

1	Server Setup.....	4
1.1	Creating Needed Active Directory Objects .....	4
1.1.1	Add Users & Groups to Active Directory.....	4
1.1.2	Set SPN Attributes.....	5
1.1.3	Create System Management Container.....	6
1.2	Prepare Active Directory Schema .....	7
1.3	Prepare SCCM Server for Multiple Sites/Servers.....	7
1.4	Limit Drives for Site Server Roles.....	8
1.5	Install Role & Feature prerequisites .....	8
1.5.1	Add Features and Roles .....	8
1.6	Install Microsoft SQL Server.....	10
1.7	Set Microsoft SQL Server Memory Restrictions.....	16
1.8	Install Microsoft Administration Deployment Kit.....	18
2	Install SCCM .....	21
2.1	Create a Downloads folder in root of the S: Drive.....	21
2.2	Download SCCM.....	21
2.3	Install SCCM .....	21
3	Configure SCCM .....	24
3.1	Configure Discovery Methods.....	24
3.2	Configure Boundaries .....	28
3.3	Configure Site Roles / Endpoint Protection .....	29
3.4	Configure Network Access Account.....	30
3.5	Configure Client Agent Installation Method .....	31
3.6	Configure Client Agent Settings .....	33
3.6.1	Client Cache Settings.....	33
3.6.2	Computer Agent.....	33
3.6.3	Endpoint Protection.....	33
3.6.4	Remote Tool.....	34
3.7	Configure Site Deployment Verification .....	35
3.8	Enable PXE support .....	36
3.8.1	DHCP Settings for PXE .....	37

4	Collections.....	38
4.1	Creating Device Collection .....	38
4.1.1	To configure a query rule.....	39
4.1.2	To configure a direct rule.....	42
4.2	Set Collection Variables for Imaging.....	43
5	Software Deployment.....	44
5.1	Software Distribution Share.....	44
5.2	Software Package.....	45
5.2.1	Create Software Package .....	45
5.2.1.1	JAVA (EXE INSTALL).....	45
5.2.2	Distribute Software Package.....	47
5.2.3	Deploy Software Package - Required.....	48
5.2.4	Deploy Software Package – Available.....	50
5.3	Software Application.....	50
5.3.1	Adobe Reader.....	50
5.3.2	Chrome.....	53
5.3.3	Deploy Office 2019 – Office 365 .....	55
5.4	Distribute Software Application.....	59
5.5	Deploy Software Application .....	60
5.6	Update / Supersede Application.....	61
6	Configure Operating System Deployment (Imaging).....	62
6.1	Copy Source Images.....	62
6.2	Customize & Distribute Boot Images to the Distribution Points .....	62
6.3	Capture Prepared Windows Image.....	65
6.4	Add Operating System DVD Image (Install.WIM) .....	68
6.5	Add Operating System Captured Image (CapturedWindows10.WIM).....	69
6.6	Create the Base (DVD) Operating System Installation Task Sequence.....	72
6.7	Create the Captured Image Deployment Installation Task Sequence .....	77
6.8	Deploy the Base DVD OS Install Task Sequence. ....	80
6.9	Add Software Applications/Packages to Image Task Sequence. ....	81
6.10	Import Device Drivers .....	85
7	Configuring Reporting Services.....	88
7.1	Install the Reporting Services Point Role .....	88
7.2	Configure Reporting.....	88
8	Backup and Restore SCCM Primary Site .....	89

8.1 Backup SCCM Site Server ..... 90

8.2 Restore SCCM Site Server ..... 93

# 1 Server Setup

- 1 Server built based on APSCN LAN Support installation document.
- 2 Server Volumes
  - C: 100 GB – System (*recommended at least 100 GB in production environment*)
  - Q: 100 GB – SQL Database (*recommended **at least** 100 GB in production*)
  - S: 200 GB – SCCM Installation & Distribution Files (*recommended **at least** 200 GB*)
- 3 Server must be FULLY patched (including **.NET Frameworks 4 – All Windows Updates Ran**).
- 4 If Server OS was from an image, SYSPREP must be run on target hardware.
- 5 Verify Active Directory Sites and Services Configuration. Sites must be created, and subnets assigned.
- 6 Verify in DNS that reverse lookup zones have been created for IP Subnets.
- 7 If Windows Firewall (or any software-based firewall), ensure that proper ports are opened to client stations.
- 8 SQL Server and SCCM installed on same physical hardware and Windows installation instance.

## 1.1 Creating Needed Active Directory Objects

### 1.1.1 Add Users & Groups to Active Directory

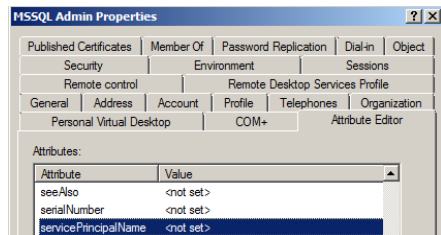
\*On **DC-1** Domain Controller

- 1 Create Security Group "**MSSQL Admins**"
- 2 Create User "**MSSQL Admin**" (*Used for MS SQL Service Account*).
- 3 Add "**MSSQL Admin**" User to "**MSSQL Admins**" Security Group
- 4 Create Security Group "**SCCM Admins**"
- 5 Create User "**SCCM Admin**" (*Used to give SCCM admin rights on all workstations*).
- 6 Add "**SCCM Admin**" user account to **Domain Admins** Security Group, **MSSQL Admins** Security Group, and **SCCM Admins** Security Group. (*This can be tightened down later*)
- 7 Create Security Group "**SCCM Servers**" and add your SCCM Server/Servers to be members of "**SCCM Servers**" Security Group.

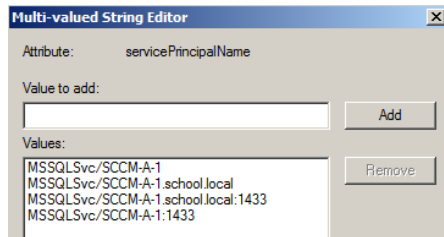
## 1.1.2 Set SPN Attributes

\*On **DC-1** Domain Controller

- 1 Open **Active Directory Users and Computers**
- 2 Click on **View** on the menu bar
- 3 Click **Advanced Features**
- 4 Find the <YOUR\_DOMAIN>\MSSQL Admin user
- 5 **Right Click** and Click **Properties**



- 6 **Attribute Editor** tab -> **ServicePrincipalName** -> **Edit**. Add the following:



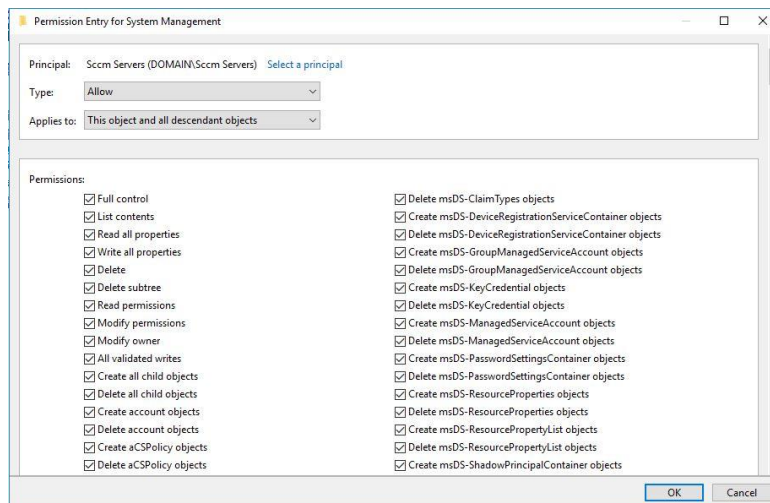
- **MSSQLSvc/<YOUR\_SCCM\_SERVER>**
- **MSSQLSvc/<YOUR\_SCCM\_SERVER>.<YOUR\_DOMAIN>.local**
- **MSSQLSvc/<YOUR\_SCCM\_SERVER>.<YOUR\_DOMAIN>.local:1433**
- **MSSQLSvc/<YOUR\_SCCM\_SERVER>:1433**

### 1.1.3 Create System Management Container

\*On **DC-1** Domain Controller

Create System Management Container in ADSI Editor and Add “SCCM Servers” Security group to System Management with Full Control to this object.

- 1 Click **ADSI Edit** and Connect to **Default naming context**. Click **OK**
- 2 Double Click Default naming context and browse down and find **CN=System**
- 3 Right Click **System** and Select **New -> Object-> Container**. Click Next
- 4 Name the Container **System Management** and Click **Next** and **Finish**.
- 5 Right Click this new container and Click **Properties**. Go to the **Security Tab**.
- 6 Click **Advanced-> Add**. Click on **Select a Principle** and add **SCCM Servers** group object.
- 7 Allow **Full control** and make sure the **Applies to** drop down box is set to **This object and all descendant objects**. Click and **Ok** then exit **ADSI Edit**.



## 1.2 Prepare Active Directory Schema

\* On the **Doman Controller** running the **Schema Master** role: (*netdom /query fsmo*)

- 1 Mount SCCM Installation ISO
- 2 Open **Command Prompt**
- 3 Use command **CD** to change directory to newly mounted ISO
- 4 Type **CD SMSSETUP\BIN\x64** and Press Enter
- 5 Type **EXTADSCH.EXE** and Press <enter>
- 6 **\*\*Close the command prompt when you receive the **Successfully extended the Active Directory schema** message.**
- 7 You can check the log file for errors at **C:\ExtADSch.log**
- 8 Unmount the SCCM Installation ISO

## 1.3 Prepare SCCM Server for Multiple Sites/Servers

\*On **SCCM Servers**, Add object to the Local **Administrators Group**

- 1 Right click the start/Windows button
- 2 Click **Computer Management**
- 3 Select **Local Users and Groups -> Groups -> Administrators**
- 4 Click **Add**
- 5 Add the following to the local **Administrators** Security group.
  - 1.a <YOUR\_DOMAIN>\MSSQL Admins
  - 1.b <YOUR\_DOMAIN>\SCCM Admins
  - 1.c <YOUR\_DOMAIN>\SCCM Server

## 1.4 Limit Drives for Site Server Roles

\*On <YOUR\_SCCM\_SERVER>

To prevent Configuration Manager from installing files on a specific drive.

- 1 In a new **File Explorer** screen click **View** -> **Change Folder and Search Options**
- 2 Click the **View** tab -> Select **Show hidden files, folders, and drive** -> **UNCHECK** the box next to **Hide extensions for known file types**
- 3 Click **Apply** -> **Ok**
- 4 Navigate to **System Drive (C:)** -> Right click and select **New** -> **Text Document**
- 5 Name this document **no\_sms\_on\_drive.sms** (Make sure the file extension is **.sms** **NOT .txt**) Click **Yes** when prompted about the file becoming unusable.
- 6 Copy the **no\_sms\_on\_drive.sms** file at the root folder of the **SQL Drive (Q:)** and any other drive that you want to prevent Configuration Manager from installing files on. **This will include any USB or External Drives you have connected to the server.**

## 1.5 Install Role & Feature prerequisites

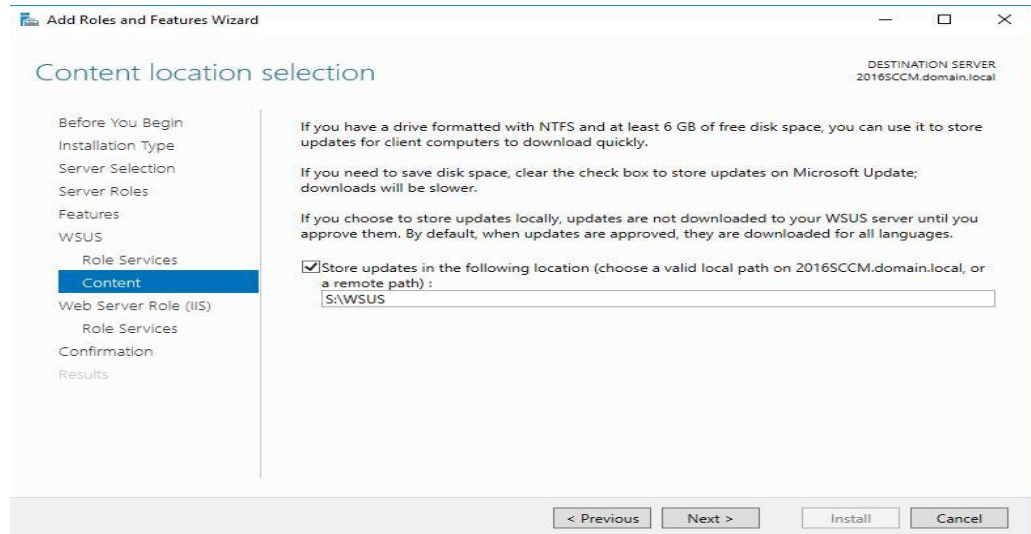
### 1.5.1 Add Features and Roles

\*On <YOUR\_SCCM\_SERVER> – Be sure to be logged in as **DOMAIN Administrator I.E. <YOUR\_DOMAIN>\Administrator. DO NOT LOG IN AS YOURSELF EVEN IF YOU ARE A MEMBER OF THE DOMAIN ADMIN SECURITY GROUP!!** This applies to any install and management of any server related tasks including SQL, SCCM, etc.

1. Mount **Windows Server (2016/2012) ISO** for future use
2. In **Server Manager**, select **Manage** -> **Add Roles and Features**
3. Select **Role-based or feature-based installation** -> **Next**
4. On the **Server Selection** page make sure your server is selected -> **Next**
5. Select the box next to **Windows Server Update Services** (Click **Add Features** in the pop-up)
6. On the Features page, select the following features:
  - A. Select **.Net Framework 3.5 Features**
    - **.Net Framework 3.5** (this is listed under the **.Net Framework 3.5 Features**)
    - **HTTP Activation** (Click **Add Features** in the pop-up)

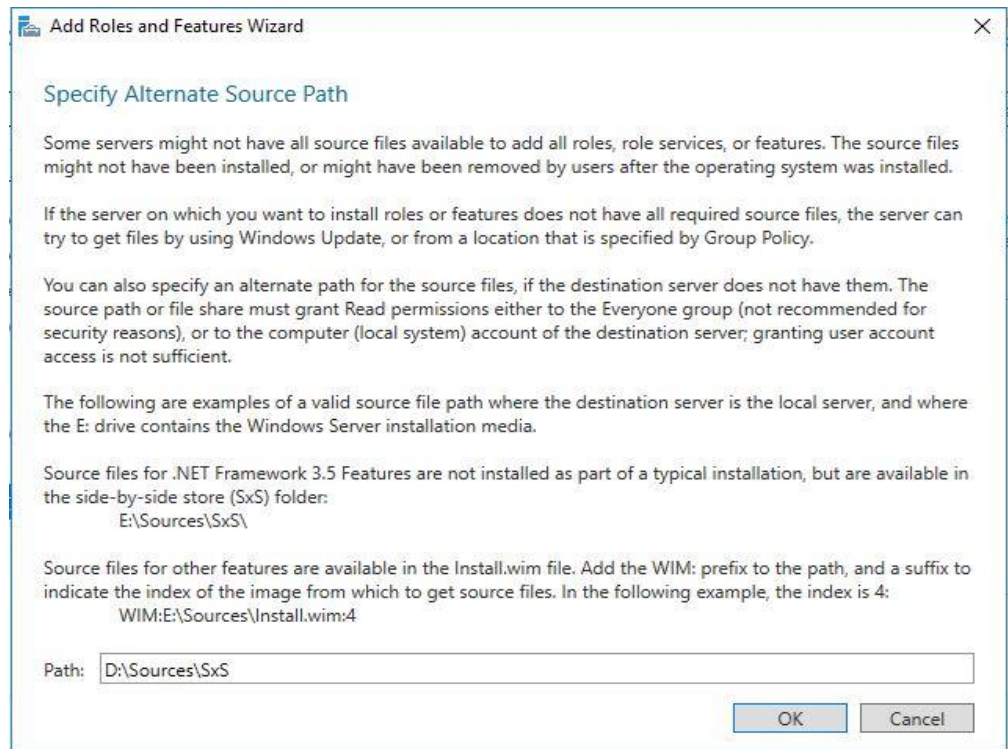


- B. Select **Background Intelligent Transfer Service (BITS)** - (Click **Add Features** in the pop-up)
  - C. Select **Remote Differential Compression**
  - D. Click **Next**
7. On the **WSUS** page click **Next**
  8. On the **Role Services** page click **Next**
  9. On the **Content** page type **<Your\_SCCM\_Volume\_Drive\_Letter>:\WSUS** in the empty box and click **Next**



10. On the **Web Server Role (IIS)** page, click **Next**
11. On the **Role Services** page, leave the defaults already selected and select the following additional options:
  - A. Under **Common HTTP Features** select:
    - **WebDAV Publishing**
  - B. Under **Application Development** select:
    - **ASP**
  - C. Under **Management Tools -> IIS 6 Management Compatibility** select:
    - **IIS 6 WMI Compatibility**
  - D. Under **Management Tools** select:
    - **IIS Management Scripts and Tools**

12. On the **Confirmation** page you will see a yellow banner across the top asking if you need to “**specify an alternate source path?**” You do need to do this.
  - A. Select **Specify an alternate source path** in blue letters at the bottom of the page
  - B. In the **Path** text box, type <Your\_Mounted\_ISO\_Drive\_Letter>:\Sources\SxS



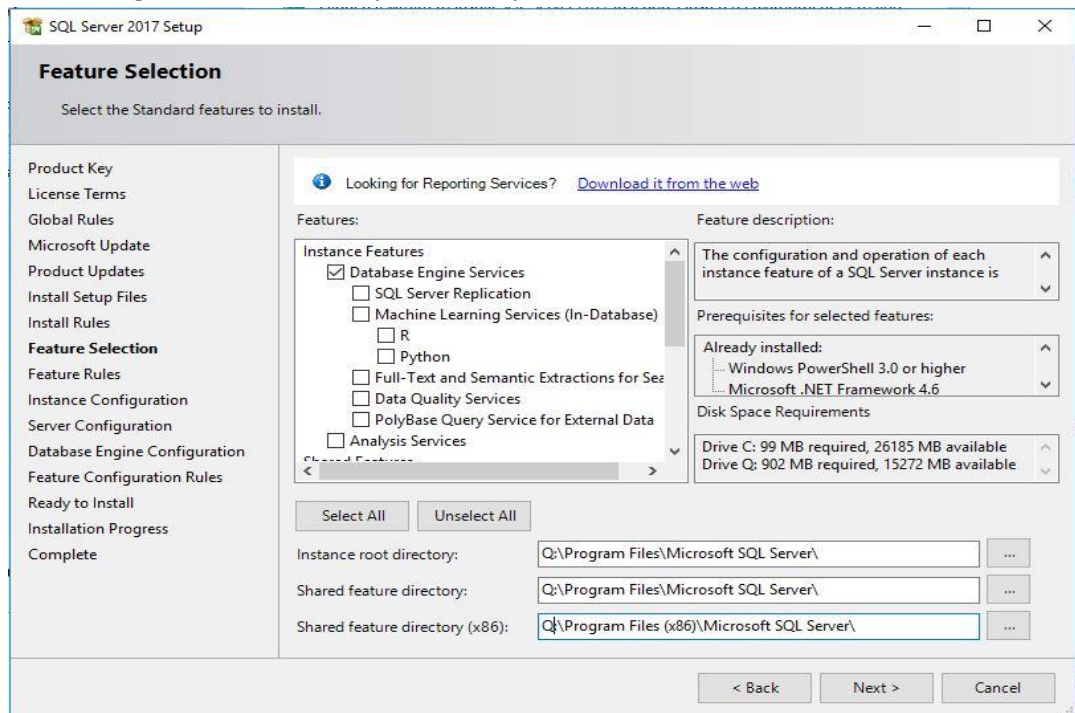
13. Click **OK** -> **Install**.
14. After the install completes, go to your **Server Manager**, click the flag in the top right and run **Post-Installation Configuration**
15. **Restart** your server upon completion.

## 1.6 Install Microsoft SQL Server

\*On <YOUR\_SCCM\_SERVER>

1. Verify that Windows Firewall is disabled for SQL Installation.
2. Mount the SQL Server 2016 Installation ISO on your **SCCM Server**.
3. Navigate to the mounted ISO and run **setup.exe**
4. **NOTE:** You may be prompted to enable **.NET Framework Core role**. Click **OK** on this message.

- 5 Once the SQL Server Installation Center screen comes up, click **Installation** on the left side of the window.
- 6 Click ***New SQL Server stand-alone installation or add features to an existing installation.***
- 7 Enter the **Product Key** from your **Volume Licensing Agreement Portal -> Next**
- 8 Put a check in the box next to **I accept the license terms -> Next**
- 9 SQL 2016 will auto update and install needed files. Wait for it to complete.
- 10 On the **Feature Selection** page, select the following:
  - A. Check the box next to **Database Engine Service**
  - B. **NOTE:** If you are using SQL 2012 or 2014, you will also need to select **Management Tools and Reporting Service.**
  - C. **NOTE:** If you are using SQL 2016 or above, Management Tools and Reporting Service will be a separate install.
- 11 Change your **Instance root directory** drive letter to that of your SQL partition (**Q:\**) and delete **Program Files** from the path already listed. Click **Next.**



- 12 On the **Instance Configuration** page, click **Next**

13 On the **Server Configuration** page, change the **Account Name, Password and Startup Type** fields to match the list below then click **Next**:

**A. SQL Server Agent**

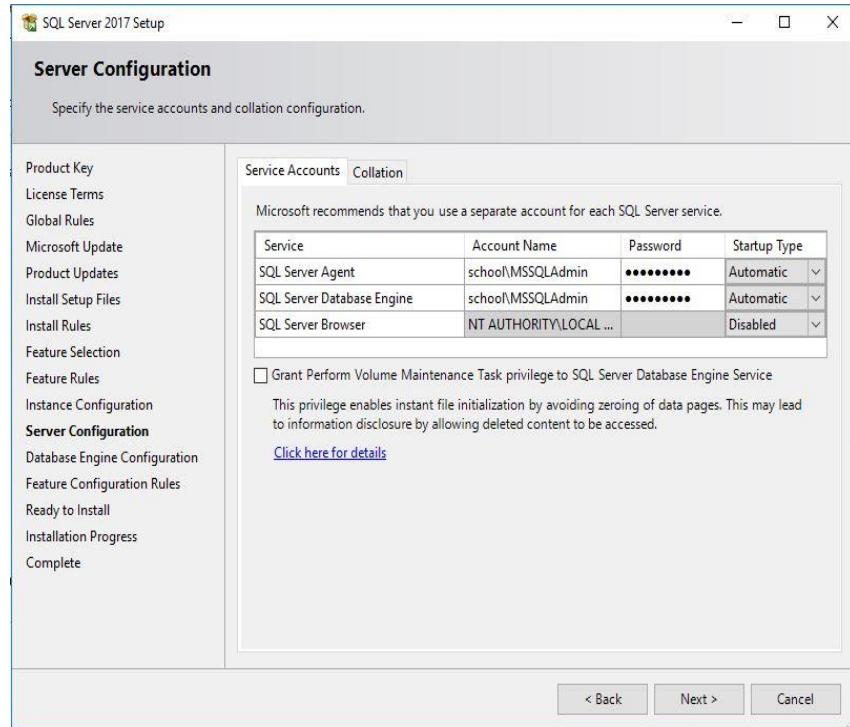
- i. **Account Name – <YOUR\_DOMAIN>\MSSQL.Admin**
- ii. Enter the **Password**
- iii. **Startup Type – Automatic**

**B. SQL Server Database Engine**

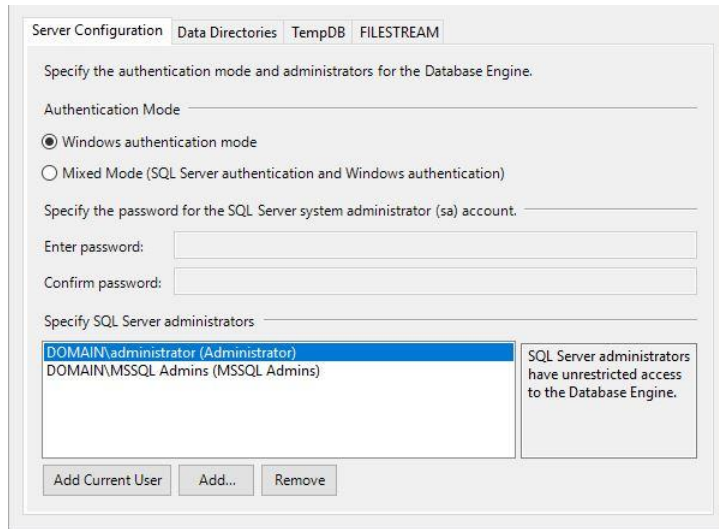
- i. **Account Name – <YOUR\_DOMAIN>\MSSQL.Admin**
- ii. Enter the **Password**
- iii. **Startup Type - Automatic**

**C. SQL Server Browser**

- i. **LEAVE THE DEFAULT SETTINGS ALREADY IN PLACE**



- 14 On the **Database Engine Configuration** page, select **Add Current User** then select **Add** and add the **MSSQL Admins Security Group** and click **Next**.



- 15 On the **Feature Configuration Rules** page, click **Next**.

- 16 On the **Ready to Install** page, click **Install**.

- 17 Verify all Features installed with a Status of **Succeeded**.

Information about the Setup operation or possible next steps:

Feature	Status
✓ Reporting Services - Native	Succeeded
✓ Database Engine Services	Succeeded
✓ SQL Browser	Succeeded
✓ SQL Writer	Succeeded
✓ SQL Client Connectivity	Succeeded
✓ SQL Client Connectivity SDK	Succeeded

**NOTE: The next 7 steps are for those using SQL 2016 and above ONLY**

- 18 Open the **SQL Server Installation Center** window that should still be open from installing the SQL Database above.
- 19 Select **Install SQL Server Management Tools**. This will open a browser window allowing you to download the latest version of the **SQL Server Management Studio**.

- 20 Select **Download SQL Server Management Studio (16.5.3)** Note: This version number is subject to change at any time. Please select the latest version that states **Current release for production use.**



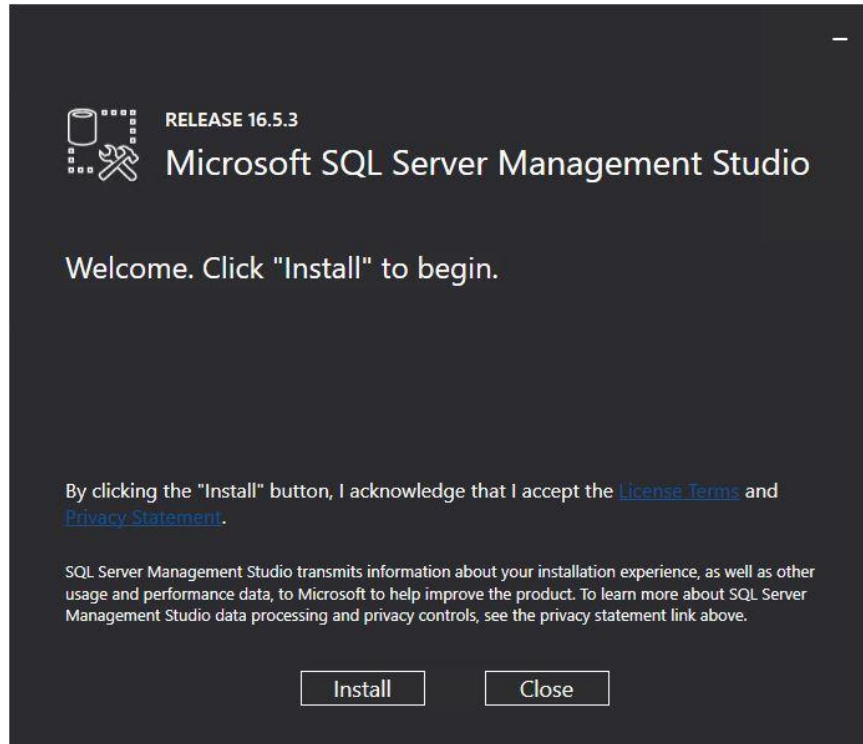
**Download SQL Server Management Studio (16.5.3)**

Current release for production use.

**Download SQL Server Management Studio - Release Candidate (17.0 RC3)**

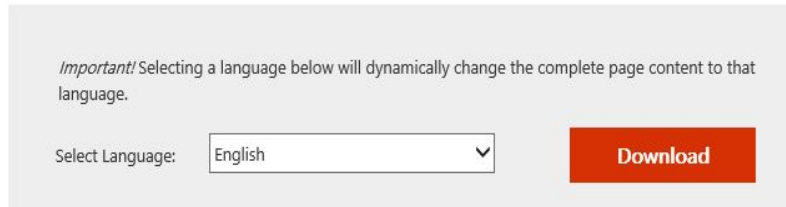
Includes support for SQL Server vNext CTP1.3, and works side-by-side with 16.x, but not recommended for production use.

- 21 Save the file in your **SQL Directory**
- 22 Navigate to the download location and run the **SSMS-Setup-ENU.exe** that you just downloaded.



- 23 Click **Install**
- 24 After the automatic setup completes, Click **Close**.

- 25 Open the **SQL Server Installation Center** window that should still be open from installing the SQL Database above.
- 26 Select **Install SQL Server Reporting Services**. This will open a browser window allowing you to download the latest version of the **SQL Server Reporting Services**.  
Microsoft SQL Server 2017 Reporting Services



SQL Server Reporting Services is a server-based reporting platform that provides comprehensive reporting functionality.

- 27 Select **Install Reporting Services**.



- 28 **Enter the product key**, and click **Next**.
- 29 Check box to **Accept license terms**, and click **Next**.
- 30 On the Install location, click **Install**.
- 31 After the install completes click **Close**.

