Department of Information Systems
Arkansas. A State of Technology.

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

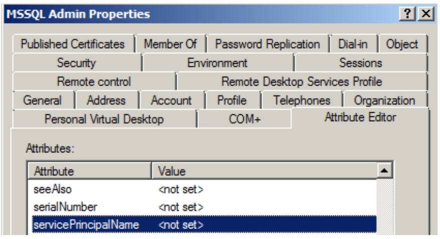
1 Open **Active Directory Users and Computers**

2 Click on **View** on the menu bar

3 Click **Advanced Features**

4 Find the **<YOUR_DOMAIN>\MSSQL Admin** user

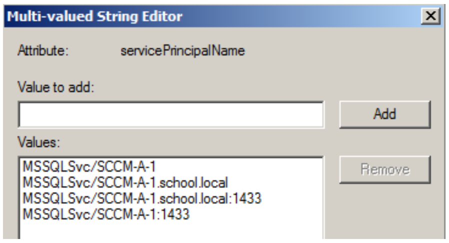
5 **Right Click** and Click **Properties**



Attributes:

Attribute	Value
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	<not set>

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



Attribute: servicePrincipalName

Value to add:

Values:

MSSQLSvc/SCCM-A-1
MSSQLSvc/SCCM-A-1.school.local
MSSQLSvc/SCCM-A-1.school.local:1433
MSSQLSvc/SCCM-A-1:1433

- **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**

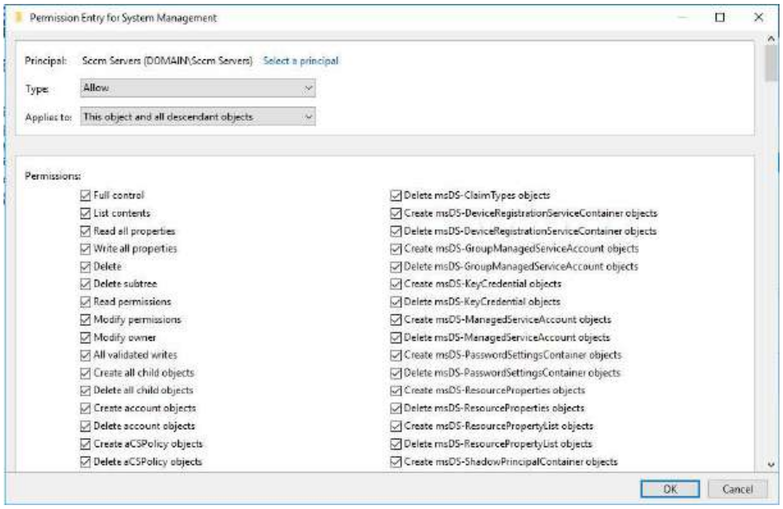
3 Right Click **System** and Select **New** -> **Object-> Container.** Click Next

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**.



Permission Entry for System Management

Principal: Sccm Servers (DOMAIN\Sccm Servers) Select a principal

Type: Allow

Applies to: This object and all descendant objects

Permissions:

☑ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☑ Delete
☑ Delete subtree
☑ Read permissions
☑ Modify permissions
☑ Modify owner
☑ All validated writes
☑ Create all child objects
☑ Delete all child objects
☑ Create account objects
☑ Delete account objects
☑ Create aCSPolicy objects
☑ Delete aCSPolicy objects
☑ Delete msDS-ClaimTypes objects
☑ Create msDS-DeviceRegistrationServiceContainer objects
☑ Delete msDS-DeviceRegistrationServiceContainer objects
☑ Create msDS-GroupManagedServiceAccount objects
☑ Delete msDS-GroupManagedServiceAccount objects
☑ Create msDS-KeyCredential objects
☑ Delete msDS-KeyCredential objects
☑ Create msDS-ManagedServiceAccount objects
☑ Delete msDS-ManagedServiceAccount objects
☑ Create msDS-PasswordSettingsContainer objects
☑ Delete msDS-PasswordSettingsContainer objects
☑ Create msDS-ResourceProperties objects
☑ Delete msDS-ResourceProperties objects
☑ Create msDS-ResourcePropertyList objects
☑ Delete msDS-ResourcePropertyList objects
☑ Create msDS-ShadowPrincipalContainer objects

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)

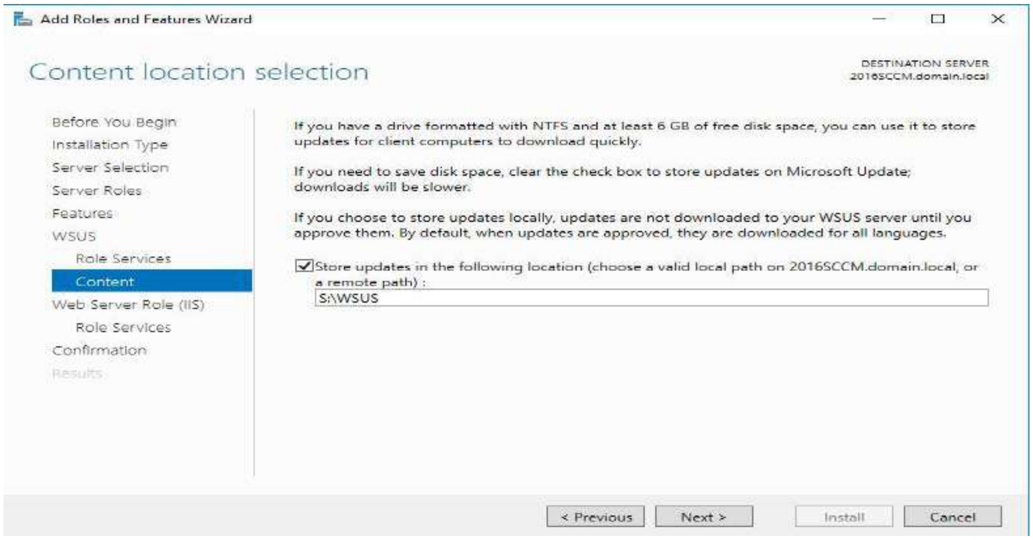
C. Select **Remote Differential Compression**

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**



Content location selection

DESTINATION SERVER
2016SCCM.domain.local

If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

☑ Store updates in the following location (choose a valid local path on 2016SCCM.domain.local, or a remote path) :

S:\WSUS

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**

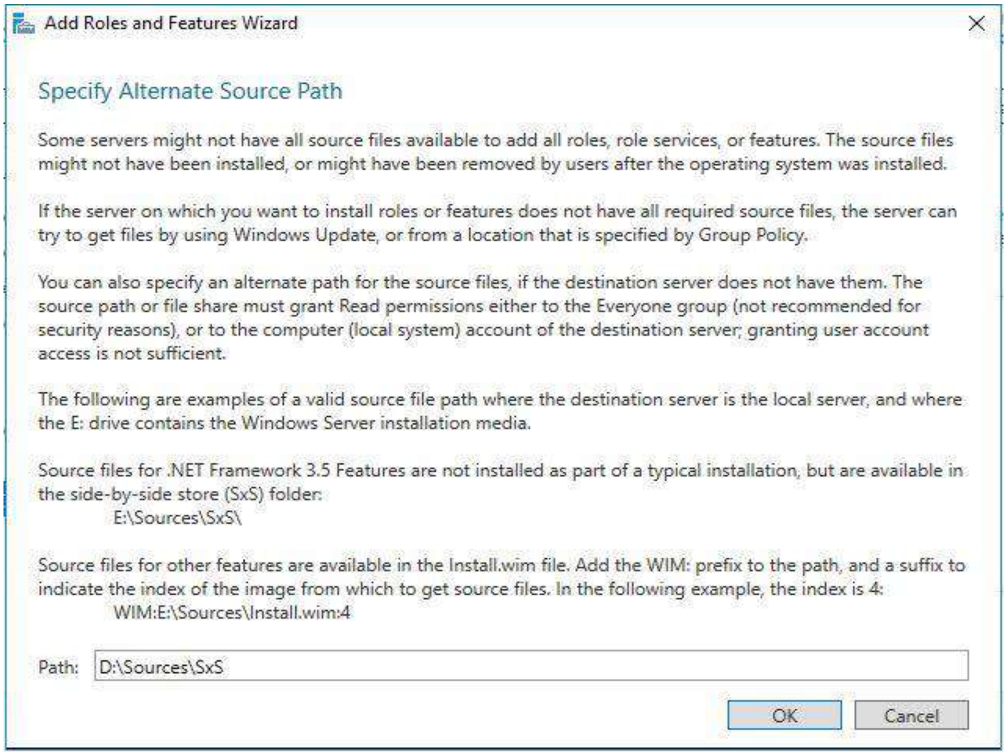
D. Under **Management Tools** select:

- **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**



Specify Alternate Source Path

Some servers might not have all source files available to add all roles, role services, or features. The source files might not have been installed, or might have been removed by users after the operating system was installed.

If the server on which you want to install roles or features does not have all required source files, the server can try to get files by using Windows Update, or from a location that is specified by Group Policy.

You can also specify an alternate path for the source files, if the destination server does not have them. The source path or file share must grant Read permissions either to the Everyone group (not recommended for security reasons), or to the computer (local system) account of the destination server; granting user account access is not sufficient.

The following are examples of a valid source file path where the destination server is the local server, and where the E: drive contains the Windows Server installation media.

Source files for .NET Framework 3.5 Features are not installed as part of a typical installation, but are available in the side-by-side store (SxS) folder:
E:\Sources\SxS\

Source files for other features are available in the Install.wim file. Add the WIM: prefix to the path, and a suffix to indicate the index of the image from which to get source files. In the following example, the index is 4:
WIM:E:\Sources\Install.wim:4

Path: D:\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.

