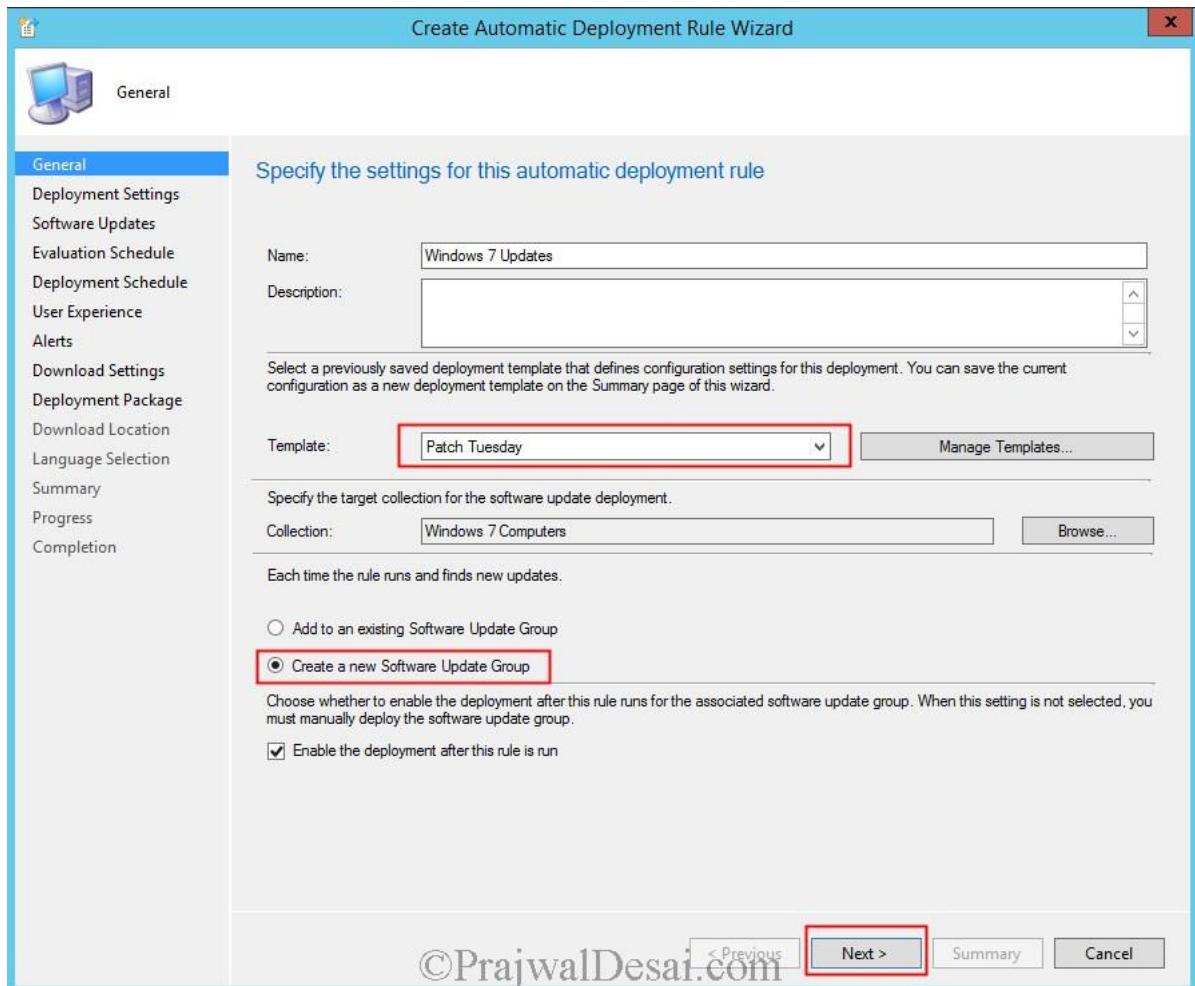
Create Automatic Deployment Rule In SCCM 2012 R2

To create ADR, right click on **Automatic Deployment Rules** under **Software Library > Software Updates** and click **Create Automatic Deployment Rule**.



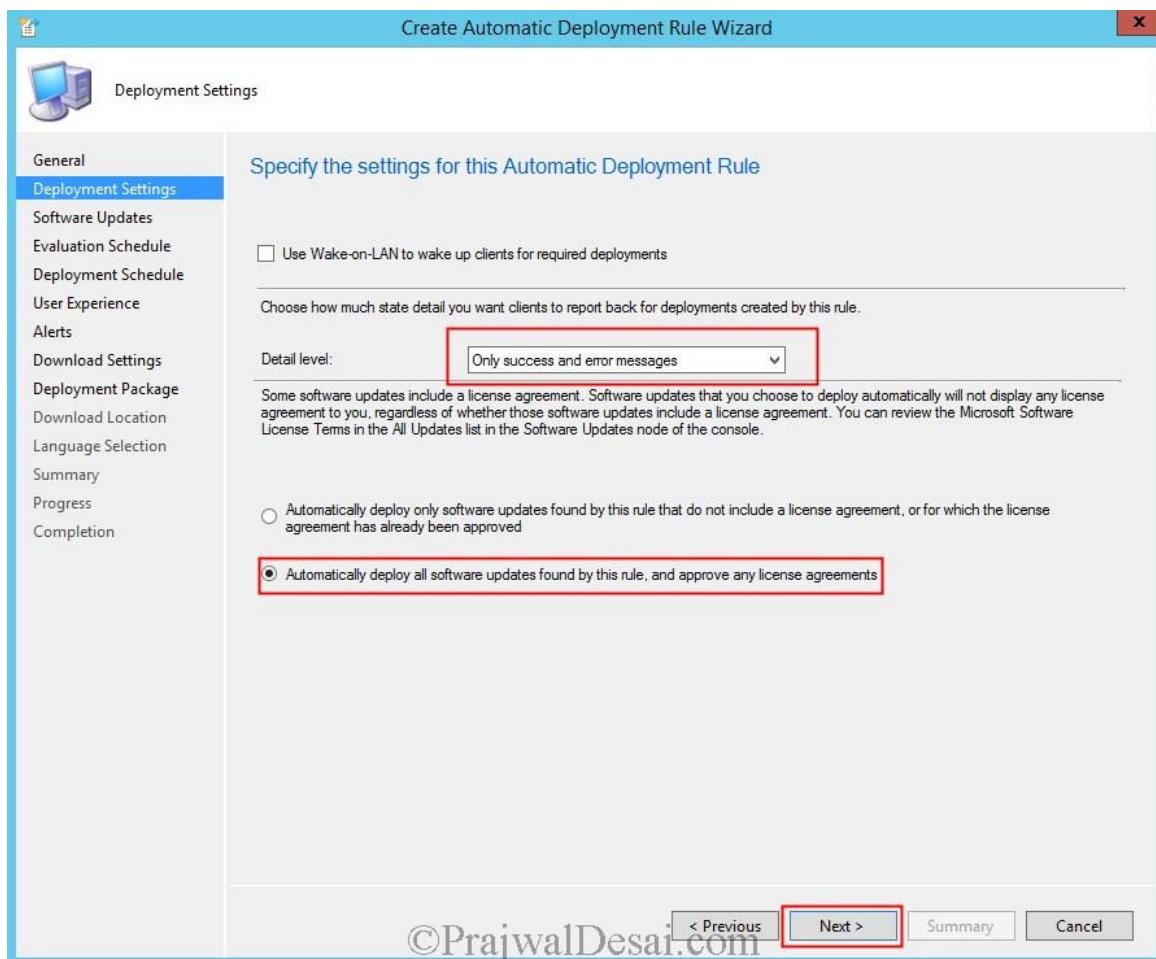
©PrajwalDesai.com

Specify the name for the ADR. Choose the template, click **Browse** and select the target collection for update deployment. Next choose **Create a new Software Update Group**. If you choose to add to an existing update group, a new one is created the first time the ADR is evaluated and reused for each subsequent evaluation of the ADR. If you choose to use a new update group, then a new update group is created for every evaluation of the ADR. Leave the box checked for **Enable the deployment after this rule is run**. Click **Next**.



On the Deployment Settings page, choose the detail level as **Only success and error messages**. Next, choose **Automatically deploy all software updates found by this rule and approve any license agreements**.

Click Next.

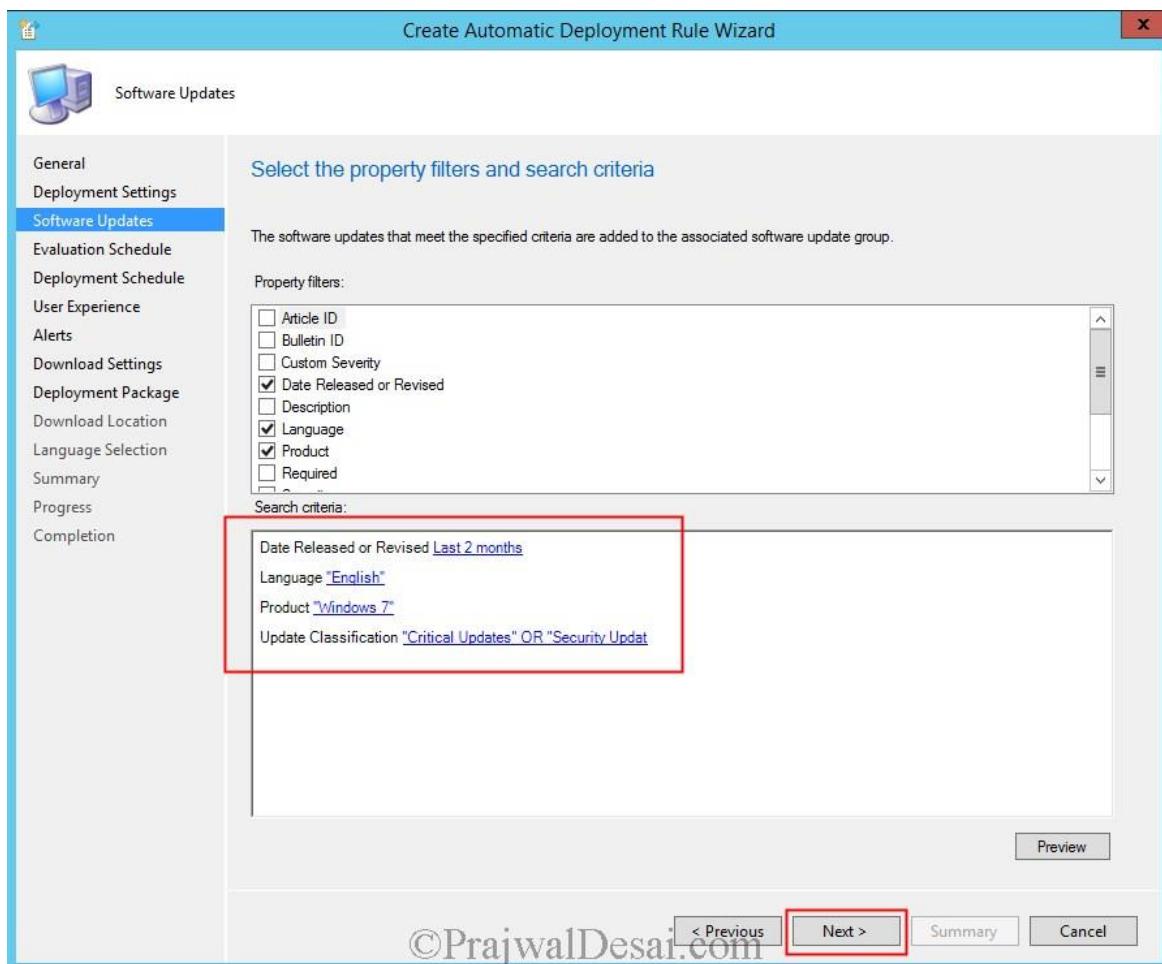


ADRs populate an update deployment with references to updates based on a pre-defined filter similar to console filters described in **All Software Updates**” section. A subset of the filter criteria is displayed on this page, where you select and define the criteria for finding the updates for inclusion in the update deployment.

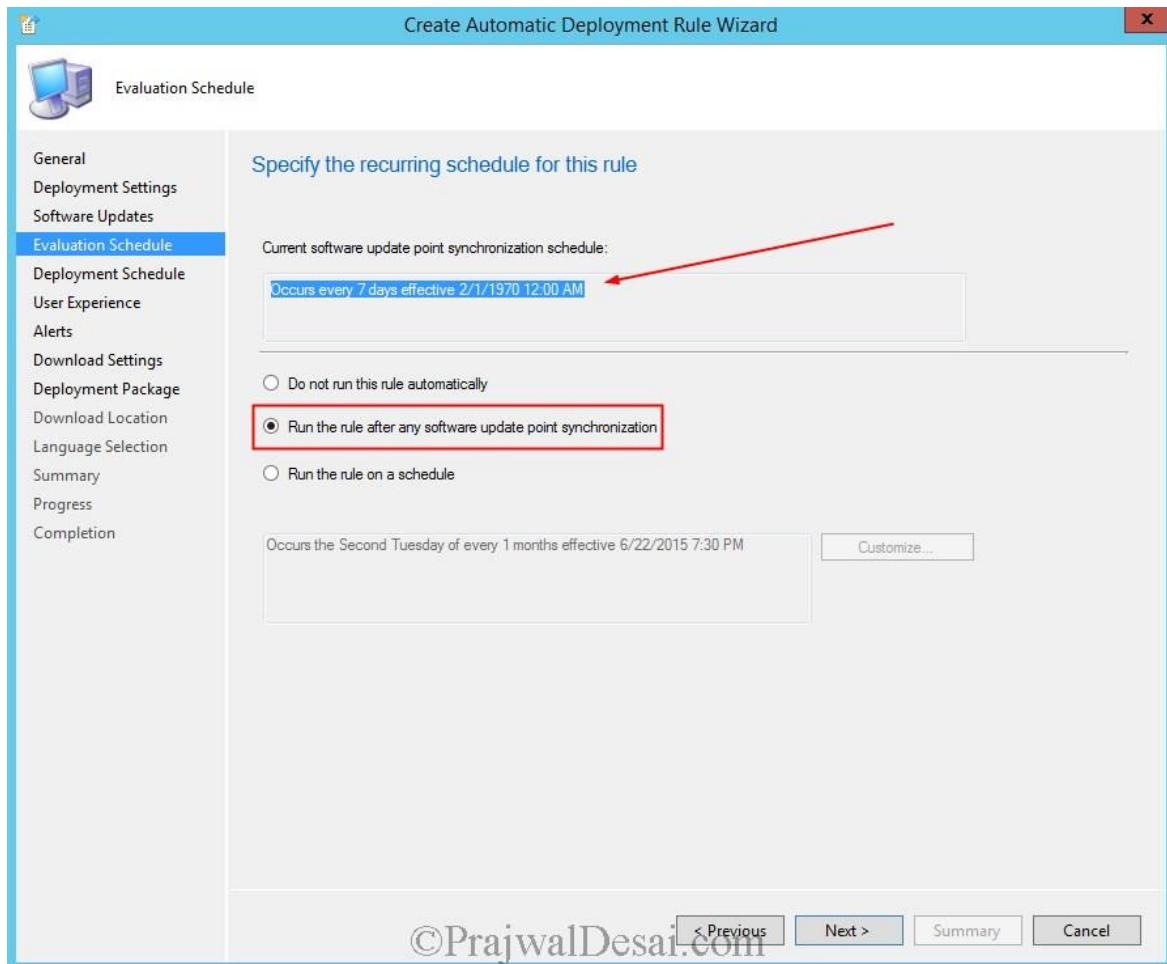
I will be choosing the following property filters.

- 1) Date Released or revised for last 2 months.
- 2) Updates to be in English language.
- 3) Updates target Windows 7 Product.
- 4) Updates have to be Critical updates or Security Updates.

Click **Next**.

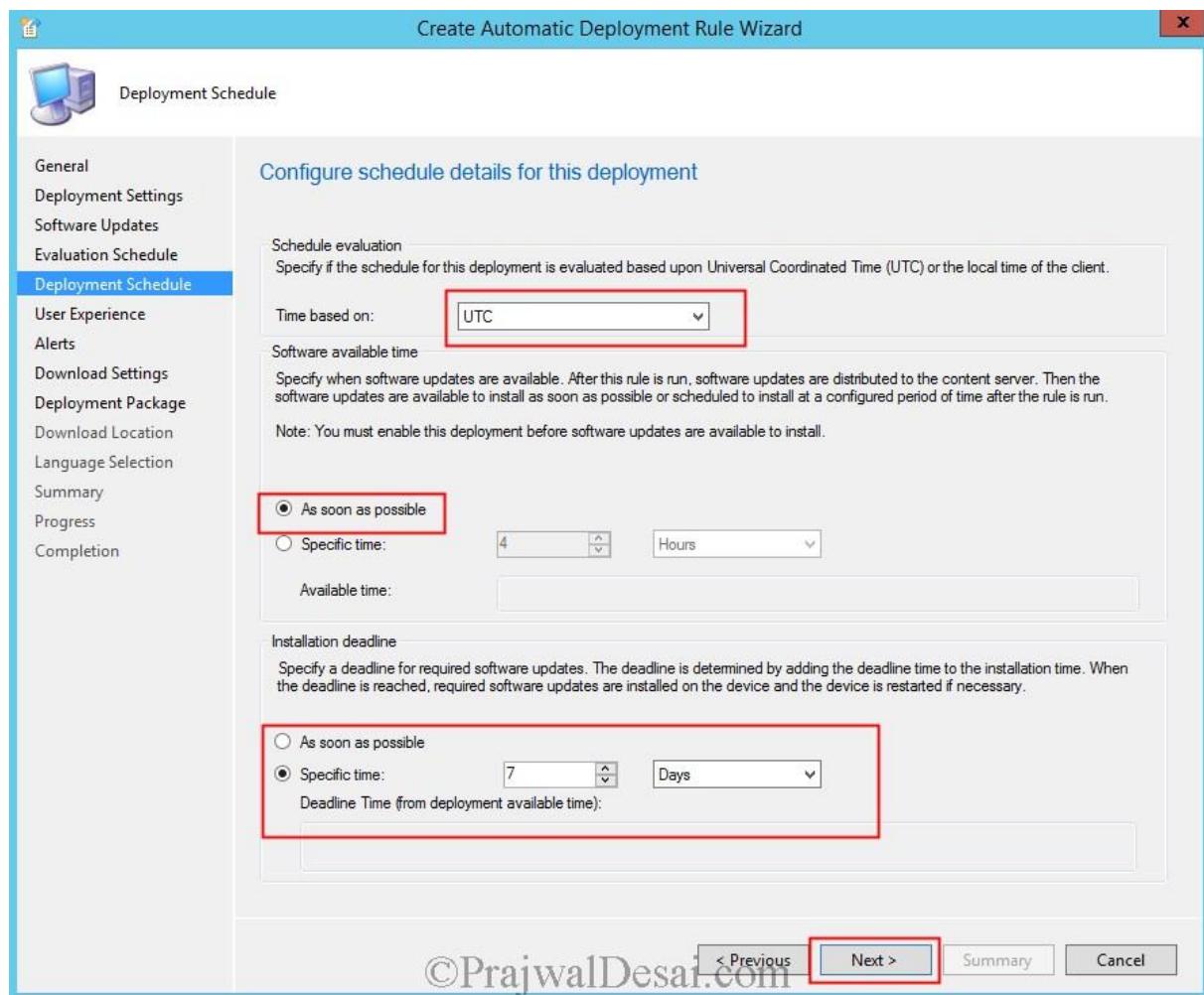


This page lets you configure when you want the ADR rule to be evaluated. This is important because the ADR rule runs as per the schedule that you configure here so configure this carefully. For convenience, it also shows the SUP synchronization time so you can coordinate the two times. Note – It doesn't make sense to run an ADR evaluation more frequently than the SUP synchronization time because there will be no new updates to find. You can also disable the automatic, scheduled evaluation of an ADR, leaving it to be initiated manually. In this example I will choose to run the rule after SUP synchronization. So my rule would be run every 7 days when the SUP sync happens. Click **Next**.



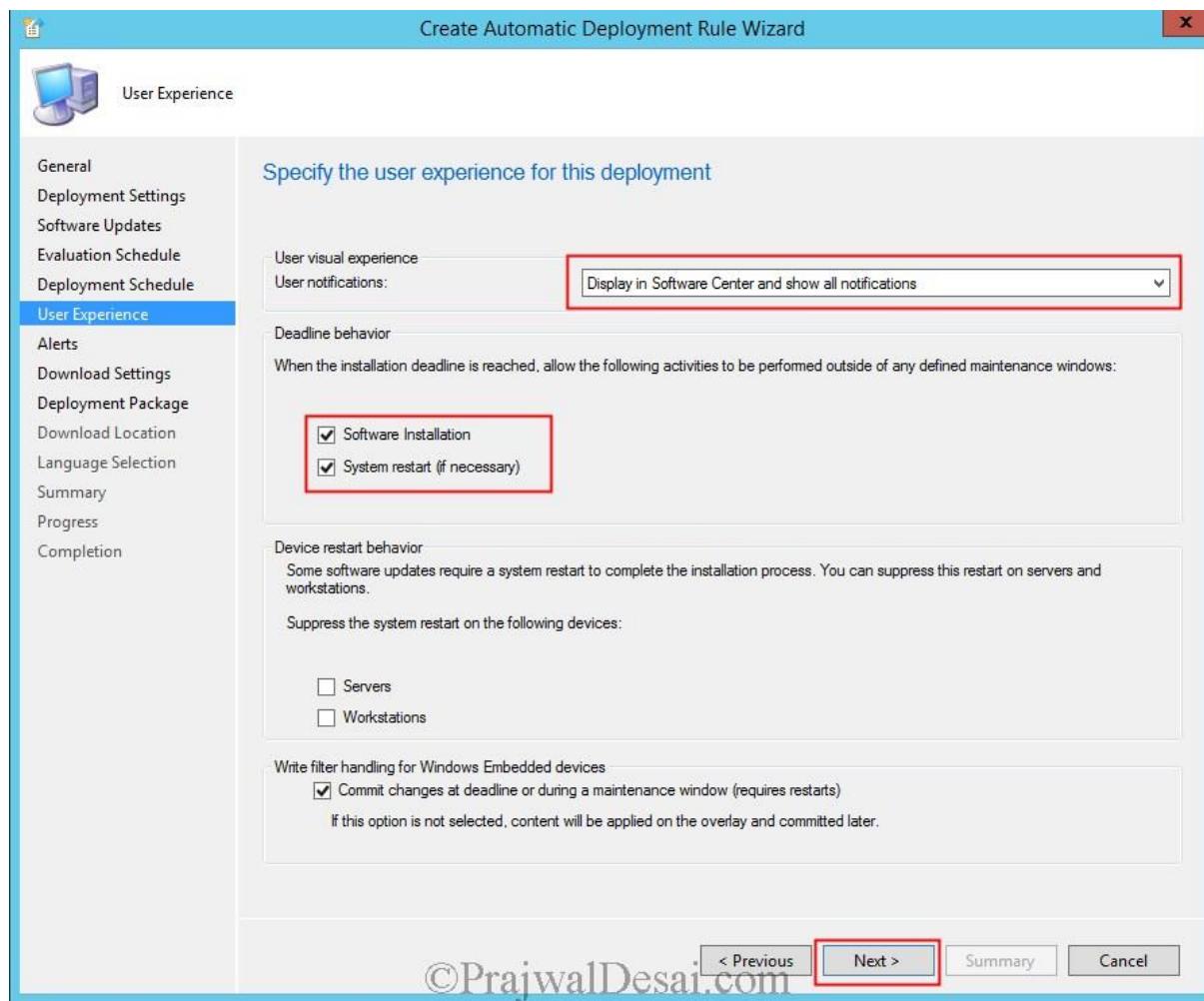
Specify the schedule details for the deployment, set **Time based on** to UTC. Choose the **Software available time** to As soon as possible and **Installation deadline** to 7 days. I know 7 days is a lot of time, you could choose your settings here.

Click Next.

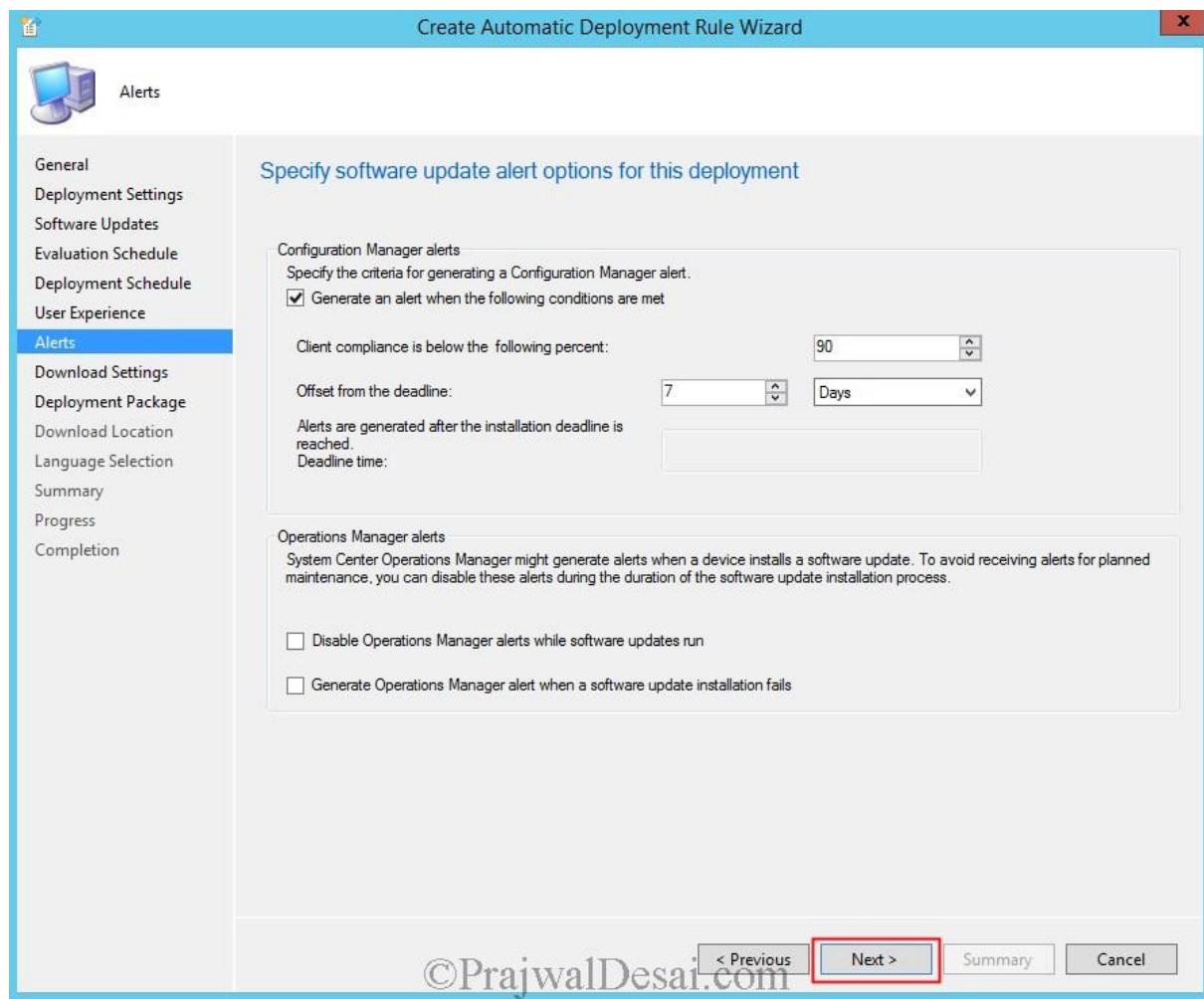


©PrajwalDesai.com

User Experience – Choose the settings as shown in the below screenshot and click **Next**.

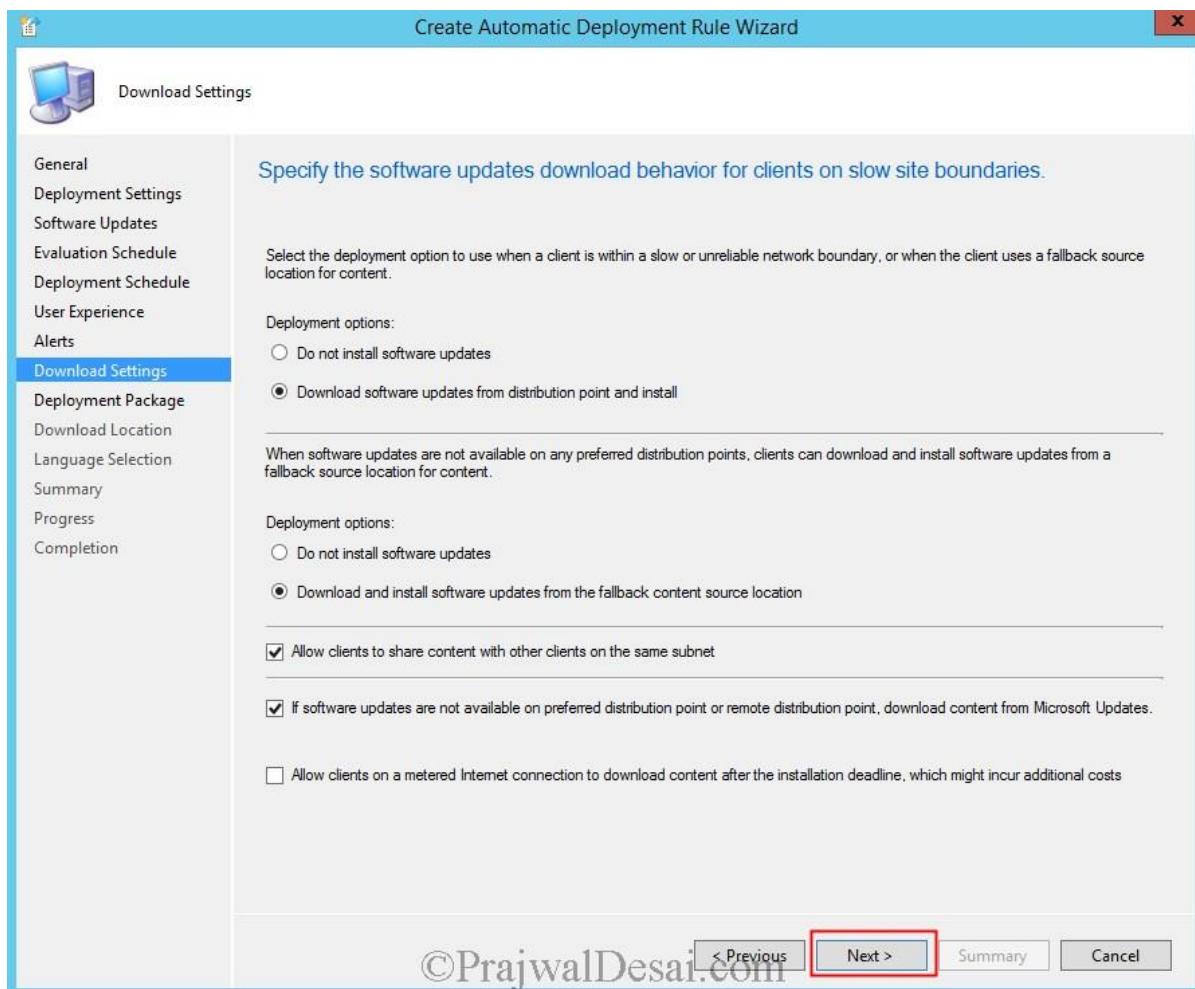


Alerts – I haven't configured anything here. Click **Next**.



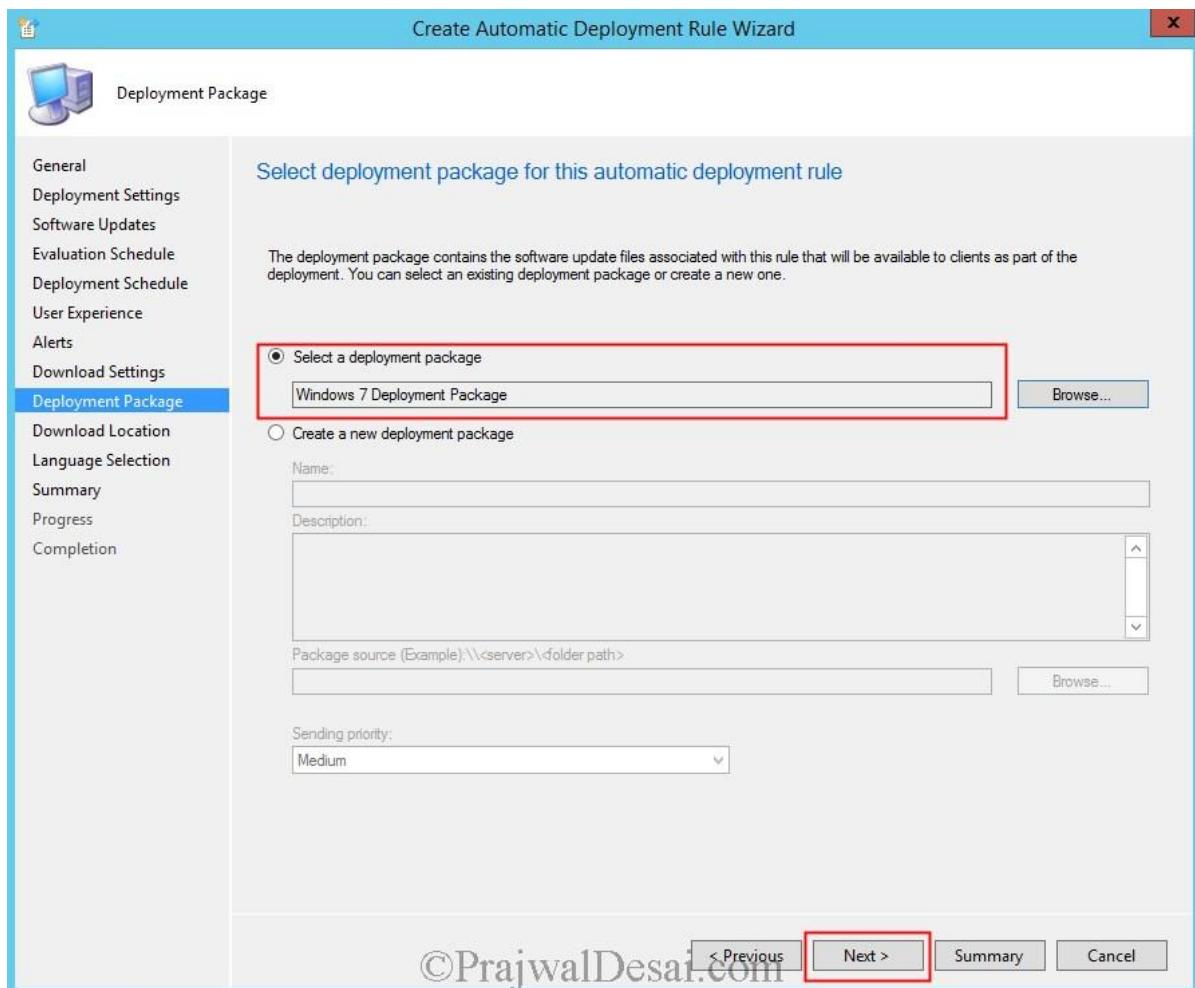
©PrajwalDesai.com

Click Next.



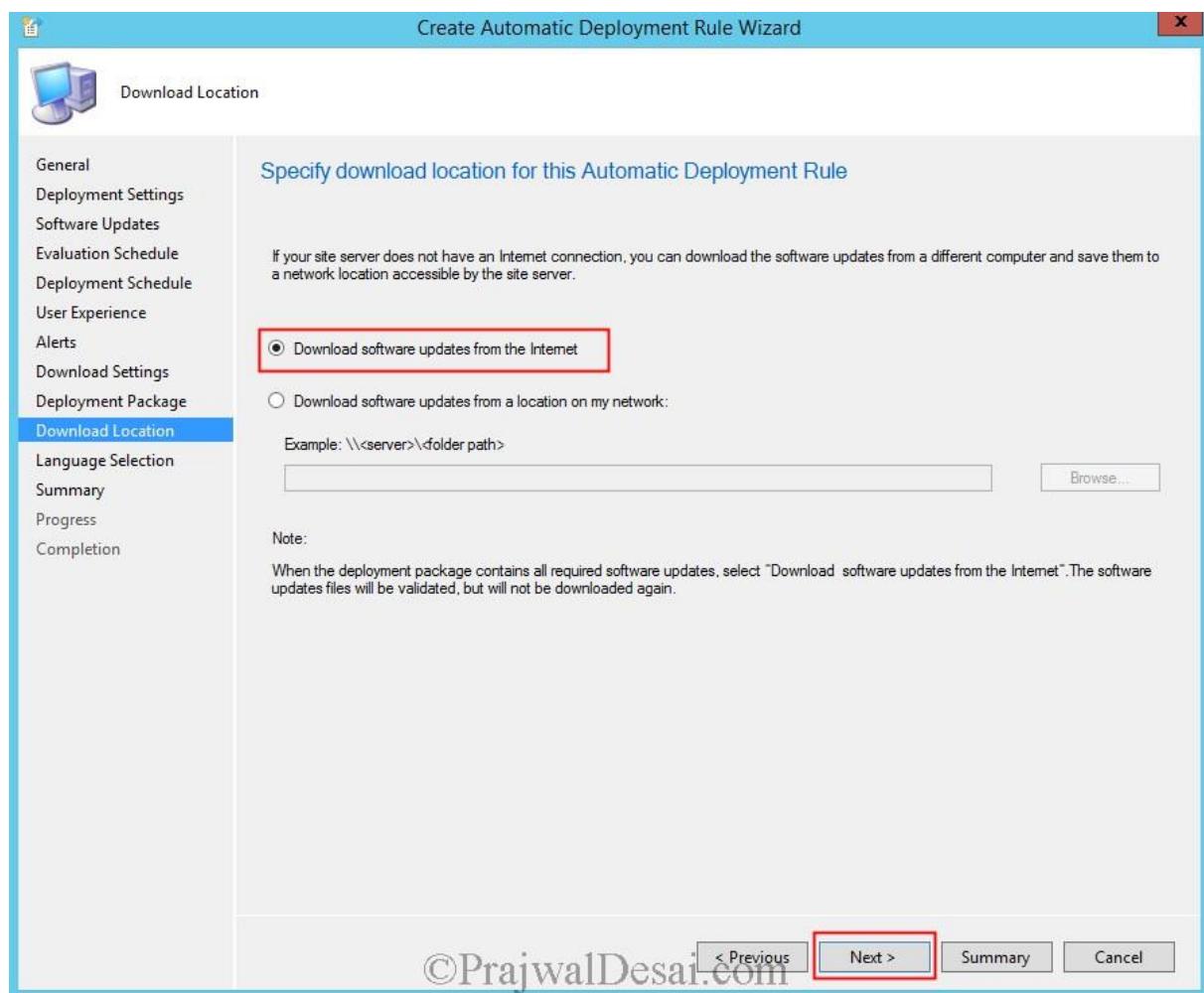
You need to specify a deployment package. Click on Browse and select the deployment package. If you have not created one then click on **Create a new deployment package**. If you want to know the steps to create deployment package click this [link](#).

What are Deployment Packages – Similar to software distribution packages, deployment packages are simply the collection of files needed for a set of updates. They must have a source folder and be available to clients by assigning them to distribution points. There is no way to create a deployment package from the console, you can only create one using the Deploy Software Updates Wizard or the Download Software Updates Wizard.

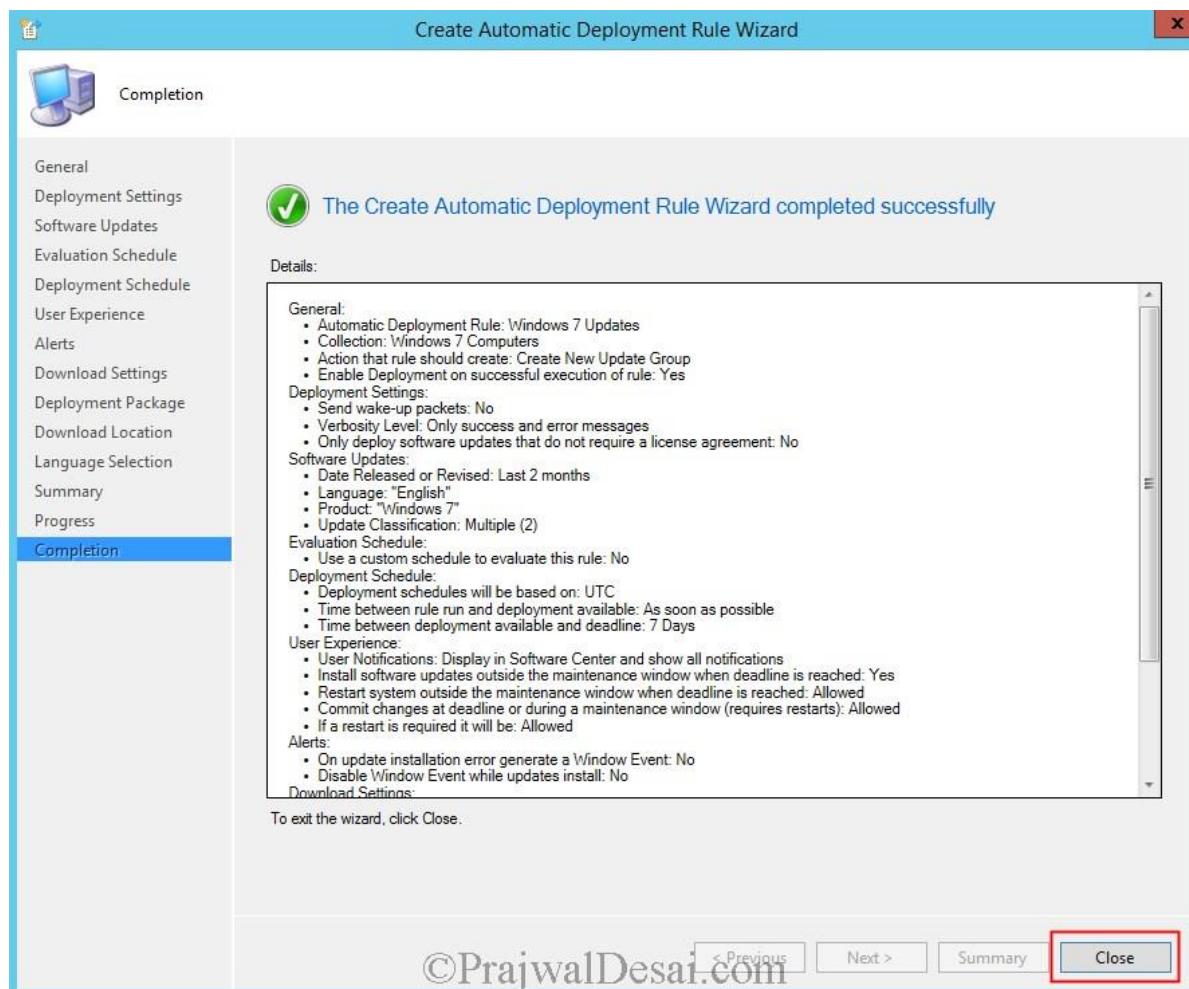


Choose Download software updates from Internet.

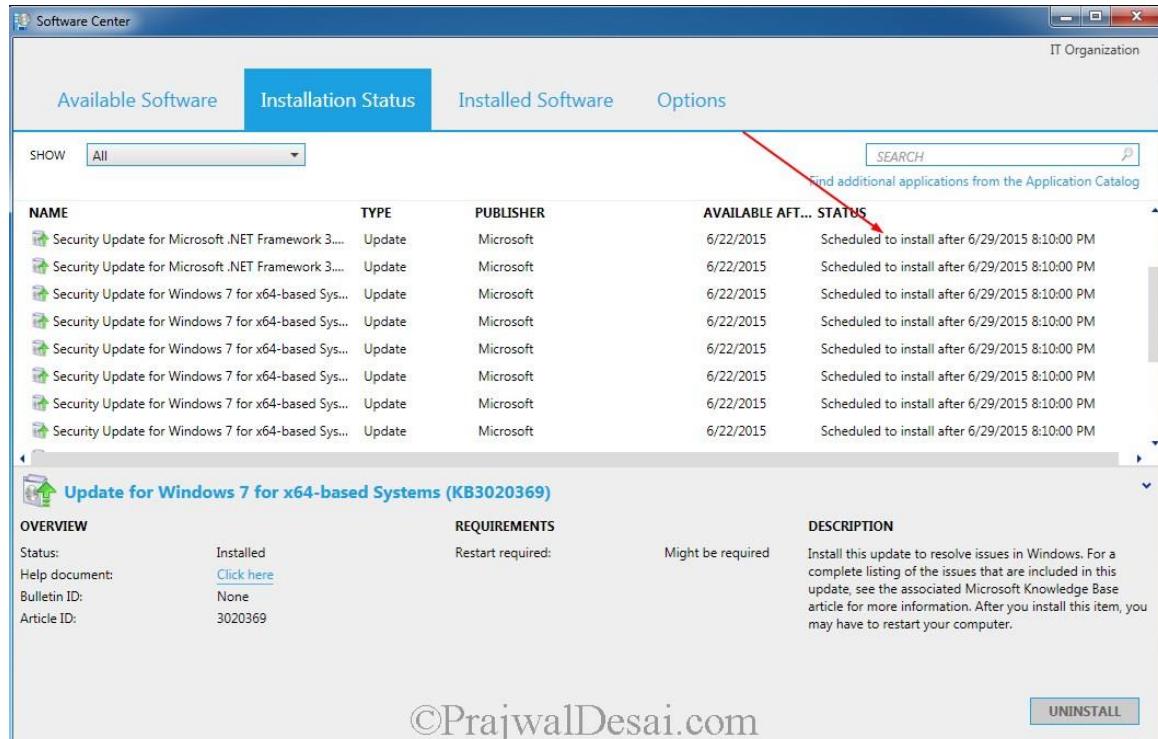
Click Next.



Complete the wizard. Click **Close**.



Wait for sometime and on the client machine launch the software center. We see that the deployment is scheduled to run 7 days after the creation of rule i.e. on 29th.



The screenshot shows the Software Center window with the 'Installation Status' tab selected. A red arrow points from the status column to the 'Status' column, highlighting the scheduled installation times. Below the table, a specific update for Windows 7 is detailed.

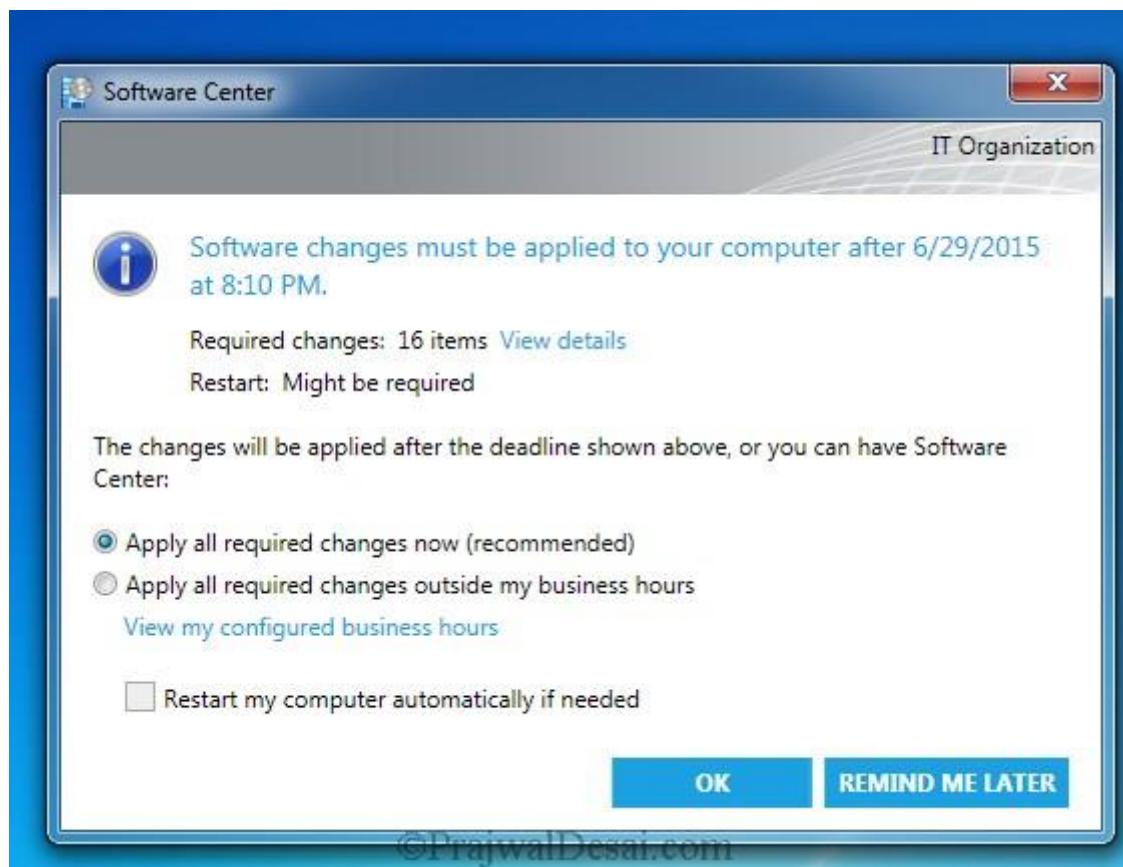
NAME	TYPE	PUBLISHER	AVAILABLE AFT...	STATUS
Security Update for Microsoft .NET Framework 3....	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Microsoft .NET Framework 3....	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM
Security Update for Windows 7 for x64-based Sys...	Update	Microsoft	6/22/2015	Scheduled to install after 6/29/2015 8:10:00 PM

Update for Windows 7 for x64-based Systems (KB3020369)

OVERVIEW	REQUIREMENTS	DESCRIPTION
Status: Installed Help document: Click here Bulletin ID: None Article ID: 3020369	Restart required: Might be required	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

©PrajwalDesai.com UNINSTALL

On the client machine we also see a software updates notification.



The screenshot shows a software update notification dialog box. It displays a message about required changes, the number of items, and restart requirements. It includes options for applying changes now or outside business hours, and a checkbox for automatic restart. At the bottom, there are 'OK' and 'REMIND ME LATER' buttons.

Software changes must be applied to your computer after 6/29/2015 at 8:10 PM.

Required changes: 16 items [View details](#)

Restart: Might be required

The changes will be applied after the deadline shown above, or you can have Software Center:

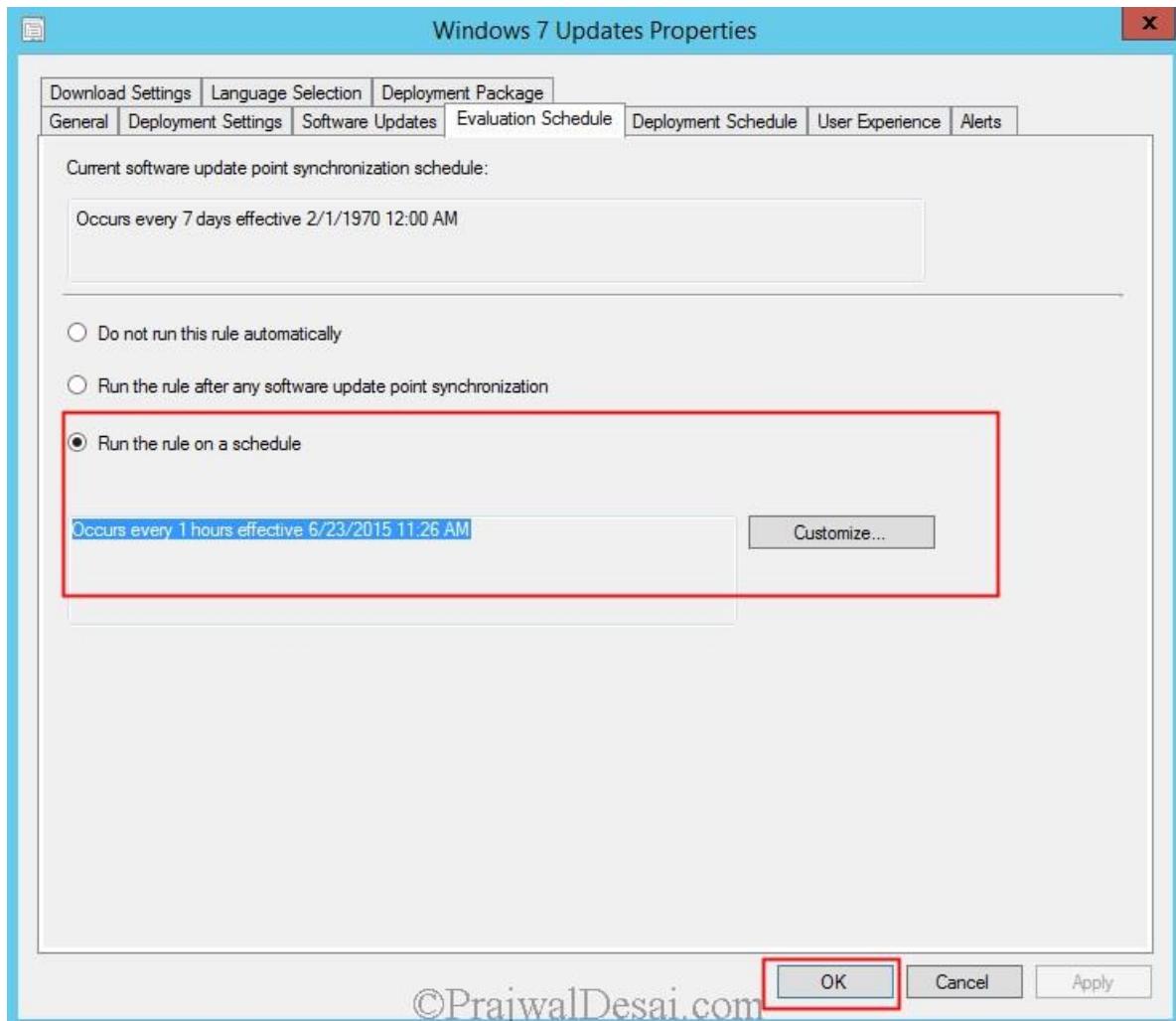
Apply all required changes now (recommended)
 Apply all required changes outside my business hours
[View my configured business hours](#)

Restart my computer automatically if needed

OK **REMIND ME LATER**

©PrajwalDesai.com

Note – I am making this change to show the updates deployment quickly. We know that updates will be deployed on 29th. Instead of waiting for next 7 days I will now change the evaluation schedule of the ADR. Right the ADR rule and click on **Properties**. Click Evaluation Schedule and choose **Run the rule on a schedule**. I have set the rule to run every one hour (You need not try this on Production environment, just stick to the schedule that you had configured earlier). Click **OK**.



On the client machine open the software center and now we see that the updates are scheduled to install on 23rd at 1:27 PM.

The screenshot shows the Windows Software Center interface. The 'Available Software' tab is selected. A green oval highlights the 'STATUS' column for several updates, which all show 'Scheduled to install after 6/23/2015 1:27:00 PM'. A red arrow points from the status bar area towards this highlighted section. Below the table, a specific update for Internet Explorer is detailed:

Cumulative Security Update for Internet Explorer 8 for Windows 7 for x64-based Systems (KB3049563)				
OVERVIEW		REQUIREMENTS		DESCRIPTION
Status:	Scheduled to install after 6/23/2015 1:27:00 PM	Restart required:	Might be required	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
Help document:	Click here			
Bulletin ID:	MS15-043			
Article ID:	3049563			

At the bottom right of the Software Center window, there are 'SCHEDULE' and 'INSTALL' buttons.

