



SCCM 1606-1702 Step by Step Installation Guide

By

Eddie Jackson

Version 1

SCCM – Step by Step Installation Guide

The following guide will take you through the installation of SCCM with a simple Primary Server approach and with the SQL 2012 server located on the same device. Before installing SCCM, you will need to run through some prep work to get Active Directory configured and extended, along with some application, role, and feature installs.

But first, download everything you will need to get started.

SQL 2012 (or 2014, 2016)

<https://www.microsoft.com/en-us/download/details.aspx?id=29066>

SQL SP3 (only needed for SQL 2012)

<https://www.microsoft.com/en-us/download/details.aspx?id=49996>

W10 ADK

<https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit>

SCCM Source Files

<https://www.microsoft.com/en-us/evalcenter/evaluate-system-center-2016>

Now, it is assumed you already have an AD DC with DNS, DHCP, etc. And, that a member server (for SCCM) has been set up. I would also recommend having client computers ready to go.

Welcome to the heaven, the hell, and the purgatory—the best and worst experiences of your life—SCCM. I hope this document will be useful to you. Email me at mrnettek@gmail.com for corrections, additions, or questions. As this is only Version 1 of the document, I hope to continue adding to it. Good luck!

CONTENTS

[Network Diagrams](#)

[Create the “System Management” Container in Active Directory](#)

[Extend the Schema](#)

[Add IIS Components](#)

[Configure IIS](#)

[Install Windows Assessment and Deployment Kit \(Windows ADK\) for Windows 10](#)

[Install SQL Server](#)

[Install SCCM {current build}](#)

[Discovery Methods and Boundary Configuration](#)

[Enable Automatic Client Push](#)

[Add Distribution Point to Boundary Groups](#)

[Updating SCCM Configuration Manager](#)

[Create a Package](#)

[Pre-Deploy a Package](#)

[Deploy Package](#)

[Monitoring a Deployment](#)

[WDS Setup](#)

[PXE Setup](#)

[Imaging Setup](#)

[Deploy Image](#)

[WSUS Setup](#)

[Deploy Updates](#)

[Report Setup, Reporting Services Point](#)

[Set up a Distribution Point at Another Site](#)

[Set up a WSUS at another Site](#)

[Deploying SCCM Clients Using Group Policy](#)

[Hierarchies and Sites](#)

[SCCM Scripts](#)

[Troubleshooting](#)

[More Advanced WSUS Troubleshooting](#)

[Tips](#)

[Logs and Descriptions](#)

[Client Log Files](#)

[Server Log Files](#)

[Admin Console Log Files](#)

[Management Point Log Files](#)

[Mobile Device Management Log Files](#)

[Mobile Device Client Log Files](#)

[Operating System Deployment Log Files](#)

[Network Access Protection Log Files](#)

[System Health Validator Point Log Files](#)

[Desired Configuration Management Log Files](#)

[Wake On LAN Log Files](#)

[Software Updates Site Server Log Files](#)

[WSUS Server Log Files](#)

[Software Updates Client Computer Log Files](#)

[Windows Update Agent Log File](#)

[Client Error/Return Codes](#)

[Server Error/Return Codes](#)

[CCMEval and Remediation](#)

[Hardware Requirements](#)

[Reference](#)

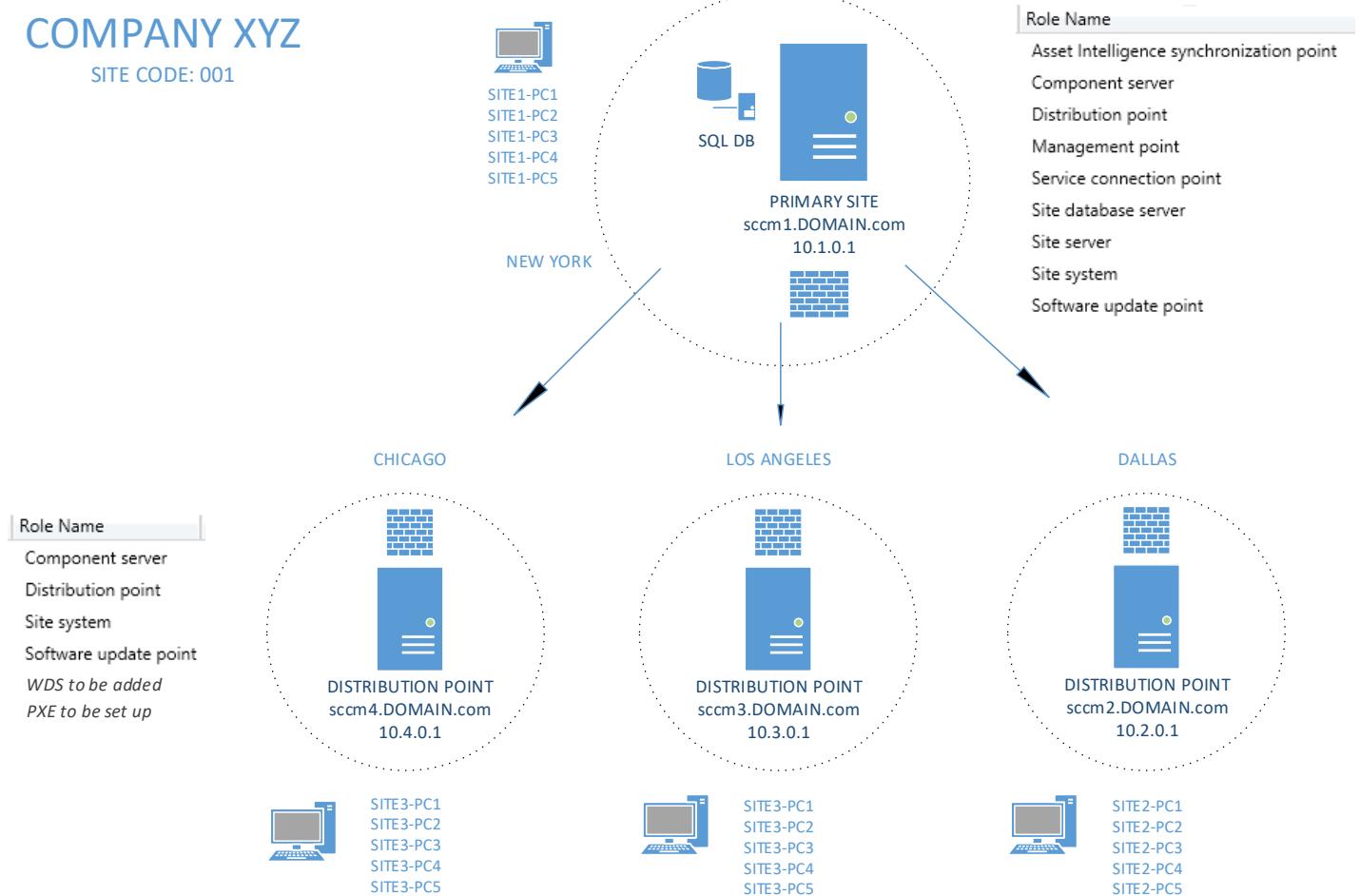
Future topics: Capture Image, Customize Image, Dual Boot Menu Options, More Scripts, Harden Security, Reporting

EXTERNAL LINKS

[Full SCCM Manual](#)

Network Diagrams

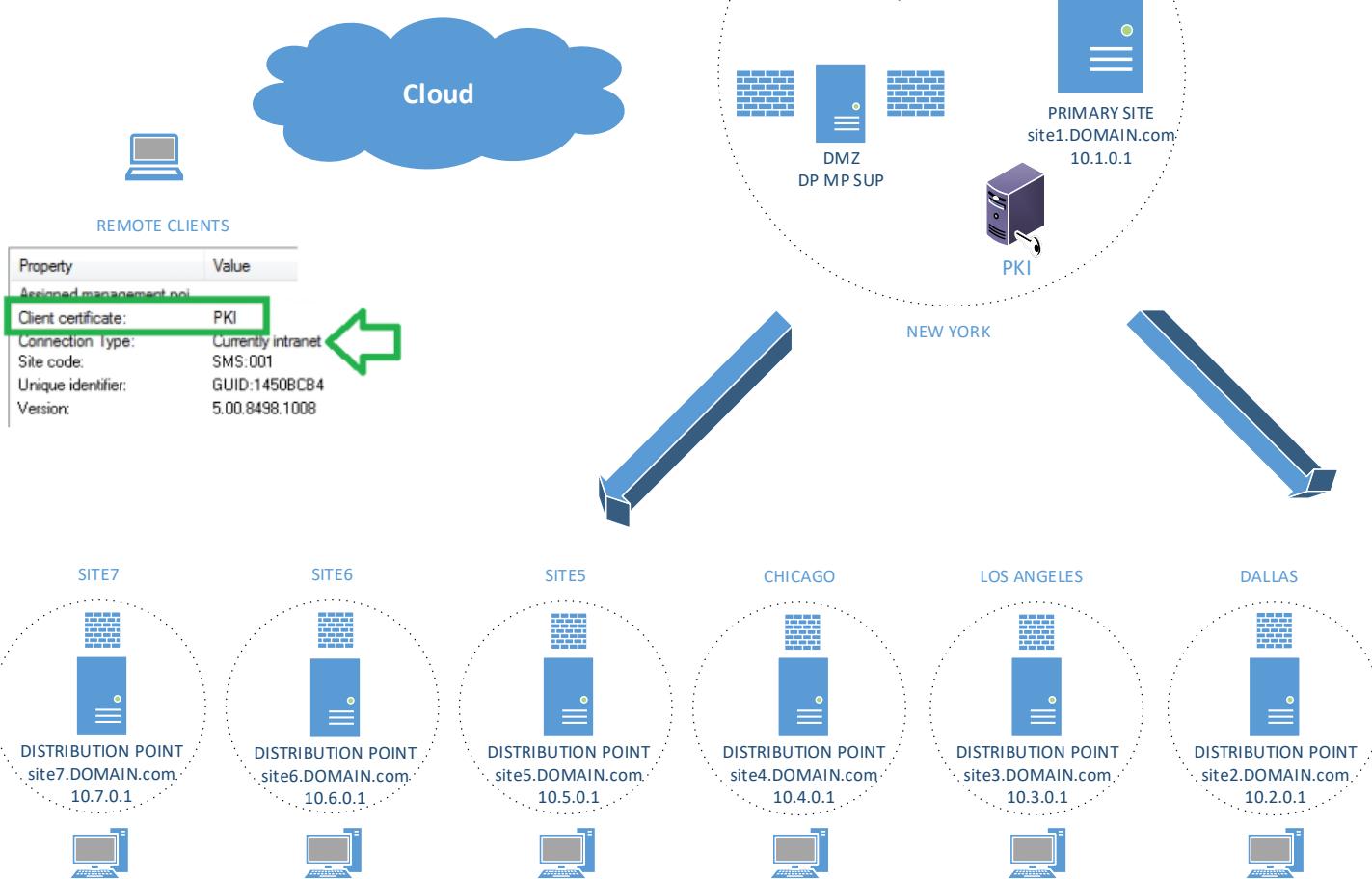
Layout 1



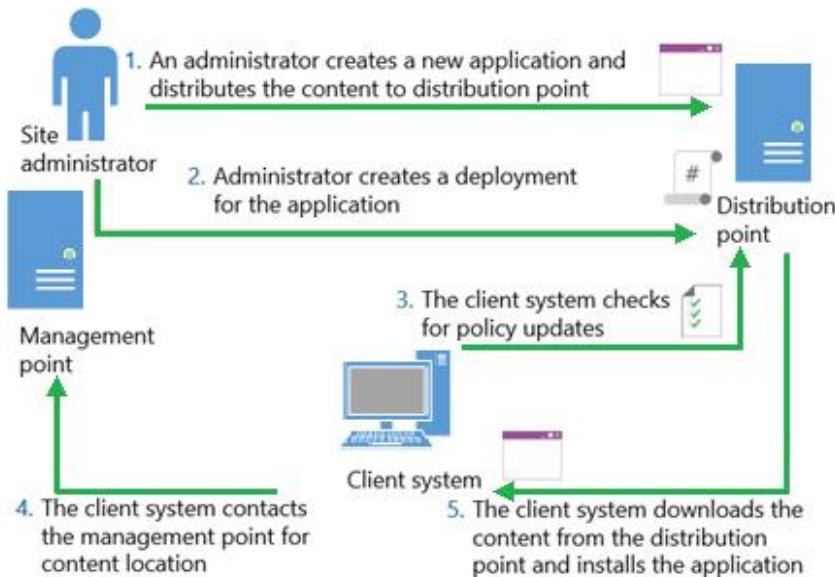
Layout 2

COMPANY XYZ

SITE CODE: 001



Package Delivery in SCCM



Package Management in the SCCM Console

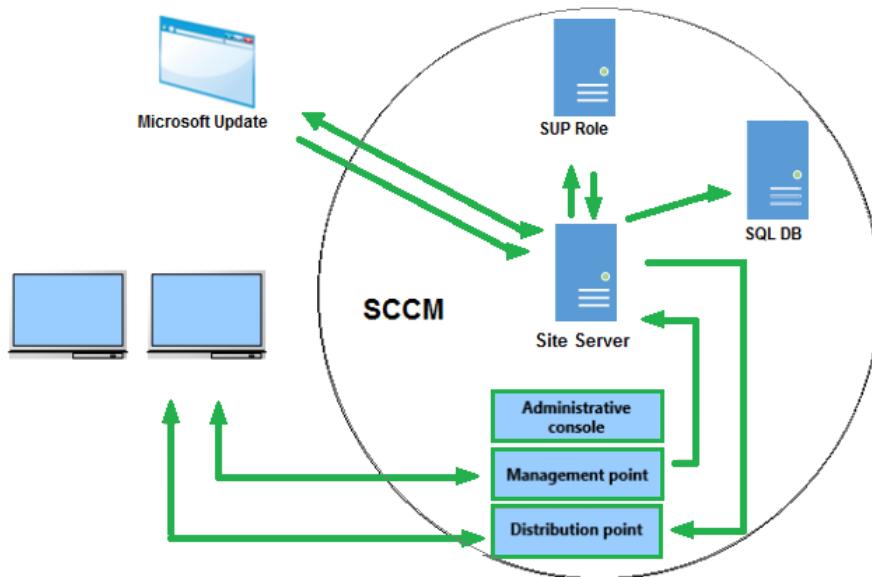
The screenshot shows the SCCM Application Management console. The left navigation pane displays the following hierarchy:

- Software Library
 - Overview
 - Application Management** (selected)
 - Applications
 - License Information for Store Apps
 - Packages
 - Approval Requests
 - Global Conditions
 - App-V Virtual Environments
 - Windows Sideload Keys
 - Application Management Policies
 - App Configuration Policies

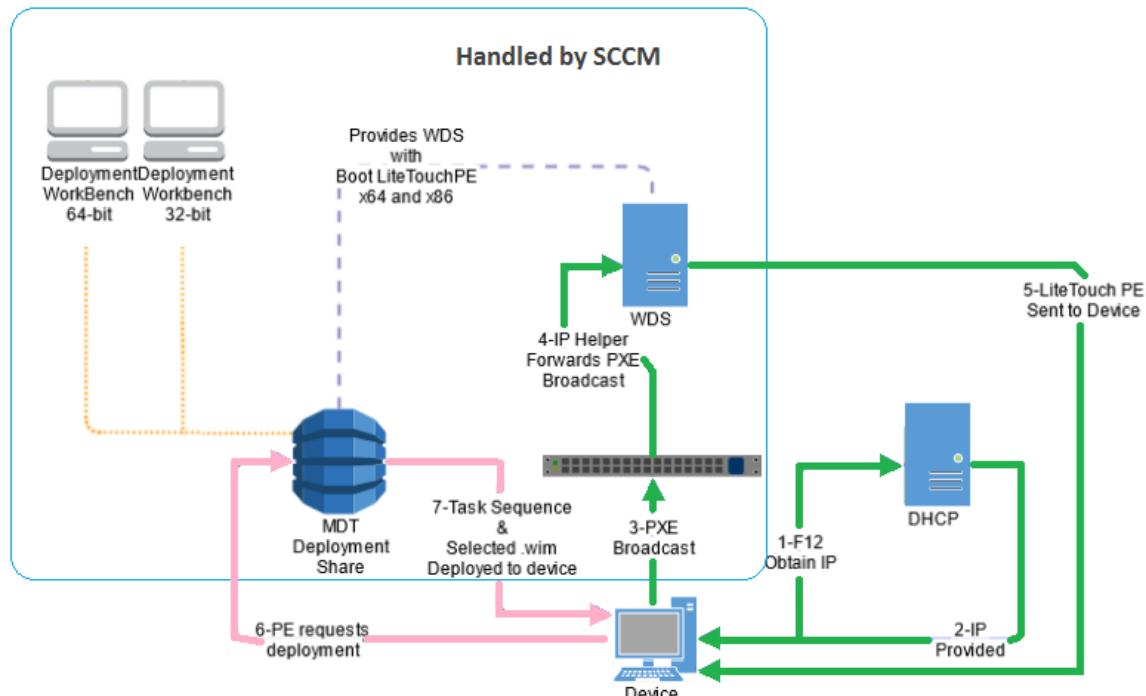
The main content area is titled "Application Management" and contains a "Navigation Index" with the following links:

- Applications:** Manage and deploy applications to users and devices, and configure rules to install and uninstall applications.
- Packages:** Manage packages that contain the files and instructions to deploy programs to users and devices.
- Global Conditions:** Manage global conditions for all applications in the site hierarchy.
- Windows Sideload Keys:** Windows Sideload Keys
- App Configuration Policies:** Manage app configuration policies.
- License Information for Store Apps:** Manage Licensed Store Applications
- Approval Requests:** Manage application requests from users for Software Center applications that require approval.
- App-V Virtual Environments:** Virtual Environment
- Application Management Policies:** Configure application management policies for the hierarchy.

Windows Update in SCCM



PXE Imaging in SCCM

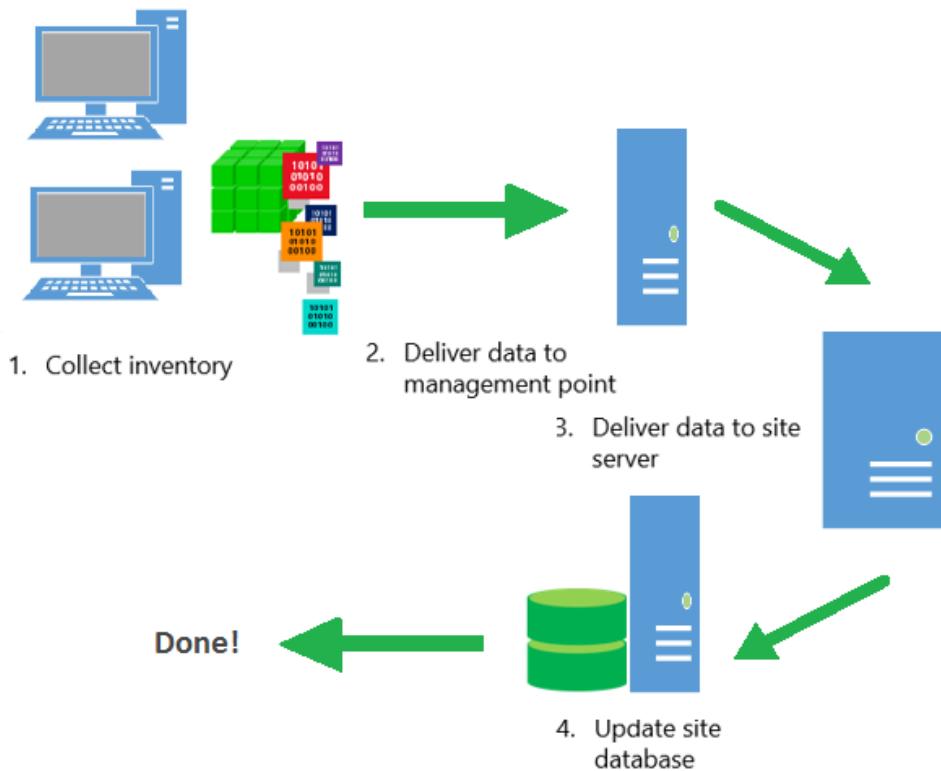


Imaging Management in the SCCM Console

The screenshot shows the left navigation pane of the SCCM console. The 'Operating Systems' node is expanded, revealing sub-items: Drivers, Driver Packages, Operating System Images, Operating System Upgrade Packages, Boot Images, Task Sequences, and Virtual Hard Disks. To the right, a 'Navigation Index' pane provides detailed descriptions for each of these sub-items.

Category	Description
Drivers	Manage device drivers and device driver catalogs to deploy operating systems.
Driver Packages	Manage device driver packages.
Operating System Images	Manage Windows image files for operating system deployment.
Operating System Upgrade Packages	Manage operating system upgrade packages.
Boot Images	Manage boot images for operating system deployment.
Task Sequences	Manage task sequences that automate steps or tasks on client computers.
Virtual Hard Disks	Manage Virtual Hard Disks.

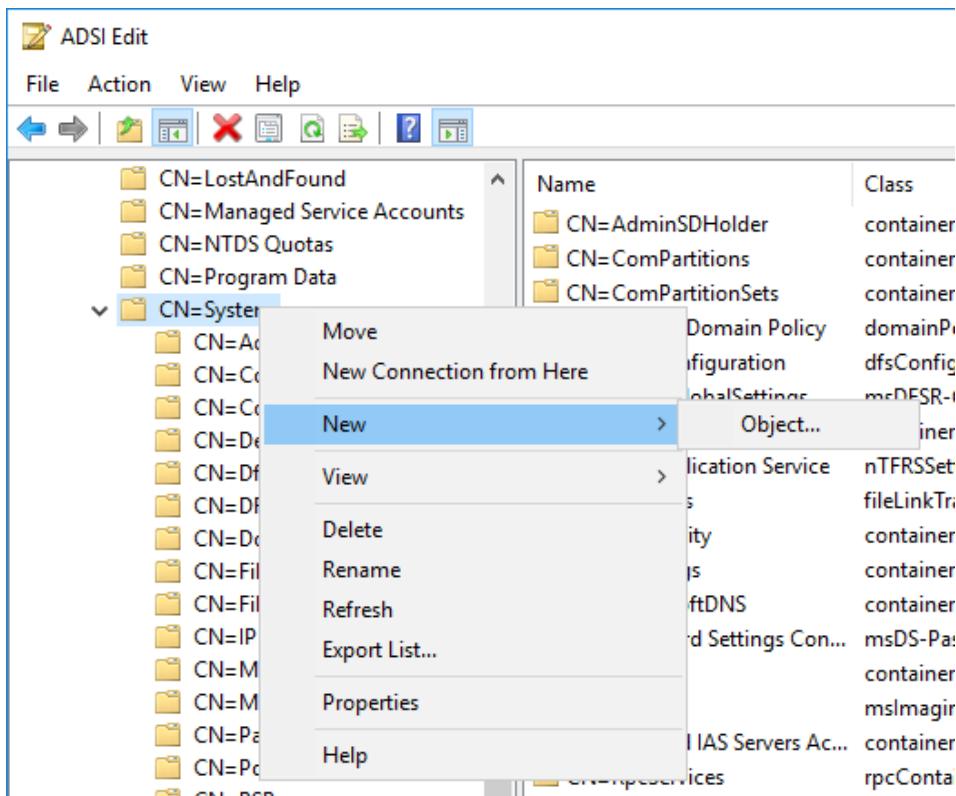
Inventory Collection in SCCM



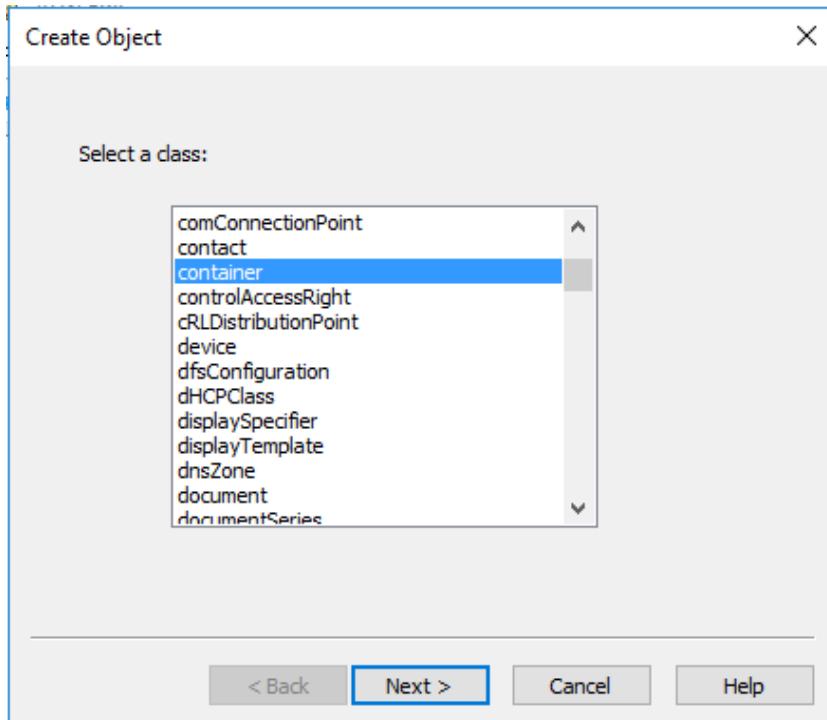
Prepare Active Directory for Configuration Manager

Create the “System Management” Container in Active Directory

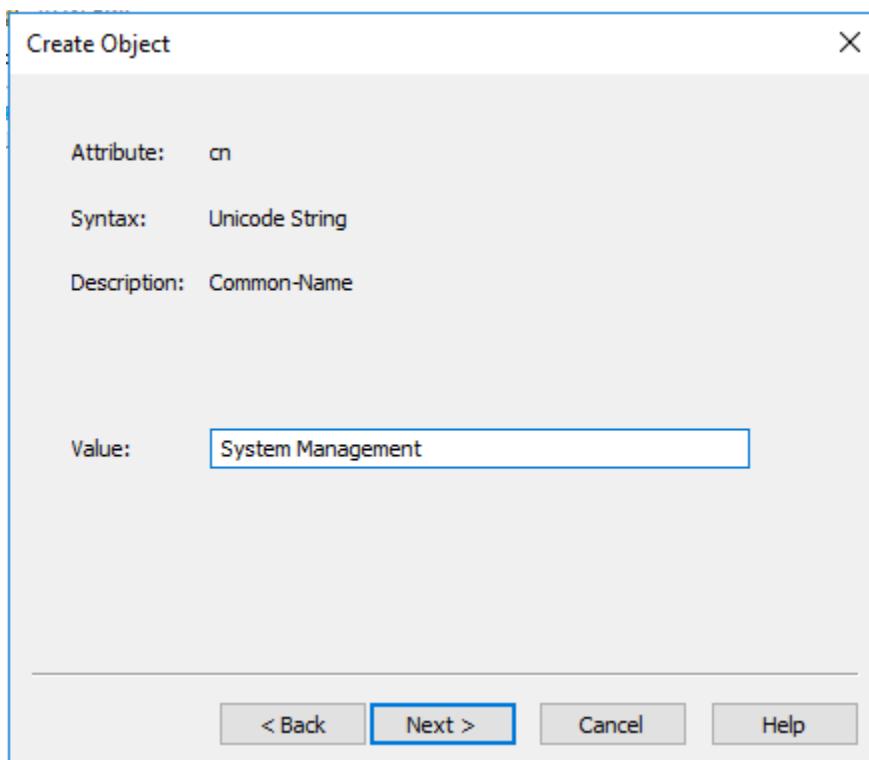
Connect to a domain controller and load ADSI Edit. Under the System OU create a new Object.



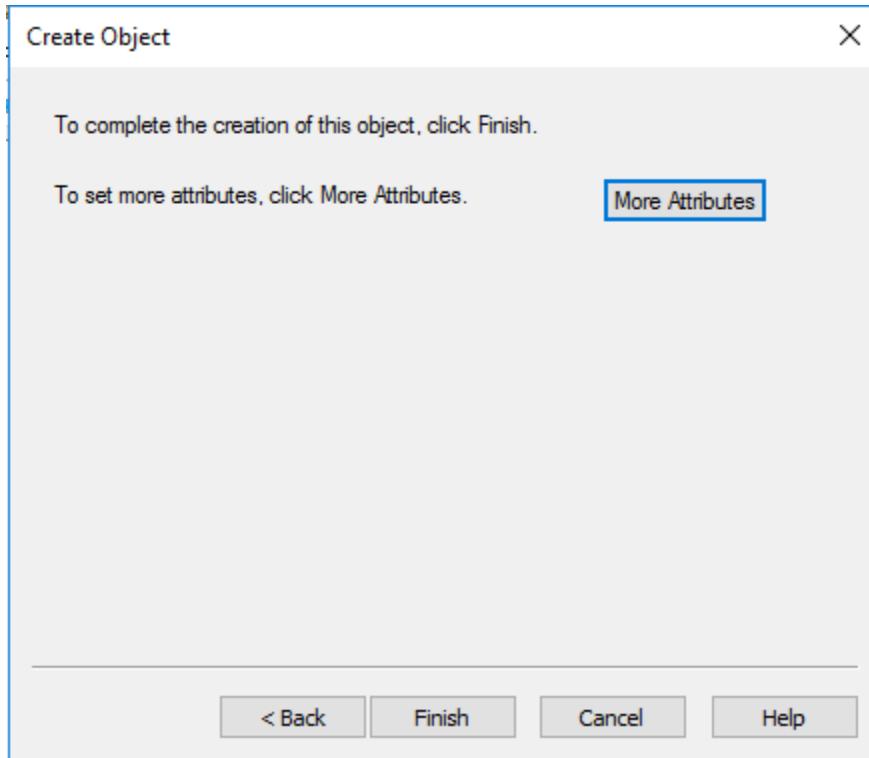
Choose **container** and click **Next**.



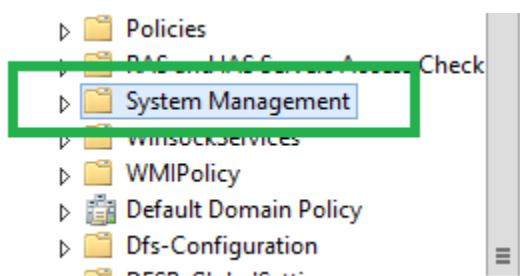
Enter the name **System Management** and click **Next**.



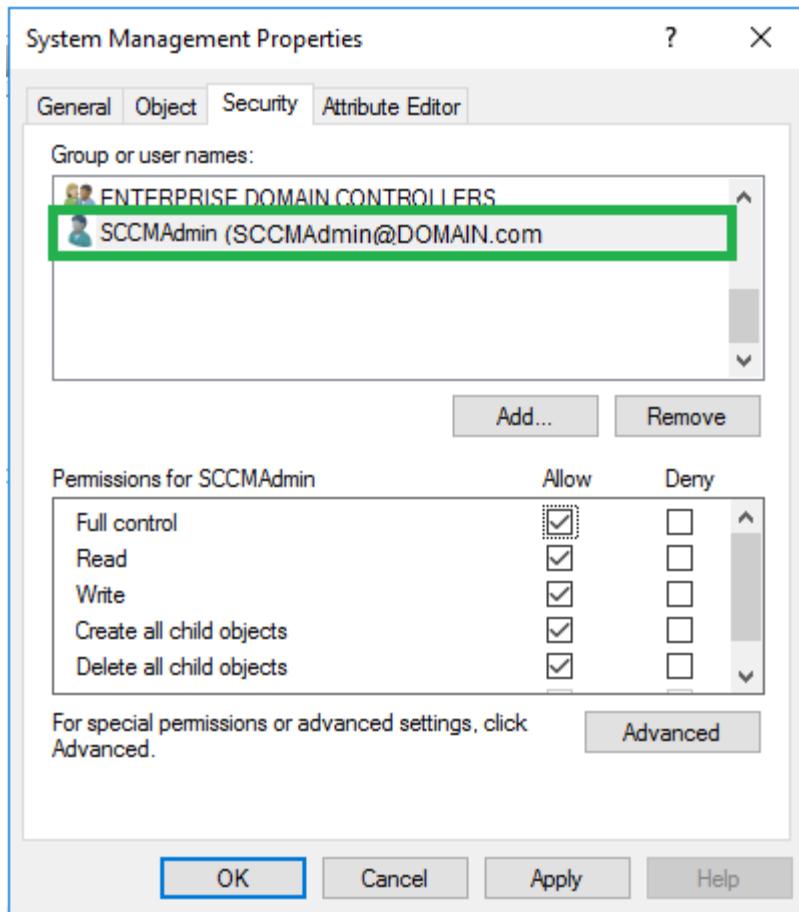
Complete the wizard and close ADSIEdit.



Next, launch Active Directory Users and Computers, Select View, Advanced, and then find **System Management**.

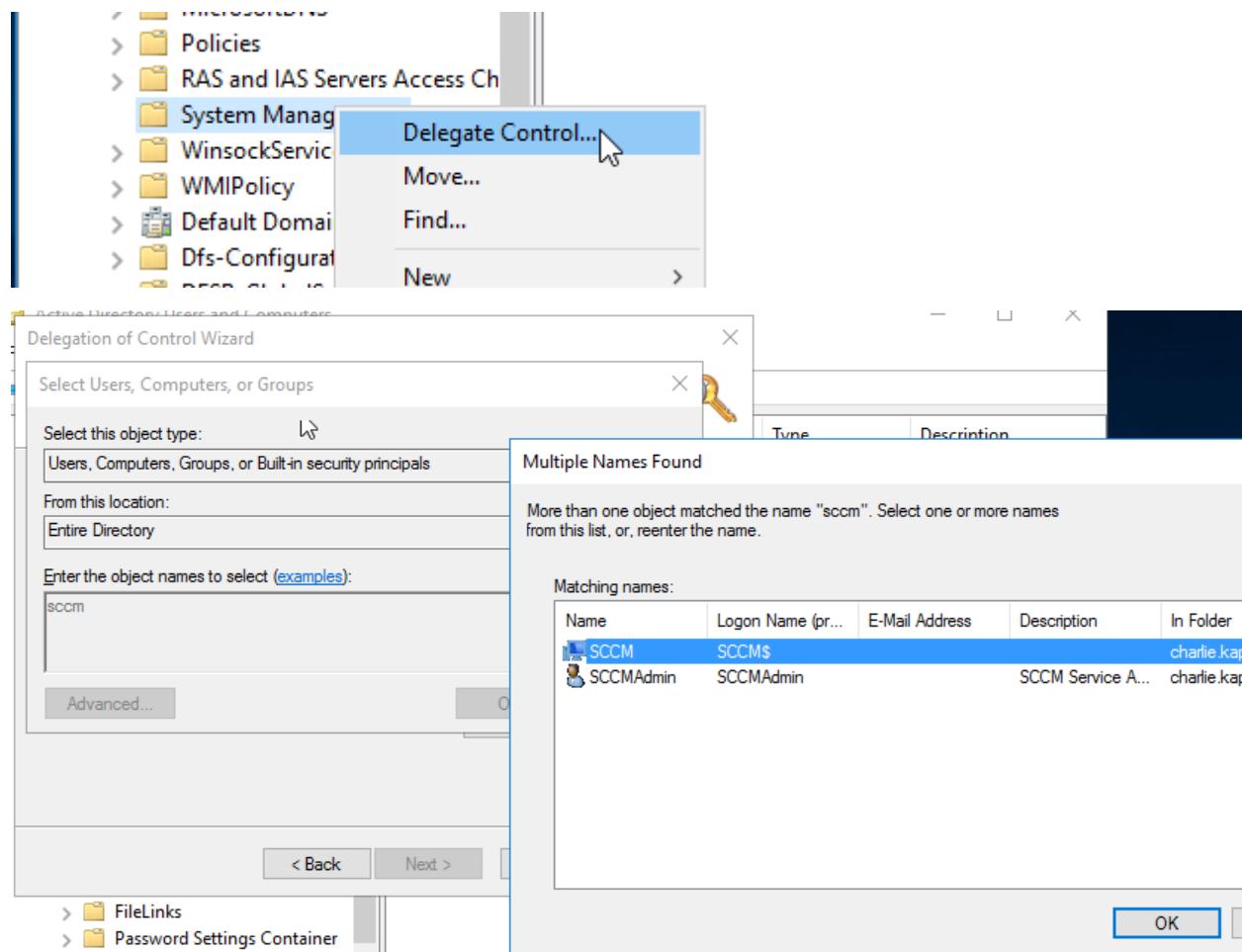


Right-click on **System Management**, select **Properties**, and then the **Security Tab**. Add the **SCCM admin** account and the **SCCM server name --- Full control**. Click **OK** to close.

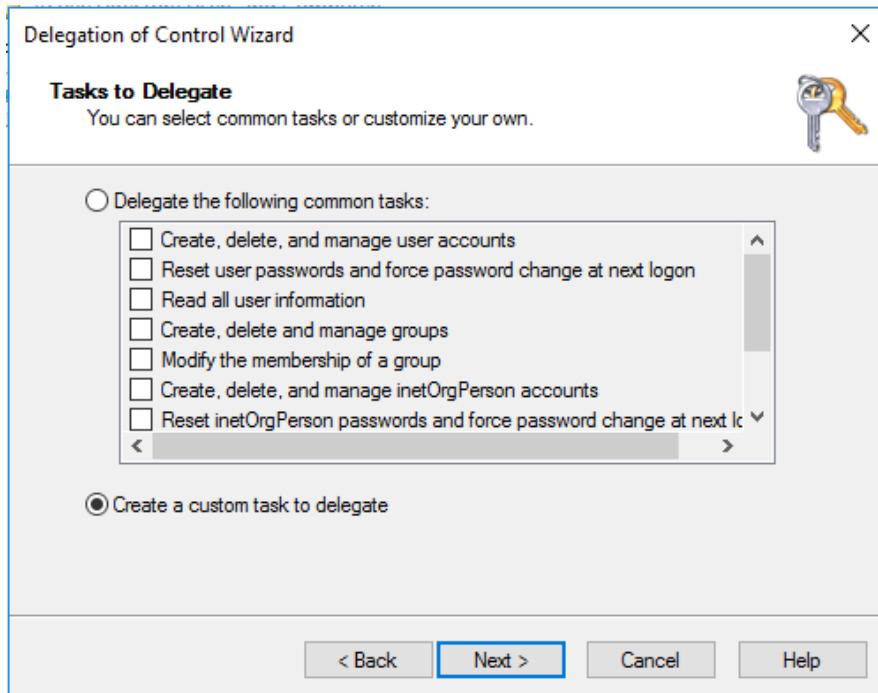


Next, **Delegate control** to the **SCCM site server** (ex: **SCCMServer**) to **System Management** container in

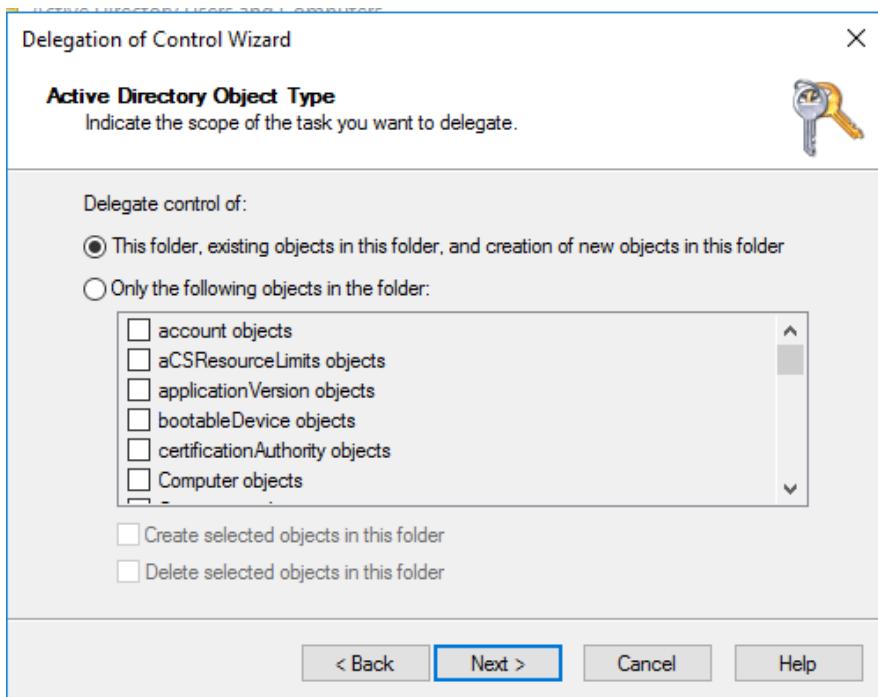
AD Users and Computers.



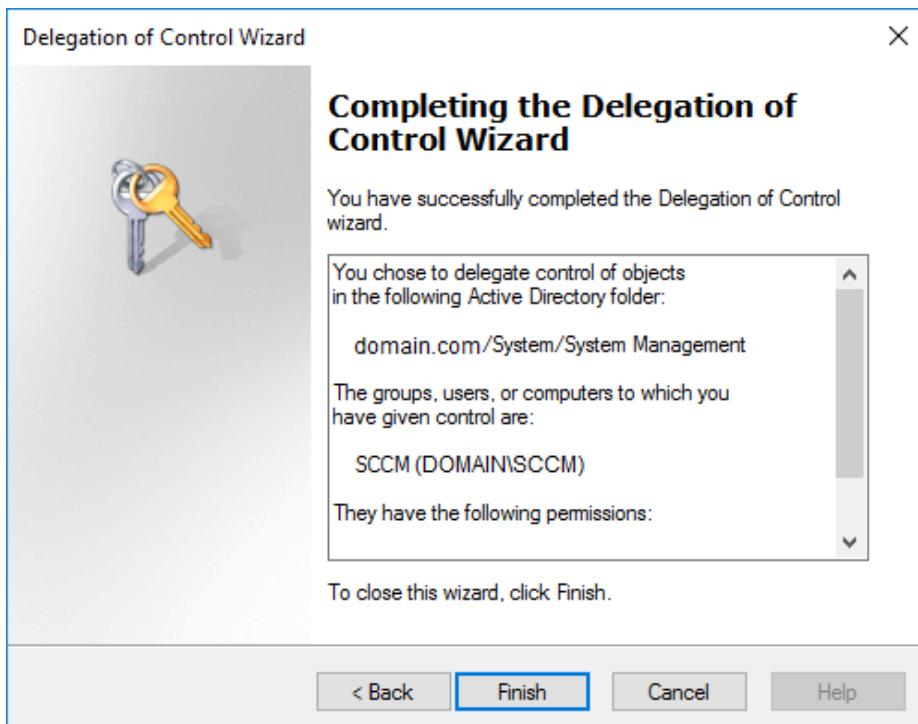
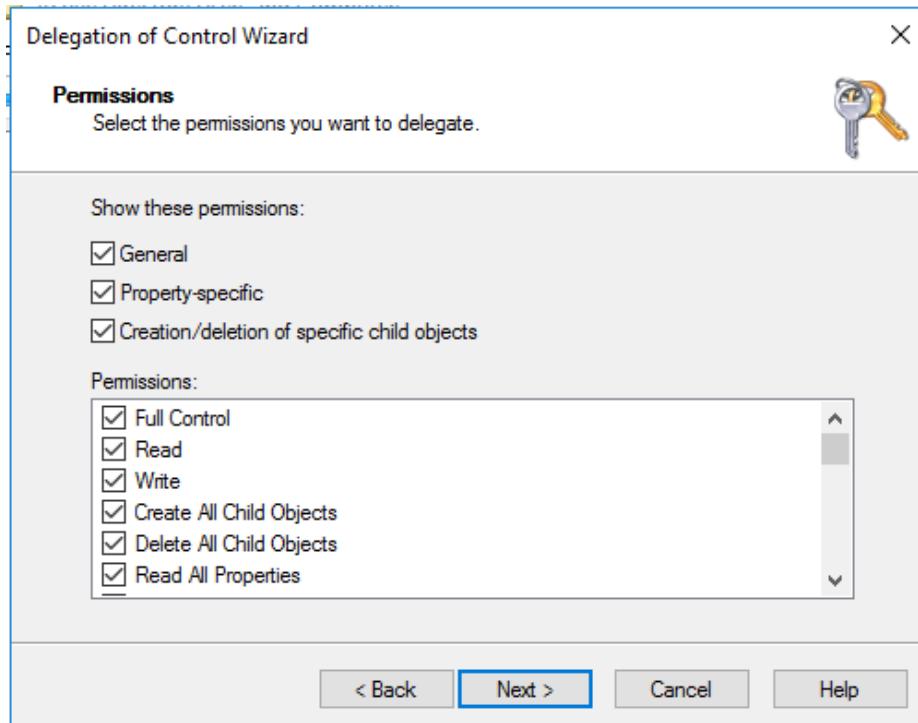
Select **Create a Custom task to delegate**. Click **Next**.



Choose **This folder, existing objects in this folder and creation of new objects in this folder**. Click **Next**.

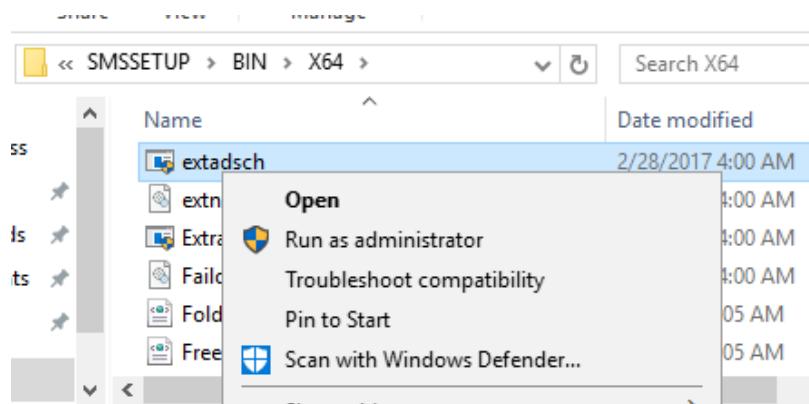


Check all Permission boxes and complete the wizard by selecting **Next**.



Extend the Schema

From the SCCM 2016 media copy the \SMSSetup\Bin\x64\ folder to a Domain Controller holding the Schema Master Role. Ensure the account used is a member of the Schema Admins group in AD, right-click the **Extadsch.exe** and choose **Run as administrator**.



A log file ExtADSch.log will be generated on the root of the C: Drive (**C:\ExtADSch.log**). Check for the entry **Successfully extended the Active Directory schema**.

```
<05-11-2017 14:24:37> Defined class cn=MS-SMS-Roaming-Boundary-Range.  
<05-11-2017 14:24:37> Successfully extended the Active Directory schema.
```

Install Site Server Prerequisites

The following roles and features need to be installed onto the SCCM Site Server prior to installation:

- **BITS (2 of 2 features)**
- **Remote Differential Compression**
- **IIS Components**
- **.Net Framework 3.5**

Add IIS Components

Common HTTP Features

Static Content

Default Document

Directory Browsing

HTTP Errors

HTTP Redirection

WebDAV Publishing

Application Development

ASP.NET 3.5 and 4.6

.NET Extensibility 3.5 and 4.6

ASP

ISAPI Extensions

ISAPI Filters

Health and Diagnostics

HTTP Logging

Custom Logging

Logging tools

Request Monitor

Tracing

Security

Request Filtering

Basic Authentication

Client Certificate Mapping Authentication

URL Authorization

IP and Domain Restrictions

Windows Authentication

Performance

Static Content Compression

Management Tools

IIS Management Console

IIS Management Scripts and Tools

Management Service

IIS 6 Management Compatibility

IIS 6 Metabase Compatibility

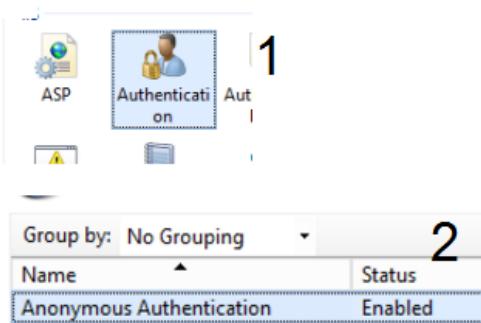
IIS 6 WMI Compatibility

IIS 6 Scripting Tools

IIS 6 Management Console

Configure IIS

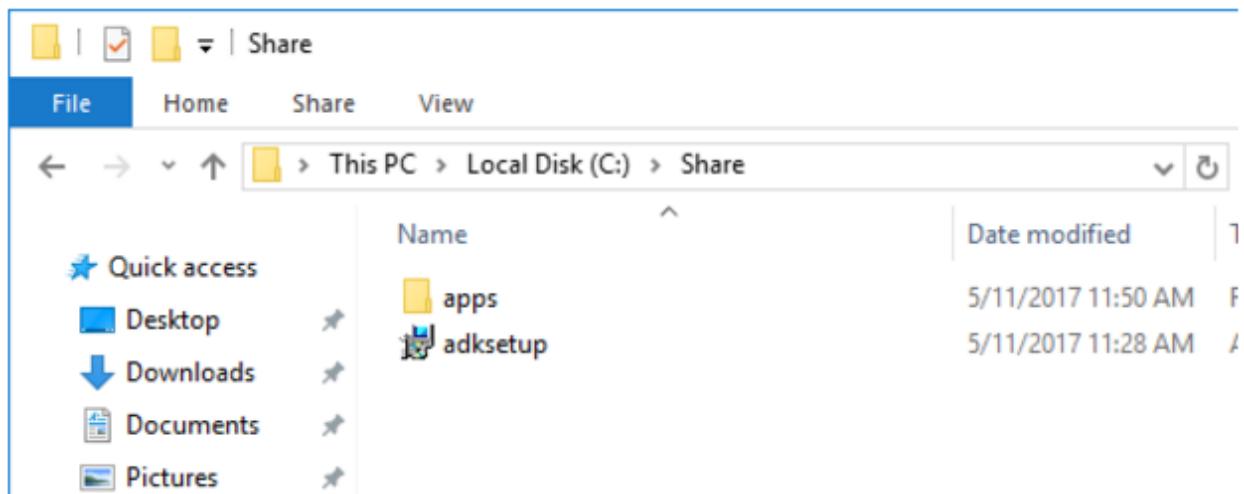
Launch IIS from Server Manager Dashboard. Select **Default Web Site**, select **Authentication**, and make sure **Anonymous Authentication** is set to **Enabled**.



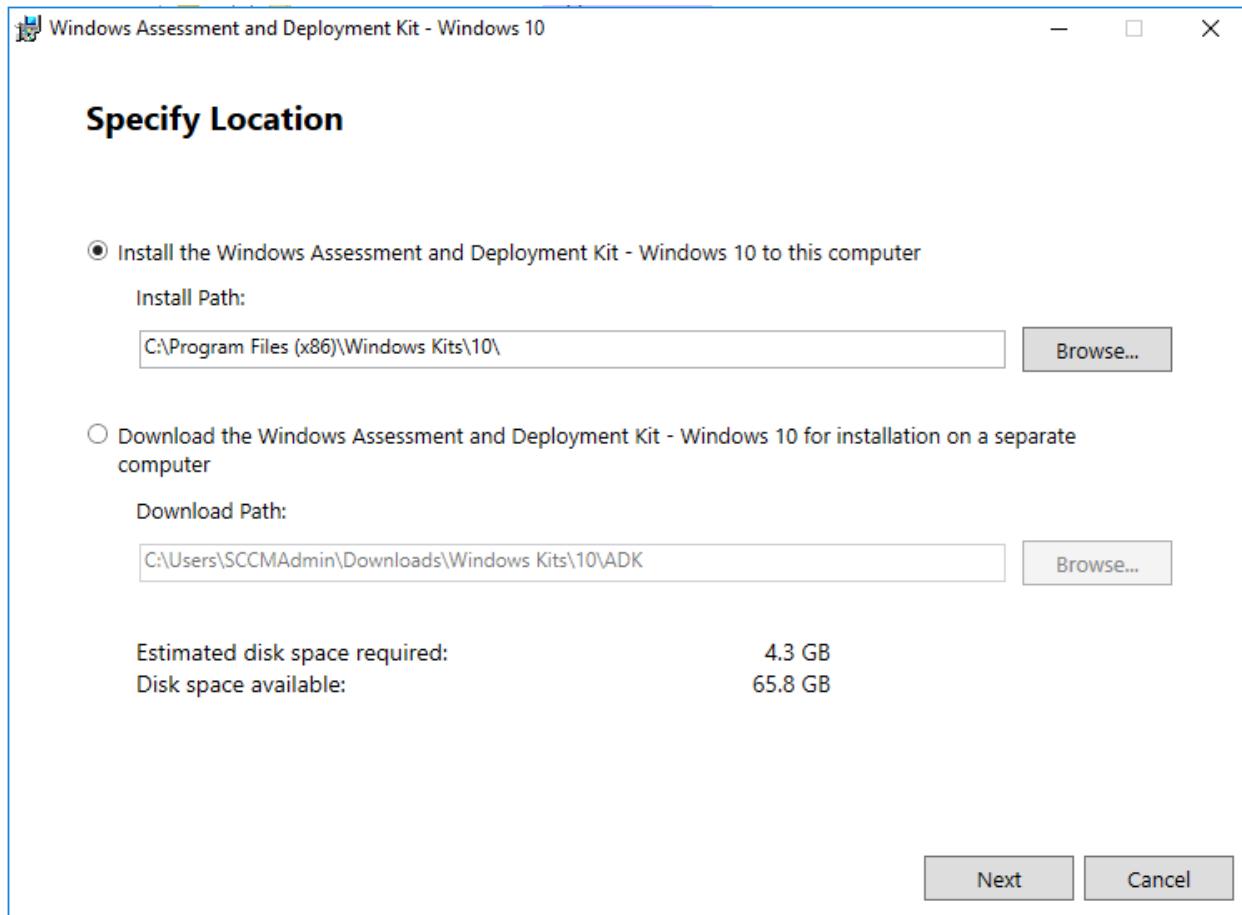
Install Windows Assessment and Deployment Kit (Windows ADK) for Windows 10

Access the ADK source files you downloaded. You may have to mount the ISO to view the files.

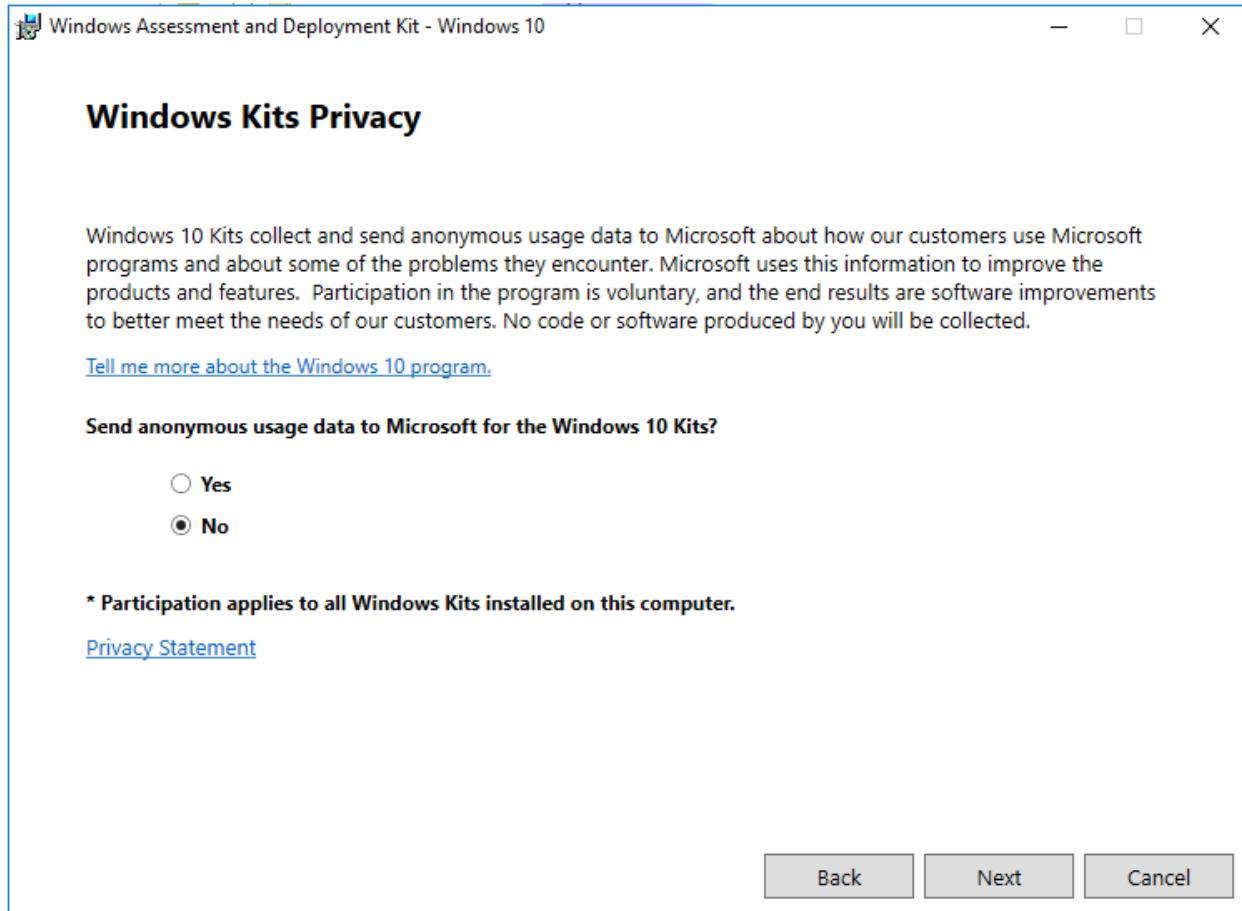
Run the **adksetup.exe** file.



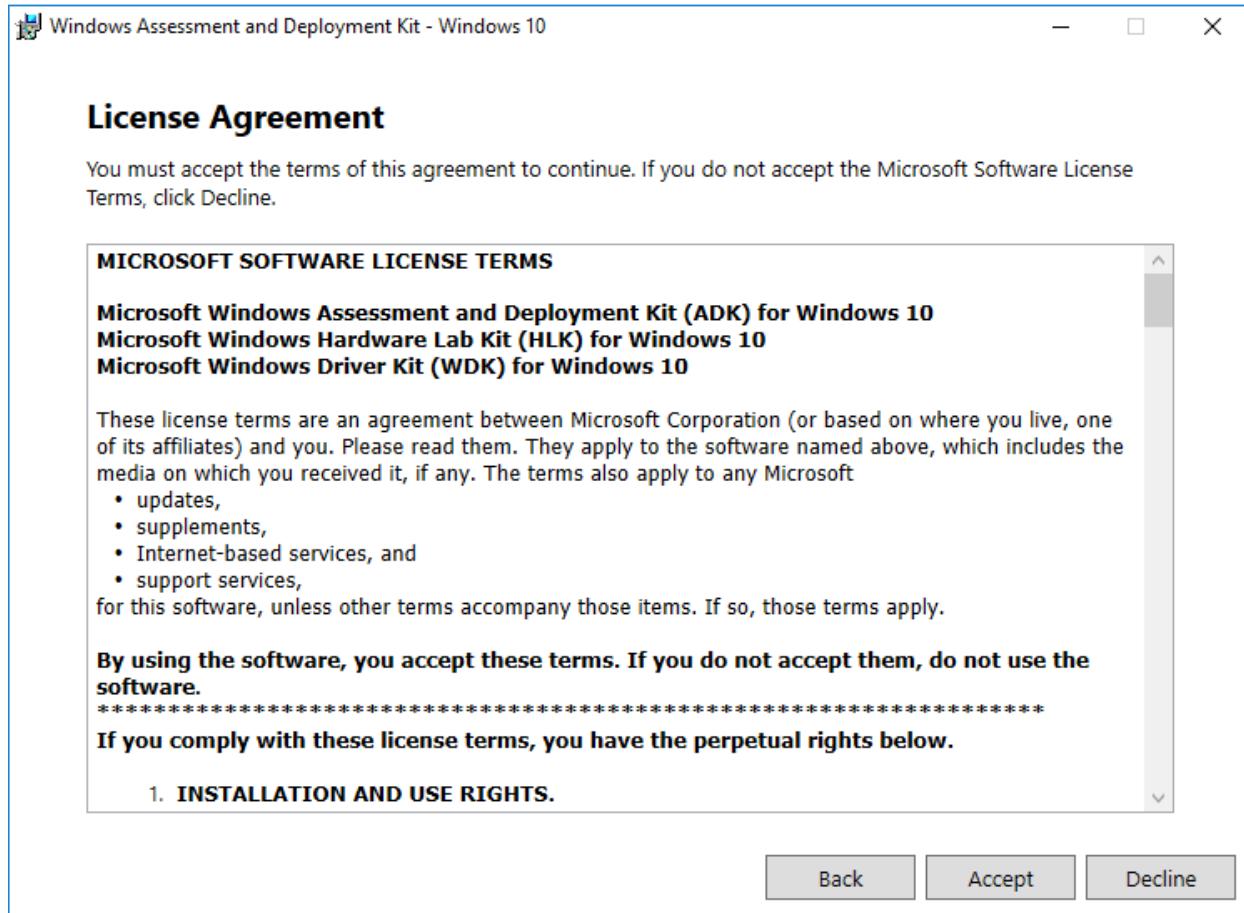
Use the default location for installation and click **Next**.



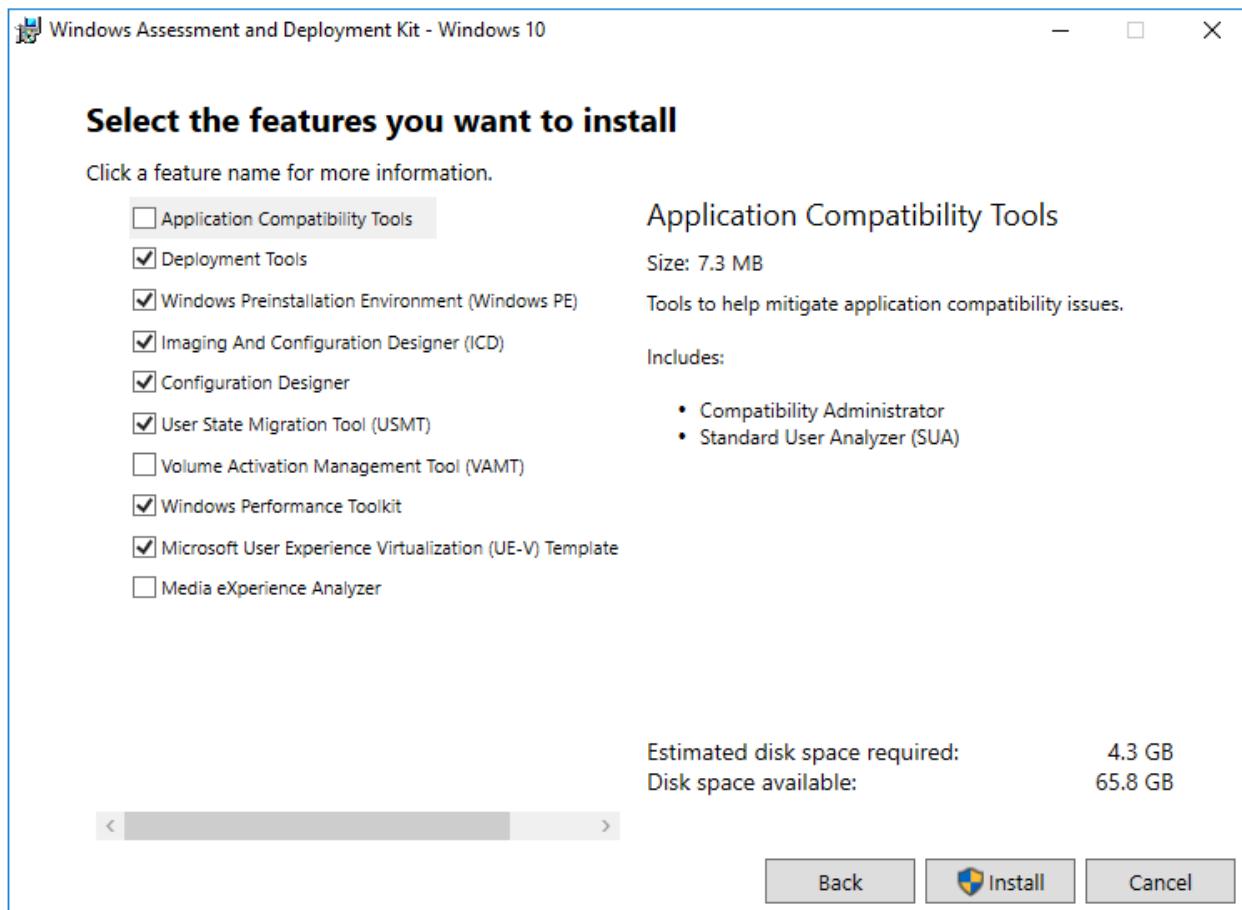
Select whether to join the CEIP and click **Next**.

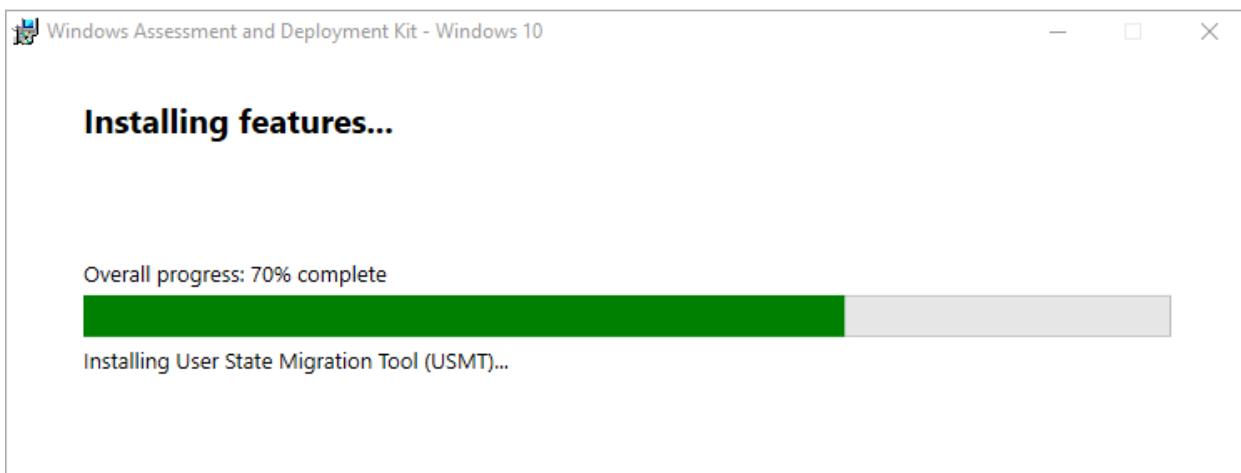
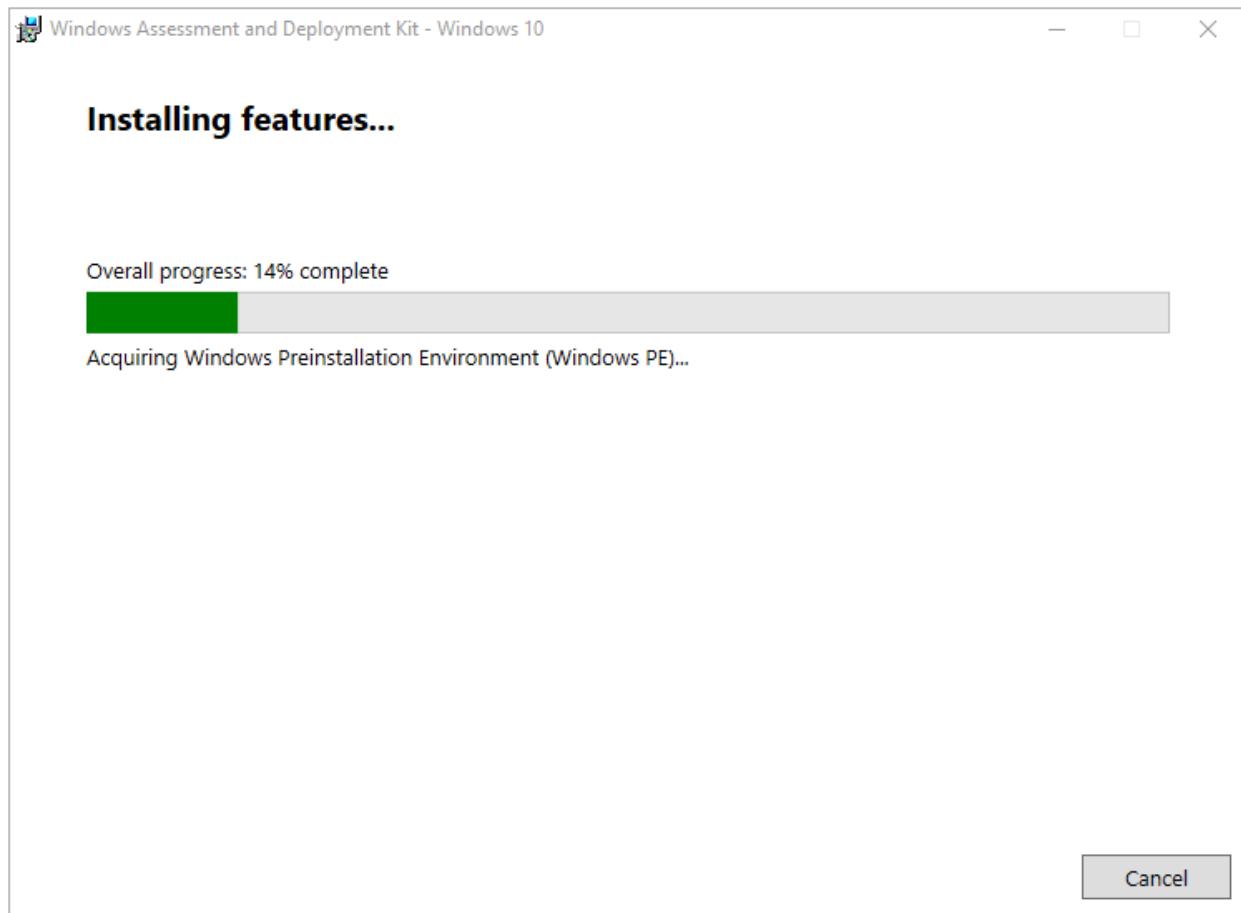


Accept the license agreement.

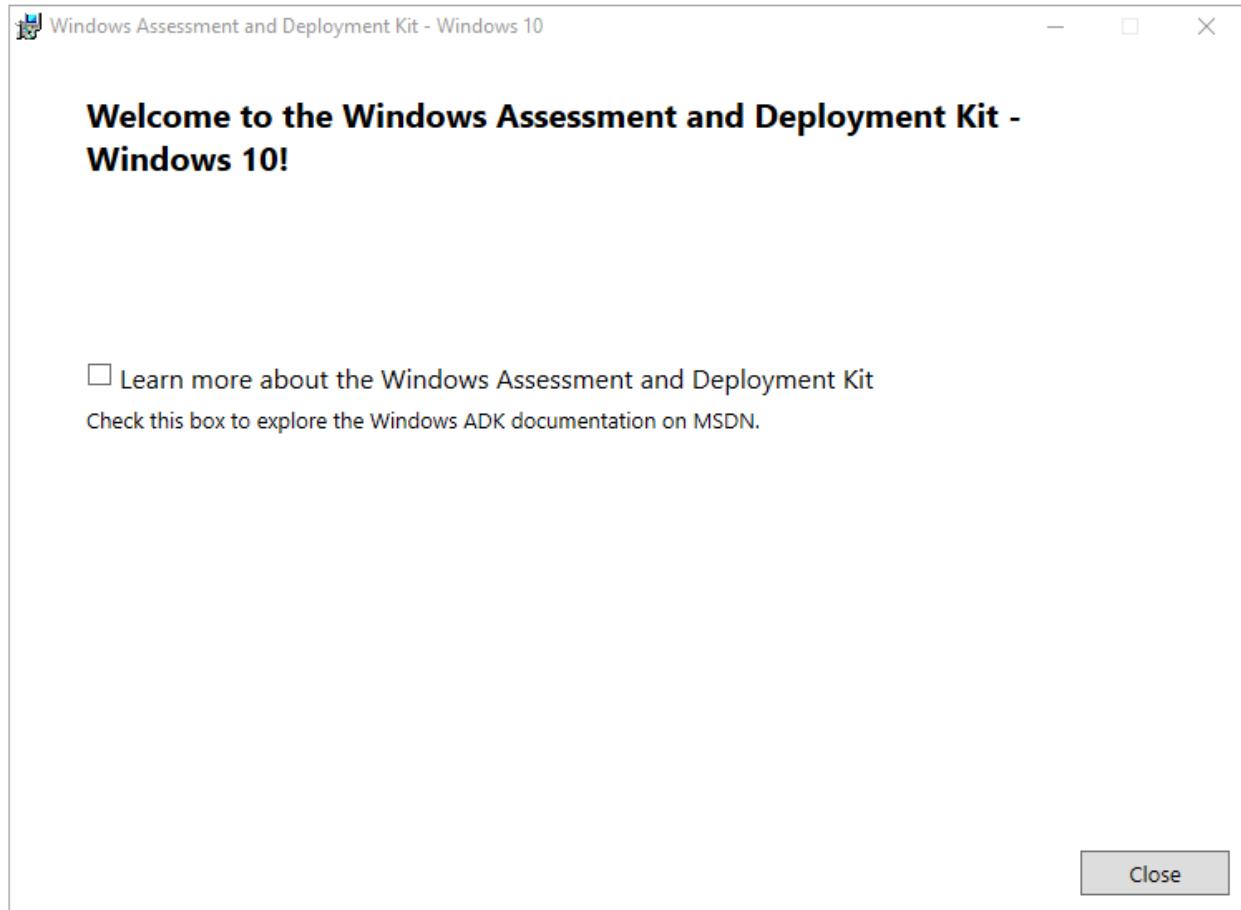


Install the following **Features** and then click **Install**.





Once complete, click **Close**.



Install SQL Server

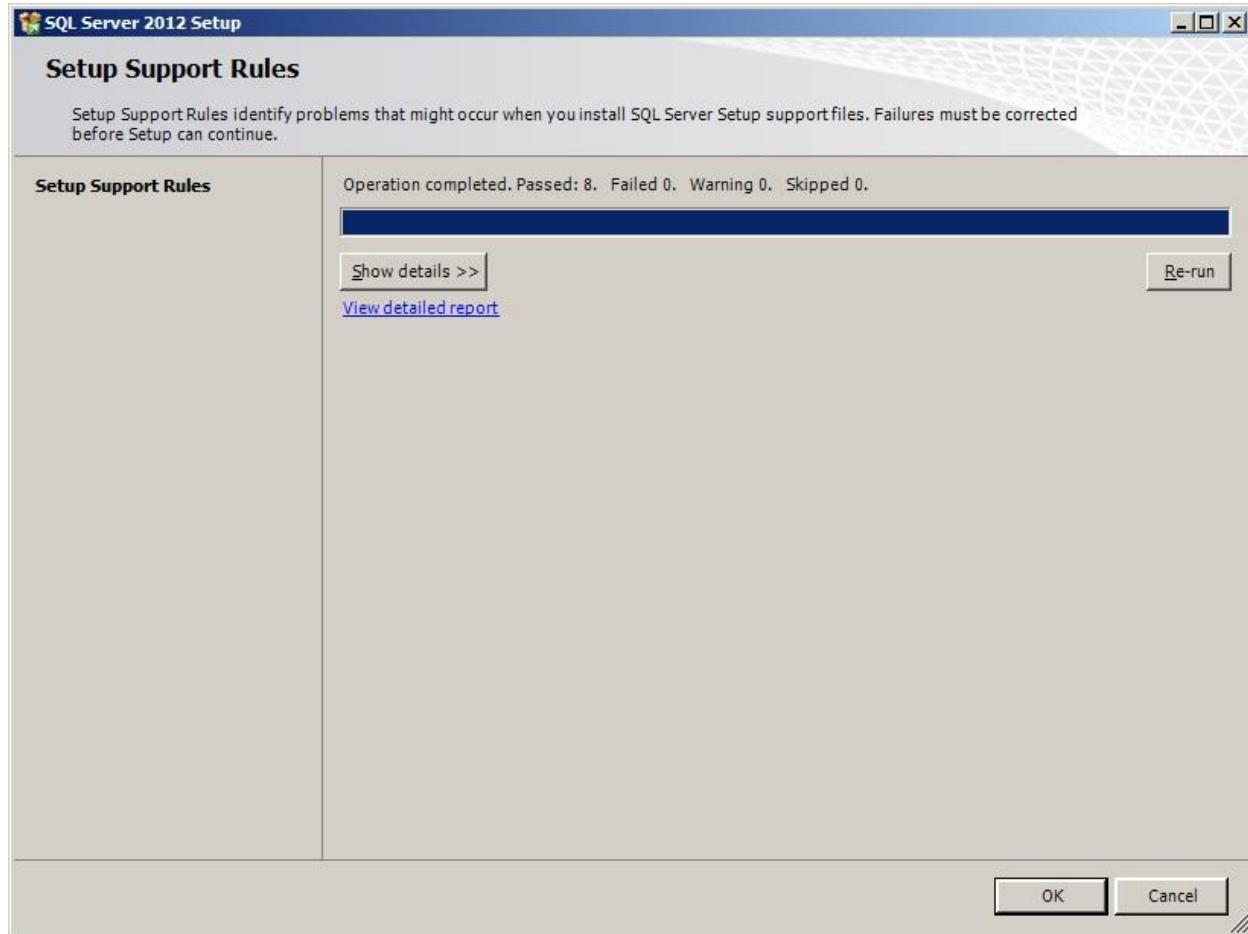
SQL Server 2012 SP1 is being installed as the SCCM database. Note, I needed SP3 for SCCM 1606+; going to SQL 2016, I did not need the patches. Run the **setup.exe** (I have included the 2012 and 2016 snapshots).

SQL 2012 Installation

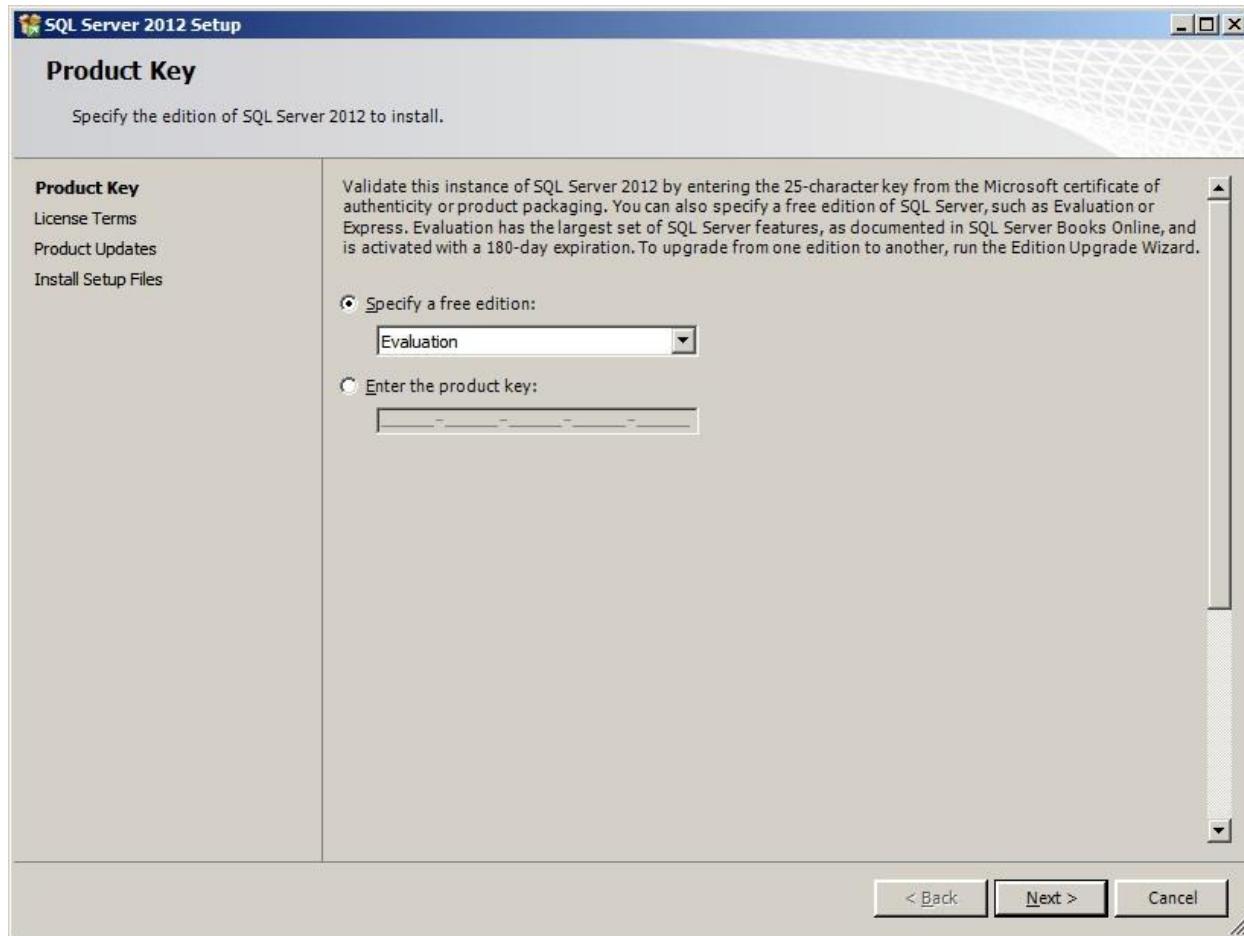
Select **New SQL Server stand-alone installation.**



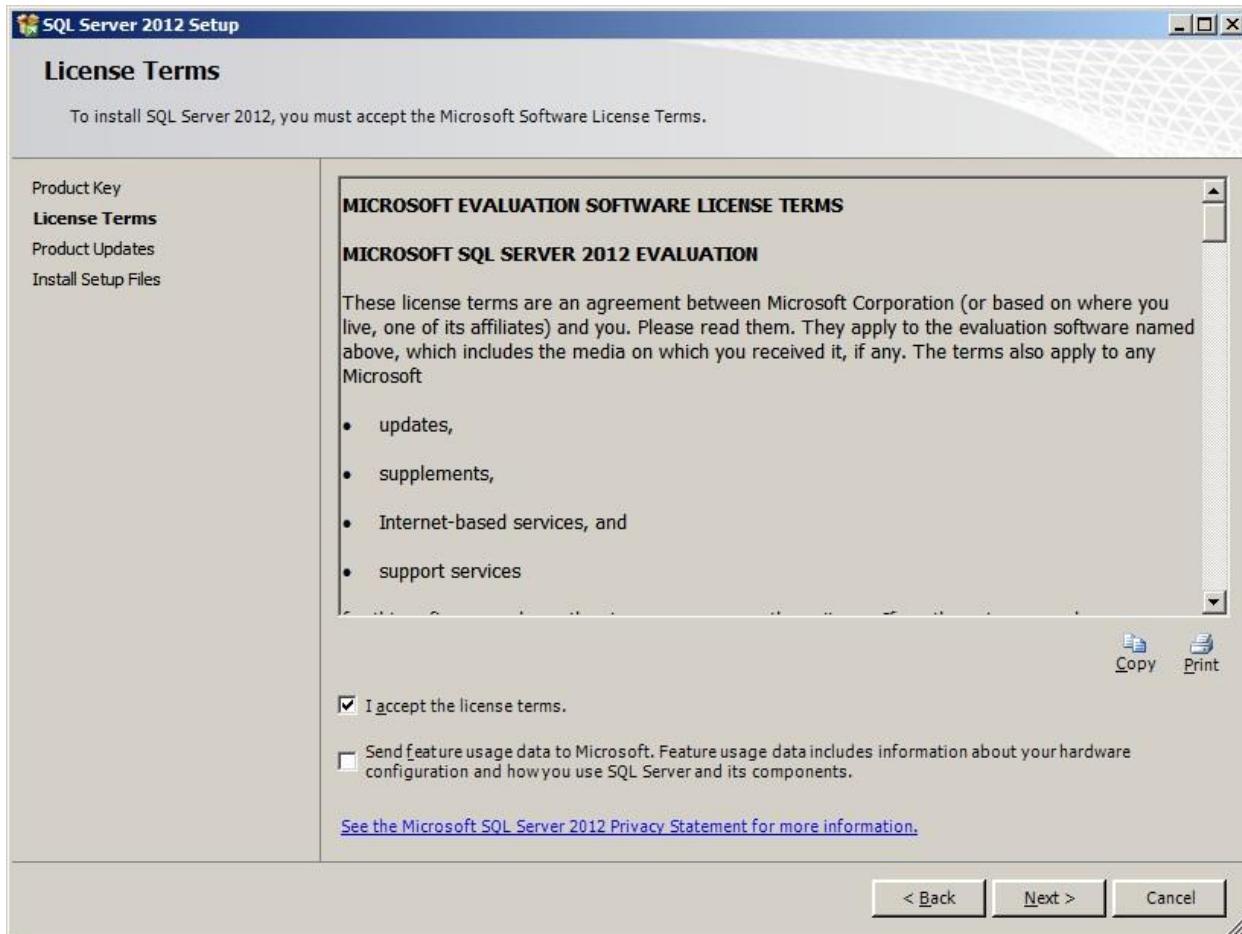
Click **OK**.



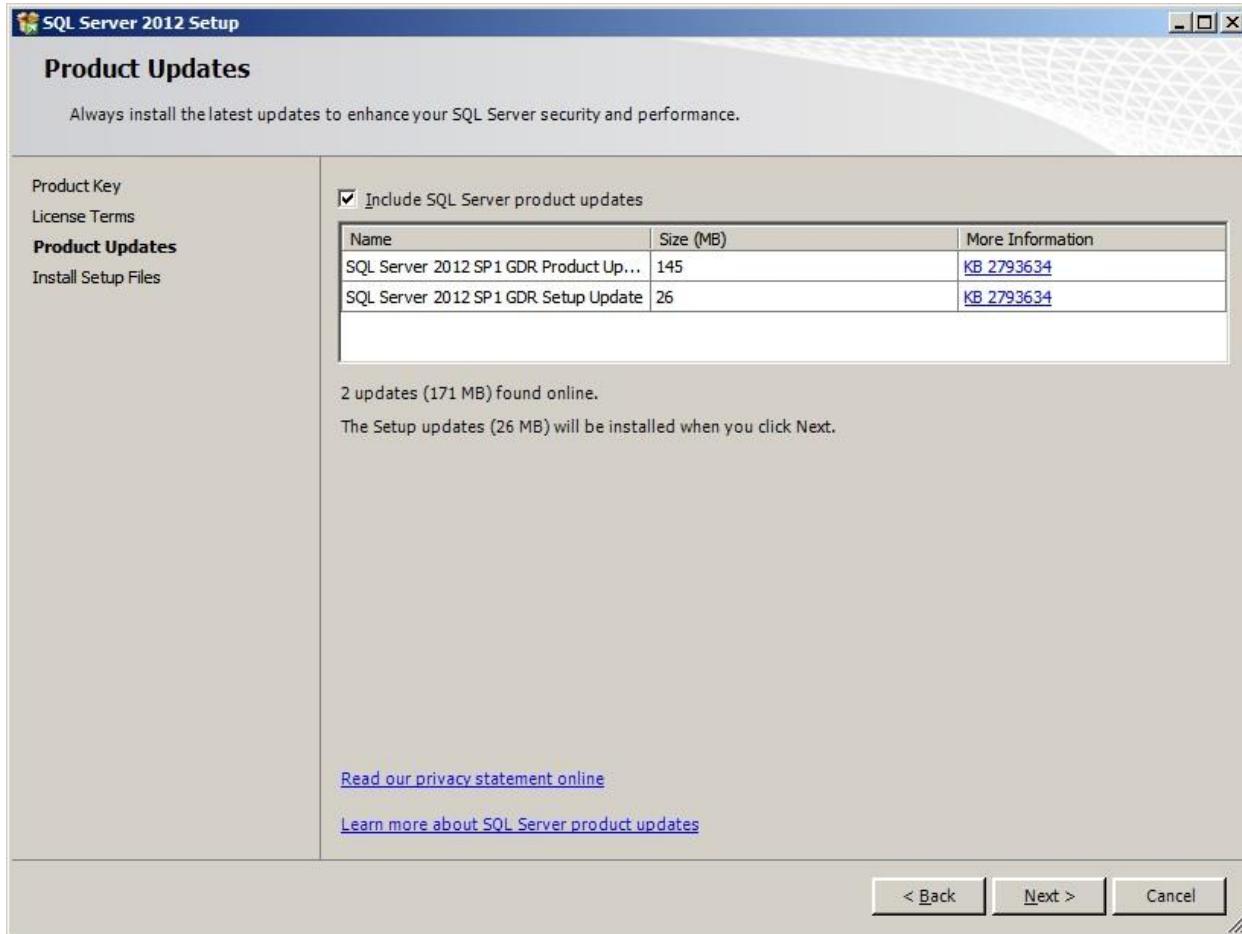
Install the product key or run in evaluation mode. Click **Next**.



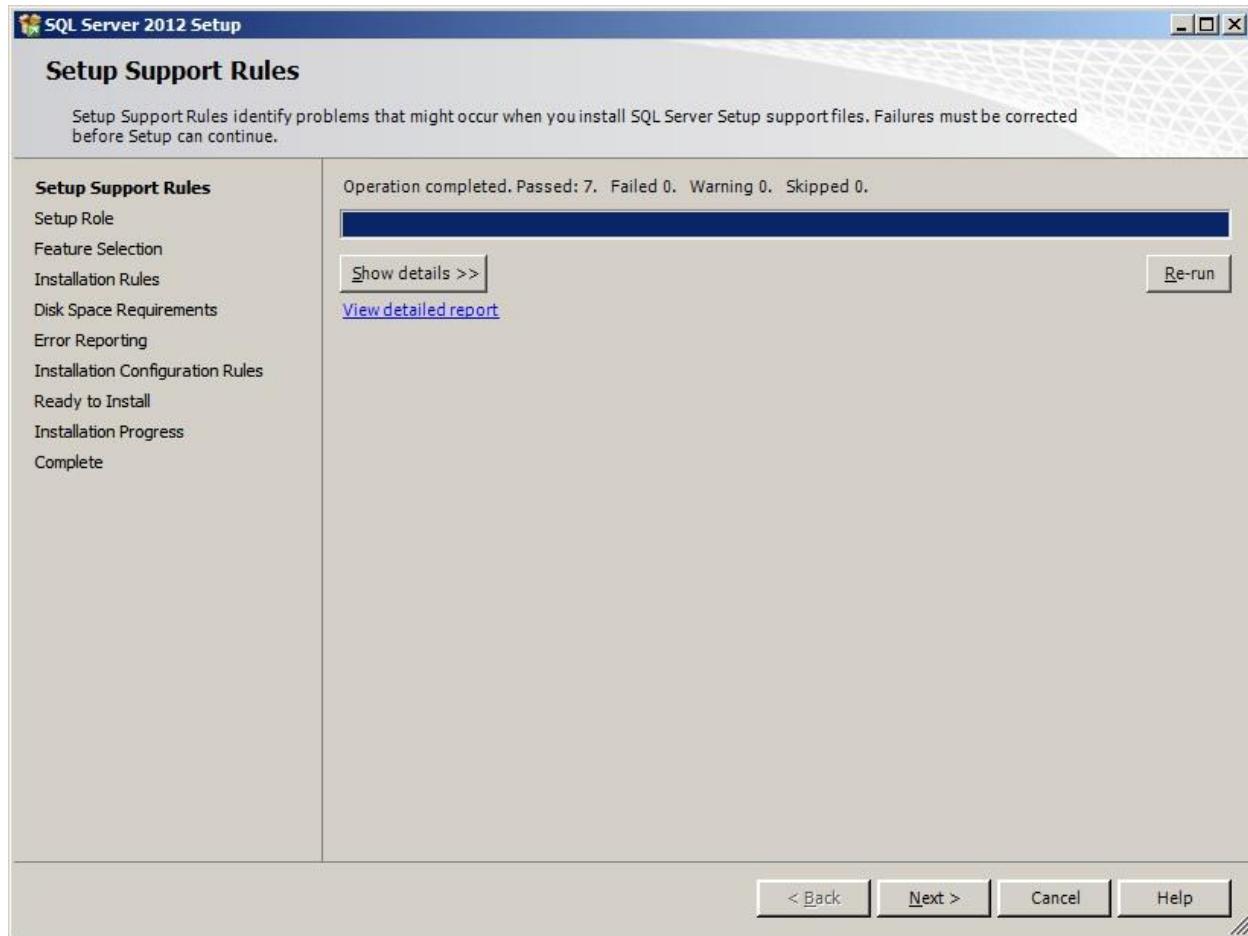
Accept the license agreement and click **Next**.



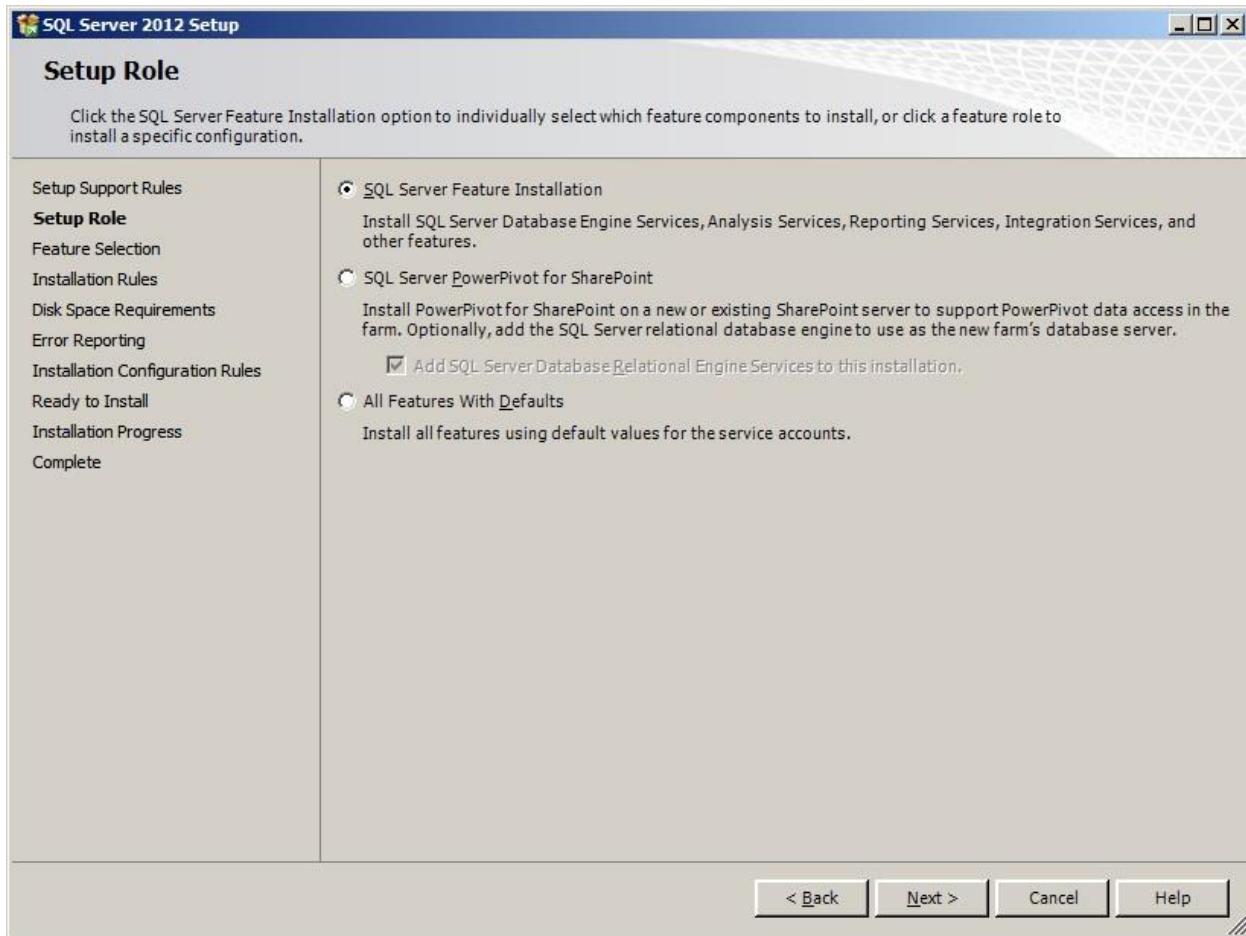
Include any product updates. Click **Next**.



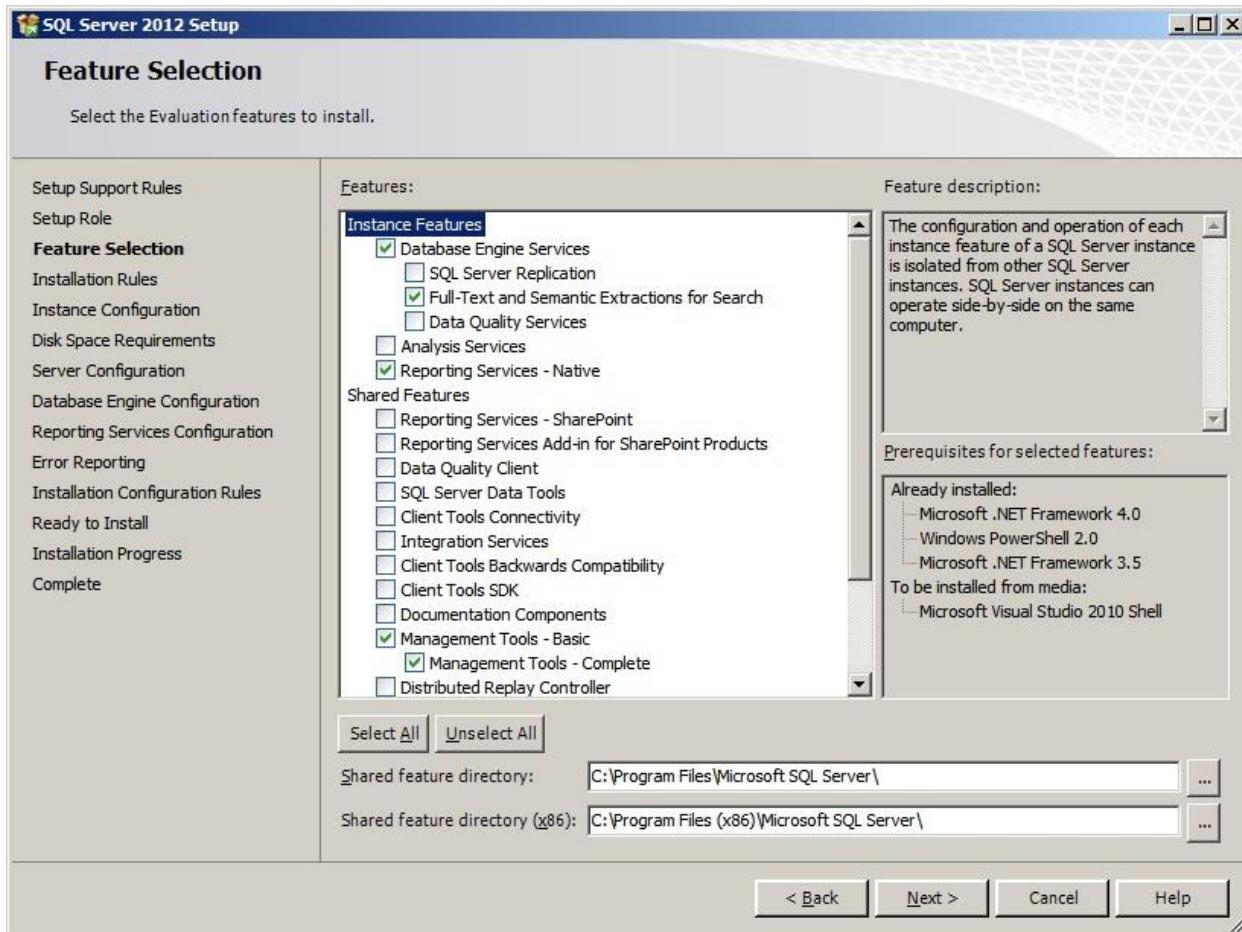
Click **Next**.



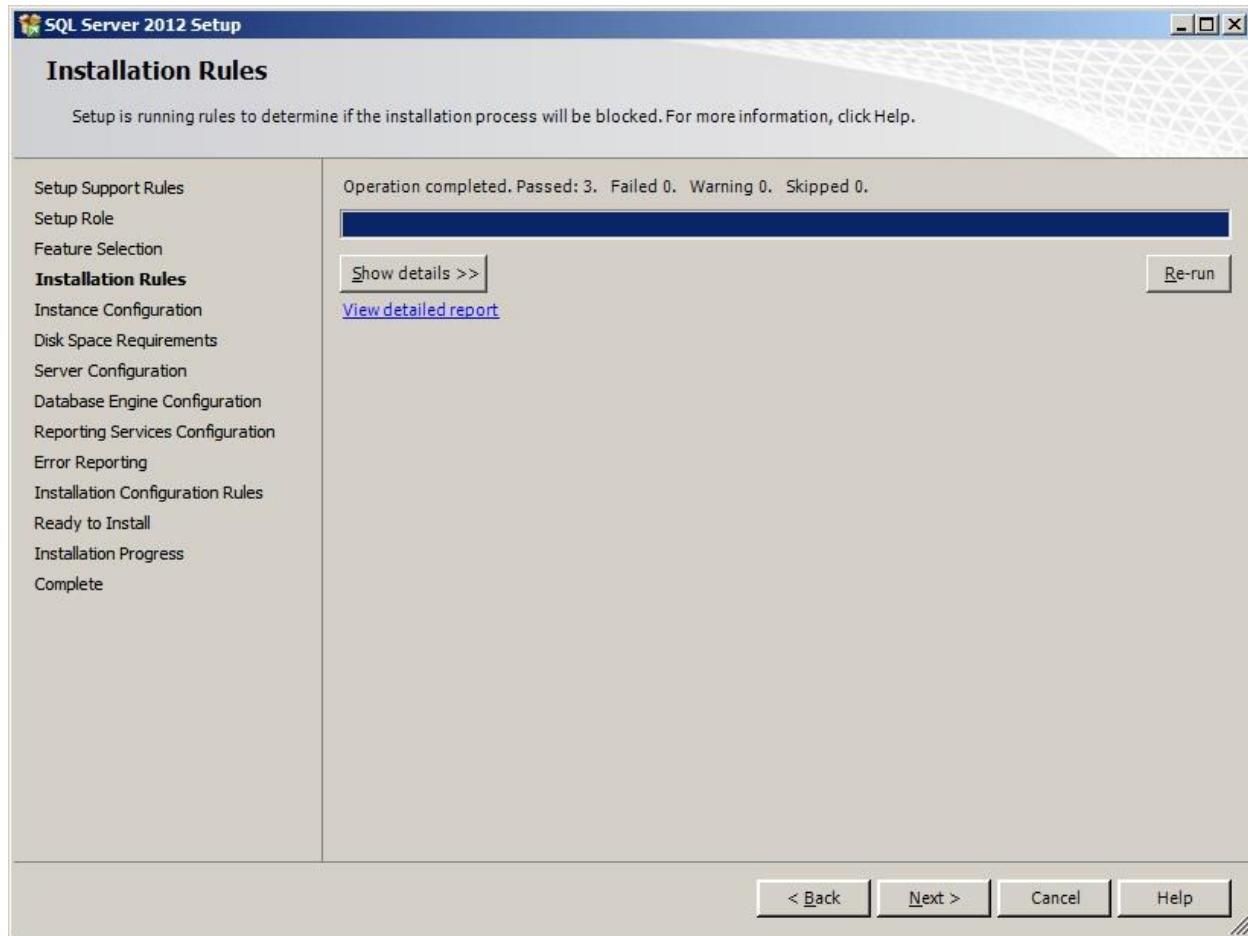
Choose the **SQL Server Feature Installation** and click **Next**.



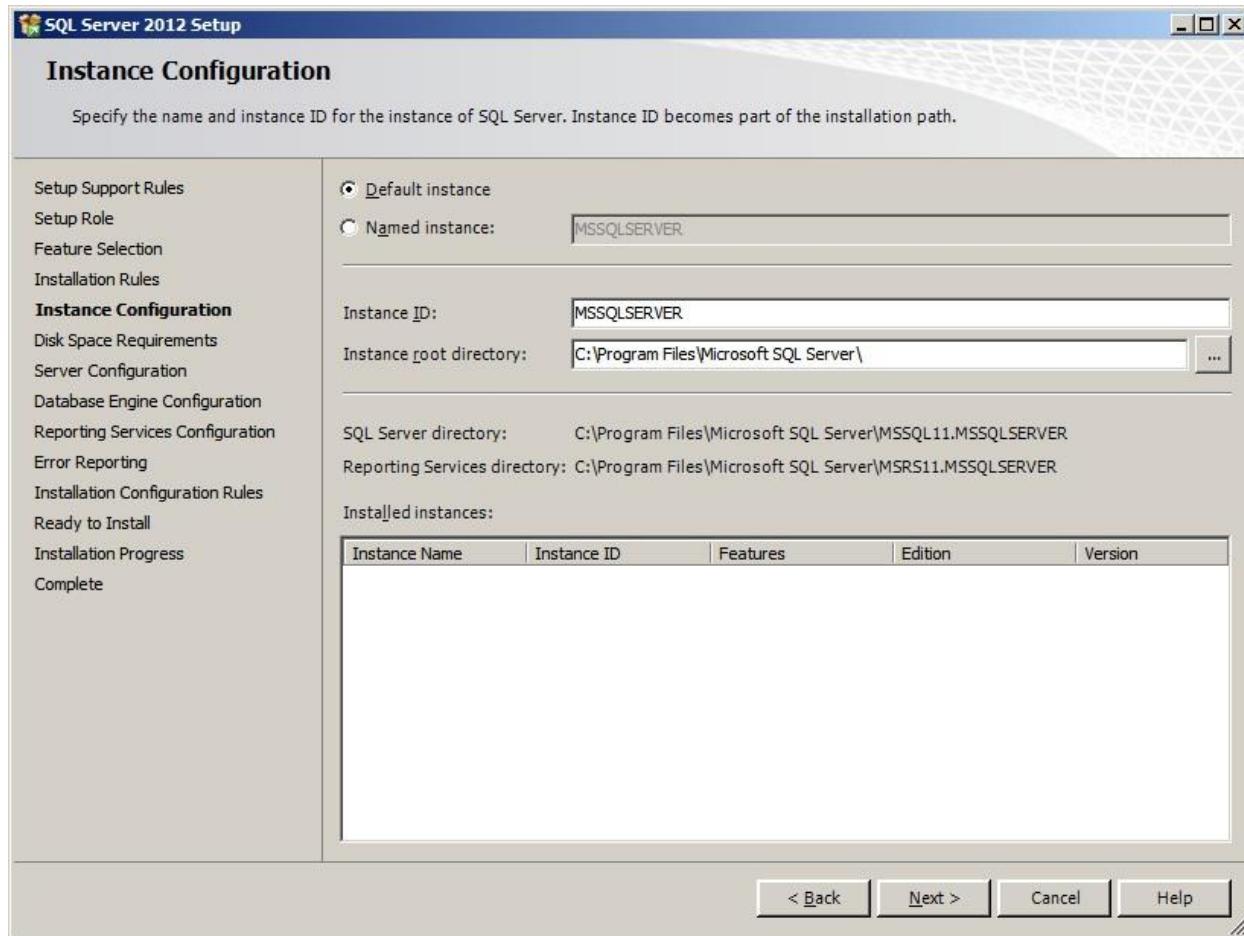
Install the **selected** features and click **Next**.



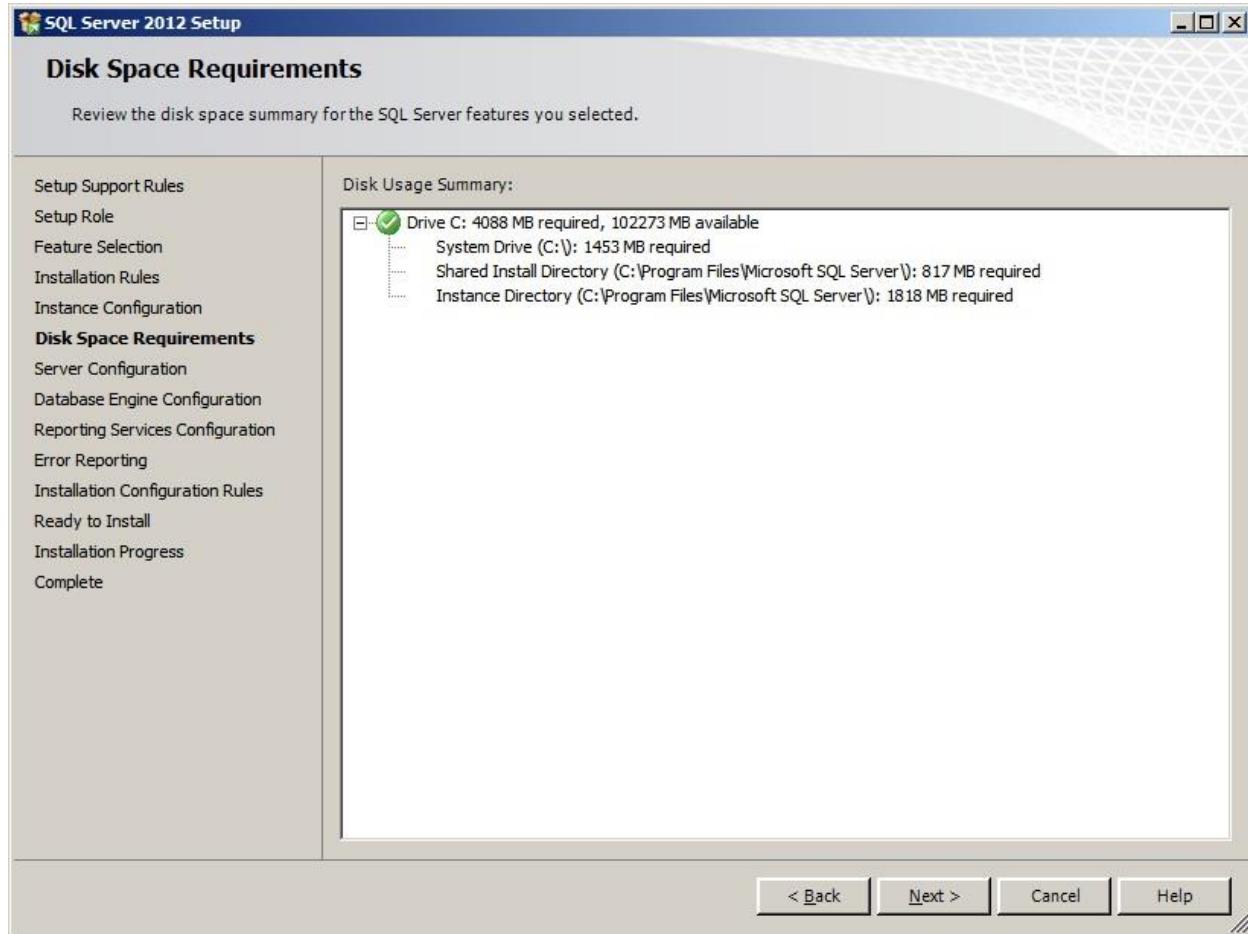
Click **Next**.



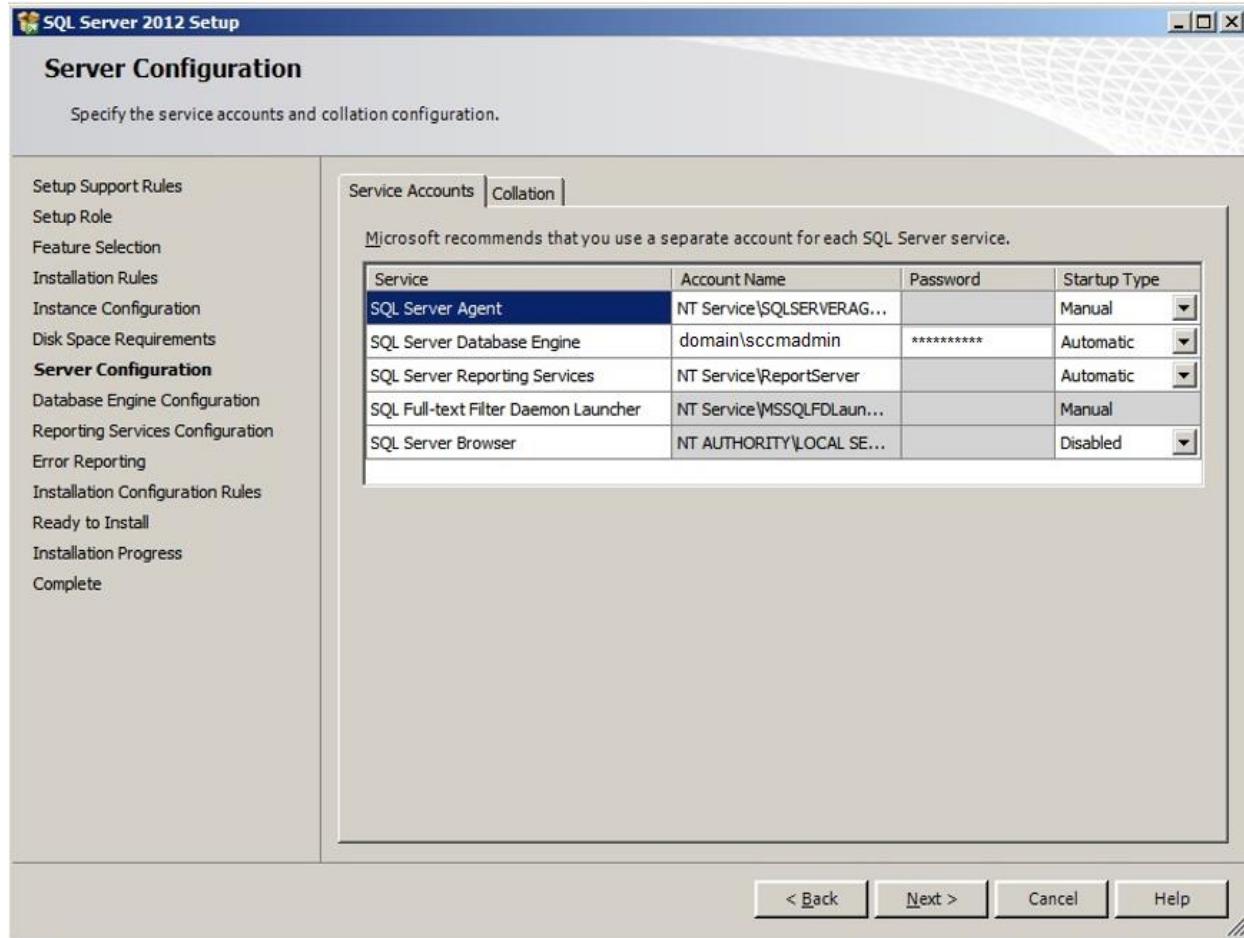
Leave as the **default** instance and click **Next**.



Click **Next** at the disk space requirements screen.

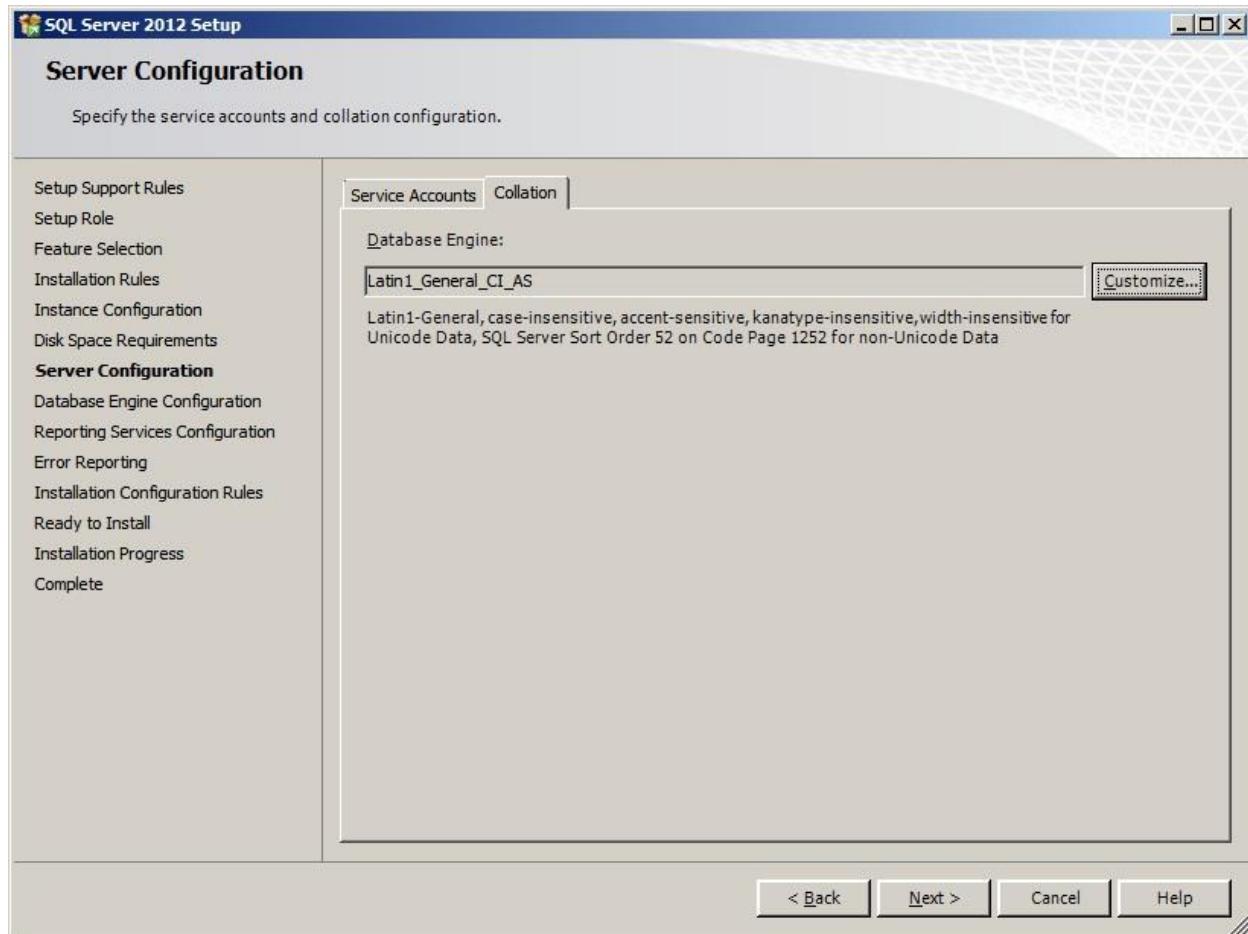


Select the accounts to run the SQL services, in this instance the defaults have been selected – then configure the **SQL Server Database Engine** to use the **SCCM service account** (this must be a domain account). Once confirmed, click the **Collation tab**.



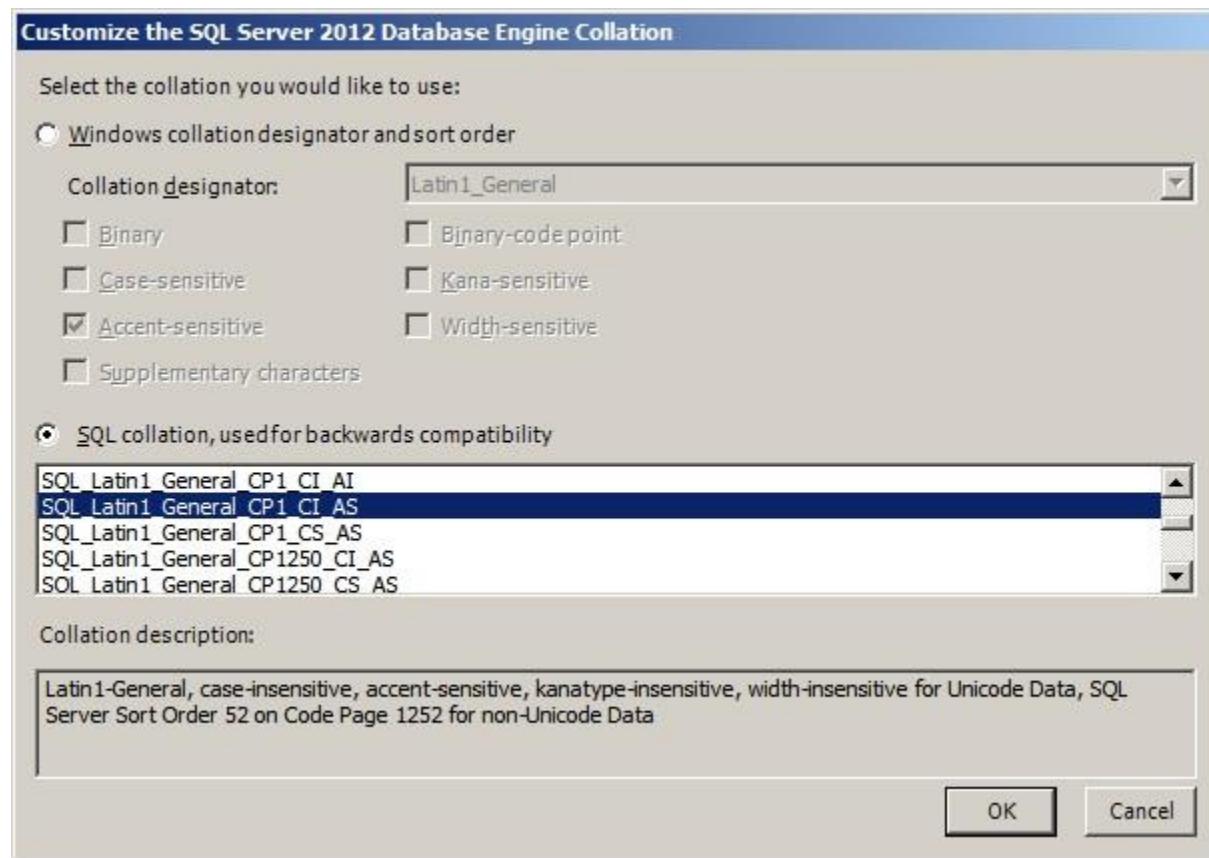
Note: If you're having SQL issues, ones that are privilege related, just use the SCCMAdmin account for the top three services, and set service startup type to Automatic.