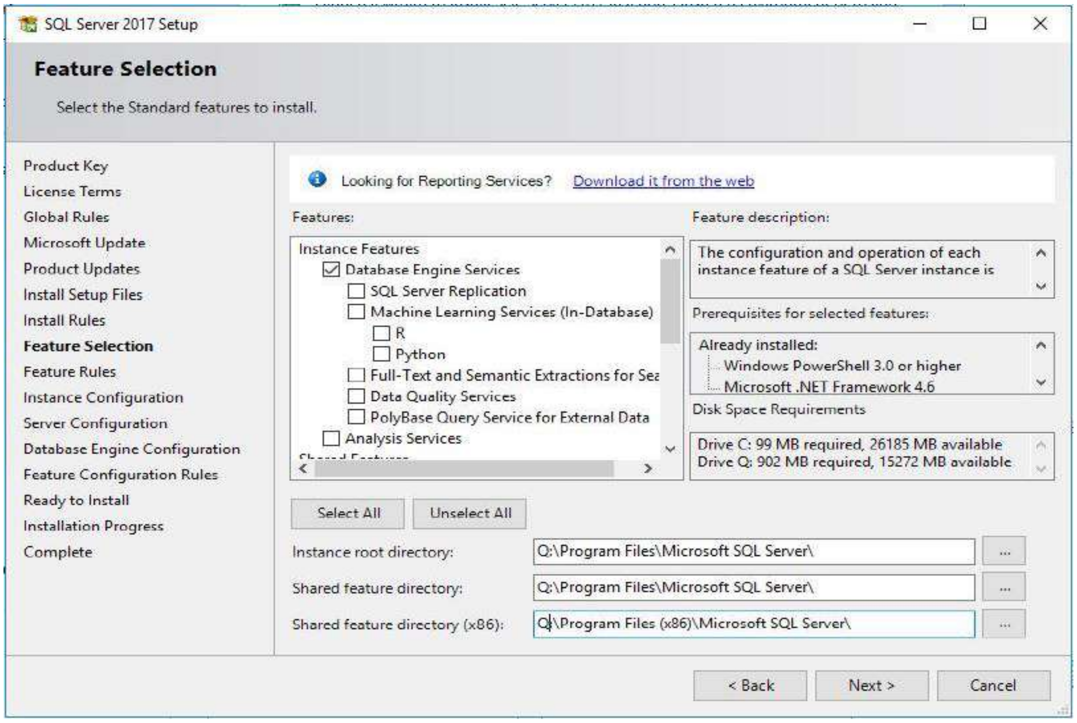
10 On the **Feature Selection** page, select the following:

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.**



SQL Server 2017 Setup

Feature Selection

Select the Standard features to install.

Looking for Reporting Services? Download it from the web

Features:

Instance Features
☑ Database Engine Services
□ SQL Server Replication
□ Machine Learning Services (In-Database)
□ R
□ Python
□ Full-Text and Semantic Extractions for Sea
□ Data Quality Services
□ PolyBase Query Service for External Data
□ Analysis Services

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is

Prerequisites for selected features:

Already installed:
Windows PowerShell 3.0 or higher
Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 99 MB required, 26185 MB available
Drive Q: 902 MB required, 15272 MB available

Instance root directory: Q:\Program Files\Microsoft SQL Server\

Shared feature directory: Q:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): Q:\Program Files (x86)\Microsoft SQL Server\

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**

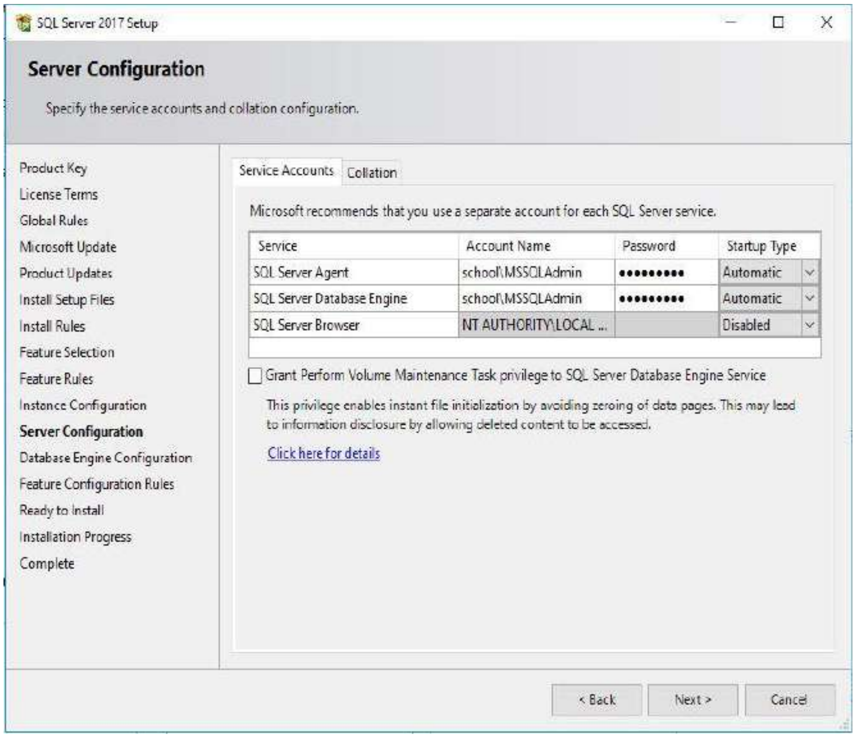
   i. **Account Name – <YOUR_DOMAIN>\MSSQL.Admin**

   ii. Enter the **Password**

   iii. **Startup Type - Automatic**

C. **SQL Server Browser**

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



Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

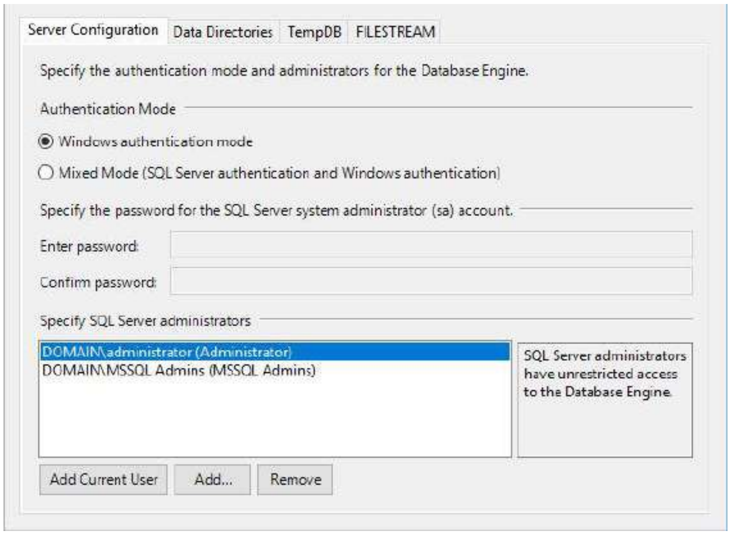
Service	Account Name	Password	Startup Type
SQL Server Agent	school\MSSQLAdmin	•••••••••	Automatic
SQL Server Database Engine	school\MSSQLAdmin	•••••••••	Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

□ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

Click here for details

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



Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

● Windows authentication mode

○ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

Specify SQL Server administrators

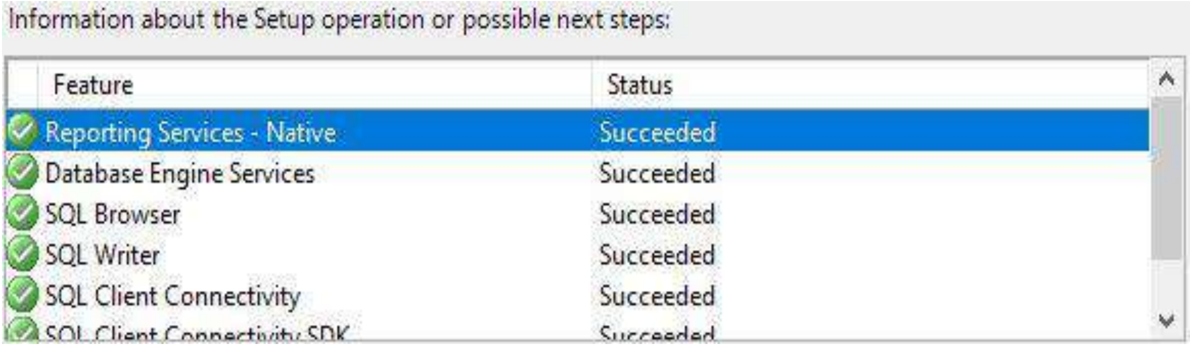
DOMAIN\administrator (Administrator)
DOMAIN\MSSQL Admins (MSSQL Admins)

SQL Server administrators have unrestricted access to the Database Engine.

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:

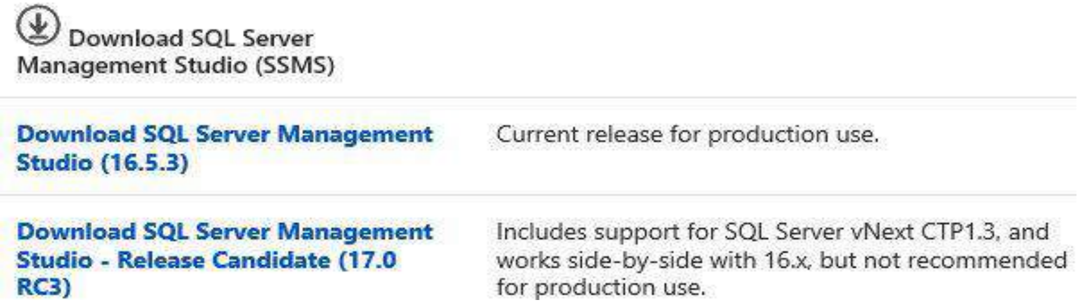
Feature	Status
✓ Reporting Services - Native	Succeeded
✓ Database Engine Services	Succeeded
✓ SQL Browser	Succeeded
✓ SQL Writer	Succeeded
✓ SQL Client Connectivity	Succeeded
✓ SQL Client Connectivity SDK	Succeeded

<u>NOTE: The next 7 steps are for those using SQL 2016 and above ONLY</u>

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.**

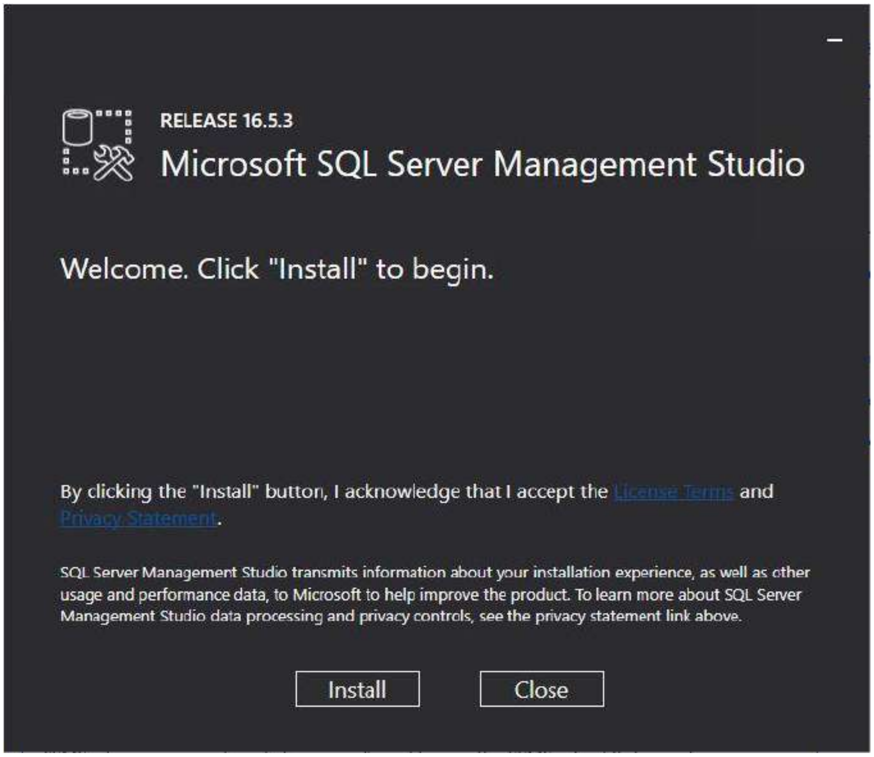


Download SQL Server Management Studio (SSMS)

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.