At 1:28 PM we see that the status of updates were seen as Waiting to install. The updates are not being installed.

The screenshot shows the Software Center interface with the 'Installation Status' tab selected. A red box highlights the 'STATUS' column, which lists various update items as 'Waiting to install'. Another red box highlights the 'Installed' status of the 'Modify SCCM Client Cache - Script' application. A callout bubble points to the 'REINSTALL' button with the text 'Check the Time. its 1:28 PM.' A red arrow points from the 'REINSTALL' button towards the status column. The system tray at the bottom right shows the date as 6/23/2015 and the time as 1:28 PM.

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
Cumulative Security Update for Internet Explorer 8 for Wi...	Update	Microsoft	6/22/2015	Waiting to install
Cumulative Security Update for Internet Explorer 8 for Wi...	Update	Microsoft	6/22/2015	Waiting to install
Modify SCCM Client Cache - Script	Application		5/29/2015	Installed
Security Update for Microsoft .NET Framework 3.5.1 on...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Microsoft .NET Framework 3.5.1 on...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Microsoft .NET Framework 3.5.1 on...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install
Security Update for Windows 7 for x64-based Systems (K...	Update	Microsoft	6/22/2015	Waiting to install

OVERVIEW

Status:	Installed
Language:	English
Version:	
Date published:	5/29/2015
Date Modified:	5/29/2015

REQUIREMENTS

Restart required:	No
Download size:	Less than 1 MB
Estimated time:	Not specified
Total components:	1

DESCRIPTION

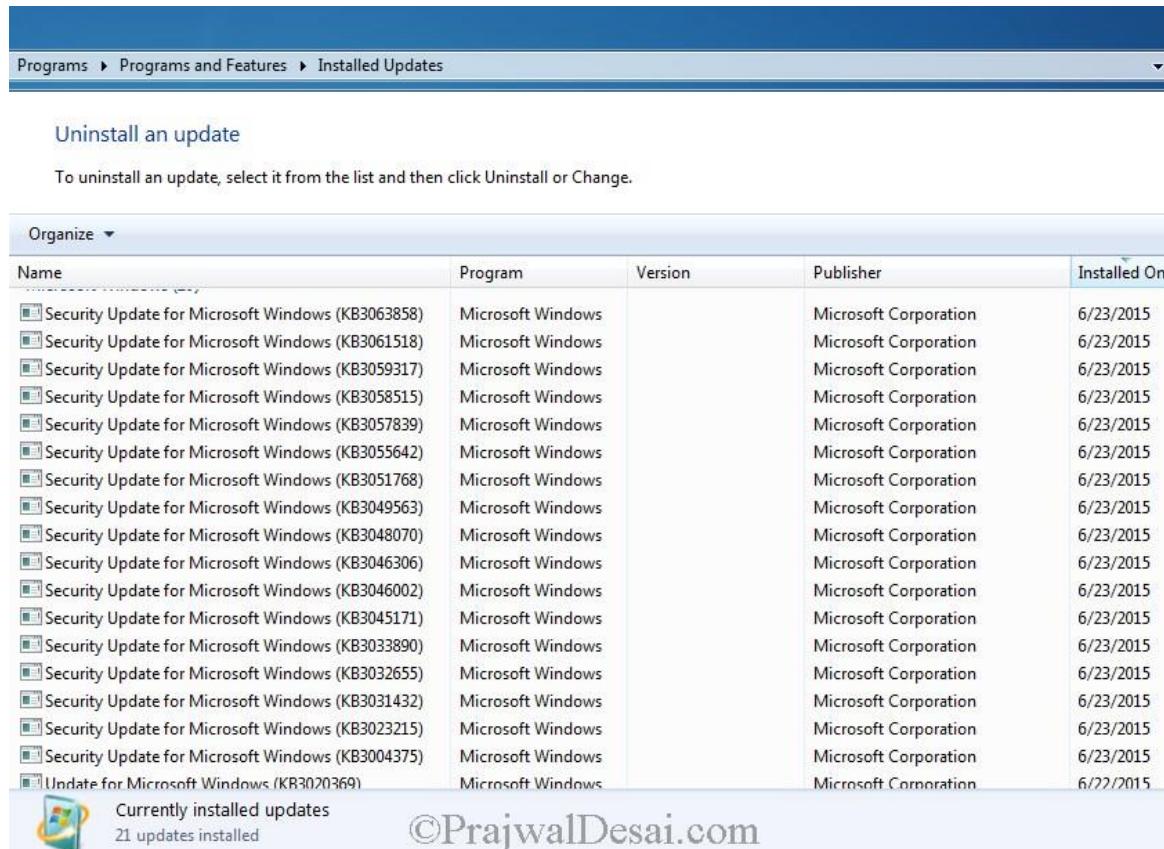
REINSTALL

Check the Time.
its 1:28 PM.

1:28 PM
6/23/2015

The updates have been installed and the client machine needs to a restart.

After the client computer is restarted, launch the control panel, click on **Programs > Programs and Features** and click on **Installed Updates**. You should now see the list of updates installed on the client machine deployed via ADR.



The screenshot shows the Windows Control Panel with the path 'Programs > Programs and Features > Installed Updates'. The title bar says 'Uninstall an update' and a note below it says 'To uninstall an update, select it from the list and then click Uninstall or Change.' A table lists 21 security updates for Microsoft Windows, all installed on 6/23/2015 except for one on 6/22/2015. The table has columns for Name, Program, Version, Publisher, and Installed On. At the bottom left, there's a Windows logo icon and the text 'Currently installed updates 21 updates installed'.

Name	Program	Version	Publisher	Installed On
Security Update for Microsoft Windows (KB3063858)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3061518)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3059317)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3058515)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3057839)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3055642)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3051768)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3049563)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3048070)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3046306)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3046002)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3045171)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3033890)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3032655)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3031432)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3023215)	Microsoft Windows		Microsoft Corporation	6/23/2015
Security Update for Microsoft Windows (KB3004375)	Microsoft Windows		Microsoft Corporation	6/23/2015
Update for Microsoft Windows (KB3020369)	Microsoft Windows		Microsoft Corporation	6/22/2015

©PrajwalDesai.com

Troubleshooting

- 1) Once you deploy the ADR, the status of that new deployment should be checked regularly by looking at **Monitoring | Deployments**.
- 2) Review **ruleengine.log** for troubleshooting purpose.

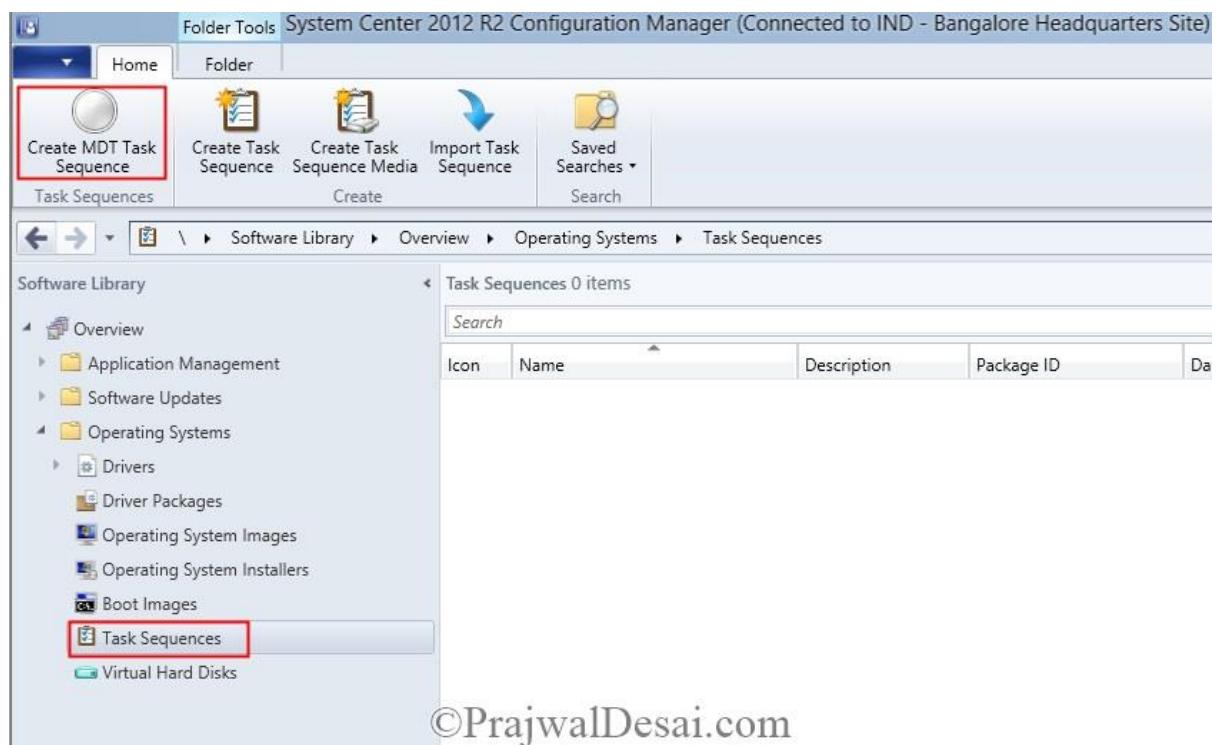
A lot of effort has gone in putting all this together. If you have got any questions then do write in comments.

[Deploying Windows 7 Using MDT UDI](#)

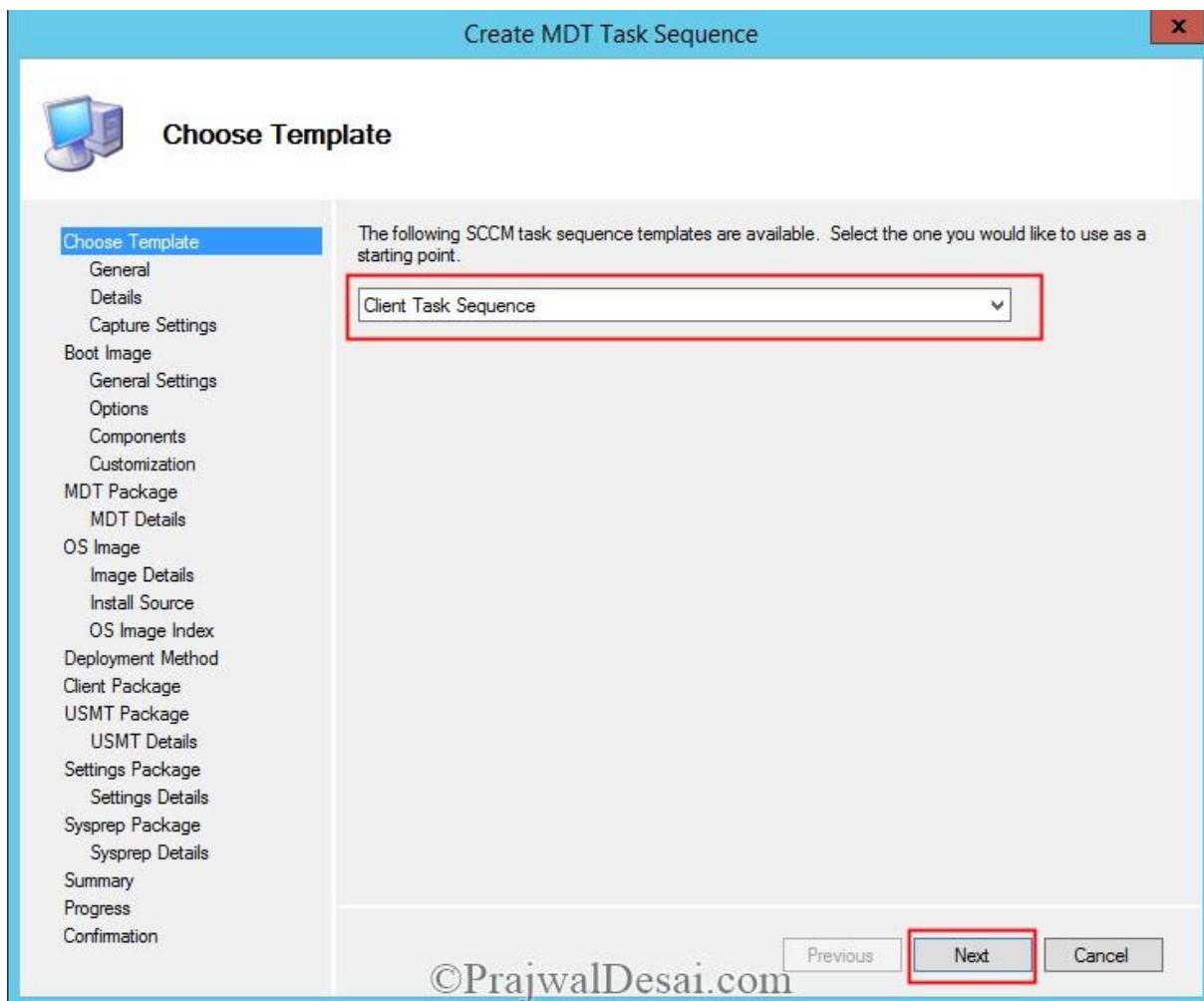
The Microsoft Deployment Toolkit (MDT) supports three types of deployments Zero Touch Installation (ZTI), Lite Touch Installation (LTI), and User Driven Installation (UDI). However each deployment type is different. LTI deployments require limited user interaction. ZTI is a fully automated deployment scheme in which installation requires no user interaction whatsoever. UDI deployments require full manual intervention to respond to every installation prompt, such as machine name, password or language setting. ZTI and UDI deployments both require a Microsoft System Center infrastructure. User Driven Installation helps simplify the deployment of Windows client operating systems, such as Windows 7, 8.1, to computers using the operating system deployment (OSD) feature in Microsoft System Center 2012 R2 Configuration Manager. UDI is part of the [Microsoft Deployment Toolkit](#) (MDT). Basically UDI provides a wizard-driven interface that allows you to provide configuration information immediately prior to performing the deployment. User Driven Installation would provide your organization with a highly customizable deployment method that allows deployment choices to be done by the user and also provides greater flexibility in the deployment process. In this post we will see the steps for deploying Windows 7 using MDT UDI method. Before we do that the MDT has to be [integrated with SCCM](#).

Deploying Windows 7 Using MDT UDI

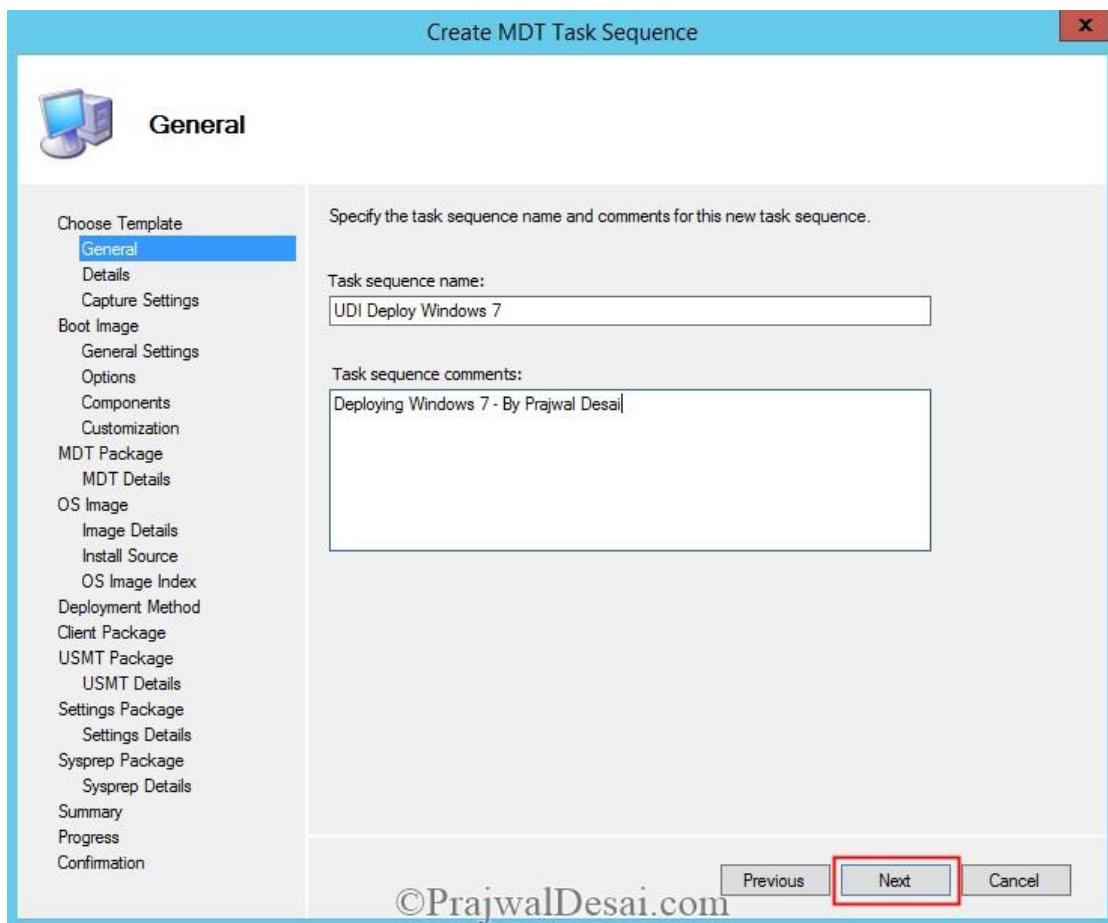
In the Configuration Manager console, in the navigation pane, click **Software Library**. In the Software Library workspace, go to **Overview > Operating Systems > Task Sequences**. On the Ribbon, on the Home tab, in the Task Sequences group, click **Create MDT Task Sequence**.



Select **Client Task Sequence**, and then click **Next**.

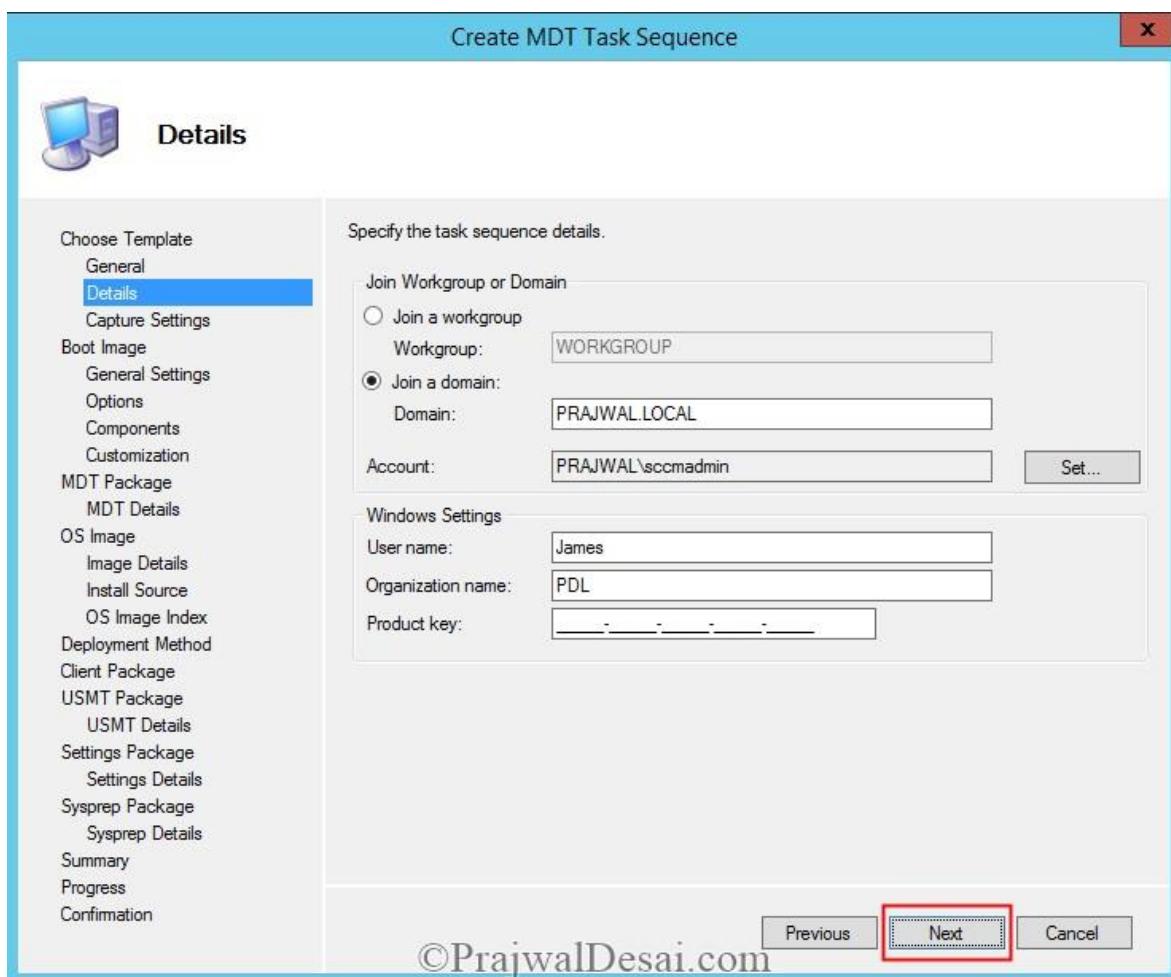


Provide a name to the TS and click **Next**.



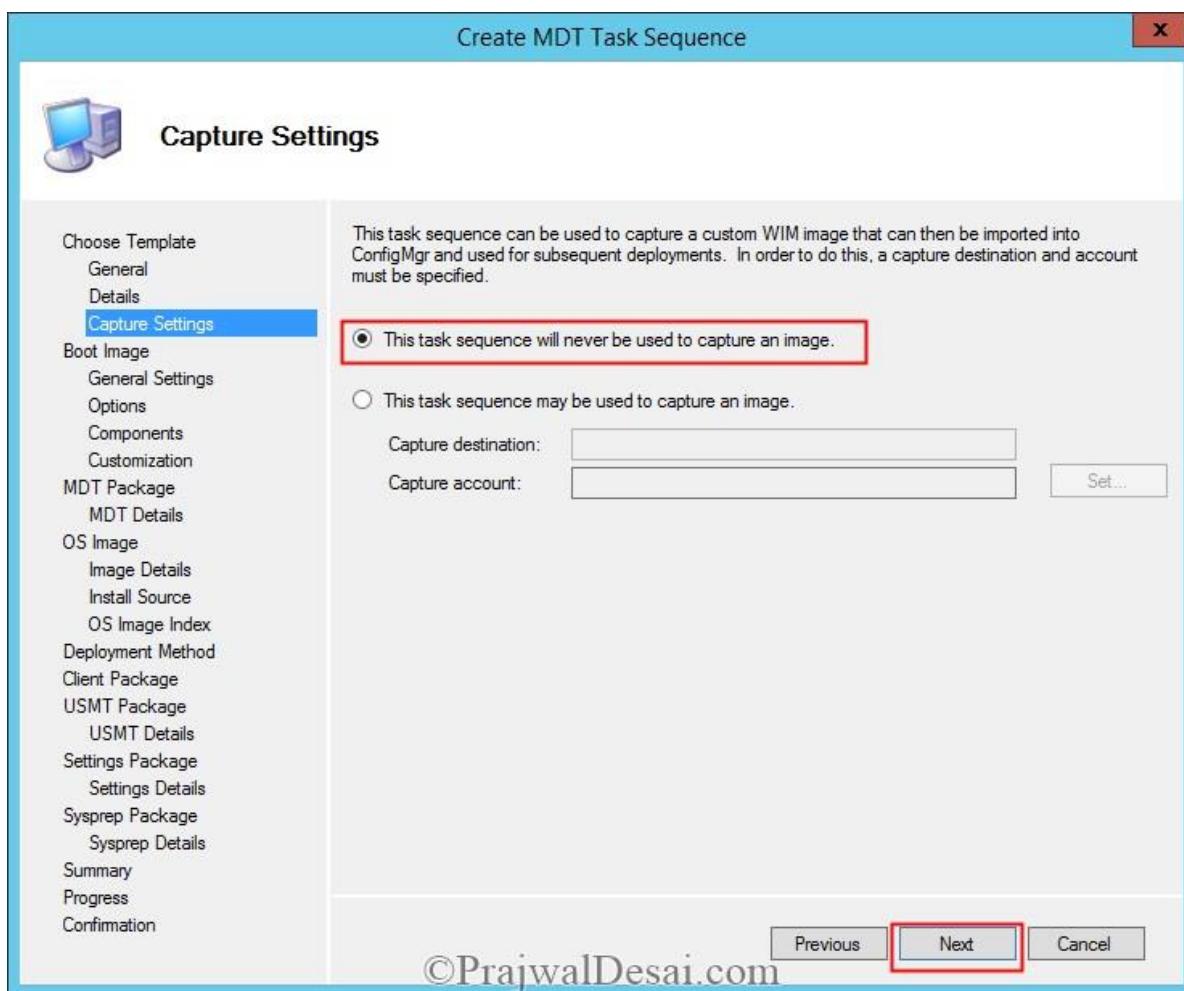
You could choose to join the computer to workgroup or to the domain. In this case we will be joining the PC to the domain, so provide the Domain name, User Name, Organization Name.

Click Next.



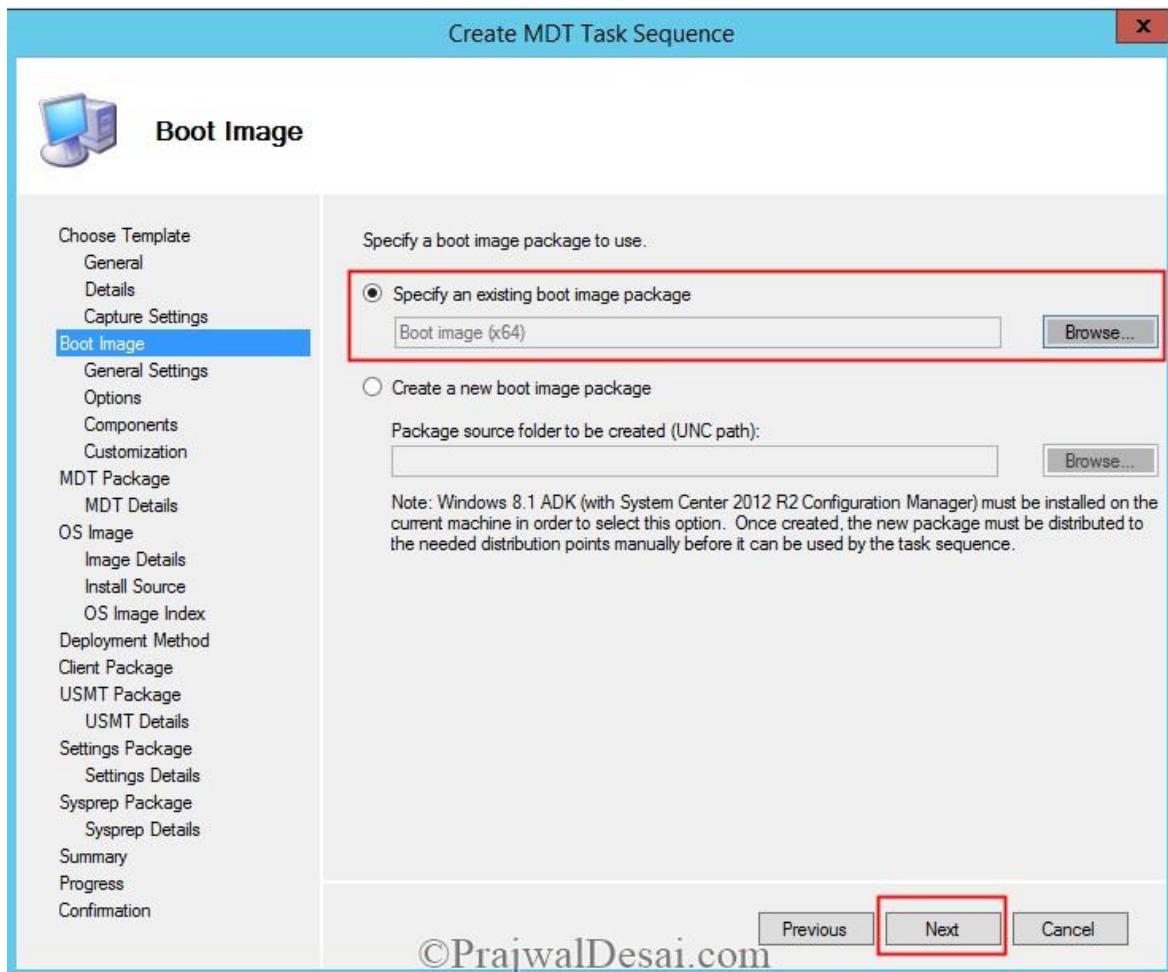
Click This task sequence will never be used to capture and image.

Click **Next**.



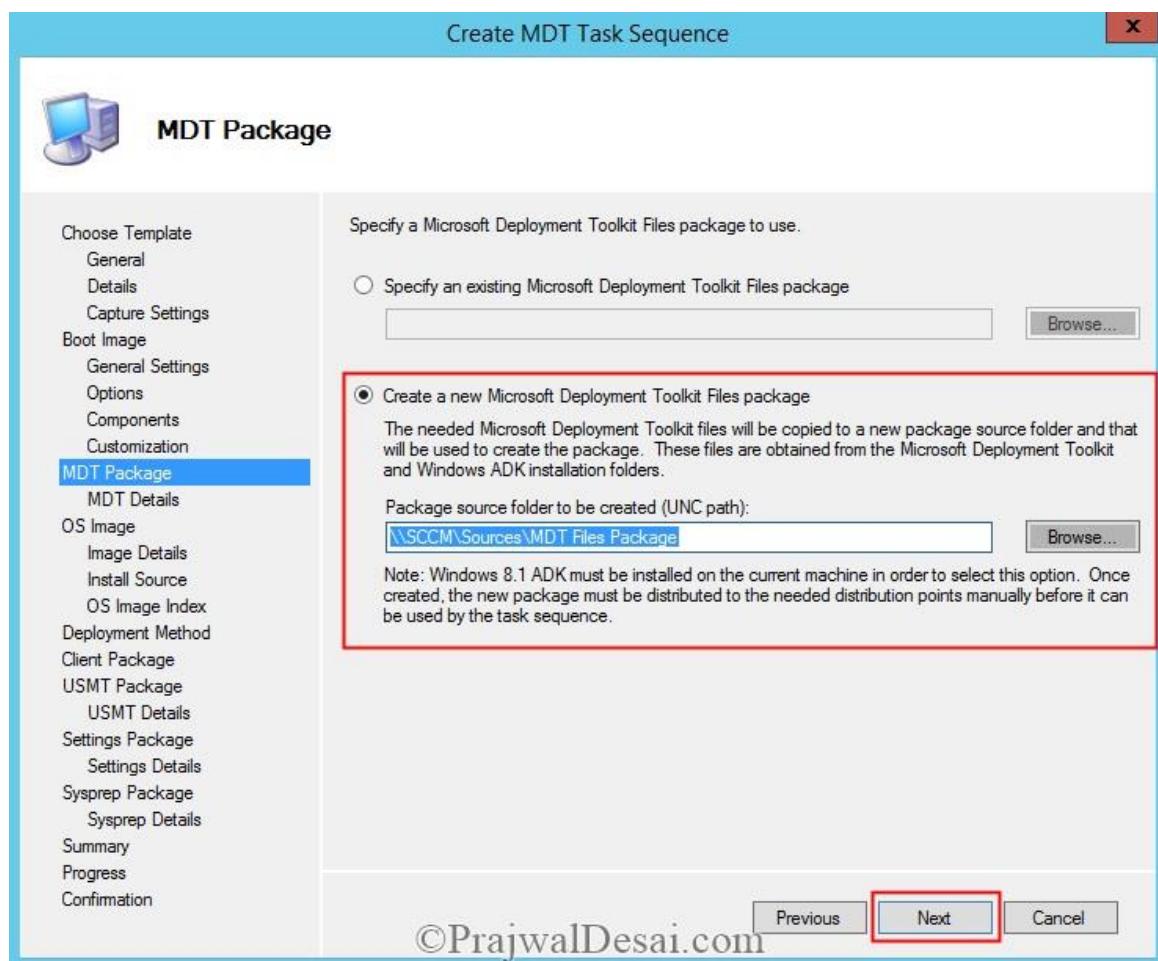
Click on **Browse** and specify the boot image.

Click **Next**.



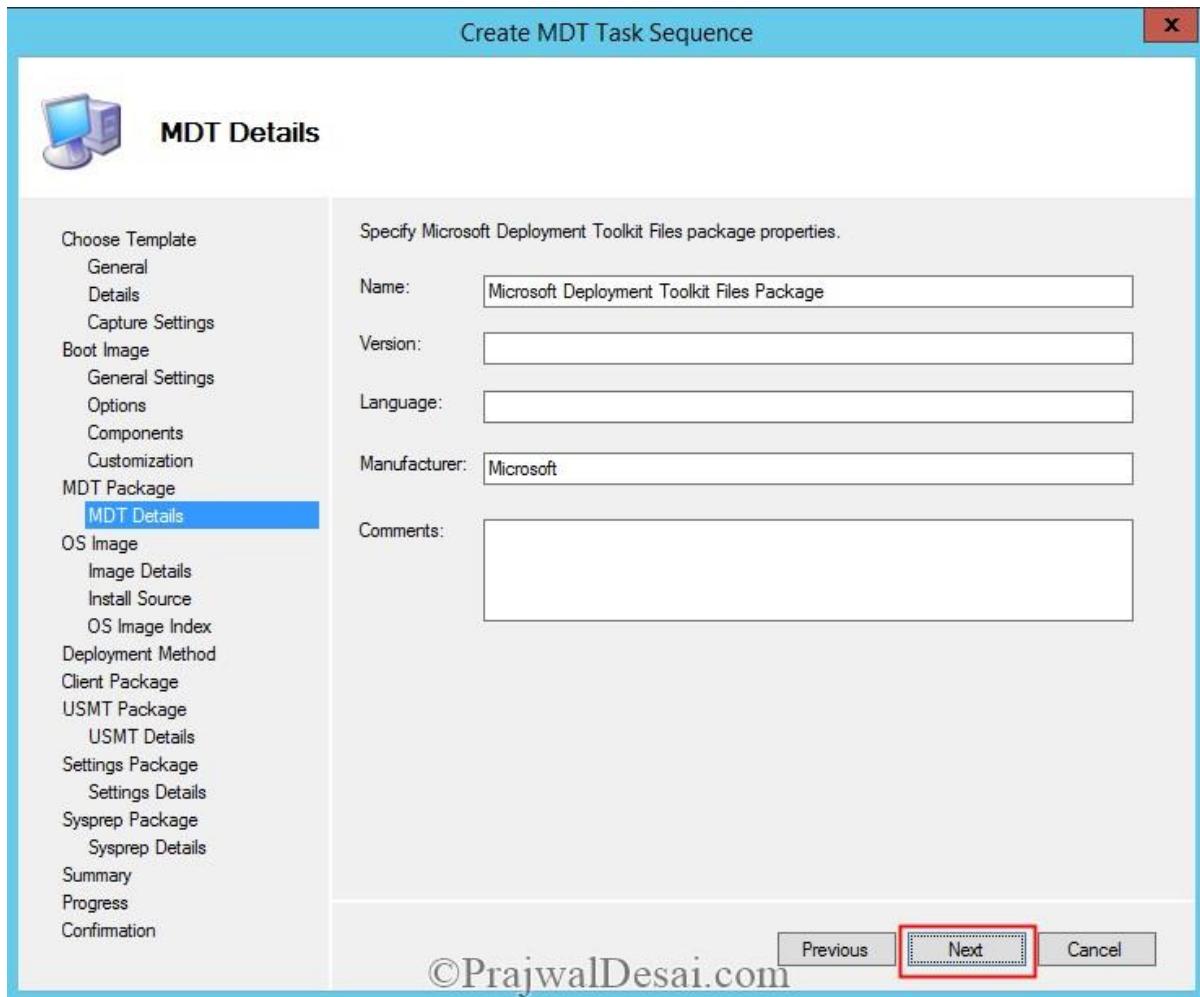
Click **Create a new Microsoft Deployment Toolkit Files package**. Provide a shared folder path where the MDT files package should be stored.

Click Next.



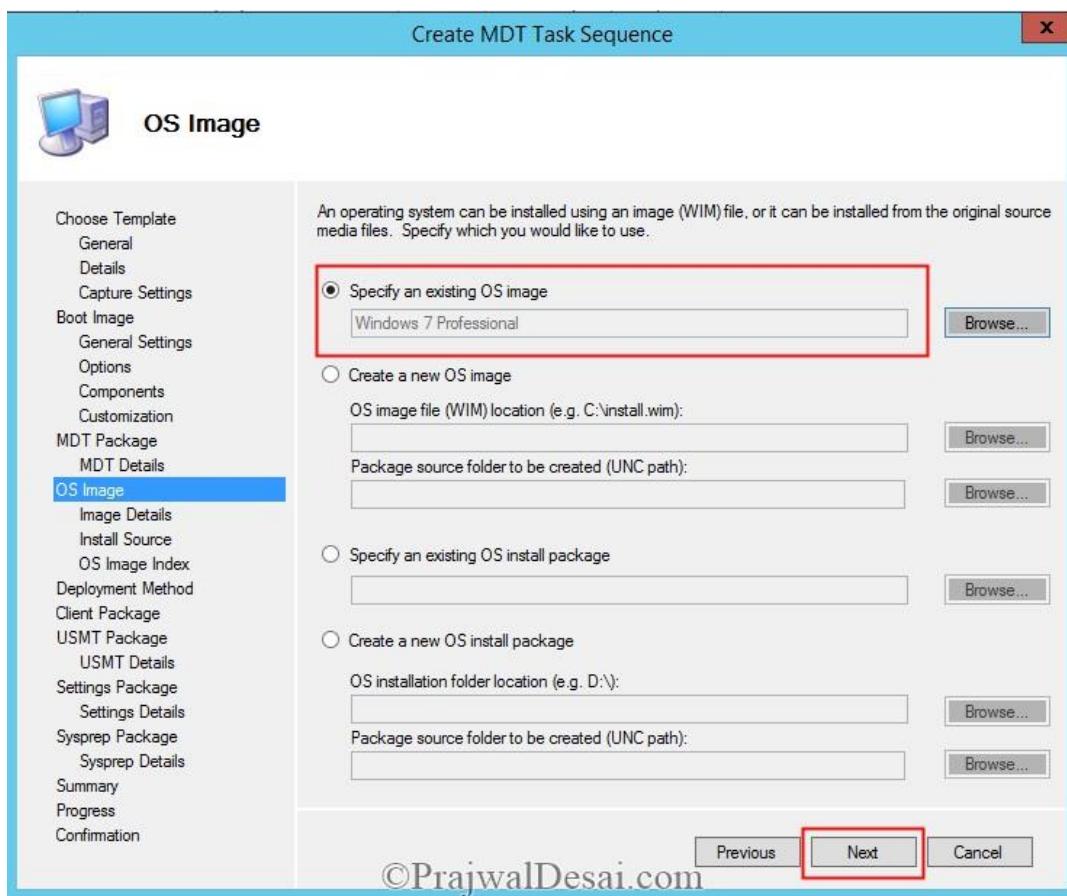
©PrajwalDesai.com

Provide a name to the package and click **Next**.

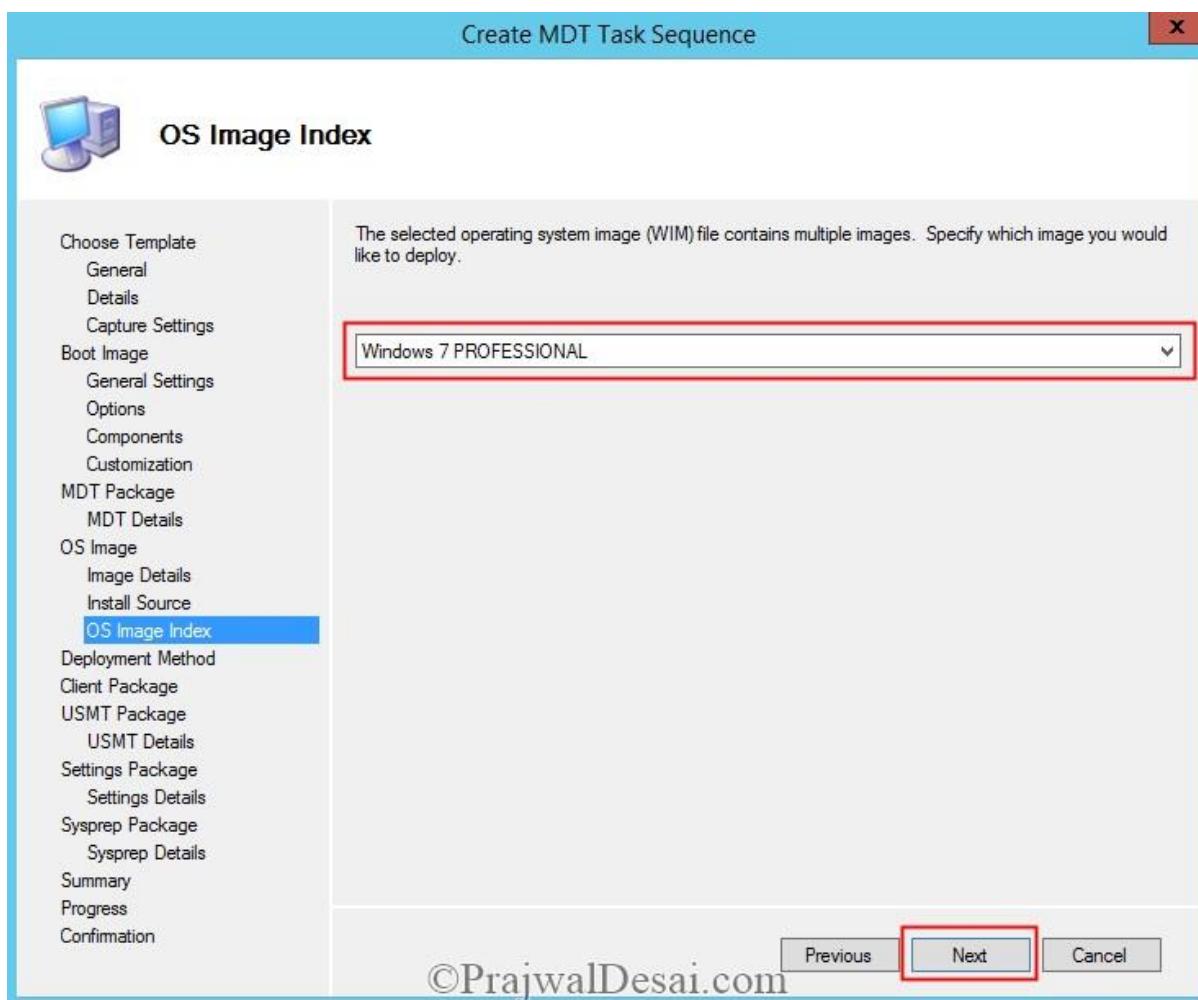


Click **Specify an existing OS image**, click **Browse** and select the desired OS Image. If you are unable to find OS image then ensure that you have added the OS image in the Configuration Manager and distributed it to DP's.

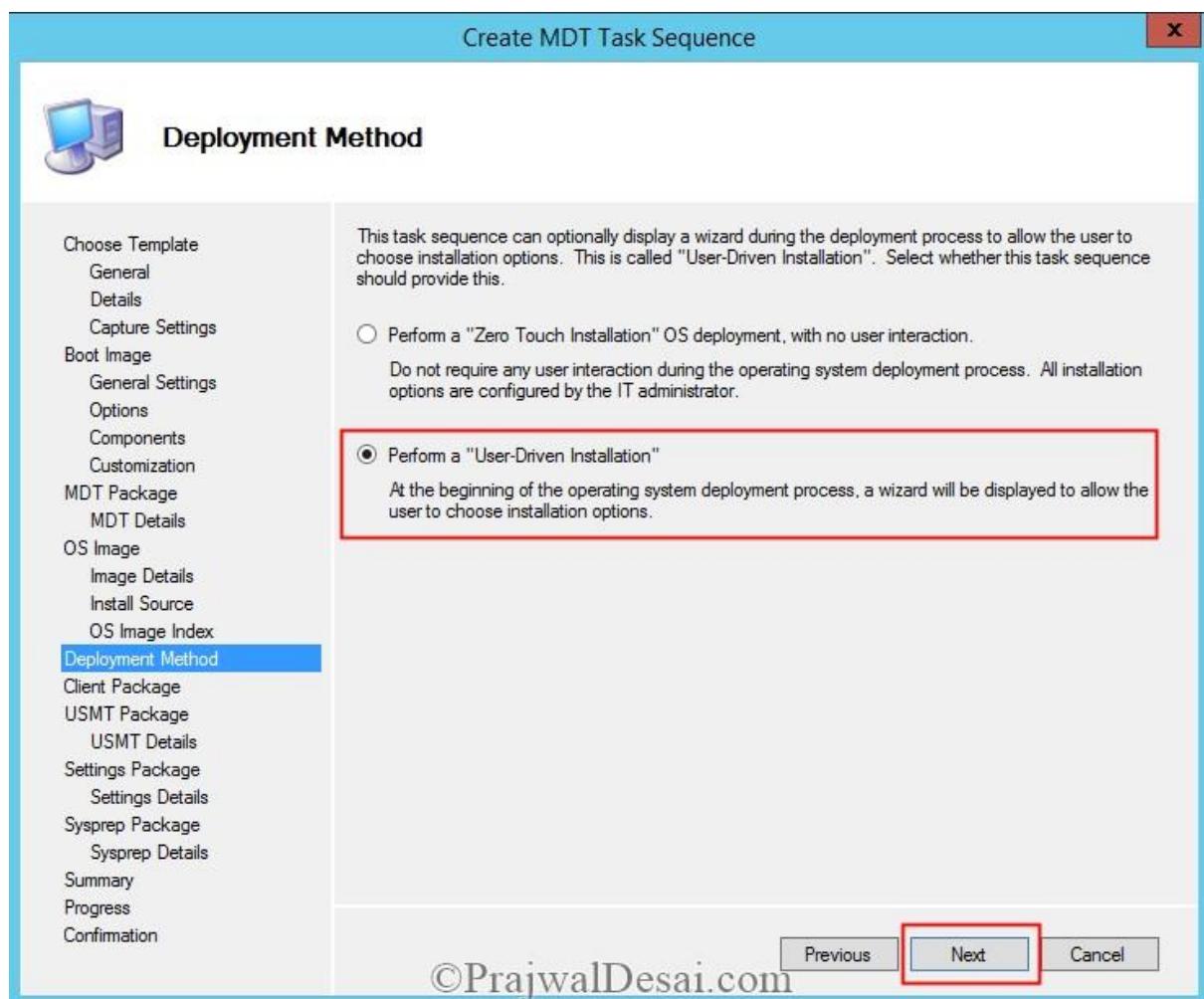
Click Next.



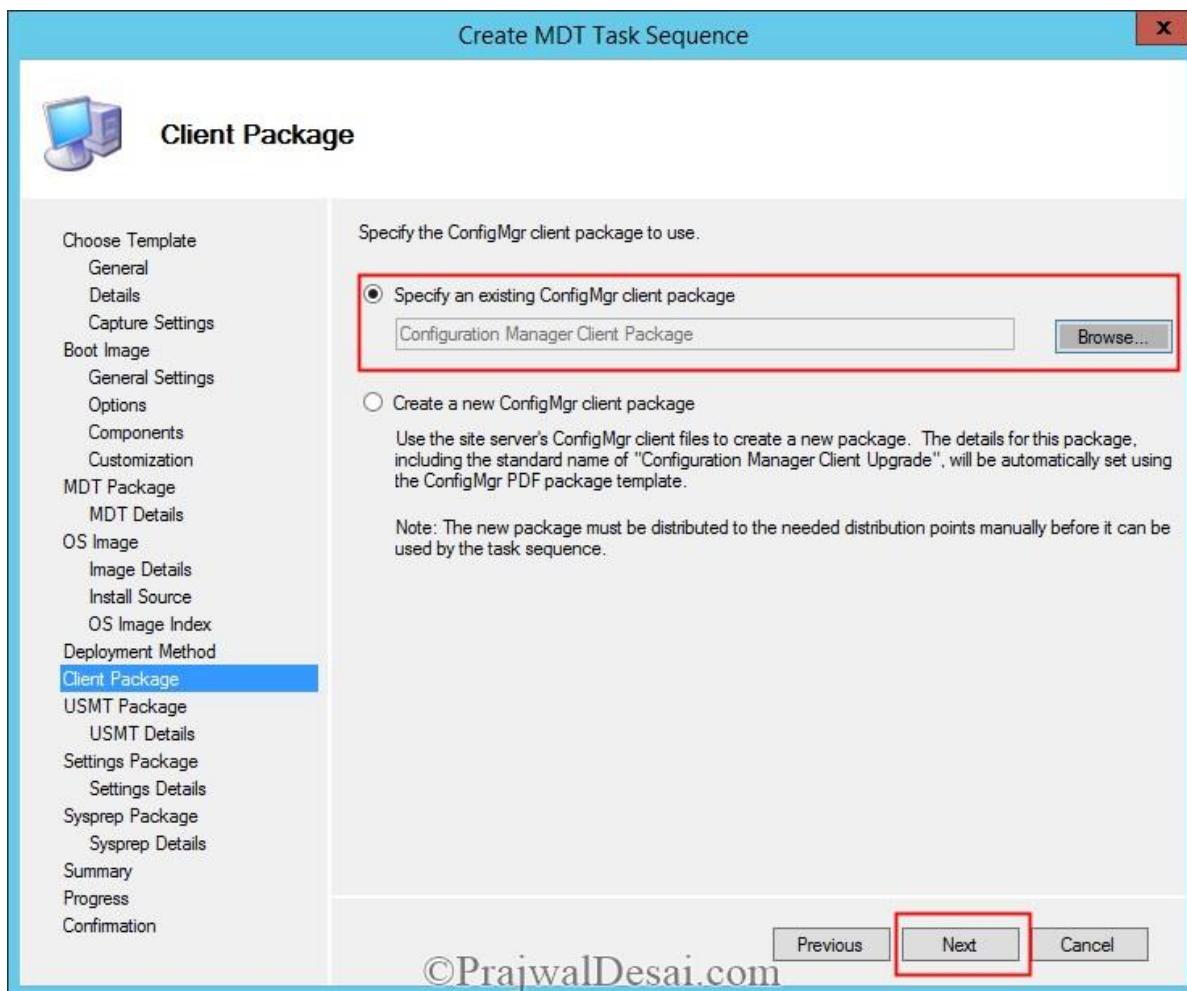
Choose the OS edition that you want to install. Click **Next**.



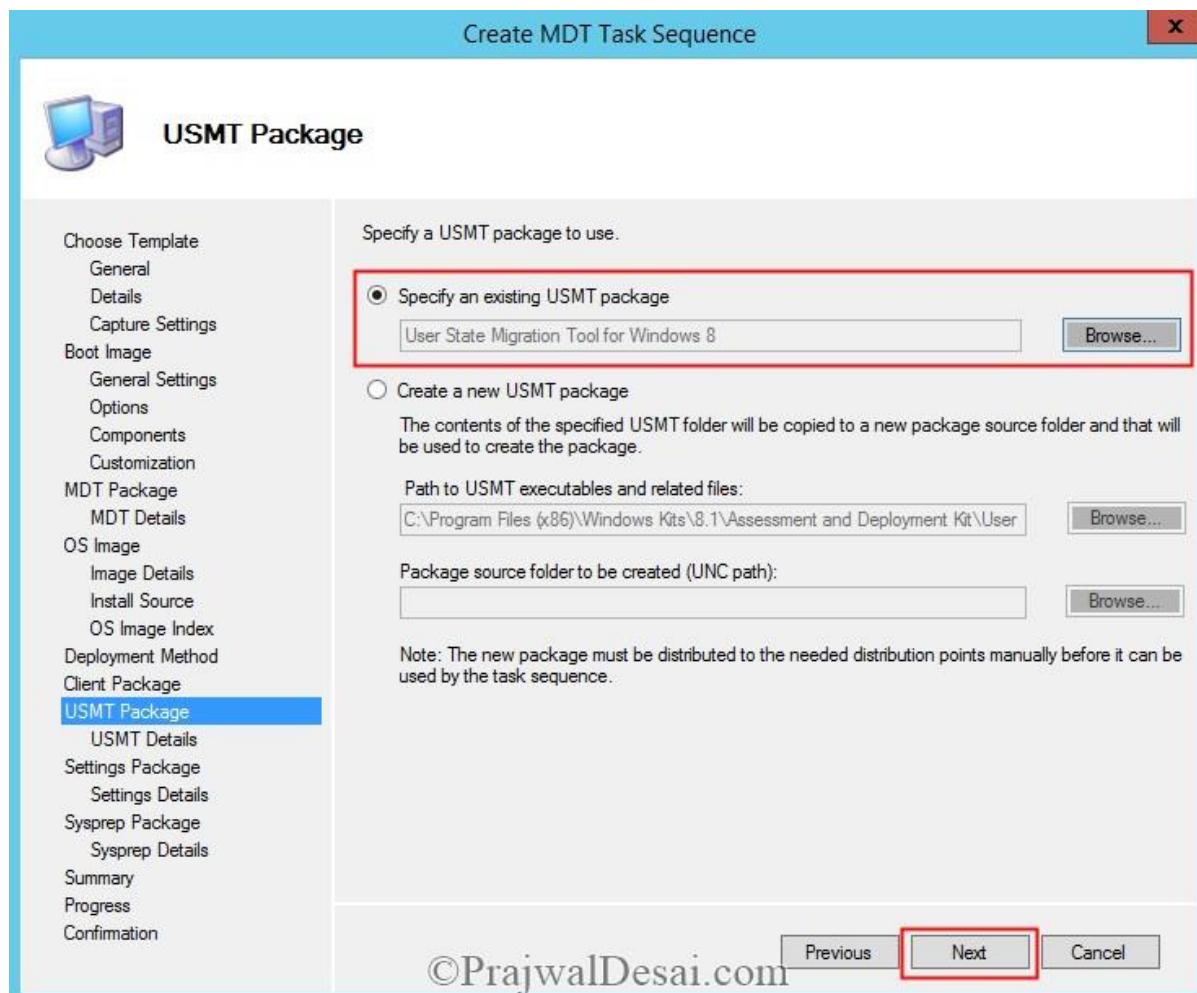
Choose **Perform a “User-driven Installation”**. Click **Next**.