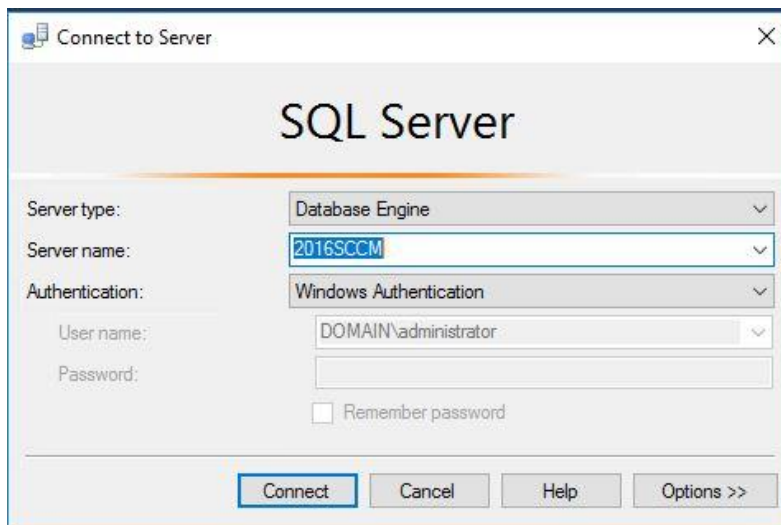
## 1.7 Set Microsoft SQL Server Memory Restrictions

\* On <YOUR\_SCCM\_SERVER>

- 1 Click **Start Menu**, Select **Microsoft SQL Server 2016** and select **Microsoft SQL Management Studio**

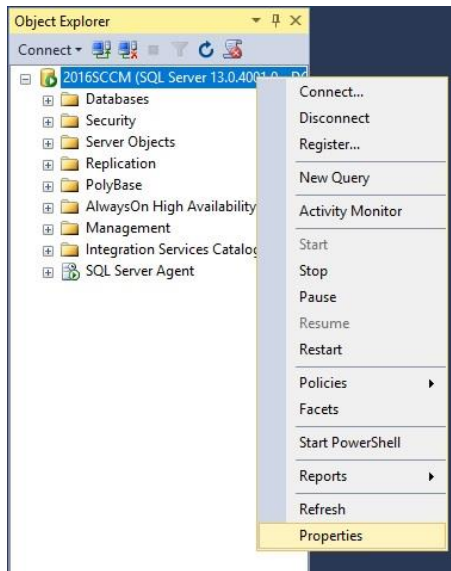


- 2 Click **Connect**

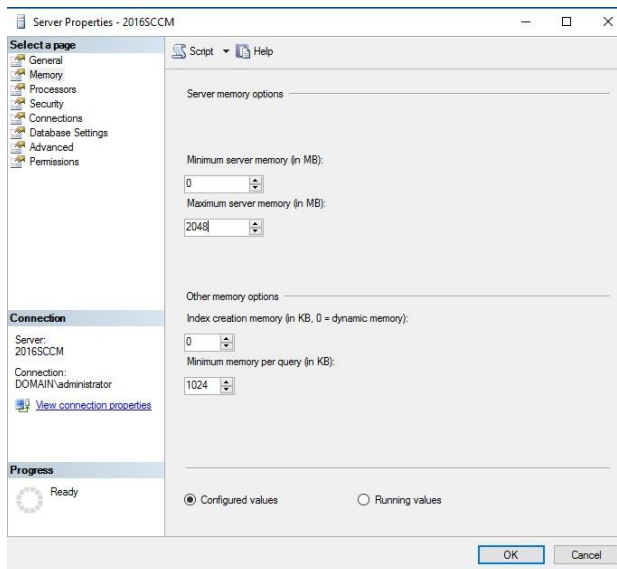




### 3 Right Click Server and Select **Properties**



### 4 Select **Memory**, set the **Maximum server memory** to at least **8192 MB** or ½ of your server's total memory.



### 5 Click Ok, and Close out **SQL Server Management Studio**.

## 1.8 Install Microsoft Administration Deployment Kit

\*On <YOUR\_SCCM\_SERVER> – At the time of creation of this guide, **WADK 2004** was the latest version released. **WADK 2004** has been tested and verified for use in a production environment by ASPCN LAN. This guide will use **WADK 2004** for this reason.

- 1 For SCCM Server 2103 (At the time of creation of this guide, the 2103 ISO is the latest release from Microsoft to be installed via ISO.)
  - A. Download Windows Assessment and Deployment Kit (WADK) for Windows 10 (<https://go.microsoft.com/fwlink/?linkid=2086042>) and Windows PE add-on for the ADK (<https://go.microsoft.com/fwlink/?linkid=2087112>).
  - B. Create two folders called **WADK** and **PE** on your **S: (SCCM)** volume and download the **Windows ADK** and **PE for Windows 10, Version 2004** to these locations.
- 2 Run the **adksetup.exe** when the file is downloaded from the **WADK** folder. In the **Install Path** box, leave the default location selected, and then click **Next**.

### Specify Location

Install the Windows Assessment and Deployment Kit - Windows 10 to this computer

Install Path:

Download the Windows Assessment and Deployment Kit - Windows 10 for installation on a separate computer

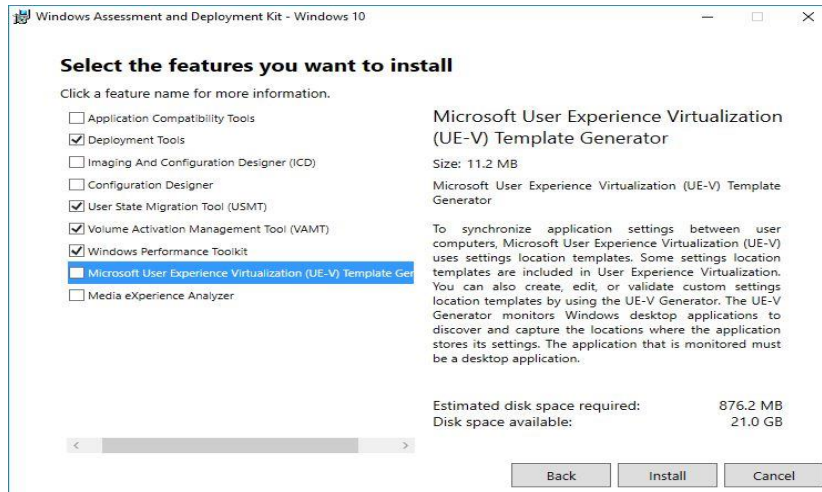
Download Path:

Estimated disk space required: 7.4 GB  
Disk space available: 26.8 GB

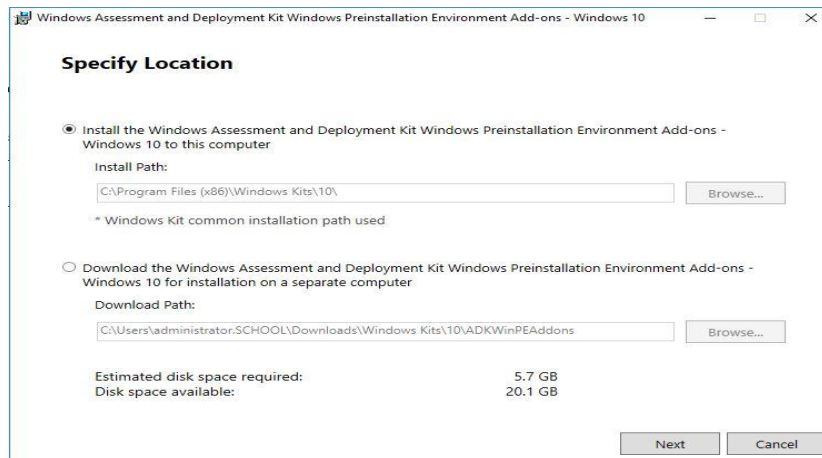
- 3 On the **Windows Kits Privacy** page, select **No** -> **Next**
- 4 On the **License Agreement** page, click **Accept**

5 Select the following Windows ADK features:

- **Deployment Tools**
- **User State Migration tool (USMT)**
- **Volume Activation Management Tool (VAMT)**
- **Windows Performance Toolkit**



6 Click **Install** and wait for the installation to finish.



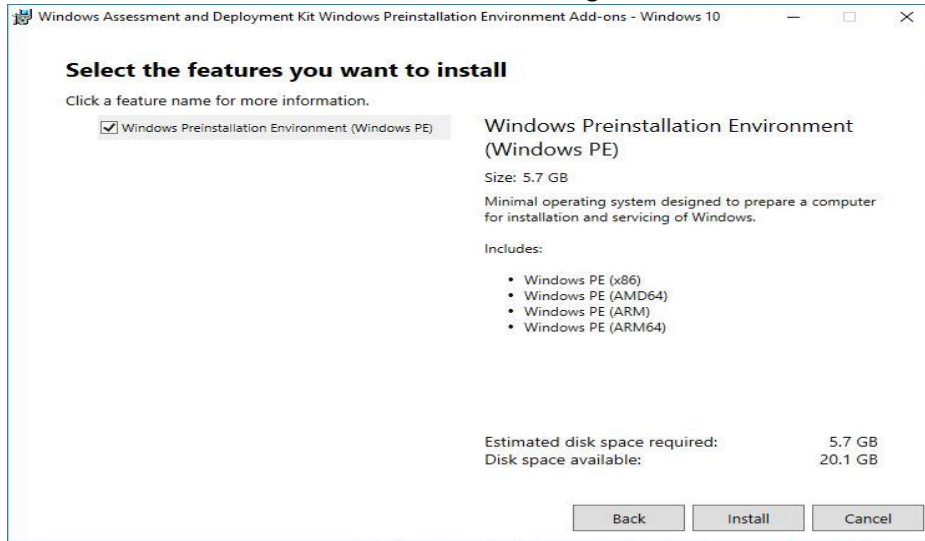
7 Run the **adkwinpesetup.exe** when the file is downloaded from the **PE** folder. In the **Install Path** box, leave the default location selected, and then click **Next**.

8 On the **Windows Kits Privacy** page, select **No** -> **Next**

9 On the **License Agreement** page, click **Accept**.

10 Make sure **(Windows PE)** is checked and click **Install**.

11 This will take some time to download the PE images. Click **Close** when it finishes.



## 2 Install SCCM

### 2.1 Create a Downloads folder in root of the S: Drive.

During the installation of SCCM, you will need to download update files. This folder has to be created before the install begins.

### 2.2 Download SCCM

In your EES Portal (Microsoft Agreement) – Volume Licensing Portal

- Search for **System Center Config Mgr (current branch)**
- Select **Download** and this will drop down multiple options for you to choose from.

Export all keys: CSV 1 - 1 of 1 items

Product	Description	Download	Key
System Center Config Mgr (current branch)	Description	Download	Key

**Special Instructions**  
None Provided.

**Download Settings**  
Microsoft recommends using a Download Manager if you would like to download multiple files or large file sizes, automatically restart the download if interrupted, or pause, start and stop downloads.  
For information on the download formats, please visit the Downloads FAQ.

Download Method: Web Browser Language: English Operating System Type: 64 bit

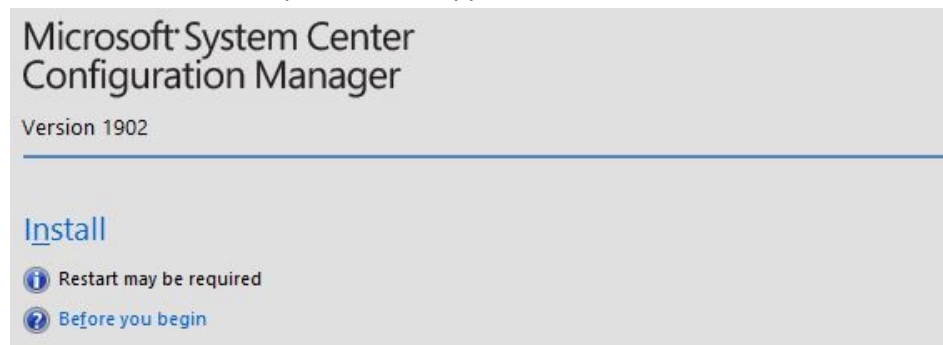
Continue

Files	OS	Size	Format	Download	SHA1 Hash
SQL Server Standard Edition 2017 64 Bit English	64 bit	1474 MB	ISO	Download	Hash
System Center DataCenter Core 2019 - Virtual Machine Manager Server Multilanguage	64 bit	1052 MB	ISO	Download	Hash
System Center Config Mgr (current branch 1902) MultiLanguage	64 bit	1612 MB	ISO	Download	Hash

- Select the highest version available to you. At the time of this writing 2103 was available. This guide will use **Version 2103**

### 2.3 Install SCCM

1. Mount your **SCCM ISO and navigate to the root of the ISO**
2. Run **Splash.hta** to start the install.
3. Click **Install** when the splash screen appears.



4. On the Before You Begin screen, click **Next**.

5. On the Getting Started screen, click **Next**.
6. On the Product Key screen, enter your valid product key and click **Next**.
7. On the **Product License Terms** screen, **Accept all terms** and click **Next**.
8. Enter **S:\Downloads** and click **Next**. (This folder must already exist.)

Setup requires prerequisite files. Setup can automatically download the files to a location that you specify, or you can use files that have been downloaded previously.

Download required files

Example: \\ServerName\ShareName or C:\Downloads

Path:

Use previously downloaded files

Example: \\ServerName\ShareName or C:\Downloads

Path:

9. On the Server Language *Selection* screen, click **Next**.
10. On the Client Language *Selection* screen, click **Next**.
11. On the Site and Installation Settings screen, enter the

- **Site Code** (Three unique letters that correspond to your District Name)
- **Site Name** (Your School Districts Full Name)
- Installation folder drive to **S:\Microsoft Configuration Manager**.
- Click **Next**.

System Center Configuration Manager Setup Wizard

Site and Installation Settings

Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.

Site code:

Specify a site name that helps to identify the site. Example: Contoso Headquarters Site

Site name:

Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.

Installation folder:

Specify whether to install the Configuration Manager console to manage the Configuration Manager site from this computer. You can remotely manage the site when you do not install the Configuration Manager console.

Install the Configuration Manager console

< Previous  Cancel

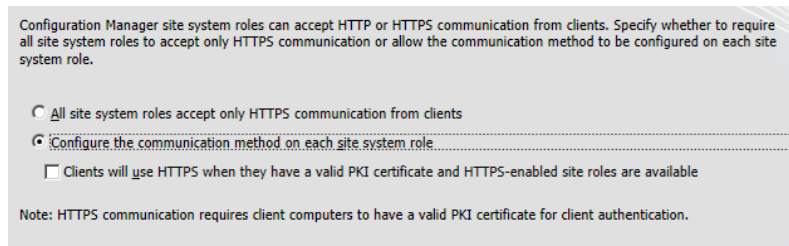
12. On the Primary Site Installation screen, select **Install the primary site as a stand-alone site**, and click **Next**.

Join the primary site to an existing hierarchy

Central administration site server (FQDN): (Example: server1.corp.contoso)

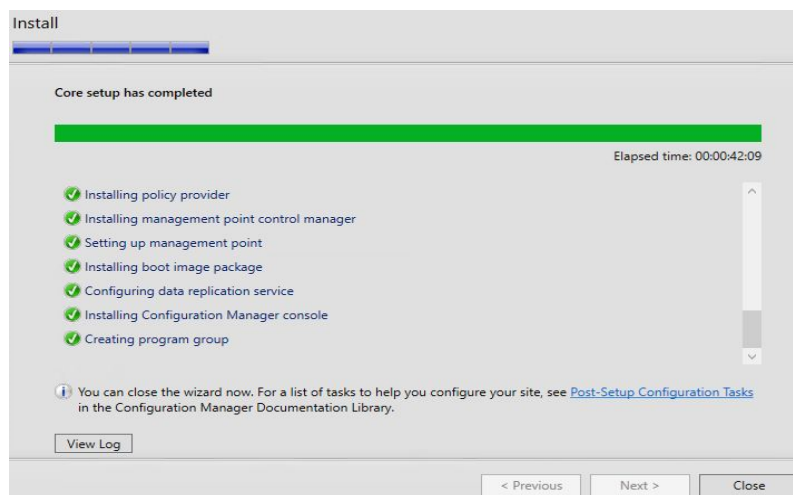
Install the primary site as a stand-alone site

13. Click **Yes** to the Pop-up.
14. On the Database Information screen, click **Next**.
15. On the second Database Information screen, Click **Next**.
16. On the SMS Provider Settings screen, click **Next**.
17. On the Client Computer Communication Settings screen, Select **Configure the communication method on each site system role**. Make sure the sub-option check box is **unchecked**, and click **Next**.



***\*\*If you are doing the SSL (Certificates) do not clear the “Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available”***

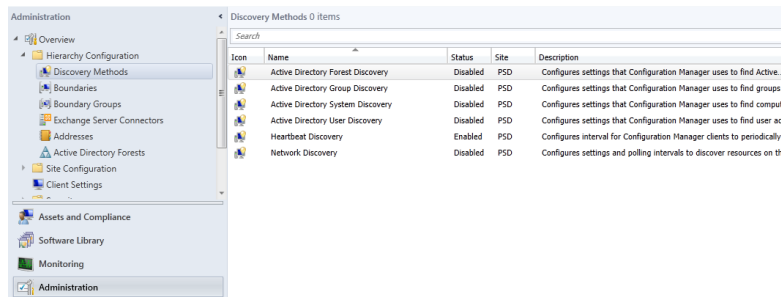
18. On the Site System Roles, click **Next**.
19. On the Diagnostic and Usage Data screen, click **Next**.
20. On the Service Connection Point Setup screen, verify that **“Yes, let’s get connected (recommended)”** is selected and click **Next**.
21. On the Settings Summary screen, click **Next**.
22. On the Prerequisite Check screen, make sure there are no **errors** and click **Begin Install**.
23. Click **Close** when the installation finishes.



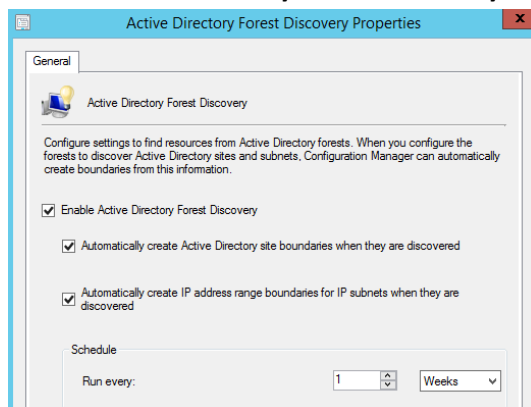
## 3 Configure SCCM

### 3.1 Configure Discovery Methods

- 1 Open the **Configuration Manager Console** from the start menu under **Microsoft System Center**.
- 2 Select **Administration** in the lower left of the screen.
- 3 Expand **Hierarchy Configuration**.
- 4 Click **Discovery Methods**.



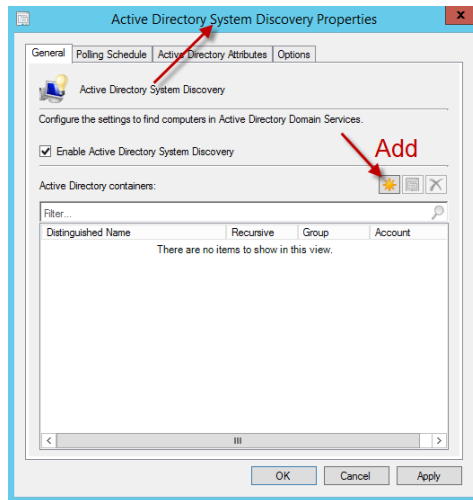
- 5 Double-click **Active Directory Forest Discovery**.
- 6 **Enable Active Directory Forest Discovery**.



- 7 Enable **All** options, leave schedule alone, click **Apply**.
- 8 Click **Yes** when prompted to run full discovery and then click **OK**.

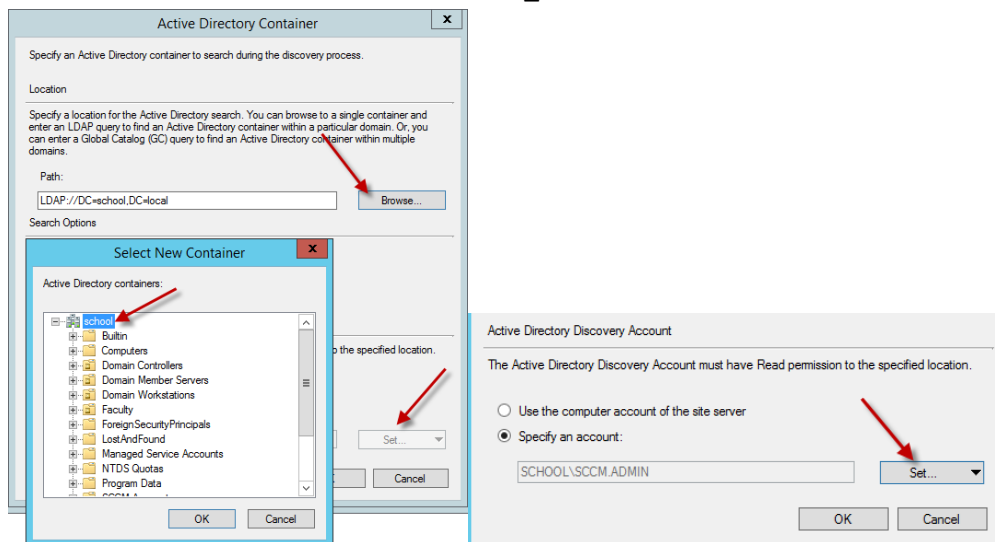


9 Double-click **Active Directory System Discovery**.

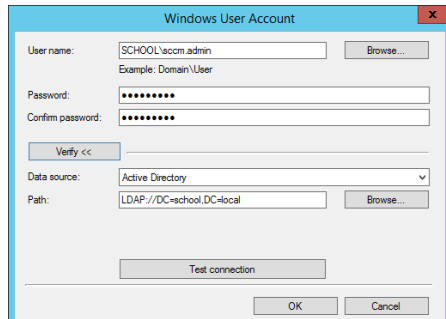


10 Enable Active Directory System Discovery.

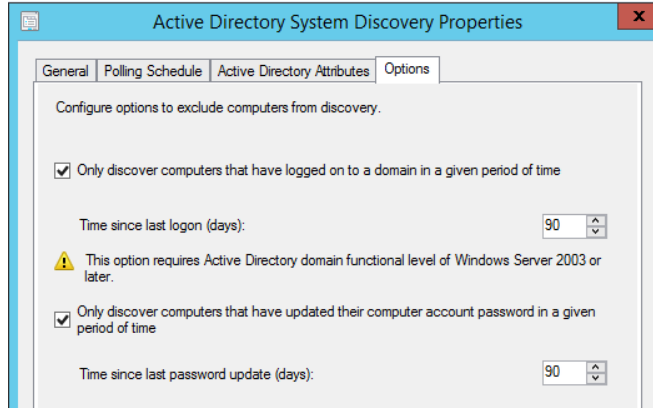
11 Click **Add**. Select **Browse** and Select **<YOUR\_DOMAIN>** and Click **OK**



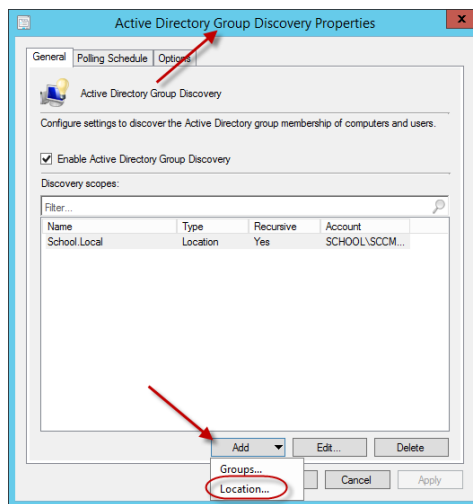
12 Select **Specify an Account**, Click **Set**, Click **New Account**. Browse and select **<YOUR\_DOMAIN>\SCCM.Admin**. Enter Password and click **Verify -> Test Connection** and **OK**.



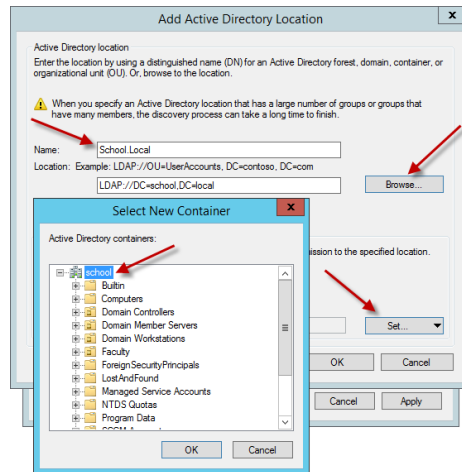
- 13 Click Options, Check **“Only discover computers that have logged on to a domain in a given period of time”** and **“Only discover computers that have updated their computer account password in a given period of time”**



- 14 Click **Apply**
- 15 Click **Yes** when prompted to run full discovery and then click **OK**.
- 16 Double-click **Active Directory Group Discovery**.
- 17 Click **Enable Active Directory Group Discovery**
- 18 Click **Add > Location**.

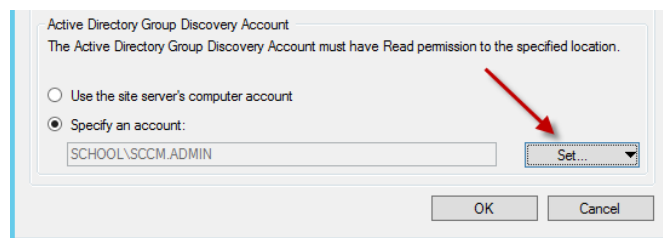


19 For the name enter the FQDN of your Active Directory Domain.

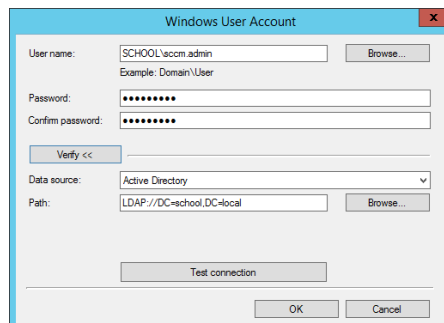


20 Click **browse** and select the root of your Active Directory Domain.

21 Click **OK**.



22 Select **Specify an Account**, Click **Set**, Click **New Account**. Browse and find <YOUR\_DOMAIN>\SCCM.Admin. Enter Password and click **Verify, Test connection** and **OK**.



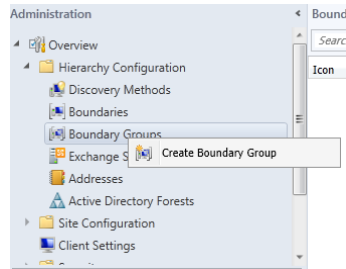
23 Click **Apply, Yes**, and **OK**.

24 Perform Steps 9-15 for all remaining Active Directory discovery methods.

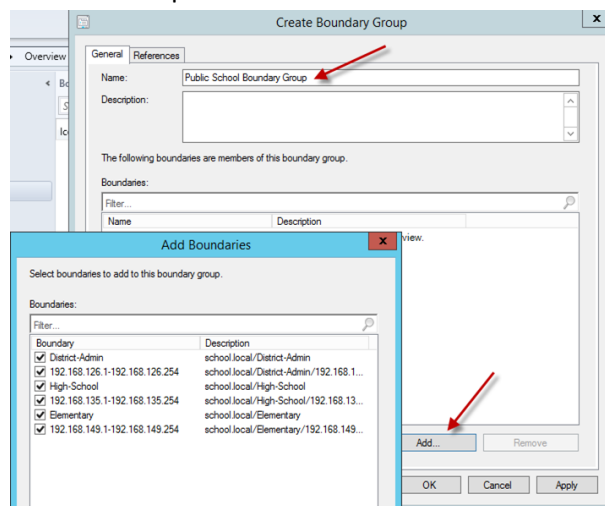
25 Ignore **Network Discovery**

### 3.2 Configure Boundaries

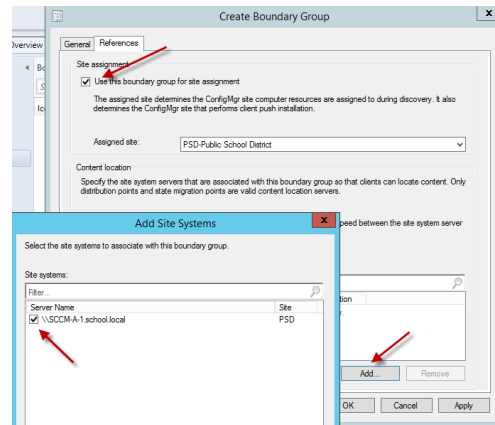
- 1 The IP Subnet and Active Directory Sites should already be created in the Boundaries. Verify that they do exist by going to **Administration -> Hierarchy Configuration -> Boundaries**.
- 2 Now, Right-click **Boundary Groups** and select **Create Boundary Group**.



- 3 Enter respective name and click **Add**.
- 4 Select the respective AD Site and Subnets and click **OK**.