Click the **Customize** button.

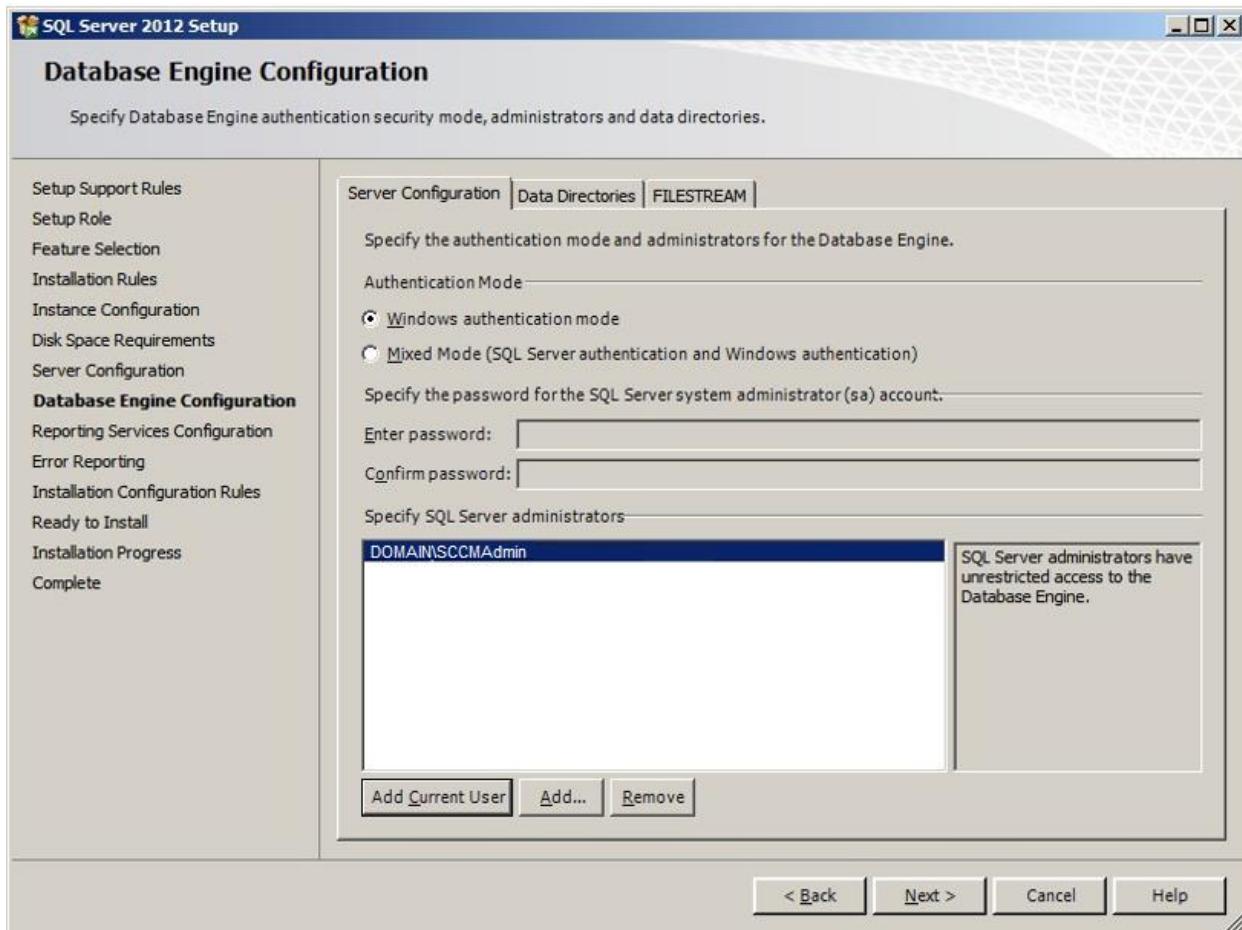


Choose the **SQL Collation, used for backwards compatibility** option and select

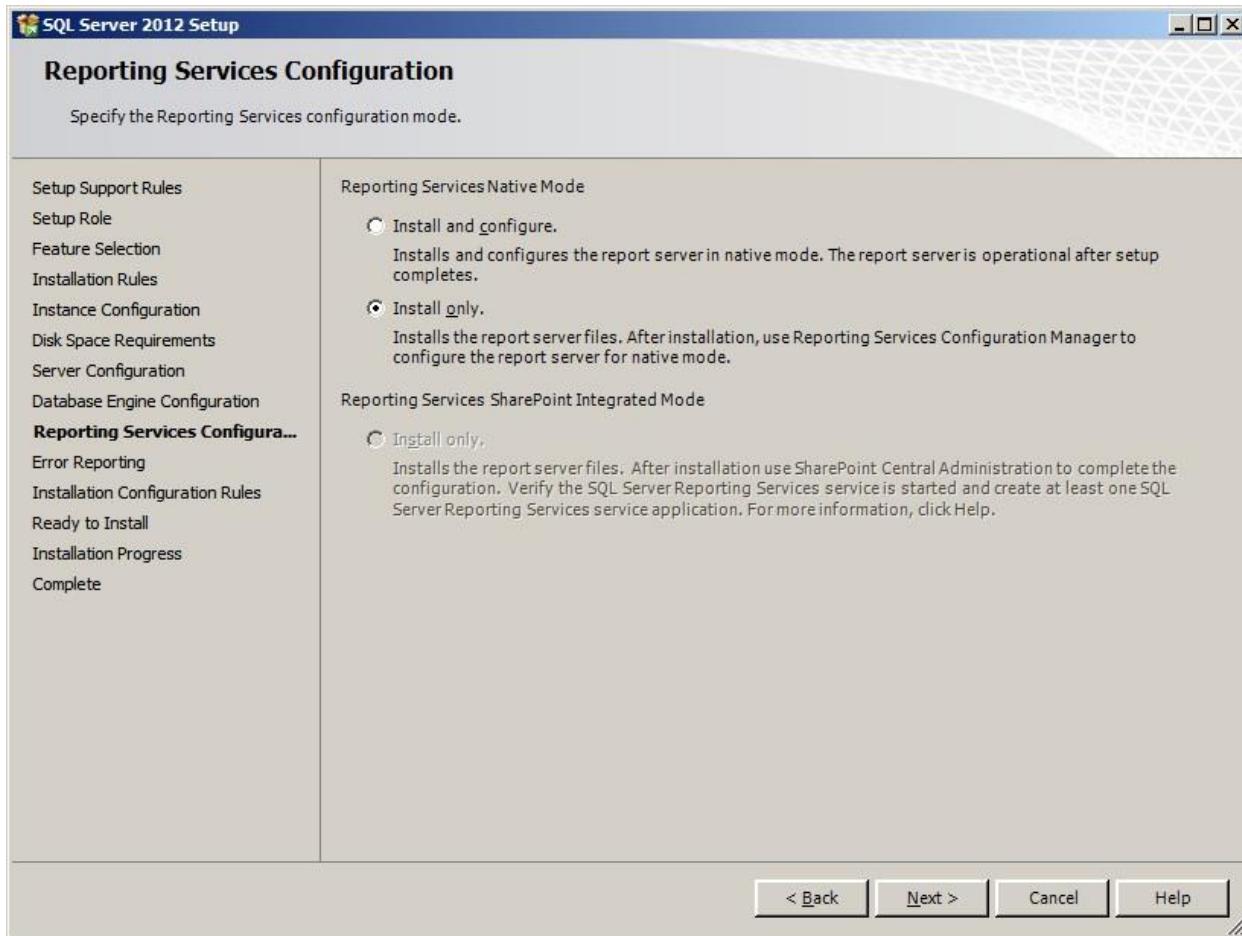
SQL_Latin1_General_CI_AS. Click **OK**. Click **Next**.



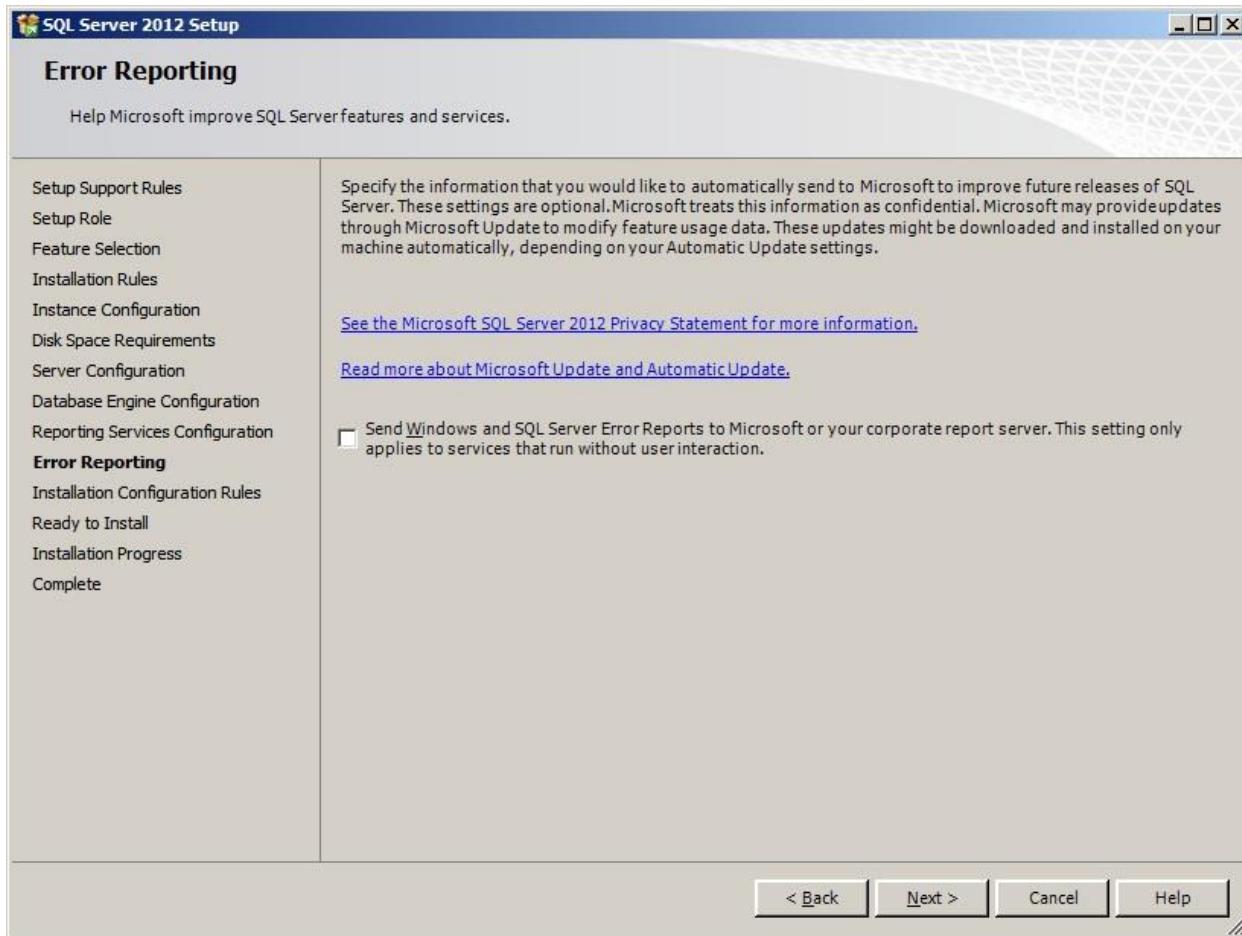
Use Windows authentication and Add the current user. Click Next.



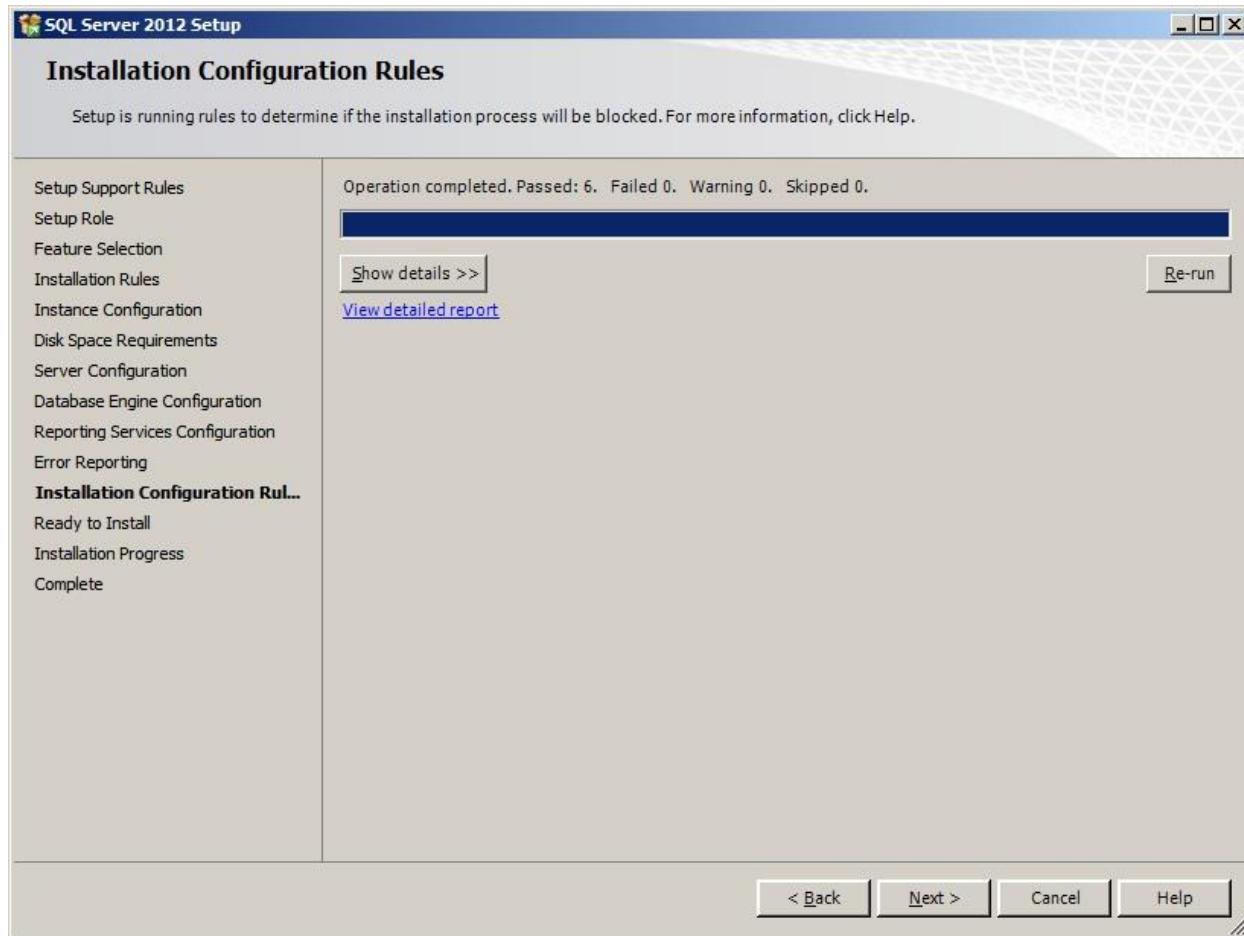
Set Reporting Services to **Install only**. Click **Next**.



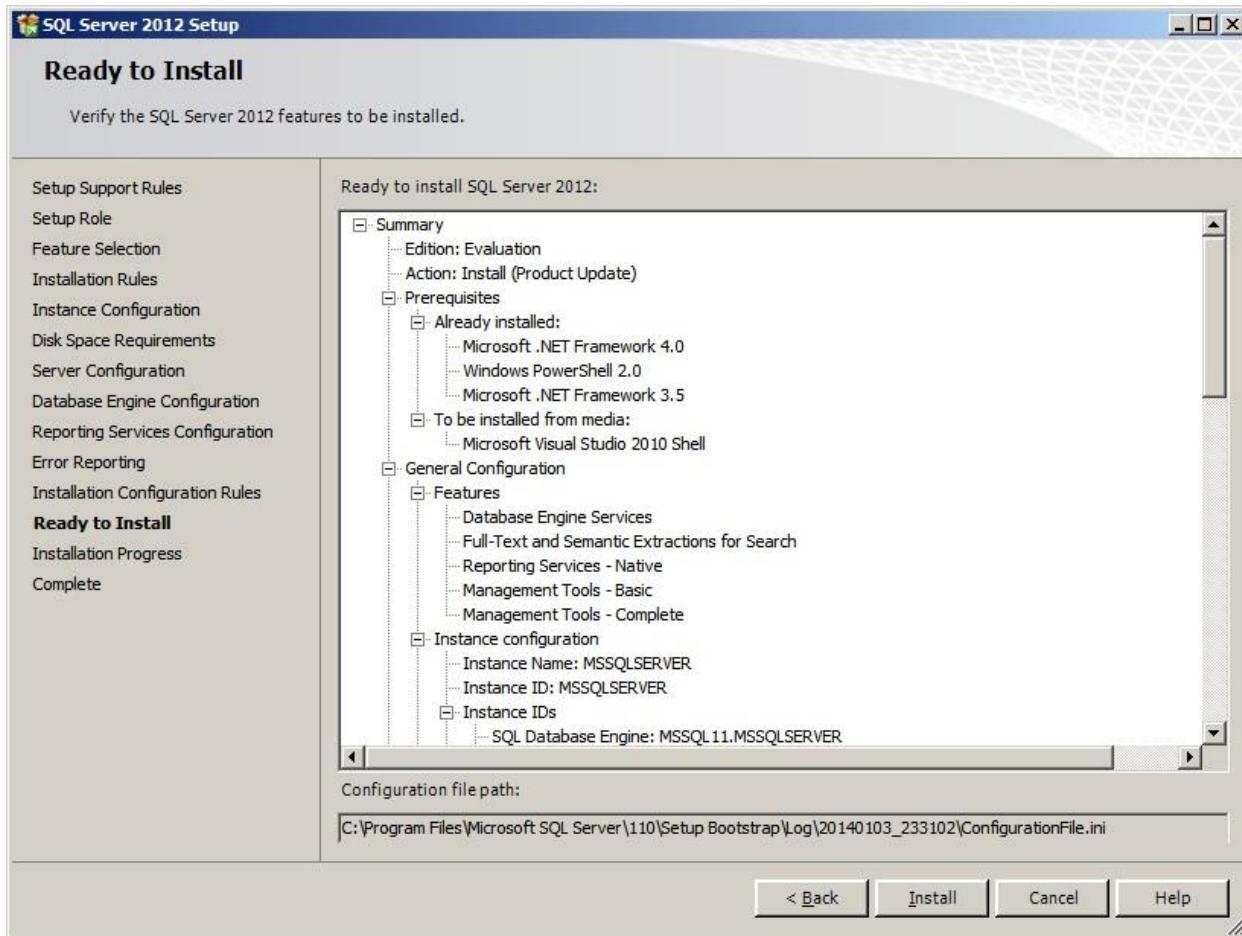
Set error reporting preferences and click **Next**.



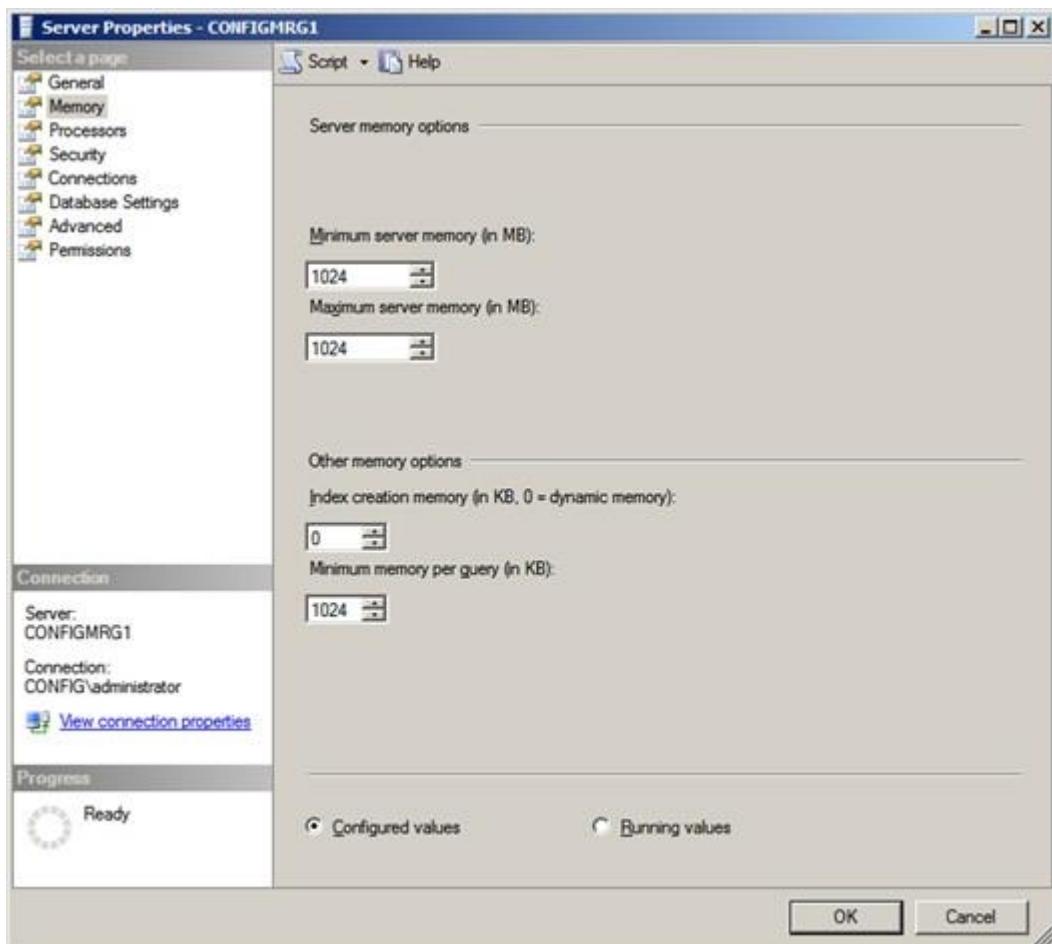
Click **Next**.



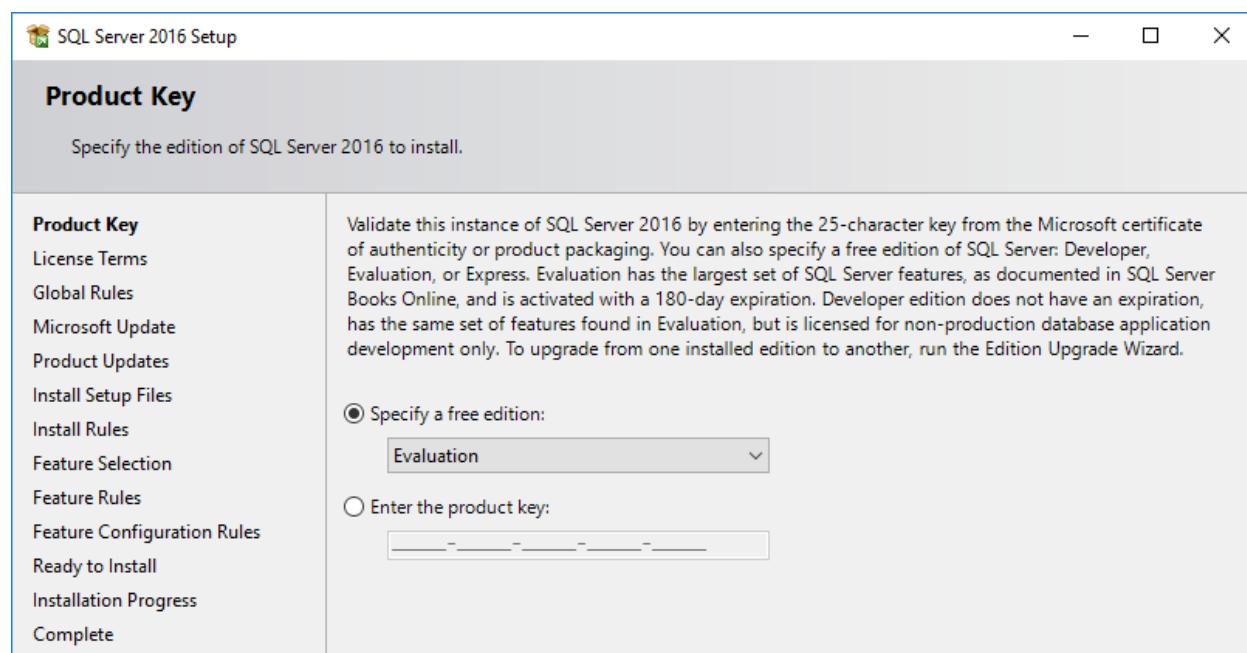
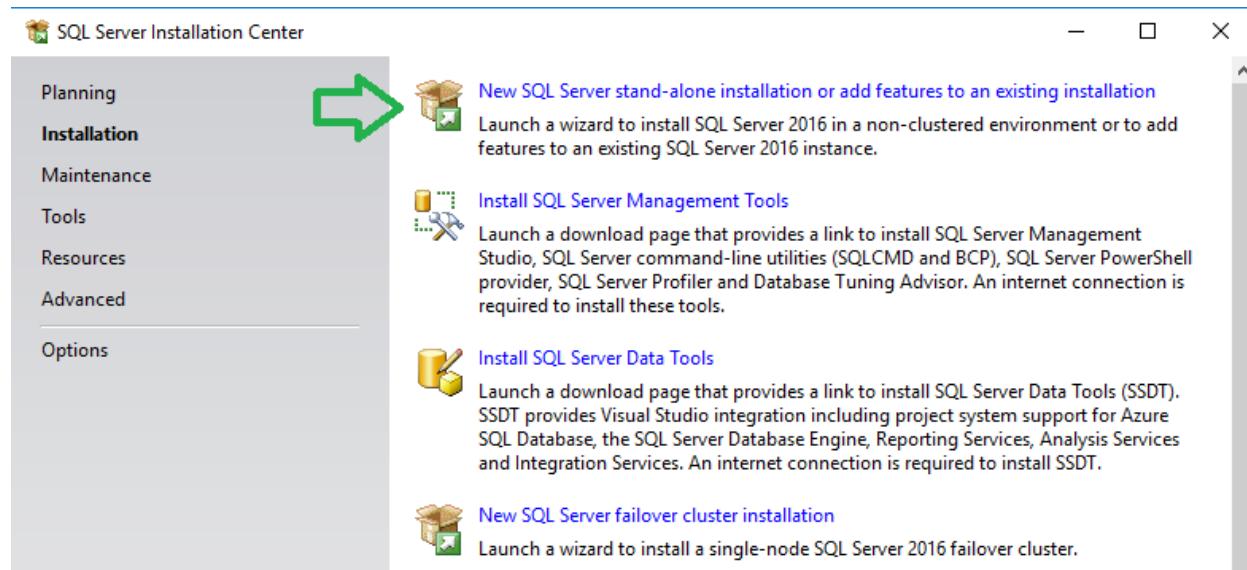
Click **Install** to begin the installation process.

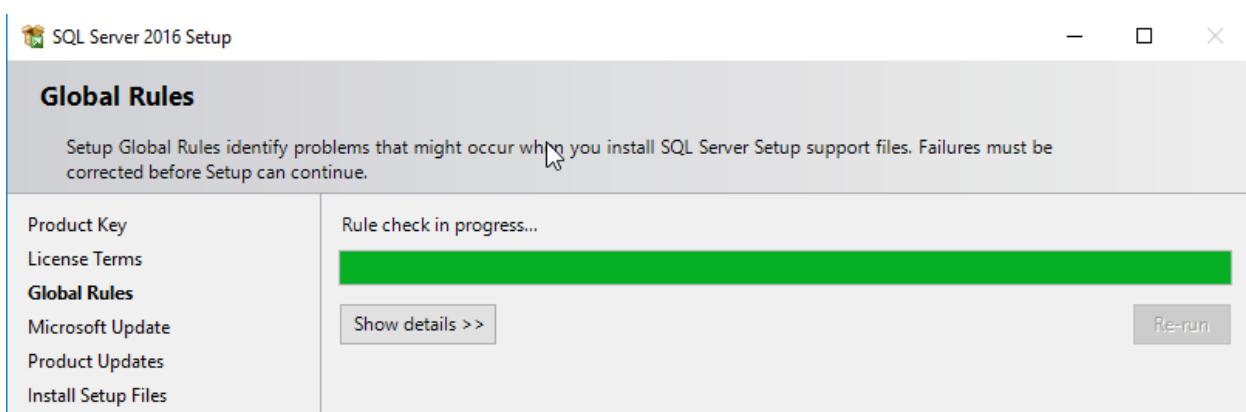
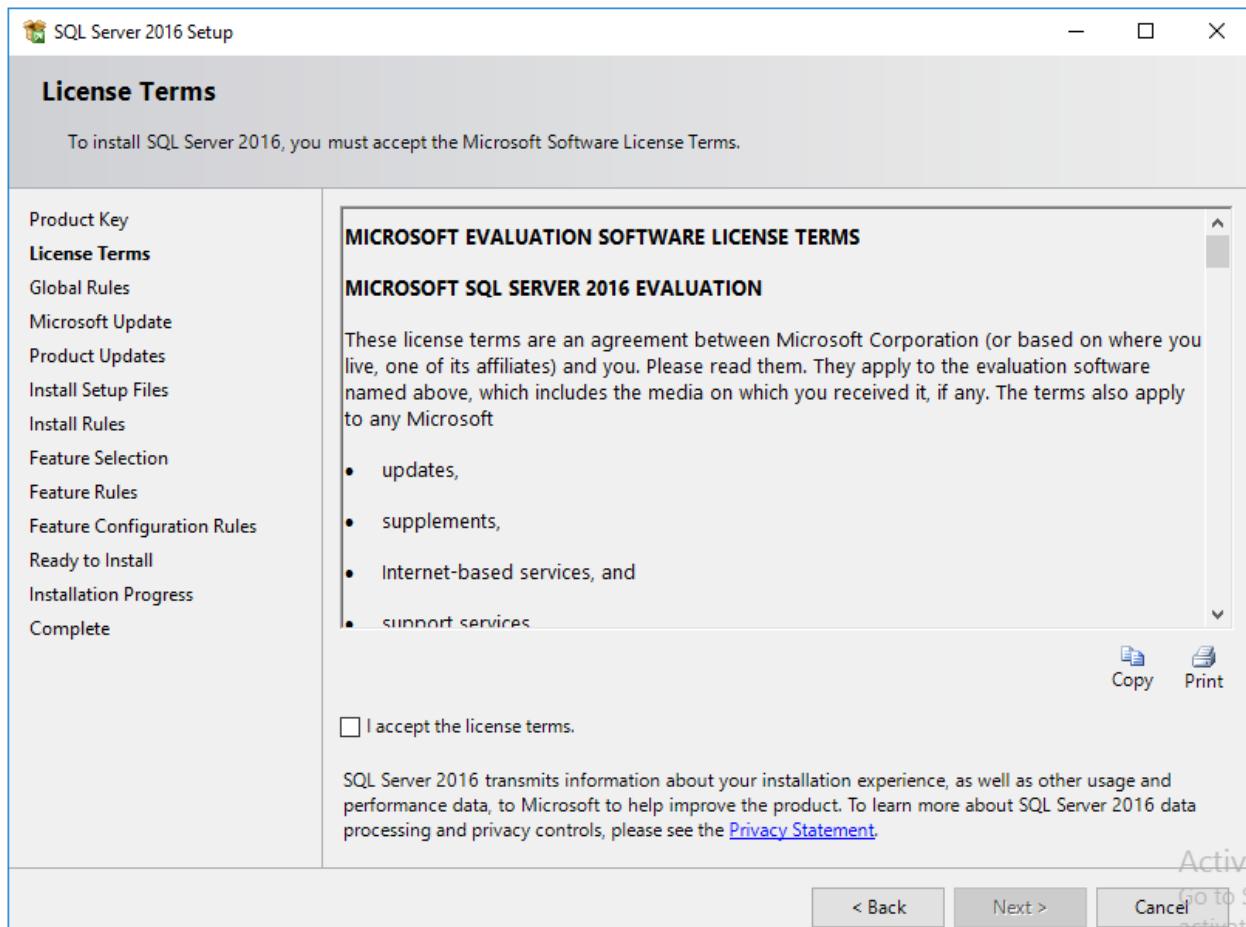


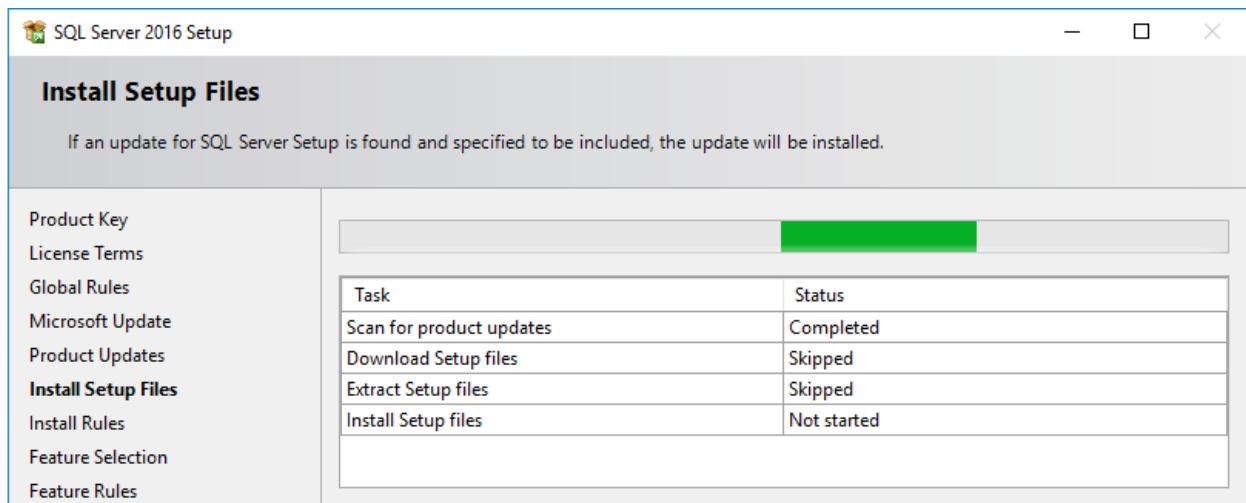
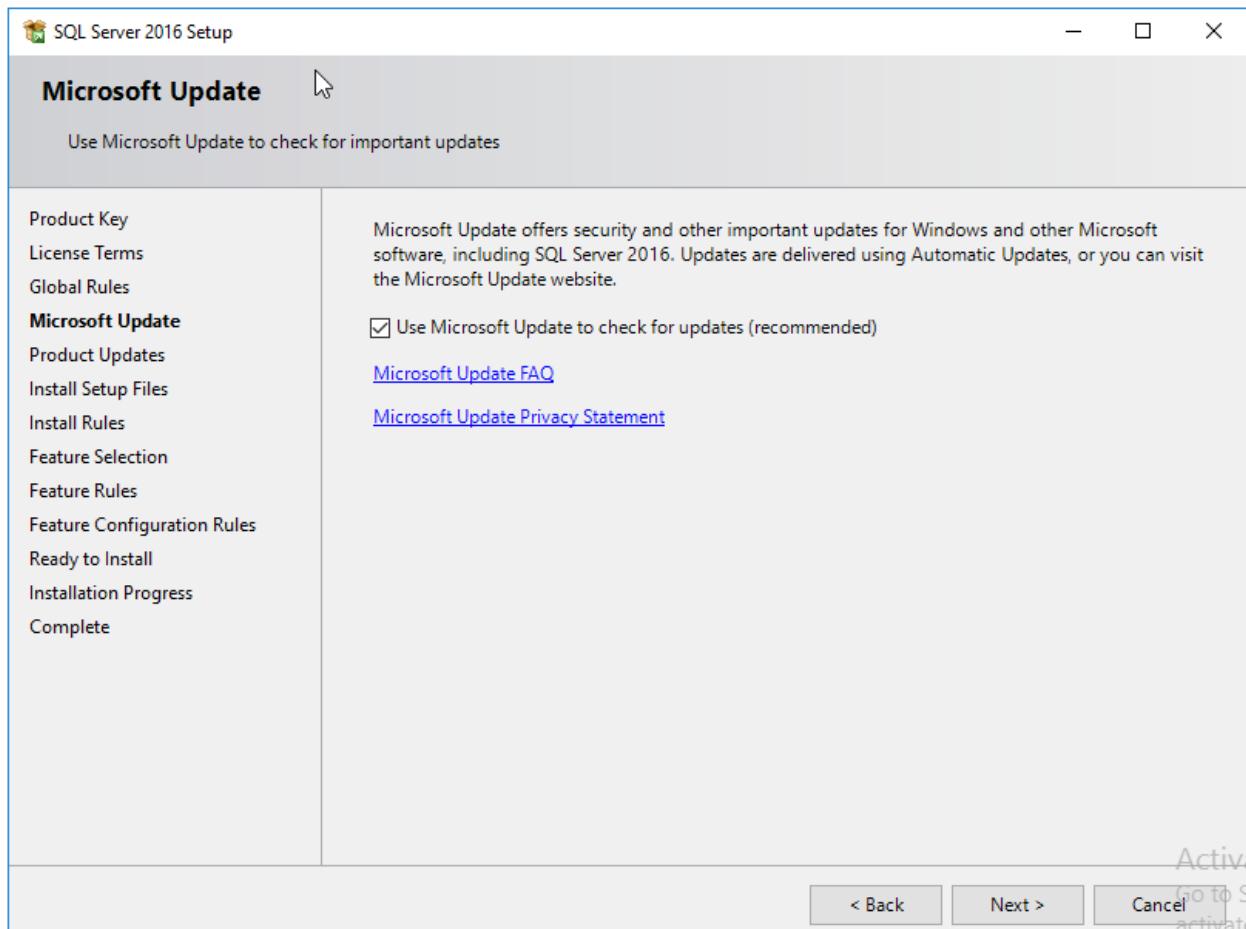
Once installed, open up **SSMS** and **limit** the amount of RAM SQL can use to 50% of total RAM. Set the value for both max and min (this is a critical setting, as SQL is a resource hog). Click **OK**.



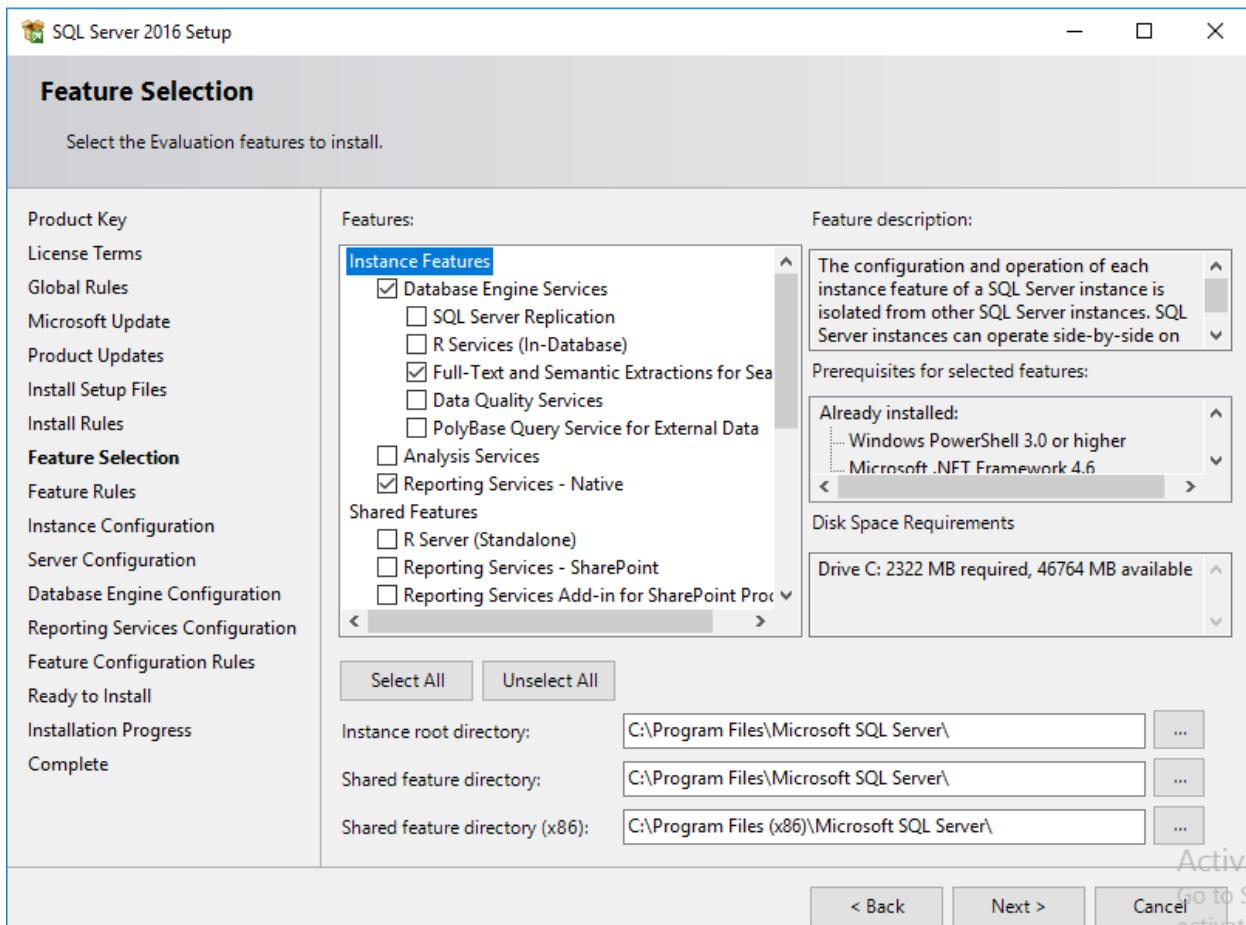
SQL 2016 Installation

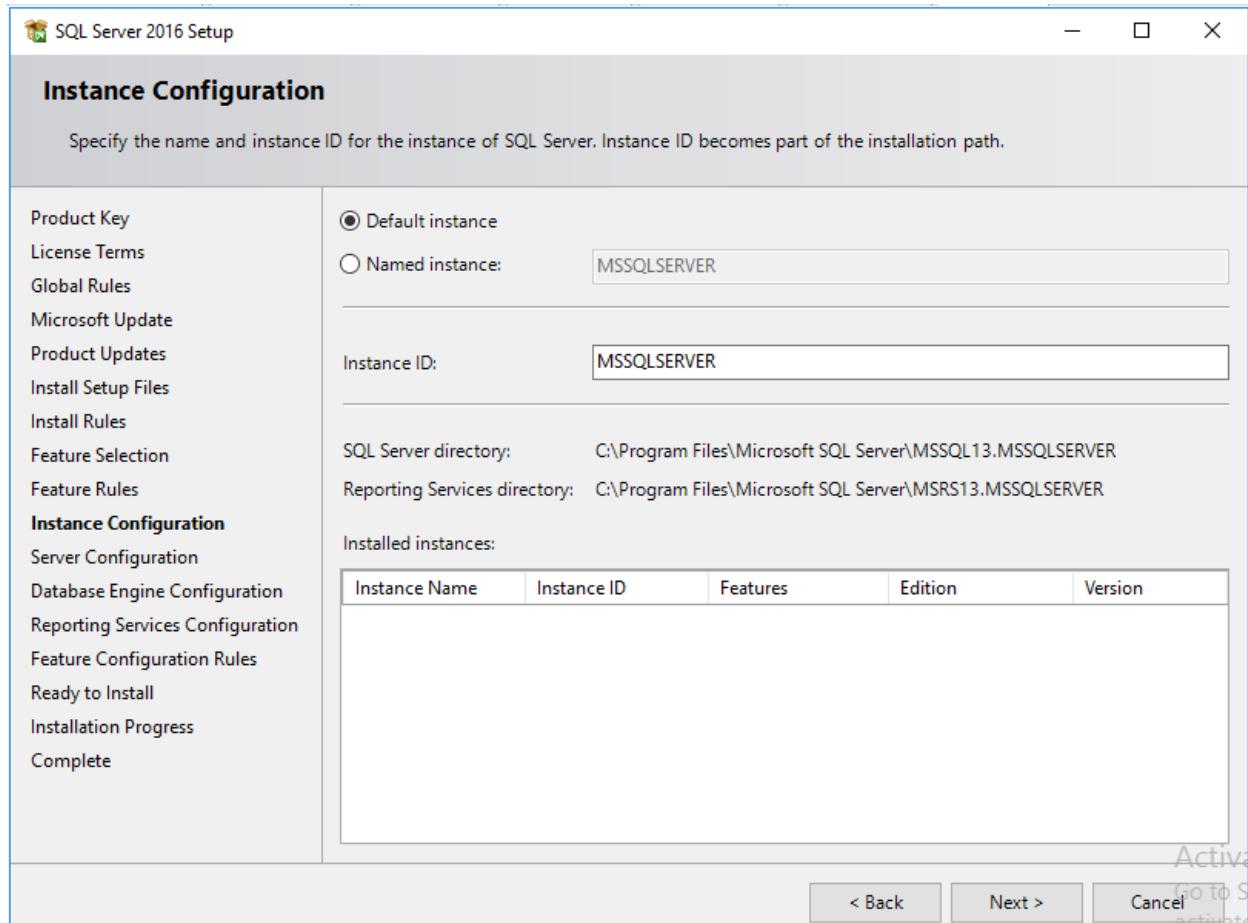


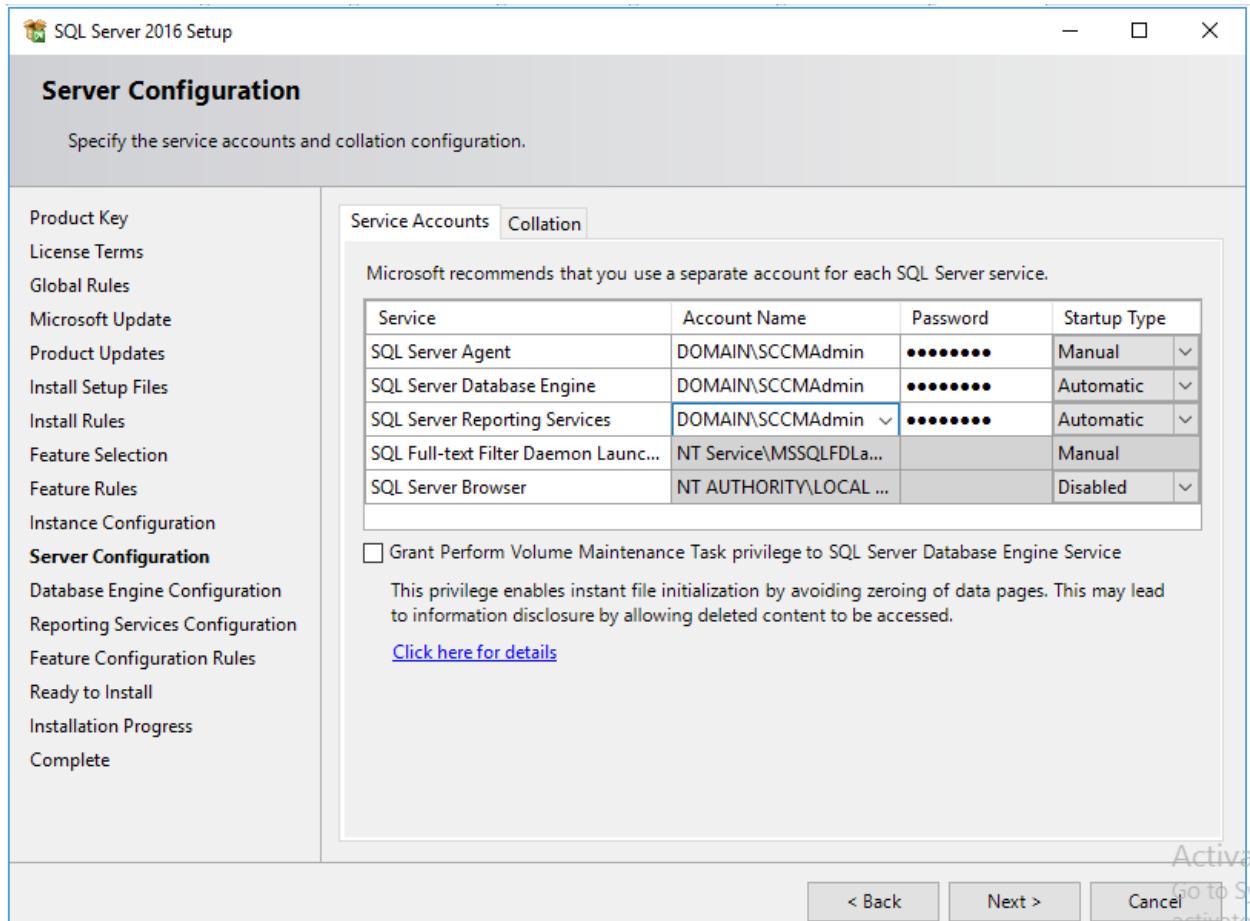


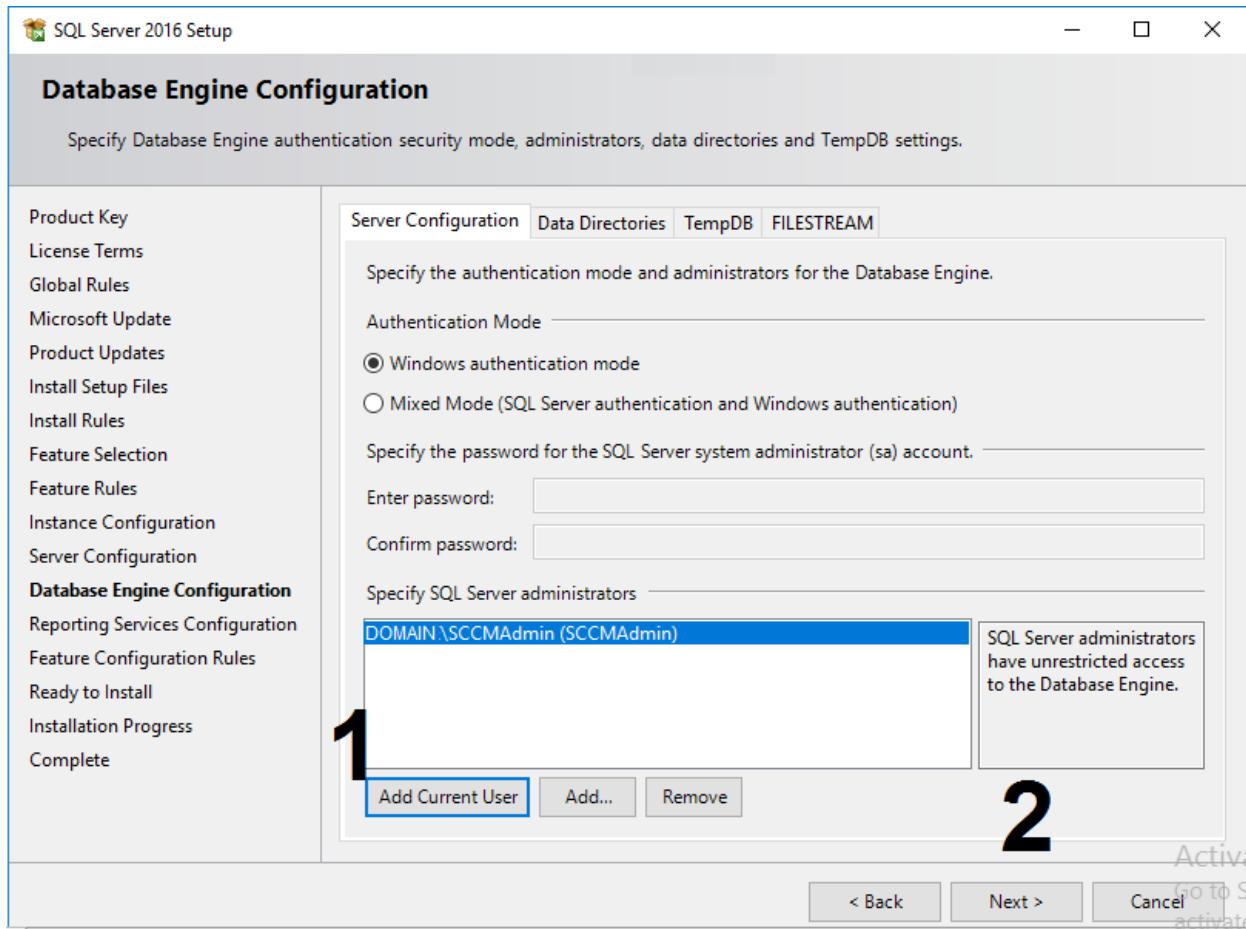


If you forget to add the Reporting Services - Native, you'll have to come back and install it before setting up Reporting in SCCM.









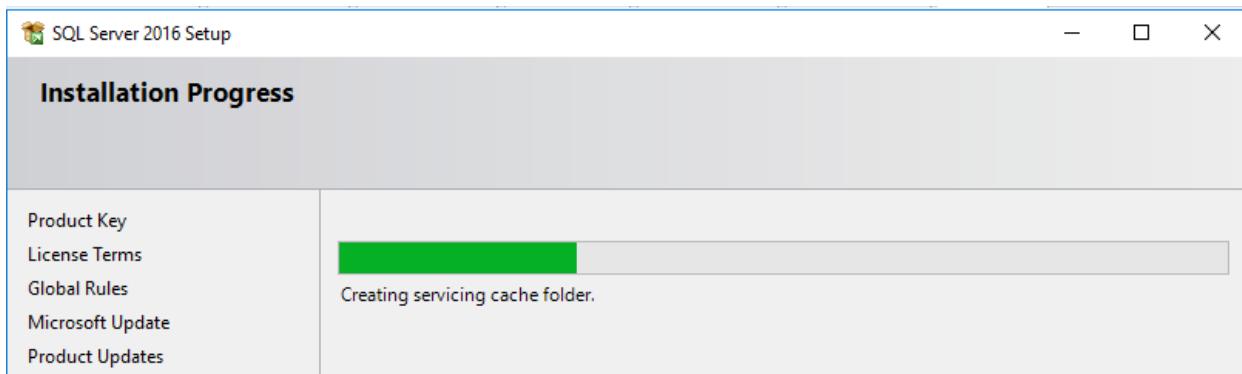
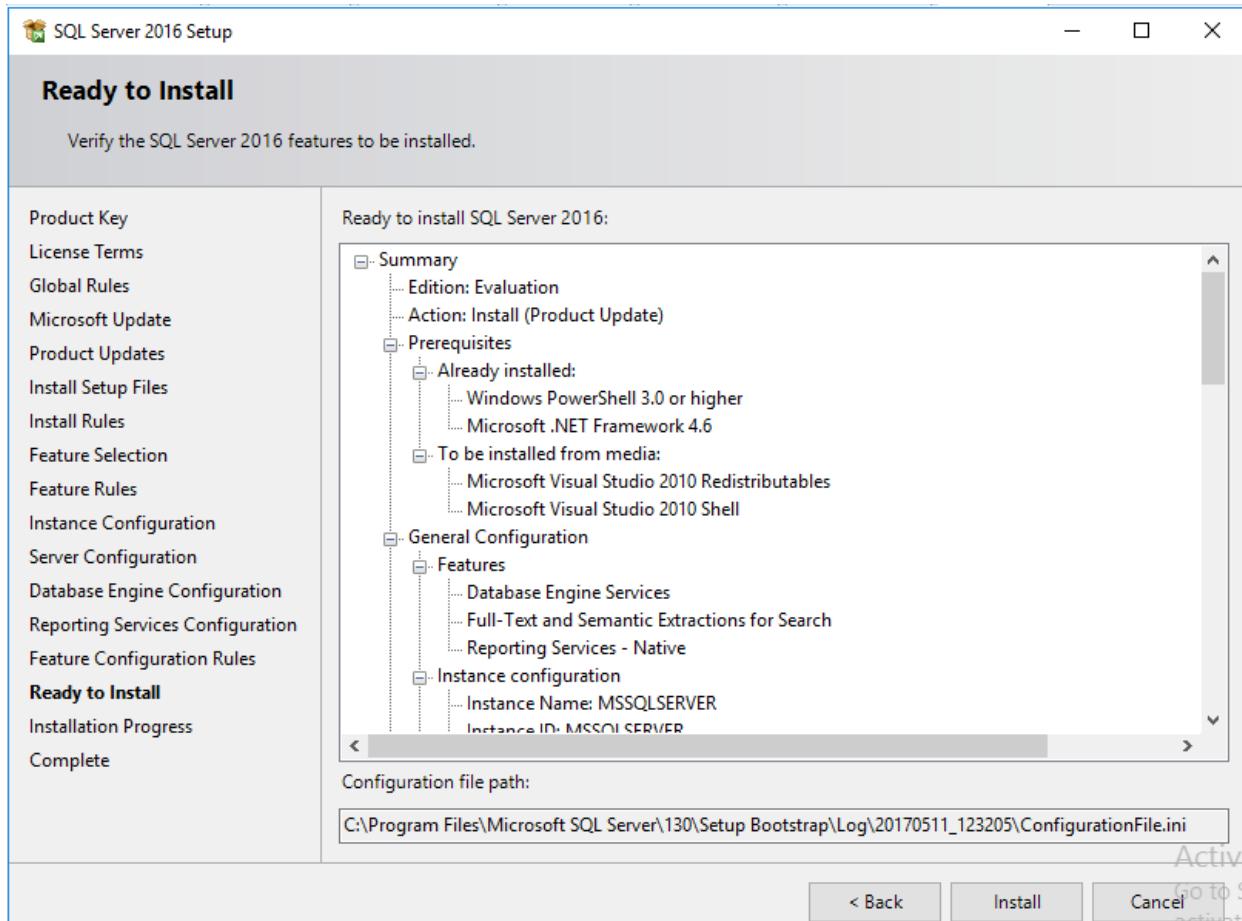
SQL Server 2016 Setup

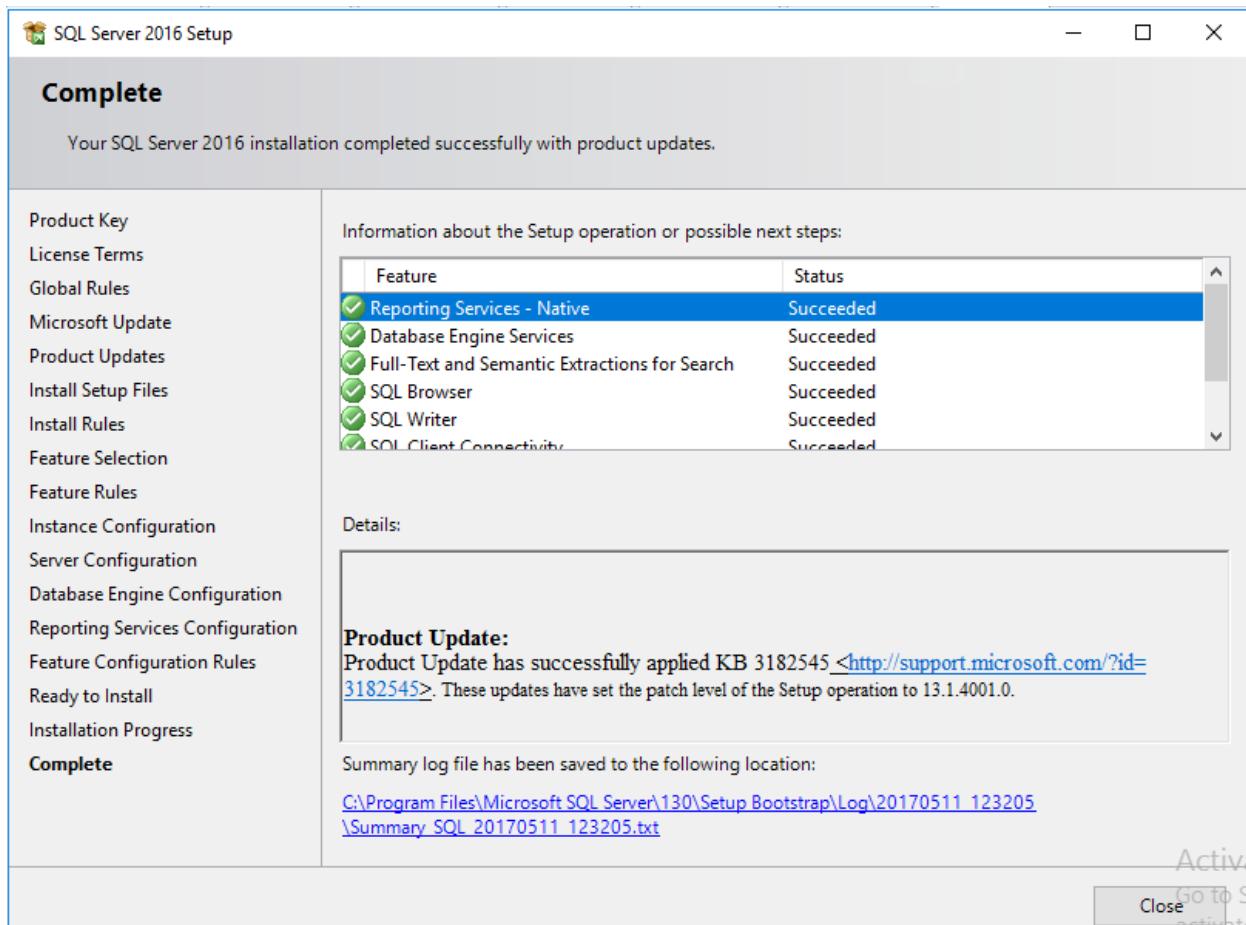
Reporting Services Configuration

Specify the Reporting Services configuration mode.

Product Key	Reporting Services Native Mode
License Terms	<input checked="" type="radio"/> Install and configure. Installs and configures the report server in native mode. The report server is operational after setup completes.
Global Rules	
Microsoft Update	
Product Updates	<input type="radio"/> Install only. Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.
Install Setup Files	
Install Rules	
Feature Selection	Reporting Services SharePoint Integrated Mode
Feature Rules	<input type="radio"/> Install only. Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.
Instance Configuration	
Server Configuration	
Database Engine Configuration	
Reporting Services Configuration	
Feature Configuration Rules	
Ready to Install	
Installation Progress	
Complete	

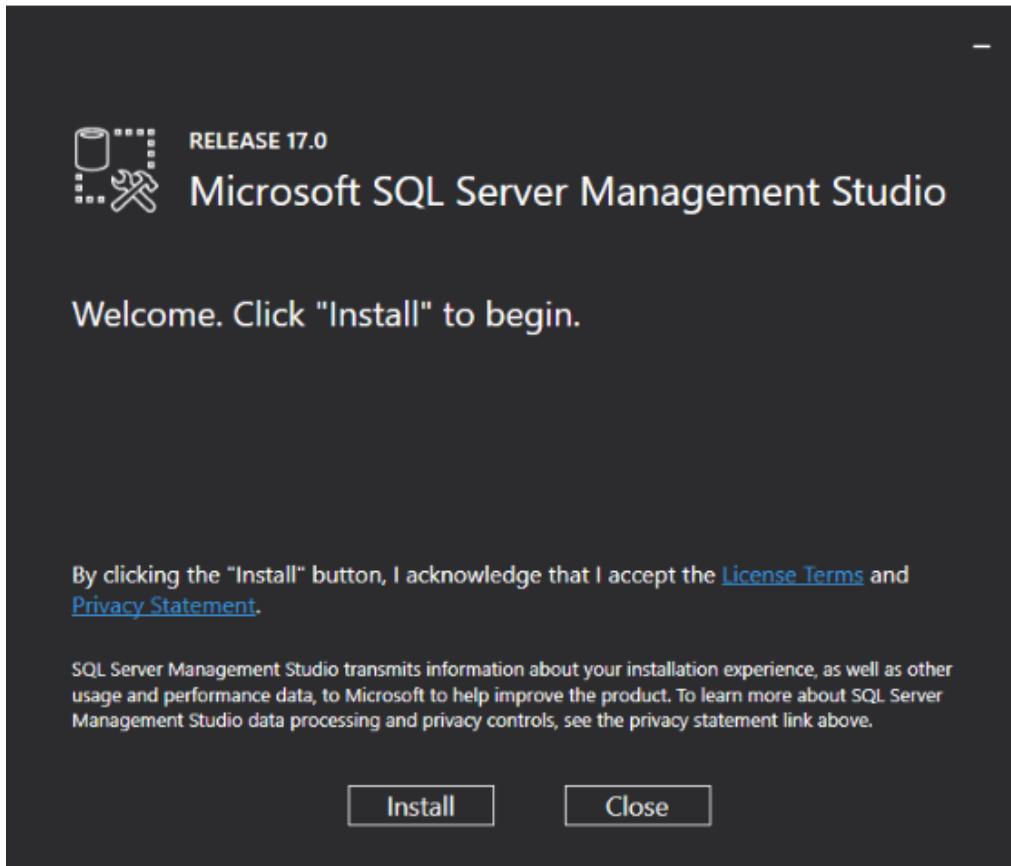
< Back Next > Cancel Go to S...
activate

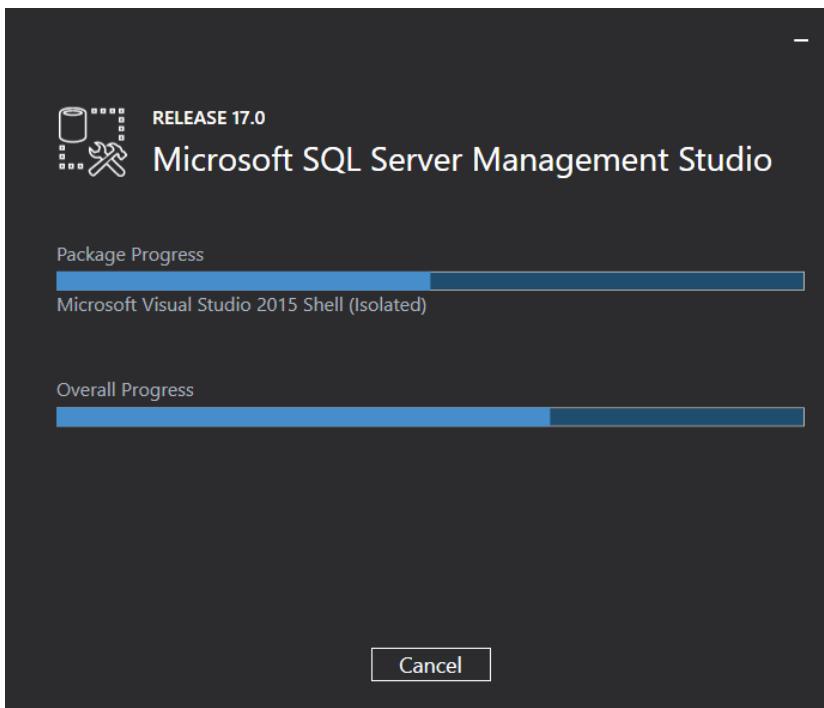
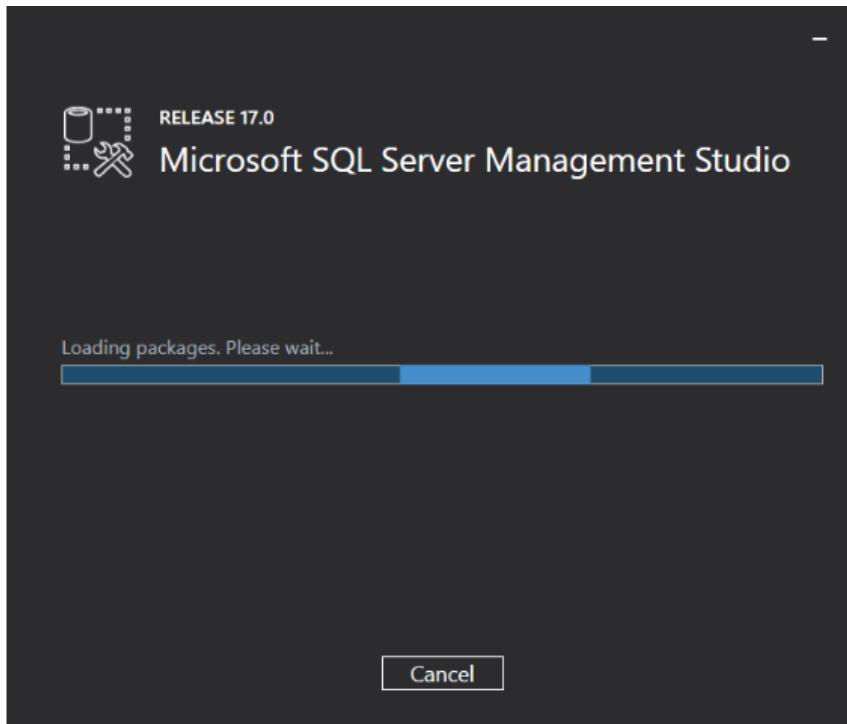


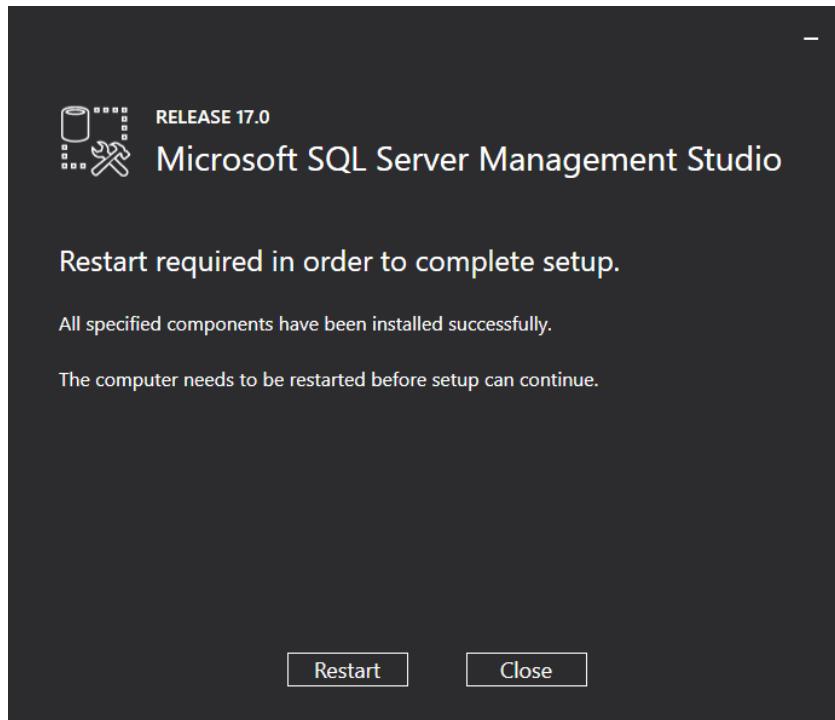


Download SQL Server Management Studio - 17.0

<https://go.microsoft.com/fwlink/?LinkId=847722>







If you would like to use the PowerShell module, download here:

<https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-ps-module>

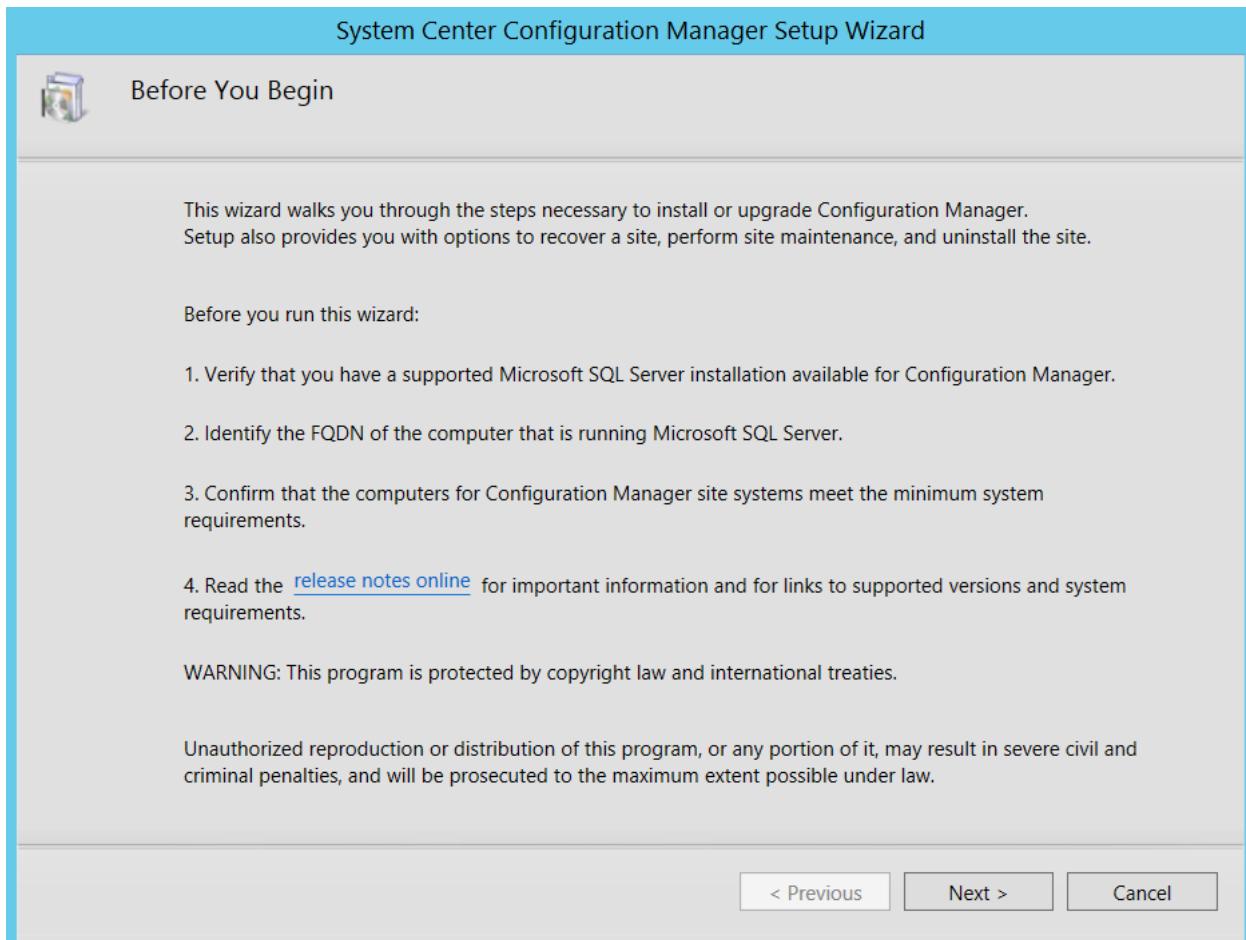
Install SCCM {current build}

Pre-req: Install .NET Framework 3.5 Features.

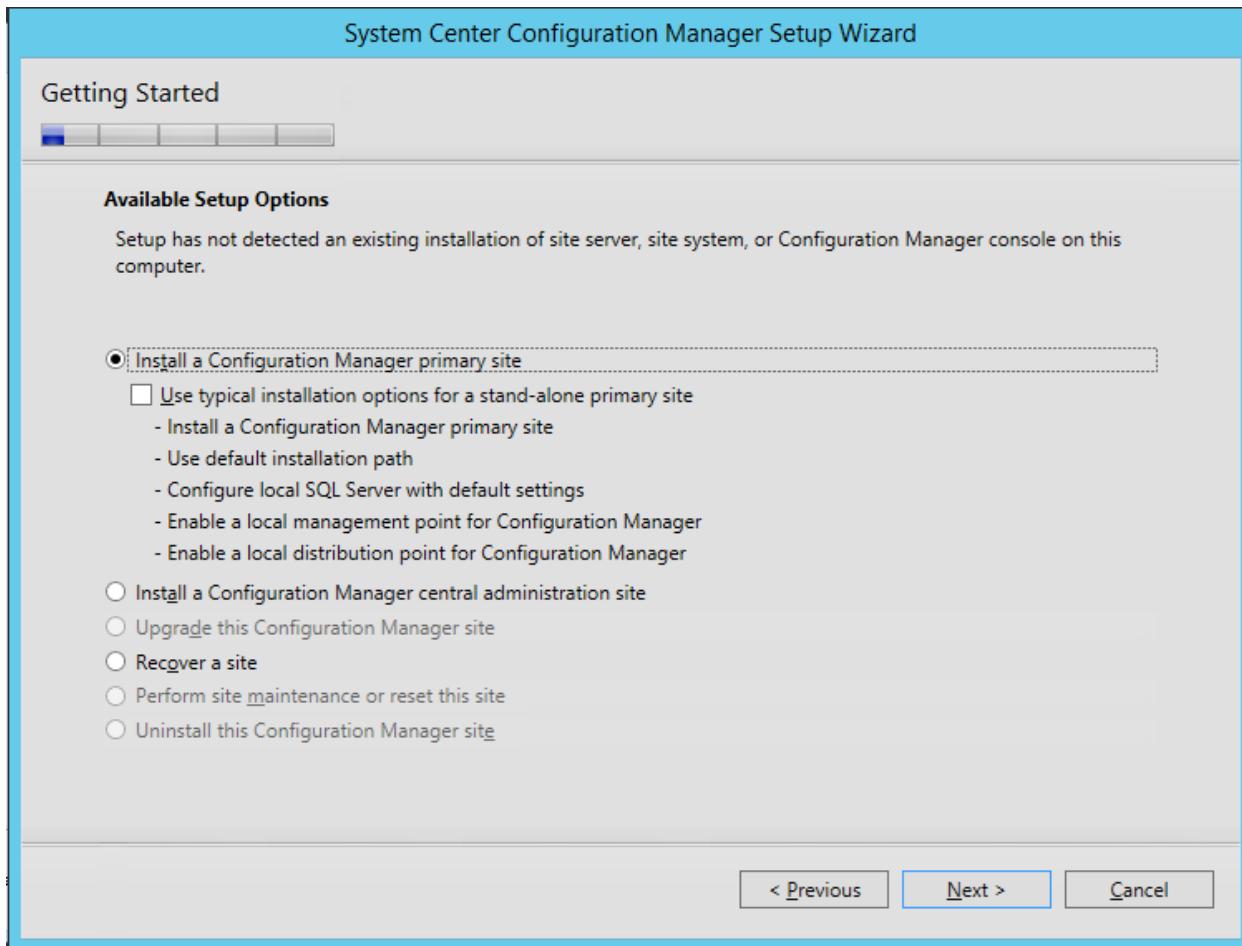
Begin the installation of SCCM by launching **splash.hta**. Click **Install**.



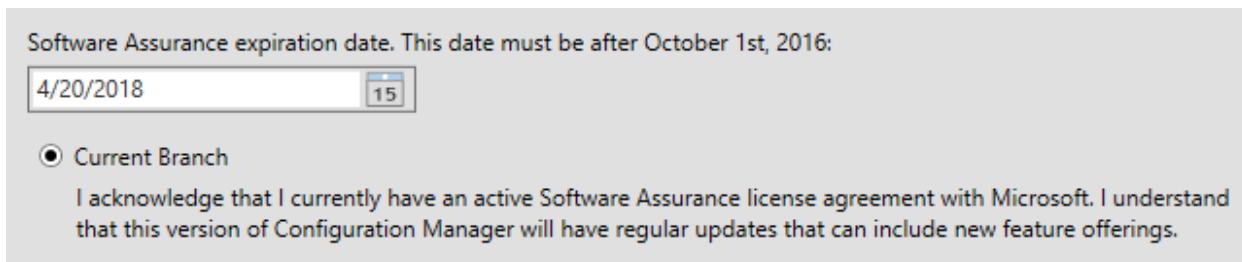
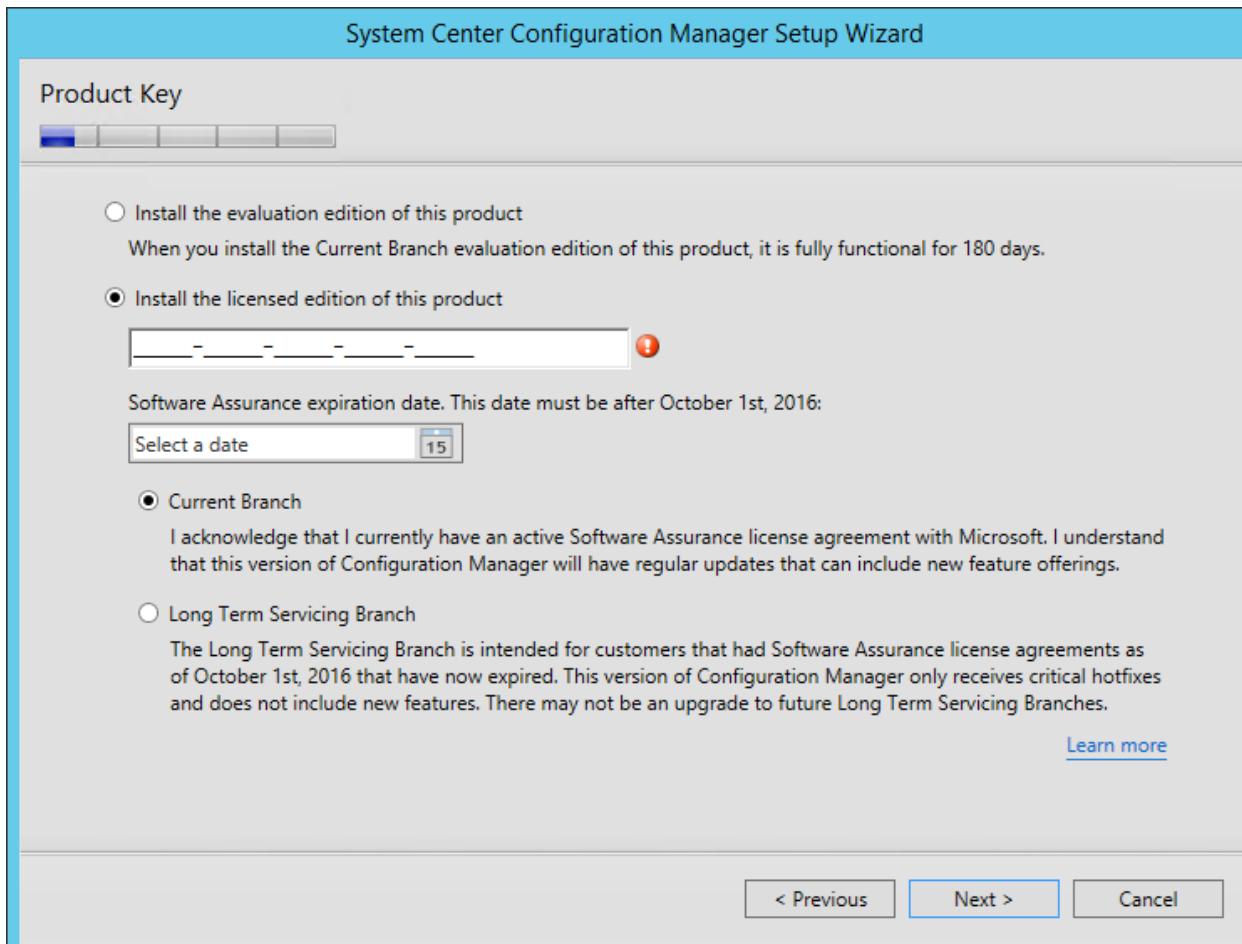
Click **Next**.



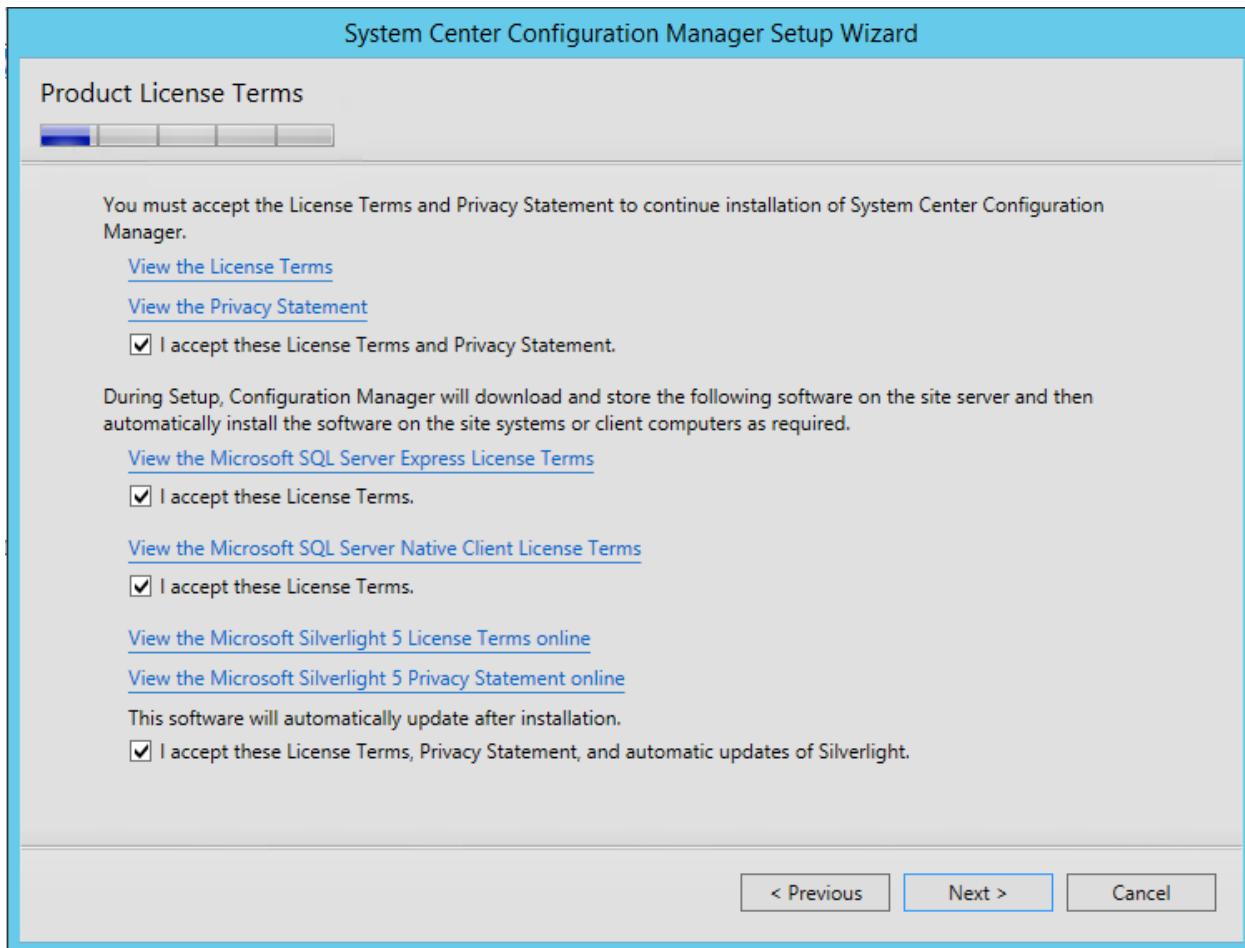
Choose **Install a Configuration Manager primary site**. Click **Next**.



Enter a license key or evaluate. Click **Next**.



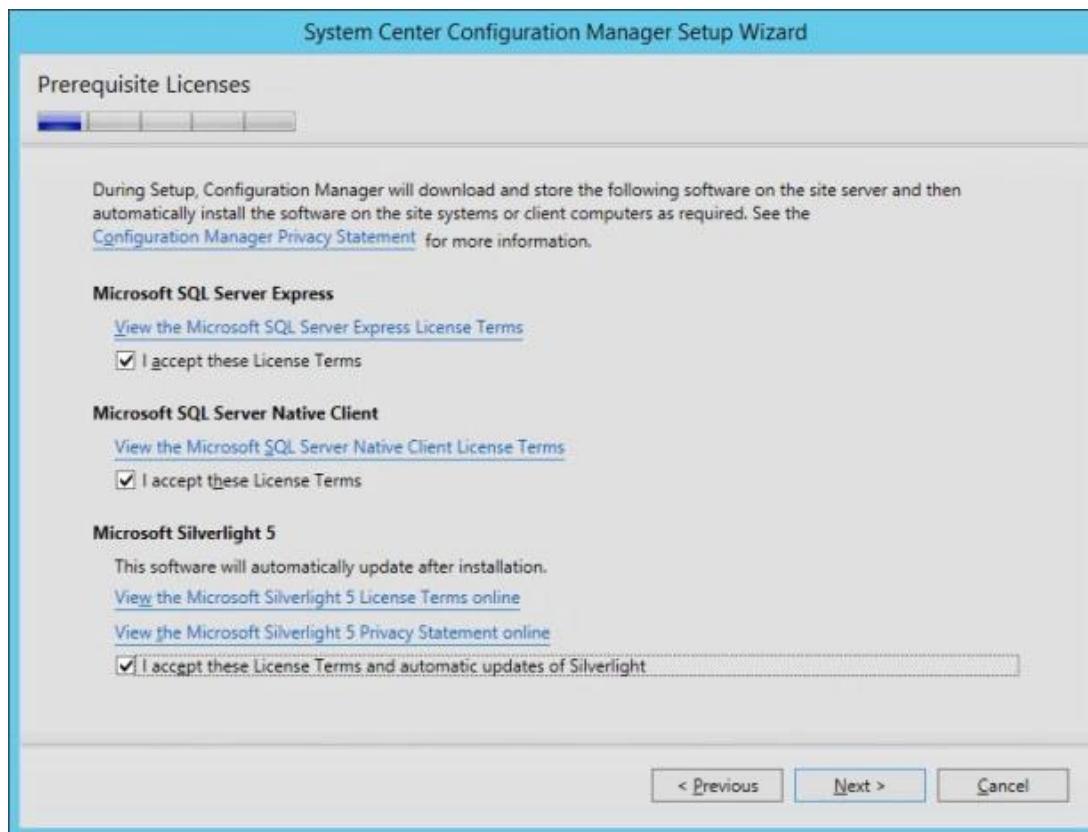
Accept the license agreement and click **Next**.



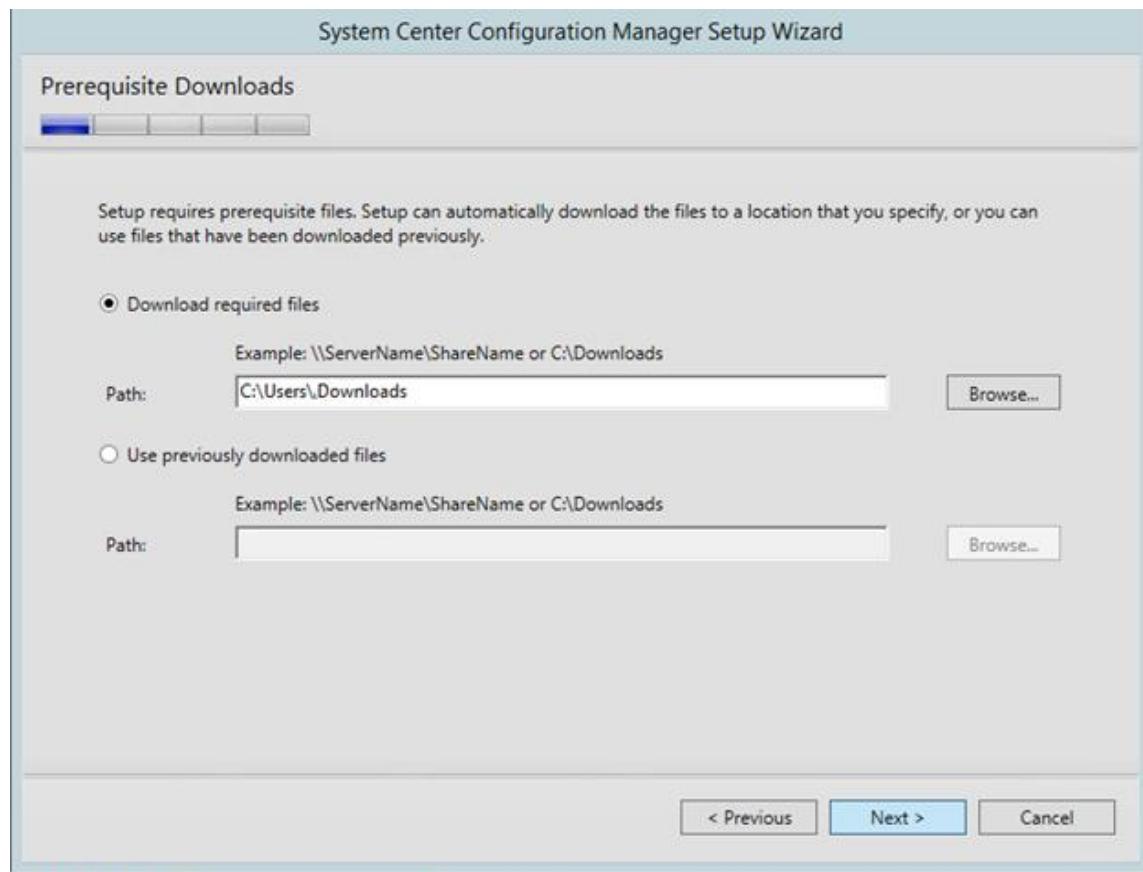
Note: If you enter a license key on previous screen, it may skip this screen and go directly to accepting the Prerequisite Downloads screen. Click **Next**.



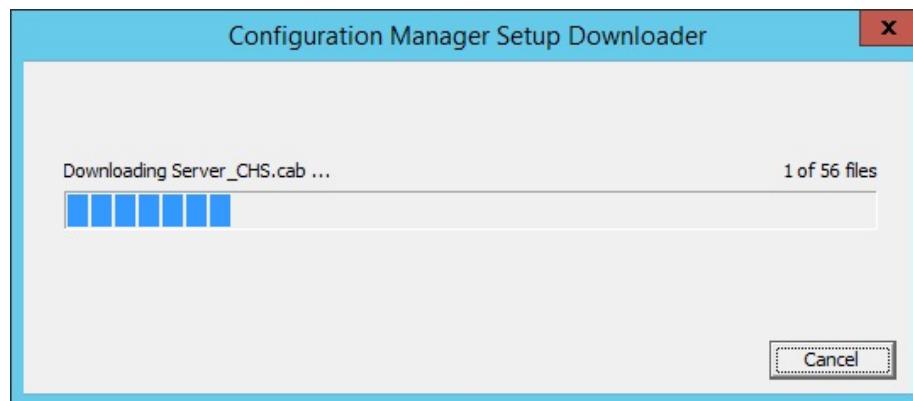
Accept pre-req licenses and click **Next**.



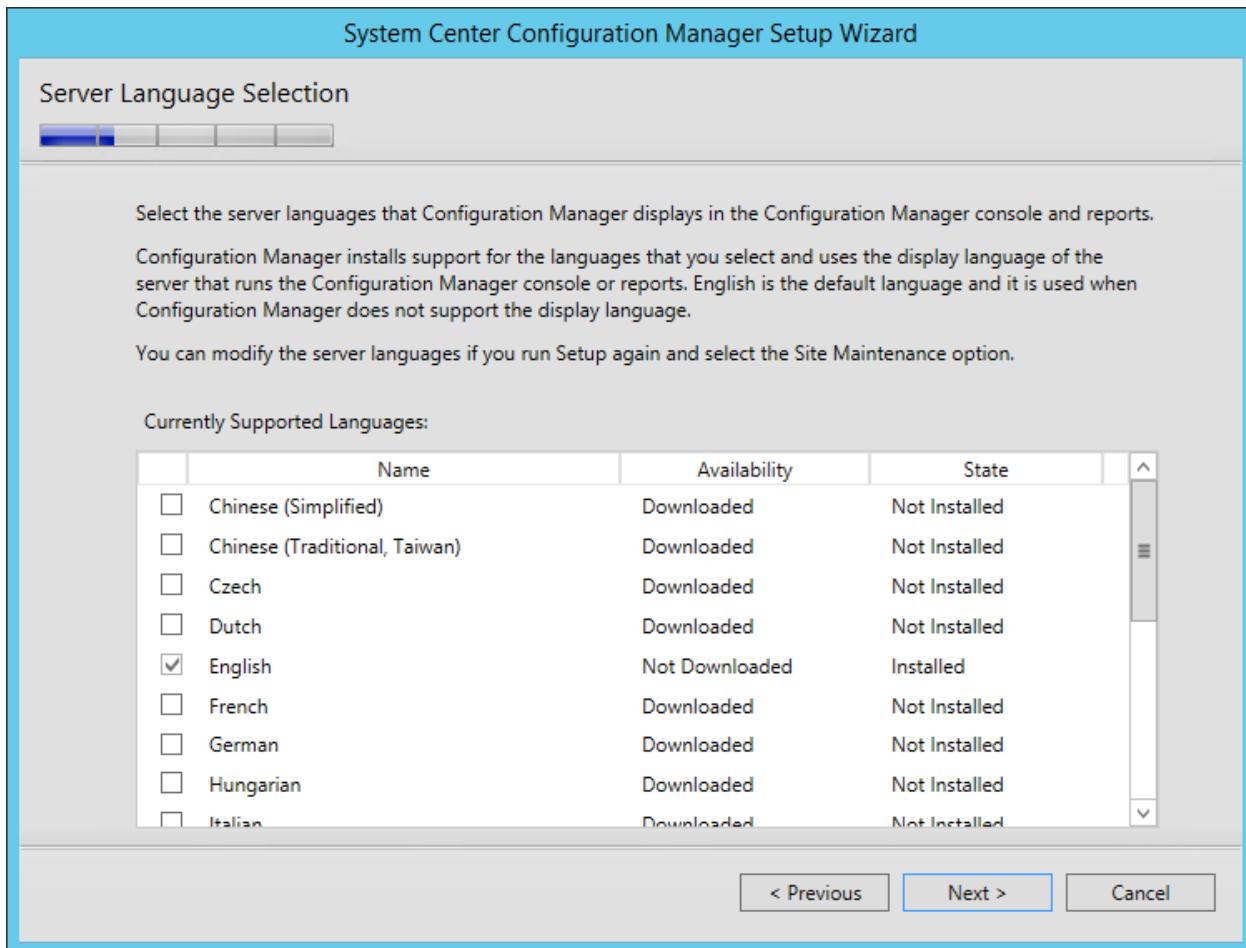
Create a **folder** to store install updates and **point** the SCCM install to that location. Click **Next**.



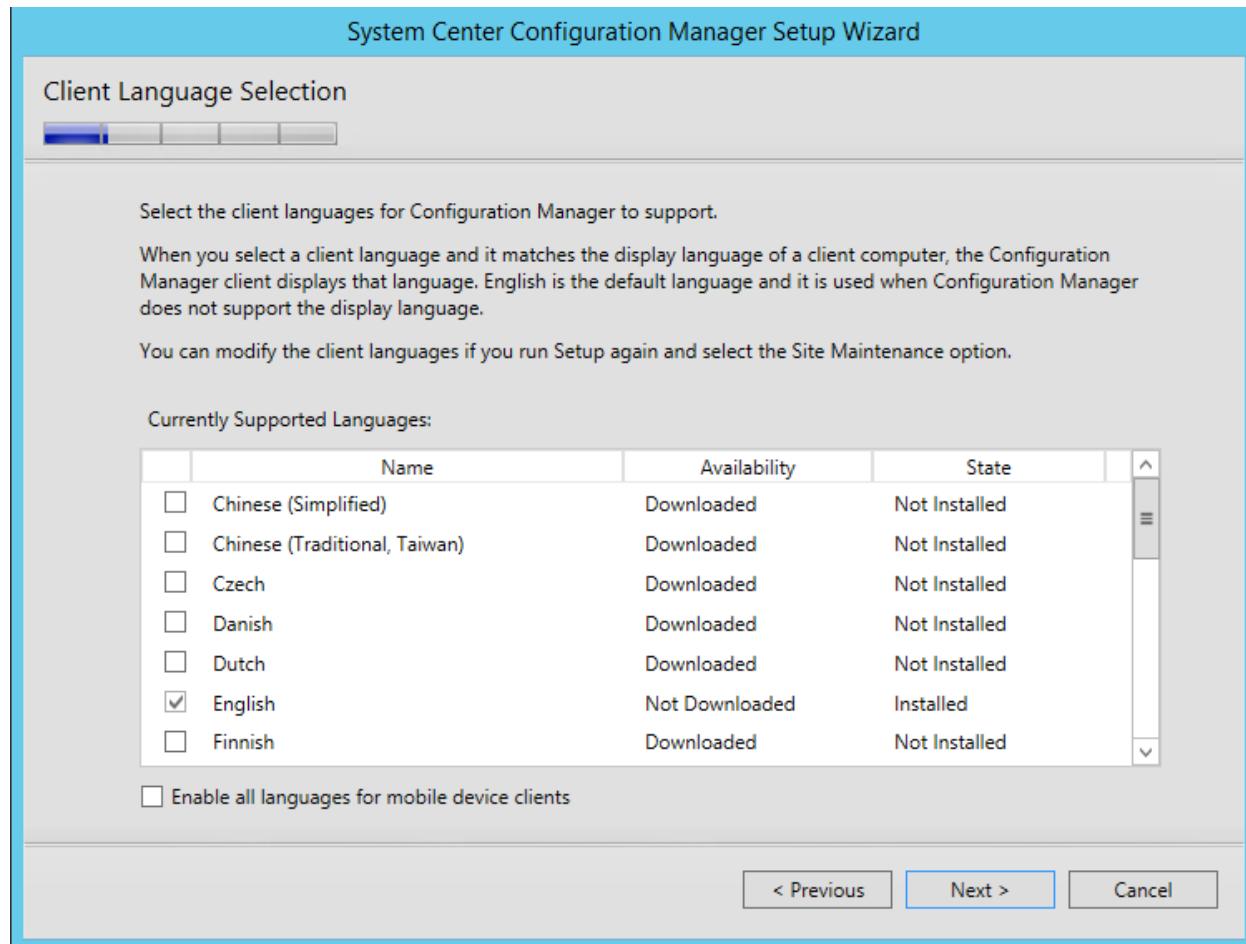
Updates will download and install.



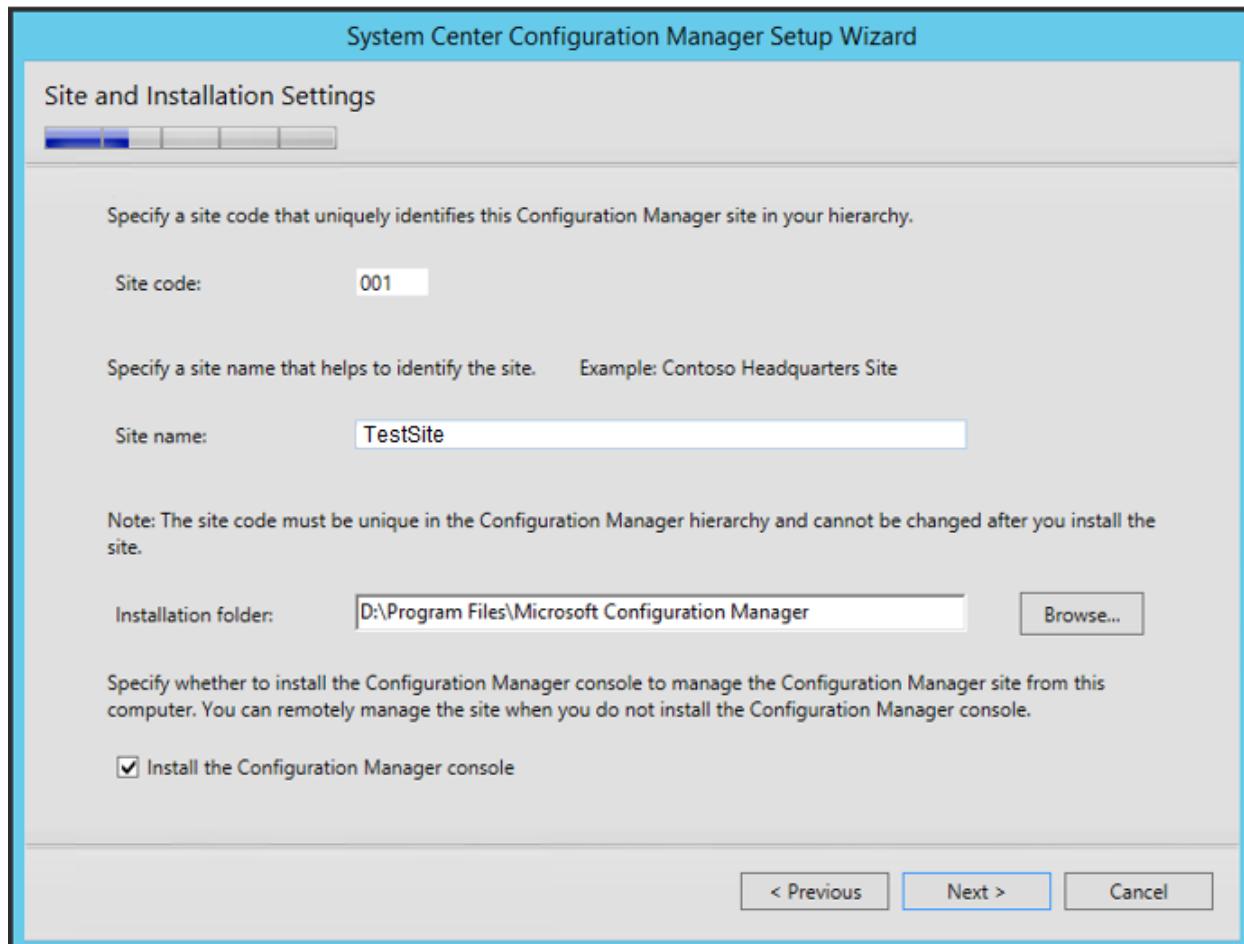
Select **language** requirements for the SCCM server and click **Next**.



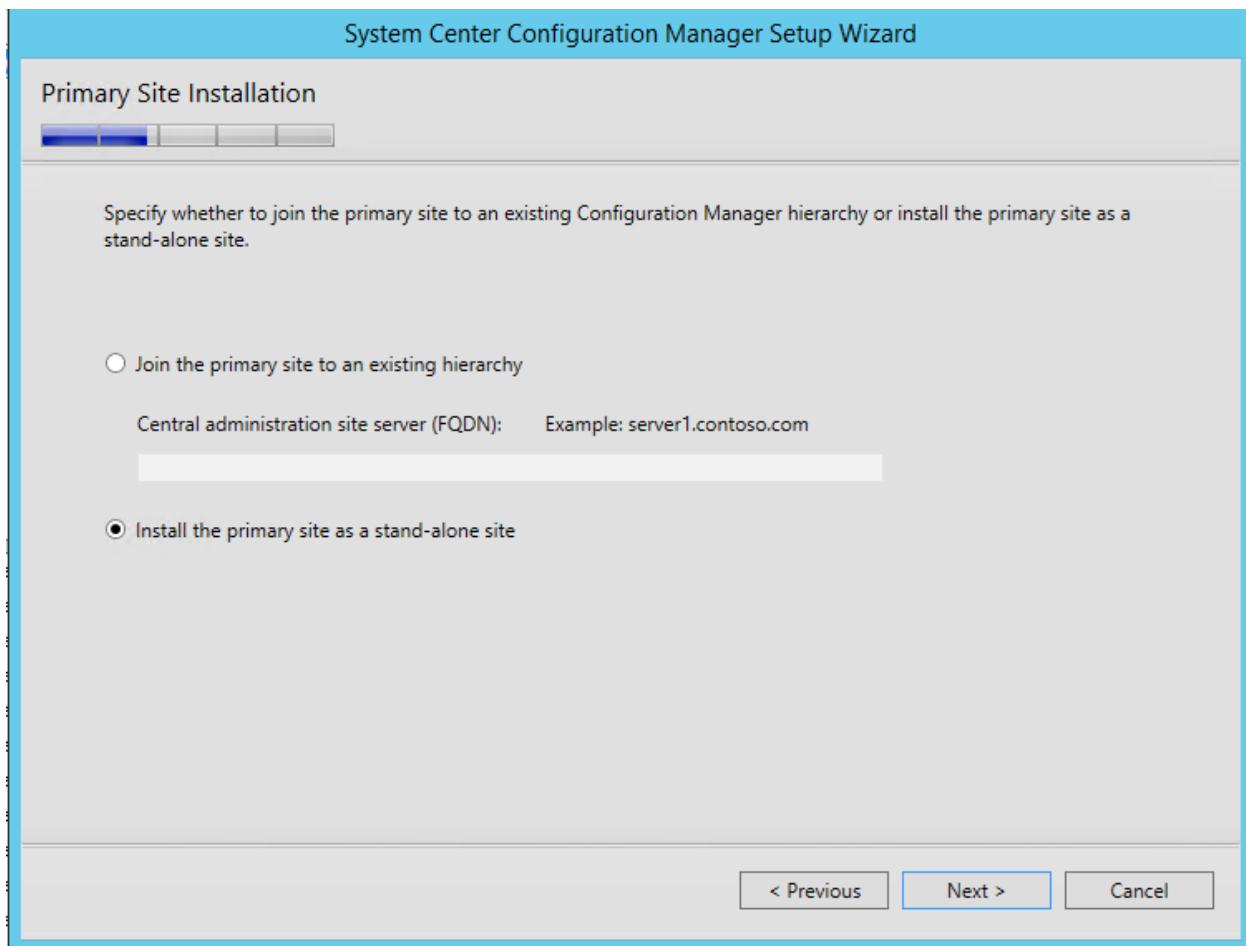
Select client **language** requirements and click **Next**.



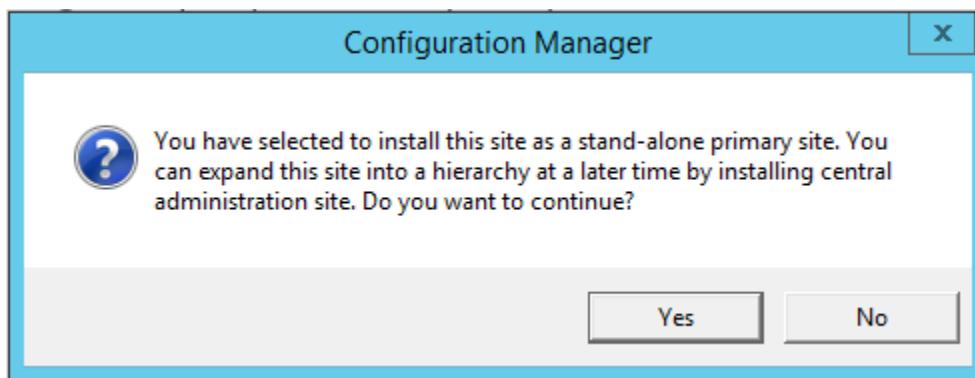
Enter a **3 digit site code** and **description** and click **Next**.



Choose whether to run the **Primary as stand-alone site** or join to an existing hierarchy. Click **Next**.

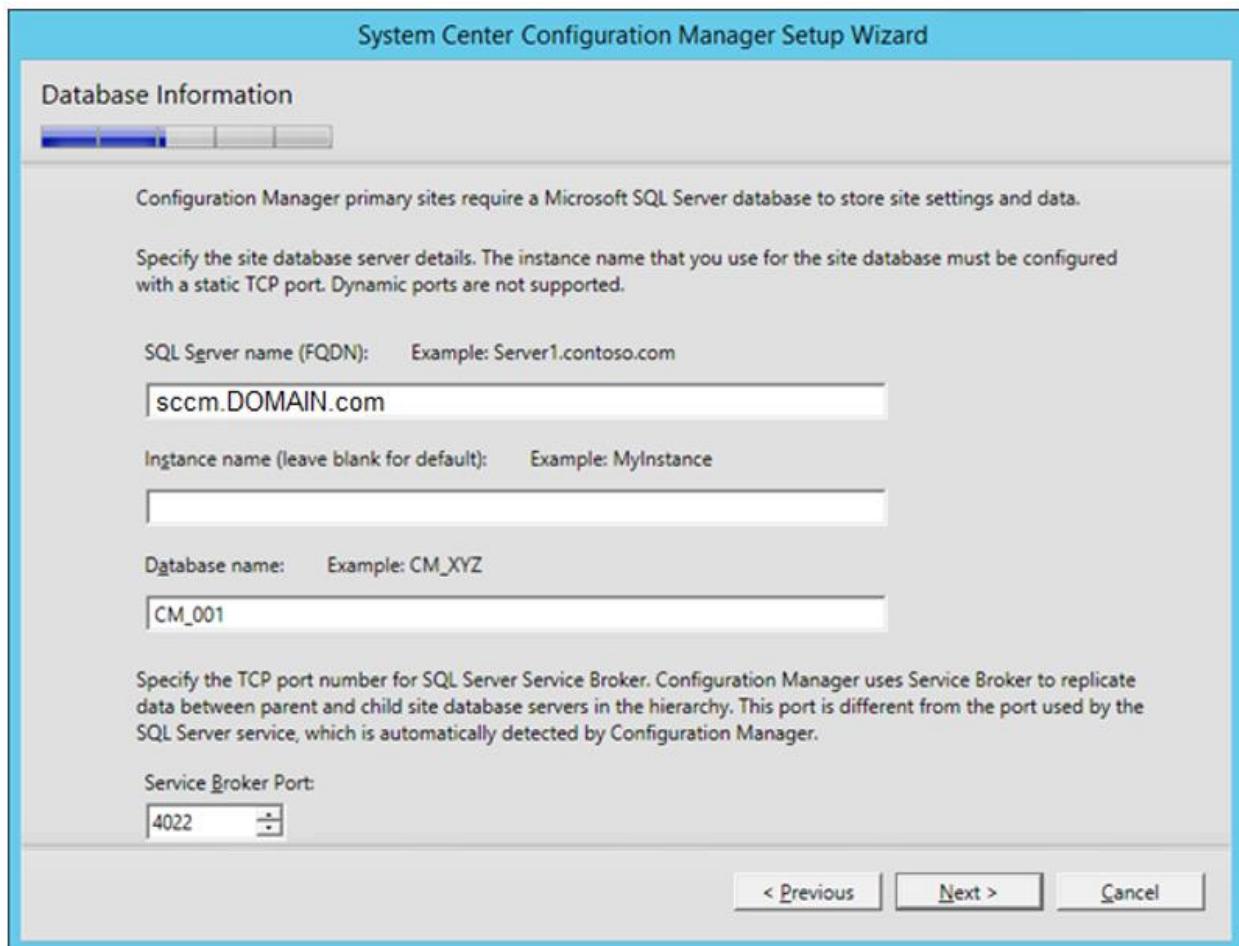


In this instance, a **stand-alone primary** is being installed. Click **Yes** to accept.

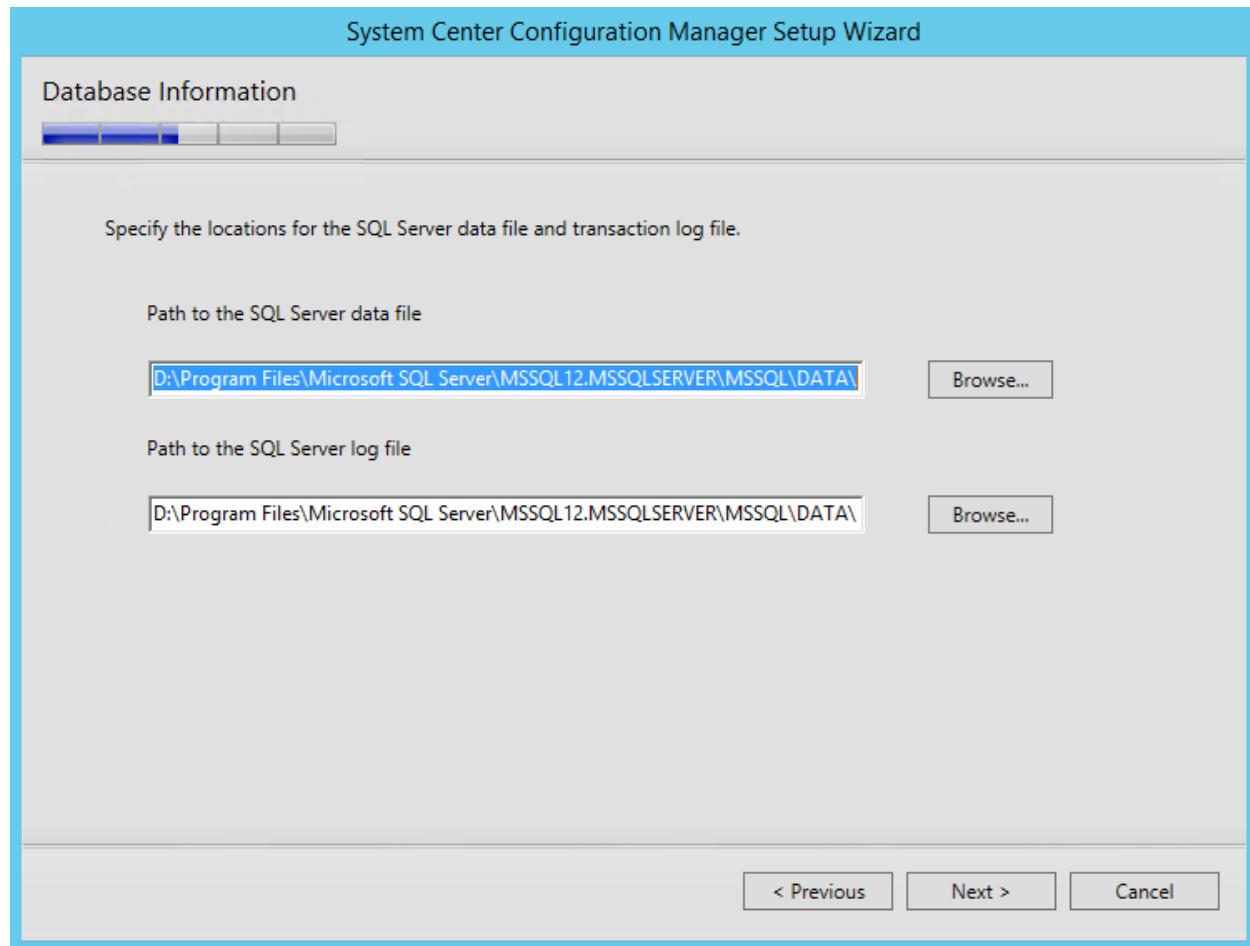


Use the database **default** configuration, **do not** enter an Instance name, and click **Next**.