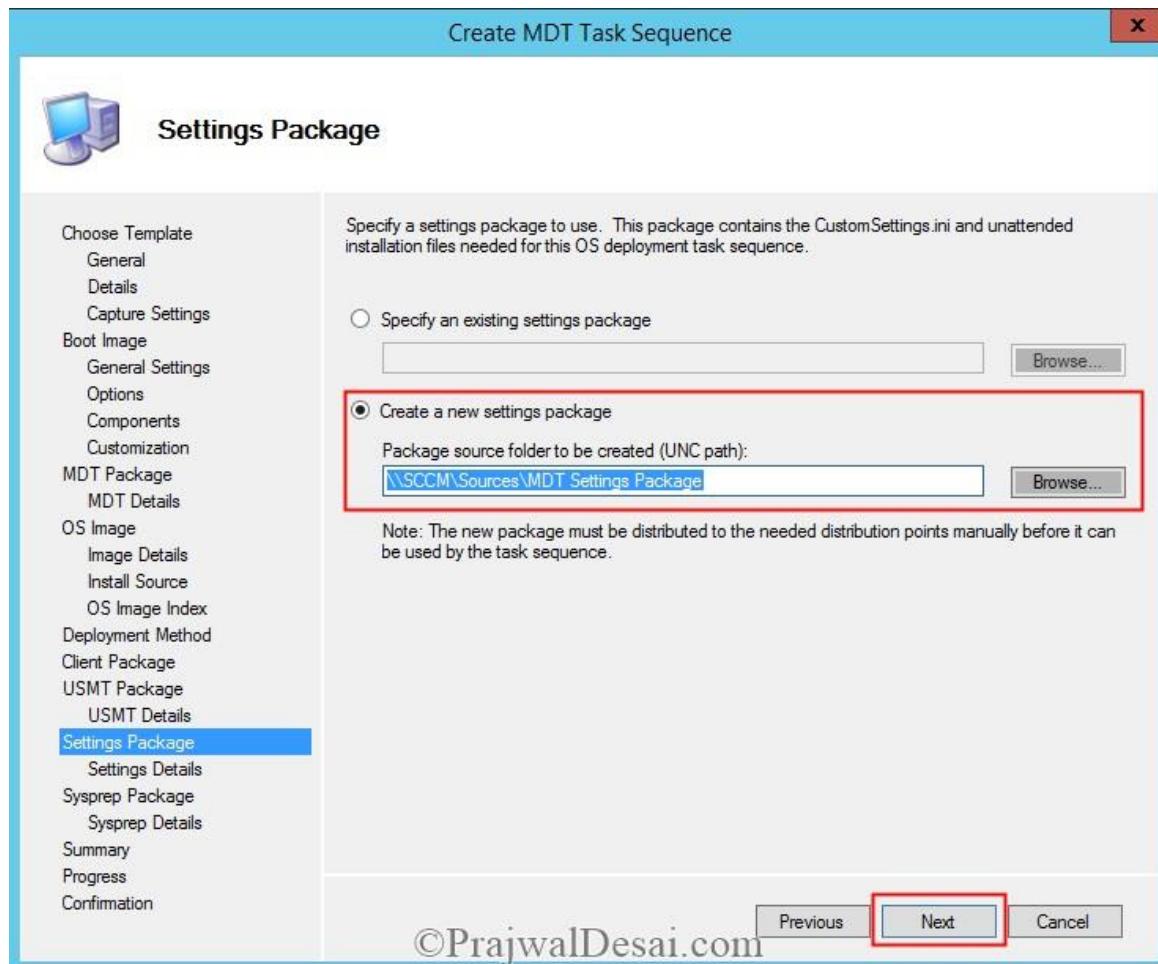
Click **Browse** and specify ConfigMgr client package. Click **Next**.



Click **Browse** and specify an existing USMT package. Click **Next**.

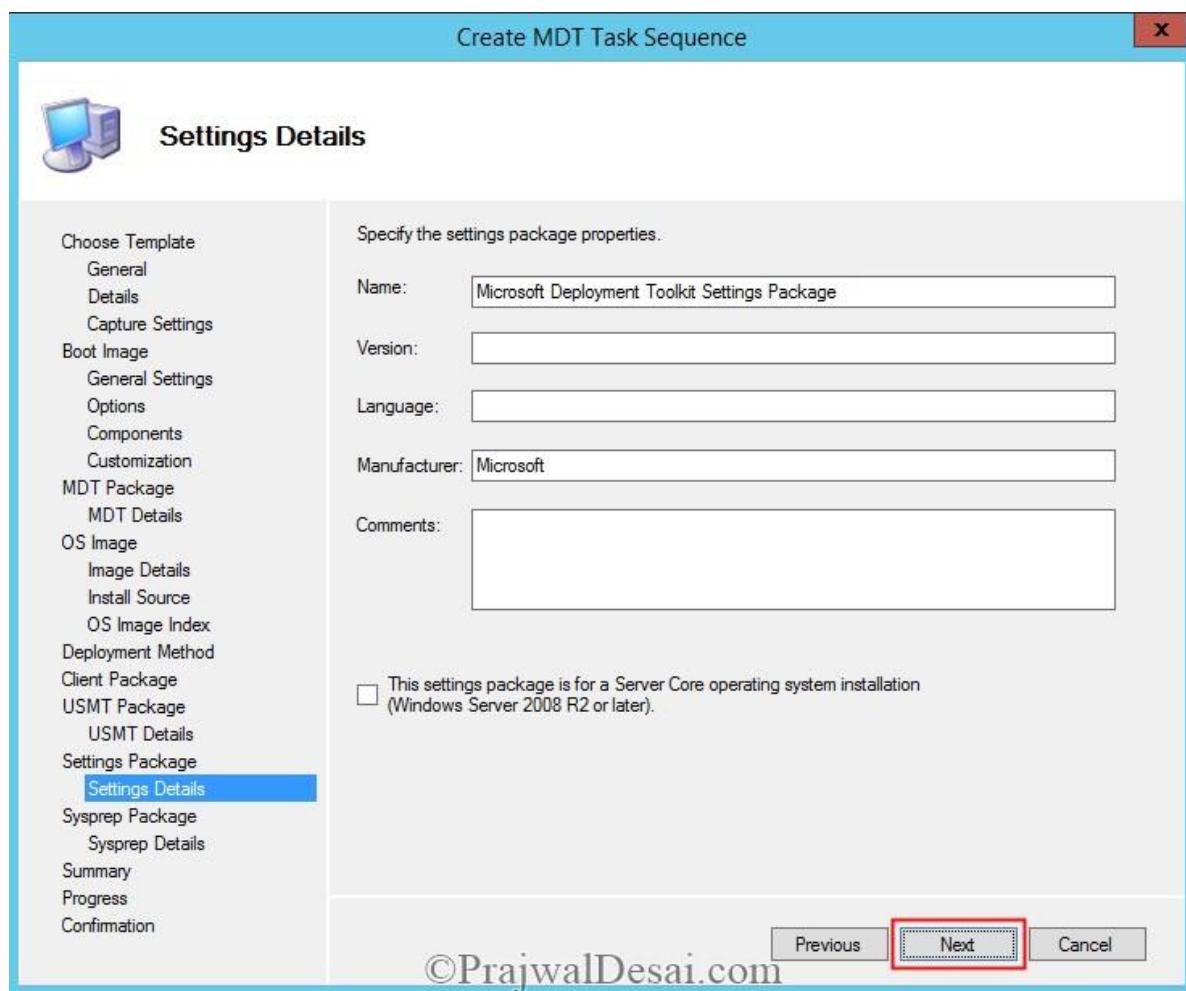


Click **Create a new settings package**. Provide a path where the settings should be stored. Click **Next**.

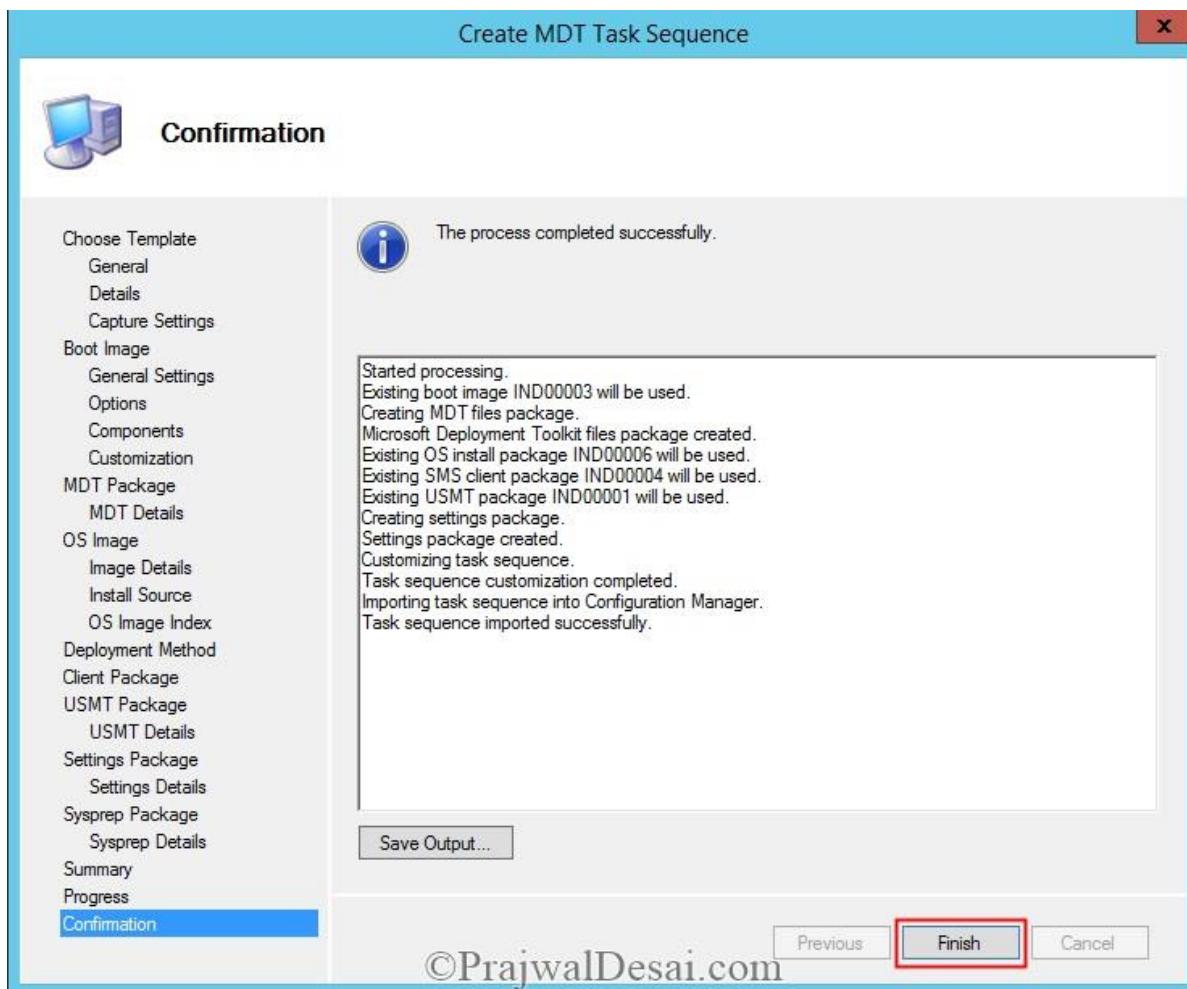


©PrajwalDesai.com

Provide some details such as name to settings package. Click **Next**.

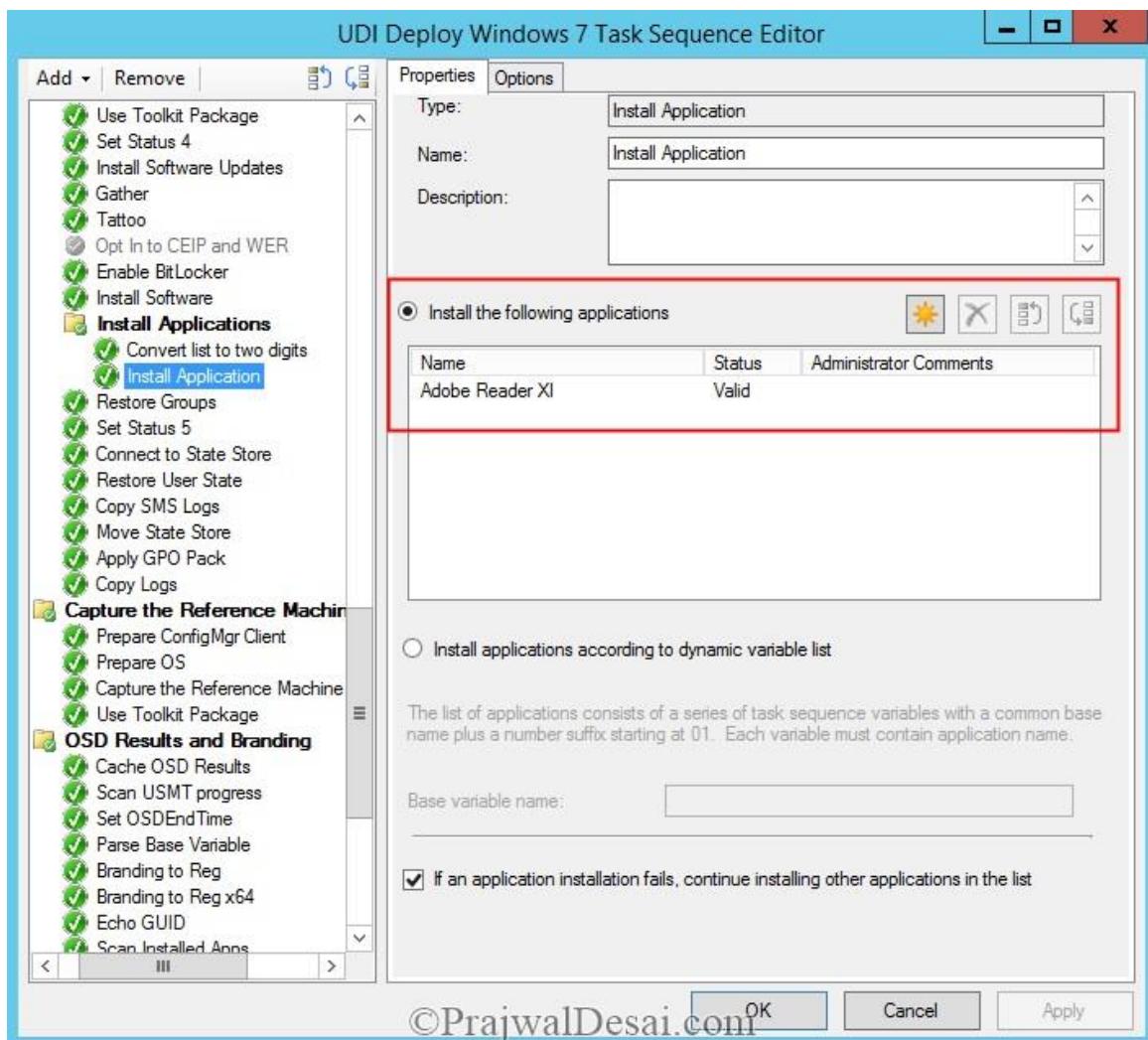


Complete the remaining steps and click **Finish**.

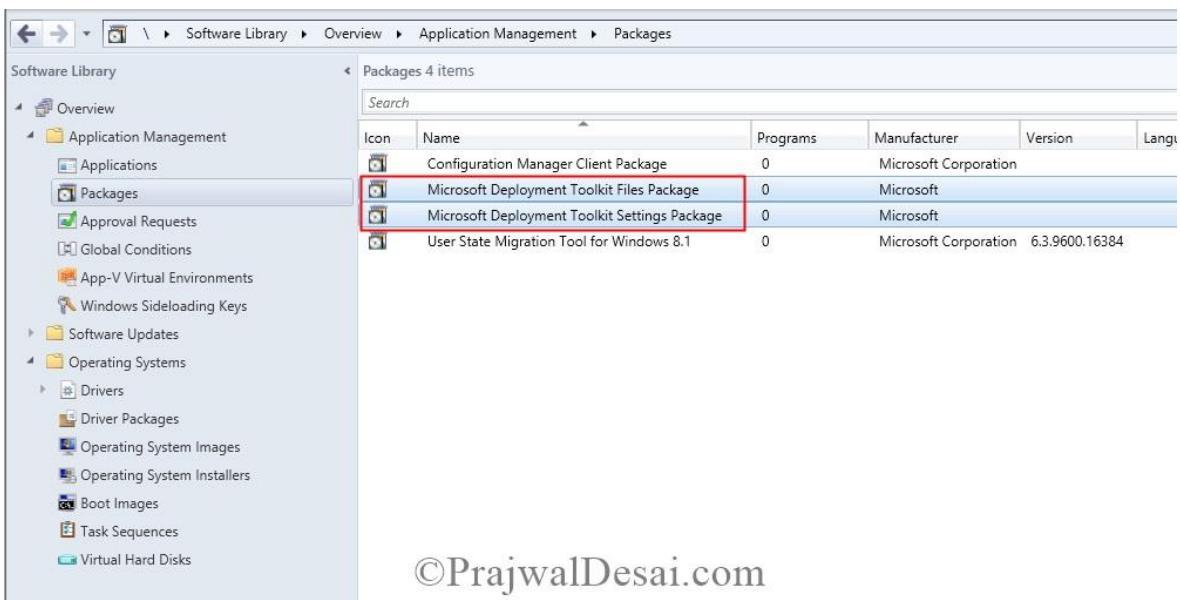


To edit the TS, right-click the TS and click **Edit**. This will open the Task Sequence Editor. In the below screenshot, I have added the applications to be installed after OS is installed. You can add more apps if required.

Click OK.

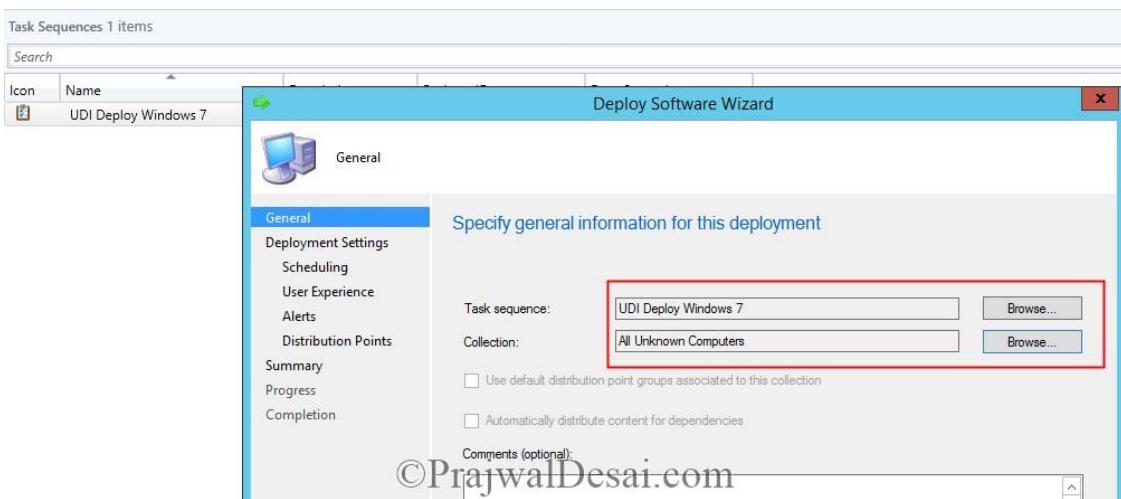


Once you have the TS ready, you have an option to customize the UDI wizard. The UDI Wizard pages are customizable and this can be done with a utility called [UDI Wizard Designer](#). I have not included those steps here, check this [link](#) to customize the UDI Wizard pages. After you do this step, you need to update the MDT files and settings package to the distribution points.



©PrajwalDesai.com

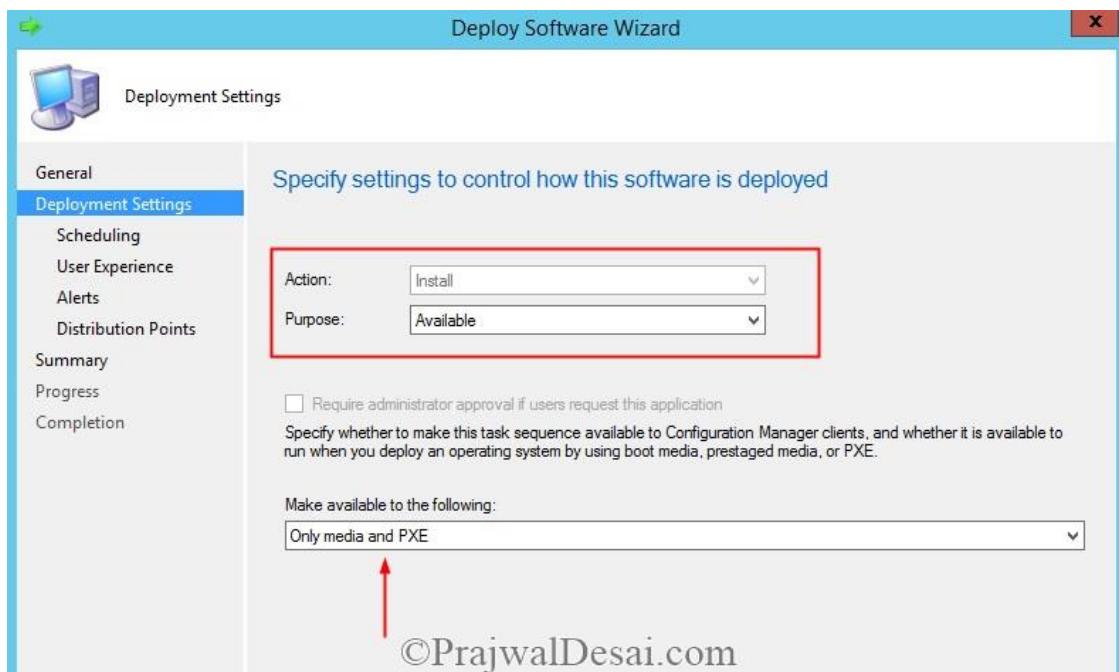
To deploy the TS, right click on the TS and click **Deploy**. Click on **Browse** and choose the collection as **All Unknown Computers**.



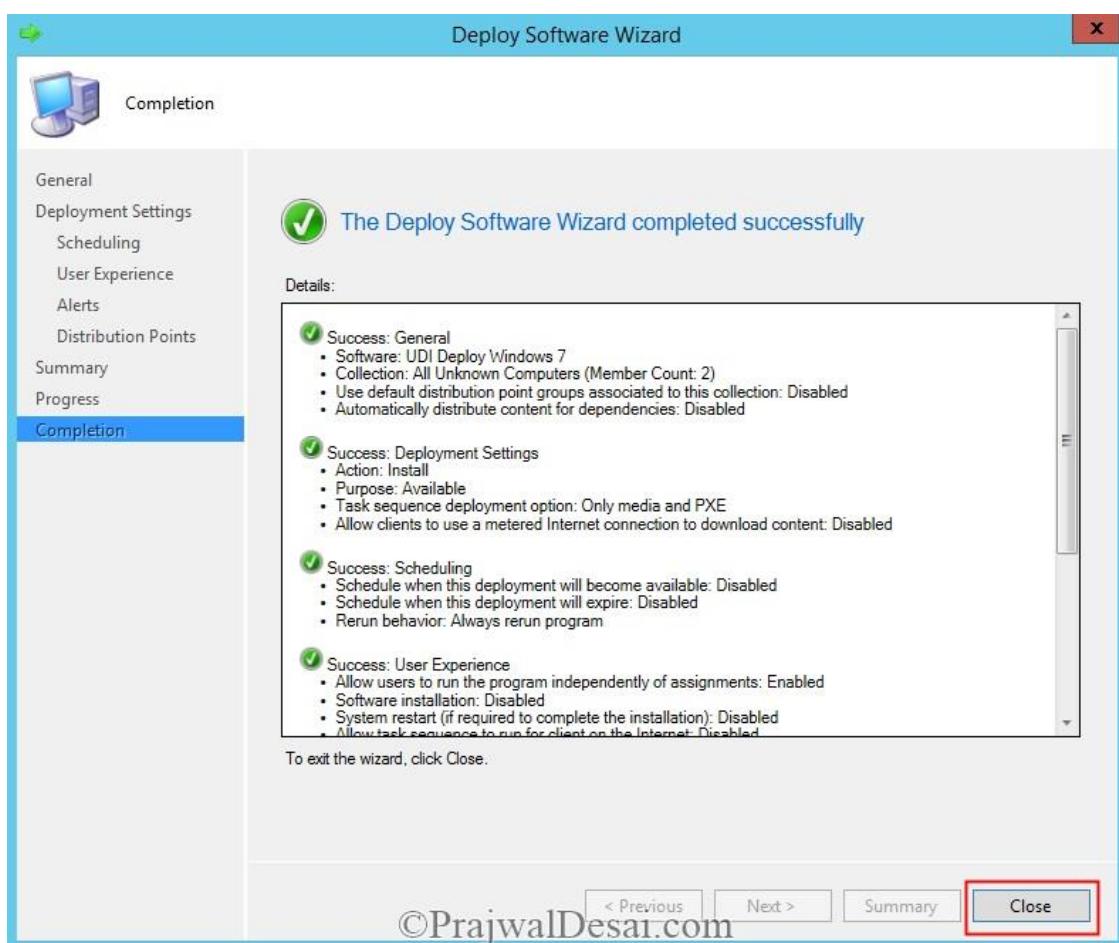
©PrajwalDesai.com

Set the purpose as **Available** and make the TS available to “**Only media and PXE**“.

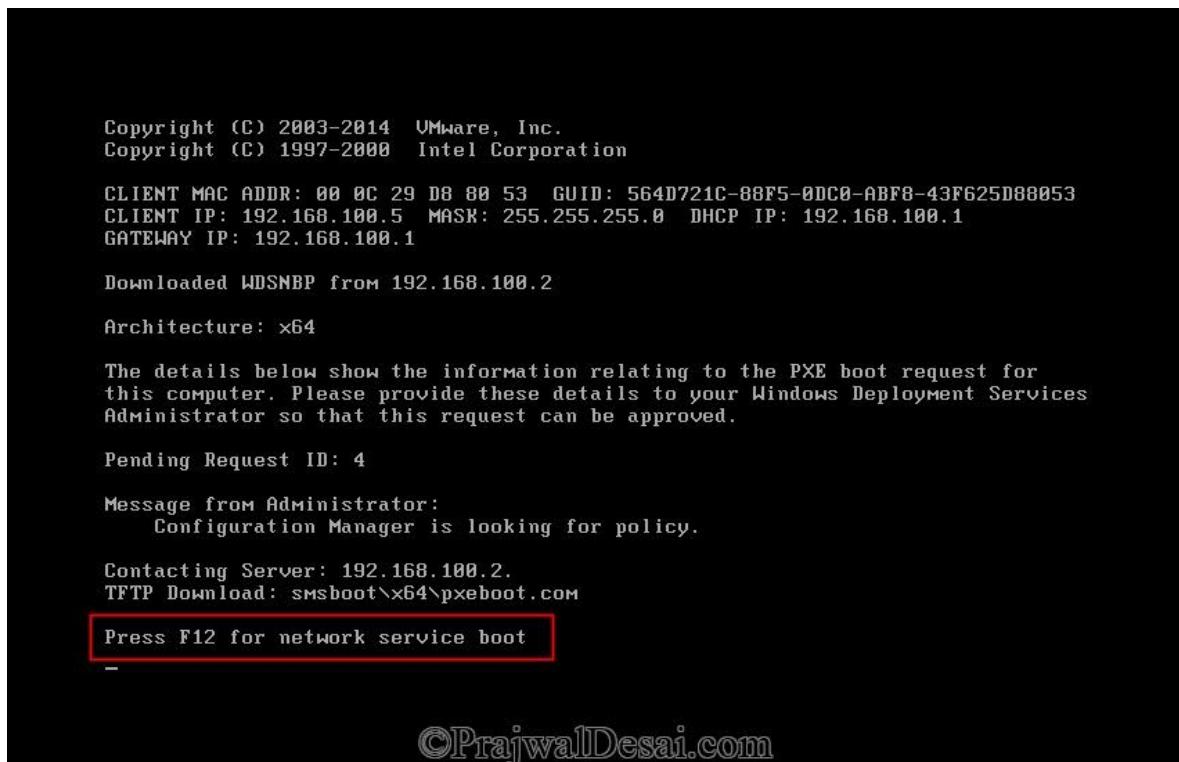
Click Next.



Complete the steps in the wizard and click on **Close**.

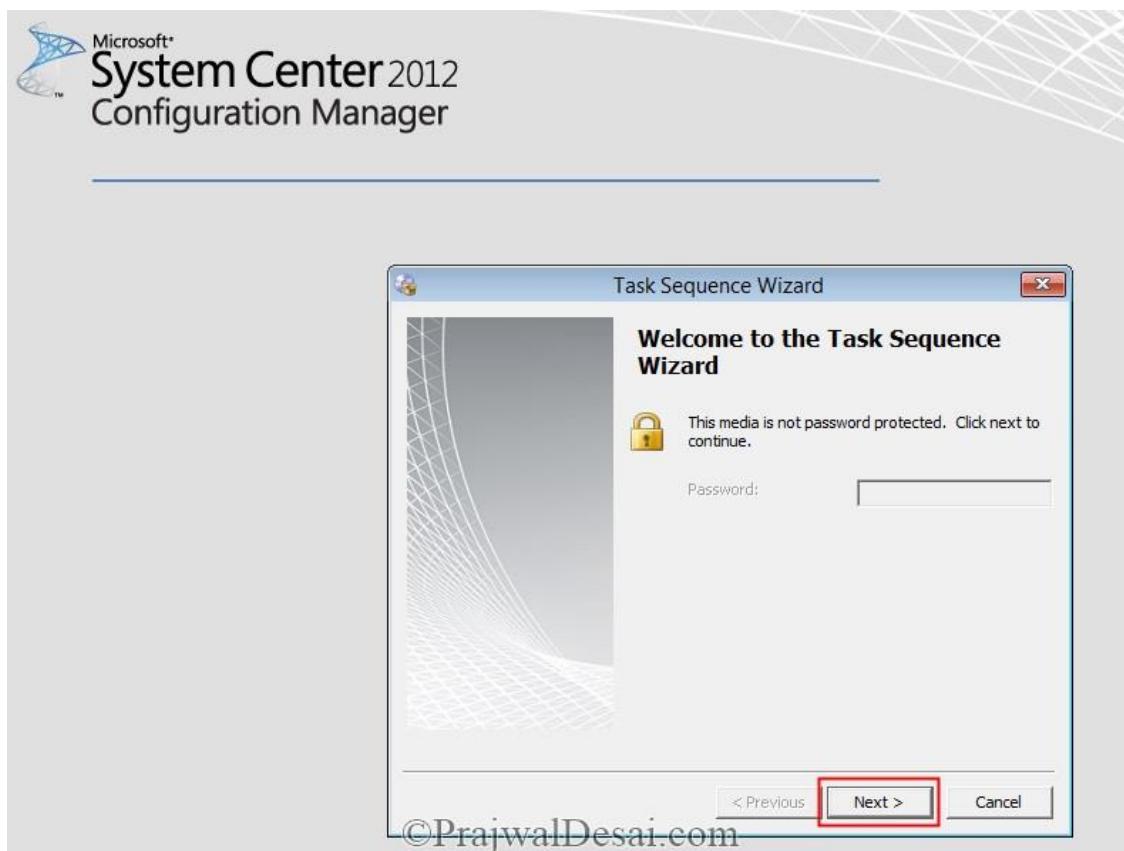


Now boot the machine and allow it to boot from the network. Press **F12** key to start the network service boot.



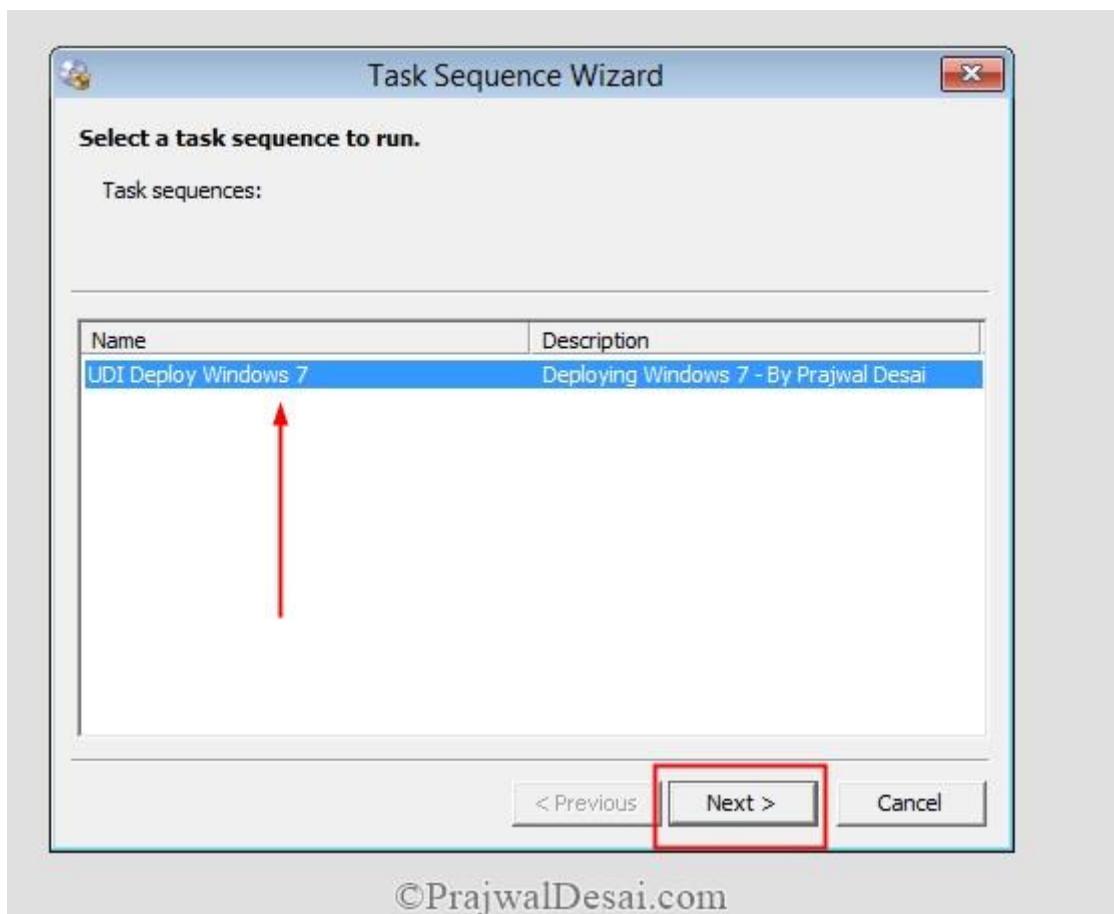
©PrajwalDesai.com

Click Next.



©PrajwalDesai.com

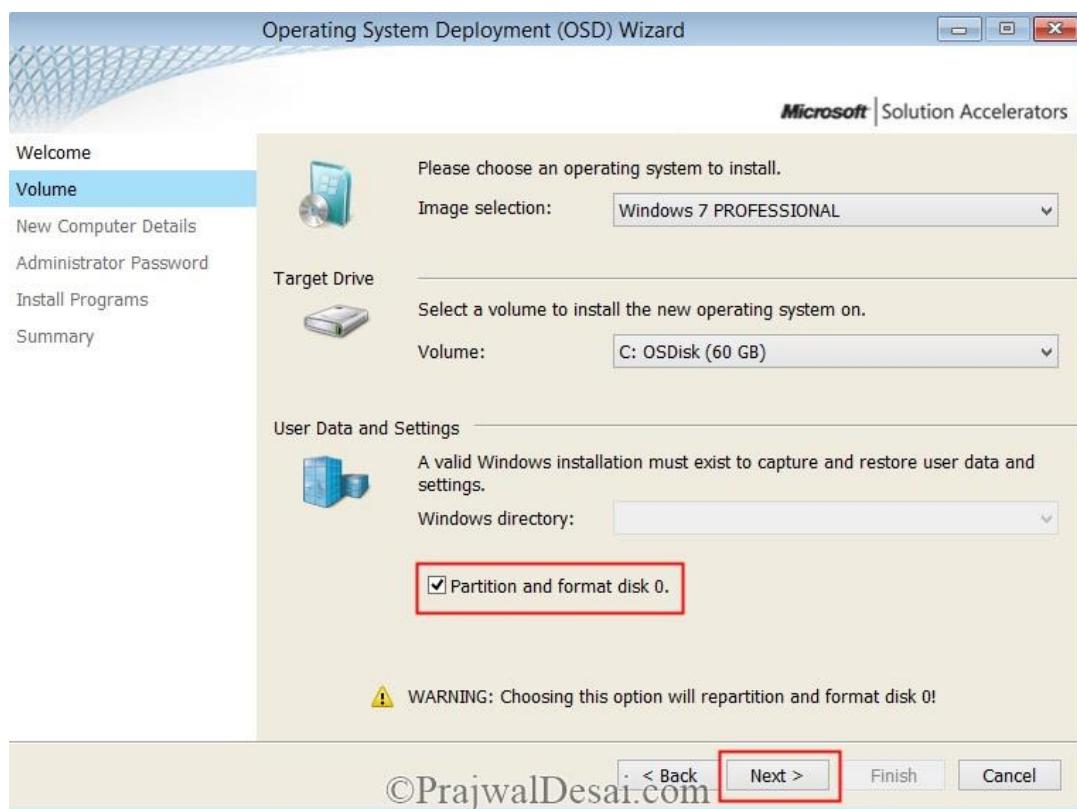
Select the Task Sequence and click **Next**.



©PrajwalDesai.com

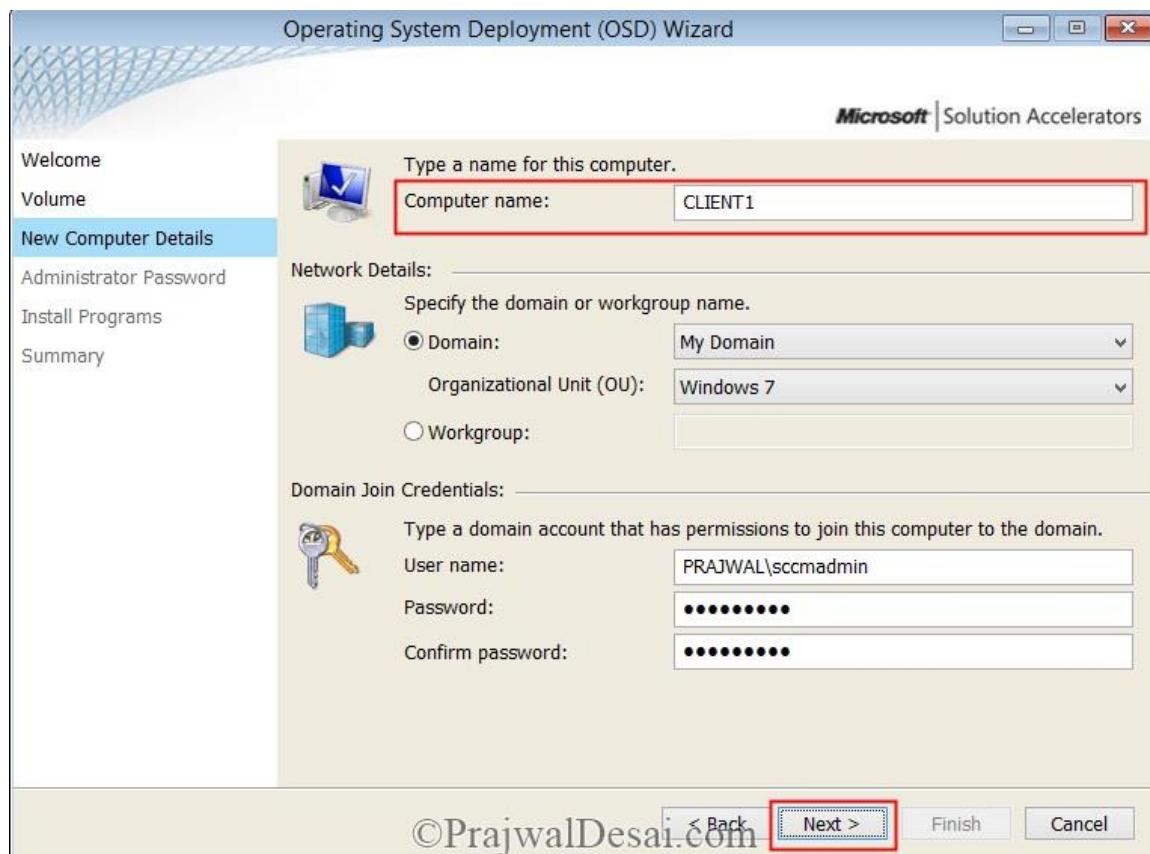
Choose the OS, Target Drive and check the box partition and format disk 0.

Click Next.



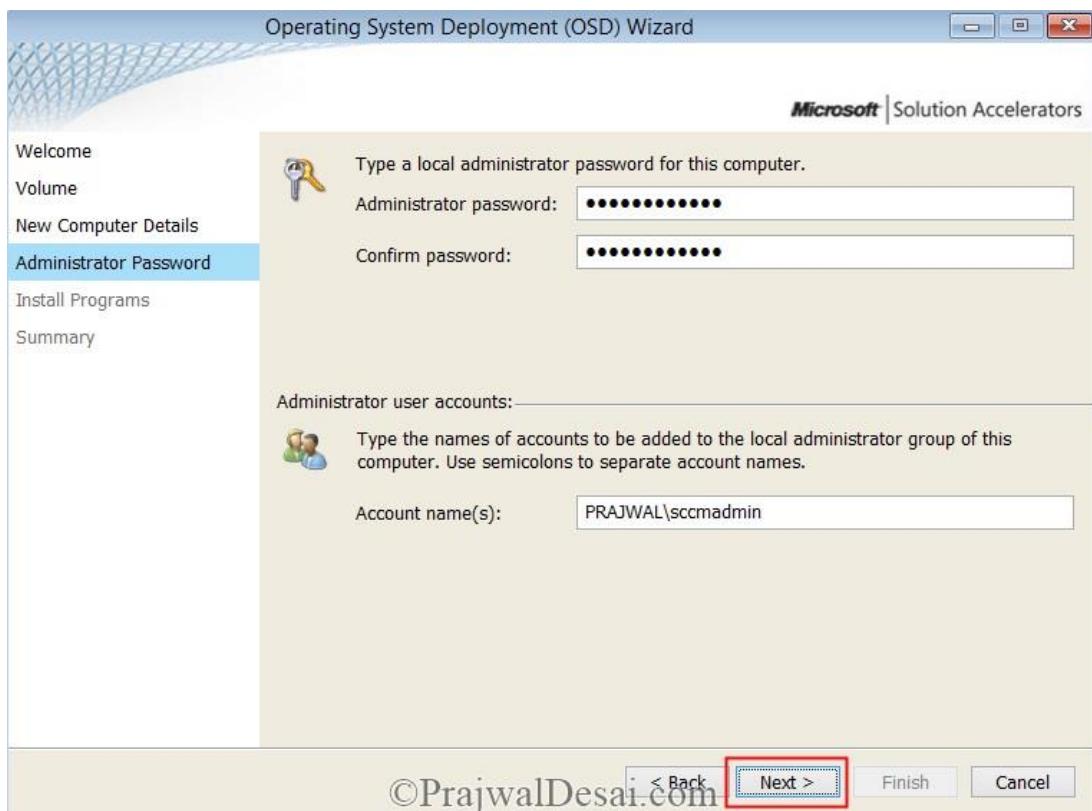
Provide few details such as Computer name, select domain, OU and domain join credentials.

Click Next.

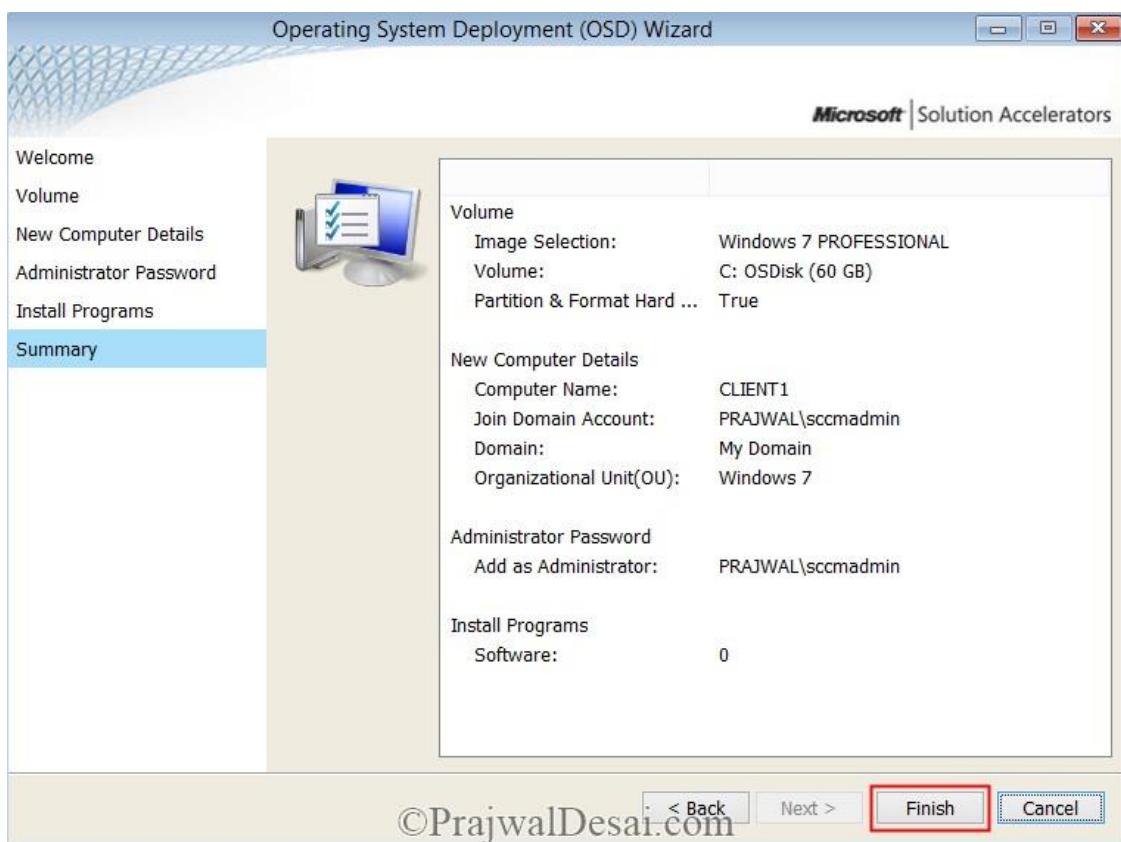


Set the local administrator password.

Click Next.



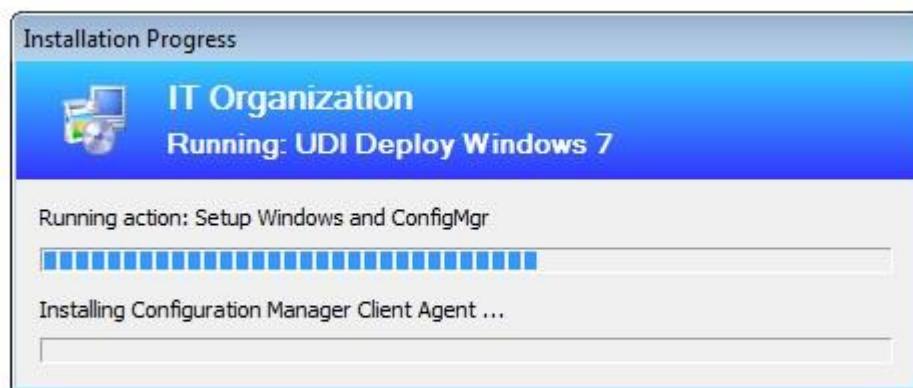
Click Finish.



Wait for the task sequence to install the OS.

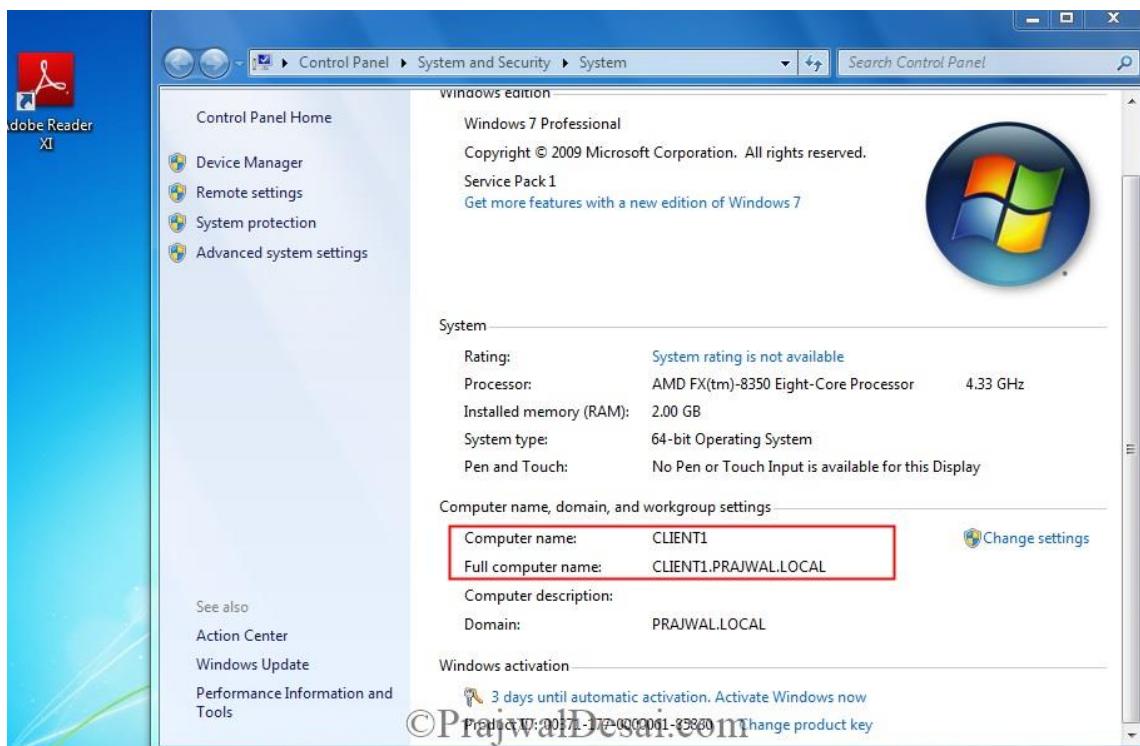


A screenshot where we see that ConfigMgr agent is being installed.



©PrajwalDesai.com

Nice to see newly imaged computer with applications installed on it :).

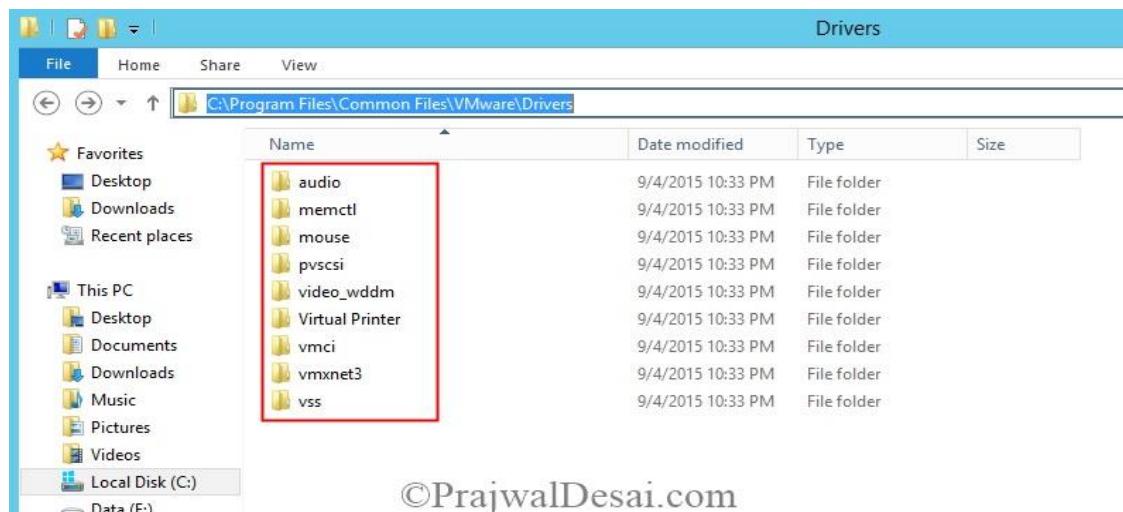


[Import VMware drivers to your SCCM boot image](#)

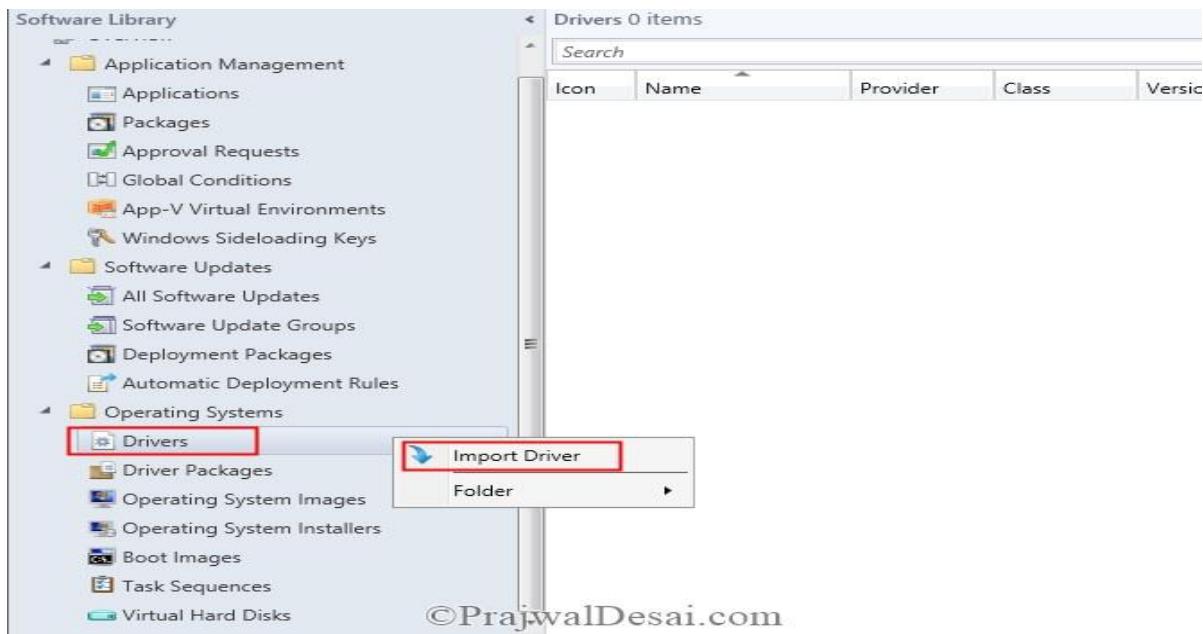
In this post we will see how to import VMware drivers to your SCCM boot image. [Imported device drivers](#) can be added to boot image packages or driver packages and can be installed as part of an Operating System Deployment task sequence using the Auto Apply Driver and Apply Driver Package task sequence steps. When you want to deploy a new VMware virtual machine with System Center Configuration Manager, you could encounter an error during the WinPE phase. The VM will start WinPE but there shall be reboots. This happens because Configuration Manager does not have drivers for a VMware Virtual Machine. A lot of people get stuck here because they forget to import VMXnet3 drivers to their boot image. Unlike Dell, VMware doesn't provide the driver package file in .cab format. You have to import VMware drivers into your WinPE boot image.

Import VMware drivers to your SCCM boot image

On the VM which has VMware tools installed, the drivers are located under **C>Program Files>Common Files>VMware>Drivers**. Copy the driver files you want to import to a UNC accessible location (typically under Sources > Drivers). In the below screenshot you see lot of drivers, just select all and copy the folders to a shared folder.