5 Click **Apply** and **OK**.

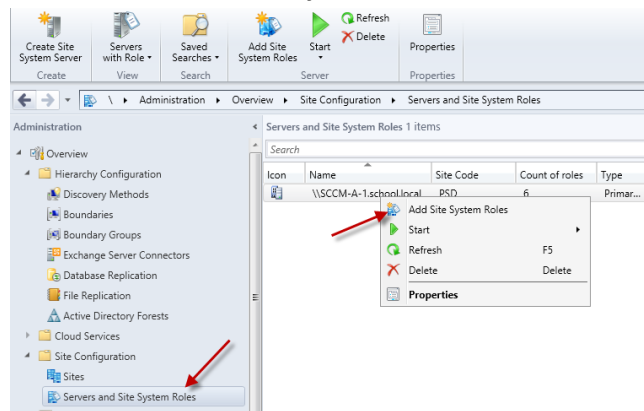


6 Right click the newly created **Boundary Group**, click **Properties**, and go to the **References Tab** of the boundary group. Select **Use this boundary group for site assignment** and **add** the site server to the boundary group. Click **Apply** and **Ok**.

### 3.3 Configure Site Roles / Endpoint Protection

1 Select **Administration** in the lower left of the screen and expand **Site Configuration**.

2 Select **Servers and Site System Roles**.



3 Right-click **<YOUR\_SCCM\_SERVER>** and click **Add Site System Role**.

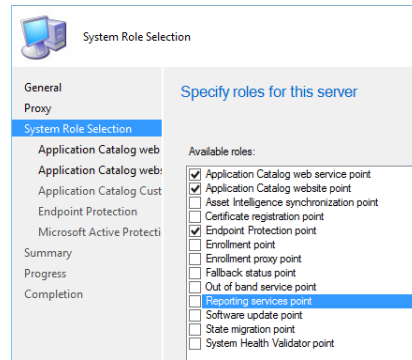
4 On the **General** screen, click **Next**.

5 On the **Proxy** screen, click **Next**

6 On the **System Role Selection** screen

- **Endpoint Protection** roles, Click **Ok** on the pop-up

- Click **Next**.



- 7 On the **Cloud Protection Service membership type** screen, select **Do not join Cloud Protection Service** and click **Next**.

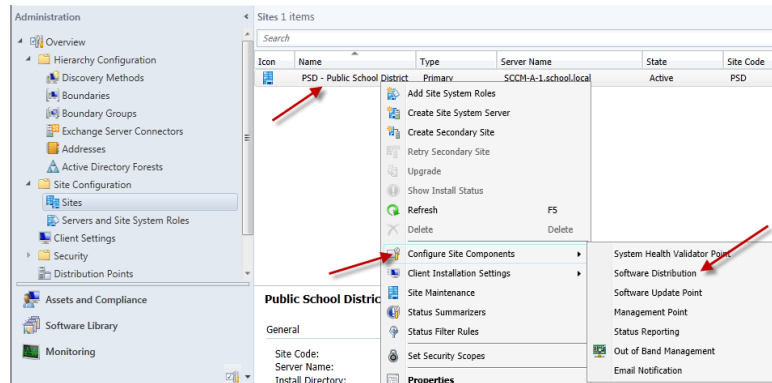


- 8 On the **Summary** screen, click **Next**.
- 9 Click **Close** when the wizard is finished.

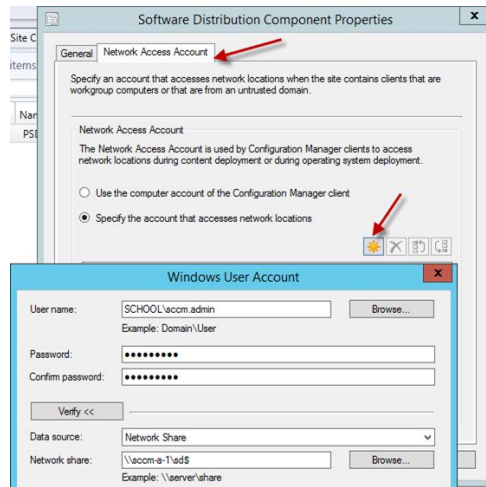
### 3.4 Configure Network Access Account

- 1 Select **Administration** in the lower left of the screen and expand **Site Configuration**.
- 2 In the left-hand pane, select **Sites**.

- Right-click the **Primary Site**, and click **Configure Site Components -> Software Distribution**.



- Select **Network Access Account**, click the Set button and set the **<YOUR\_DOMAIN>\SCCM.Admin** account and password.



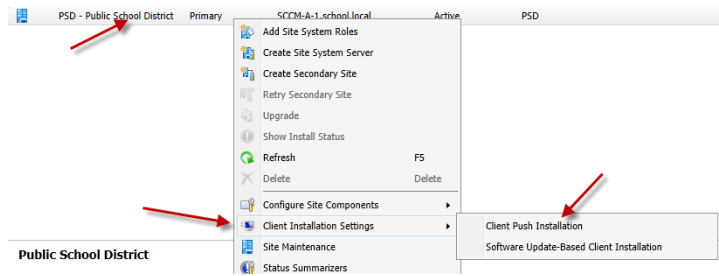
- Click **Apply** and **Ok**.

### 3.5 Configure Client Agent Installation Method

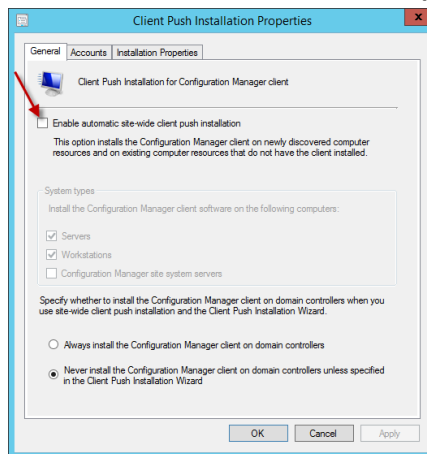
**\*\*\*Please verify the client push manually before you select "Enable automatic site-wide client push installation"**

- Select **Administration** in the lower left of the screen and expand **Site Configuration**.
- In the left-hand pane, select **Sites**.

- Right-click the **Primary Site**, and click **Client Installation Settings -> Client Push Installation**.

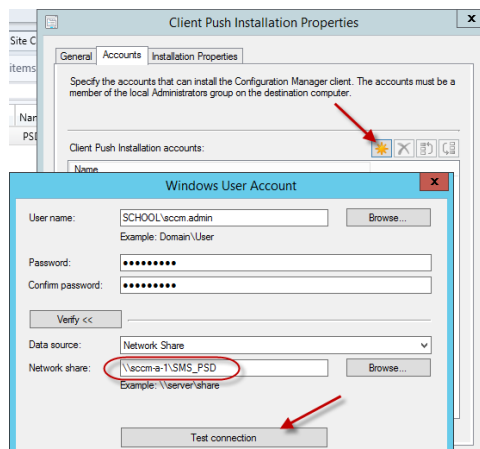


- Enable automatic site-wide client push installation.



- Check/Uncheck **Servers** and **Configuration Manager site system servers** if you want/don't want to push SCCM client to servers.

- Select the **Accounts** tab, Click **Add**.



- Enter **<YOUR\_DOMAIN>\SCCM.ADMIN** and click **OK**.

- Enter the account password, and click **Verify**.



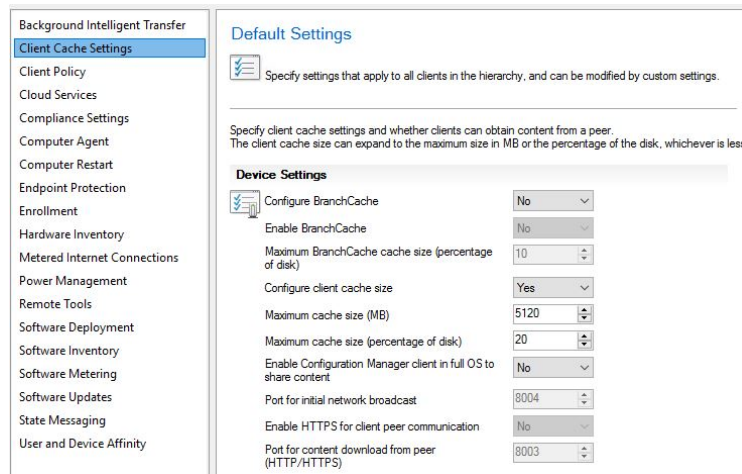
9 For the Network Share enter \\<YOUR\_SCCM\_SERVER>\SMS\_PSD (PSD will be replaced with your Site Code), and click the **Test Connection** button.

10 Click **OK**, and then **Apply** and **OK**.

## 3.6 Configure Client Agent Settings

### 3.6.1 Client Cache Settings

- 1 Select **Administration** in the lower left of the screen.
- 2 In the left-hand pane, select **Client Settings**.
- 3 In the right-hand pane, double-click on **Default Settings**.
- 4 Select **Client Cache Settings**.
- 5 Select the drop down next to **Configure Client Cache Size**
- 6 Select **Yes**, leave everything else default



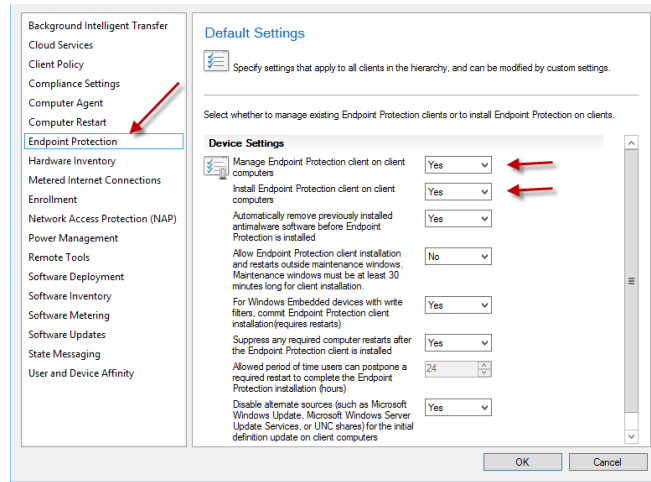
### 3.6.2 Computer Agent

- 1 Select **Administration** in the lower left of the screen.
- 2 In the left-hand pane, select **Client Settings**.
- 3 In the right-hand pane, double-click on **Default Settings**.
- 4 Select **Computer Agent**.
- 5 Enter the **Organization Name** to be displayed in Software Center

### 3.6.3 Endpoint Protection

- 1 Select **Administration** in the lower left of the screen.
- 2 In the left-hand pane, click **Client Settings**.

- 3 In the right-hand pane, double-click on **Default Settings**
- 4 In the left-hand pane, select **Endpoint Protection**.



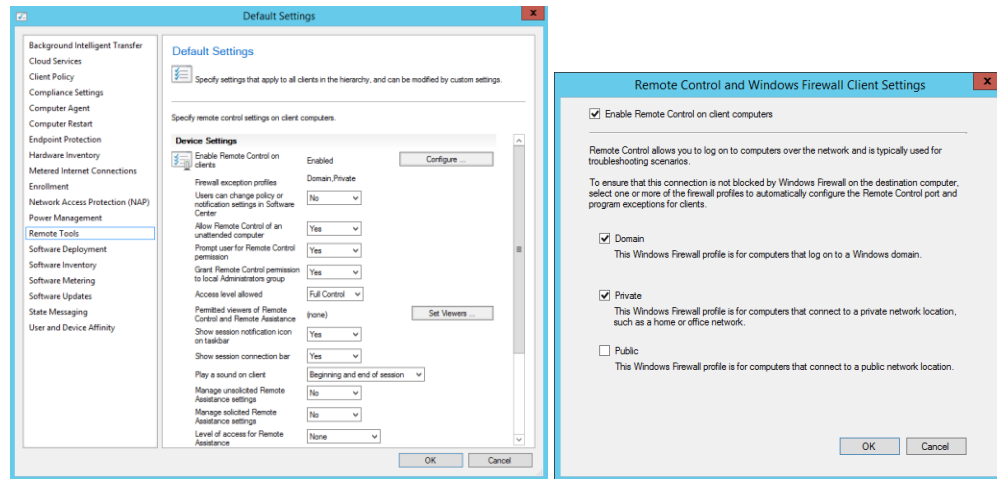
- 5 Adjust the following device settings as listed:

- **Manage Endpoint Protection client on client computers: Yes**
- **Install Endpoint Protection client on client computers: Yes**

### 3.6.4 Remote Tool

- 1 Select **Administration** in the lower left of the screen
- 2 In the Left-hand pane, select **Client Settings**.
- 3 In the right-hand pane, double-Click on the **Default Settings**
- 4 Select **Remote Tools**
- 5 Click **Configure**

## 6 Select Enable Remote Control on client computers for Domain and Private



## 7 Adjust the following device settings as listed:

Allow Remote Control of an unattended computer: **Yes**

Prompt User for Remote Control permission: Yes/No – **(Administration’s choice)**

Grant Remote Control permission to local Administrators group: **Yes**

Show session notification icon on taskbar: Yes/No – **(Administration’s choice)**

Show session connection bar: Yes/No – **(Administration’s choice)**

Play a sound on client: **No sound**

Manage Remote Desktop settings: **Yes**

Allow permitted viewers to connect by using Remote Desktop connection: **Yes**

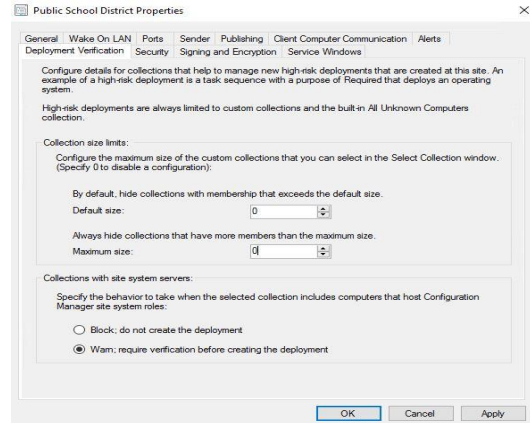
Require network level authentication on computers that run Windows Vista system operating system and later versions: **No**

## 8 Click **OK** to accept the settings.

### 3.7 Configure Site Deployment Verification

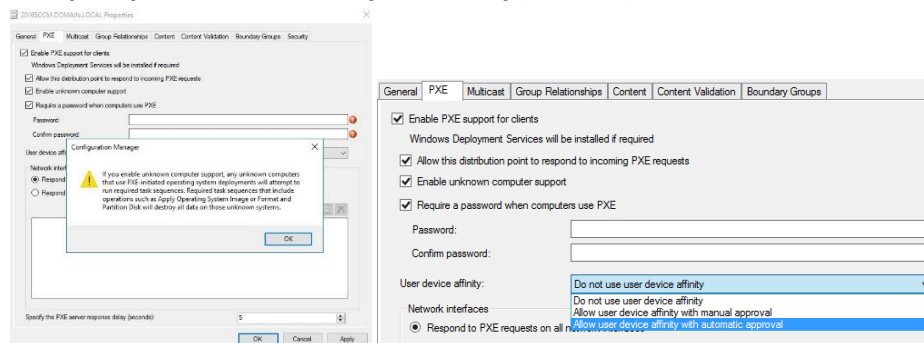
- 1 Select **Administration** in the lower left of the screen
- 2 Drop down the **Site Configuration** folder on the left side
- 3 Select **Sites**
- 4 In the right hand side of SCCM select your primary site: ***i.e.* PSD – Public School District**

- 5 Right click your primary site and select **Properties**
- 6 Select the **Deployment Verification** tab
- 7 In the **Collection Size Limits** box put a **0** in both boxes
- 8 In the **Collections with site system server** box, select **Warn**, require verification before creating the deployment



### 3.8 Enable PXE support

- 1 In the SCCM Console, click on **Administration -> Distribution Points**
- 2 Right click your **Distribution Point** in the right side of SCCM and select **Properties**.
- 3 Select the **PXE** tab and place a checkmark in **Enable PXE support for Clients**. Click on **Yes** when prompted about firewall ports.
- 4 Enable all options.
- 5 Set the **Require a password when computers use PXE**.
- 6 Set **User Device Affinity** option to **Allow User Device Affinity with Automatic Approval**.
- 7 Set **Specify the PXE server response delay (seconds)** to 5



- When this Role has finished installing, you will find the directory **S:\RemoteInstall**. Please verify that inside that directory you have an smsboot\x86 and smsboot\x64 with content. If the folders are empty, please wait before continuing to the next section.

### 3.8.1 DHCP Settings for PXE

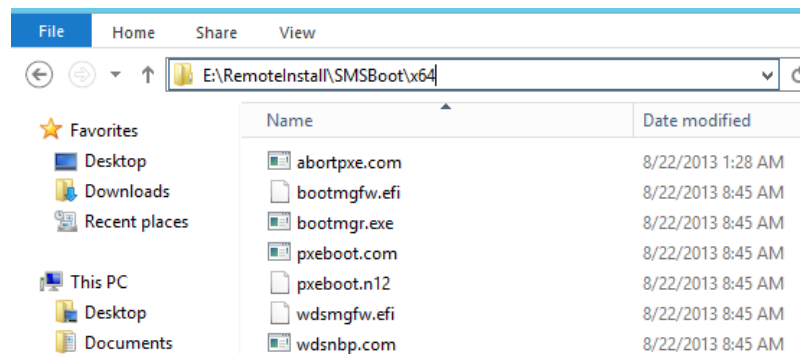
**NOTE: The following is now necessary for the clients to choose if they are UEFI or BIOS.**

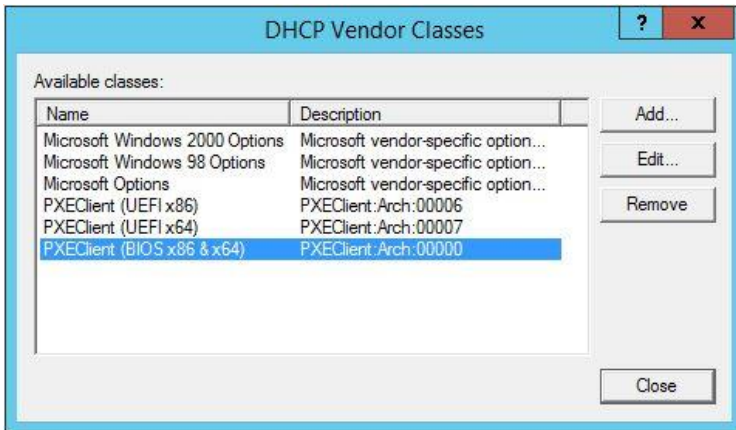
Defining DHCP Vendor Classes:

The first thing to do is to define the vendor classes for the BIOS PXE Client x84 and x64 and the UEFI PXEClient x86 and x64. To do this:

- Go to **DHCP**, right-click on **IPv4**, click **Define Vendor Classes**.
- In the DHCP Vendor Classes window, click **Add**.
- For the Name enter **PXEClient (UEFI x86)**.
- For the Description enter **PXEClient:Arch:00006**.
- Click in the **ASCII** column and type the text **PXEClient:Arch:00006** (you will not be able to paste this text, and it's also case-sensitive).
- Click **OK** to add it to the list.
- Now repeat steps 2 – 6 for **PXEClient (UEFI x64)** with **PXEClient:Arch:00007** as the Description and ASCII value.
- Finally, repeat steps 2 – 6 for **PXEClient (BIOS x86 & x64)** with **PXEClient:Arch:00000** (five zero's) as the Description and ASCII value.

You should now have three additional vendor classes.





Creating the DHCP Policies:

Now we're going to create policies in DHCP so that the correct files are served to the correct clients. You will need to do this for each DHCP scope that you will PXE on.

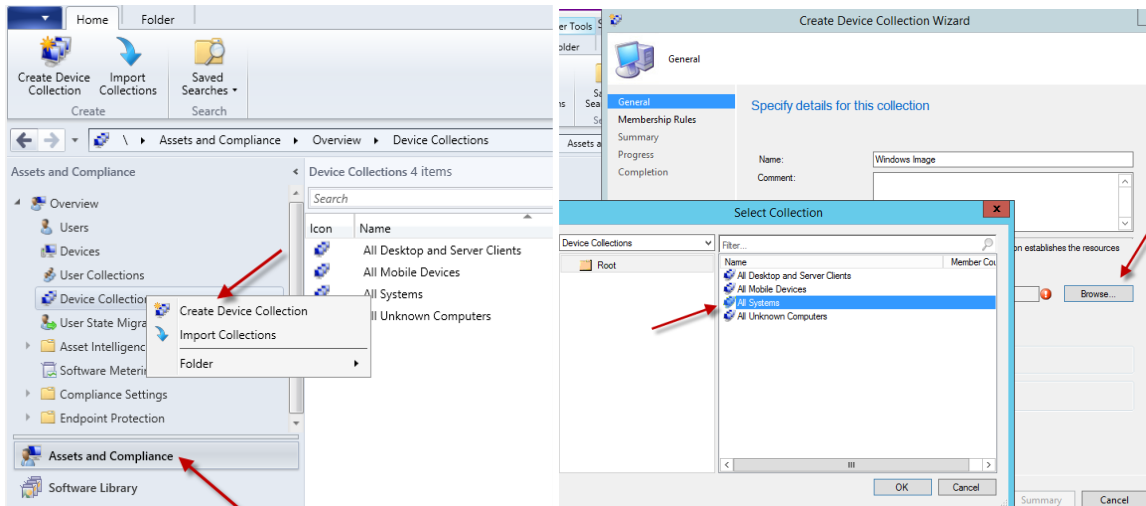
1. Go to **DHCP Console** and expand the scope you wish to create a policy for.
2. Right-click on **Policies** and choose **New Policy**.
3. Enter **PXEClient (UEFI x64)** for the name.
4. Enter a Description if you want. Click **Next**.
5. On the Configure Conditions for the policy screen, click **Add**.
6. In the Add/Edit Condition window, click the **Value:** drop down menu.
7. Choose the **PXEClient (UEFI x64)** vendor class you created earlier.
8. Check the **Append wildcard(\*)** check box and then click **Add** and finally **OK**.
9. Click **Next** on the Configure Conditions for the policy screen.
10. On the Configure settings for the policy screen, click **No** for the Do you want to configure an IP address range for the policy. Click **Next**.
11. On the Configure settings for the policy screen, scroll down until you see options **066** and **067**.
13. Check option **066** and enter **<IP-Number-of-SCCM-PXE-Server>**.
14. Check option **067** and enter **boot\x64\wdsmgfw.efi** – this is the x64 UEFI boot file for SCCM. Click **Next**.
15. On the Summary screen, if all the details are correct, click **Finish**.
16. Now repeat steps 2 – 15 for **PXEClient (UEFI x86)** with **boot\x86\wdsmgfw.efi** as option **067**.
17. Finally, repeat steps 2 – 15 once again for **PXEClient (BIOS x86 & x64)** with **boot\x64\wdsnbp.com** as option **067**.

## 4 Collections

### 4.1 Creating Device Collection

- 1 In the Configuration Manager console, click **Assets and Compliance**.

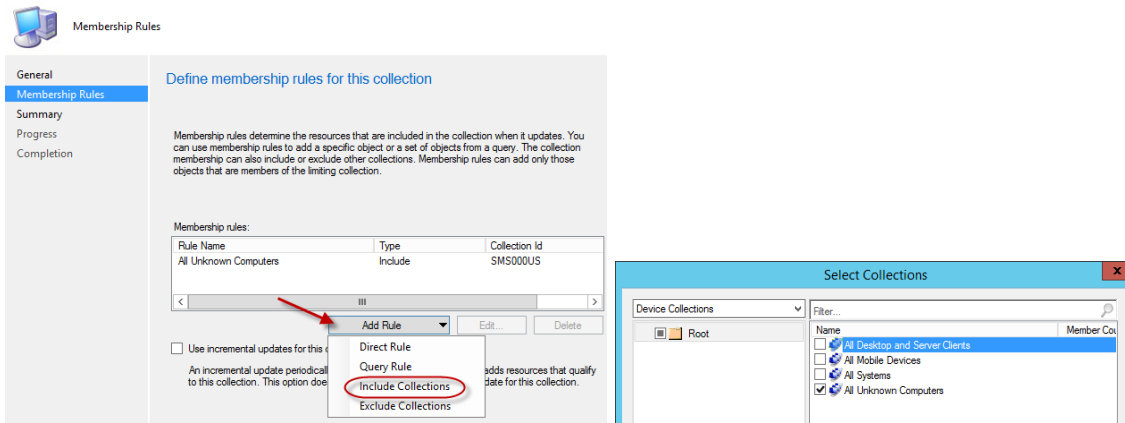
- 2 In the **Assets and Compliance** workspace, Right click **Device Collections** and Select **Create Device Collection**.



- 3 On the General page of the Create Device Collection Wizard, specify the following information:

- 3.a Name: **Windows Imaging Collection**.
- 3.b Limiting collection: Click Browse and select **All Systems**.

- 4 On the Membership Rules page of the Create Device Collection Wizard, Click **Add Rule**, select **Include Collections**. Select **All Unknown Computers** and click **OK**.



- 5 **Next** and Complete the wizard to create the new collection. The new collection is displayed in the Device Collections node of the Assets and Compliance workspace.

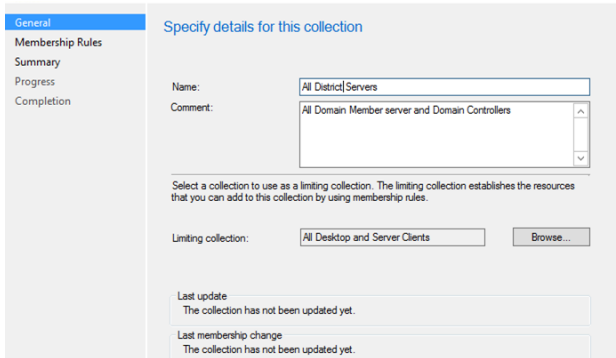
#### 4.1.1 To configure a query rule

- 1 In the Configuration Manager console, click **Assets and Compliance**.
- 2 In the **Assets and Compliance** workspace, Right click **Device Collections** and Select **Create Device Collection**.

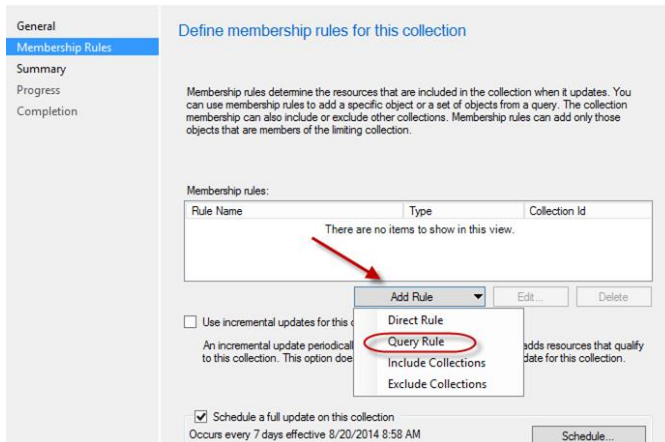
3 On the General page of the Create Device Collection Wizard, specify the following information:

3.a Name: **All District Servers.**

3.b Limiting collection: Click Browse to select **All Desktop and Server Clients.**



4 On the Membership Rules page of the Create Device Collection Wizard, specify the following information:



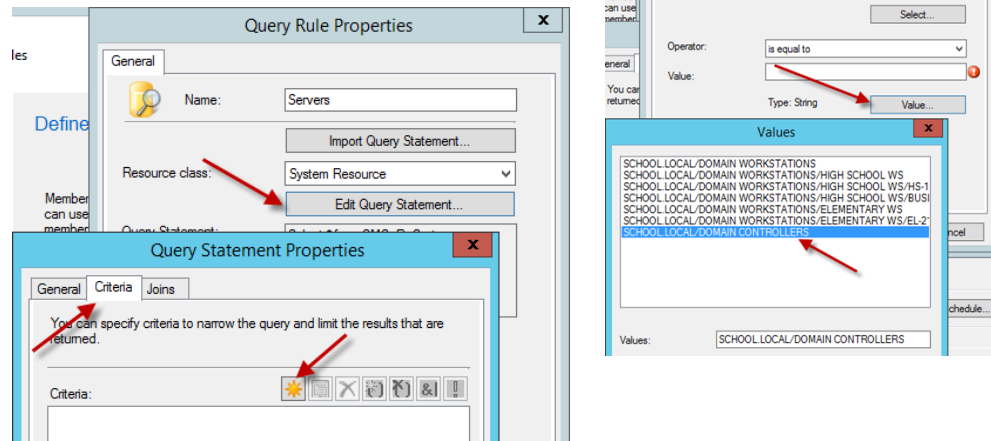
In the Query Rule Properties dialog box, specify the following information:

1.a Name: **Server**

1.b Resource class: **System Resource**



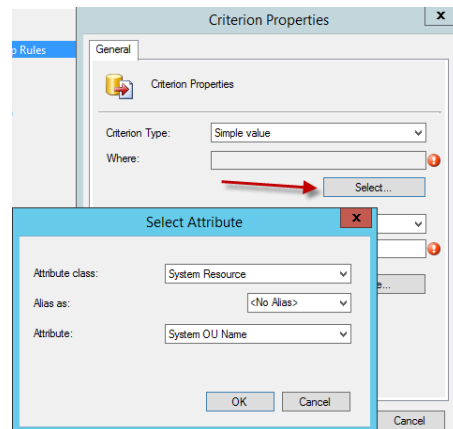
4.a Click **Edit Query Statement** -> **Criteria** tab ->  
Click the **Add Star**



1.b.i Attribute Class: **System Resource**

1.b.ii Alias as: **<No Alias>**

1.b.iii Attribute: **System OU Name** and click **OK**



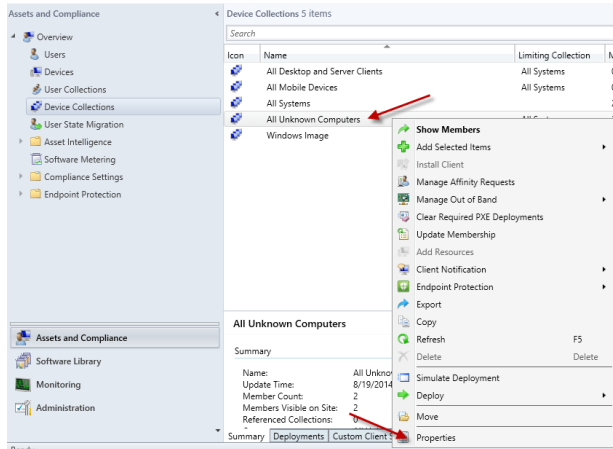
- 5 On **Criterion Properties** Click **Value** and Select **<YOUR\_DOMAIN>/Domain Controllers**.
- 6 Repeat these steps in the same rule but select **<YOUR\_DOMAIN>/DOMAIN SERVERS** in the last step
- 7 Click **OK** to close the Query Statement Properties dialog box
- 8 Click **OK** to close the **Query Rule Properties** box
- 9 Click **Next** -> **Next** -> **Close** to finish the query rule.