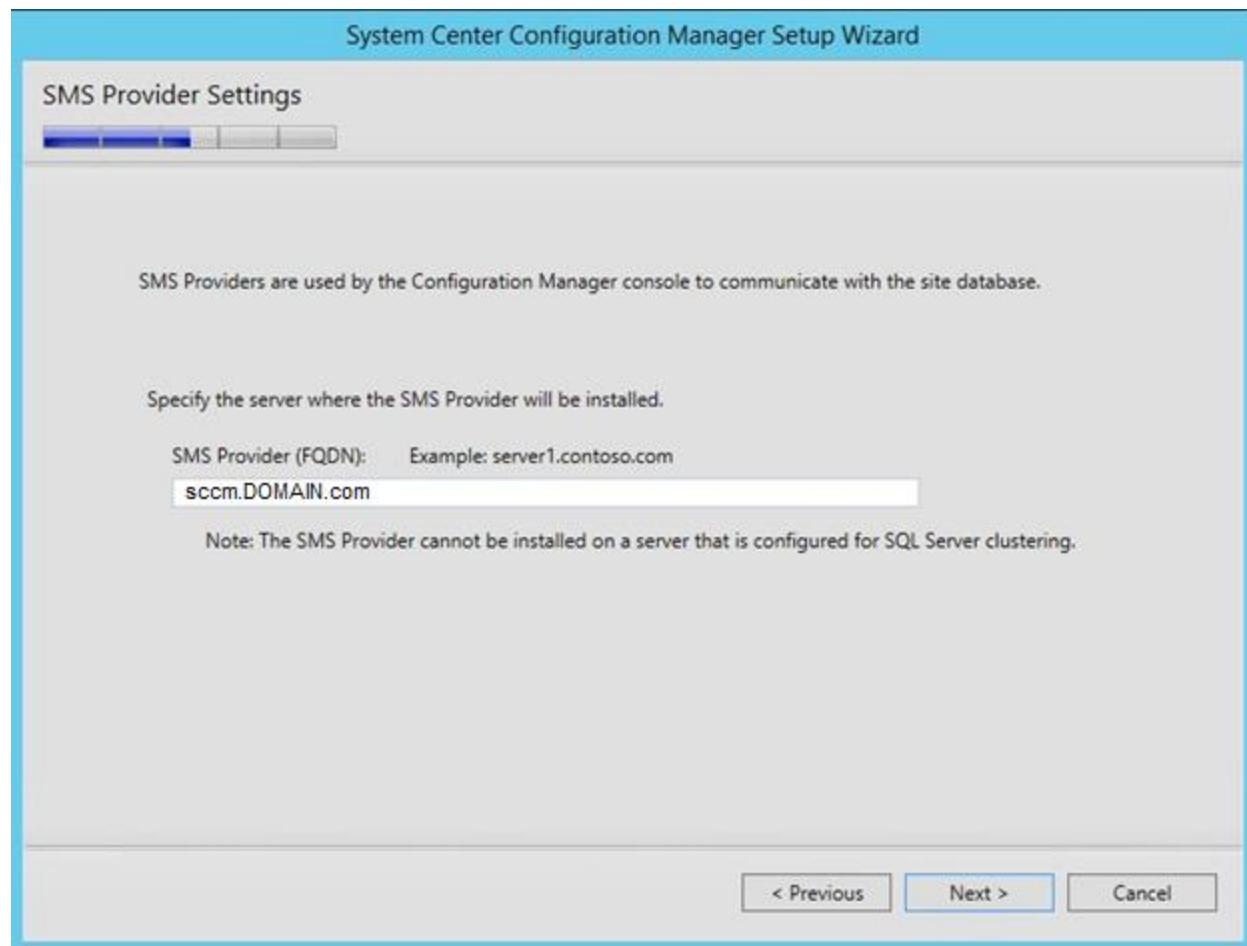
Note, if the SQL DB is on another server, use that server name in the top field.



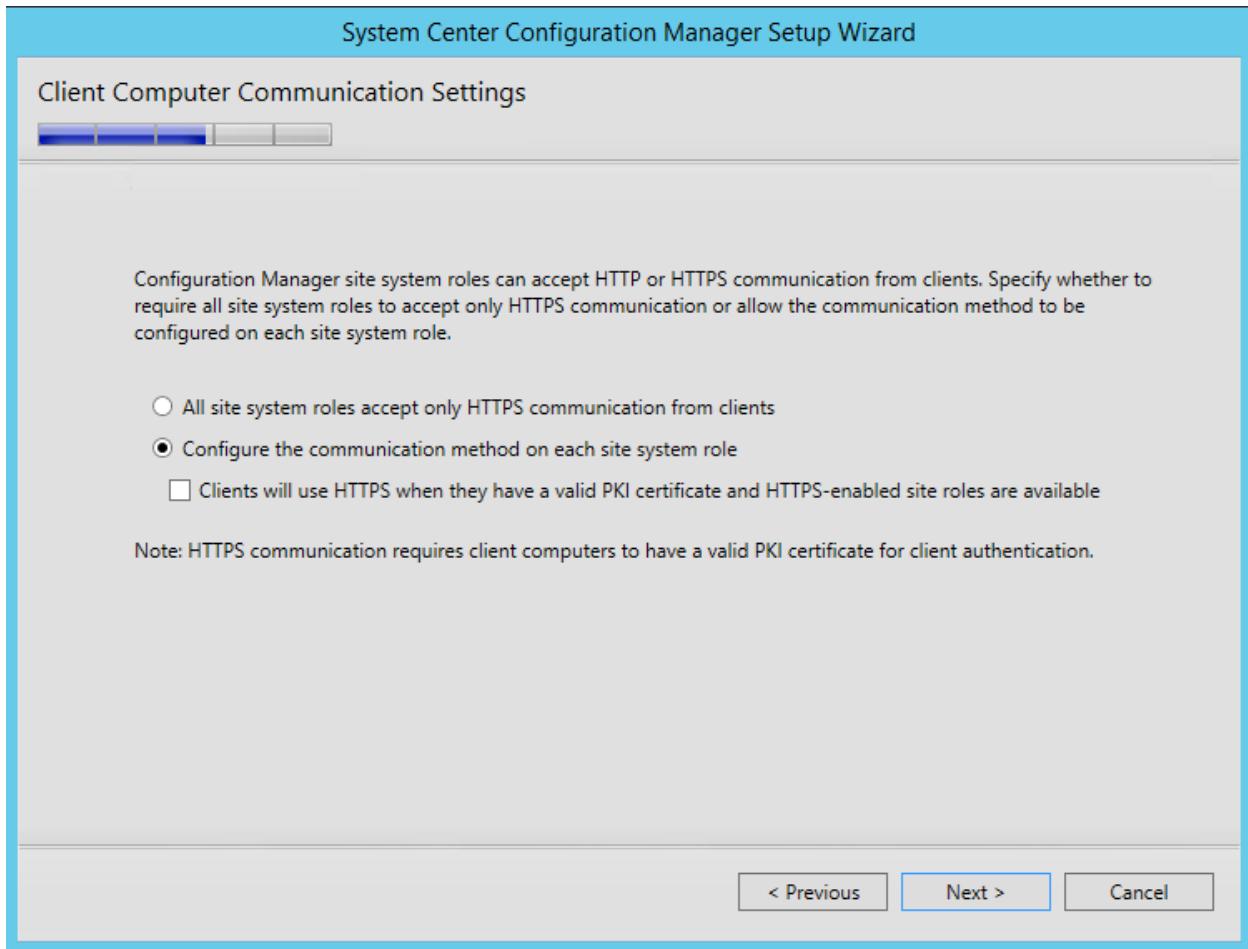
Specify the path to the SQL database file and log file. In this instance, it is the defaults. Click **Next**.



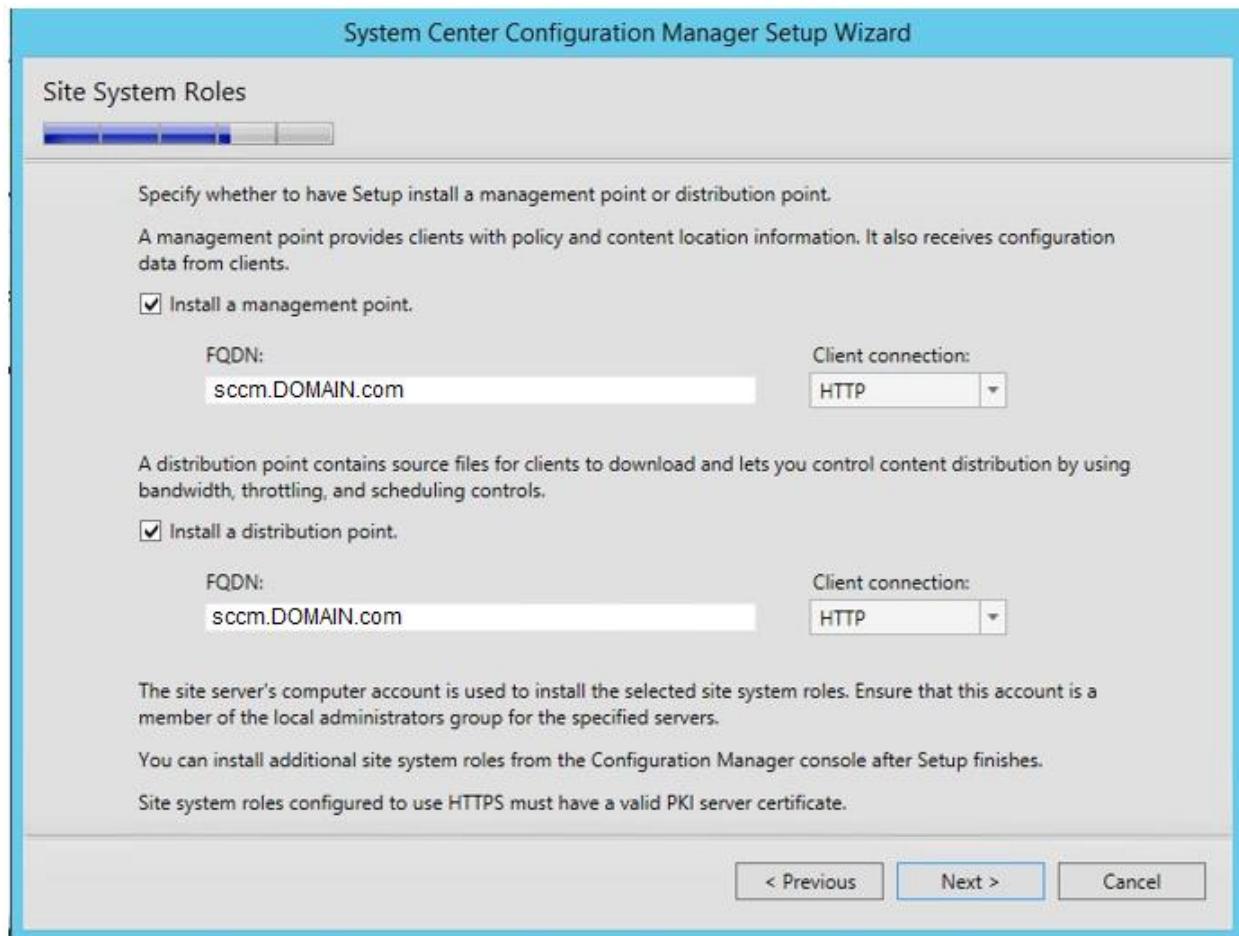
Click **Next** to set the **current server** as the SMS Provider.



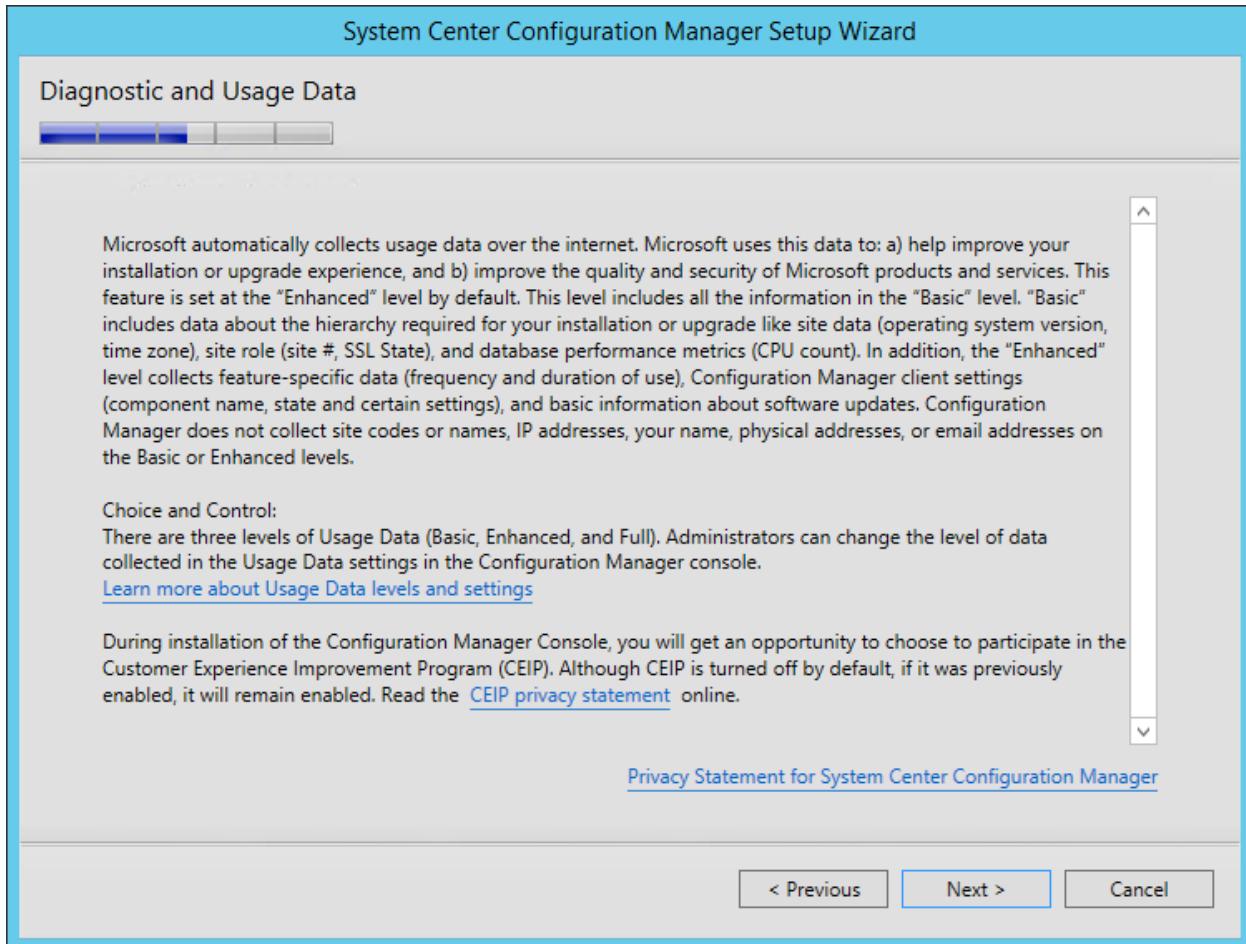
Set **Configure the communication method on each site system role** as a PKI infrastructure is not being used. Click **Next**.



Install both a **MP** and a **DP** onto the site server. Click **Next**.

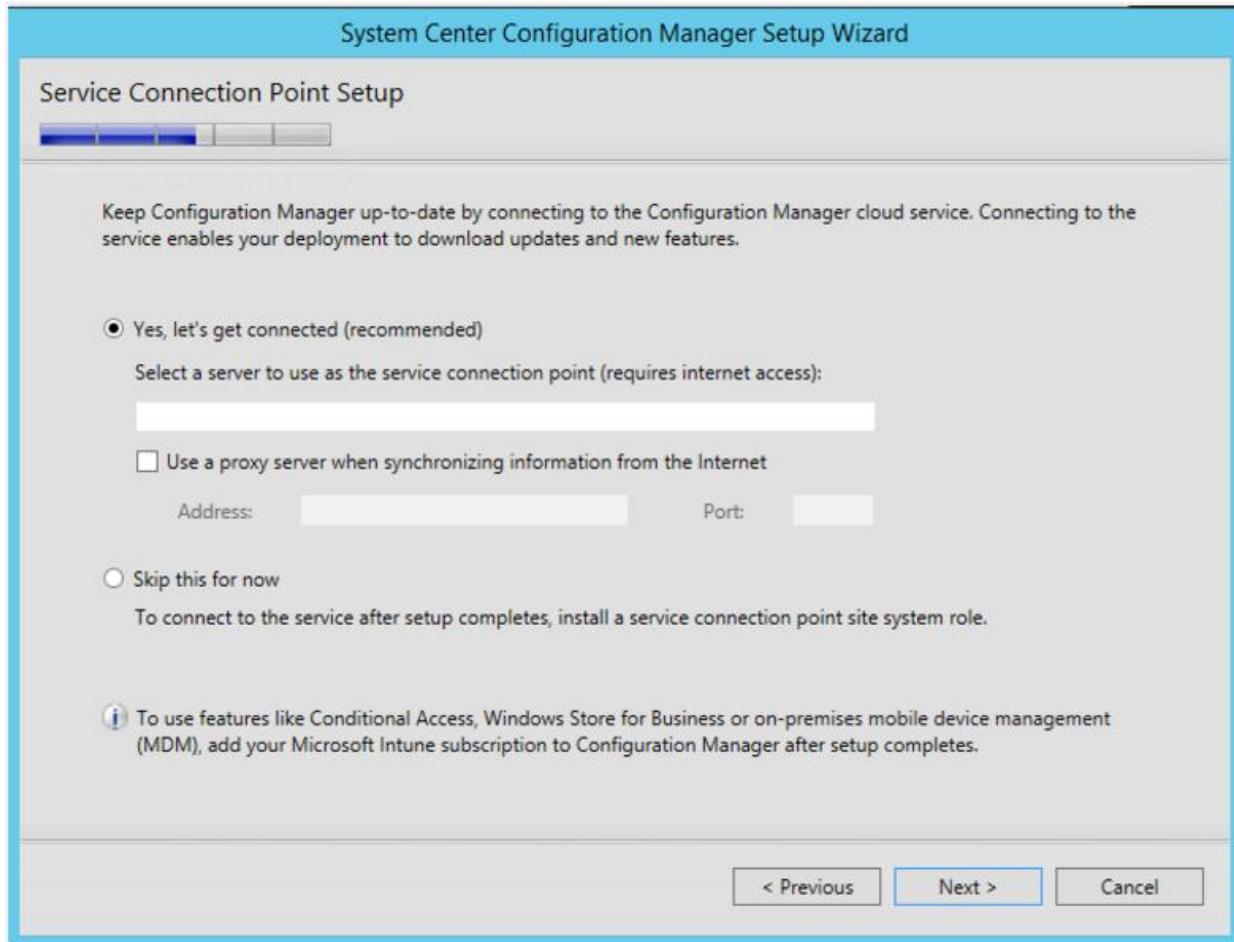


Click **Next** at the Usage Data screen.

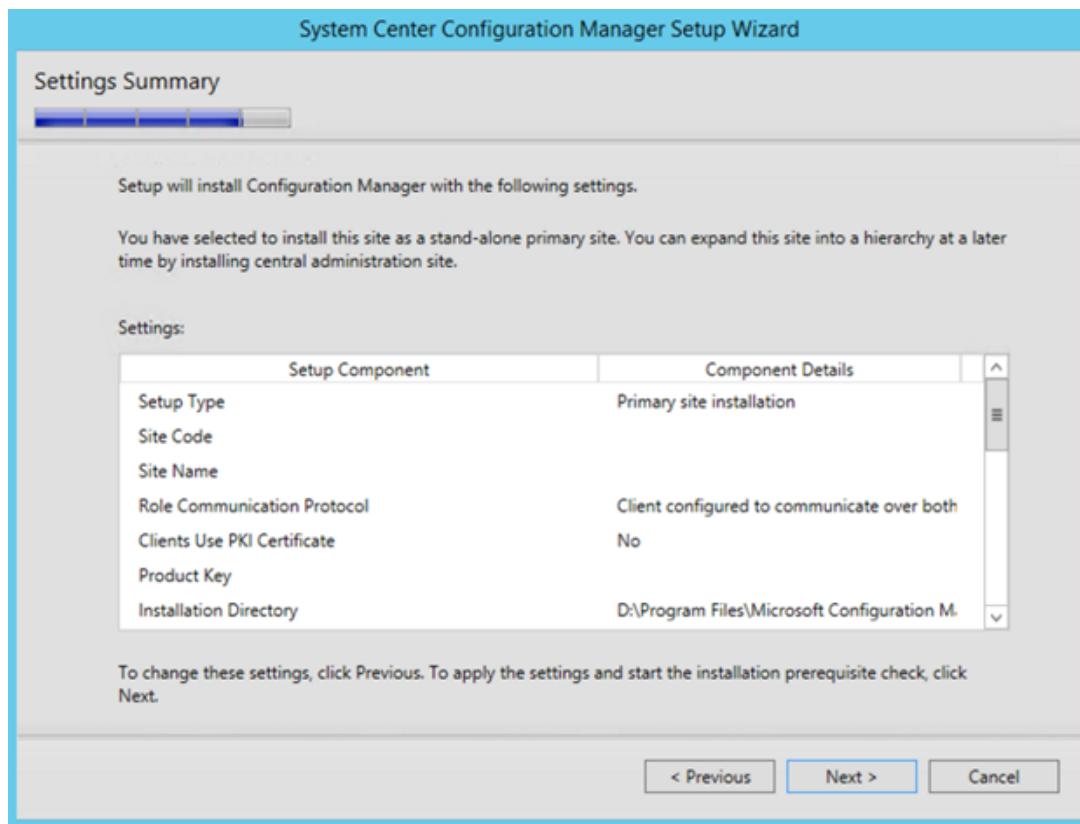


Select **Yes, let's get connected** to take advantage of the new Service Connection Point feature. Click

Next.

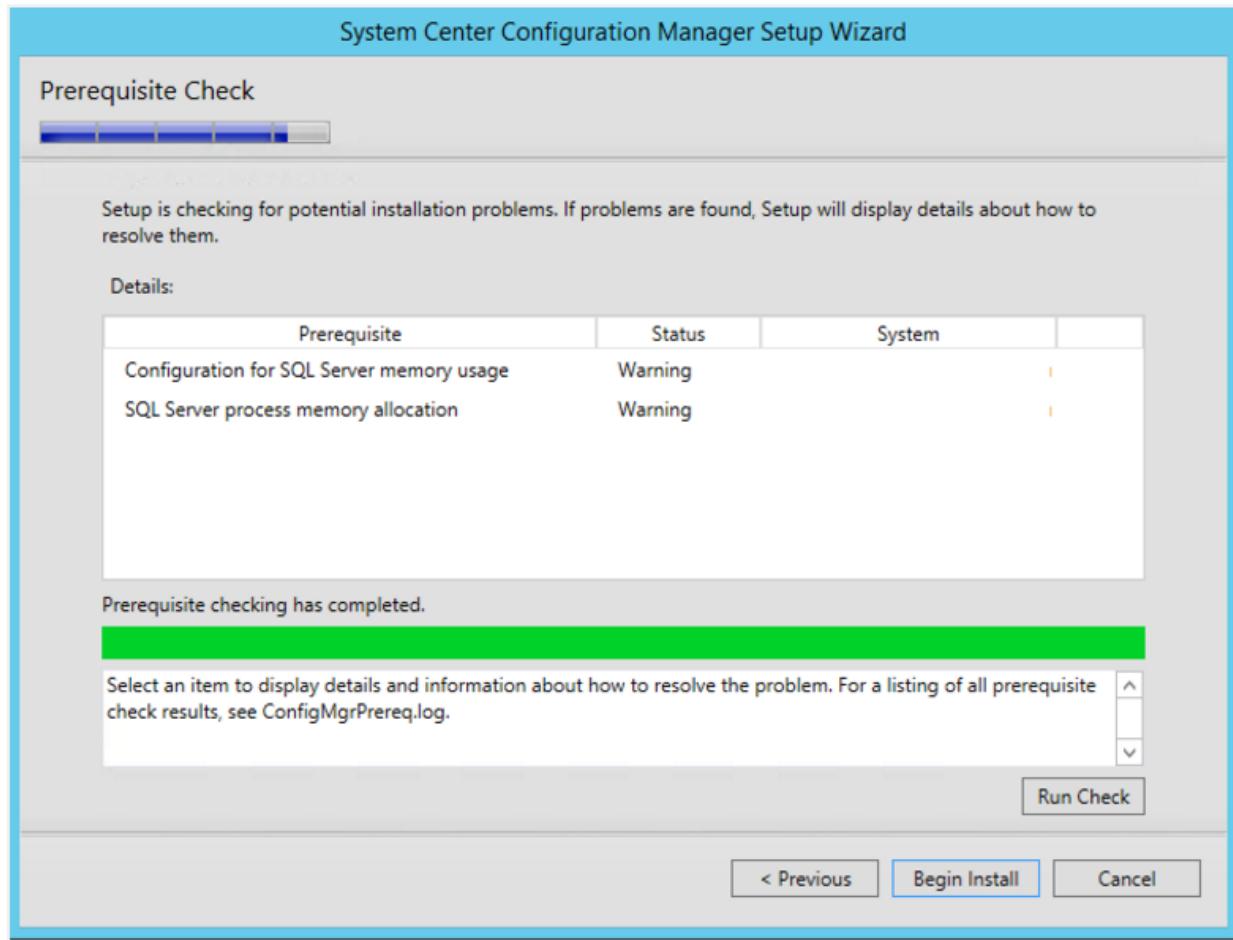


Click **Next** at the Summary Screen.

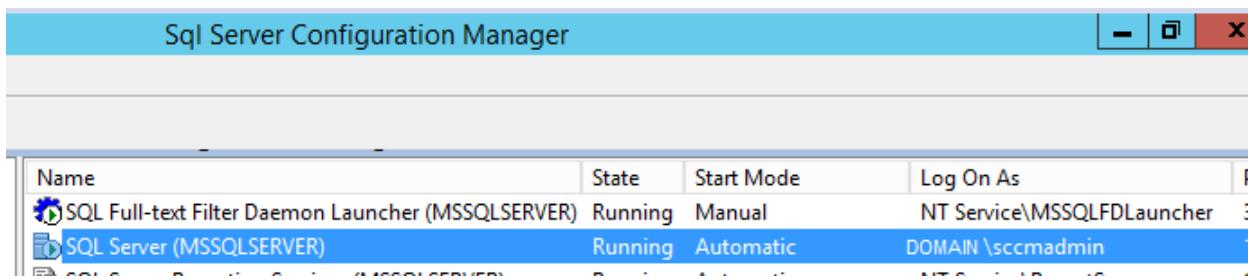


Pre-requisite checks will run. Address any failed statuses. You may have to change the SQL Server service to run with a **domain** service account.

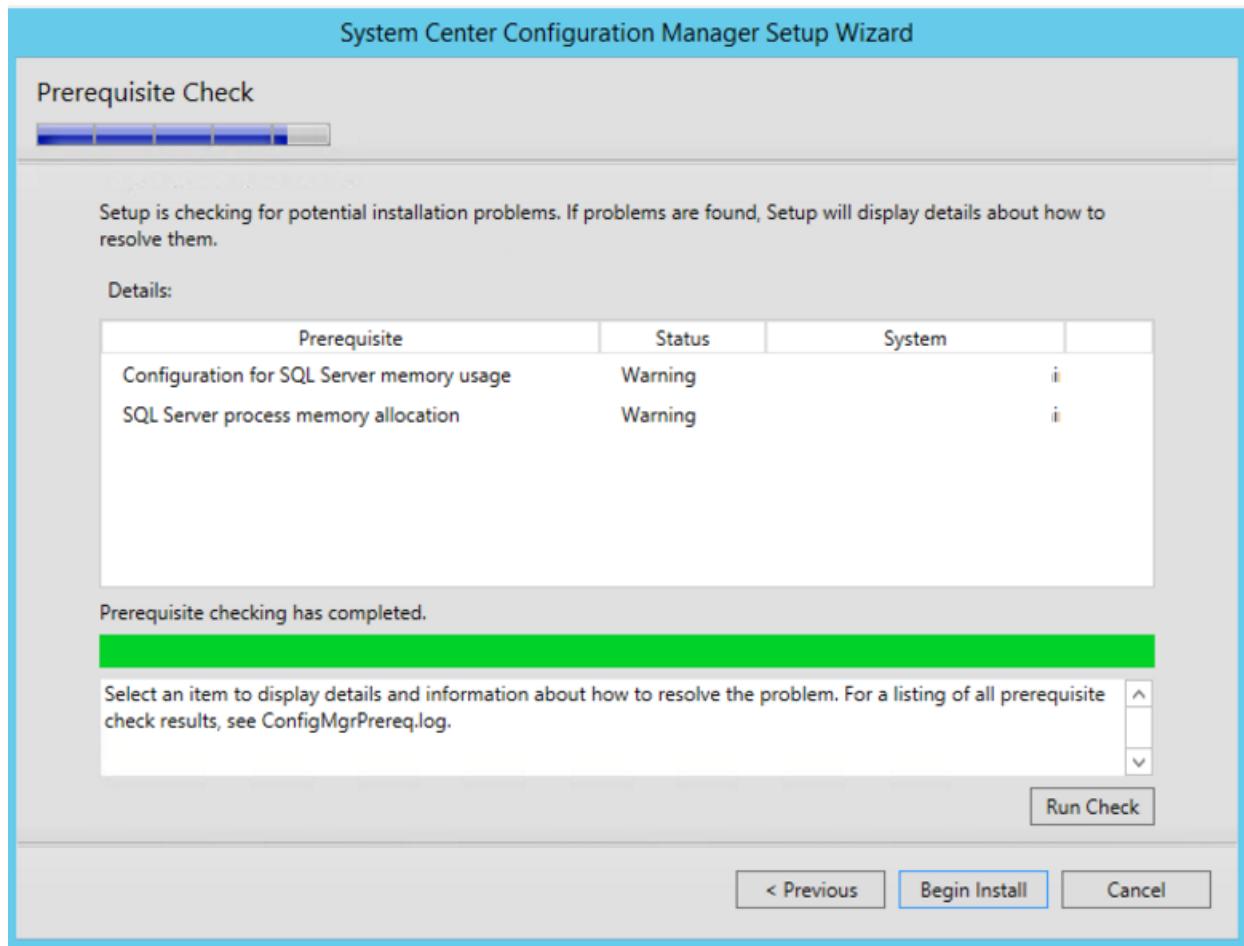
Note: Ignore any Warning statuses.

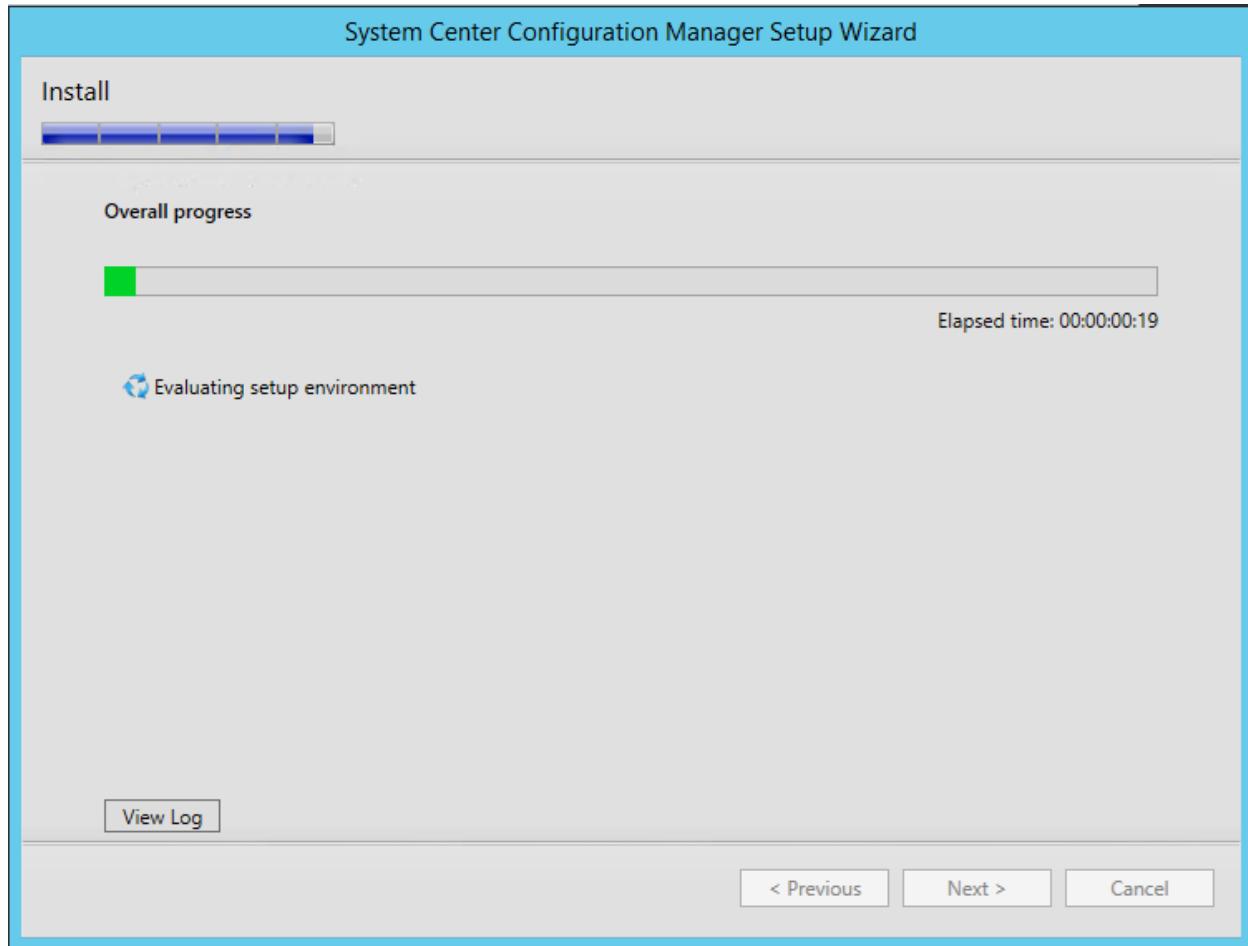


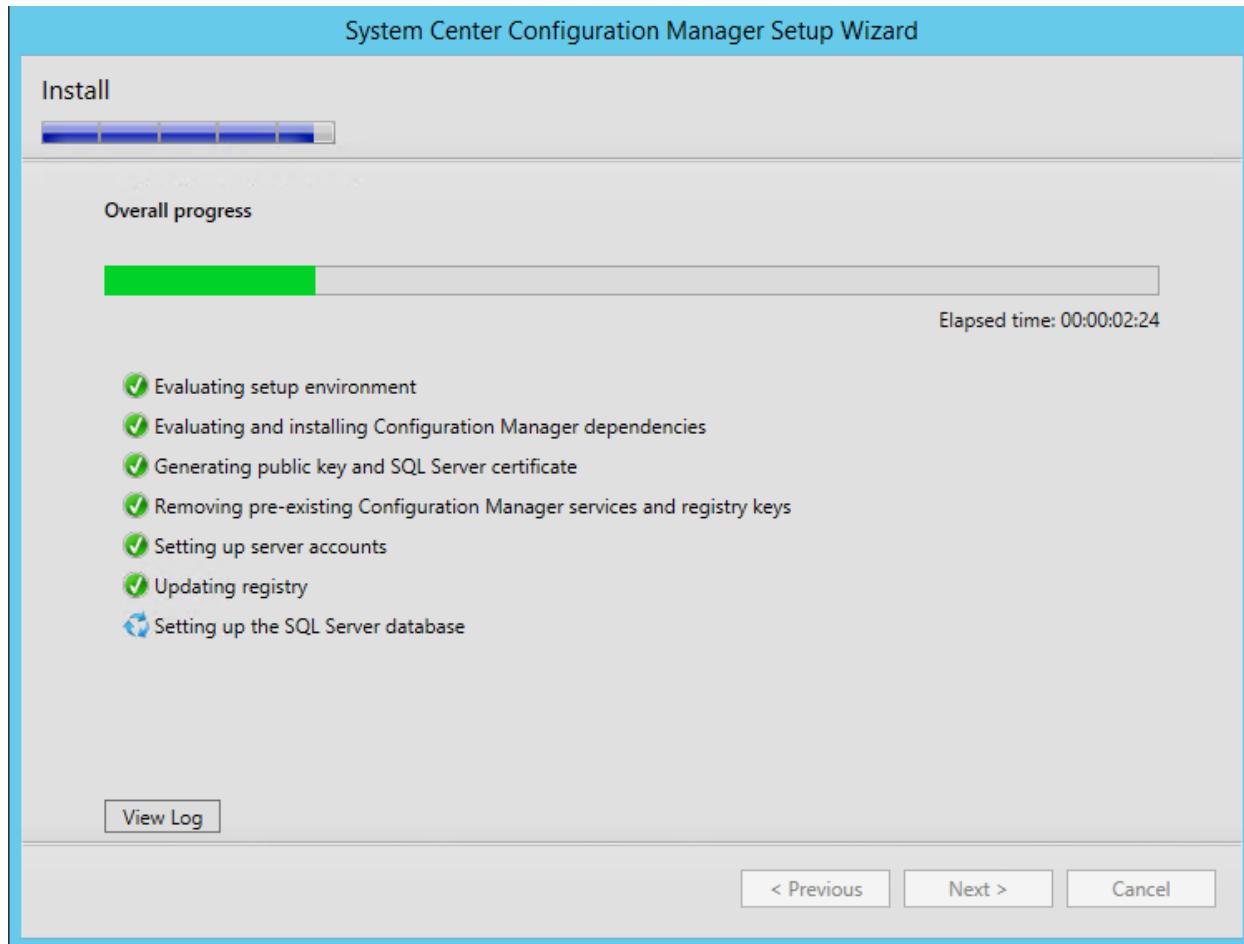
If you do have a SQL error, the SQL Server service should use a **domain** account.



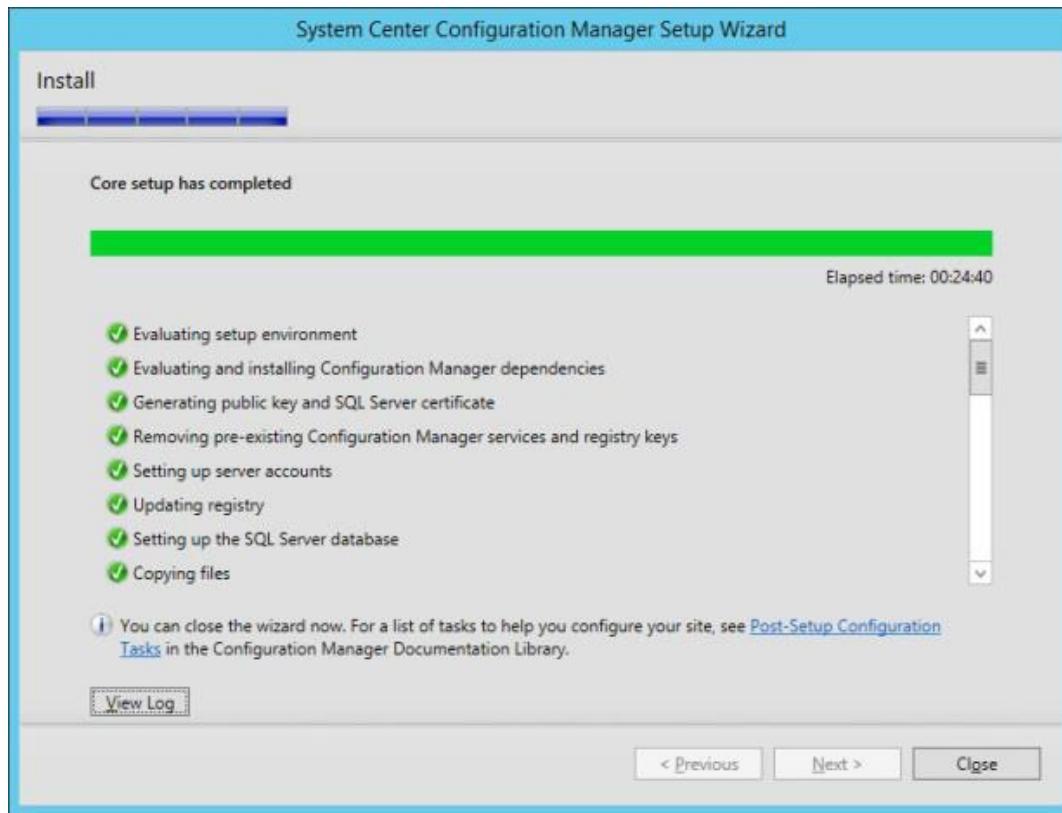
You can continue on Warnings, but take a look at those post install. Click **Begin Install**.







Click **Close** once the installation has completed.



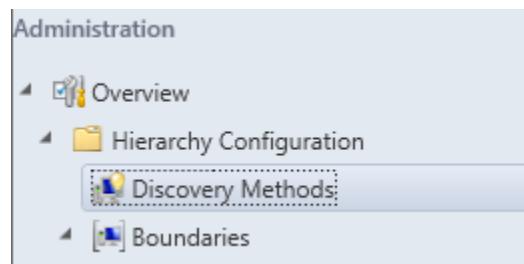
Launch the **SCCM Console**. Ensure the **site and database** report as **healthy** in the **Monitoring** workspace under **System Status > Site Status**.

Site Status 7 items							
Icon	Status	Site System	System Role	Storage...	Total	Site Code	
✓	OK	\sccm.DOMAIN.com	Component server	\SCCM...	60 GB	001	
✓	OK	\sccm.DOMAIN.com	Distribution point	\sccm....	60 GB	001	
✓	OK	\sccm.DOMAIN.com	Service connection point	\SCCM...	60 GB	001	
✓	OK	\sccm.DOMAIN.com	Management point	\SCCM...	60 GB	001	
✓	OK	\sccm.DOMAIN.com	Site server	\sccm....	60 GB	001	
✓	OK	\sccm.DOMAIN.com	Site database server	CM_00...	5 GB	001	
✓	OK	\sccm.DOMAIN.com	Site database server	CM_00...	379.4 MB	001	

Discovery Methods and Boundary Configuration

Once the **Site Status** is all green, now it is time to configure the **Discovery Methods** and **Boundaries**.

Under **Administration**, select **Discovery Methods**.



Now, in the right pane, we want to ‘enable’ System Discovery and User Discovery.

Discovery Methods 6 items			
Icon	Name	Status	Site
!	Active Directory Forest Discovery	Disabled	001
!	Active Directory Group Discovery	Disabled	001
!	Active Directory System Discovery	Disabled	001
!	Active Directory User Discovery	Disabled	001
!	Heartbeat Discovery	Disabled	001
!	Network Discovery	Disabled	001

Add the appropriate AD Computer OU in System Discovery.

Active Directory System Discovery Properties

General Polling Schedule Active Directory Attributes Options

Active Directory System Discovery

Configure the settings to find computers in Active Directory Domain Services.

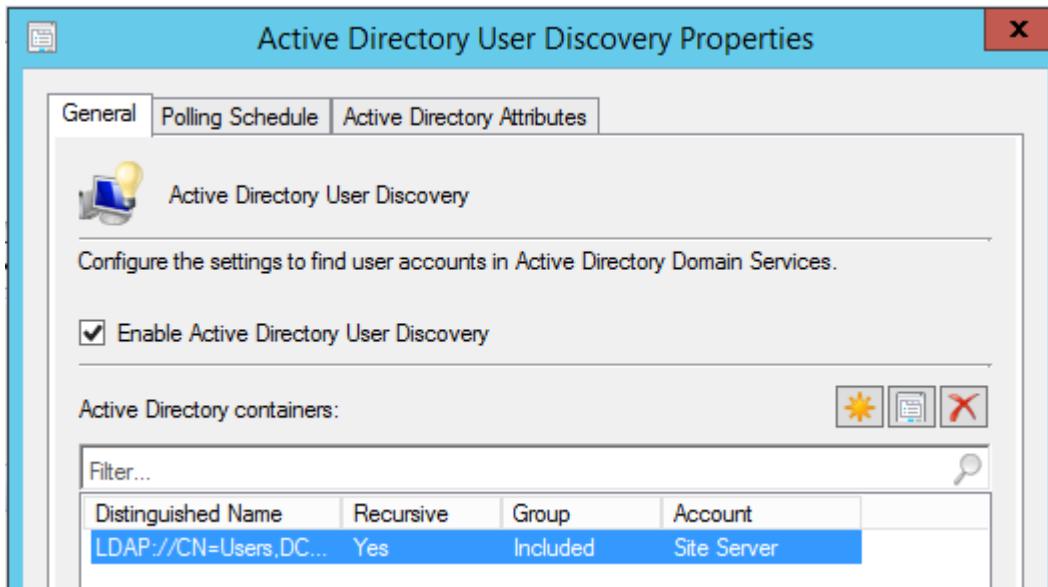
Enable Active Directory System Discovery

Active Directory containers:

Filter...

Distinguished Name	Recursive	Group	Account
LDAP://CN=Computers,DC...	Yes	Included	Site Server

Add the appropriate AD User OU in **System Discovery**.



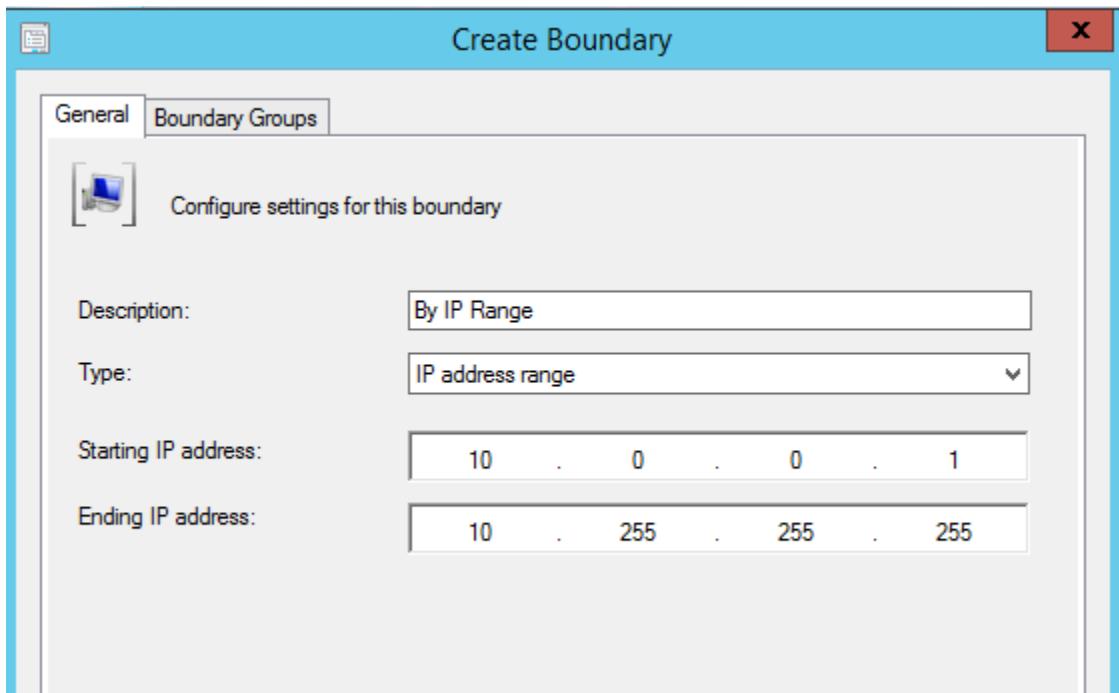
Now, **System Discovery** and **User Discovery** should be **enabled**.

Active Directory Forest Discovery	Disabled	001
Active Directory Group Discovery	Disabled	001
Active Directory System Discovery	Enabled	001
Active Directory User Discovery	Enabled	001
Heartbeat Discovery	Enabled	001
Network Discovery	Disabled	001

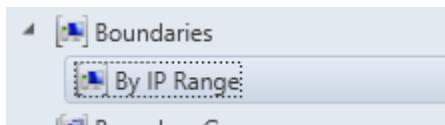
Next, Select **Boundaries** and right-click to **Create Boundary**.



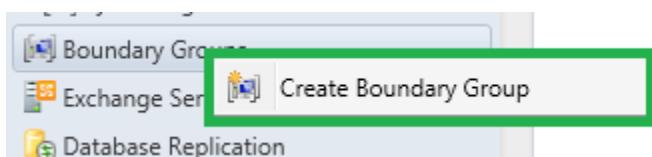
I selected **IP address range**, and entered the range of my network. Eventually, you'll want to select by Active Directory Site.



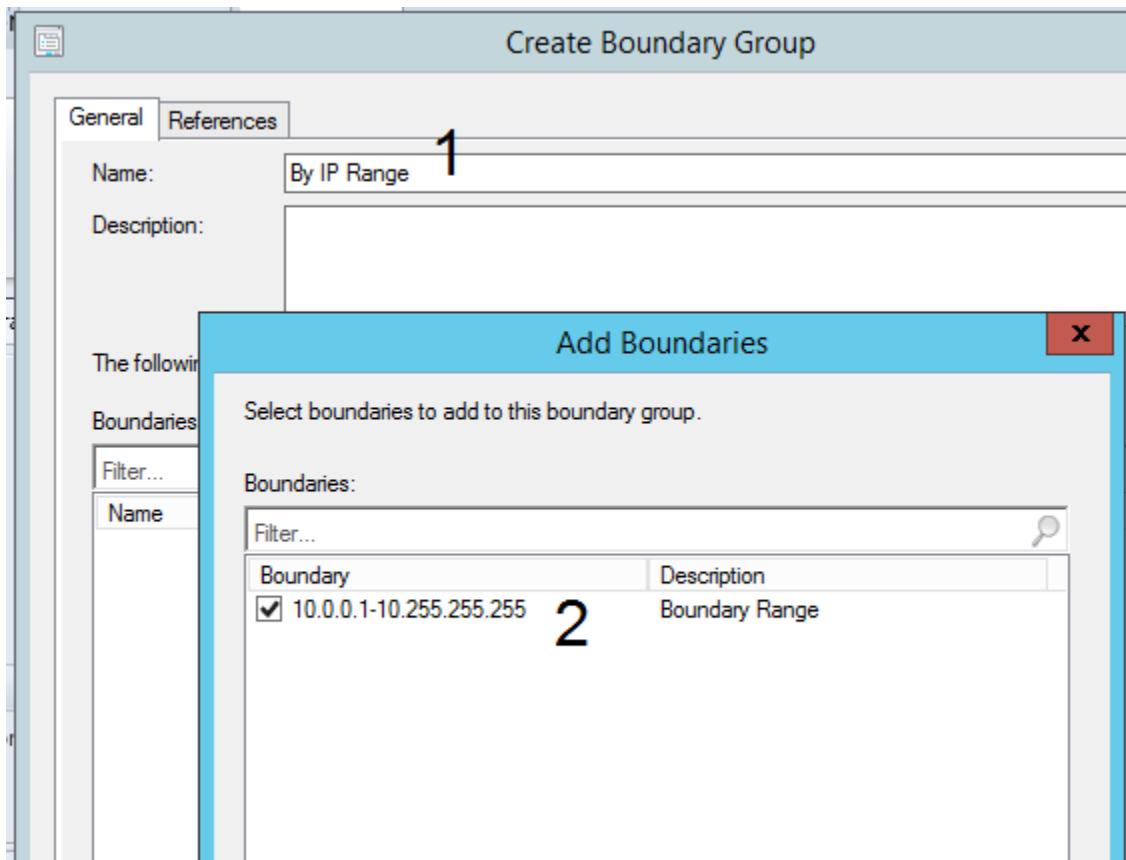
You will see it appear under Boundaries: By IP Range.



Under **Boundary Groups**, right-click to **Create Boundary Group**.



Add Name of Group and click Add Boundary button, select the range, click OK.

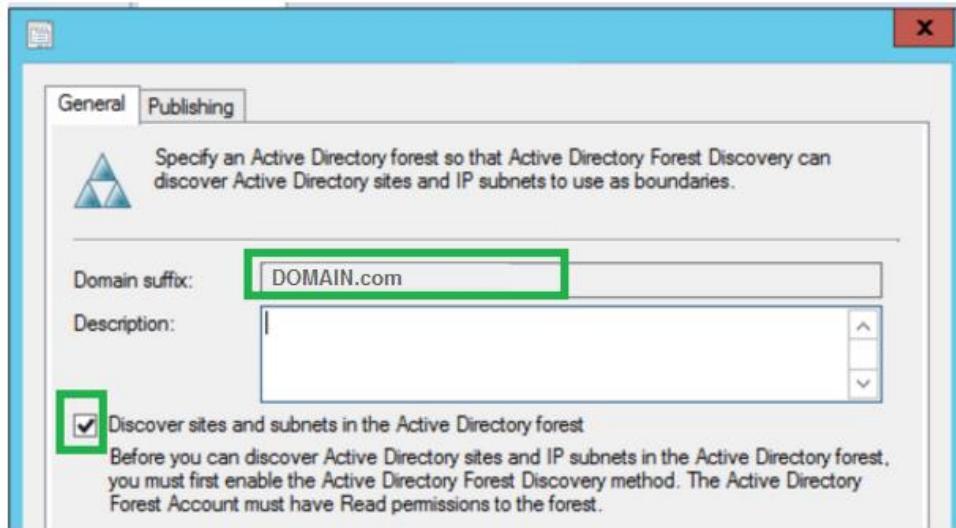


Verify a **Forest** exists in SCCM, if not, add one.

The following screenshot shows the SCCM Administration interface under the 'Active Directory Forests' section. A single item named 'DOM..' is listed in the table, which is highlighted with a green border.

Icon	Do...	Description	Date Created
△		DOM..	3/20/2017 11:37 AM

If you need to add a domain suffix, just **add suffix** and check **Discover sites and subnets**.



Prompt a **System Discovery** (this will scan AD looking for devices). **Right-click** and select **Run Full Discovery Now**.

Icon	Name	Status	Site	Description
💡	Active Directory Forest Discovery	Disabled	001	Configures set
💡	Active Directory Group Discovery	Disabled	001	Configures set
💡	Active Directory System Discovery			
💡	Active Directory User Discovery			
💡	Heartbeat Discovery			
💡	Network Discovery			

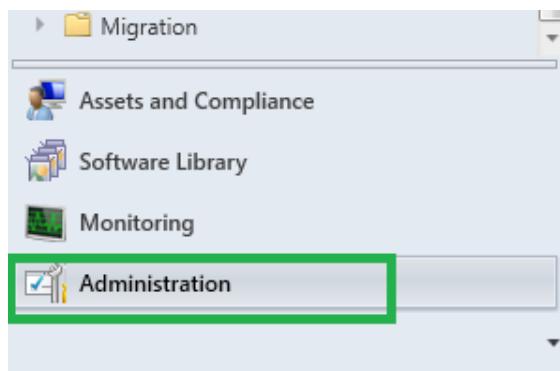
A context menu is open over the 'Active Directory System Discovery' row. The menu items are: 'Run Full Discovery Now' (with a green arrow pointing to it), 'Refresh' (with a green arrow pointing to it), and 'Properties'.

Under **Assets and Compliance, Devices**, check devices for **Client Type**, **Site Code**, and **Activity** (this will not be instant; it takes several minutes—let's say 10 minutes).

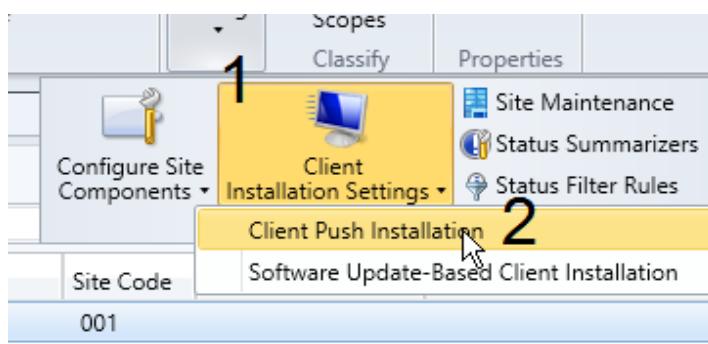
All Systems 1 items					
Icon	Name	Client Type	Client	Site Code	Client Activity
✓	CLIENTW7	Computer	Yes	001	Active
✓	SCCM	Computer	Yes	001	Active
💻	x64 Unknown Computer...	None	No	001	
💻	x86 Unknown Computer...	None	No	001	

Enable Automatic Client Push

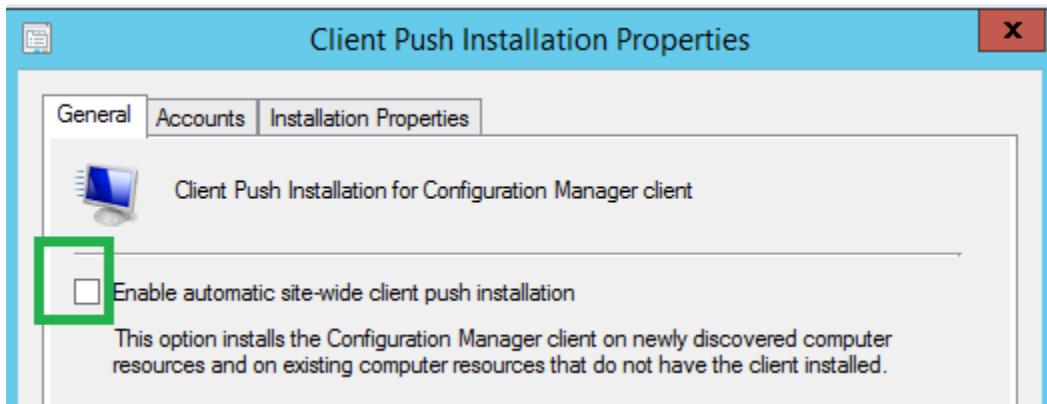
To enable **automatic** client pushes, select **Administration**.



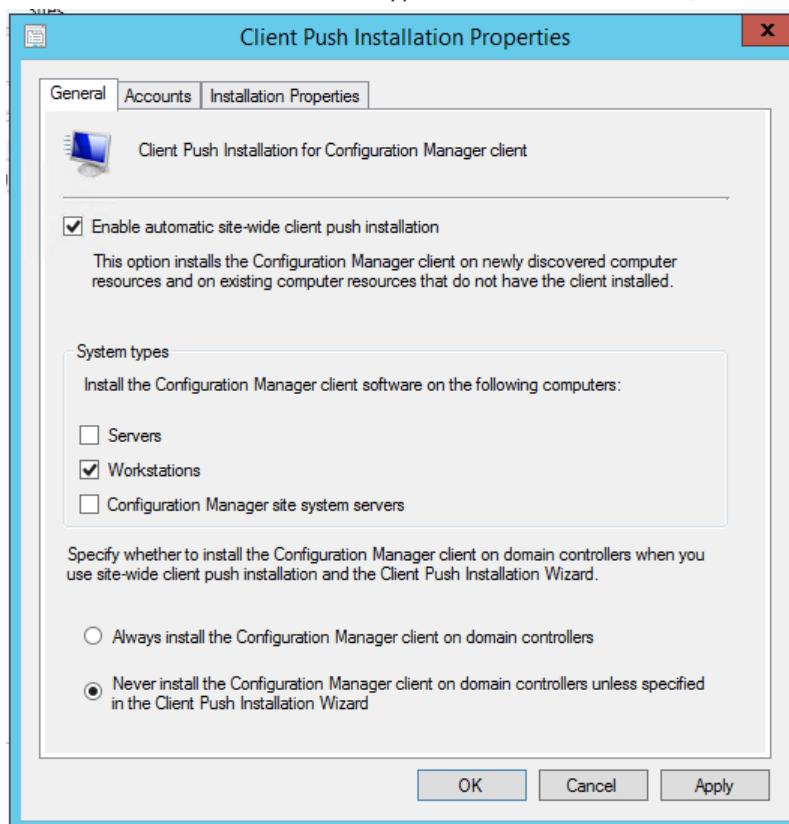
Next, click **Site**, then click the **Client Installation Settings** option on the ribbon and then choose **Client Push Installation**.



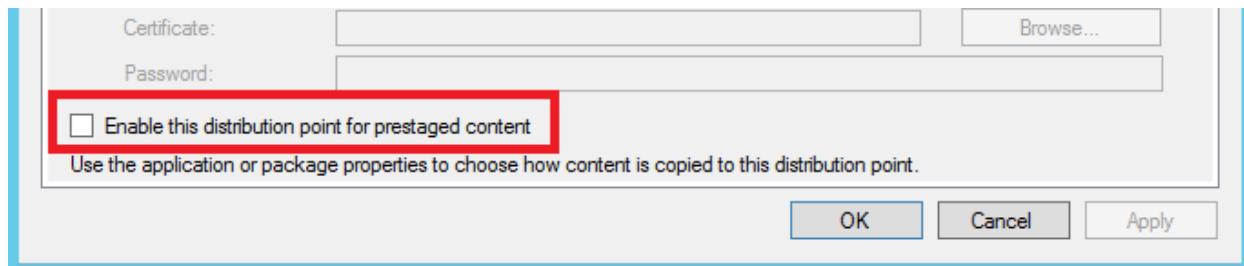
Then, check the **Enable automatic site-wide client push installation**. The jury is out on whether or not this is best practice. Some say this setting should not be used once you roll out to your enterprise; a better solution is to use Group Policy to deploy the client. Though, in all honesty, if the AD schema has been properly extended, and you don't have other primary servers in your enterprise, automatic push should be fine.



Add a **check** next to the device types to receive the client, click **OK** to continue.

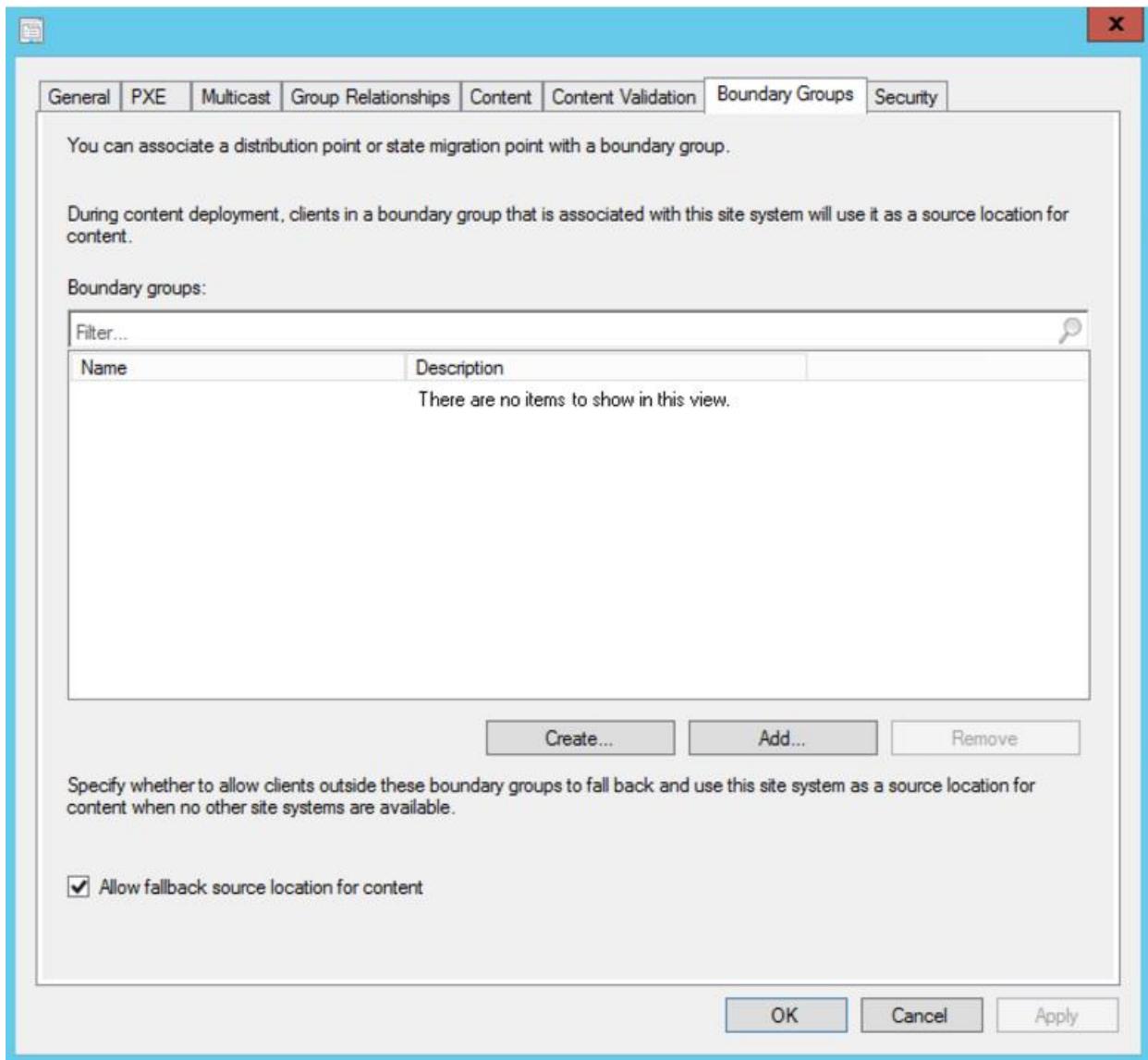


NOTE: If the workstations are **not receiving** the client, make sure **prestaged content** has **NOT** been checked under the **Distribution Point** (right-click on Distribution Point, select properties).

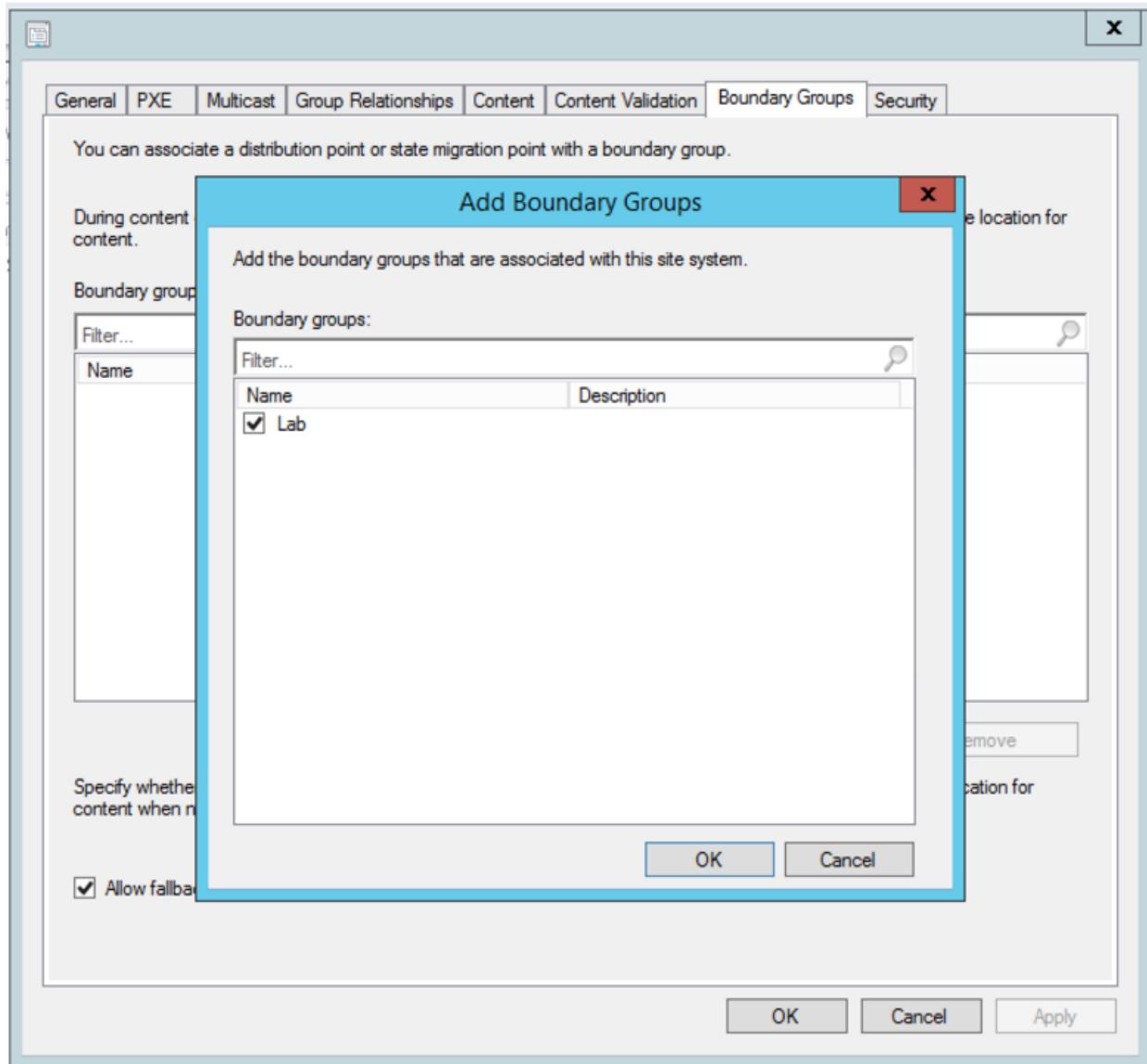


Add Distribution Point to Boundary Groups

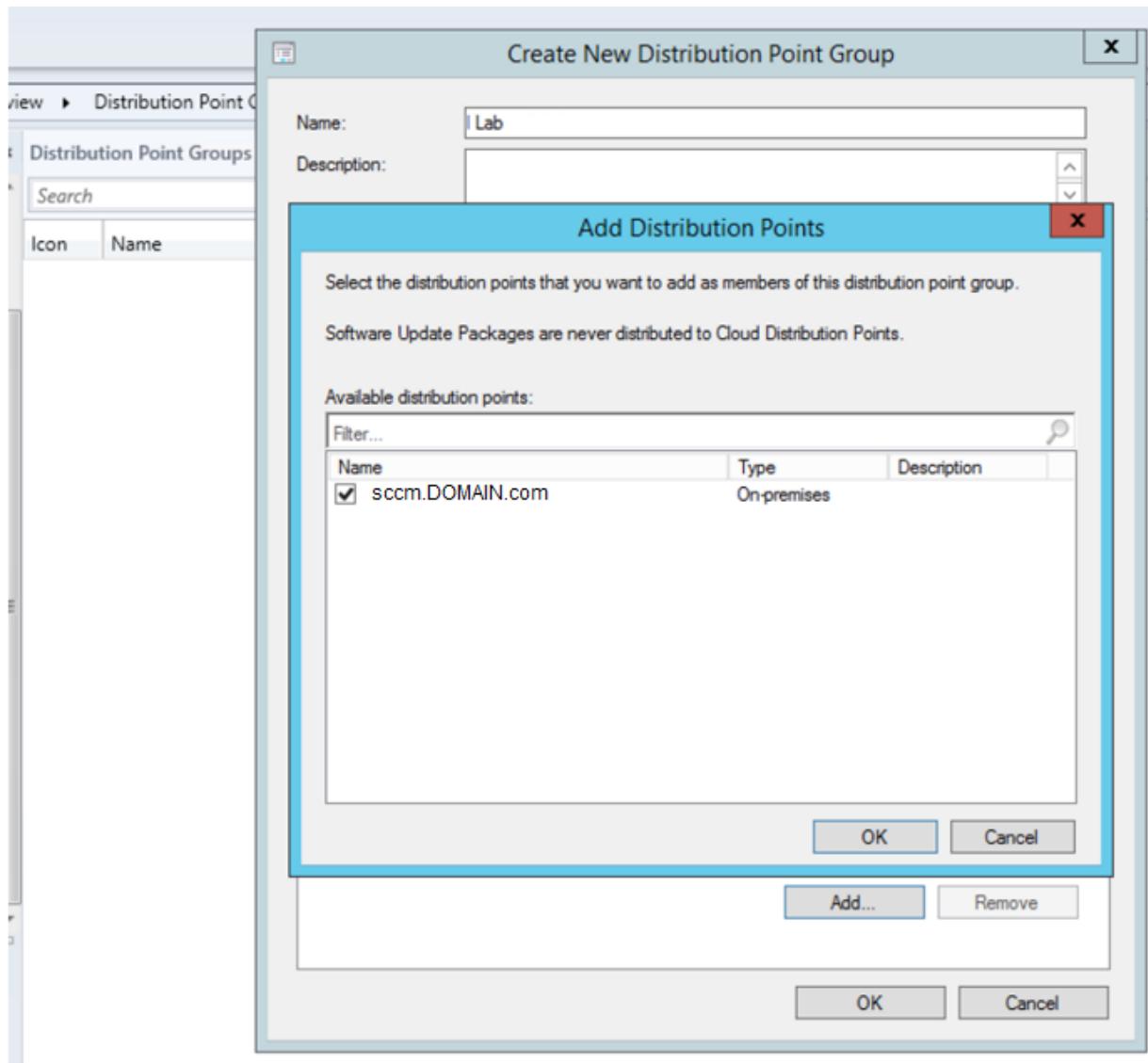
To add a **Boundary Group** to a **Distribution point**, click **Administration > Distribution Points** > right-click on the configured **distribution point** and select **Properties**. Click the **Add** button.



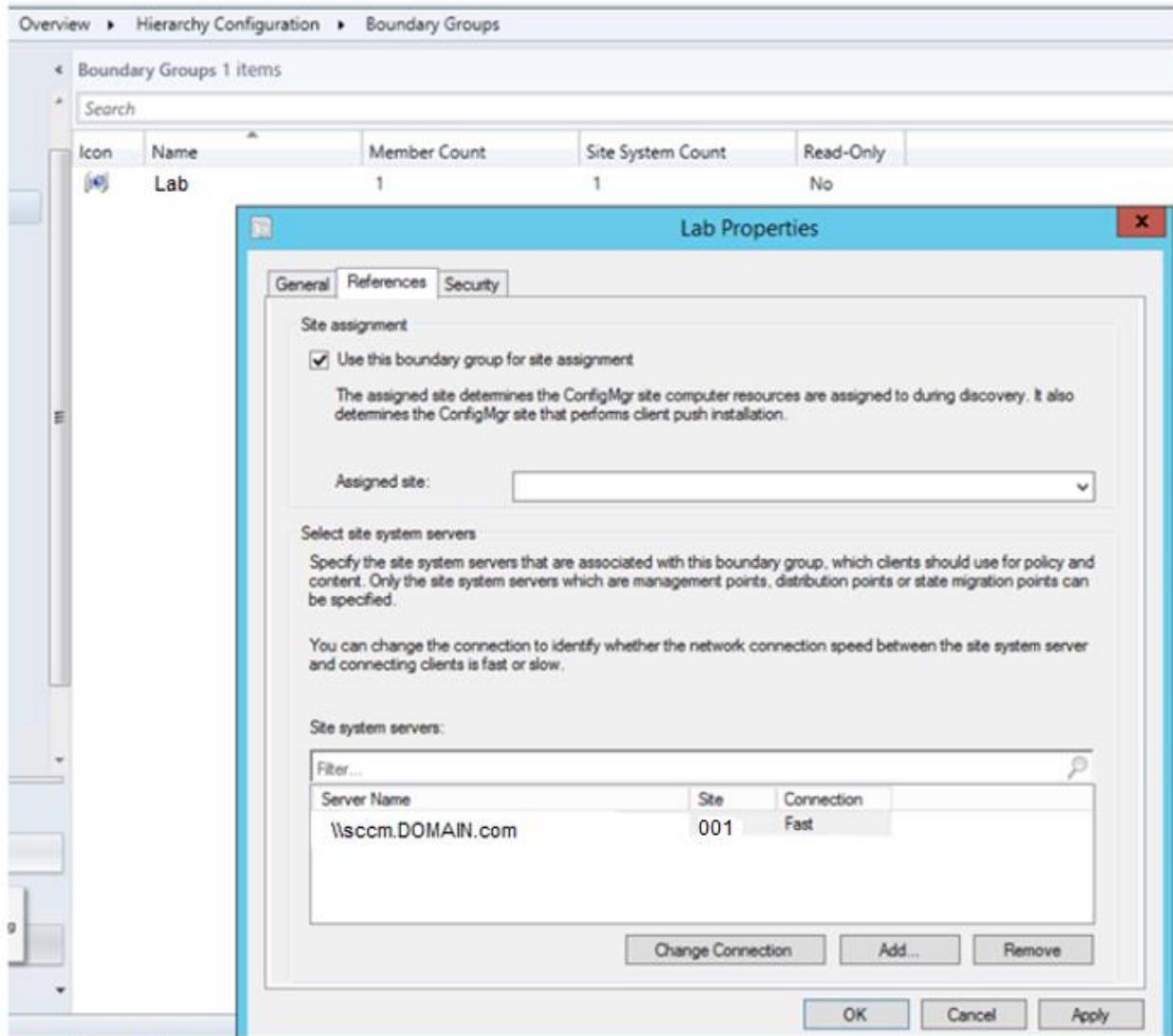
Check the managed **Boundary group**. Select **OK** to continue.



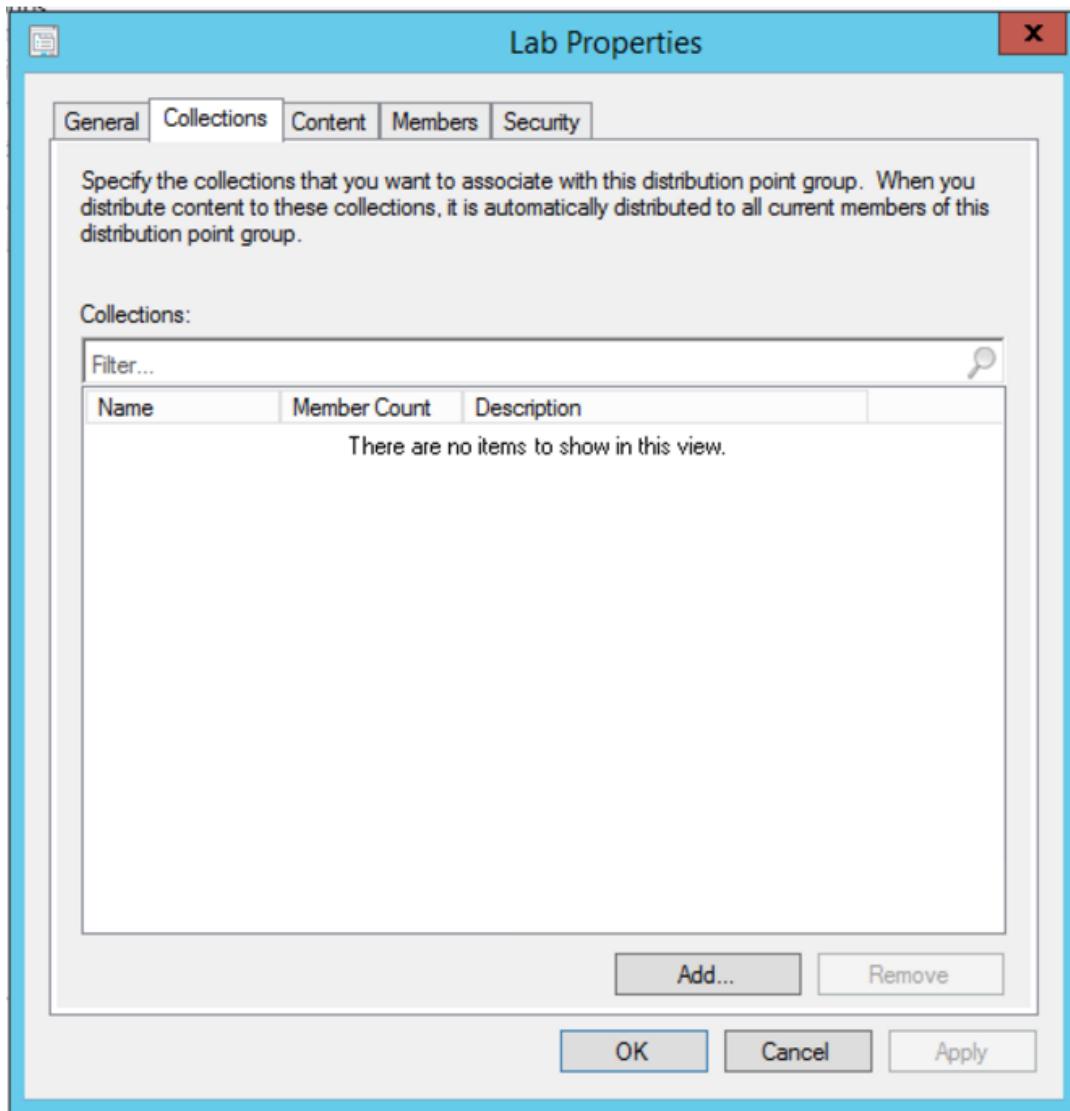
Next, create a **Distribution Group**, and link the group to the managed **Distribution Point**. Click **OK** and **OK** to finish configuring the Distribution setup.



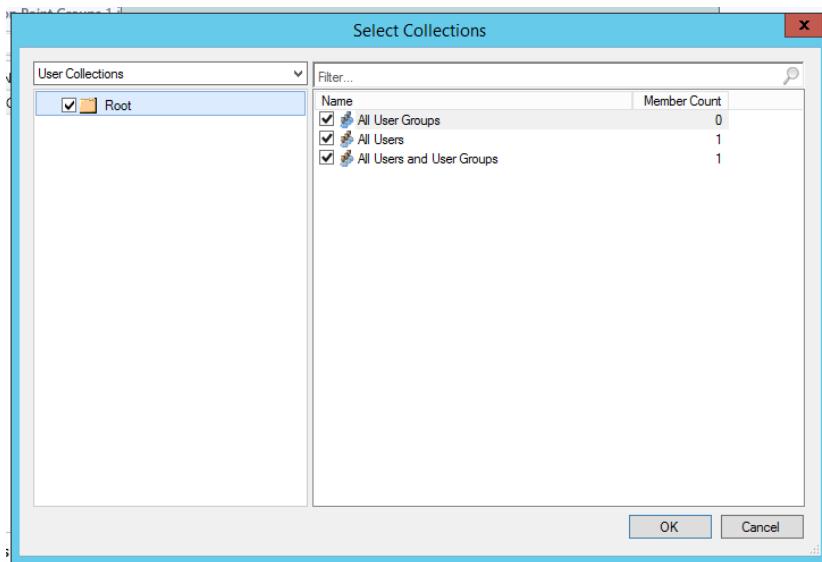
Now, link the managed **Boundary Group Site**, to any **Boundary Groups**. Select the **Boundary Group** (right-click and select properties), open the **References** Tab, and check the **Use this boundary group for site assignment**.



Next, link **Distribution Groups** to **Collections**. Select **Distribution Point Groups** (right-click and properties). Click **Add**.

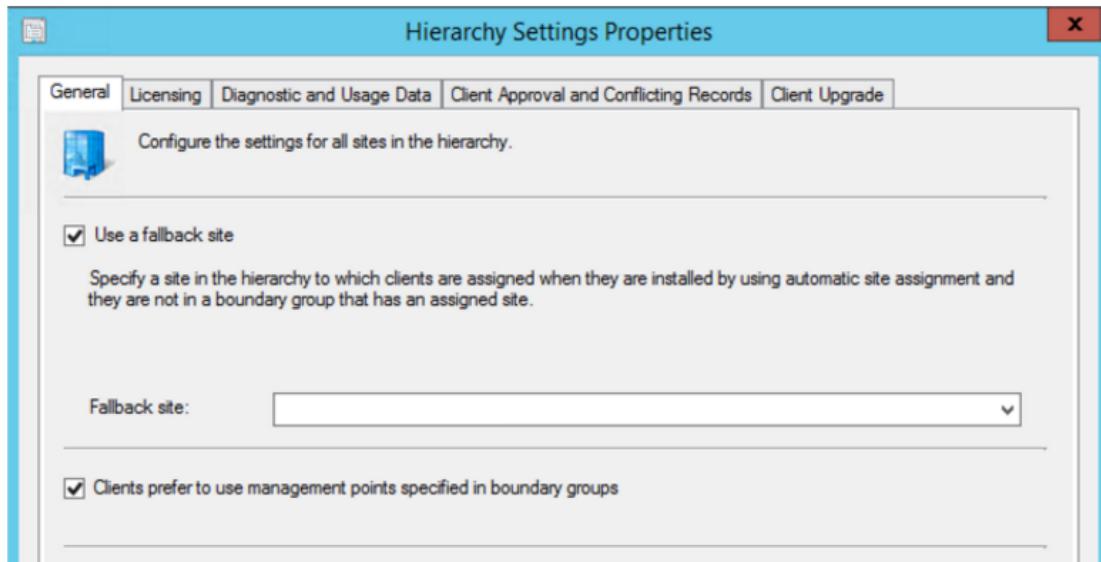


Select **Root**, and **OK** to continue.



Finally, under **Administration**, select **Sites**, right-click and select Properties. Check **Use a fallback site** (useful for catching clients outside of boundaries) and **Clients prefer to use management points in boundary groups**. **OK** to close.

Note, you may NOT want to select this option if you don't want to manage machines that haven't been specifically added to boundaries.



Updating SCCM Configuration Manager

Go to the **Updates and Servicing** under **Cloud Services** (or just below Overview). If there are any updates marked *Available*, the updates can be downloaded and installed. To do this, right-click on the update and select **Install Update Pack**.

The screenshot shows the SCCM Administration interface. In the navigation pane, a green arrow points down to the 'Updates and Servicing' link under the 'Administration' category. The 'Updates and Servicing' link is highlighted with a dashed border. In the main content area, a table titled 'Updates and Servicing 2 items' lists two updates:

Name	Date Released	State	Prereq Or
Configuration Manager 1602 Hotfix (KB3155482)	27-05-2016 14:09:00	Available	No
Configuration Manager 1602	09-05-2016 14:09:00	Available	No

A context menu is open over the second row (Configuration Manager 1602). The menu items are:

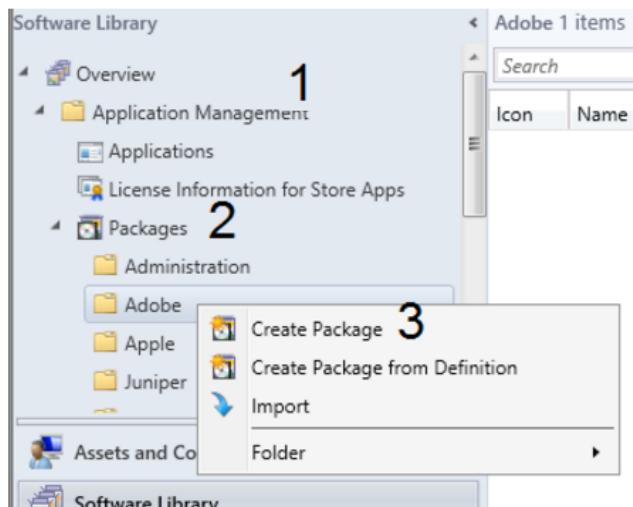
- Install Update Pack (highlighted with a green box and labeled '1')
- Run prerequisite check
- Retry installation
- Client Update Options

The 'Install Update Pack' option is highlighted with a green box and labeled '2'.

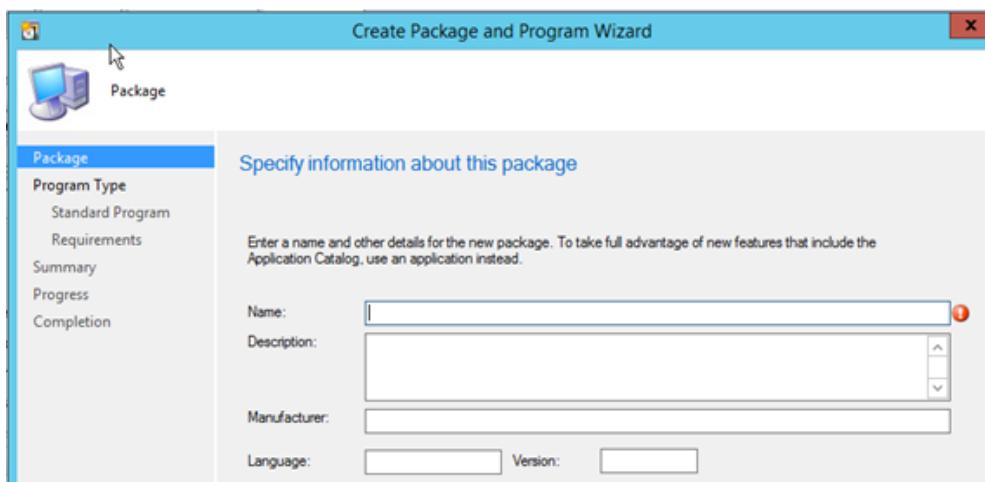
Create a Package

To deploy a package, you must first **Create** the package in SCCM. To start, access **Software Library**.

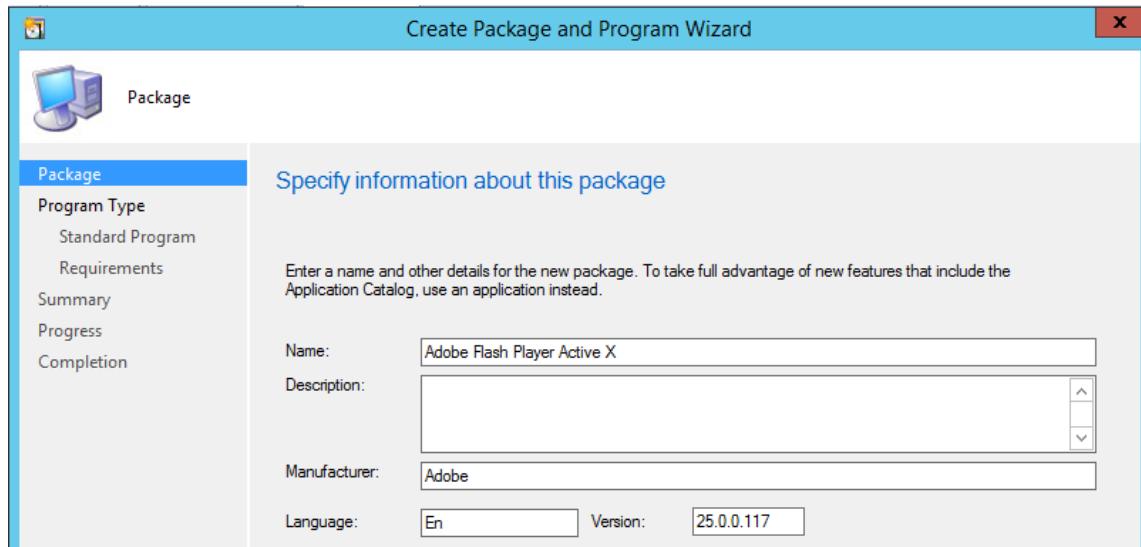
Then, **Application Management > Packages** and right-click on **Packages** and select **Create Package**.



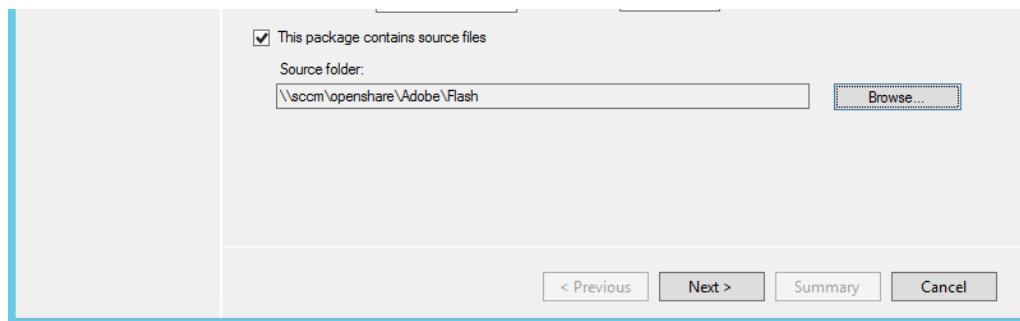
Now, start a package by **entering the details** of the package.



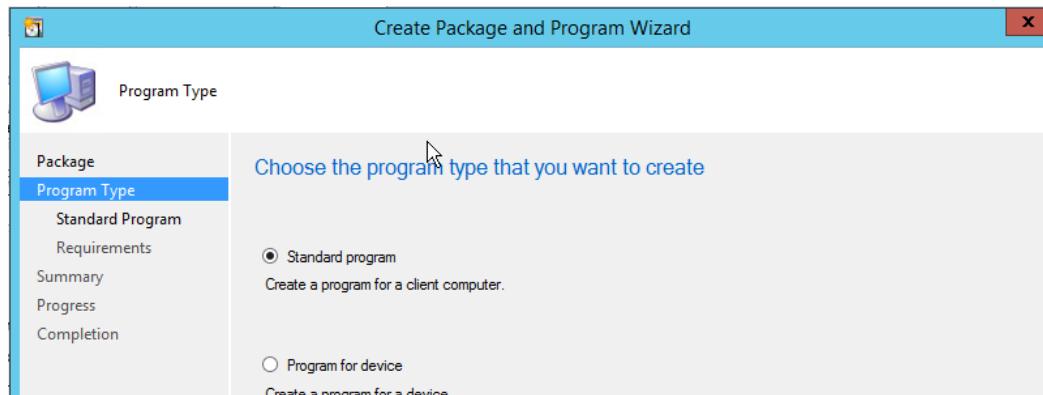
Package with Details



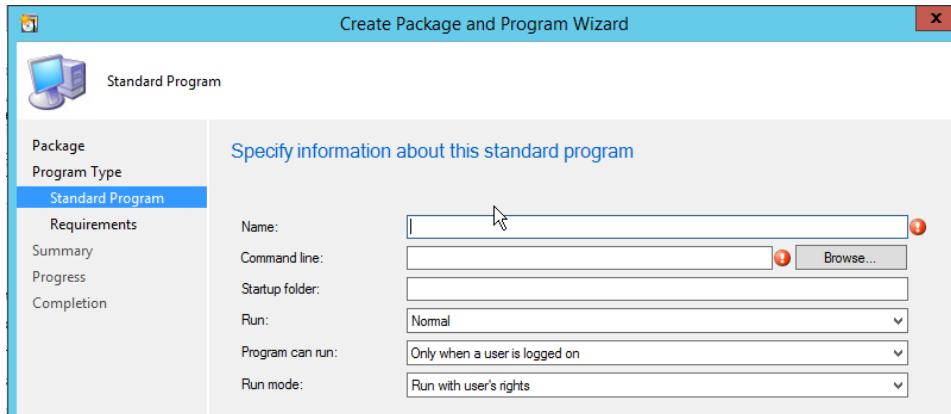
Then, check **This package contains source files** and select **FQDN UNC path** to source files. Click **Next** to continue.



Select **Standard program**. Click **Next** to continue.



Now, enter standard program information.



Once complete, click **Next** to continue.

Specify information about this standard program

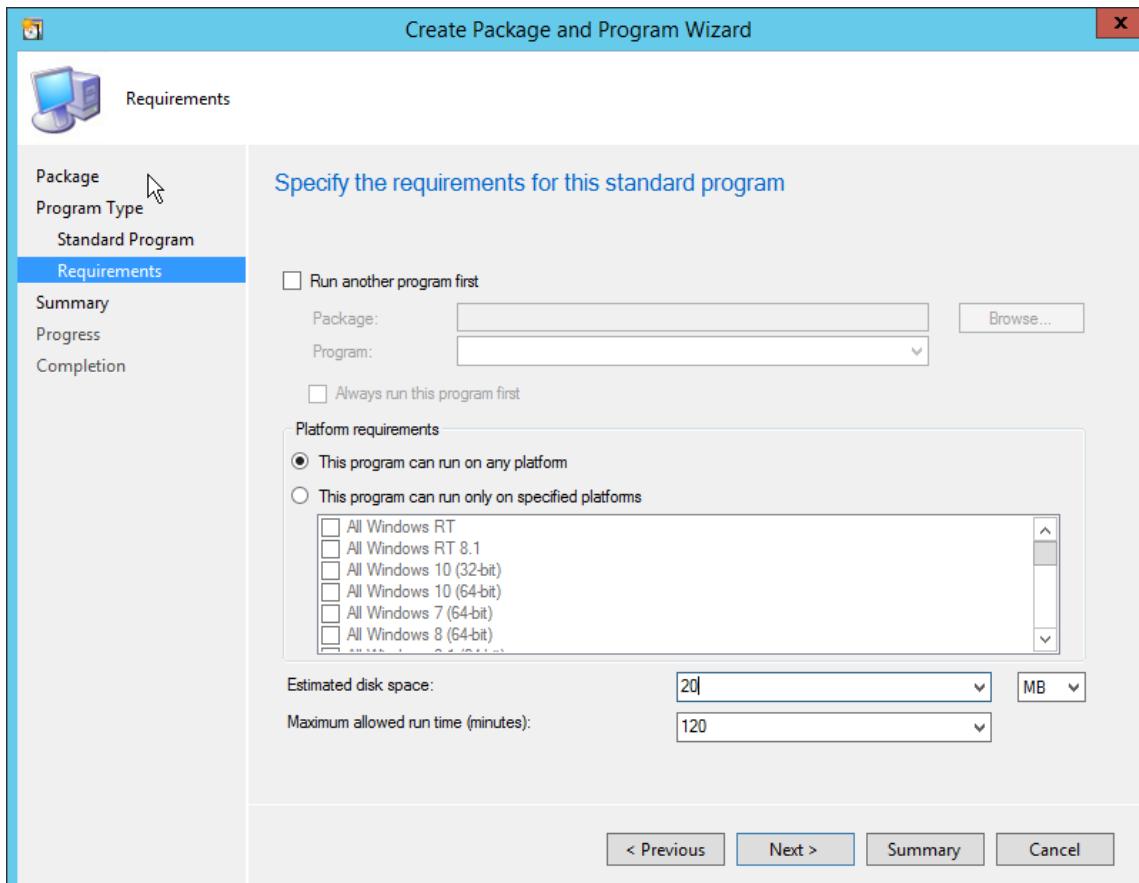
Name:	<input type="text"/> (SDP)
Command line:	<input type="text"/> Adobe_Flash_Player_25.0.0.148_Active_X_! <input type="button" value="Browse..."/>
Startup folder:	<input type="text"/>
Run:	Normal
Program can run:	Only when a user is logged on
Run mode:	Run with administrative rights

Allow users to view and interact with the program installation

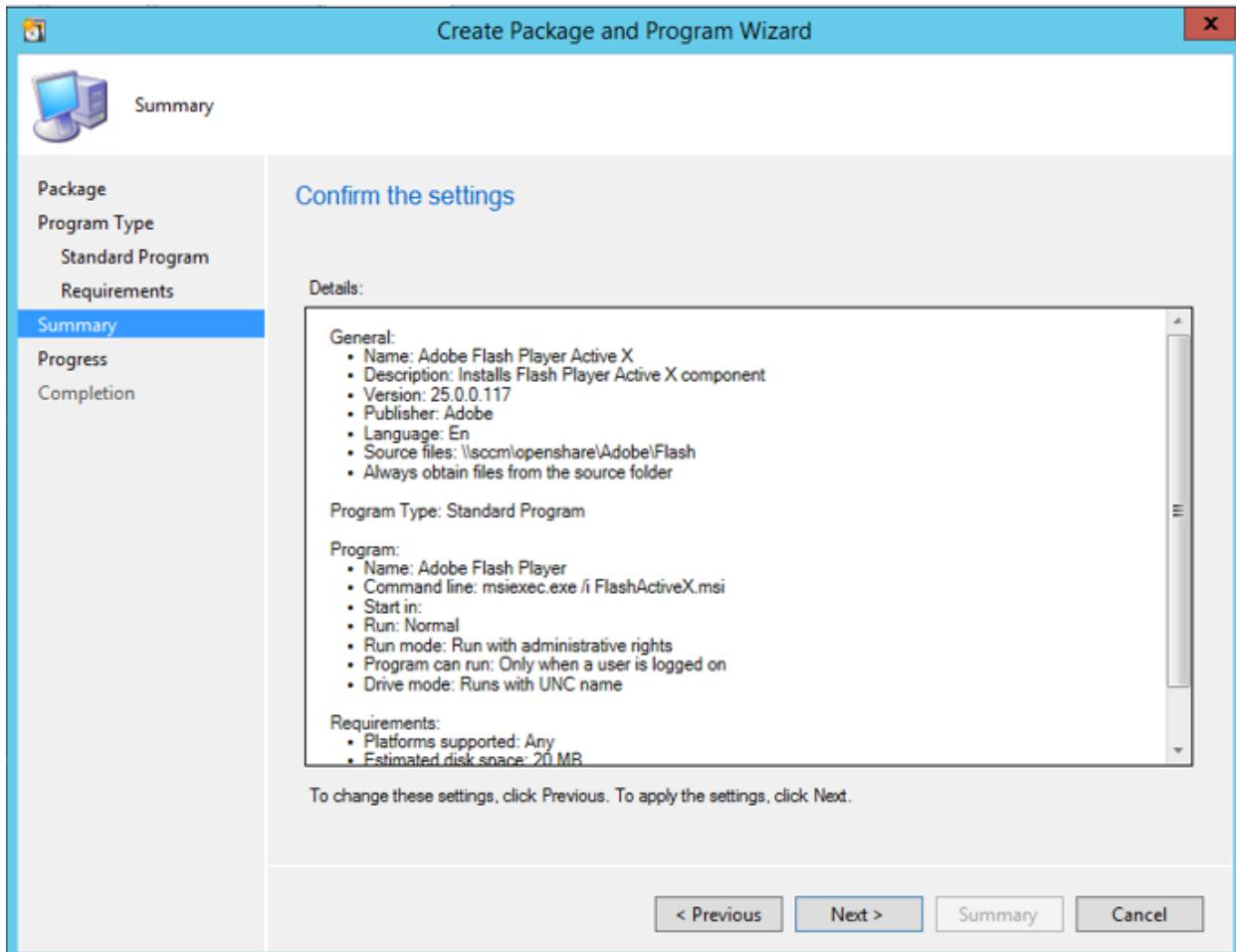
Drive mode: Runs with UNC name

Reconnect to distribution point at log on

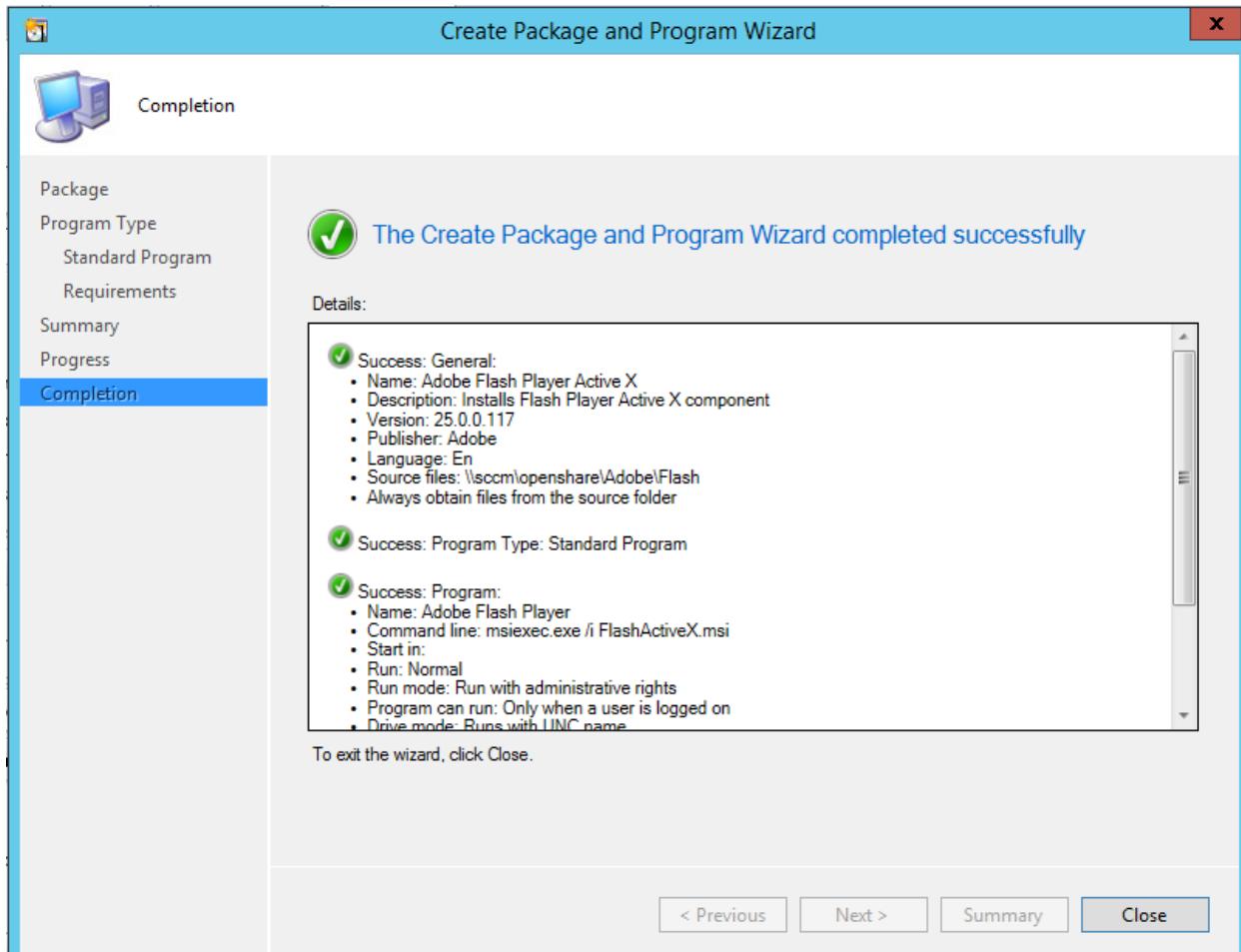
On the next screen, you can specify the **estimated disk space** and **platform**, then click **Next** to continue.



Review the summary screen, if everything is okay, click **Next** to continue.

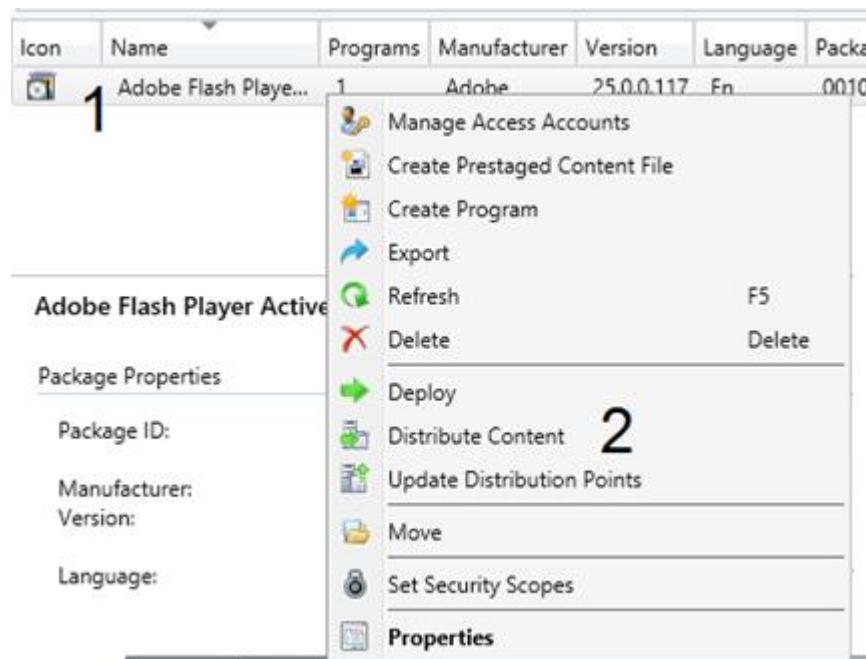


At this point, you have successfully created a package and program in SCCM. Click **Close**.

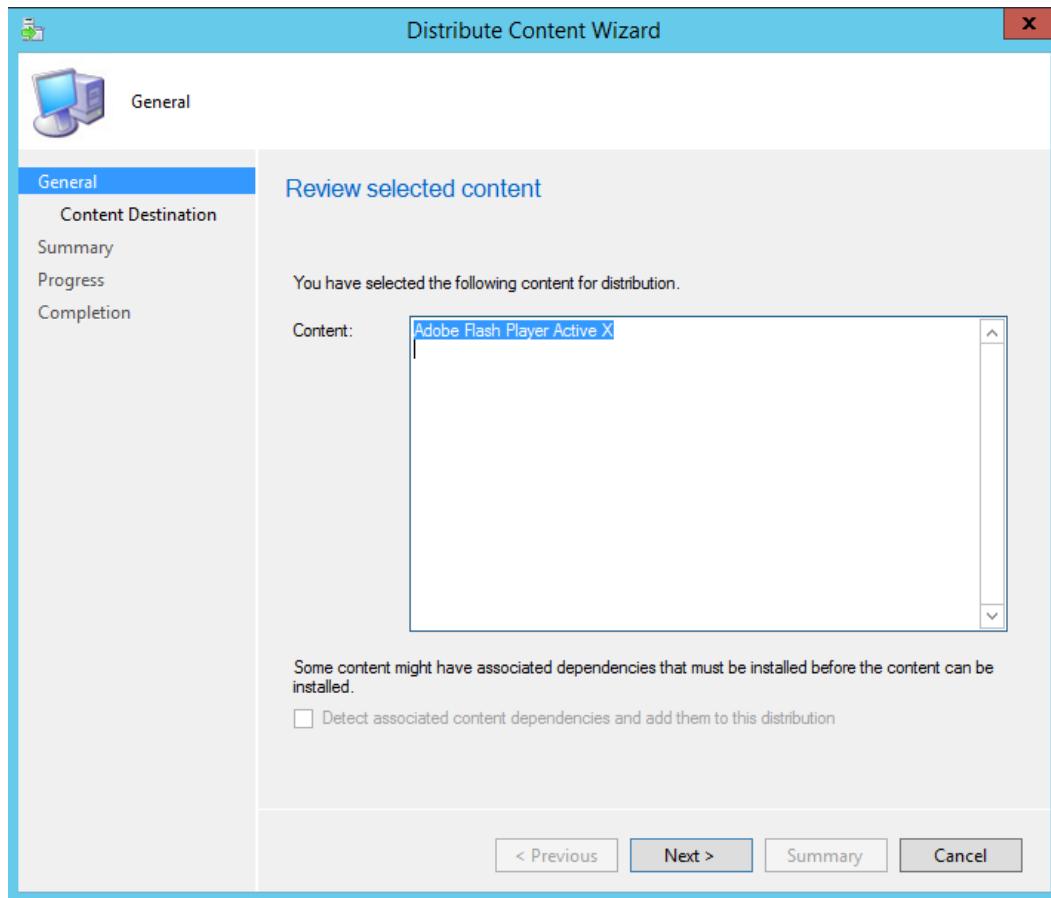


Pre-Deploy a Package

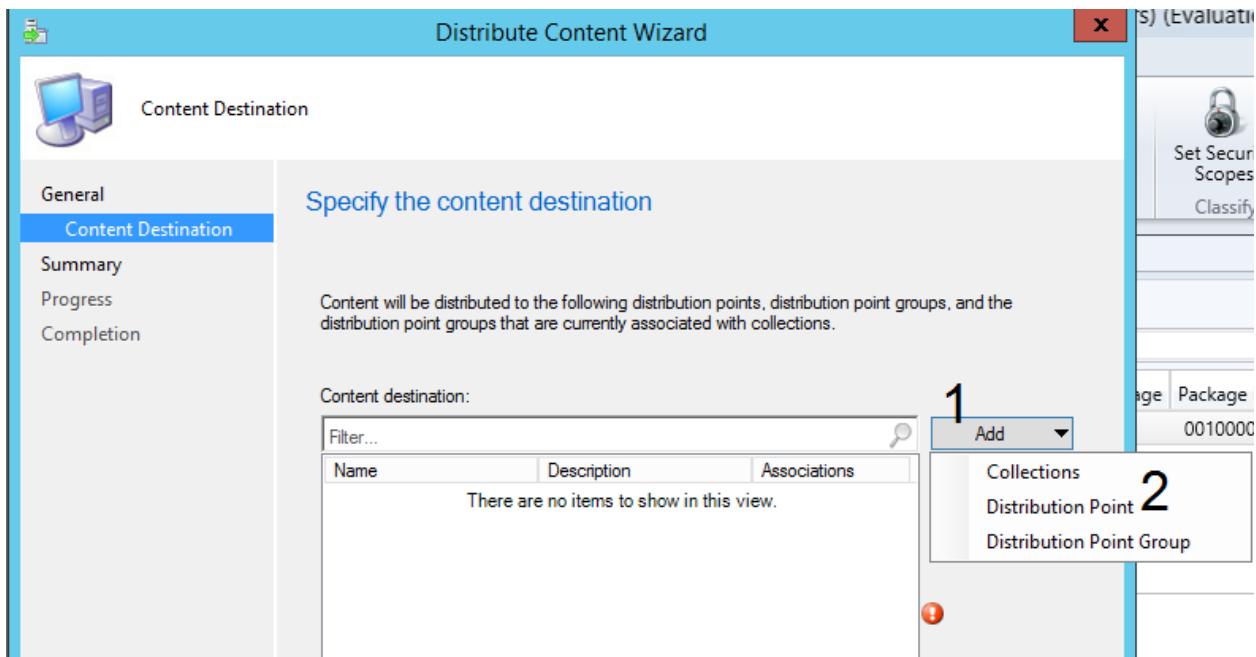
Once a package has been **Created** in SCCM, now you can set up a deployment. It is good practice to make sure the package has been **added to the distribution point** (if it has not, it will not deploy). To do this, right-click on the **package**, and select **Distribute Content**. You can then monitor the distribution status under **Administration > Monitoring > Content Status**.



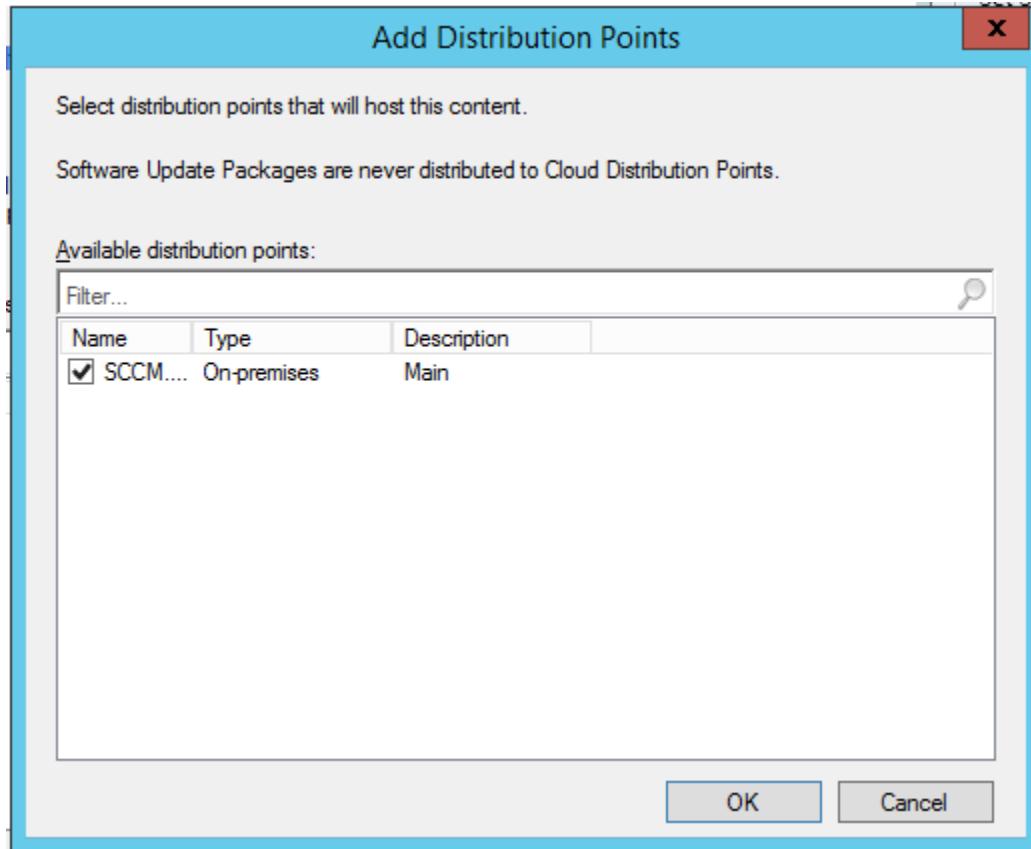
Click **Next** to continue.



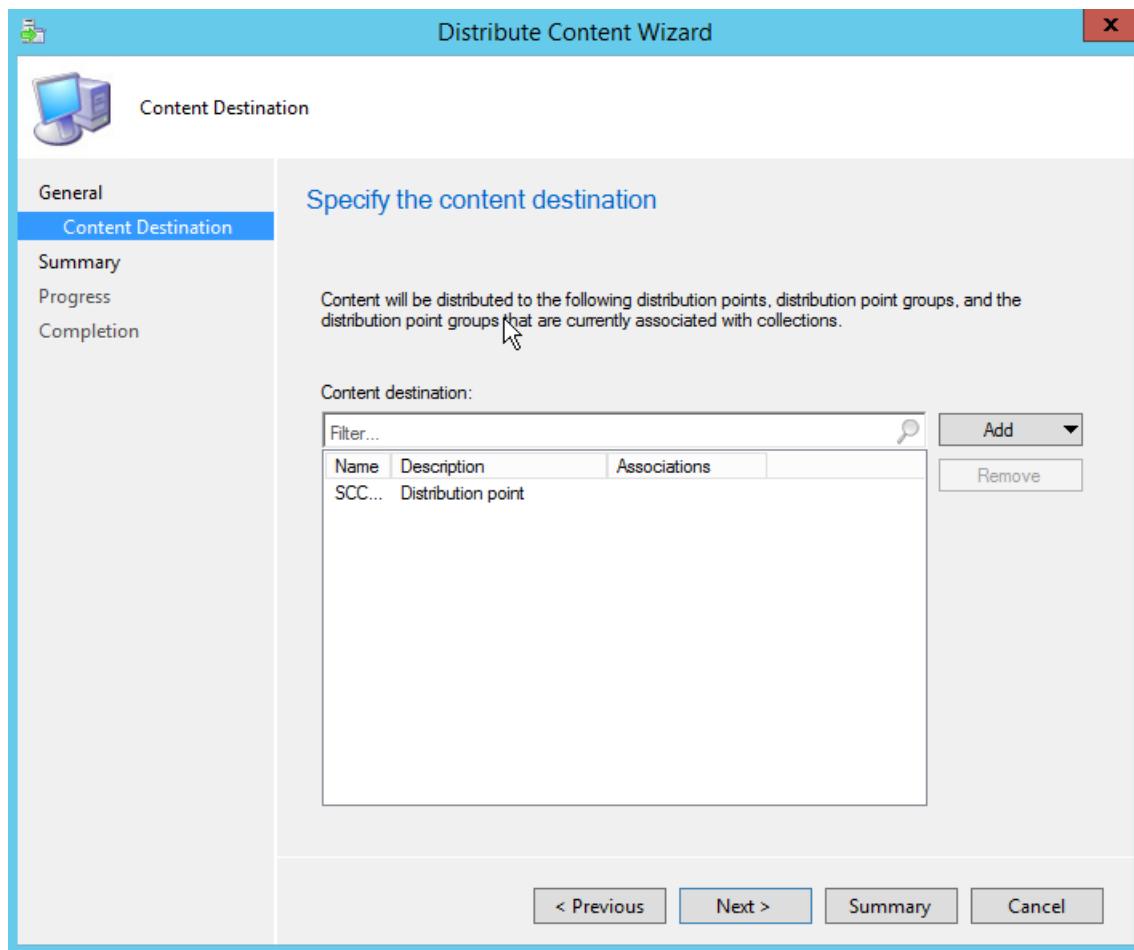
Click the **Add** button and select **Distribution Point**.



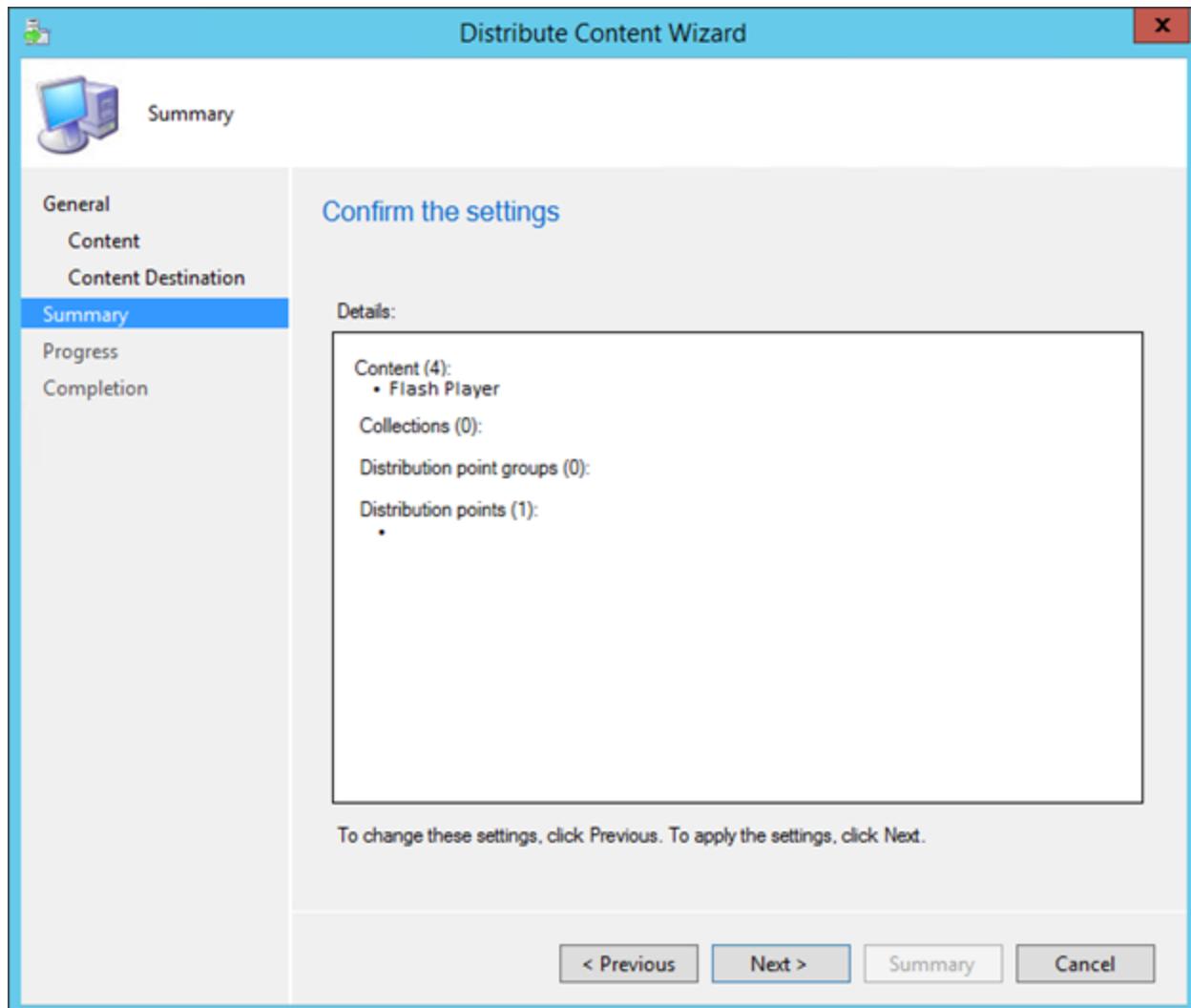
Select available **distribution** point. Click **OK** to continue. If no distribution is available, it means the package is already available on the distribution point. In that case, just **Cancel** and move to **Deploy Package**.