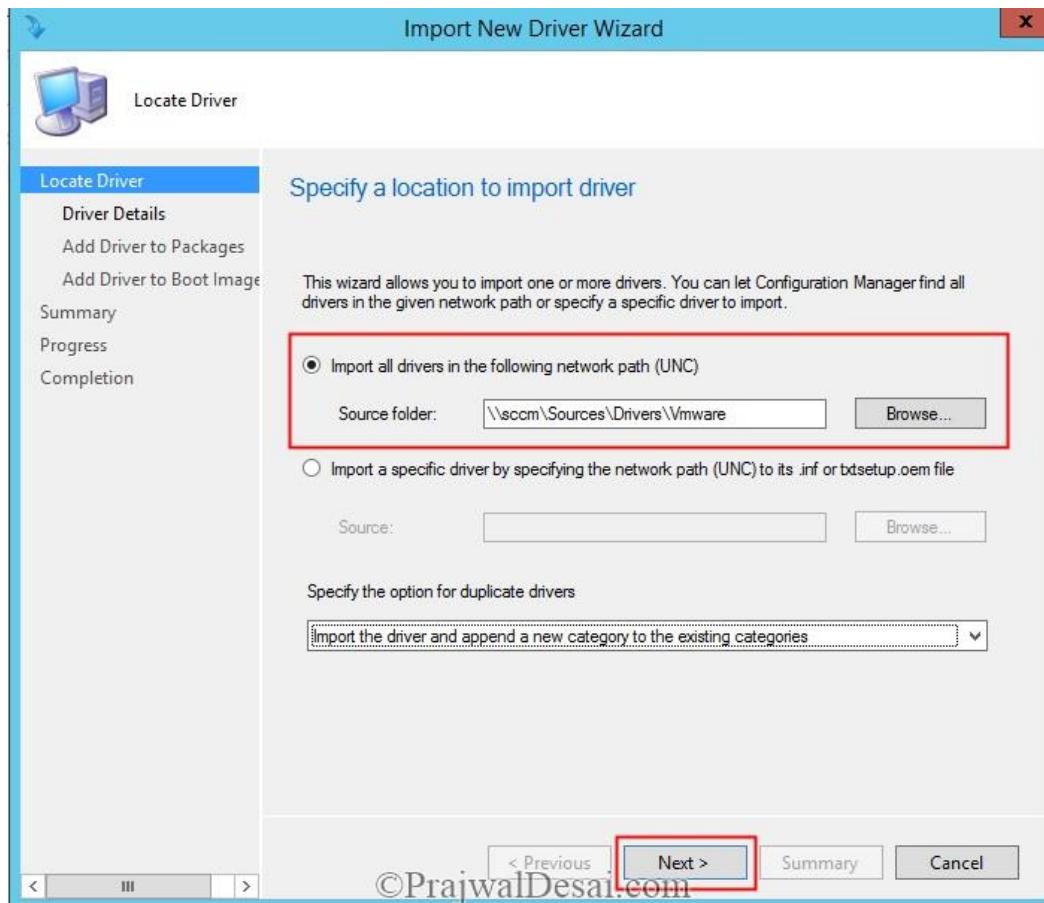


Using the Drivers node, you import drivers into the ConfigMgr drivers catalog. Launch the Configuration Manager console. Navigate to **Software Library -> Overview -> Operating Systems -> Drivers**. Select **Drivers**. Right click on **Drivers** and click **Import Driver**.



©PrajwalDesai.com

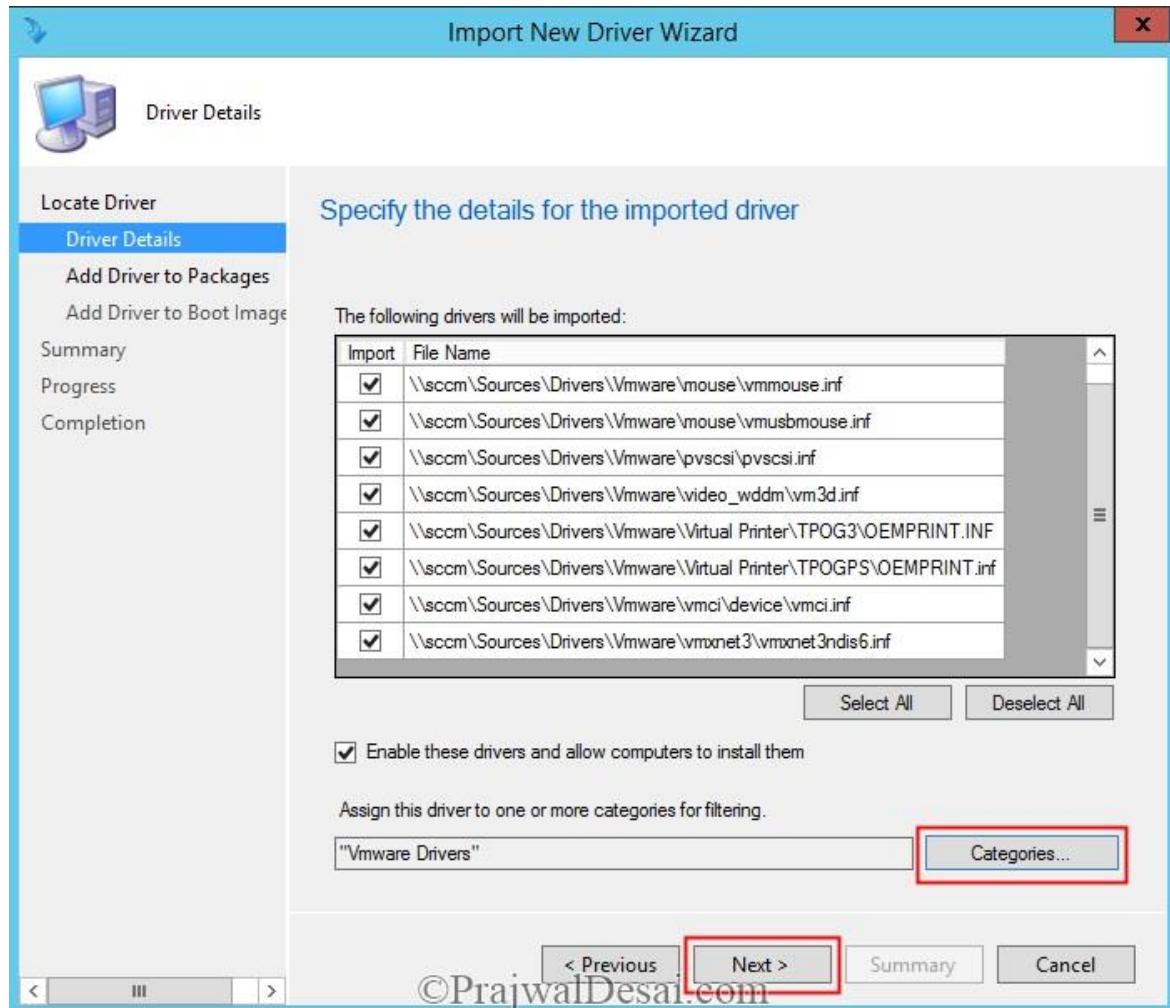
In this step you need to specify the source folder where the drivers are present. Click on **Browse** and provide the path where drivers are located. If you have only a single driver to import, choose the second radio button and then browse to the exact UNC location of the .inf or txtsetup.oem file. For multiple drivers, or to allow ConfigMgr to auto-locate all available drivers in a given path including all subfolders, use the first option, **Import all drivers in the following network path (UNC)**. Click **Next**.



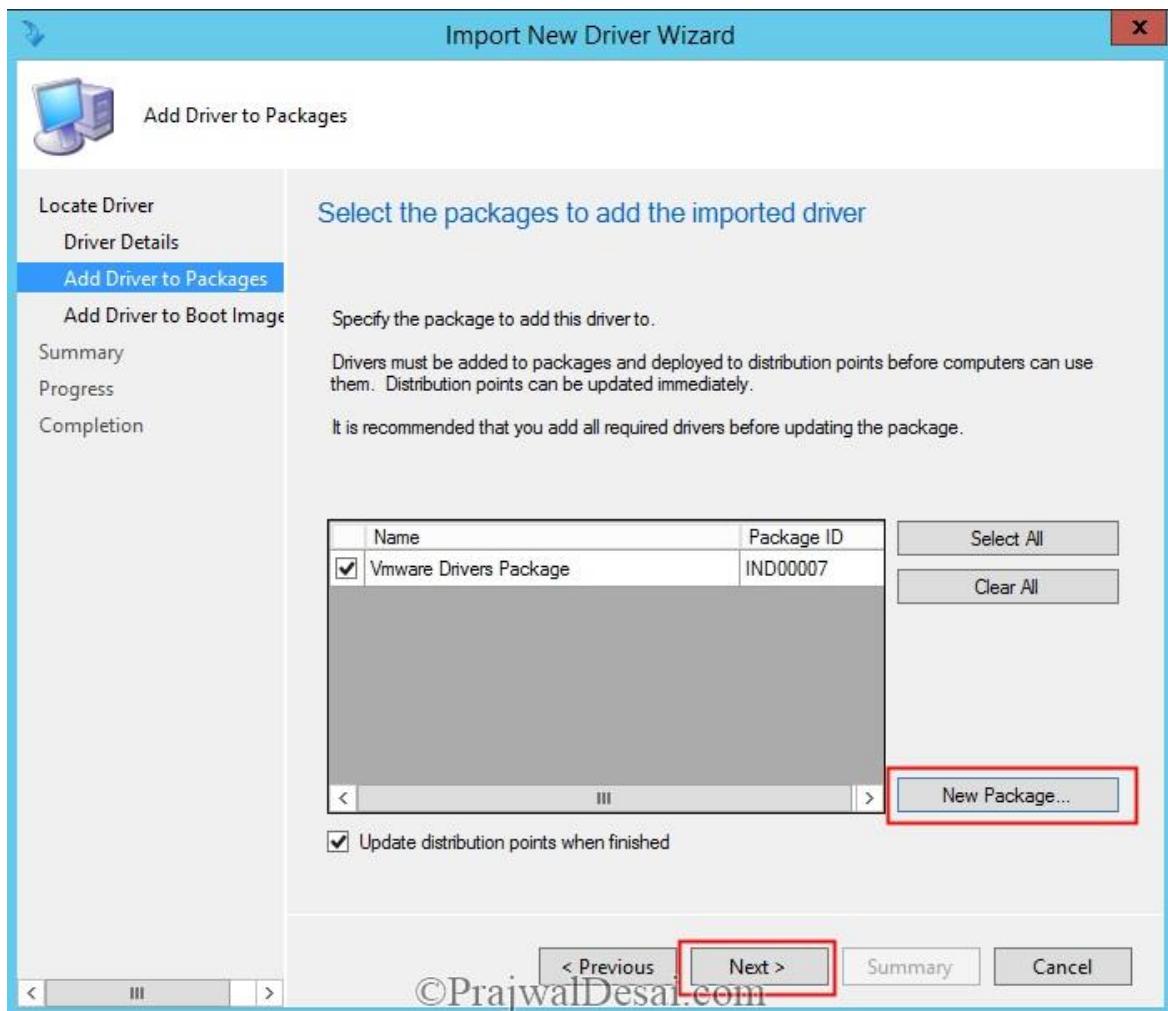
©PrajwalDesai.com

After you specify the location of drivers, all drivers found based on the location entered on the **Locate Driver** page are shown in a list box, where you can review the drivers and uncheck those that you do not want to import. You can also assign the drivers to a category.

Categories often are used to designate different hardware models or manufacturers. This enables you to limit the scope of drivers considered during the plug-and-play detection done by the task sequence, speeding up the process and reducing or eliminating the chance that a bad driver is installed and used. Click **Categories** and provide a name to it. Ensure that **Enable these drivers and allow computers to install them** box is checked. Click **Next**.

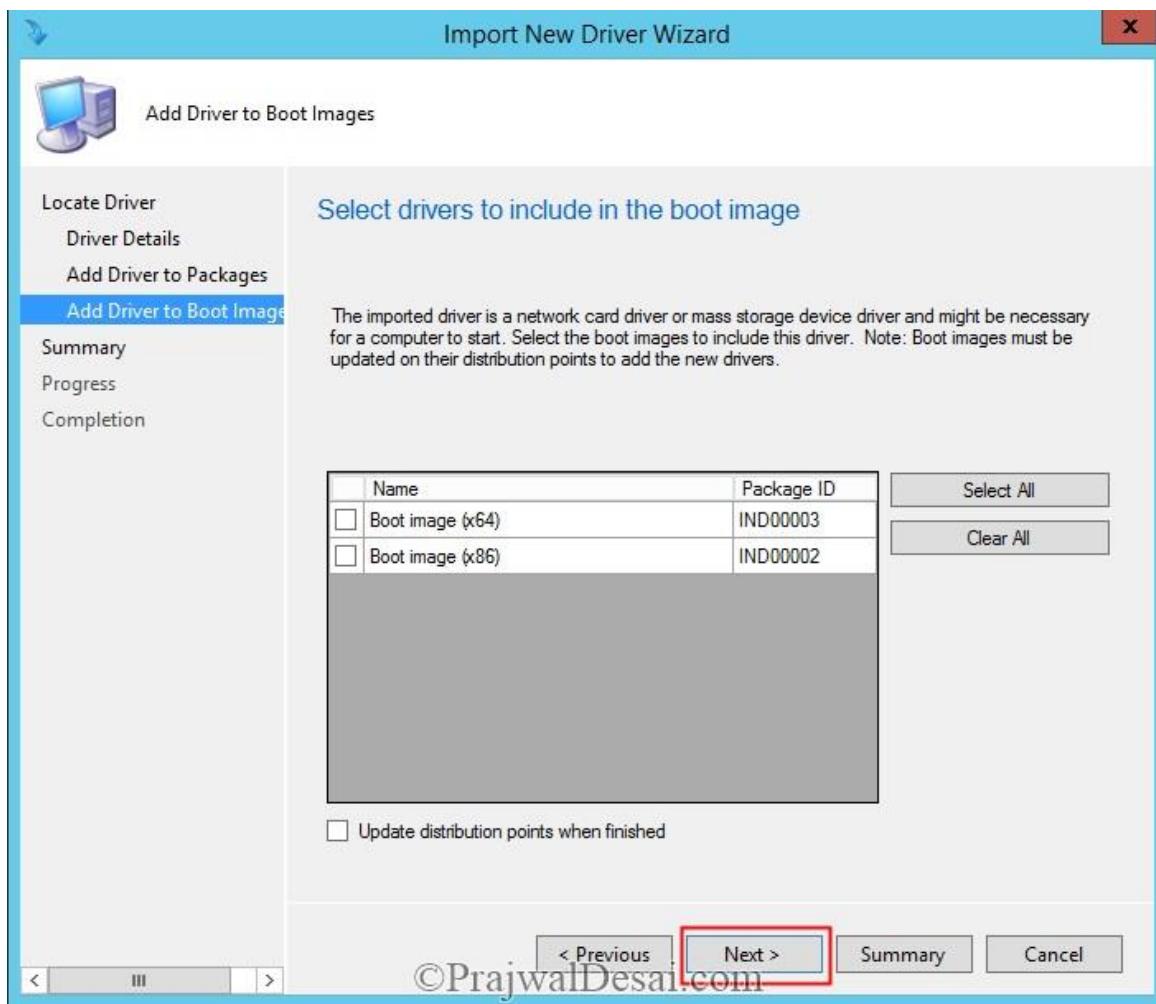


When you have group of drivers, it needs to be added to a package and deployed to distribution points. Drivers must exist in a driver package to be accessible and usable during OSD. Click on **New Package** and provide a folder path where the driver package is to be stored. However note that the Driver Package Path, and the Driver Source, can't be the same target. Click **Next**.



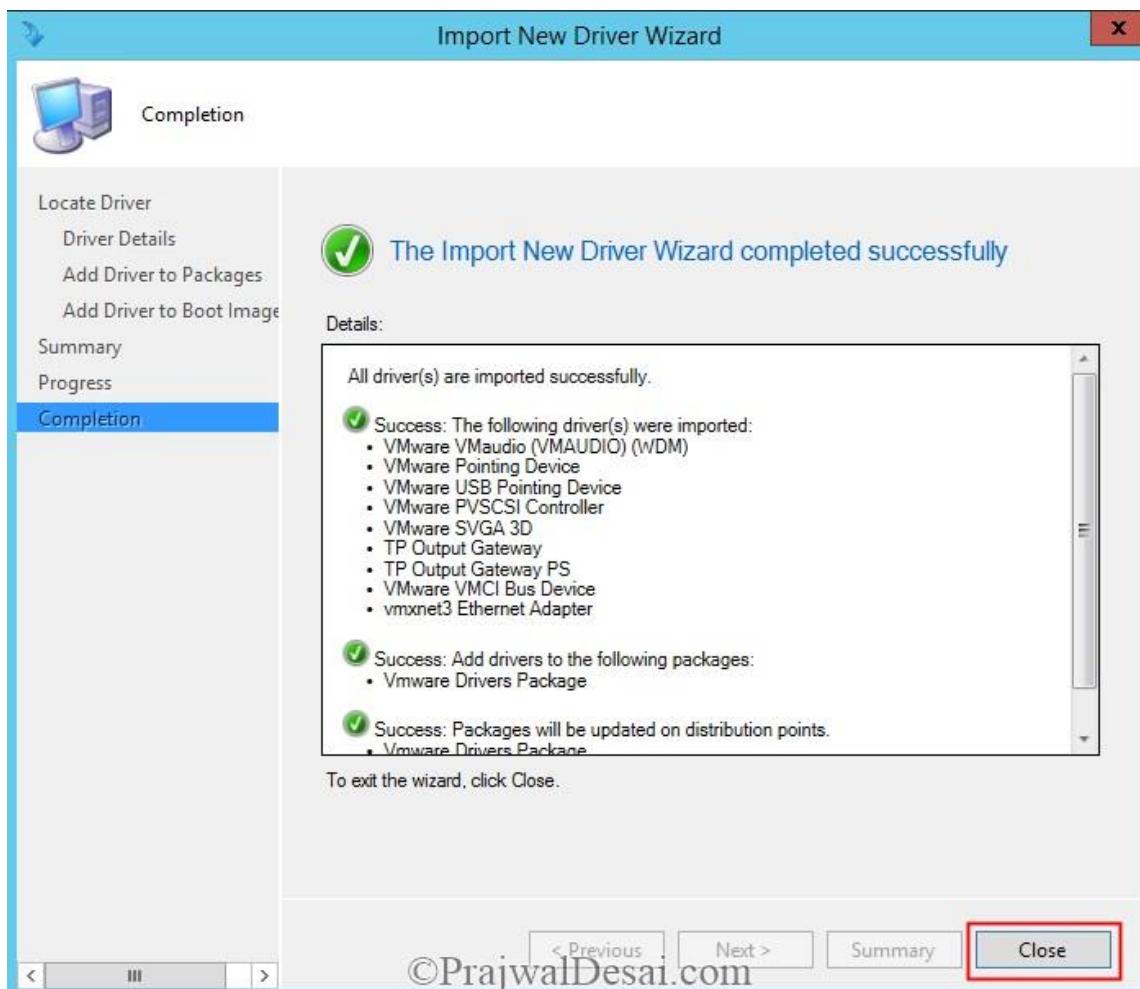
In this step you have got an option to choose which boot images to add the drivers to in addition to placing them into the driver repository and driver packages. For now we will not select any boot image, we shall configure this later.

Click Next.



You can see that the drivers are now imported successfully.

Click **Close**.

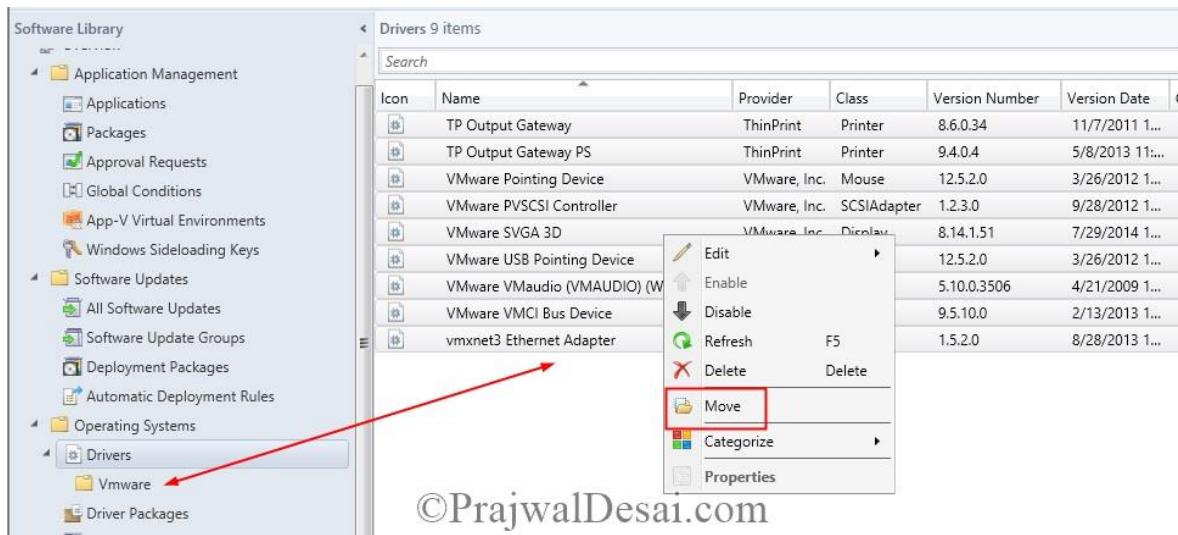


The list of imported drivers are seen under **Drivers**.

The screenshot shows the 'Software Library' interface. On the left, a tree view shows 'Application Management', 'Software Updates', and 'Operating Systems'. Under 'Operating Systems', there is a 'Drivers' folder. An arrow points from this 'Drivers' folder to a table on the right. The table is titled 'Drivers 9 items' and lists the imported drivers with columns for Icon, Name, Provider, Class, Version Number, Version Date, Categories, and Status. The drivers listed are: TP Output Gateway, TP Output Gateway PS, VMware Pointing Device, VMware PVSCSI Controller, VMware SVGA 3D, VMware USB Pointing Device, VMware VMaudio (VMAUDIO) (WDM), VMware VMCI Bus Device, and vmxnet3 Ethernet Adapter. A red arrow points from the 'Drivers' folder in the tree view to the table.

Icon	Name	Provider	Class	Version Number	Version Date	Categories	Status
TP Output Gateway	ThinPrint	Printer	8.6.0.34	11/7/2011 1...	"Vmware Drive...	Enabled	
TP Output Gateway PS	ThinPrint	Printer	9.4.0.4	5/8/2013 11...	"Vmware Drive...	Enabled	
VMware Pointing Device	VMware, Inc.	Mouse	12.5.2.0	3/26/2012 1...	"Vmware Drive...	Enabled	
VMware PVSCSI Controller	VMware, Inc.	SCSIAdapter	1.2.3.0	9/28/2012 1...	"Vmware Drive...	Enabled	
VMware SVGA 3D	VMware, Inc.	Display	8.14.1.51	7/29/2014 1...	"Vmware Drive...	Enabled	
VMware USB Pointing Device	VMware, Inc.	Mouse	12.5.2.0	3/26/2012 1...	"Vmware Drive...	Enabled	
VMware VMaudio (VMAUDIO) (WDM)	VMware	MEDIA	5.10.0.3506	4/21/2009 1...	"Vmware Drive...	Enabled	
VMware VMCI Bus Device	VMware, Inc.	System	9.5.10.0	2/13/2013 1...	"Vmware Drive...	Enabled	
vmxnet3 Ethernet Adapter	VMware, Inc.	Net	1.5.2.0	8/28/2013 1...	"Vmware Drive...	Enabled	

As you add another set of drivers, the list of drivers are listed in the same page. To make it easy, create a folder under **Drivers**, select the drivers and move them to a folder.



Next step is to add the drivers to the boot image. Right click on the **Boot Image** and click on **Drivers** tab, select the **Add** button.

Icon	Name	Version	Comment	Image ID
Boot image (x64)	6.3.9600.16384		IND00003	
Boot image (x86)	6.3.9600.16384		IND00002	

Boot image (x64) Properties

Content Locations Optional Components Security

General Images Drivers Customization Data Source Data Access Distribution Settings

Drivers:

Filter...

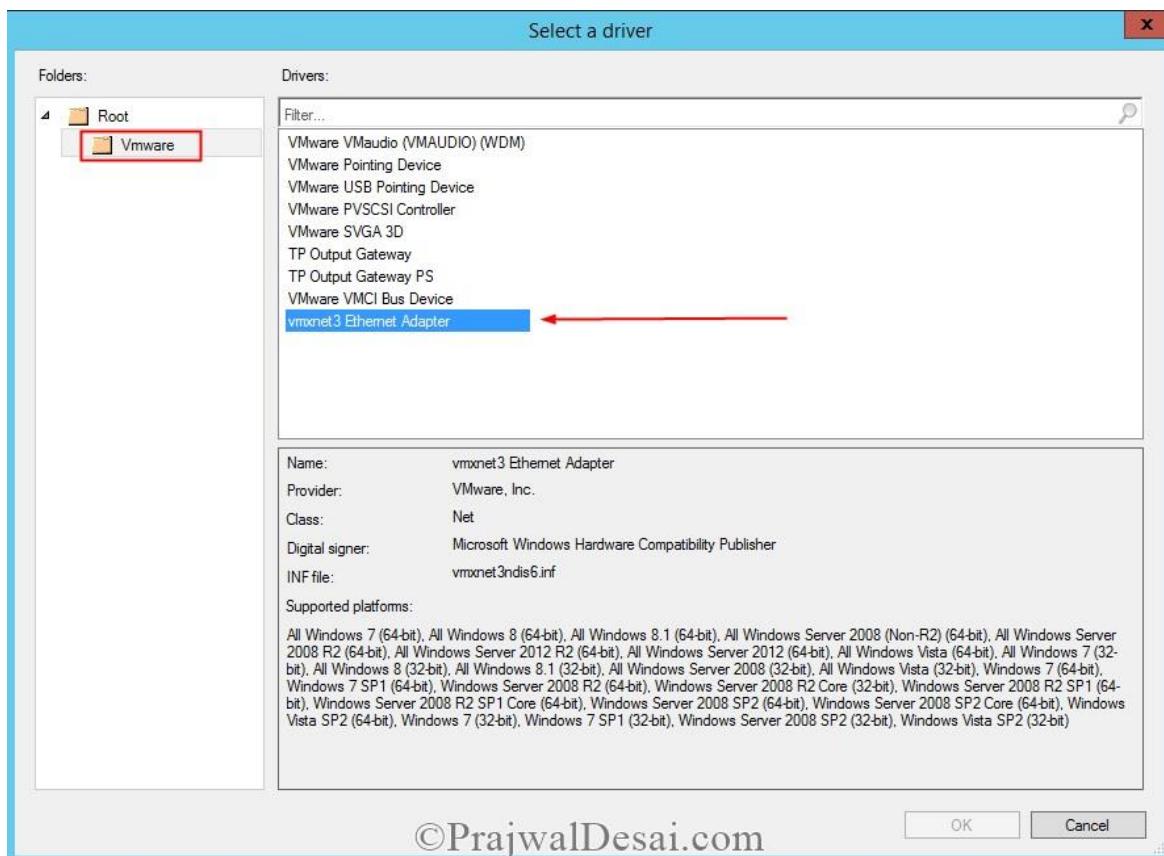
Driver name

There are no items to show in this view.

©PrajwalDesai.com

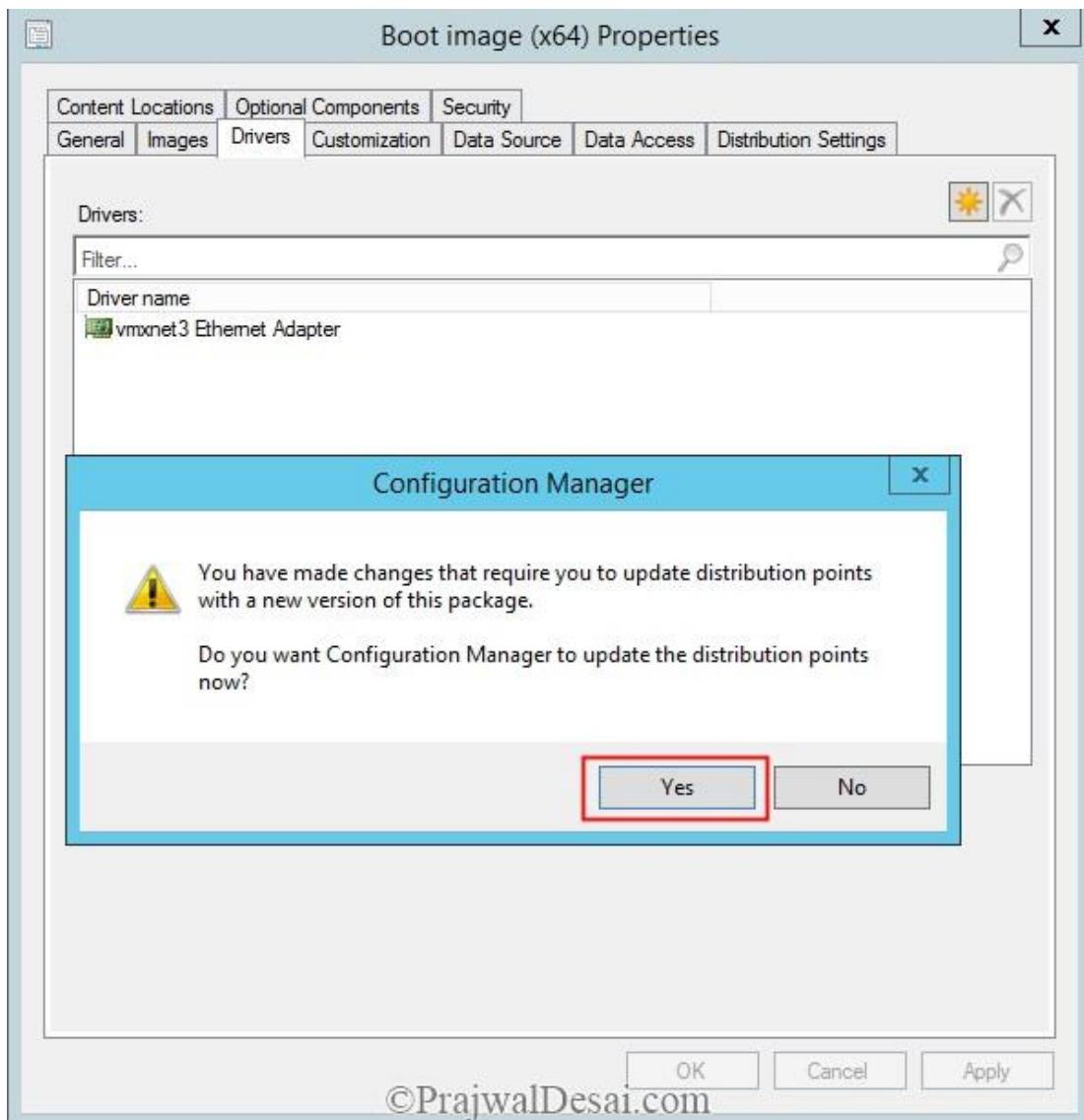
Choose the driver that you want to import to the boot image. You need to double click the driver to add it.

Click OK.



©PrajwalDesai.com

Once you have added the drivers to the boot image, it is essential to update the DP's. Click on Yes. Else you could right click on boot image and click **Update Distribution Points**.



The Driver Package is now imported, and you could use that while deploying the task sequence.

How to Deploy Office 2016 Using SCCM 2012 R2

How to deploy Office 2016 using SCCM 2012 R2 In this post we will see how to deploy Office 2016 using SCCM 2012 R2. Along with [Office 2016](#), Microsoft has released office 2016 deployment tool. [The Office 2016 Deployment Tool](#) allows the administrator to customize and manage Office 2016 Click-to-Run deployments. This tool will help administrators to manage installations sources, product or language combinations, and deployment configuration options for Office Click-to-Run. If you are confused between between Office 2016 and Office 365 here is some info about it. Microsoft Office 2016 is an Office suite that includes Microsoft Word, Excel, PowerPoint, Visual Basic for Applications, and Microsoft Query. There is a Mac version and a Windows version of Office 2016. Office 365 is the name Microsoft gives to a subscription service. Within this service various options are available depending on what you need and want to pay for. Microsoft Office 2016 for Mac and Windows are both available within an Office 365 subscription. Talking about the deployment of office 2016, I have got the Microsoft Office Professional Plus 2016 32bit volume license copy with me, we shall see how to deploy it.

Getting Started Guide for Deploying Office 365 ProPlus

Note – Microsoft Office 2016 can also be deployed using Office 2016 deployment tool, I will cover this in another post.

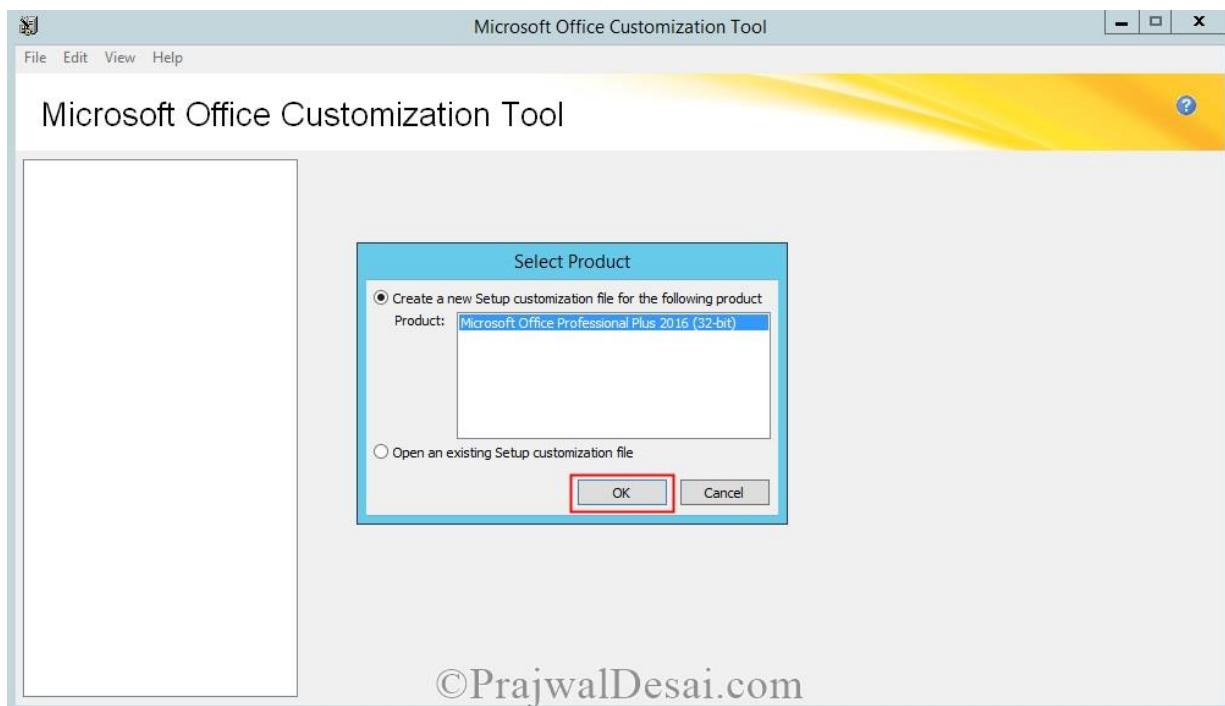
How to deploy office 2016 using SCCM 2012 R2

On the Configuration Manager server run the command prompt as administrator, change the path where office 2016 setup files are located. Run the command **setup.exe /admin**.



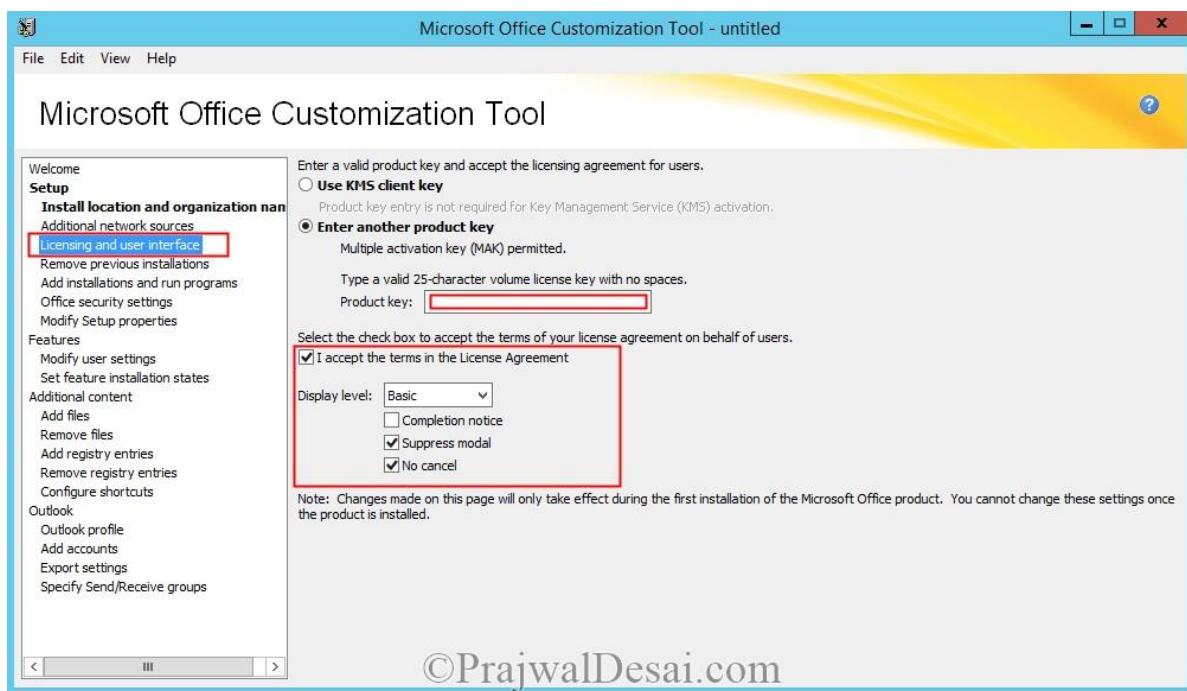
You will now see **Microsoft Office Customization Tool**, Choose **Create a new setup customization file for following product**, verify that correct product is selected.

Click on **OK**.



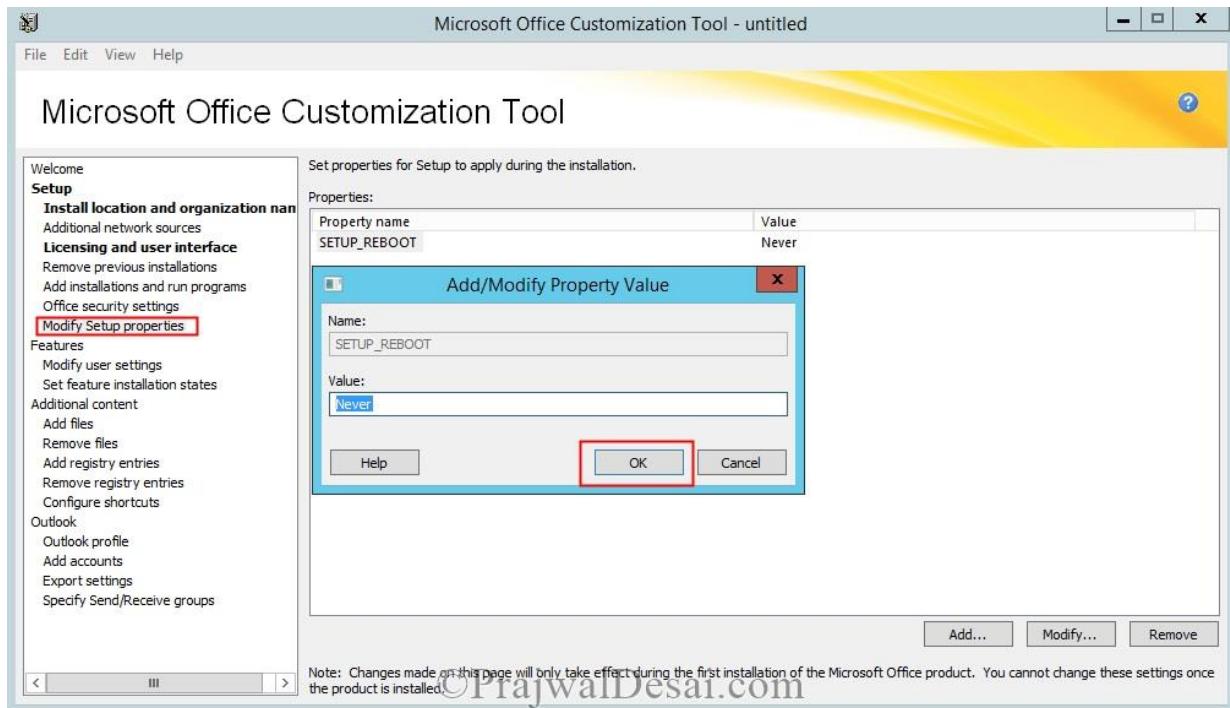
©PrajwalDesai.com

Click on **Licensing and user interface**, choose the option **Use KMS client key** if you have KMS server in your organization for activating office 2016, else choose **Enter another product key** and enter the office 2016 key. Click on **I accept the terms in the license agreement**. Select the **Display level** as **Basic**, check the box for **Suppress modal** and **No cancel**.

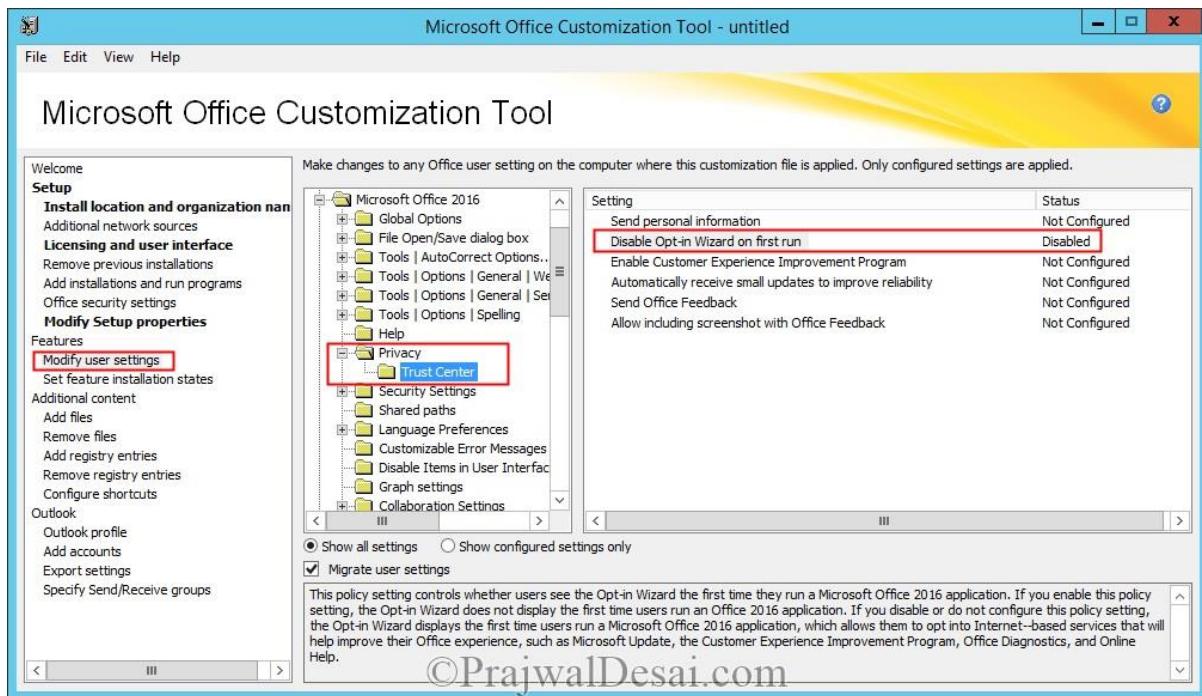


©PrajwalDesai.com

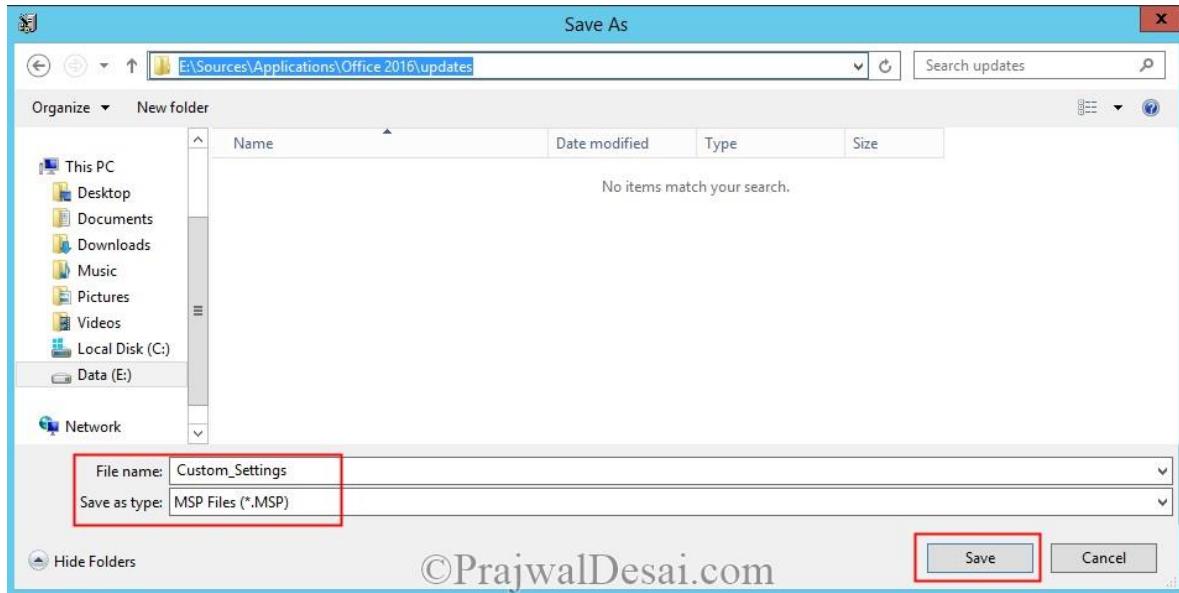
Now click on **Modify Setup properties**. Click **Add**, provide the **Name** as **SETUP_REBOOT** and **Value** as **Never**. Click **OK**.



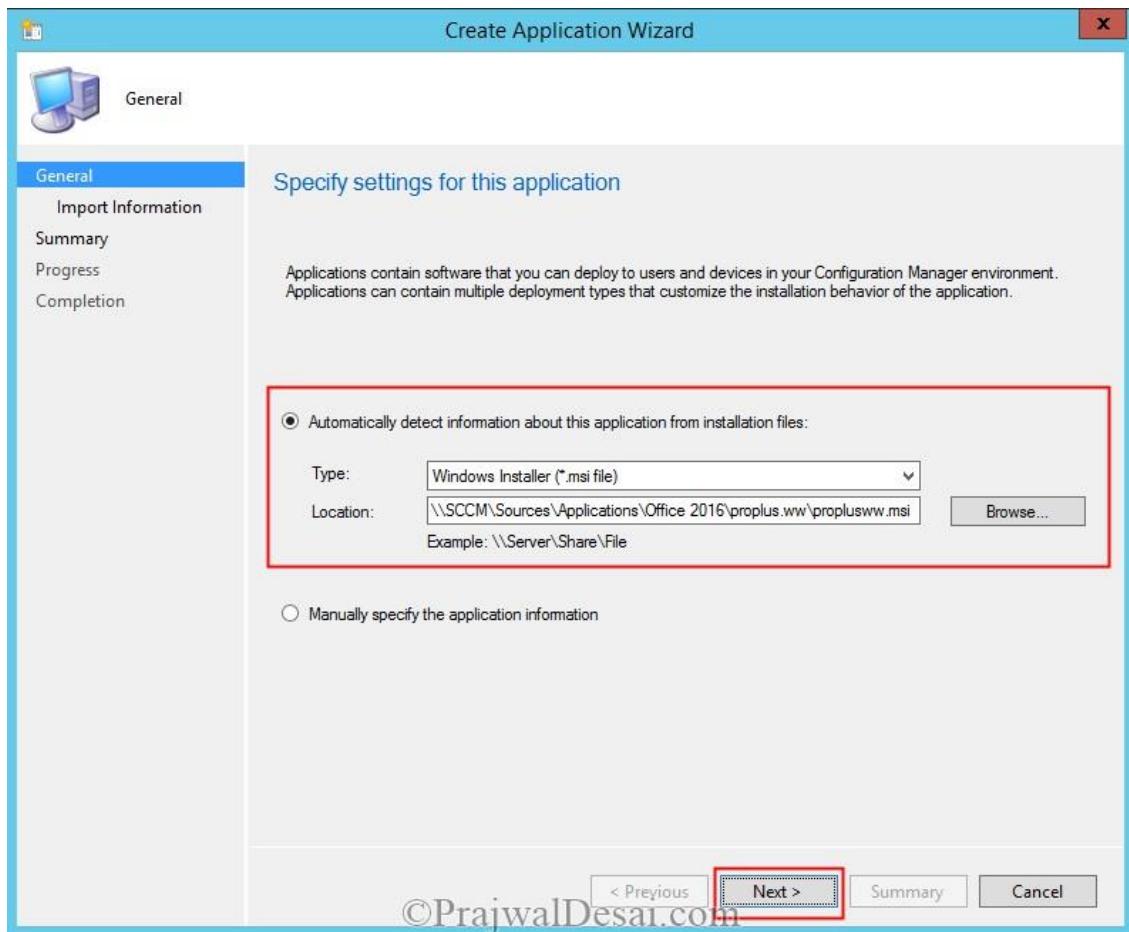
Select **Modify user settings > Microsoft Office 2016 > Privacy > Trust Center**. Double click the setting **Disable Opt-in Wizard** on first run and set the status as **Enabled**.



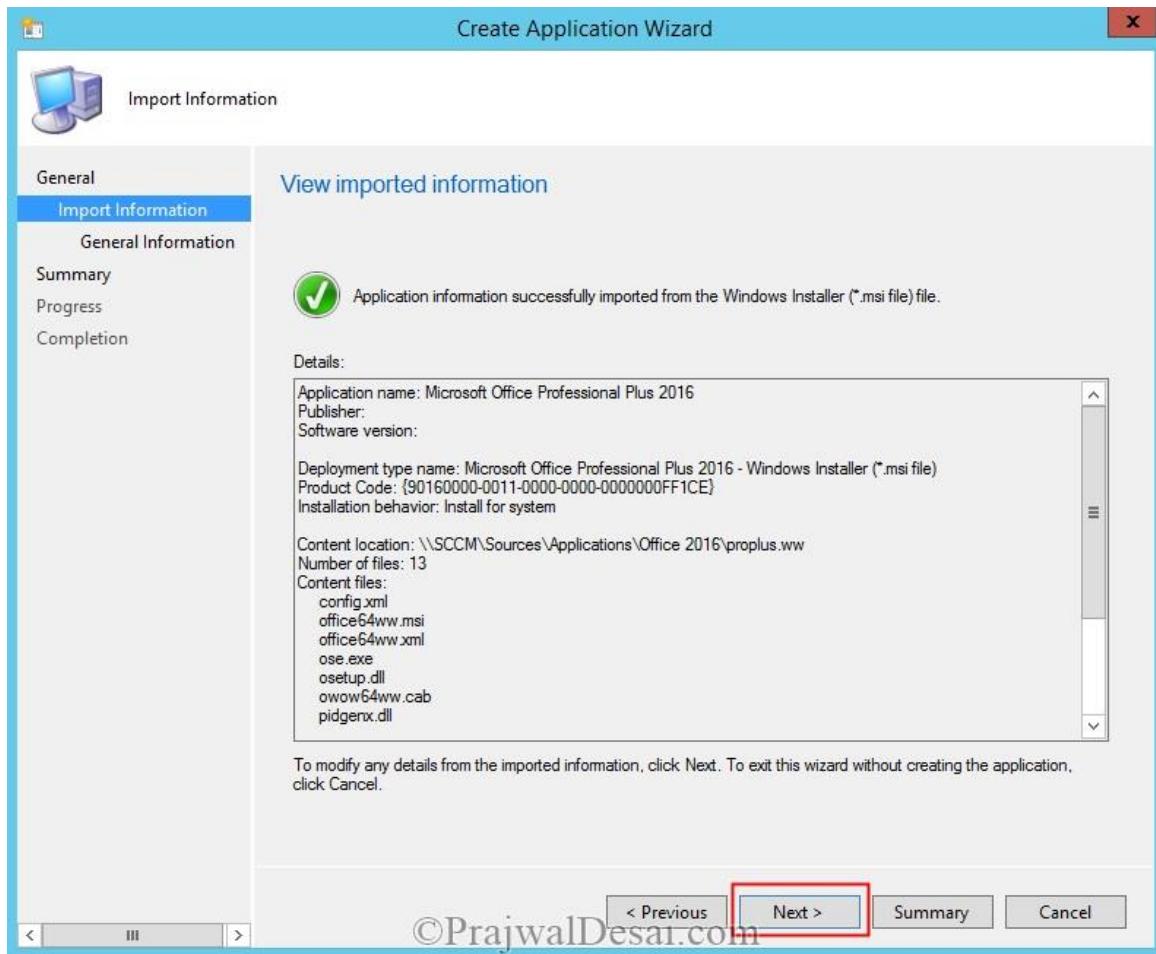
Now click on **File -> Save As** -> save the customization file inside **Updates** folder. Close the OCT tool.



Open the SCCM 2012 R2 console, under the **Application Management**, right click **Applications** and click **Create Application**. Choose **Automatically detect information** and provide the path to file **proplusww.msi**. Click **Next**.