RELEASE 16.5.3

Microsoft SQL Server Management Studio

Welcome. Click "Install" to begin.

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

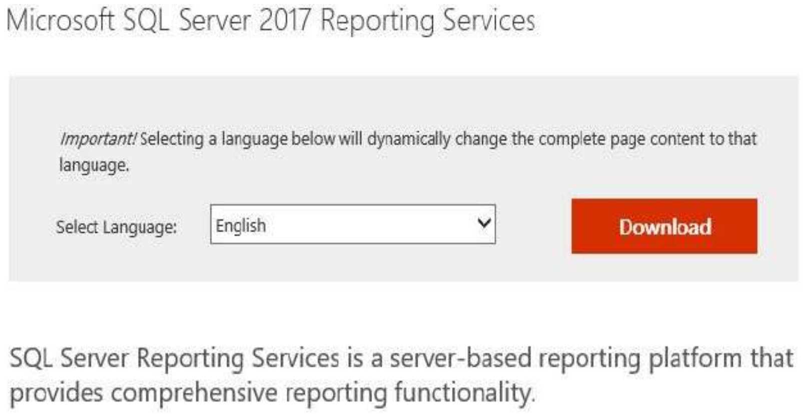
SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server Management Studio data processing and privacy controls, see the privacy statement link above.

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.**



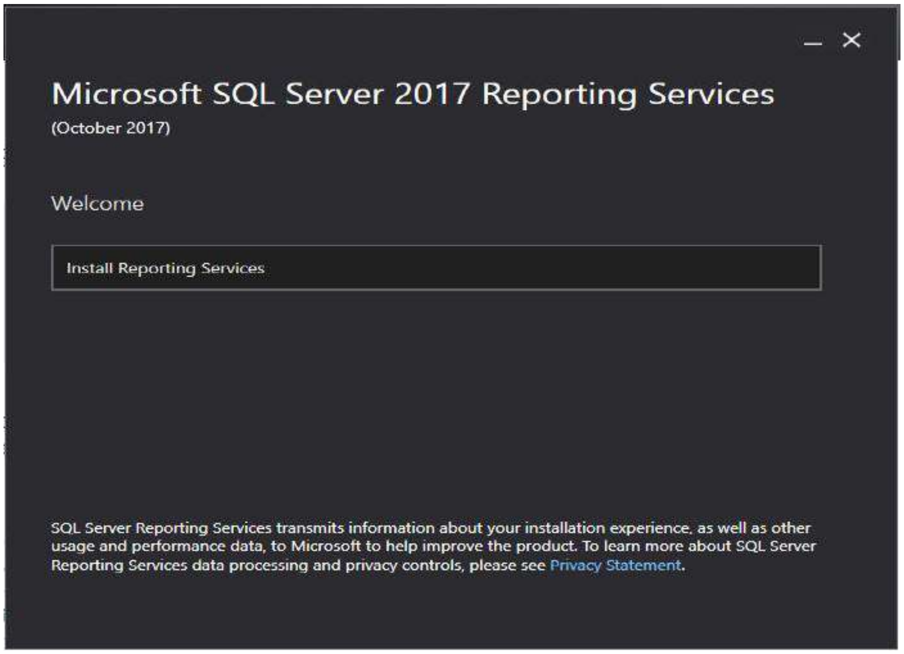
Microsoft SQL Server 2017 Reporting Services

Important! Selecting a language below will dynamically change the complete page content to that language.

Select Language: English

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

27 Select **Install Reporting Services.**



Microsoft SQL Server 2017 Reporting Services

(October 2017)

Welcome

SQL Server Reporting Services transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server Reporting Services data processing and privacy controls, please see Privacy Statement.

28 **Enter the product key,** and click **Next.**

29 Check box to **Accept license terms,** and click **Next.**

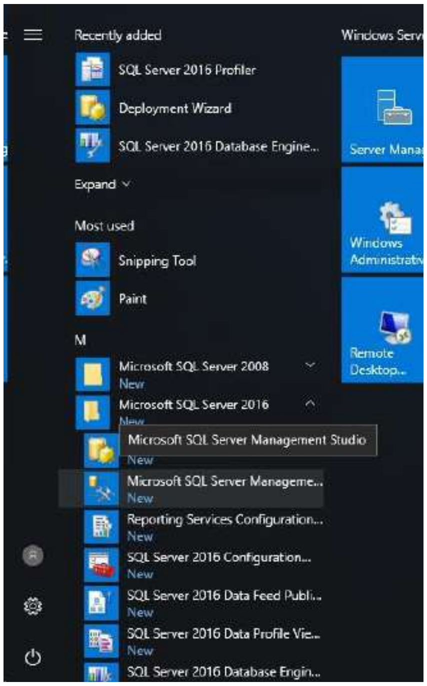
30 On the Install location, click **Install.**

31 After the install completes click **Close.**

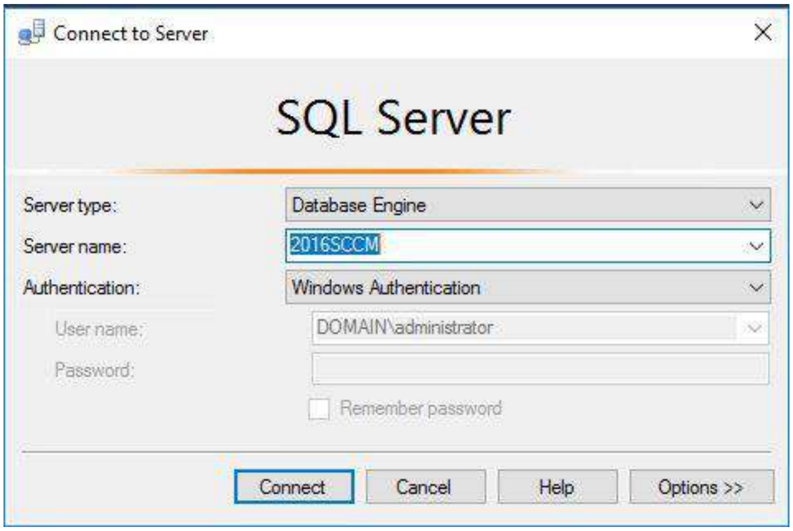
1.7 Set Microsoft SQL Server Memory Restrictions

* On **<YOUR_SCCM_SERVER>**

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


Recently added
SQL Server 2016 Profiler
Deployment Wizard
SQL Server 2016 Database Engine...
Expand
Most used
Snipping Tool
Paint
M
Microsoft SQL Server 2008
New
Microsoft SQL Server 2016
New
Microsoft SQL Server Management Studio
New
Microsoft SQL Server Manageme...
New
Reporting Services Configuration...
New
SQL Server 2016 Configuration...
New
SQL Server 2016 Data Feed Publi...
New
SQL Server 2016 Data Profile Vie...
New
SQL Server 2016 Database Engin...
Windows Serv
Server Mana
Windows Administrativ
Remote Desktop...

2 Click **Connect**



Server type: Database Engine

Server name: 2016SCCM

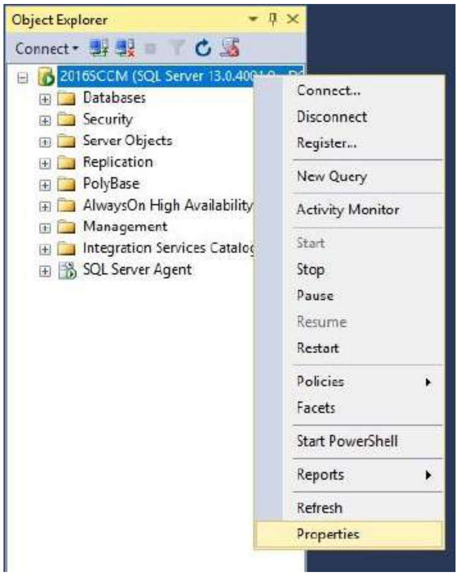
Authentication: Windows Authentication

User name: DOMAIN\administrator

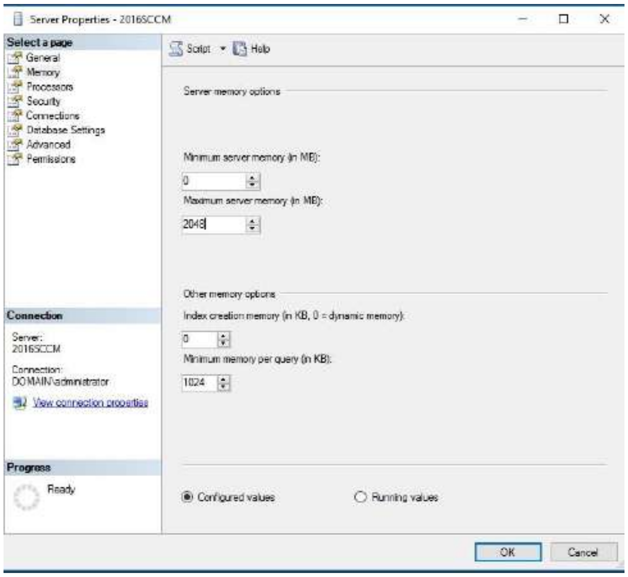
Password:

□ Remember password

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.