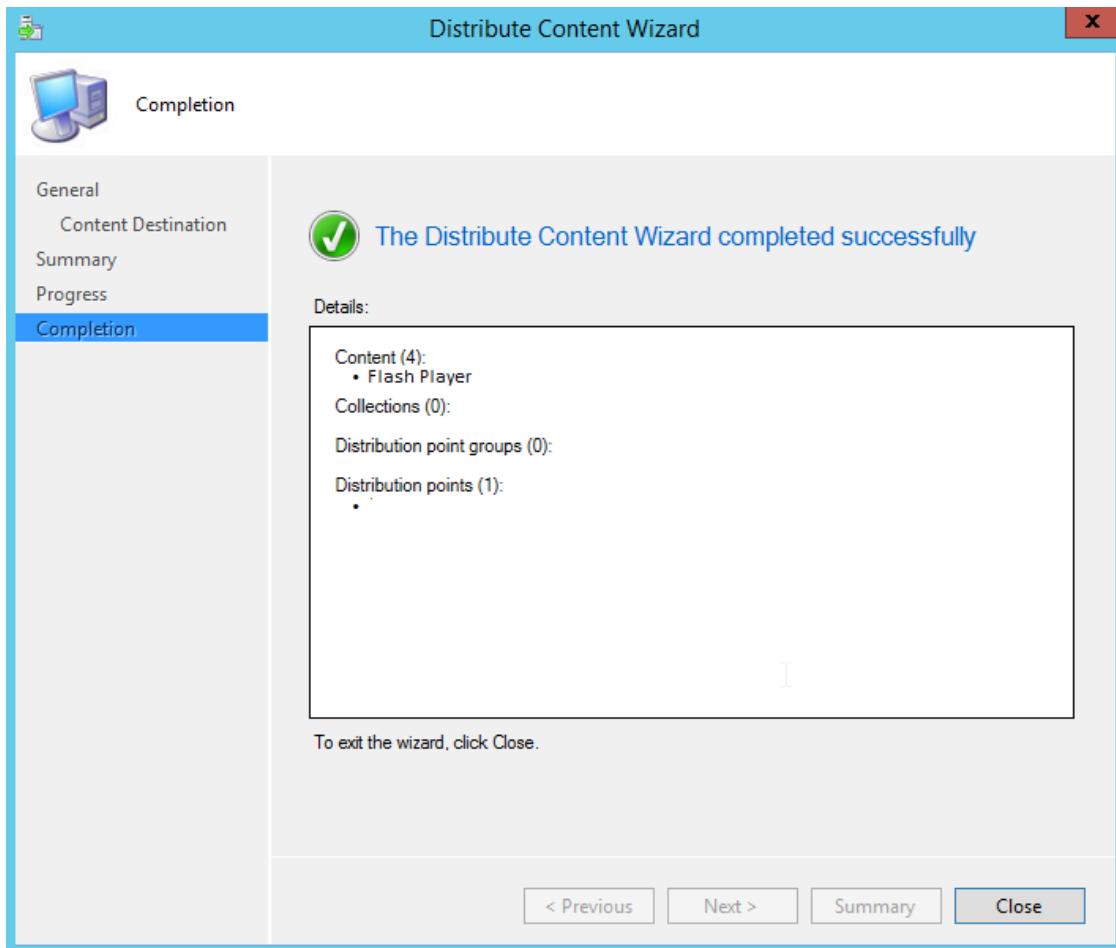
Click **Next**.



Click **Next**.



Click **Close**.



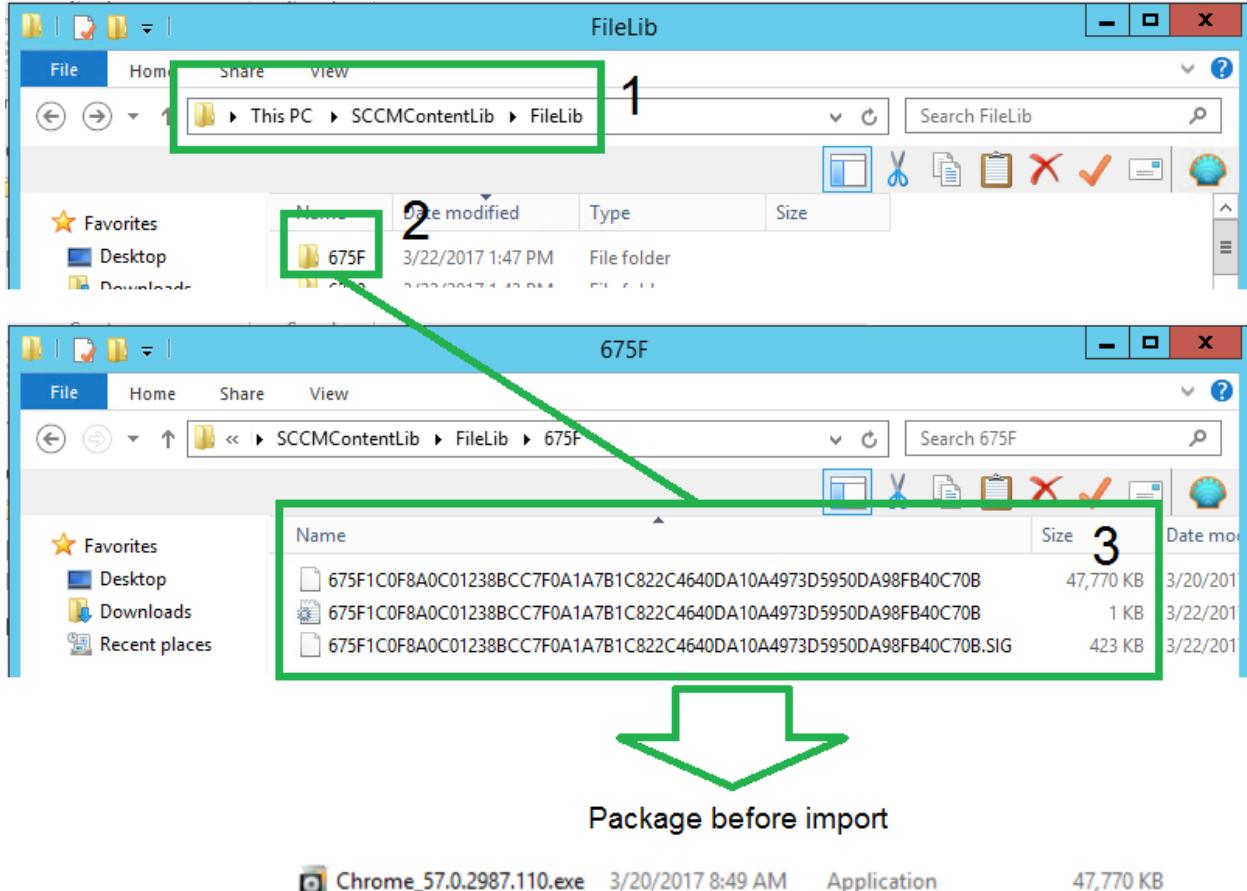
A Successful Content Distribution

The screenshot shows the 'Monitoring' interface with a tree view on the left. Under 'Monitoring', 'Database Replication' is expanded, showing 'Distribution Status' and 'Content Status'. 'Content Status' is also expanded, showing 'Adobe Flash Active X 25.0.0.148 En'. To the right, a 'Content Status' panel is open with the title 'Content Status' and the subtitle 'Content Distribution: Adobe Flash Active X 25.0.0.148 En'. It includes a legend: 'Success' (green), 'In Progress' (yellow), 'Error' (red), and 'Unknown' (grey). A table below shows the status of the distribution: 'Successfully distributed content' with 1 asset and a status type of 'Success'.

Status	Assets	Status Type
Successfully distributed content	1	Success

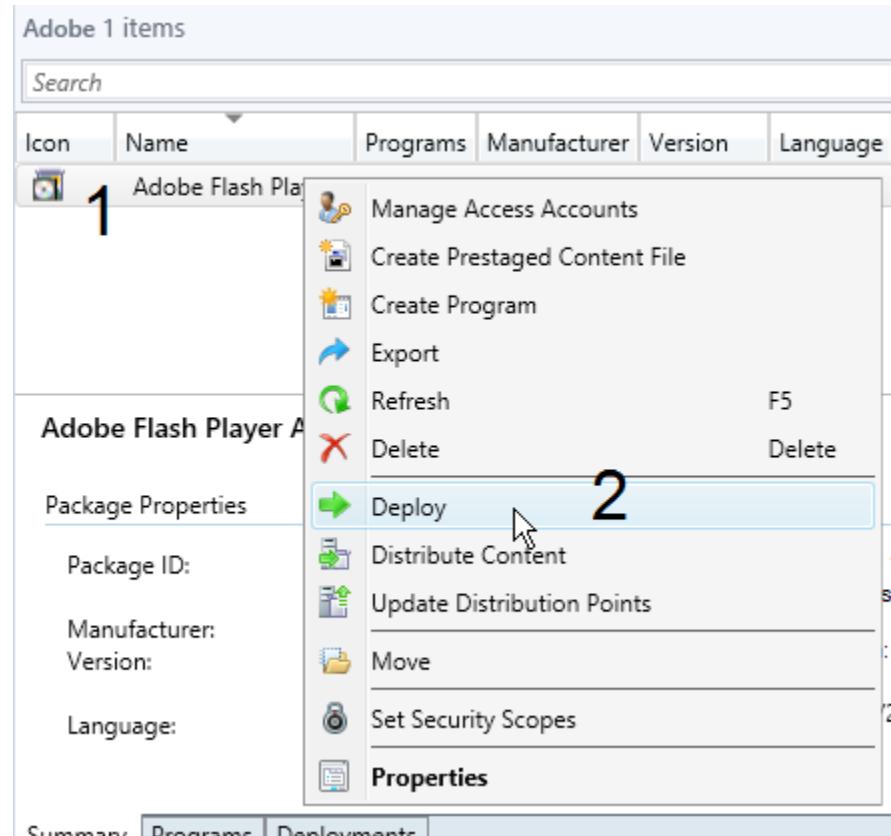
As a side note, packages are not stored in the distribution point in their original form, such as MSI or EXE. Packages in the distribution point can be found in the following location:

SCCMContentLib\FileLib

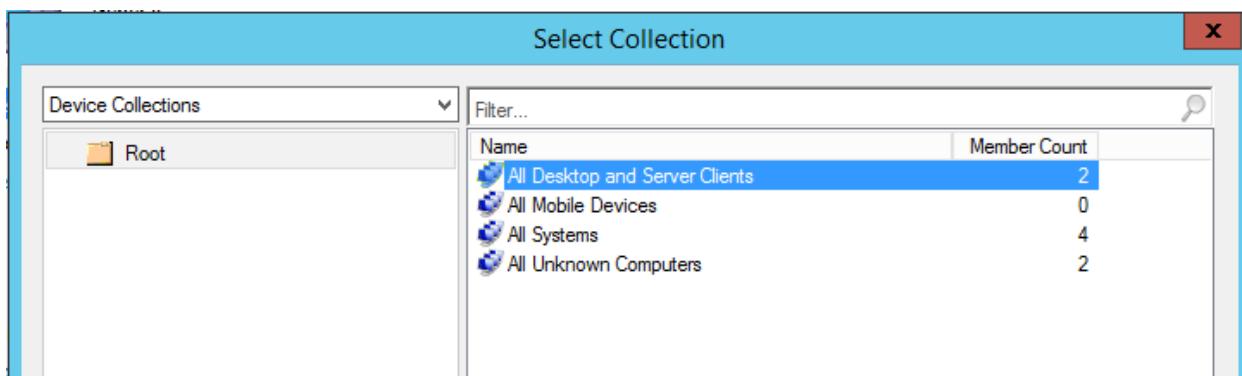
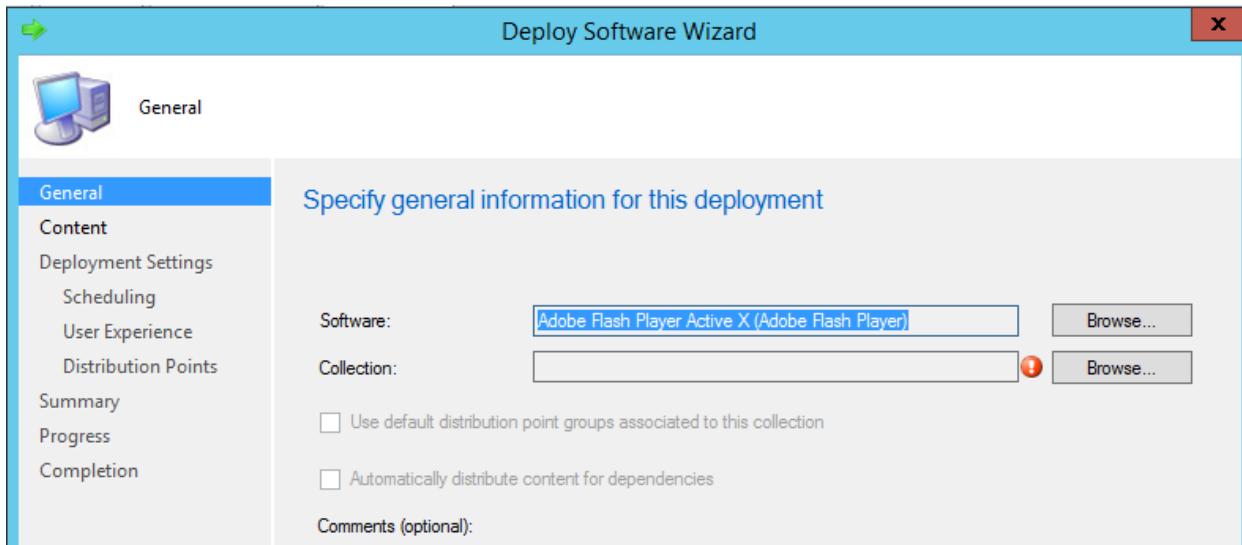


Deploy Package

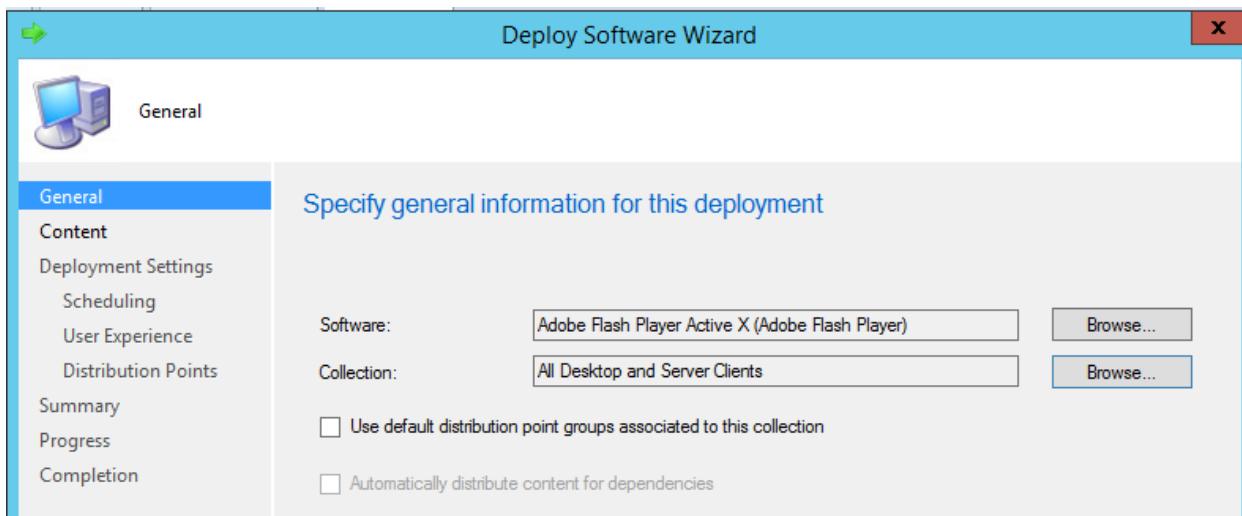
To Deploy a package, right-click on the package and select **Deploy** from the menu.



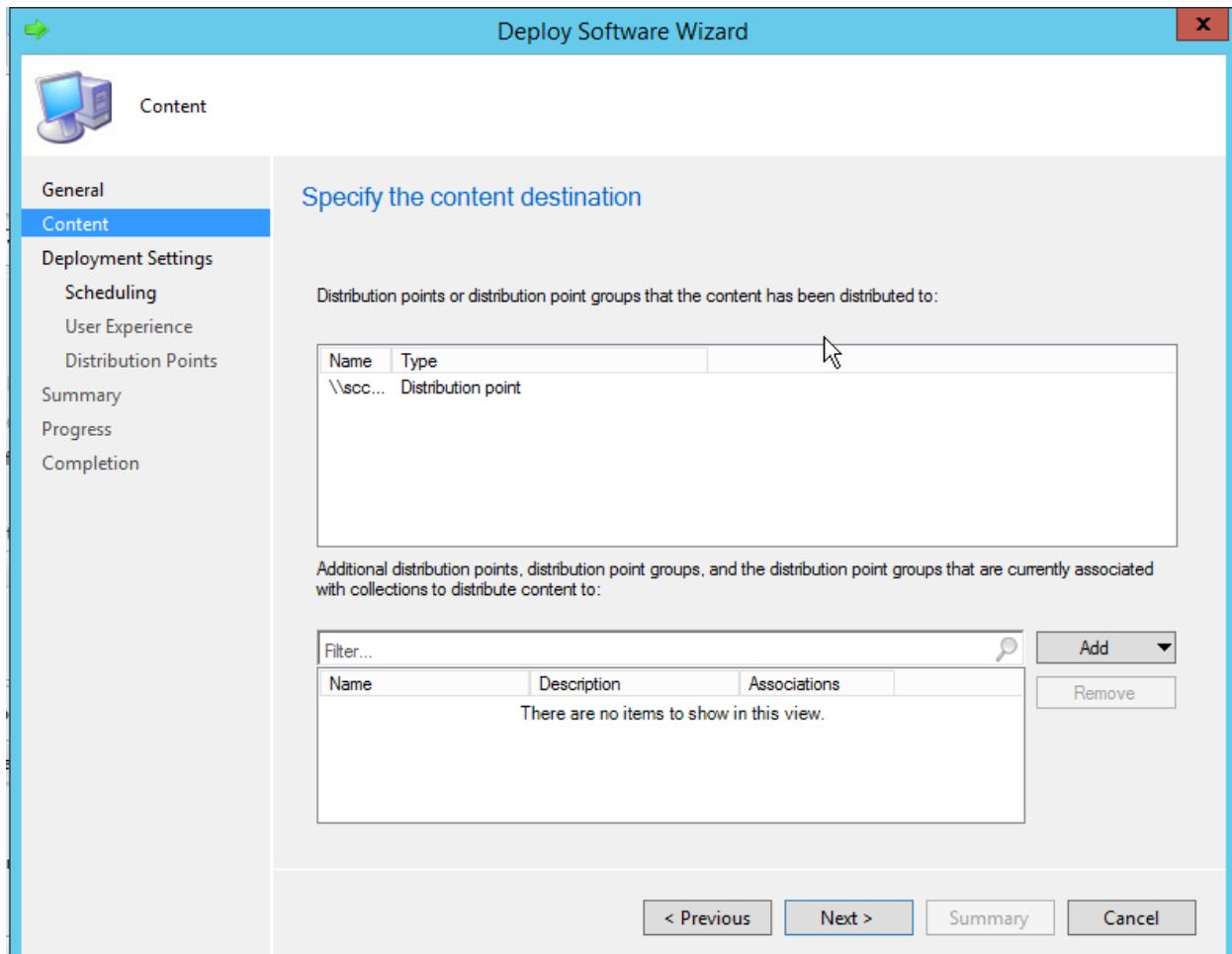
Select which **Collection** should receive the package by **Browsing** to collections.



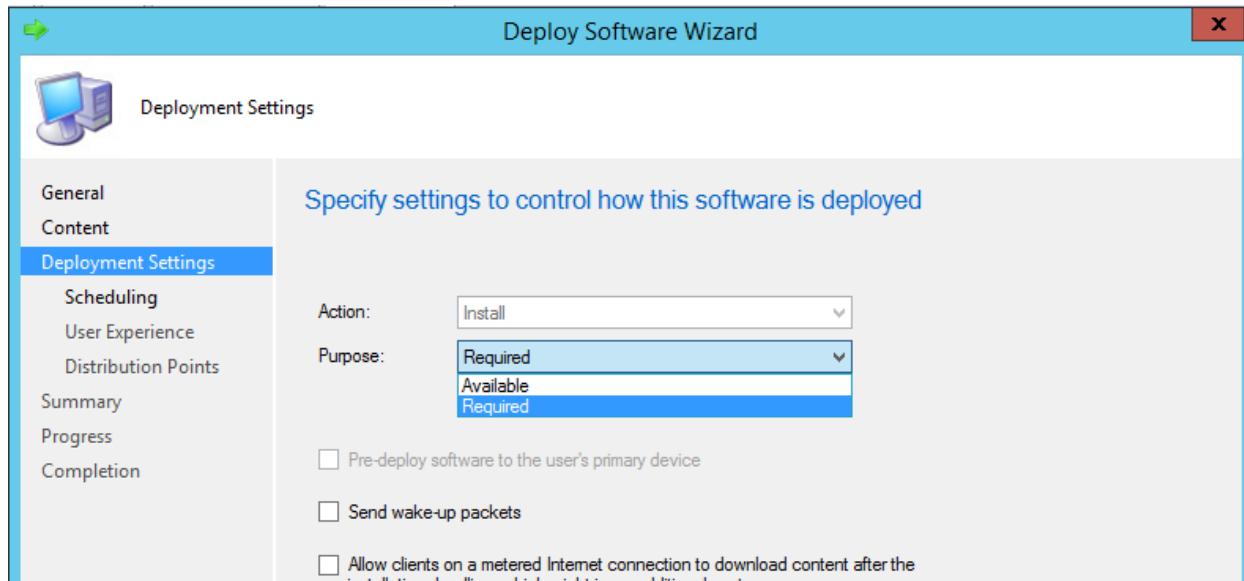
Click **Next** to continue.



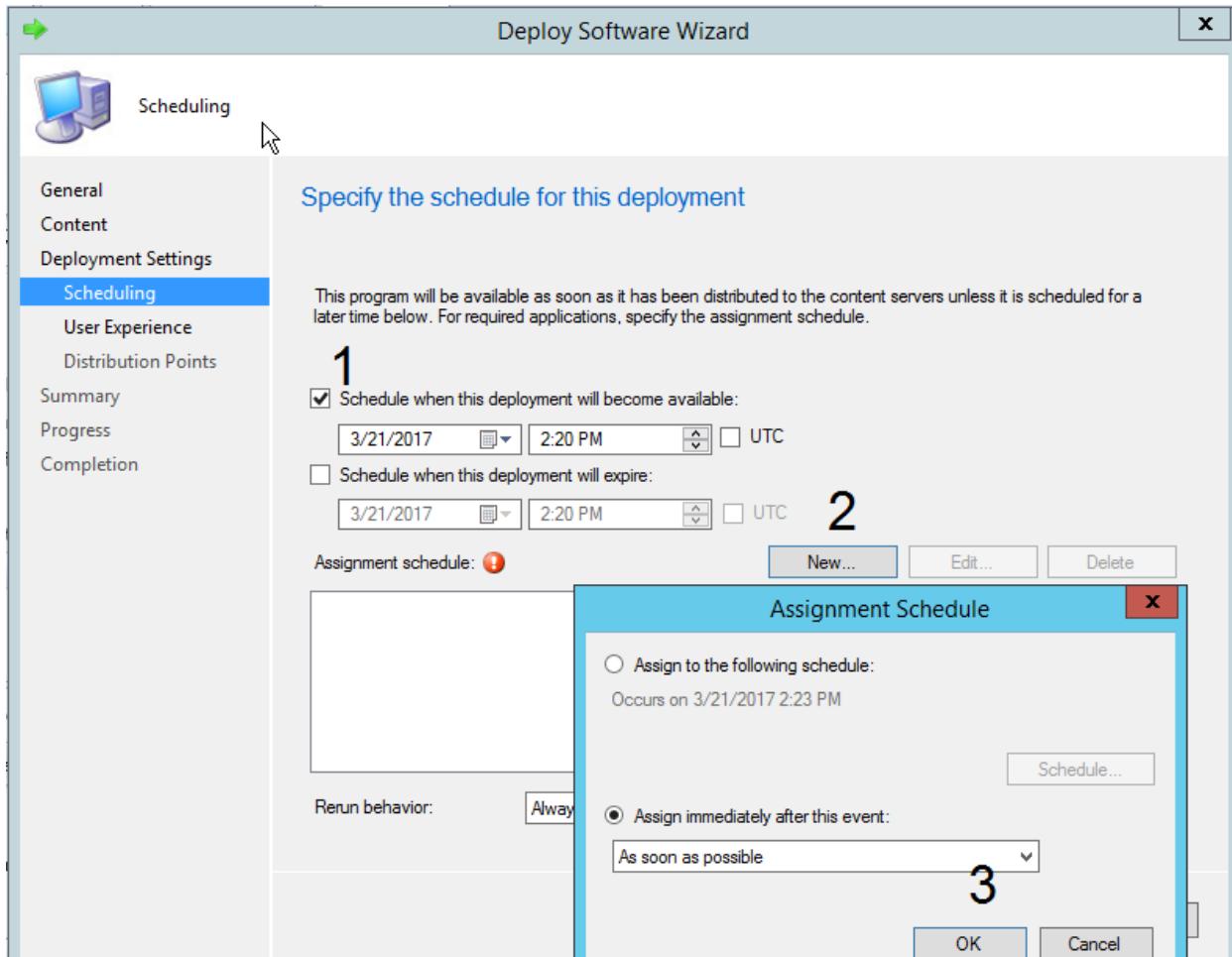
Click **Next** to continue.



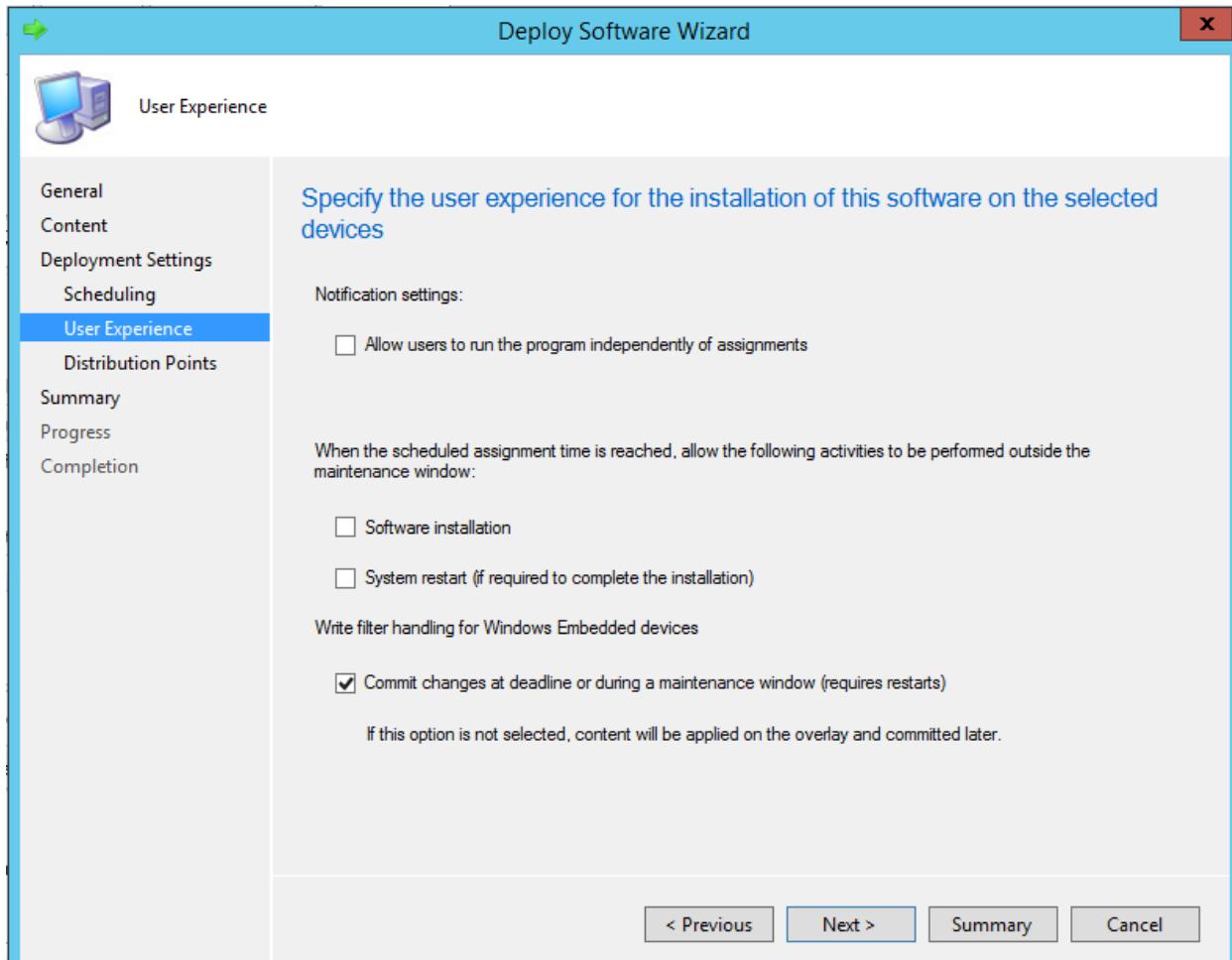
Select whether **Required** or **Available**. Click **Next** to continue.



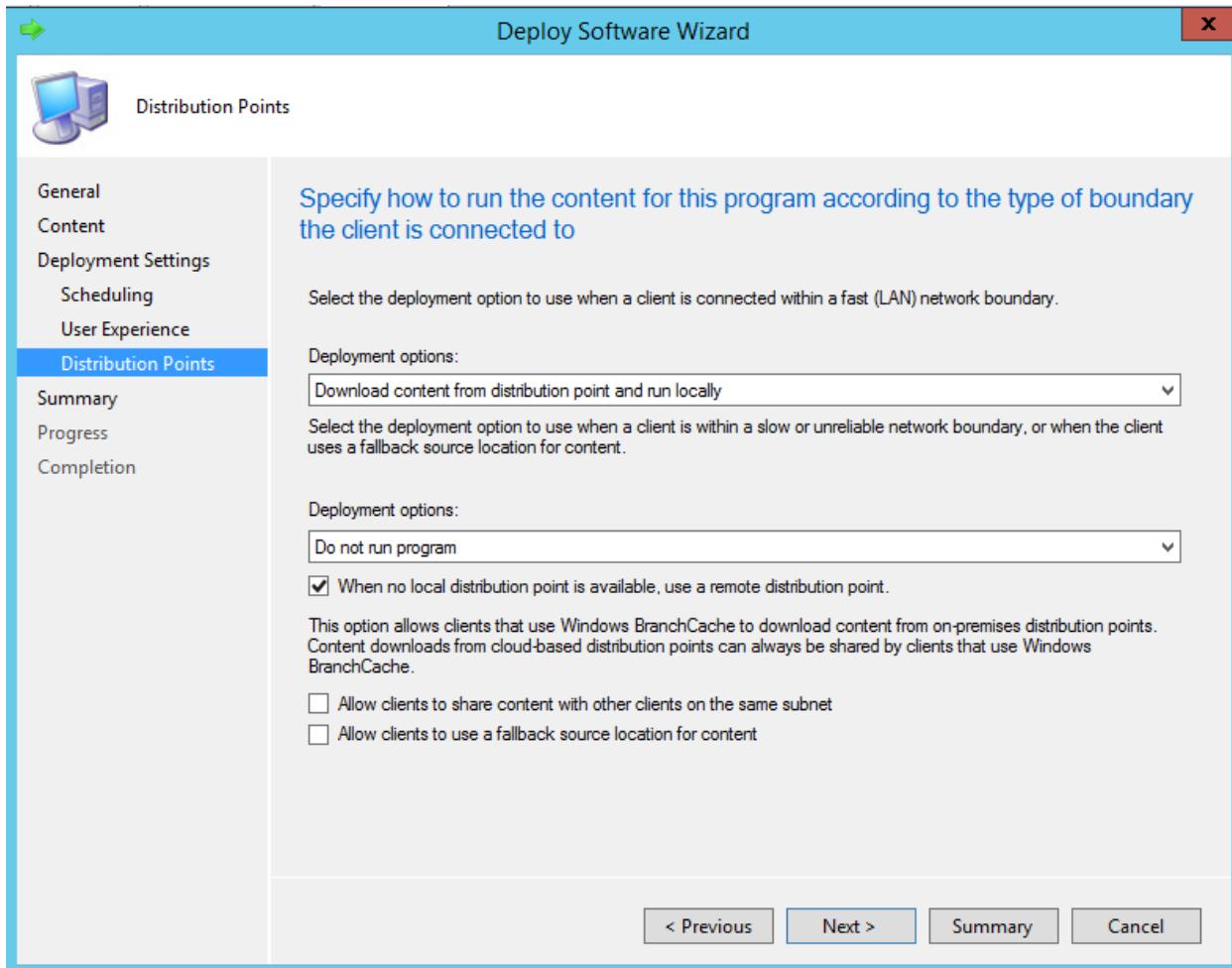
Set up package **Scheduling**. Click **Next** to continue.



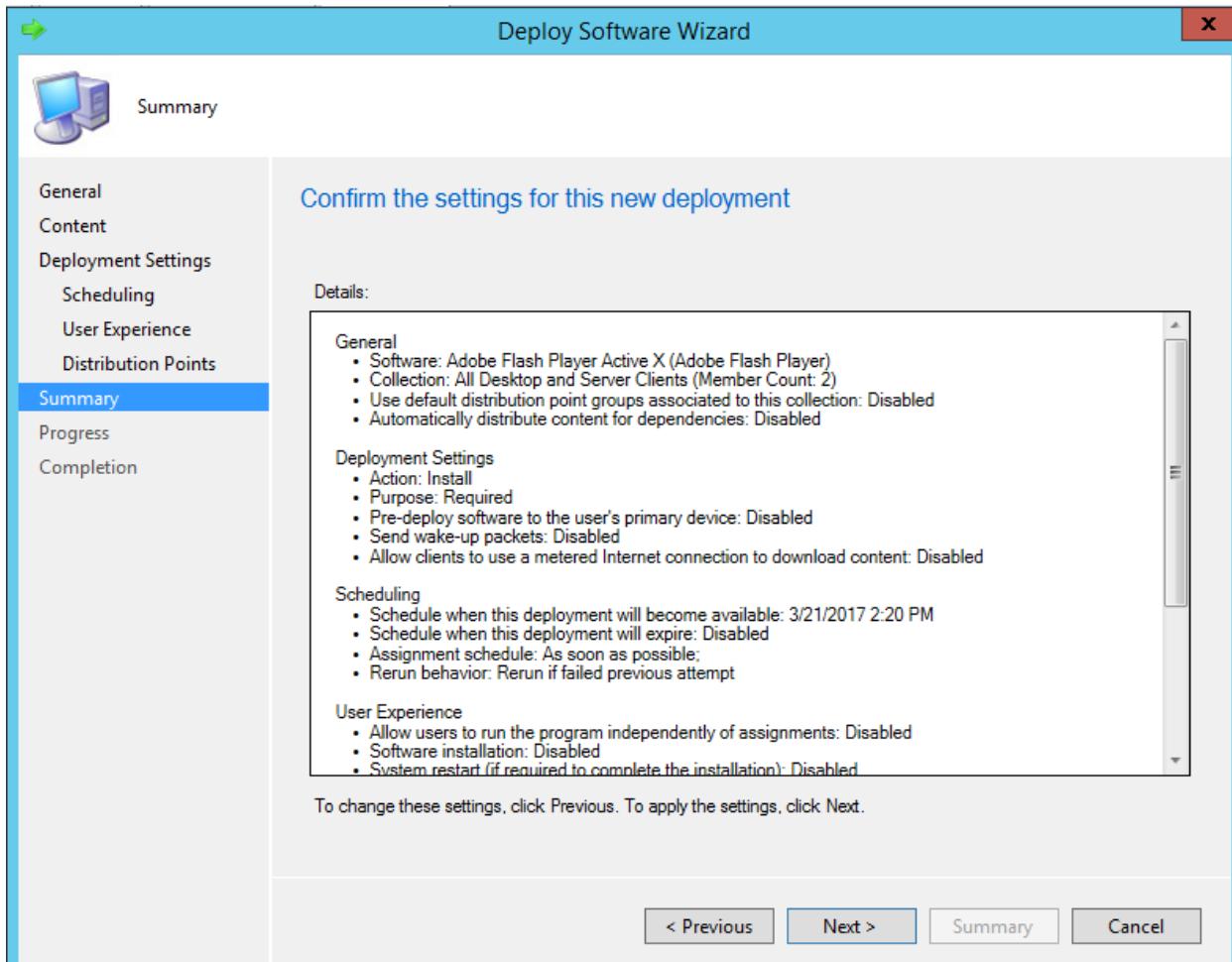
Make changes to the **User Experience**. Click **Next** to continue.



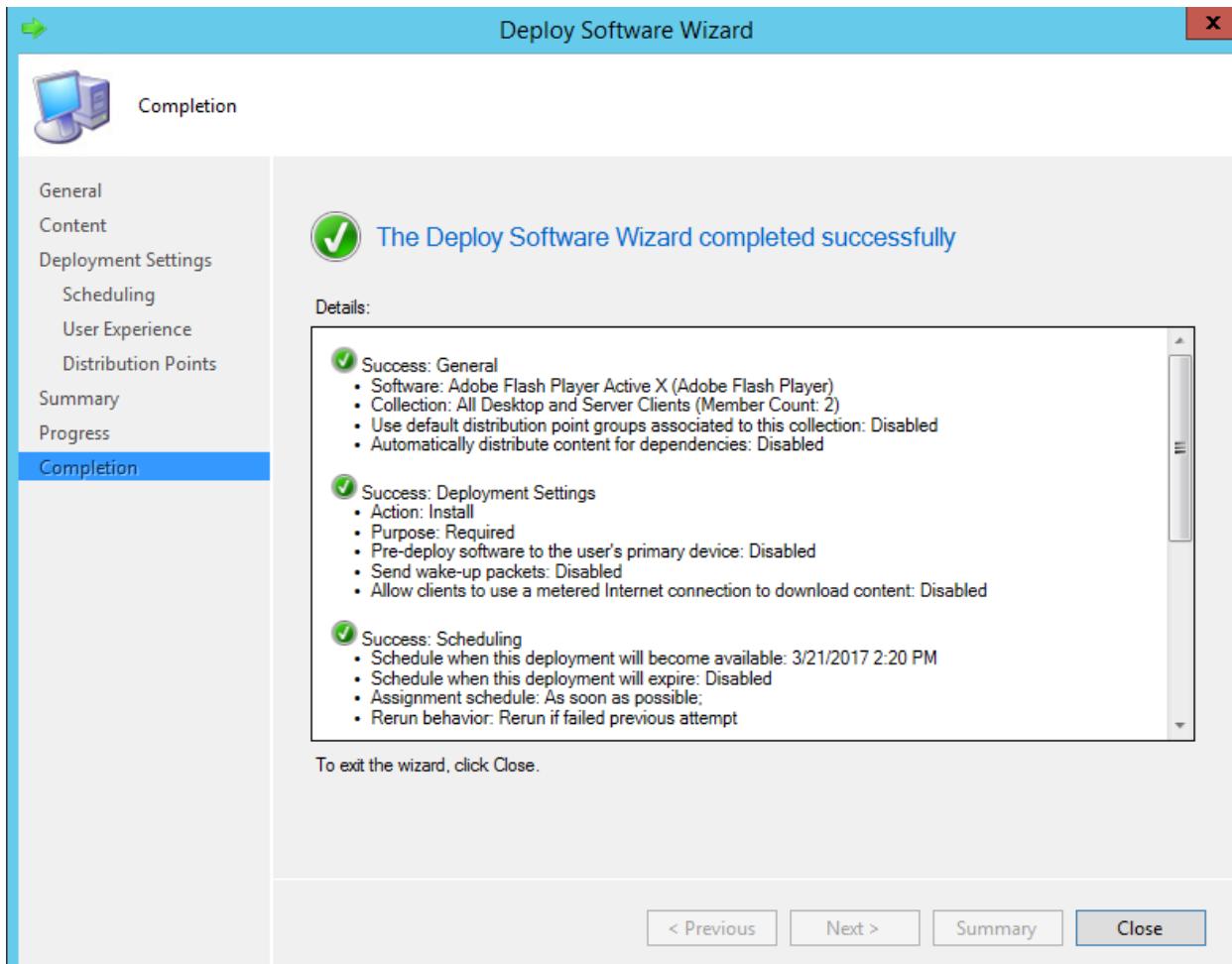
Make changes to **Distribution Options**. Click **Next** to continue.



Review Summary. Click **Next** to continue.



The Deployment has been successful. Click **Close** to exit deploy wizard.

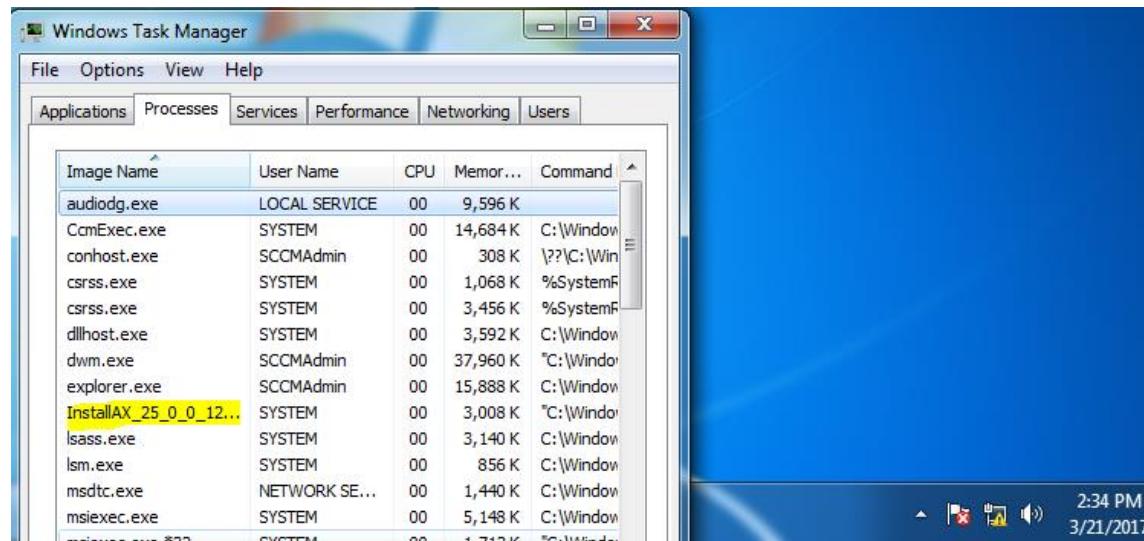


Monitoring a Deployment

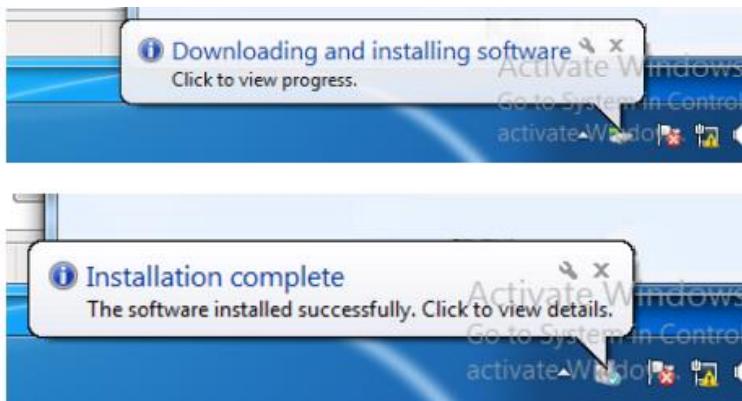
Once a package has been set to be delivered to a **Collection**, the deployment can be monitored from the client or the SCCM server.

On the client, **Task Manager** can be used to track the installation process. Frontend **Notifications** can also be sent, so the end user knows a package is being downloaded, installed, and completed. If you like logs, check out C:\Windows\CCM\logs\AppEnforce.log, which records details about enforcement actions (install and uninstall) taken for applications on the client. **Client cache** can also be monitored, to see if the package is downloading. That is located here: C:\Windows\ccmcache\1

Silent Install - No Notifications



Install - With Notifications



On the SCCM Server, under **Monitoring > Deployments**, the package deployment status can be monitored in **Deployment Status**.

A screenshot of the SCCM Management Console. The left sidebar shows navigation categories like Monitoring, System Status, Deployments, Assets and Compliance, Software Library, Monitoring (which is selected and highlighted in grey), and Administration. The main pane is titled "Deployment Status" and displays information for a deployment of "Adobe Flash Player Active X (Adobe Flash Player)" to the "All Desktop and Server Clients" collection. It shows a summary table with columns for Success, In Progress, Error, Requirements Not Met, and Unknown. The "Success" column is highlighted with a green background. Below the table, a message states "Status information is currently unavailable for this deployment." A section titled "Asset Details" also displays a message stating "Asset Detail information is currently unavailable for this deployment." On the right side of the main pane, there are buttons for "Run Summarization" and "Refresh", and a note that "Summarization Time: Never".

A Successful Deployment

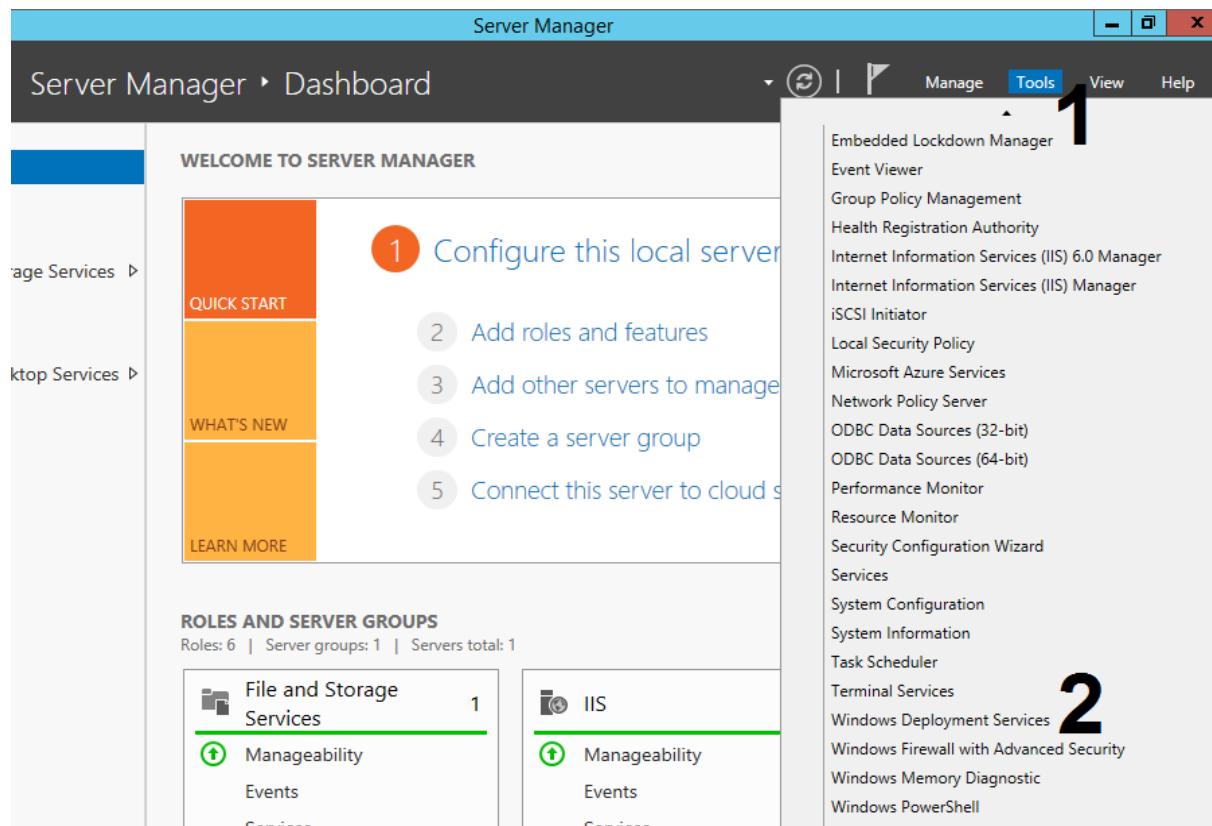
The screenshot shows the 'Deployment Status' interface. On the left, a navigation tree includes 'Monitoring' (selected), 'System Status', 'Site Status', 'Component Status', 'Conflicting Records', 'Status Message Queries', 'Deployments' (selected), 'Client Operations', 'Client Status', 'Assets and Compliance', 'Software Library', 'Monitoring' (selected), and 'Administration'. The main area displays the 'Deployment Status' for 'Program: Adobe Flash Player Active X (Adobe Flash Player)' and 'Collection: All Desktop and Server Clients'. A status bar at the top right shows 'Run Summarization | Refresh' and 'Summarization Time: Never'. Below this is a legend: Success (green), In Progress (yellow), Error (red), Requirements Not Met (blue), and Unknown (grey). A table lists one deployment entry: Deployment ID 00120011, Assets 1, Message ID 10008, and Status Type Success. The 'Asset Details' section below shows a single row: Device CLIENTW7, User NT AUTHORITY\SYSTEM, Message ID 10008, Status Type Success, and Description 'Program completed with success'.

Deployment ID	Assets	Message ID	Status Type
00120011	1	10008	Success

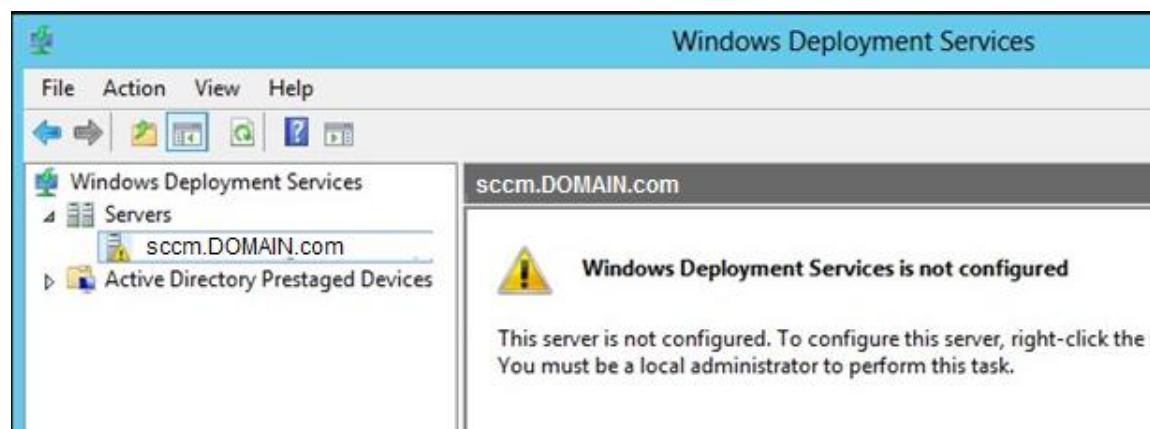
Device	User	Message ID	Status Type	Description
CLIENTW7	NT AUTHORITY\SYSTEM	10008	Success	Program completed with success

WDS Setup

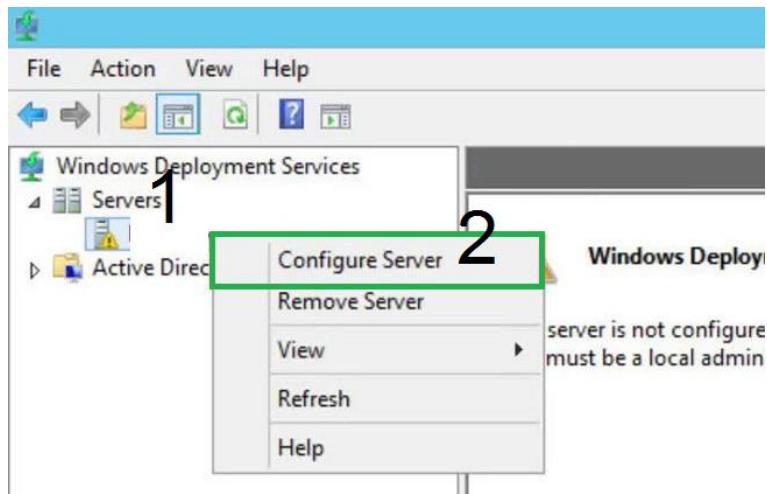
Normally, you wouldn't do anything after installing the WDS service from the Dashboard. But, if there are errors or alerts, you'll want to make sure you resolve those first, *before* moving on to SUP and PXE setup in SCCM.



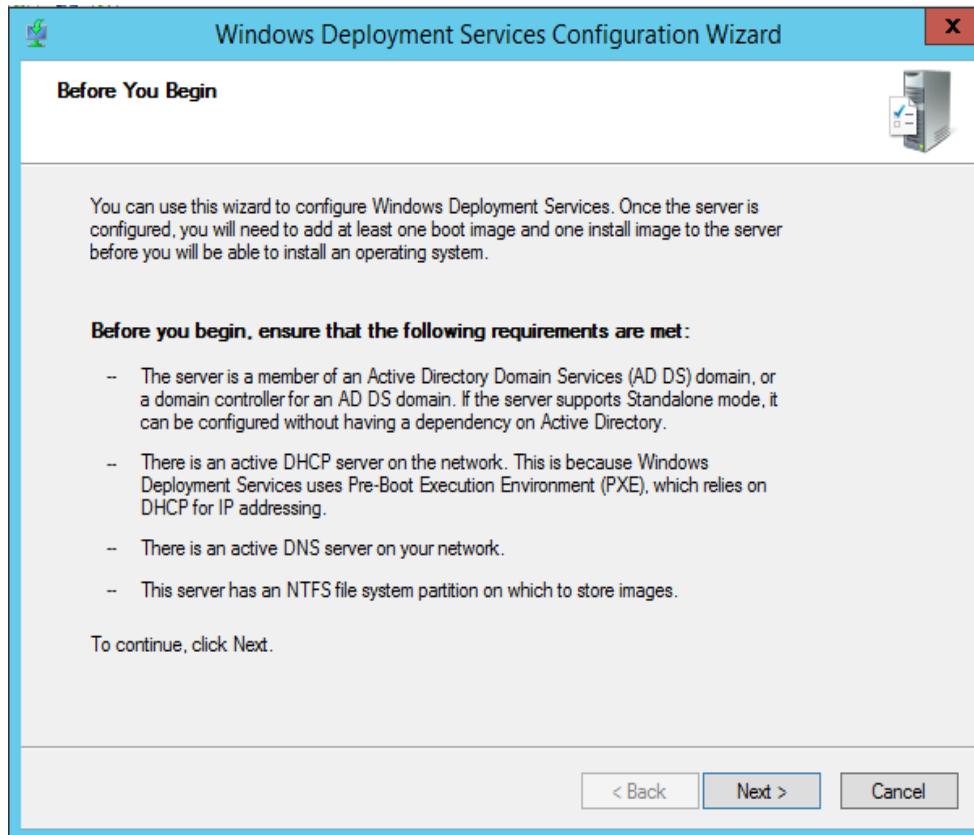
Notice how there is an alert.



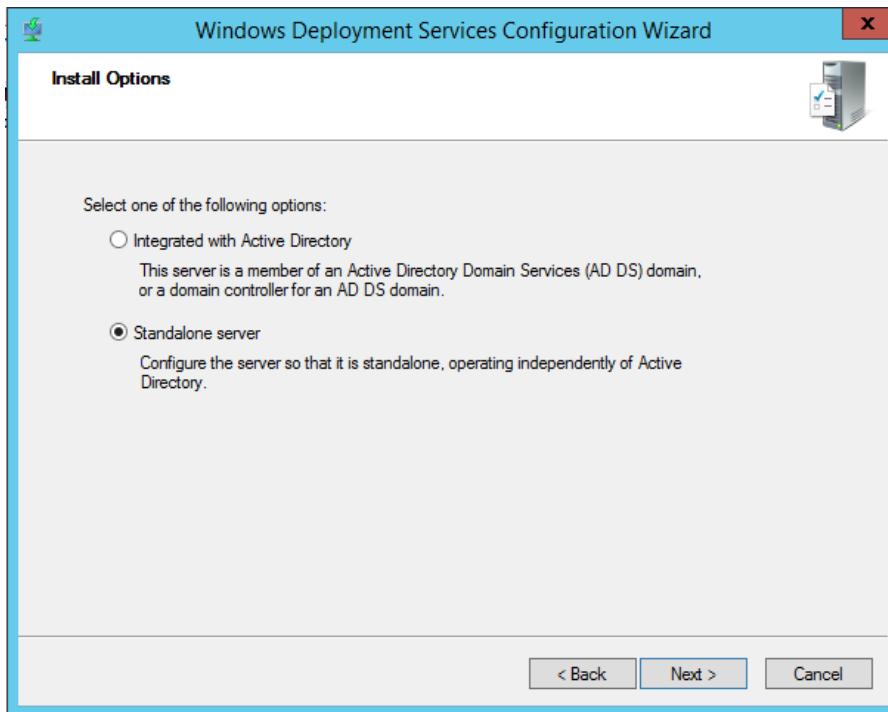
Right-click on the **server** and select **Configure Server**.



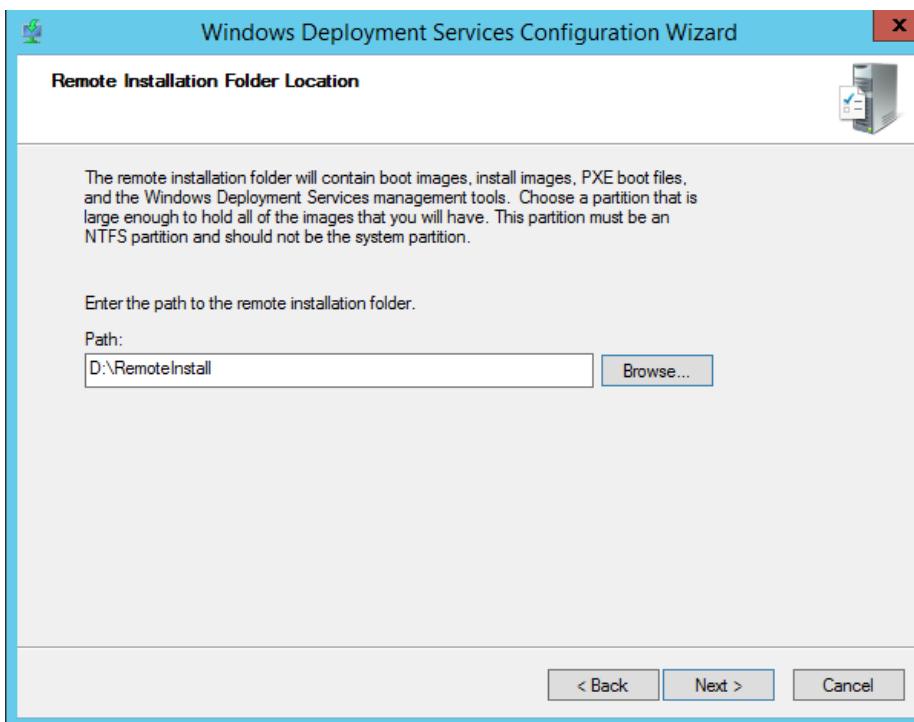
Click **Next**.



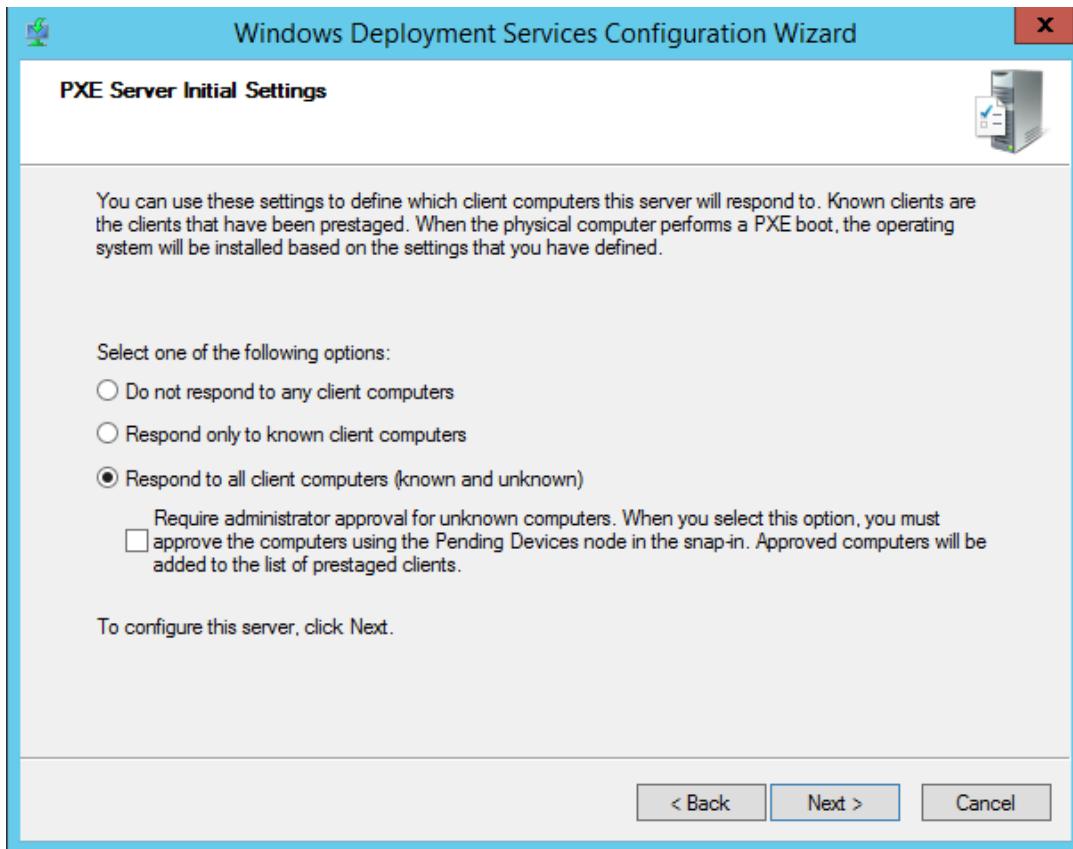
Select **Standalone**. Click **Next**.



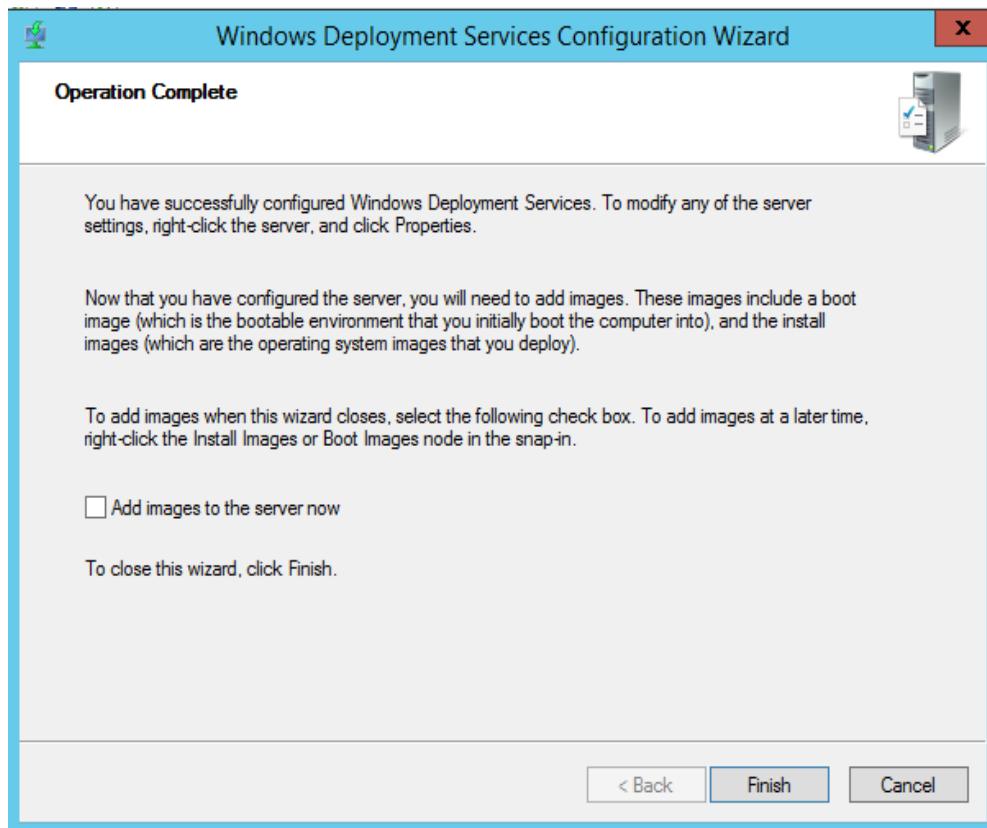
The **RemoteInstall** location must be correct. Click **Next**.



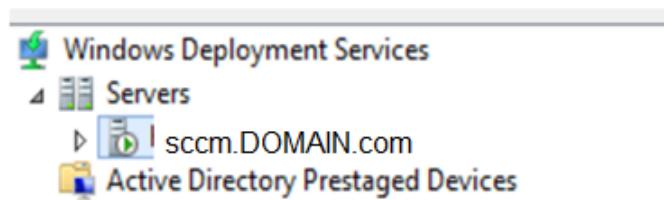
Respond to all (this setting will also be in SCCM). Click **Next**.



Do not add images here. Click **Finish**.



Leave WDS looking like this, **Active without Alerts**.



PXE Setup

Required

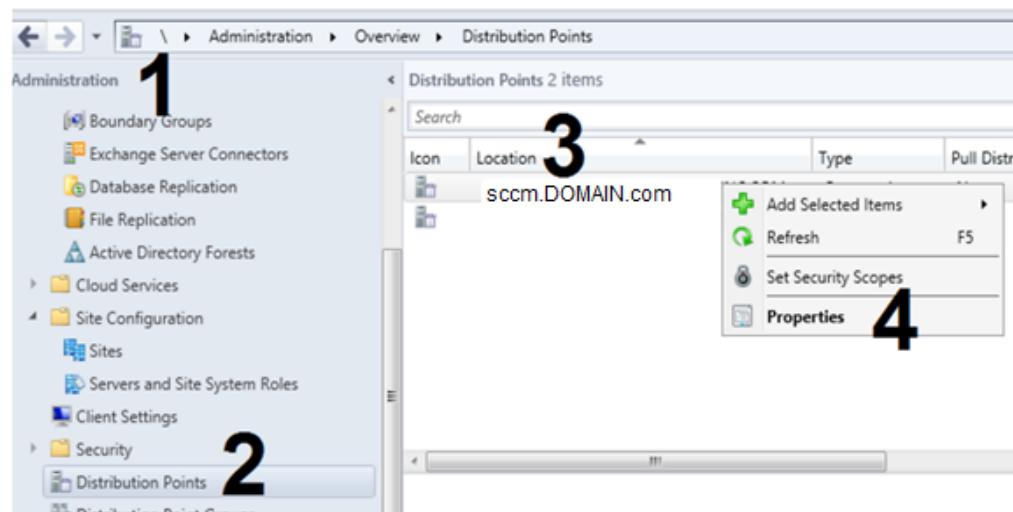
When you use PXE, client computers use the following ports to connect to this site system server:

For PXE requests: UDP ports 67, 68, 69, and 4011.

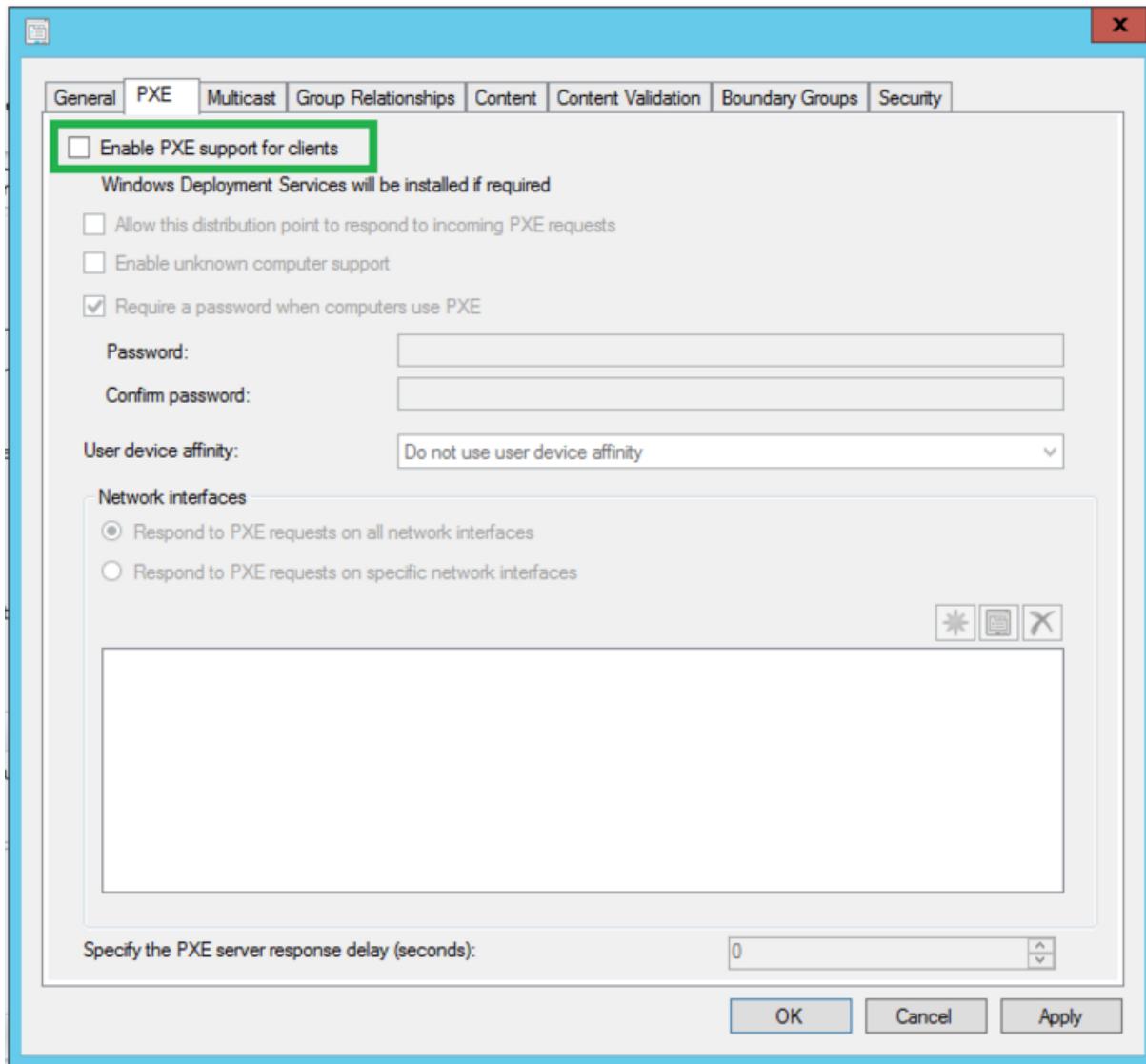
For operating system installation: UDP port 69.

If you use Windows Firewall on this server, Configuration Manager automatically configures rules to allow these ports. If you use other firewalls, you must configure them to allow these ports.

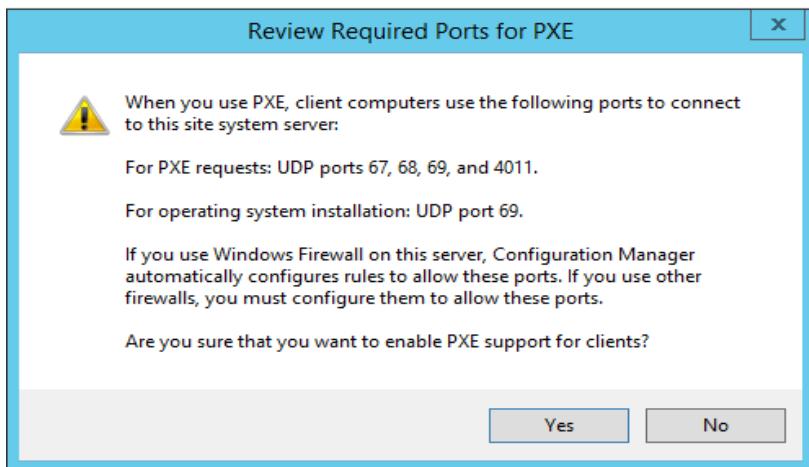
To begin PXE setup in SCCM, select **Administration > Distribution Points > Distribution Point > Properties**.



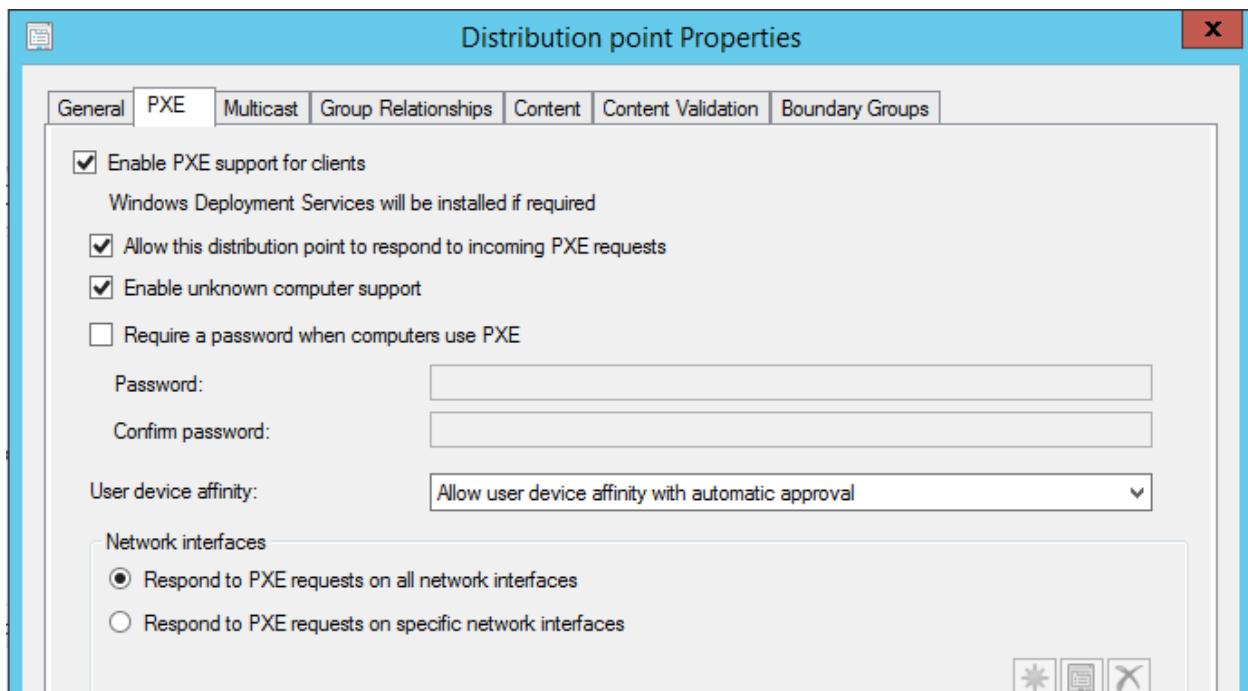
Select **Enable PXE support for clients**.



Click **Yes**.



Click **OK** to continue.



Side Note

If there is another PXE server boot WIM currently in use, **import** the WIM into the SCCM Boot Images section -- **before** configuring **DHCP**. You want the original boot WIM and the new boot WIM to be available on the boot menu. Of course, you may not care about maintaining both the old and new solution.

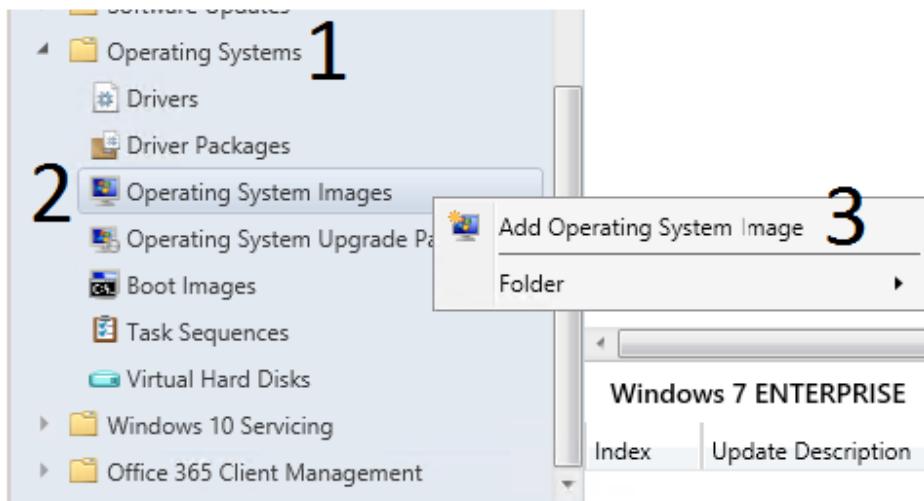
Configure DHCP

In DHCP,

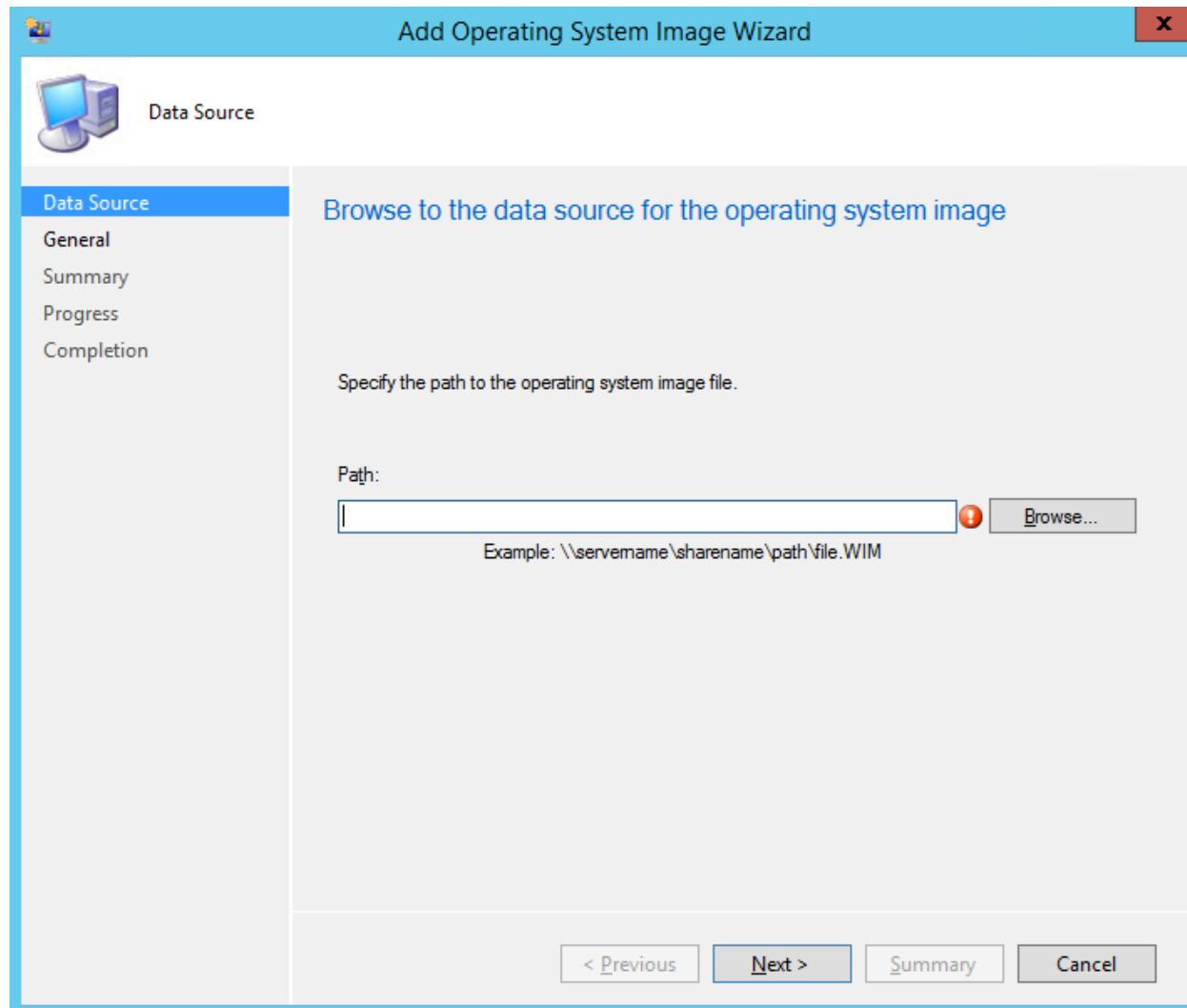
- (1) Expand IPv4.
- (2) Expand the IP Scope you want to edit for PXE.
- (3) Right-Click Scope Options.
- (4) Click Configure Options.
- (5) Check **066 Boot Server Host Name** and type the PXE FQDN sccm.DOMAIN.com or 10.1.0.1 (Primary)
- (6) Check **067 Bootfile Name** and type smsboot\x86\wdsnbp.com

Imaging Setup

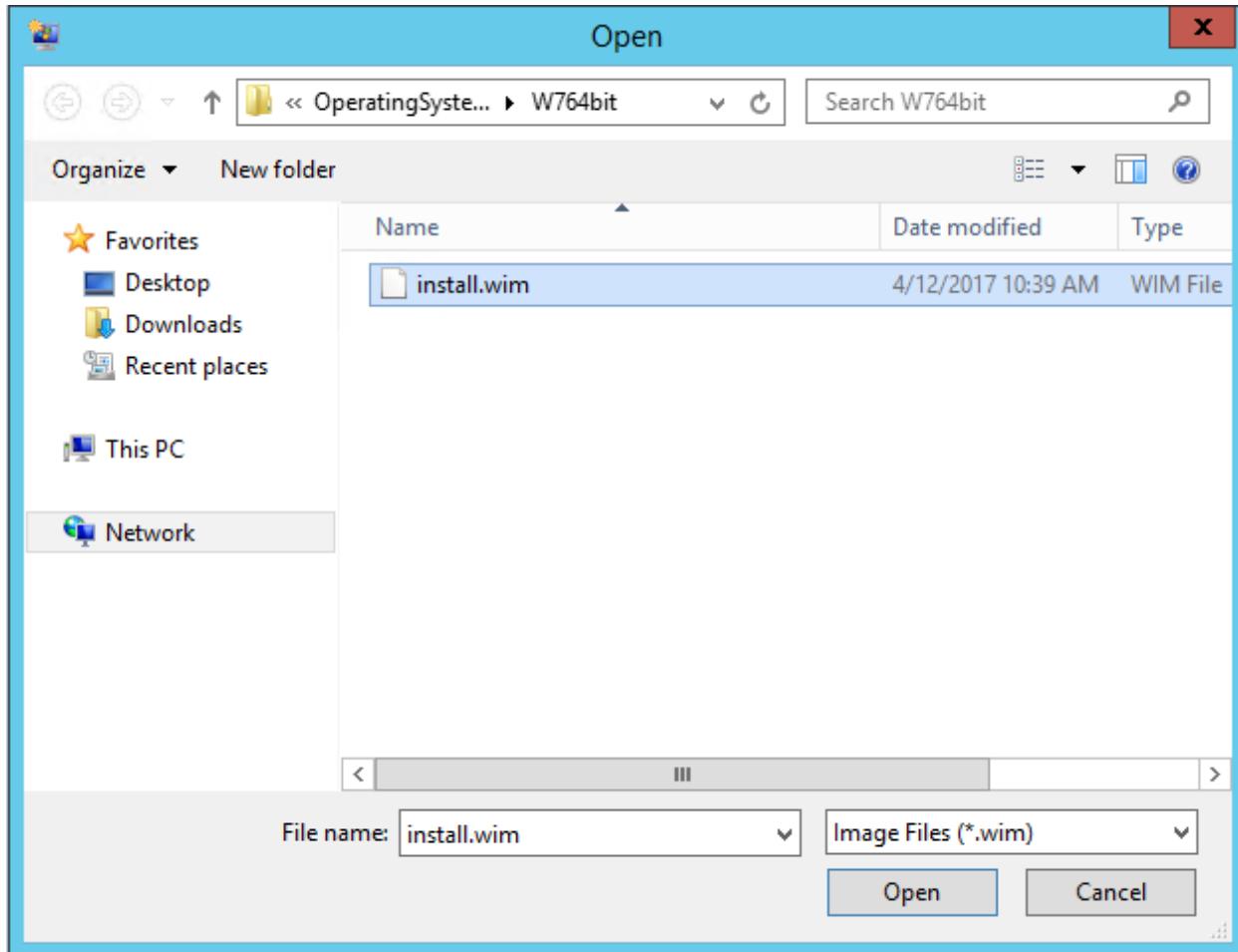
To **deploy** an operating system, you must first **add an OS WIM** to SCCM. To add a WIM, select **Software Library, Operating Systems**, right-click on **Operating System Images**, and select **Add Operating System Image**.



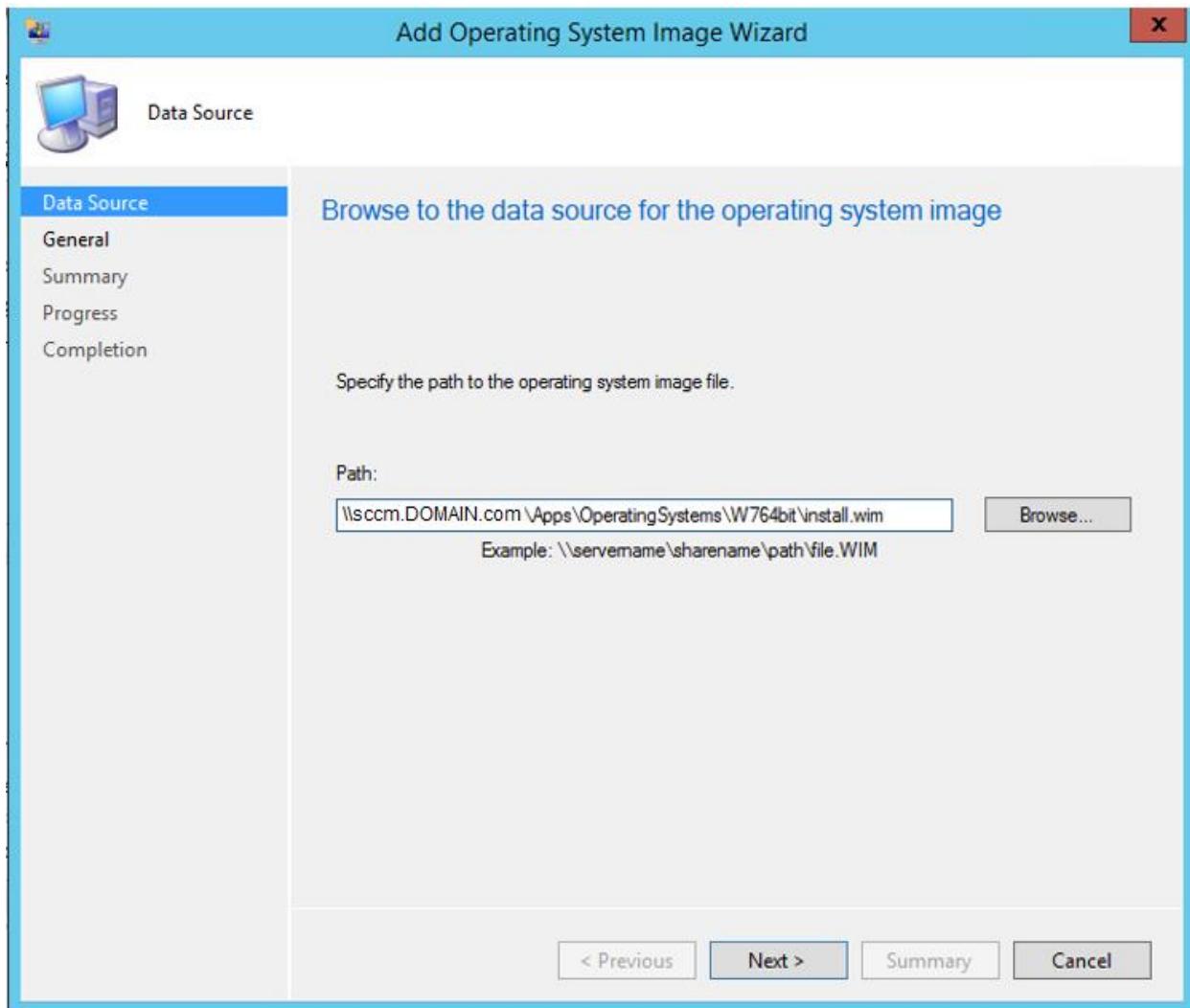
Now, navigate to the **WIM**. This should be a **FQDN UNC location**.



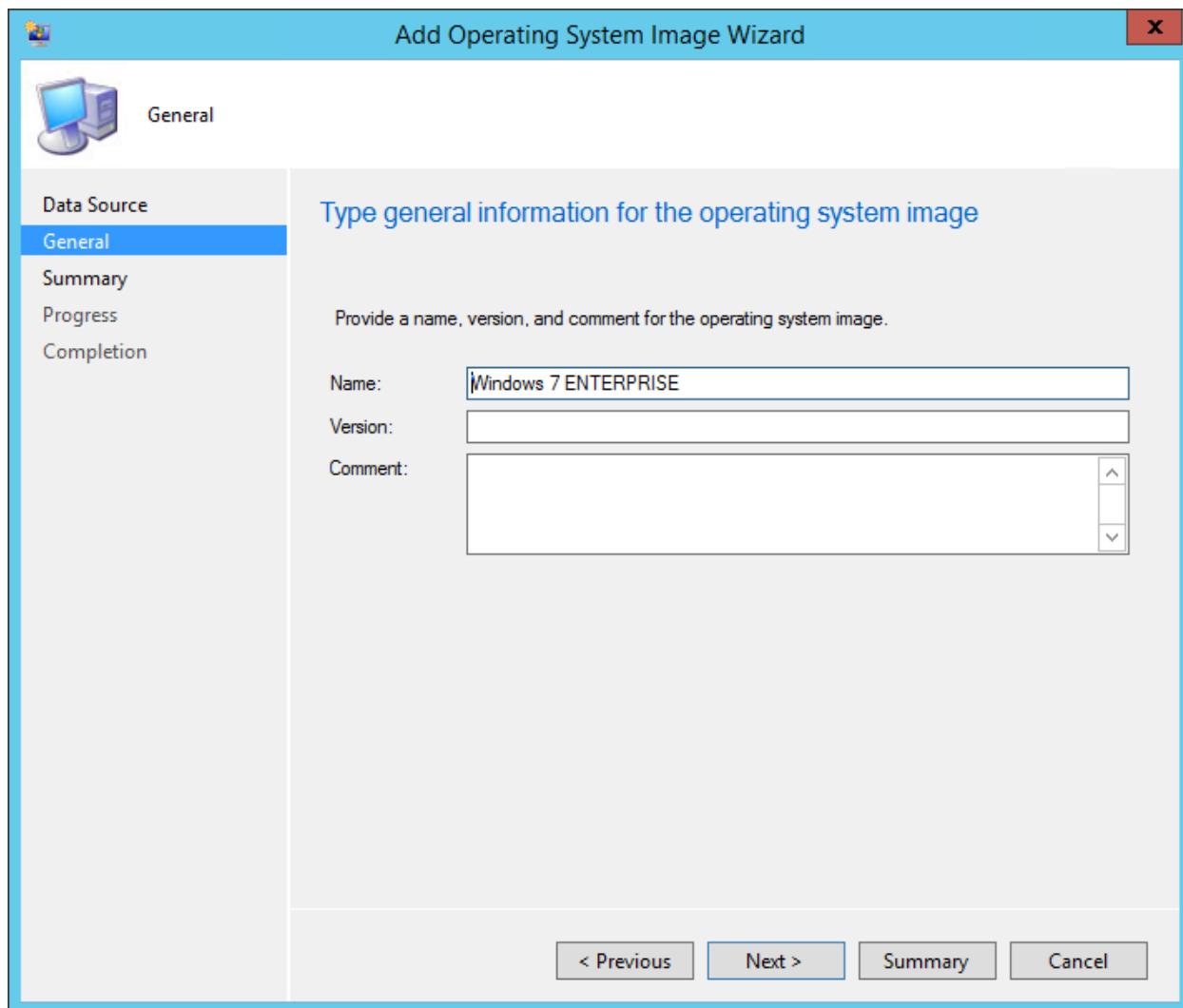
Select **WIM** and click the **Open** button.



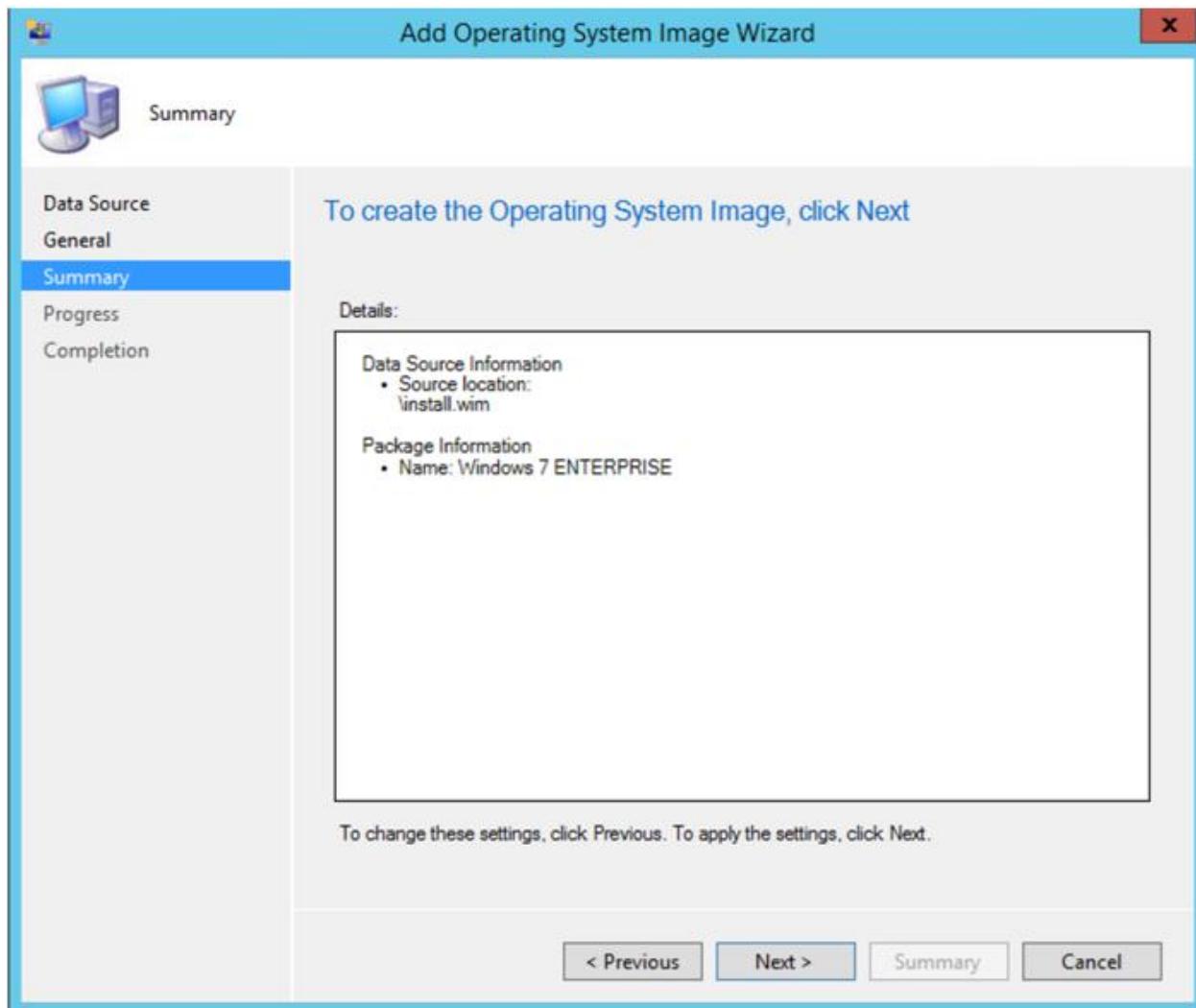
Click **Next**.



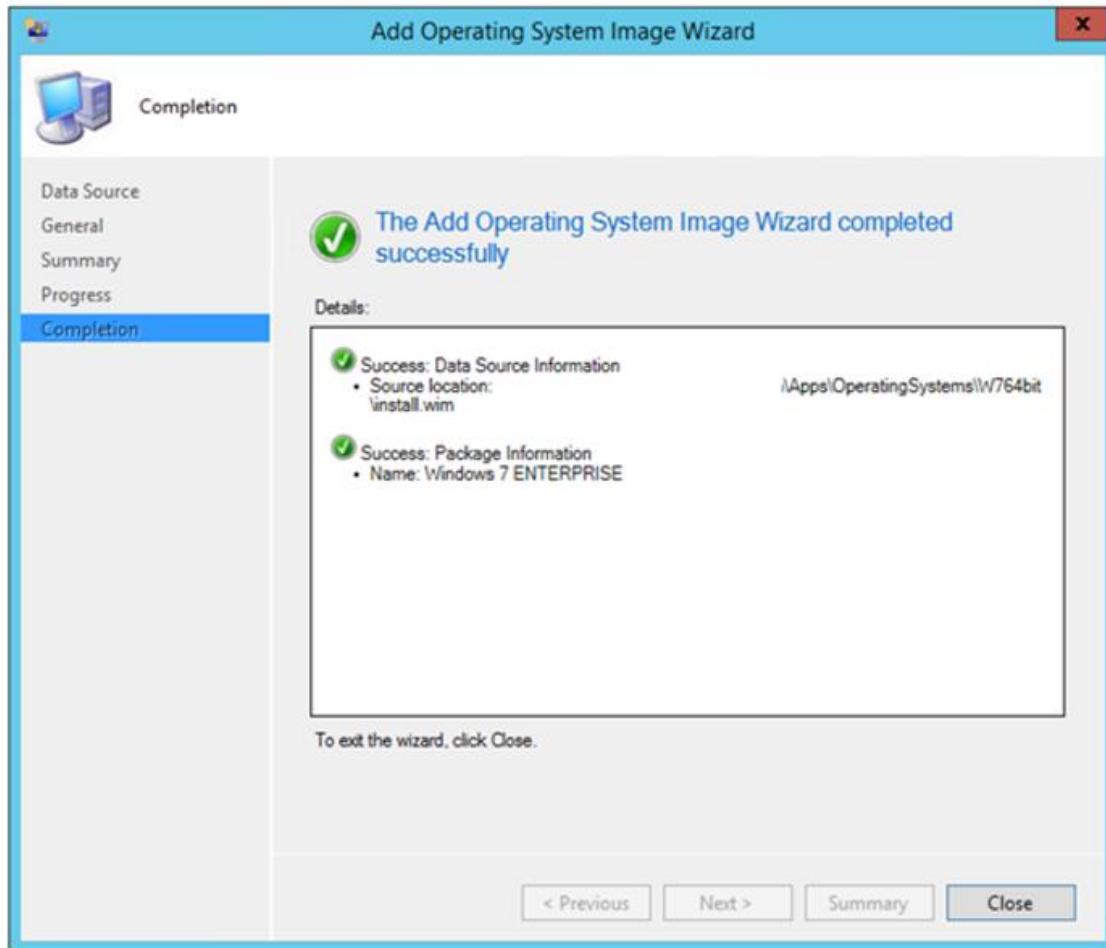
Click **Next**.



Click **Next**.

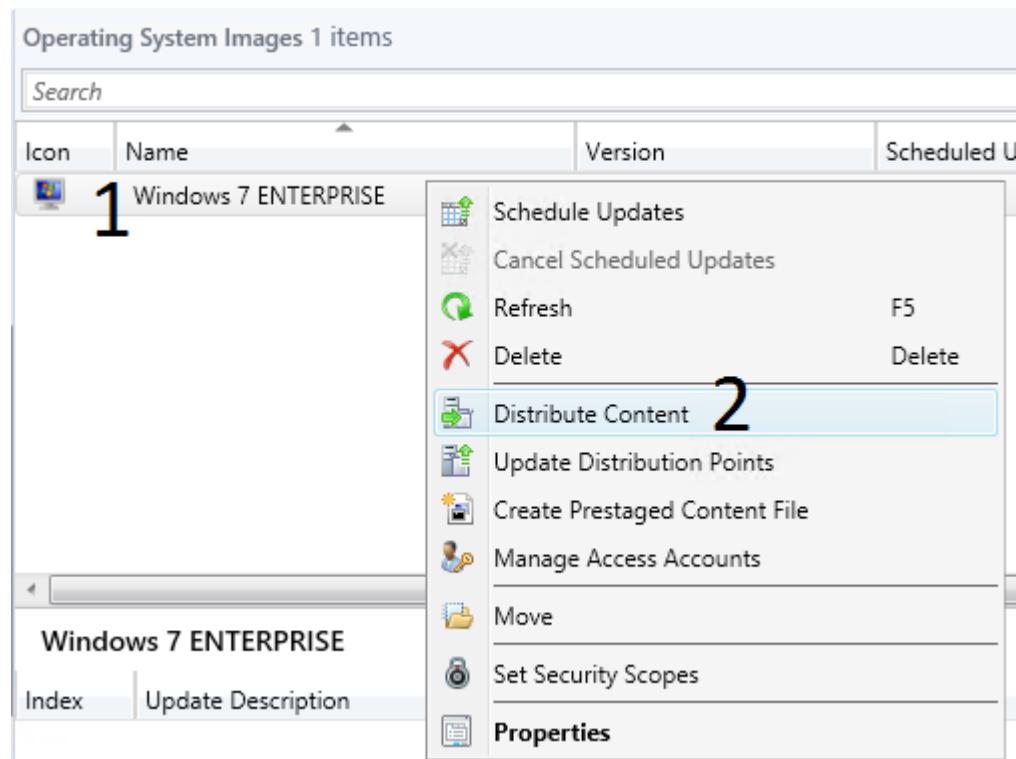


Click **Close**.

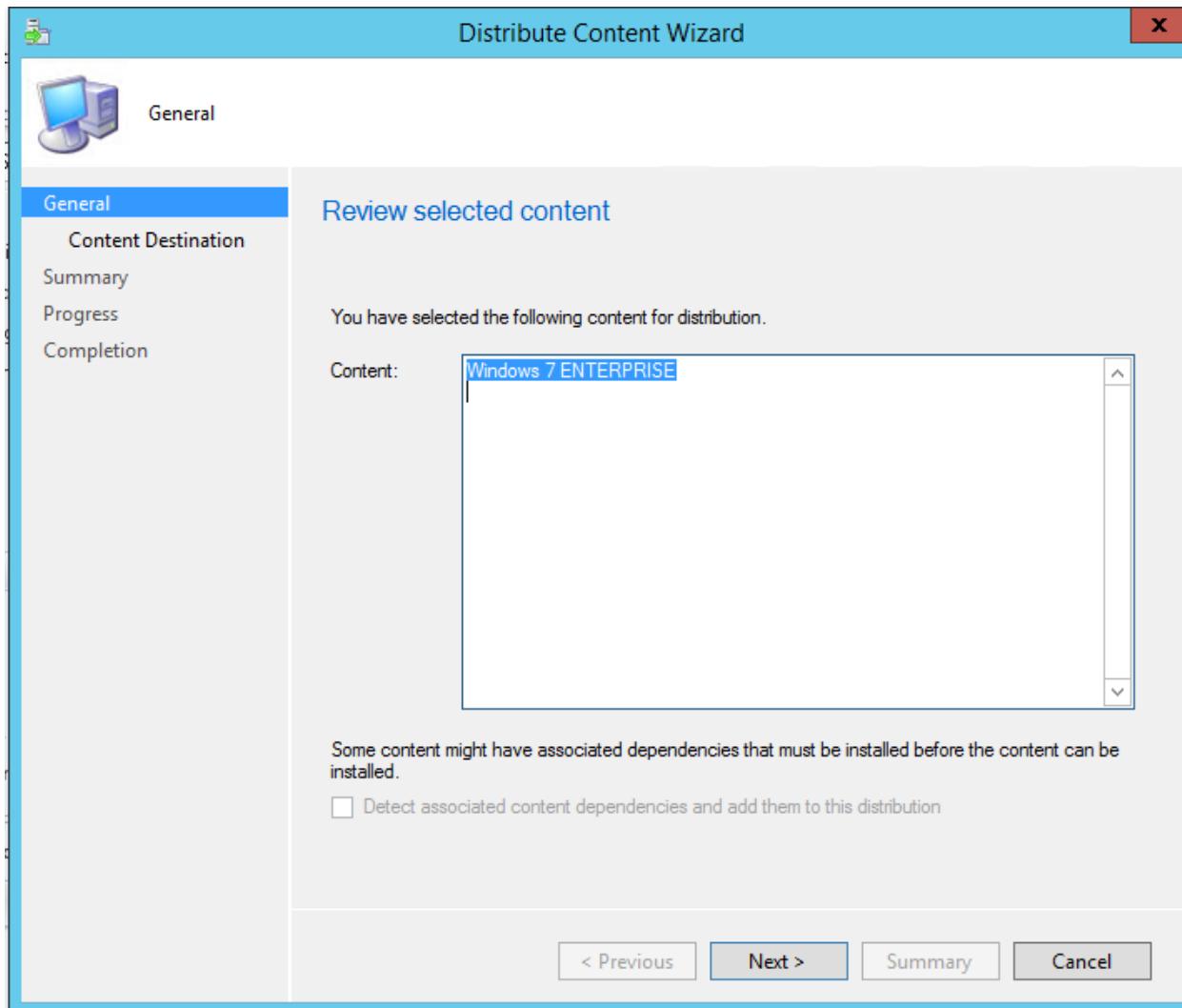


Now, you want to **distribute** the WIM. Right-click on the newly imported image, and click **Distribute**

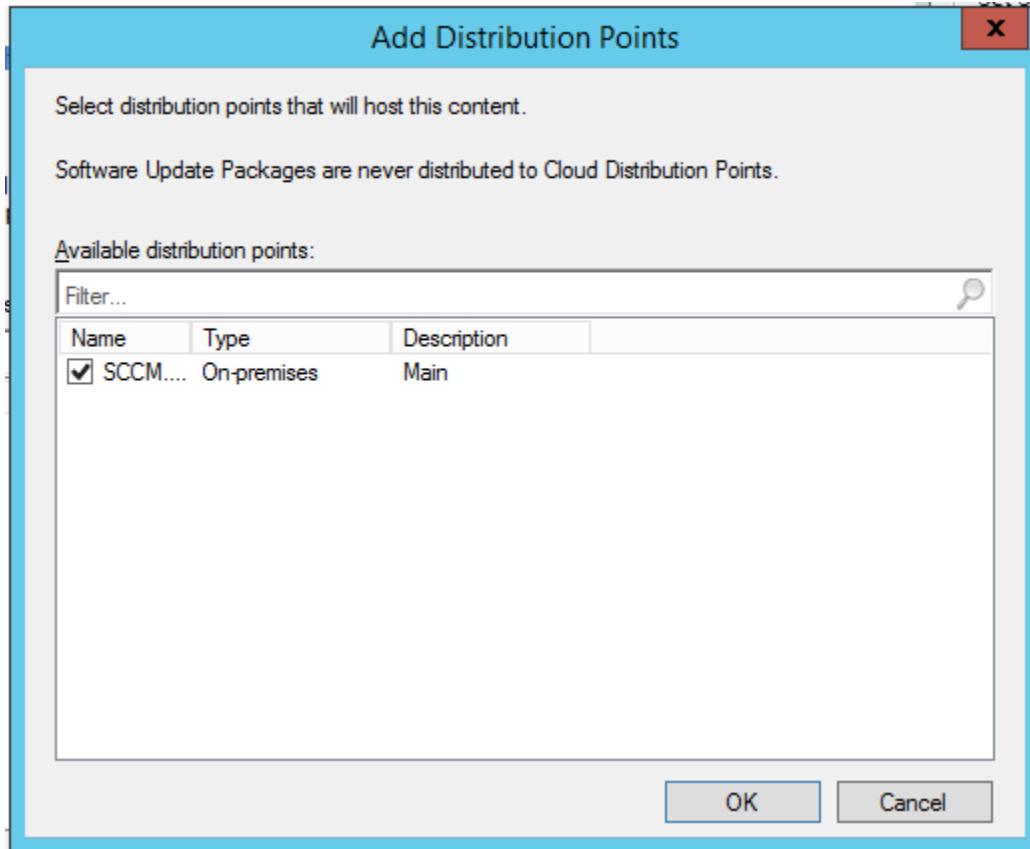
Content.



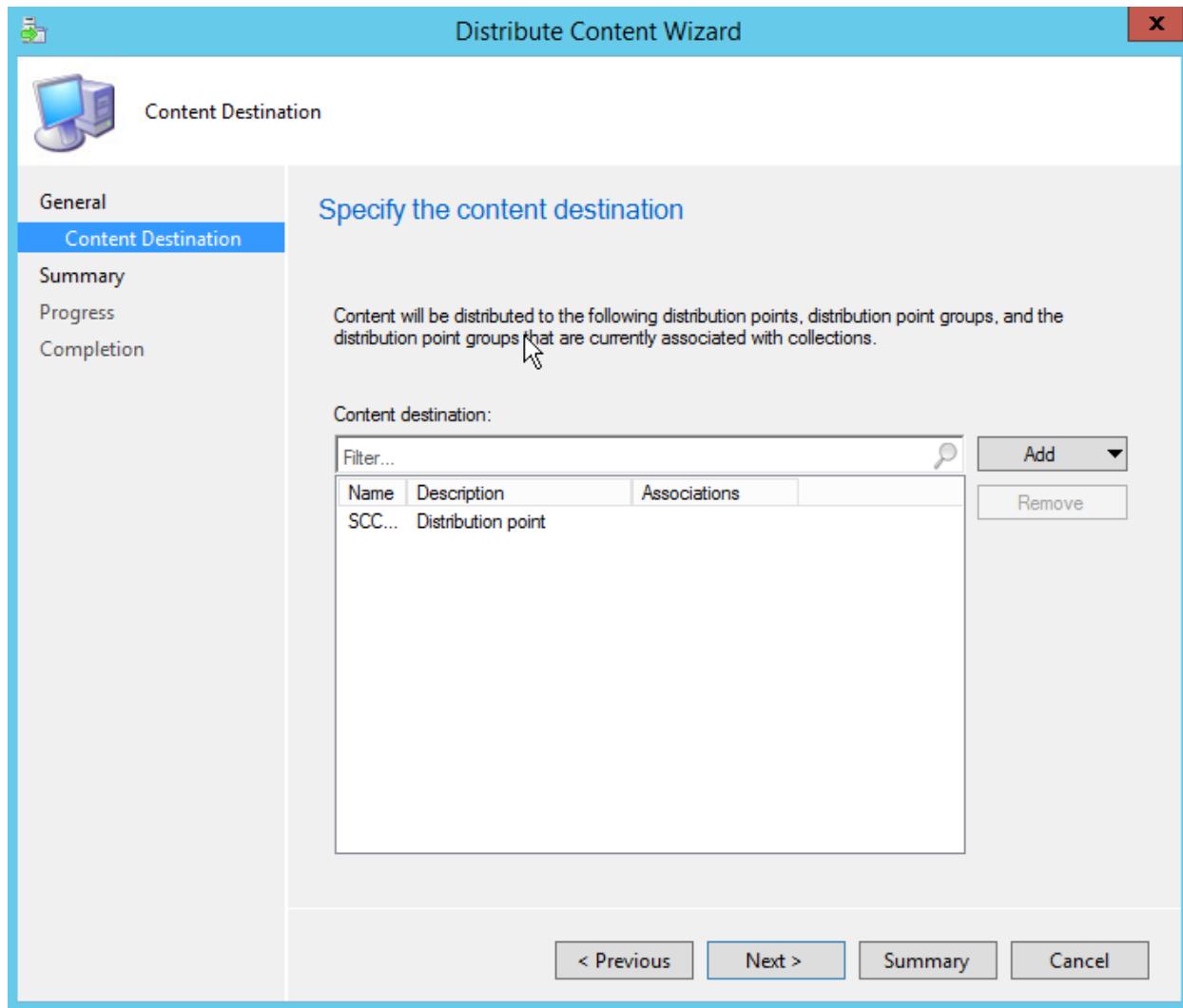
Click **Next**.



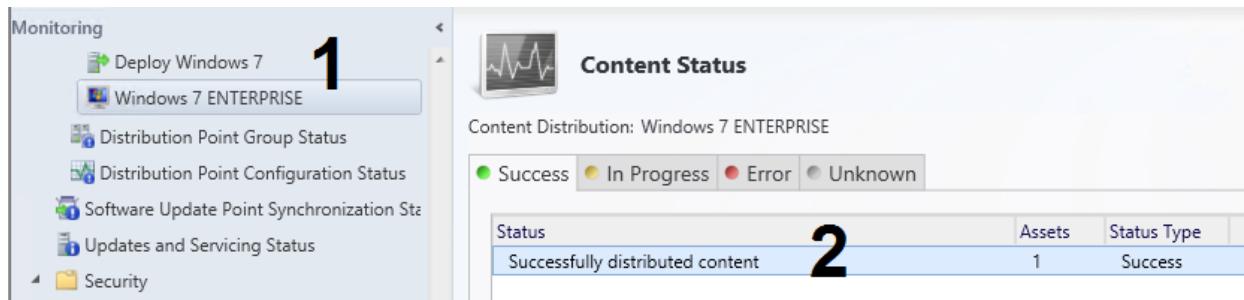
Select appropriate **distribution point**. **OK** to continue. If no distribution is available, it could mean the package is already available on the distribution point. In that case, just **Cancel** and move to **Deploy Steps**.



Next, Next, Close.

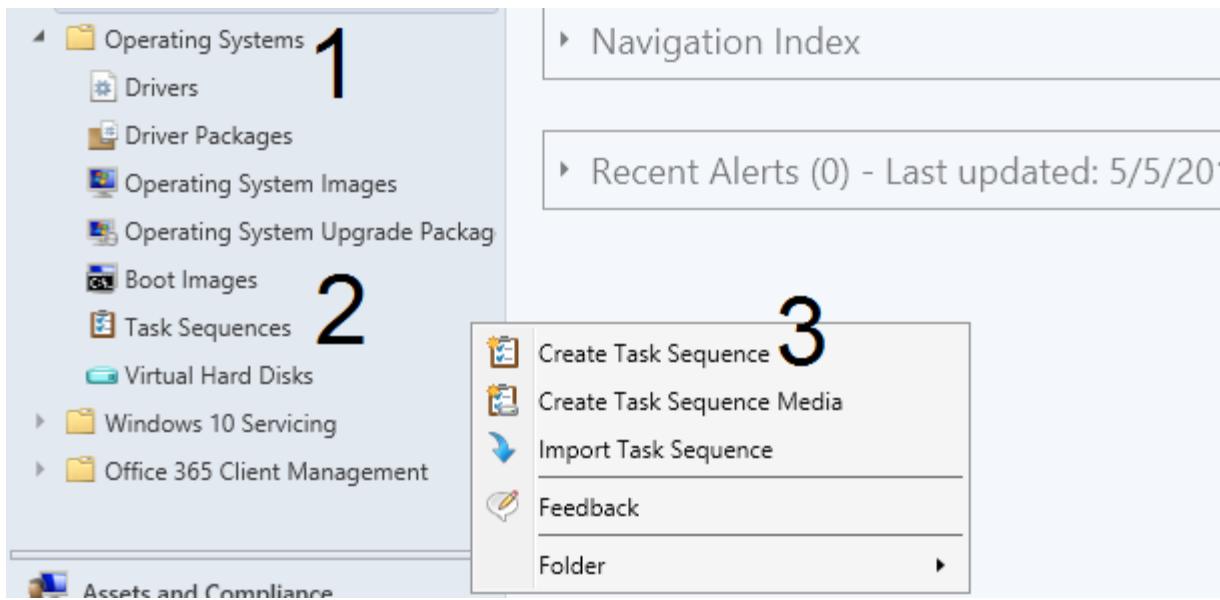


You can monitor the **Distribution Status** under **Administration > Monitoring > Content Status**.