#### 4.1.2 To configure a direct rule

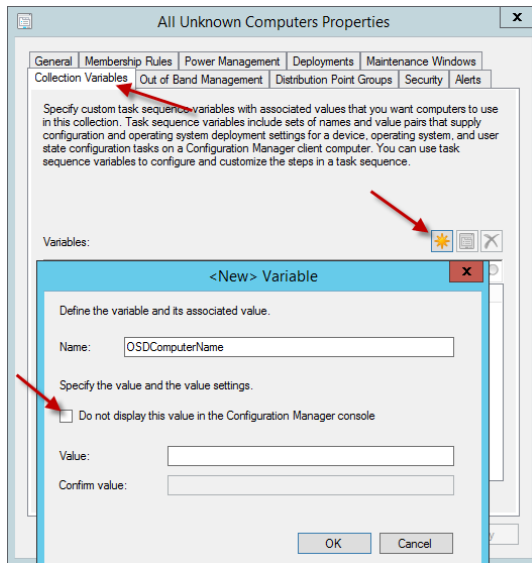
- 1 In the Configuration Manager console, click **Assets and Compliance**.
- 2 In the **Assets and Compliance** workspace, Right click **Device Collections** and Select **Create Device Collection**.
- 3 On the **General page** of the Create Device Collection Wizard, fill in the corresponding information
- 4 On the **Membership Rules page** of the Create Device Collection Wizard, select **Add Rule -> Direct Rule**
- 5 On the **Search for Resources page** of the Create Direct Membership Rule Wizard, specify the following information:
  - 1.a **Resource class:** In the list, select the type of resource you want to search for and add to the collection. Select from System Resource values to search for inventory data returned from client computers or select Unknown Computer to search for values returned by unknown computers.
  - 1.b **Attribute name:** In the list, select the attribute associated with the selected resource class that you want to search for. For example, if you want to select computers by their NetBIOS name, select System Resource in the Resource class list and NetBIOS name in the Attribute name list.
  - 1.c **Exclude resources marked as obsolete** – If a client computer is marked as obsolete, do not include this value in the search results.
  - 1.d **Exclude resources that do not have the Configuration Manager client installed** – If the search results include a resource that does not have a Configuration Manager client installed, this value will not be displayed in the search results.
  - 1.e **Value:** Enter a value for which you want to search the selected attribute name. You can use the percent character % as a wildcard. For example, if you wanted to search for computers that have a NetBIOS name beginning with 'M', enter M% in this field.
- 2 On the **Select Resources** page of the Create Direct Membership Rule Wizard, select the resources that you want to add to the collection in the Resources list, and then click Next.
- 3 Complete the Create Direct Membership Rule Wizard.

## 4.2 Set Collection Variables for Imaging

### 1 Right Click **All Unknown Computers**, Select **Properties**.



### 2 Select **Collection Variables** Tab, Click the add **Star**



### 3 Enter Name: **OSDComputerName**, and uncheck “**Do not display the value in the Configuration Manager Console**”. Click **Ok**, **Apply** and **Ok** to close the Properties Window.

## 5 Software Deployment

### 5.1 Software Distribution Share

- 1 On the S: Drive, create a folder called **Software Distribution**, right click and select **Properties**.
- 2 Click on **Sharing** tab, **Advanced Sharing** and share this folder out with the following settings:
  - 3.a.i Share name: **SD\$** - (**\$ is used to make the share hidden**).
  - 3.a.ii Caching: **No files or programs from the shared folder are available offline**
  - 3.a.iii Permissions: Add the following permissions for the share:
    - **Domain Admins: Full Control**
    - **SCCM Admins: Full Control**
    - **SCCM Servers: Full Control**
    - **SYSTEM: Full Control**
    - **Authenticated Users: Change and Read**
    - **Local Administrators Group: Full Control**
    - When done click **Apply** -> **OK** -> **Apply** again -> **Ok** again
- 3 Click on **Security** tab -> **Advanced** -> **Change Permissions** -> **Disable Inheritance**. On the pop-up click **Remove all inherited permissions from this object** and then **Apply** and **OK** to get back to the **Security settings**.
- 4 Click on **Edit** and then **add** the following groups:
  - **Administrators: Full Control**
  - **Domain Admins: Full Control**
  - **SCCM Admins: Full Control**
  - **SCCM Servers: Full Control**
  - **SYSTEM: Full Control**
  - **Authenticated Users: Read & execute, List Folder Contents** and **Read**
  - When done click **Apply**, **Ok** and **Close** to finish.

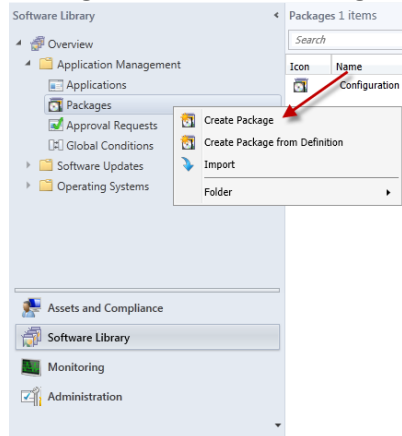
- 5 In the **Software Distribution** folder, create folders called **Images**, **Drivers** and **Software**.

## 5.2 Software Package

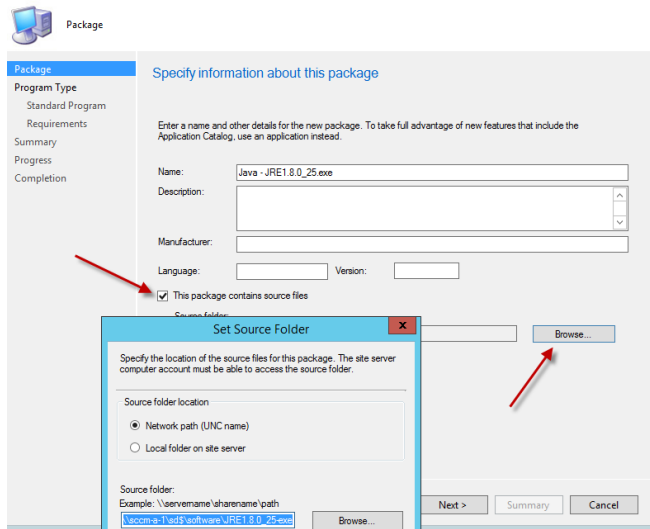
### 5.2.1 Create Software Package

#### 5.2.1.1 JAVA (EXE INSTALL)

- 1 In the Configuration Manager console, click **Software Library**.
- 2 In the **Software Library** workspace, expand **Application Management**, and then right click **Packages**. Click **Create Package**.



- 3 On the **Package** page of the **Create Package and Program Wizard**, specify the following information:



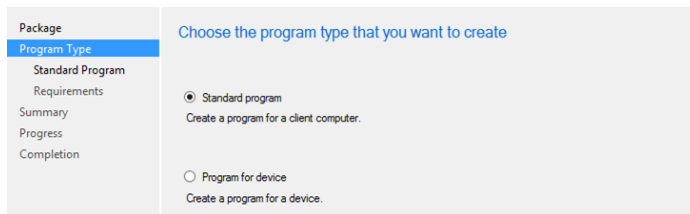
Name: **Jre-8u333-windows-i586.exe**

**Check** This package contains source files

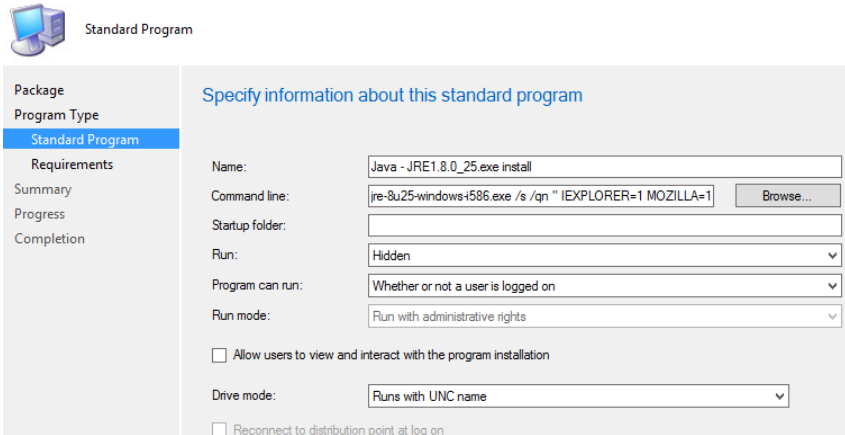
Source Folder: **Network path (UNC name)**

**\\<YOUR\_SCCM\_SERVER>\sd\$\software\JRE8u333-exe**

- 4 On the **Program Type** page of the **Create Package and Program Wizard**, select the type of program you want to create and then click **Next**. You can create a program for a computer, a device or skip this step and create a program later.



- 5 On the **Program Type** page of the **Create Package and Program Wizard**, select **Standard Program**, and then click **Next**.



On the **Standard Program** page of the Wizard, specify the following information.

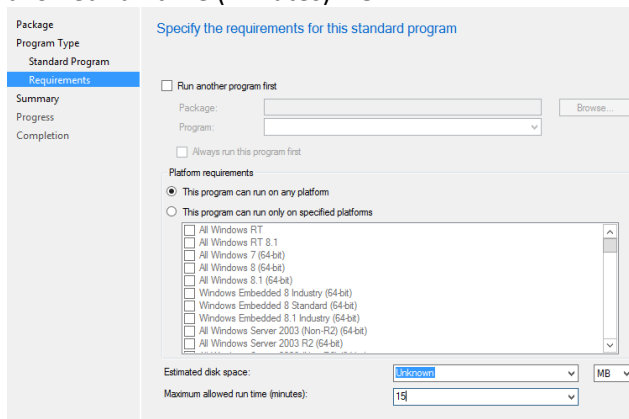
Name: **Jre-8u333-windows-i586.exe install**

Command line: **jre-8u333-windows-i586.exe /s /qn " IEXPLORER=1 MOZILLA=1 REBOOT=Suppress JAVAUPDATE=0 WEBSTARTICON=0"**

Run: **Hidden**

Program can run: **Only When a user is logged on**

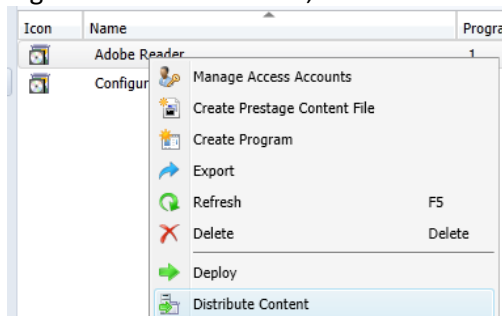
- On the **Requirements** page of the Create Package and Program Wizard, set maximum allowed run time (minutes): **15**



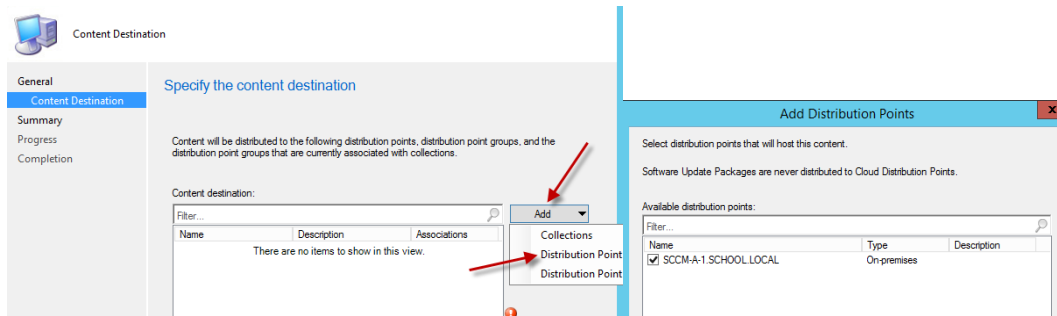
- Click **Next** and **finish** the wizard.

## 5.2.2 Distribute Software Package

- Right Click Adobe Reader, Select **Distribute Content**

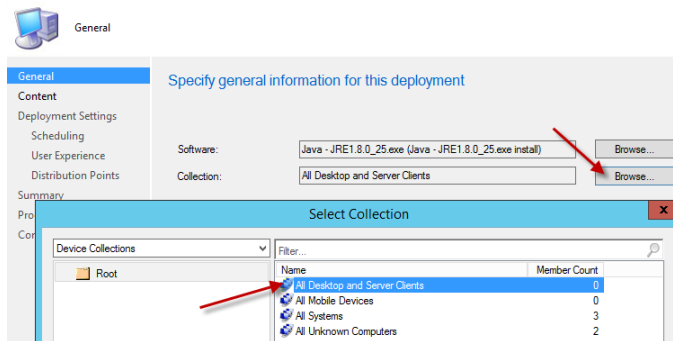


- 2 On the Content Destination screen Click **Add** and Chose **Distribution Point** and Select the **\\<YOUR\_SCM\_SERVER>.<YOUR\_DOMAIN>.local** and click **OK** and **Next** and **Finish** the Wizard.

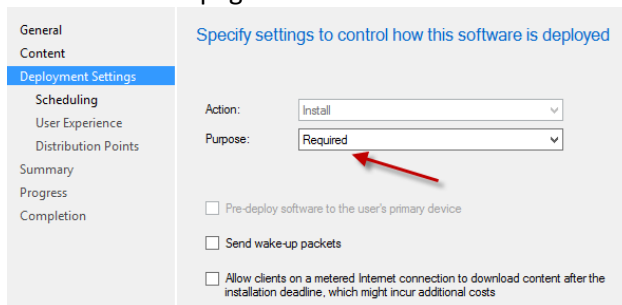


### 5.2.3 Deploy Software Package - Required

- 1 Right Click your Package and Select Deploy
- 2 On the **General** page of the **Deploy Software Wizard**, specify the following information:  
**Software** – Displays the application you want to deploy. You can click **Browse** to select a different application to deploy.  
**Collection** – Click **Browse** to select the collection you want to deploy the application to.

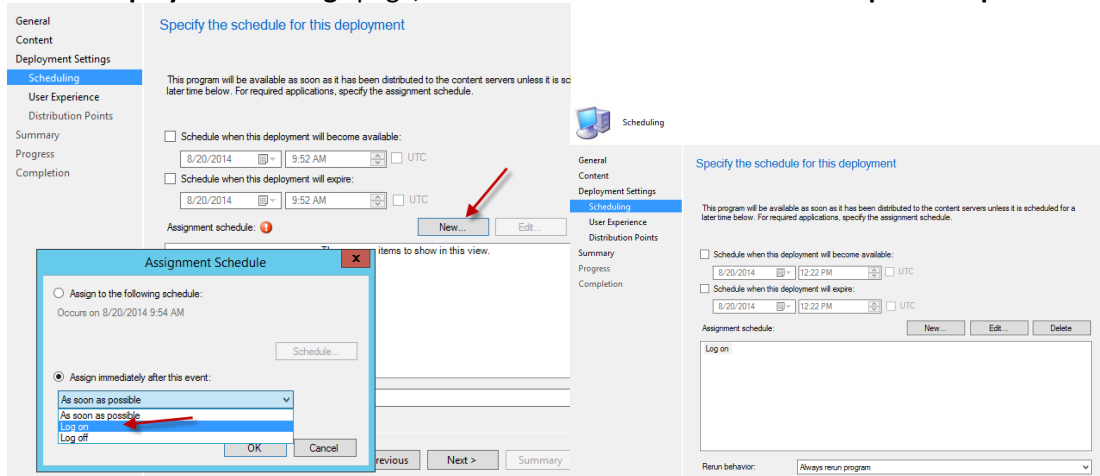


- 3 On the **Content** page Click **Next**





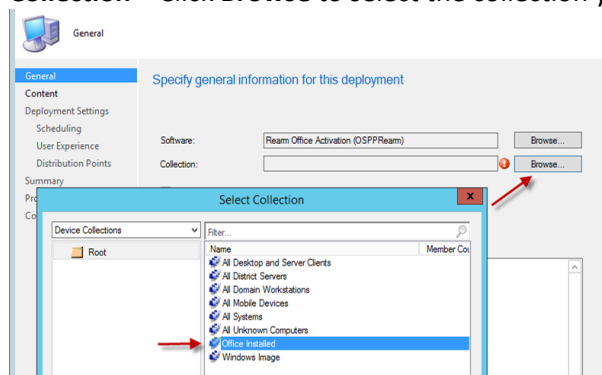
4 On the **Deployment Settings** page, Chose the **Action: Install** and the **Purpose: Required**.



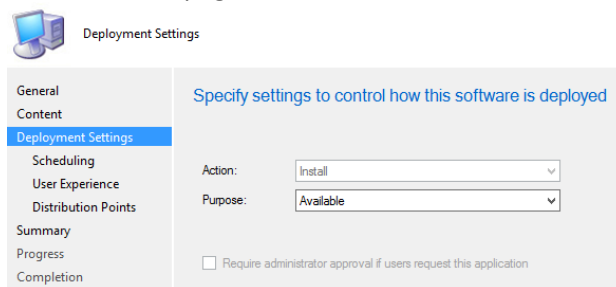
5 On the **Scheduling** page, Select **New** and **Assign immediately after this event: Log On**. Change the Rerun Behavior to **Always rerun** program. Click **OK** and Click **Next** to finish out the wizard. This policy will take a few reboots to take effect. Because we marked this Package as a "Required" deployment, you will NOT see it in the Software Center. You will have to check the log files to verify it worked.

## 5.2.4 Deploy Software Package – Available

- 1 Right Click your Package and Select Deploy
- 2 On the **General** page of the **Deploy Software Wizard**, specify the following information:  
**Software** – Displays the application you want to deploy. You can click **Browse** to select a different application to deploy.  
**Collection** – Click **Browse** to select the collection you want to deploy the application to.



- 3 On the **Content** page Click **Next**




- 4 On the **Deployment Settings** page, Chose the **Action: Install** and the **Purpose: Available**. Click **Next** through the rest of the wizard.

## 5.3 Software Application

### 5.3.1 Adobe Reader

- 1 Download The Latest Version <AdbeRdr11007\_en\_US.exe> from Adobe - Adobe Reader download - <http://get.adobe.com/reader/enterprise/>

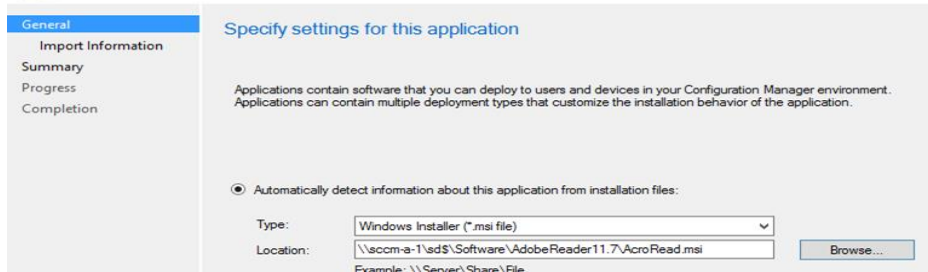
- 2 Extract the contents of .exe using the following command <File\_Download\_Location>\AcroRdrDC2200120117\_en\_US.exe -nos\_o C:\AdobeReader -nos\_ne

 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

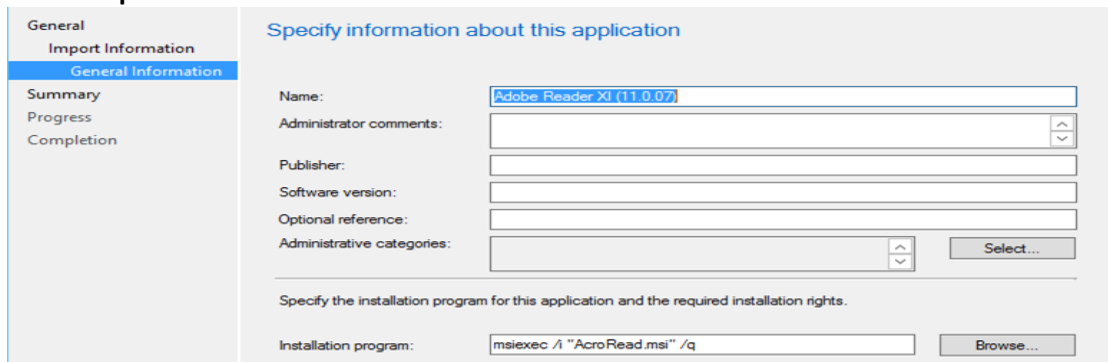
Open:

- 3 Copy the files from the above folder **C:\AdobeReader** to a folder in your Software Distribution. \\<YOUR\_SCCM\_SERVER>\sd\$\software\AcrobatReader and **Create Application**.

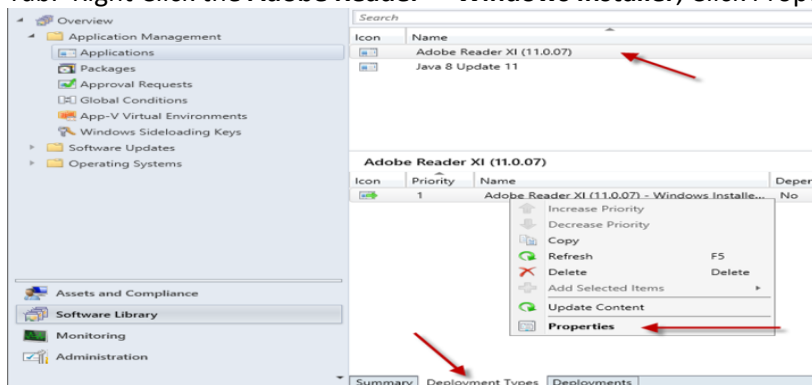
- 4 In the Configuration Manager console, click **Software Library**
- 5 In the **Software Library** workspace, expand **Application Management**, and then right click **Applications**. Click **Create Application**
- 6 On the **General Page**, Specify **Type Windows Installer (\*.msi file)**.  
In Locations put `\\<YOUR_SCCM_SERVER>\sd$\software\AdobeReader\AcroRead.msi`, and click **Next**. Click **Next** on the **Important Information**.



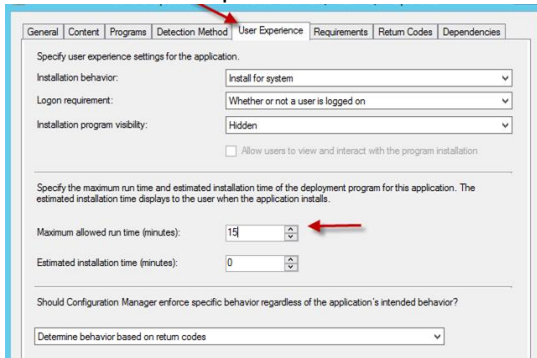
- 7 Enter the Information on the General Information Screen, Check **Run installation program as 32-bit process on 64-bit clients** and Click **Next** and Finish the Wizard.



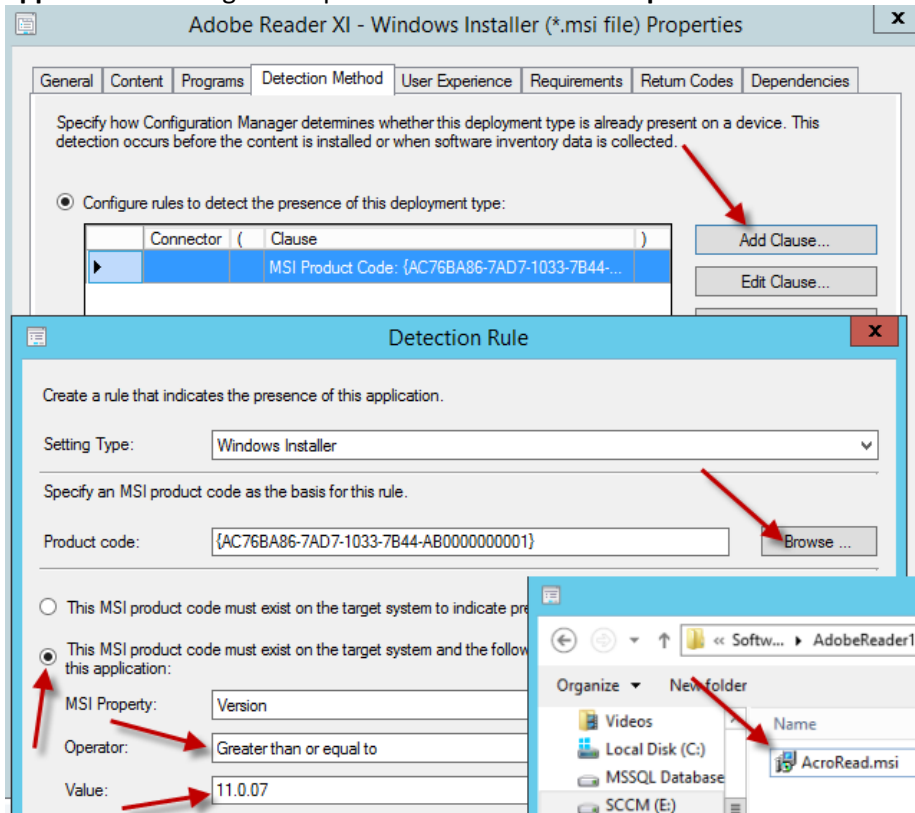
- 8 Click the **Adobe Reader** Application. At the bottom of the page click the **Deployment Types** Tab. Right Click the **Adobe Reader – Windows Installer**, Click **Properties**



9 Under the User Experience set Maximum allowed run time (minutes): **15**. Click **Ok** and **Apply**



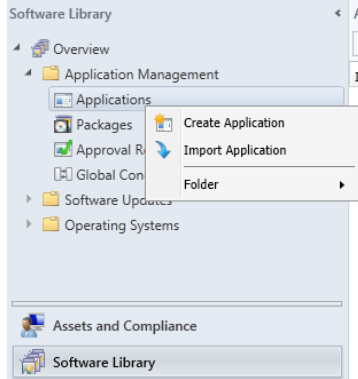
10 Under the Detection Method Tab, Click **Add Clause**. Change Setting Type: **Windows Installer**. Product code, Click **Browse** to find the **AcroRead.msi**. **Select The MSI product code must exist on the target system and the following condition must be met to indicate the presence of the application**. Change the Operator: **Greater than or equal to**. Leave the default Value.



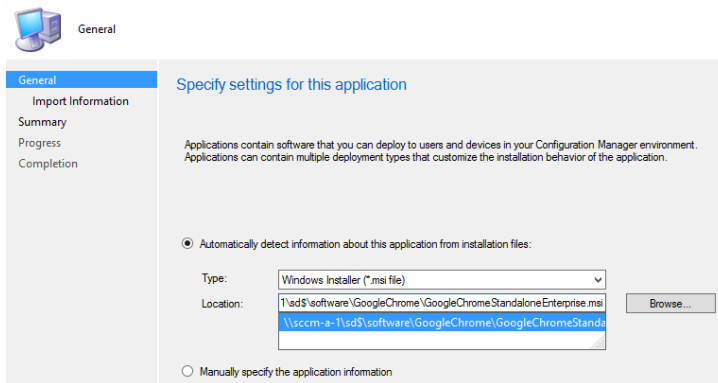
11 Click **Ok** and **Apply**.

### 5.3.2 Chrome

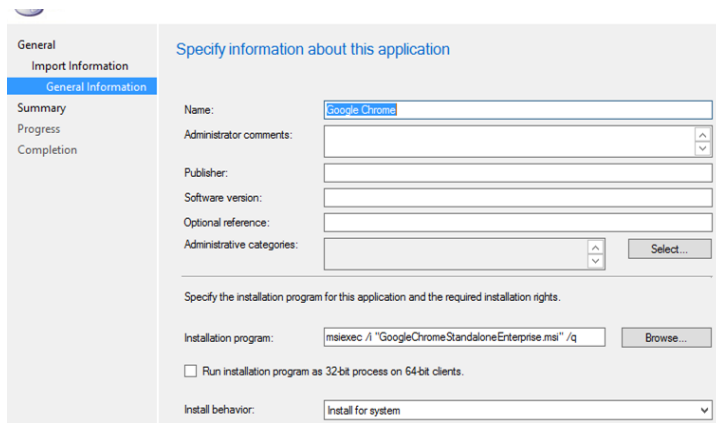
- 1 In the Configuration Manager console, click **Software Library**
- 2 In the **Software Library** workspace, expand **Application Management**, and then right click **Applications**. Click **Create Application**



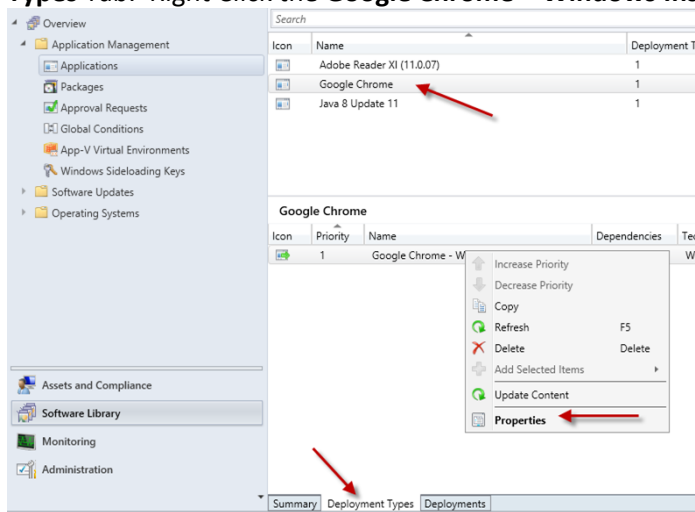
- 3 On the **General Page**, Specify **Type Windows Installer (.msi file)**. In Locations put **\\<YOUR\_SCCM\_SERVER>\sd\$\software\GoogleChrome\GoogleChromeStandaloneEnterprise.msi**
- 4 Click **Next**.