Server memory options

Minimum server memory (in MB): 0

Maximum server memory (in MB): 2048

Other memory options

Index creation memory (in KB, 0 = dynamic memory): 0

Minimum memory per query (in KB): 1024

● Configured values ○ Running values

Server: 2016SCCM

Connection: DOMAIN\administrator

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

1.8 Install Microsoft Administration Deployment Kit

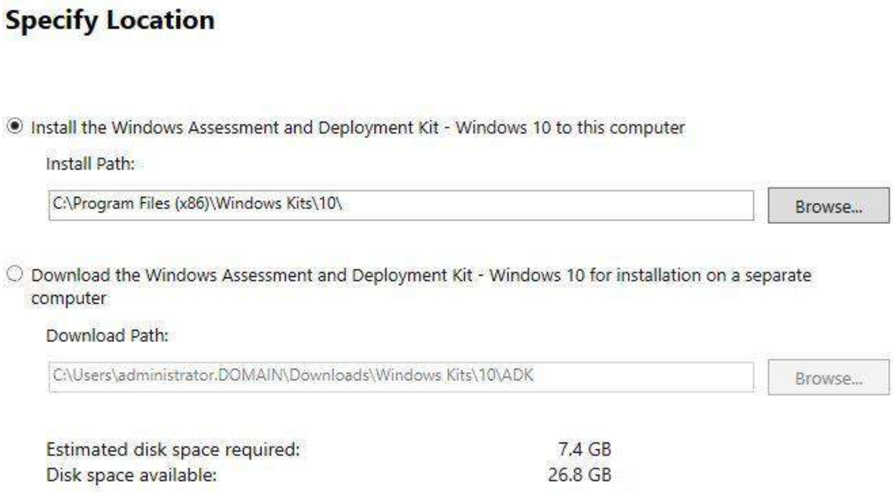
*On **<YOUR_SCCM_SERVER>** – At the time of creation of this guide, **WADK 2004** was the latest version released. **WADK 2004** has been tested and verified for use in a production environment by ASPCN LAN. This guide will use **WADK 2004** for this reason.

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:

C:\Program Files (x86)\Windows Kits\10\

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

Download Path:

C:\Users\administrator.DOMAIN\Downloads\Windows Kits\10\ADK

Estimated disk space required: 7.4 GB

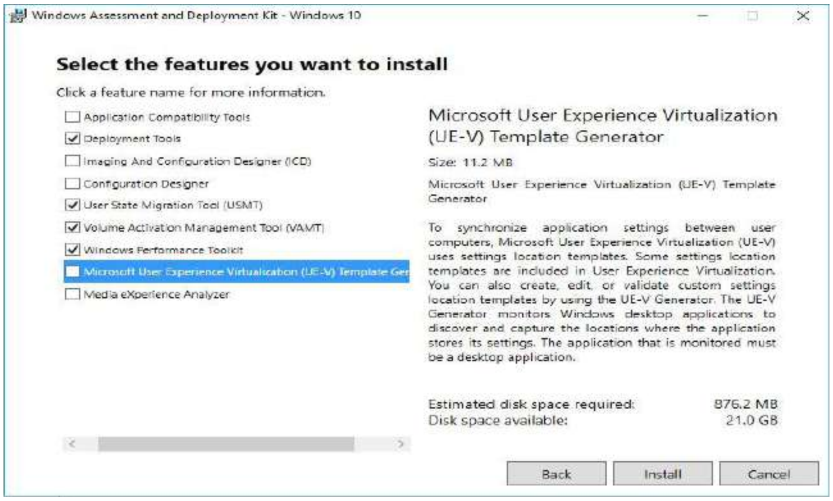
Disk space available: 26.8 GB

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**



Select the features you want to install

Click a feature name for more information.

☐ Application Compatibility Tools
☑ Deployment Tools
☐ Imaging And Configuration Designer (ICD)
☐ Configuration Designer
☑ User State Migration Tool (USMT)
☑ Volume Activation Management Tool (VAMT)
☑ Windows Performance Toolkit
☐ Microsoft User Experience Virtualization (UE-V) Template Ger
☐ Media eXperience Analyzer

Microsoft User Experience Virtualization (UE-V) Template Generator

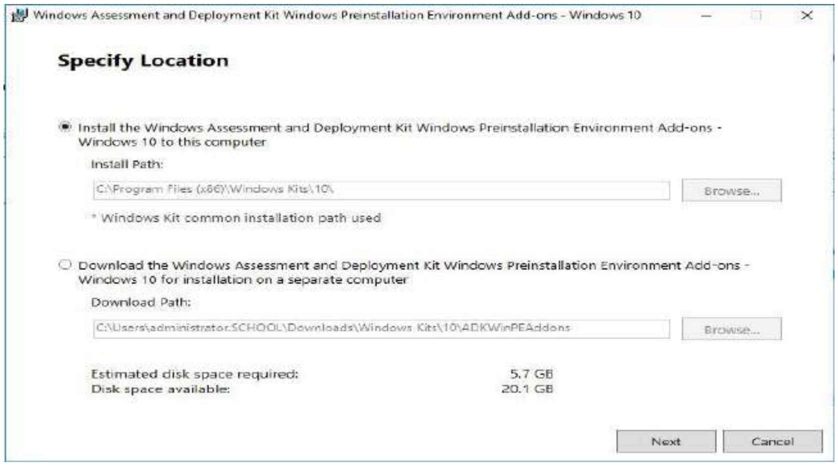
Size: 11.2 MB

Microsoft User Experience Virtualization (UE-V) Template Generator

To synchronize application settings between user computers, Microsoft User Experience Virtualization (UE-V) uses settings location templates. Some settings location templates are included in User Experience Virtualization. You can also create, edit, or validate custom settings location templates by using the UE-V Generator. The UE-V Generator monitors Windows desktop applications to discover and capture the locations where the application stores its settings. The application that is monitored must be a desktop application.

Estimated disk space required: 876.2 MB
Disk space available: 21.0 GB

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


Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10
Browse...
Browse...
Next
Cancel

Specify Location

● Install the Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10 to this computer

Install Path:

C:\Program Files (x86)\Windows Kits\10\

* Windows Kit common installation path used

○ Download the Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10 for installation on a separate computer

Download Path:

C:\Users\administrator.SCHOOL\Downloads\Windows Kits\10\ADKWinPEAddons

Estimated disk space required: 5.7 GB
Disk space available: 20.1 GB

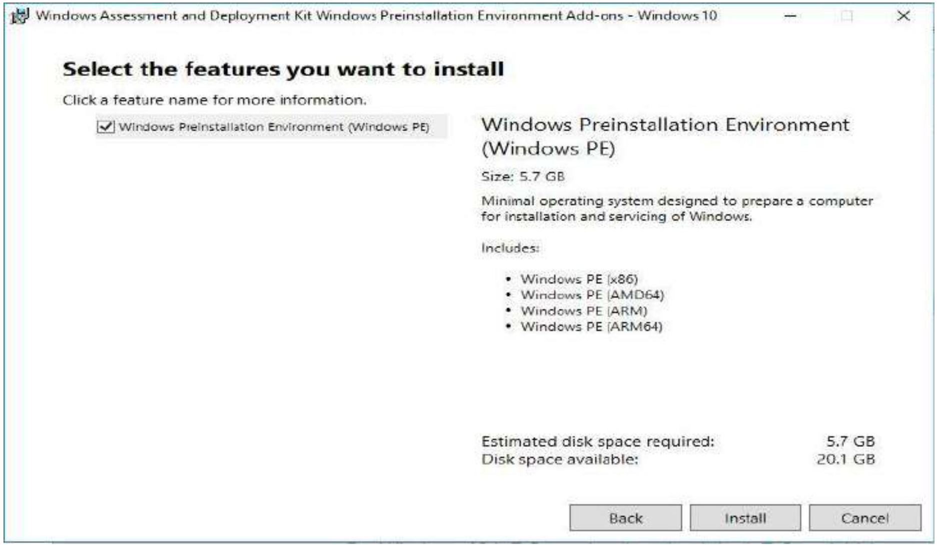
7 Run the **adkwinpesetup.exe** when the file is downloaded from the **PE** folder. In the **Install Path** box, leave the default location selected, and then click **Next**.

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.



Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10

Select the features you want to install

Click a feature name for more information.

☑ Windows Preinstallation Environment (Windows PE)

Windows Preinstallation Environment (Windows PE)

Size: 5.7 GB

Minimal operating system designed to prepare a computer for installation and servicing of Windows.

Includes:

- Windows PE (x86)
- Windows PE (AMD64)
- Windows PE (ARM)
- Windows PE (ARM64)

Estimated disk space required:	5.7 GB
Disk space available:	20.1 GB

2 Install SCCM

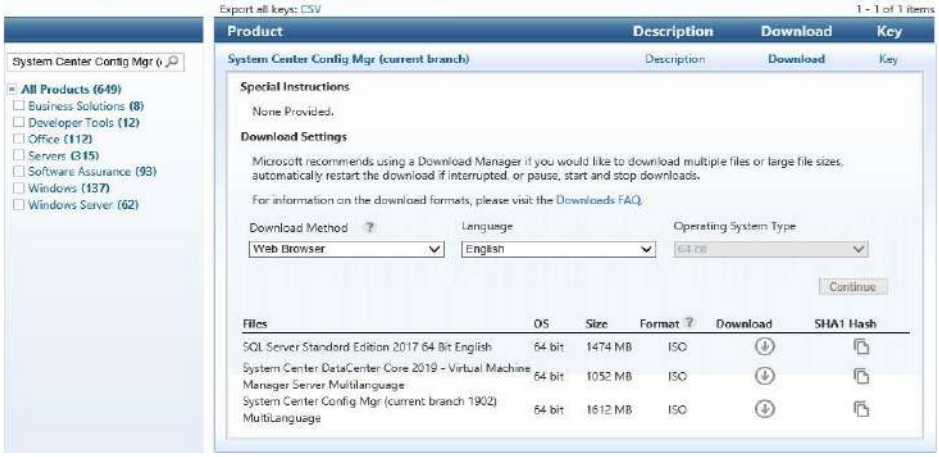
2.1 Create a Downloads folder in root of the S: Drive.

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.



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

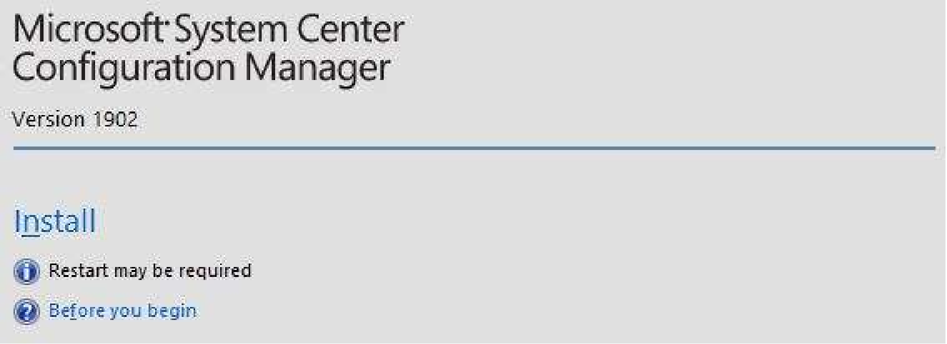
Operating System Type: 64 bit

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

- Select the highest version available to you. At the time if 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.