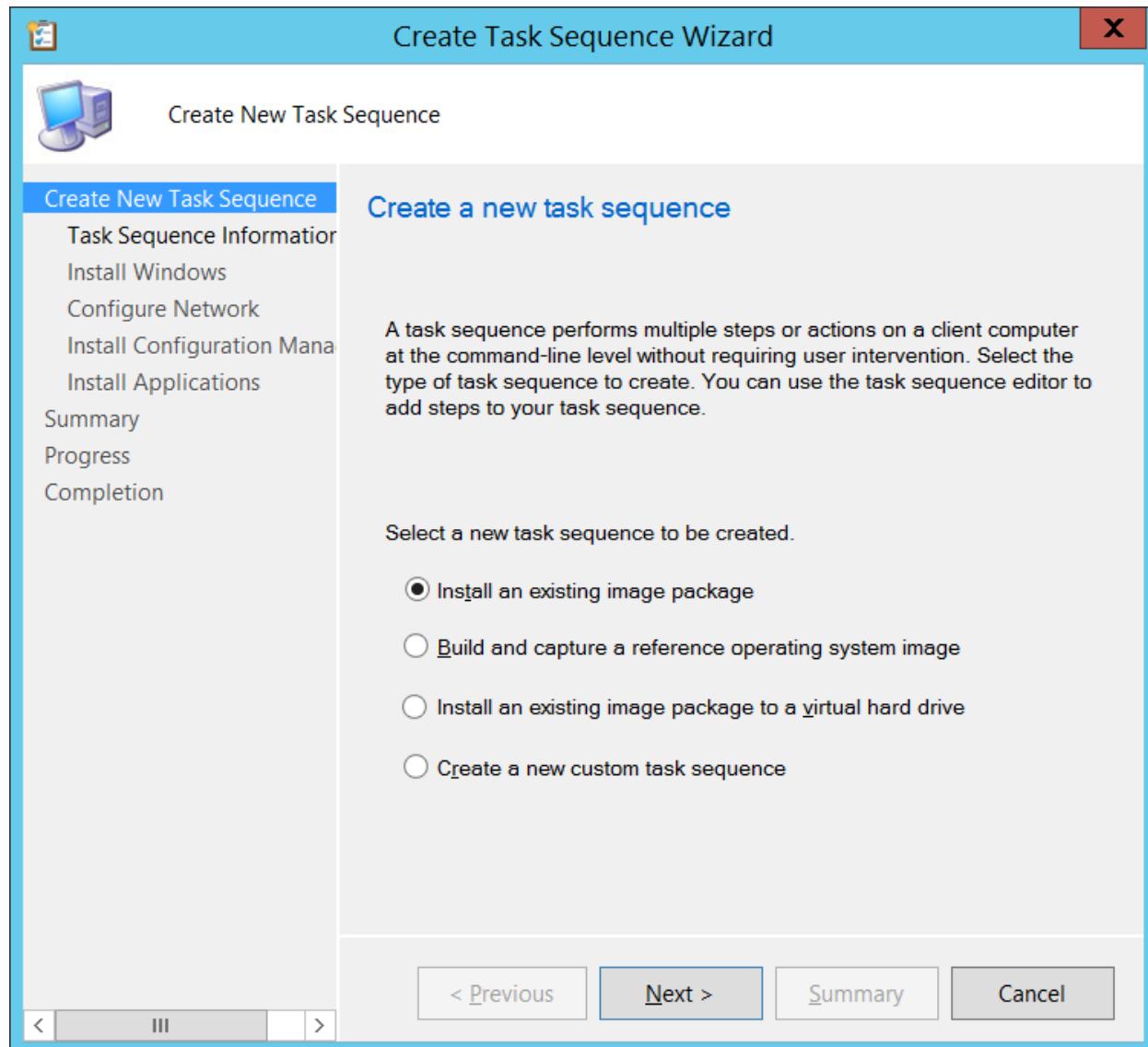


Deploy Image

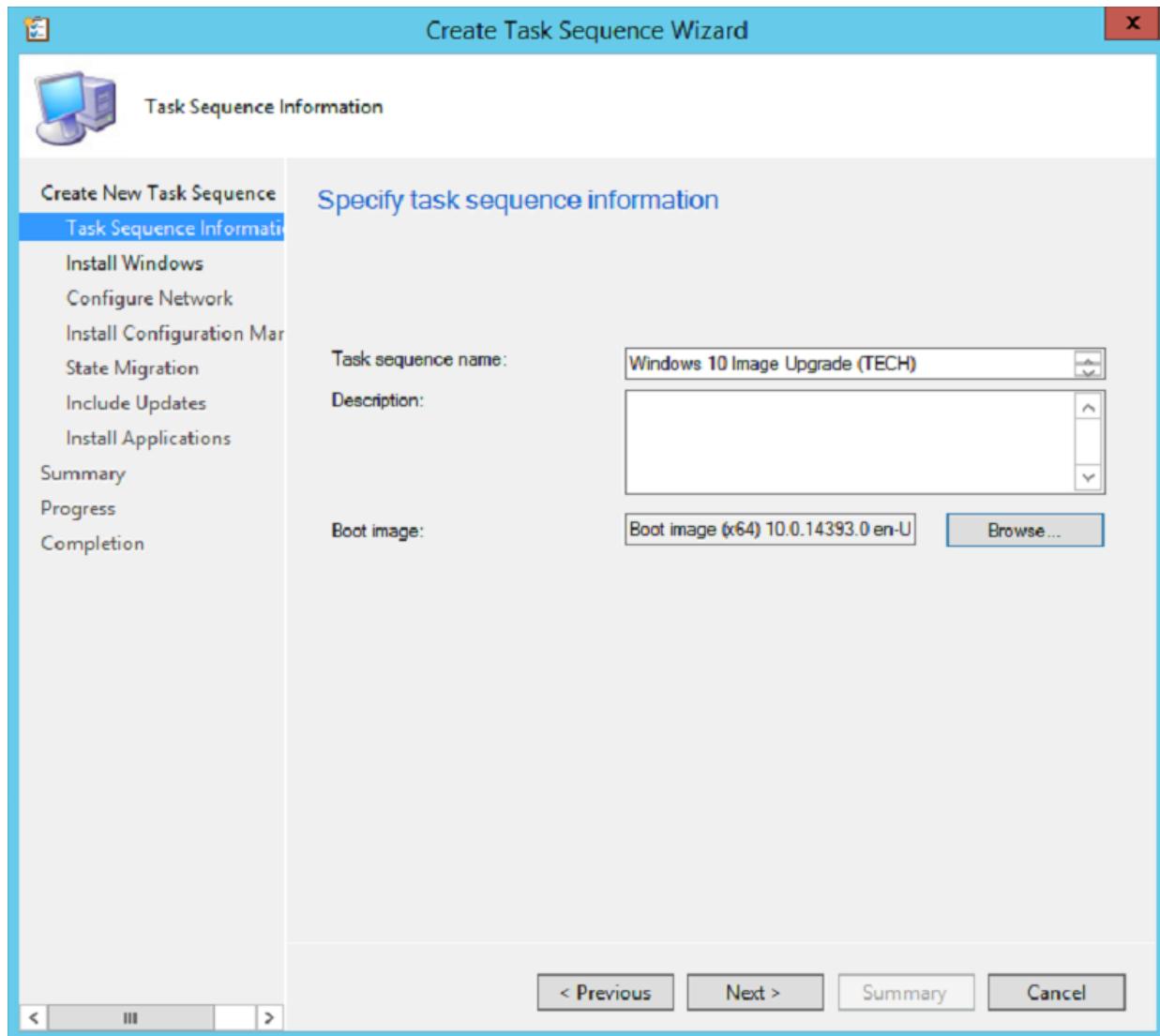
To be deploy an image, start in the **Operating Systems** and **Task Sequences**. Right-click and click **Create Task Sequence**.



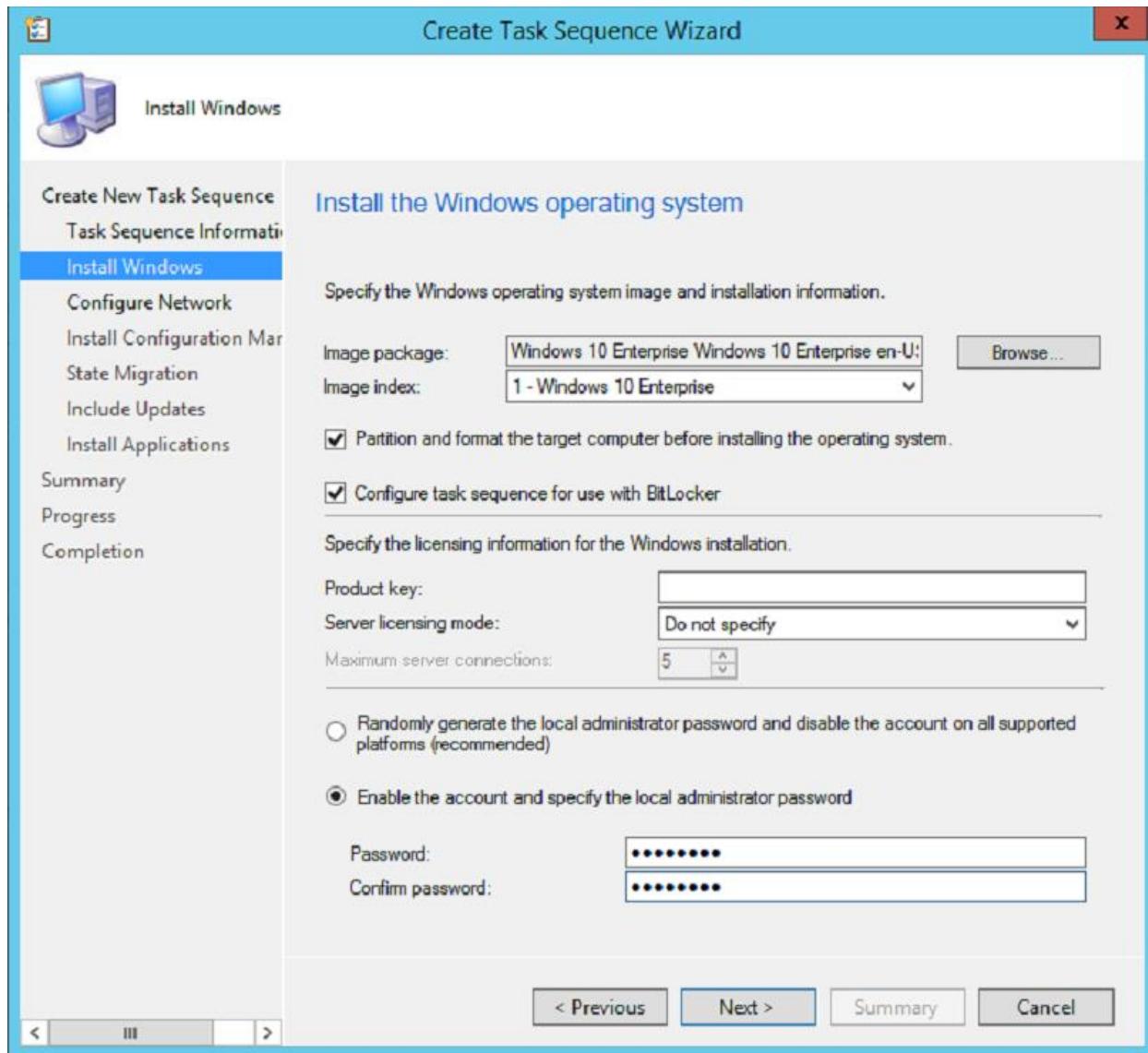
Select **Install an existing image package**. Click **Next**.



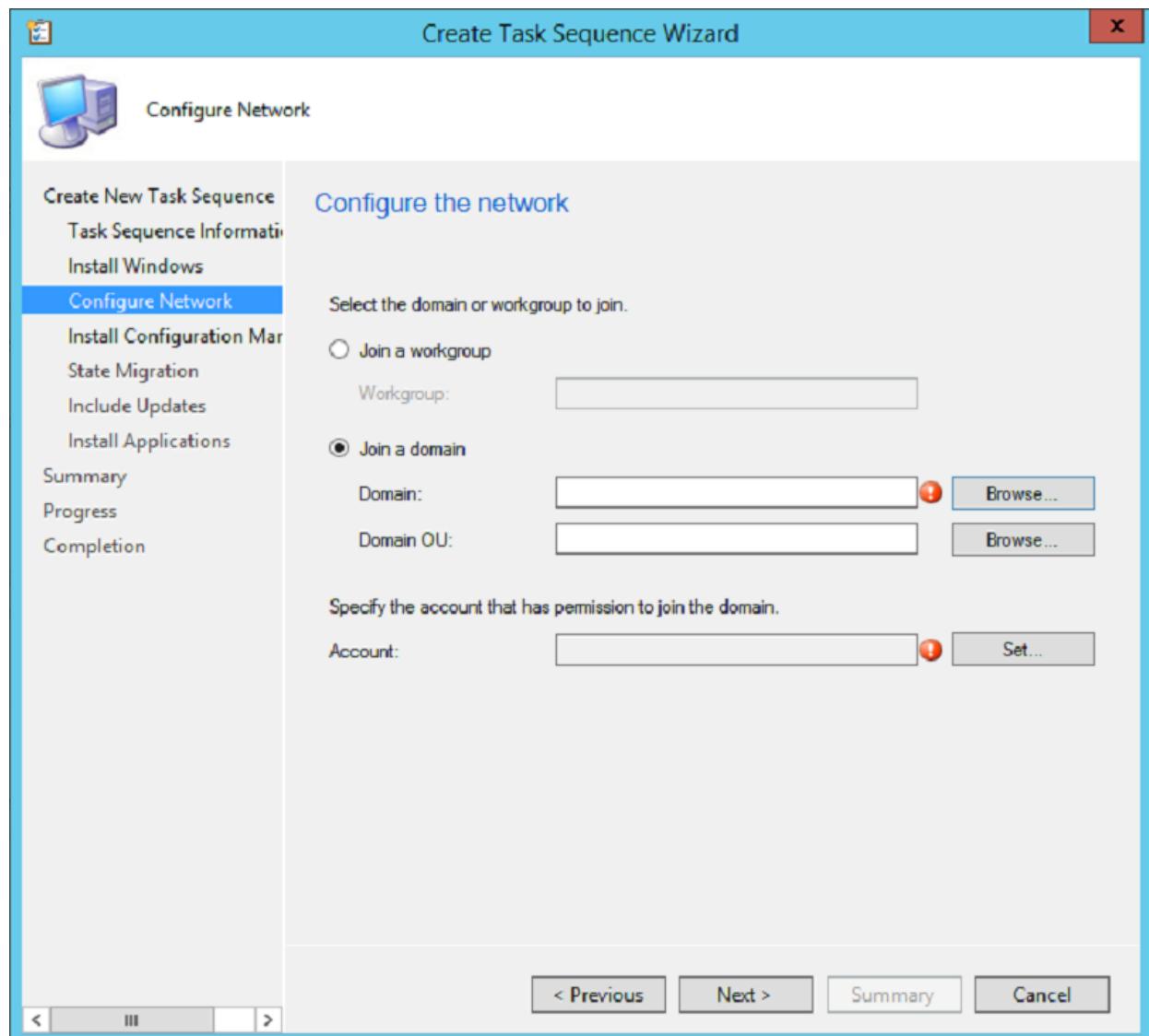
Enter **Task sequence name** and select **Boot image**. Click **Next**.



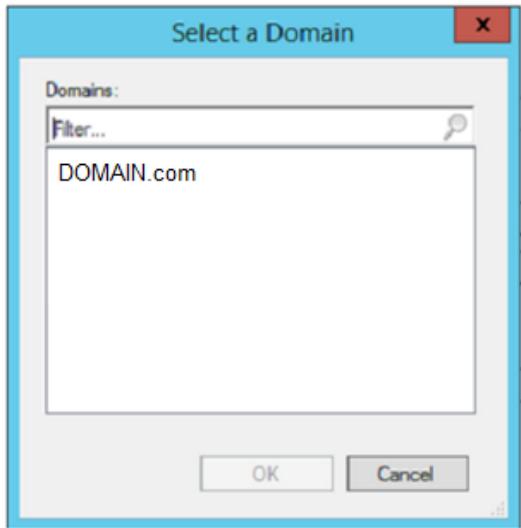
Select the **Image package/Operating System**, and **Enable** and **set admin password**. Click **Next**.



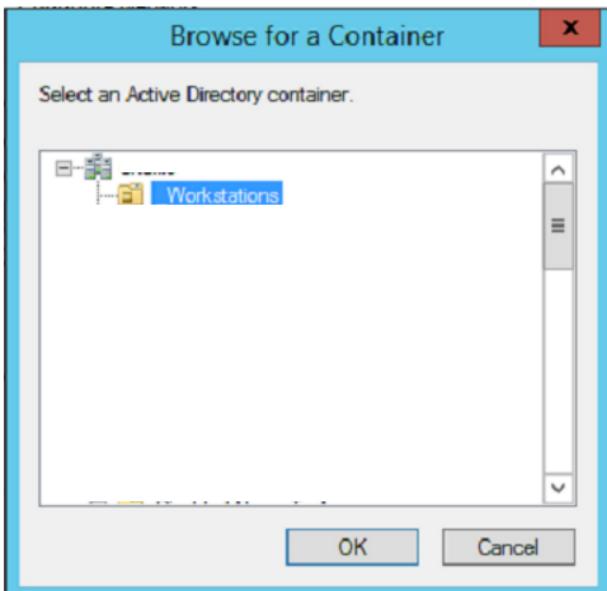
Select Join a Domain.



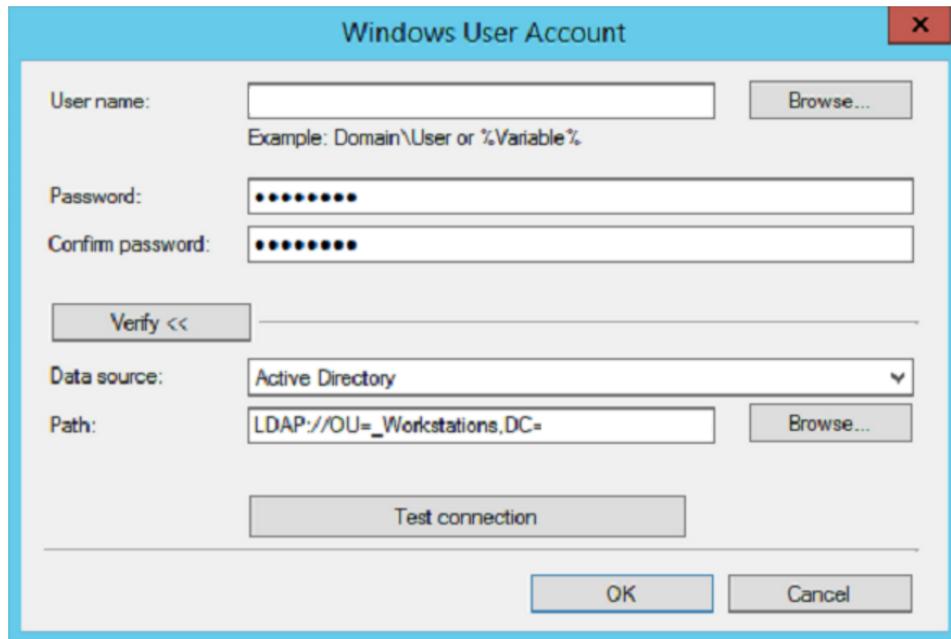
And then highlight the **domain**. Click **OK**.



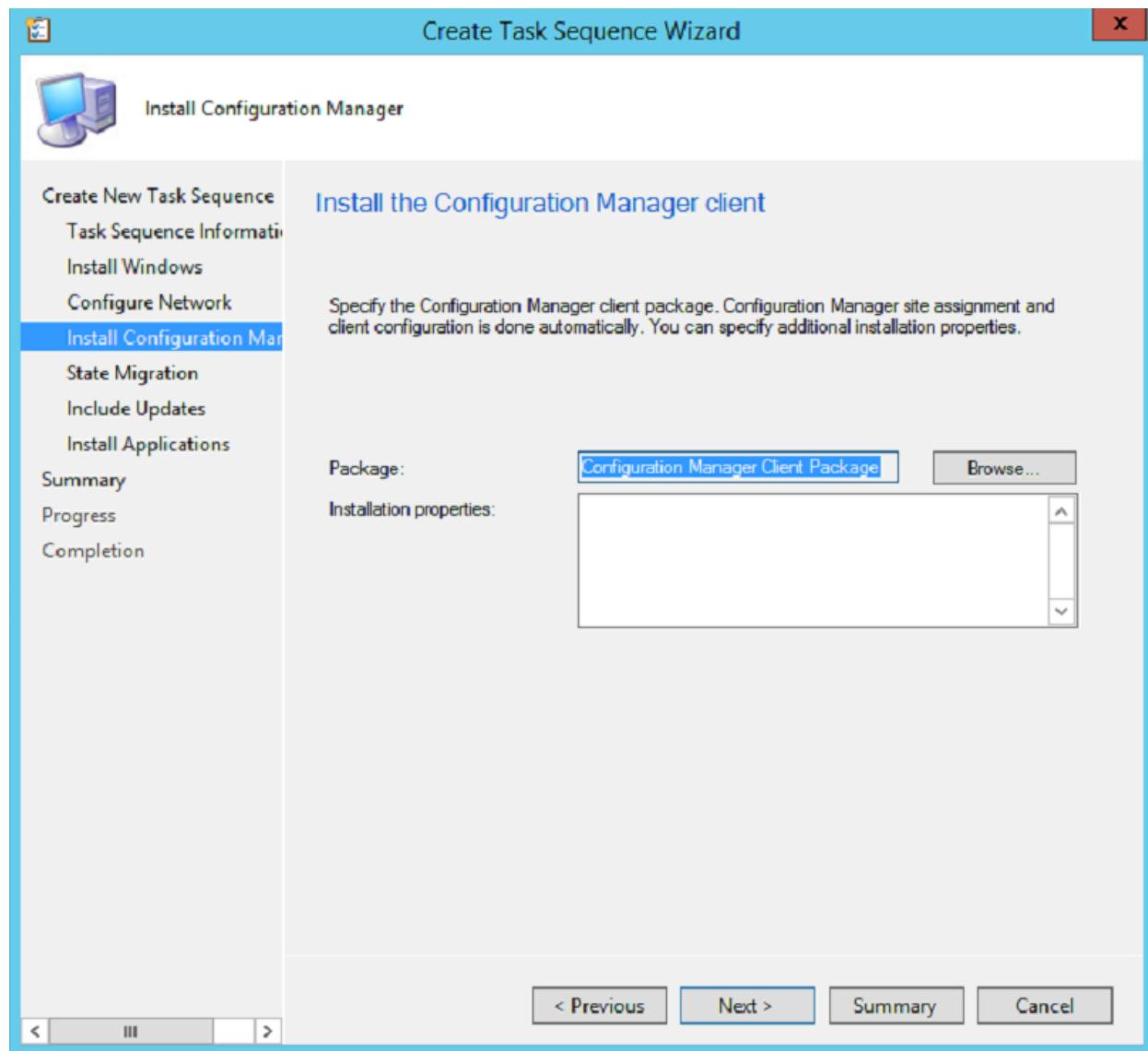
Browse to **Domain**. Highlight Domain. Click **OK**.



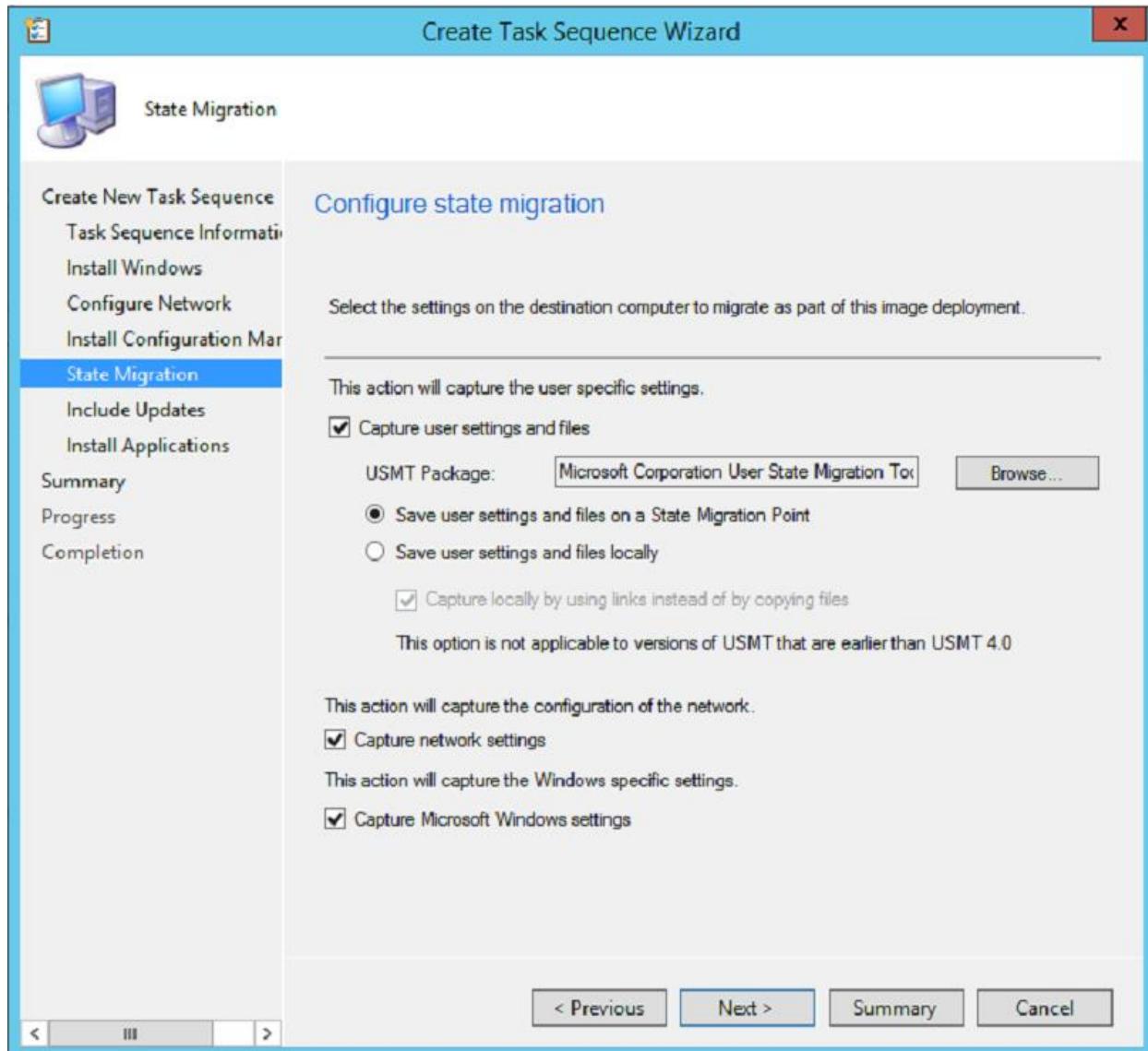
Click the **Set** button to enter the account that will be used to join the domain. **Test connection**. Click **OK** to continue. Click **Next**.



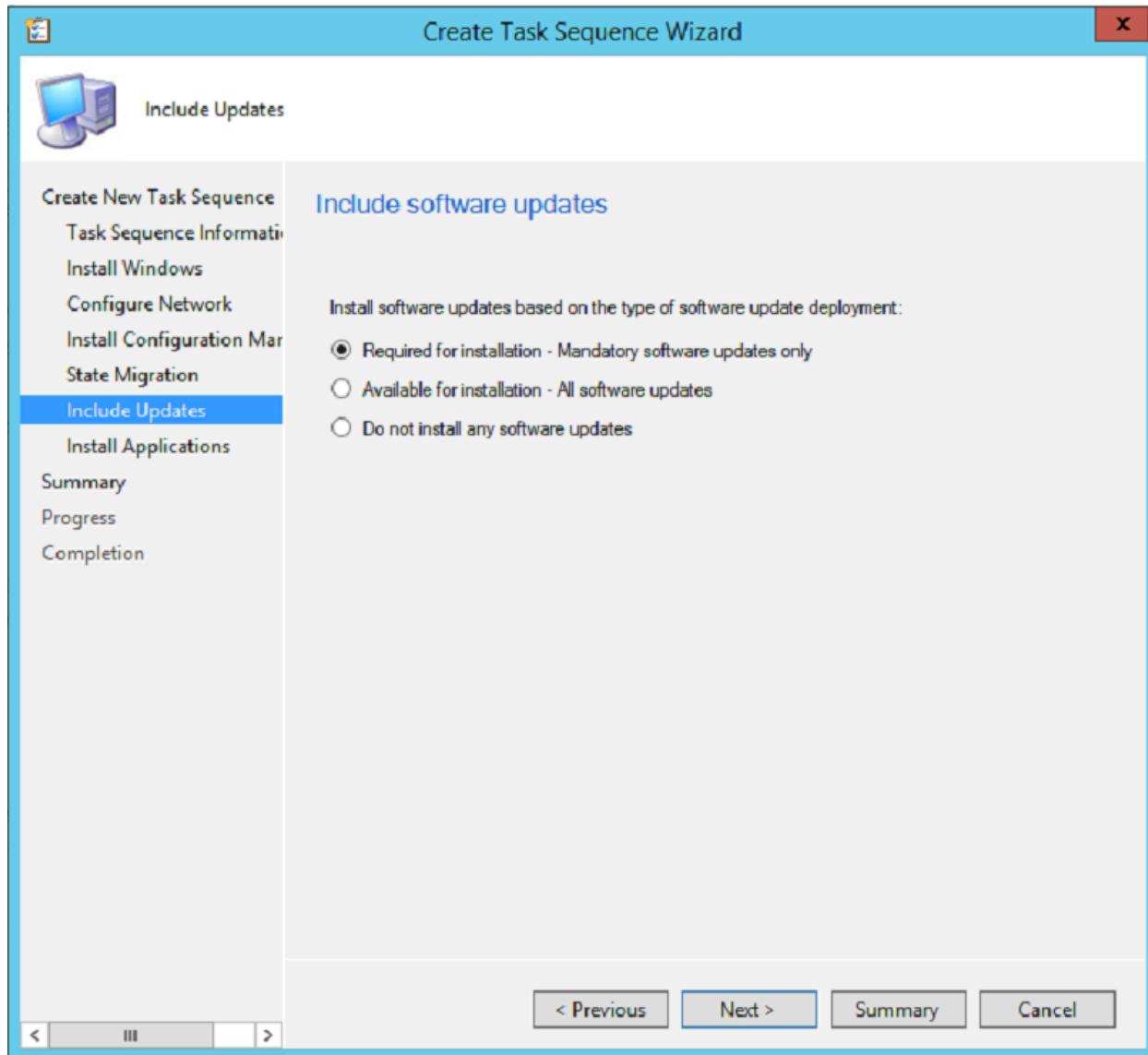
Click **Next**.



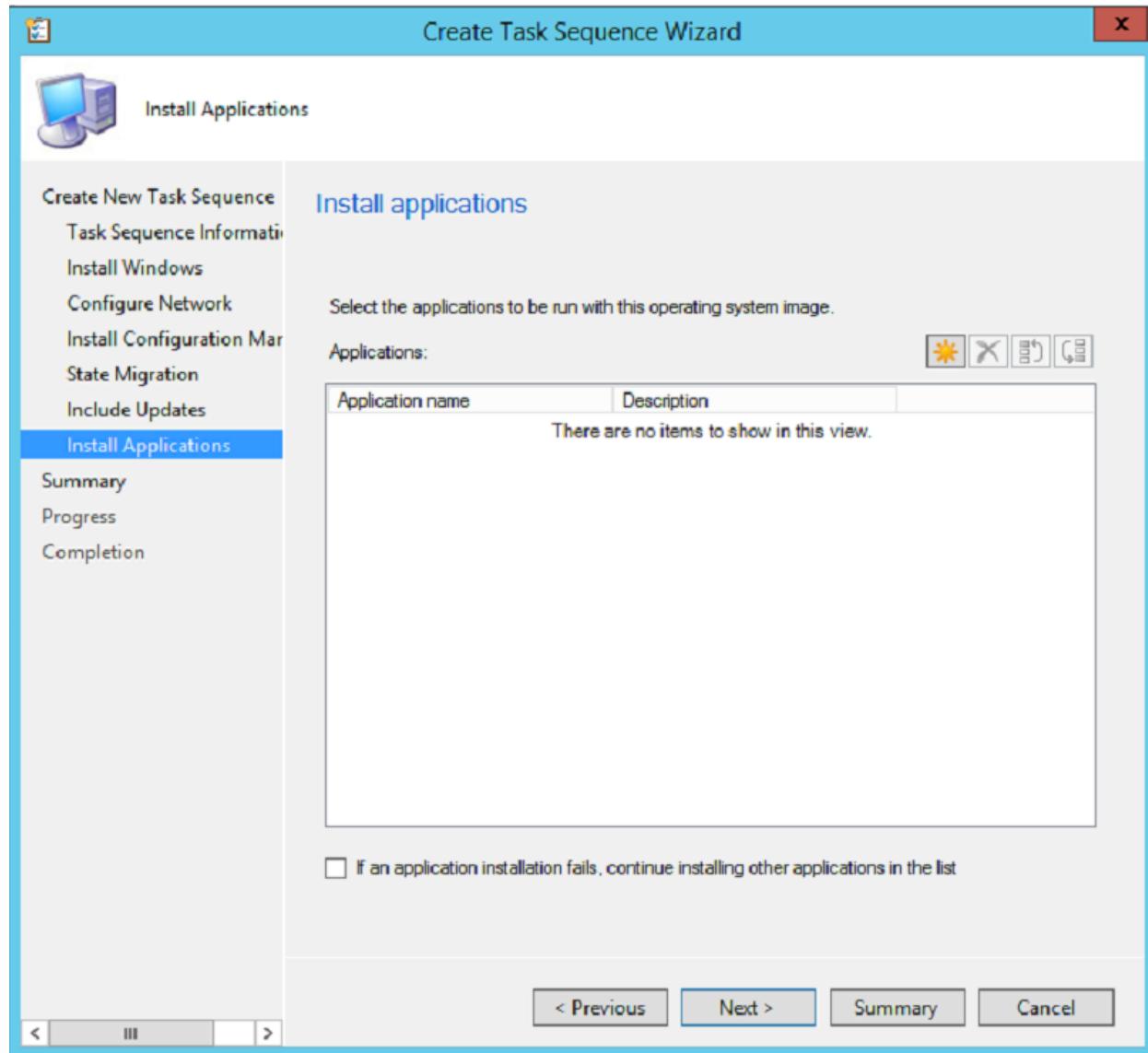
If this is an Upgrade, configure the state migration, otherwise uncheck these options. Click **Next**.



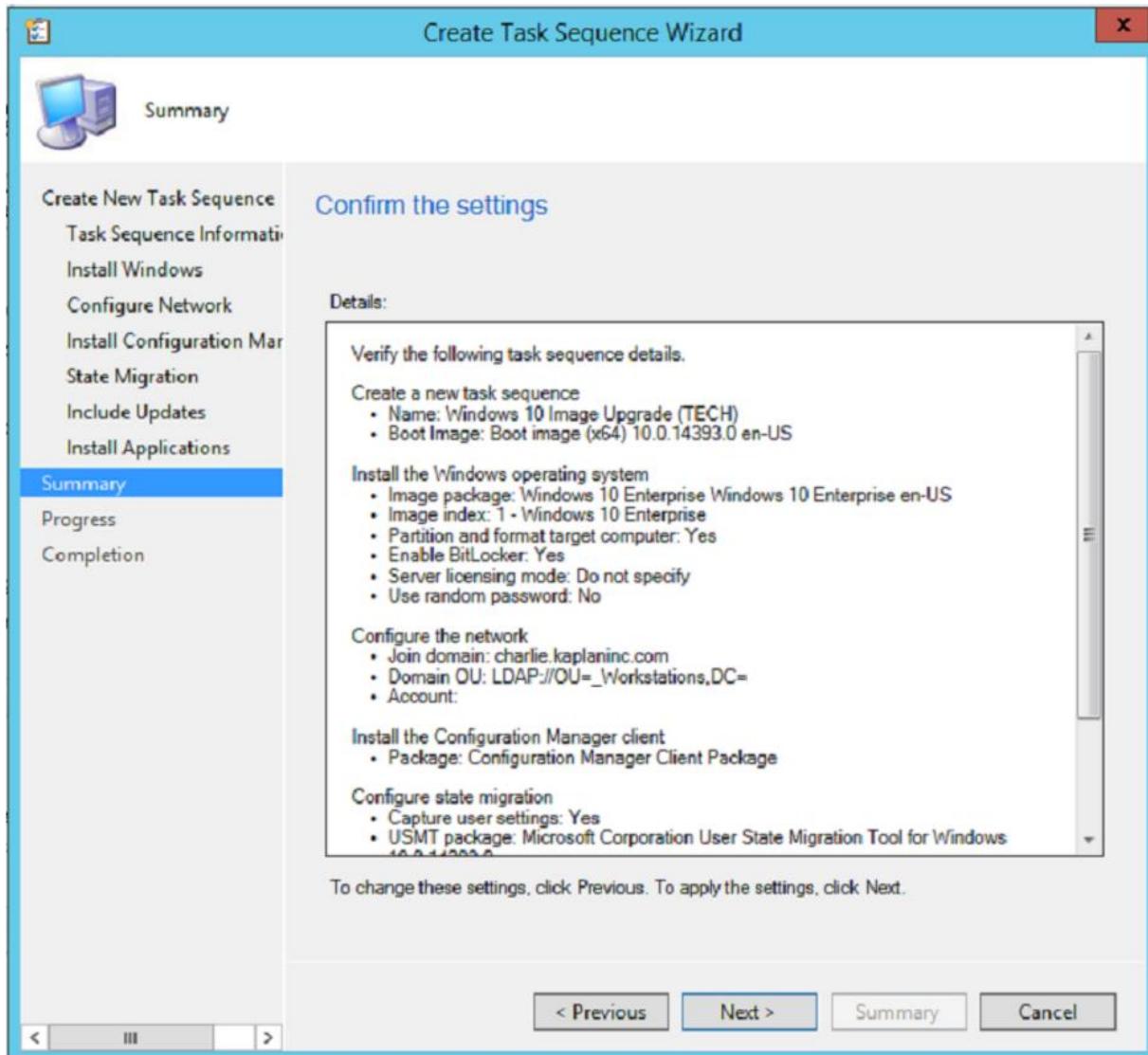
Select the **Updates** option. Click **Next**.



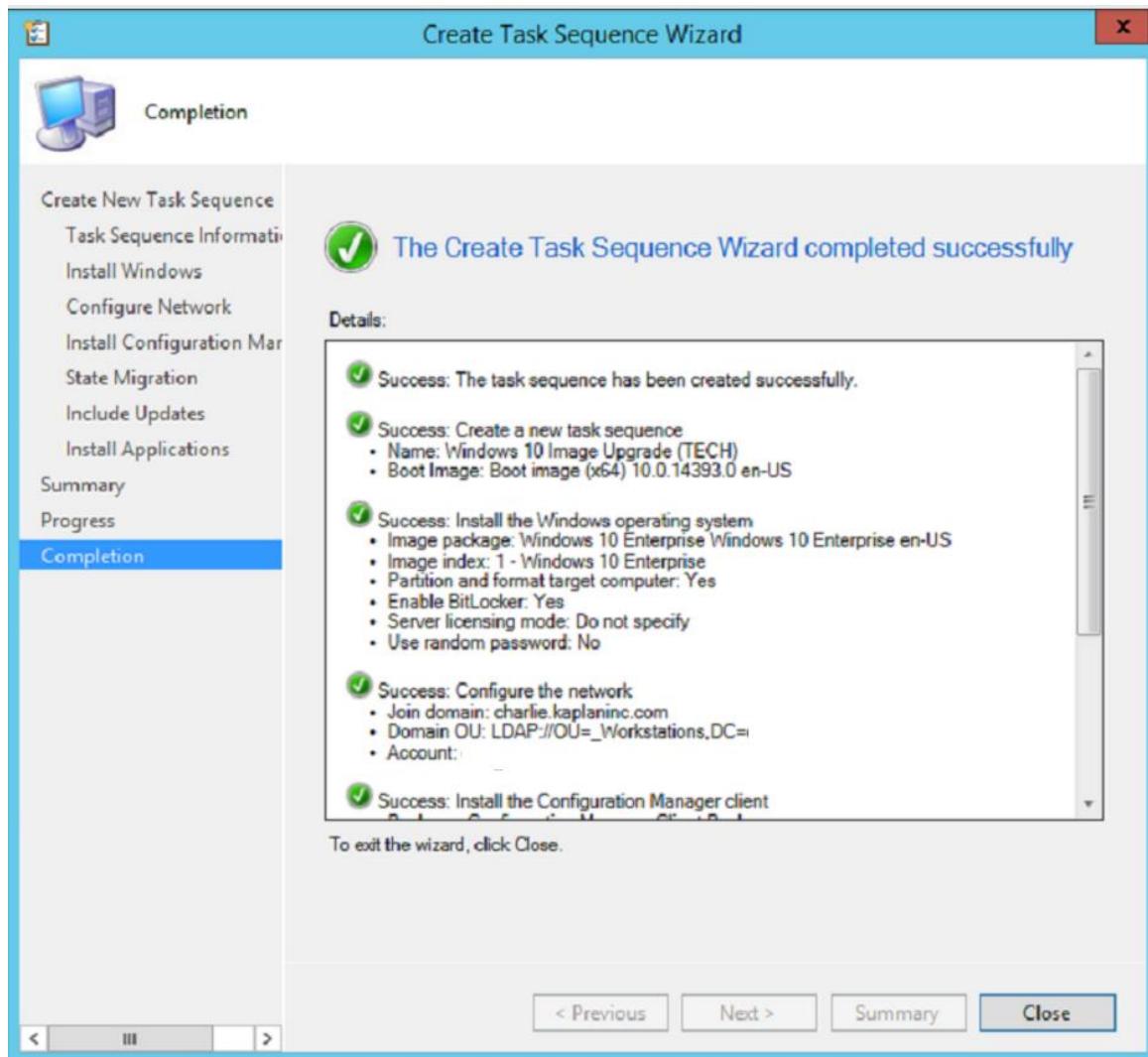
Select any **applications** to be installed. Click **Next**.



Confirm the settings. Click **Next**.



Click **Close**.



Distribute the Content to appropriate Distribution Points, and you're ready to deploy. To start the deploy, right-click on task sequence and select **Deploy**.

Task Sequences 2 items

Icon	Name	Description	Package ID	Date Created
Windows 10 Image Upgrade (ADMIN)	Windows 10 Image Upgrade (ADMIN)		015	4/27/2017 5:01 PM
Windows 10 Image Upgrade (TECH)	Windows 10 Image Upgrade (TECH)		015	5/1/2017 2:09 PM

1

2

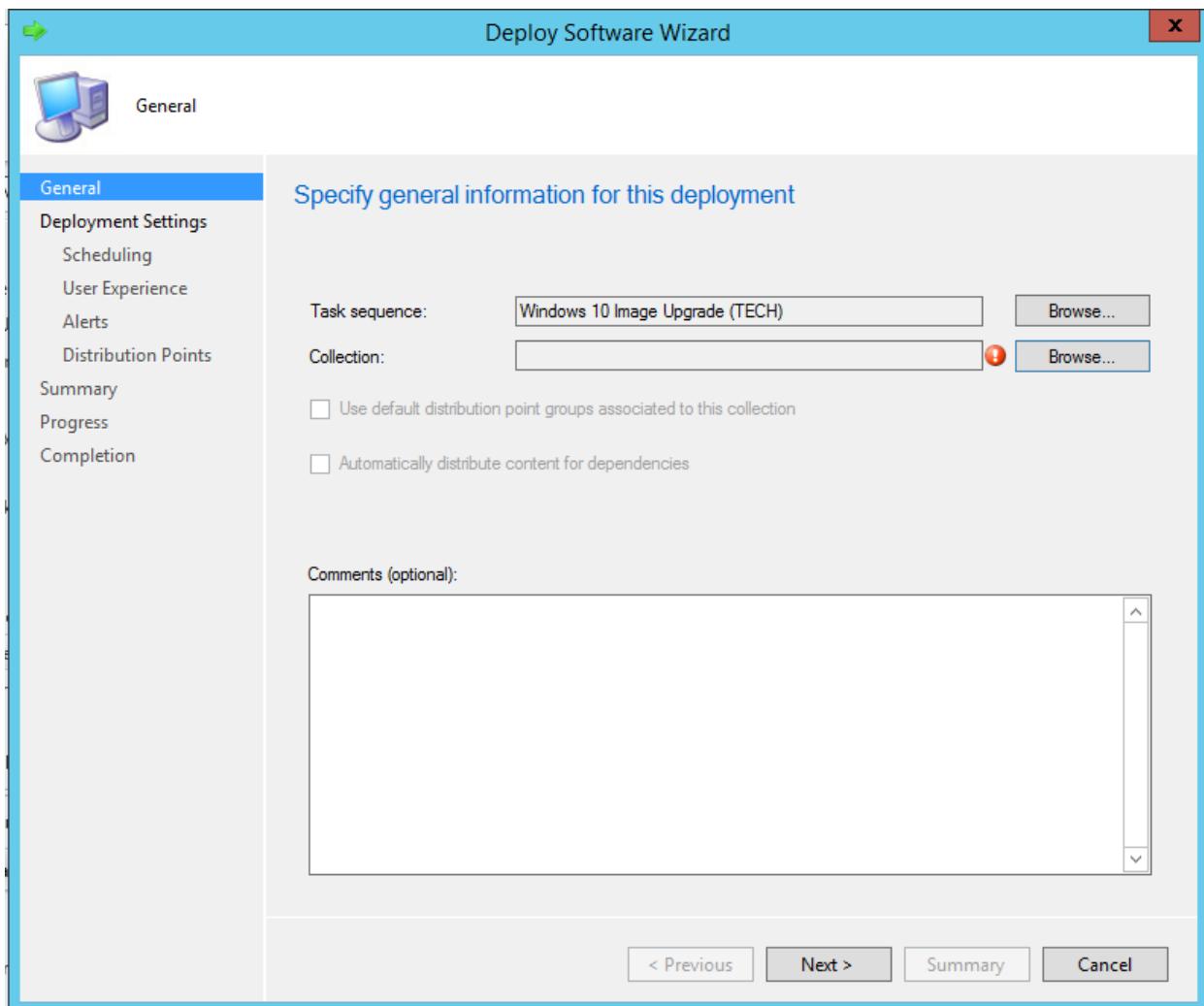
Windows 10 Image Upgrade (TECH)

Summary

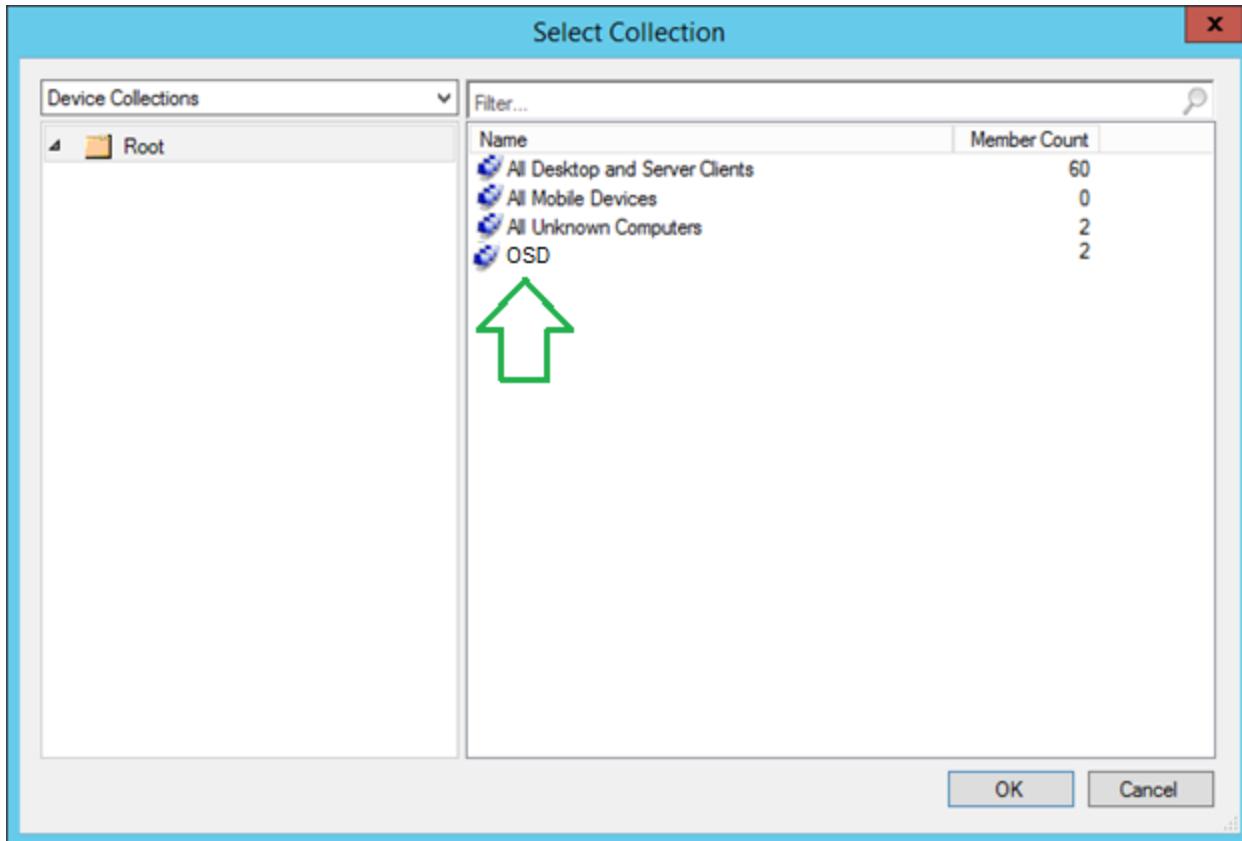
Name:	Windows 10 Image
Description:	
Package ID:	
Package Type:	4
Boot Image ID:	

Edit
Enable
Disable
Export
Copy
Refresh F5
Delete Delete
Deploy
Distribute Content
Create Prestaged Content File
Move
Set Security Scopes
Properties

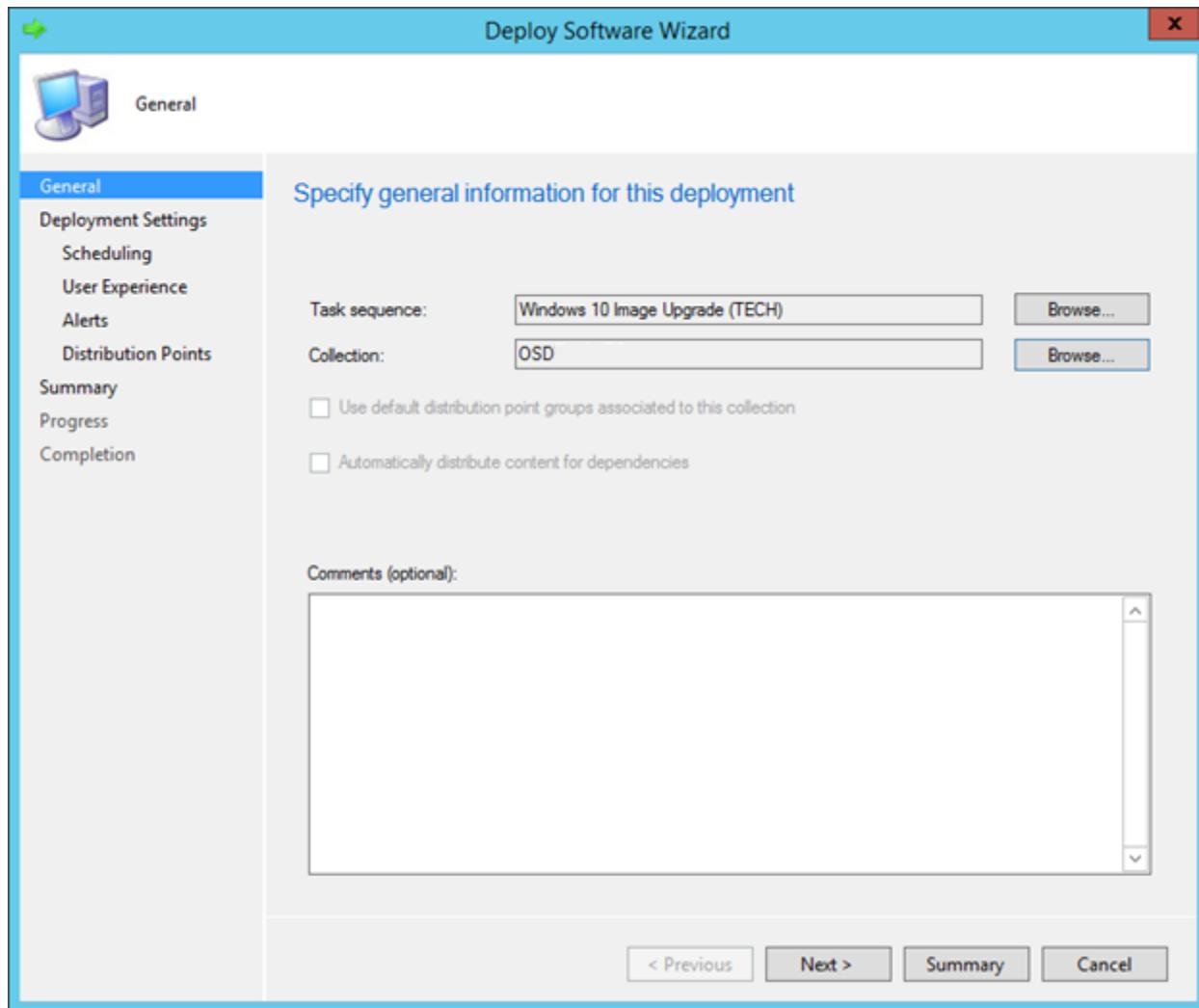
Browse to Collections.



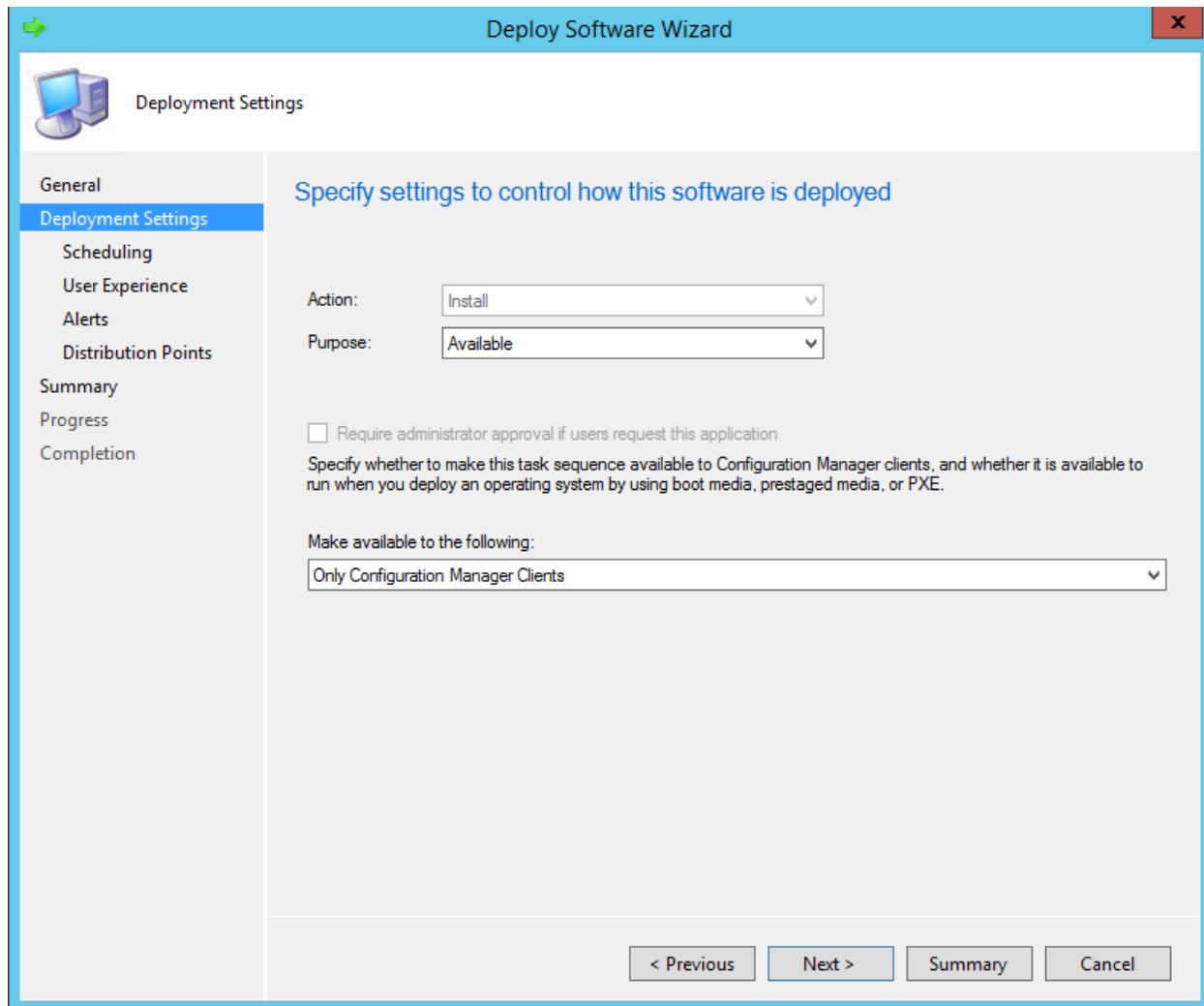
Select **Collection** (OSD is my imaging collection). Click **OK**.



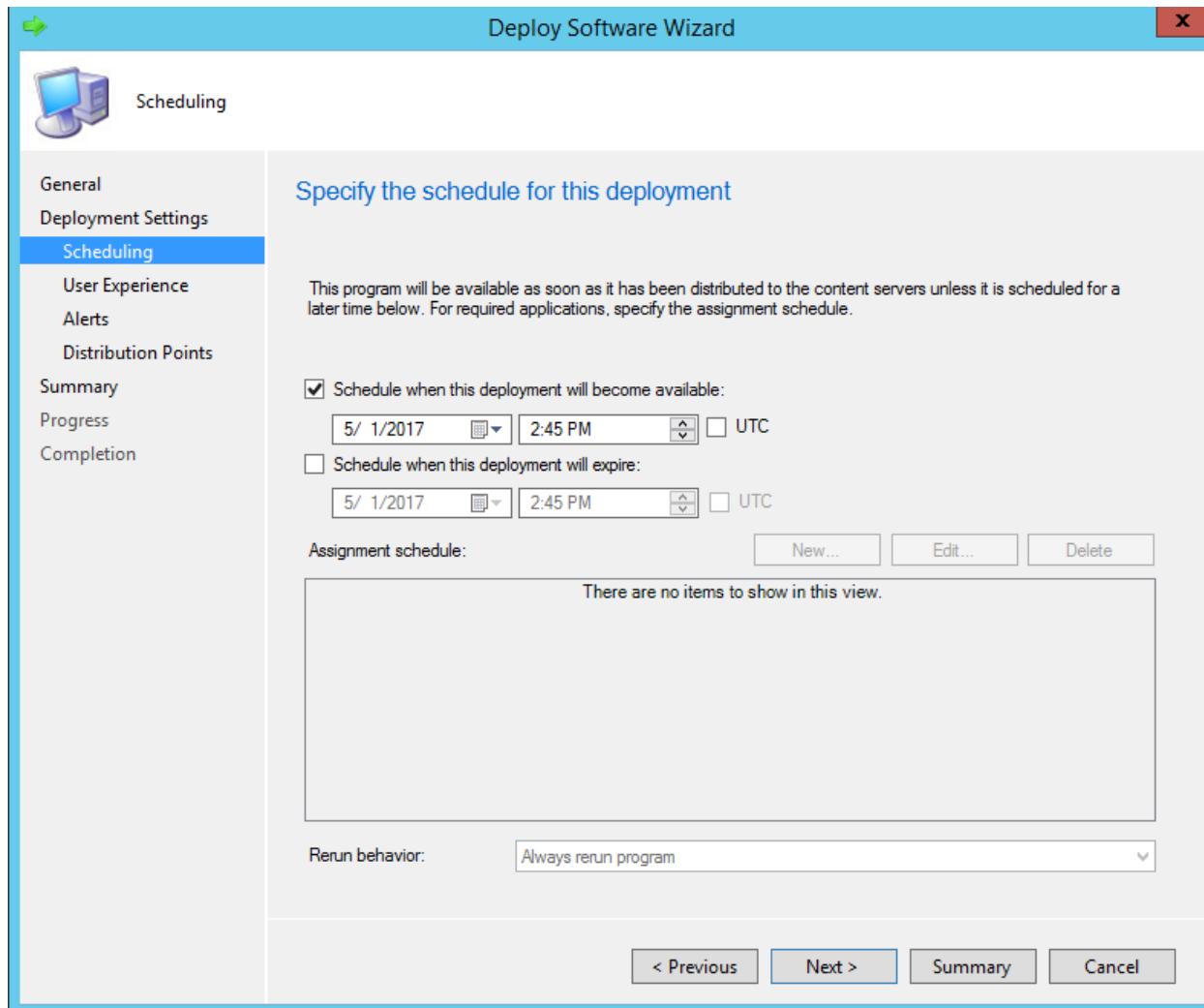
Click **Next**.



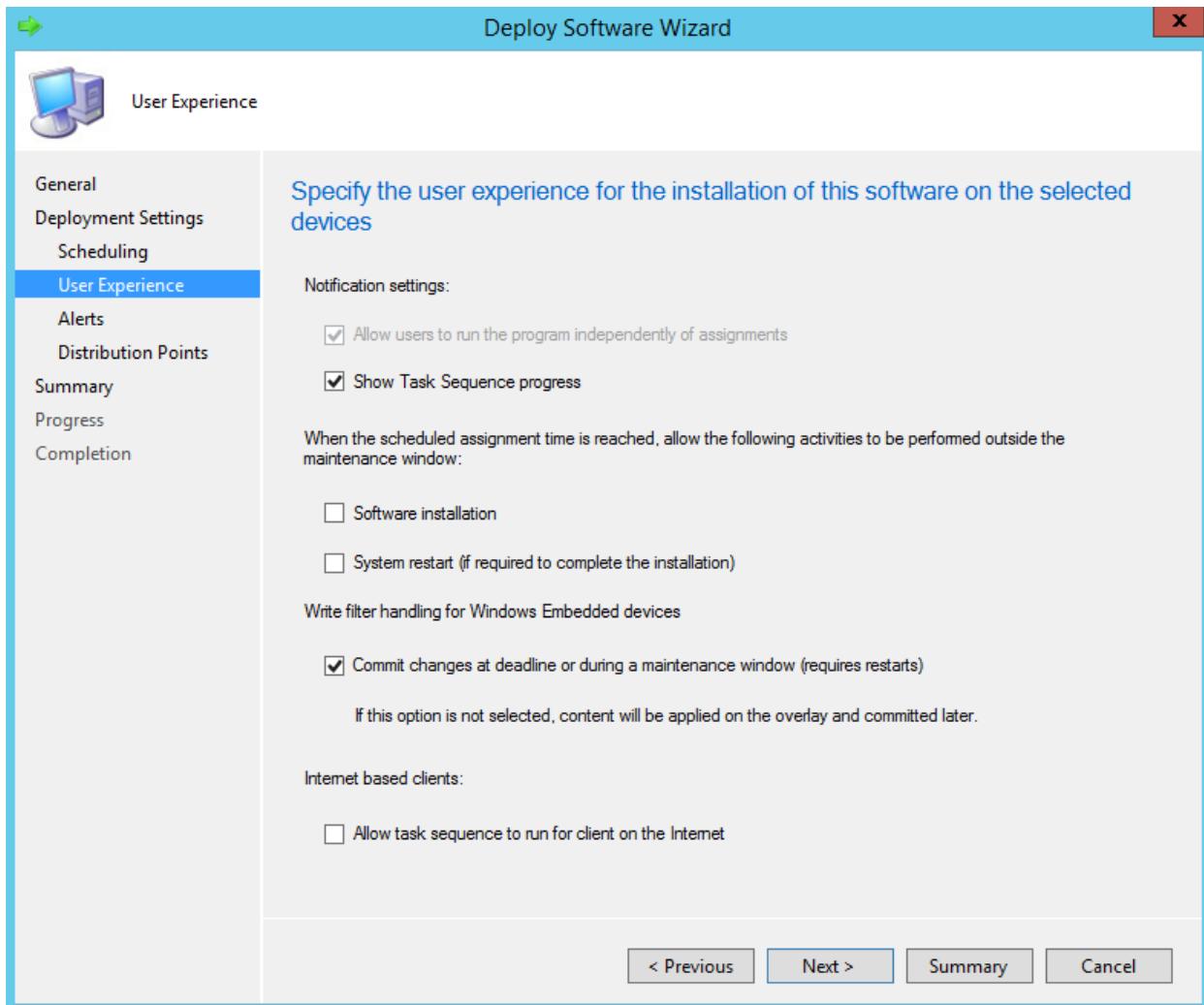
Specify **Purpose**. Click **Next**.



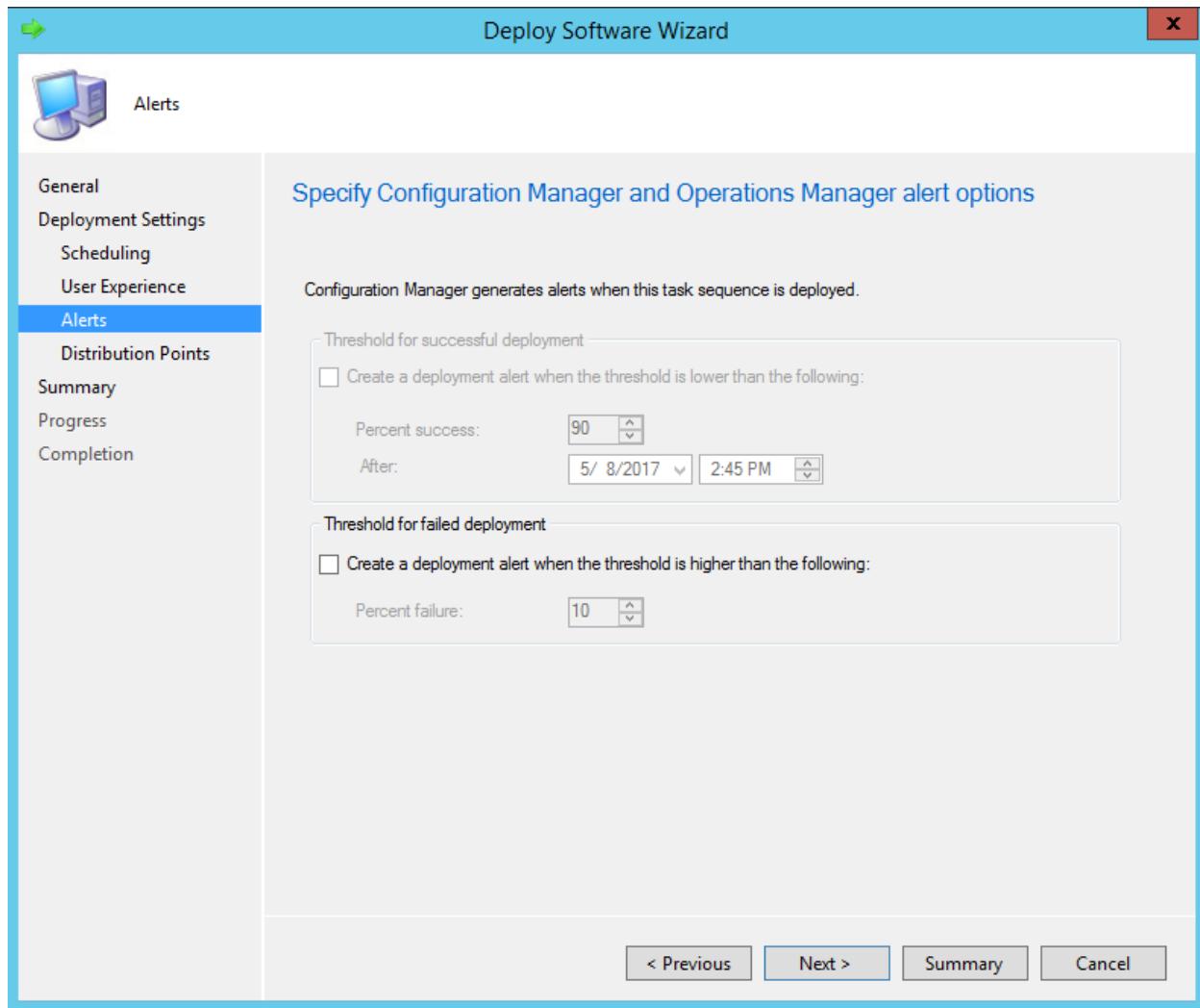
Specify **schedule**. Click **Next**.



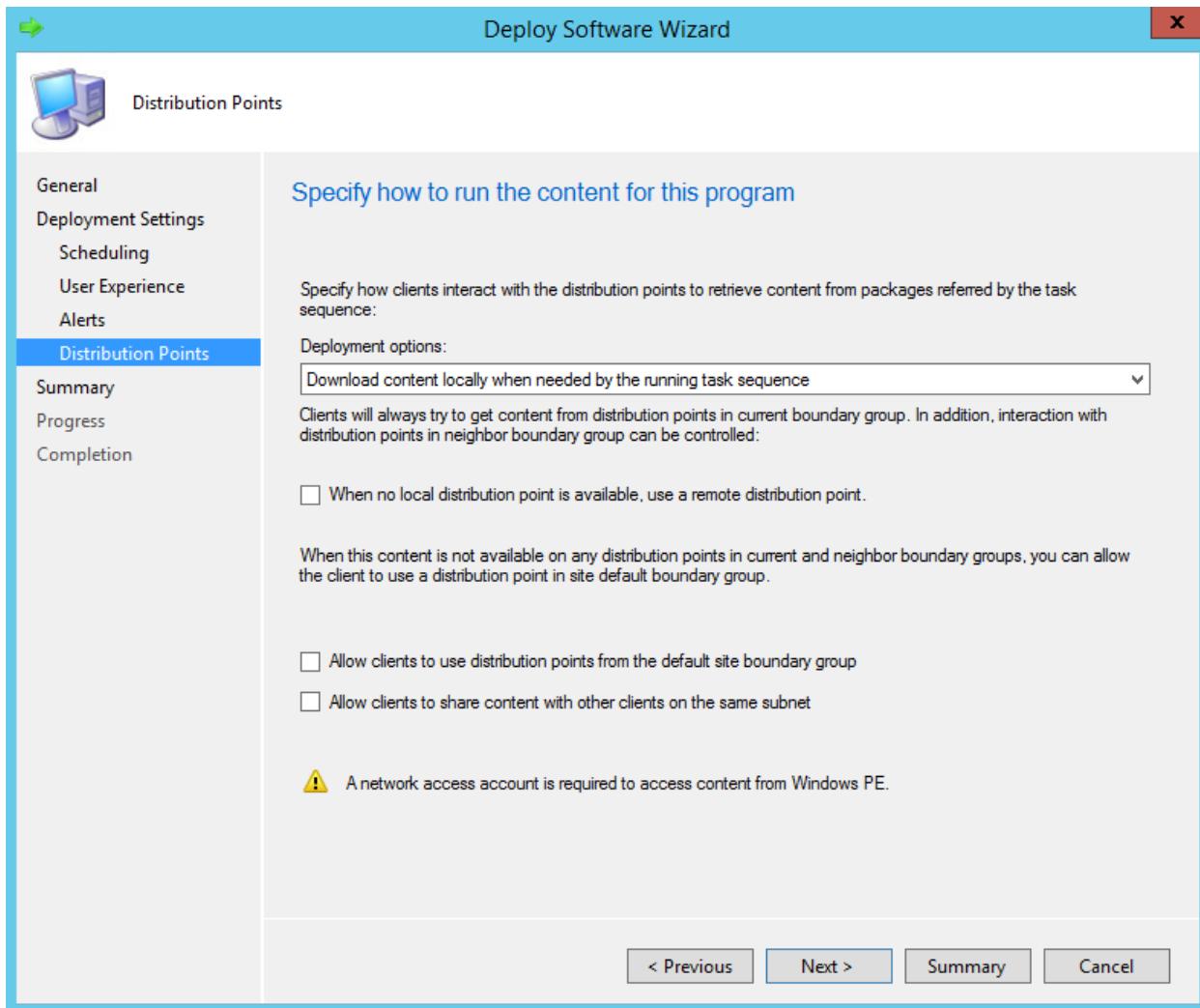
Click **Next**.



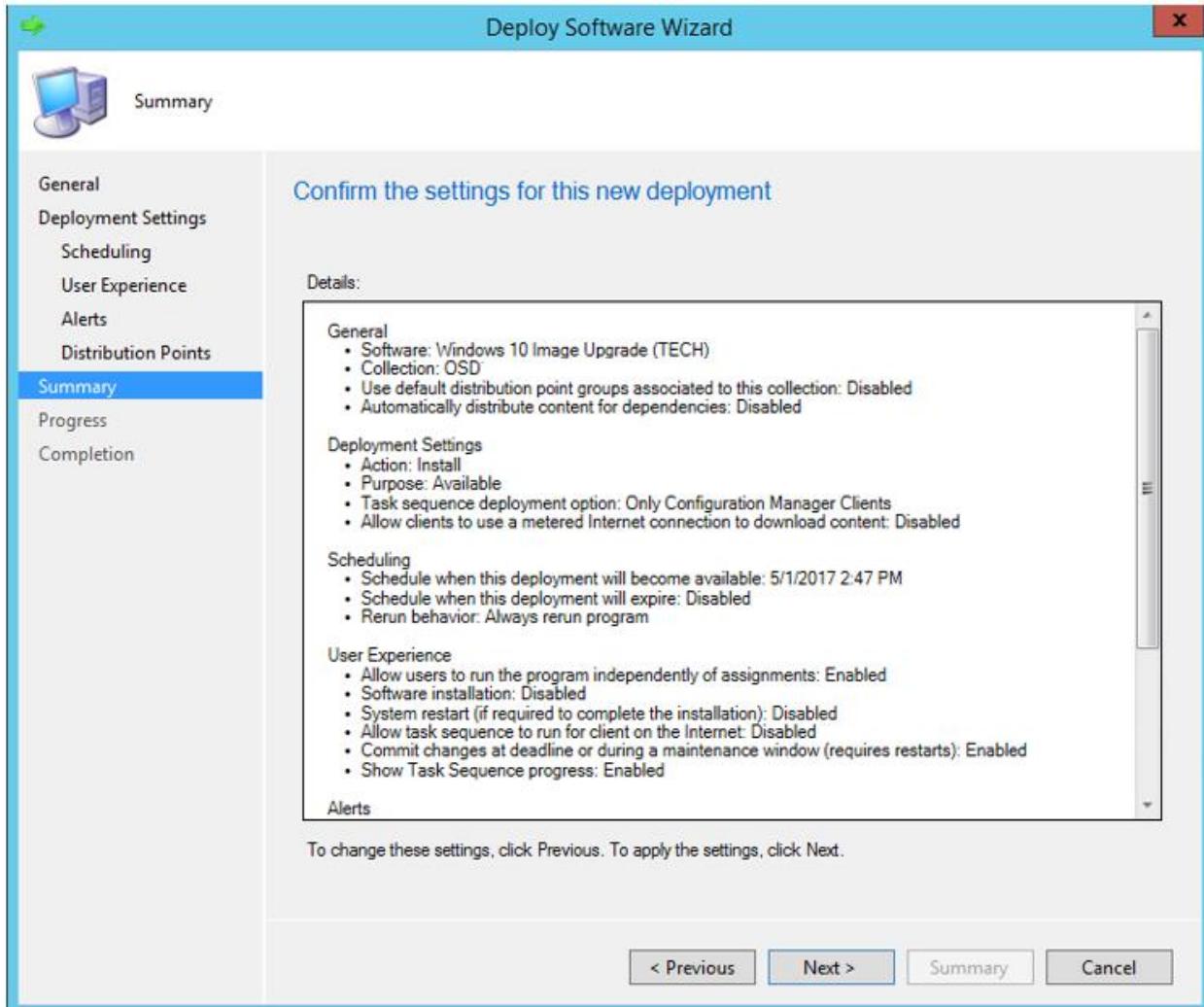
Click **Next**.



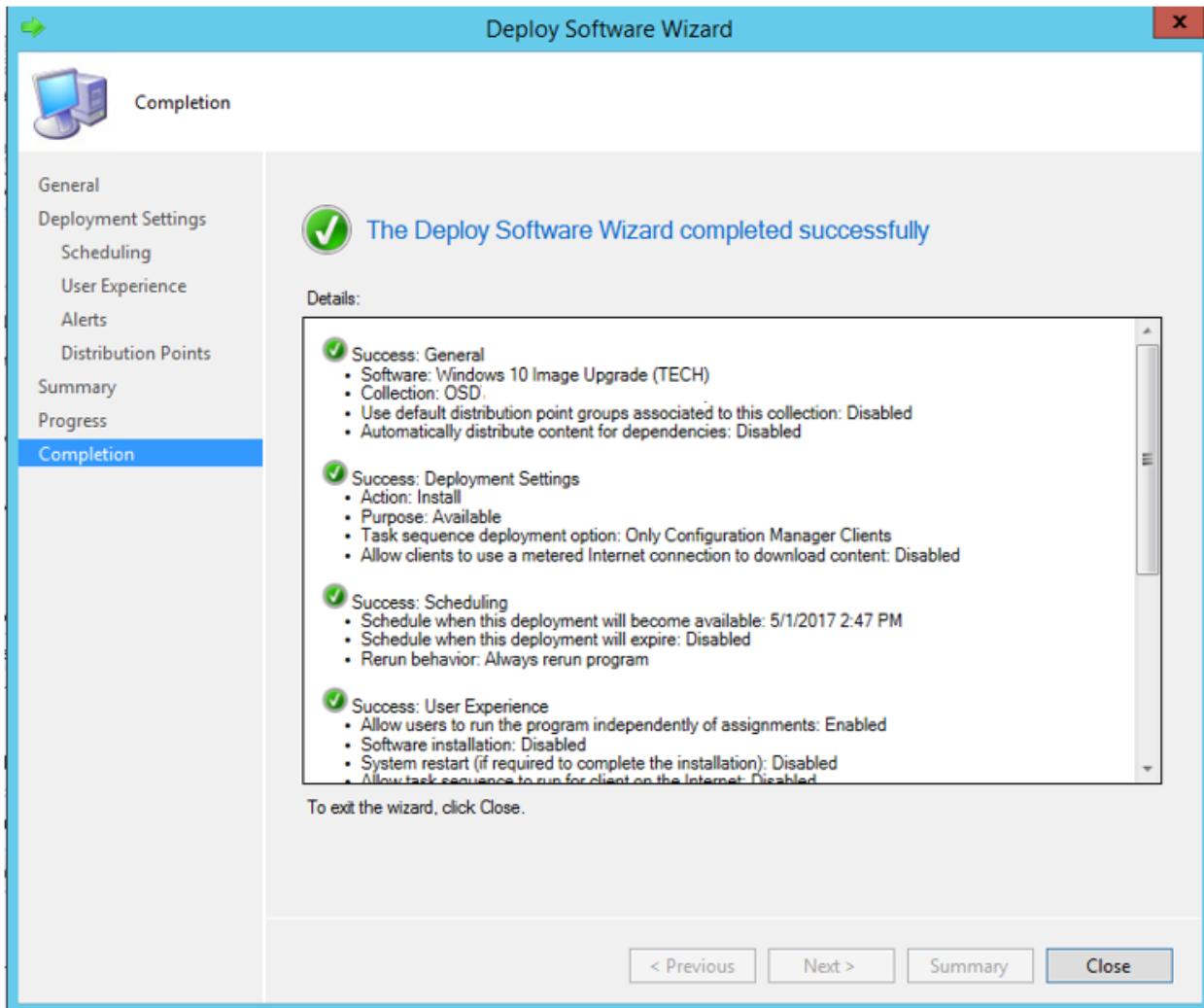
Click **Next**.



Click **Next**.

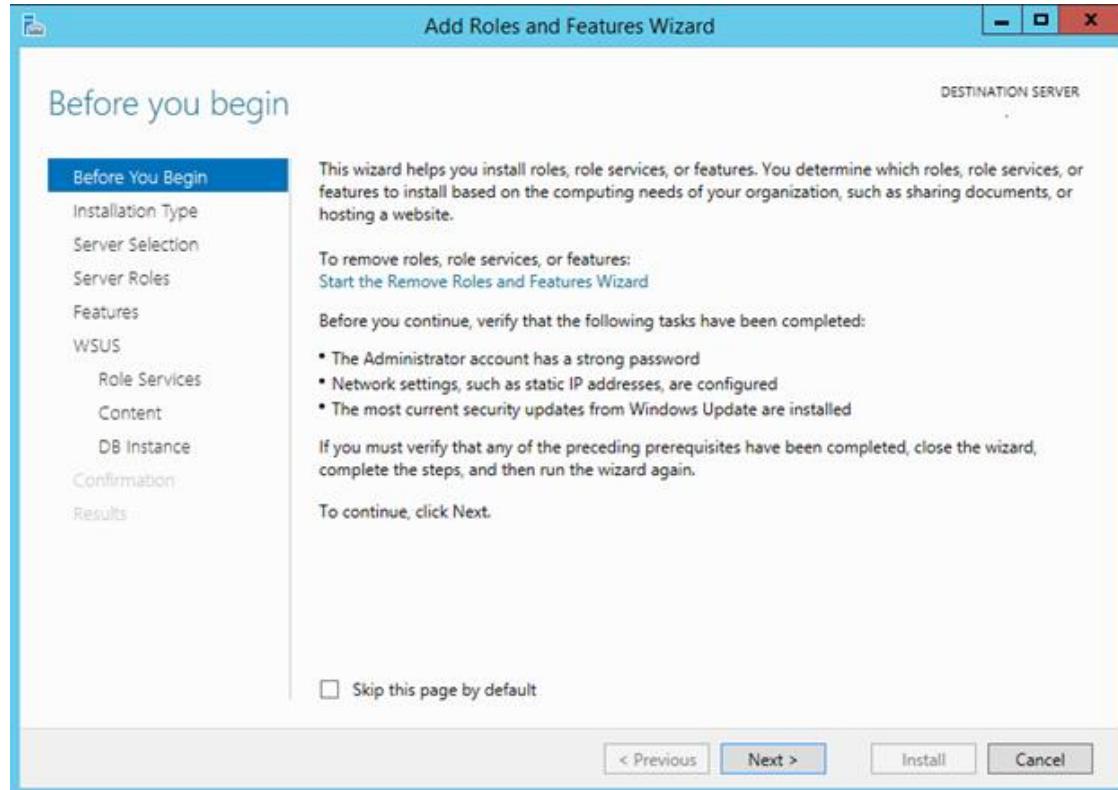


Click **Close**.

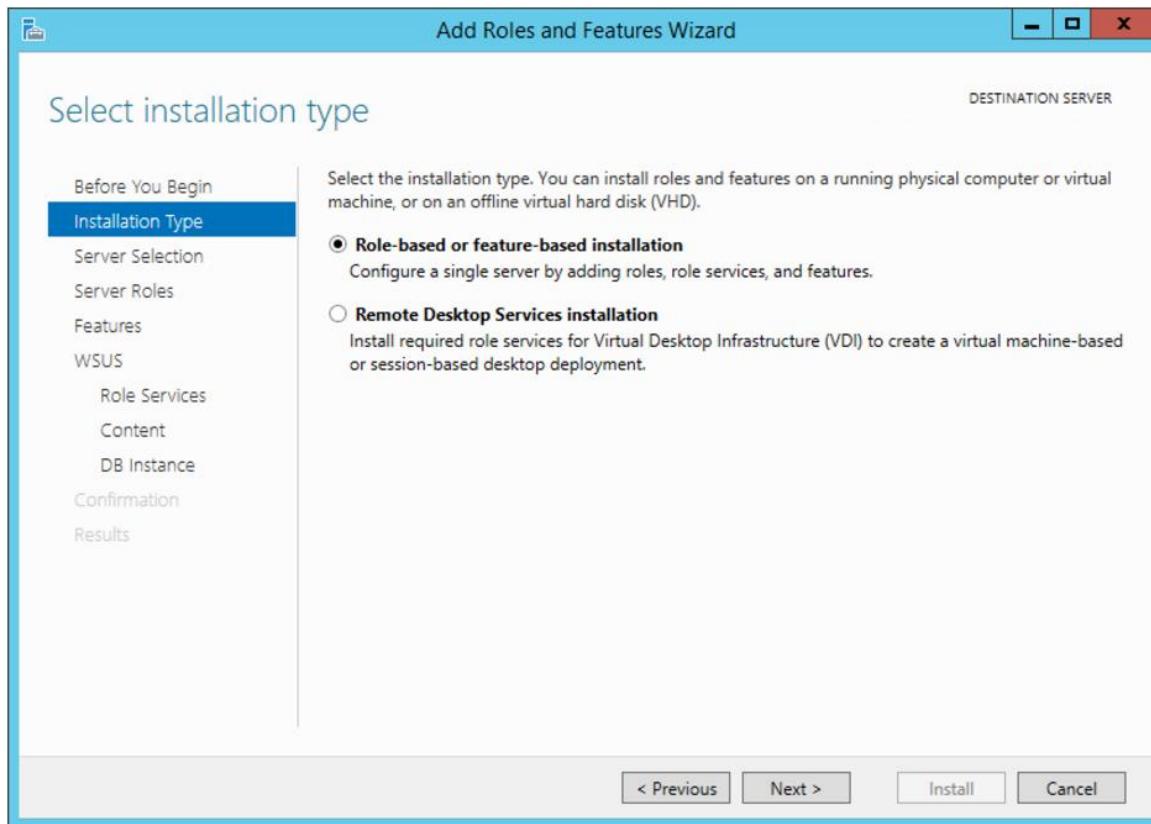


WSUS Setup

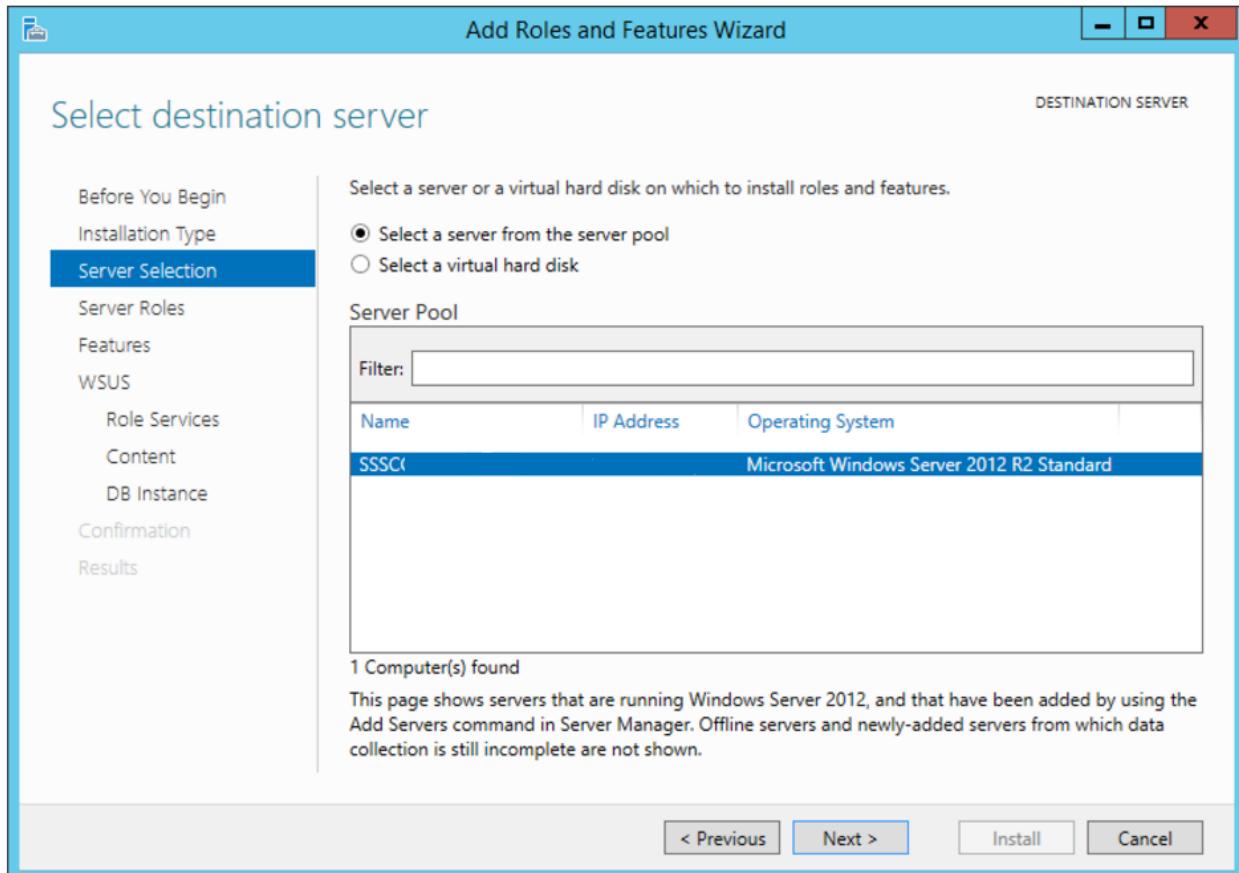
To begin WSUS setup, launch the **Add Roles and Features Wizard**. Click **Next**.



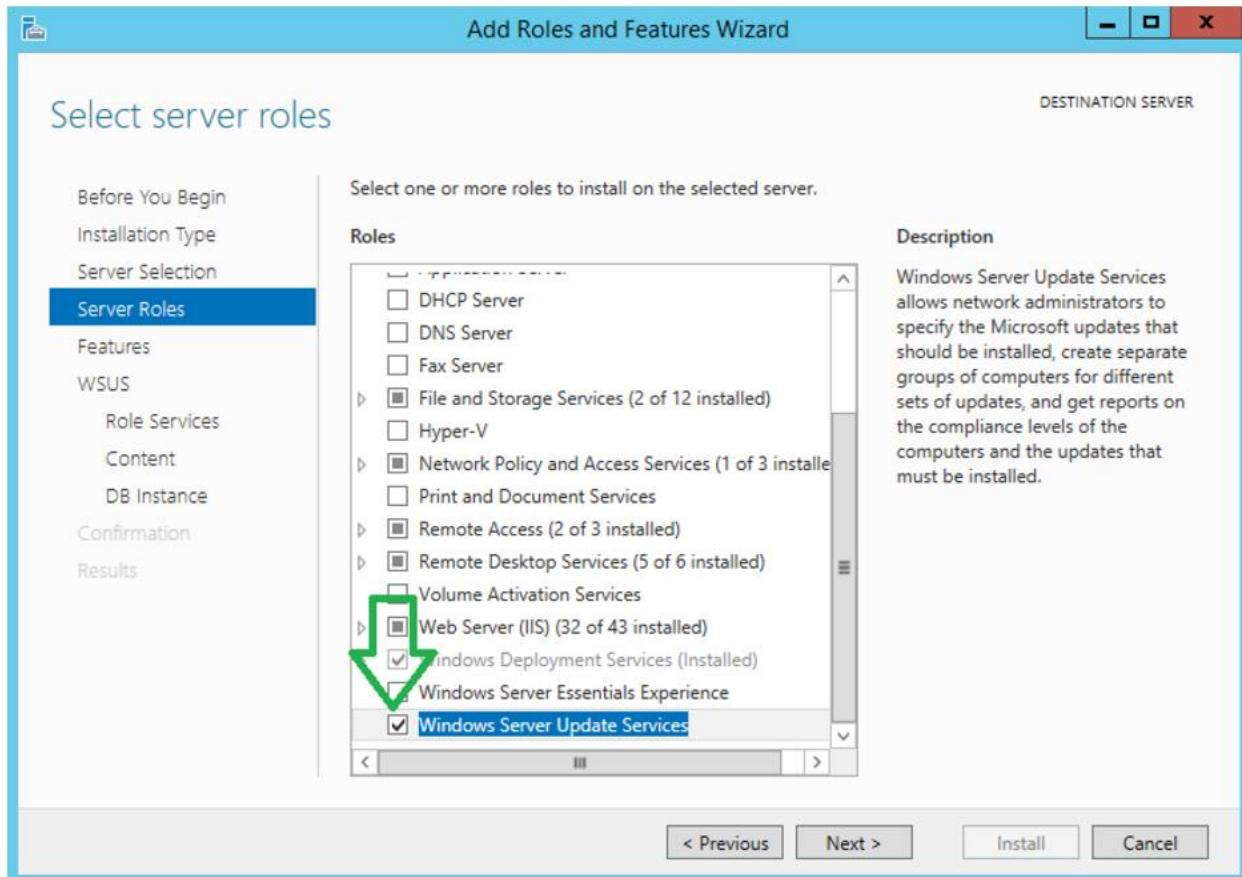
Click **Next**.



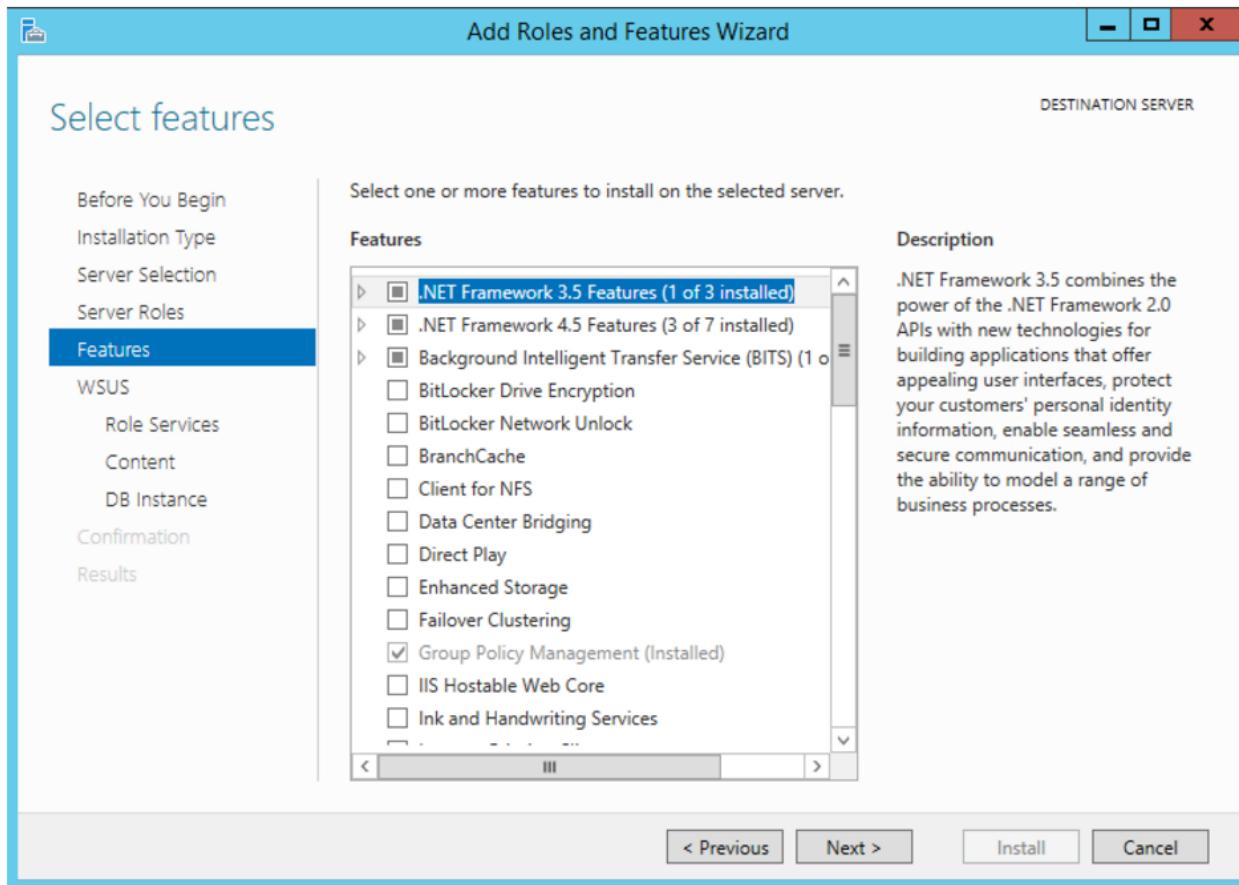
Click **Next**.



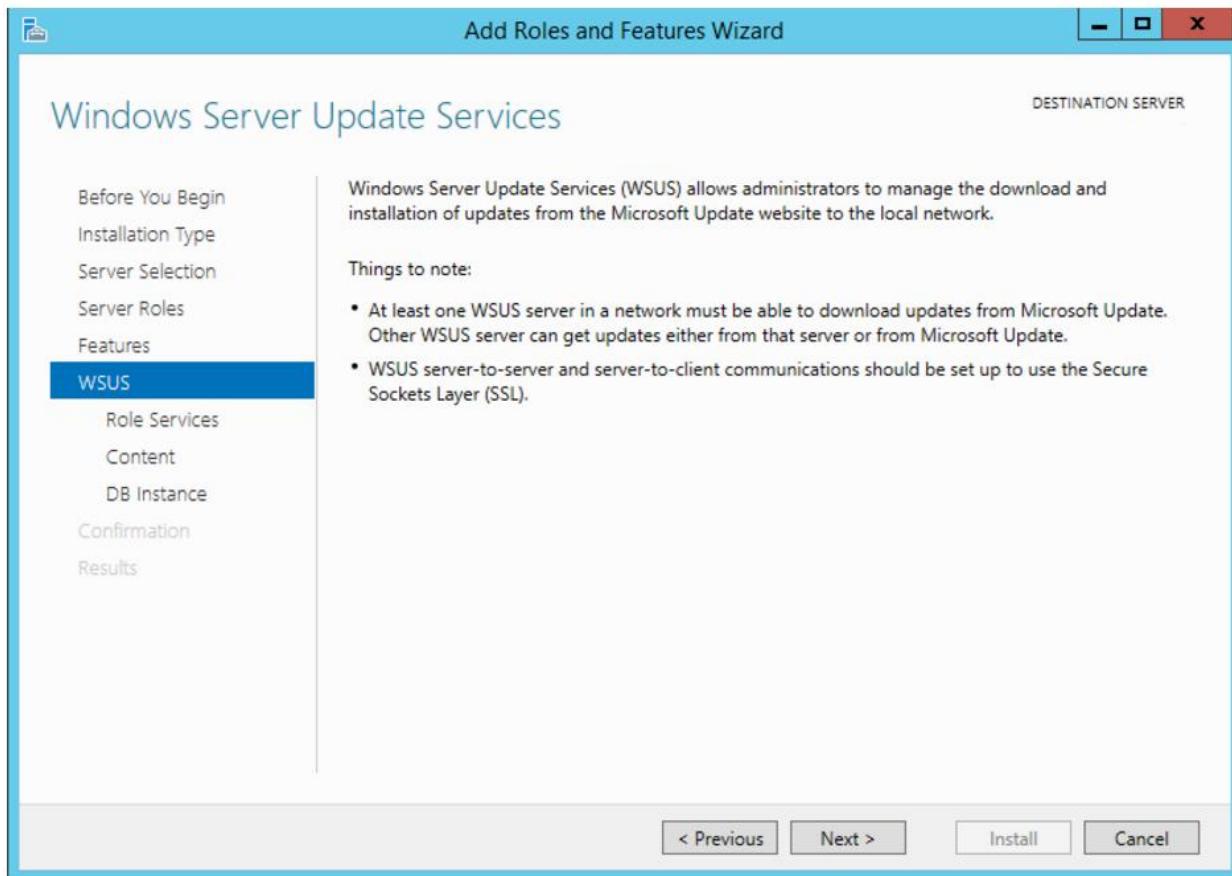
Check **Windows Server Update Services**, and click **Next** to continue.



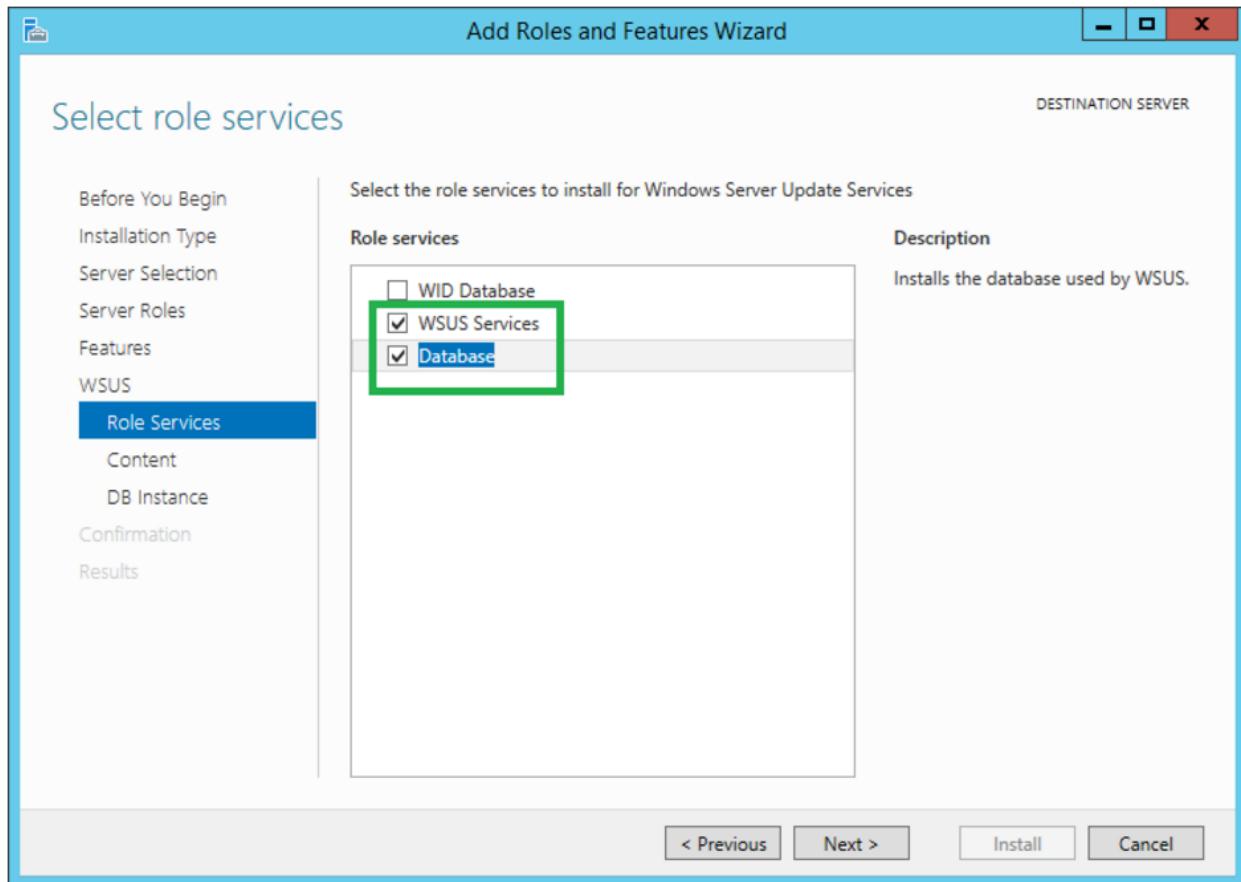
Click **Next**.



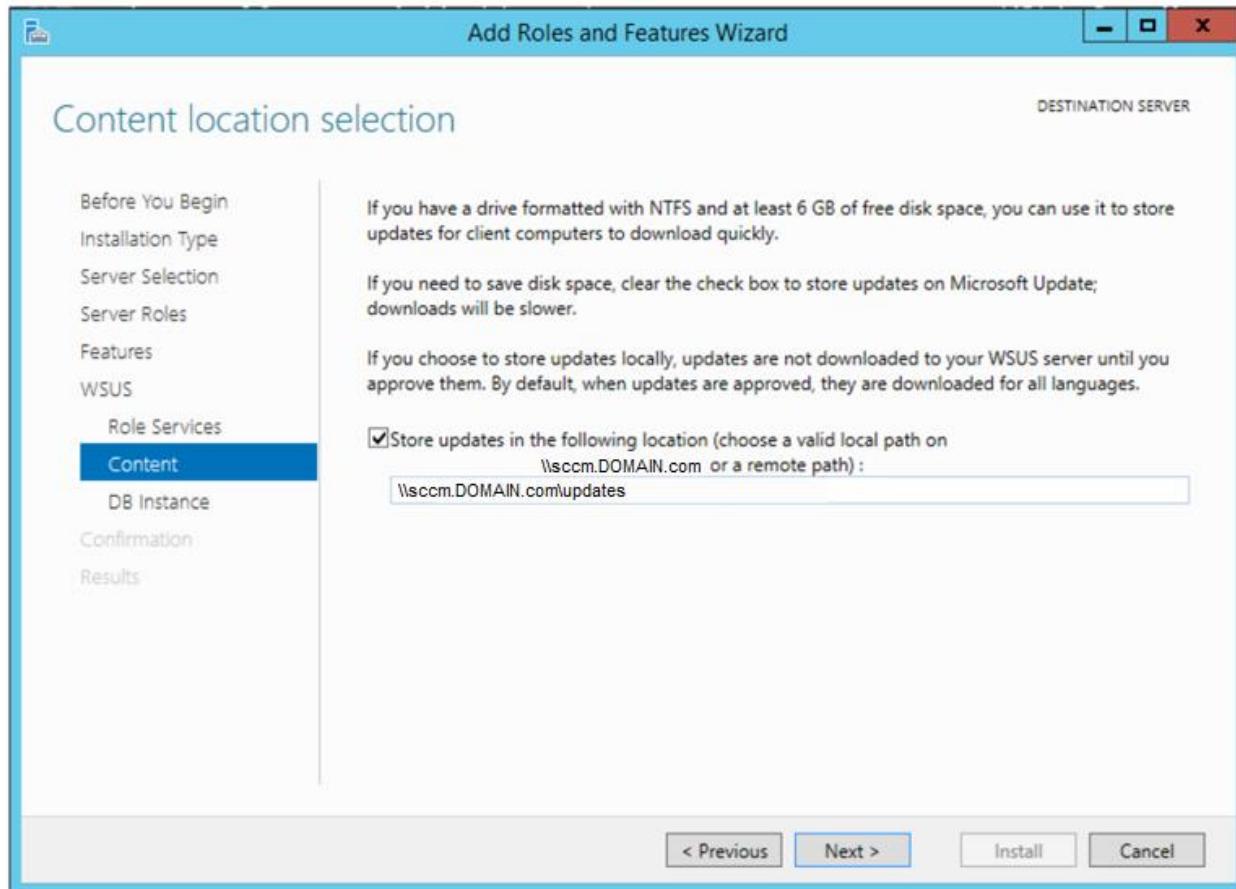
Click **Next**.



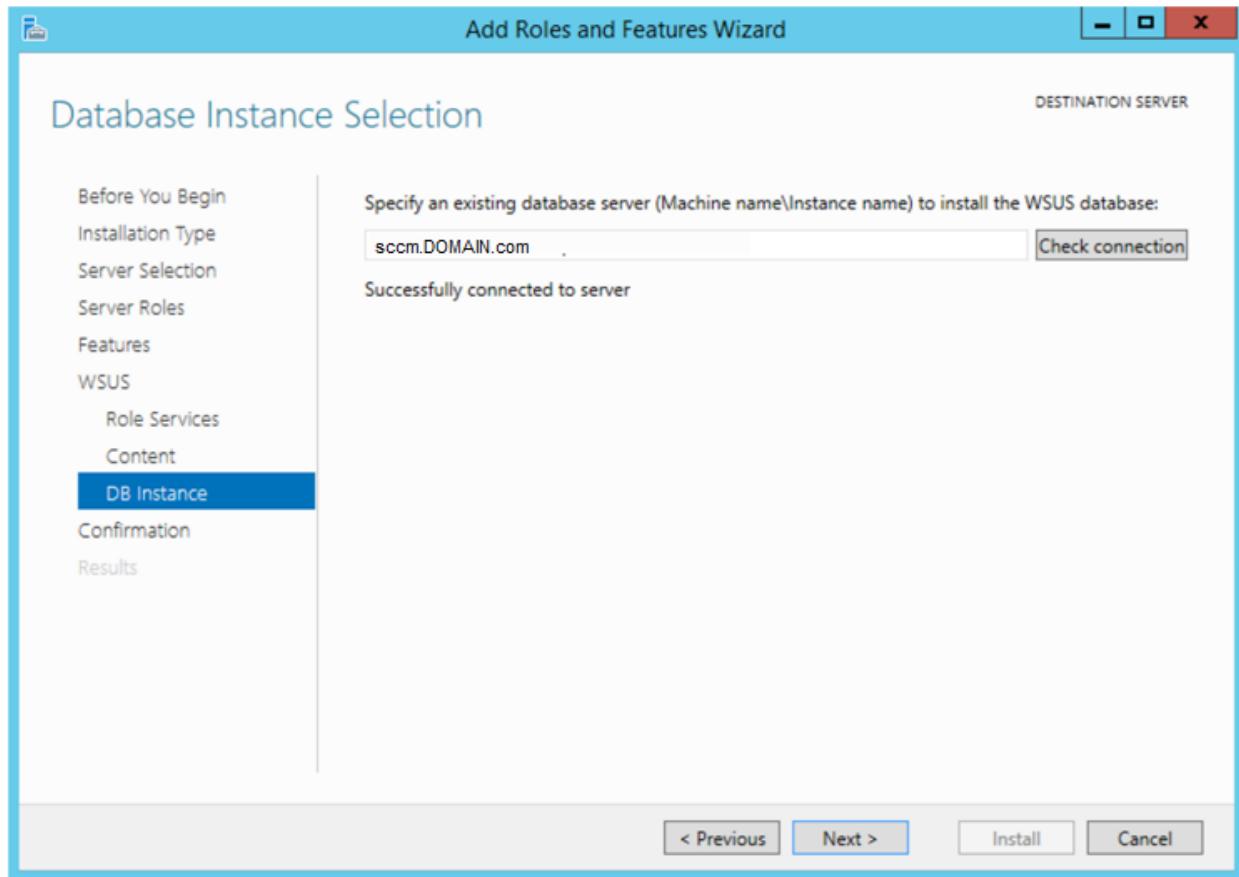
Select **WSUS Services and Database**, and click **Next** to continue.



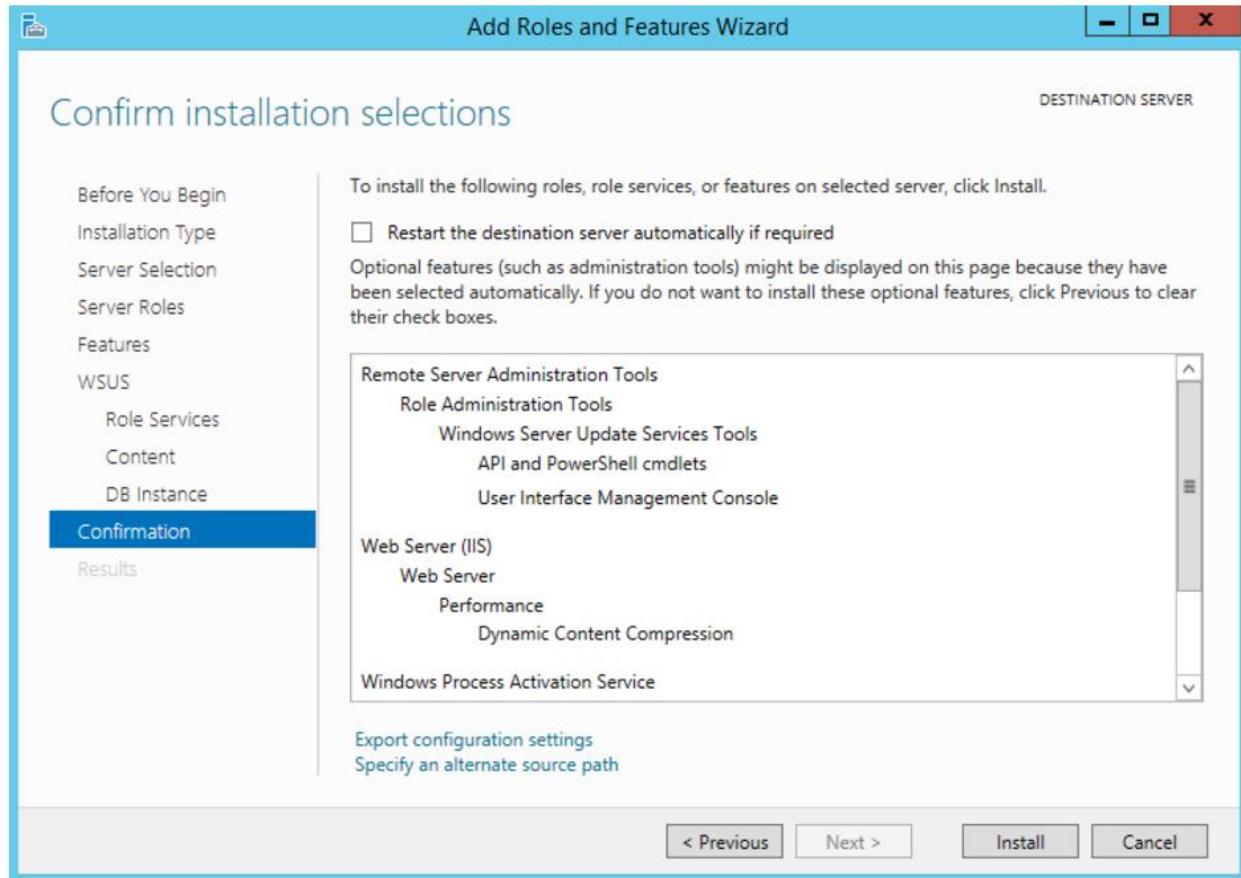
Enter the local or UNC path where the Windows Updates will download to, and click **Next** to continue.



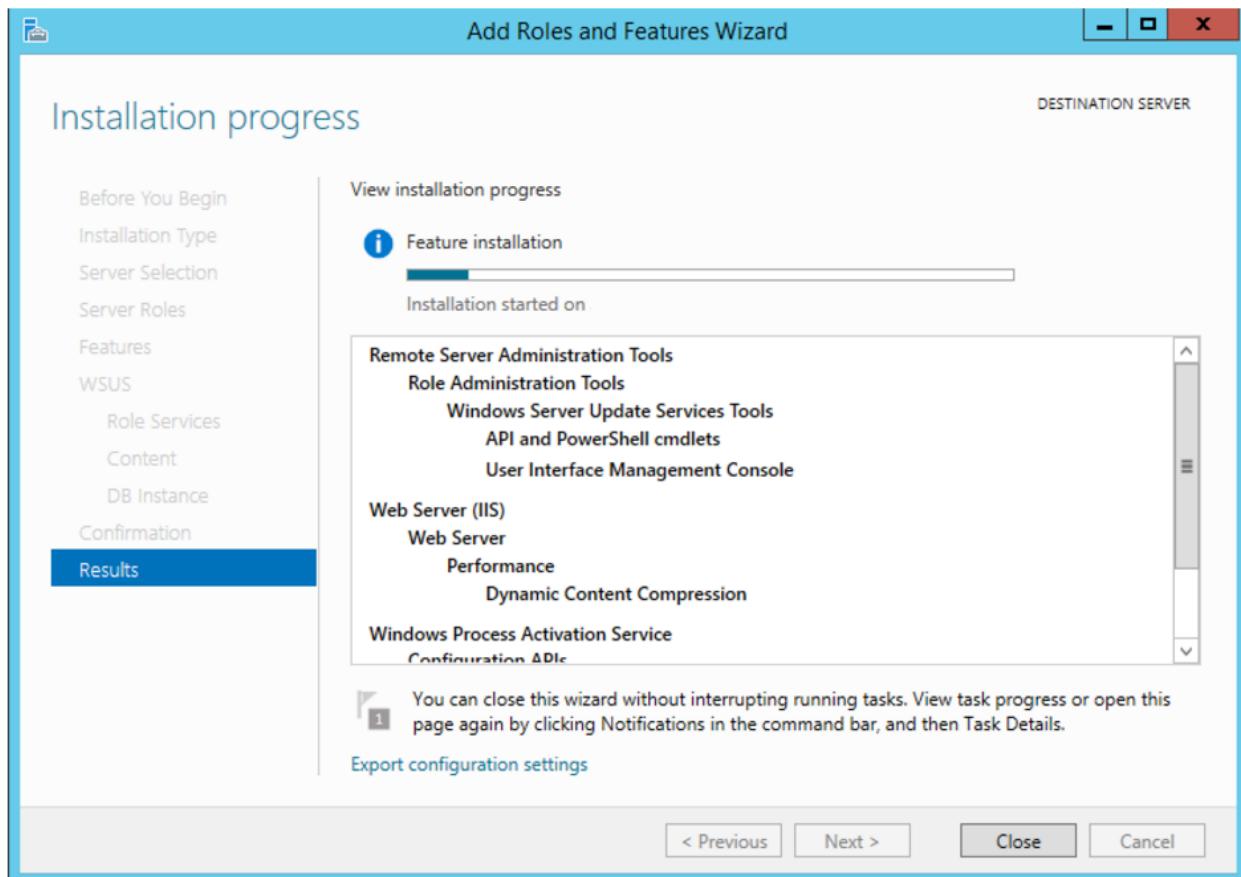
Enter path to the **database**, and click the **Check connection**. Click **Next**.



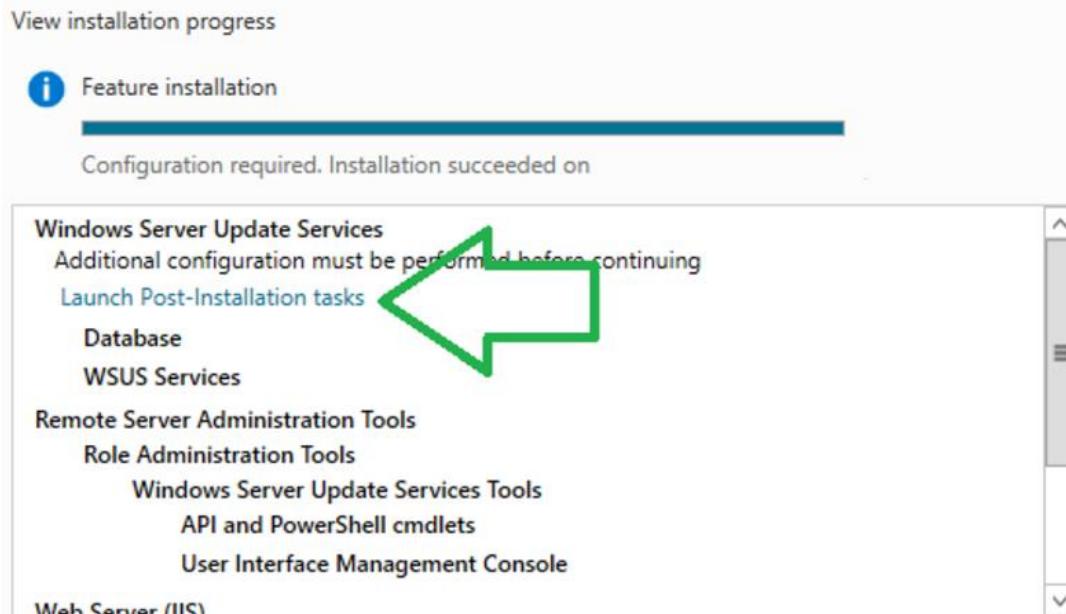
Click **Install** to start WSUS installation.



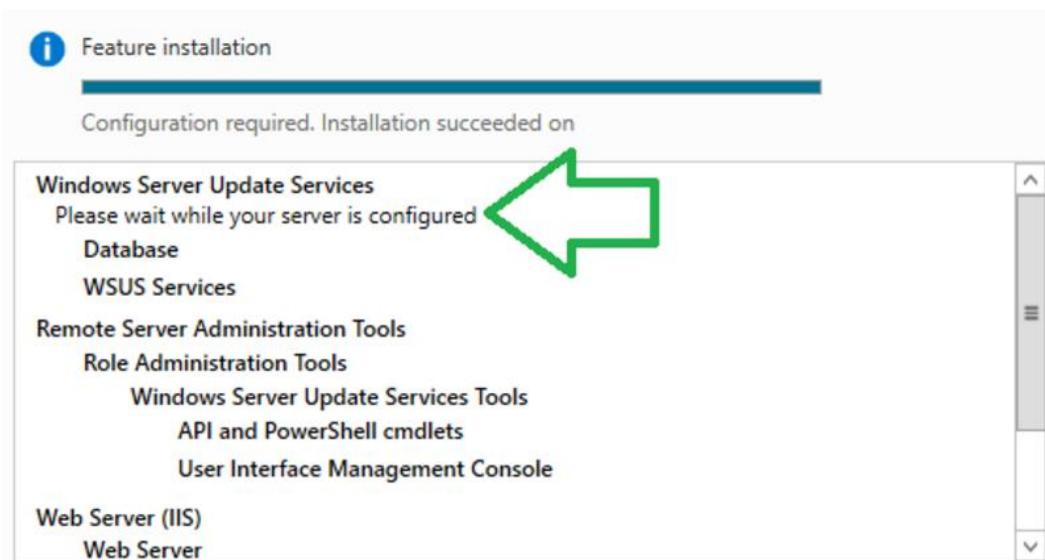
WSUS will install.



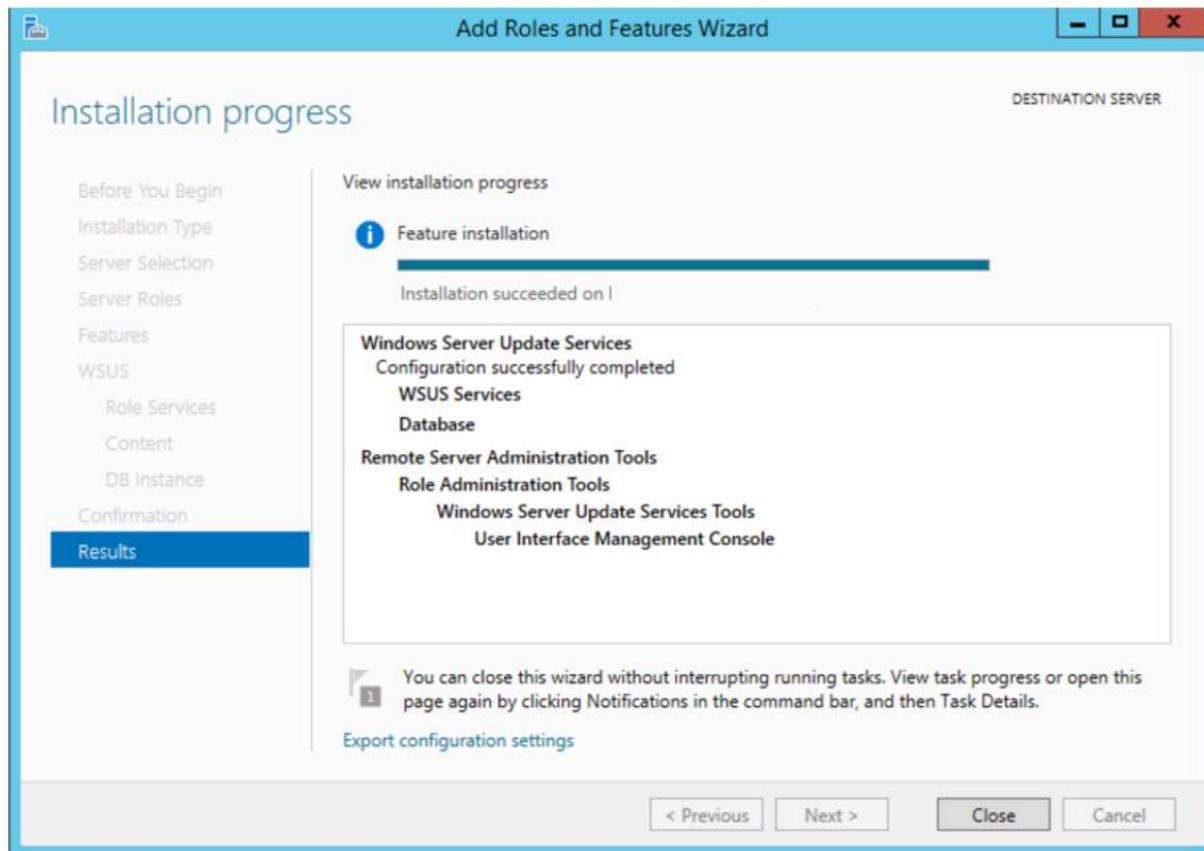
Click Launch Post-Installation tasks.