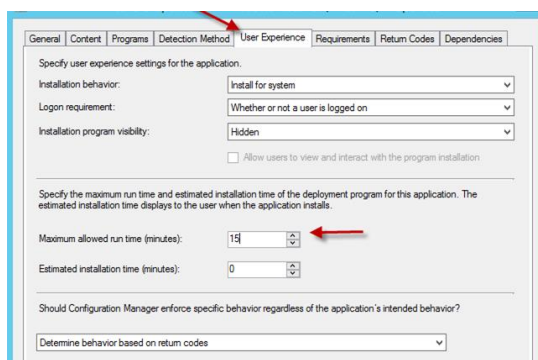
- 5 Click **Next** on the Important Information Screen. Enter the Information on the General Information Screen, **Check Run installation program as 32-bit process on 64-bit clients** and Click Next and Finish the Wizard.



- 6 Click the **Google Chrome** Application. At the bottom of the page click the **Deployment Types** Tab. Right Click the **Google Chrome – Windows Installer**, Click **Properties**

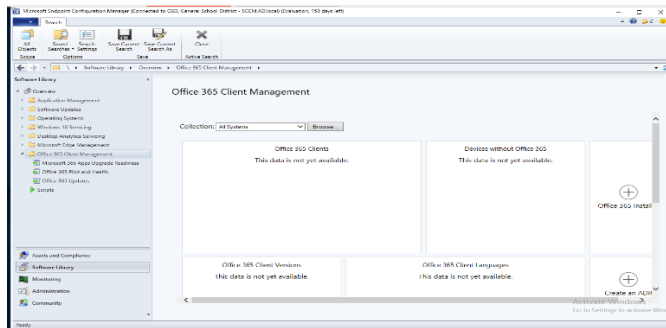


- 7 Under the User Experience set Maximum allowed run time (minutes): 15

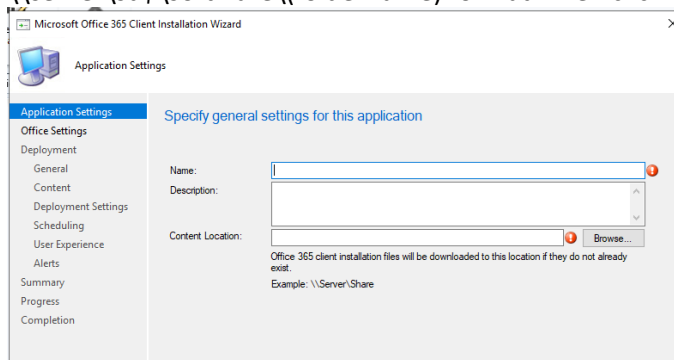


### 5.3.3 Deploy Office 2019 – Office 365

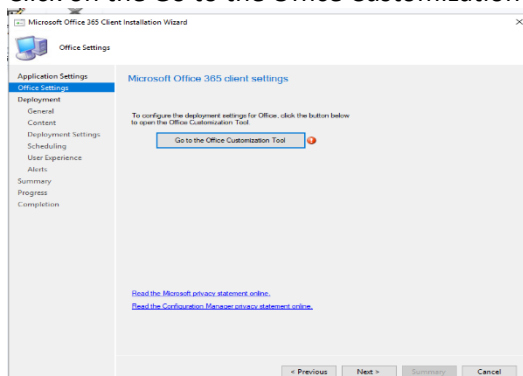
- 1 In the Configuration Manager console, click **Software Library**.
- 2 In the Software Library click on the Office 365 Client Management.
- 3 On the far-right side of the screen Click Office 365 Installer.



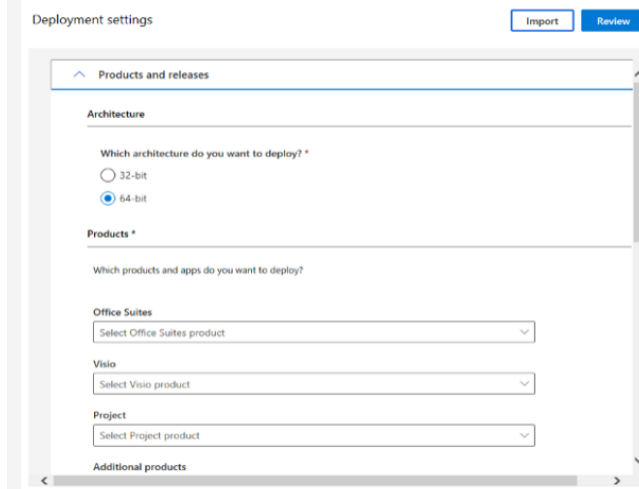
- 4 Enter the name of the Application and select the content folder. This will be in the `\\server\sd$\software\{foldername}` format. Then click Next.



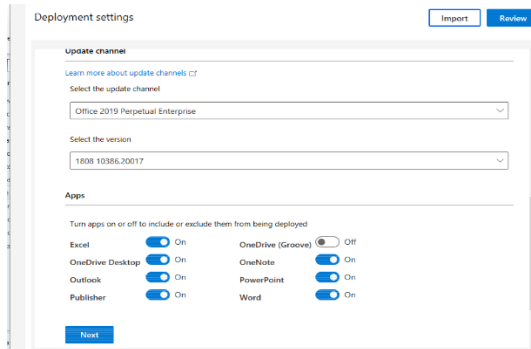
- 5 Click on the Go to the Office Customization Tool.



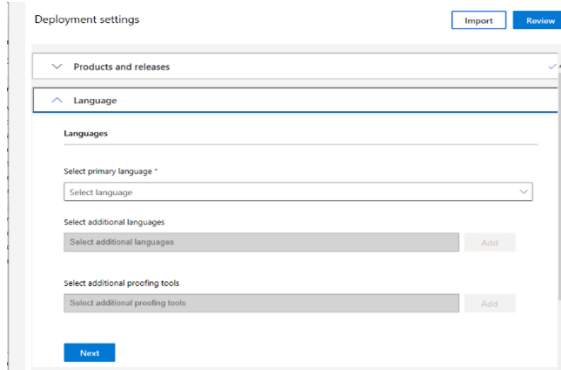
- 6 Select your architecture Office suit version and if you want Visio or Project installed as well. Then click next.



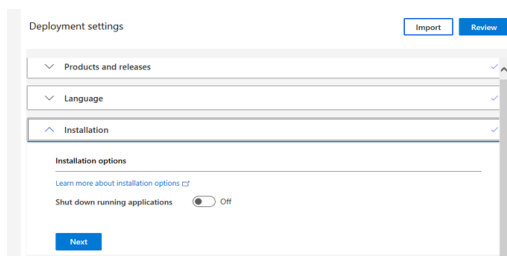
- 7 Set which apps you would like deployed with the installation as well as the update channel to use. Click Next.



- 8 Set your language after that click next again.

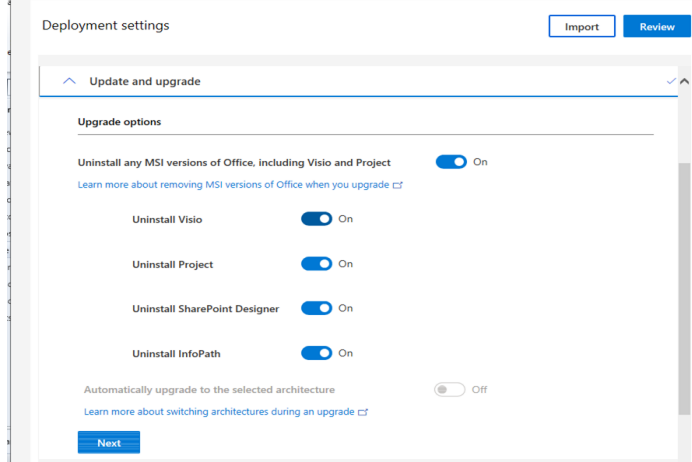


- 9 On the installation option set Shutdown applications. Then click next.

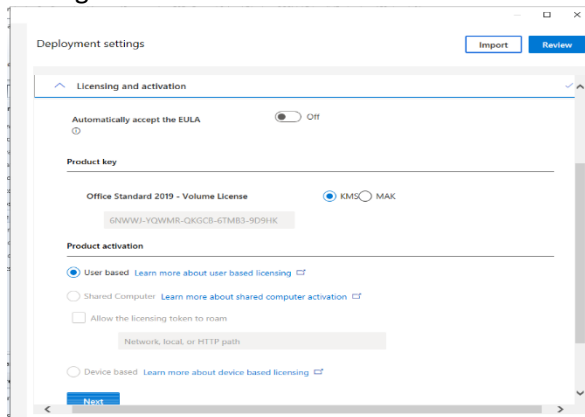




- 10 On the Update and Upgrade option set if you want it to uninstall old versions of office. Then Click next.

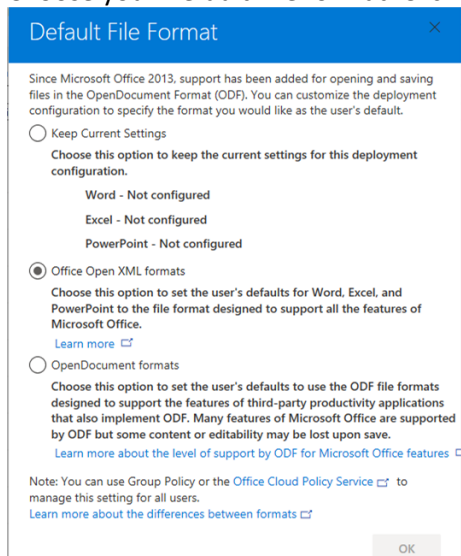


- 11 Set that you accept the EULA and configure your product key and product activation settings. Then click next.

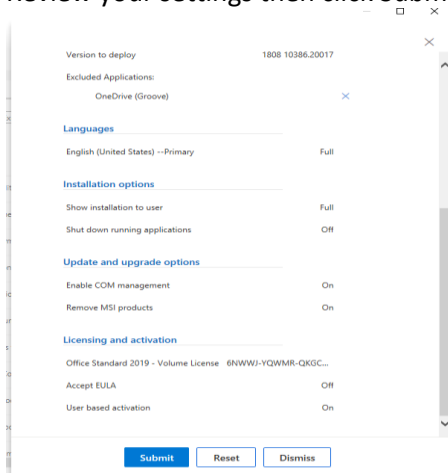


- 12 Next passed the deployment settings.

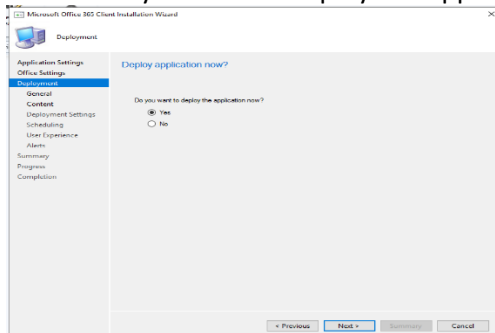
- 13 Choose your Default File format. Click ok then click Review.



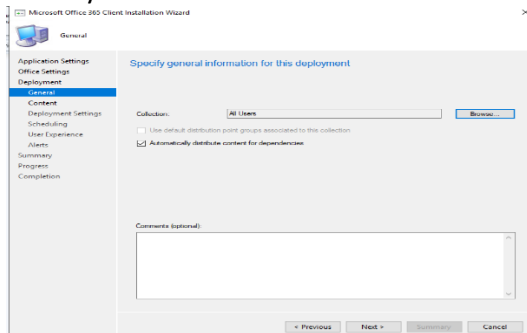
14 Review your settings then click Submit.



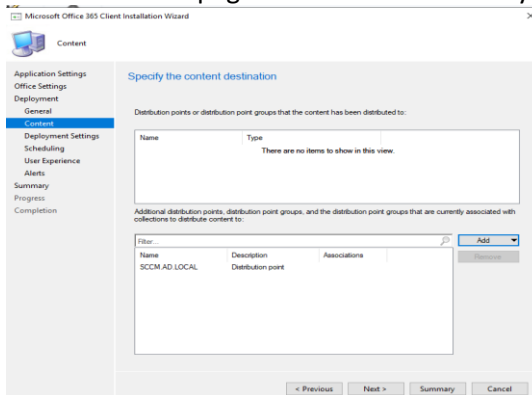
15 Select that you want to deploy this application now and click next.



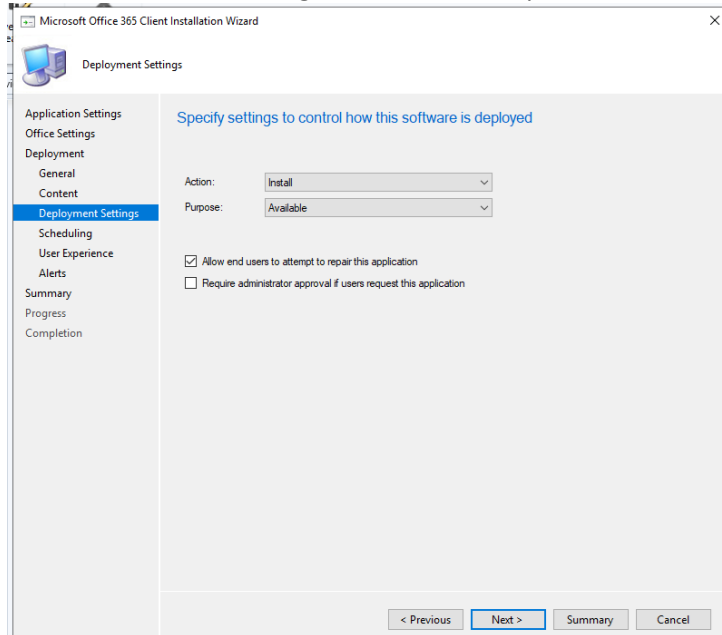
16 Select your collection and click next.



17 On the Content page select add and select your distribution point. Click next.

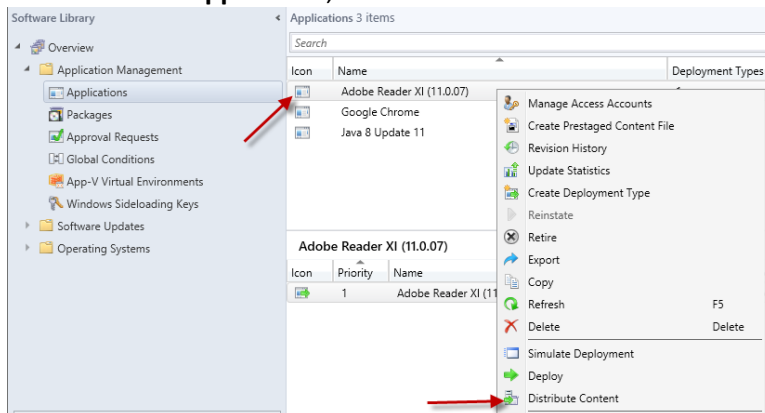


- On the Deployment settings be sure to set that you want it to install and choose required if you want to force it out or available if you want to make it available for users to install. Also make a check mark by the option to allow end users to attempt to repair the software. You can now click next through the rest of the options and finish the deployment.

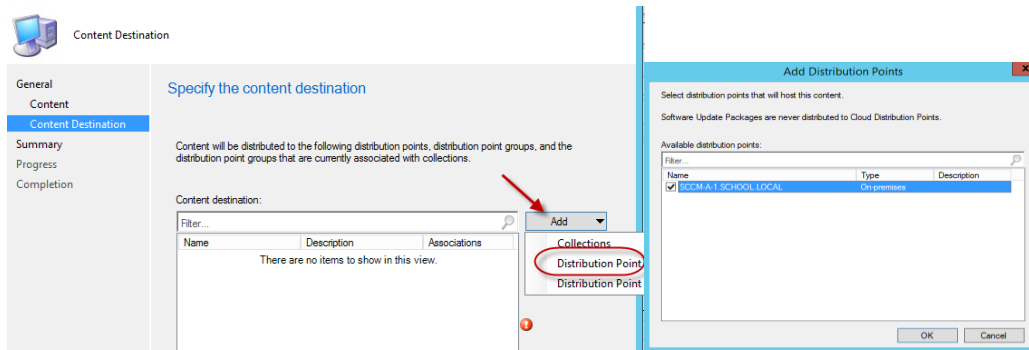


## 5.4 Distribute Software Application

- In the Configuration Manager console, click **Software Library**
- In the **Software Library** workspace, expand **Application Management**, and then Right Click **Adobe Reader Application**, Select **Distribute Content**



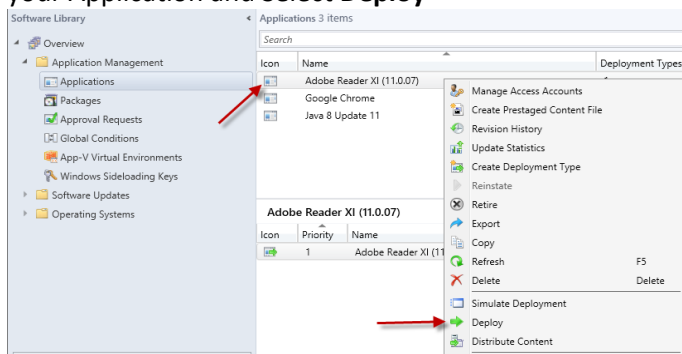
- Click **Next** On General Screen. Click **Next** On the Content Screen. On the Content Destination screen Click **Add** and hose **Distribution Point** and Select the `\\<YOUR_SCCM_SERVER>.<YOUR_DOMAIN>.local` and click **OK** and



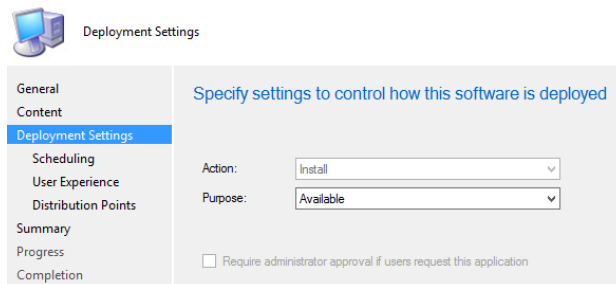
4 **Next and Finish.**

## 5.5 Deploy Software Application

- 1 In the Configuration Manager console, click **Software Library**
- 2 In the **Software Library** workspace, expand **Application Management**, and then Right Click your Application and Select **Deploy**

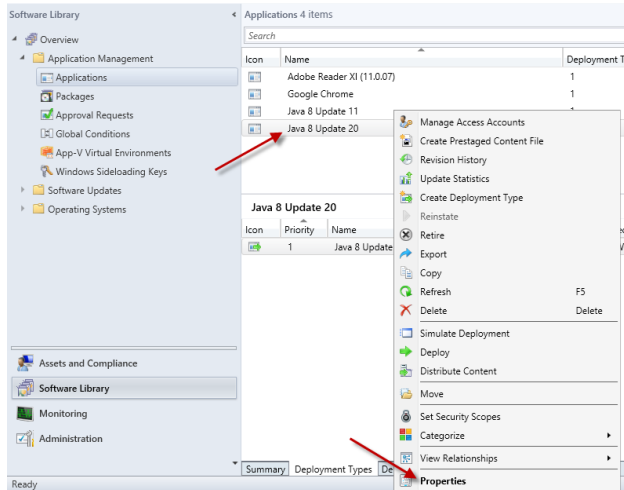


- 3 On the **General** page of the **Deploy Software Wizard**, specify the following information:  
**Software** – Displays the application you want to deploy. You can click **Browse** to select a different application to deploy.  
**Collection** – Click **Browse** to select the collection you want to deploy the application to.
- 4 On the **Content** page Click **Next**
- 5 On the **Deployment Settings** page, Chose the **Action: Install** and the **Purpose: Available**. Click **Next** through the rest of the wizard.

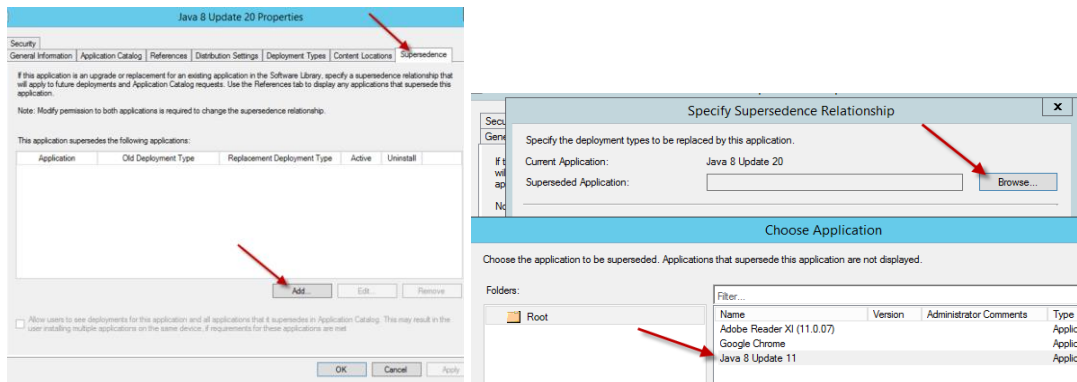


## 5.6 Update / Supersede Application

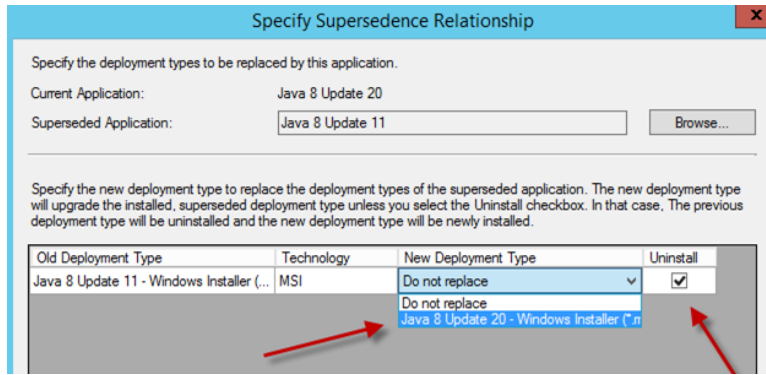
- 1 Create Software Application (See 5.3.1) for Latest Software Application.
- 2 Distribute Software Application (See 5.3.2).
- 3 In the **Software Library** workspace, expand **Application Management**, and then Right Click your New Application and Select **Properties**



- 4 On the **Supersedence** Tab, Under **the application supersedes the following application**, Click **Add** and Click **Browse**. Select the Application to be superseded (**Java 8 Update 130**) and Click **OK**.



- 5 Under the New Deployment Type, Drop down the box and select the new Application that will supersede the old application (**Java 8 Update 131 – Windows Installer (\*msi)**). Check the **Uninstall** if you need to for the old application to be removed. Click **OK** and **Apply**.



- 6 Deploy Software Application (See 5.3.3)
- 7 Once your workstation have updated to the latest software (1-3 weeks), delete the old application and clean up the software distribution directory.

## 6 Configure Operating System Deployment (Imaging)

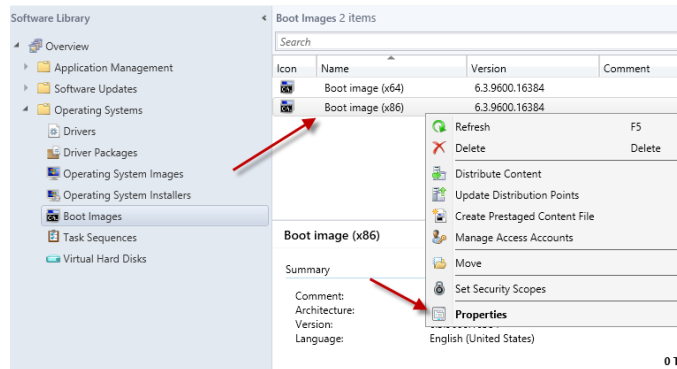
### 6.1 Copy Source Images

- 1 In the **Software Distribution** folder, under **Images** folder create sub folders **Win10x64**.
- 2 Copy **install.wim** file for Windows 10 x64, which is present on the Windows 10 DVD under the **Sources** folder.

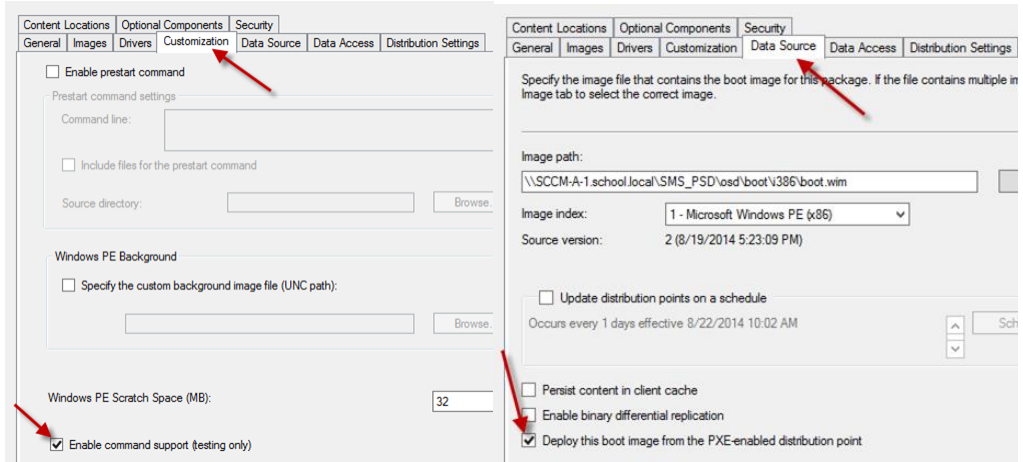
### 6.2 Customize & Distribute Boot Images to the Distribution Points

**\*\*\* Do this for both x64 and x86 images**

- 1 From the bottom left of the SCCM console screen, select **Software Library**.
- 2 Expand **Operating Systems** and select **Boot Images**.



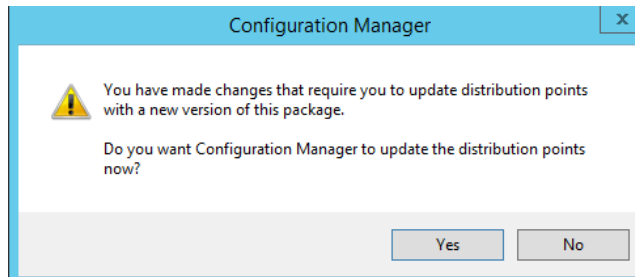
3 Double-click **Boot Image (x86)**.



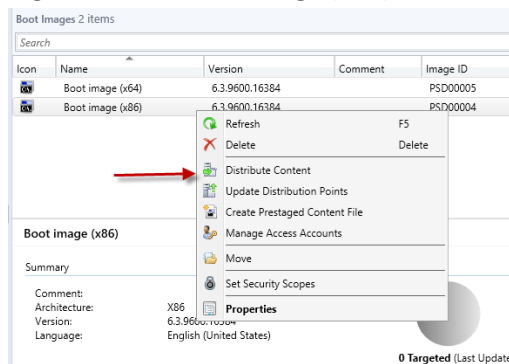
4 Select the **Customization** tab and select **Enable command support**.

5 Select the **Data Source** tab to make sure **Deploy the boot image from the PXE service point** is checked and then click **OK**.

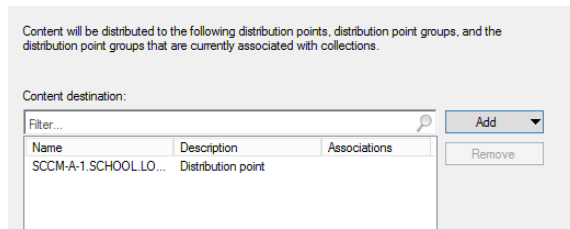
6 When prompted to update the Distribution Points, click **Yes** and then **OK** to close.



7 Right-click the **Boot Image (x86)** and choose **Distribute Content**.



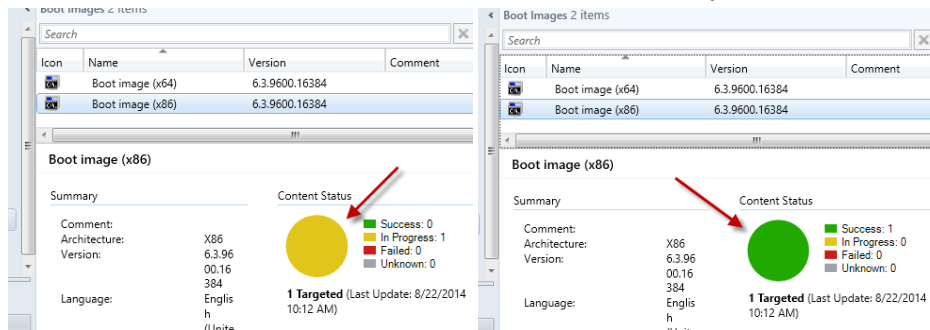
- 8 Select **Add > Distribution Point** to select the server (**SCCM-A-1.SCHOOL.LOCAL**).



- 9 Click **OK** and **Next**.

- 10 Repeat Steps for **Boot Image (x64)**.