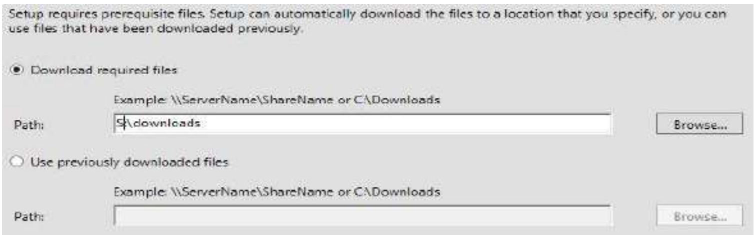
4. On the Before You Begin screen, click **Next**.

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: S:\downloads

○ Use previously downloaded files

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

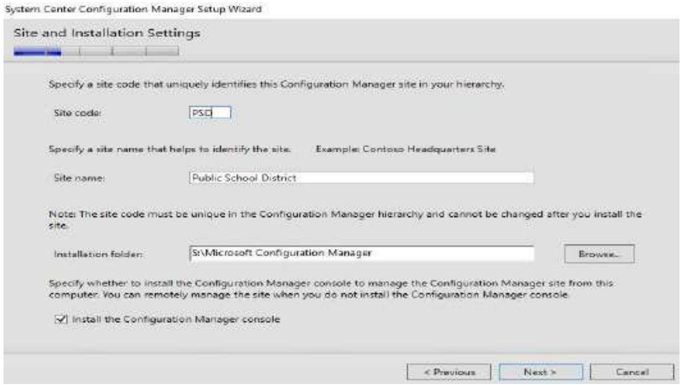
Path:

9. On the Server Language *Selection* screen, click **Next**.

10. On the Client Language *Selection* screen, click **Next**.

11. One 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: PSD

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

Site name: Public School District

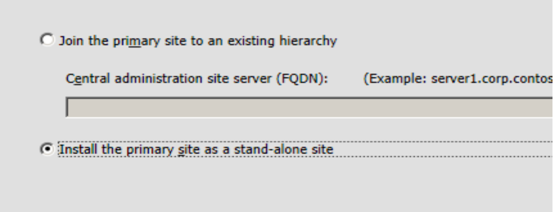
Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.

Installation folder: S:\Microsoft Configuration Manager

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

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.contos

● Install the primary site as a stand-alone site

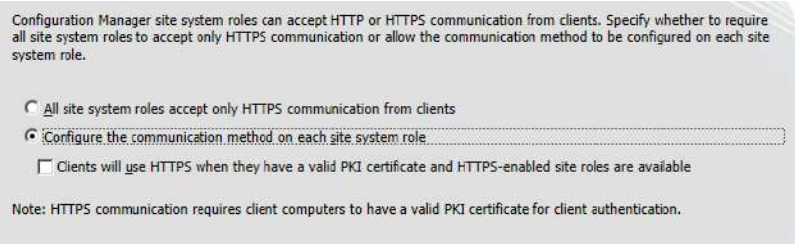
13. Click **Yes** to the Pop-up.

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 **<u>unchecked</u>**, and click **Next**.



Configuration Manager site system roles can accept HTTP or HTTPS communication from clients. Specify whether to require all site system roles to accept only HTTPS communication or allow the communication method to be configured on each site system role.

○ All site system roles accept only HTTPS communication from clients

● Configure the communication method on each site system role

□ Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available

Note: HTTPS communication requires client computers to have a valid PKI certificate for client authentication.

*****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**.

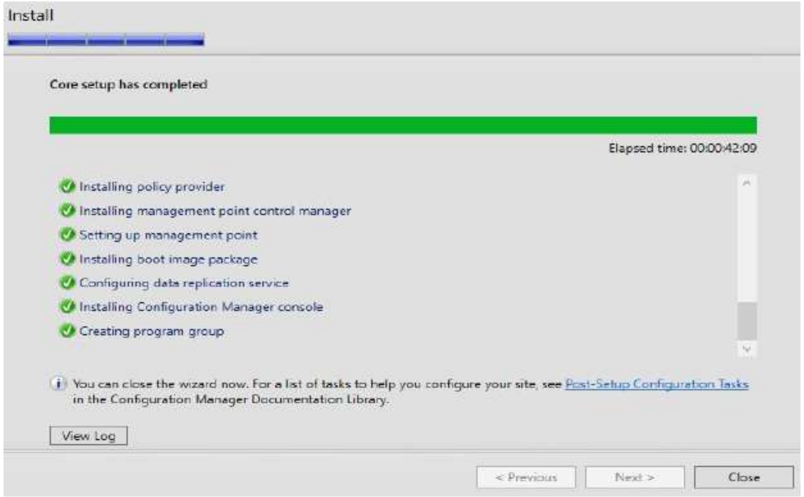
19. On the Diagnostic and Usage Data screen, click **Next.**

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 **<u>errors</u>** and click **Begin Install**.

23. Click **Close** when the installation finishes.



Install

Core setup has completed

Elapsed time: 00:00:42:09

✓ Installing policy provider
✓ Installing management point control manager
✓ Setting up management point
✓ Installing boot image package
✓ Configuring data replication service
✓ Installing Configuration Manager console
✓ Creating program group

You can close the wizard now. For a list of tasks to help you configure your site, see Post-Setup Configuration Tasks in the Configuration Manager Documentation Library.

3 Configure SCCM

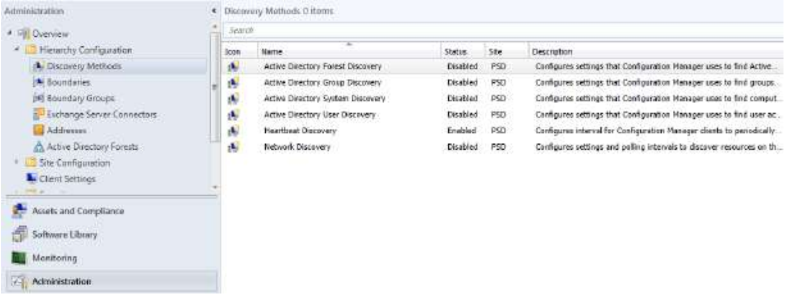
3.1 Configure Discovery Methods

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**.

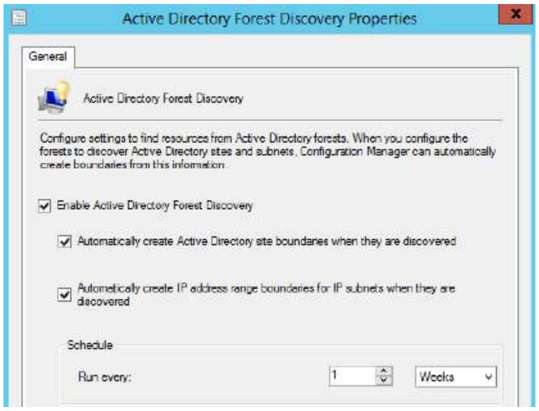


Discovery Methods 0 items

Icon	Name	Status	Site	Description
	Active Directory Forest Discovery	Disabled	PSD	Configures settings that Configuration Manager uses to find Active...
	Active Directory Group Discovery	Disabled	PSD	Configures settings that Configuration Manager uses to find groups...
	Active Directory System Discovery	Disabled	PSD	Configures settings that Configuration Manager uses to find comput...
	Active Directory User Discovery	Disabled	PSD	Configures settings that Configuration Manager uses to find user ac...
	Heartbeat Discovery	Enabled	PSD	Configures interval for Configuration Manager clients to periodically...
	Network Discovery	Disabled	PSD	Configures settings and polling intervals to discover resources on th...

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

6 **Enable Active Directory Forest Discovery**.


Active Directory Forest Discovery Properties
General
Active Directory Forest Discovery
Schedule

Configure settings to find resources from Active Directory forests. When you configure the forests to discover Active Directory sites and subnets, Configuration Manager can automatically create boundaries from this information.

☑ Enable Active Directory Forest Discovery

☑ Automatically create Active Directory site boundaries when they are discovered

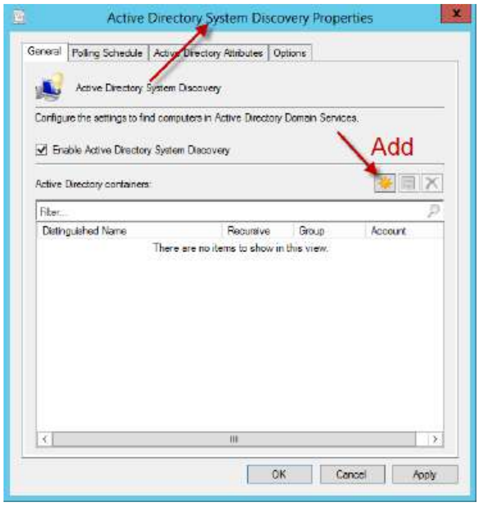
☑ Automatically create IP address range boundaries for IP subnets when they are discovered

Run every: 1 Weeks

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**.


Active Directory System Discovery Properties
General
Polling Schedule
Active Directory Attributes
Options
Add
OK
Cancel
Apply

Active Directory System Discovery

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

☑ Enable Active Directory System Discovery

Active Directory containers:

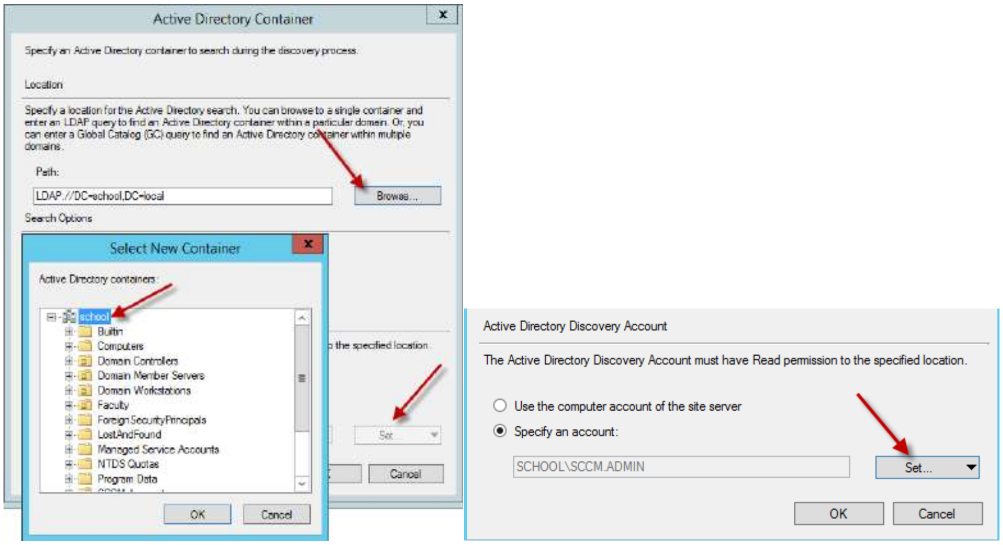
Filter...