WSUS will continue installation



Click **Close**.



In SCCM, add a system role.

The screenshot shows the SCCM Administration interface. On the left, the navigation pane is open with the following structure:

- Administration
- Overview
- Updates and Servicing
- Hierarchy Configuration
- Cloud Services
- Site Configuration (highlighted with a red box labeled 1)
 - Sites
 - Servers and Site System Roles (highlighted with a red box labeled 2)
 - Client Settings
 - Security
 - Distribution Points
 - Distribution Point Groups
 - Migration

The main pane displays a table titled "Servers and Site System Roles 2 items". The table has columns: Icon, Name, Site Code, Count of roles, and Type. There are two entries:

Icon	Name	Site Code	Count of roles	Type
2	\sccm.DOMAIN.com		3	

A context menu is open over the first entry, showing the following options:

- Add Site System Roles (highlighted with a red box labeled 3)
- Start
- Refresh
- Delete (disabled)
- Properties

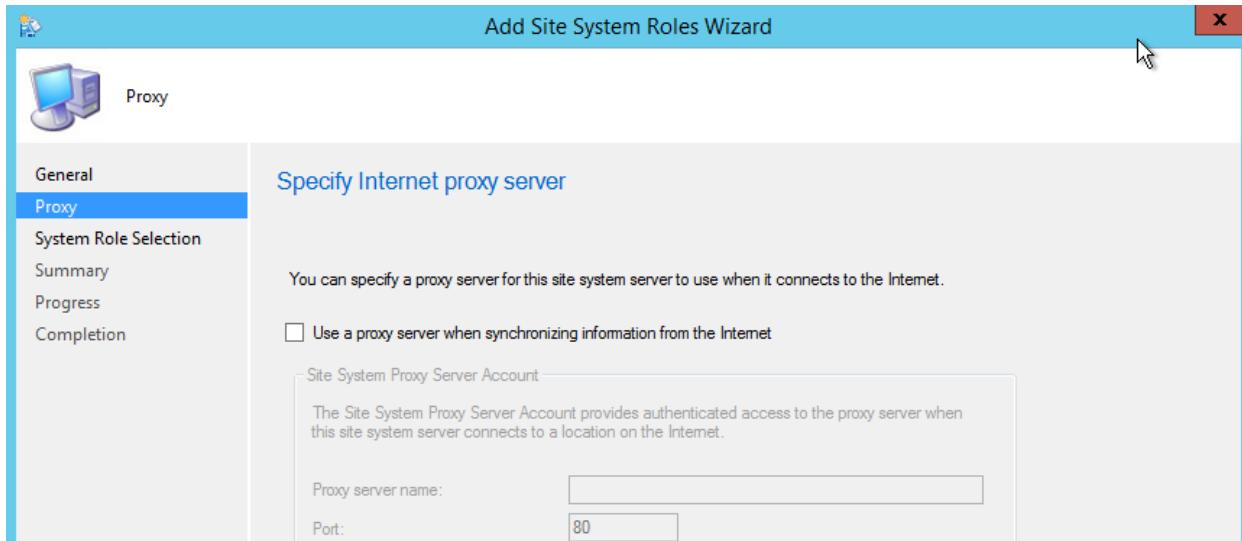
Click Next.

The screenshot shows the "Add Site System Roles Wizard" dialog box. The title bar says "Add Site System Roles Wizard". The left sidebar shows the steps: General (highlighted with a red box), Proxy, System Role Selection, Summary, Progress, and Completion.

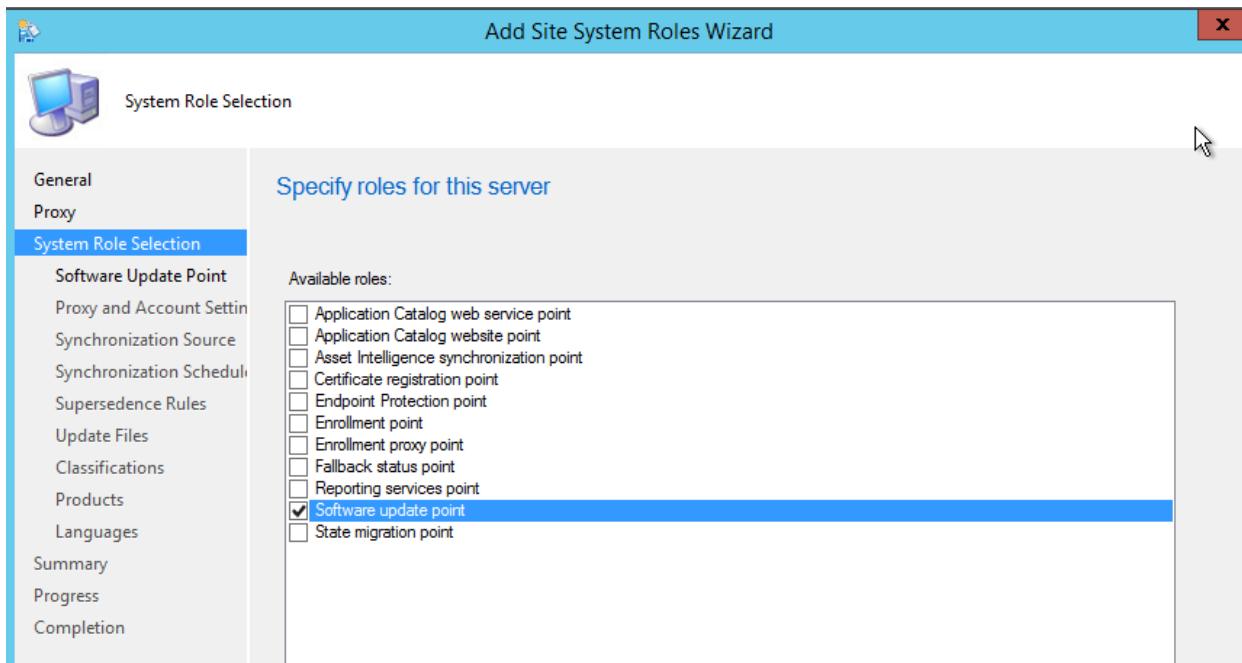
The main area is titled "Select a server to use as a site system". It contains the following fields:

- Name (example: server1.corp.contoso.com):
- Site code:
- Specify an FQDN for this site system for use on the Internet
Internet FQDN (example: intemetsrv2.contoso.com):
- Require the site server to initiate connections to this site system
After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.
- Site System Installation Account
 - Use the site server's computer account to install this site system
 - Use another account for installing this site system
- Active Directory membership:
- Active Directory forest:
- Active Directory domain:

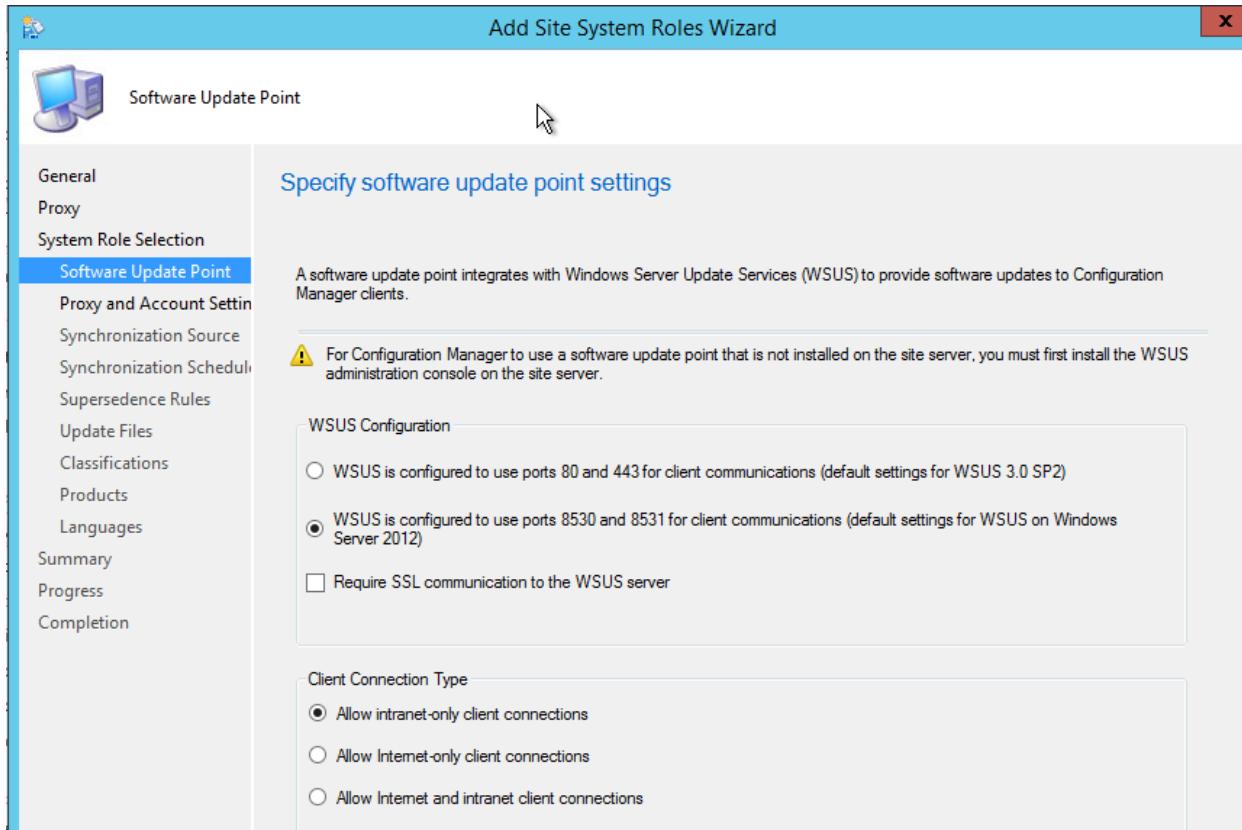
Click **Next**.



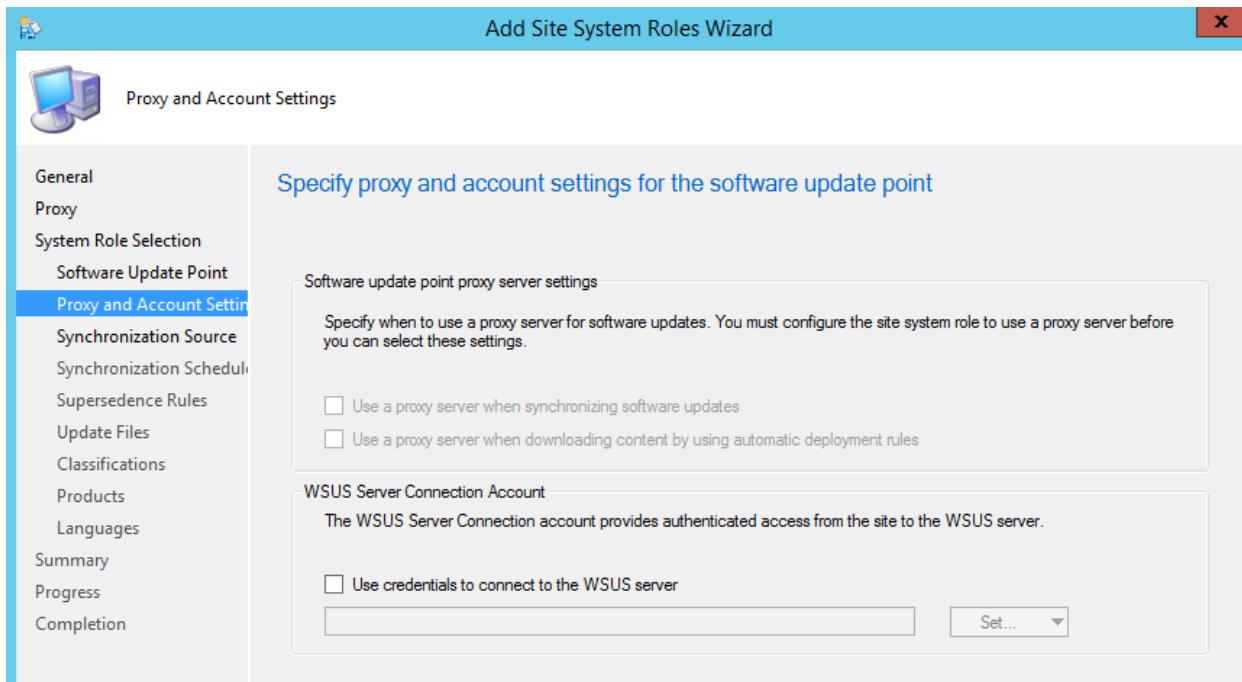
Check **Software update point** and click **Next** to continue.



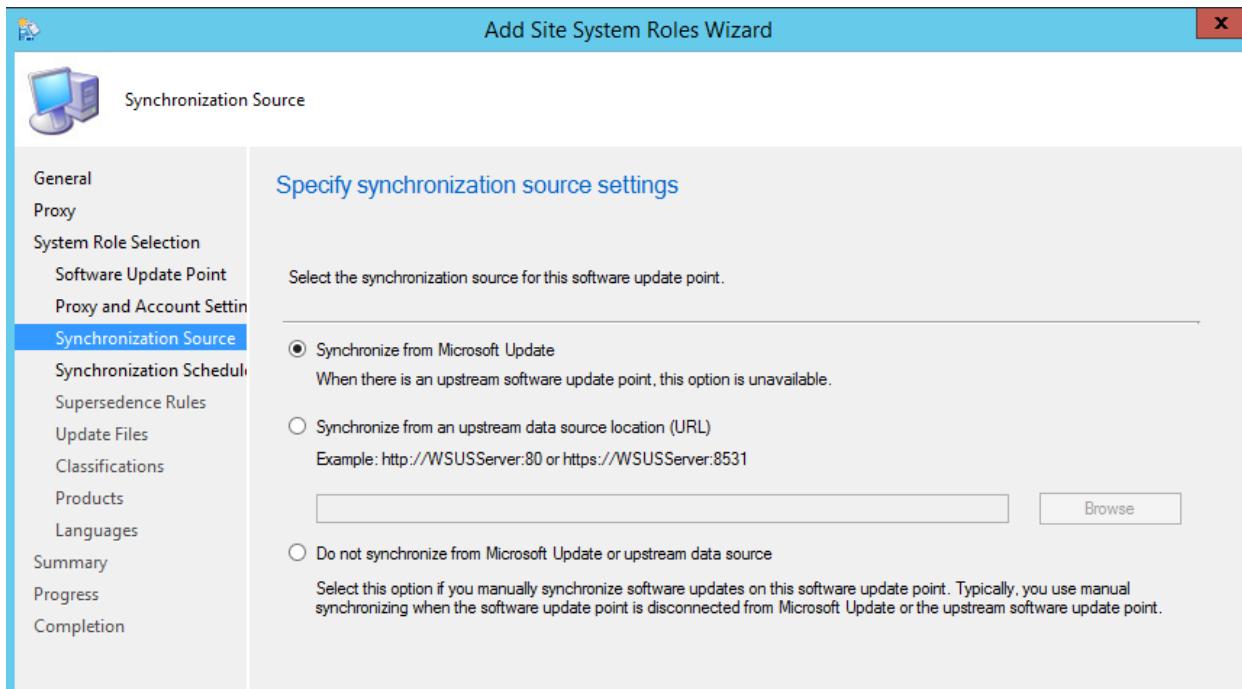
Select the **WSUS 8530 and 8531** option.



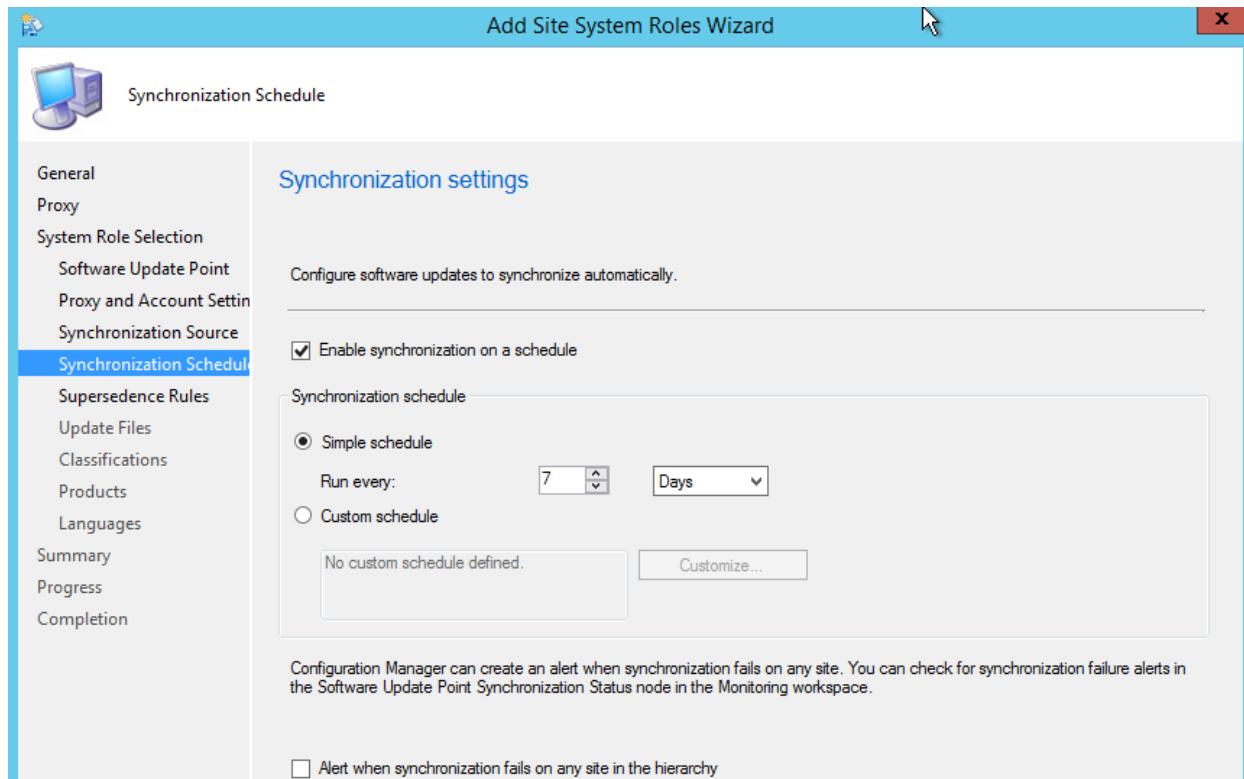
Click **Next**.



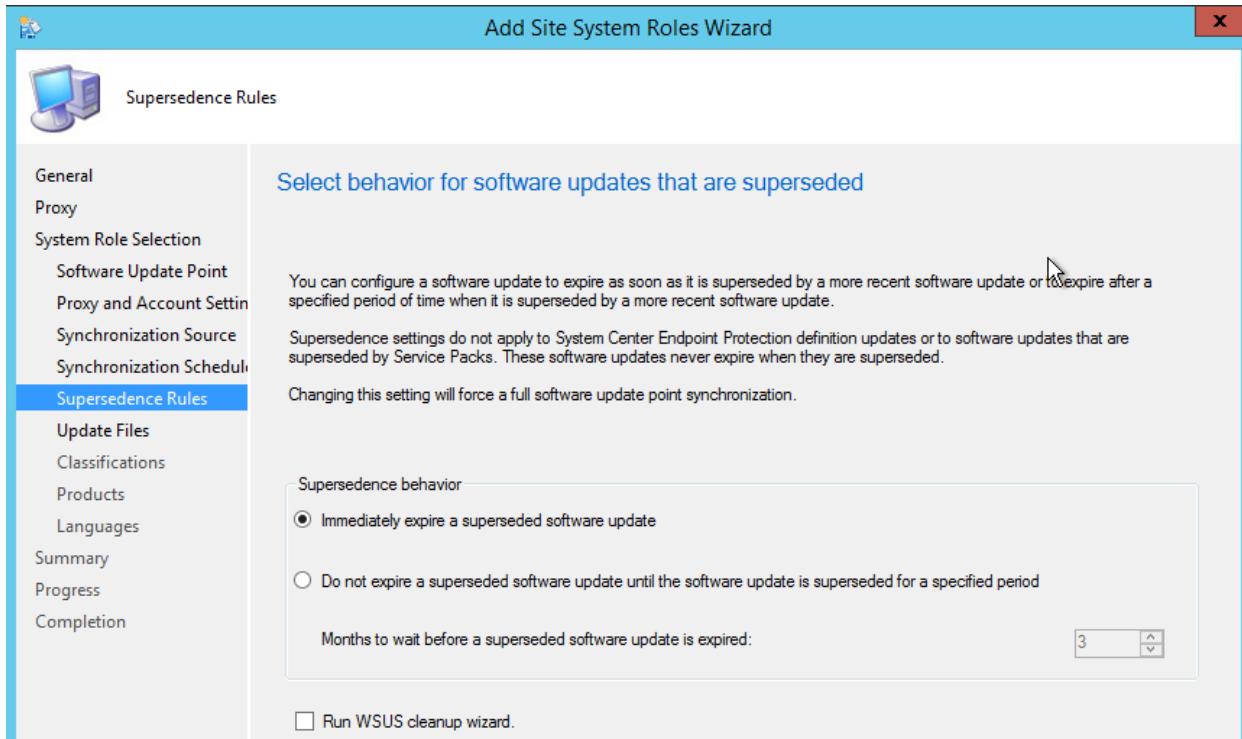
Click **Next**.



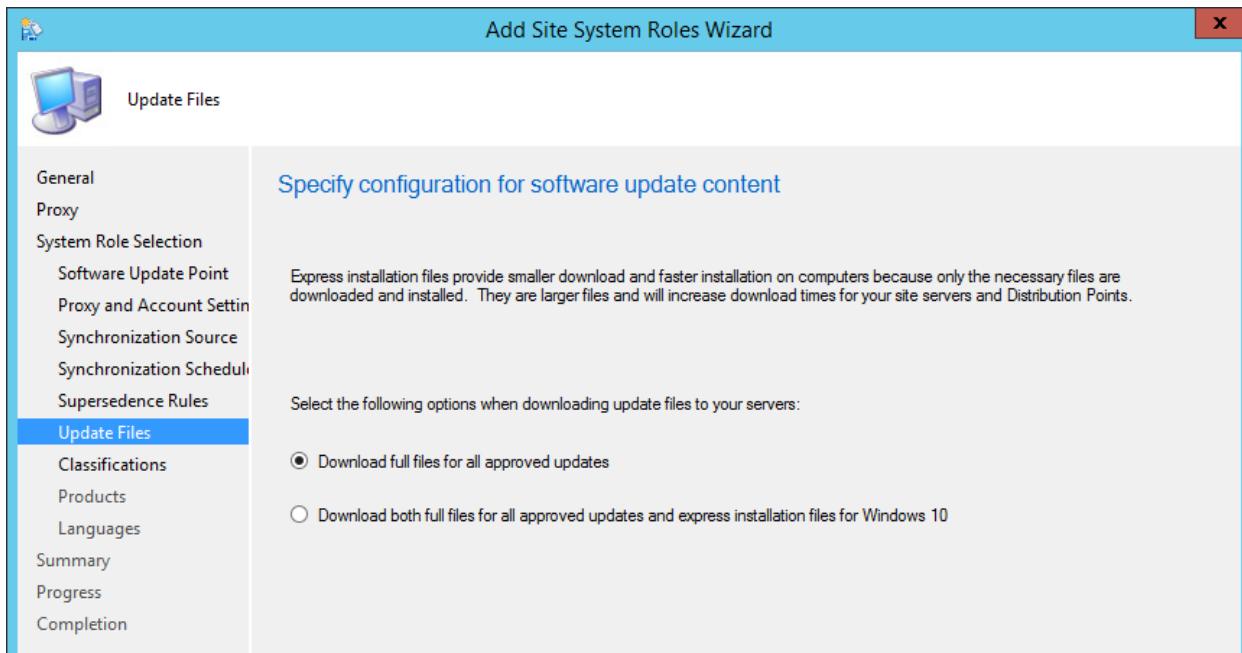
Click **Next**.



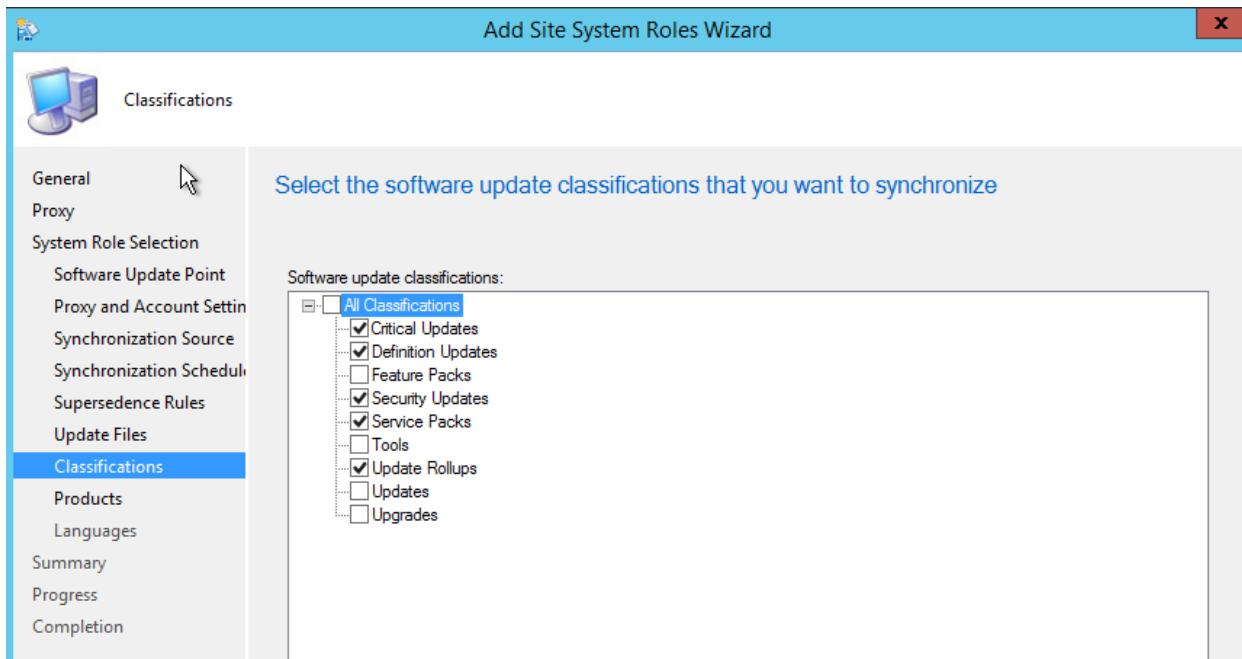
Click **Next**.



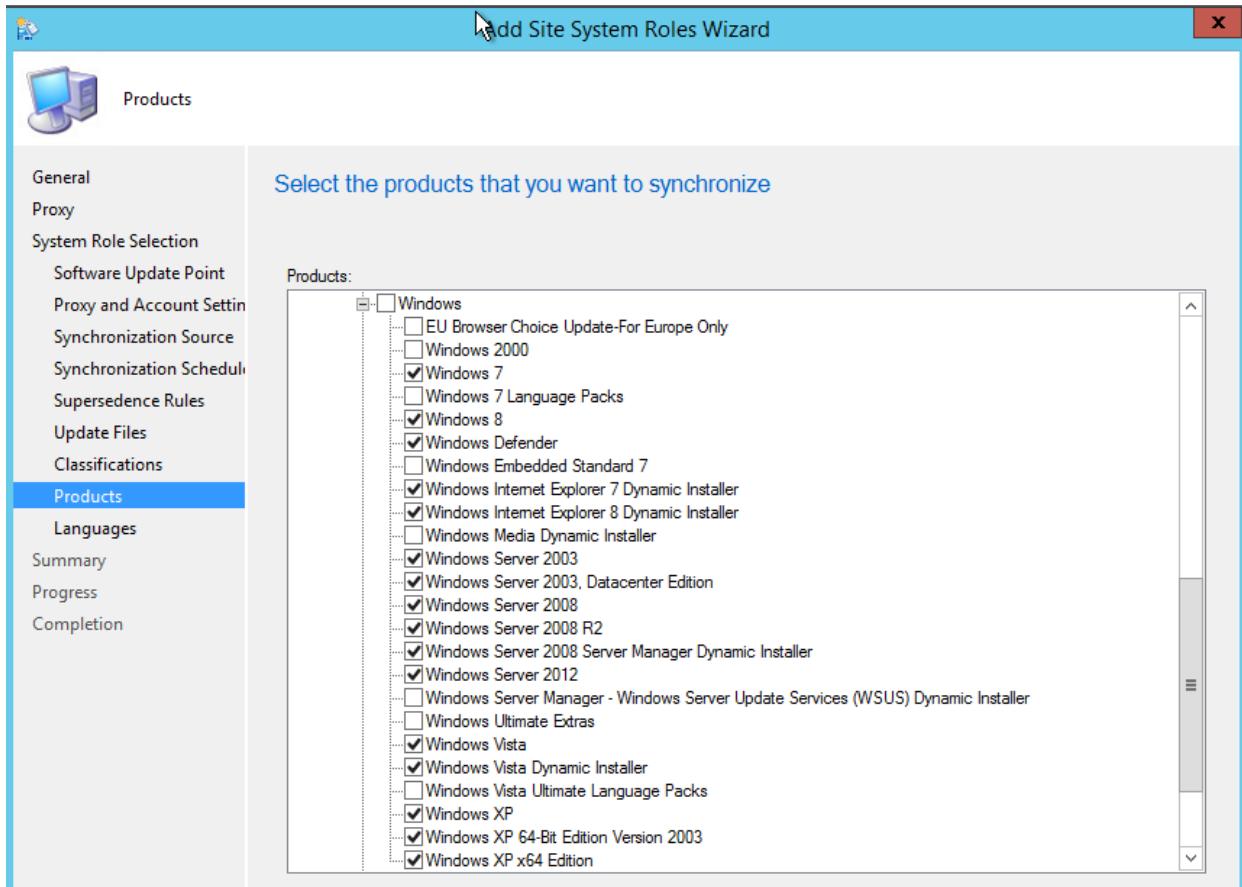
Select **Next**.



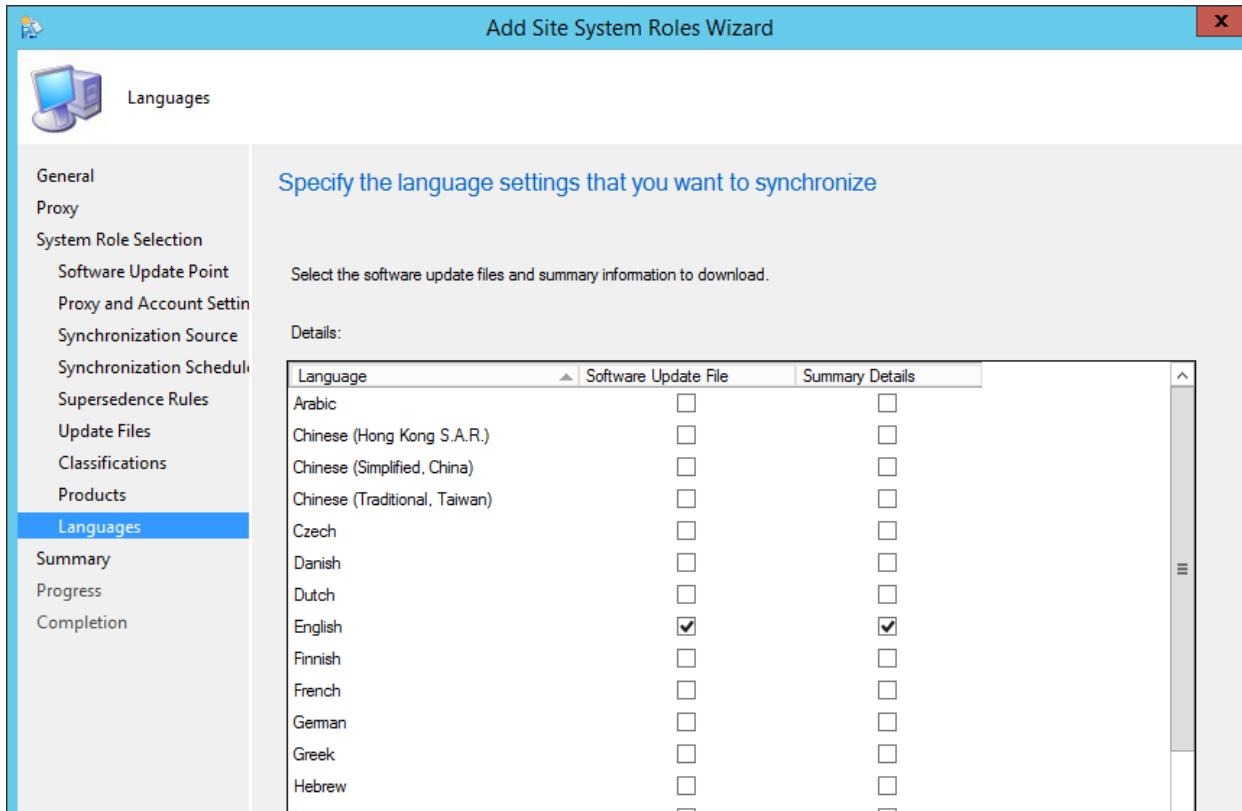
Select **Next**.



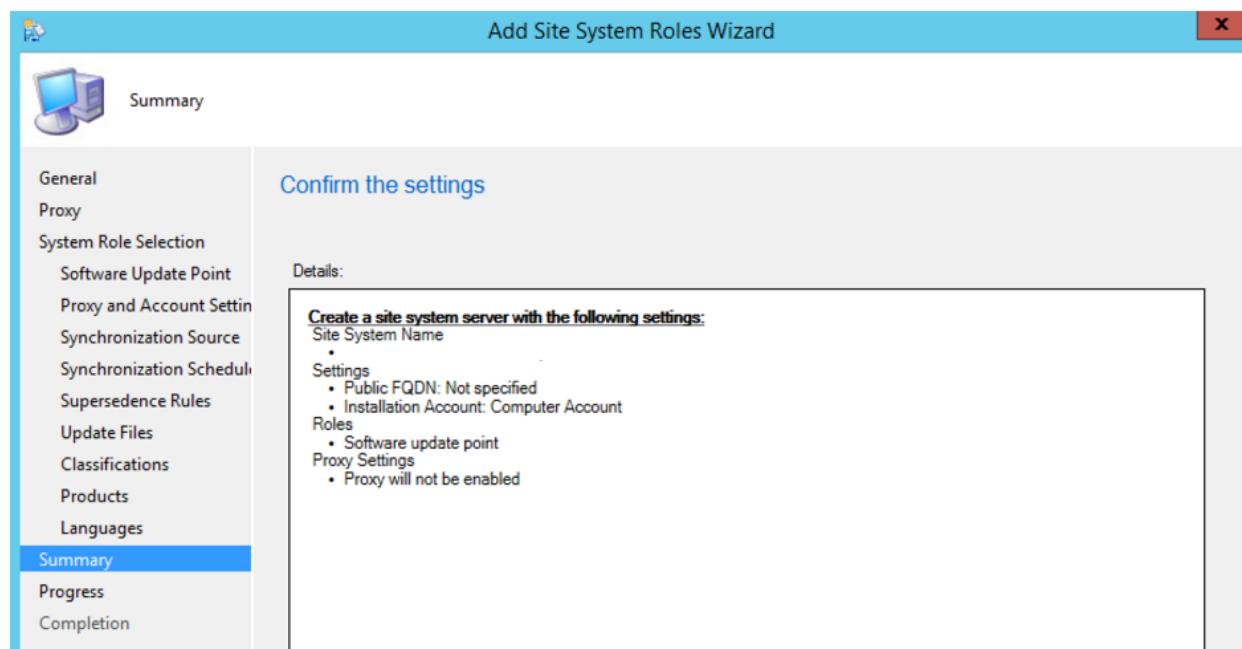
Click **Next**.



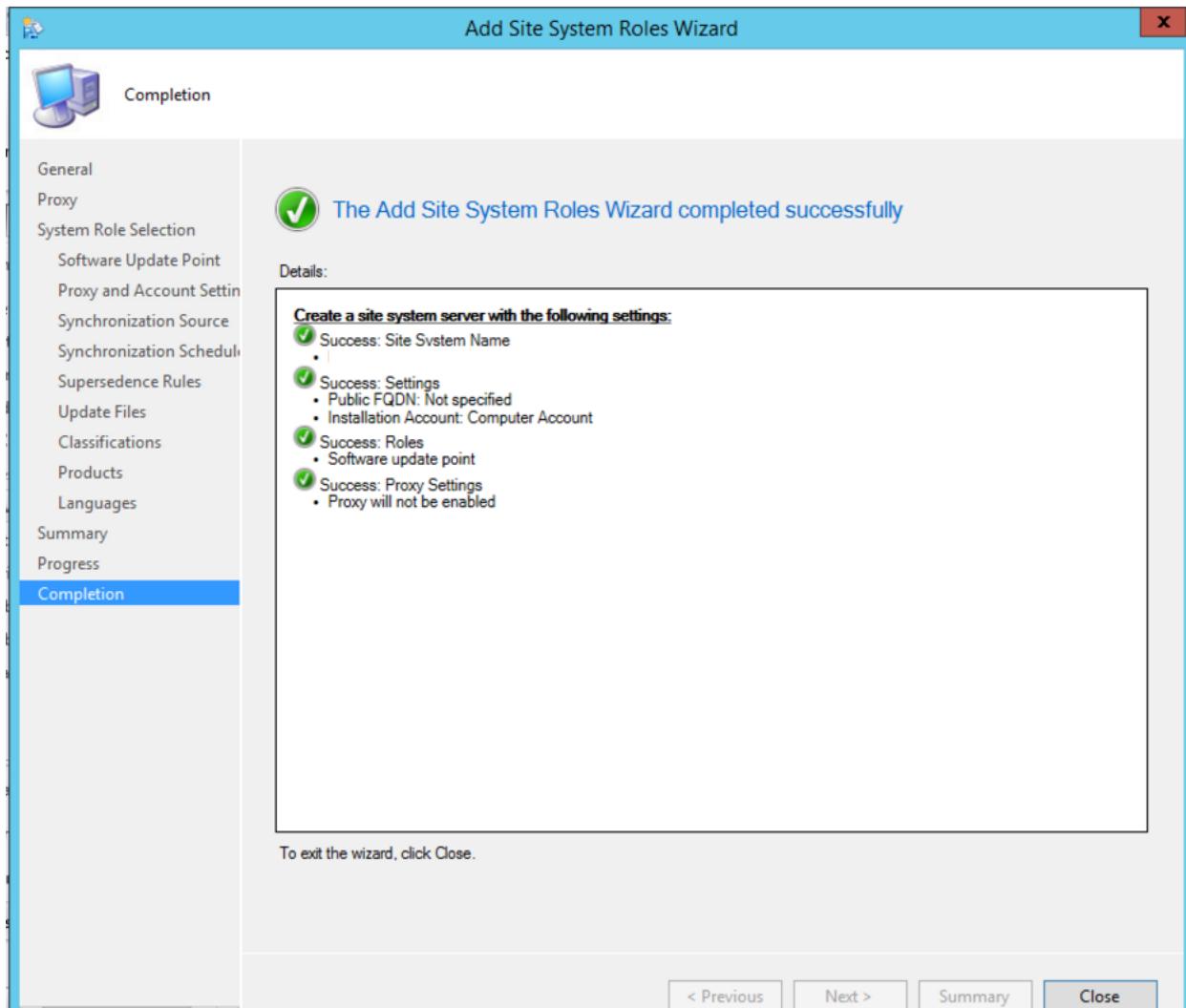
Select **English** and then click **Next**.



Click **Next**.



Click **Close**.



Windows Update Logs on D:

The screenshot shows a Windows File Explorer window titled "Logs". The address bar indicates the path: "Program Files > Microsoft Configuration Manager > Logs". The left sidebar includes "Favorites" (Desktop, Downloads, Recent places) and "This PC". The main area displays a table of log files:

Name	Date modified	Type	Size
CMUpdate	4/28/2017 7:25 PM	LOG File	277 KB
policypv	4/28/2017 7:25 PM	LOG File	1,047 KB
wsyncmgr	4/28/2017 7:28 PM	LOG File	118 KB
bgbmgr	4/28/2017 7:28 PM	LOG File	858 KB
CloudMgr	4/28/2017 7:28 PM	LOG File	38 KB
rcmctrl	4/28/2017 7:28 PM	LOG File	1,394 KB
compsumm	4/28/2017 7:25 PM	LOG File	1,637 KB
EPMgr	4/28/2017 7:28 PM	LOG File	2,149 KB
statmgr	4/28/2017 7:28 PM	LOG File	1,595 KB
cloudusersync	4/28/2017 7:28 PM	LOG File	814 KB
smsdbmon	4/28/2017 7:25 PM	LOG File	2,254 KB
WCM	4/28/2017 7:25 PM	LOG File	450 KB
smsexec	4/28/2017 7:25 PM	LOG File	1,568 KB

Wsyncmgr.log

```
sync: WSUS synchronizing updates
sync: WSUS synchronizing updates, processed 346 out of 49279 items (0%), ETA in 02:21:25
sync: WSUS synchronizing updates, processed 778 out of 49279 items (1%), ETA in 02:05:43
sync: WSUS synchronizing updates, processed 1369 out of 49279 items (2%), ETA in 01:45:34
sync: WSUS synchronizing updates, processed 2169 out of 49279 items (4%), ETA in 01:27:36
sync: WSUS synchronizing updates, processed 2925 out of 49279 items (5%), ETA in 01:20:01
sync: WSUS synchronizing updates, processed 3867 out of 49279 items (7%), ETA in 01:11:02
sync: WSUS synchronizing updates, processed 4457 out of 49279 items (9%), ETA in 01:11:03
sync: WSUS synchronizing updates, processed 5298 out of 49279 items (10%), ETA in 01:07:06
```

WCM.log

Log Text	Date/Time	Thread
Attempting connection to WSUS server: SCCM.DOMAIN.com, port: 8530, useSSL: False	SI 5/12/2017 9:23:22 AM	1048 (0x418)
Successfully connected to server: SCCM.DOMAIN.com, port: 8530, useSSL: False	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:041e4f9f-3a3d-4f58-8b2f-5e6fe95c4591 (Office 2007) not found on WSUS	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:26997d30-08ce-4f25-b2de-699c36a8033a (Windows Vista) not found on WSUS	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:2ee2ad83-828c-4405-9479-544d767993fc (Windows 8) not found on WSUS	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:4cb6ebd5-e38a-4826-9f76-1416a6f563b0 (Windows XP x64 Edition) not found...	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:5312e4f1-6372-442d-aeb2-15f2132c9bd7 (Windows Internet Explorer 8 Dyna...	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:84ff5f325-30d7-41c4-81d1-87a0e6535b66 (Office 2010) not found on WSUS	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:8c3fcc84-7410-4a95-8b89-a166a0190486 (Windows Defender) not found on ...	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:90e135fb-ef48-4ad0-afb5-10c4ceb4ed16 (Windows Vista Dynamic Installer) n...	SI 5/12/2017 9:23:23 AM	1048 (0x418)
Category Product:a105a108-7c9b-4518-bbbe-73f0fe30012b (Windows Server 2012) not found o...	SI 5/12/2017 9:23:23 AM	1048 (0x418)

Server Side Software Update Logs:

SUPSetup.log – Installation of SUP Site Role.

WCM.log, WSUSCtrl.log – Configuration of WSUS Server/SUP.

WSyncMgr.log – SMS/WSUS Updates Synchronization Issues.

Objreplmgr.log – Policy Issues for Update Assignments/CI Version Info policies.

RuleEngine.log – Auto Deployment Rules.

Client Side Software Update Logs:

UpdatesDeployment.log – Deployments, SDK, UX.

UpdatesHandler.log – Updates, Download.

ScanAgent.log – Online/Offline scans, WSUS location requests.

WUAHandler.log – Update status, WU interaction.

UpdatesStore.log – Update status (missing/installed).

%windir%/WindowsUpdate.log – Scanning/Installation of updates.

Note, it will take a couple of hours to completely sync Windows Updates, perhaps longer depending on your setup.

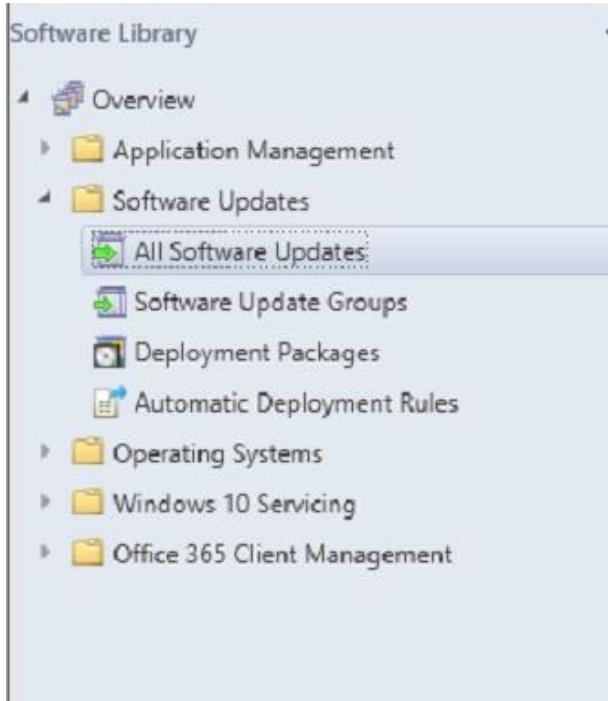
The screenshot shows the 'Software Library' interface with the path 'Software Library > Overview > Software Updates > All Software Updates'. The left sidebar has a tree view with 'Overview', 'Application Management', 'Software Updates' (selected), 'Software Update Groups', 'Deployment Packages', 'Automatic Deployment Rules', 'Operating Systems', 'Windows 10 Servicing', and 'Office 365 Client Management'. The main area displays a table titled 'All Software Updates 1929 items' with columns: Icon, Title, Bulletin ID, Required, Installed, and Percent Compliant. The table lists several updates, including various Microsoft Office Service Packs and Security Rollups for .NET Framework and Windows 7. A tooltip at the bottom right of the table area reads 'April, 2017 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 (KB40149)'.

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant
[Icon]	2007 Microsoft Office Servers Service Pack 1 (SP1)	0	0	6	
[Icon]	2007 Microsoft Office Servers Service Pack 1 (SP1), 64-bit edi...	0	0	6	
[Icon]	2007 Microsoft Office Suite Service Pack 1 (SP1)	0	0	6	
[Icon]	April, 2017 Security and Quality Rollup for .NET Framework 3...	0	0	6	
[Icon]	April, 2017 Security and Quality Rollup for .NET Framework 3...	1	0	6	
[Icon]	April, 2017 Security and Quality Rollup for .NET Framework 3...	0	0	6	
[Icon]	April, 2017 Security Monthly Quality Rollup for .NET Framework 3...	0	2	13	
[Icon]	April, 2017 Security Monthly Quality Rollup for Windows 7 (...)	0	0	6	
[Icon]	April, 2017 Security Monthly Quality Rollup for Windows 7 f...	0	2	13	
[Icon]	April, 2017 Security Monthly Quality Rollup for Windows 8.1...	0	0	6	
[Icon]	April, 2017 Security Monthly Quality Rollup for Windows 8.1...	0	0	6	
[Icon]	April, 2017 Security Only Quality Update for Windows 7 (KB4...	0	0	6	

Side note, if you happen to have another primary SCCM server with the SUP role, it may conflict with your server. For me, I noticed a different primary SCCM server in the server logs. So, I had to strip out all the WSUS info, remove the CM Client from our server, block the other WSUS server (primary server) in the host file, and rebuild WSUS and reconfigure the SUP role. After that, I monitored the WSUS logs and saw my server syncing properly.

Deploy Updates

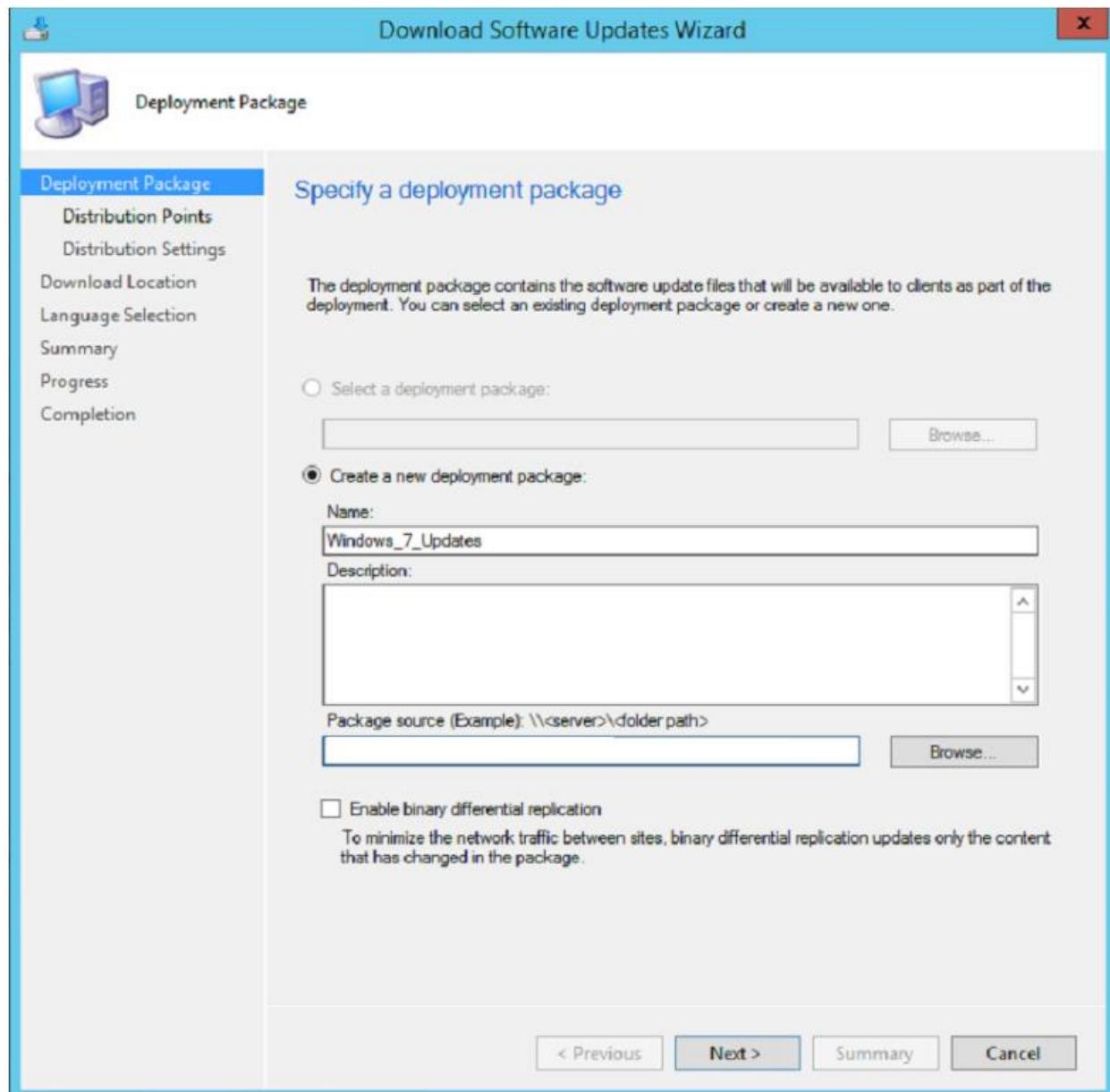
Click on the All Software Updates under Software Library > Overview.



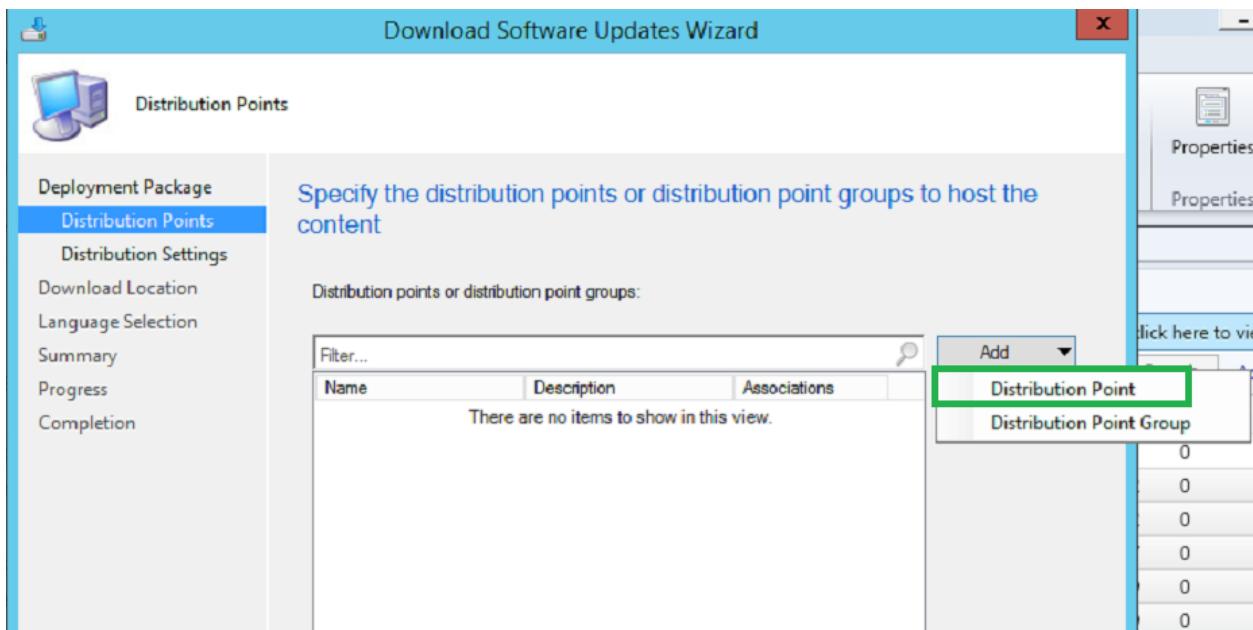
Select **updates** to be downloaded, right-click and choose **Download**.

Icon	Title	Bulletin ID	Required	Installed
	Windows Malicious Software Removal Tool x64 - March 2017 (KB890830)		0	0
	Security Update for Windows 7 for x64-based Systems (KB3108381)	MS15-132	0	2
	Security Update for Windows 7 for x64-based Systems (KB3108371)	MS15-132	0	2
	Security Update for Windows 7 for x64-based Systems (KB3101720)	MS15-117	0	2
	Security Update for Windows 7 for x64-based Systems (KB309352)		2	
	Security Update for Windows 7 for x64-based Systems (KB309262)		2	
	Security Update for Windows 7 for x64-based Systems (KB308622)		2	
	Security Update for Windows 7 for x64-based Systems (KB308412)		2	
	Security Update for Windows 7 for x64-based Systems (KB308042)		1	
	Security Update for Windows 7 for x64-based Systems (KB310862)		2	
	Security Update for Windows 7 for x64-based Systems (KB307862)		1	
	Security Update for Windows 7 for x64-based Systems (KB307522)		1	
	Security Update for Windows 7 for x64-based Systems (KB3075220)	MS15-082	0	1
	Security Update for Windows 7 for x64-based Systems (KB3071756)	MS15-085	0	2
	Security Update for Windows 7 for x64-based Systems (KB3060716)	MS15-090	0	2
	Security Update for Windows 7 for x64-based Systems (KB3046017)	MS15-088	0	2
	Security Update for Windows 7 for x64-based Systems (KB3042058)		0	1

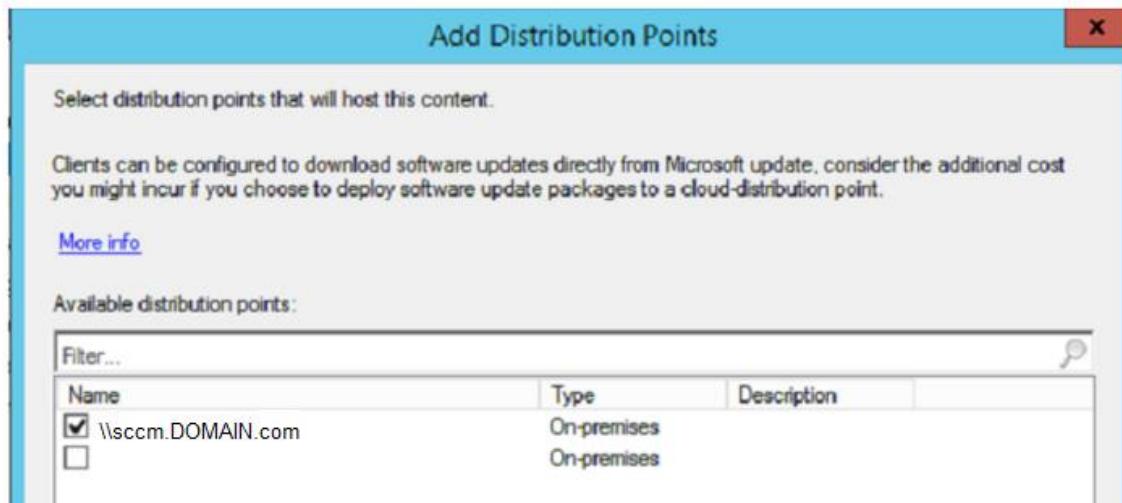
Click **Next**.



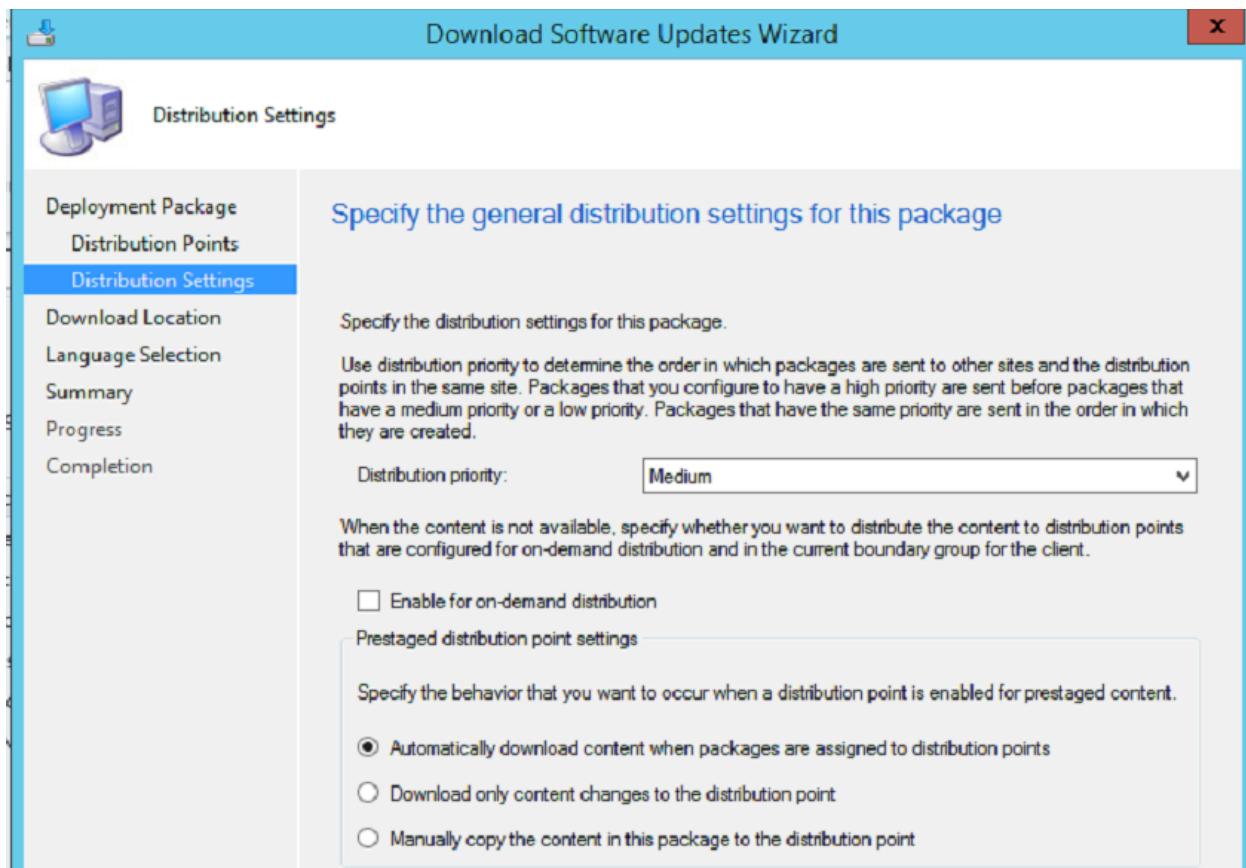
Select **Distribution Point** option.



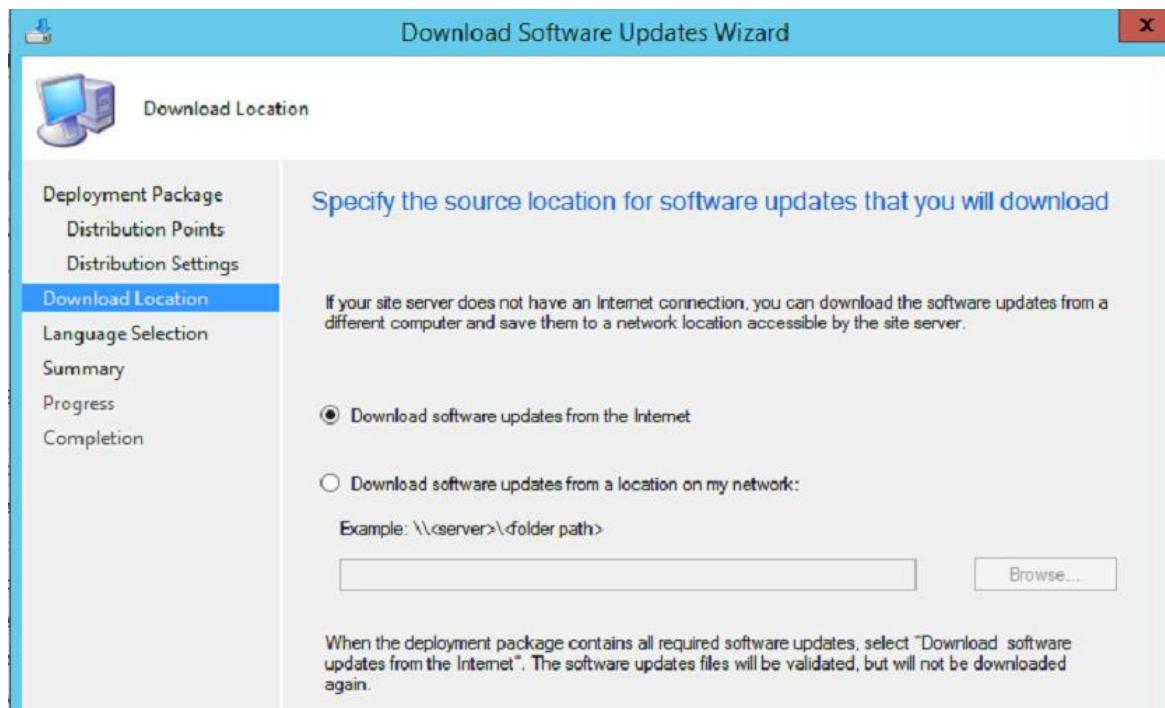
Check the appropriate distribution points. Click **OK** and **Next**.



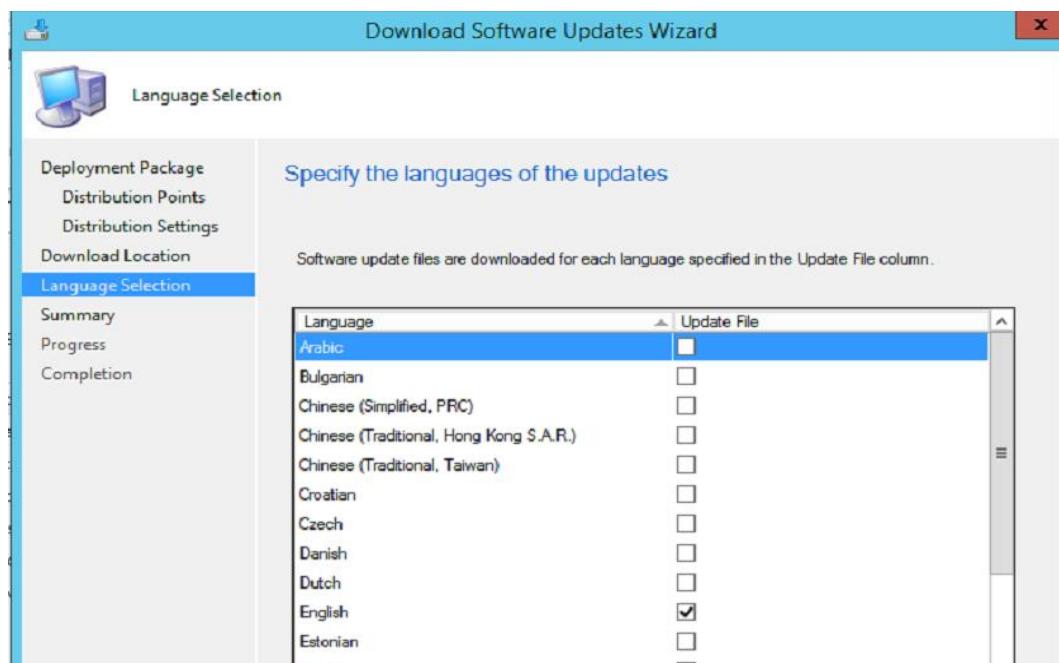
Click **Next**.



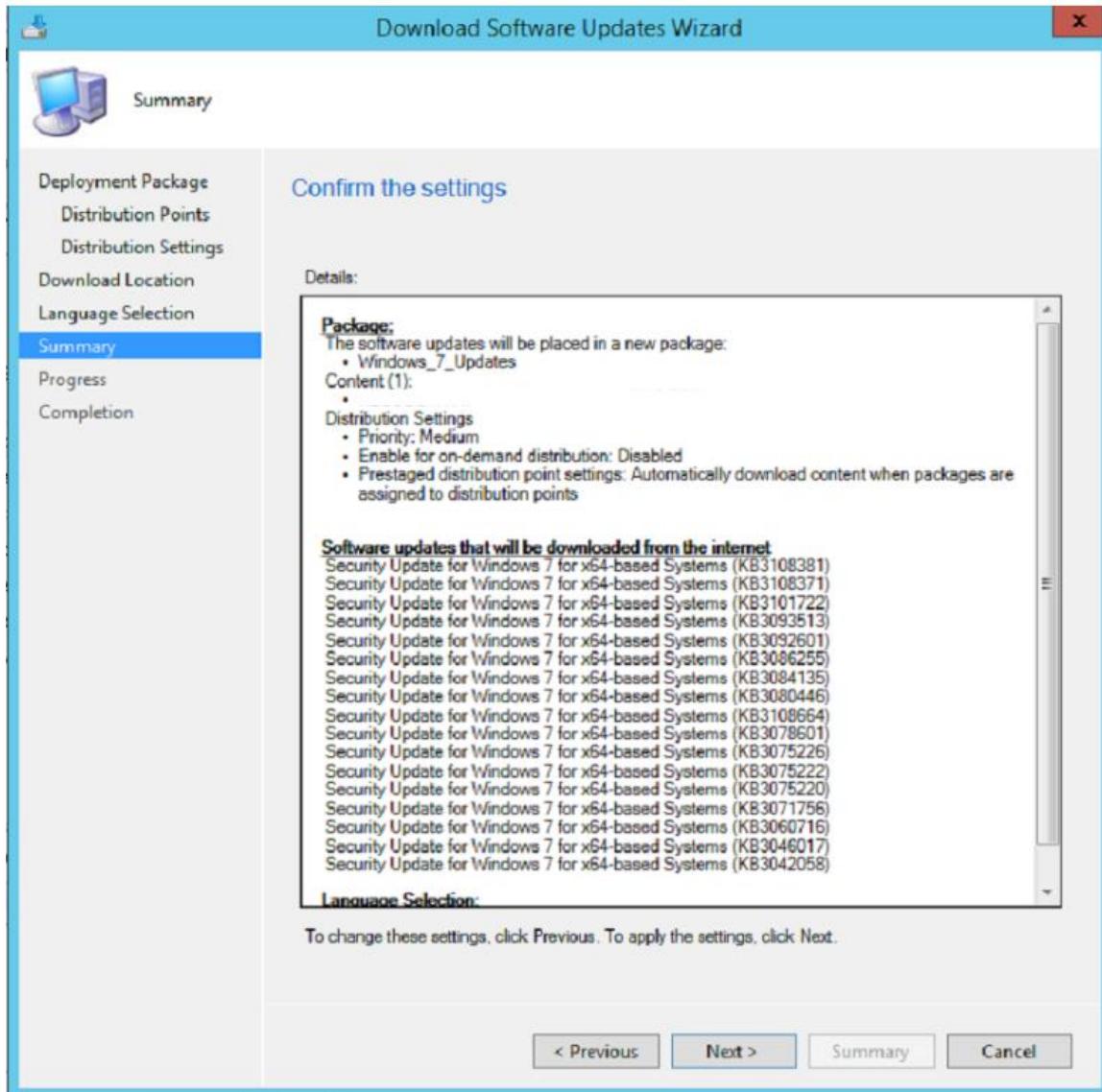
Click **Next**.

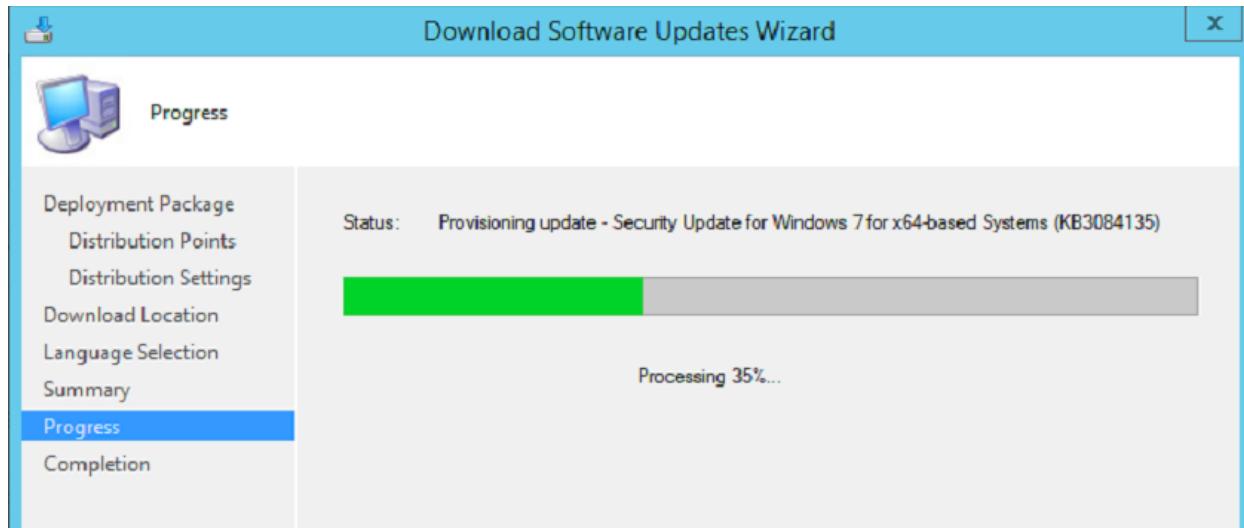


Click **Next**.

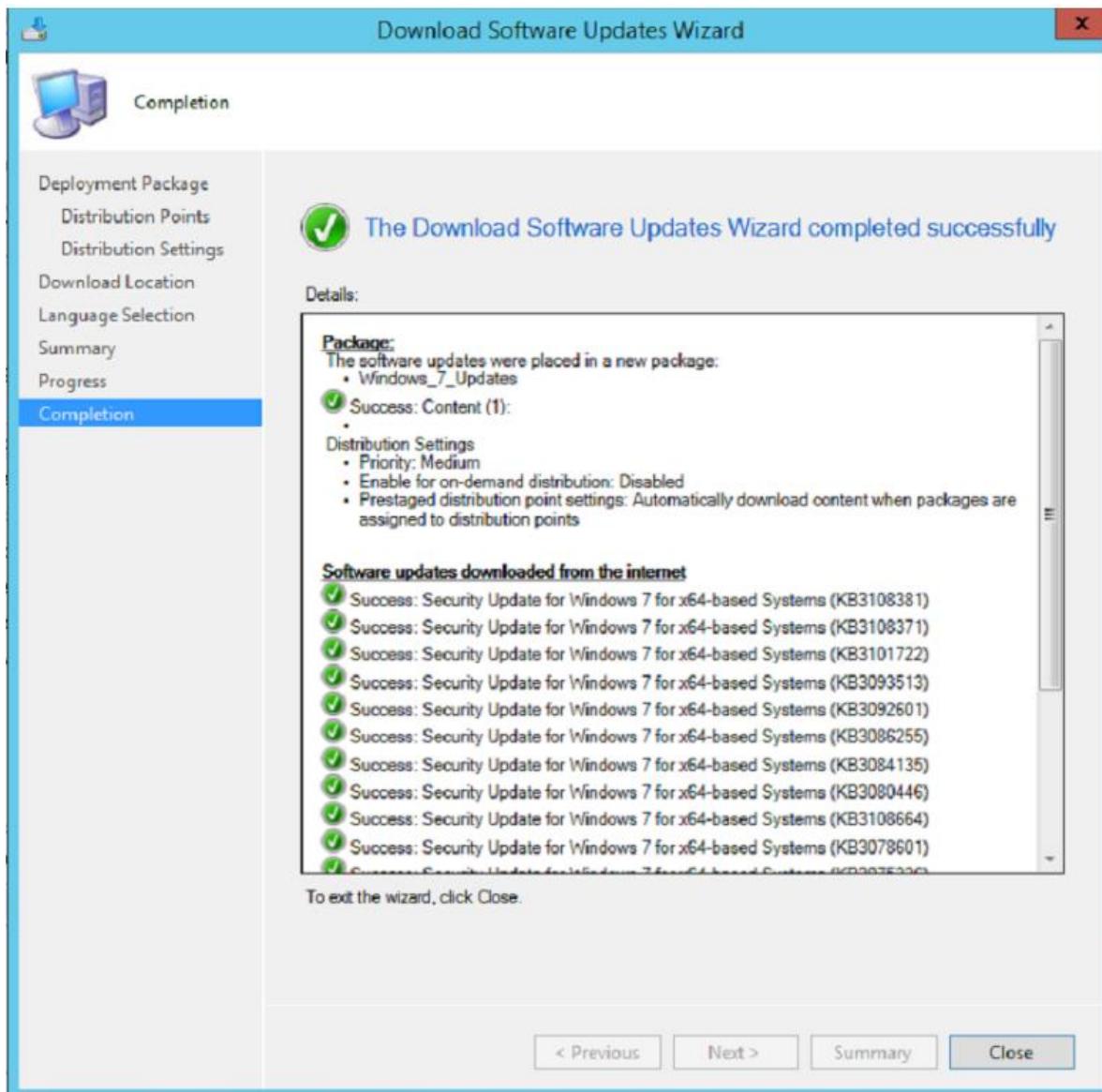


Click **Next**.

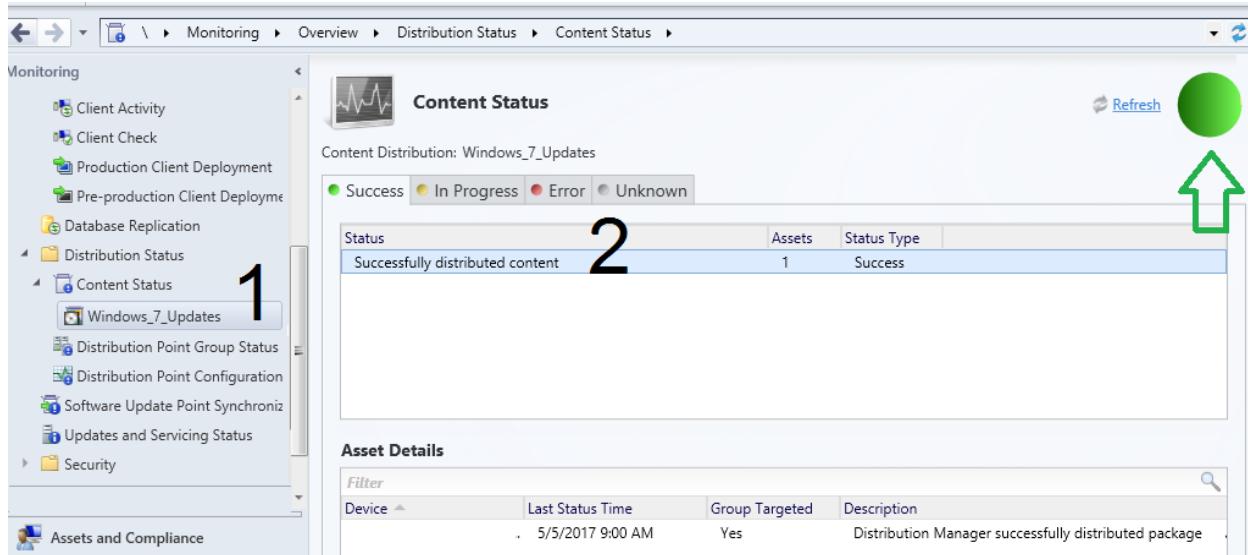




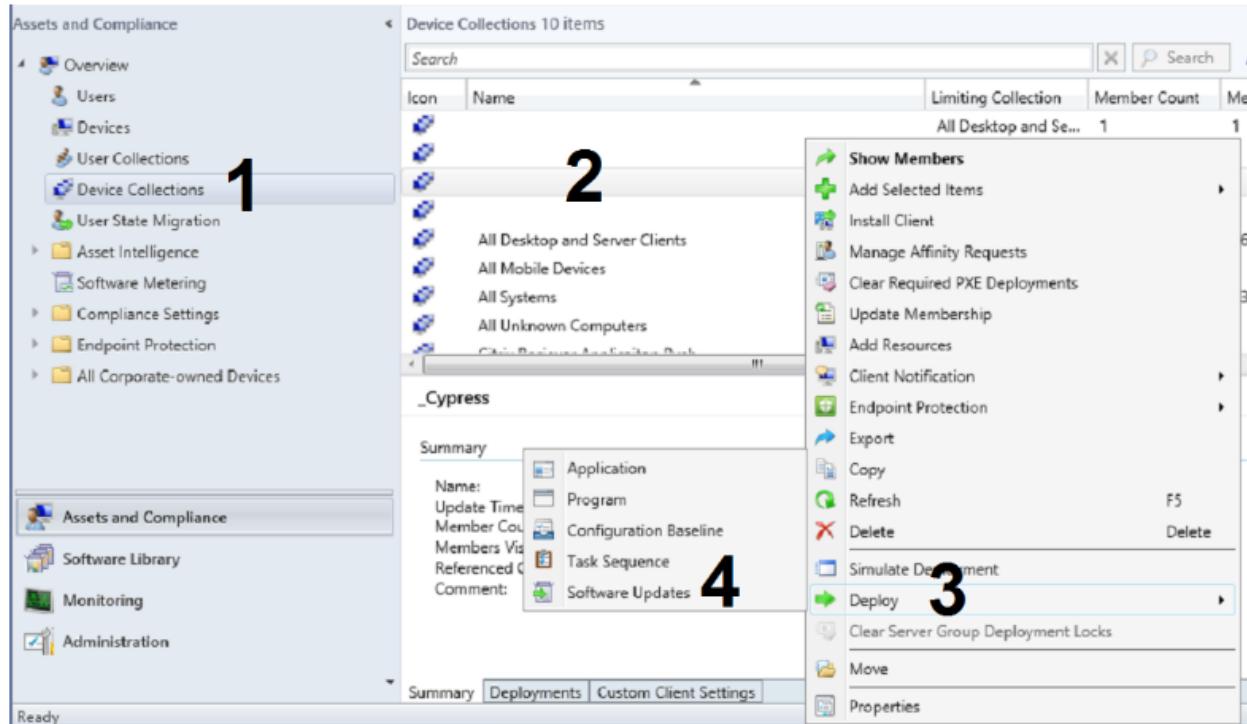
Click **Close**.



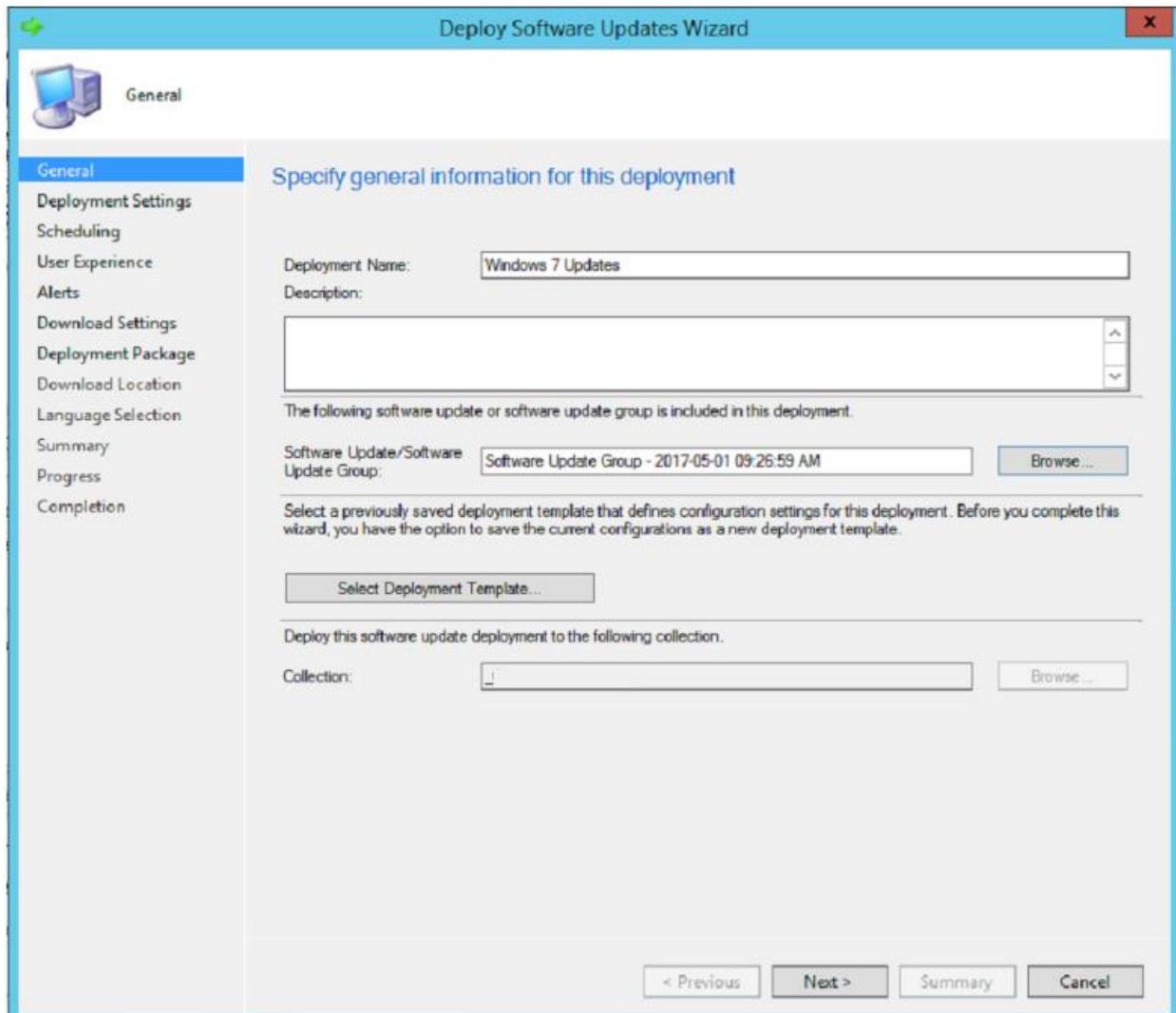
The distribution status can be monitored under **Monitoring > Distribution Status > Content Status**.



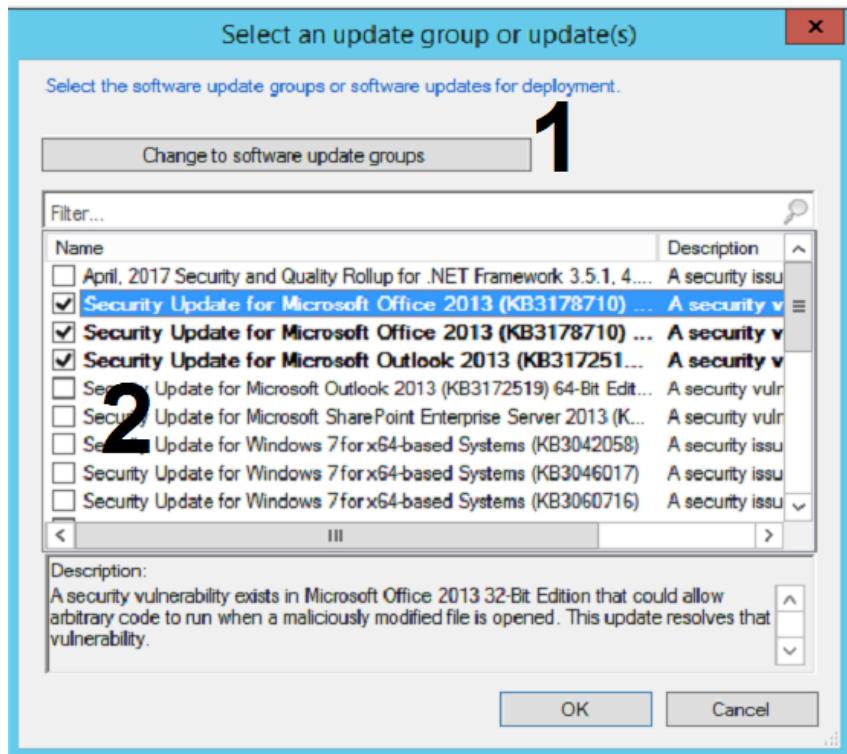
Once the content has been distributed, right-click on **Device Collection**, select **Deploy**, and select **Software Updates**.



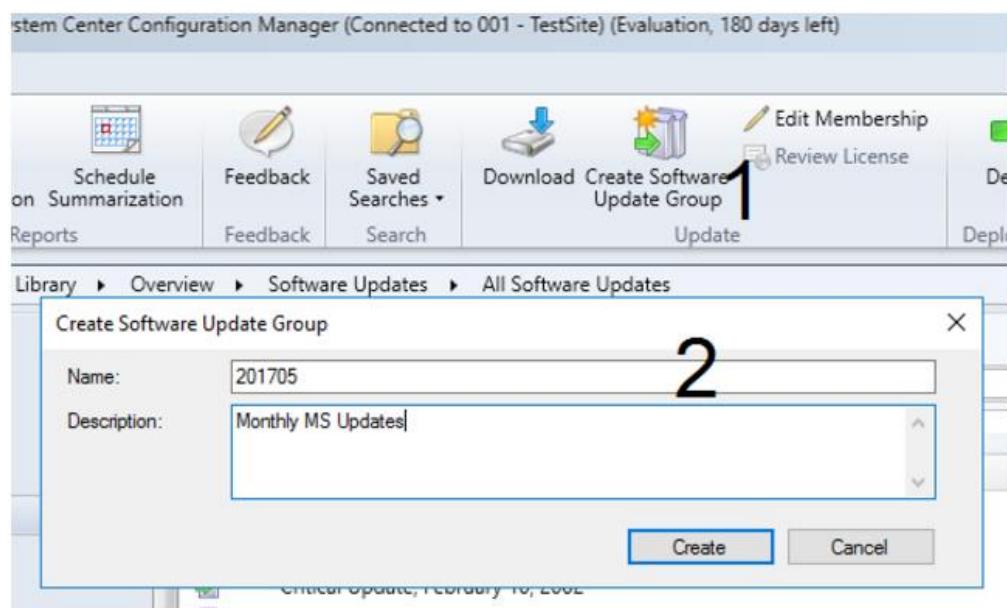
Enter Deployment Name. Browse to Software Update Group.

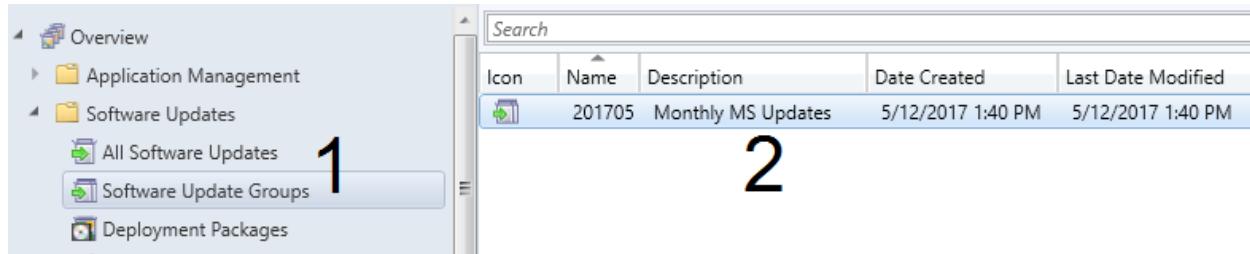


Click **Change to software update groups**. Choose the update(s). Click **OK**. Note, you could have already created a software group. In that case, just select the group, there is no need to change.

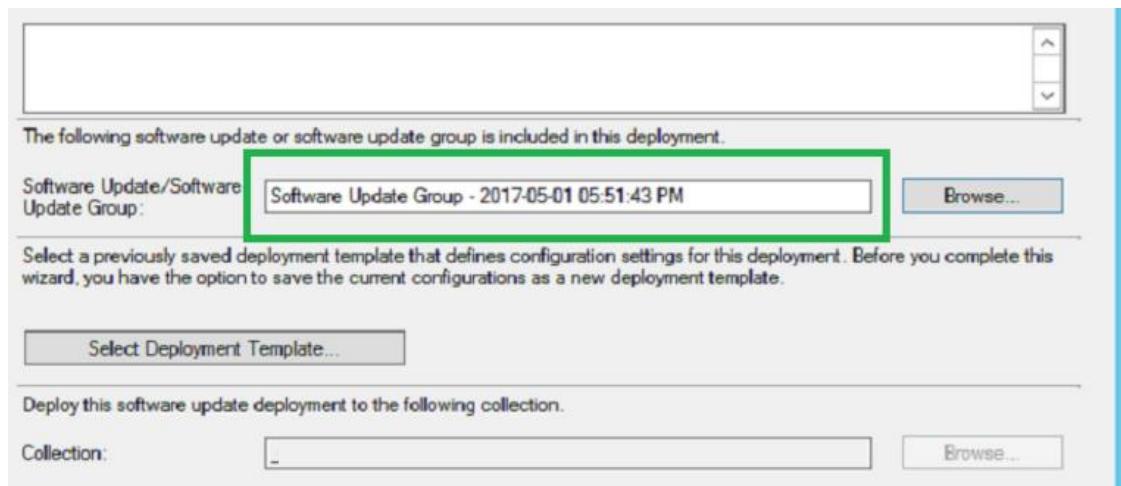


Side note, this is how to create a software update group.

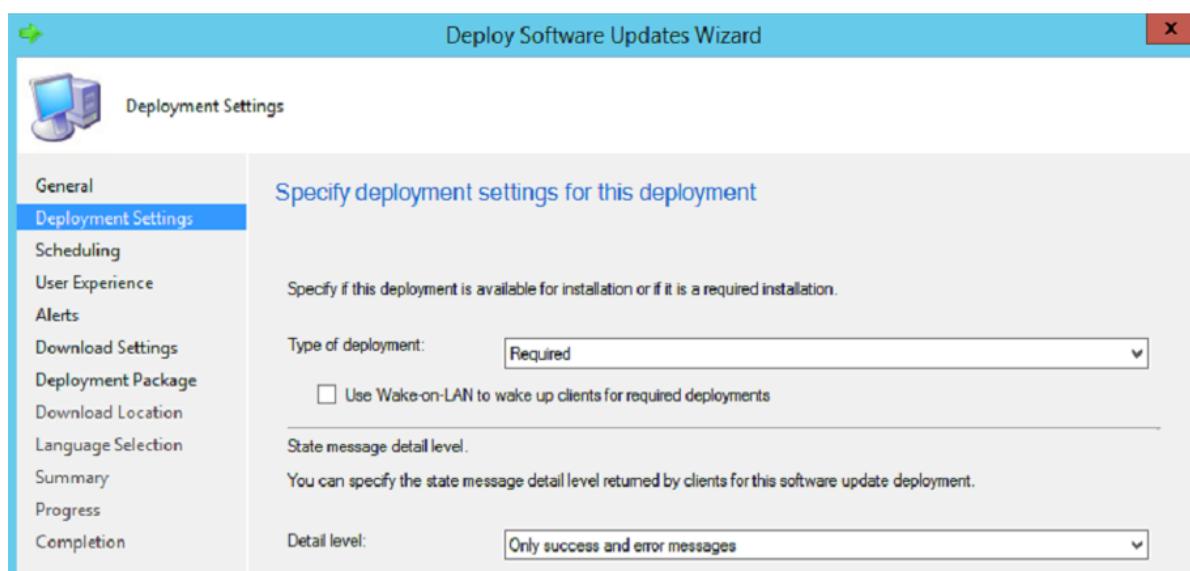




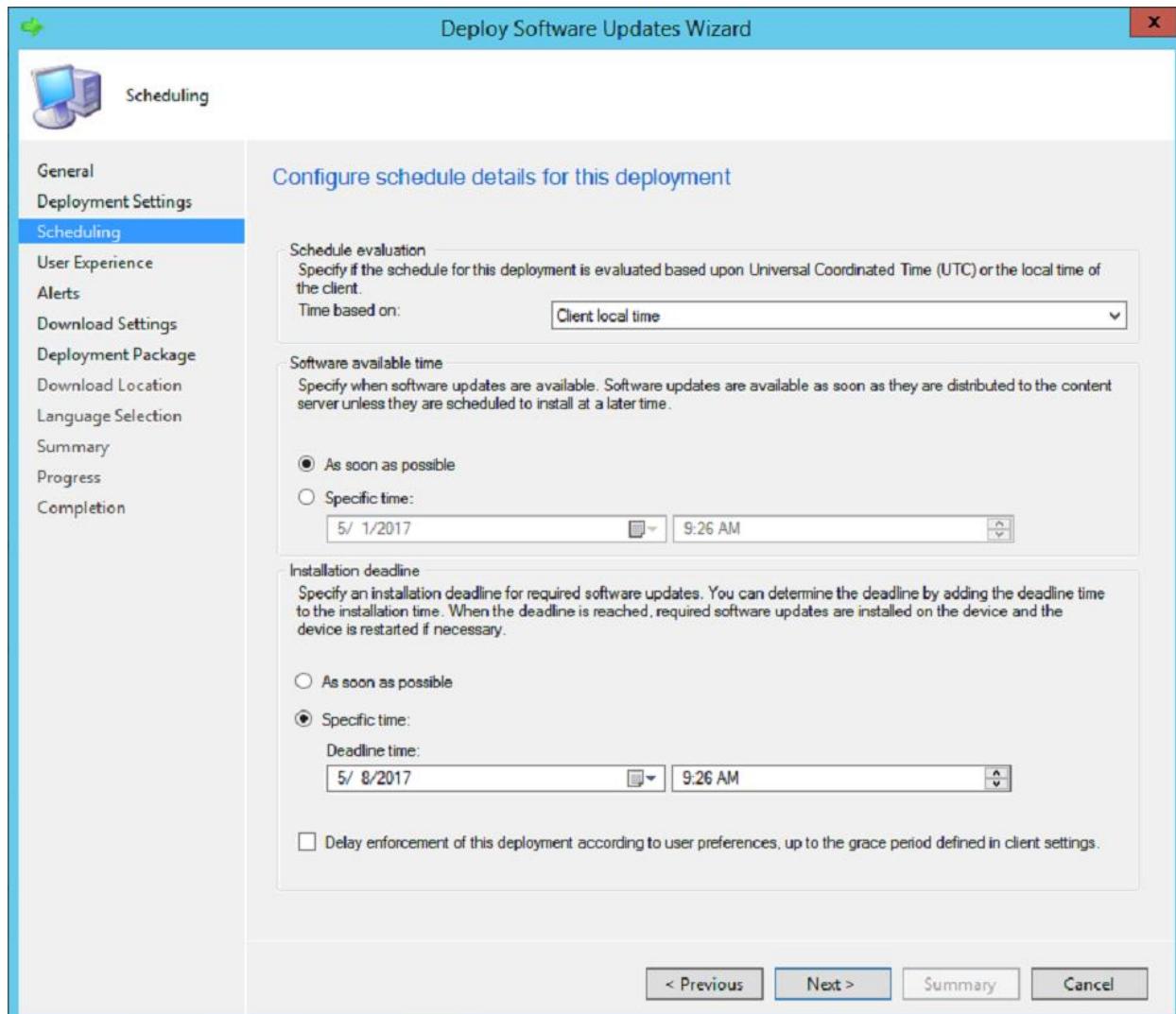
The group name will be populated (you can rename this). Click **Next**.



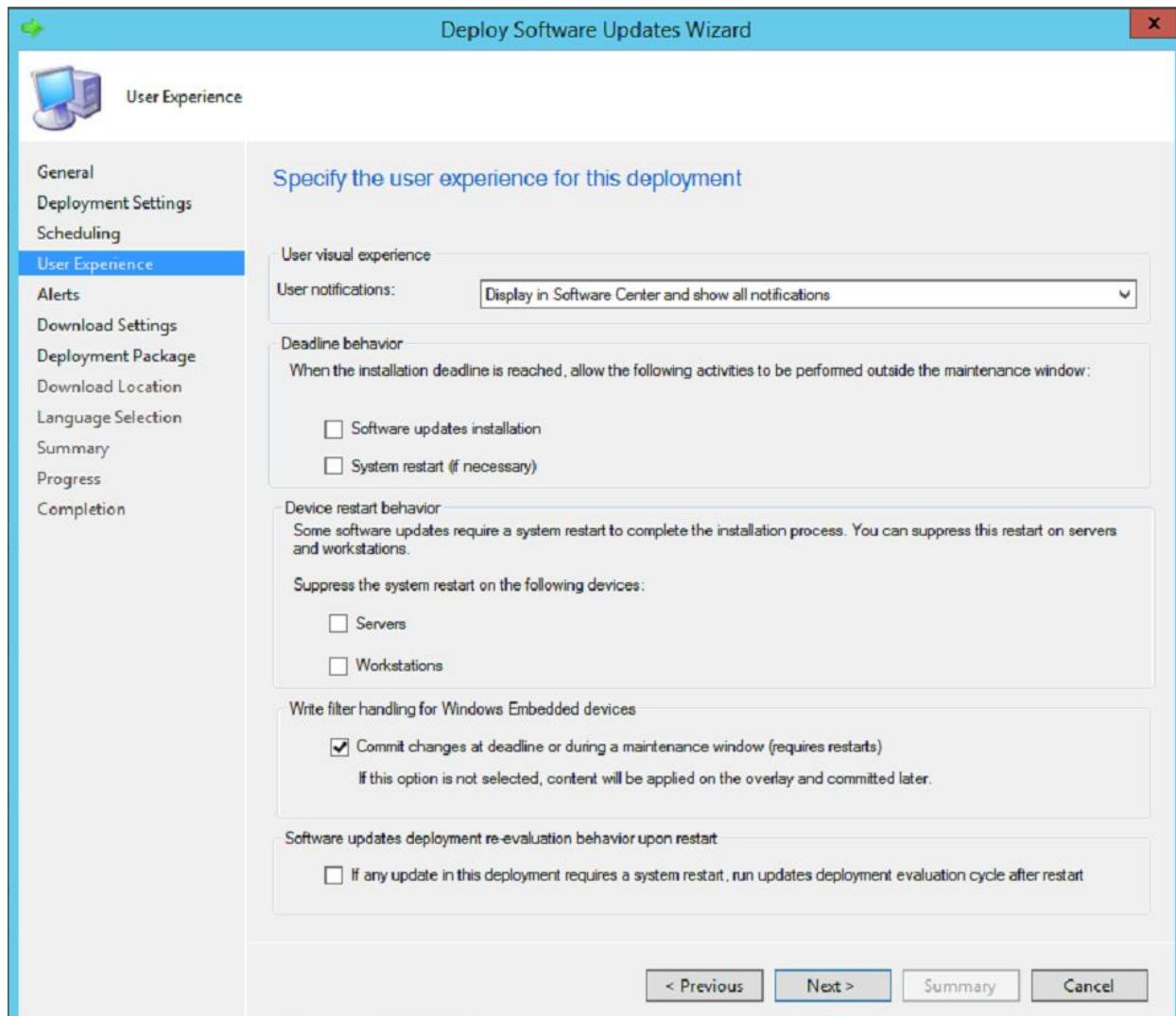
Specify **type** of deployment. Click **Next**.



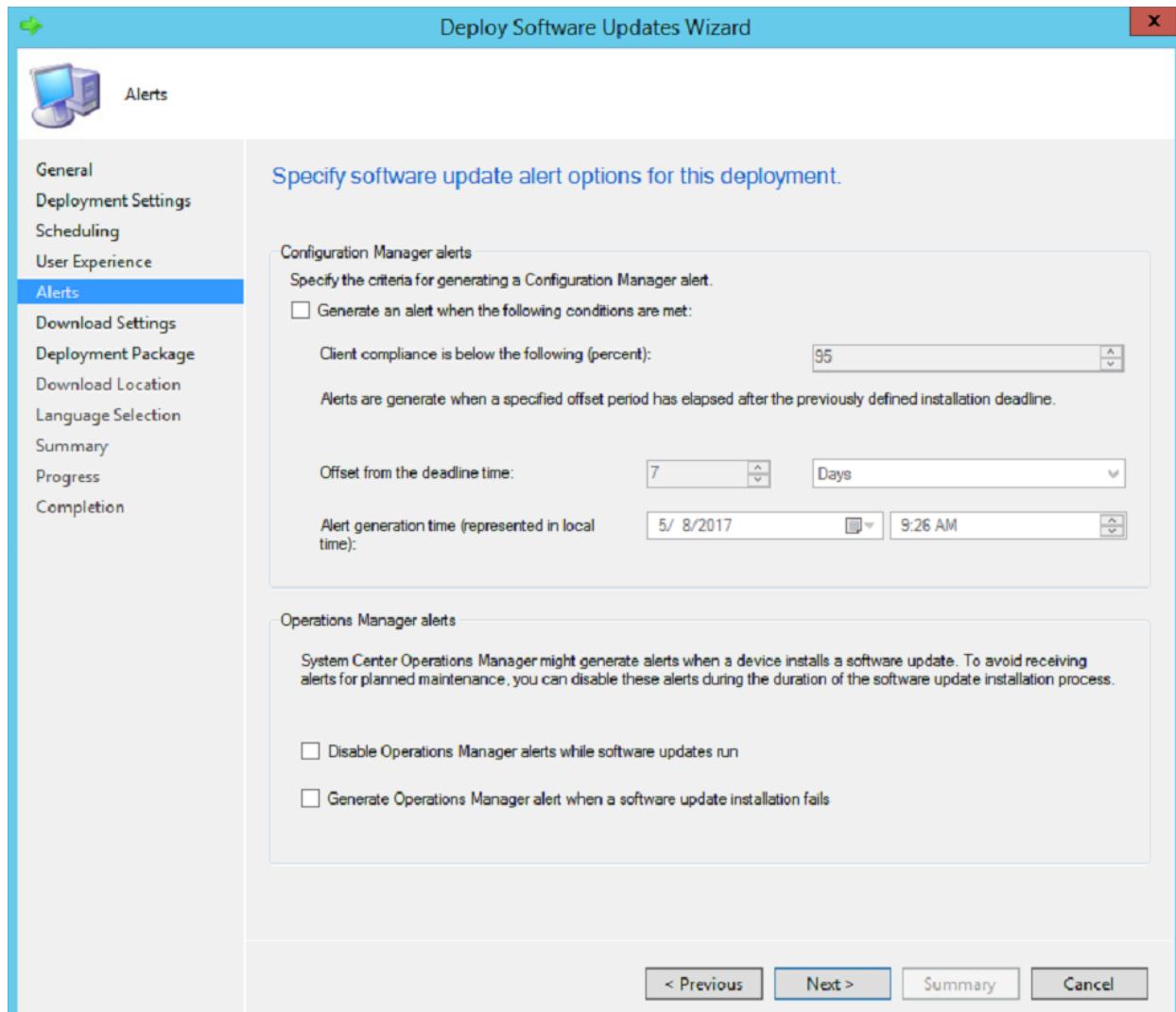
Enter the **schedule** for the deployment. Click **Next**.



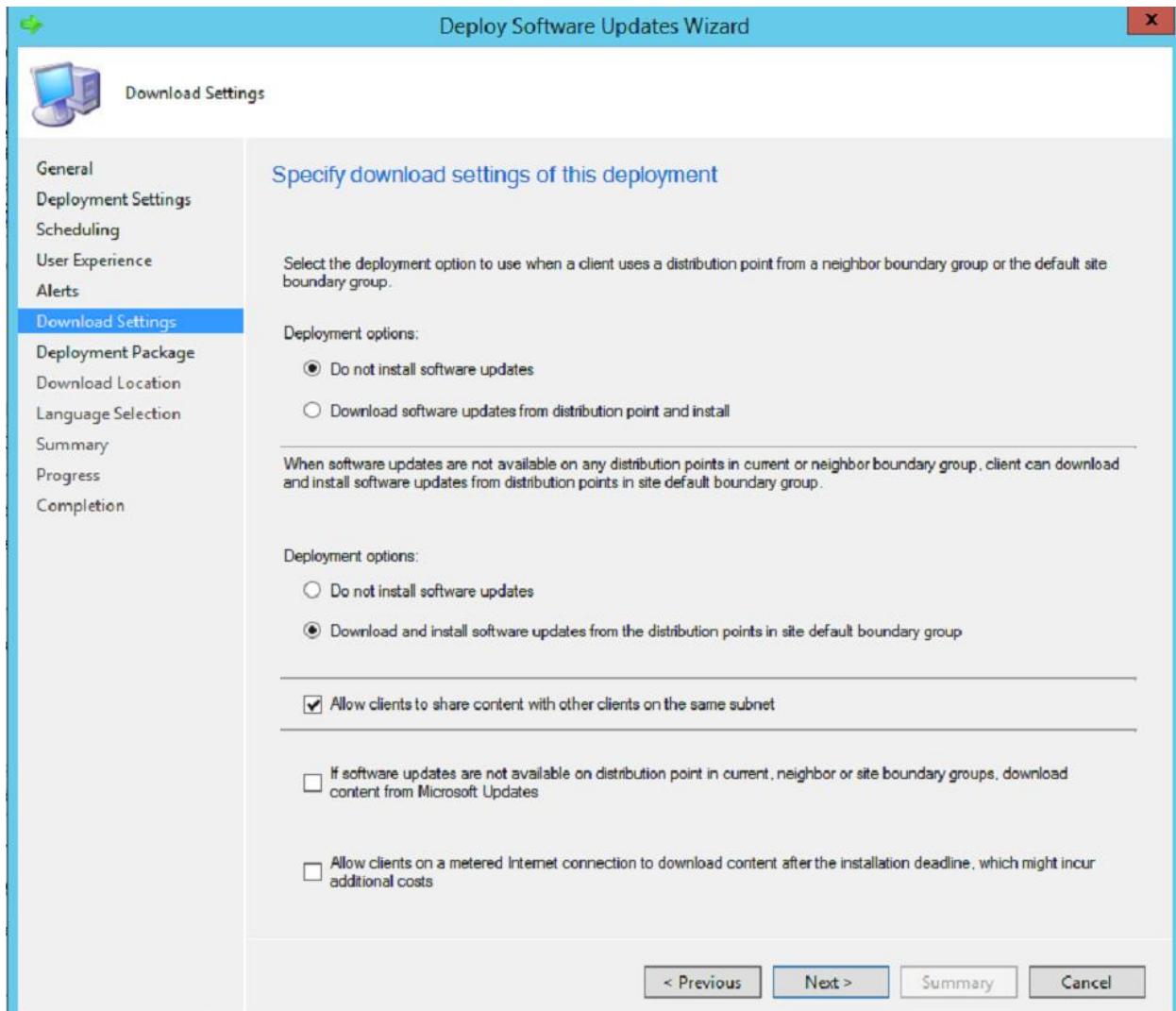
Specify the **user experience**. Click **Next**.



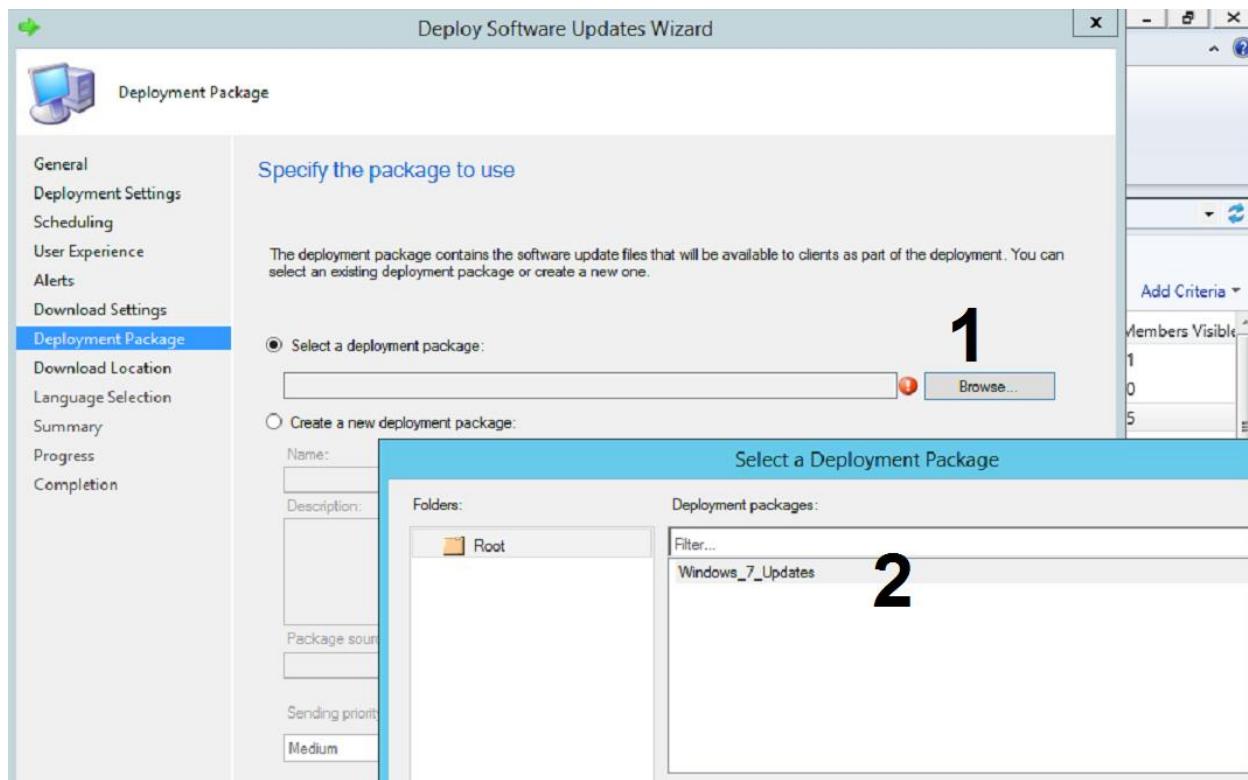
Specify the update alert options. Click Next.



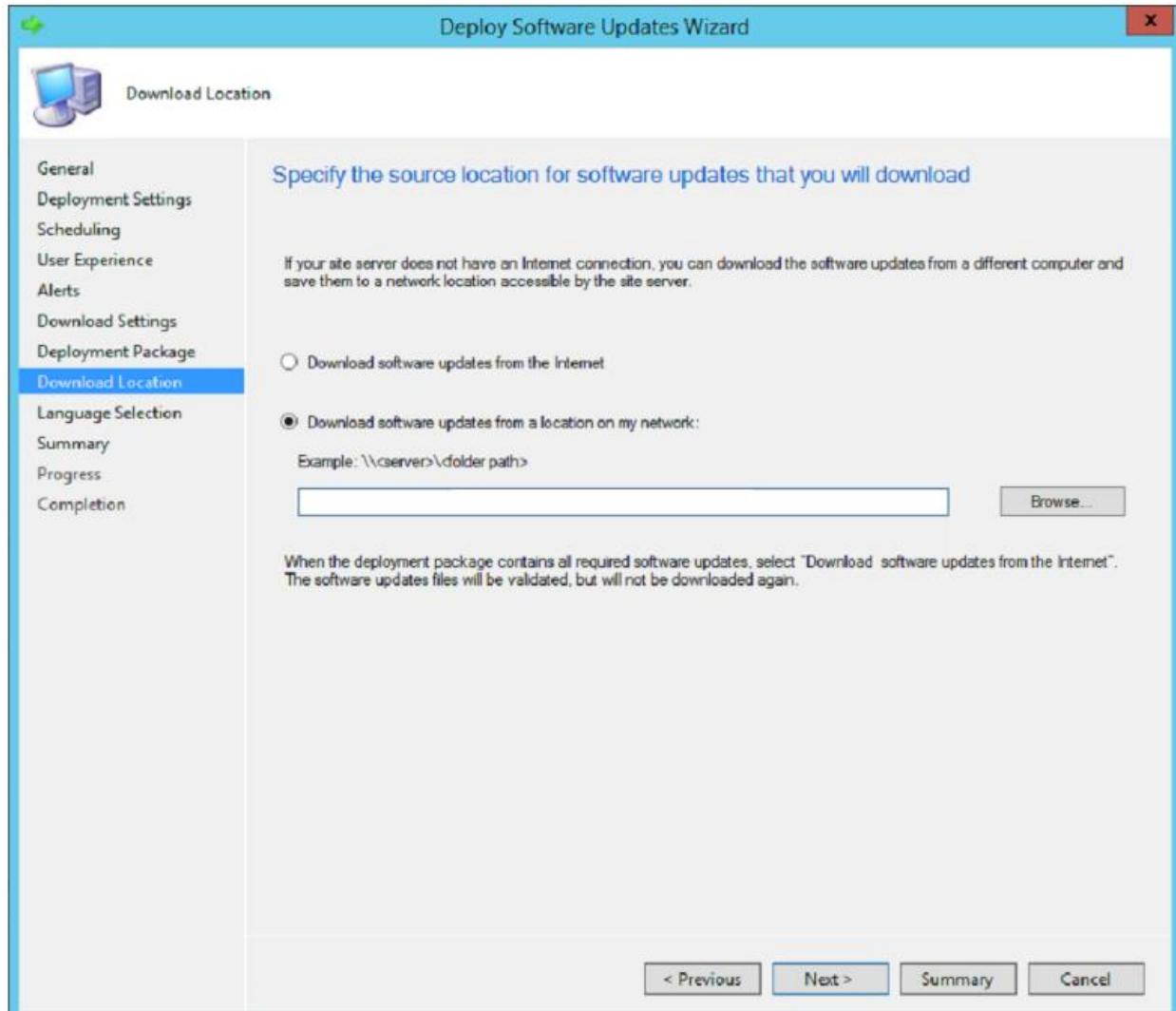
Specify the **download settings**. Click **Next**.



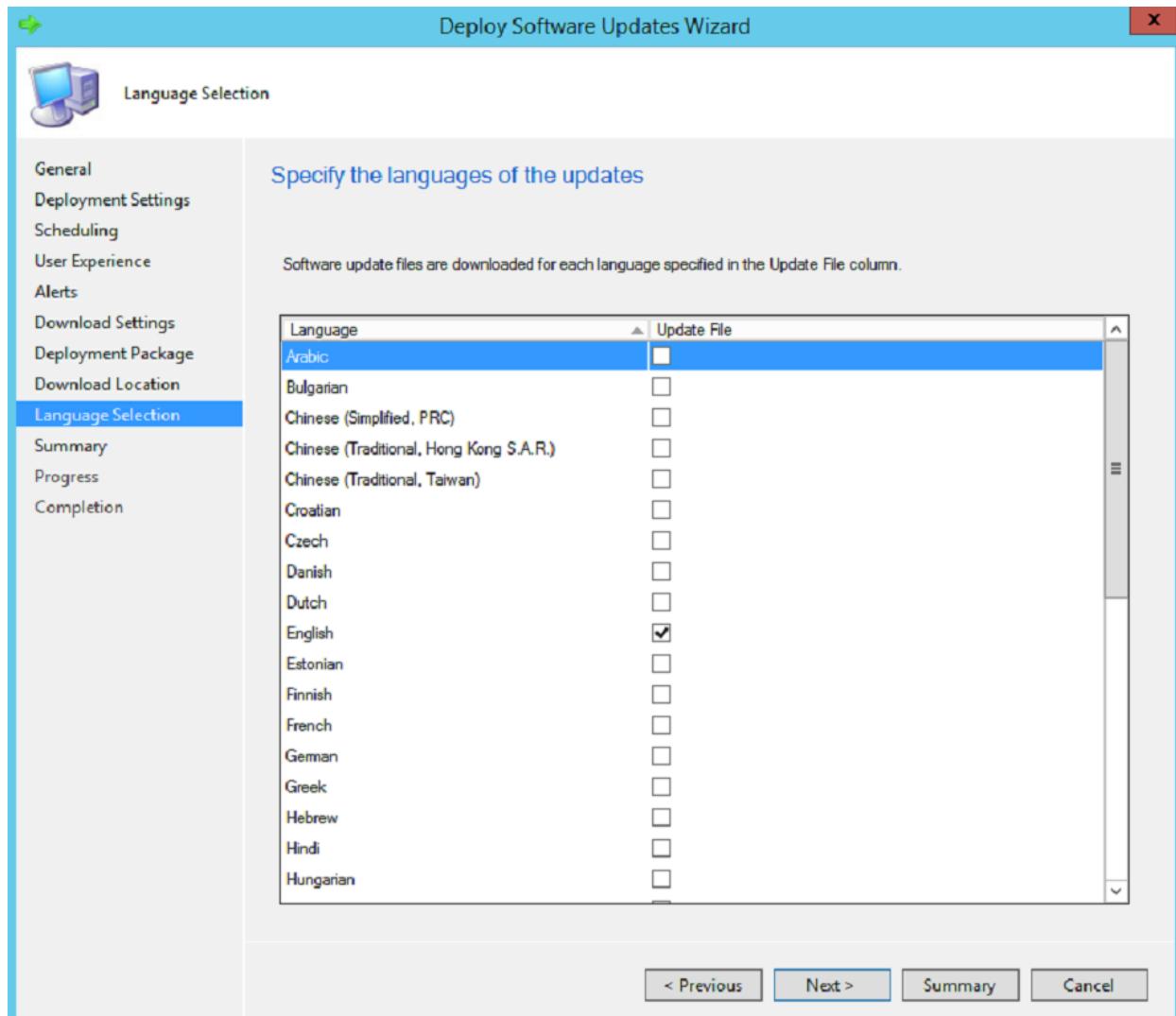
Select a **deployment package** or create a new one. Click **Next**.