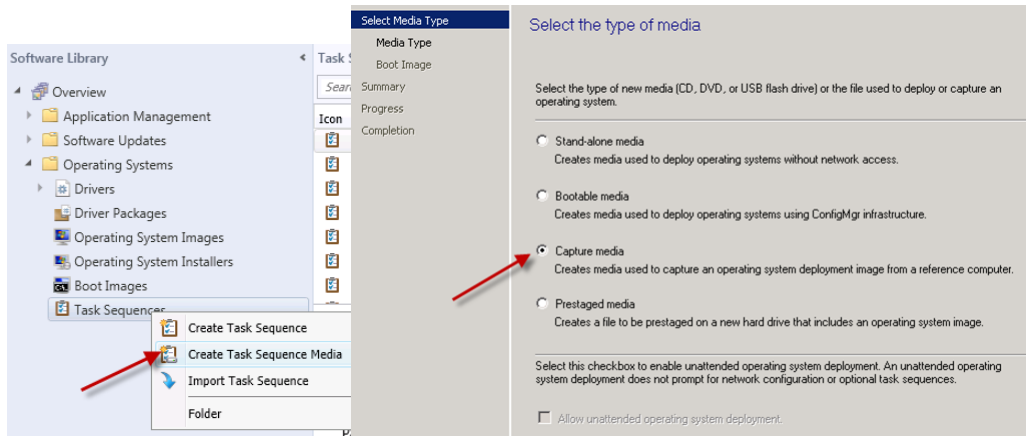
- 11 Make sure the Content Status is Green (Successful) before you continue.



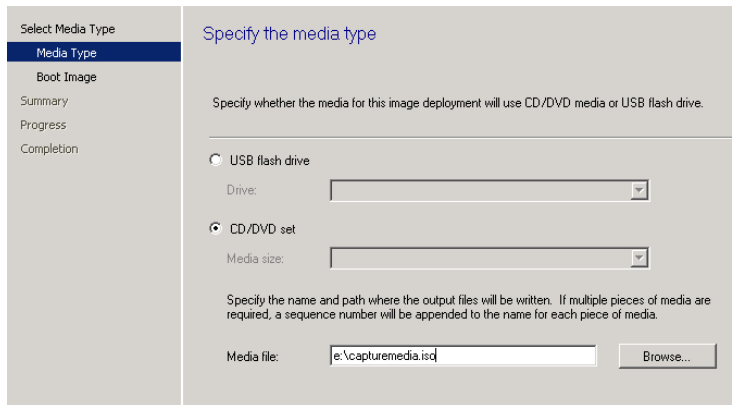


## 6.3 Capture Prepared Windows Image

- 1 Right click on Software Library, Operating Systems, Task Sequences. Click on Create Task Sequence Media when the Create Task Sequence Media

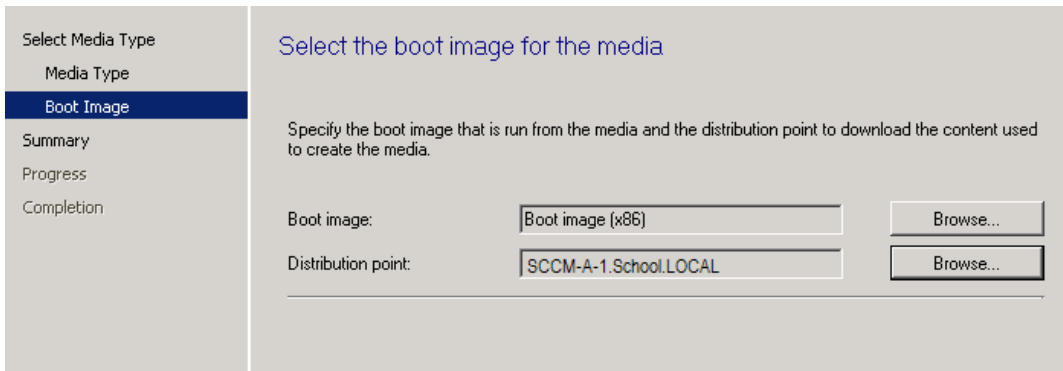


- 2 On the Select Media Type Page, Select the Capture Media, Click Next.
- 3 On the Media Type Page, Select **CD/DVD** set. In the Media File, browse to the path of where you want to store the ISO file, give it a name like **e:\capturemedia.iso**. Click Next.

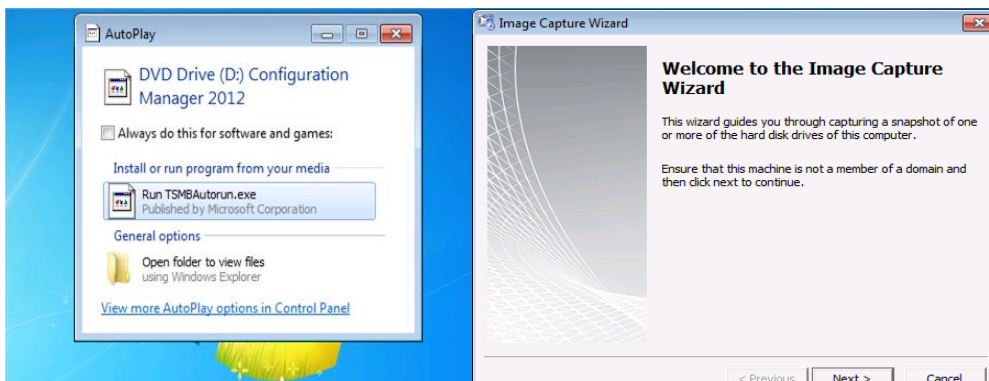


- 4 On the Boot Image Page, browse beside boot image, select your X86 boot image, click ok, then click on Browse beside Distribution Point, select your distribution point. Click next to continue

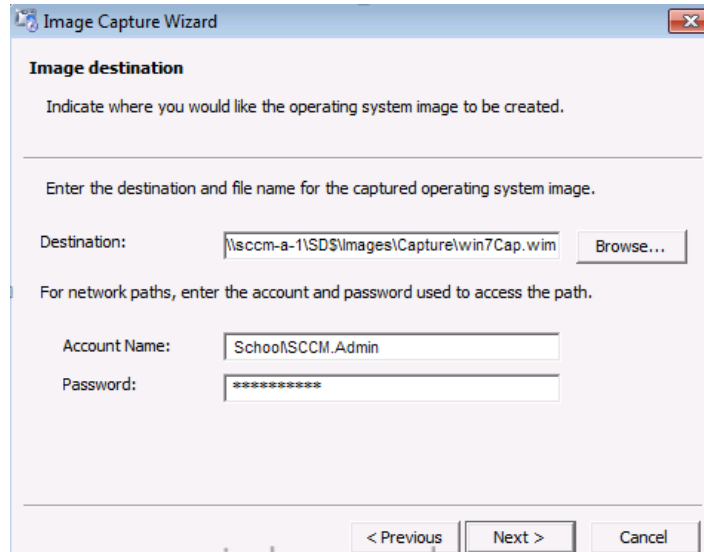
through the wizard.



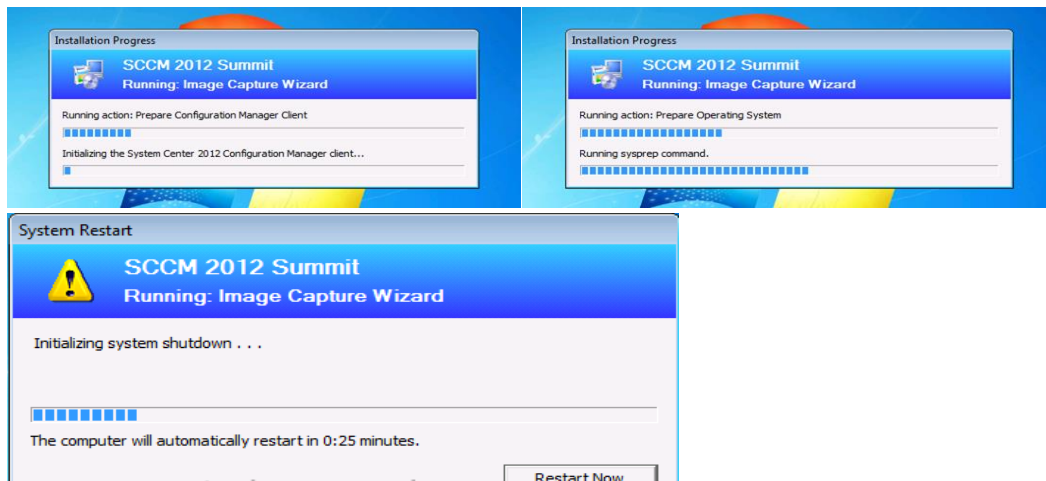
- 5 Burn this CaptureMedia.ISO to a CDROM or save it to a network share.
- 6 Log into Prepare Windows Workstation as **Domain Administrator**
- 7 While in Windows of the Prepare Windows Workstation, Remove the workstation from the Domain
  - 7.a Click on Start, Right click on Computer, choose properties
  - 7.b Click on change settings to the right of the Computer Name
  - 7.c Click on Change, type in the name of a workgroup to join and click ok
  - 7.d You will be welcomed to the workgroup, click ok
  - 7.e You will be prompted to reboot the workstation. **DO NOT** reboot. We will continue with the capture process and then reboot
- 8 Insert the ISO/CD/DVD on the Computer, While still in Windows (do not try to boot from this ISO/CD/DVD) you should see the following



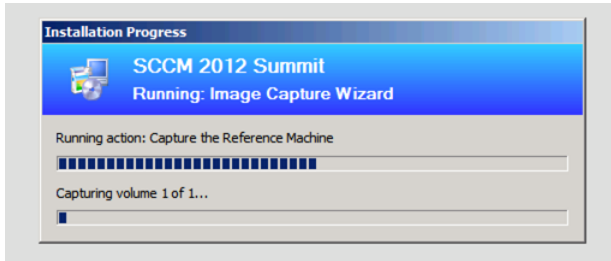
- 9 Click on Run TSMBAutorun.exe, Welcome to the Image Capture Wizard appears, click next..



- 10 Enter a path and name for the WIM file  
**\\<YOUR\_SCCM\_SERVER\SD\$\Images\captured\CapturedWin10.x86.wim** and then enter the credentials of a user with permissions to write to that location **School\SCCM.Admin**, Click next.  
Enter Image Information



- 11 Click Next and Click finish to start the capture process, notice how it prepares the config manager client and then it syspreps before rebooting into Windows PE to capture the system.

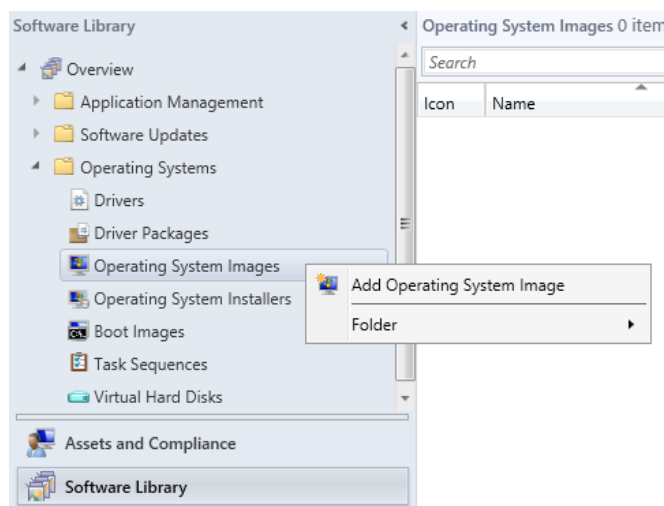


- 12 Your workstation will reboot automatically into Windows PE **without** you having to press the F12. You will only need to monitor the progress from here to the end of the process.
- 13 Once the workstation has finished the capture process there will be a win10cap.wim file located on the SCCM server that you can Create an Operating System Image and a Task Sequence to be deployed.

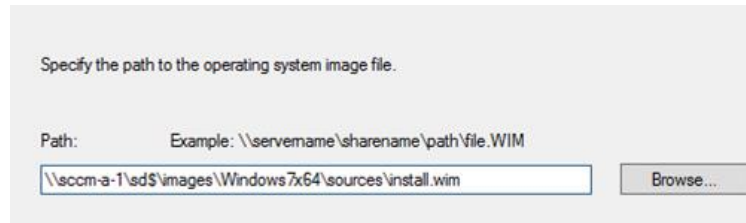
#### 6.4 Add Operating System DVD Image (Install.WIM)

This will be the **install.wim** image file copied from the Windows 7 or Windows 8 DVD.

- 1 In the SCCM Console, click on **Software Library**.
- 2 Expand **Operating Systems**, right-click **Operating System Images** and choose **Add Operating System Image**.

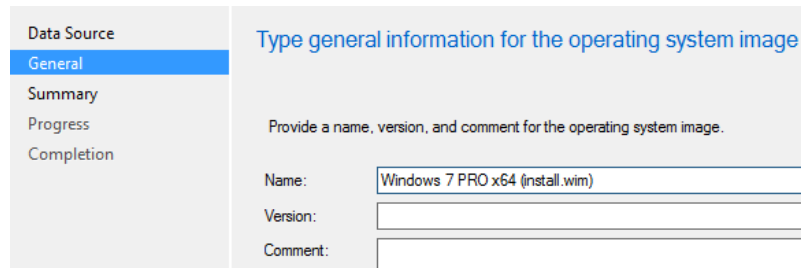


- Browse to `\\<YOUR_SCCM_SERVER>\SD$\Images\Windows10x64\sources\` to find and select the **install.wim** from this folder.

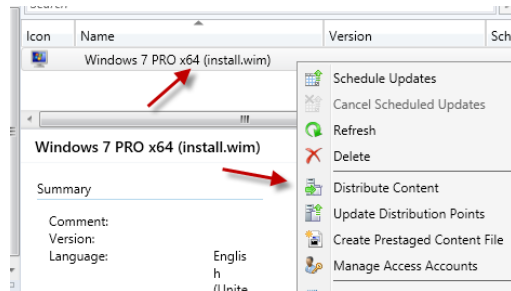


- Enter the **Name**, **Version** number, **Comment** and complete the wizard. Make sure the name is descriptive enough to know what this image contains.

#### Windows 10 x64 (install.wim)



- Distribute Content** after the image has been added successfully.

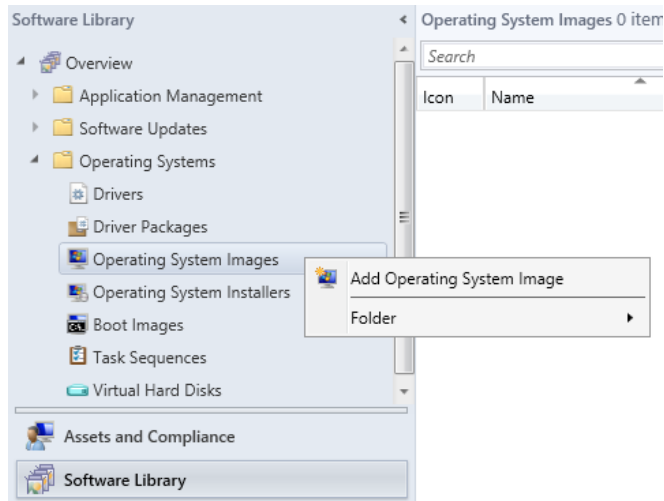


- Repeat** steps for each **Version** of Windows you intend to deploy.

### 6.5 Add Operating System Captured Image (CapturedWindows10.WIM)

This will be the image file captured from the WDS or SCCM Capture Process.

- In the SCCM Console, click on **Software Library**.
- Expand **Operating Systems**, right-click **Operating System Images** and choose **Add Operating System Image**.



- Browse to `\\<YOUR_SCCM_SERVER>\SD$\Captured` to find and select the **CapturedWin10x64.wim** file from this folder.

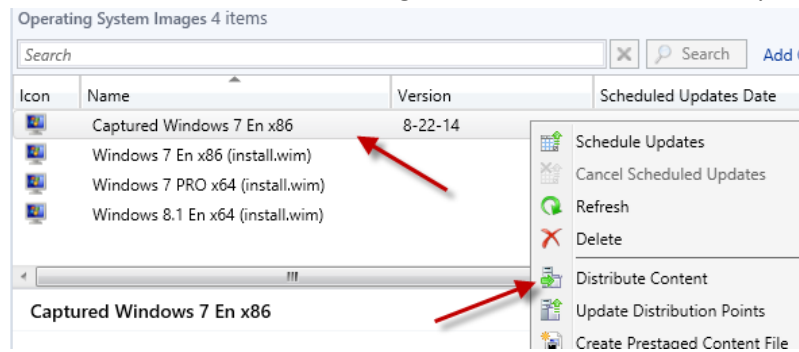
Specify the path to the operating system image file.

Path:  Example: `\\servername\sharename\path\file.WIM`

- Enter the **Name (Captured Windows 10 En x64)**, **Version number (Date Captured)**, **Comment** and Click **Next** and complete the wizard. Make sure the name is descriptive enough to know what this image contains. You will need these comment to know what images are what in the future. Recommend that you put the date the image was captured.

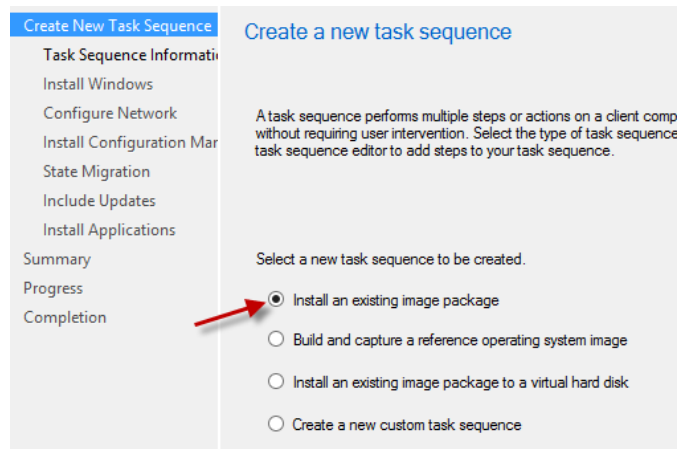
Data Source	<p>Type general information for the operating system image</p> <p>Provide a name, version, and comment for the operating system image.</p> <p>Name: <input type="text" value="Captured Windows 7 En x86"/></p> <p>Version: <input type="text" value="8-22-14"/></p> <p>Comment: <input type="text" value="Image Captured from Workstation"/></p>
<b>General</b>	
Summary	
Progress	
Completion	

11 **Distribute Content** after the image has been added successfully.

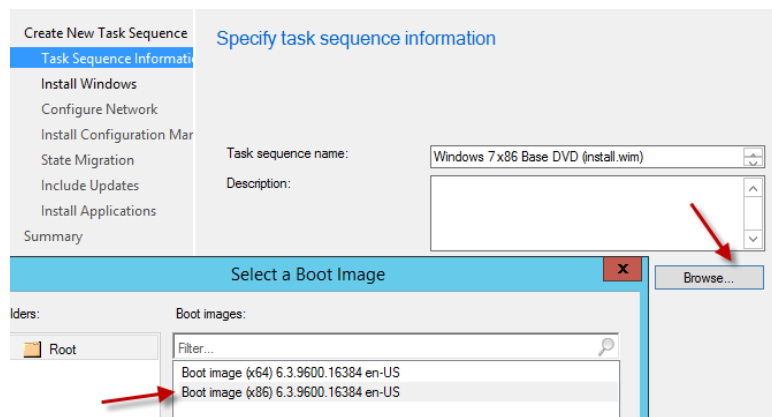


## 6.6 Create the Base (DVD) Operating System Installation Task Sequence

- 1 From the bottom left of the SCCM console screen, select **Software Library**.
- 2 Expand **Operating Systems** and right click on **Task Sequences**, and select **Create Task Sequence**.
- 3 Select **Install an existing image package** and click **Next**

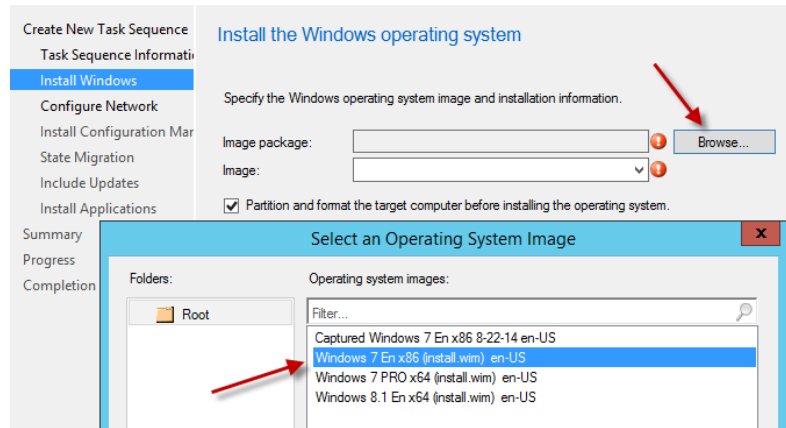


- 4 Fill in the **Task Sequence name** that will be visible during imaging and click **Browse** to select the corresponding **Boot image**.

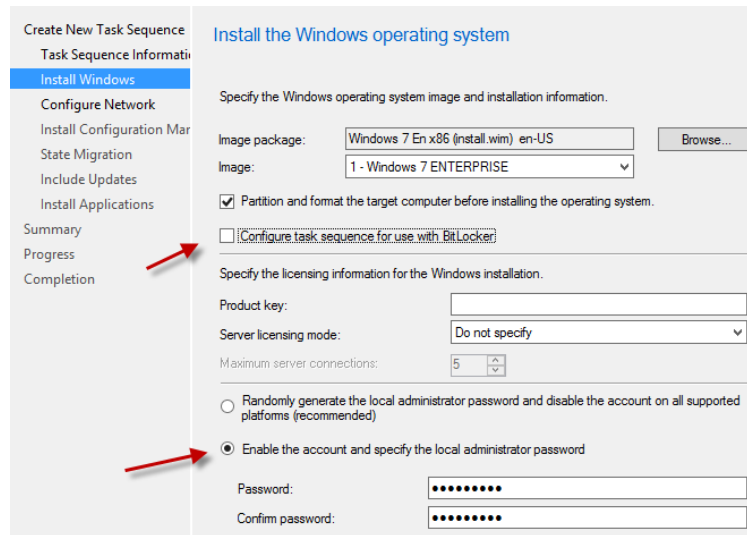




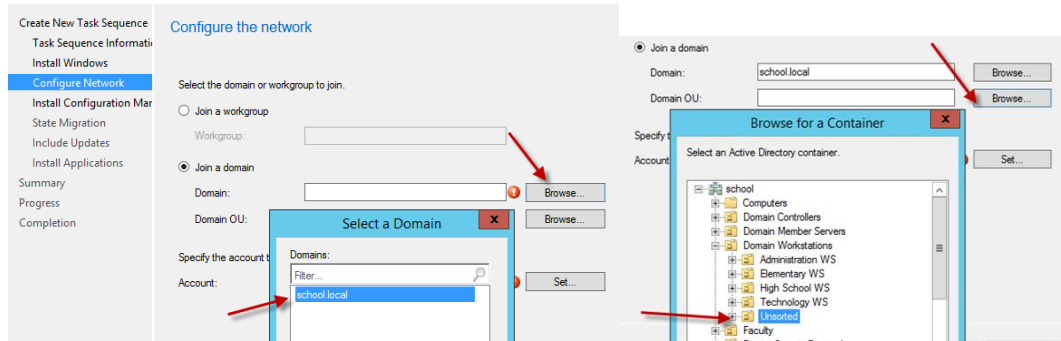
- 5 On the Install the Windows Operating System screen, click on **Browse** and select the corresponding Windows Image.



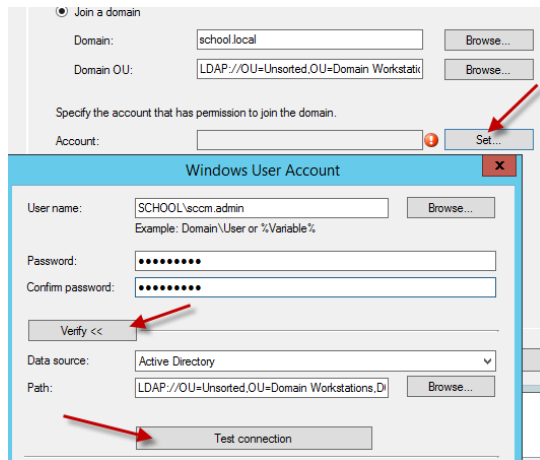
- 6 Make sure **Partition and format the target computer before installing the operating system** is **Checked**. If you do not plan to use BitLocker, **Uncheck Configure task sequence for use with BitLocker**. Do not Use a product key, enter a password for the **Local Administrator** and click **Next**.



- 7 On the **Configure Network** screen, select **Join a Domain** and click **Browse** for **Domain** and select **<YOUR\_DOMAIN>.local**, click **OK**. Select **Browse** for Domain OU and select **Domain Workstations\Unsorted** and Click **OK**.

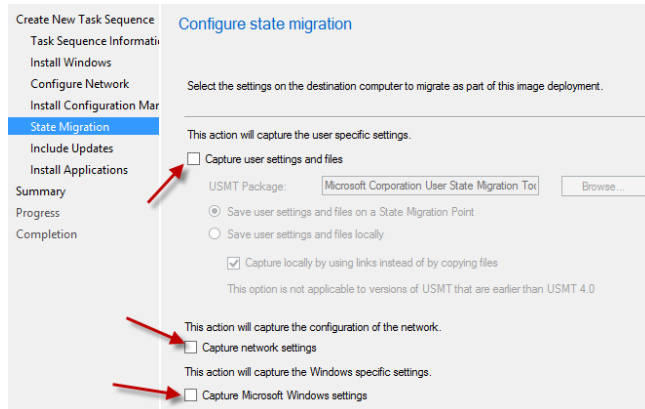


- 8 Click **Set** for Account name, Browse for **SCCM.Admin**. Enter **Password** and click **OK**.

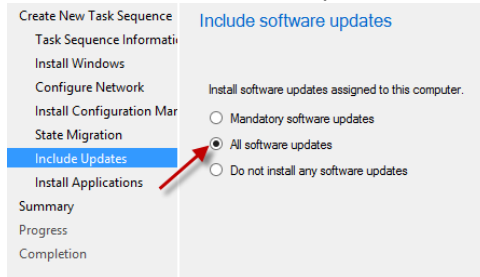


**\*\*Make sure SCCM Admin has rights to join machines to the Domain.**

- 9 Click **Next** on Install the Configuration Manager Client. On the configure State Migration screen, uncheck all the **Capture** options and click **Next**.



10 On the Include Software Updates screen, select **All software updates** and click **Next**.

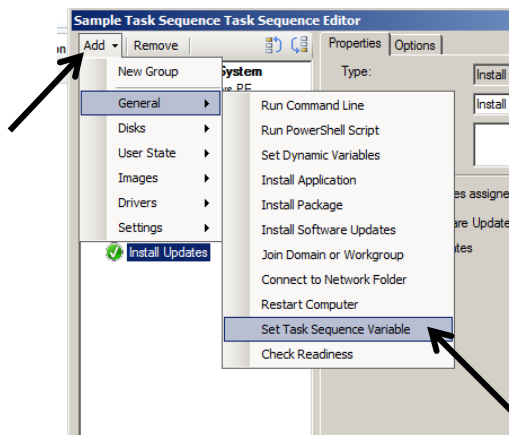


11 On the Install Applications screen Click **Next**, click **Next** through the following screens and complete the wizard.

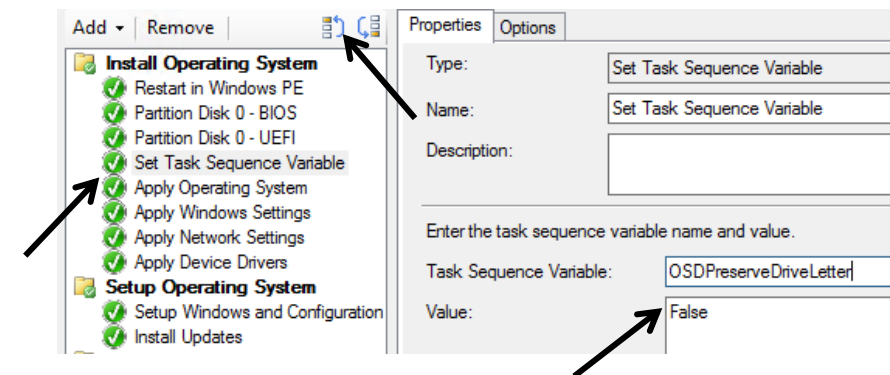
12 Right-click the newly created Task Sequence and select **Edit**.

13 Click on **Add -> General -> Set Task Sequence Variable**.

**\*\* This step is ONLY required if the install.wim file is used from Windows 7 DVD**



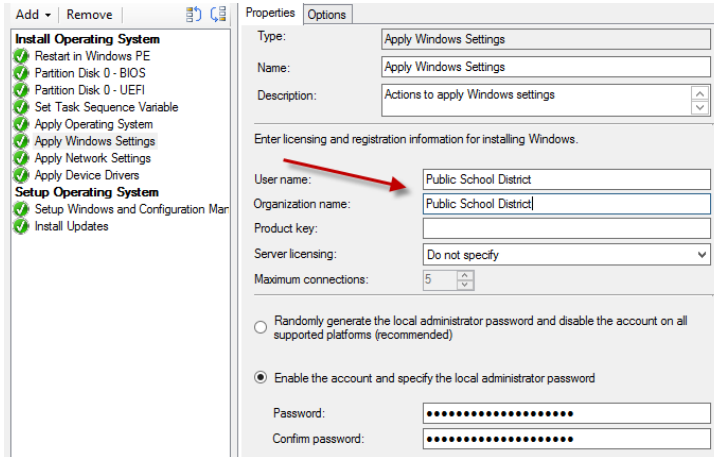
14 In the **Task Sequence Variable** put **OSDPreserveDriveLetter** and **FALSE** in the value field. Move up **Set Task Sequence Variable** above **Apply Operating System** using the icon to move variables.