Distinguished Name	Recursive	Group	Account

There are no items to show in this view.

10 **Enable Active Directory System Discovery**.

11 Click **Add.** Select **Browse** and Select **<YOUR_DOMAIN>** and Click **OK**



Specify an Active Directory container to search during the discovery process.

Location

Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.

Path: LDAP://DC=school,DC=local

Active Directory containers:

Active Directory Discovery Account

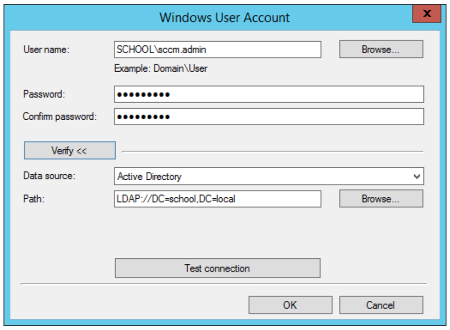
The Active Directory Discovery Account must have Read permission to the specified location.

○ Use the computer account of the site server

● Specify an account:

SCHOOL\SCCM.ADMIN

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**.



User name: SCHOOL\sccm.admin

Example: Domain\User

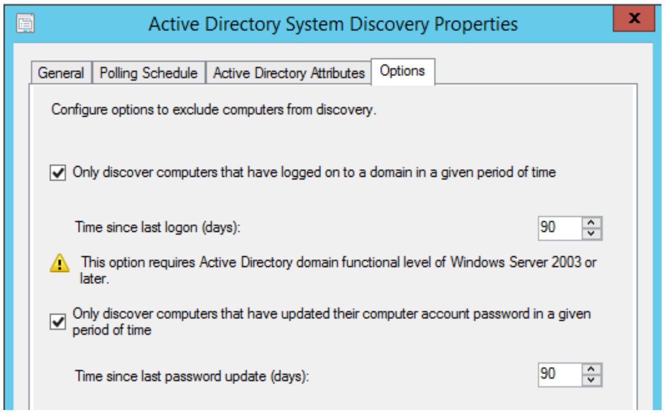
Password: •••••••••

Confirm password: •••••••••

Data source: Active Directory

Path: LDAP://DC=school,DC=local

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**"


Active Directory System Discovery Properties
General
Polling Schedule
Active Directory Attributes
Options

Configure options to exclude computers from discovery.

☑ Only discover computers that have logged on to a domain in a given period of time

Time since last logon (days): 90

This option requires Active Directory domain functional level of Windows Server 2003 or later.

☑ Only discover computers that have updated their computer account password in a given period of time

Time since last password update (days): 90

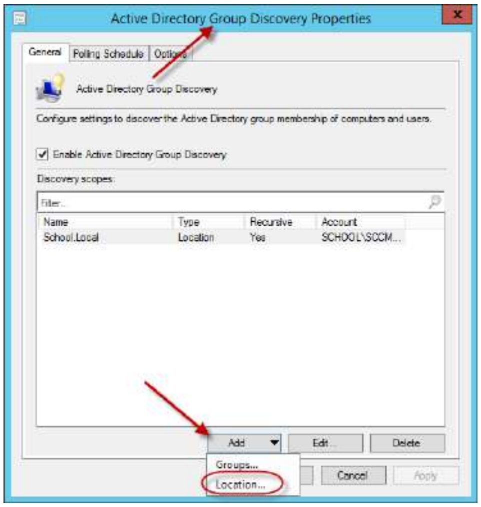
14 Click **Apply**

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**.



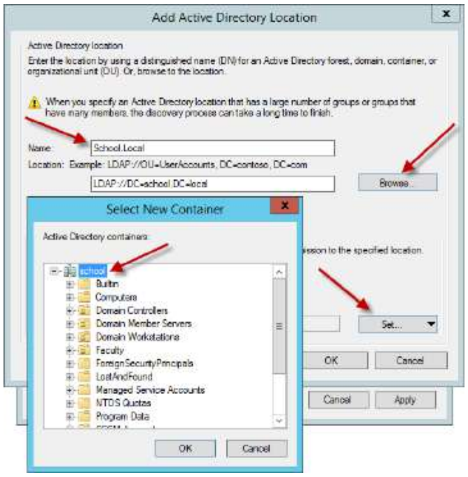
Configure settings to discover the Active Directory group membership of computers and users.

☑ Enable Active Directory Group Discovery

Discovery scopes:

Name	Type	Recursive	Account
School.Local	Location	Yes	SCHOOL\SCCM...

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



Add Active Directory Location

Active Directory location

Enter the location by using a distinguished name (DN) for an Active Directory forest, domain, container, or organizational unit (OU). Or, browse to the location.

When you specify an Active Directory location that has a large number of groups or groups that have many members, the discovery process can take a long time to finish.

Name: School.Local

Location: Example: LDAP://OU=UserAccounts, DC=contoso, DC=com

LDAP://DC=school,DC=local

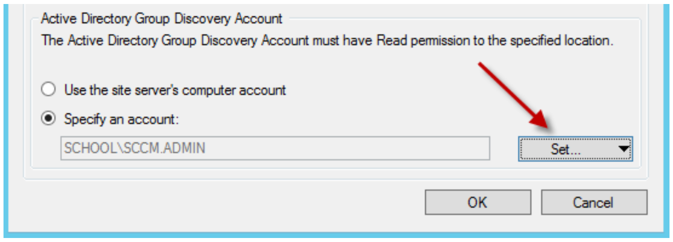
Select New Container

Active Directory containers:

- school
  - Builtin
  - Computers
  - Domain Controllers
  - Domain Member Servers
  - Domain Workstations
  - Faculty
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accounts
  - NTDS Quotas
  - Program Data

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

21 Click **OK**.



Active Directory Group Discovery Account

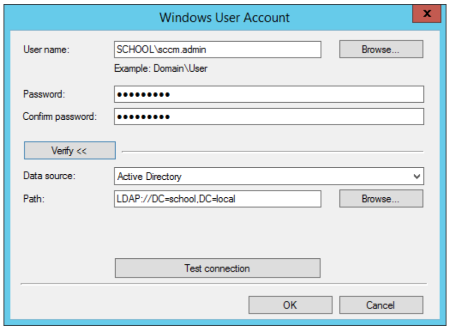
The Active Directory Group Discovery Account must have Read permission to the specified location.

○ Use the site server's computer account

● Specify an account:

SCHOOL\SCCM.ADMIN

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**.



Windows User Account

User name: SCHOOL\sccm.admin

Example: Domain\User

Password: •••••••••

Confirm password: •••••••••

Data source: Active Directory

Path: LDAP://DC=school,DC=local

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

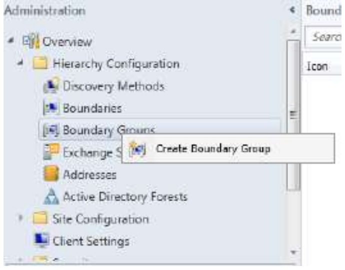
24 Perform Steps 9-15 for all remaining Active Directory discovery methods.

25 Ignore **Network Discovery**

3.2 Configure Boundaries

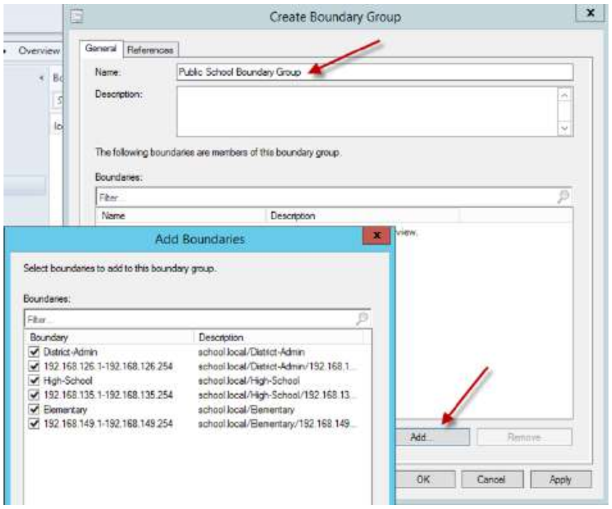
1. The IP Subnet and Active Directory Sites should already be created in the Boundaries. Verify that they do exist by going to **Administration -> Hierarchy Configuration -> Boundaries**.

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**.



Name: Public School Boundary Group

Description:

The following boundaries are members of this boundary group.

Boundaries:

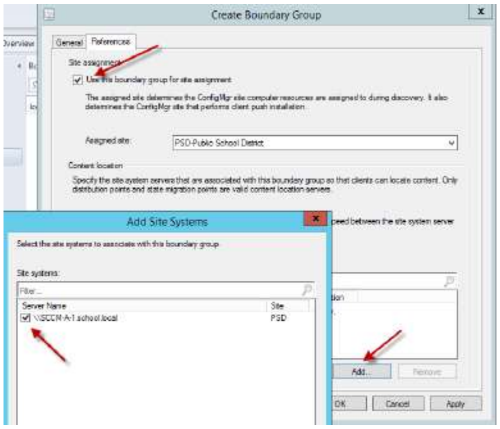
Name	Description

Select boundaries to add to this boundary group.

Boundaries:

Boundary	Description
☑ District-Admin	school.local/District-Admin
☑ 192.168.126.1-192.168.126.254	school.local/District-Admin/192.168.1...
☑ High-School	school.local/High-School
☑ 192.168.135.1-192.168.135.254	school.local/High-School/192.168.13...
☑ Elementary	school.local/Elementary
☑ 192.168.149.1-192.168.149.254	school.local/Elementary/192.168.149...

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



☑ Use this boundary group for site assignment

The assigned site determines the ConfigMgr site computer resources are assigned to during discovery. It also determines the ConfigMgr site that performs client push installation.

Assigned site: PSD-Public School District

Specify the site system servers that are associated with this boundary group so that clients can locate content. Only distribution points and state migration points are valid content location servers.

Select the site systems to associate with this boundary group

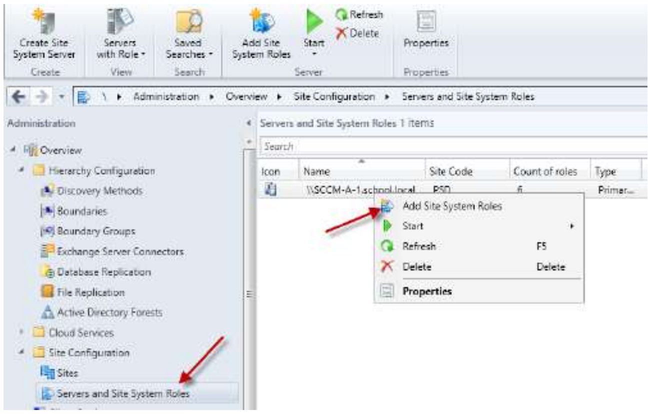
Server Name	Site
☑ \\SCCM-A-1.school.local	PSD

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**.