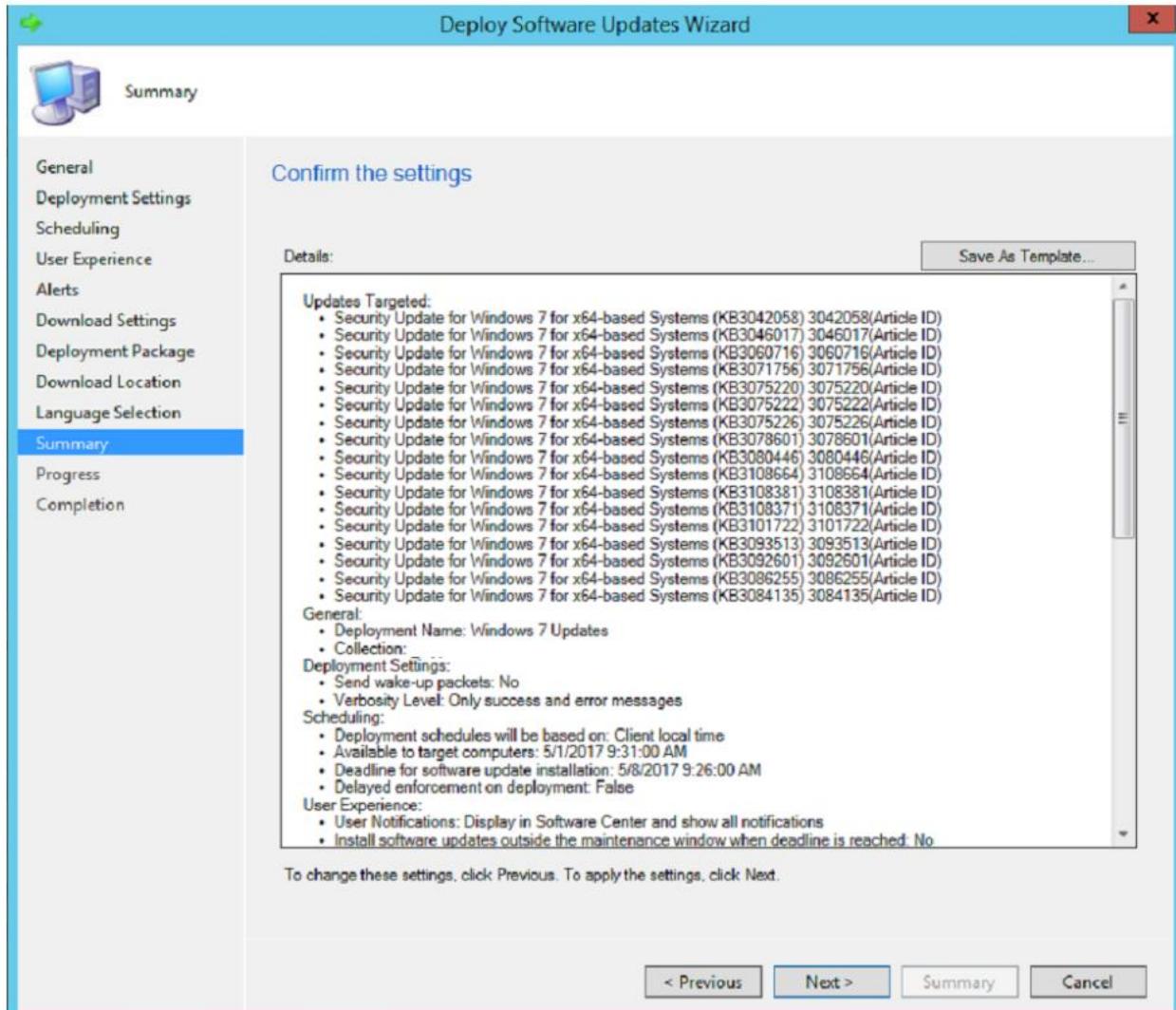
Select **Download software updates from a location on my network**. Enter FQDN path. Click **Next**.



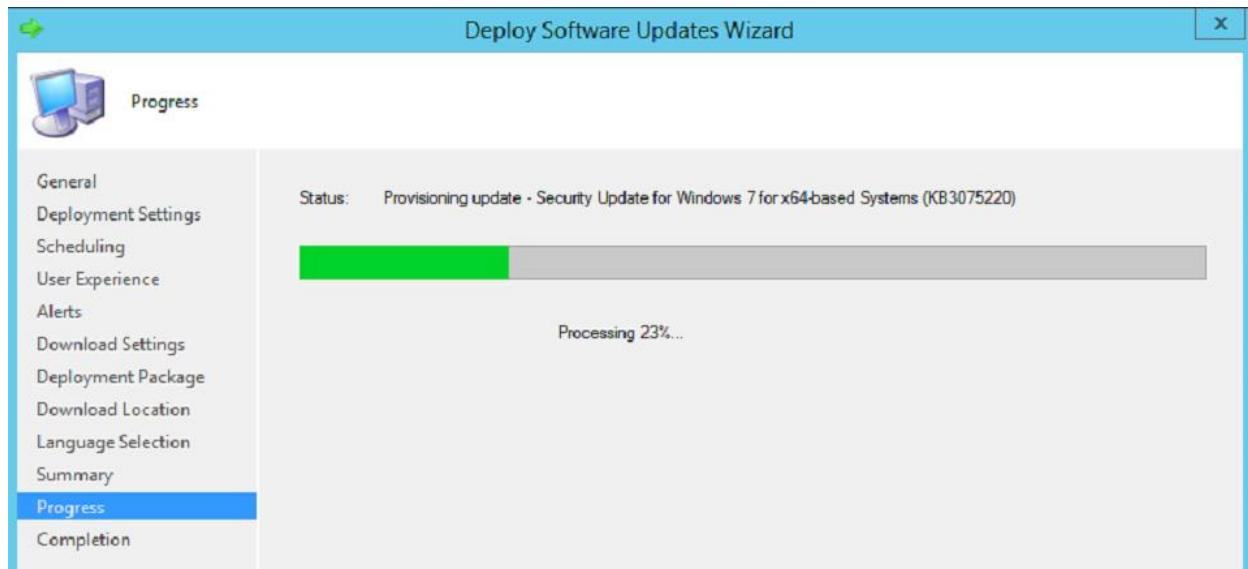
Specify **languages**. Click **Next**.



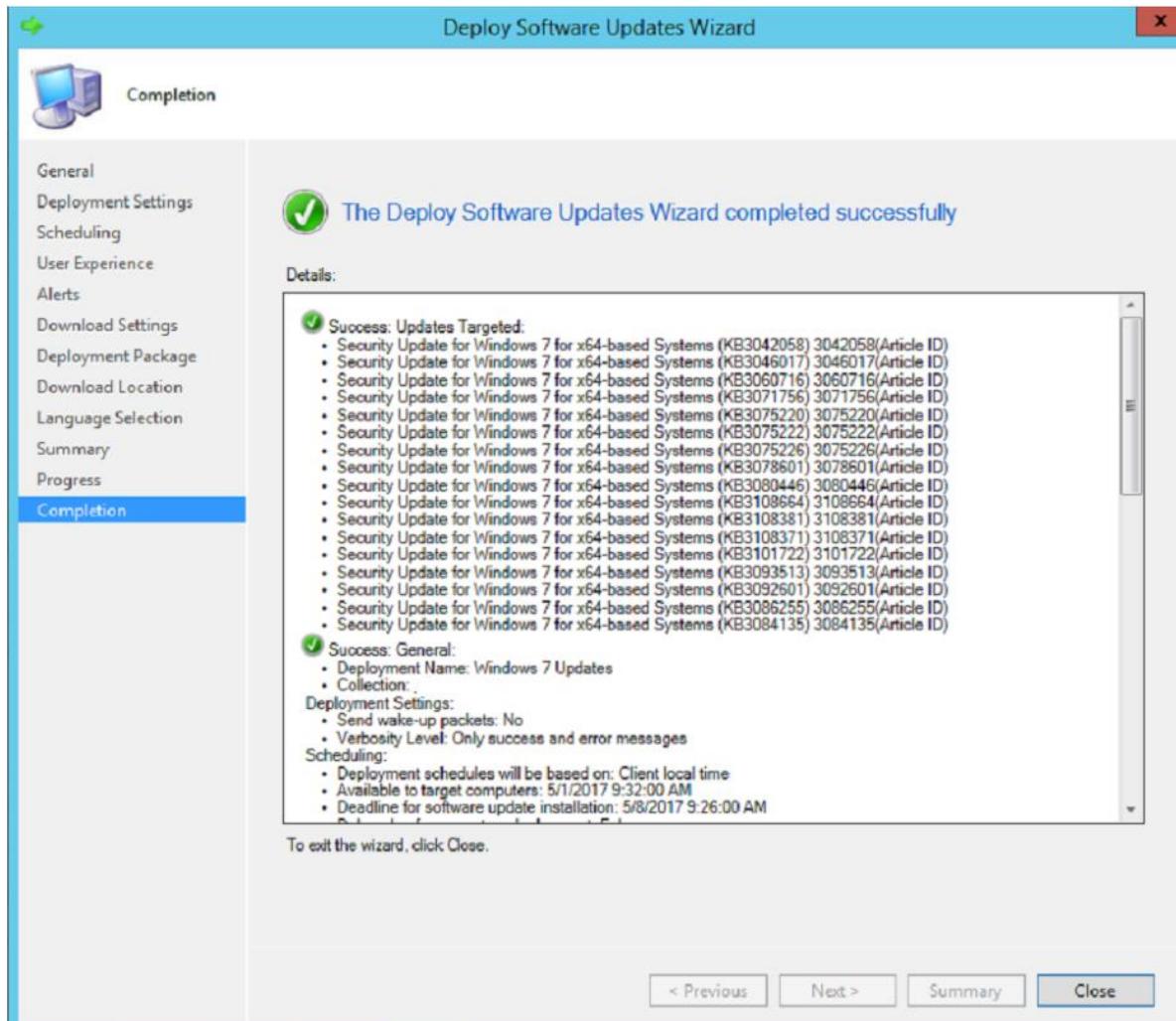
Confirm settings. Click Next.



Deployment package will be provisioned.



Review summary. Click **Close**.



The Deploy status can be monitored under **Monitoring > Deployments**.

The screenshot shows the SCCM console interface. On the left, the navigation pane is open with the following structure:

- Monitoring
 - Overview
 - Alerts
 - Queries
 - Reporting
 - Site Hierarchy
 - System Status
 - Deployments**
 - Software Update Group - 2017-05-01 9:26:59 AM
 - Client Operations
 - Client Status
 - Database Replication
 - Distribution Status
 - Software Update Point Synchronization Stz
 - Updates and Servicing Status
- Assets and Compliance
- Software Library
- Monitoring** (highlighted with a large black number 1)
- Administration

A large black number 2 is overlaid on the 'Deployments' node in the tree view.

The main content area displays the 'Deployment Status' report. At the top, it shows 'Software Update: Software Update Group - 2017-05-01 09:26:59 AM' and 'Collection:'. Below this is a status bar with four colored indicators: Compliant (green), In Progress (yellow), Error (red), and Unknown (grey). A large black number 3 is overlaid on the status bar.

Total	Category
5	Client check passed/Acti...

Below the report is a section titled 'Asset Details' with a table:

Device	User	Category
		Client check passed/Active

Once a client has received and **completed** the installation, the device will appear under **Compliant**.

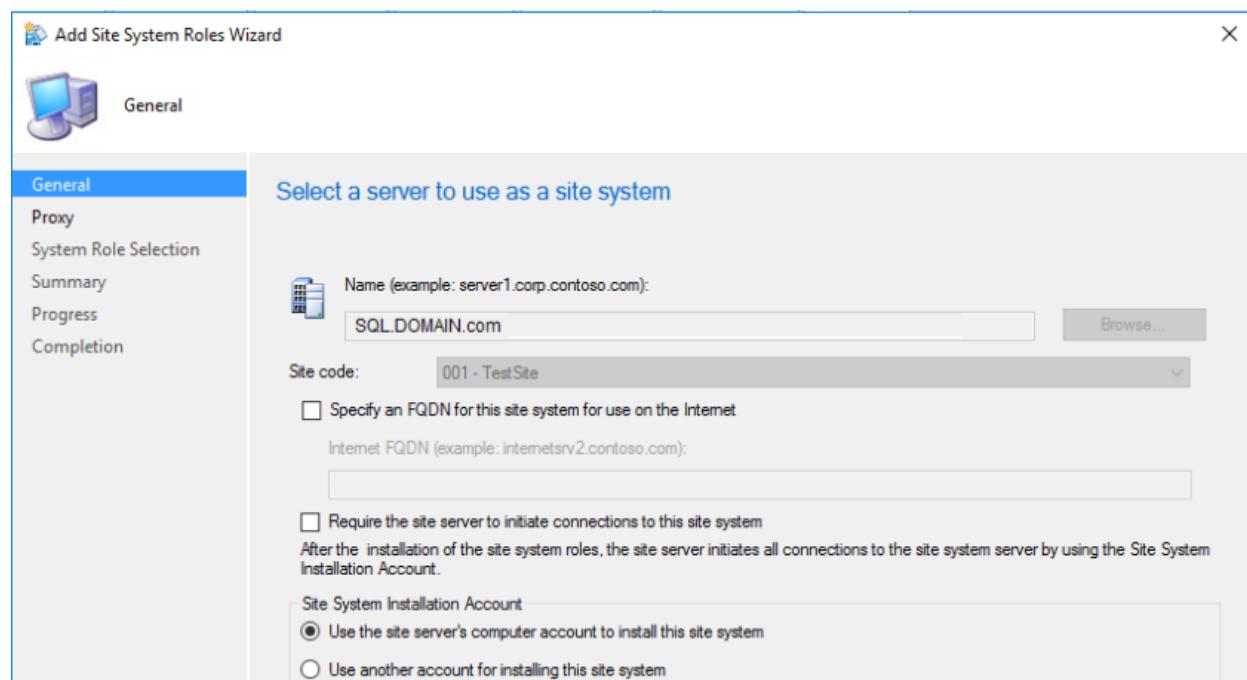
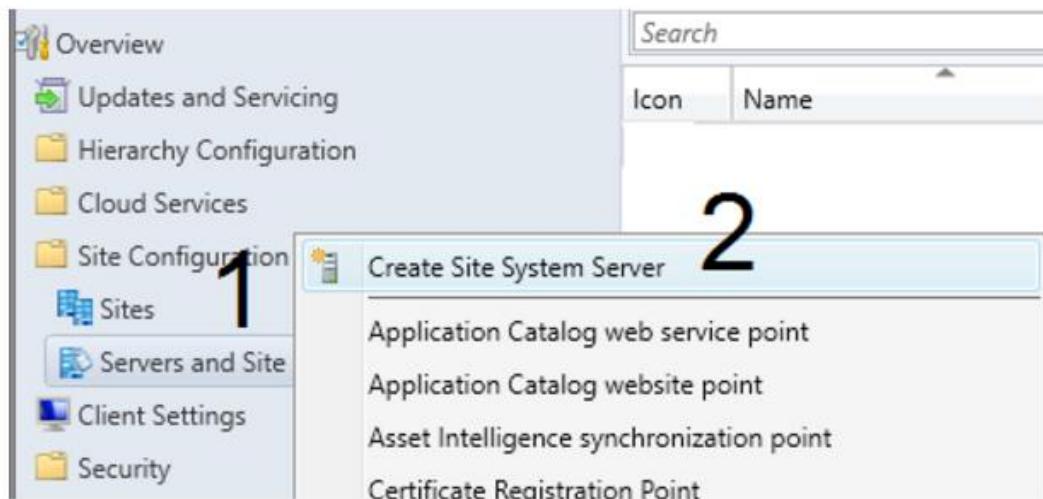
The screenshot shows the 'Deployment Status' page. At the top, there is a header with a bar chart icon, the title 'Deployment Status', and buttons for 'Run Summarization' and 'Refresh'. Below the header, it says 'Summarization Time: 5/1/2017 9:45:36 AM'. A pie chart indicates 100% completion. The main area displays a table of assets:

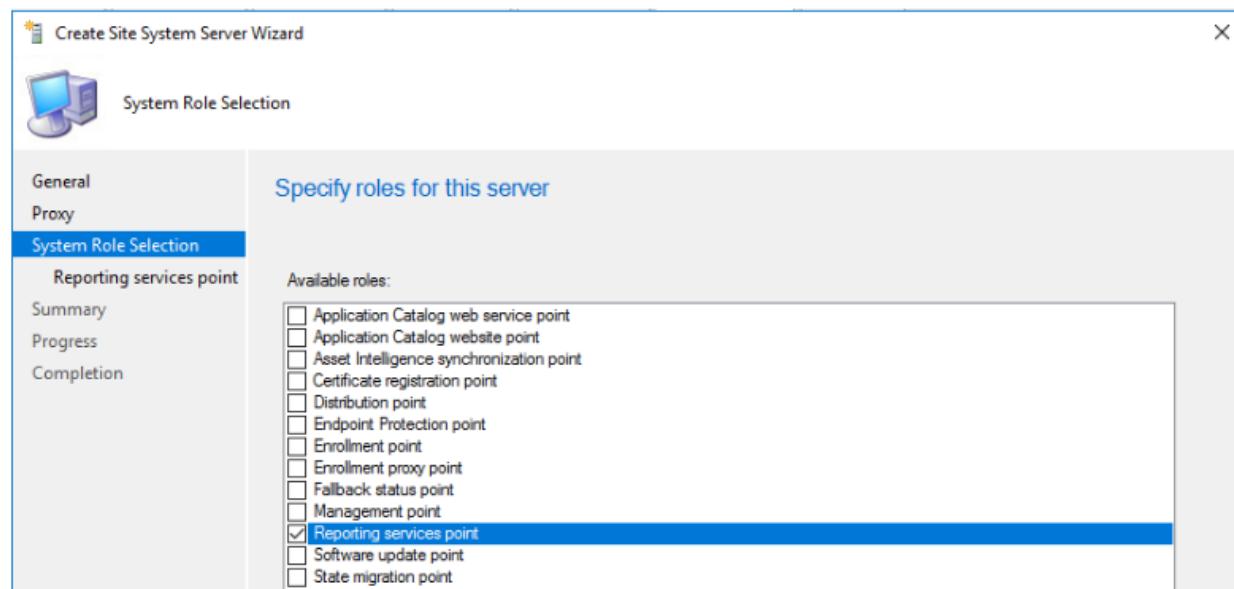
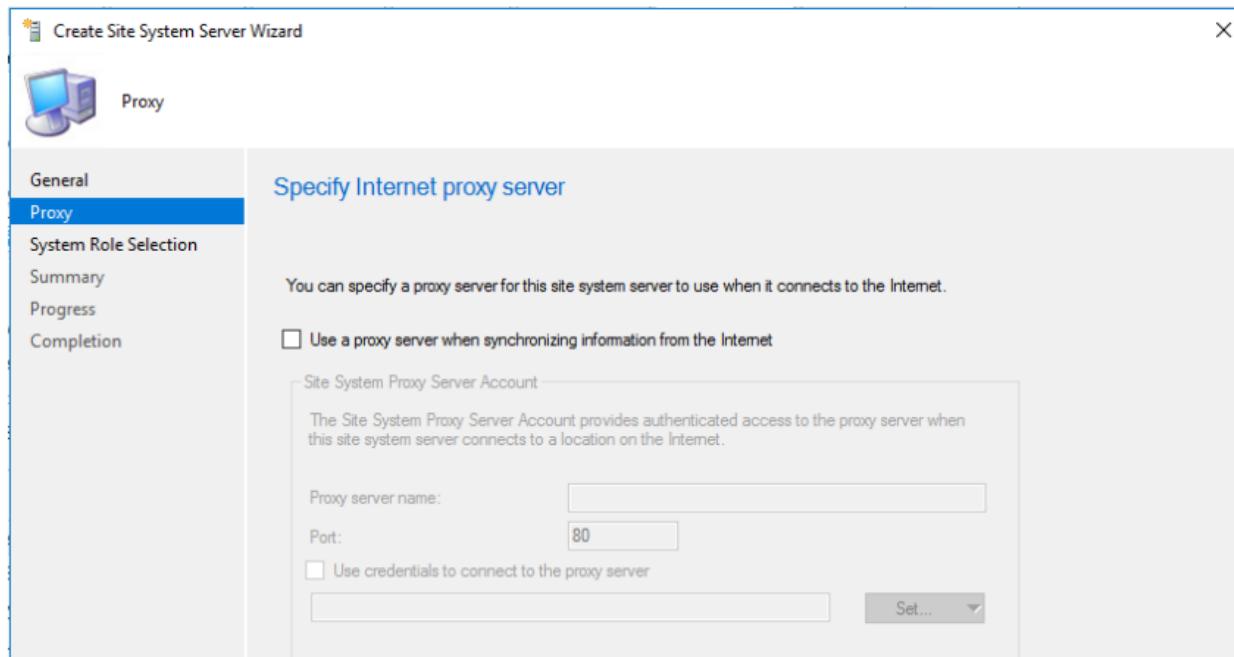
Total Assets	Status	Last Status Time
1	Compliant	5/1/2017 9:38 AM

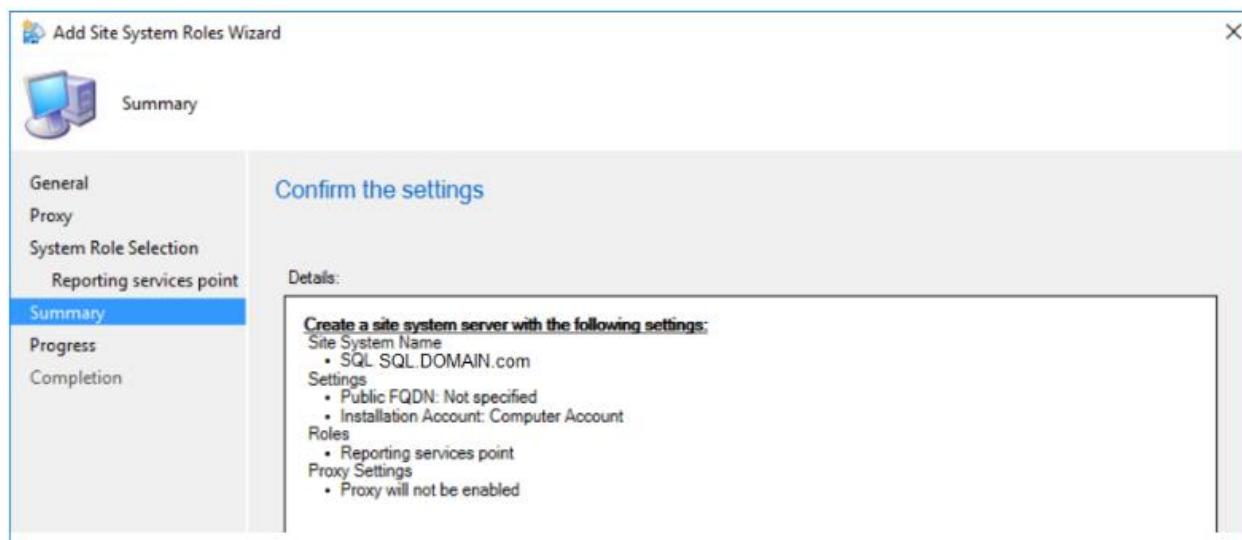
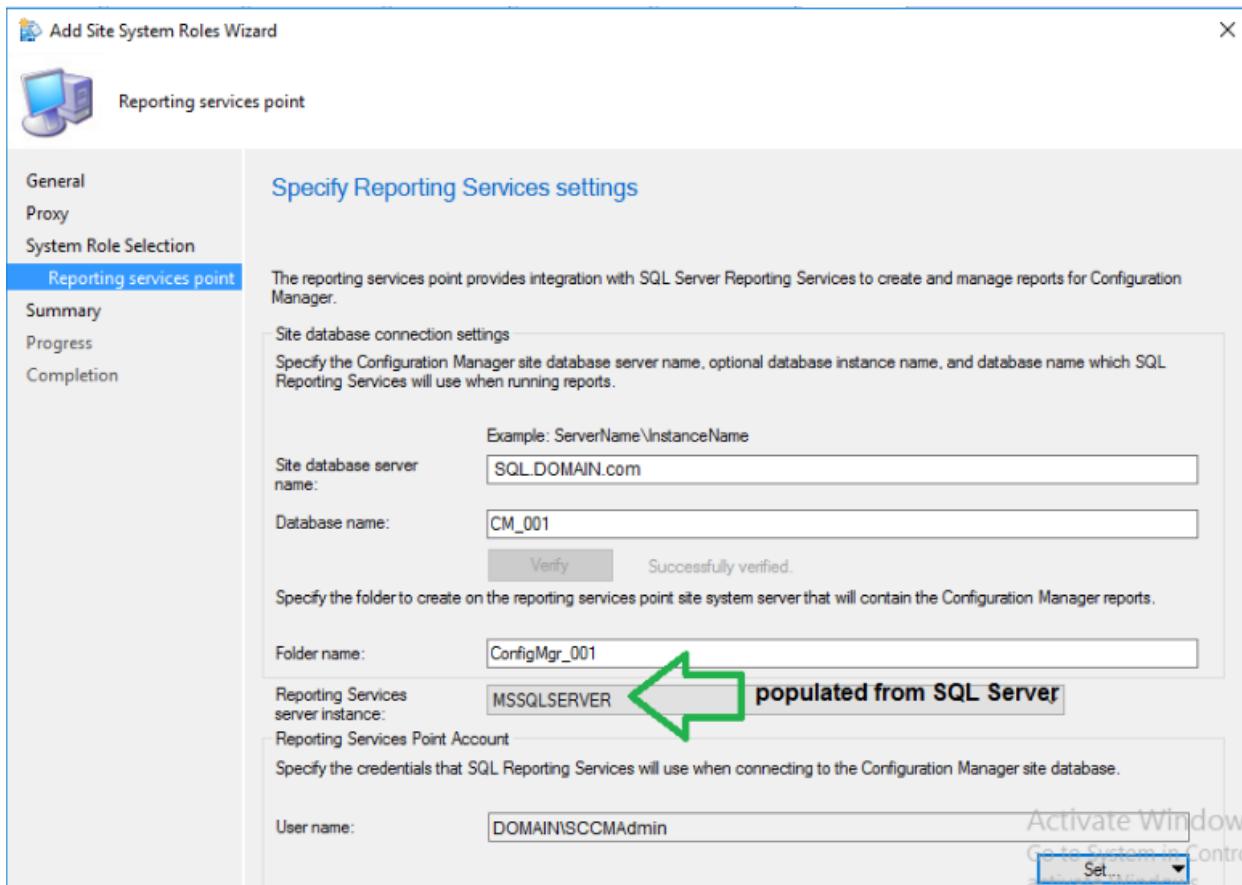
Below the table, the 'Asset Details' section shows the following information for the single asset:

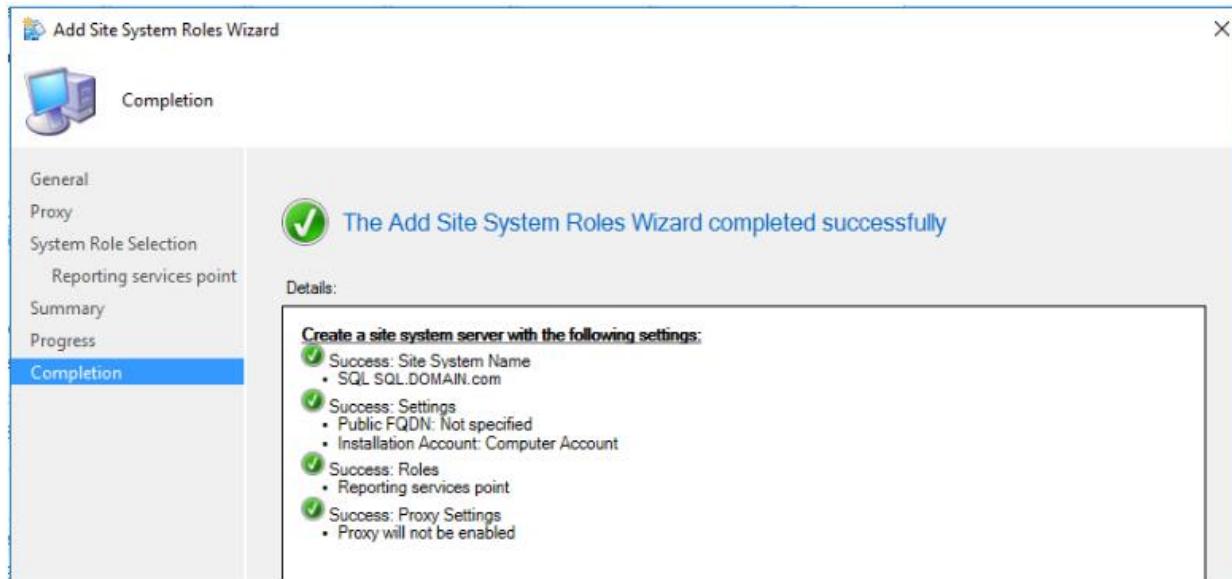
Device	Last Logged On User	Last Compliance State	Last Compliance Message Time
(SYSTEM)		Compliant	5/1/2017 9:38 AM

Report Setup, Reporting Services Point









Successful Reporting Setup

Icon	Name	Category
Administrative Security	Administration activity log	Administrative Security
Administrative Security	Administrative users security assignments	Administrative Security
Alerts	Alert scorecard	Alerts
Alerts	Alerts Generated Most Often	Alerts
Asset Intelligence	All corporate-owned mobile devices	Device Management
Client Push	All drivers	Driver Management
Client Status	All drivers for a specific platform	Driver Management
Company Resource Access	All drivers in a specific boot image	Driver Management
Compliance and Settings Management	All drivers in a specific category	Driver Management
Data Warehouse	All drivers in a specific package	Driver Management
Device Management	All mobile device clients	Device Management
Device Management	Antimalware activity report	Endpoint Protection
Device Management	Antimalware overall status and history	Endpoint Protection
Assets and Compliance	Application deployment - Historical	Data Warehouse
Software Library	Categories for a specific driver	Driver Management
Monitoring	CD-ROM information for a specific computer	Hardware - CD-ROM
Administration	Certificate issuance history	Company Resource Access
Administration	Certificate issues on mobile devices that are managed by the Configura...	Device Management
Administration	Client assignment detailed status report	Site - Client Information
Administration	Client assignment failure details	Site - Client Information

Set up a Distribution Point at Another Site

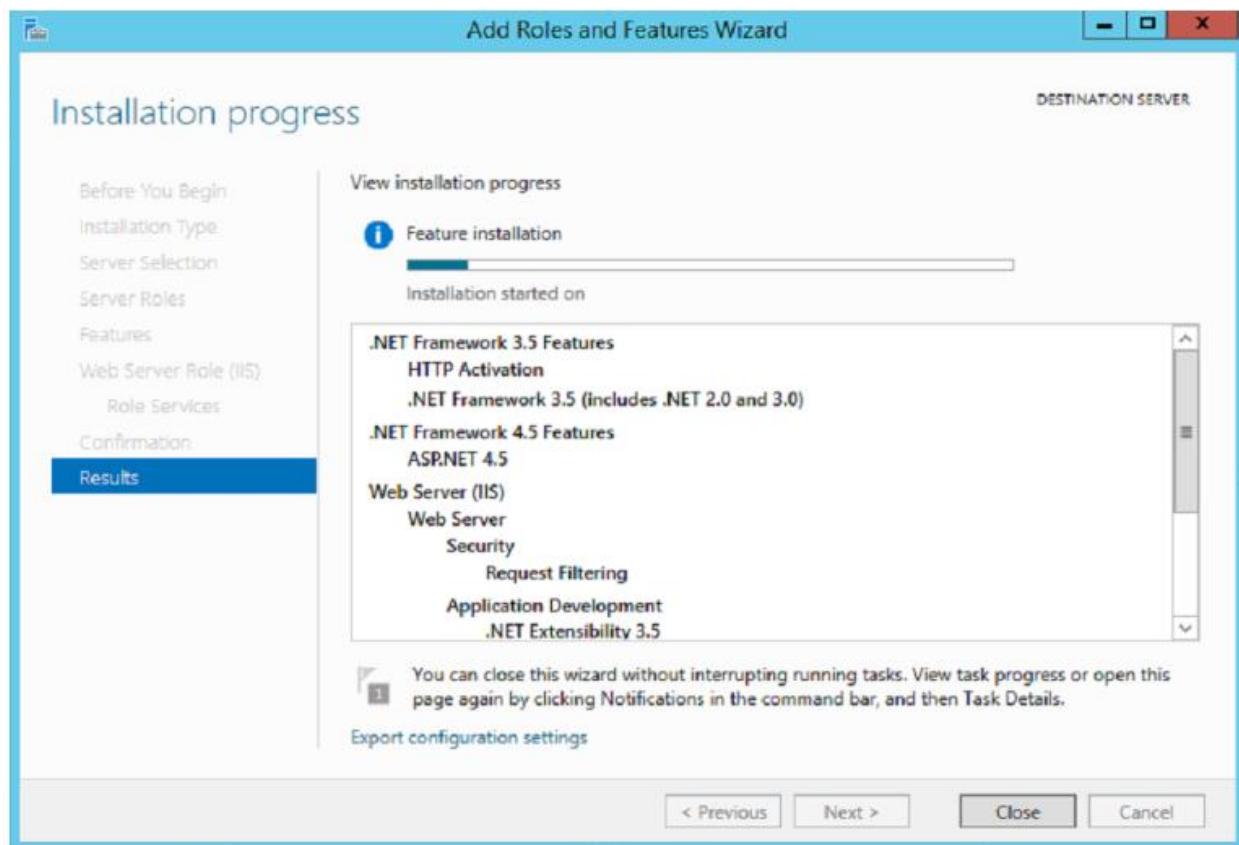
Set up base server. Set static IP. Add server name into the Administrators group. Add SCCM service account into the Administrators group. For testing purposes only, disable the firewall.

Download current SCCM build (it should be the same build as the primary server).

If .NET 3.5 isn't installed, you will have to add a role and select the 3.5 features.

1. Insert Windows Server 2012 DVD or mount ISO.
2. Open Add Roles and Features Wizard.
3. Select .NET Framework 3.5 Features and then click Next.
4. Select Specify an alternate source path link in the Confirm installation selections screen.
5. Path: D:\Sources\SxS and then click OK.
6. Finally click Install button.

Features will install. Click **Close** when done.



Add Roles in Add Roles and Features Wizard

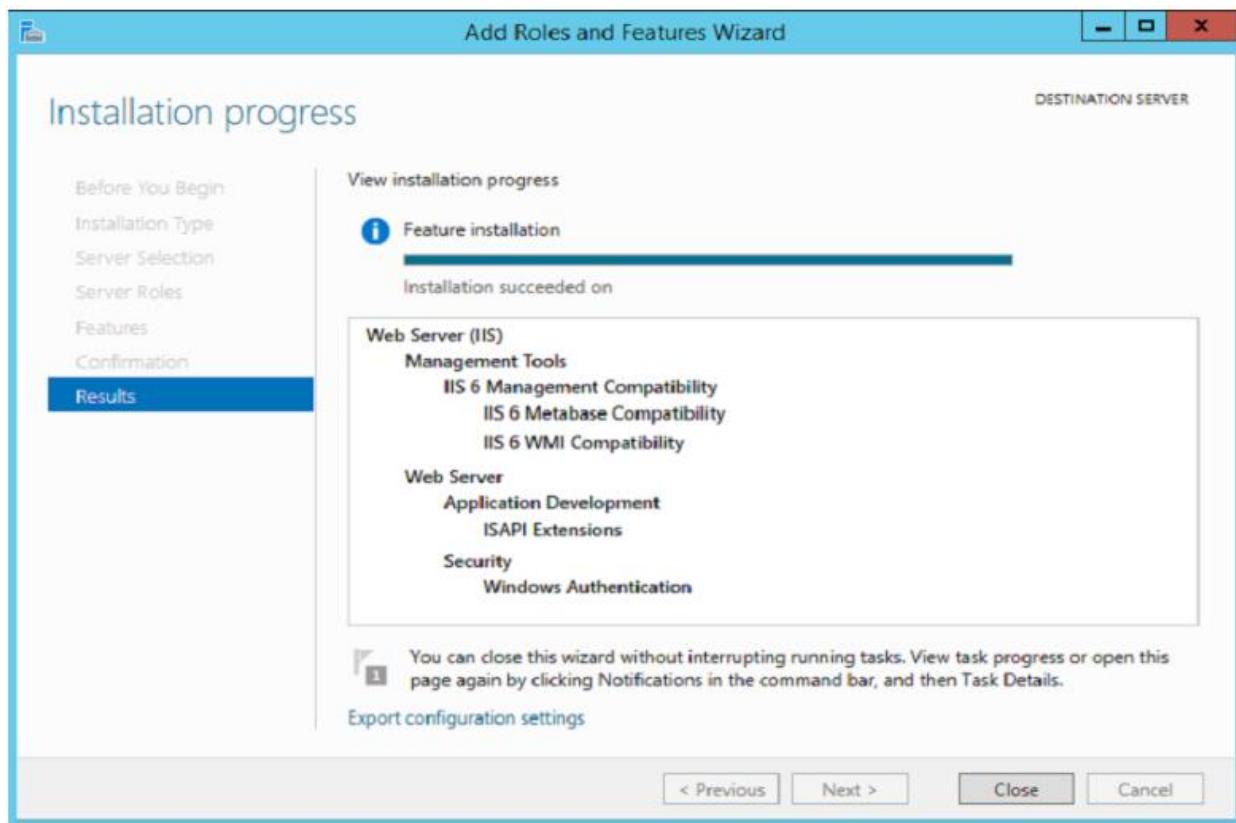
Remote Differential Compression

IIS Configuration

Application Development: ISAPI Extensions

Security: Windows Authentication

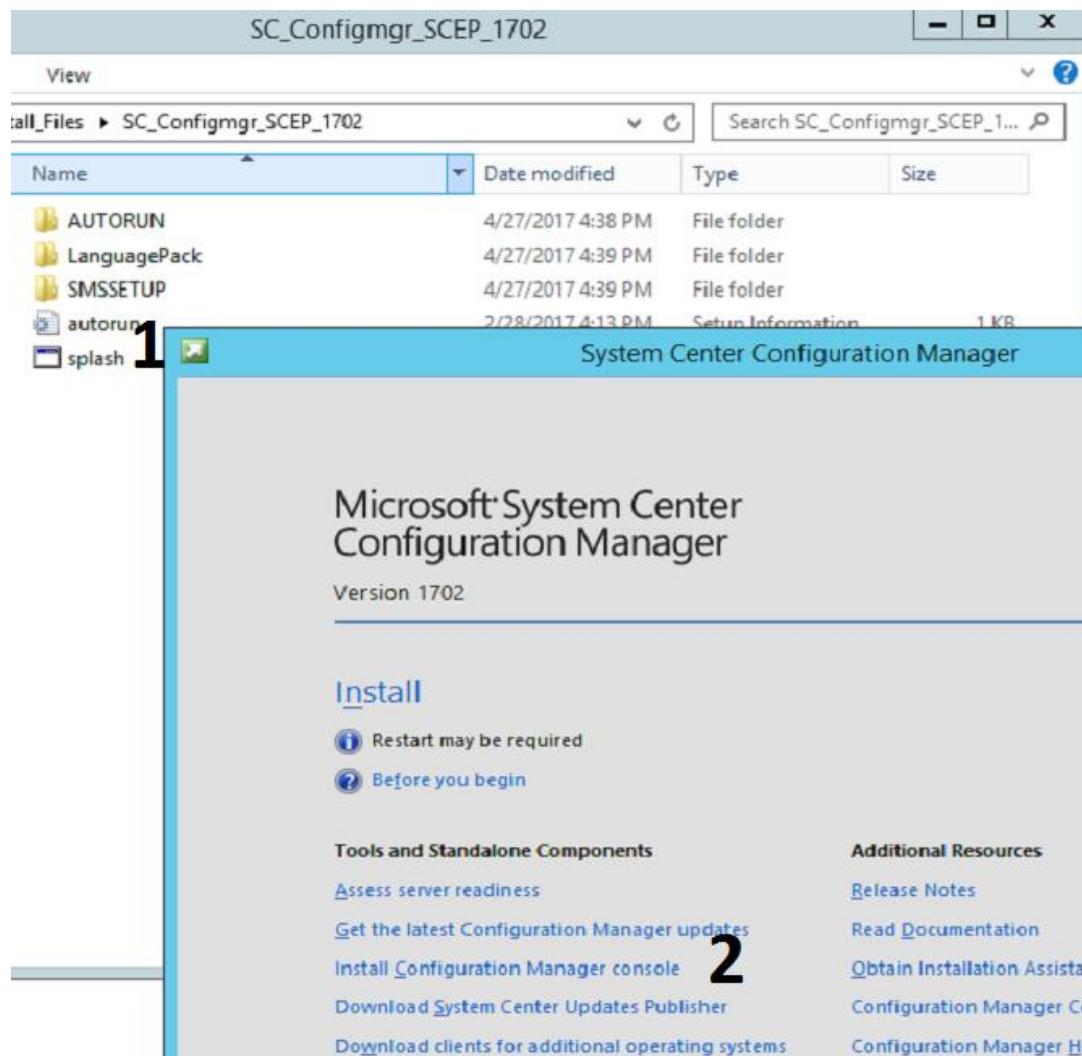
IIS 6 Management Compatibility: IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility.



WDS/PXE

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.

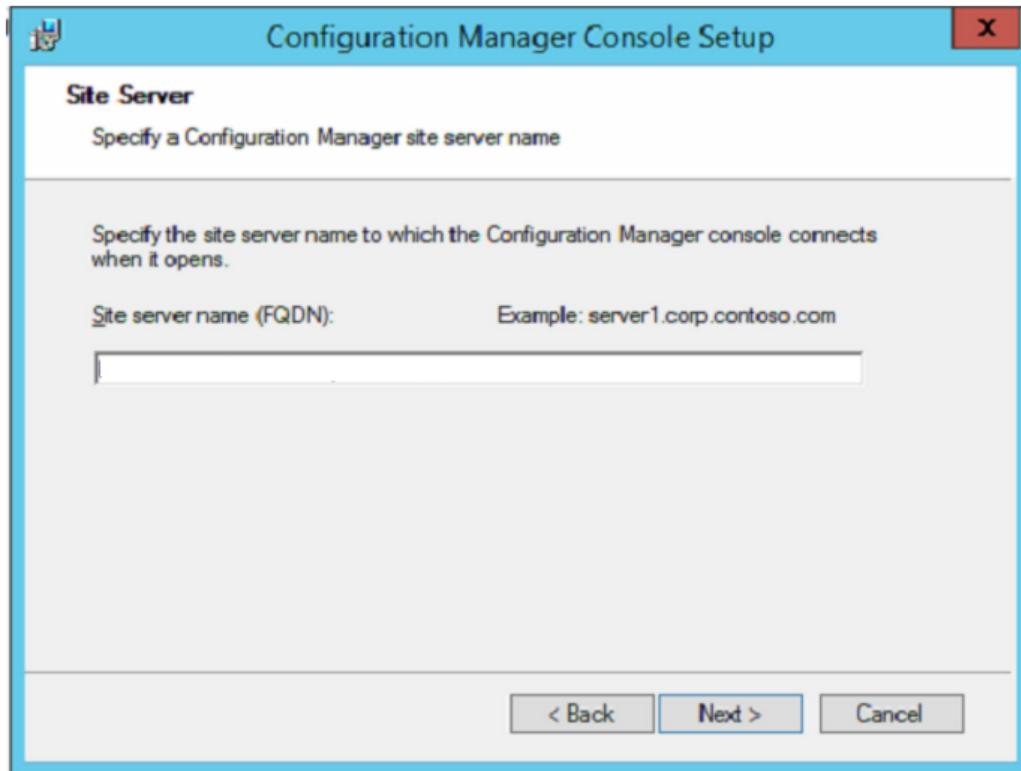
Now, extract the SCCM files and begin the SCCM installation by selecting **Install Configuration Manager console**.



Select **Next**.

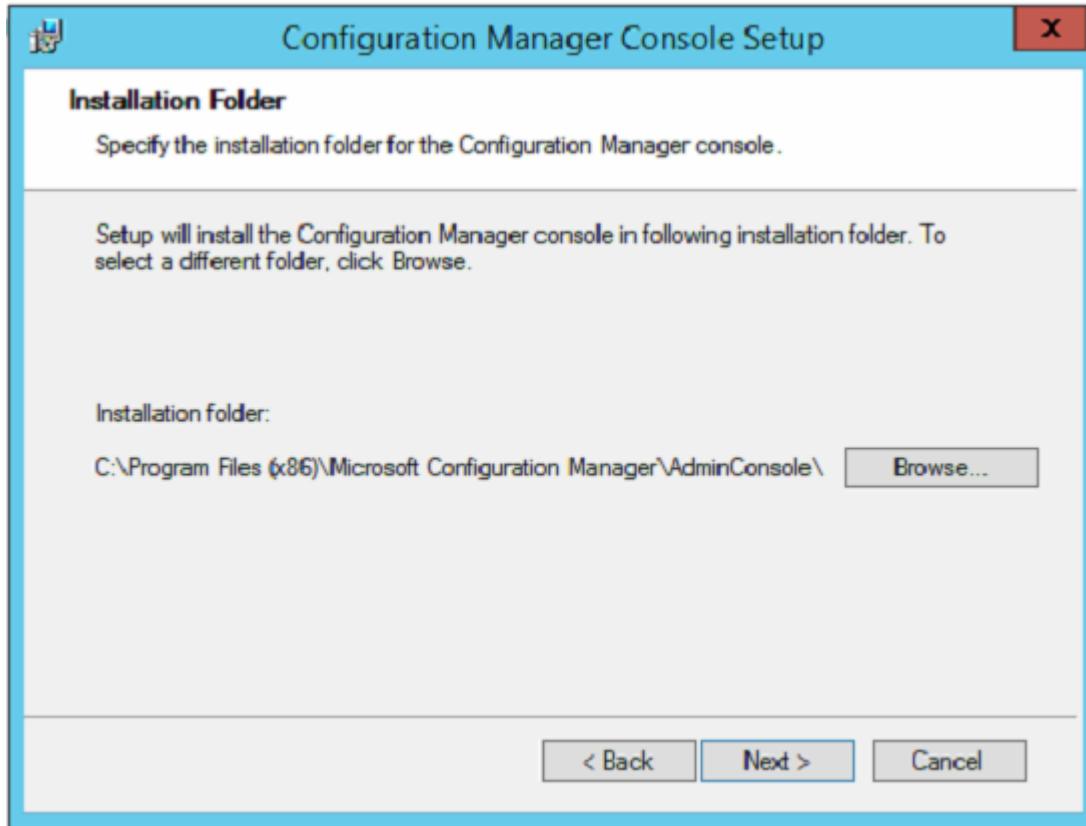


Enter Primary server FQDN, then click **Next**.

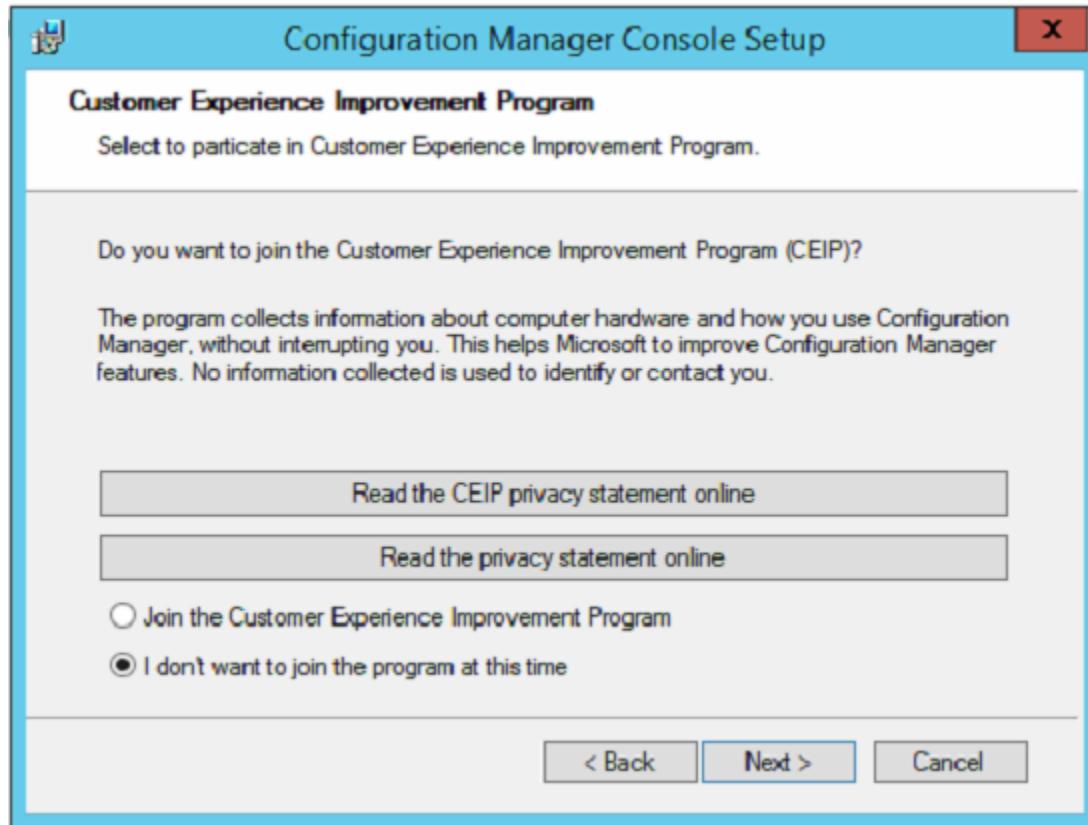


I do recommend installing the Configuration Manager on a different drive than your boot/system drive, if the environment permits; but for a lab, this is fine.

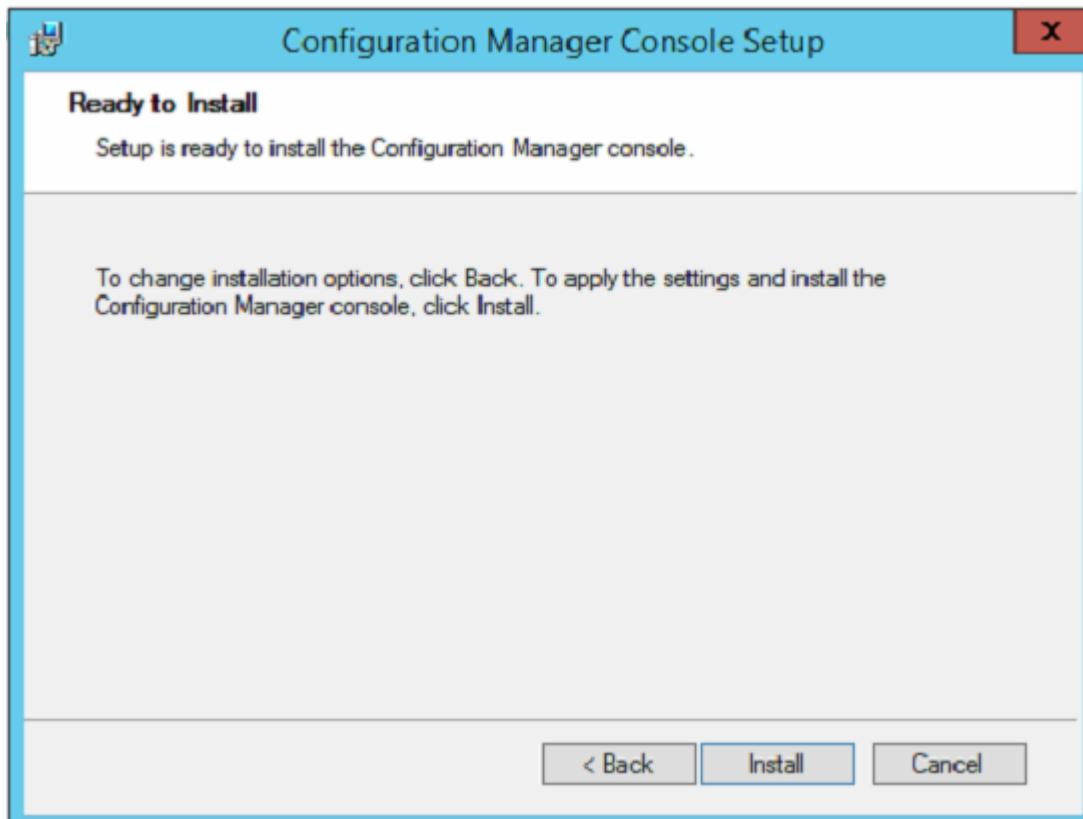
Click **Next**.



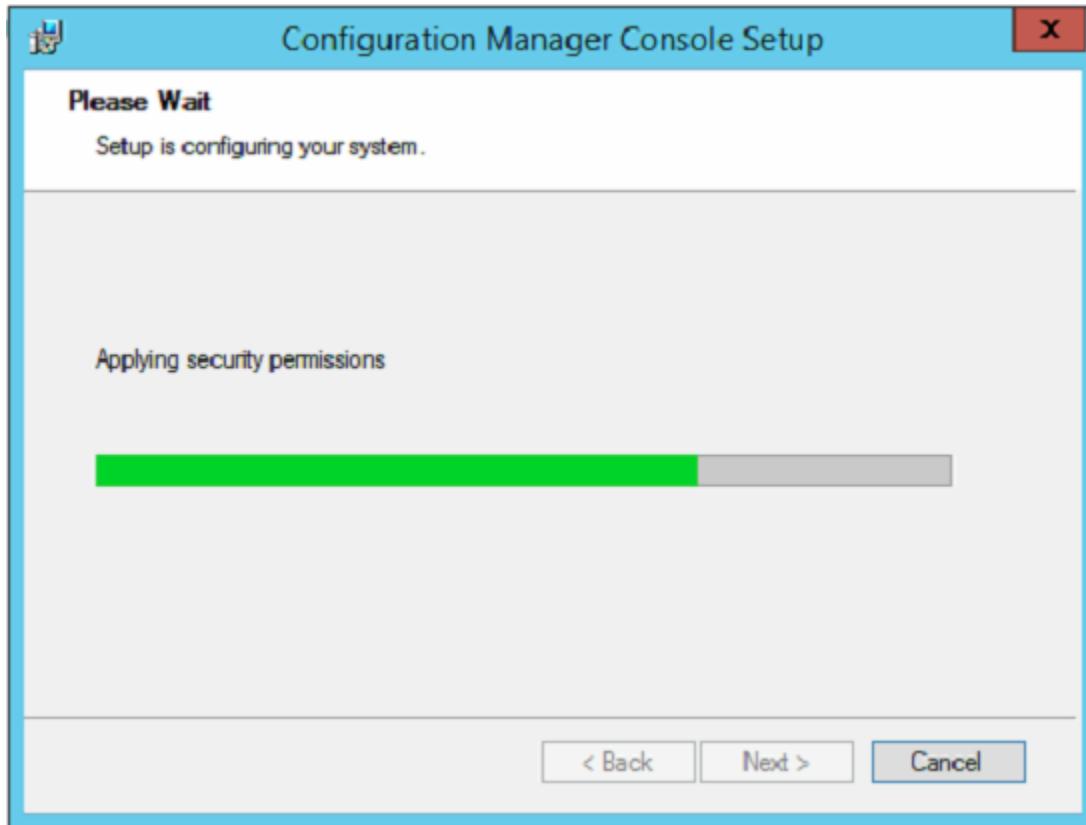
Click **Next**.



Click **Install**.



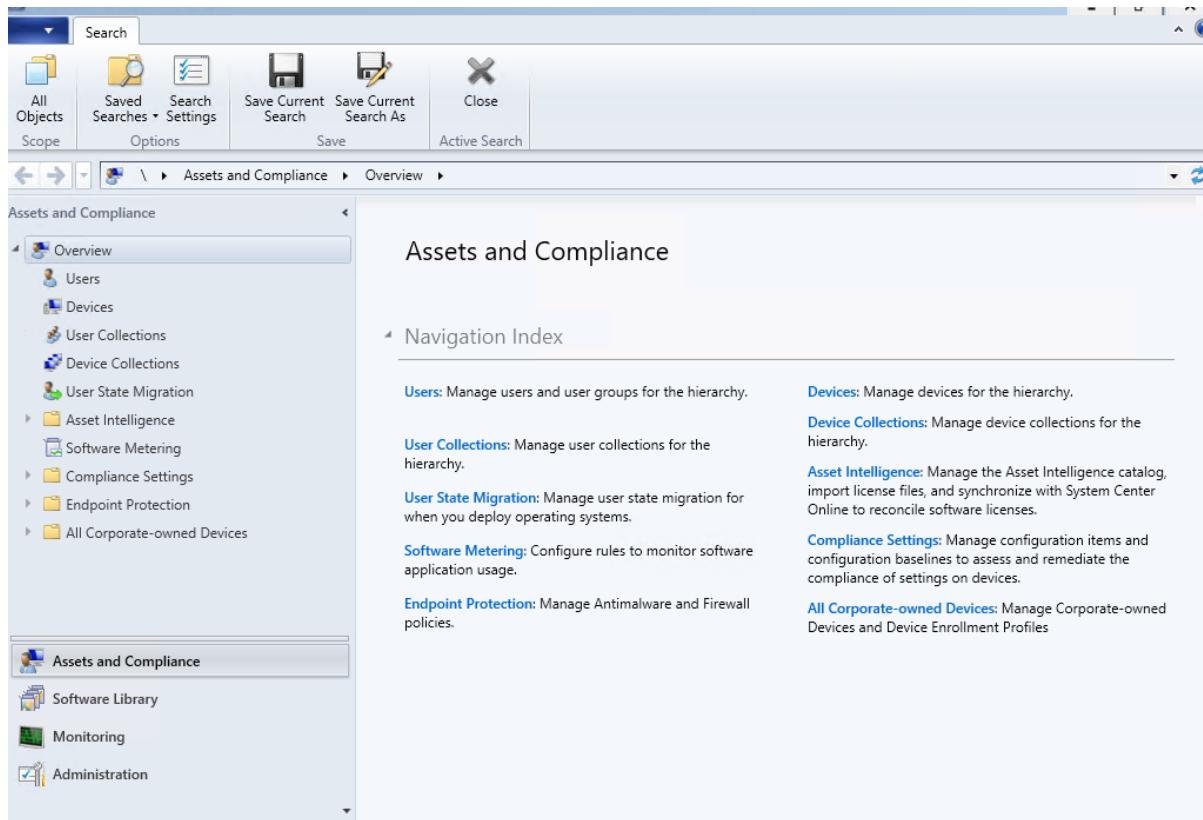
The CM will install.



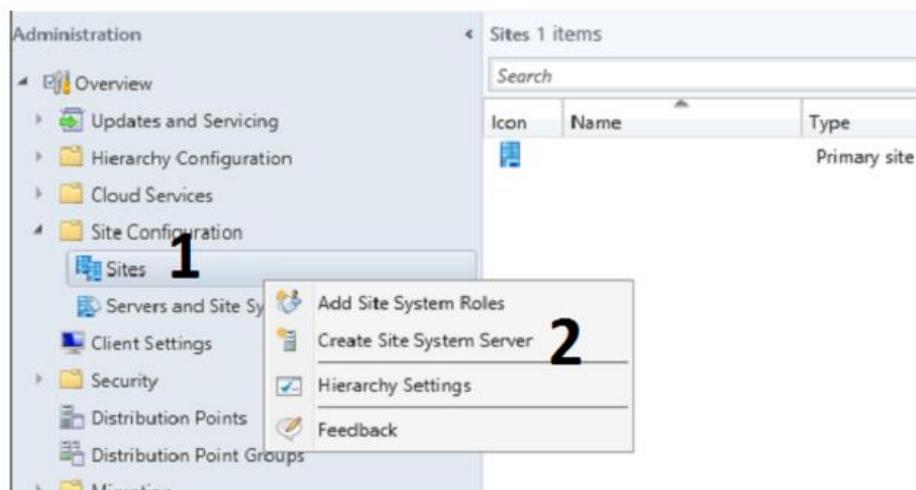
Click **Finish**.



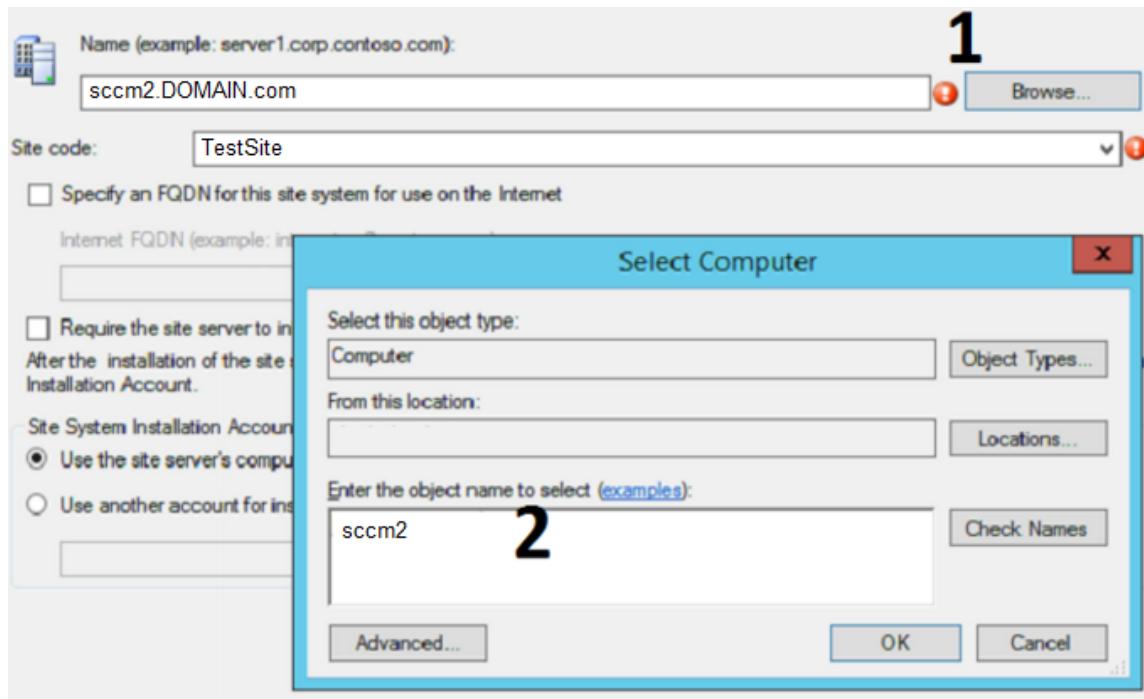
The SCCM Console will load.



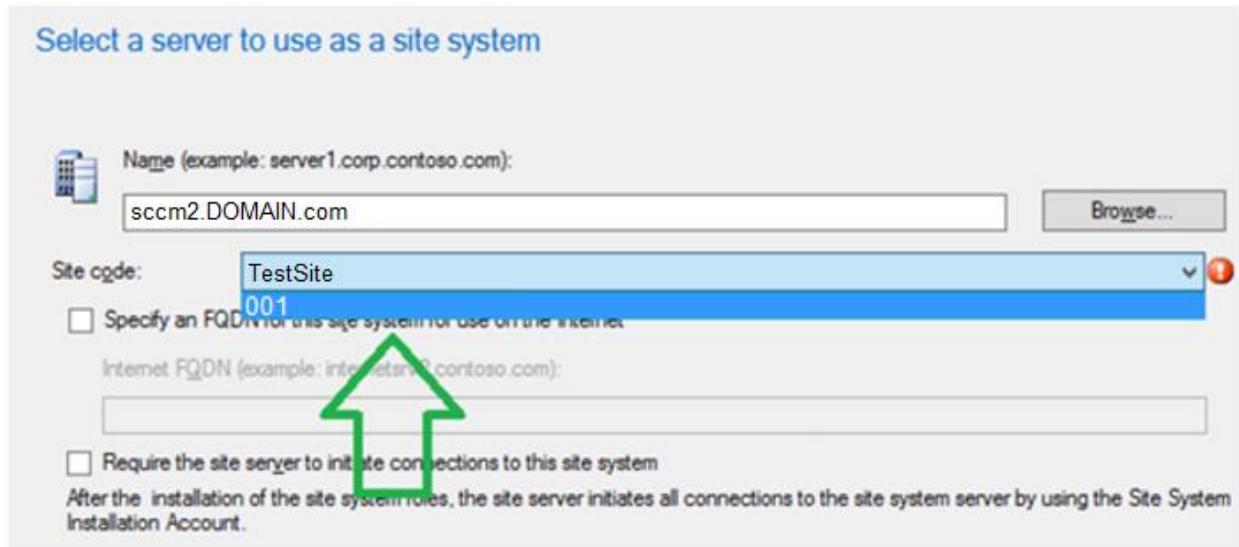
In the console, navigate to **Administration > Overview > Site Configuration**. Right-click on **Sites** and select **Create Site System Server**.



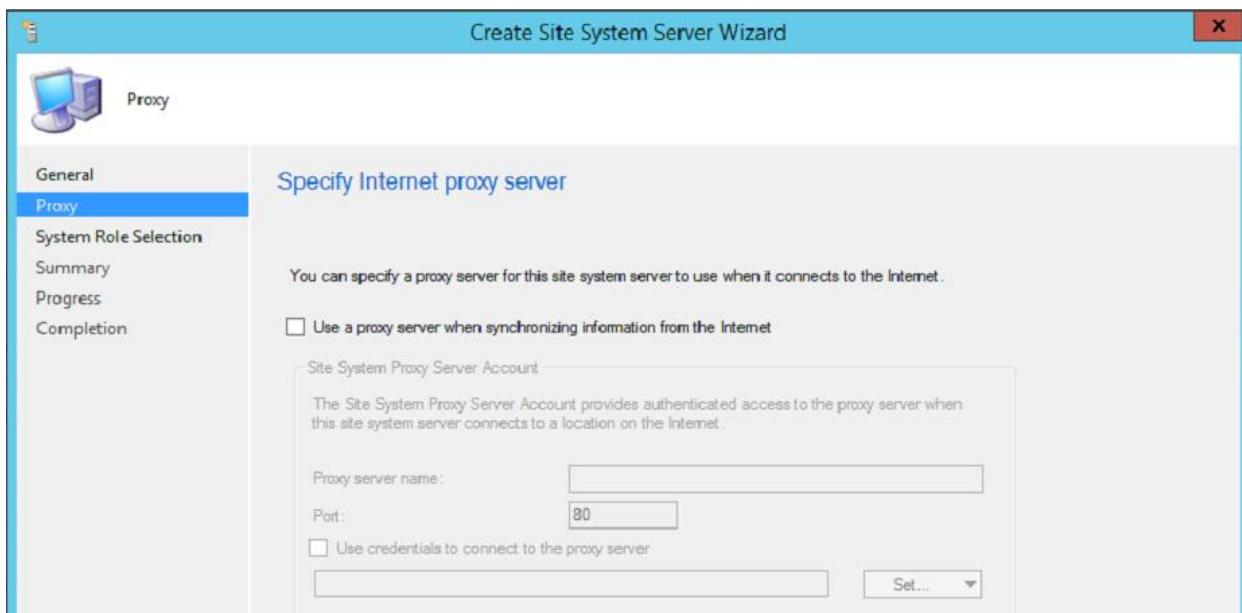
In the **Create Site System Server Wizard**, click **Browse** and select the **server name** on which the DP role is to be installed.



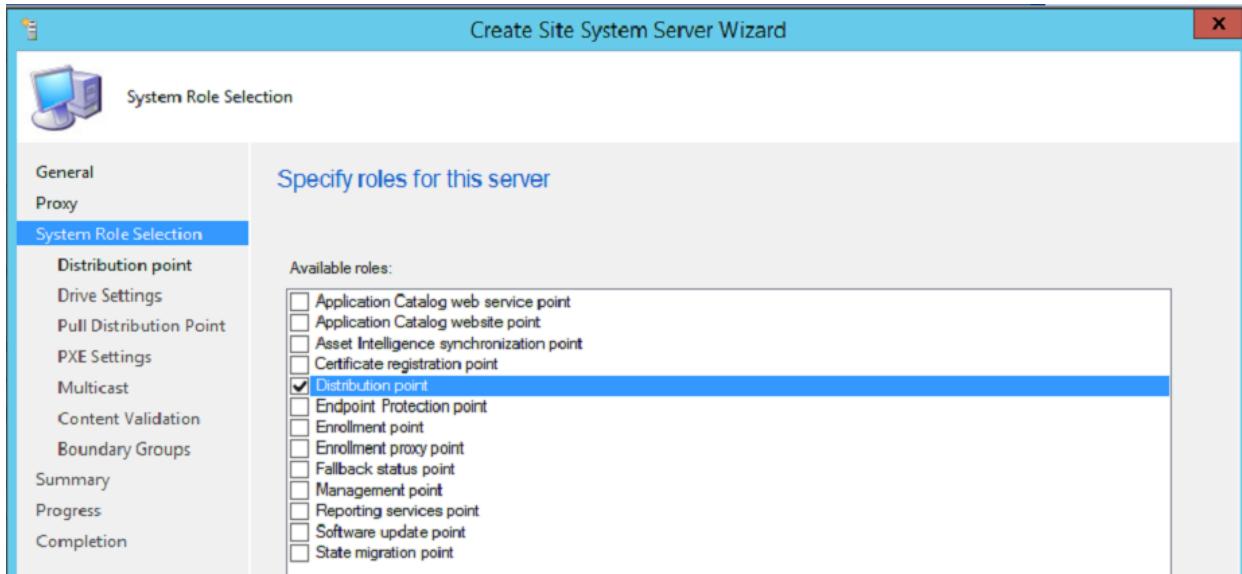
Select the **Site code** and then click **Next**.



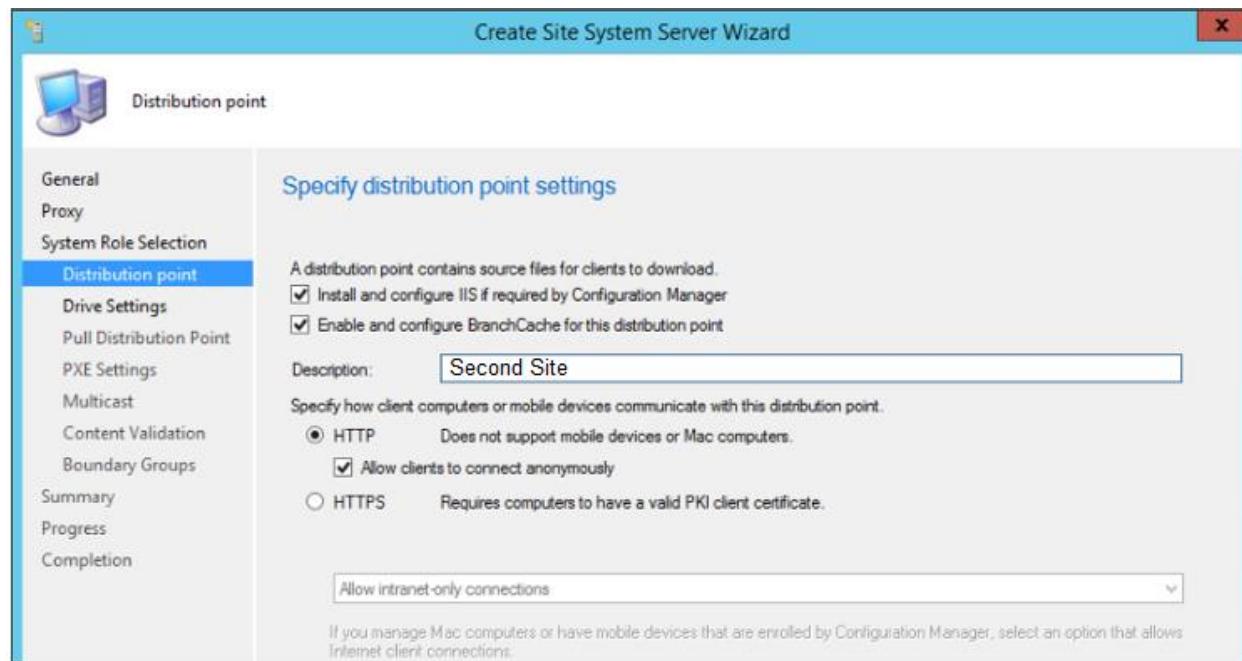
Click **Next**.



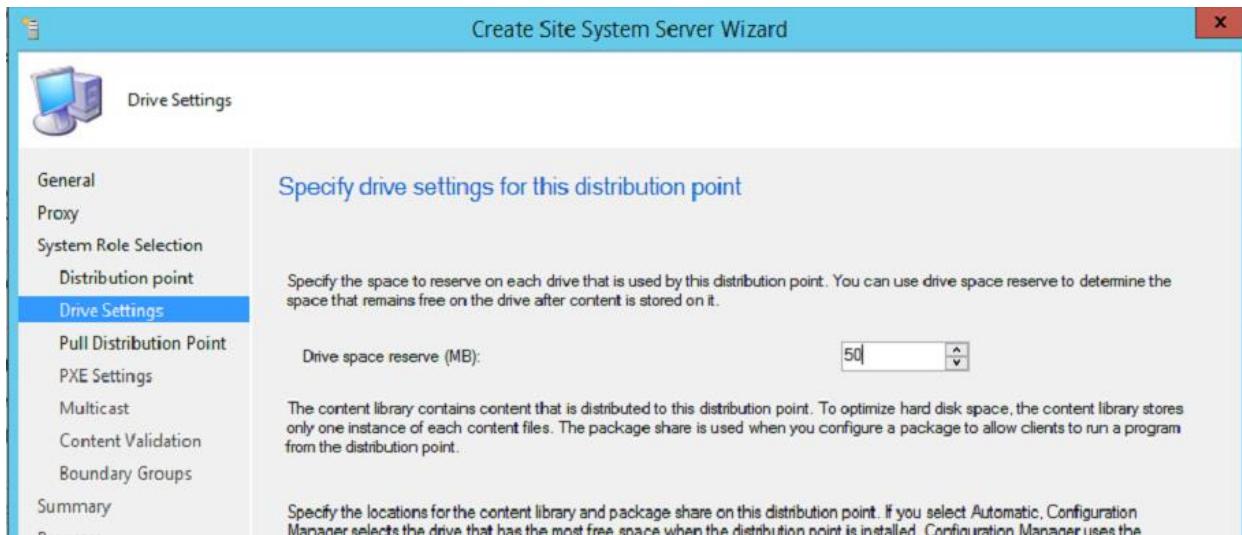
Check the **Distribution point** role, and then click **Next**.



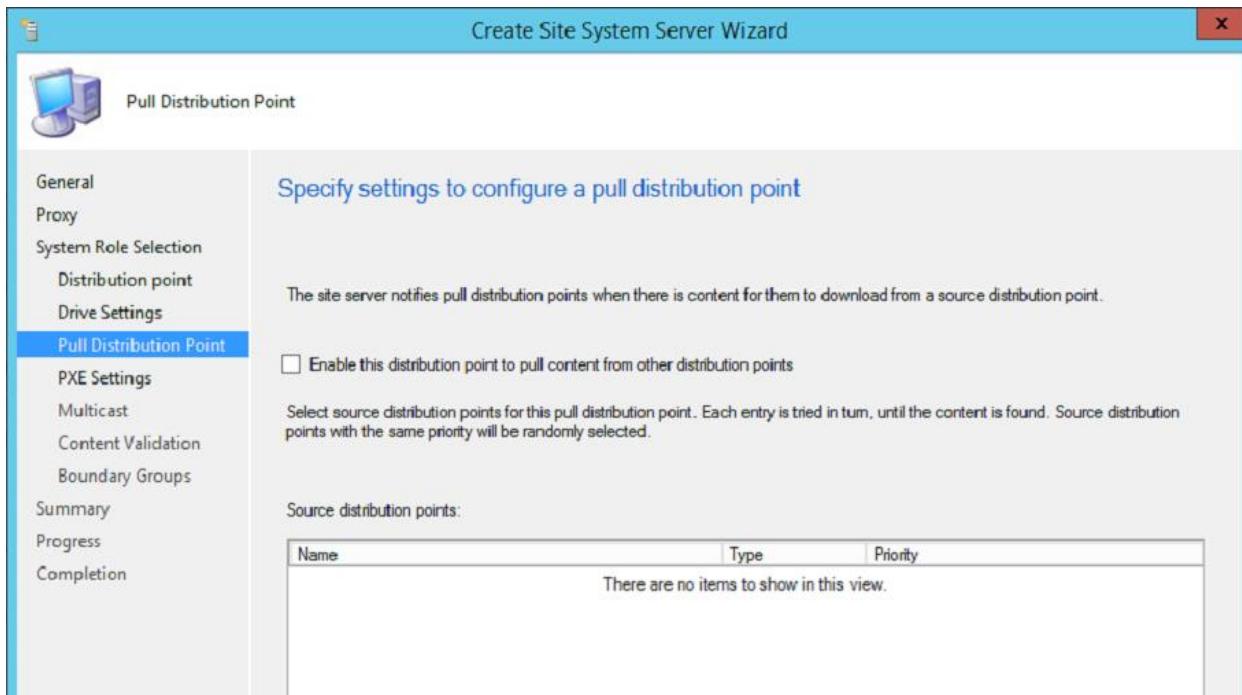
Configure the **distribution point settings**, and then click **Next** to continue.



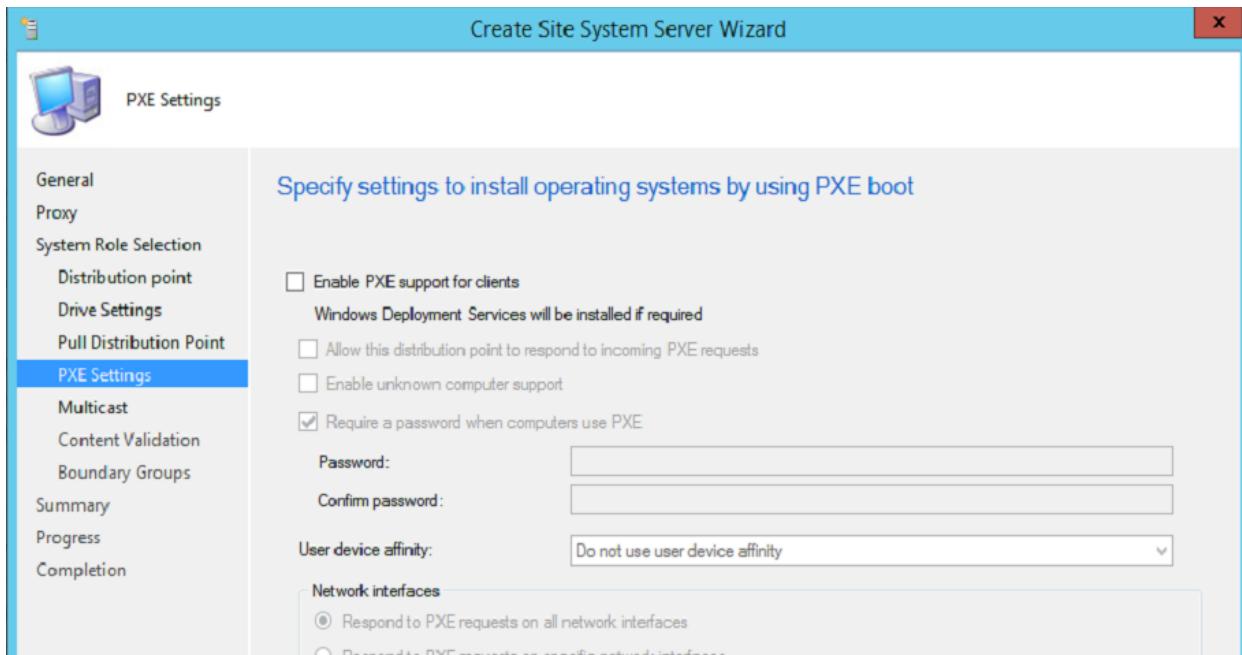
Click **Next**.



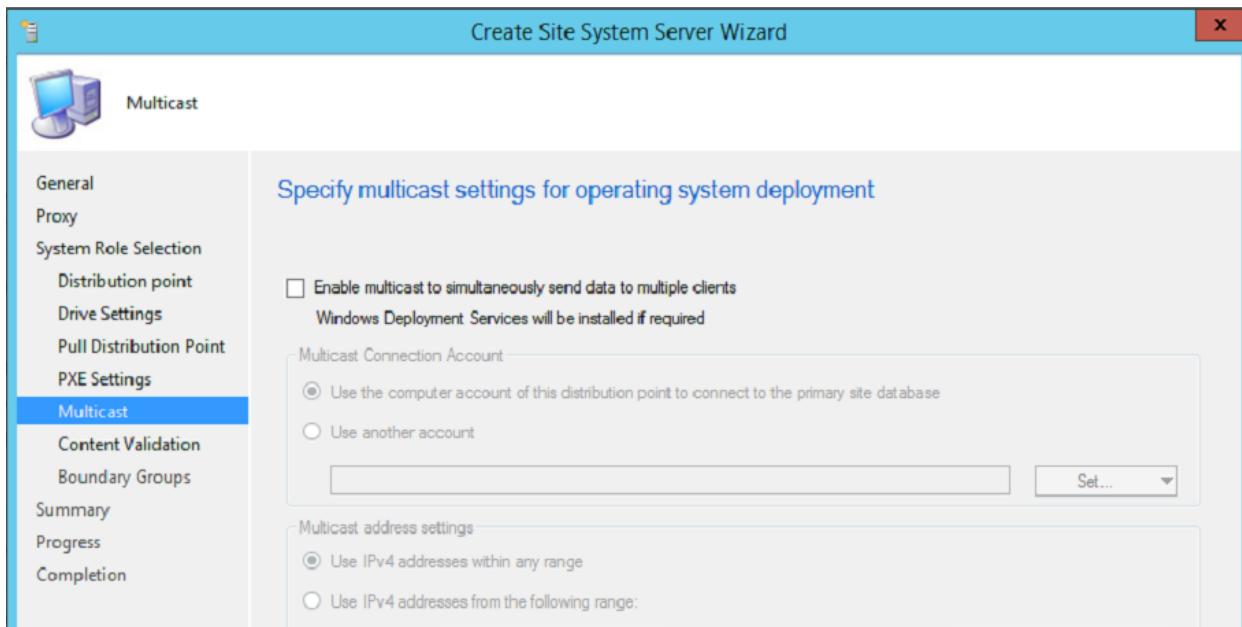
Click **Next**.



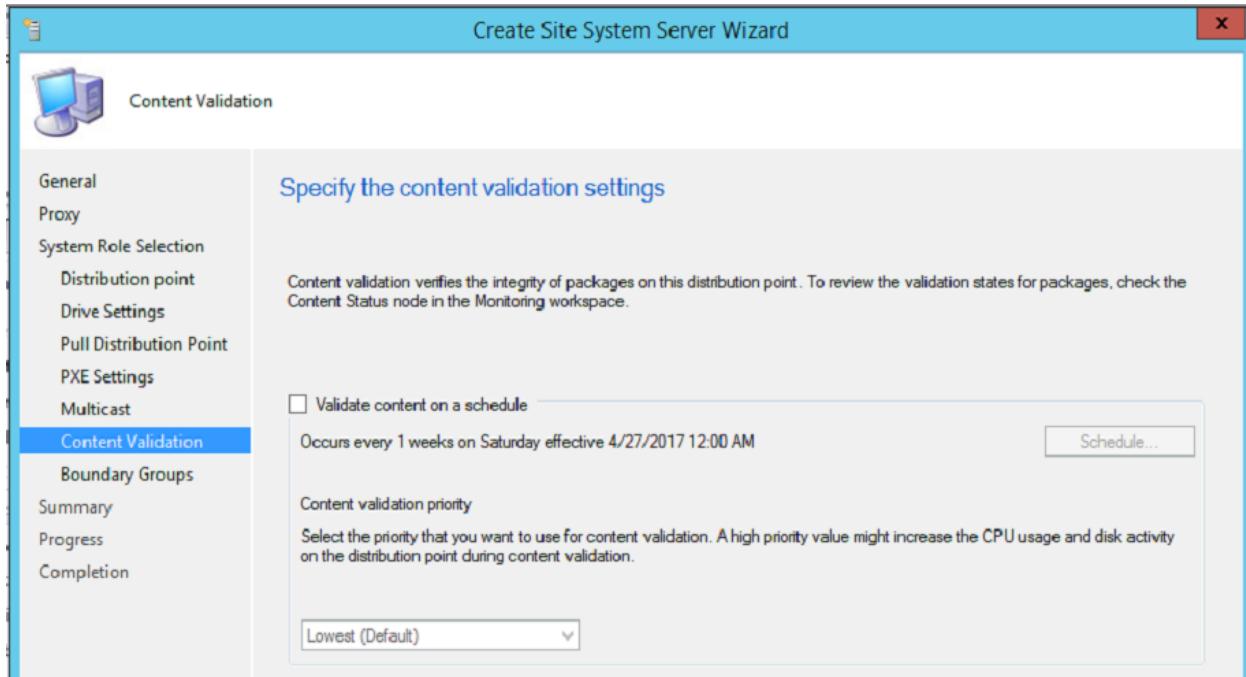
Click **Next**.



Click **Next**.



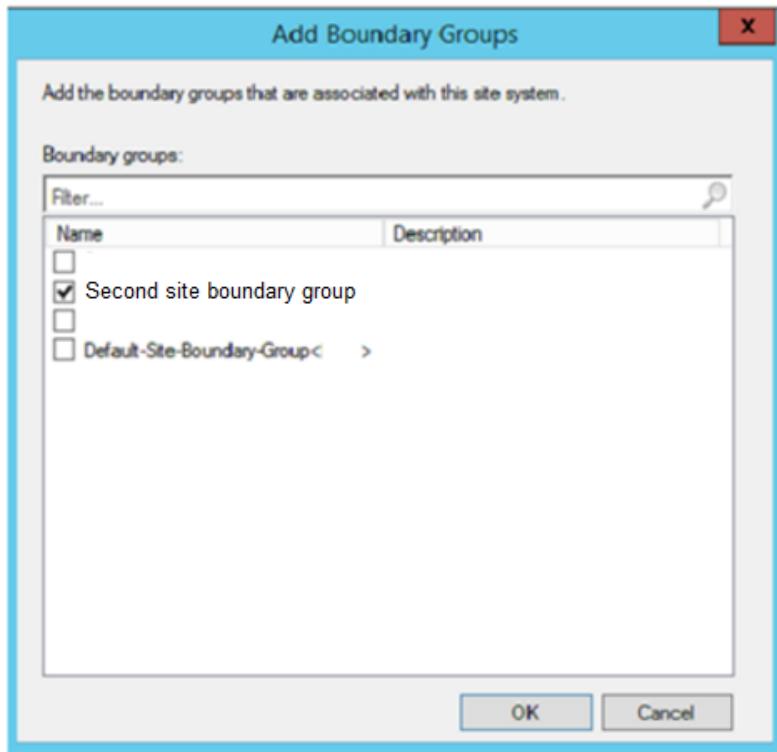
Click **Next**.



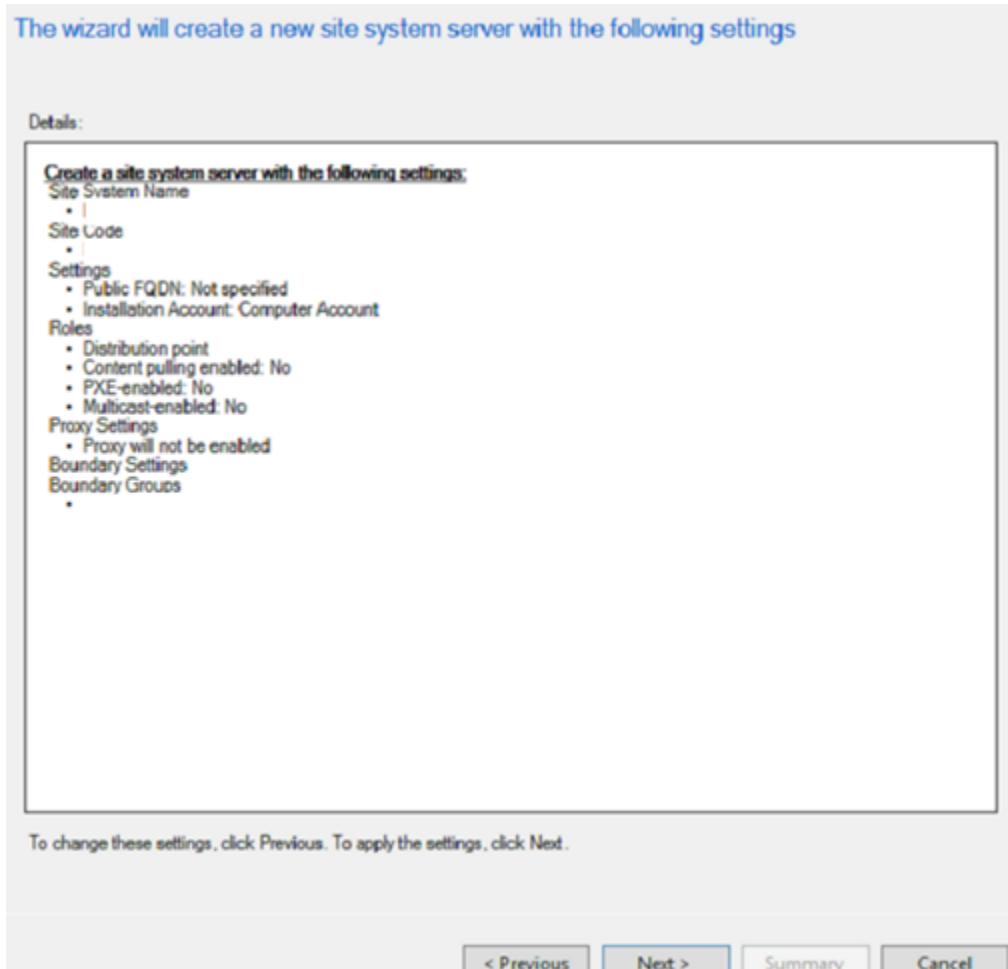
Add the **Boundary Group** for the location. Click **Add**, and select the appropriate **boundary group**.

The screenshot shows a management interface for boundary groups. A message at the top states, 'You can associate a site system role to a boundary group.' Below this, another message says, 'During content deployment, clients in a boundary group that is associated with this site system will use it as a source location for content.' A section titled 'Boundary groups:' is shown with a table. The table has columns for 'Name' and 'Description'. A search bar and filter input are at the top of the table area. The message 'There are no items to show in this view.' is displayed. At the bottom of the interface are three buttons: 'Create...', 'Add...', and 'Remove'.

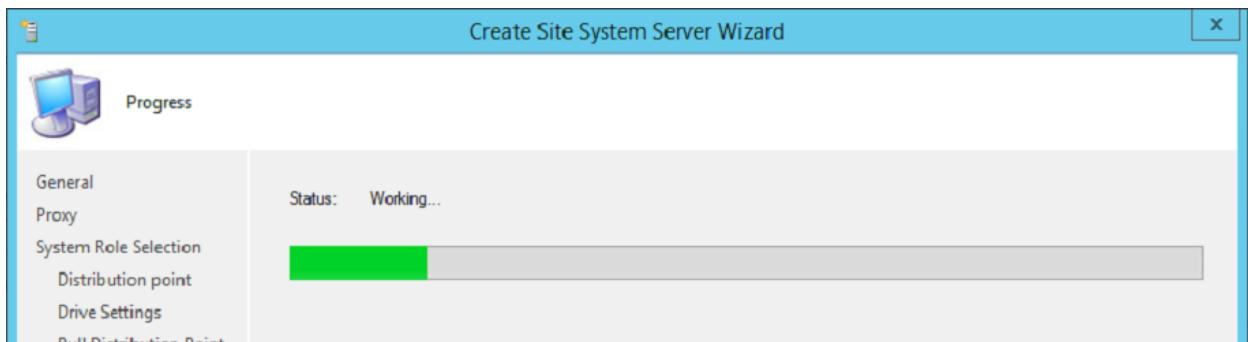
Click **OK**.



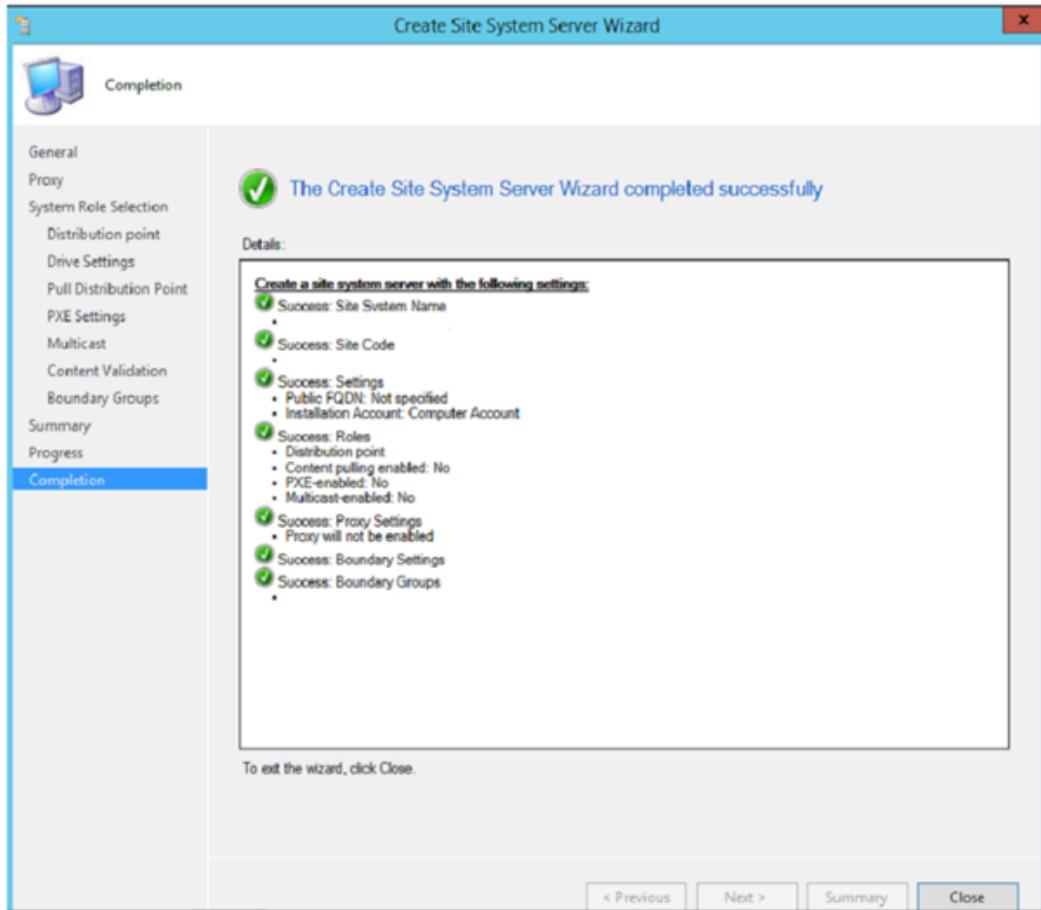
The wizard will show the summary. Click **Next**.



Status will show Working...



Completion is displayed. Click **Close**.

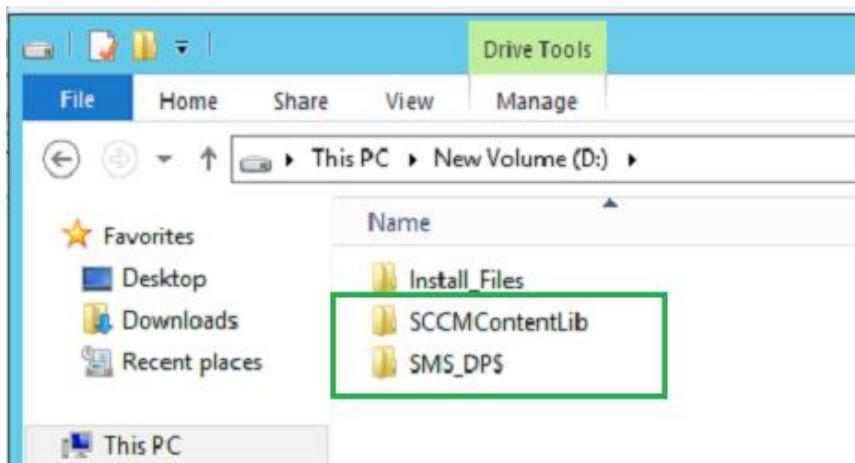


Verify that the **distribution point** is working by looking at **Site Status** under **Monitoring**. You want white check marks on green.

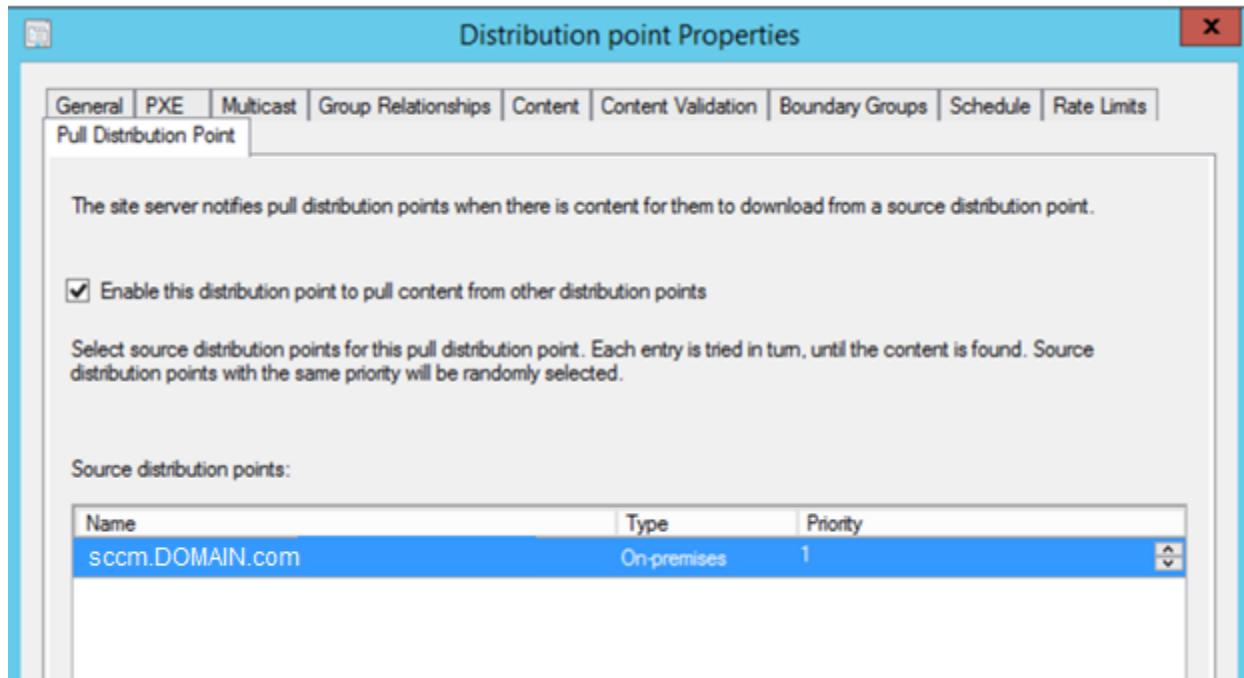
The screenshot shows the SCCM Site Status monitoring interface. On the left, there's a navigation tree with items like Overview, Alerts, Queries, Reporting, Site Hierarchy, System Status (which is selected), Site Status (selected), Component Status, and Conflicting Records. On the right, a table titled 'Site Status 10 items' lists various site systems and their roles. One row for 'sccm2.DOMAIN.com' is highlighted with a green border and a large number '2' next to it, indicating it is a Distribution point. The table columns are: Icon, Status, Site System, and Site System Role. The status column shows green checkmarks for all items.

Icon	Status	Site System	Site System Role
✓	OK		Component server
✓	OK	sccm2.DOMAIN.com	Distribution point
✓	OK		Endpoint Protection point
✓	OK		Management point
✓	OK		Application Catalog we...
✓	OK		Site server
✓	OK		Site database server

Also check to see if the **Distribution point** folders have been generated.

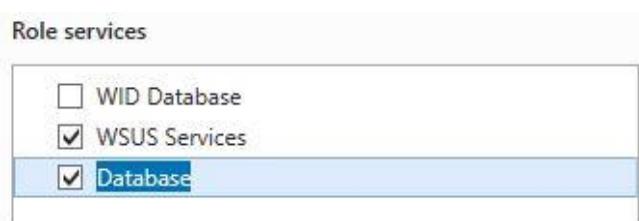


Finally, if you want this distribution point to ‘pull’ content from a primary distribution point (which in most cases you do), launch the distribution point properties and check **Enable this distribution point to pull content from other distribution points**. The source distribution point should be the primary server.

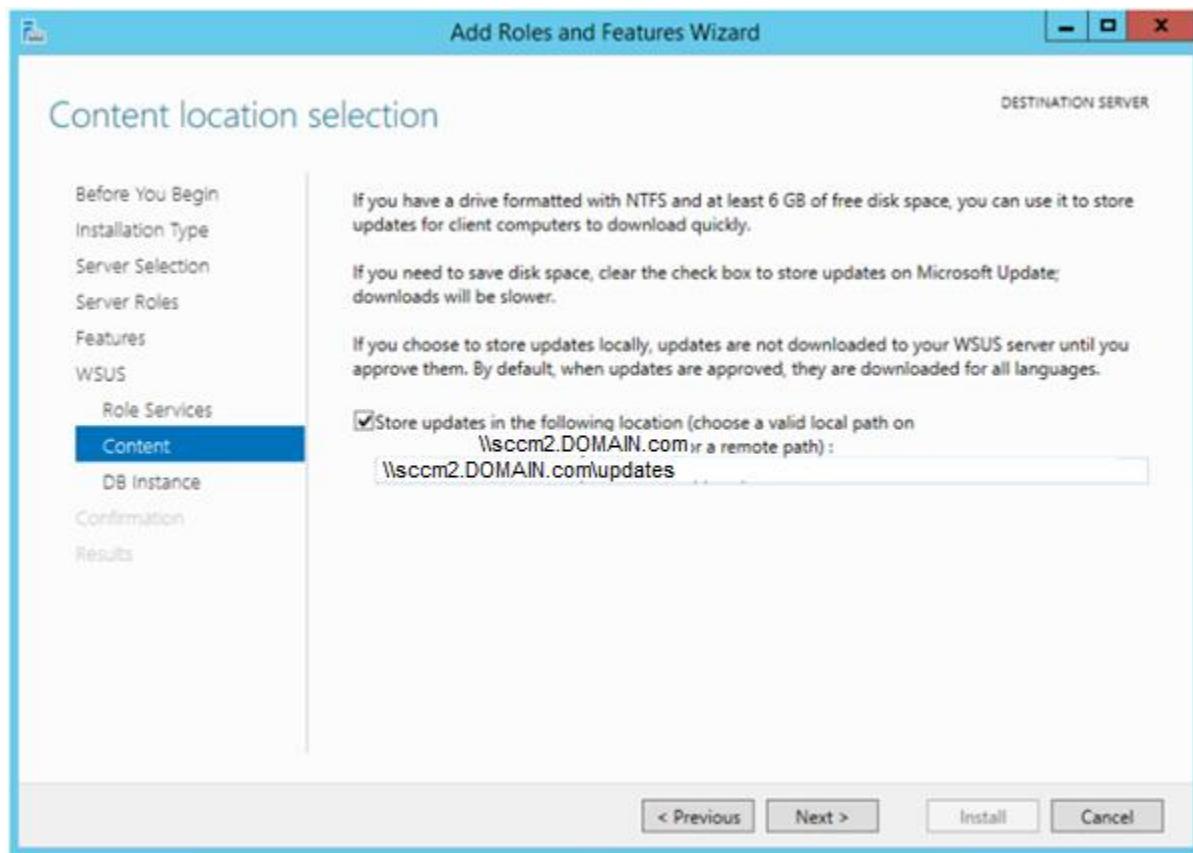


Set up a WSUS at another Site

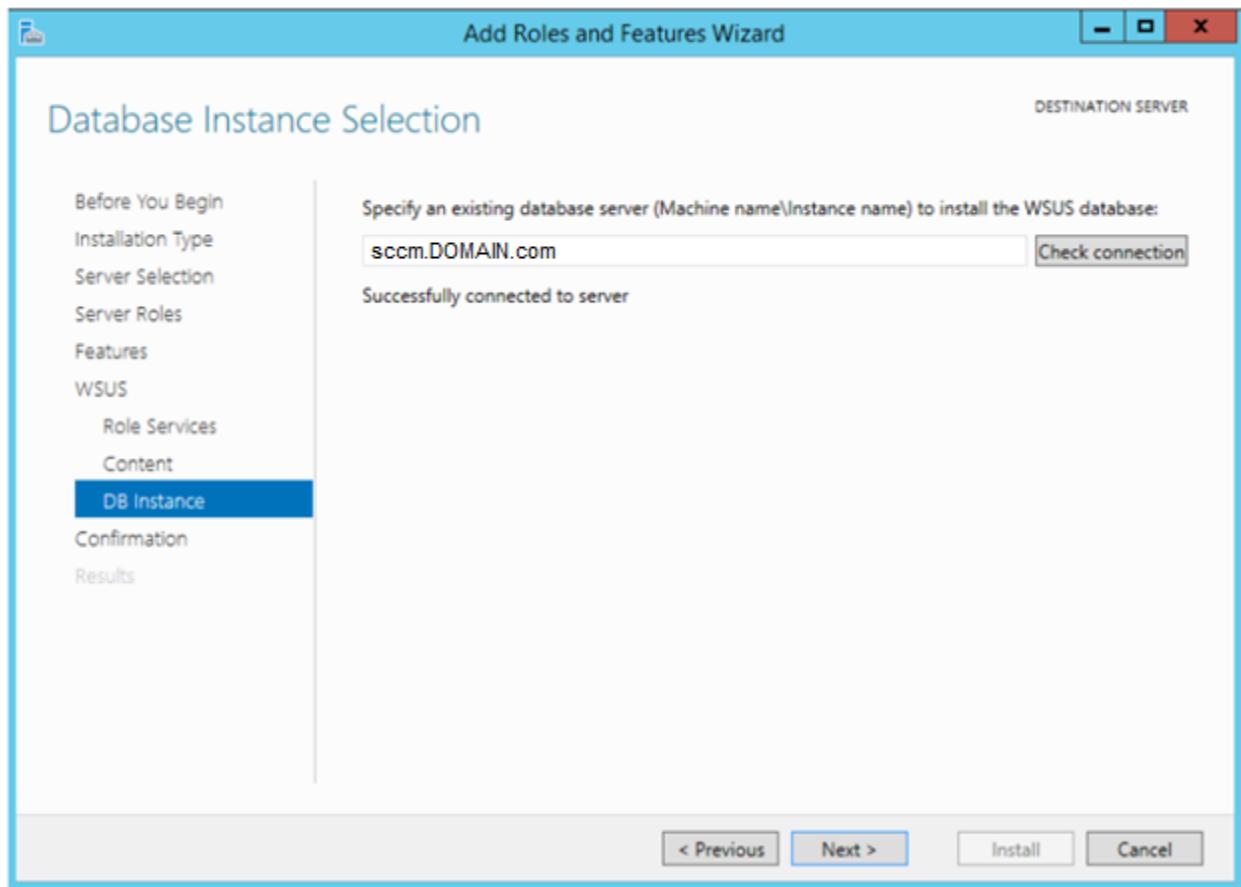
On the second server hosting the SUP role, SUP2, install **WSUS with the Database option** (no need to install SQL). Click **Next**.



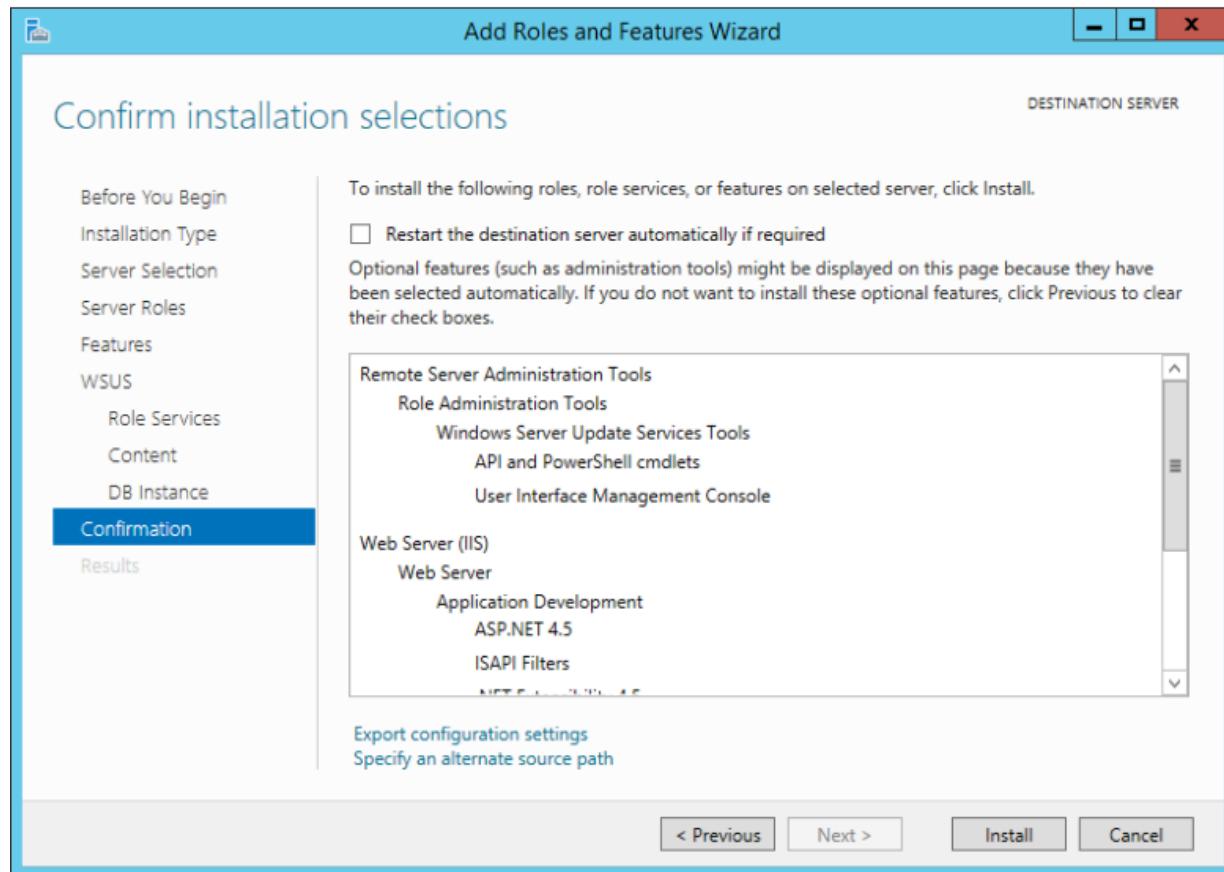
On the **Store updates** in the following location, enter the **FQDN** to the new **SUP2 server**. Click **Next**.



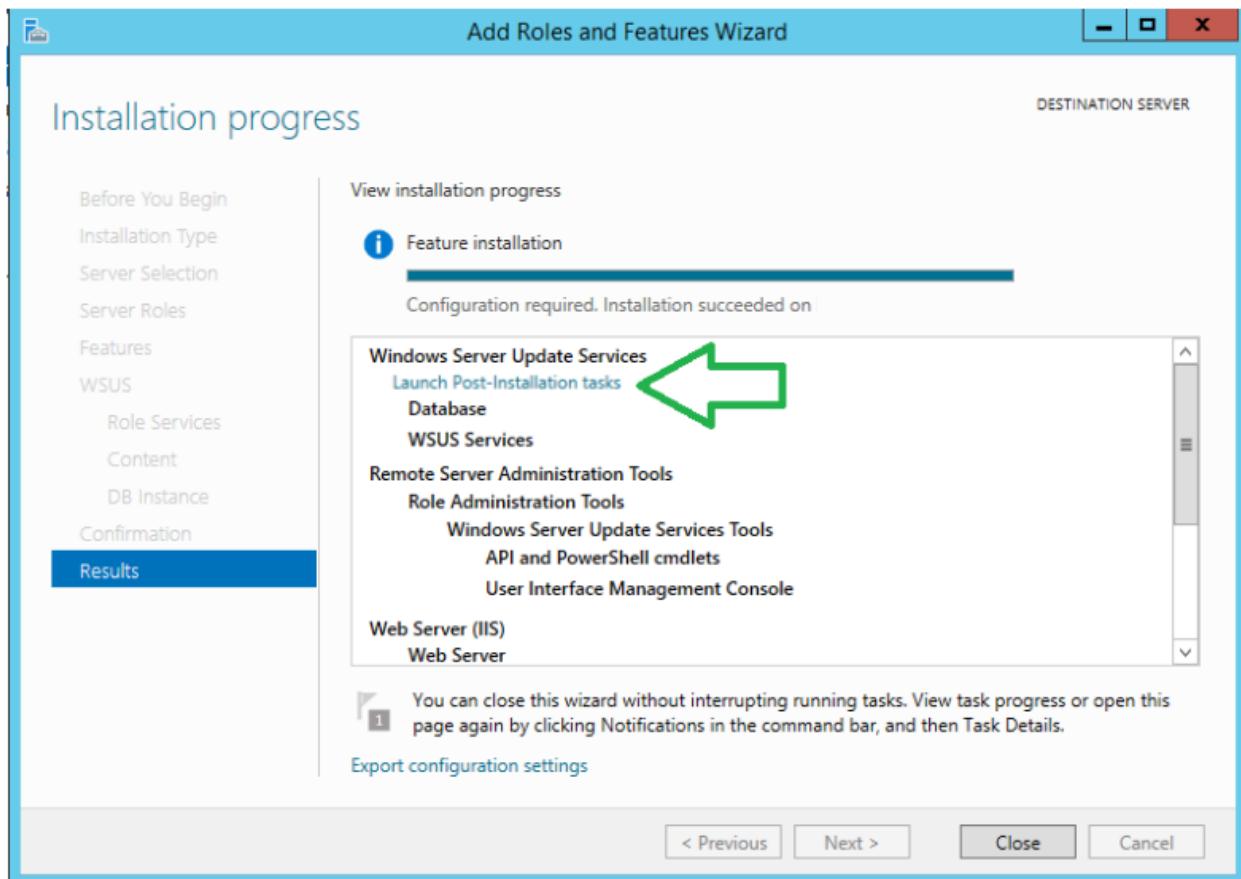
Specify the **database server** (from SUP1). Click **Check connection**. Click **Next**.



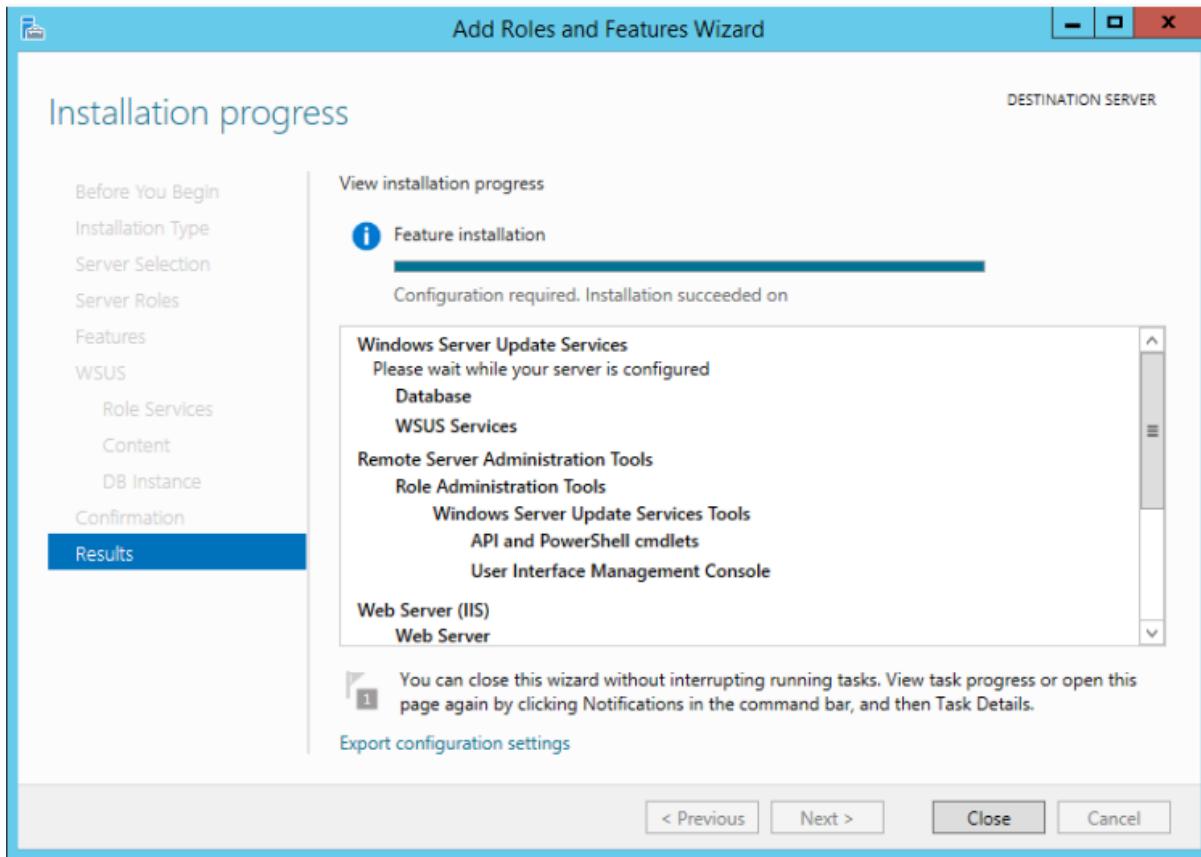
Click **Install**.



Click **Launch Post-Installation tasks**.



Once successful, click **Close**.



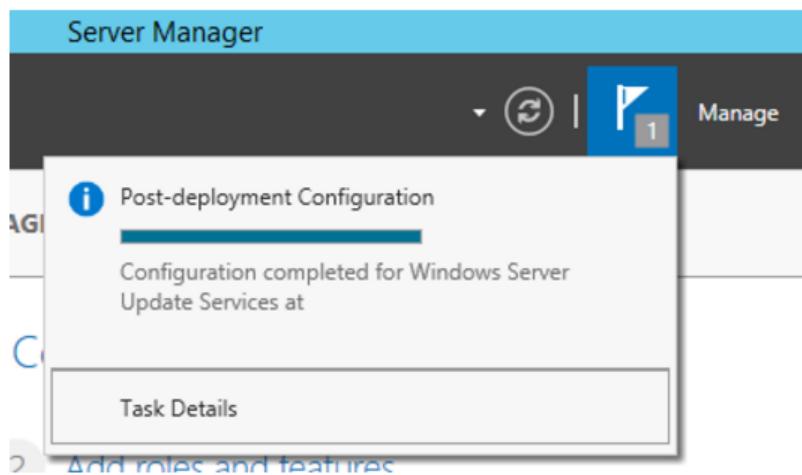
If there are no errors, skip down to **Install the SCCM SUP**.

If you see another **Configuration required** --- remove the SUP role (if it exists) from the second server, and look at the steps below.

On the second server, launch the WSUS services from **Server Manager Dashboard > Tools** and enter the FQDN for the second WSUS.



At this point, you should see a **Configuration completed for Windows Updates Services at ServerName**.



If there are still errors, remove SUP, remove the WSUS service, delete the WSUS site in IIS, and reboot and start over.

Install the SCCM SUP Role

Next, install the SCCM SUP role on the second site server. Go to **Administration > Servers and Site System Roles** > right-click on **new server**, and click the **Add Site System Roles** option.

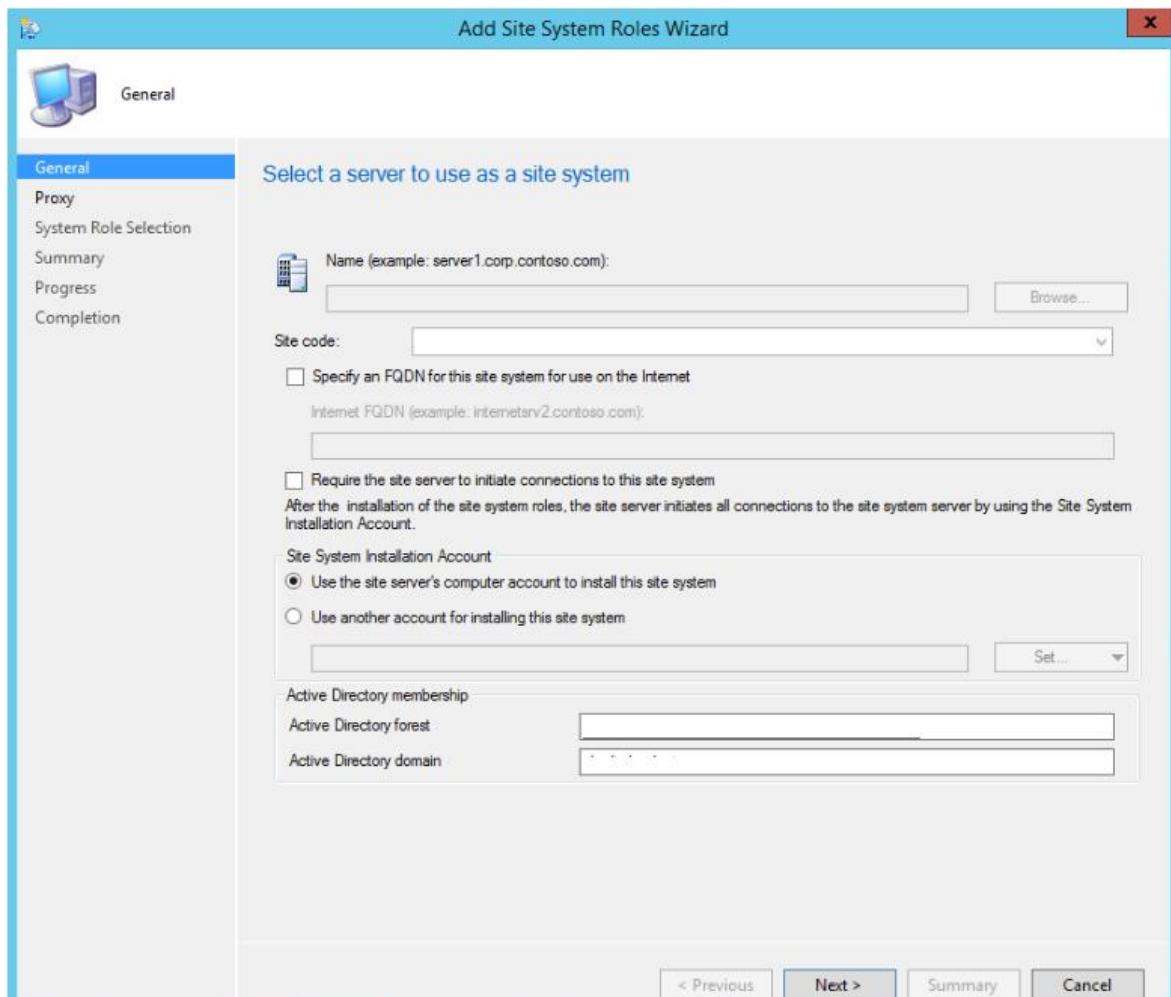
The screenshot shows the 'Servers and Site System Roles' interface in the SCCM console. At the top, there's a search bar and a table with columns: Icon, Name, Site Code, Count of roles, and Type. Two servers are listed: '\sccm.DOMAIN.com' (Site Code: 9, Primary) and '\sccm2.DOMAIN.com' (Site Code: 0, Secondary). A context menu is open over the '\sccm2.DOMAIN.com' entry, indicated by a large number '1'. The menu items are: Add Site System Roles (highlighted with a large number '2'), Start, Refresh (with F5 key), Delete (with Delete key), and Properties.