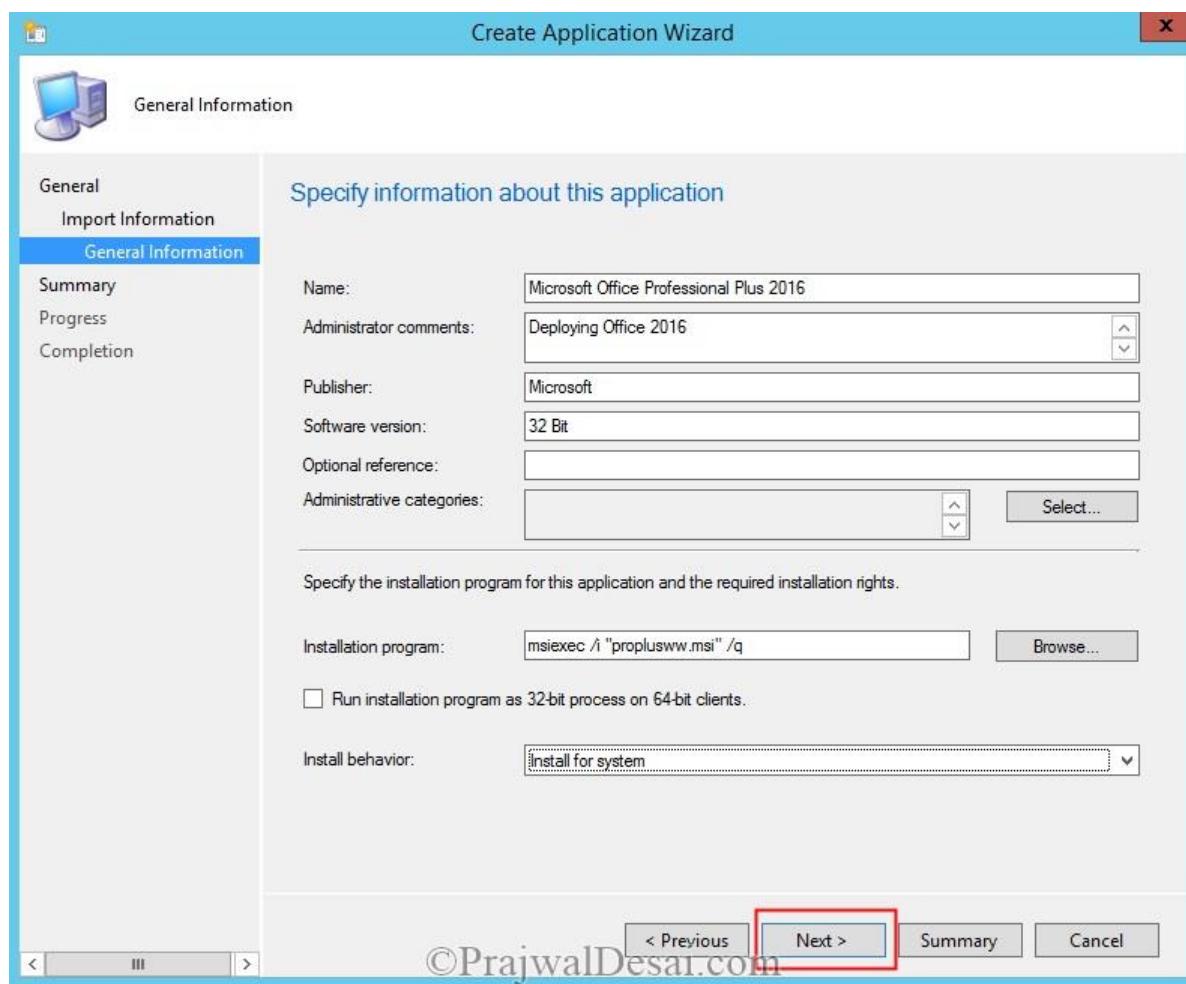


The application information has been imported from msi file. Click **Next**.



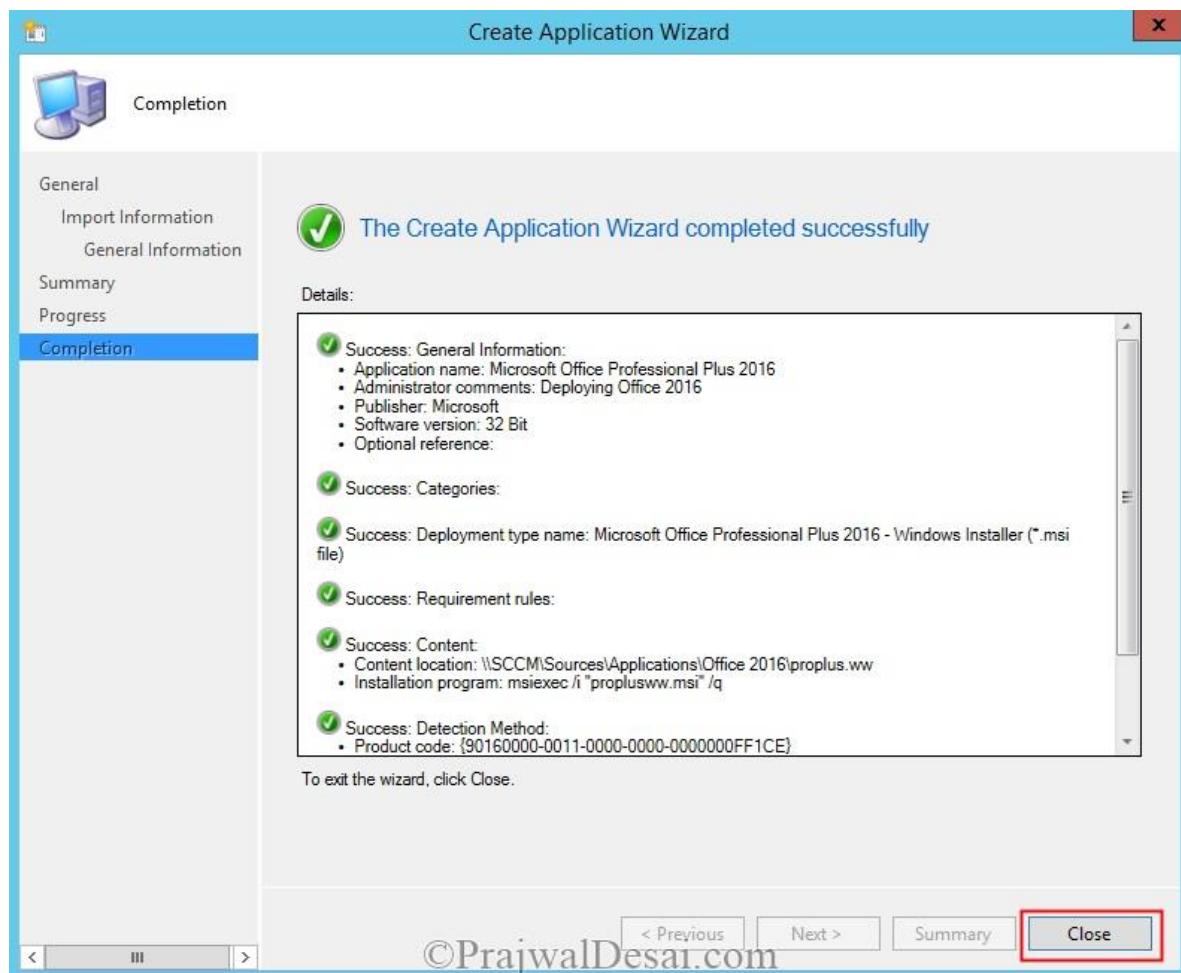
You can specify a little information about this application. We will change the **Installation program** command later. Choose the **Install behavior** as **Install for system**.

Click **Next**.



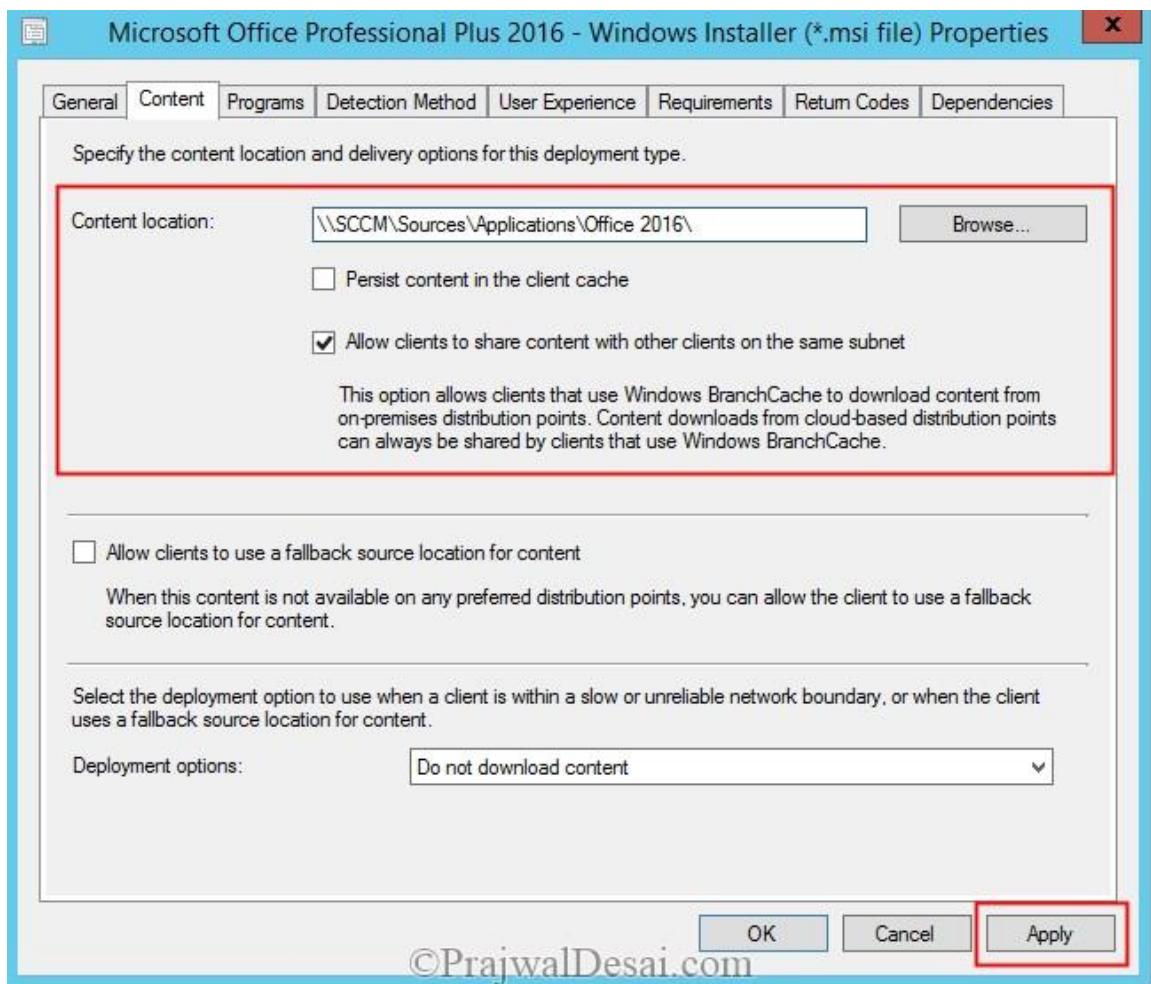
The Application has been created successfully.

Click **Close**.



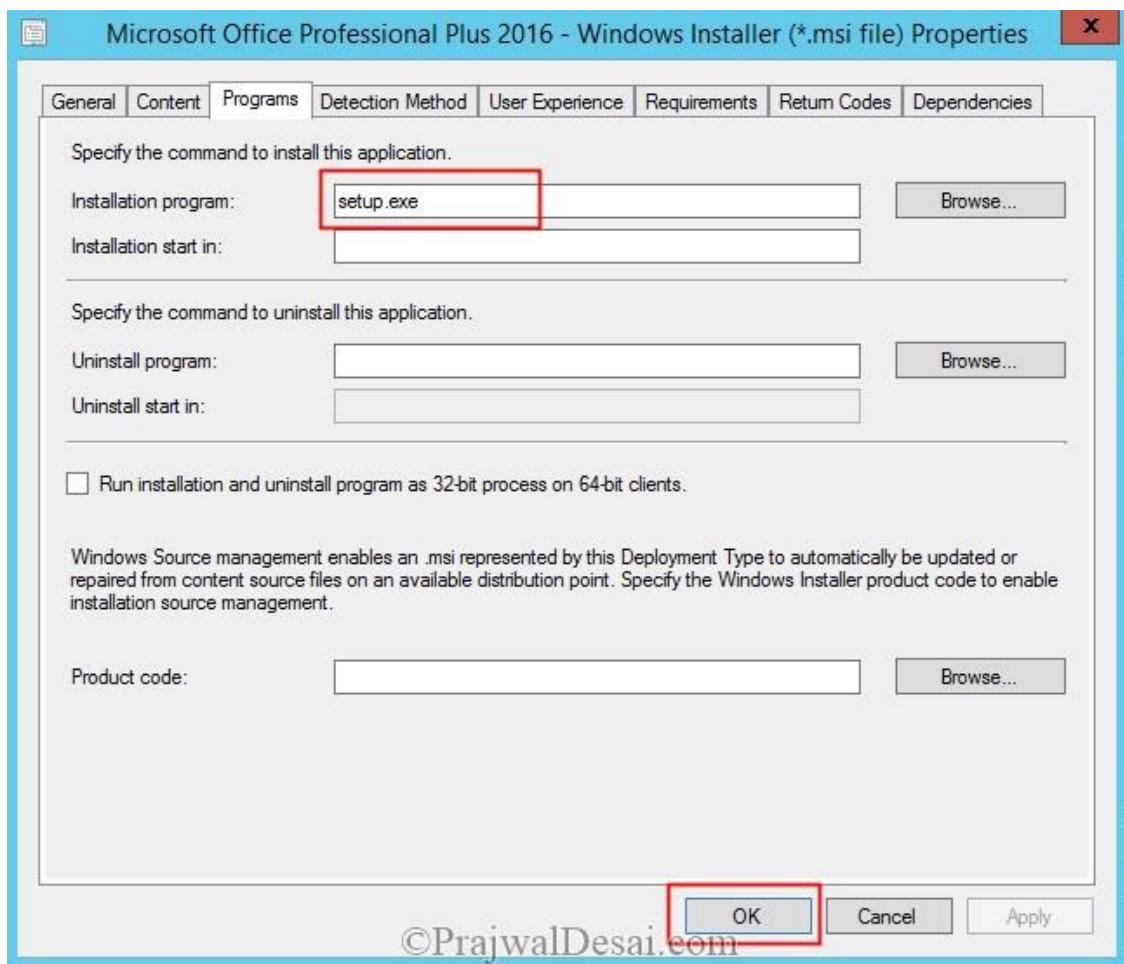
Right click the Office 2016 application, click on **Properties**. Click on **Deployment Types** tab, click on the msi file and click **Edit**. Click on **Content** tab, set the Content location to Office 2016 folder (or a folder where Office 2016 installation files are present, remove **proplus.ww** after **Office 2016**).

Click on **Apply**.



Click on **Programs** tab, change the **Installation Program** command to **setup.exe**.

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



The next step is to make the application available to DP. Right click the Office 2016 application, click on **Distribute Content**, choose you DP and wait until the application is available with DP. You can verify this by checking the Content Status of the Office 2016 application under Distribution Status.

Deploy the Office 2016 application to the desired collection. Right click on the Office 2016 application and click on **Deploy**. Choose the Device Collection and choose the **Action as Install** and **Purpose as Available**. (I haven't covered the screenshots of deploying application as it's simple to deploy an application to collection).

After few minutes, on the client computer we see that the application is available. Select the software and click on **Install Selected**.

The screenshot shows the Software Center window with the following details:

- Available Software** tab is selected.
- Search bar: **SEARCH**, **Find additional applications from the Application Catalog**.
- Filter: **SHOW** dropdown set to **All**, **Show optional software** checkbox checked.
- Table headers: **NAME**, **TYPE**, **PUBLISHER**, **AVAILABLE...**, **STATUS**.
- Table data: Microsoft Office Professional Plus... (Application, Microsoft, 10/16/2015, Available).
- Details for Microsoft Office Professional Plus 2016:

OVERVIEW		REQUIREMENTS		DESCRIPTION
Status:	Available	Restart required:	Might be required	Deploying Office 2016
Version:	32 Bit	Download size:	820 MB	
Date published:	Not specified	Estimated time:	Not specified	
Help document:	None	Total components:	1	
- INSTALL SELECTED** button.

Open **Appenforce.log** file in case you face issues with installation. You could also monitor the installation process.

The screenshot shows the Configuration Manager Trace Log Tool displaying the **Appenforce.log** file. The log entries are as follows:

```

Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\AppEnforce.log]
File Tools Window Help
Log Text Component Date/Time Thread
+++ Starting Install enforcement for App DT "Microsoft Office Professional Plus 2016 - Windows Installer (*.msi file)"...
A user is logged on to the system.
Performing detection of app deployment type Microsoft Office Professional Plus 2016 - Windows Installer (*.msi fil...
+++ Application not discovered. [AppId: Scopeld_4B36E891-4305-4237-B3AF-656B16EAD8D4/DeploymentType_6...
App enforcement environment: Context: MachineCommand line: setup.exeAllow user interaction: NoUI mode: 0U...
Prepared working directory: C:\Windows\ccmcache\2
Prepared command line: "C:\Windows\ccmcache\2\setup.exe"
Executing Command line: "C:\Windows\ccmcache\2\setup.exe" with user context
Working directory C:\Windows\ccmcache\2
Post install behavior is BasedOnExitCode
Waiting for process 3864 to finish. Timeout = 120 minutes.
Process 3864 terminated with exitcode: 0
Looking for exit code 0 in exit codes table...
Matched exit code 0 to a Success entry in exit codes table.
Performing detection of app deployment type Microsoft Office Professional Plus 2016 - Windows Installer (*.msi fil...
+++ Discovered application [AppDT Id: Scopeld_4B36E891-4305-4237-B3AF-656B16EAD8D4/DeploymentType_6e54...
++++++ App enforcement completed (229 seconds) for App DT "Microsoft Office Professional Plus 2016 - Windows...
Date/Time: 10/16/2015 1:33:10 AM Component: AppEnforce
Thread: 1144 (0x478) Source: appprovider.cpp:2448
++++++ App enforcement completed (229 seconds) for App DT "Microsoft Office Professional Plus 2016 - Windows Installer (*.msi file)" [ScopeId: 4B36E891-4305-4237-B3AF-656B16EAD8D4/DeploymentType_6e54a38-422f-4d53-99b4-8f1fe54a8c40], Revision: 2, User SID: ] ++++++
Elapsed time is 0h 40m 36s 575ms (2436.575 seconds)

```

A red arrow points to the final log entry indicating the completion of the app enforcement process.

The application is first downloaded to the client computer and then installed. We now see that the application is installed successfully.

Software Center

PRAJWAL.LOCAL.ORG

Available Software Installation Status Installed Software Options

SHOW All SEARCH Find additional applications from the Application Catalog

NAME	TYPE	PUBLISHER	AVAILABLE...	STATUS
Microsoft Office Professional Plus 2016	Application	Microsoft	10/16/2015	Installed

 Microsoft Office Professional Plus 2016

OVERVIEW		REQUIREMENTS		DESCRIPTION
Status:	Installed	Restart required:	Might be required	Deploying Office 2016
Version:	32 Bit	Download size:	820 MB	
Date published:	Not specified	Estimated time:	Not specified	
Help document:	None	Total components:	1	
Date Modified:	10/16/2015			

UNINSTALL

©PrajwalDesai.com



How to Deploy Fonts Using SCCM 2012 R2

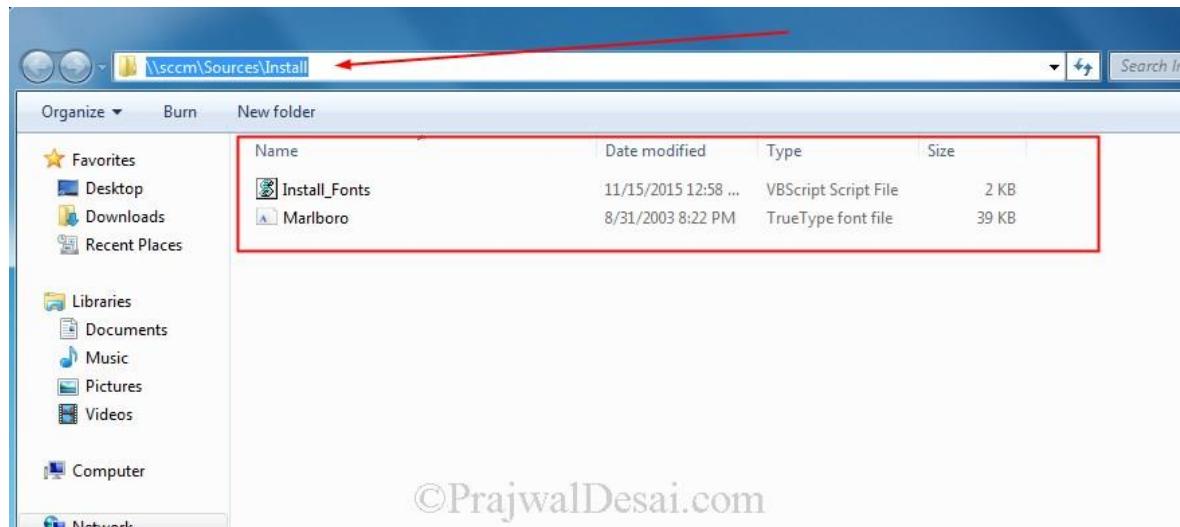
In this post we will see steps on how to deploy fonts using Configuration Manager 2012 R2. If you have been tasked with deploying fonts using SCCM this post should help you. A font is a set of printable or displayable text characters in a specific style and size. One of the most popular outline font software programs on today's computers is **TrueType** fonts. TrueType fonts come with both Windows and Macintosh operating systems. Normally if you want to install a font the easiest way is to double-click on a font file to open the font preview and select '**Install**'. But if you want to deploy the same font on multiple computers, we have to make use of script that does the job. When you deploy a script (SCCM Package) to install the font, the user that is logged on to the computer will not be able to use or see these new fonts until they log out and log in back. If you run this script on a standalone computer the fonts are installed and can be seen used by users. The strange thing is when SCCM deploys the same package and runs the same script the fonts gets installed correctly but they appear to be missing. After a log off and login the fonts can be seen.

As mentioned earlier we will use a script to deploy font. You can download the script by clicking on the below button.

[Download Install Fonts Script](#)

How to deploy fonts using Configuration Manager 2012 R2

Copy the script file and font to a shared folder. The font that I be deploying is Marlboro font which is available free for [Download](#).



Open the script file with notepad or any editor, set the font source path to the location where the font is located. You just need to specify the path up to the folder where the font is present. Save and close the file.

```

Install_Fonts - Notepad
File Edit Format View Help
Dim objshell, objFSO, wshshell
Dim strFontSourcePath, objFolder, objFont, objNameSpace, objFile

set objshell = CreateObject("shell.Application")
Set wshshell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")

Wscript.Echo "-----"
Wscript.Echo " Script to install Fonts "
Wscript.Echo "-----"
Wscript.Echo " "

strFontSourcePath = "\\\\$ccm\\Sources\\Install"

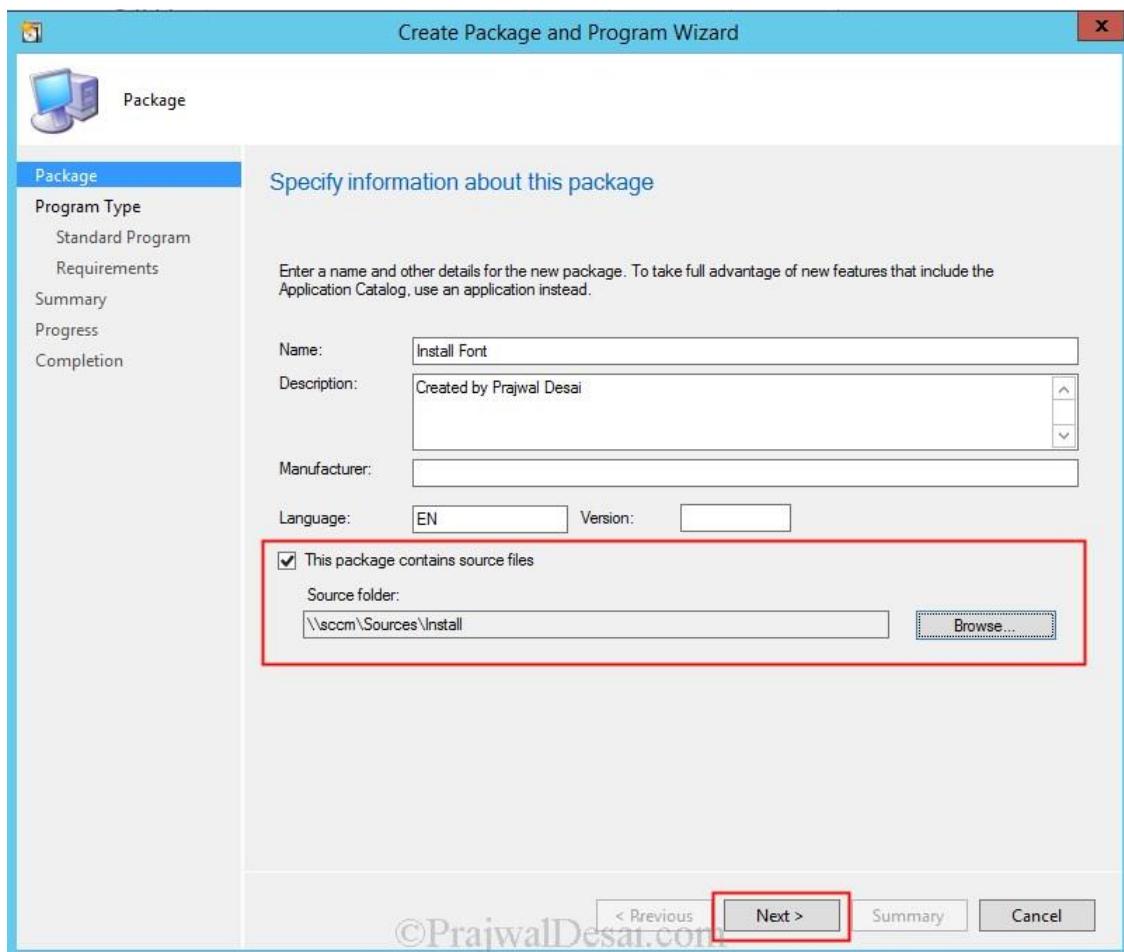
If objFSO.FolderExists(strFontSourcePath) Then

Set objNamespace = objshell.Namespace(strFontSourcePath)
Set objFolder = objFSO.GetFolder(strFontSourcePath)

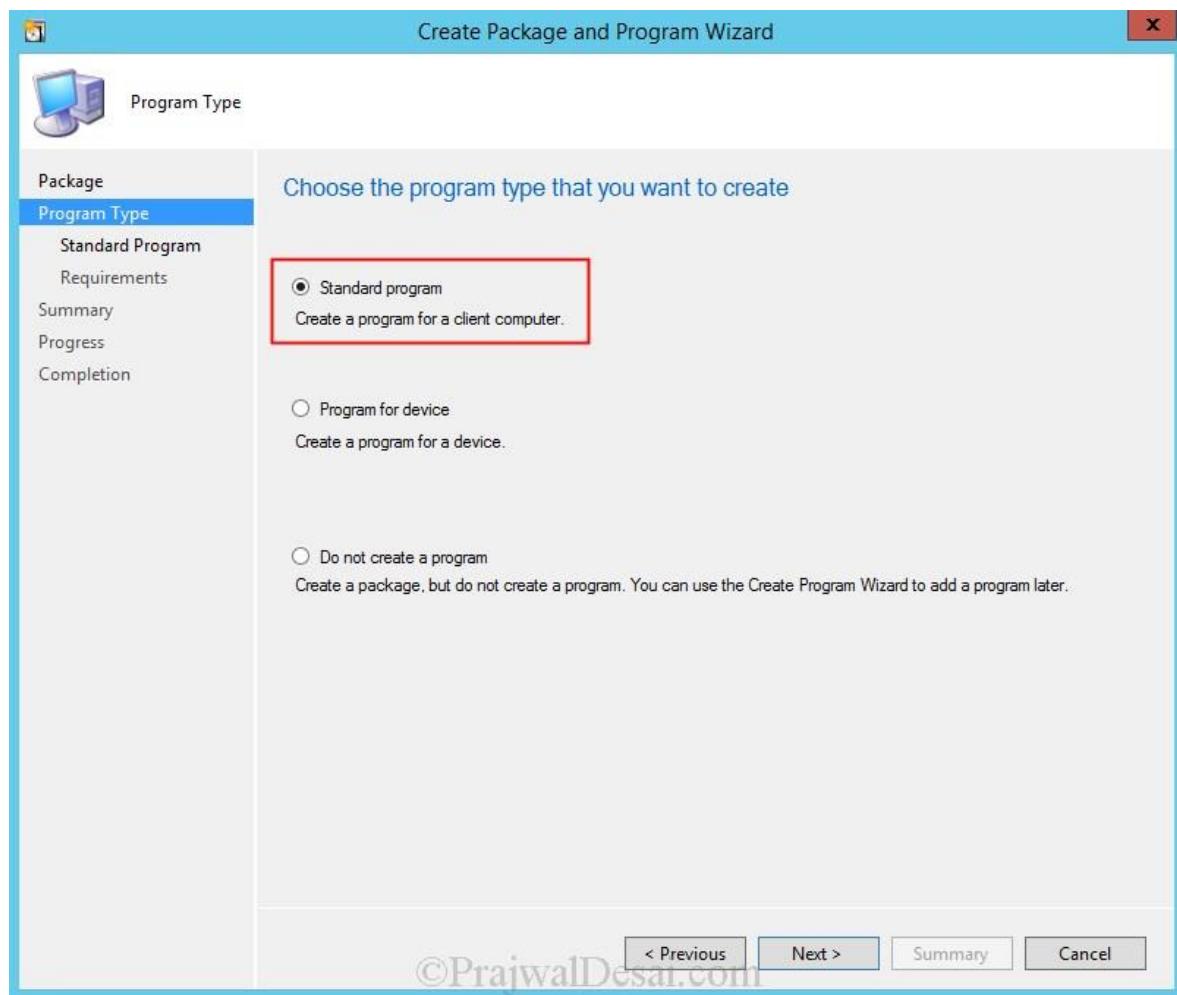
```

©PrajwalDesai.com

In Configuration Manager console, choose **Software Library**. In the **Software Library** workspace, expand **Application Management**, and then choose **Packages**. Right click **Packages** and click **Create Package**. Specify the **Name**, **Source folder** and click **Next**.

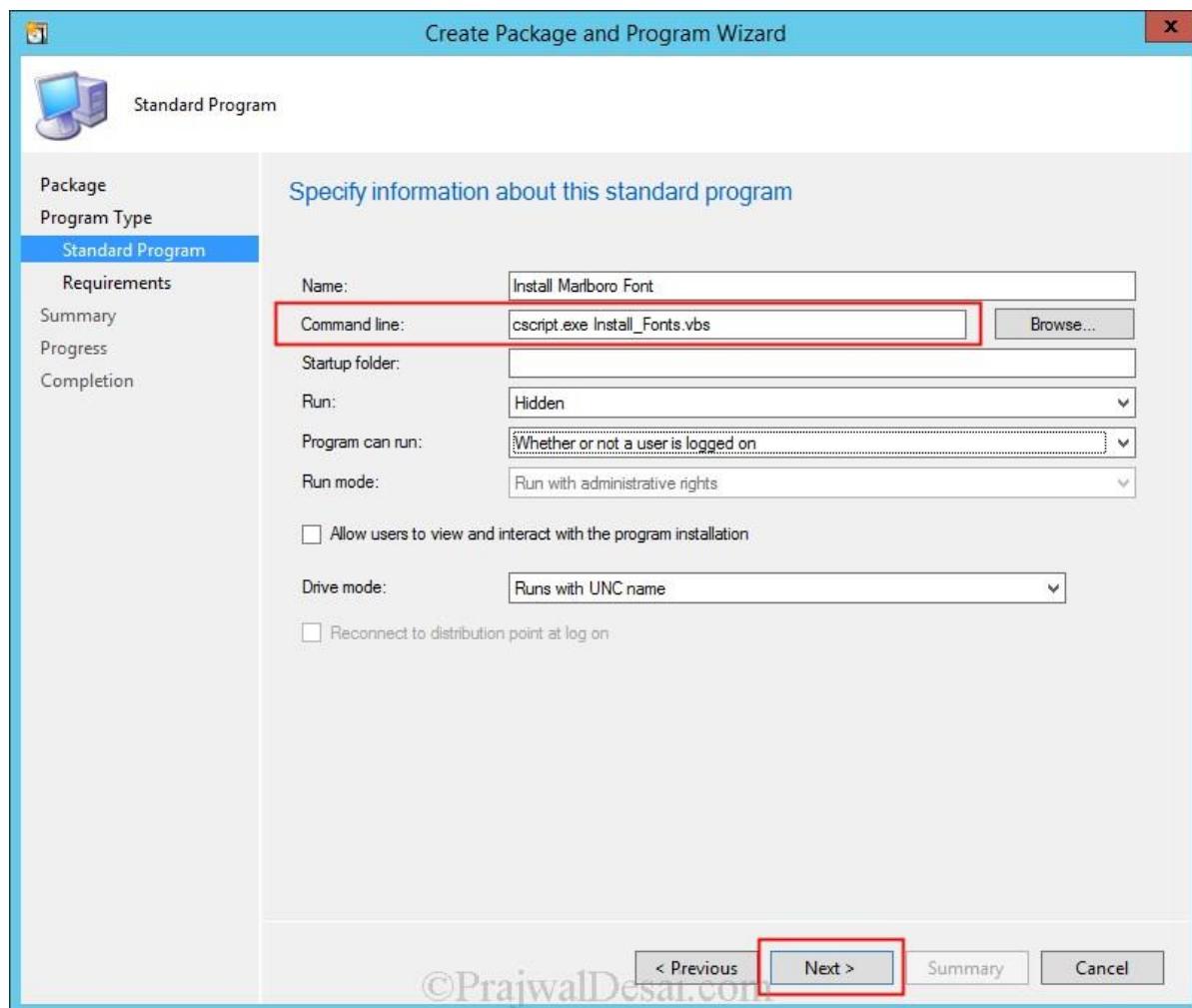


Choose the **Program Type** as **Standard Program**. Click **Next**.

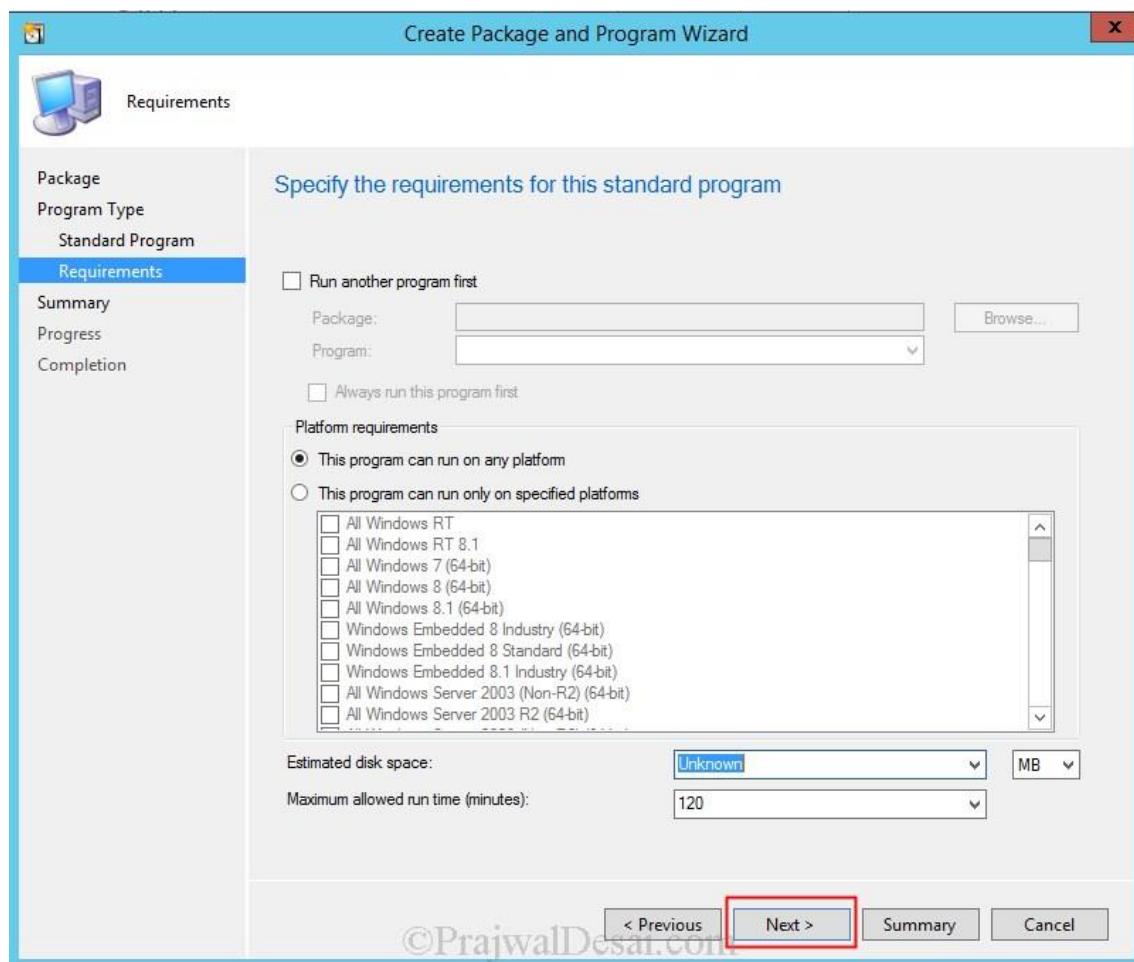


Specify the **Name** for the standard program, enter the Command line as ***cscript.exe filename.vbs***.

Choose the program to run whether or not a user is logged on. click **Next**.

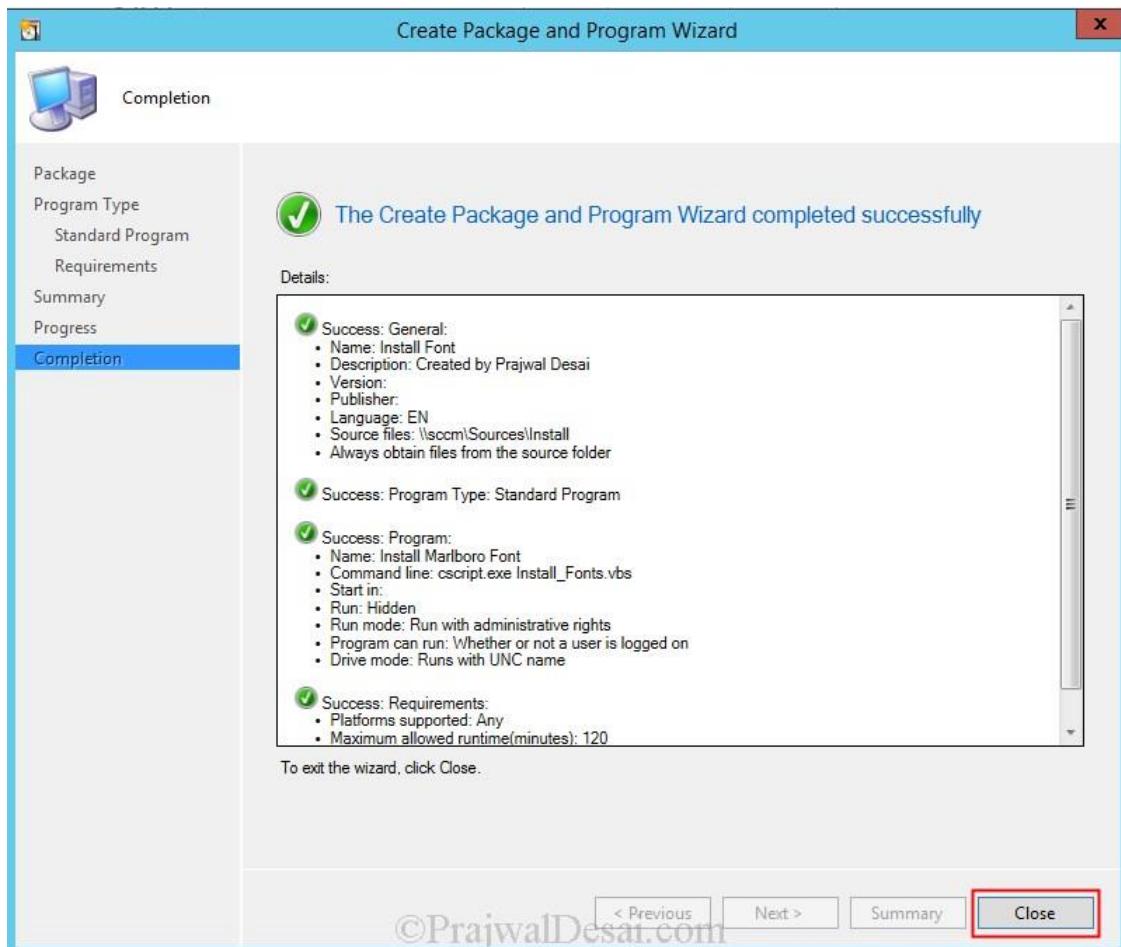


Click Next.



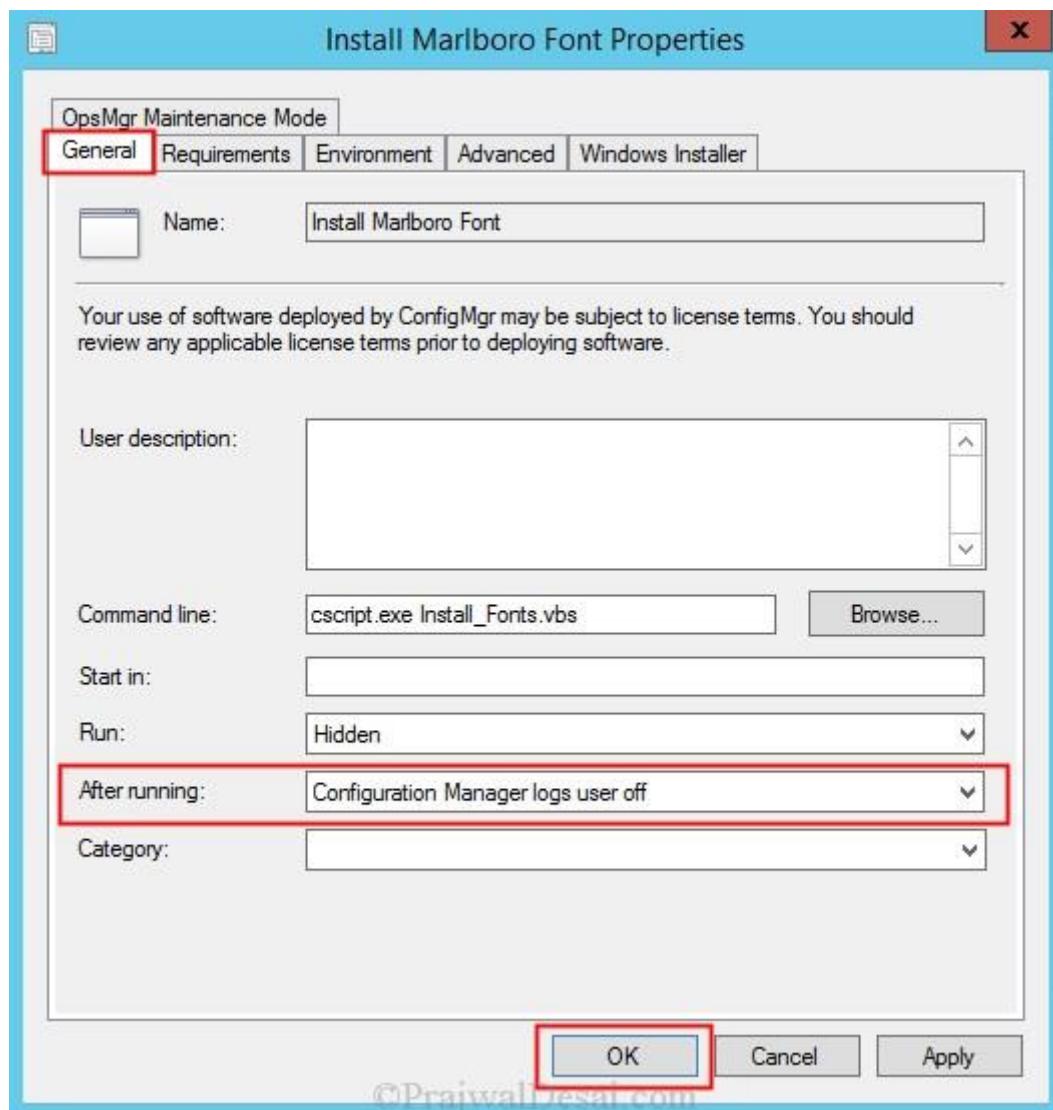
The package has been created successfully.

Click **Close**.

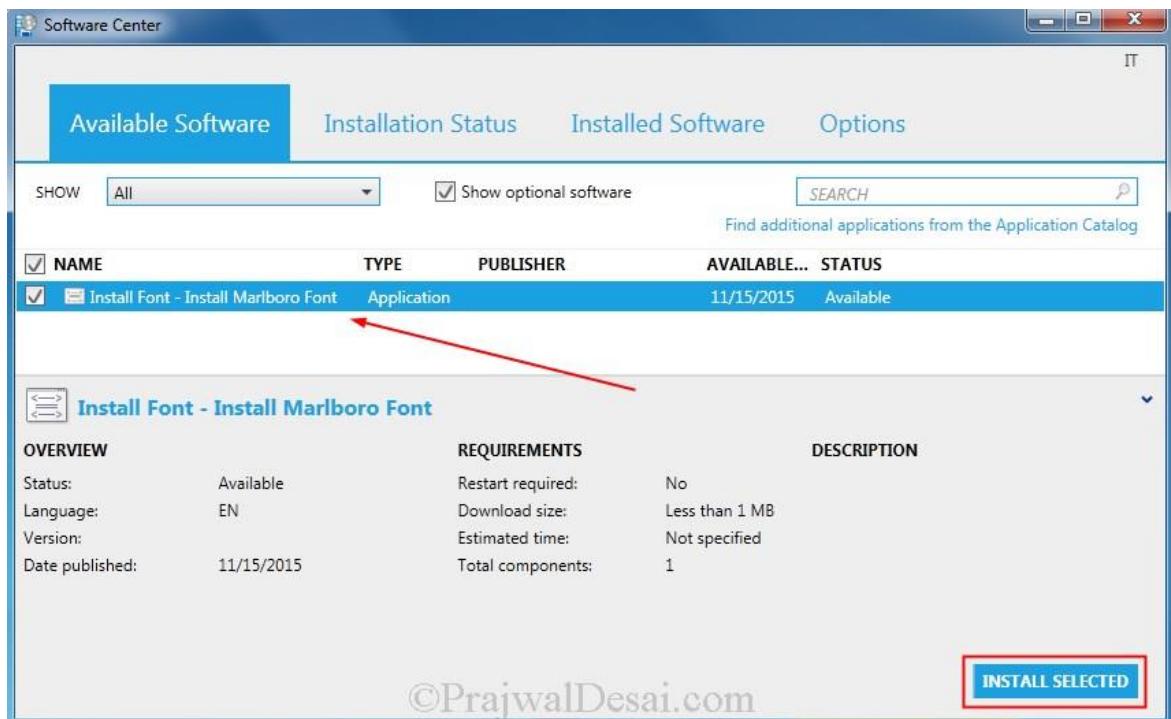


After the package is created, click on the package and at the bottom pane, click the **Programs** tab. Right click the Program and click **Properties**. On the **General** tab, choose **After running** option to **Configuration Manager logs user off**. As I mentioned in the beginning of the post that when the script installs new font, until the user logs out and logs in back the font is not seen.

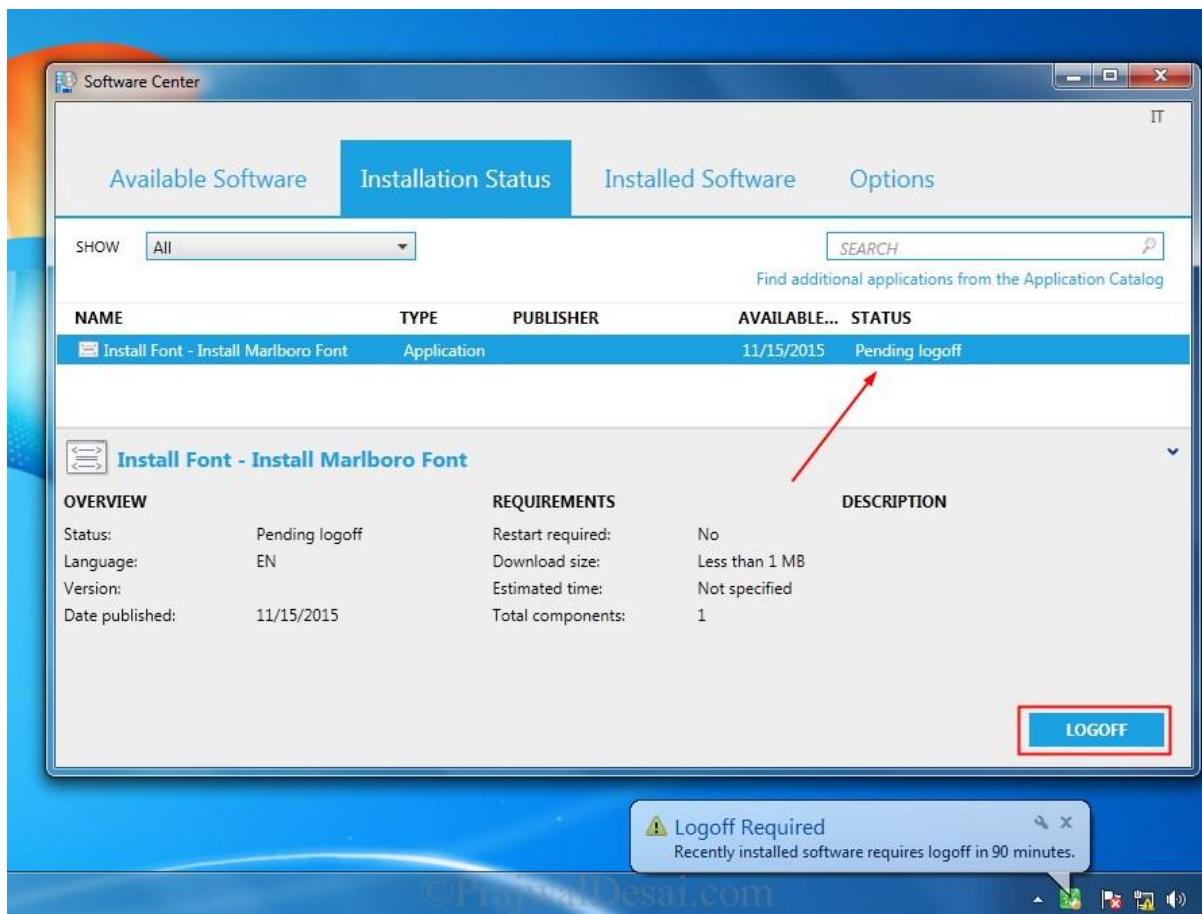
Click **Apply** and **OK**.



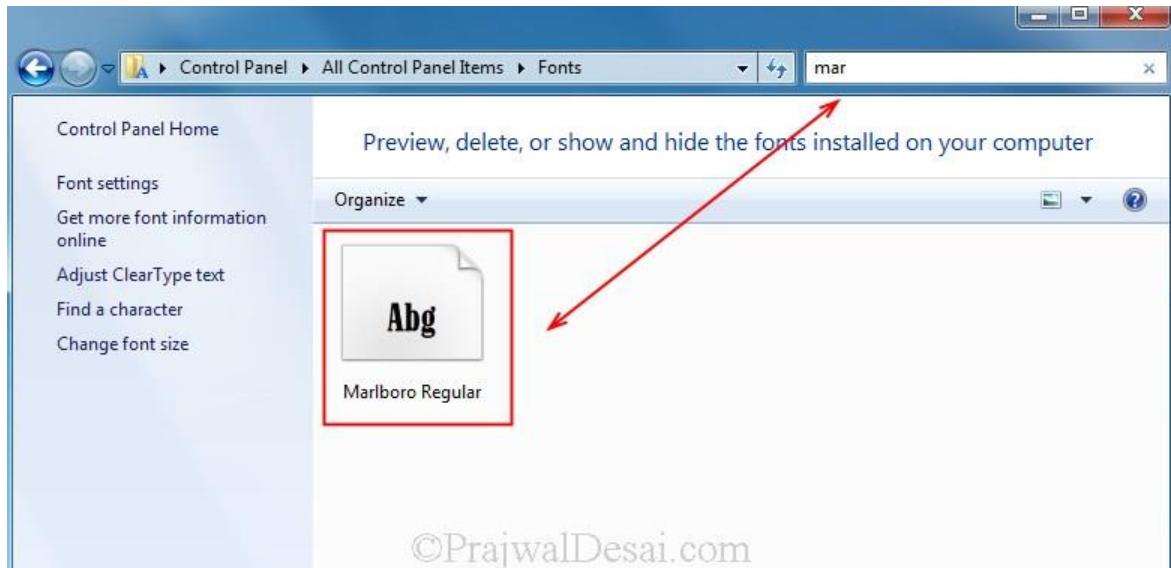
Your package is ready to be deployed. Right click on the package and Distribute the content to the DP. Once the content is available with the DP, right click the package and click **Deploy**. Deploy the package to the desired collection. Choose the deployment purpose as Available or Required. Since a log off is required after we deploy this package, I will be deploying this package as Available. A log off notification will be seen by user when the software is installed from the Software Center. After you deploy the package, wait for few minutes, the package will be available for install in the software center. To install the software click **Install Selected**.



After the software is installed, the status is now Pending Logoff. To log off click on **Logoff**.



After the user logs in, on the client computer, launch the Control Panel, click on **Fonts** and in the search bar type the font name. You can see that the font Marlboro Regular is in list of fonts.



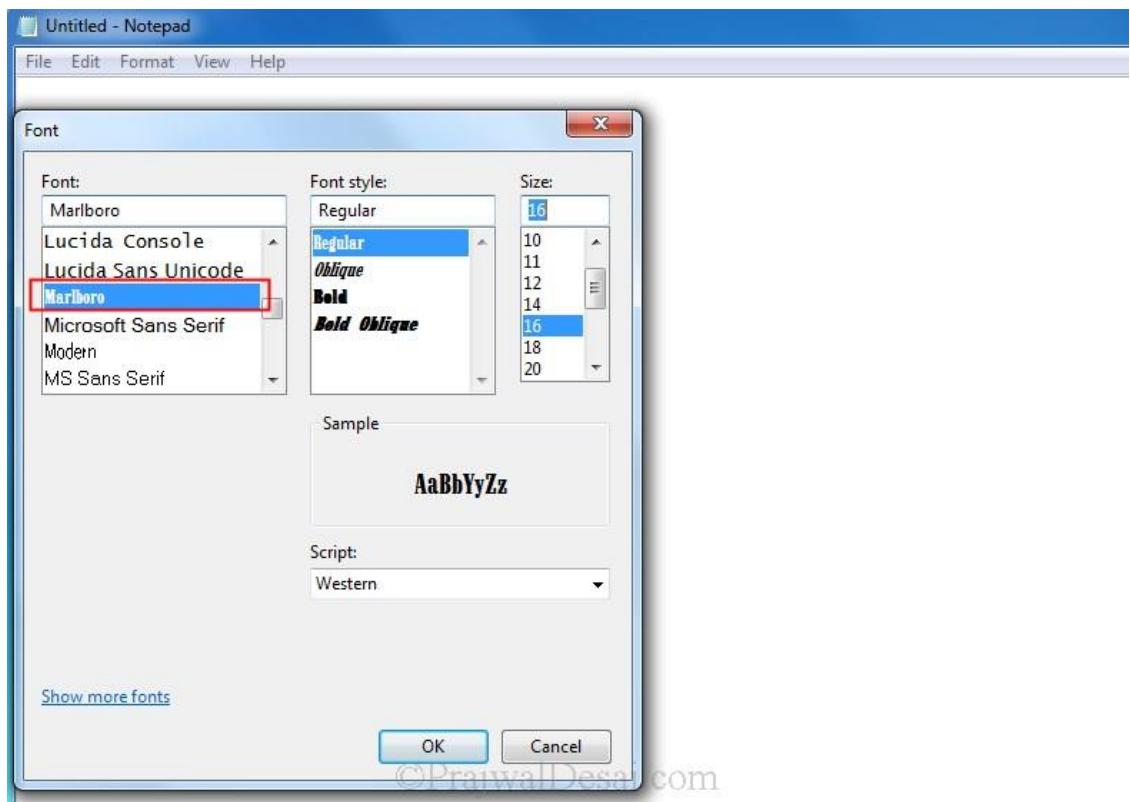
©PrajwalDesai.com

On the client computer open execmgr.log file for troubleshooting the deployment. In the below screenshot we see that the Marlboro font has been installed successfully.

Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\execmgr.log]			
	Component	Date/Time	Thread
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00006",ProgramI...	execmgr	11/15/2015 3:20:11 AM	3896 (0xF38)
MTC task with id {344FD001-B4DC-424D-873F-68B5CD854CA4}, changed state from 4 to 5	execmgr	11/15/2015 3:20:11 AM	3532 (0x DCC)
Program exit code 0	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Looking for MIF file to get program status	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Script for Package:IND00006, Program: Install Marlboro Font succeeded with exit code 0	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Raising event:[SMS_CodePage(437), SMS_LocaleID(1033)]instance of SoftDistProgramCompletedSuccessful...	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Raised Program Success Event for Ad:IND20001, Package:IND00006, Program: Install Marlboro Font	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Execution is complete for program Install Marlboro Font. The exit code is 0, the execution status is Success...	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Raising client SDK event for class NULL, instance NULL, actionType 5!, value 14475378145400900, user NULL...	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
Raising client SDK event for class CCM_Program, instance CCM_Program.PackageID="IND00006",ProgramI...	execmgr	11/15/2015 3:20:14 AM	3548 (0x DDC)
The user has logged off.	execmgr	11/15/2015 3:20:40 AM	816 (0x330)
The user logged off while program Install Marlboro Font is notifying the user for logoff. Consider execution...	execmgr	11/15/2015 3:20:40 AM	816 (0x330)
Requesting MTC to delete task with id: {344FD001-B4DC-424D-873F-68B5CD854CA4}	execmgr	11/15/2015 3:20:40 AM	816 (0x330)
MTC task with id: {344FD001-B4DC-424D-873F-68B5CD854CA4} deleted successfully.	execmgr	11/15/2015 3:20:40 AM	816 (0x330)
A user has logged on.	execmgr	11/15/2015 3:20:45 AM	3852 (0xF0C)
The logged on user is PRAJWAL\test	execmgr	11/15/2015 3:20:45 AM	3852 (0xF0C)
Execution Manager timer has been fired.	execmgr	11/15/2015 3:21:40 AM	2128 (0x850)
Date/Time: 11/15/2015 3:20:14 AM Component: execmgr			
Thread: 3548 (0x DDC) Source: execmgr.cpp:4165			
Execution is complete for program Install Marlboro Font. The exit code is 0, the execution status is SuccessLogoffRequired			
Elapsed time is 205h 50m 53s 459ms (741053.459 seconds)			

So how do you verify whether the font is available for use ?. Open Ms Word or notepad, look for changing the default fonts and you will see the installed font under Fonts.

©PrajwalDesai.com



PKI requirements for SCCM 2012 R2

PKI Certificate Requirements for SCCM 2012 R2 In this post we will see the PKI certificate requirements for SCCM 2012 R2. This is one of the post which is a part [Deploy PKI Certificates for SCCM 2012 R2 Step by Step Guide](#). Before we proceed let's get to know what PKI is. Public-key cryptography (also called asymmetric-key cryptography) uses a key pair to encrypt and decrypt content. The key pair consists of one public and one private key that are mathematically related. An individual who intends to communicate securely with others can distribute the [public key](#) but must keep the [private key](#) secret. Content encrypted by using one of the keys can be decrypted by using the other. PKI can be used to secure e-mail, secure web communications, secure web sites, digital signing of software files etc.

When you use Active Directory Certificate Services and certificate templates, the [Microsoft PKI solution](#) can ease the management of the certificates. One thing to note here is template-based certificates can be issued only by an enterprise certification authority running on the Enterprise Edition or Datacenter Edition of the server operating system. The HTTPS protocol provides client-to-server communications that are mutually authenticated, signed, and encrypted. Internet clients must use HTTPS, and all clients are more secure if configured to use HTTPS. You must deploy the required certificate to each client and site system that will use HTTPS.

PKI Certificate Requirements for SCCM 2012 R2

The following table lists the types of PKI certificates that are required for Configuration Manager 2012 R2 . I have not listed all the PKI certificates required for SCCM, you can find the complete list of certificates [here](#).

Certificate Requirement	Certificate Description
Web server certificate for site systems that run IIS	This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run IIS and that are configured in Configuration Manager to use HTTPS.
Client certificate for Windows computers	This certificate is used to authenticate Configuration Manager client computers to site systems that are configured to use HTTPS. It can also be used for management points and state migration points to monitor their operational status when they are configured to use HTTPS. It must be installed externally from Configuration Manager on computers.
Client certificate for distribution points	The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the Enable PXE support for clients distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system.

Certificate Requirement	Certificate Description
Client certificate for Mac computers	This certificate is used to authenticate Configuration Manager Mac computers to management points and distribution points that are configured to support HTTPS. You can request and install this certificate from a Mac computer when you use Configuration Manager enrollment and select the configured certificate template as a mobile device client setting.

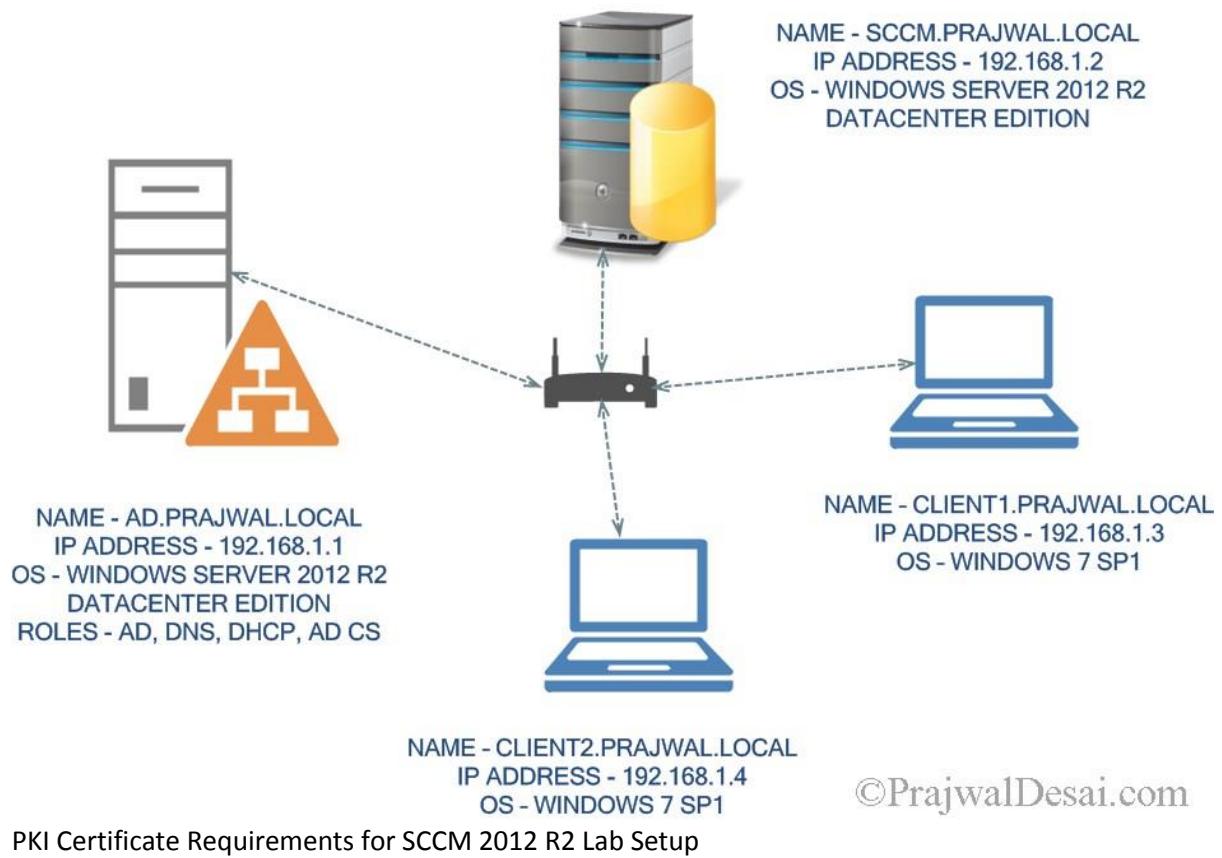
A typical PKI consists of the following elements.

Element	Description
Certification Authority	Acts as the root of trust in a public key infrastructure and provides services that authenticate the identity of individuals, computers, and other entities in a network.
Registration Authority	Is certified by a root CA to issue certificates for specific uses permitted by the root. In a Microsoft PKI, a registration authority (RA) is usually called a subordinate CA.
Certificate Database	Saves certificate requests and issued and revoked certificates and certificate requests on the CA or RA.
Certificate Store	Saves issued certificates and pending or rejected certificate requests on the local computer.
Key Archival Server	Saves encrypted private keys in the certificate database for recovery after loss.

Lab Setup

In my current lab setup, I have got a machine that is running Windows Server 2012 R2 Datacenter edition OS. It is a domain controller (AD.PRAJWAL.LOCAL) that is also configured as DNS, DHCP and AD CS (Active Directory Certificate Services). On the second machine, I have installed Windows Server 2012 R2 Datacenter edition OS. This machine is running System Center 2012 R2 Configuration Manager and SQL server. You can have few client machines for testing the PKI deployment. The procedures use an enterprise certification authority (CA) and certificate templates. The steps are appropriate for a test network only, as a proof of concept. Because there is no single method of deployment for the required certificates, you must consult your particular PKI deployment documentation for the required procedures and best practices to deploy the required certificates for a production environment.

You can log in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.



©PrajwalDesai.com

PKI Certificate Requirements for SCCM 2012 R2 Lab Setup

[Deploying Web Server Certificate for Site Systems that Run IIS](#)

In this post we will see the steps for deploying web server certificate for site systems that run IIS. This is one of the posts out of [Deploy PKI Certificates for SCCM 2012 R2 Step by Step Guide](#). In my previous post we saw the [PKI Certificate Requirements for SCCM 2012 R2](#) and understood much about PKI, the certificates required for SCCM if you are using PKI etc. The next step is to deploy web server certificate for the site systems. You can log in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.

Deploying Web Server Certificate for Site Systems that Run IIS

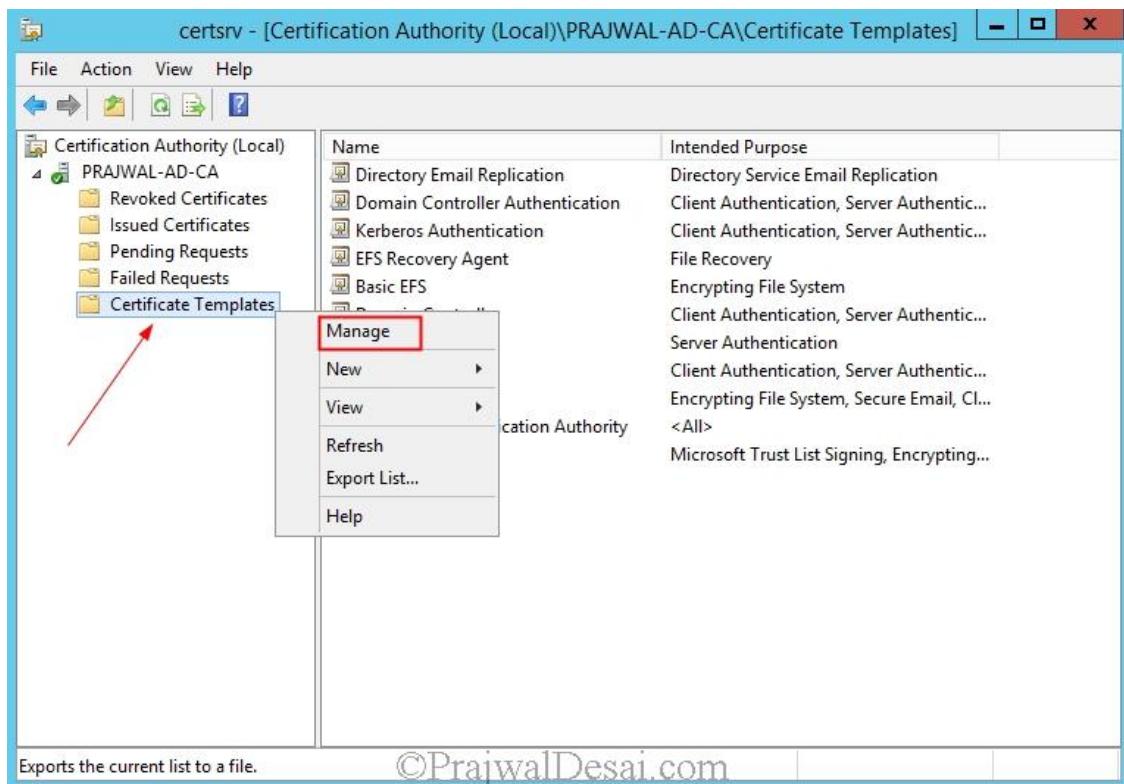
Basically in this post we will be performing the following steps

- 1) Creating and Issuing the Web Server Certificate Template on the Certification Authority
- 2) Requesting the Web Server Certificate
- 3) Configuring IIS to Use the Web Server Certificate

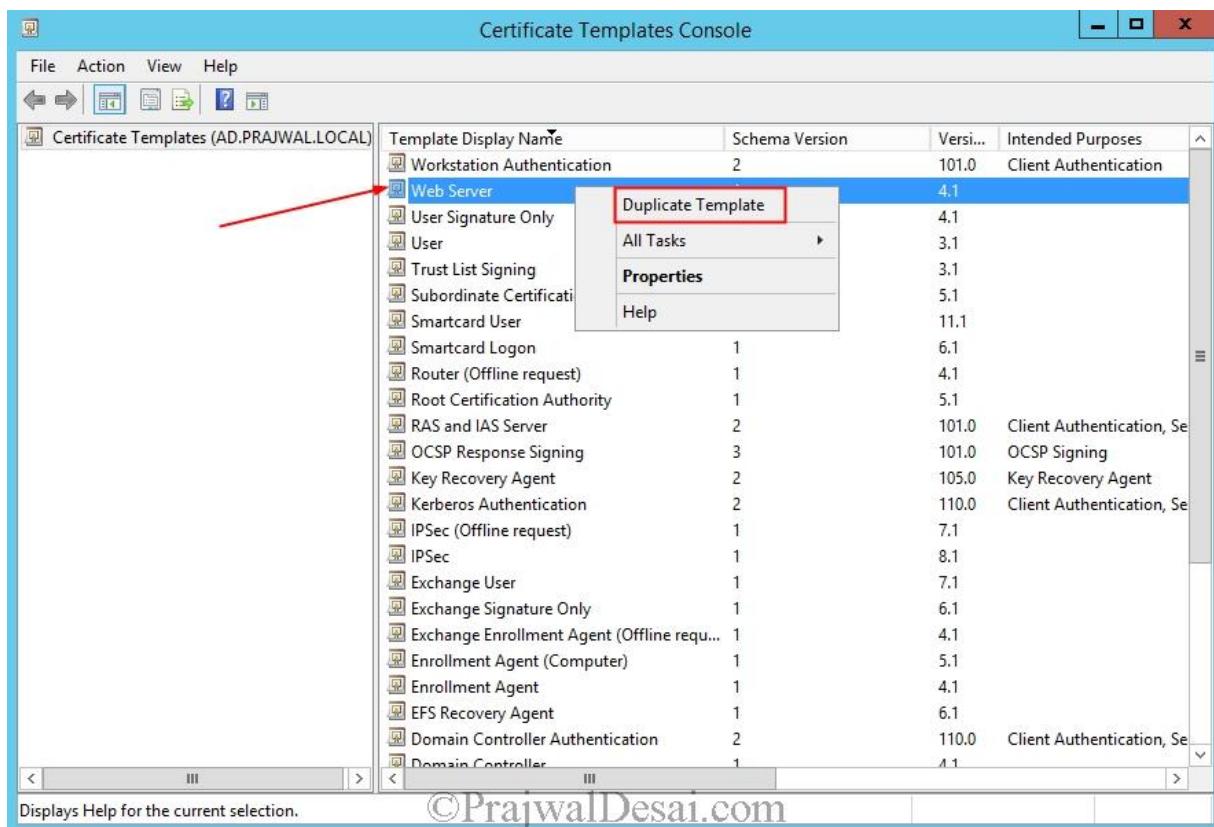
This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run IIS and that are configured in Configuration Manager to use HTTPS.

Creating and Issuing the Web Server Certificate Template on the Certification Authority

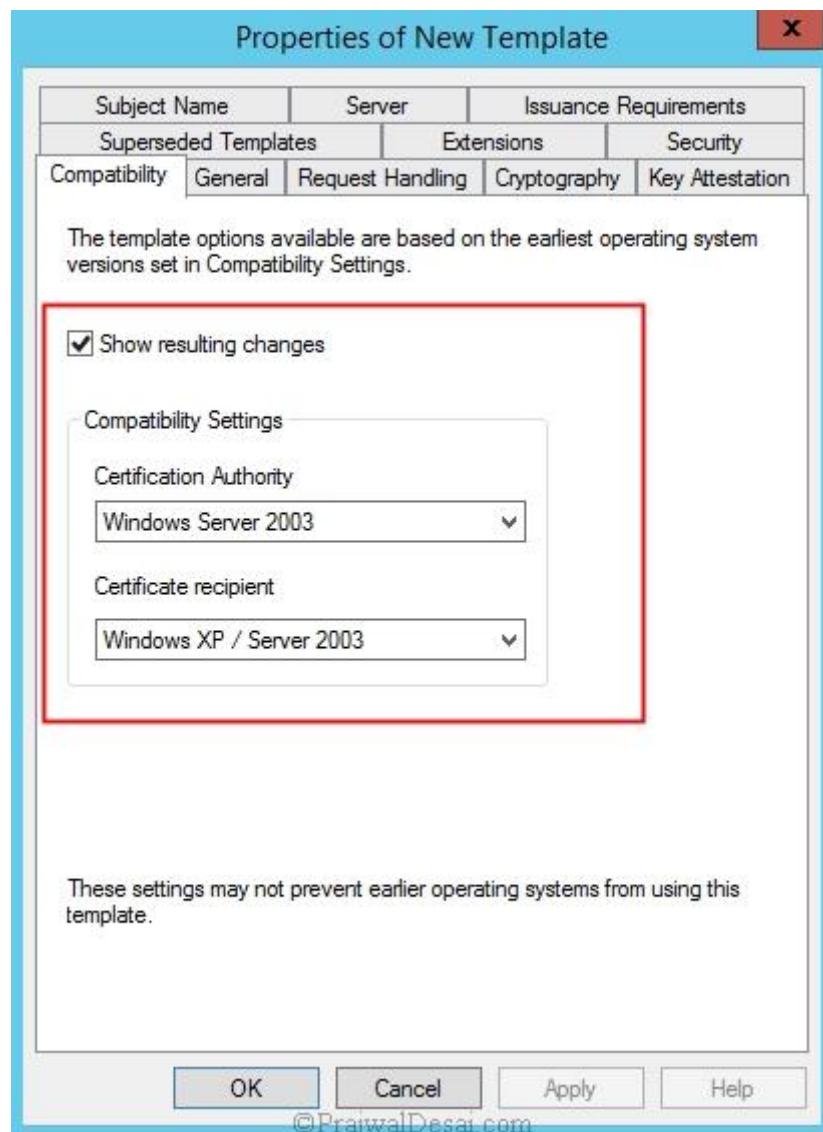
Create a security group named **SCCM IIS Servers** that contains the member servers to install System Center 2012 Configuration Manager site systems that will run IIS. On the member server that has Certificate Services installed, in the **Certification Authority** console, right-click **Certificate Templates** and click **Manage** to load the **Certificate Templates** console.



In the results pane, right-click the entry that displays **Web Server** in the column **Template Display Name**, and then click **Duplicate Template**.



In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server** is selected, and then click **OK**.



In the **Properties of New Template** dialog box, on the **General** tab, enter a template name to generate the web certificates that will be used on Configuration Manager site systems. Click the **Subject Name** tab, and make sure that **Supply in the request** is selected.

Properties of New Template

X

Subject Name	Server	Issuance Requirements		
Superseded Templates	Extensions	Security		
Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

SCCM Web Server Certificate

Template name:

SCCMWebServerCertificate

Validity period:

2 years ▾

Renewal period:

6 weeks ▾

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

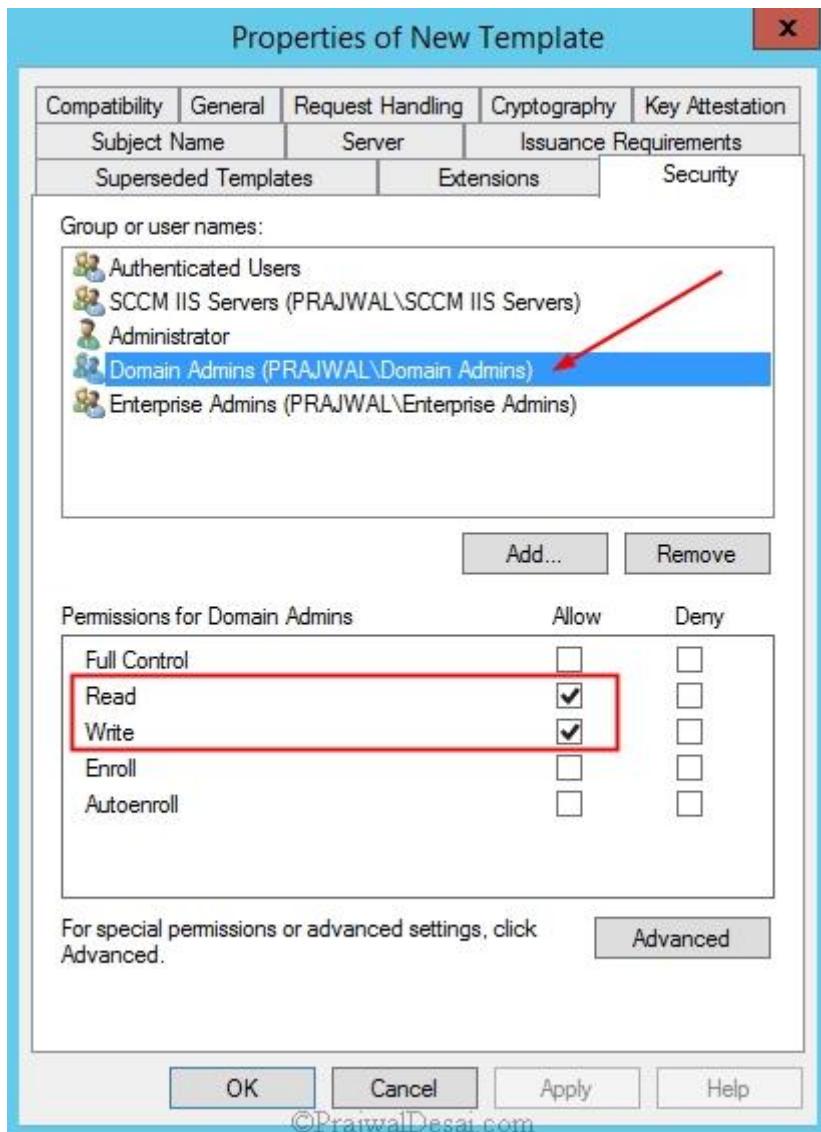
OK

Cancel

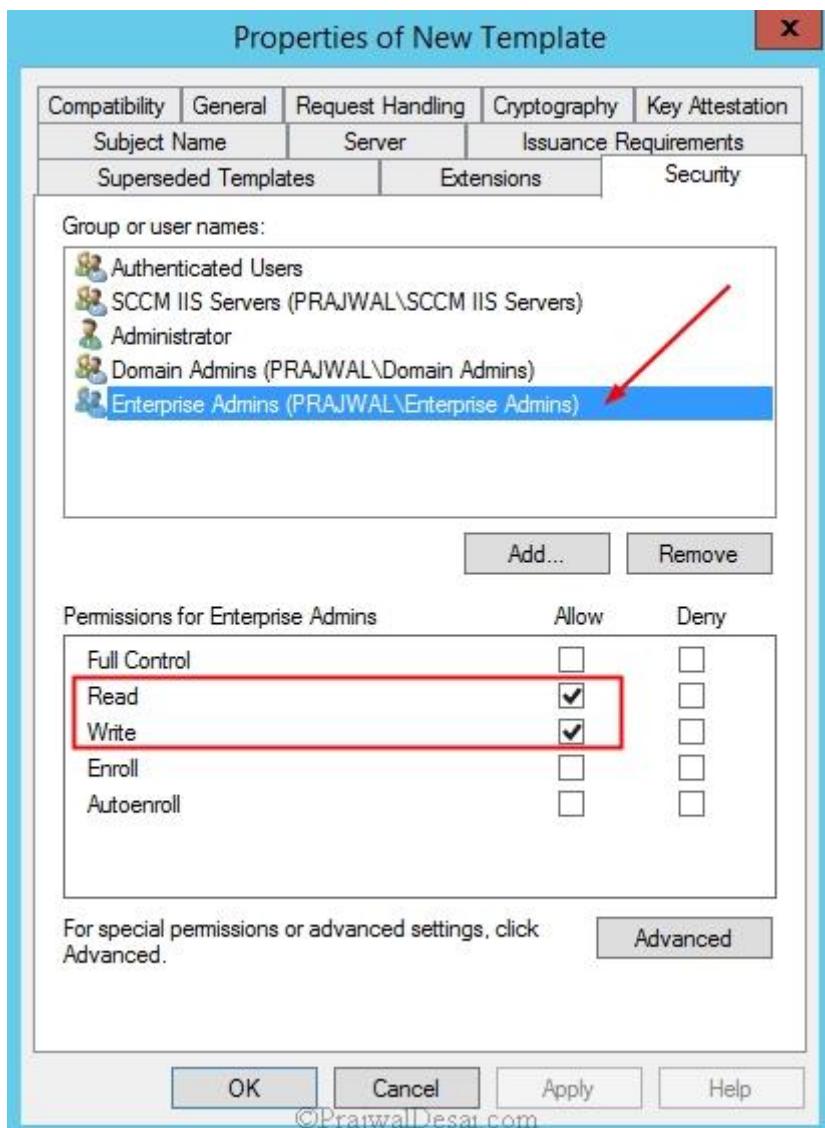
Apply

Help

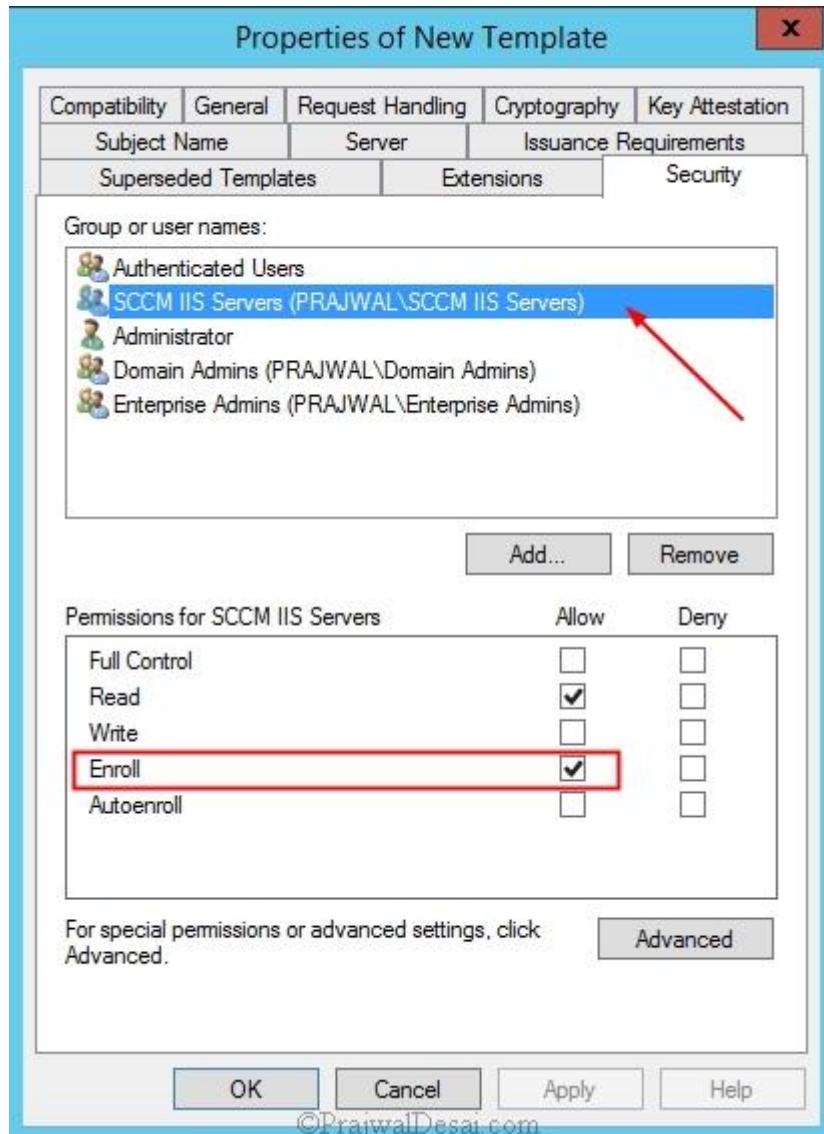
Click the **Security** tab, and remove the **Enroll** permission from the security groups **Domain Admins**.



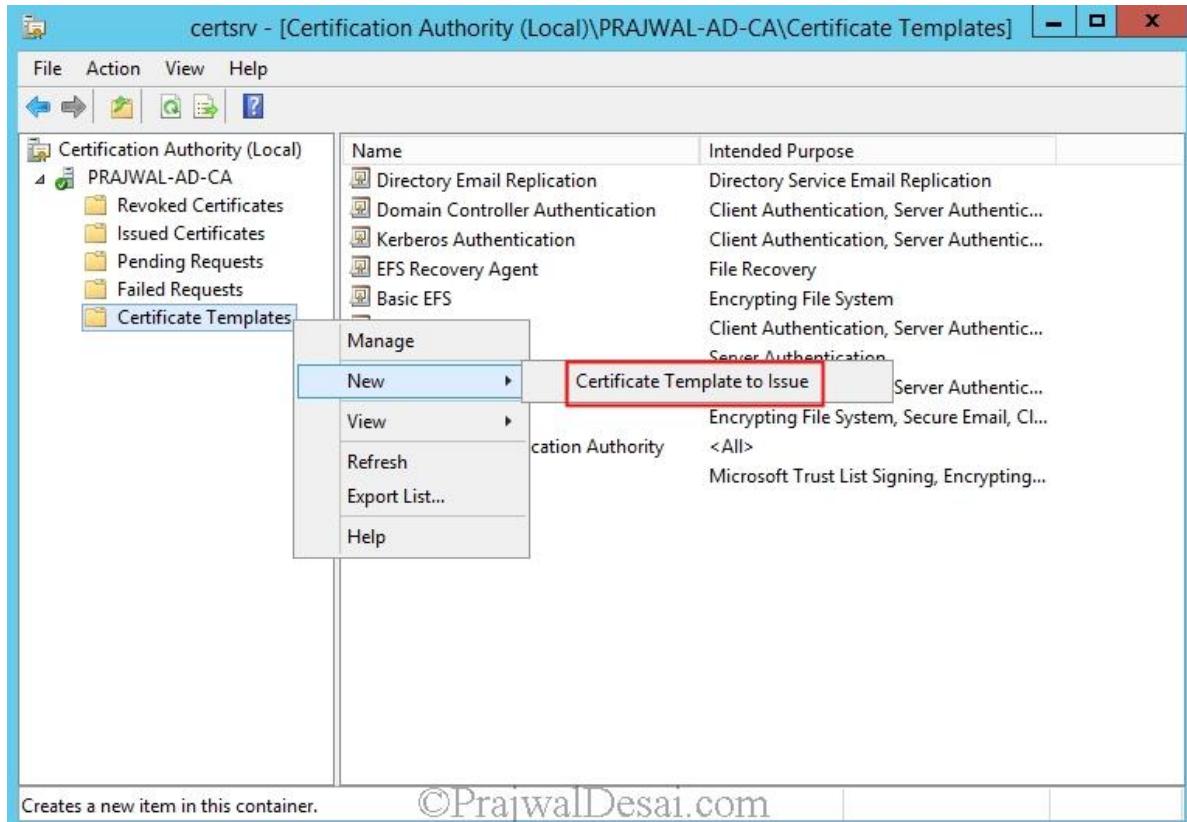
Also remove the **Enroll** permission from the security groups **Enterprise Admins**.



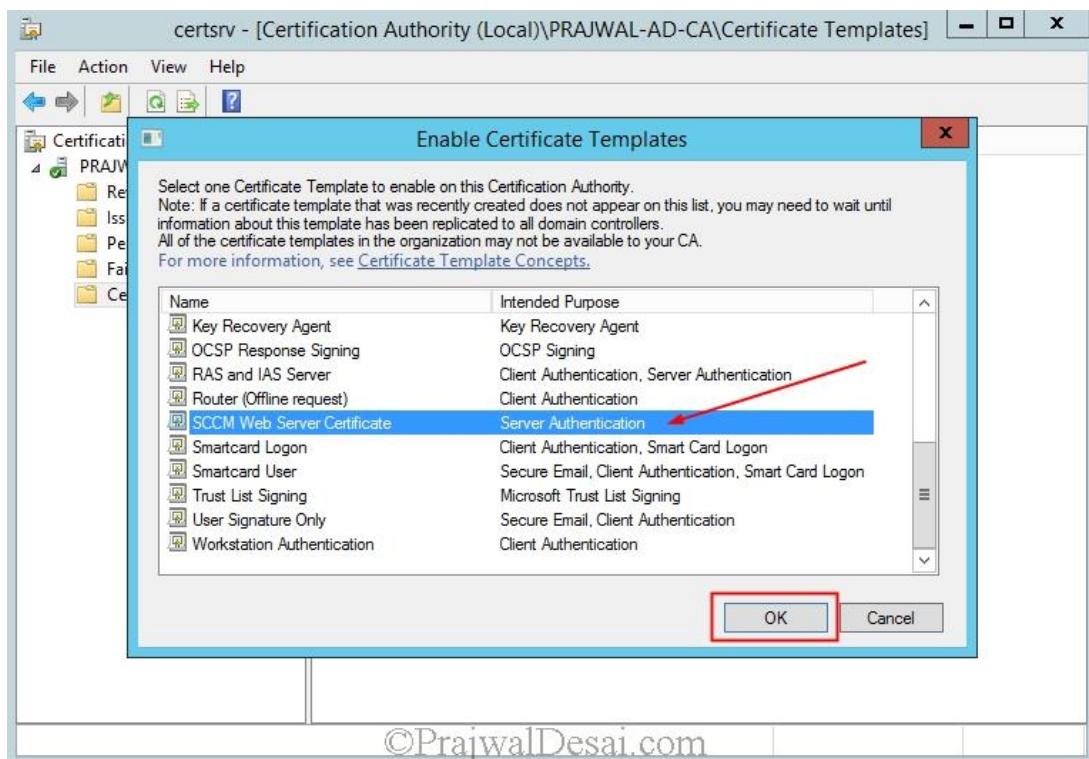
Click **Add**, enter **SCCM IIS Servers** in the text box, and then click **OK**. Select the **Enroll** permission for this group, and do not clear the **Read** permission. Click **OK**, and close the **Certificate Templates Console**.



In the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**.



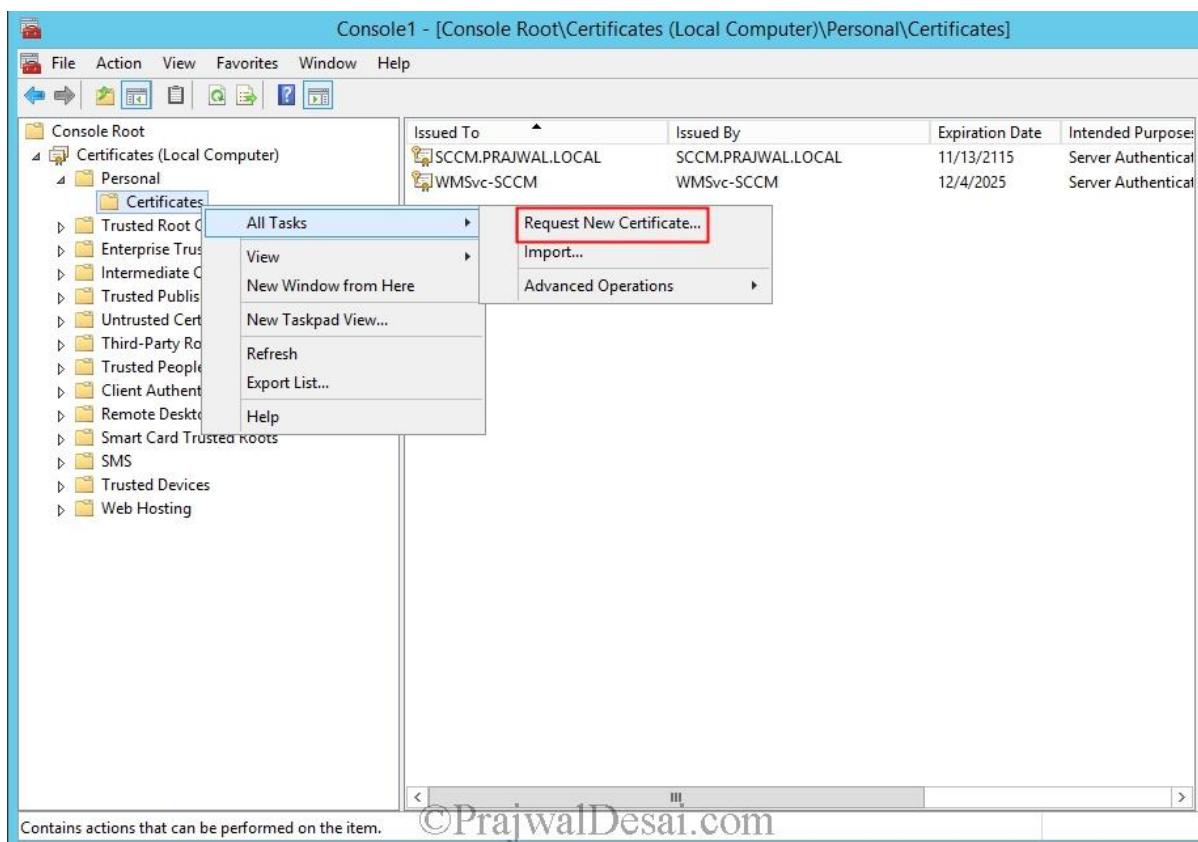
In the **Enable Certificate Templates** dialog box, select the new template that you have just created, **SCCM Web Server Certificate**, and then click **OK**.



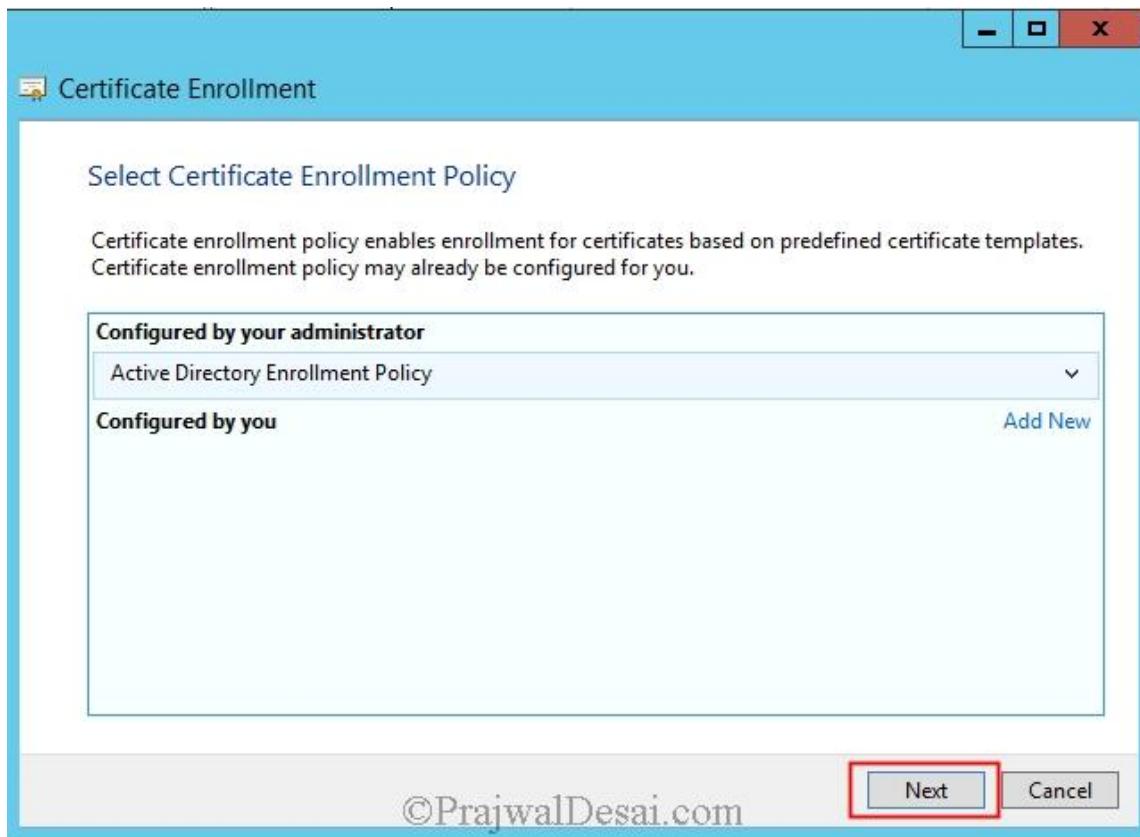
Requesting the Web Server Certificate

The steps that we perform now will install the web server certificate on to the member server that runs IIS. Microsoft recommends you to restart the member server that runs IIS. This is just to ensure that the computer can access the certificate template that you created.

Run the mmc.exe command. In the empty console, click **File**, and then click **Add/Remove Snap-in**. In the Add or Remove Snap-ins dialog box, select **Certificates** from the list of Available snap-ins, and then click **Add**. In the Certificate snap-in dialog box, select **Computer account**, and then click **Next**. In the Select Computer dialog box, ensure **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. In the Add or Remove Snap-ins dialog box, click **OK**. In the console, expand **Certificates (Local Computer)**, and then click **Personal**. Right-click **Certificates**, click **All Tasks**, and then click **Request New Certificate**.

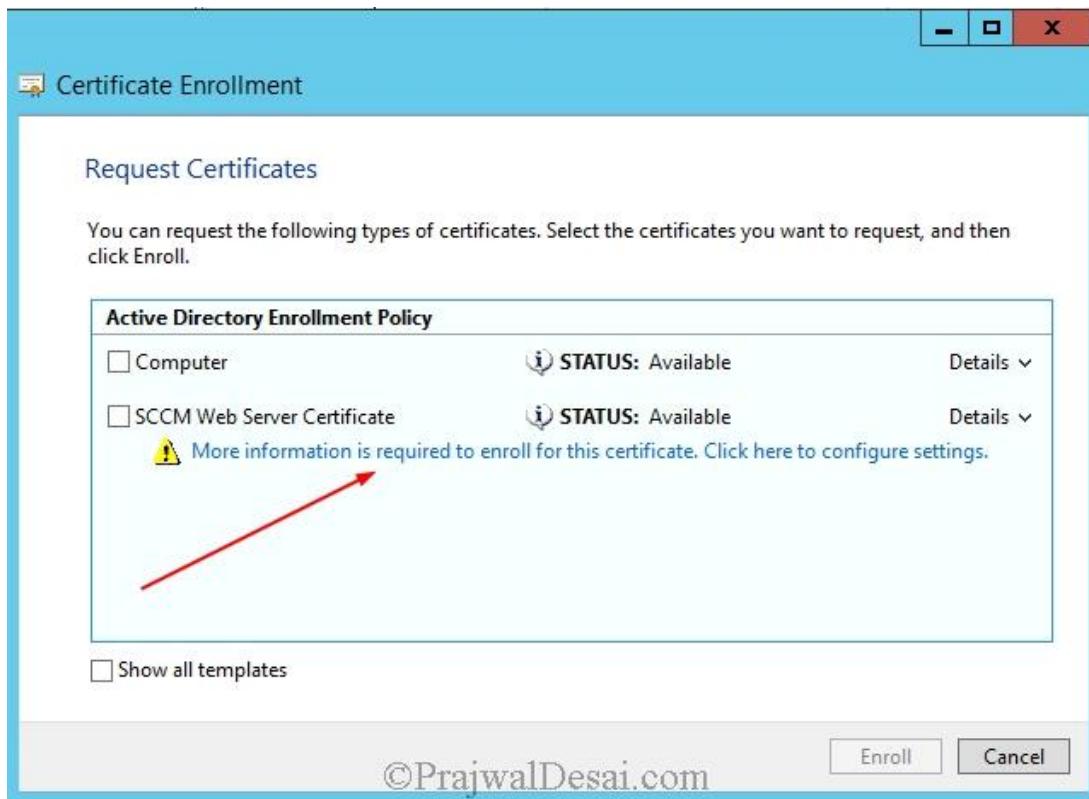


On Select Certificate Enrollment Policy page, click Next.



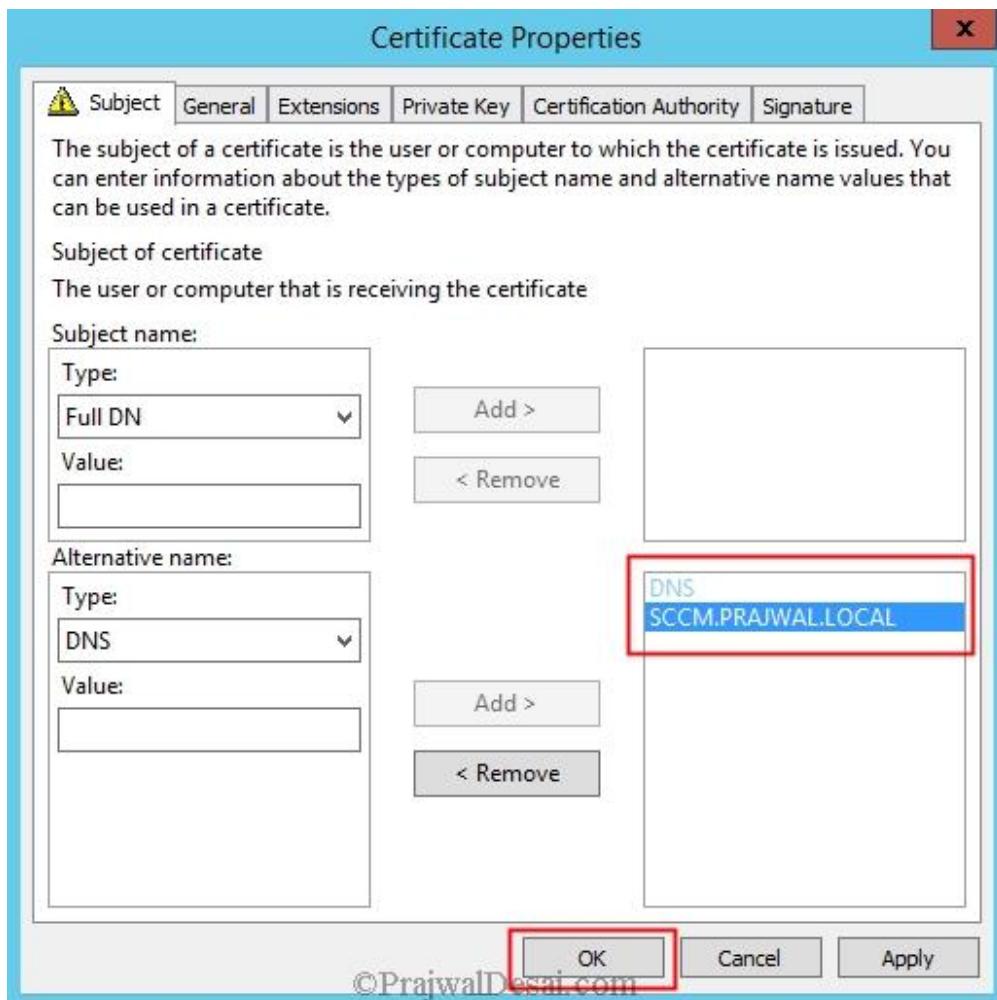
On the **Request Certificates** page, identify the **SCCM Web Server Certificate** from the list of displayed certificates, and then click **More information is required to enroll for this certificate**.

Click here to configure settings.

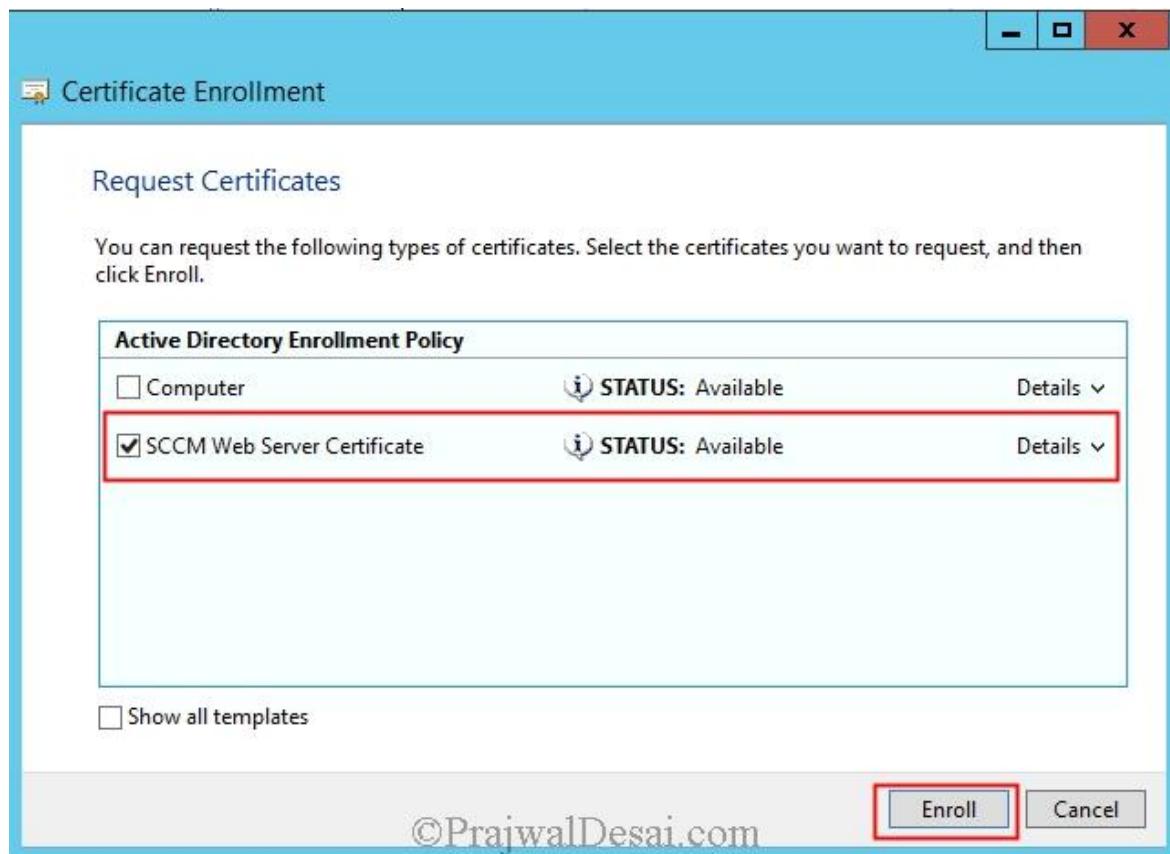


In the **Certificate Properties** dialog box, in the **Subject** tab, do not make any changes to the **Subject name**. This means that the **Value** box for the **Subject name** section remains blank. Instead, from the **Alternative name** section, click the **Type** drop-down list, and then select **DNS**.

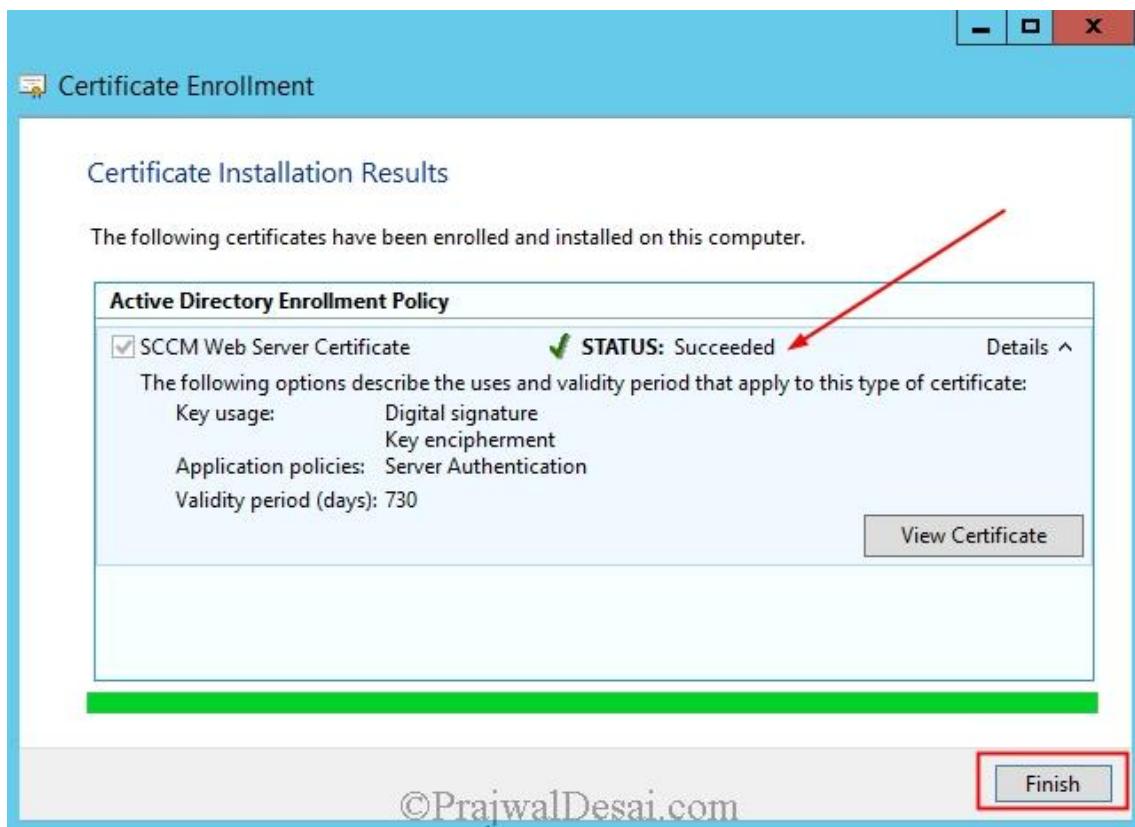
In the **Value** box, specify the FQDN values that you will specify in the Configuration Manager site system properties, and then click **OK** to close the **Certificate Properties** dialog box.