Icon	Name	Site Code	Count of roles	Type
	\\SCCM-A-1.school.local	PSD	6	Primar...

3 Right-click **<YOUR_SCCM_SERVER>** and click **Add Site System Role**.

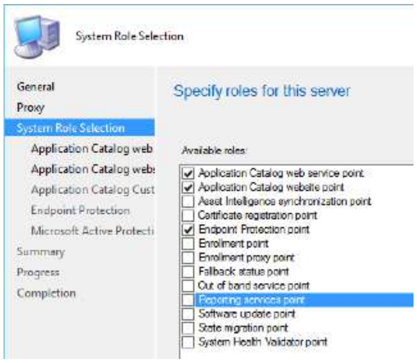
4 On the **General screen**, click **Next**.

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**.

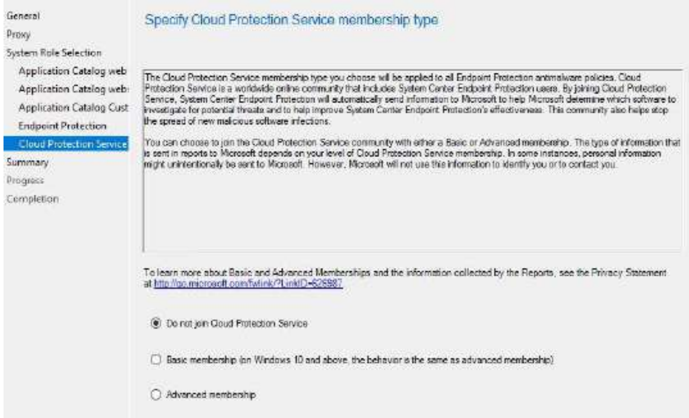


Specify roles for this server

Available roles:

- ☑ Application Catalog web service point
- ☑ Application Catalog website point
- □ Asset Intelligence synchronization point
- □ Certificate registration point
- ☑ Endpoint Protection point
- □ Enrollment point
- □ Enrollment proxy point
- □ Fallback status point
- □ Out of band service point
- □ Reporting services point
- □ Software update point
- □ State migration point
- □ System Health Validator point

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



Specify Cloud Protection Service membership type

The Cloud Protection Service membership type you choose will be applied to all Endpoint Protection antimalware policies. Cloud Protection Service is a worldwide online community that includes System Center Endpoint Protection users. By joining Cloud Protection Service, System Center Endpoint Protection will automatically send information to Microsoft to help Microsoft determine which software to investigate for potential threats and to help improve System Center Endpoint Protection's effectiveness. This community also helps stop the spread of new malicious software infections.

You can choose to join the Cloud Protection Service community with either a Basic or Advanced membership. The type of information that is sent in reports to Microsoft depends on your level of Cloud Protection Service membership. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or to contact you.

To learn more about Basic and Advanced Memberships and the information collected by the Reports, see the Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=626987

● Do not join Cloud Protection Service

□ Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)

○ Advanced membership

8 On the **Summary screen**, click **Next**.

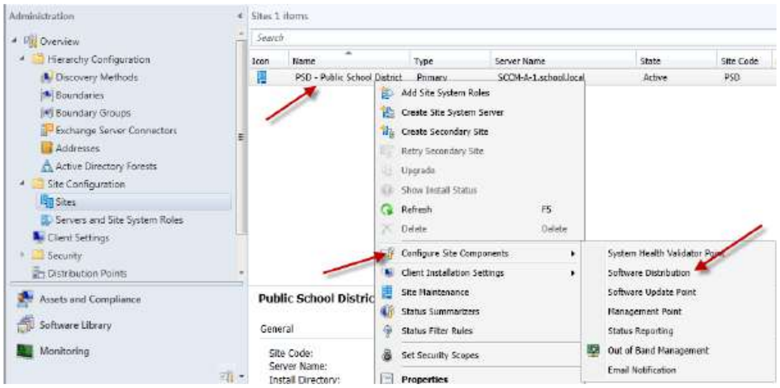
9 Click **Close** when the wizard is finished.

3.4 Configure Network Access Account

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

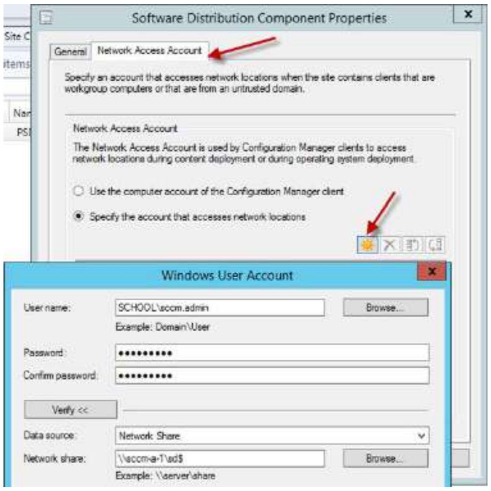
2 In the left-hand pane, select **Sites**.

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



Icon	Name	Type	Server Name	State	Site Code
	PSD - Public School District	Primary	SCCM-A-1.school.local	Active	PSD

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



Specify an account that accesses network locations when the site contains clients that are workgroup computers or that are from an untrusted domain.

Network Access Account

The Network Access Account is used by Configuration Manager clients to access network locations during content deployment or during operating system deployment

○ Use the computer account of the Configuration Manager client

● Specify the account that accesses network locations

User name: SCHOOL\sccm.admin

Example: Domain\User

Password: •••••••••

Confirm password: •••••••••

Data source: Network Share

Network share: \\sccm-a-1\sd$

Example: \\server\share

5 Click **Apply** and **Ok**.

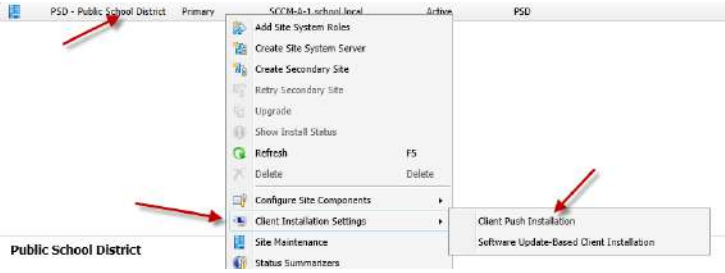
3.5 Configure Client Agent Installation Method

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

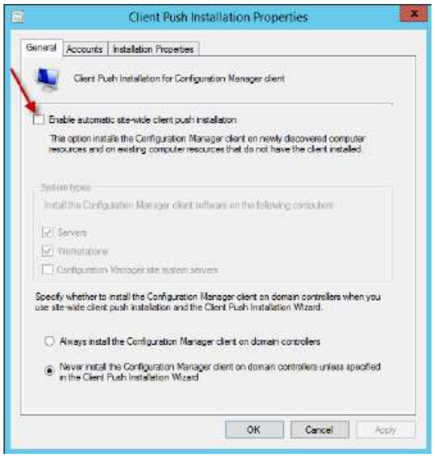
1 Select **Administration** in the lower left of the screen and expand **Site Configuration**.

2 In the left-hand pane, select **Sites**.

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



4 **Enable automatic site-wide client push installation**.



Client Push Installation for Configuration Manager client

□ Enable automatic site-wide client push installation

This option installs the Configuration Manager client on newly discovered computer resources and on existing computer resources that do not have the client installed.

System types

Install the Configuration Manager client software on the following computers

☑ Servers

☑ Workstations

□ Configuration Manager site system servers

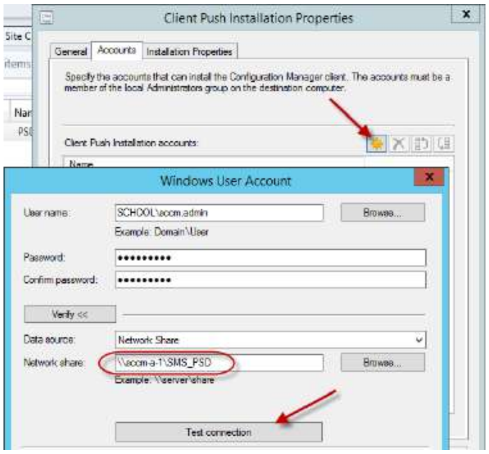
Specify whether to install the Configuration Manager client on domain controllers when you use site-wide client push installation and the Client Push Installation Wizard.

○ Always install the Configuration Manager client on domain controllers

● Never install the Configuration Manager client on domain controllers unless specified in the Client Push Installation Wizard

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

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



Specify the accounts that can install the Configuration Manager client. The accounts must be a member of the local Administrators group on the destination computer.

Client Push Installation accounts:

Name

User name: SCHOOL\sccm.admin

Example: Domain\User

Password: ••••••••••

Confirm password: ••••••••••

Data source: Network Share

Network share: \\sccm-a-1\SMS_PSD

Example: \\server\share

7 Enter **<YOUR_DOMAIN>\SCCM.ADMIN** and click **OK**.

8 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.

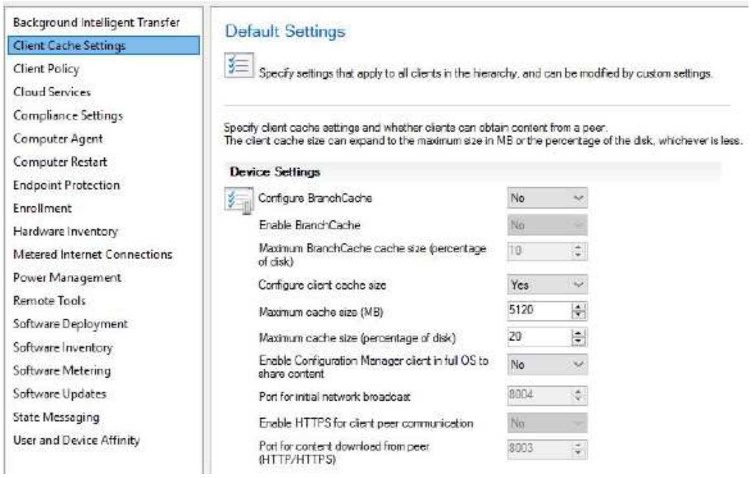
2 In the left-hand pane, select **Client Settings**.

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



Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modifed by custom settings.

Specify client cache settings and whether clients can obtain content from a peer.
The client cache size can expand to the maximum size in MB or the percentage of the disk, whichever is less.