15 Select the **Apply Windows Settings**. Change the following:

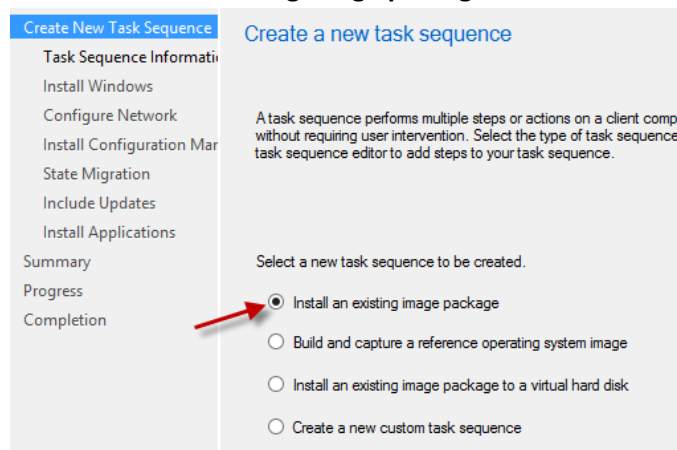
- User name: **Public School District**
- Organization Name: **Public School District**



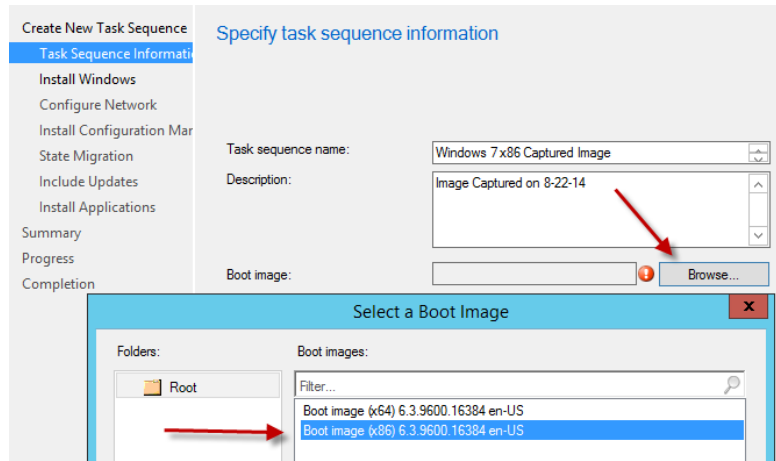
16 Click **Apply** and **OK** to save and close

## 6.7 Create the Captured Image Deployment Installation Task Sequence

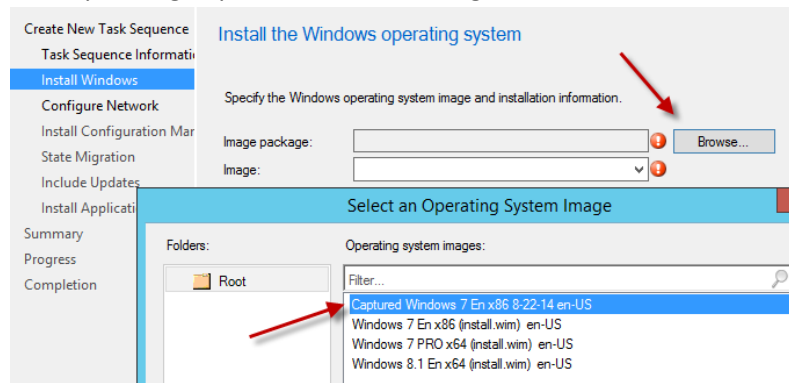
- 1 From the bottom left of the SCCM console screen, select **Software Library**.
- 2 Expand **Operating Systems** and right click on **Task Sequences**, and select **Create Task Sequence**.
- 3 Select **Install an existing image package** and click **Next**



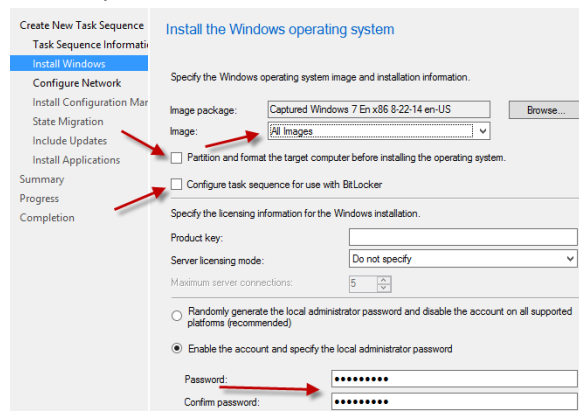
- 4 Fill in the **Task Sequence name** that will be visible during imaging and click **Browse** to select the corresponding **Boot image**.



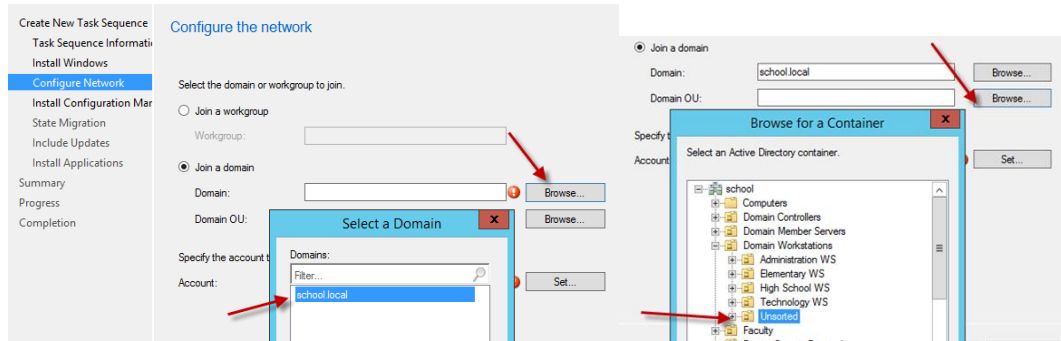
- 5 On the Install the Windows Operating System screen, click on **Browse** and select the corresponding Captured Windows Image.



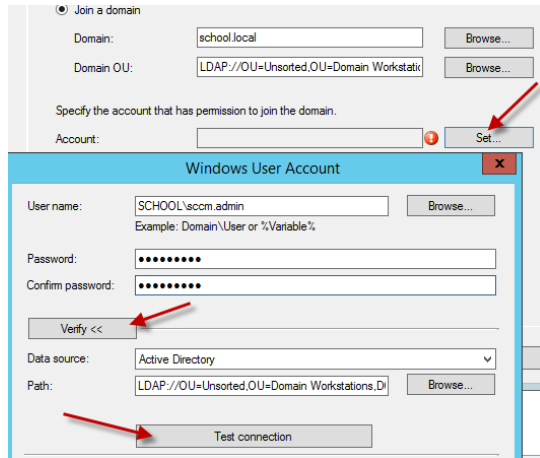
- 6 If you have more than partition from your captured image, make sure you have the Image **All Images** selected. If you only want the system partition from the Captured Image, select the 1:1 Image. Make sure **Partition and format the target computer before installing the operating system** is **Checked**. If you do not plan to use BitLocker, **Uncheck Configure task sequence for use with BitLocker**. Do not Use a product key, enter a password for the **Local Administrator** and click **Next**.



- On the **Configure Network** screen, select **Join a Domain** and click **Browse** for **Domain** and select **<YOUR\_DOMAIN>.local**, click **OK**. Select **Browse** for **Domain OU** and select **Domain Workstations\Unsorted** and Click **OK**.

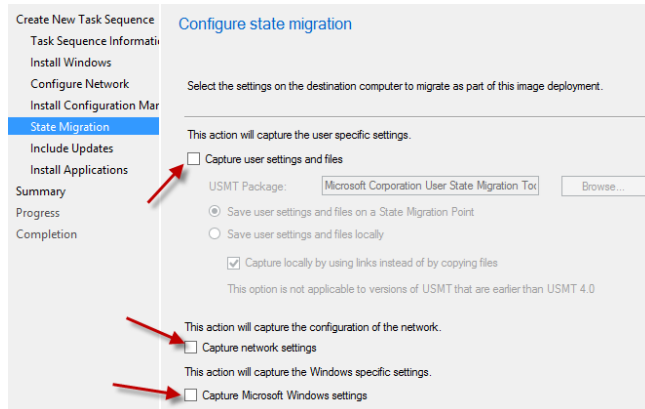


- Click **Set** for Account name, Browse for **SCCM.Admin**. Enter **Password** and click **OK**.

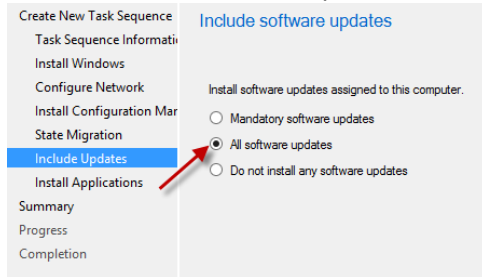


**\*\*Make sure SCCM Admin has rights to join machines to the Domain.**

- Click **Next** on Install the Configuration Manager Client. On the configure State Migration screen, uncheck all the **Capture** options and click **Next**.



10 On the Include Software Updates screen, select **All software updates** and click **Next**.

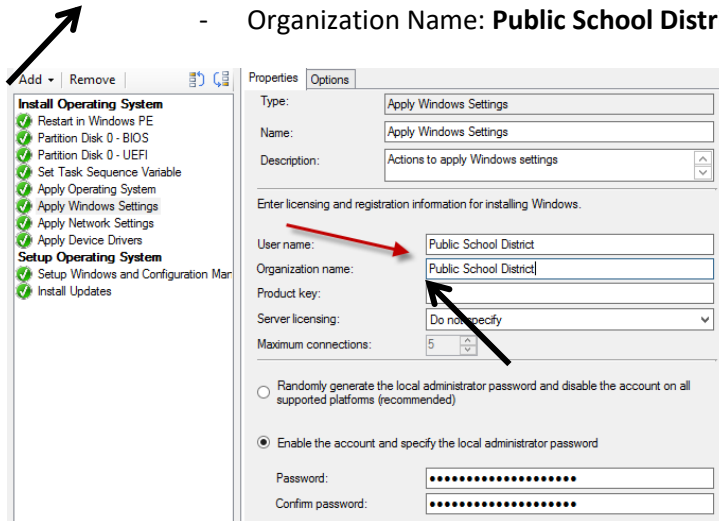


11 On the Install Applications screen Click **Next**, click **Next** through the following screens and complete the wizard.

12 Right-click the newly created Task Sequence and select **Edit**.

13 Select the **Apply Windows Settings**. Change the following:

- User name: **Public School District**
- Organization Name: **Public School District**



14 Click **Apply** and **OK** to save and close

## 6.8 Deploy the Base DVD OS Install Task Sequence.

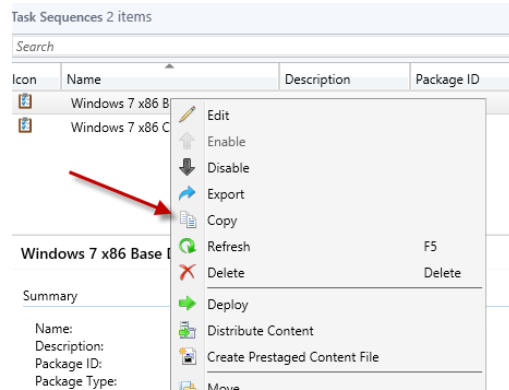
- 1 Click **Software Library, Task Sequences** and right-click on the **Windows 7 x86** task sequence, and select **Deploy**.
- 2 Click **Browse** to select the **Windows Imaging Collection** Device Collection and click **OK**.
- 3 If prompted with a message that the collection does not contain any members, click **OK**.
- 4 Click **Next**.



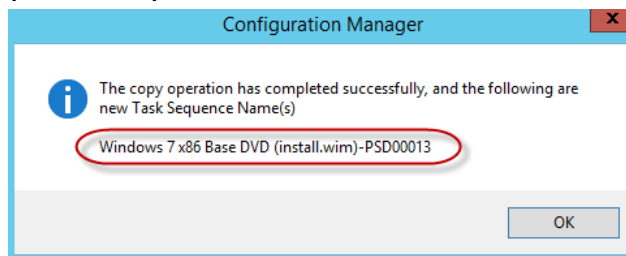
- 5 On the Deployment Settings screen, check the Make available to boot media and PXE and then click Next.
- 6 Click Next through the rest of the screens and complete the wizard
- 7 Add workstation objects you wish to image to the Windows Image Collection. Make sure the All Unknown Computer Collection is a member of this collection also.

## 6.9 Add Software Applications/Packages to Image Task Sequence.

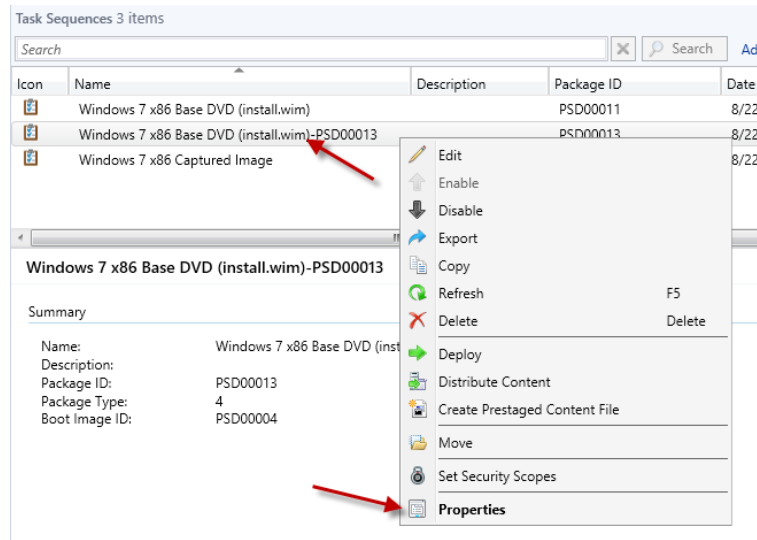
- 1 Click **Software Library, Task Sequences** and right-click on the **Windows 7 x86 Base DVD (install.wim)** task sequence, and select **Copy**.



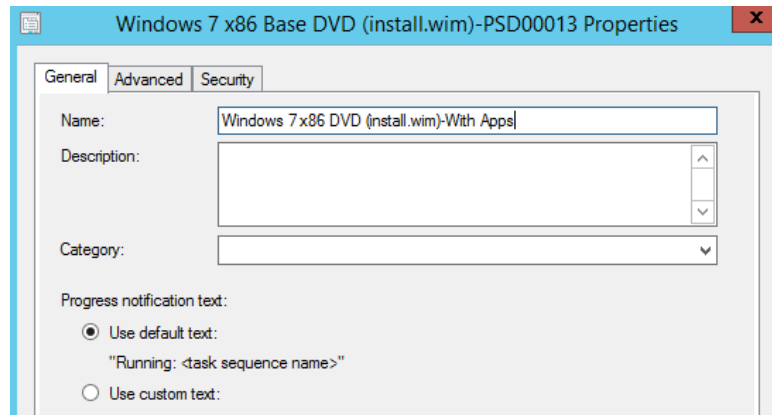
- 2 Click OK to confirm the copy was successful. Notice the name **Windows 7 x86 Base DVD (install.wim)-PSD00013**. This is the name of the new task sequence that was created.



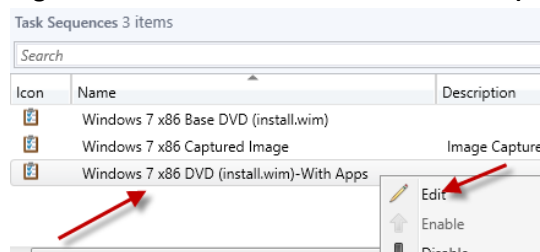
- Right Click the new **Windows 7 x86 Base DVD (install.wim)-PSD00013** task sequence and select **Properties**.



- On the General Tab, Change the name to **Windows 10 x64 DVD (install.wim) –With Apps**.

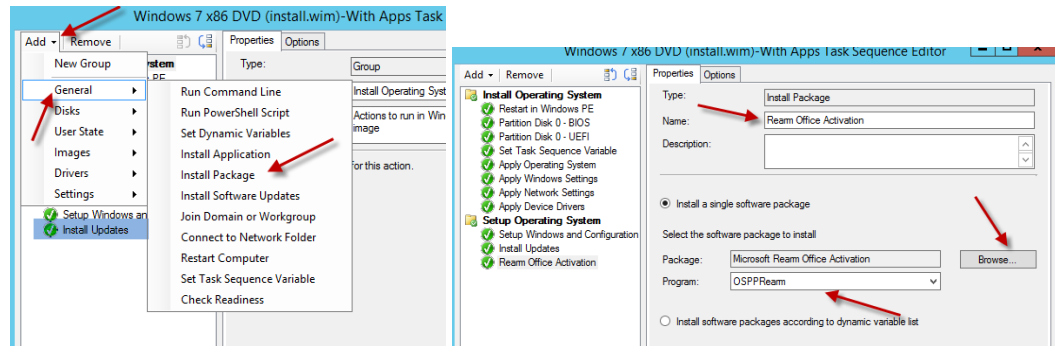


- Click **OK**.
- Right Click the new **Windows 10 x64 DVD (install.wim) –With Apps** and Click Edit.

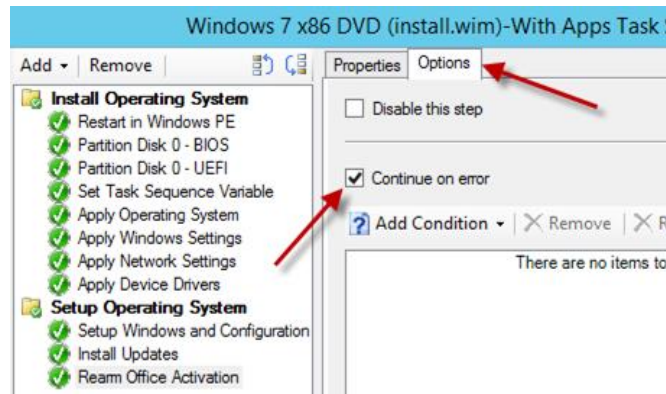


- Make sure you have **Install Updates** Highlighted and Click **Add** and Select **General**. Click **Install Package**. Enter the Name of the Package **Rearm Office Activation**. Click **Browse** and Select the **Microsoft Rearm Office Activation Package** and verify that the Program

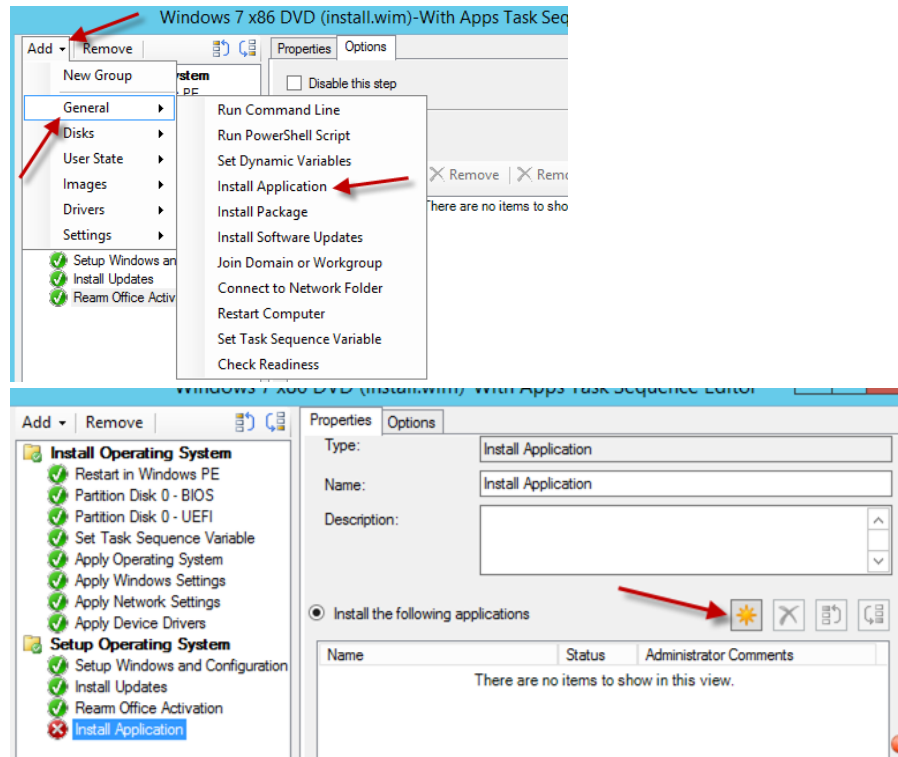
## OSPPRearm



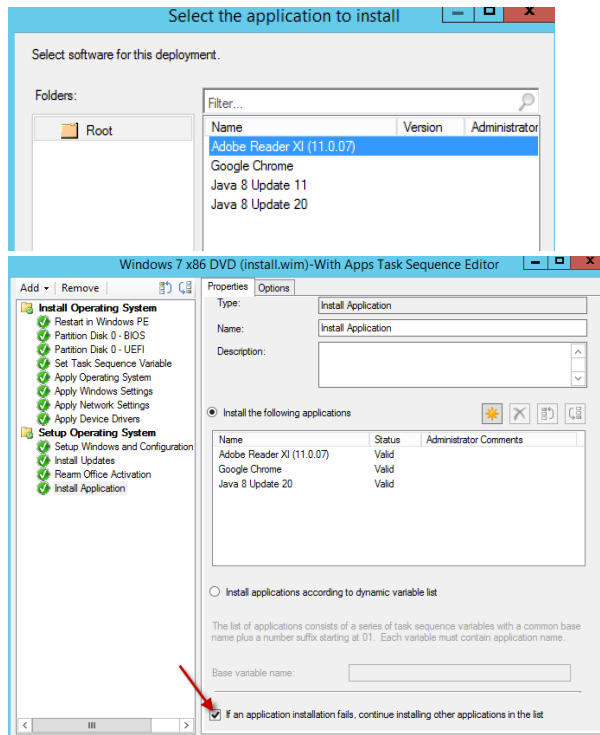
- 8 Click on the **Options** Tab and Check the box **Continue on error**.



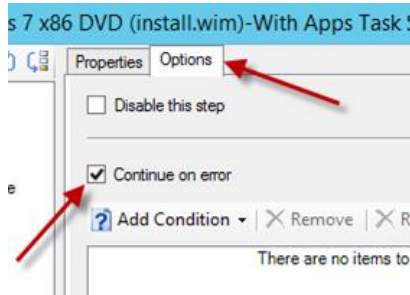
- 9 Click **Install Application**. Click the Add (**Star**).



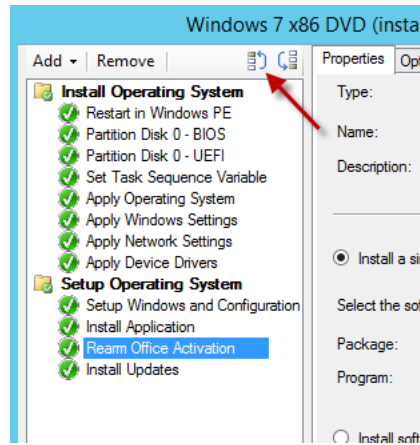
- 10 Select the Application you would like to add to the image and Click OK. Repeat the Process until you have added all the applications you would like to add. Make sure you check the box **If an application installation fails, continue installing other applications in the list.**



- 11 Click on the **Options** Tab and Check the box **Continue on error.**



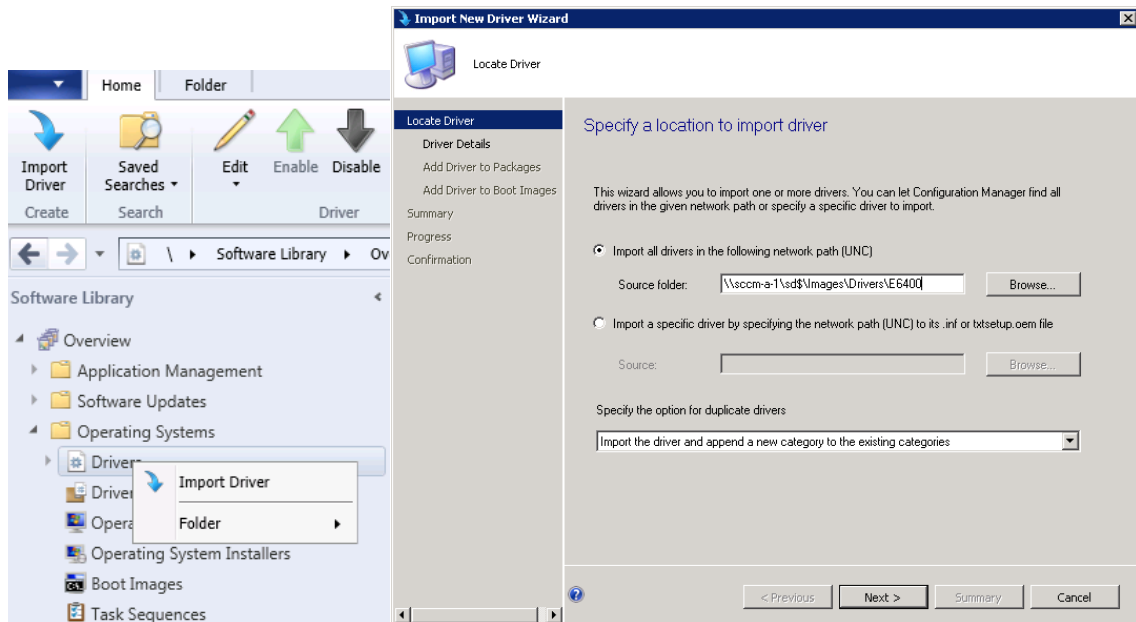
- 12 Use the button at the top to rearranging the tasks to have the Install Applications above Packages and Updates



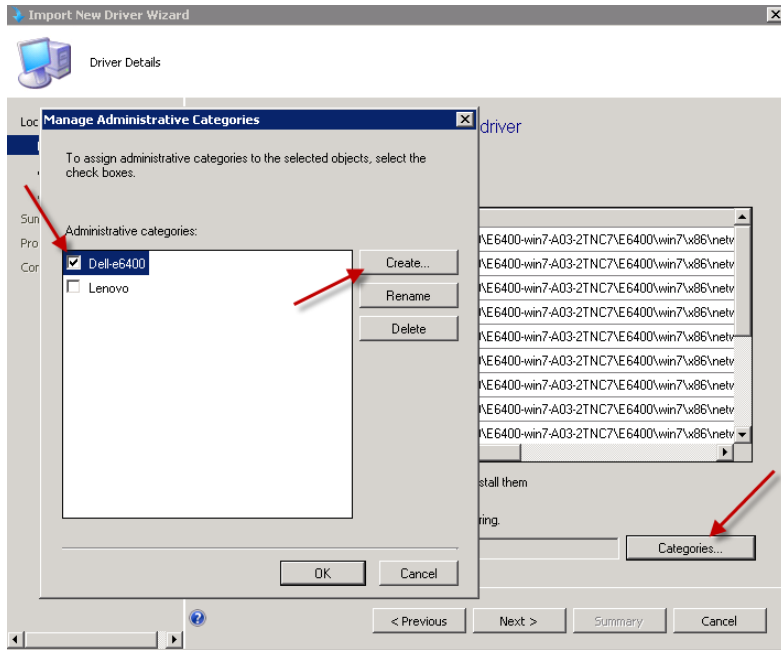
- 13 Click **Apply** and **OK**.

## 6.10 Import Device Drivers

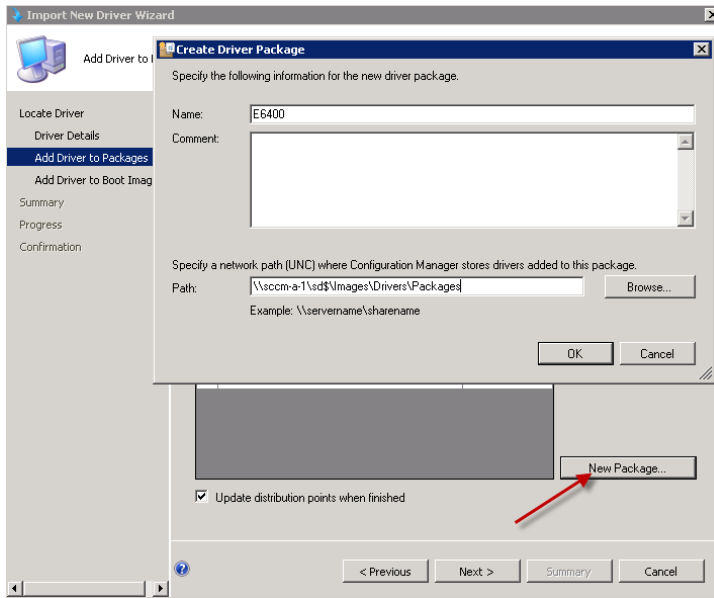
- 1 Right Click **Software Library, Operating Systems, Drivers**, Select **Import Driver**



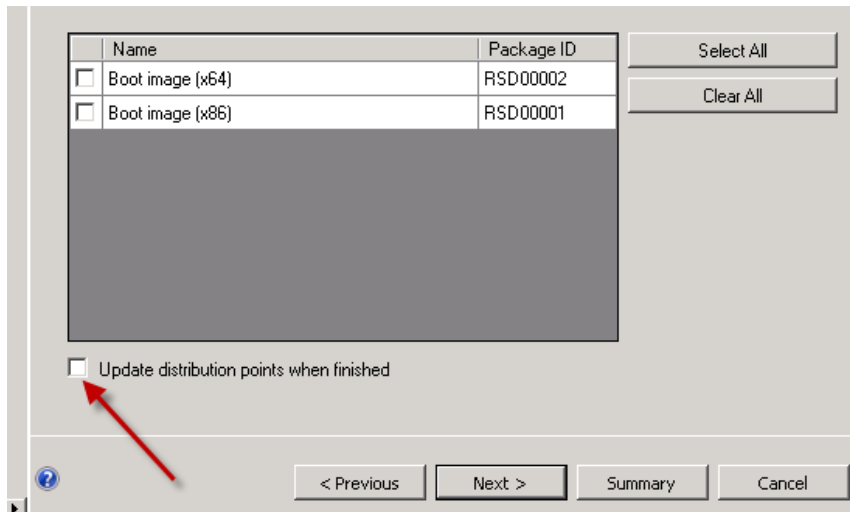
- 2 On the Driver location page, Browse to your drivers folder  
**\\<YOUR\_SCCM\_SERVER>\SD\$\Images\Drivers\E6400**, click Next.