On the **Request Certificates** page, select **SCCM Web Server Certificate** from the list of displayed certificates, and then click **Enroll**.

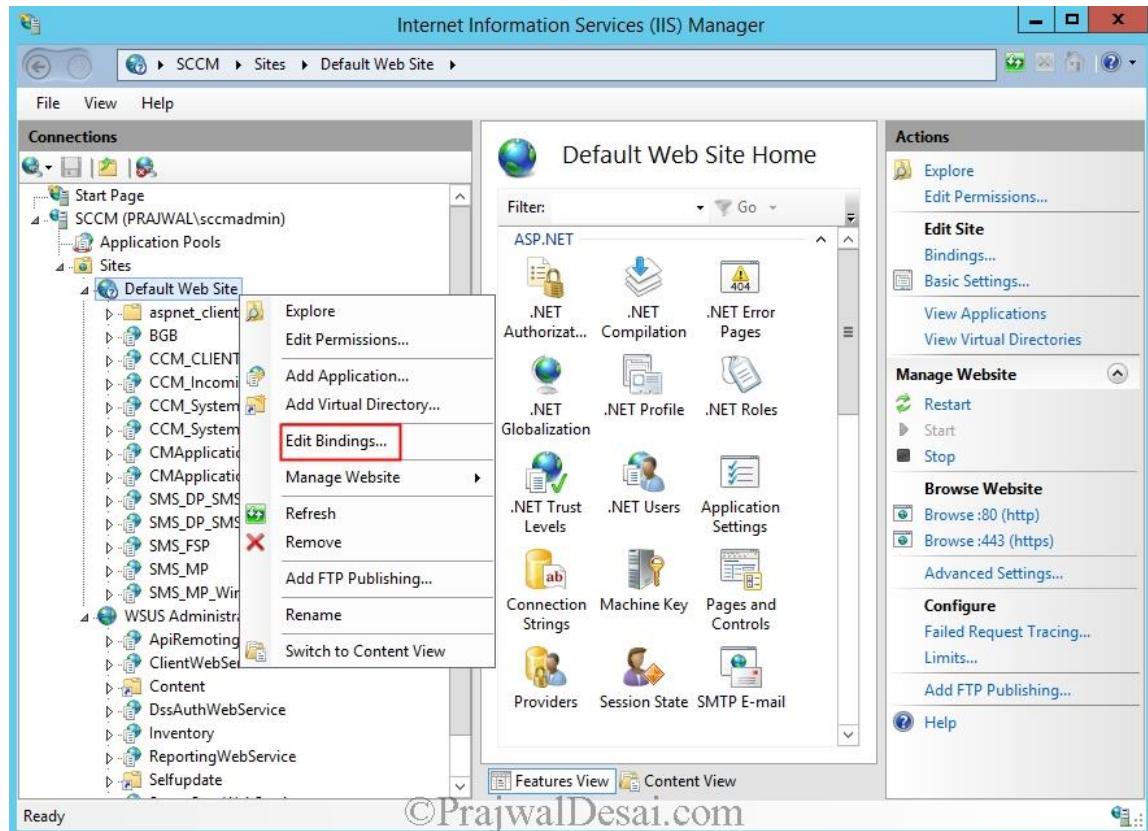


On the **Certificates Installation Results** page, wait until the certificate is installed (the status should show **Succeeded**), and then click **Finish**.



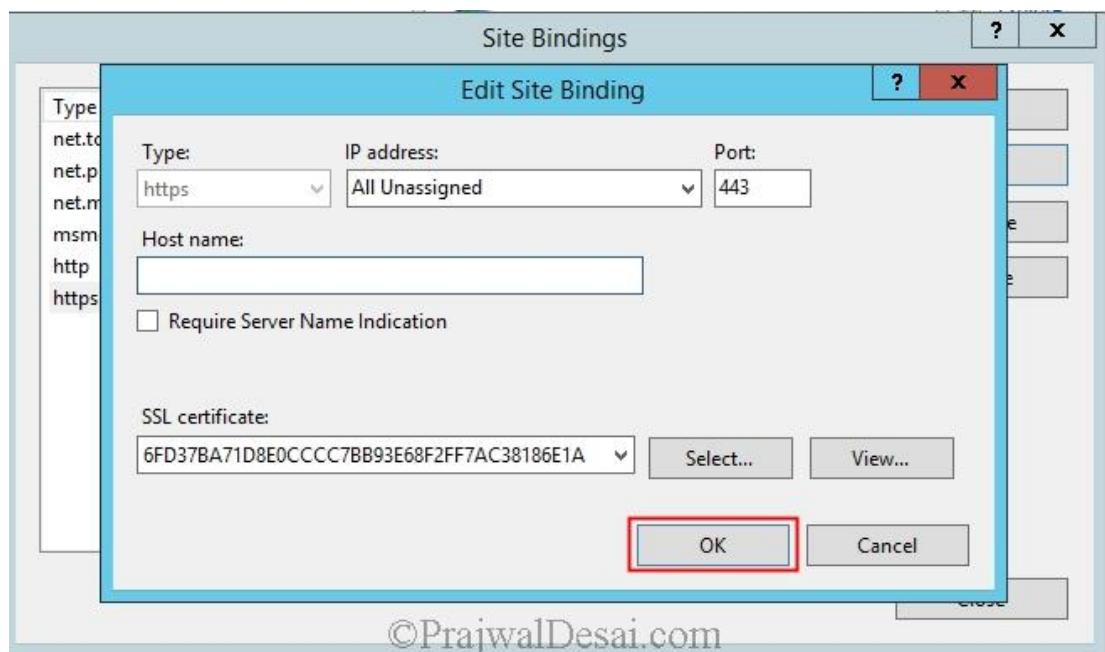
Configuring IIS to Use the Web Server Certificate

The steps that we perform now will configure IIS to use the web server certificate that we had configured in the above steps. On the member server that has IIS installed, launch the Internet Information Services (IIS) Manager. Expand **Sites**, right-click **Default Web Site**, and then select **Edit Bindings...**.



In the **Edit Site Binding** dialog box, select the certificate that you requested by using the SCCM Web Server Certificates template, and then click **OK**.

You have now configured IIS to use the web server certificate.



©PrajwalDesai.com

Deploying the Client Certificate for Windows Computers

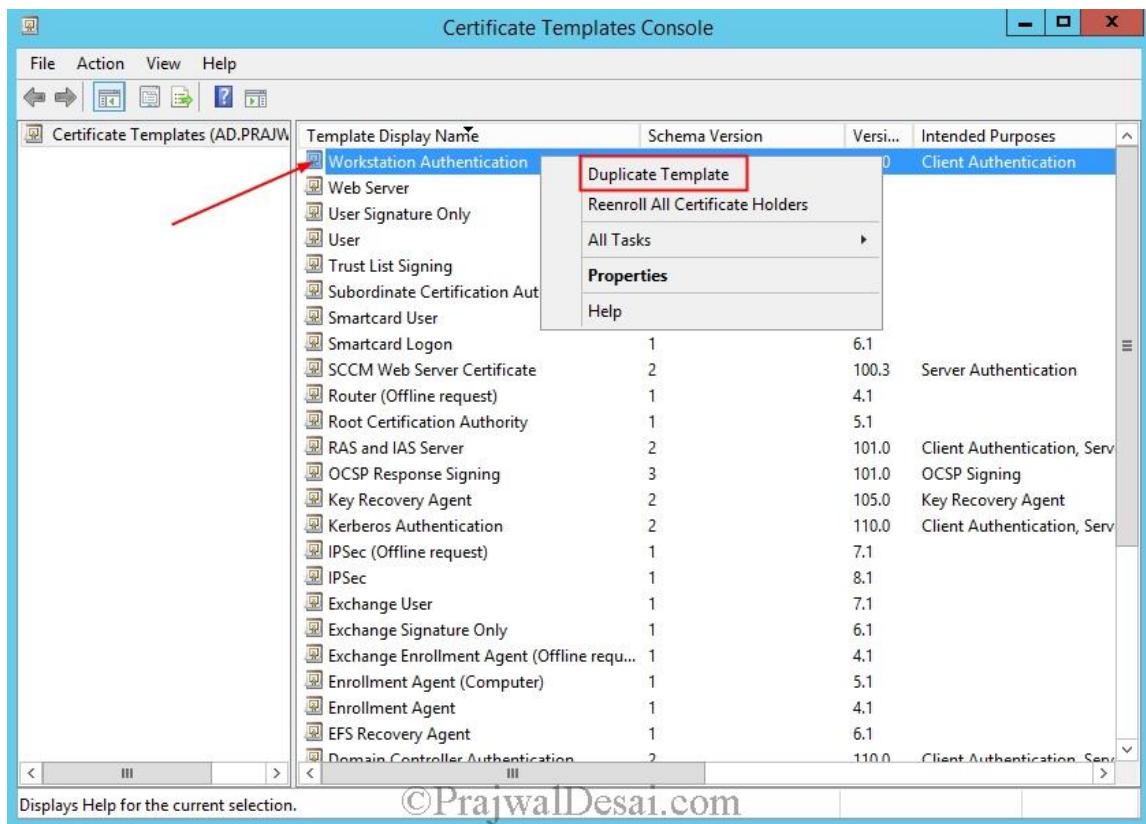
In this post we will see the steps for deploying the client certificate for windows computers. This post is a part of [Deploy PKI Certificates for SCCM 2012 R2 Step by Step Guide](#). In the previous post we saw the [PKI certificate requirements for SCCM 2012 R2](#), [how to deploy web server certificate for site systems that run IIS](#). The next step is to deploy the client certificate for windows computers. You can log in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.

This [certificate deployment](#) for windows computers has the following procedures:

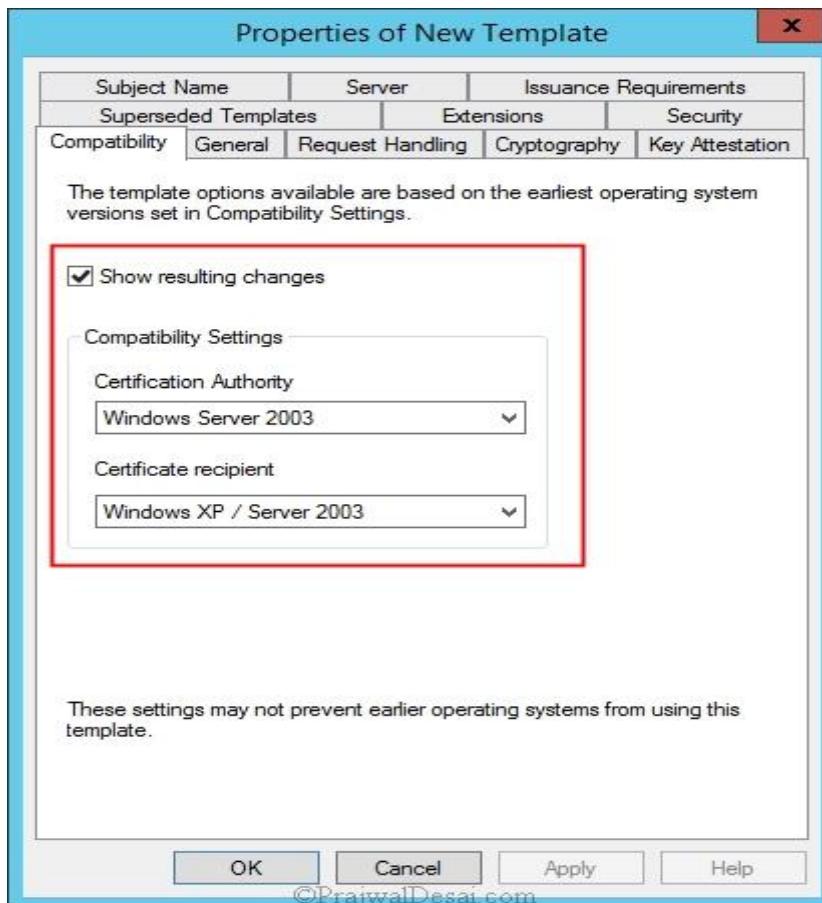
- 1) Creating and Issuing the Workstation Authentication Certificate Template on the Certification Authority
- 2) Configuring Auto enrollment of the Workstation Authentication Template by Using Group Policy
- 3) Automatically Enrolling the Workstation Authentication Certificate and Verifying Its Installation on Computers

Creating and Issuing the Workstation Authentication Certificate Template on the Certification Authority

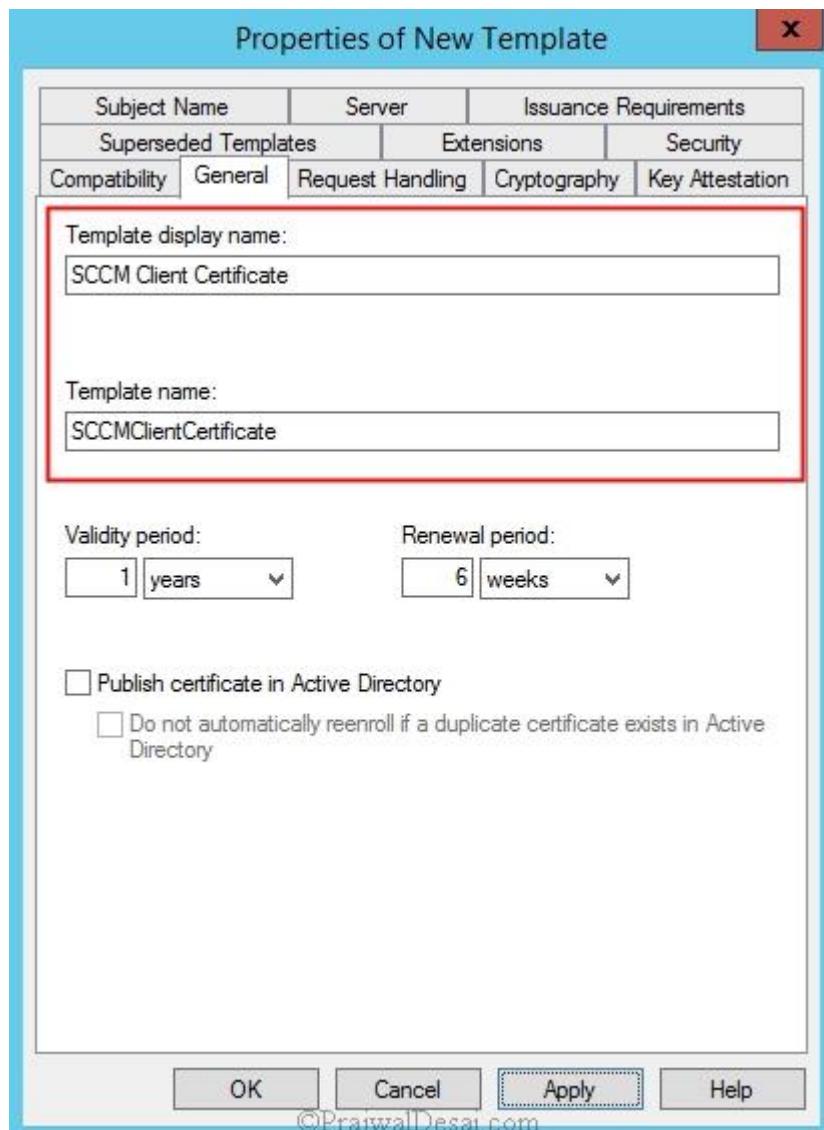
On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then click **Manage** to load the Certificate Templates management console. In the results pane, right-click the entry that displays **Workstation Authentication** in the column Template Display Name, and then click **Duplicate Template**.



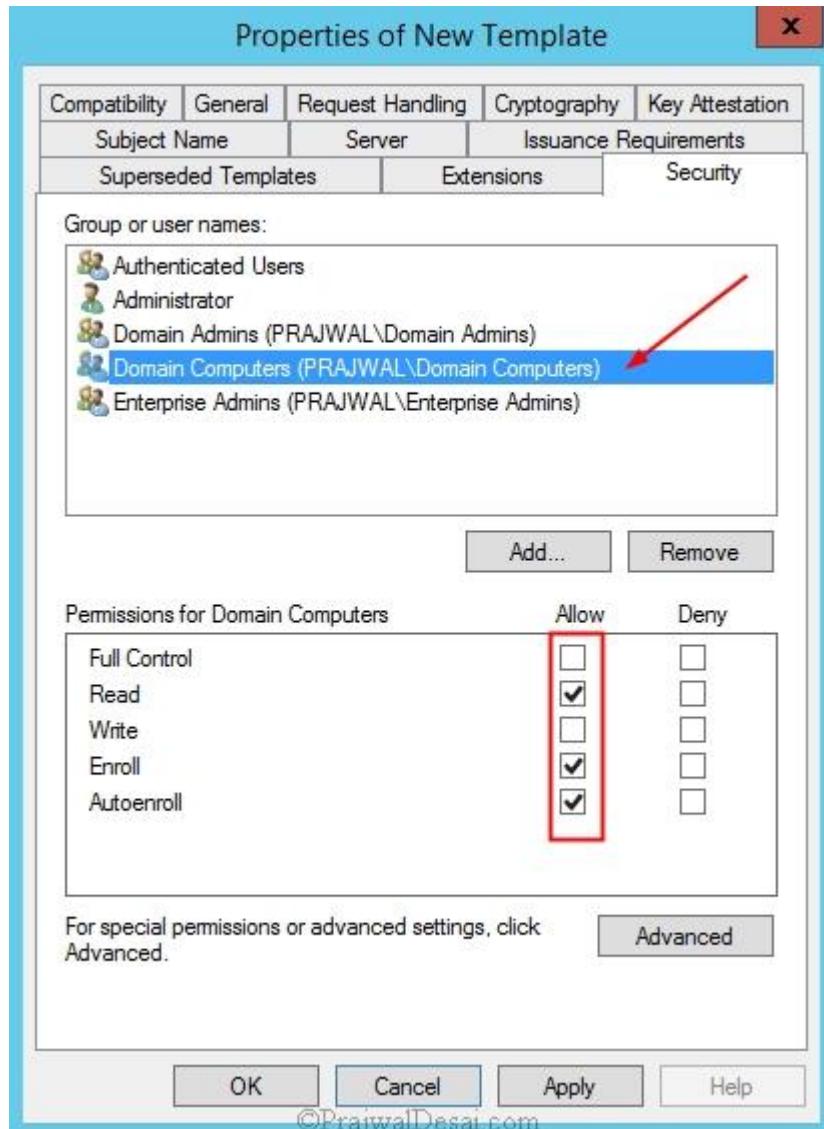
In the **Duplicate Template** dialog box, ensure that **Windows Server 2003** is selected.



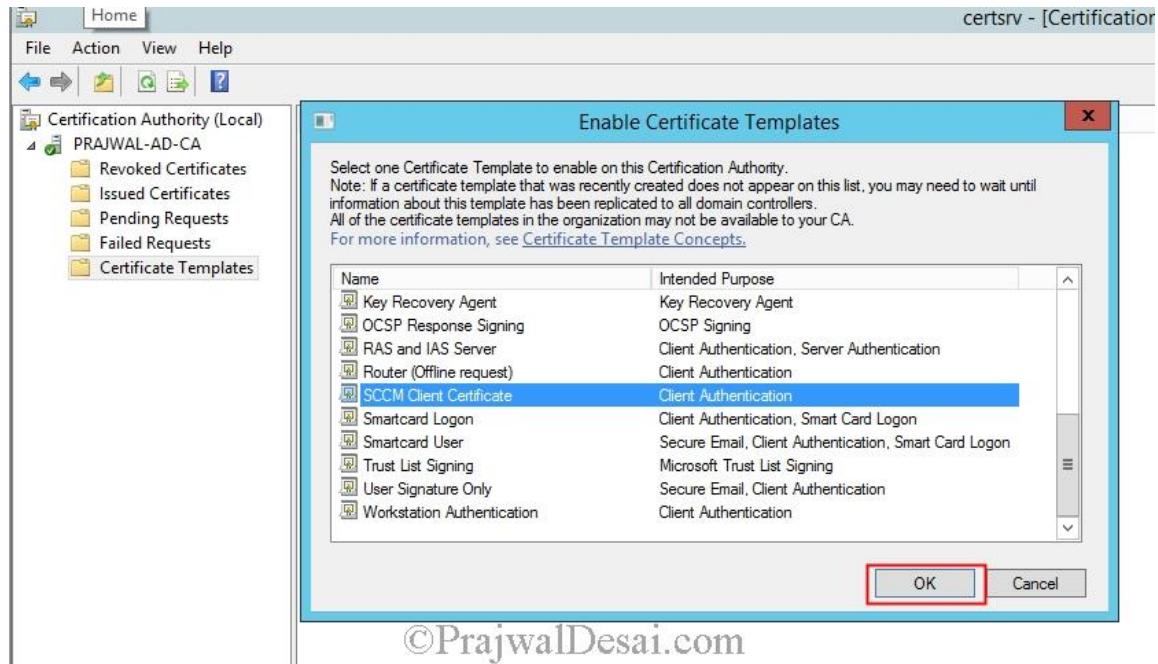
In the **Properties of New Template** dialog box, on the **General** tab, enter a template name to generate the client certificates that will be used on Configuration Manager client computers, such as **SCCM Client Certificate**.



Click the **Security** tab, select the **Domain Computers** group, and select the additional permissions of **Read** and **Autoenroll**. Do not clear **Enroll**. Click **OK** and close **Certificate Templates Console**.

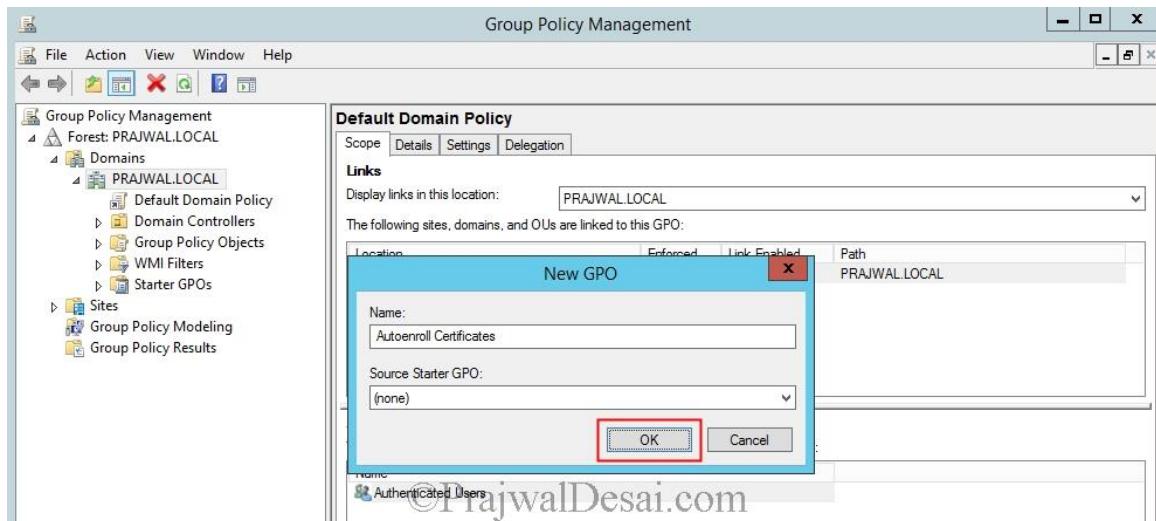


In the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**. In the **Enable Certificate Templates** dialog box, select the new template that you have just created, **SCCM Client Certificate**, and then click **OK**. Close **Certification Authority**.

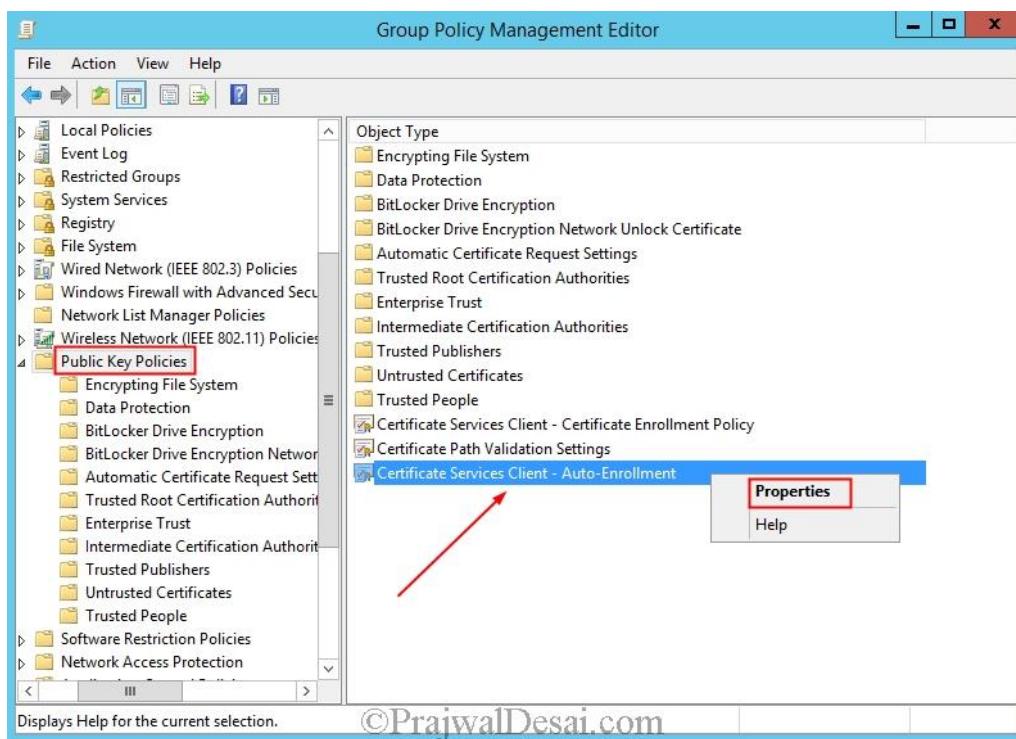


Configuring Auto enrollment of the Workstation Authentication Template by Using Group Policy

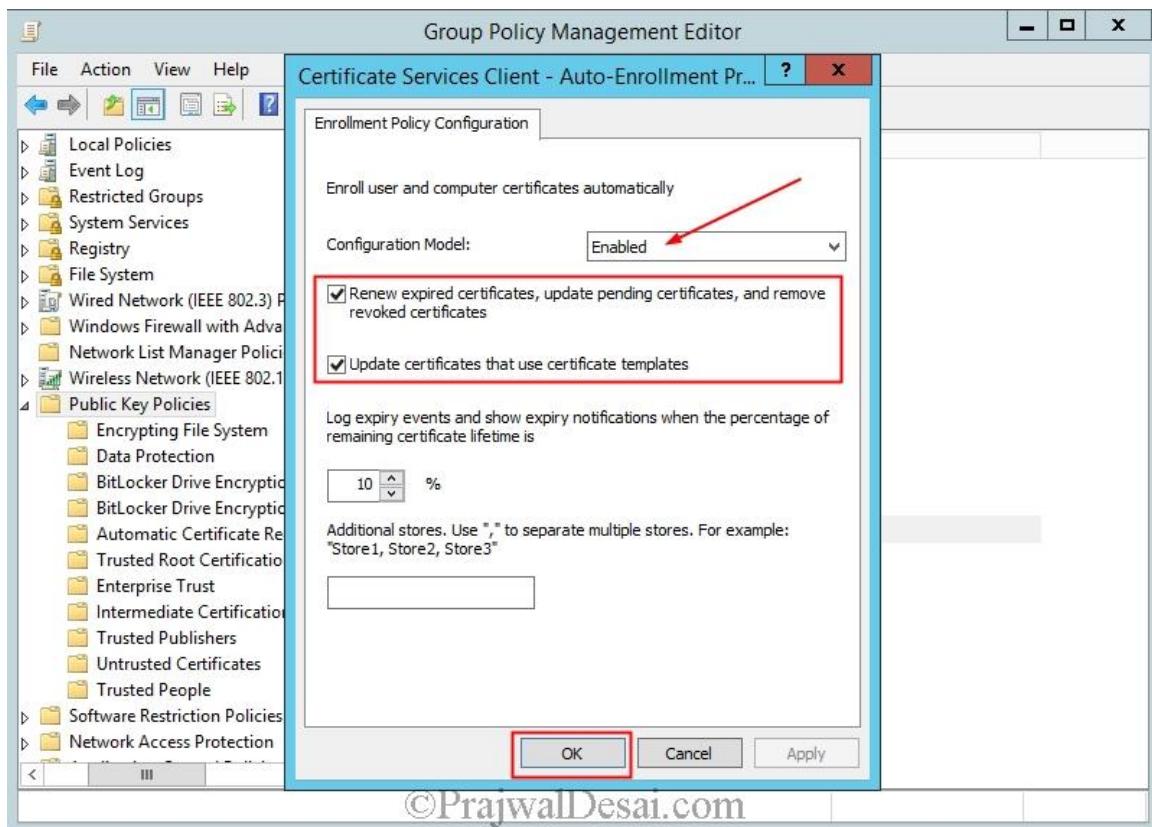
On the domain controller, launch the **Group Policy Management**. Navigate to your domain, right-click the domain, and then select Create a GPO in this domain, and Link it here. In the **New GPO** dialog box, enter a name for the new Group Policy, such as **Autoenroll Certificates**, and click **OK**



In the results pane, on the **Linked Group Policy Objects** tab, right-click the new Group Policy, and then click **Edit**. In the **Group Policy Management Editor**, expand **Policies** under **Computer Configuration**, and then navigate to **Windows Settings > Security Settings > Public Key Policies**. Right-click the object type named **Certificate Services Client – Auto-enrollment**, and then click **Properties**

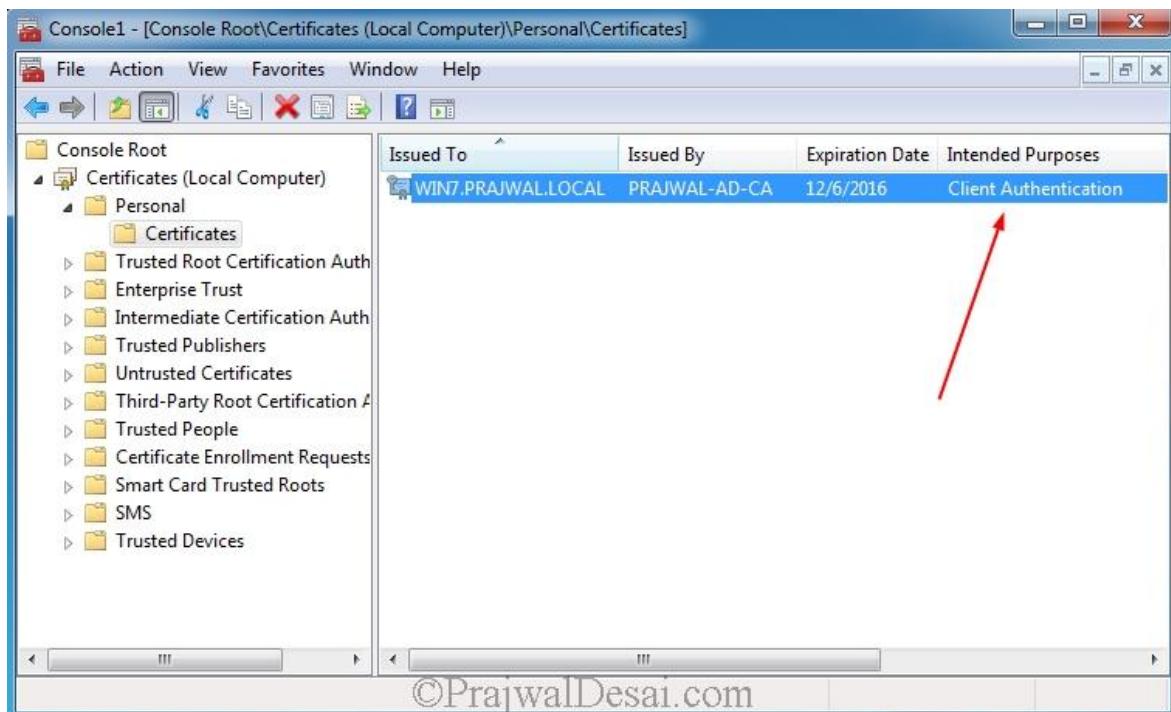


From the **Configuration Model** drop-down list, select **Enabled**, select **Renew expired certificates, update pending certificates, and remove revoked certificates**, select **Update certificates that use certificate templates**, and then click **OK**. Close the GPMC.



Automatically Enrolling the Workstation Authentication Certificate and Verifying Its Installation on Computers

In the above steps we have configured auto enrollment of the workstation authentication template by using group policy. This procedure installs the client certificate on computers and verifies the installation. Restart the workstation computer, and wait a few minutes before logging on. Using the mmc command open the **Certificate snap-in** dialog box, select **Computer account**, and then click **Next**. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. In the console, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**. In the results pane, confirm that a certificate is displayed that has **Client Authentication** displayed in the **Intended Purpose** column, and that **SCCM Client Certificate** is displayed in the **Certificate Template** column. Close the console.



You need to repeat same steps for the member server to verify that the server that will be configured as the management point also has a client certificate. The computer is now provisioned with a Configuration Manager client certificate.

Deploying the Client Certificate for Distribution Points

In this post we will see the steps for deploying the client certificate for distribution points. This is one of the posts of [Deploy PKI Certificates for SCCM 2012 R2 Step by Step Guide](#). In the previous post we understood more about [PKI certificate requirements](#), [deploying web server certificate for site systems that run IIS](#), [deploying client certificates for windows computers](#). The next step is to deploy the client certificate for distribution points.

This certificate serves two purposes. The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the Enable PXE support for clients distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system. You can log in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.

This [certificate deployment](#) has the following procedures:

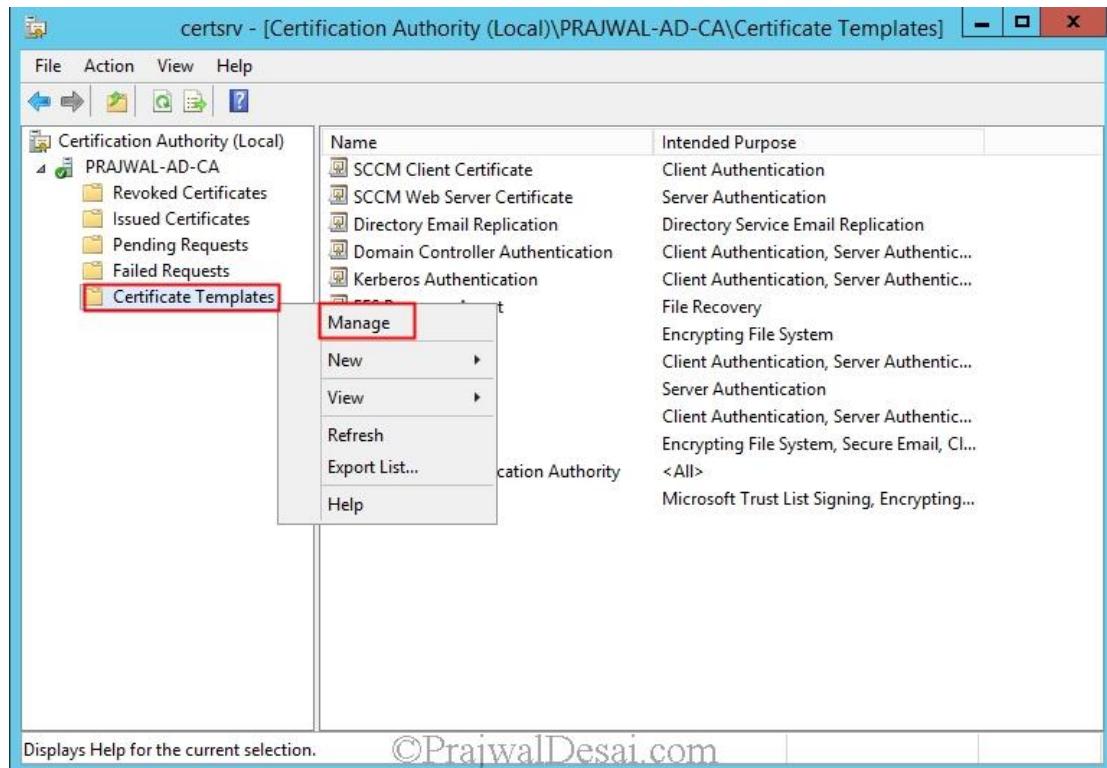
Creating and Issuing a Custom Workstation Authentication Certificate Template on the Certification Authority

Requesting the Custom Workstation Authentication Certificate

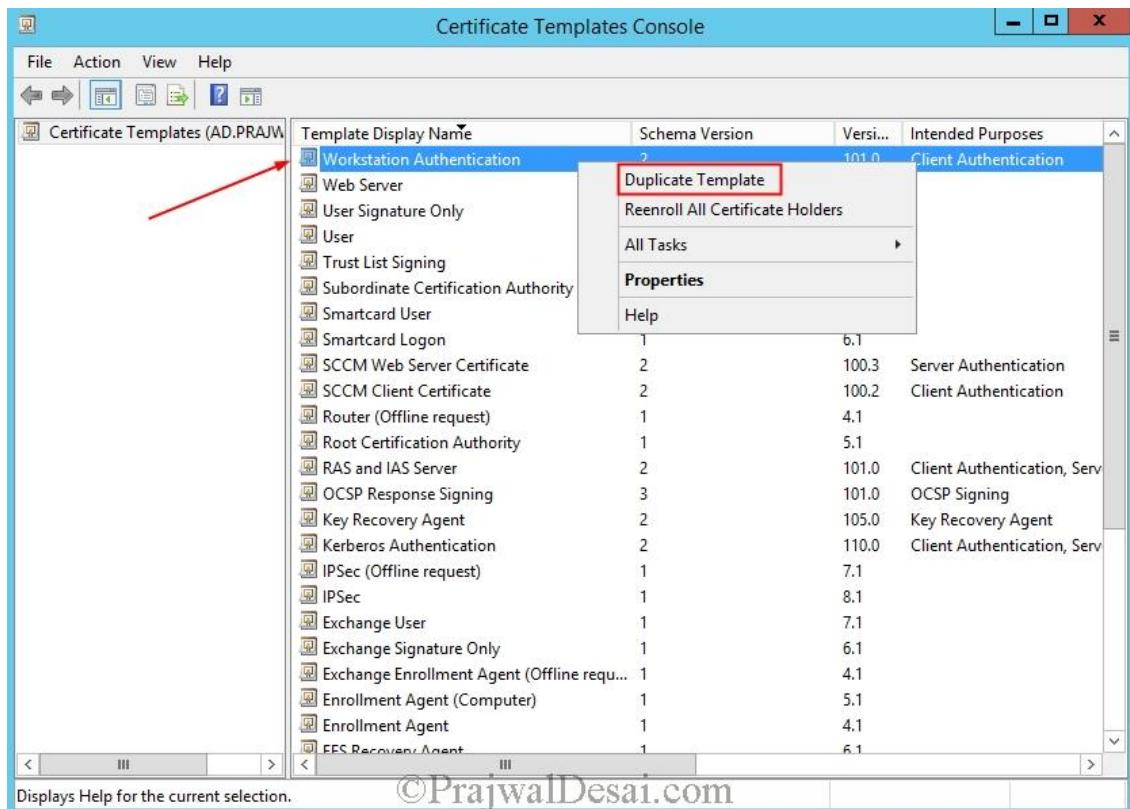
Exporting the Client Certificate for Distribution Points

Creating and Issuing a Custom Workstation Authentication Certificate Template on the Certification Authority

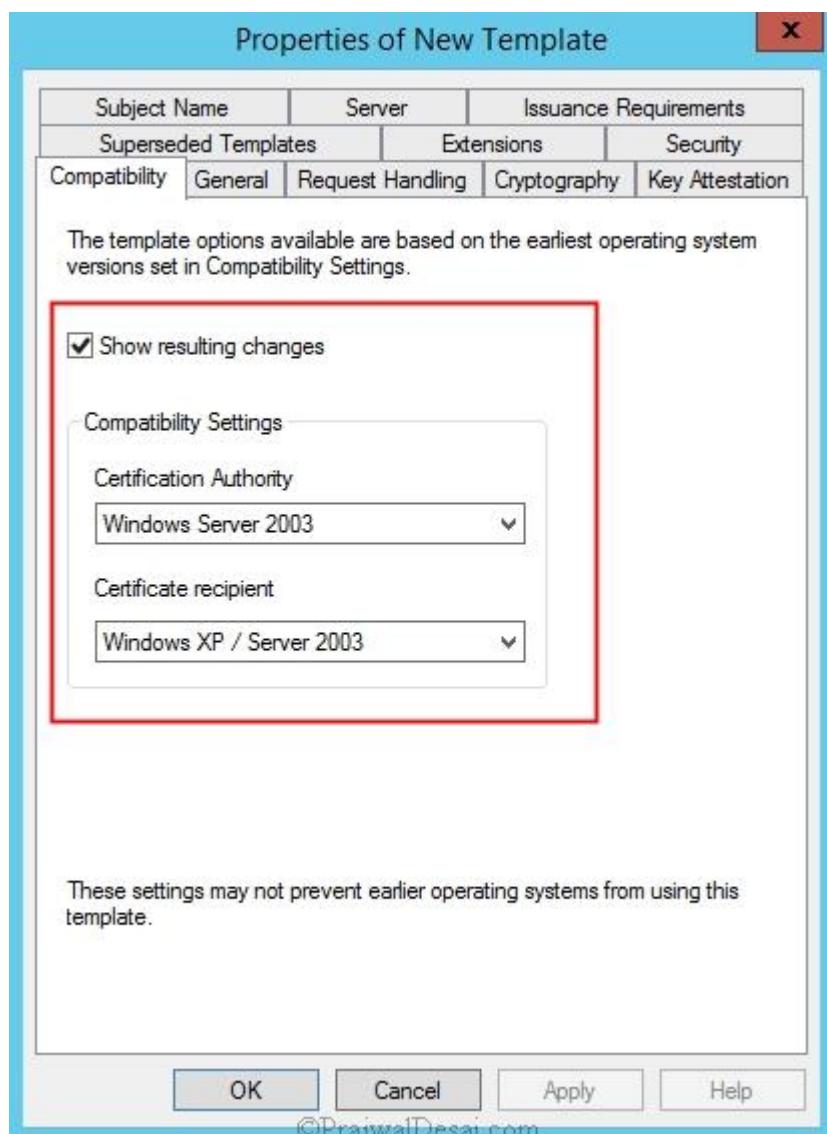
On the member server that is running the Certification Authority console, right-click Certificate Templates, and then click Manage to load the Certificate Templates management console.



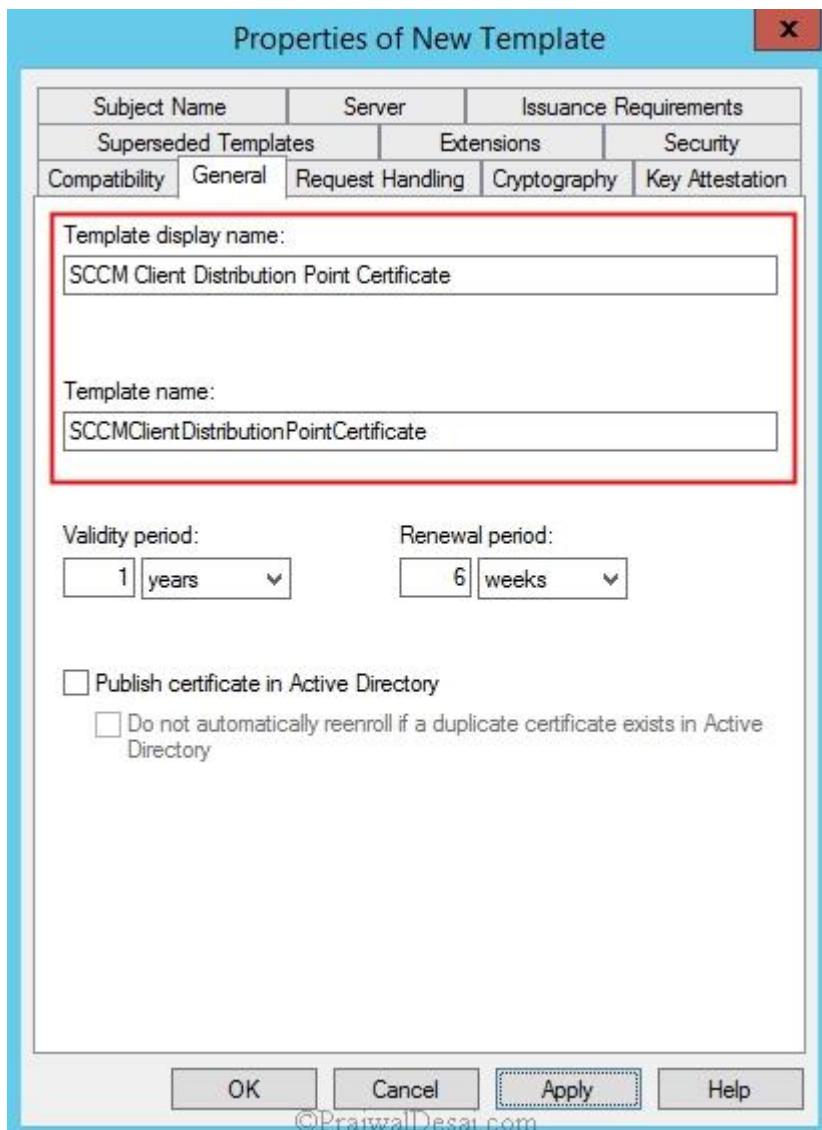
In the results pane, right-click the entry that displays Workstation Authentication in the column Template Display Name, and then click **Duplicate Template**.



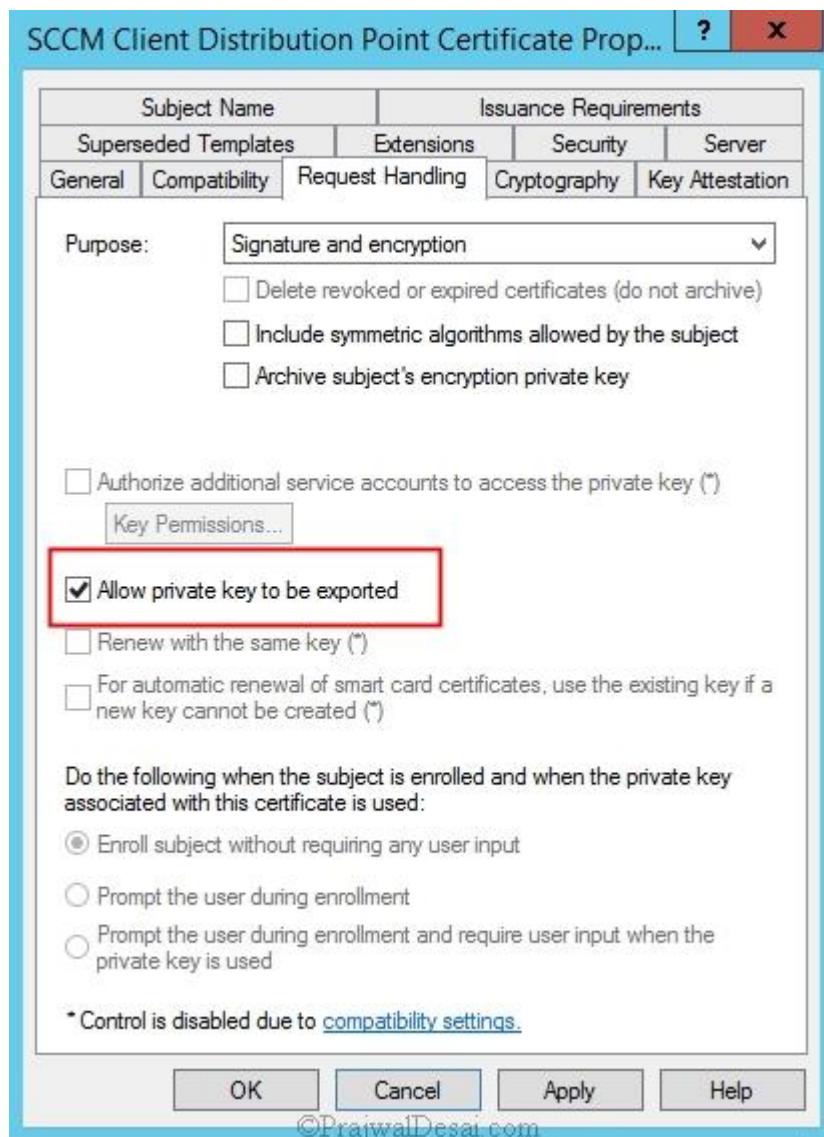
In the Duplicate Template dialog box, ensure that Windows 2003 Server is selected.



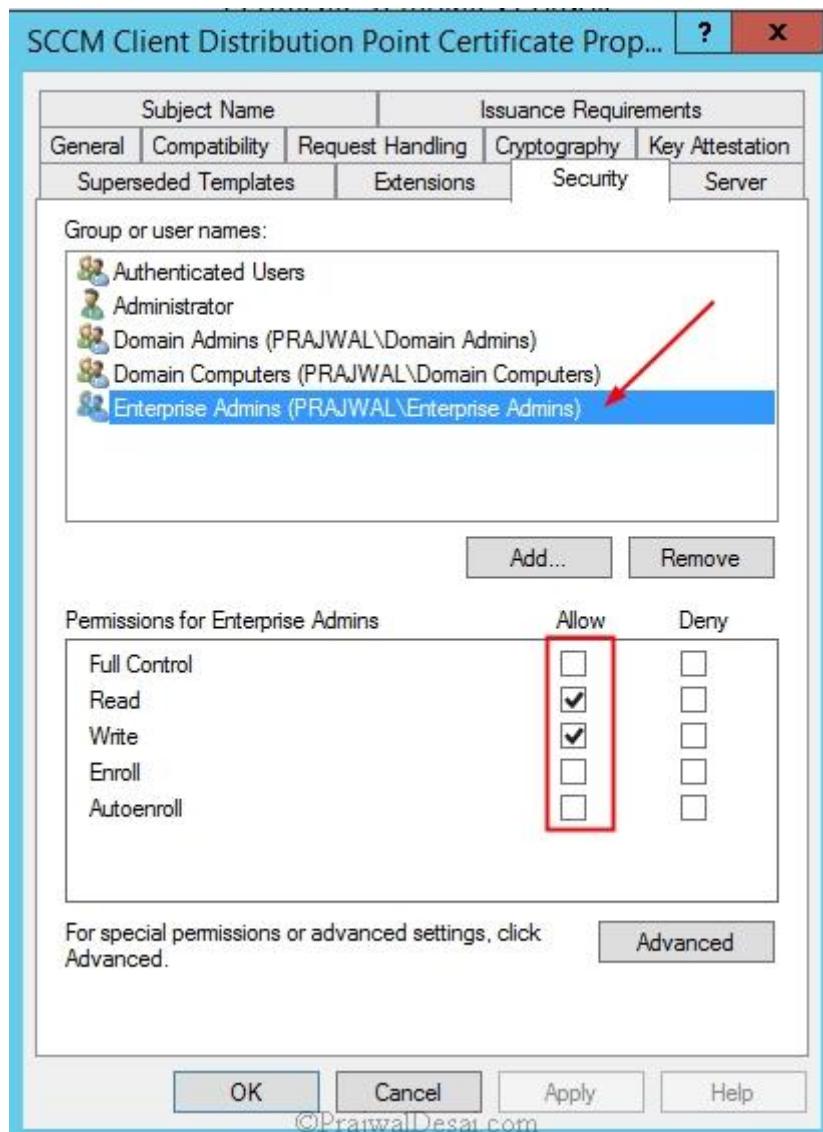
In the Properties of New Template dialog box, on the **General** tab, enter a template name to generate the client authentication certificate for distribution points, such as SCCM Client Distribution Point Certificate.



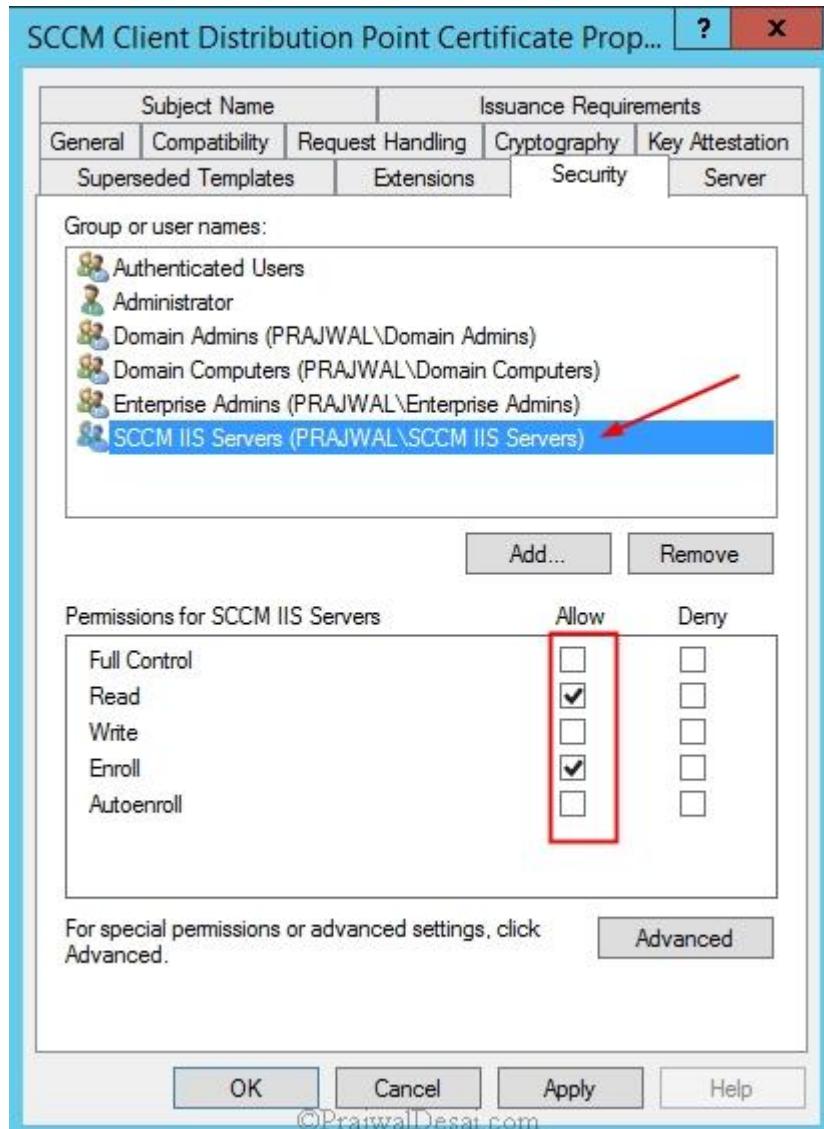
Click the **Request Handling** tab, and select **Allow private key to be exported**.