Icon	Name	Site Code	Count of roles	Type
File icon	\sccm.DOMAIN.com	9	Primary	
File icon	\sccm2.DOMAIN.com	0	Secondary	

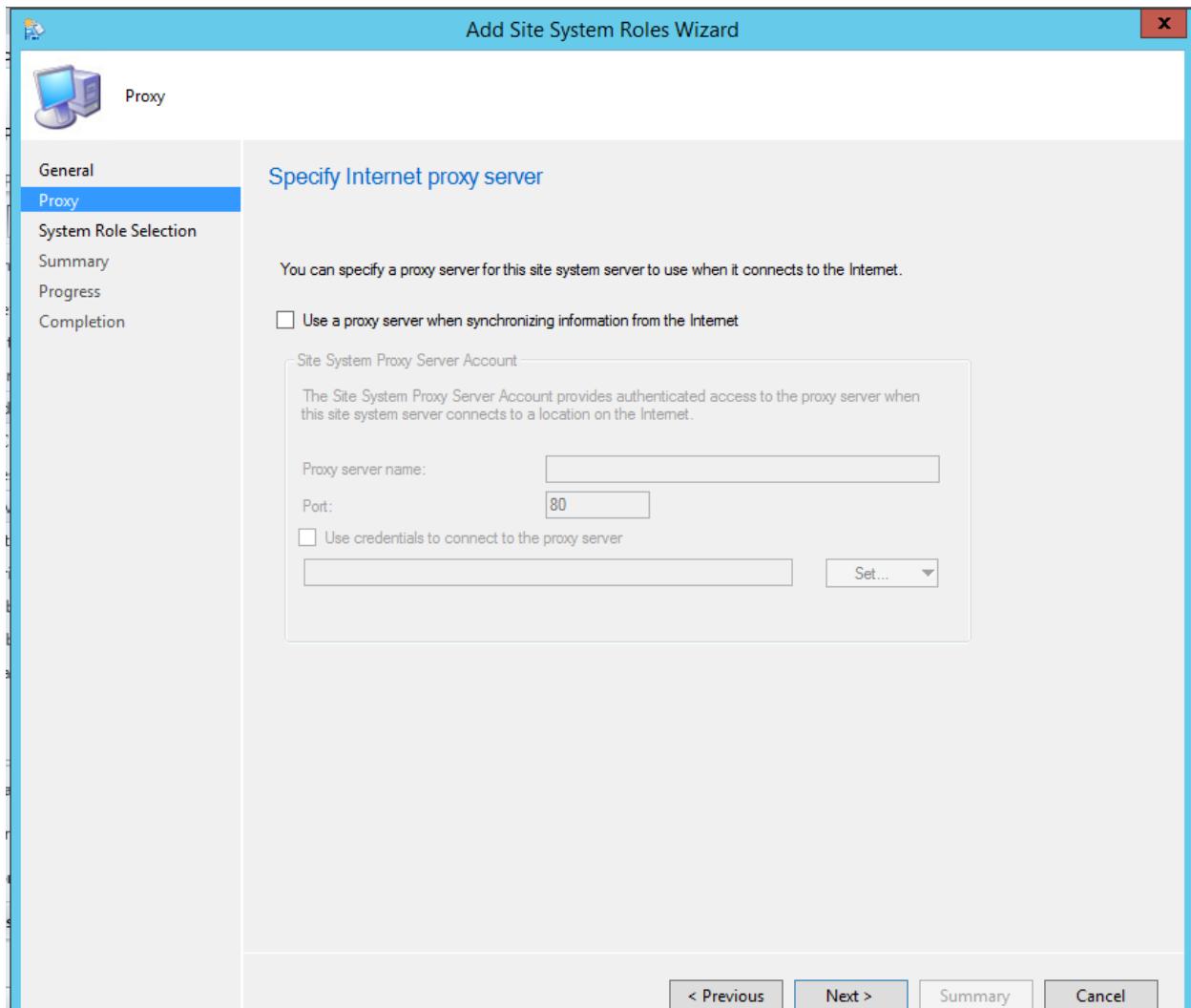
Site System Roles

Icon	Role Name	Role Description
File icon	Distribution point	A Configuration Manager server role that stages packages for distribution.
File icon	Site system	A server or server share that hosts one or more site systems.

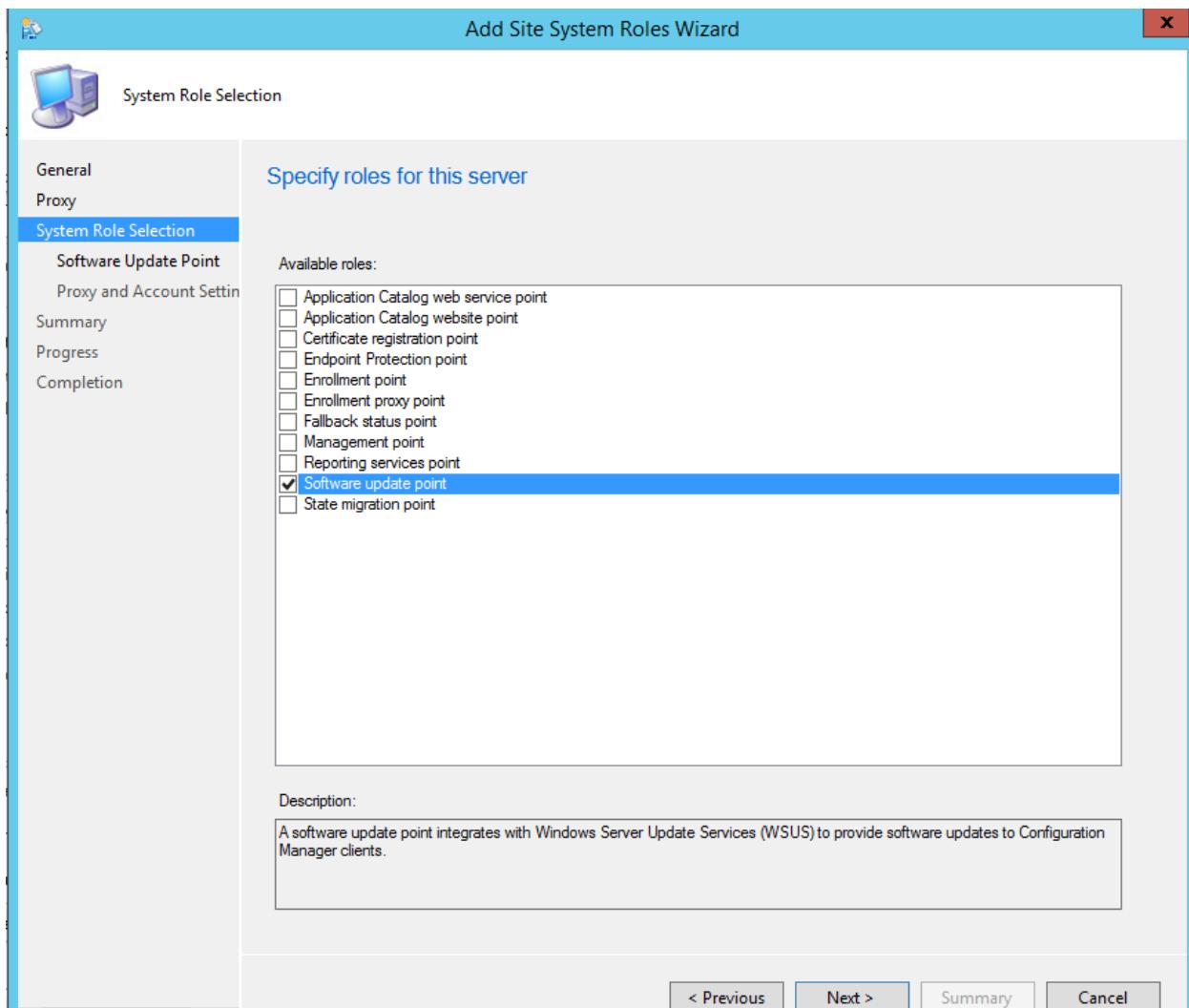
Click **Next**.



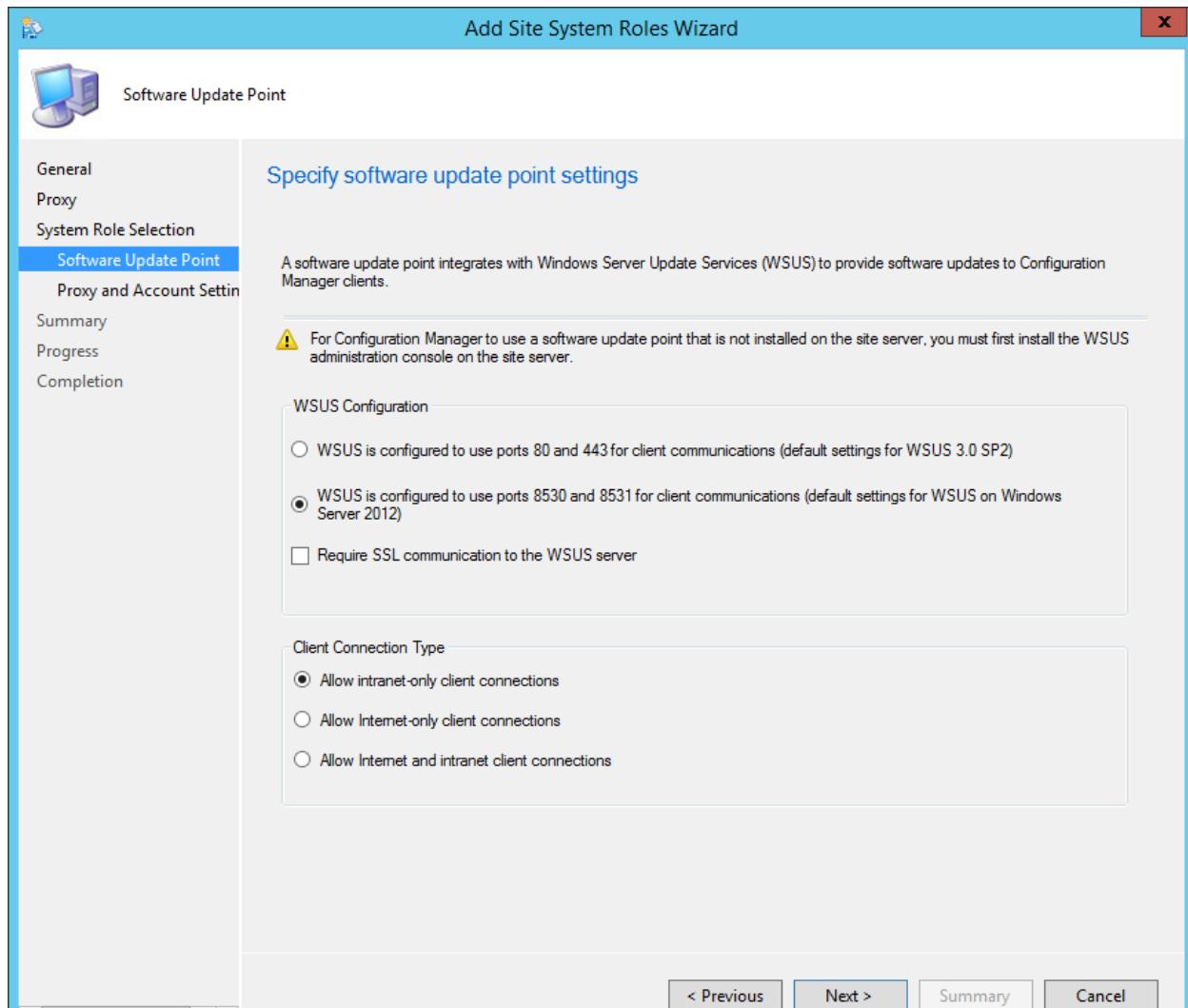
Click **Next**.



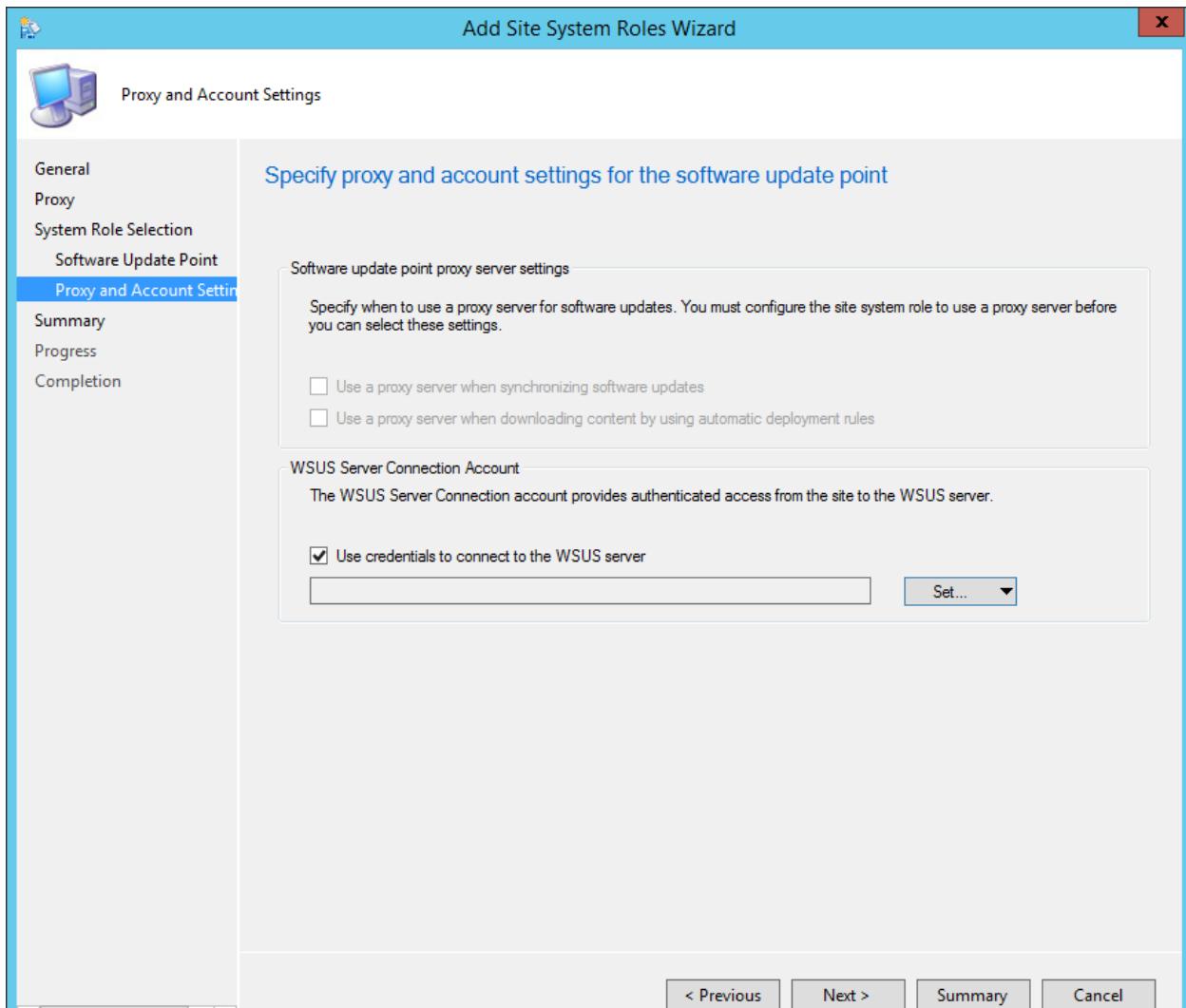
Check the **Software update point** role. Click **Next**.



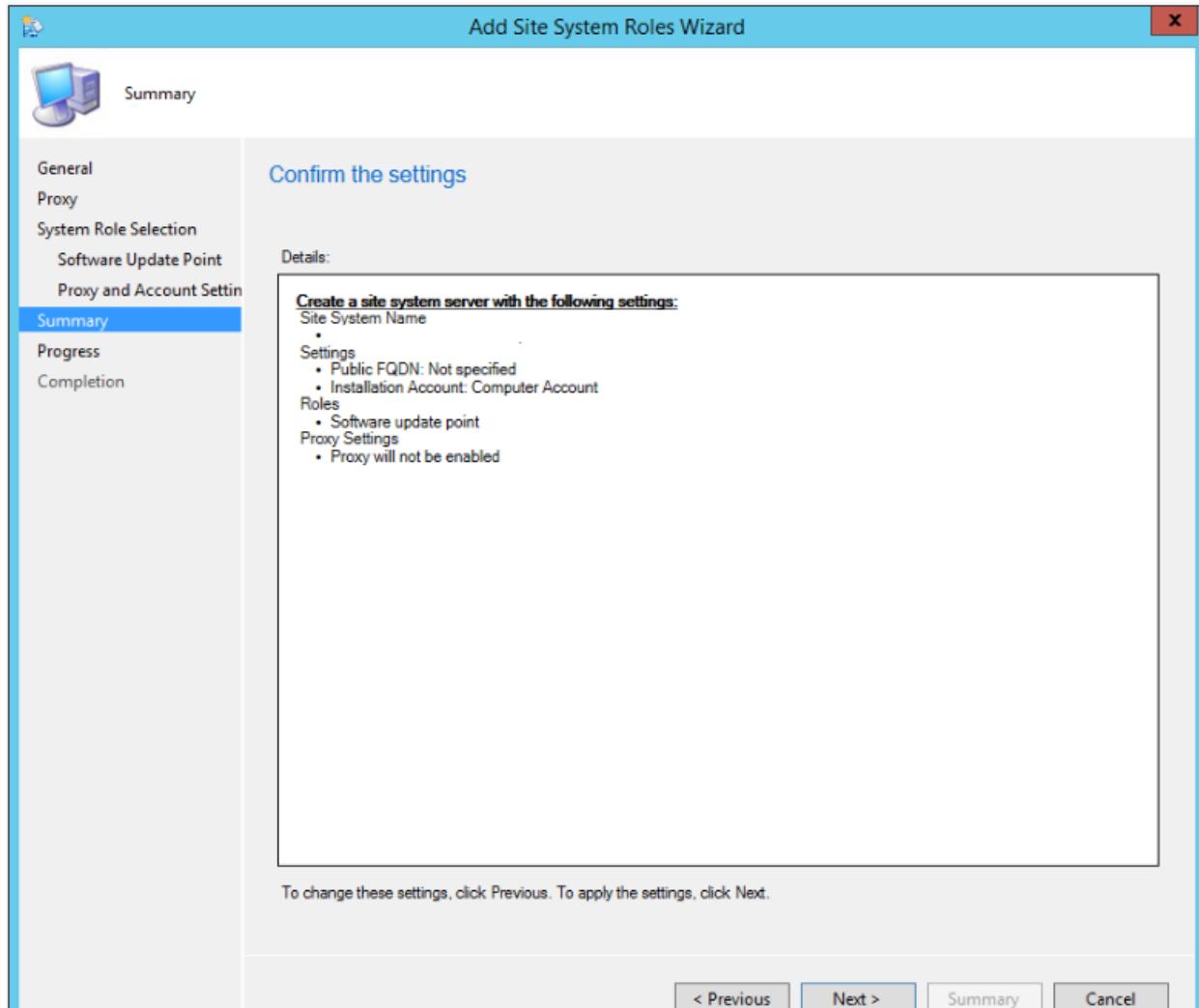
Select the **8530 8531 WSUS option**. Click **Next**.



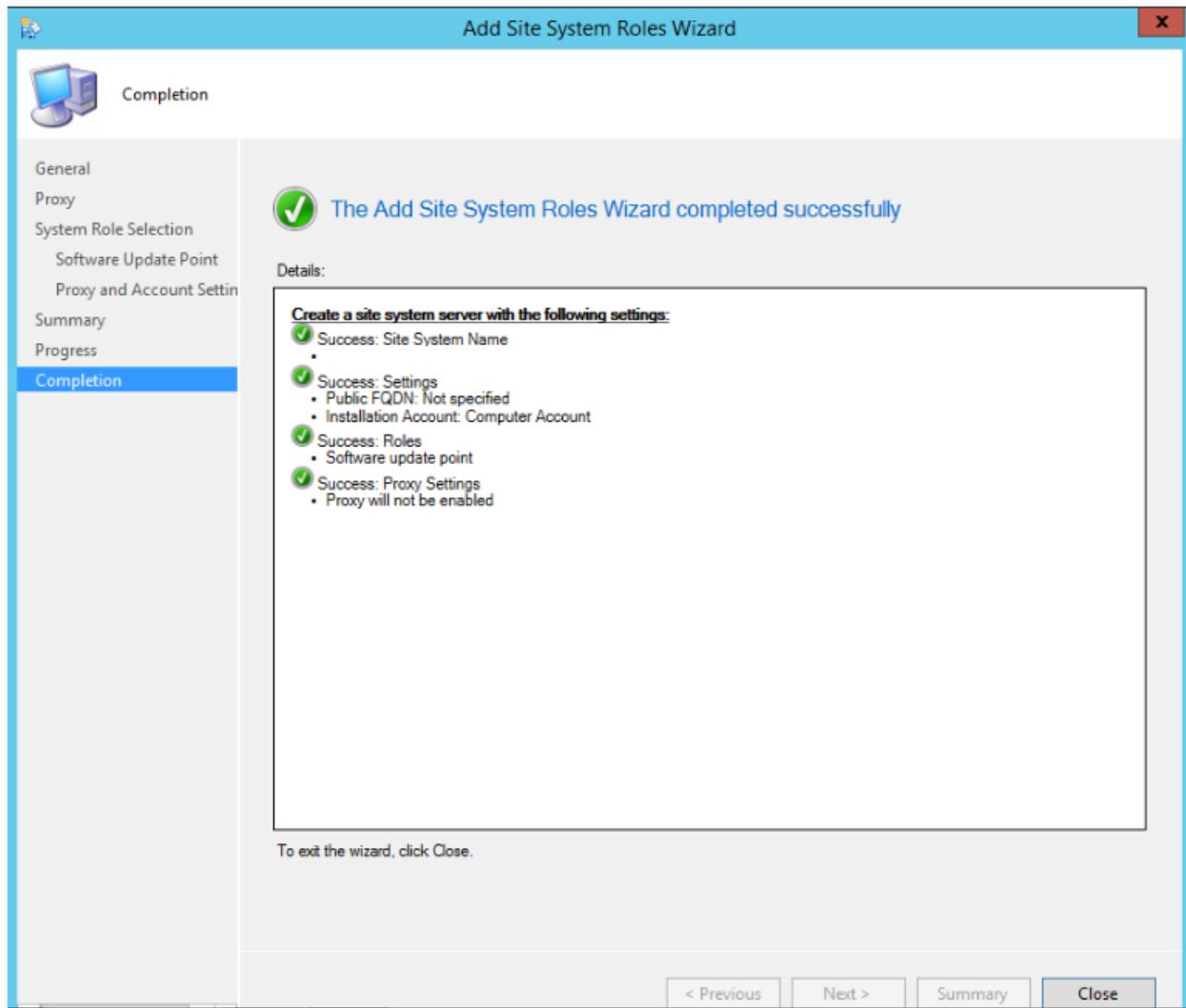
Enter the **service account**. Click **Next**.



Click **Next**.



Click **Close**.



You can verify that the SUP role installation and configuration was a success by viewing the status under **Monitoring > System Status > Site Status**.

Site Status 14 items			
Search			
Icon	Status	Site System	Site System Role
✓	OK	\sccm2.DOMAIN.com	Component server
✓	OK	\sccm2.DOMAIN.com	Software update point
✓	OK	\sccm2.DOMAIN.com	Distribution point

The current status can also be viewed under the **Software Update Point Synchronization Status**. Notice how the primary SUP (top line) points to Microsoft Update, and SCCM2 (SUP2) points to SCCM (SUP1).

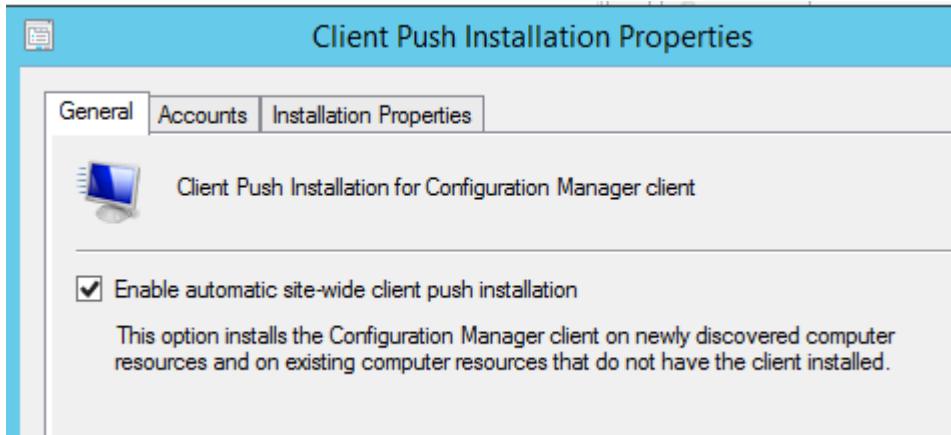
The screenshot shows the SCCM Monitoring interface. On the left, there is a navigation tree under 'Monitoring' with several collapsed categories like System Status, Deployments, Client Operations, Client Status, Database Replication, Distribution Status, Content Status, Distribution Point Group Status, Distribution Point Configuration, Software Update Point Synchronization (which is currently selected and highlighted in blue), and Updates and Servicing Status. A large number '1' is overlaid on the 'Content Status' item. On the right, there is a table titled 'Software Update Point Synchronization Status' with two rows of data. A large number '2' is overlaid on the table area. The table has columns for Icon, Site Code, Software Update Point, and Synchronization Source. The data is as follows:

Icon	Site Code	Software Update Point	Synchronization Source
Green checkmark	001	sccm.DOMAIN.com	Microsoft Update
Green checkmark	001	sccm2.DOMAIN.com	sccm.DOMAIN.com

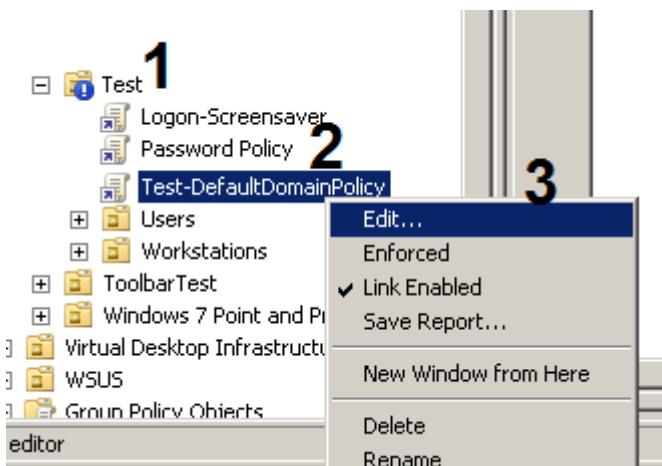
Deploying SCCM Clients Using Group Policy

First, uncheck the option **Enable Automatic site wide client push installation**.

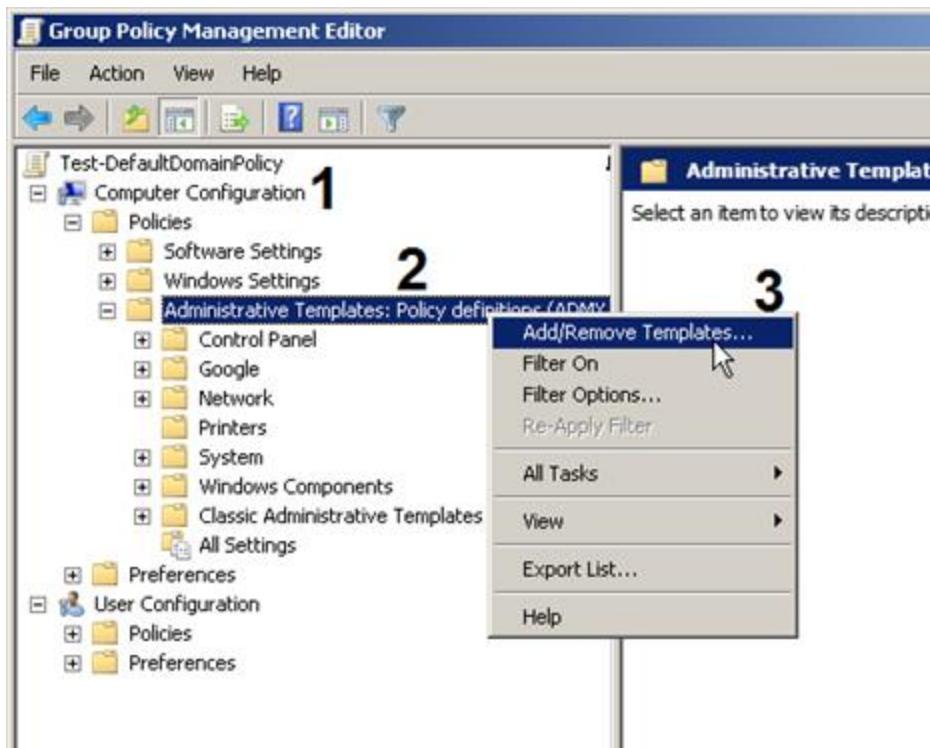
Sites > Settings > Client Push Installation > General Tab.



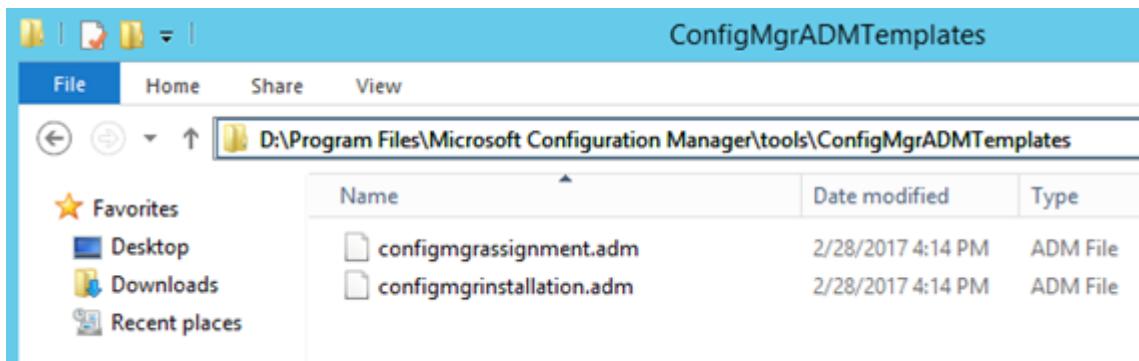
Next, create a **new group policy**, in **GPMC**, find the **SCCM GPO** and click **Edit**.



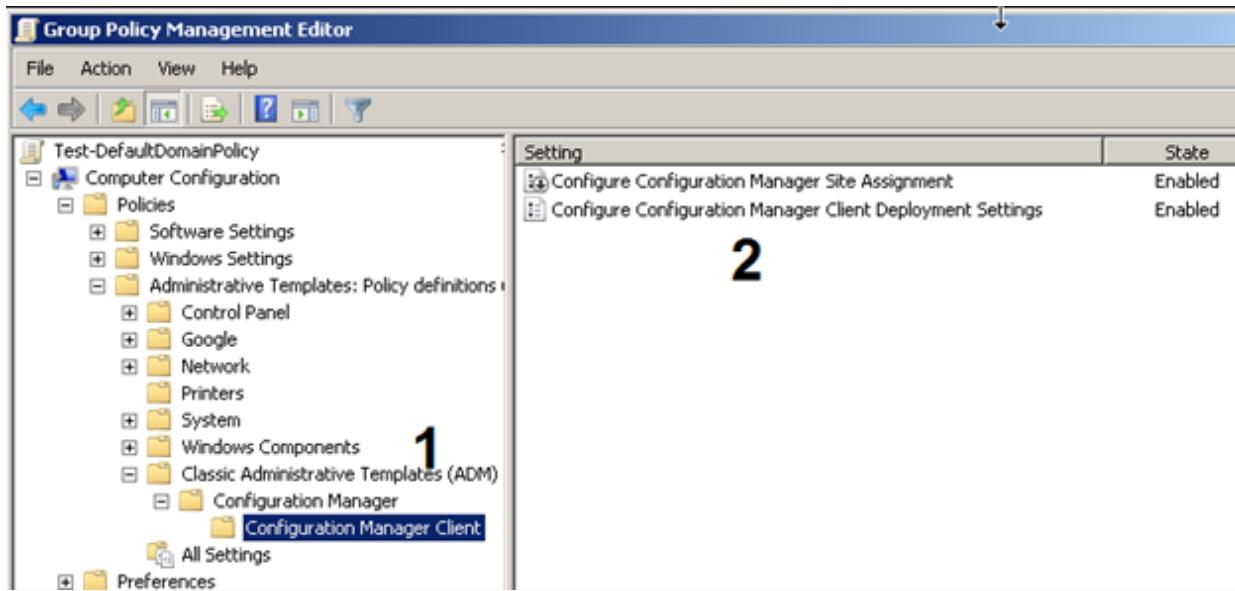
Expand Computer Configuration, Policies and right-click on Administrative Templates and click on Add/Remove Templates.



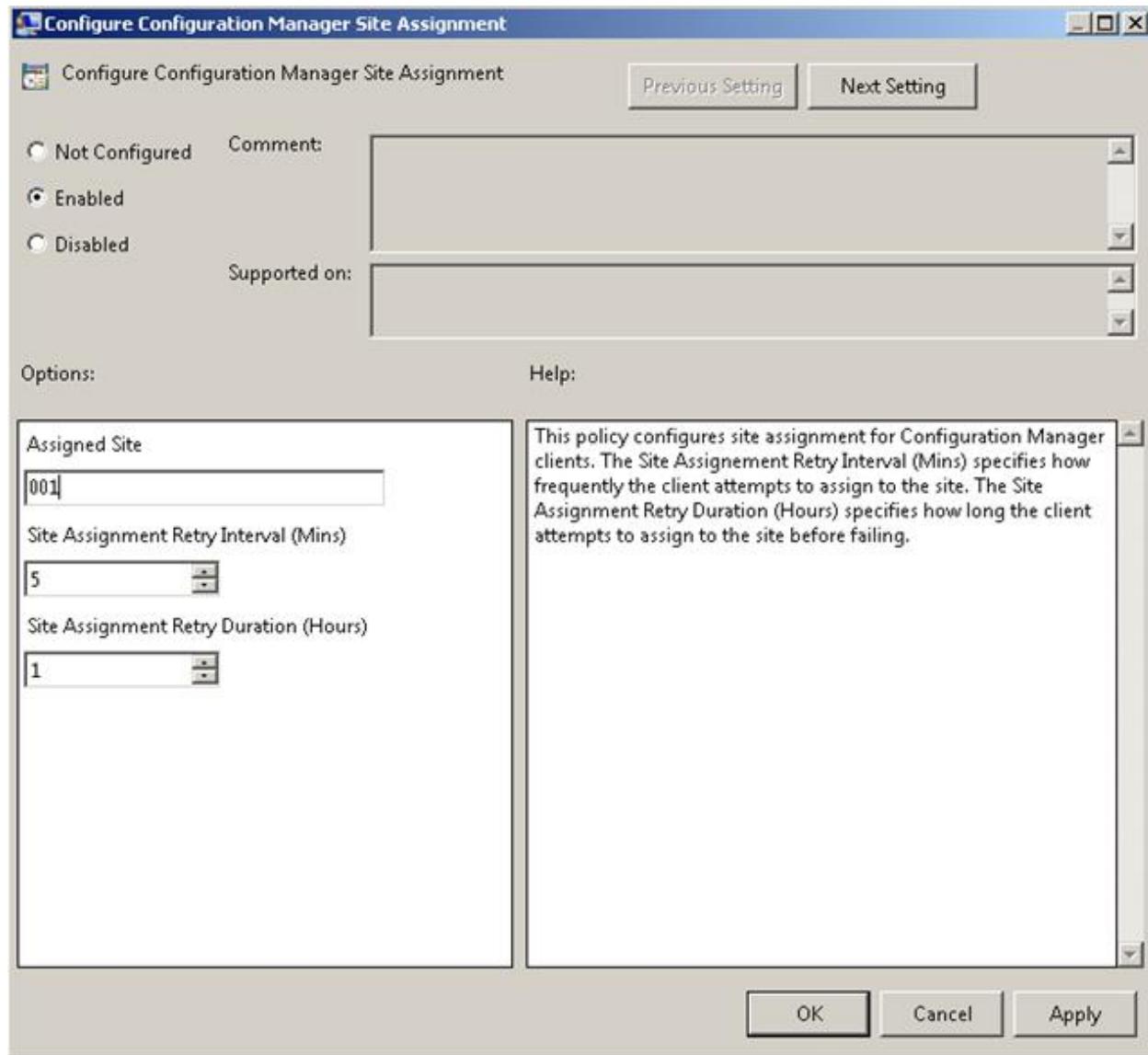
The templates can be found on D:\Program Files\Microsoft Configuration Manager\tools\ConfigMgrADMTemplates or on DVD\SMSSETUP\TOOLS\ConfigMgrADMTemplates



Import both templates. Once imported, access the configuration under **Classic Administrative Templates (ADM) > Configuration Manager > Configuration Manager Client**.

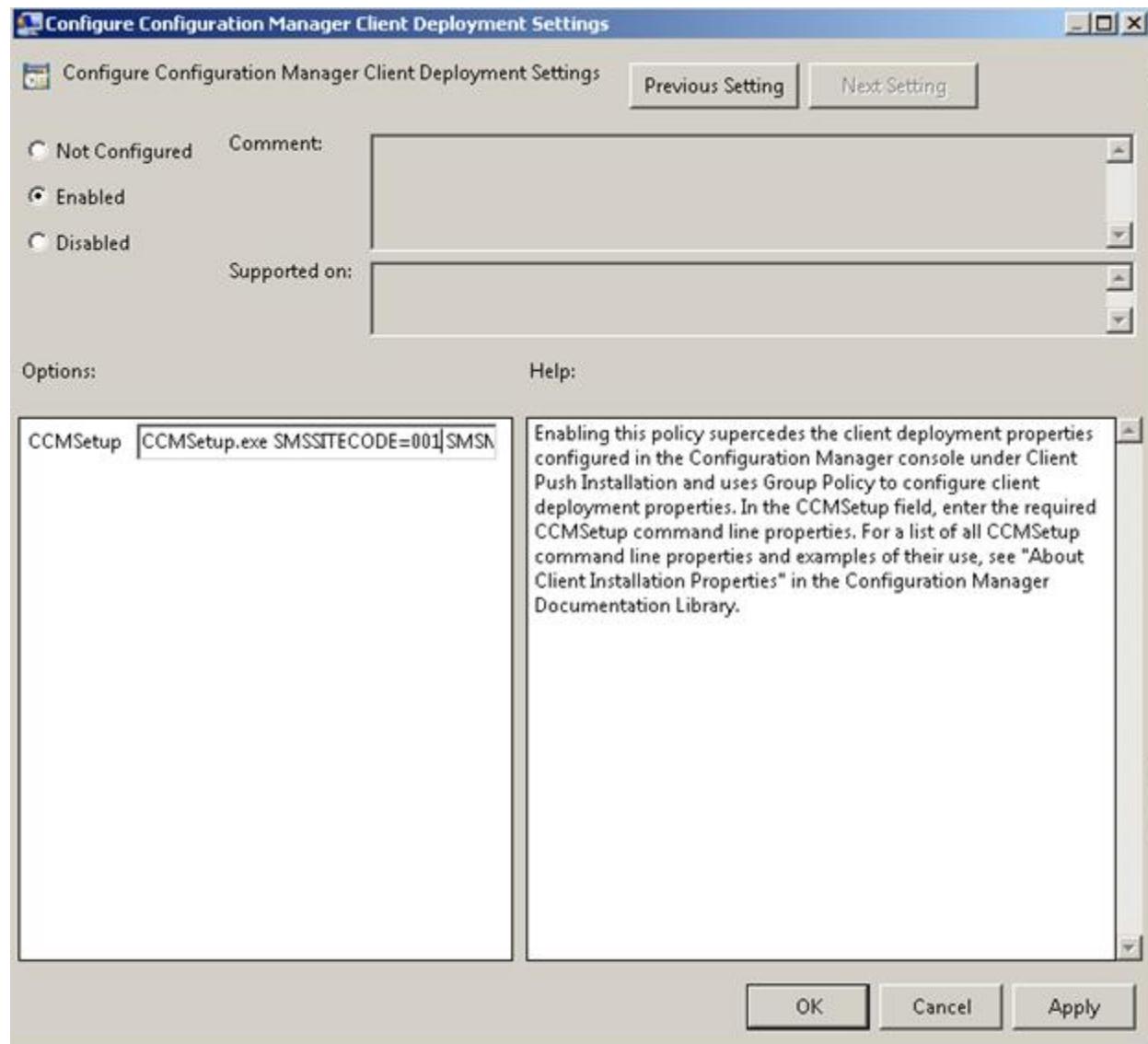


Enable and configure Site Assignment. Click **Apply** and then **OK**.

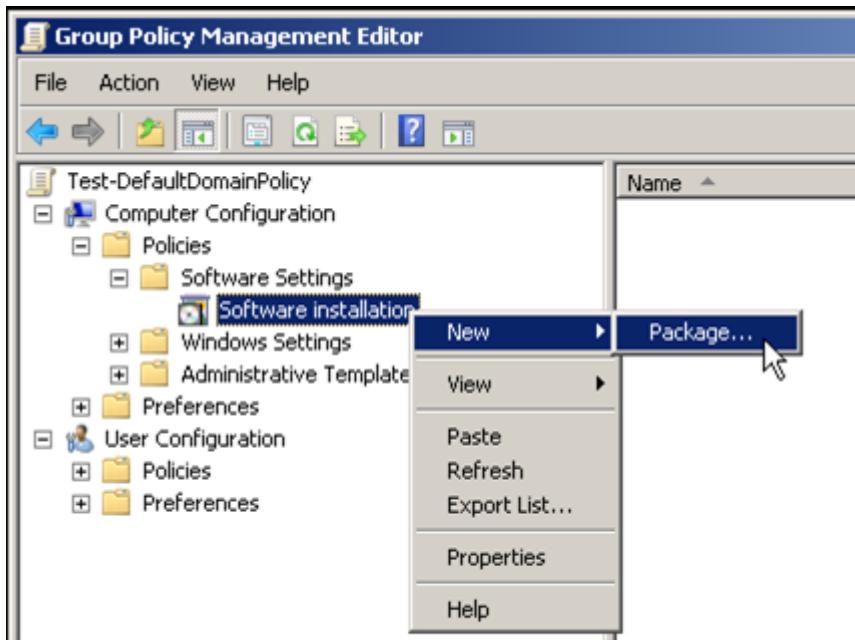


Enable and configure Client Deployment Settings. Click **Apply** and then **OK**.

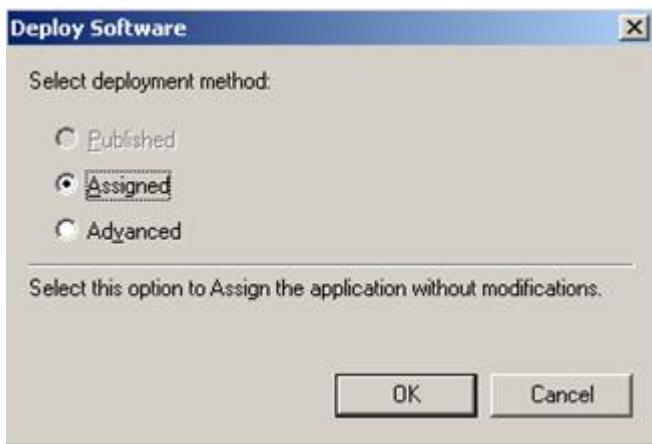
CCMSetup.exe SMSSITECODE=001 SMSMP=SCCM.DOMAIN.COM



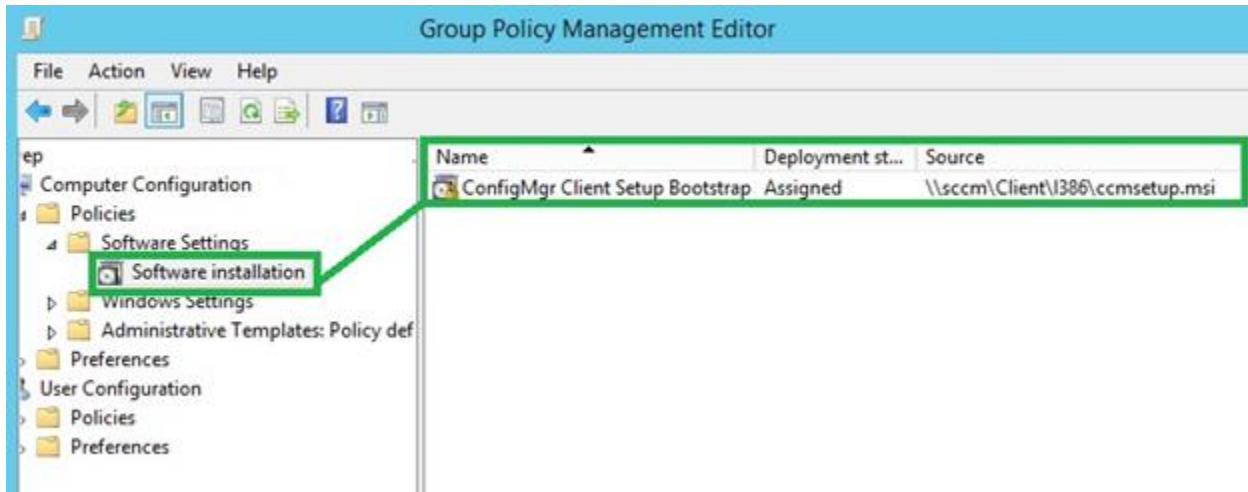
Next, go to **Policies > Software Settings** > right click **Software installation** and select **Package**.



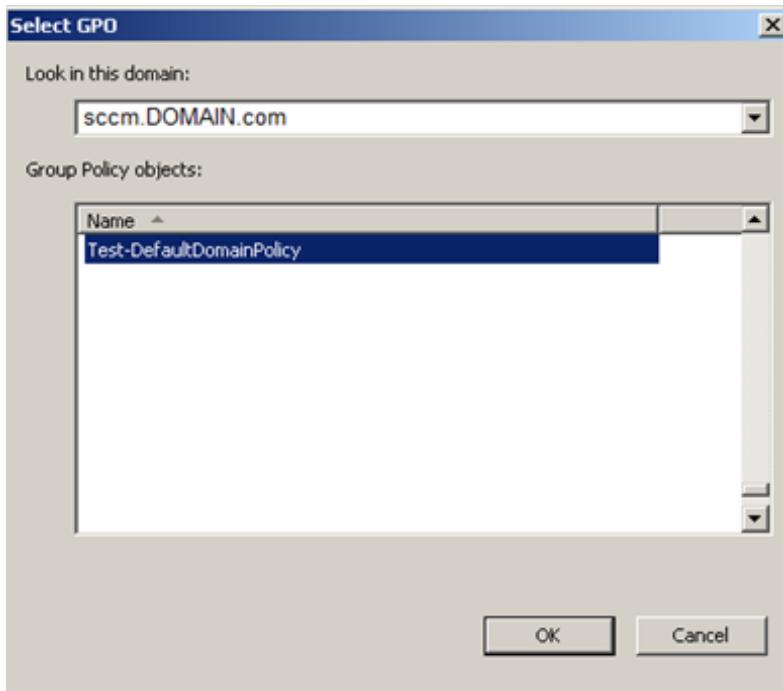
The **ccmsetup.msi** can be found in **\sccm.DOMAIN.com\SMS_001\Client\i386** or **DVD\SMSSETUP\BIN\I386**. If using a DVD, copy the msi to a shared readable folder (EVERYONE), and select **Assigned**, otherwise just use the UNC and select **Assigned**.



The end result is an assigned software policy.



You can choose to apply this policy at domain level or at the OU level. If you apply it at the domain level, then every computer in the domain will receive the SCCM client installation the next time GP syncs. To link the policy to an OU (suggested for testing), right click on the Test OU, click **Link an existing GPO**, choose the GPO **Test-DefaultDomainPolicy** (or whatever you named the policy) and click **OK**.



Design

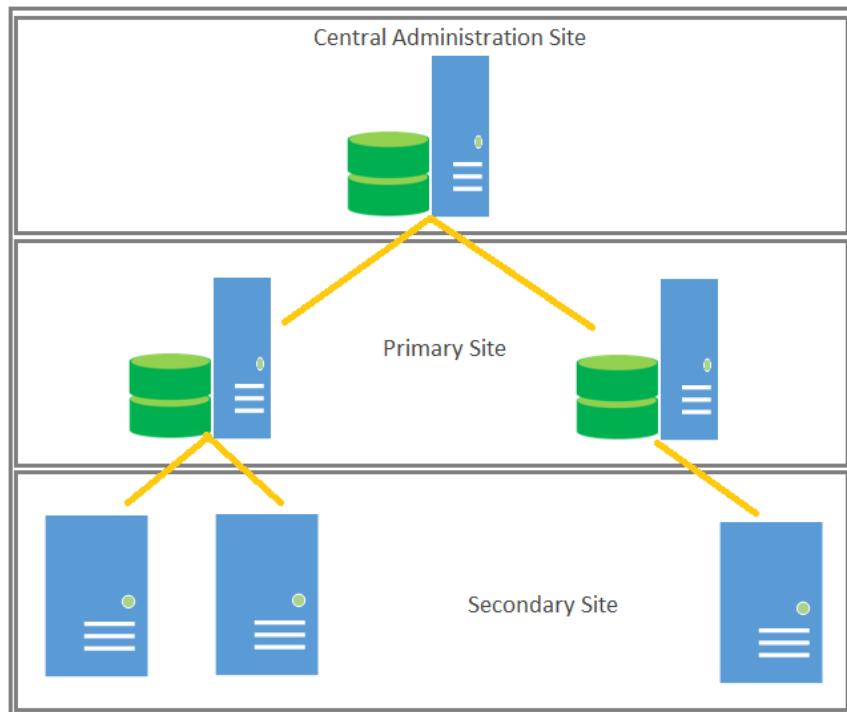
Hierarchies and Sites

1. Hierarchies and Sites

A site is the core role of Configuration Manager. A Configuration Manager hierarchy consists of sites that are linked directly or indirectly and have a parent-child relationship. The Configuration Manager 2012 infrastructure is simplified from earlier versions of the product, and consists of three different site types, Central Administration Site, Primary Site and Secondary site ([1](#)).

A hierarchy of sites can be described by one of three basic configurations,

- A single stand-alone primary site that has no additional sites.
- A primary site that has one or more secondary sites.
- A central administration site as the top-level site that has one or more primary child sites.
The primary sites can each support secondary sites.



Example of a SCCM Hierarchy

Central Administration Site (CAS)

CAS is the recommended location for all administration and reporting for the hierarchy, if you choose to deploy a hierarchy with a CAS. Central Administration sites are used in scenarios where you need more than one Primary Site, such as when you need to manage more than 100 000 clients. The maximum number of clients supported for an entire Configuration Manager 2012 hierarchy is 400 000. The CAS supports only primary sites as child sites. It has limited site roles available, has no clients assigned, and doesn't process client data. The CAS requires SQL Server for data that is gathered from the hierarchy.

Primary Site

A required site that manages clients in well-connected networks. All clients are assigned to a primary site. Primary sites cannot be tiered below other primary sites. Each Primary site can support up to 250 secondary sites, 100 000 clients and 10 management points (for load balancing). A SQL server is required for primary sites. If an organization has less than 100 000 clients, it should only use a single stand-alone primary site.

Secondary Site

Secondary sites can be used to service clients in remote locations where network control is needed. General recommendation though is to avoid usage of secondary sites in such scenarios, and rather deploy Distribution Points in remote locations, because they allow controlling, or throttling, network bandwidth for content distribution between a site and a remote distribution point. Secondary sites are installed through the Configuration Manager console. A management point and distribution point are automatically deployed when the site is installed. SQL Server Express or a full instance of SQL Server is required for a secondary site. If neither is installed when the site is installed, SQL Server Express is automatically installed.

Secondary sites must be direct child sites below a primary site, but can be configured to send content to other secondary sites. They also receive a subset of the Configuration Manager database. Clients cannot be assigned directly to secondary sites.

Because administrative consoles can connect only to a central administration or primary site, secondary sites are typically used in locations that do not have administrators, or in locations where you need clients to scan for software updates compliance without needing to talk to a primary site server. The latter can be achieved by installing the software update point role on a secondary site server.

Site System Roles

Site System Roles are roles that can be installed on Configuration Manager 2012 R2 site servers. Any computer hosting a site system role is referred to as a site system server. You can assign multiple roles to one site system server. There are five site system roles that must exist in each site and must be configured during installation of a CAS or a Primary site, while the rest of the site system roles are optional.

Default Site System Roles

Component Server

Any server running the Configuration Manager Executive service. It is automatically installed with all site system roles except the Distribution Point, and is used to run Configuration Manager services.

Site Database Server

Server with Microsoft SQL Server installed, hosting the Configuration Manager site database. This database is used to store information about assets and site data.

Site Server

Contains components and services required to run a central administration, primary, or secondary site.

Site System

Supports both required and optional site system roles. Any server (or share) with an assigned role automatically receives this role.

SMS Provider

A WMI provider operating as an interface between the Configuration Manager console and the site database. Secondary sites do not install SMS providers.

Optional Site System Roles

Application Catalog Web Service Point

Publishes software information from the software library to the Application Catalog Website.

Application Catalog Website Point

Publishes the available software for a user on the Application Catalog Website.

Asset Intelligence Synchronization Point

Synchronizes Asset Intelligence data from System Center Online by downloading Asset Intelligence catalog data and uploading custom catalog data. This role can only be installed on the CAS or a stand-alone primary site server.

Certificate Registration Point

Communicates with the server that runs the Network Device Enrollment Service of Active Directory Certificate Services to manage device certificate requests that use the Simple Certificate Enrollment Protocol (SCEP).

Distribution Point

This role stages packages (source files), such as application content, software packages, software updates, operating system images, and boot images to clients. A Distribution Point cannot be connected to a CAS, it always communicates with a primary site or a secondary site. A single Distribution Point is capable of supporting up to 4000 clients. A site can hold up to 250 Distribution Points.

Endpoint Protection Point

This role is configured at the Central Administration Site or a stand-alone primary site. With the System Center Endpoint Protection role, you can secure your clients and servers from viruses and malware by deploying (and managing) Microsoft System Center 2012 Endpoint Protection to clients. Microsoft System Center 2012 Endpoint Protection provides an antimalware and security solution for the Microsoft platform.

Enrollment Point

Facilitates enrollment of Intel's Active Management Technology (AMT)-based computers and mobile devices.

Enrollment Proxy Point

Allows the management of mobile device enrollment through Configuration Manager.

Fallback Status Point

Provides an alternative location for clients to send up status messages during installation when they cannot communicate with their management point.

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. One Management Point can support up to 25 000 clients.

Out-of-Band Service Point

Allows out of band management of AMT-based computers.

Reporting Services Point

Used to integrate reporting through SQL Server Reporting Services and is required if using reports.

Software Update Point

Provides software update management for Configuration Manager clients by integrating with Windows Server Update Services (WSUS).

State Migration Point

When using OSD, the state migration point holds the user state data for migration to the new operating system.

System Health Validator Point

When implementing Network Access Protection (NAP) a system health validator point validates the Configuration Manager NAP policies. The role must be installed on the NAP health policy server.

Windows Intune Connector

When managing mobile devices via Windows Intune you need to install the Windows Intune connector to be able to retrieve status messages and inventory messages from the mobile devices that are enrolled in Windows Intune.

SCCM Scripts

Manually Repair CM Client using PowerShell

```
function repairclient([String] $strComputer) { $SMScli = [wmiclass] "\\$strComputer\root\ccm:sms_client"$SMScli.RepairClient() }
```

Policy: VBScript

```
On Error Resume Next  
Dim oCPAppletMgr  
Set oCPAppletMgr = CreateObject("CPApplet.CPAppletMgr")  
Dim oClientActions Set oClientActions = oCPAppletMgr.GetClientActions()  
Dim oClientAction  
For Each oClientAction in oClientActions  
If oClientAction.Name = "Request & Evaluate Machine Policy"  
Then oClientAction.PerformAction  
End If  
Next
```

Change Site Code: Client

```
Set objShell = CreateObject("WScript.Shell")  
set objSMSClient = CreateObject ("Microsoft.SMS.Client")  
  
'update site code  
objSMSClient.SetAssignedSite "ABC",0  
  
'restart process  
objShell.Run "C:\Windows\CCM\CcmRestart.exe",0,true  
  
msgbox " Site code has been changed!"
```

Repair Client with Certificate: Client

```
Set objShell = CreateObject("WScript.Shell")  
set objSMSClient = CreateObject ("Microsoft.SMS.Client")  
  
'import certificate  
objShell.Run "cmd /k certutil.exe -addstore Root ""C:\Windows\ccmsetup\certificate.cer"" ", 9, True  
objShell.Run "cmd /k certutil.exe -addstore TrustedPublisher ""c:\Windows\ccmsetup\certificate.cer"" ",  
9, True
```

```
'update site code
objSMSClient.SetAssignedSite "ABC",0

'repair
objShell.Run "cmd /k C:\Windows\CCM\ccmrepair.exe",9,true

'repair policy
objShell.Run "cmd /k msieexec /x c:\Windows\ccmsetup\MicrosoftPolicyPlatformSetup.msi /qn",9,true
objShell.Run "cmd /k msieexec /i c:\Windows\ccmsetup\MicrosoftPolicyPlatformSetup.msi /qn",9,true

'restart process
objShell.Run "cmd /k C:\Windows\CCM\CcmRestart.exe",9,true

msgbox " SCCM Client has been repaired!"
```

Force Status Update: Client

```
'Initialize the UpdatesStore variable.
Dim newCCMUpdatesStore

'Create the COM object.
set newCCMUpdatesStore = CreateObject ("Microsoft.CCM.UpdatesStore")

'Refresh the server compliance state by running the RefreshServerComplianceState method.
newCCMUpdatesStore.RefreshServerComplianceState
```

```
'Output success message.
Wwscript.Echo "Ran RefreshServerComplianceState."
```

Enable Ring, Client Status Update: Client

```
# Get these as an input
$siteServer="FQDN.SCCMServer.Name"

if(!$siteServer)
{
    "Provide the CAS site server name."
    Return
```

```
}

$WmiObjectSiteClass = "SMS_SCI_SiteDefinition"
$WmiObjectClass = "SMS_SCI_Component"
$WmiComponentName = "SMS_DMP_DOWNLOADER"
$WmiComponentNameUpdateRing = "UpdateRing"

# Get provider instance
$providerMachine = Get-WmiObject -namespace "root\sms" -class "SMS_ProviderLocation" -
computername $siteServer

# Get the first provider if there are multiple
if($providerMachine -is [system.array])
{
    $providerMachine=$providerMachine[0]
}

$SiteCode = $providerMachine.SiteCode
$ProviderMachineName = $providerMachine.Machine
$WmiObjectNameSpace="root\SMS\site_$(($SiteCode))"

# Get top level site sitecode
$SiteDefinition = Get-WmiObject -Namespace $WmiObjectNameSpace -ComputerName
$ProviderMachineName -Class $WmiObjectSiteClass | Where-Object { $_.ParentSiteCode -eq "" }
$SiteCode = $SiteDefinition.SiteCode

#Get component
$WmiObject = Get-WmiObject -Namespace $WmiObjectNameSpace -ComputerName
$ProviderMachineName -Class $WmiObjectClass | Where-Object { $_.SiteCode -eq $SiteCode -and
$_.ComponentName -eq $WmiComponentName }

#Get embedded property
$props = $WmiObject.Props
$props = $props | where {$_.PropertyName -eq $WmiComponentNameUpdateRing}

if (!$props) {

    #Create embedded property
```

```

$EmbeddedProperty =
([WMICLASS]"root\SMS\site_$(($SiteCode):SMS_EMBEDDEDPROPERTY").CreateInstance()
$EmbeddedProperty.PropertyName = $WmiComponentNameUpdateRing
$EmbeddedProperty.Value = 1
$EmbeddedProperty.Value1 = ""
$EmbeddedProperty.Value2 = ""

$WmiObject.Props += [System.Management.ManagementBaseObject] $EmbeddedProperty

$WmiObject.put()

}

else
{
    $props = $WmiObject.Props
    $index = 0
    ForEach($oProp in $props)
    {
        if($oProp.PropertyName -eq $WmiComponentNameUpdateRing)
        {
            $oProp.Value=1
            $props[$index]=$oProp;
        }
        $index++
    }

    $WmiObject.Props = $props
    $WmiObject.put()
}

```

Write-Host "The command(s) completed successfully"

Manually Install Client

```

Set objShell = CreateObject("WScript.Shell")
strCmd=".\\ccmsetup.exe /source:c:\\Install\\SCCMClient smssitecode=001 smsmp=FQDN.SCCM.SERVER
FSP=FQDN.SCCM.SERVER"
objShell.Run strCmd, 0, true

```

Manually Repairing CM Client using Commands

```
net stop ccmsetup
```

```
%windir%\system32\wbem\winmgmt /clearadap
%windir%\system32\wbem\winmgmt /kill
%windir%\system32\wbem\winmgmt /unregserver
%windir%\system32\wbem\winmgmt /reserve
%windir%\system32\wbem\winmgmt /resyncperf
net stop winmgmt /y
if exist %windir%\system32\wbem\repository.old rmdir /s /q
%windir%\system32\wbem\repository.old
rename %windir%\system32\wbem\repository
%windir%\system32\wbem\repository.old
regsvr32 /s %systemroot%\system32\scecli.dll
regsvr32 /s %systemroot%\system32\userenv.dll
mofcomp %windir%\system32\wbem\cimwin32.mof
mofcomp %windir%\system32\wbem\cimwin32.mfl
mofcomp %windir%\system32\wbem\rsop.mof
mofcomp %windir%\system32\wbem\rsop.mfl
cd wbem
for /f %s in ('dir /b /s %windir%\system32\wbem\*.dll') do regsvr32 /s %s
for /f %s in ('dir /b /s %windir%\system32\wbem\*.mof') do mofcomp %s
for /f %s in ('dir /b %windir%\system32\wbem\*.mfl') do mofcomp %s
net start winmgmt
net start ccmsetup
%windir%\system32\wbem\wmiprvse /regserver
```

Troubleshooting

Question

What do the client status icons mean?

Answer

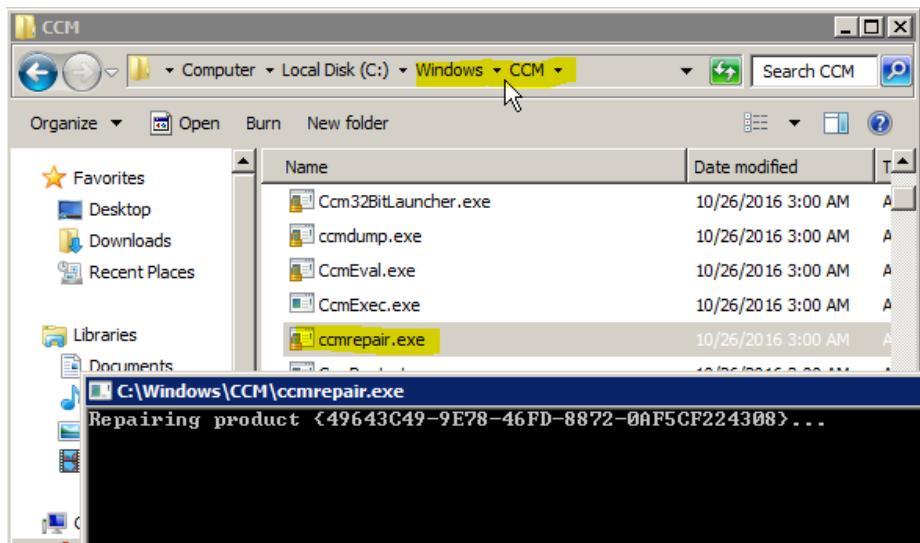
If the device has no client installed, then the icon will appear as it does today in CM12 and CM1511 (current branch). If a client is installed but no data is yet available a gray question mark will appear. If a client is installed and online, it will appear as in the screenshot above with a white tick in a green circle. If the client is completely offline, a gray X will appear.

Question

How do I repair the SCCM client?

Answer

Run the ccmrepair from C:\Windows\CCM

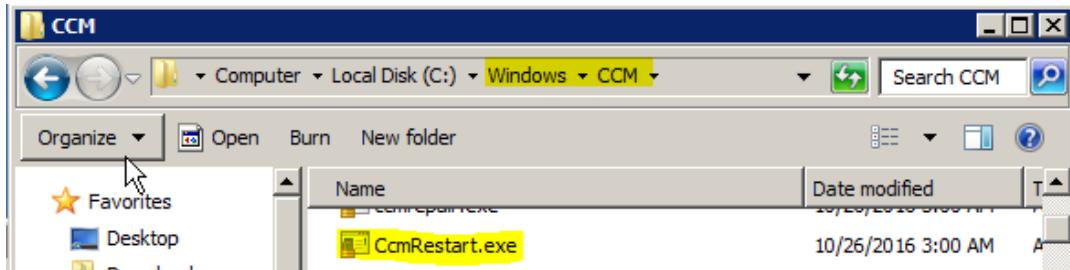


Question

How can I restart the SCCM client?

Answer

Run CcmRestart.exe from C:\Windows\CCM

**Question**

How do I enable or fix Control Alt Delete in Remote Control when it is not working?

Answer

There is a group policy option for this simulation of keys. Look under Computer policies > Admin Templates > Windows Components / Windows Logon Options and then set "Disable or enable software secure attention sequence" to 'enabled'. You must then change "Set which software is allowed to generate the secure attention sequence" to "Services and Ease of Access applications".

Error

CM client will not install, general troubleshooting.

Solution

Check boundary for the client. Make sure the Admin\$ share is accessible on the client. Make sure the machine responds to ping. The machine must have a valid service or client installation account added to the Administrators group---should be the same account used in SCCM > Sites > Client Installation Settings > Client Push Installation > Accounts.

Error

Failed to receive CCM message response. Status code = 500. Found in Logs\ccmsetup.log when trying to install the CM client.

```
component="ccmsetup" context="" type="1" thread="6384" file="httphe  
<![LOG[Failed to receive ccm message response. Status code = 500]LOG  
"ccmsetup" context="" type="2" thread="6384" file="httphelper.cpp:17  
<![LOG[GetDPLocations failed with error 0x80004005]LOG]!><time="16:  
type="3" thread="6384" file="siteinfo.cpp:596">  
<![LOG[Failed to get DP locations as the expected version from MP 'F
```

Solution

This problem occurs because the ApplicationHost.config file or the Web.config file references a module that is invalid or that does not exist. To resolve this problem: In the ApplicationHost.config file or in the Web.config file, locate the module reference or the DLL reference that is invalid, and then fix the reference. To determine which module reference is incorrect, enable Failed Request Tracing, and then reproduce the problem.

For above specific error (mentioned in this example), DynamicCompressionModule module is causing the trouble. This is because of the XPress compression scheme module (suscomp.dll) which gets installed with WSUS. Since Compression schemes are defined globally and try to load in every application Pool, it will result in this error when 64bit version of suscomp.dll attempts to load in an application pool which is running in 32bit mode.

This module entry looks like:

```
>scheme name="xpress" doStaticCompression="false" doDynamicCompression="true"  
dll="C:\Windows\system32\inetsrv\suscomp.dll" staticCompressionLevel="10"  
dynamicCompressionLevel="0" />
```

Hence to get rid of this problem:

Remove/Disable the XPress compression scheme from the configuration using the command below:

```
%windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpCompression /-  
[name='xpress']
```

Error

Failed to connect to policy namespace.

Solution

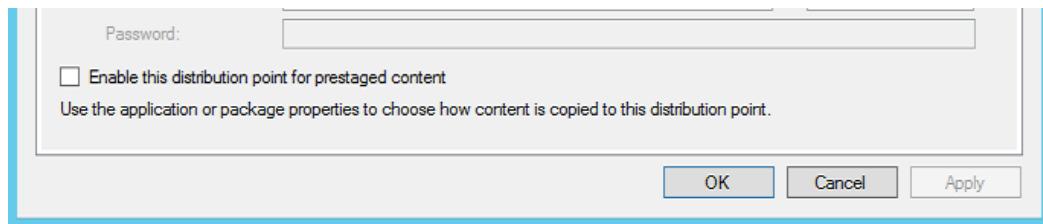
Computer object is missing from OU (the computer has not been added to OU in AD). So, add the computer to the proper OU, or change the OU in SCCM.

Error

SCCM Client is not installing on clients.

Solution

Make sure 'Prestage' is disabled: Under Security > Distribution Points > Properties of distribution point.

**Error**

Cannot install or repair Configuration Manager; cannot start SMS or SCCM services. Error 1053. Error 1053: "The service did not respond in a timely fashion".

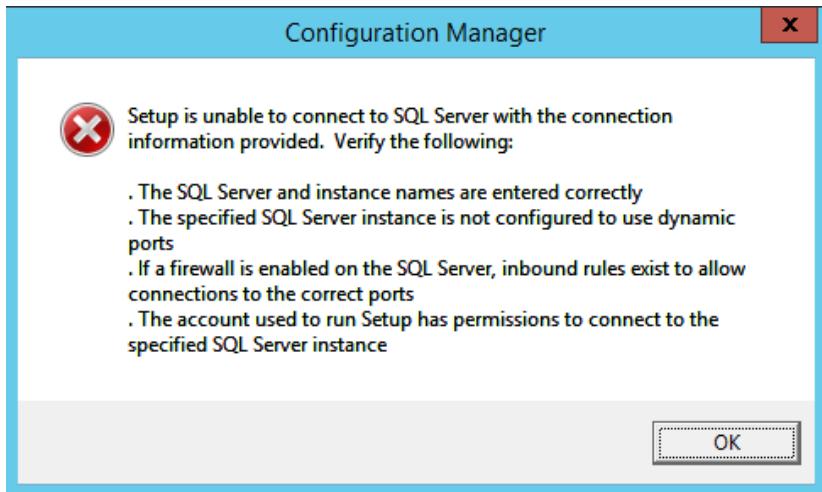
Solution

Try running the sitecode.exe manually, and look at any errors. One error that can cause these issues is: "MSVCP120.dll is missing from your computer." Fix by reinstalling [64 bit Visual C++ Redistributable Packages for Visual Studio 2013](#).

Note, sitecode.exe file can be found in the default installation folders of SCCM:
C:\Program Files\Microsoft Configuration Manager\bin\x64
D:\Program Files\Microsoft Configuration Manager\bin\x64

Error

Upon a first time a SCCM setup, 'Unable to connect to SQL Server with connection information'.



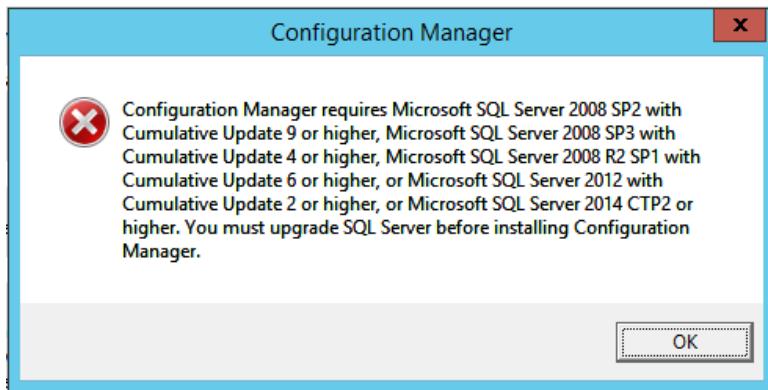
Solution

Instance name should be blank.

A screenshot of the SCCM SQL connection configuration dialog. It has three fields: "SQL Server name (FQDN)" with the value "sccm.DOMAIN.com", "Instance name (leave blank for default)" with the value redacted (yellow box), and "Database name" with the value "CM_001". Each field includes an example text to its right.

Error

Configuration Manager requires Microsoft SQL.



Solution

Install SQL Server Service Pack 3 or other updated service pack.

Error

SQL Server service running account failed

Prerequisite	Status
Firewall exception for SQL Server (stand-alone primary)	Warning
SQL Server service running account	Failed

Solution

Add a domain account.

Sql Server Configuration Manager				
Name	State	Start Mode	Log On As	
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Running	Manual	NT Service\MSQLFDLauncher	
SQL Server (MSSQLSERVER)	Running	Automatic	DOMAIN \sccmadmin	

Error

Gray X on devices; devices are offline or they appear to be offline. Beginning in version 1602 of Configuration Manager, this status indicates if the computer is online or not. A computer is considered online if it is connected to its assigned management point. To indicate that the client is online, it sends ping-like messages to the management point. If the management point does not receive a message in 5 minutes, the client is considered offline.

Solution

Installing/Reinstalling hotfixes did not work. What worked: Load SQL Server Configuration Manager. Enable Named Pipes under SQL Server Network Configuration, Protocols for MSSQLSERVER. Reset services using the Start Menu Configuration Manager Setup tool.

Error

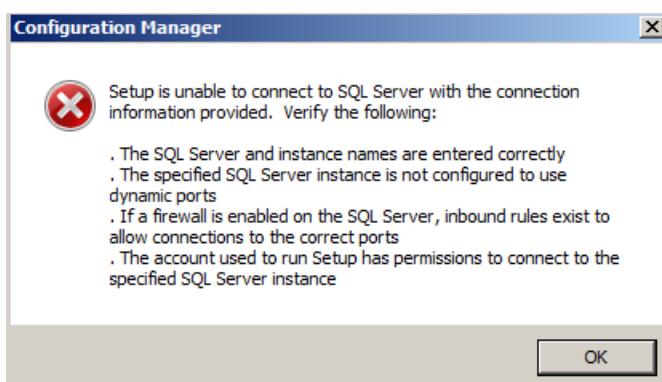
SMS_NOTIFICATION_SERVER Error 1020, 4951, Site Component Manager failed to reinstall this component on this site system.

Solution

Remove all roles but the default ones and reset services using the Start Menu 'Configuration Manager Setup' tool. Also see the next error (SQL Server connection issues will affect components).

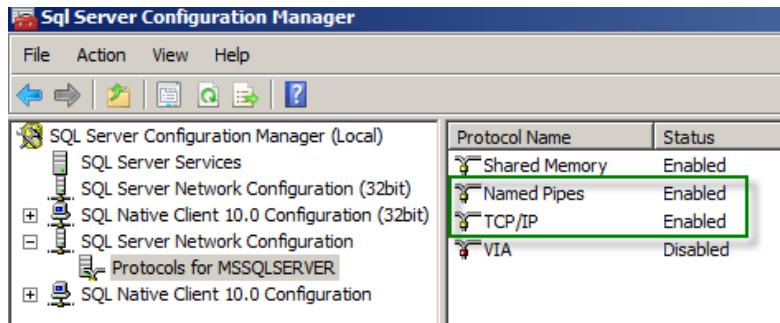
Error

Upon repairing or reinstalling SCCM, you receive *Setup is unable to connect to SQL Server with the connection information provided.*



Solution

Load SQL Server Configuration Manager. Enable Named Pipes under SQL Server Network Configuration, Protocols for MSSQLSERVER. Reset services using the Start Menu ‘Configuration Manager Setup’ tool.



Error

SCCM client computer listed as *No Results* for *Client Check Result*.

Solution

On the client, go to Start / Run and type *control schedtasks* to open the scheduled tasks control panel. Open Microsoft, then Configuration Manager and delete all listed entries. Initiate the *install client* with the *always install* option checked in the SCCM console. The scheduled tasks should be recreated when the agent installs and the computer will start checking in appropriately to the SCCM server. Check the local computers ccmeval.log file for more details.

Error

Failed to find accessible source. Waiting for retry.

Solution

Switch both the distribution point and the management point to HTTP.



More Advanced WSUS Troubleshooting

Is a GPO set to point WSUS to your SUP?

GP can mess with the results in testing and setting up WSUS/SUP. Make sure GP is exactly what you think it is. If you have doubts, block GP to your test devices.

Also, you may want to check the relative WSUS registry key.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="YOUR WSUS SERVER PATH"
"WUStatusServer"="YOUR WSUS SERVER PATH"
"TargetGroupEnabled"=dword:00000001
"TargetGroup"="THE TARGET GROUP"
```

Did WSUS create the SUSDB?

If there is no SUSDB, that means there are DB creation problems; most likely related to user rights. Something important to note, a botched WSUS setup can affect the DB and IIS.

System.Runtime.InteropServices.COMException (0x80070003): The system cannot find the path specified.

Try the command below in PowerShell...and the wsusutil.exe:

They will modify C:\Windows\System32\ServerManager\ComponentConfiguration\UpdateServices-Services.xml, and add in the content location---content location seen in bold.

```
<?xml version="1.0" encoding="utf-16"?><INSTANCE
CLASSNAME="ServerComponent_UpdateServices_Services"><PROPERTY NAME="ContentDirectory"
TYPE="string"><VALUE>\FQDN.DOMAIN.com\apps\updates</VALUE></PROPERTY><PROPERTY
NAME="ContentLocal" TYPE="boolean"><VALUE>true</VALUE></PROPERTY></INSTANCE>
```

[Install-WindowsFeature -Name UpdateServices-Services,UpdateServices-DB –IncludeManagementTools](#)

[C:\Program Files\Update Services\Tools folder\wsusutil.exe postinstall SQL_INSTANCE_NAME="FQDN.DOMAIN.com" "CONTENT_DIR=D:\Updates](#)

Other options

```
C:\Windows\system32\cmd.exe

C:\Users\SCCMAdmin>"C:\Program Files\Update Services\Tools\wsusutil"
Windows Server Update Services administration utility. Try:
    wsusutil help checkhealth
    wsusutil help configurerssl
    wsusutil help configurersslproxy
    wsusutil help csaimport
    wsusutil help deletefrontendserver
    wsusutil help listinactiveapprovals
    wsusutil help removeinactiveapprovals
    wsusutil help export
    wsusutil help healthmonitoring
    wsusutil help import
    wsusutil help listfrontendservers
    wsusutil help listunreferencedpackagefolders
    wsusutil help movecontent
    wsusutil help refreshmuurl
    wsusutil help reset
    wsusutil help usecustomwebsite
    wsusutil help postinstall

C:\Users\SCCMAdmin>
```

Something important to note, if IIS is not configured with the instance ID of 1, you may also receive invalid path.

Go to IIS manager and right click on the web site and select properties.

On the Web Site Tab click properties in the logging section.

At the bottom it shows you the log file name

It starts with W3SVCx where x is the instance ID. Make sure it contains 1.

Are the patches downloading to %windir%\ccm\cache?

- Enable deployment after run.
- Automatically deploy and accept licenses
- Install "as soon as possible" under software available and installation deadline
- Allow software installation outside of maintenance window

Check Logs

These two logs will contain most of the successes and errors of Windows Updates:

- Wsync.log
- WCM.log

The server is configured to use pass-through authentication with a built-in account to access the specified physical path. However, IIS Manager cannot verify whether the built-in account has access. Make sure that the application pool identity has Read access to the physical path. If this server is joined to a domain, and the application pool identity is NetworkService or LocalSystem, verify that <domain>\<computer_name>\$ has Read access to the physical path. Then test these settings again.

Set the application pool identity to a custom account (IIS Manager->Click your application pool->Click Advanced Settings... on the Actions panel->Process Model section). Then, grant the account permissions on the physical path.

IIS becomes corrupted, or just needs to be completely reset.

- Uninstall IIS
- Reboot system
- Uninstall WAS (Windows Process Activation Service)- WAS feature package is the dependent package for the IIS feature package.
- Reboot system
- Reinstall IIS

Missing or cannot start w3svc

Try this first

Go to Task Manager > Processes and manually **stop** the **W3SVC** process. After doing this the process should start normally when restarting IIS

Try this second

Run > appwiz.cpl > Turn windows features on or off > Uncheck **Internet Information Services** and **Windows Process Activation Service**.

Restart your machine.

Run > appwiz.cpl > install both **Internet Information Services** and **Windows Process Activation Service**

Then this...if it still doesn't work

1. Verify that **Windows Management Instrumentation** is started and its startup type is set to automatic.
2. Also make sure the following dependency services are started for **World Wide Web Publishing Service**:
 - Windows Process Activation Service
 - Remote Procedure Call (RPC)
 - DCOM Server Process Launcher
 - RPC Endpoint Mapper.
3. Open regedit, navigate to [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP]:
 - Double click on Start and change value data from 4 (disabled) to 3 (automatically).
 - Delete "NoRun" key if this key exists.
4. Uninstall **Internet information Service** and **Windows process activation service**. Restart computer.
5. Type the below command in CMD and press enter:
-- net start http
6. Reinstall **Internet information Service** from **Turn windows feature on or off (or System Manager)**.
Verify C:\Windows\System32\inetsrv\config\applicationHost.config looks correct. Check for a **system.web** section in this file which may be causing problems. Remove the section.
7. Make sure these two services running and their startup type is automatic. If they are disabled and not running right click on them and go to properties and change them.
 - Windows process activation service
 - Worldwide web publishing service
8. Start IIS and websites will start; no more "w3svc service is not running error."
9. Restart computer.

Notes

```
netstat -a -o | findstr 80  
sc config http start= auto  
sc config http start = auto  
net start w3svc
```

WSUS Console Crashes

Navigate to Application Pools, then select WsusPool, and select Advanced Settings. In the Advanced Setting window, scroll down to Recycling. Originally the Private Memory Limit (KB) is set to 1843200. Change that to 0. Once the change is made, recycle the WsusPool. The IIS Worker Process will quit spiking and the WSUS console should begin working without issue or crashing.

WSUS Cleanup Task

When you select to run the WSUS cleanup task, it will run at the next software updates synchronization. The expired software updates will be set to a status of declined on the WSUS server and the Windows Update Agent on computers will no longer scan these software updates.

When you select to run the WSUS cleanup task, it will run at the next software updates synchronization. The expired software updates will be set to a status of declined on the WSUS server and the Windows Update Agent on computers will no longer scan these software updates.

General Troubleshooting

When the active software update point is installed on a remote site system server, the Windows Server Update Services (WSUS) Administration console must be installed on the site server.

The port settings configured for the active software update point must be the same as the port settings configured for the WSUS Web site in Internet Information Services (IIS).

When there is a proxy server between the active software update point and the upstream update server or Microsoft Update, the proxy server and the software update point proxy server account must be configured, if credentials are required.

The computer and Administrator accounts must be able to access virtual directories under the WSUS Web site in IIS from the site server.

The active software update point at the central site should be configured to synchronize with Microsoft Update. This setting is automatically configured when you first create the software update point on the central site, but if the setting is modified in the WSUS Administration console, WSUS Configuration Manager does not reset this setting as it does for other WSUS settings.

WSUS Server Not Configured Error

Check the port settings configured for the active software update point, and make sure they are the same as the port settings configured for the Web site used by WSUS running on the active software update point.

Check to make sure the fully qualified domain name (FQDN) for the active software update point site system server is correct.

When the Configuration Manager site is in native mode, the WSUS Web site and virtual directories must be configured for Secure Sockets Layer (SSL) because the active software update point is automatically configured to use SSL, but WSUS is not automatically configured. When a Configuration Manager site is in mixed mode, you have the option to configure the active software update point to use SSL. In both cases, you must manually configure the WSUS Web site and virtual directories.

Check to make sure that WSUS running on the active software update point for the child primary site is not configured to be a replica. The following procedure provides the steps to check whether WSUS is configured to be a replica.

To check the update source settings in WSUS

- Open the WSUS console on the active software update point for the site.
- Click Options in the console tree pane.
- Click Update Source and Proxy Server in the display pane.
- Verify that This server is a replica of the upstream server is not selected unless you are in the WSUS console on the active software update point for a secondary site. Child primary sites should never be configured as a replica of the upstream server.

Check that Update Services is running on the WSUS server.

The Remote Name Could Not Be Resolved Error

Check the proxy settings configured for the active software update point, and make sure they are configured correctly. When there is a proxy server between the WSUS server and the upstream update source, the proxy settings must be configured. When credentials are required, you must specify the correct account information for the proxy.

When the proxy settings are configured correctly in the ConfigMgr software update point properties, you can open the WSUS console to check the proxy settings to make sure they match the settings in Configuration Manager. When the proxy settings are configured correctly, you can review the synchronization status in the WSUS console, which might provide more information about why WSUS synchronization failed.

This issue can also be caused by any number of network issues that prevent the URL address for the upstream update source from being resolved. If configuring the proxy settings does not resolve the issue, troubleshoot this issue like any other name-resolution issue on your network.

The Request Failed with HTTP Status 401: Unauthorized Error

Check the permissions on the ApiRemoting30 virtual directory under the WSUS Web site in IIS. The computer and Administrator accounts must have appropriate rights to this virtual directory. The following procedure provides the steps to check the permissions on the ApiRemoting30 virtual directory.

To check the permissions on the ApiRemoting30 virtual directory

On the WSUS server, open Internet Information Services (IIS) Manager.
Navigate to Internet Information Services \ <computername> \ Web Sites \ <WSUS Web site> \ ApiRemoting30.

Right-click ApiRemoting30, and then click Permissions.

Unable to Connect to Remote Server Error

Following are possible solutions for the Unable to connect to remote server error:

Check to make sure the IIS Admin Service and World Wide Web Publishing Service services are running.

Check the connection to the active software update point where WSUS is running.

The Request Failed with DssAuthenticationError: WebException Error

Check the IIS permissions on the DssAuthWebService virtual directory for the WSUS Web site in IIS. The virtual directory must be enabled for anonymous access. By default, the IUSR_<ComputerName> account is used for anonymous access. Check that this account has appropriate rights—for example, whether this account is a member of the Guests group where access has been denied. The following procedure provides the steps to configure the directory permissions for the virtual directory.

To configure anonymous access on the DssAuthWebService virtual directory

On the WSUS server, open Internet Information Services (IIS) Manager.

Expand Web Sites, and then expand the Web site for the WSUS server. It is recommended that the WSUS custom Web site be used, but the default Web site might have been chosen when installing WSUS.

Right-click DssAuthWebService, and then click Properties.

Click the Directory Security tab, and then click Edit in the Authentication and access control section. Verify that Enable anonymous access is selected and that the IUSR_<ComputerName> account is specified.

Force SUP Product Settings to Apply [much faster]

To work around changes not taking effect immediately, follow these steps:

Go to the Software Update Component properties and deselect all Products and Classifications which are enabled out-of-the-box.

Force the Software Update Synchronization to run. Monitor the WCM.log and WsyncMgr.log to validate the synchronization is now running successfully. Note that no updates will be synchronized at this point, but the products and classifications catalog will be synced as part of the process.

Enable the required Products and Classifications that were disabled previously, and run the synchronization again.

Sync Tip

On the Select the products that you want to synchronize screen place a checkmark in All Products and then remove it again, this will deselect everything before the first synchronization (recommended).

Restart the Whole WSUS/SUP Instance

Yes, there are going to be times you just have to start the Win Updates setup and config over again.

1. Uninstall SUP role
2. Uninstall WSUS
4. Delete SUSDB from SQL Server if any
5. Restart Server
6. Install WSUS (Choose to install DB not WID)
7. Configure Updates to be stored locally
8. Run Post Deployment Configuration from Server manager
9. Start WSUS Admin Console and ran Wizard (also choose to connect for the catalog sync) up to the Point where you select the products. Then, cancel the wizard without choosing any products.
10. Install SUP role in SCCM and configure the right Settings (WSUS on Server 2012 Defaults to its own admin Website and ports 8530 and 8531) and select the products you require.

11. Check following log file if WSUS does not sync with SCCM.

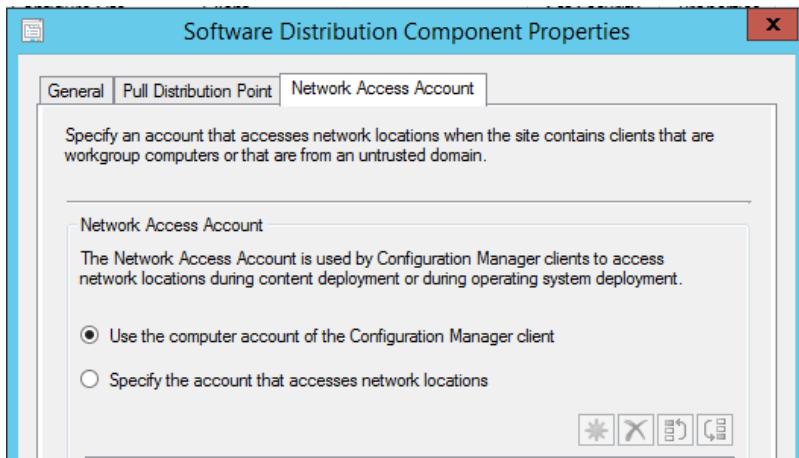
Path: D:\Program Files\Microsoft Configuration Manager\Logs

-- WCM.log
-- wsynmgr.log

12. Start synchronization in the SCCM console

Tips

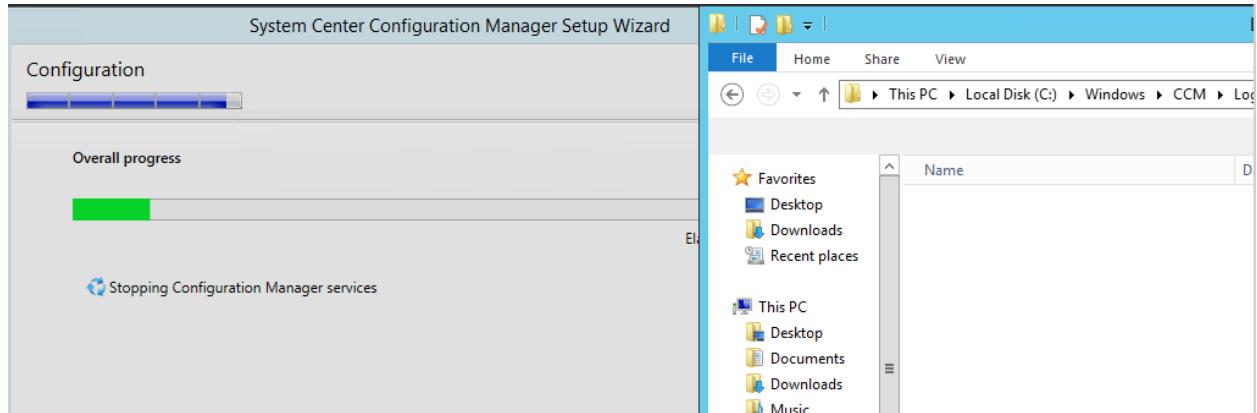
Use the computer account for the Software Distribution Component. If it fails, you can try the service account. That will tell you something is wrong with how System Management is set up in AD.



The Default System Site Roles

Icon	Role Name	Role Description
	Component server	Any server requiring a Configuration Manager service to be installed.
	Distribution point	A Configuration Manager server role that stages packages for distribution to clients.
	Management point	A site system role that replies to Configuration Manager client requests and accepts mana
	Service connection point	A service connection point connects Configuration Manager to Microsoft cloud services, a
	Site database server	A site system role that runs Microsoft SQL Server and hosts the Configuration Manager si
	Site server	The main site system role that hosts the Configuration Manager components and services
	Site system	A server or server share that hosts one or more site system roles for a Configuration Man

When repairing SCCM---using the SCCM Wizard---[backup] delete the logs, just to clear everything out.



Logs and Descriptions

This is a quick rundown of all the SCCM logs.

The client logs are located in the %WINDIR%\System32\CCM\Logs.

The SCCM server log files are located in the >INSTALL_PATH>\Logs or SMS_CCM\Logs folder. IIS logs can be found in %WINDIR%\System32\logfiles\W3SVC1 folder.

Client Log Files

- CAS – Content Access Service. Maintains the local package cache.
- Ccmexec.log – Records activities of the client and the SMS Agent Host service.
- CertificateMaintenance.log – Maintains certificates for Active Directory directory service and management points.
- ClientIDManagerStartup.log – Creates and maintains the client GUID.
- ClientLocation.log – Site assignment tasks.
- ContentTransferManager.log – Schedules the Background Intelligent Transfer Service (BITS) or the Server Message Block (SMB) to download or to access SMS packages.
- DataTransferService.log – Records all BITS communication for policy or package access.
- Execmgr.log – Records advertisements that run.
- FileBITS.log – Records all SMB package access tasks.
- Fsinvprovider.log (renamed to FileSystemFile.log in all SMS 2003 Service Packs) – Windows Management Instrumentation (WMI) provider for software inventory and file collection.
- InventoryAgent.log – Creates discovery data records (DDRs) and hardware and software inventory records.
- LocationServices.log – Finds management points and distribution points.
- Mifprovider.log – The WMI provider for .MIF files.
- Mtrmgr.log – Monitors all software metering processes.
- PolicyAgent.log – Requests policies by using the Data Transfer service.
- PolicyAgentProvider.log – Records policy changes.
- PolicyEvaluator.log – Records new policy settings.
- Remctrl.log – Logs when the remote control component (WUSER32) starts.
- Scheduler.log – Records schedule tasks for all client operations.
- Smscliui.log – Records usage of the Systems Management tool in Control Panel.
- StatusAgent.log – Logs status messages that are created by the client components.
- SWMTRReportGen.log – Generates a usage data report that is collected by the metering agent. (This data is logged in Mtrmgr.log.)

Server Log Files

- Ccm.log – Client Configuration Manager tasks.
- Cidm.log – Records changes to the client settings by the Client Install Data Manager (CIDM).
- Colleval.log – Logs when collections are created, changed, and deleted by the Collection Evaluator.
- Compsumm.log – Records Component Status Summarizer tasks.
- Cscnfsvc.log – Records Courier Sender confirmation service tasks.
- Dataldr.log – Processes Management Information Format (MIF) files and hardware inventory in the Configuration Manager 2007 database.
- Ddm.log – Saves DDR information to the Configuration Manager 2007 database by the Discovery Data Manager.
- Despool.log – Records incoming site-to-site communication transfers.
- Distmgr.log – Records package creation, compression, delta replication, and information updates.
- Hman.log – Records site configuration changes, and publishes site information in Active Directory Domain Services.
- Inboxast.log – Records files that are moved from the management point to the corresponding SMS\INBOXES folder.
- Inboxmgr.log – Records file maintenance.
- Invproc.log – Records the processing of delta MIF files for the Dataloader component from client inventory files.
- Mpcontrol.log – Records the registration of the management point with WINS. Records the availability of the management point every 10 minutes.
- Mpfdm.log – Management point component that moves client files to the corresponding SMS\INBOXES folder.
- MPMSI.log – Management point .msi installation log.
- MPSetup.log – Records the management point installation wrapper process.
- Ntsvrdis.log – Configuration Manager 2007 server discovery.
- Offermgr.log – Records advertisement updates.
- Offersum.log – Records summarization of advertisement status messages.
- Polcypv.log – Records updates to the client policies to reflect changes to client settings or advertisements.
- Replmgr.log – Records the replication of files between the site server components and the Scheduler component.
- Rsetup.log – Reporting point setup log.
- Sched.log – Records site-to-site job and package replication.
- Sender.log – Records files that are sent to other child and parent sites.
- Sinvproc.log – Records client software inventory data processing to the site database in Microsoft SQL Server.
- Sitecomp.log – Records maintenance of the installed site components.
- Sitectrl.log – Records site setting changes to the Sitectrl.ct0 file.
- Sitestat.log – Records the monitoring process of all site systems.
- Smsdbmon.log – Records database changes.
- Smsexec.log – Records processing of all site server component threads.

- Smsprov.log – Records WMI provider access to the site database.
- SMSReportingInstall.log – Records the Reporting Point installation. This component starts the installation tasks and processes configuration changes.
- SMSSHVSetup.log – Records the success or failure (with failure reason) of installing the System Health Validator point.
- Srvacct.log – Records the maintenance of accounts when the site uses standard security.
- Statmgr.log – Writes all status messages to the database.
- Swmproc.log – Processes metering files and maintains settings.

Admin Console Log Files

- RepairWizard.log – Records errors, warnings, and information about the process of running the Repair Wizard.
- ResourceExplorer.log – Records errors, warnings, and information about running the Resource Explorer.
- SMSAdminUI.log – Records the local Configuration Manager 2007 console tasks when you connect to Configuration Manager 2007 sites.

Management Point Log Files

- MP_Ddr.log – Records the conversion of XML.ddr records from clients, and copies them to the site server.
- MP_GetAuth.log – Records the status of the site management points.
- MP_GetPolicy.log – Records policy information.
- MP_Hinv.log – Converts XML hardware inventory records from clients and copies the files to the site server.
- MP_Location.log – Records location manager tasks.
- MP_Policy.log – Records policy communication.
- MP_Relay.log – Copies files that are collected from the client.
- MP_Retry.log – Records the hardware inventory retry processes.
- MP_Sinv.log – Converts XML hardware inventory records from clients and copies them to the site server.
- MP_Status.log – Converts XML.svf status message files from clients and copies them to the site server.

Mobile Device Management Log Files

- DmClientHealth.log – Records the GUIDs of all the mobile device clients that are communicating with the Device Management Point.
- DmClientRegistration.log – Records registration requests from and responses to the mobile device client in Native mode.

- DmpDatastore.log – Records all the site database connections and queries made by the Device Management Point.
- DmpDiscovery.log – Records all the discovery data from the mobile device clients on the Device Management Point.
- DmpFileCollection.log – Records mobile device file collection data from mobile device clients on the Device Management Point.
- DmpHardware.log – Records hardware inventory data from mobile device clients on the Device Management Point.
- Dmplsapi.log – Records mobile device communication data from device clients on the Device Management Point.
- dmpMSI.log – Records the MSI data for Device Management Point setup.
- DMPSsetup.log – Records the mobile device management setup process.
- DmpSoftware.log – Records mobile device software distribution data from mobile device clients on the Device Management Point.
- DmpStatus.log – Records mobile device status messages data from mobile device clients on the Device Management Point.
- Fsplsapi.log – Records Fallback Status Point communication data from mobile device clients and client computers on the Fallback Status Point.

Mobile Device Client Log Files

- DmCertEnroll.log – Records certificate enrollment data on mobile device clients.
- DMCertResp.htm (in \temp) – Records HTML response from the certificate server when the mobile device Enroller program requests a client authentication certificate on mobile device clients.
- DmClientSetup.log – Records client setup data on mobile device clients.
- DmClientXfer.log – Records client transfer data for Windows Mobile Device Center and ActiveSync deployments.
- DmCommonInstaller.log – Records client transfer file installation for setting up mobile device client transfer files on client computers.
- DmInstaller.log – Records whether DmInstaller correctly calls DmClientSetup and whether DmClientSetup exits with success or failure on mobile device clients.
- DmlnvExtension.log – Records Inventory Extension file installation for setting up Inventory Extension files on client computers.
- DmSvc.log – Records mobile device management service data on mobile device clients.

Operating System Deployment Log Files

- CCMSetup.log – Provides information about client-based operating system actions.
- CreateTSMedia.log – Provides information about task sequence media when it is created. This log is generated on the computer running the Configuration Manager 2007 administrator console.
- DriverCatalog.log – Provides information about device drivers that have been imported into the driver catalog.

- MP_ClientIDManager.log – Provides information about the Configuration Manager 2007 management point when it responds to Configuration Manager 2007 client ID requests from boot media or PXE. This log is generated on the Configuration Manager 2007 management point.
- MP_DriverManager.log – Provides information about the Configuration Manager 2007 management point when it responds to a request from the Auto Apply Driver task sequence action. This log is generated on the Configuration Manager 2007 management point.
- MP_Location.log – Provides information about the Configuration Manager 2007 management point when it responds to request state store or release state store requests from the state migration point. This log is generated on the Configuration Manager 2007 management point.
- Pxecontrol.log – Provides information about the PXE Control Manager.
- PXEMsi.log – Provides information about the PXE service point and is generated when the PXE service point site server has been created.
- PXESetup.log – Provides information about the PXE service point and is generated when the PXE service point site server has been created.
- Setupact.log Setupapi.log Setuperr.log Provide information about Windows Sysprep and setup logs.
- Smplsapi.log – Provides information about the state migration point Configuration Manager 2007 client request responses.
- Smpmgr.log – Provides information about the results of state migration point health checks and configuration changes.
- SmpMSI.log – Provides information about the state migration point and is generated when the state migration point site server has been created.
- Smsprov.log – Provides information about the SMS provider.
- Smspxe.log – Provides information about the Configuration Manager 2007 PXE service point.
- SMSMPSSetup.log – Provides information about the state migration point and is generated when the state migration point site server has been created.
- Smsts.log – General location for all operating system deployment and task sequence log events.
- TaskSequenceProvider.log – Provides information about task sequences when they are imported, exported, or edited.
- USMT Log loadstate.log – Provides information about the User State Migration Tool (USMT) regarding the restore of user state data.
- USMT Log scanstate.log – Provides information about the USMT regarding the capture of user state data.

Network Access Protection Log Files

- Ccmcca.log – Logs the processing of compliance evaluation based on Configuration Manager NAP policy processing and contains the processing of remediation for each software update required for compliance.
- CIAgent.log – Tracks the process of remediation and compliance. However, the software updates log file, *Updateshandler.log – provides more informative details on installing the software updates required for compliance.

- locationservices.log – Used by other Configuration Manager features (for example, information about the client's assigned site) but also contains information specific to Network Access Protection when the client is in remediation. It records the names of the required remediation servers (management point, software update point, and distribution points that host content required for compliance), which are also sent in the client statement of health.
- SDMAgent.log – Shared with the Configuration Manager feature desired configuration management and contains the tracking process of remediation and compliance. However, the software updates log file, Updateshandler.log, provides more informative details about installing the software updates required for compliance.
- SMSSha.log – The main log file for the Configuration Manager Network Access Protection client and contains a merged statement of health information from the two Configuration Manager components: location services (LS) and the configuration compliance agent (CCA). This log file also contains information about the interactions between the Configuration Manager System Health Agent and the operating system NAP agent, and also between the Configuration Manager System Health Agent and both the configuration compliance agent and the location services. It provides information about whether the NAP agent successfully initialized, the statement of health data, and the statement of health response.

System Health Validator Point Log Files

- Ccperf.log -Contains information about the initialization of the System Health Validator point performance counters.
- SmsSHV.log – The main log file for the System Health Validator point; logs the basic operations of the System Health Validator service, such as the initialization progress.
- SmsSHVADCacheClient.log – Contains information about retrieving Configuration Manager health state references from Active Directory Domain Services.
- SmsSHVCacheStore.log – Contains information about the cache store used to hold the Configuration Manager NAP health state references retrieved from Active Directory Domain Services, such as reading from the store and purging entries from the local cache store file. The cache store is not configurable.
- SmsSHVRegistrySettings.log – Records any dynamic changes to the System Health Validator component configuration while the service is running.
- SmsSHVQuarValidator.log – Records client statement of health information and processing operations. To obtain full information, change the registry key LogLevel from 1 to 0 in the following location: HKLM\SOFTWARE\Microsoft\SMSSHV\Logging\@GLOBAL

Desired Configuration Management Log Files

- ciagent.log – Provides information about downloading, storing, and accessing assigned configuration baselines.
- dcagent.log – Provides high-level information about the evaluation of assigned configuration baselines and desired configuration management processes.

- discovery.log – Provides detailed information about the Service Modeling Language (SML) processes.
- sdmagent.log – Provides information about downloading, storing, and accessing configuration item content.
- sdmdiscagent.log – Provides high-level information about the evaluation process for the objects and settings configured in the referenced configuration items.

Wake On LAN Log Files

- Wolmgr.log – Contains information about wake-up procedures such as when to wake up advertisements or deployments that are configured for Wake On LAN.
- WolCmgr.log – Contains information about which clients need to be sent wake-up packets, the number of wake-up packets sent, and the number of wake-up packets retried.

Software Updates Site Server Log Files

- cimgr.log – Provides information about the addition, deletion, and modification of software update configuration items.
- distmgr.log – Provides information about the replication of software update deployment packages.
- objreplmgr.log – Provides information about the replication of software updates notification files from a parent to child sites.
- PatchDownloader.log – Provides information about the process for downloading software updates from the update source specified in the software updates metadata to the download destination on the site server.
- replmgr.log – Provides information about the process for replicating files between sites.
- smsdbmon.log – Provides information about when software update configuration items are inserted, updated, or deleted from the site server database and creates notification files for software updates components.
- SUPSetup – Provides information about the software update point installation. When the software update point installation completes, Installation was successful is written to this log file.
- WCM.log – Provides information about the software update point configuration and connecting to the Windows Server Update Services (WSUS) server for subscribed update categories, classifications, and languages.
- WSUSCtrl.log – Provides information about the configuration, database connectivity, and health of the WSUS server for the site.
- wsyncmgr.log -Provides information about the software updates synchronization process.

WSUS Server Log Files

- Change.log – Provides information about the WSUS server database information that has changed.
- SoftwareDistribution.log – Provides information about the software updates that are synchronized from the configured update source to the WSUS server database.

Software Updates Client Computer Log Files

- CAS.log – Provides information about the process of downloading software updates to the local cache and cache management.
- CIAgent.log – Provides information about processing configuration items, including software updates.
- LocationServices.log – Provides information about the location of the WSUS server when a scan is initiated on the client.
- PatchDownloader.log – Provides information about the process for downloading software updates from the update source to the download destination on the site server. This log is only on the client computer configured as the synchronization host for the Inventory Tool for Microsoft Updates.
- PolicyAgent.log – Provides information about the process for downloading, compiling, and deleting policies on client computers.
- PolicyEvaluator – Provides information about the process for evaluating policies on client computers, including policies from software updates.
- RebootCoordinator.log – Provides information about the process for coordinating system restarts on client computers after software update installations.
- ScanAgent.log – Provides information about the scan requests for software updates, what tool is requested for the scan, the WSUS location, and so on.
- ScanWrapper – Provides information about the prerequisite checks and the scan process initialization for the Inventory Tool for Microsoft Updates on Systems Management Server (SMS) 2003 clients.
- SdmAgent.log – Provides information about the process for verifying and decompressing packages that contain configuration item information for software updates.
- Service WindowManager.log – Provides information about the process for evaluating configured maintenance windows.
- smscliUI.log – Provides information about the Configuration Manager Control Panel user interactions, such as initiating a Software Updates Scan Cycle from the Configuration Manager Properties dialog box, opening the Program Download Monitor, and so on.
- SmsWusHandler – Provides information about the scan process for the Inventory Tool for Microsoft Updates on SMS 2003 client computers.
- StateMessage.log – Provides information about when software updates state messages are created and sent to the management point.
- UpdatesDeployment.log – Provides information about the deployment on the client, including software update activation, evaluation, and enforcement. Verbose logging shows additional information about the interaction with the client user interface.
- UpdatesHandler.log – Provides information about software update compliance scanning and about the download and installation of software updates on the client.
- UpdatesStore.log – Provides information about the compliance status for the software updates that were assessed during the compliance scan cycle.
- WUAHandler.log – Provides information about when the Windows Update Agent on the client searches for software updates.

- WUSSyncXML.log – Provides information about the Inventory Tool for the Microsoft Updates synchronization process. This log is only on the client computer configured as the synchronization host for the Inventory Tool for Microsoft Updates.

Windows Update Agent Log File

- WindowsUpdate.log – Provides information about when the Windows Update Agent connects to the WSUS server and retrieves the software updates for compliance assessment and whether there are updates to the agent components.

[more...](#)

Client Error/Return Codes

Error Code	Meaning
0	Success
6	Error
7	Reboot Required
8	Setup already running
9	Prerequisite evaluation failure
10	Setup manifest hash validation failure

Server Error/Return Codes

Error Code	Source	Meaning	Solution
2		The system cannot find the file specified This error occur when the WMI service is corrupt	TechNet Resolution WMI Repair
5		Access denied	Make sure that the installation account is member of the Administrator Group
52		You were not connected because a duplicate name exists on the network	Check for duplicate name in DNS (IP)
53		Unable to locate Cannot connect to admin\$ Computer Browser not started	Add File & Print sharing to Exceptions in Firewall Turn file and print on KB920852
58		The specified server cannot perform the requested operation	

64	Windows	The specified network name is no longer available	
67		Network name cannot be found	Check if client has a DNS entry or invalid DNS
86		Incorrect network configuration	
112		Not enough disk space	Free some space on the computer
1003		Cannot complete this function	
1053		The service did not respond to the start or control request in a timely fashion	
1068		The dependency service or group failed to start	
1130	Windows	Not enough server storage is available to process this command	

1203		The network path was either typed incorrectly, does not exist, or the network provider is not currently available Please try retyping the path or contact your network administrator	
1208	Windows	An extended error has occurred	
1305		The revision level is unknown	
1396	Login Failure	The target account name is incorrect	Check for duplicate name in DNS (IP) NBTSTAT -a reverse lookup
1450	Windows	Insufficient system resources exist to complete the requested service	
1603		CCMExec could not be stopped	Reboot and install the client as administrator
1618	MSI	This error is caused by a multiple client.msi installation at the same time	Stop all related MSI install process

1789		The trust relationship between this workstation and the primary domain failed	<u>KB2771040</u>
12002		Failed to send HTTP Request	Check firewall ports
8007045D	MSI	Setup was unable to create the WMI namespace CCM	Delete all SCCM folders and rebuilt WMI Repository
800706BA	WMI	Unable to connect to WMI on remote machine	<u>See post</u>
80041001	MSI	Setup was unable to create the WMI namespace CCM Warning 25101. Setup was unable to delete WMI namespace CIMV2\SMS	<u>WMI Repair</u>
8004103B	WMI	Unable to create the WMI Namespace	Rebuild WMI Repository
80070070		Setup failed due to unexpected circumstances	Rebuild WMI Repository
87D0029E	WMI	CCMSetup Failed	<u>See post</u>
2147023174		The RPC server is unavailable	Check out firewall or Anti-Virus

2147024891		Access is denied	
2147749889	WMI	Generic failure	
2147749890	WMI	Not found	<u>WMI Repair</u>
2147749904	WMI	Invalid class	
2147749908	WMI	Initialization failure	
2147942405		Access is Denied	Missing Firewall rules McAfee-HIPS
2147944122		The RPC server is unavailable	<u>KB899965</u> Dcom is miss-configured for security
2148007941		Server Execution Failed	

CCMEval and Remediation

There are a number of checks that are performed by CCMEval and remediation can range from enabling a service to reinstalling the client:

CCMEval Task	Potential Remediation Action	Task Description
Verify CCMEval task has run in recent cycles.	Launch CCMEval from CCMExec	Check if the scheduled task has executed at least once in the past three days
Verify/Remediate client prerequisites.	Install ConfigMgr prerequisites	Checks for prerequisites listed in ccmsetup.xml
WMI Repository Integrity Test.	Reinstall Configuration Manager client	Check the existence of some CM's important WMI classes/namespace/instance
Verify/Remediate SMS Agent Host status.	Restart SMS Agent Host Service	Checks SMS Agent Host status
WMI Event Sink Test.	Restart CCMExec	Check whether CM's related WMI event sink is lost
Verify WMI service exists	No remediation	Checks for WMI service

Verify/Remediate client installation.	Attempts to reinstall client	Verifies that client is installed
---------------------------------------	------------------------------	-----------------------------------

WMI Repository Read/Write Test.	Reset WMI repository and reinstall Configuration Manager client	Performs WMI repository read/write test
---------------------------------	---	---

Verify/Remediate Antimalware service status.	Reset service status to Manual	Checks antimalware service status
--	--------------------------------	-----------------------------------

Verify/Remediate Antimalware service startup type.	Reset service status to Running	Checks antimalware service startup type
--	---------------------------------	---

Verify/Remediate Windows Update service startup type.	Reset service startup type to Automatic	Checks Windows Update service startup type
---	---	--

Verify/Remediate SMS Agent Host startup type.	Reset service startup to Automatic	Checks SMS Agent Host startup type
---	------------------------------------	------------------------------------

Verify/Remediate WMI service status.	Reset service status to Running	Checks WMI service status
--------------------------------------	---------------------------------	---------------------------

Verify/Remediate SQL CE database is healthy.	CCMEval on next run will notice flag and repair client, thereby creating a new/empty CCMStore.sdf. Then runs global evaluation again to repopulate data	Checks if CCMStore.sdf exists, can be opened and calls the SQL CE Verify DB API on the CCMStore.sdf. Checks done by client on startup, if validation fails DB removed and this state is flagged.
--	---	--

Verify/Remediate Microsoft Policy Platform service	Reset service status to Manual	Check Lantern Service Startup type
--	--------------------------------	------------------------------------

Verify BITS service exists.	No Remediation	Checks for BITS service
-----------------------------	----------------	-------------------------

Verify/Remediate BITS	Reset service startup to Automatic	Checks BITS service startup type
-----------------------	------------------------------------	----------------------------------

Verify/Remediate Network Inspection service startup	Reset service startup type to Manual if installed	Checks if Network Inspection service is installed and if so checks service startup type
---	---	---

Verify/Remediate WMI service startup type.	Reset service startup to Automatic	Checks WMI service startup type
--	------------------------------------	---------------------------------

Verify/Remediate Windows Reset service startup type to Checks Windows Update service
Update service startup type Automatic startup type
on Windows 8.

Verify SMS Agent Host No Remediation Check for SMS Agent Host service
service exists.

Verify/Remediate Client Obsolete task Obsolete task
language packs.

Verify/Remediate Windows Reset service status to Active Checks Windows Update service status
Update Service status

Verify/Remediate Reset service startup type to Checks CM Remote Control service
Configuration Manager Automatic startup type
Remote Control service
startup type

Verify/Remediate Reset service status to Active Checks CM Remote Control service
Configuration Manager status
Remote Control service
status

Hardware Requirements

Site Servers

Use the following recommendations for each Configuration Manager site server.

Site details	Suggested minimum configuration
<p>Central administration site with the Standard edition of SQL Server</p> <ul style="list-style-type: none">• SQL Server is located on the site server computer.• This configuration supports a hierarchy with up to 50,000 clients.	<ul style="list-style-type: none">• 8 cores (Intel Xeon 5504 or comparable CPU)• 32 GB of RAM• 300 GB of disk space for the operating system, Configuration Manager, SQL Server, and all database files.
<p>Central administration site with the Enterprise or Datacenter edition of SQL Server</p> <ul style="list-style-type: none">• SQL Server is located on the site server computer• This configuration supports a hierarchy with up to 400,000 clients• Beginning with System Center 2012 R2 Configuration Manager with cumulative update 3, this configuration supports 500,000 clients.	<ul style="list-style-type: none">• 16 cores (Intel Xeon L5520 or comparable CPU)• 64 GB of RAM• 1.5 TB of disk space for the operating system, Configuration Manager, SQL Server, and all database files.
<p>Beginning with System Center 2012 Configuration Manager SP2:</p> <p>Central administration site with the Enterprise or Datacenter edition of SQL Server</p> <ul style="list-style-type: none">• SQL Server is located on the site server computer• This configuration supports a hierarchy with up to 600,000 clients	<ul style="list-style-type: none">• 16 cores (Intel Xeon E5-2650 v2 or comparable CPU)• 128 GB of RAM• 2.5 TB of disk space for the operating system, Configuration Manager, SQL Server, and all database files.

<p>Stand-alone primary site</p> <ul style="list-style-type: none"> • Up to 100,000 clients • SQL Server is installed on the site server computer 	<ul style="list-style-type: none"> • 8 cores (Intel Xeon E5504 or comparable CPU) • 32 GB of RAM • 550 GB hard disk space for the operating system, SQL Server, and all database files
<p>Beginning with System Center 2012 Configuration Manager SP2:</p> <p>Stand-alone primary site</p> <ul style="list-style-type: none"> • Up to 150,000 clients • SQL Server is installed on the site server computer 	<ul style="list-style-type: none"> • 16 cores (Intel Xeon E5-2650 v2 or comparable CPU) • 64 GB of RAM • 900 GB hard disk space for the operating system, SQL Server, and all database files
<p>Primary site in a hierarchy</p> <ul style="list-style-type: none"> • Up to 50,000 clients • SQL Server is installed on the site server computer. 	<ul style="list-style-type: none"> • 4 cores (Intel Xeon 5140 or comparable CPU) • 16 GB of RAM • 300 GB of hard disk space for the operating system, Configuration Manager, SQL Server, and all database files.
<p>Primary site in a hierarchy</p> <ul style="list-style-type: none"> • Up to 100,000 clients • SQL Server is remote from the site server computer 	<p>Site Server:</p> <ul style="list-style-type: none"> • 4 cores (Intel Xeon 5140 or comparable CPU) • 8GB of RAM • 200 GB of disk space for the operating system and Configuration Manager. <p>Remote SQL Server:</p> <ul style="list-style-type: none"> • 8 cores (Intel Xeon E5504 or comparable CPU) • 32 GB of RAM

	<ul style="list-style-type: none">• 550 GB of hard disk space for the operating system, SQL Server, and all database files.
Secondary site <ul style="list-style-type: none">• Communications from up to 5,000 clients• SQL Server must be installed on the site server computer	<ul style="list-style-type: none">• 4 cores (Intel Xeon 5140 or comparable CPU)• 8 GB of RAM• 100 GB of hard disk space for the operating system, Configuration Manager, SQL Server, and all database files.
Beginning with System Center 2012 Configuration Manager SP2: Secondary site <ul style="list-style-type: none">• Communications from up to 10,000 clients• SQL Server must be installed on the site server computer	<ul style="list-style-type: none">• 4 cores (Intel Xeon E5504 or comparable CPU)• 16 GB of RAM• 127 GB of hard disk space for the operating system, Configuration Manager, SQL Server, and all database files.

Disk Space Configurations

Because disk allocation and configuration contributes to the performance of System Center 2012 Configuration Manager, disk space requirements can be greater than for previous product versions. Use the following information as guidelines when you determine the amount of disk space Configuration Manager requires. Because each Configuration Manager environment is different, these values can vary from the following guidance.

For the best performance, place each object on a separate, dedicated RAID volume. For all data volumes (Configuration Manager and its database files), use RAID 10 for the best performance.

Reference

(1) shabaztech.com

<https://docs.microsoft.com/en-us/sccm/core/get-started/set-up-your-lab>

<https://sccmentor.com/2014/01/08/sccm-2012-r2-step-by-step-installation-guide/>

<https://social.technet.microsoft.com/wiki/contents/articles/25696.how-to-uninstall-or-remove-sccm-client.aspx>

http://www.sqlservercentral.com/blogs/rocks/2012/01/09/revised-difference-between-collation-sql_latin1_general_cp1_ci_as-and-latin1_general_ci_as/

<https://technet.microsoft.com/en-us/library/hh427342.aspx?f=255&MSPError=-2147217396>

Other Notes

CCMSetup.exe /mp:SMSMP01 /UsePKICert SMSSITECODE=AUTO CCMHTTPSSTATE=63

About the Author



Eddie Jackson is a computer systems engineer, working for the Kaplan, Inc. Information Technology Department. His credentials include over 30 computer and network certifications, a B.Sc. degree in Liberal Studies (2013) and a M.Sc. degree in Information Technology Security Assurance (2015). His discipline in the field of technology has been recognized by multiple companies and employers, where he has been nominated and presented with numerous awards. Over the years, he has written hundreds of technical documents, authored white papers, and created training videos in the areas of computer science and information technology. His professional career started in 1994, where he worked in computer repair and provided end-user support for hardware and software. He transitioned into network administration, and eventually into desktop engineering, which evolved into computer systems engineering. From there, he pioneered scripts and applications to automate thousands of server and desktop processes. His knowledge and professional research span a wide-range of technology topics, including scripting, programming, encryption, mathematics, ethics, databases, and the maintenance and administration of technology-based systems.

Contact

For questions, to submit a correction, or just general communication, please contact the author at:

MrNetTek@gmail.com : eddiejackson.net