- 3 On the Driver Detail Page, Click **Categories**, Click **Create** (if you need to add a new Category) and enter **Dell e6400**. Select the **Dell e6400** Category and Click **OK**.



- 4 On the Add Driver to Package Page, Click **New Package** (If you need to create a new package), Enter Name **E6400** and path  
**\\<YOUR\_SCCM\_SERVER>\SD\$\Images\Drivers\Packages\E6400**, Click **OK**. Make sure the **Update distribution points when finished** is Checked. Click **Next**.



5 On the Add Driver to Boot Image Page, make sure **NONE** of the Boot Image Packages are selected and the **Update distribution points when finished** are UNChecked. Click **Next** through the remain screens to finish the Wizard.

6 If these drivers are Network Card Drivers and are needed to be added to the Boot Image, you will be able to add them to the Boot Image Package manually. **\*\* We only want to put NEEDED drivers in the Boot Image Packages.**

14

## 7 Configuring Reporting Services

### 7.1 Install the Reporting Services Point Role

- 1 In the SCCM Console, click on **Administration, Site Configuration, and Servers and Site System Roles**.
- 2 Right-click the respective server and choose **Add Site System Roles**.
- 3 On the *General* screen, click **Next**.
- 4 Select **Reporting Services Point** and click **Next**.
- 5 On the Reporting Services Point screen, verify that the appropriate **server FQDN** is listed and click the **Verify** button.
- 6 Click the **Set > New Account** to assign the report user.
- 7 Use the **<YOUR\_DOMAIN>\MSSQLAdmin** account and click **OK**.
- 8 Click **OK** and complete the wizard.

### 7.2 Configure Reporting

- 1 Open Internet Explorer and browse to **http://<YOUR\_SCCM\_SERVER>.<YOUR\_DOMAIN>.local/Reports**
- 2 Select the **Properties** tab, and click on **New Role Assignment**.
- 3 Enter **<YOUR\_DOMAIN>\Administrator** (or AD Security Group) and assign desired permissions.
- 4 Click **OK**.



## 8 Backup and Restore SCCM Primary Site

This document is intended to provide the understanding of the general case backup requirements of SCCM, a sample backup strategy, and performing a restore of the site. Backing up the SCCM site process avoids loss of critical data ensuring that sites and hierarchies are restored with the least amount of data loss. Before the backup process is started on SCCM server, a few things should be kept in mind:

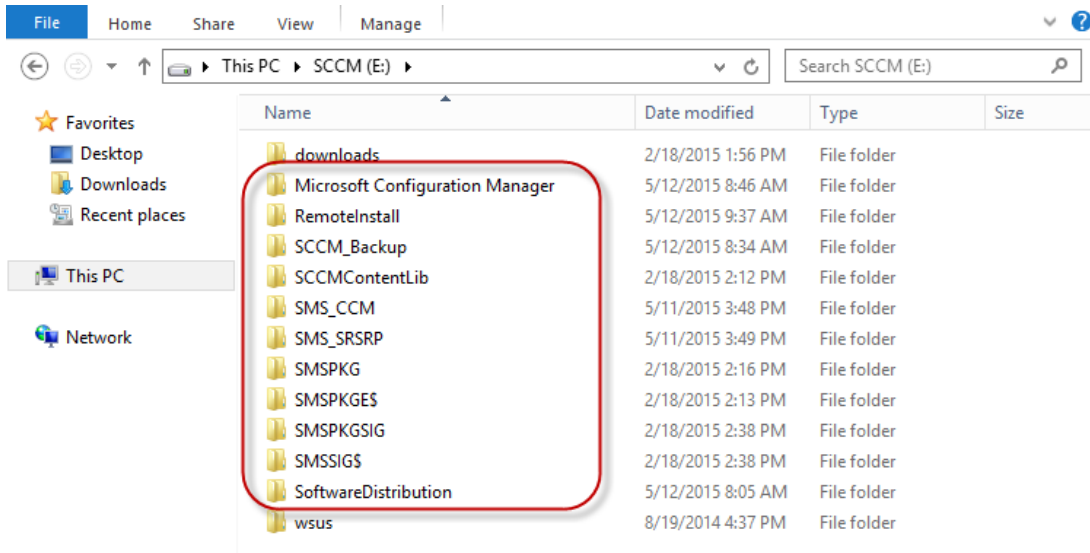
- SMS Writer service must be running for the process to complete successfully
- Backup schedule should be configured for an appropriate time that is outside active working hours to avoid any service disruptions.

The built-in Backup Site Server maintenance task performs backup of the following items:

- Configuration Manager Installation directory on site server
- NAL and SMS registry keys on the site server
- Master control file for the primary site
- Configuration Manager site database
- Information about the Content Library files

Some items are not saved automatically by the maintenance task and should be considered for inclusion in manual backup tasks. Items that are NOT backed up by the Backup Site Server maintenance automatically are:

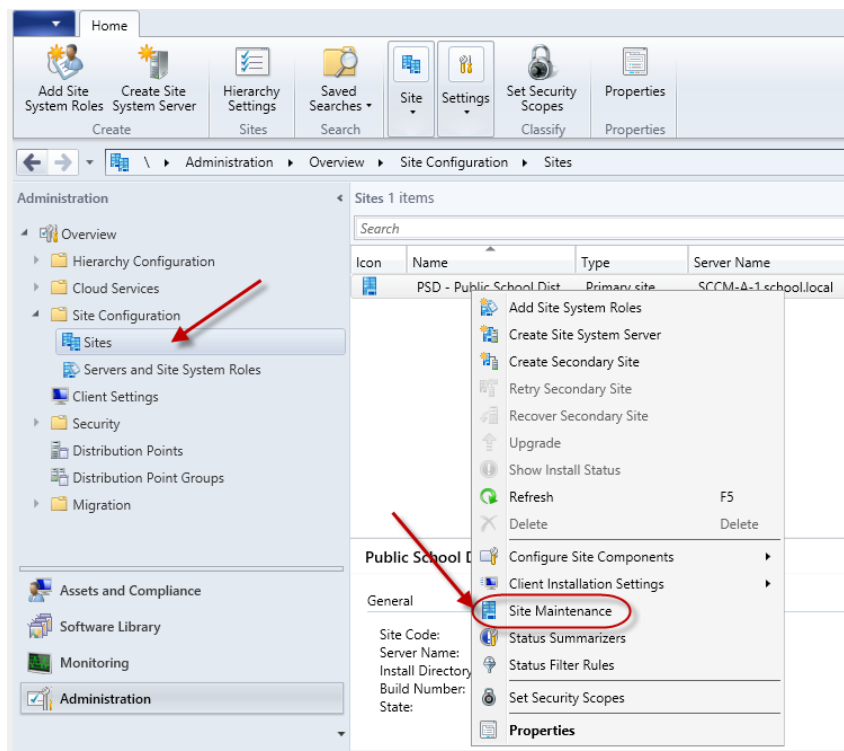
- Package, Software, and Driver source files
- User State Migration Data *(if applicable)*
- Any custom reports and extensions used to create them *(if applicable)*
- The content library stored in the <SMS-Drive:>\SCCMContentLib folder



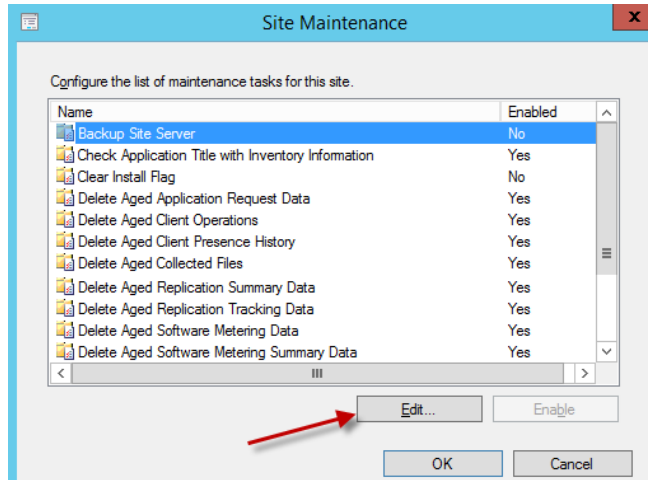
## 8.1 Backup SCCM Site Server

To configure the built-in Backup Site Server maintenance task, launch the SCCM management console. On the bottom left of the screen, select the **Administration** tab and expand **Overview**, if not already expanded. Expand **Site Configuration**, select **Sites** and on the right plane click on the name of the primary site\*\*. On the top toolbar click on **Site Maintenance**.

**\*\*Only backup of Central Administration Site OR Primary Site is supported. There is no backup support for Secondary Sites.**



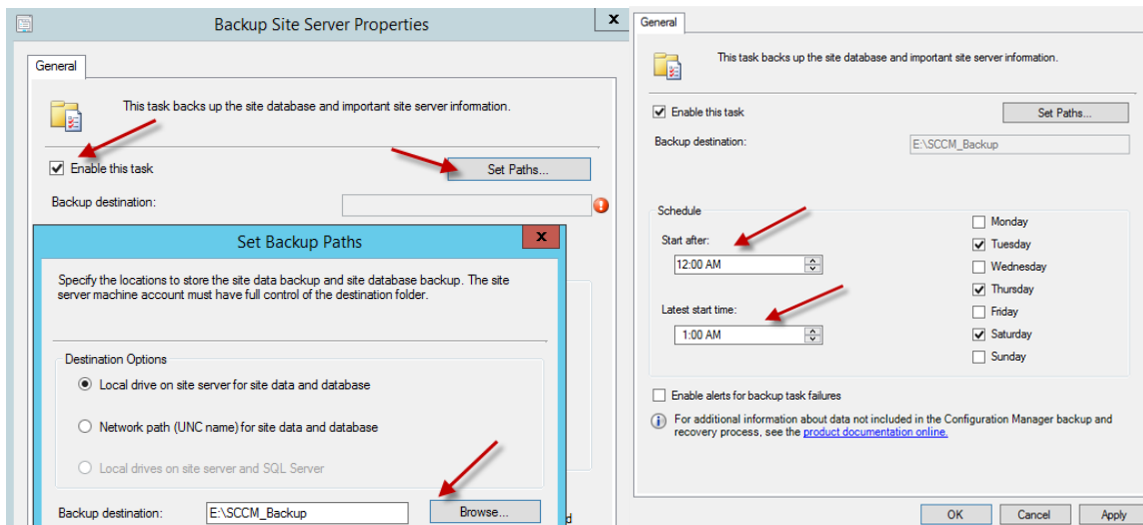
This should open the **Site Maintenance** window and a list of pre-defined tasks should be seen. Right click on the task **Backup Site Server** and select **Edit**.



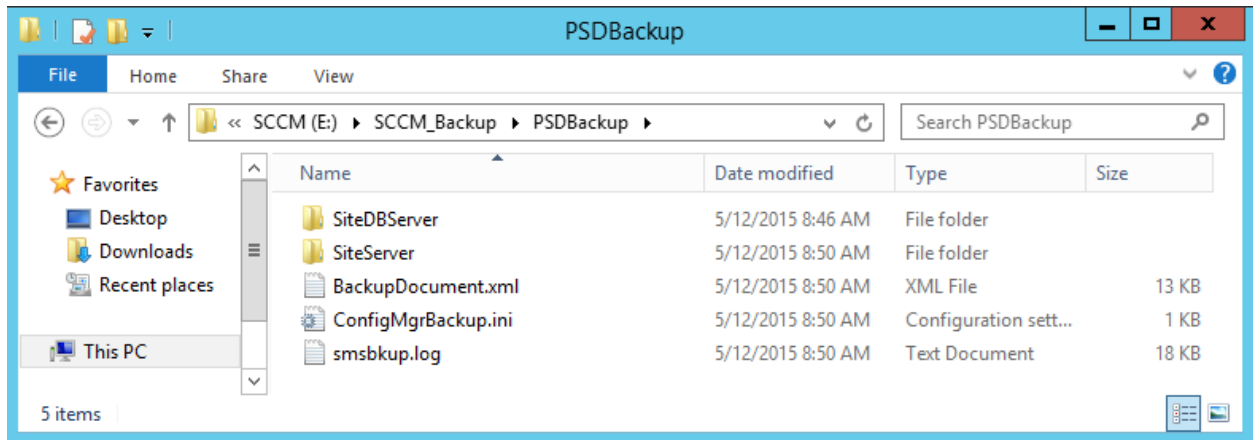
On the **Backup Site Server Properties** window, select **Enable this task**. After enabling the task click on **Set Paths\*** and browse to the location the backup files will be placed for the site server. Once the path is set, set the **Schedule** for the backup. Set the **Start after** and **Latest start time** as per your needs\*\*. Select **Enable alerts for backup task failures**. Click on **Apply** and **OK**.

*\* If you set the path to a network share, Server Object must have Full Control to the Network Share and Folder Security.*

*\*\*Recommended to schedule backups after hours. There is a minimum of 1 hour between Start and Latest Start.*



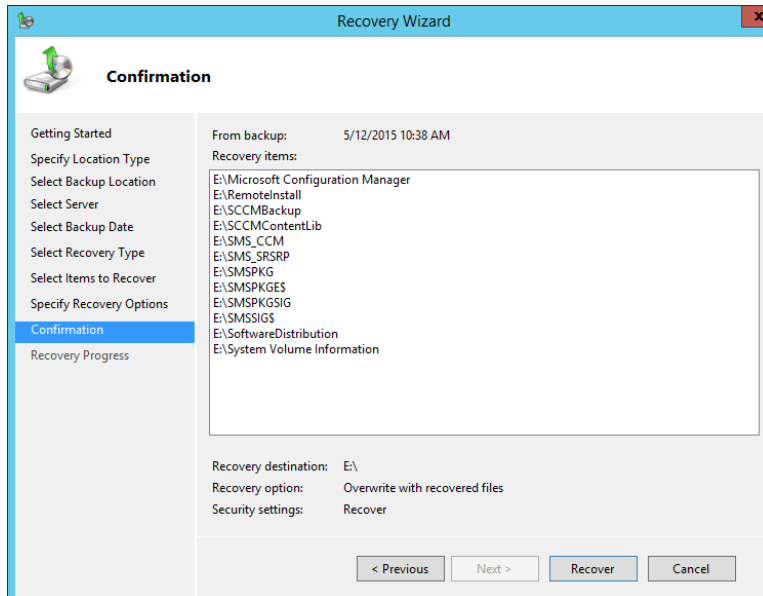
This process will enable Backup Site Server maintenance task and schedule to run with the configured settings. If you saved the SCCM Backup files to the local hard drive, make sure you back it up to another location. In the next section we will discuss how to restore the site server.



## 8.2 Restore SCCM Site Server

In Configuration Manager recovery from backup is part of the installation wizard. Before the recovery process is started make sure you have completed the following steps:

- Rebuilt the server with the same name, patched windows updates and joined to the domain
- Volume Drive letter and paths are consistent with the previous installation
- MS SQL Server instance is installed and running on the server (*if applicable*)
- Recover File system



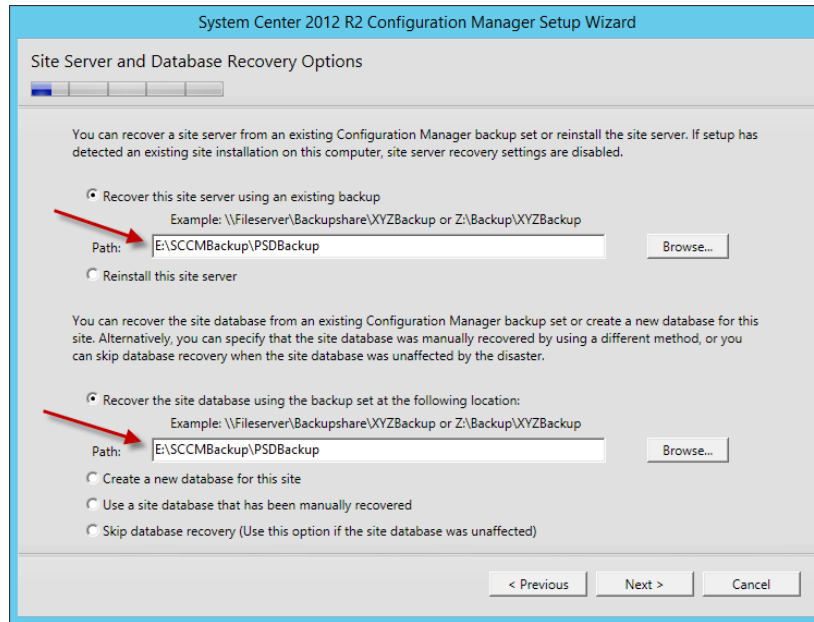
To start the recovery process, run the **setup** from System Center Configuration Manager installation media on the target server. Click on **Install** on the initial welcome screen.



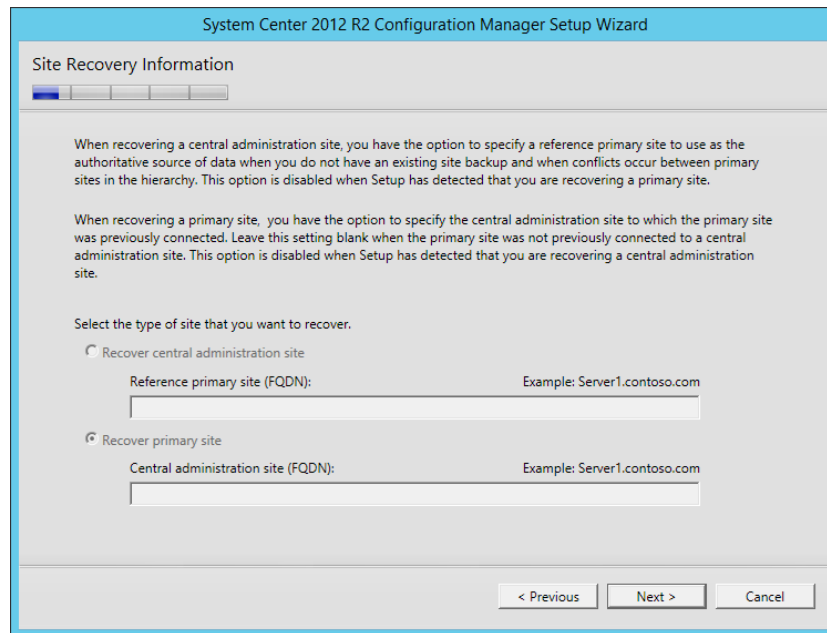
On the **Getting Started** screen select **Recover a site** to recover the primary site.



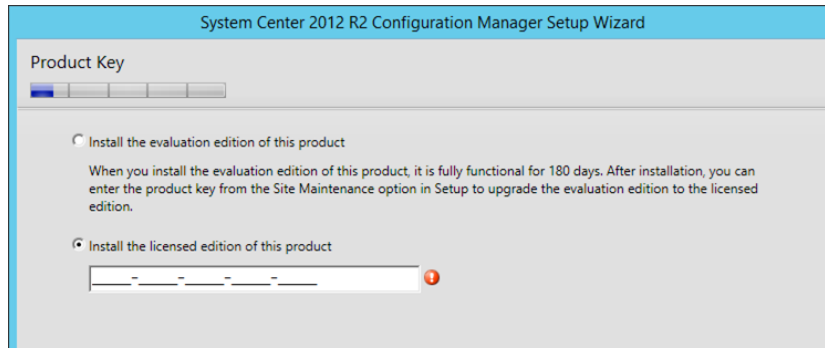
On the **Site Server and Database Recovery** screen browse to where the backup file location for both the Site Server backup and Site Database backup.



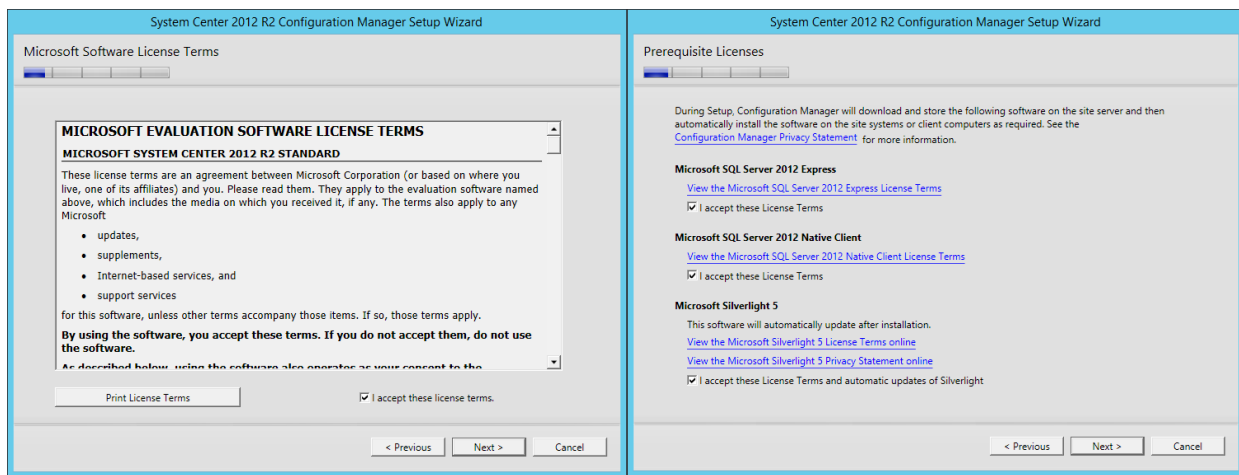
If the backup is valid, on the **Site Recovery Information** page the setup wizard will detect the primary site. Make sure that under **Recover Primary Site** option the Central Administration Site connection (CAS) field is blank if the primary site was not connected to any CAS previously



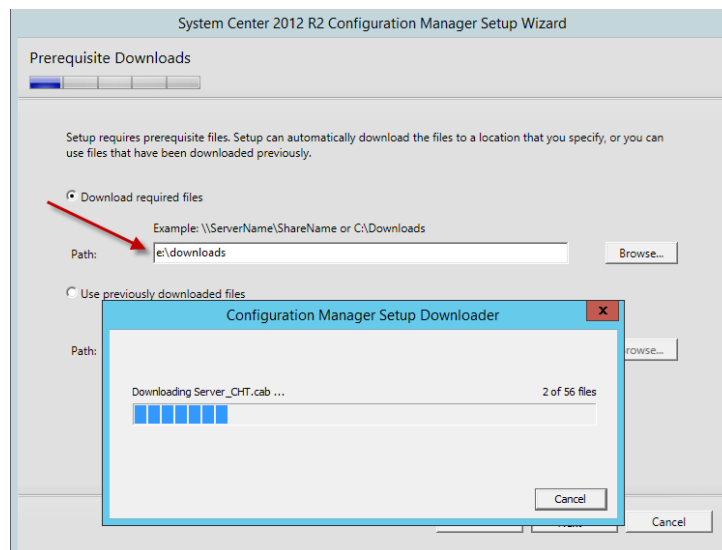
On the Product Key screen enter your SCCM Product License Key



On the next few screen Check “I accept these license terms” and click on **Next** until the **Prerequisites Download** screen.



On the **Prerequisite Downloads** screen select **Download Required Files** and browse to an empty folder e.g. Downloads on the SCCM volume, so that additional required files can be downloaded, and click **Next**





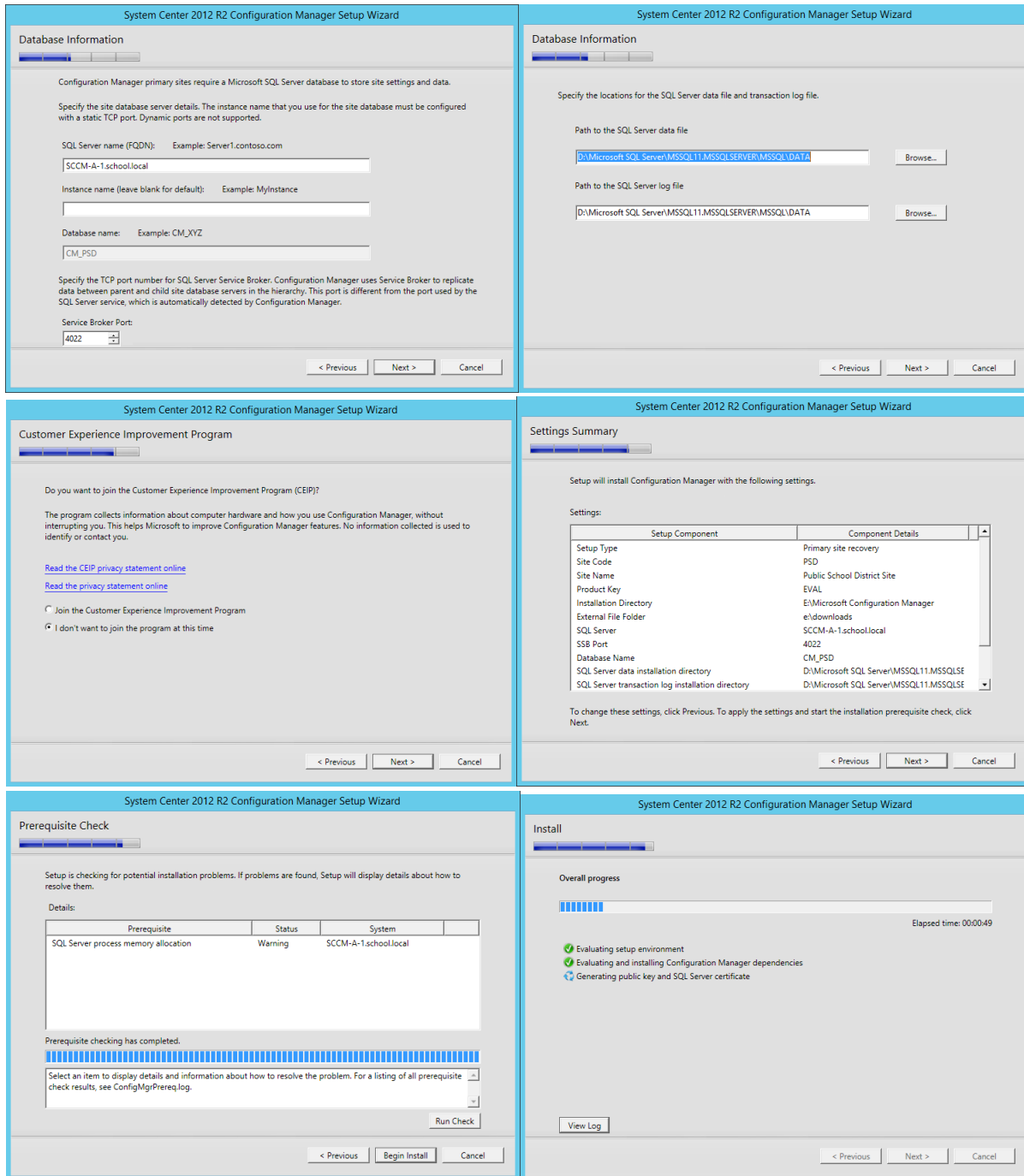
On the **Site and Installation Settings** screen notice that **Site code**, **Site name** information has already been filled from the backup files and cannot be edited. The **Installation Folder** can be edited and changed\*\*.

**\*\*It is recommended to use the identical volume drive letter and path that was used before**

The screenshot shows the 'System Center 2012 R2 Configuration Manager Setup Wizard' window, specifically the 'Site and Installation Settings' step. The window has a blue title bar and a progress indicator at the top. The main content area is light gray and contains the following elements:

- A progress bar with four steps, the first of which is highlighted in blue.
- Text: 'Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.'
- Text: 'Site code: PSD' (the text is inside a text box).
- Text: 'Specify a site name that helps to identify the site. Example: Contoso Headquarters Site'
- Text: 'Site name: Public School District Site' (the text is inside a text box).
- Note: 'Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.'
- Text: 'Installation folder: E:\Microsoft Configuration Manager' (the text is inside a text box). A red arrow points to this text box.
- Text: 'Browse...' (a button next to the installation folder text box).
- Text: 'Specify whether to install the Configuration Manager console to manage the Configuration Manager site from this computer. You can remotely manage the site when you do not install the Configuration Manager console.'
- Text: 'Install the Configuration Manager console' (a checkbox that is checked).
- Navigation buttons: '< Previous', 'Next >', and 'Cancel'.

On the **Database Information** screen everything should be left as default and click **Next**. On the **Prerequisites Check** screen click on **Run Check** to make sure all prerequisites pass and there are no errors. Click on **Begin Install** if the prerequisites check passed without errors.



Once the installation is done you will get the **Finished** screen. There will be a list of **Post-recovery actions** that will need to be addressed.