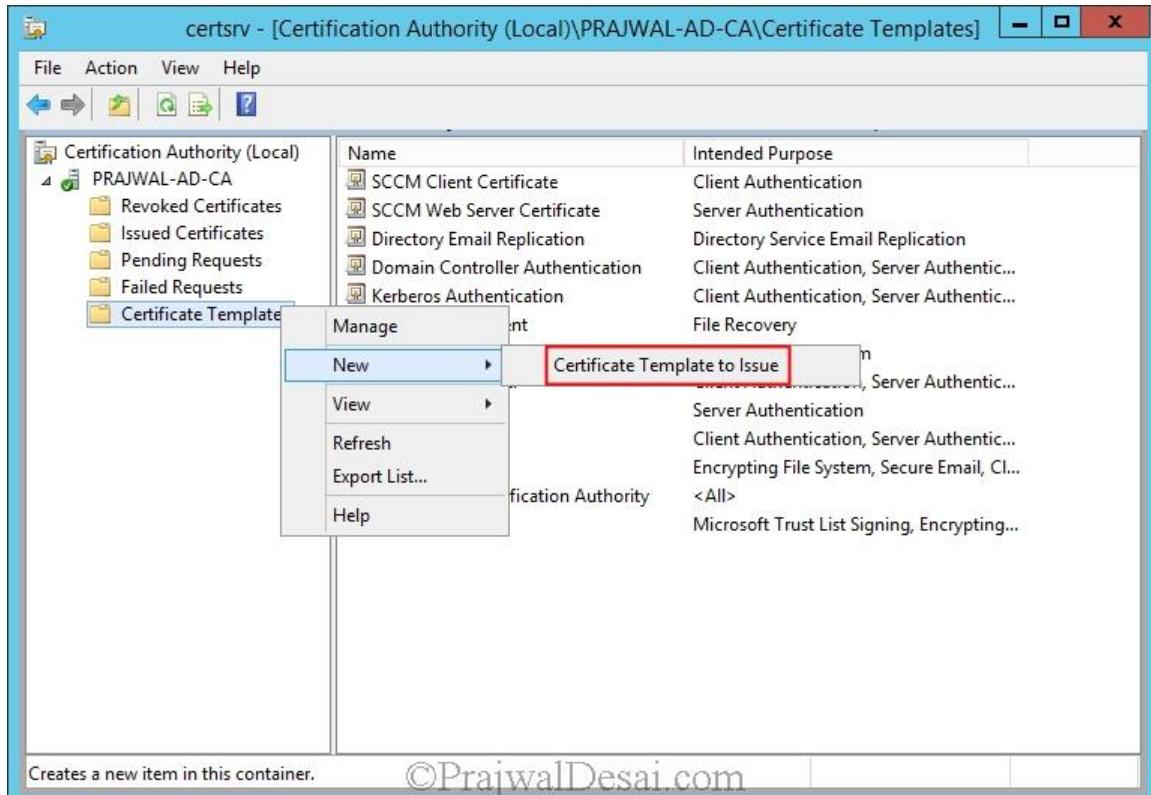
Click the **Security** tab, and remove the **Enroll** permission from the Enterprise Admins security group.



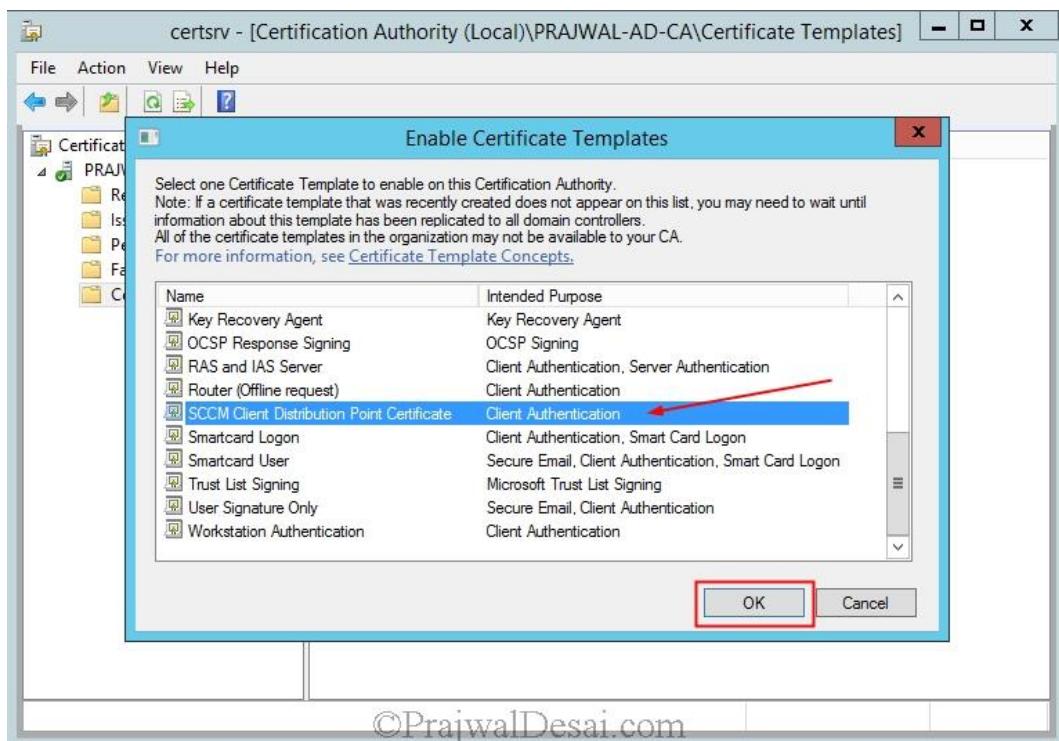
Click **Add**, enter SCCM IIS Servers in the text box, and then click **OK**. Select the **Enroll** permission for this group, and do not clear the Read permission. Click **OK** and close Certificate Templates Console.



In the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**.

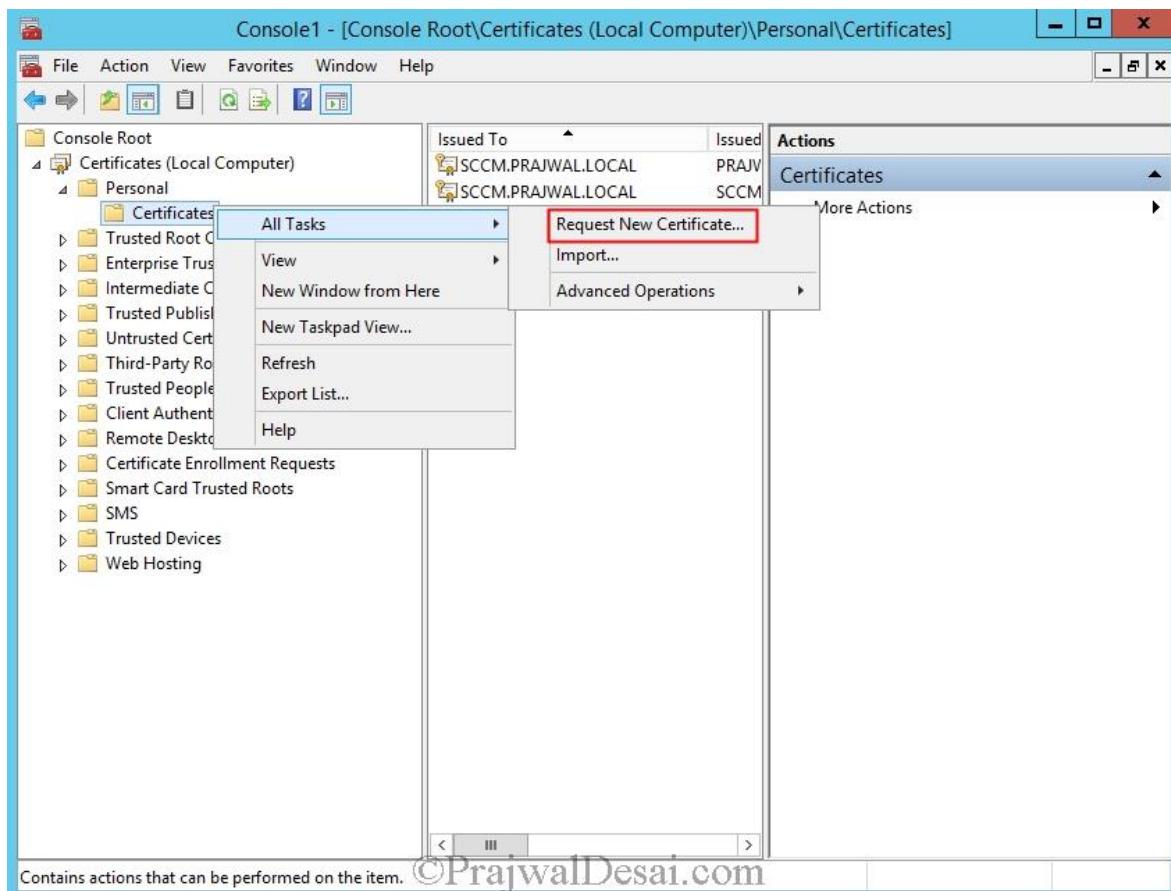


In the Enable Certificate Templates dialog box, select the new template that you have just created, SCCM Client Distribution Point Certificate, and then click OK.



Requesting the Custom Workstation Authentication Certificate

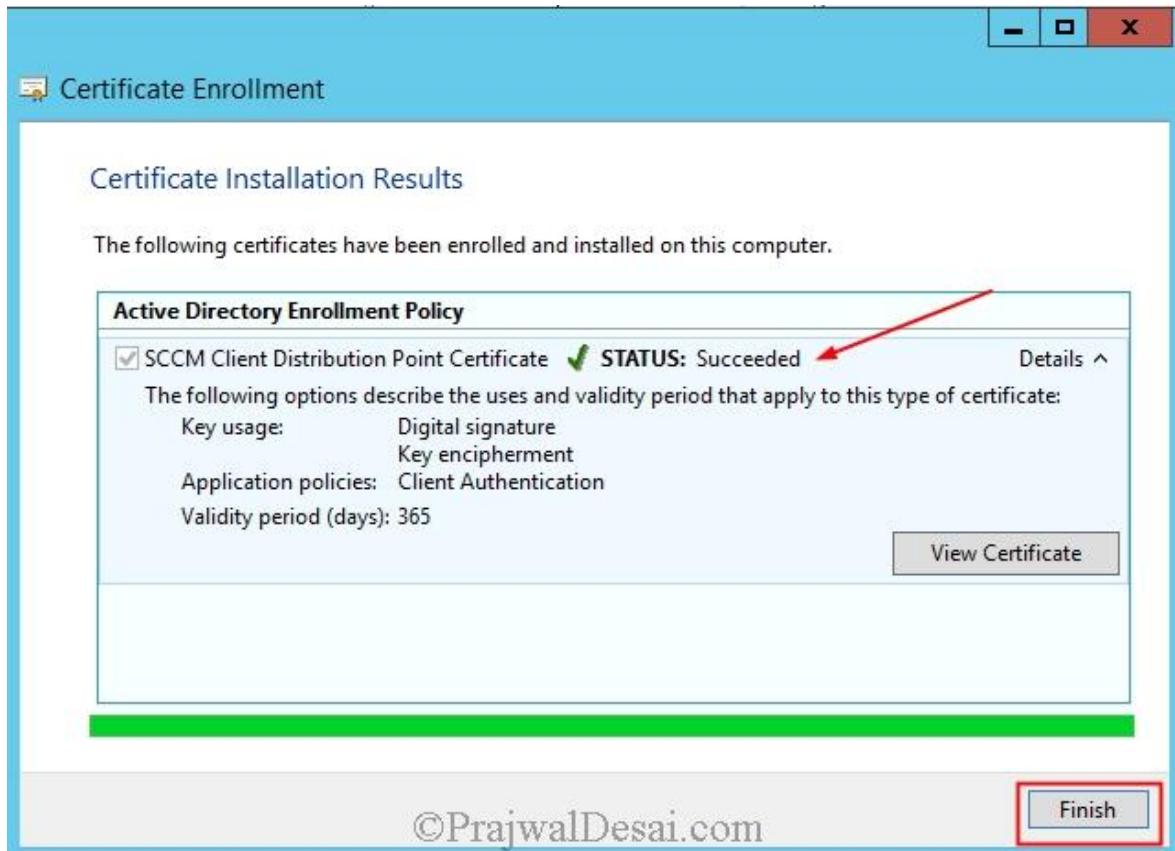
This procedure requests and then installs the custom client certificate on to the member server that runs IIS and that will be configured as a distribution point. Run the mmc command to launch the Certificate snap-in dialog box, select **Computer account** and then click **Next**. In the Select Computer dialog box, ensure **Local computer: (the computer this console is running on) is selected**, and then click **Finish**. In the Add or Remove Snap-ins dialog box, click **OK**. In the console, expand **Certificates (Local Computer)**, and then click **Personal**. Right-click **Certificates**, click **All Tasks**, and then click **Request New Certificate**.



On the **Request Certificates** page, select the **SCCM Client Distribution Point Certificate** from the list of displayed certificates, and then click **Enroll**.



On the **Certificates Installation Results** page, wait until the certificate is installed, and then click **Finish**.



In the results pane, confirm that a certificate is displayed that has **Client Authentication** displayed in the **Intended Purpose** column, and that **SCCM Client Distribution Point Certificate** is displayed in the **Certificate Template** column.

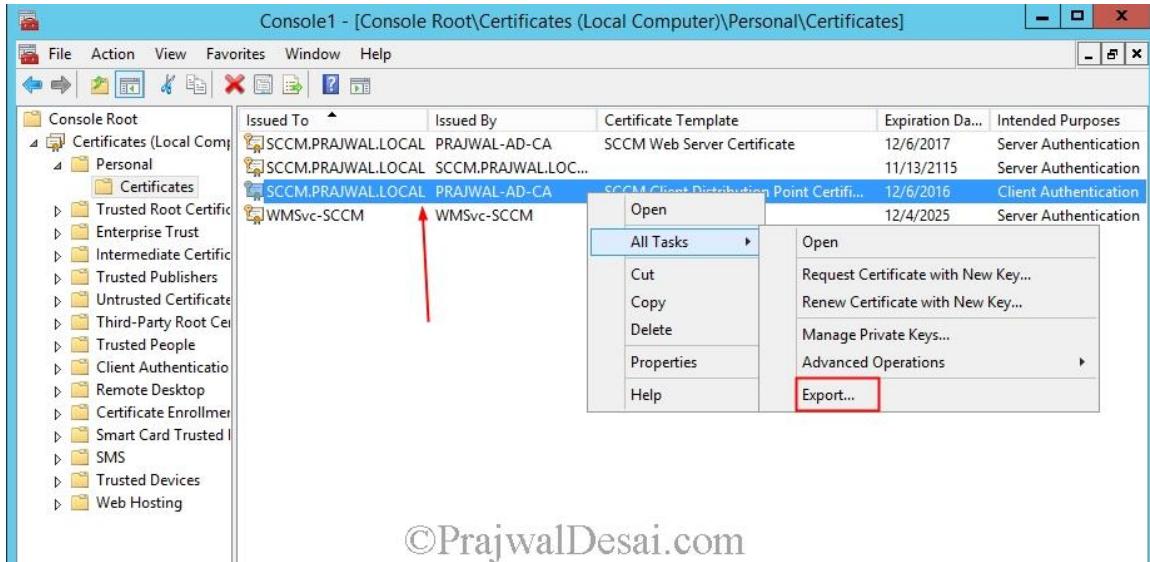
The screenshot shows the 'Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]' window. The left pane shows the certificate structure under 'Console Root\Personal\Certificates'. The right pane lists the certificates with columns for Issued To, Issued By, Certificate Template, Expiration Date, and Intended Purposes. A red arrow points from the 'Intended Purposes' column to the 'Client Authentication' entry for the selected certificate. The certificate details are as follows:

Issued To	Issued By	Certificate Template	Expiration Date	Intended Purposes
SCCM.PRAJWAL.LOCAL	PRAJWAL-AD-CA	SCCM Web Server Certificate	12/6/2017	Server Authentication
SCCM.PRAJWAL.LOCAL	SCCM.PRAJWAL.LOC...		11/13/2115	Server Authentication
SCCM.PRAJWAL.LOCAL	PRAJWAL-AD-CA	SCCM Client Distribution Point Certifi...	12/6/2016	Client Authentication
WMSvc-SCCM	WMSvc-SCCM		12/4/2025	Server Authentication

©PrajwalDesai.com

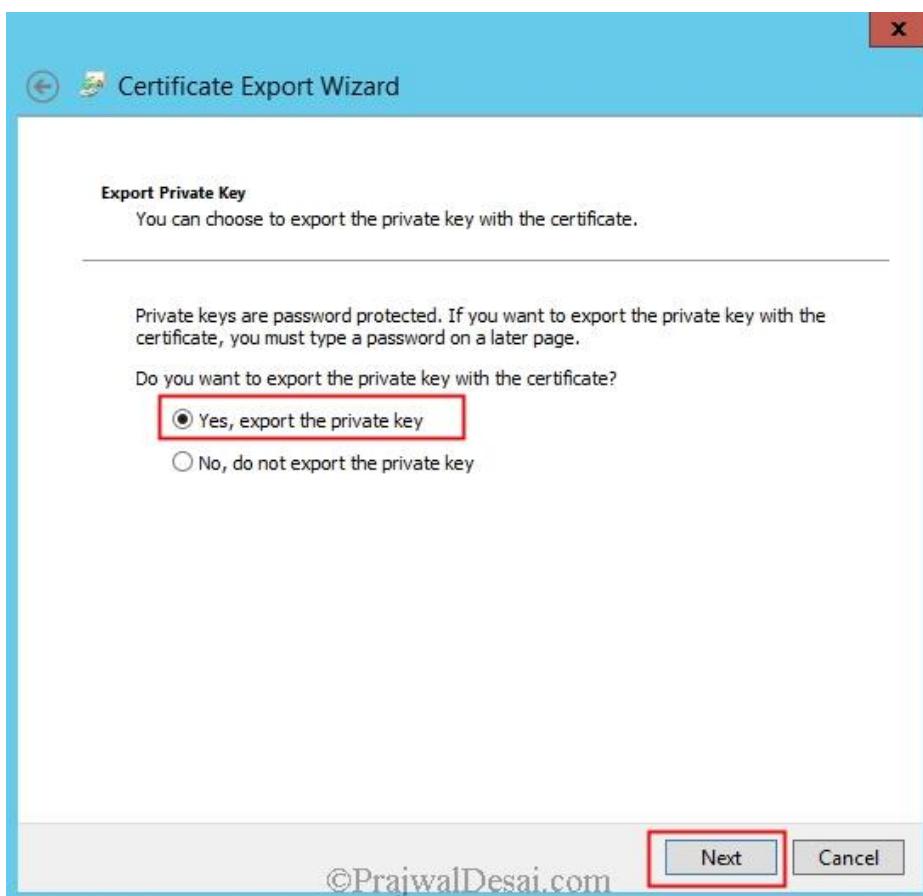
Exporting the Client Certificate for Distribution Points

In the Certificates (Local Computer) console, right-click the certificate that you have just installed, select All Tasks, and then click Export.



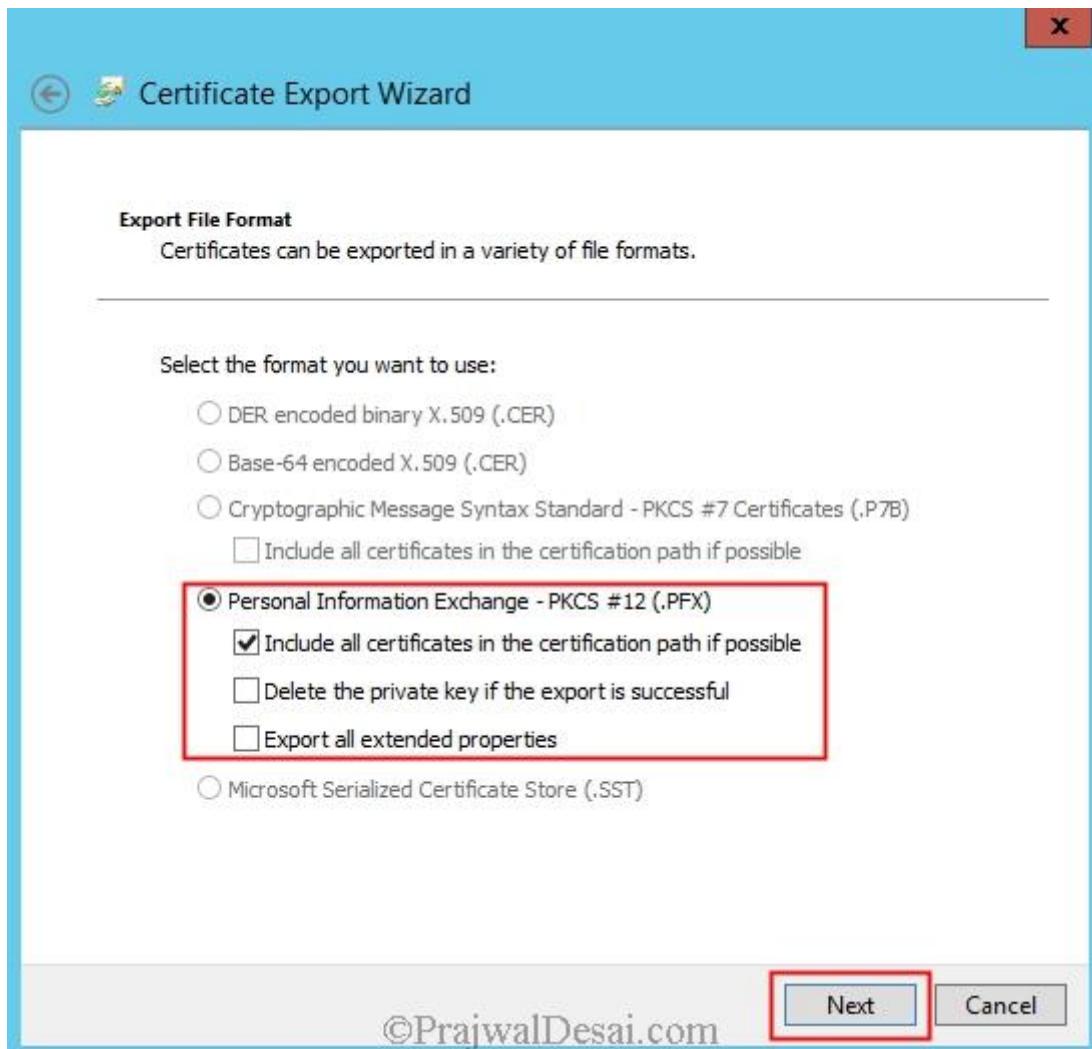
©PrajwalDesai.com

In the **Certificates Export Wizard**, click **Next**. On the Export Private Key page, select **Yes, export the private key**, and then click **Next**.

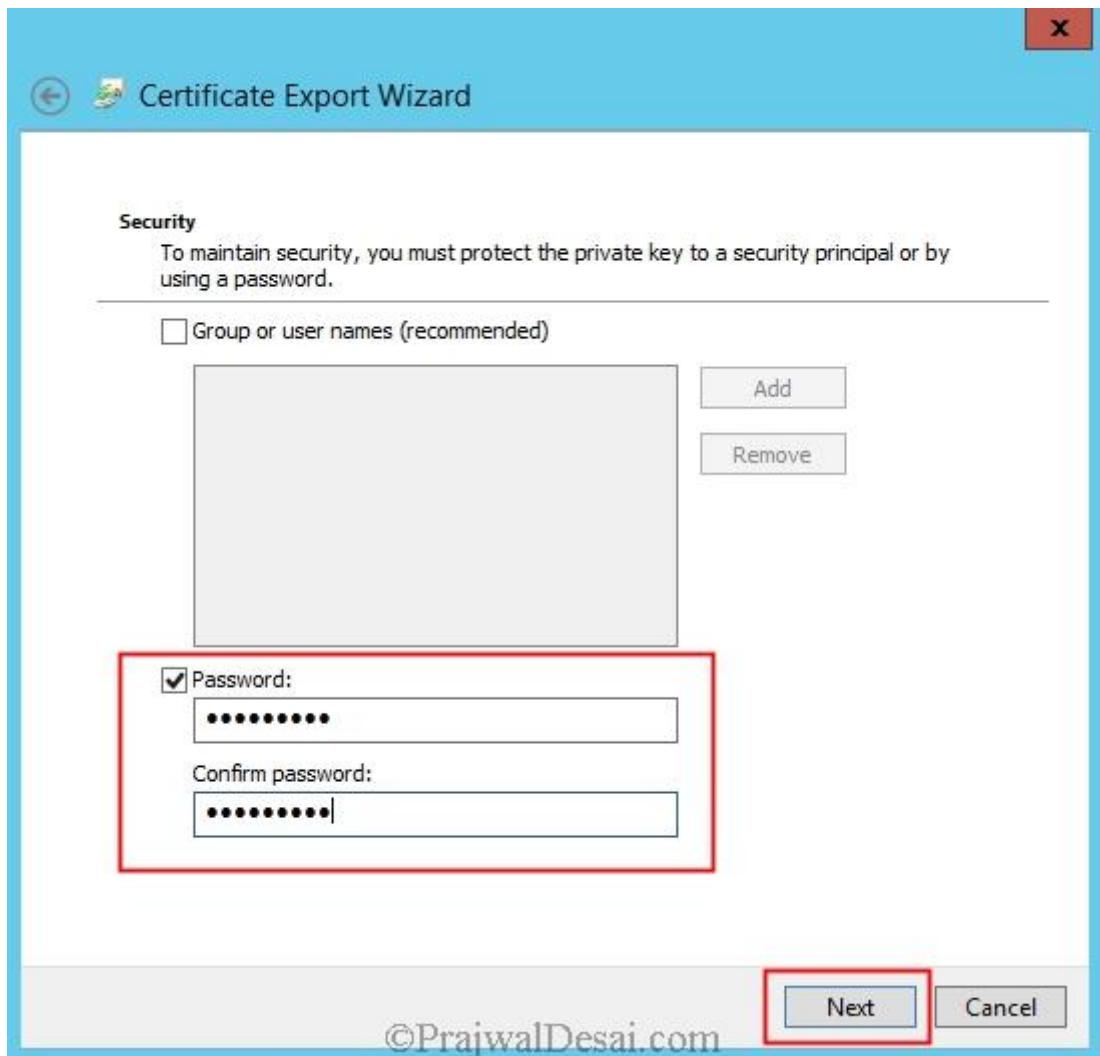


©PrajwalDesai.com

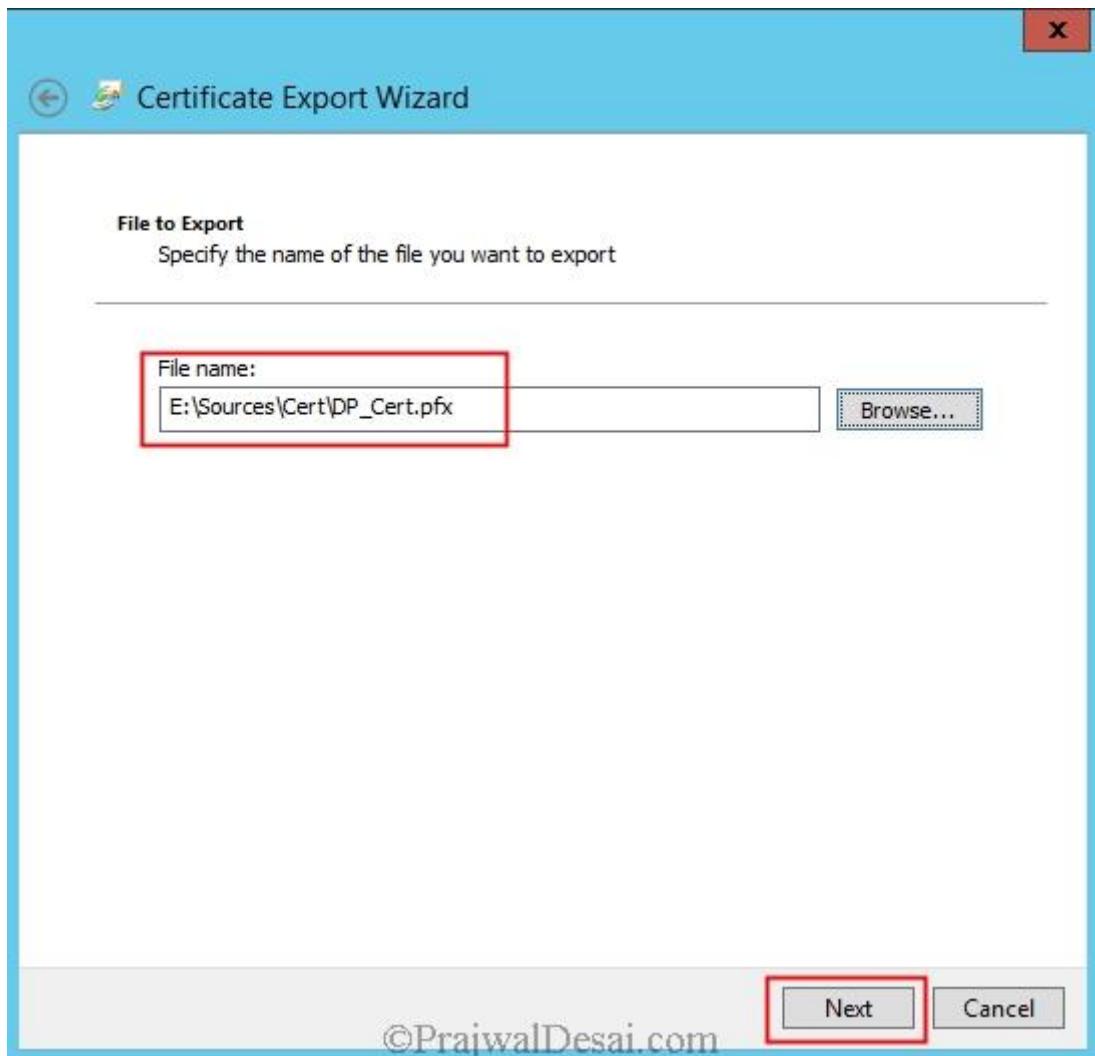
On the Export File Format page, ensure that the option Personal Information Exchange – PKCS #12 (.PFX) is selected. Click **Next**.



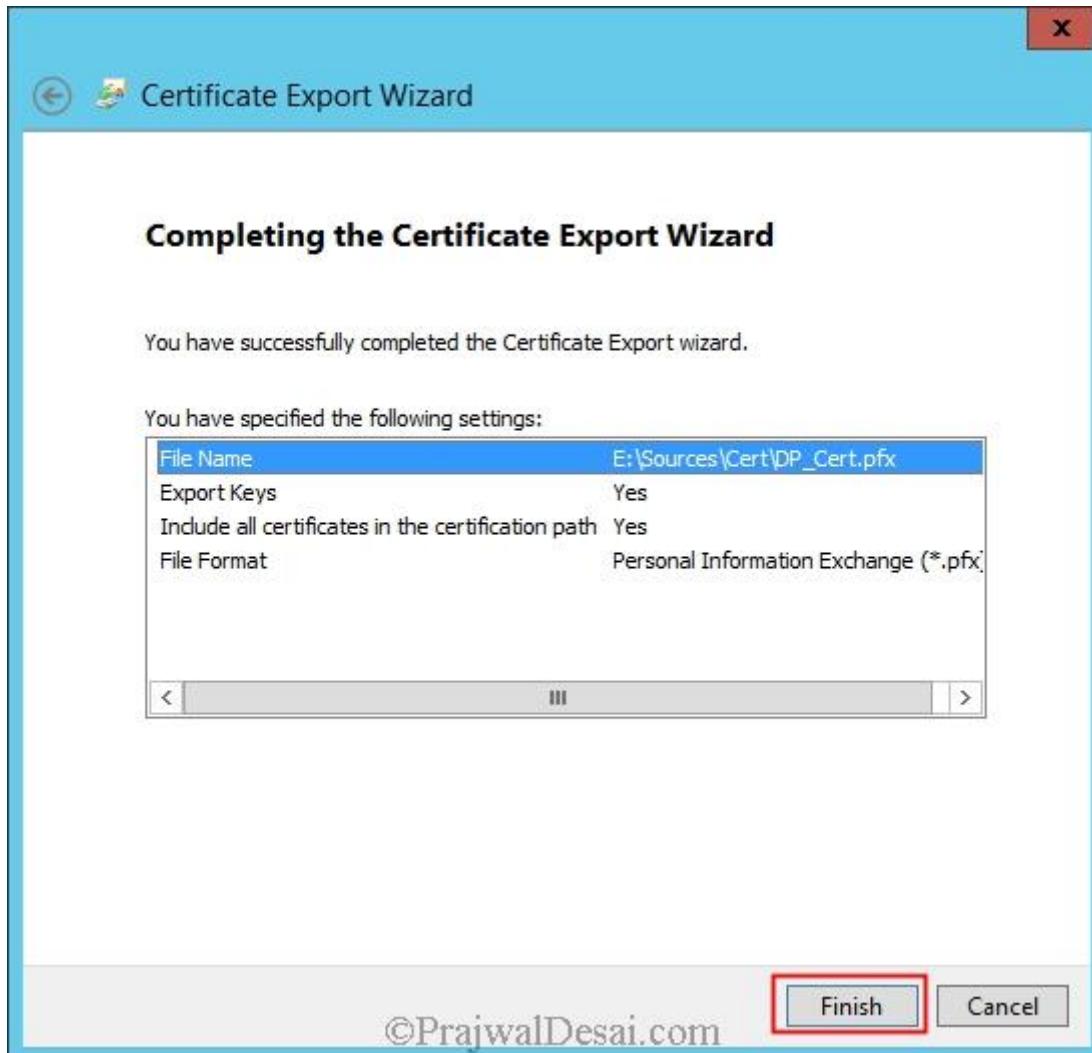
On the Password page, specify a strong password to protect the exported certificate with its private key, and then click **Next**.



On the File to Export page, specify the name of the file that you want to export, and then click **Next**.

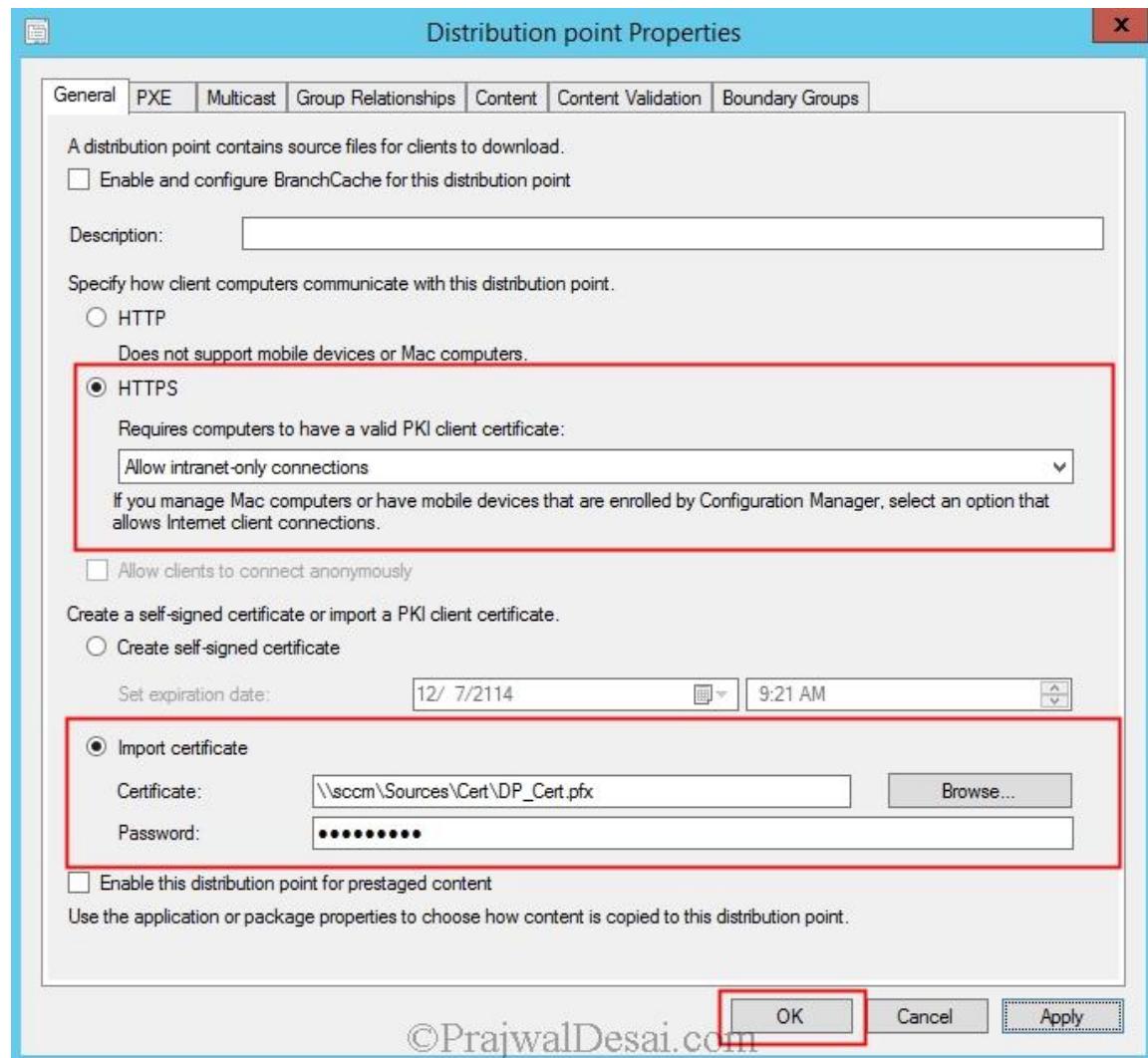


To close the wizard, click **Finish** in the Certificate Export Wizard page, and click **OK** in the confirmation dialog box. Close Certificates (Local Computer). The certificate is now ready to be imported when you configure the distribution point.

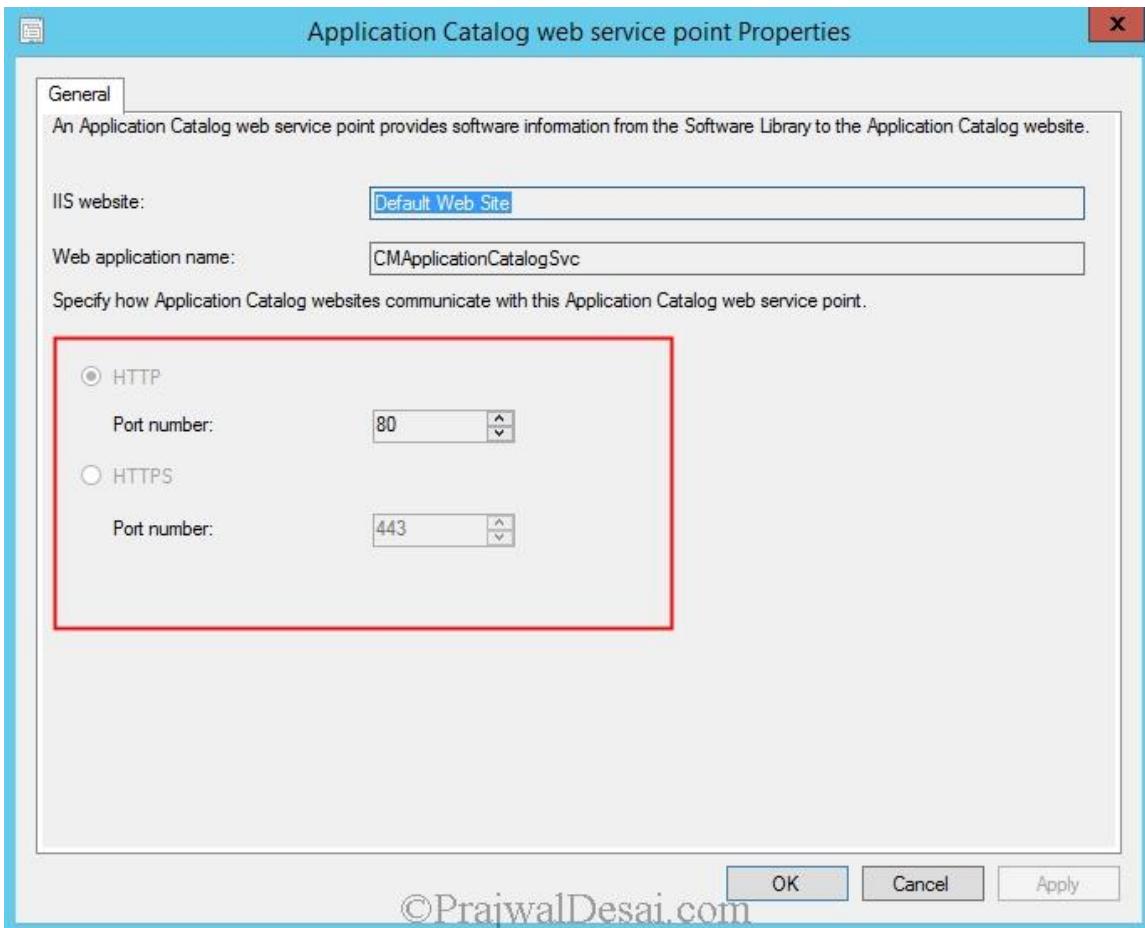


Deploying the Client Certificate for Distribution Points

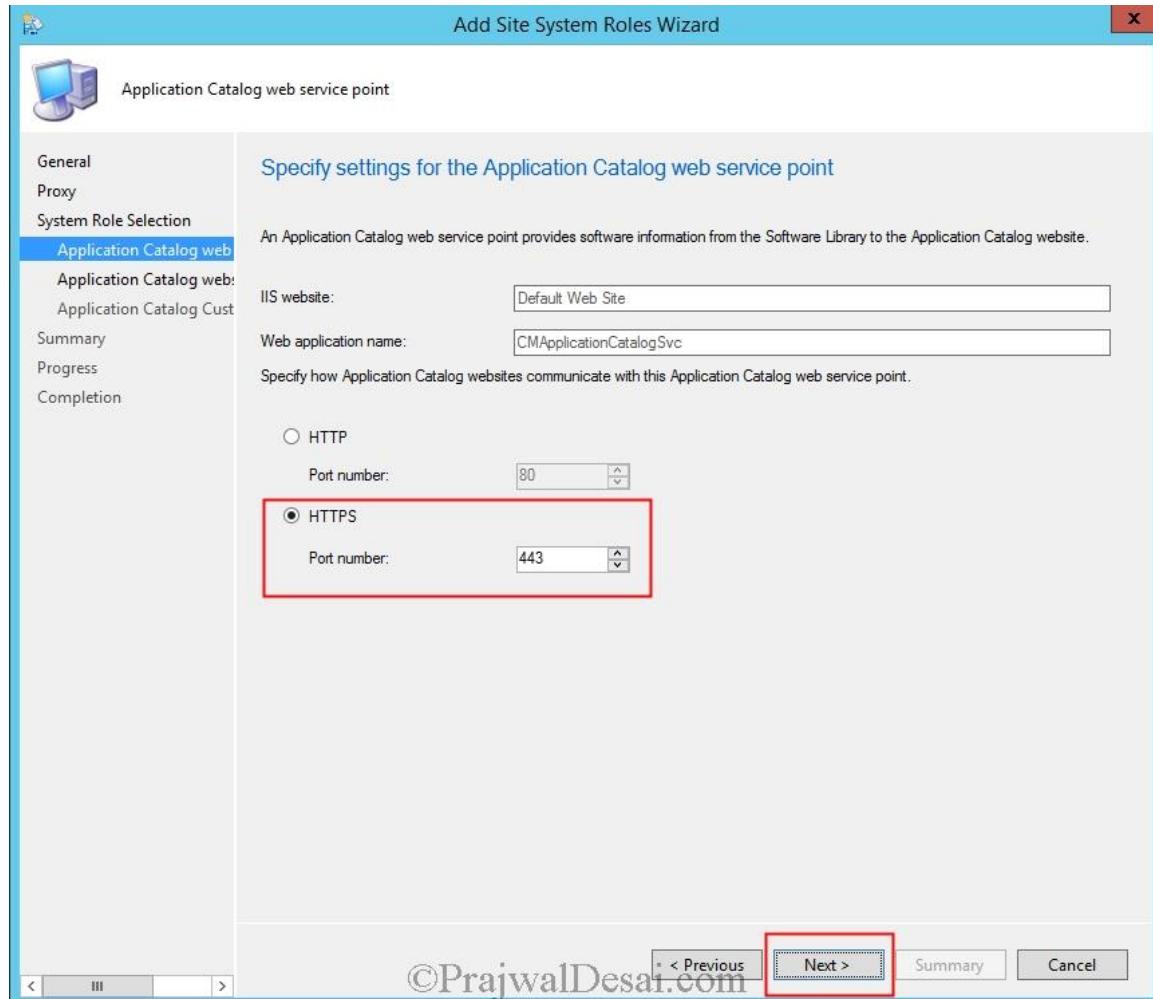
Now that we have got the client certificate for distribution points, let's assign them to the DP's. Right click on the DP and under **General** tab, choose **HTTPS** and to import the certificate click on **Browse**. Import the certificate that you have exported in the above steps, provide the password and click **OK**.



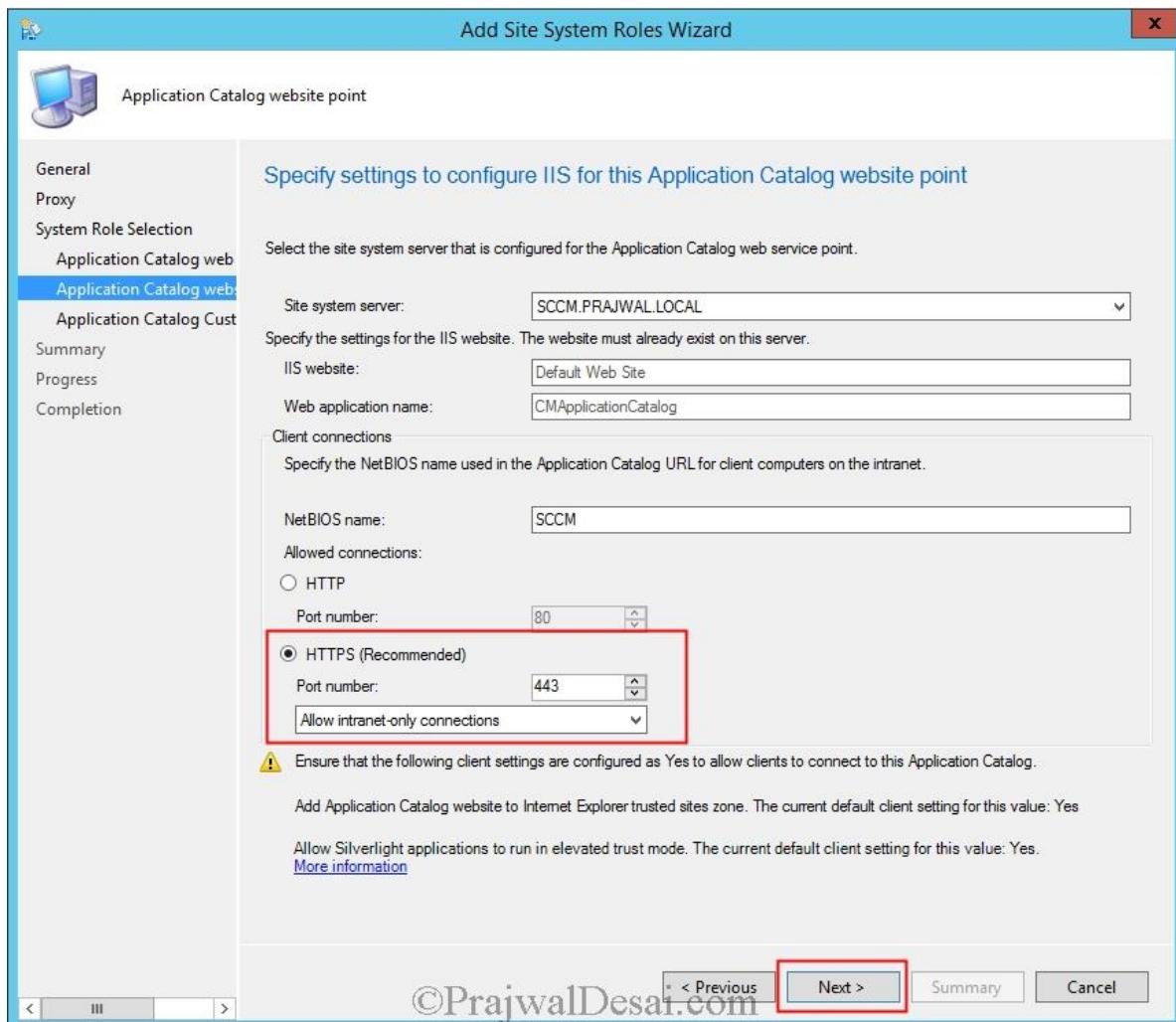
For other roles, you may not be able to switch from HTTP to HTTPS as the options are greyed out. For example on Application catalog web service point, the options are greyed out. You have to uninstall both App catalog website point and App catalog web service point role and install the roles again.



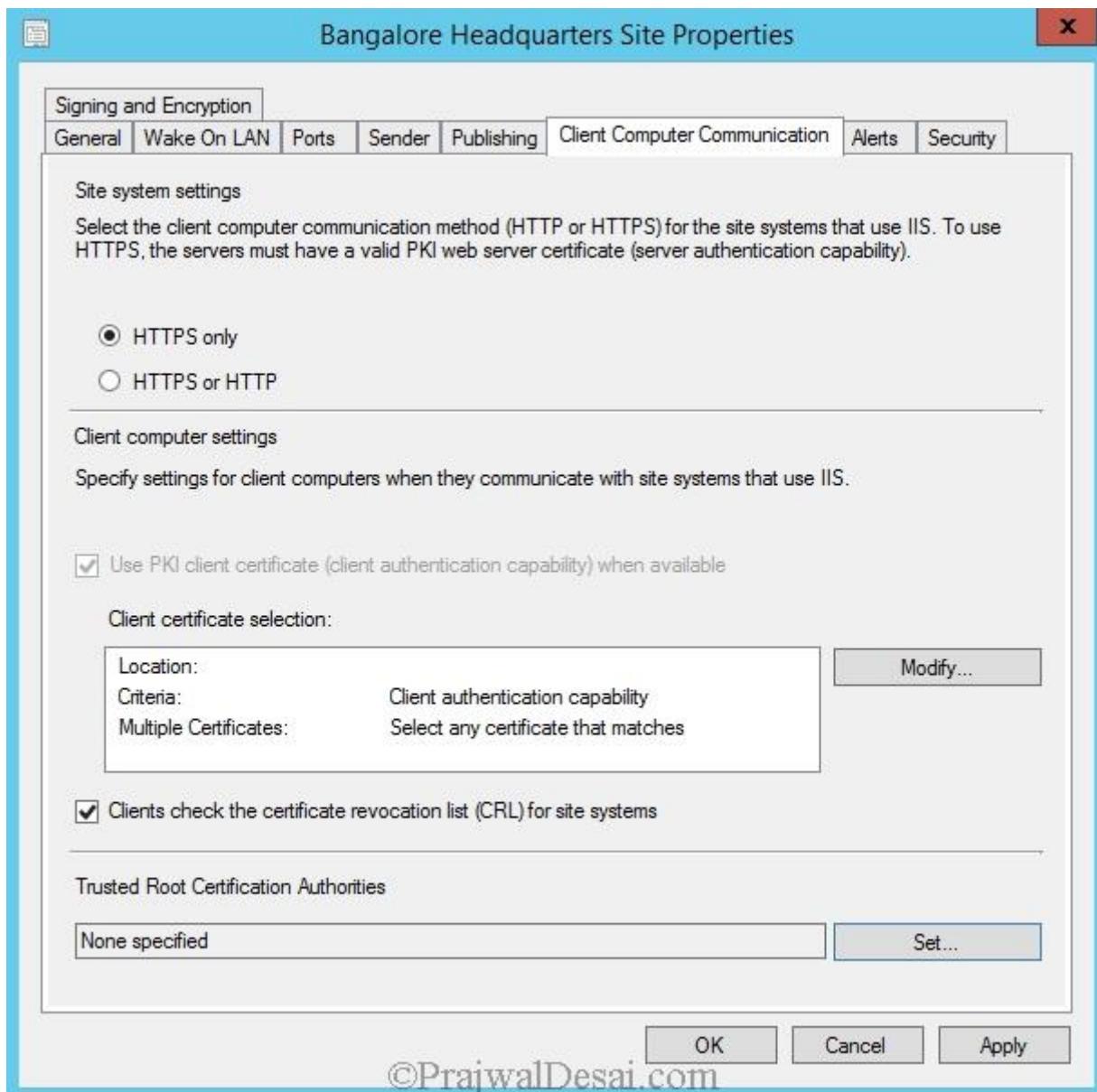
When you are reinstalling the App catalog web service point, you can now specify how App catalog website communicates with App catalog web service point. Choose HTTPS this time.



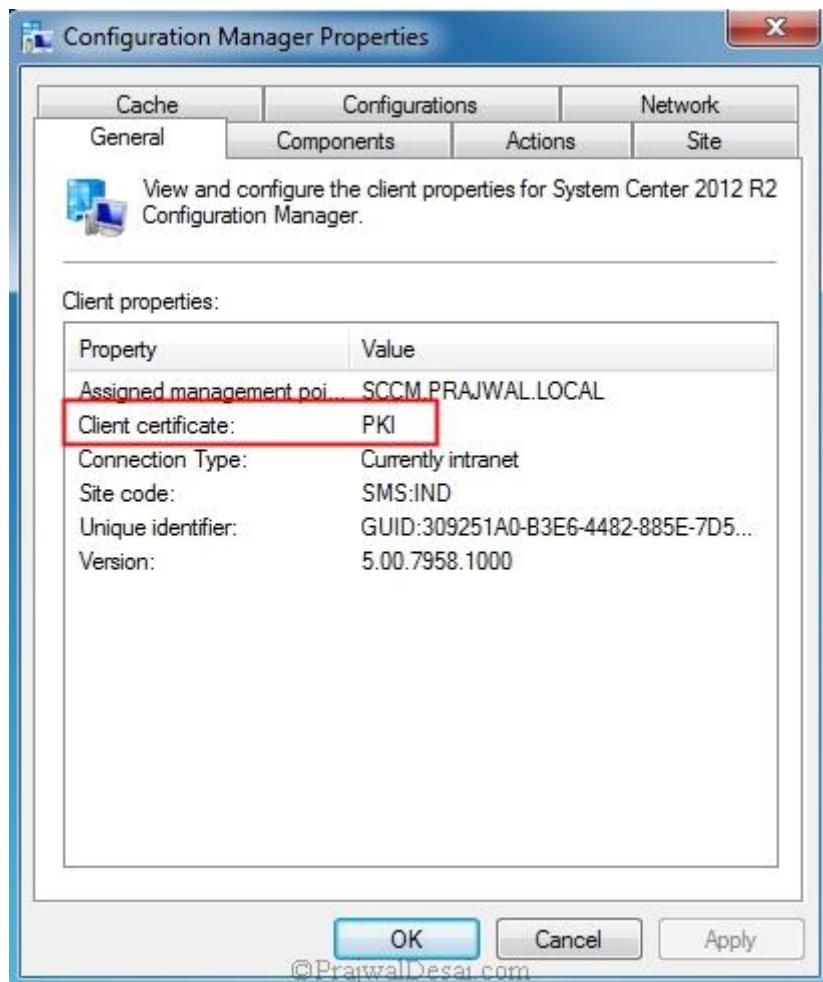
The same goes for App catalog website point. Choose HTTPS here. Click Next.



In the Configuration Manager console, navigate to **Administration > Overview > Site Configuration > Sites**. Right click on the site server and click **Properties**. Under **site system settings**, choose **HTTPS only** and click **OK**.



Login to one the computers which has Configuration Manager client installed. Look under General tab of configuration manager client properties. You will notice that Client Certificate is changed from self-signed to **PKI**.



PART 42