Device Settings

Configure BranchCache	No
Enable BranchCache	No
Maximum BranchCache cache size (percentage of disk)	10
Configure client cache size	Yes
Maximum cache size (MB)	5120
Maximum cache size (percentage of disk)	20
Enable Configuration Manager client in full OS to share content	No
Port for initial network broadcast	8004
Enable HTTPS for client peer communication	No
Port for content download from peer (HTTP/HTTPS)	8003

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

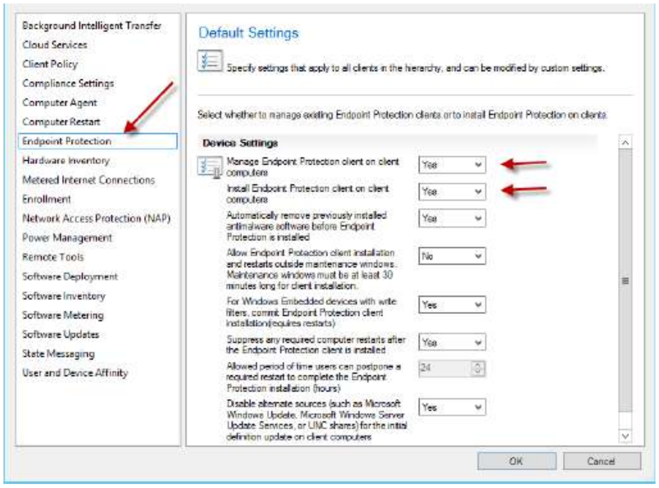
3.6.3 Endpoint Protection

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**.



Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Select whether to manage existing Endpoint Protection clients or to install Endpoint Protection on clients.

Device Settings

Manage Endpoint Protection client on client computers	Yes
Install Endpoint Protection client on client computers	Yes
Automatically remove previously installed antimalware software before Endpoint Protection is installed	Yes
Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation.	No
For Windows Embedded devices with write filters, commit Endpoint Protection client installation(requires restarts)	Yes
Suppress any required computer restarts after the Endpoint Protection client is installed	Yes
Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)	24
Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers	Yes

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

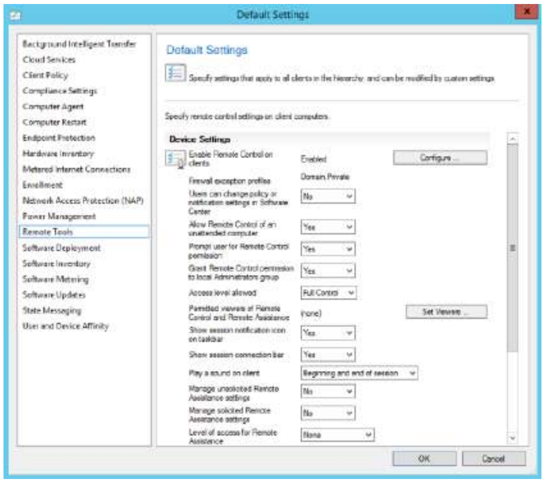
2 In the Left-hand pane, select **Client Settings**.

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**



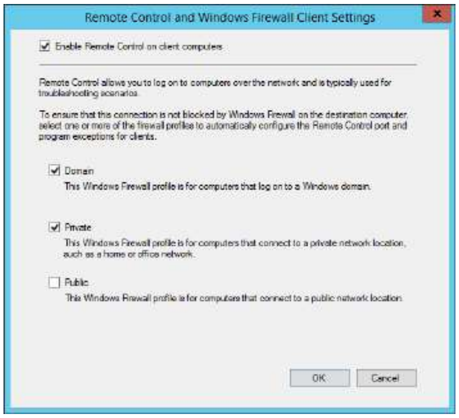
Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings

Specify remote control settings on client computers.

Device Settings

Enable Remote Control on clients	Enabled
Firewall exception profiles	Domain Private
Users can change policy or notification settings in Software Center	No
Allow Remote Control of an unattended computer	Yes
Prompt user for Remote Control permission	Yes
Grant Remote Control permission to local Administrators group	Yes
Access level allowed	Full Control
Permitted viewers of Remote Control and Remote Assistance	(none)
Show session notification icon on taskbar	Yes
Show session connection bar	Yes
Play a sound on client	Beginning and end of session
Manage unsolicited Remote Assistance settings	No
Manage solicited Remote Assistance settings	No
Level of access for Remote Assistance	None



☑ Enable Remote Control on client computers

Remote Control allows you to log on to computers over the network and is typically used for troubleshooting scenarios.

To ensure that this connection is not blocked by Windows Firewall on the destination computer, select one or more of the firewall profiles to automatically configure the Remote Control port and program exceptions for clients.

☑ Domain
This Windows Firewall profile is for computers that log on to a Windows domain.

☑ Private
This Windows Firewall profile is for computers that connect to a private network location, such as a home or office network.

☐ Public
This Windows Firewall profile is for computers that connect to a public network location.

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**

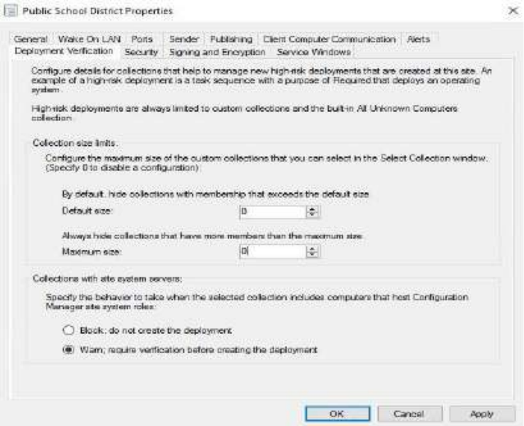
4. In the right hand side of SCCM select your primary site: ***<u>i.e.</u>*** **PSD – Public School District**

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**



Public School District Properties

Configure details for collections that help to manage new high-risk deployments that are created at this site. An example of a high-risk deployment is a task sequence with a purpose of Required that deploys an operating system.

High-risk deployments are always limited to custom collections and the built-in All Unknown Computers collection.

Collection size limits:

Configure the maximum size of the custom collections that you can select in the Select Collection window. (Specify 0 to disable a configuration)

By default, hide collections with membership that exceeds the default size

Default size: 0

Always hide collections that have more members than the maximum size

Maximum size: 0

Collections with site system servers:

Specify the behavior to take when the selected collection includes computers that host Configuration Manager site system roles:

○ Block; do not create the deployment

● 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.**

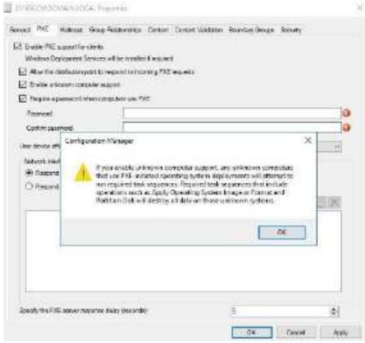
3 Select the **PXE tab** and place a checkmark in **Enable PXE support for Clients**. Click on **Yes** when prompted about firewall ports.

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



☑ Enable PXE support for clients

Windows Deployment Services will be installed if required

☑ Allow this distribution point to respond to incoming PXE requests

☑ Enable unknown computer support

☑ Require a password when computers use PXE

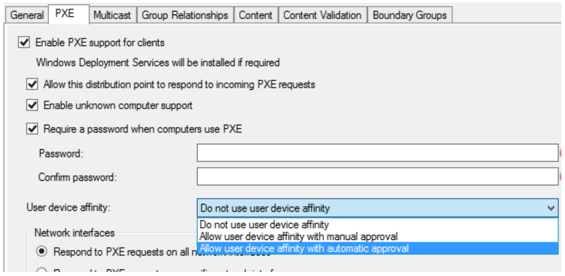
Password:

Confirm password:

Configuration Manager

If you enable unknown computer support, any unknown computers that use PXE-initiated operating system deployments will attempt to run required task sequences. Required task sequences that include operations such as Apply Operating System Image or Format and Partition Disk will destroy all data on those unknown systems.

Specify the PXE server response delay (seconds): 5



☑ Enable PXE support for clients

Windows Deployment Services will be installed if required

☑ Allow this distribution point to respond to incoming PXE requests

☑ Enable unknown computer support

☑ Require a password when computers use PXE

Password:

Confirm password:

User device affinity: Do not use user device affinity

Do not use user device affinity
Allow user device affinity with manual approval
Allow user device affinity with automatic approval

Network interfaces

● Respond to PXE requests on all n

8 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

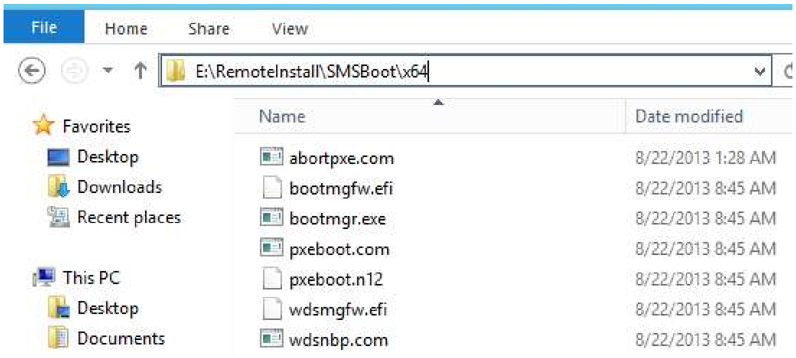
NOTE: The following is now necessary for the clients to choose if they are UEFI or BIOS.

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:

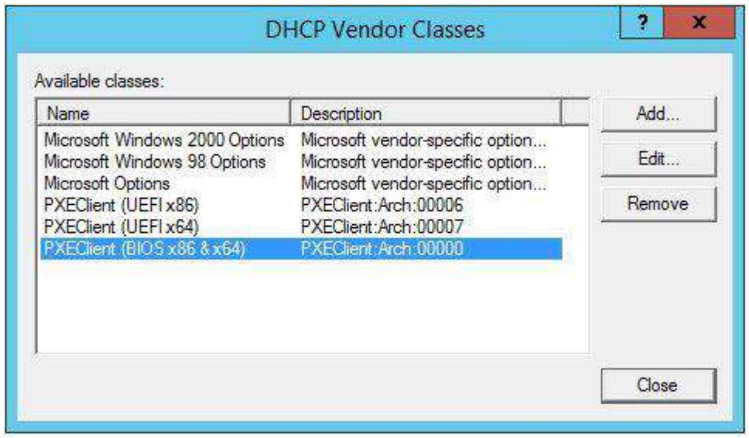
1. Go to **DHCP**, right-click on **IPv4,** click **Define Vendor Classes**.
2. In the DHCP Vendor Classes window, click **Add**.
3. For the Name enter **PXEClient (UEFI x86)**.
4. For the Description enter **PXEClient:Arch:00006**.
5. Click in the **ASCII** column and type the text **PXEClient:Arch:00006** (you will not be able to paste this text, and it's also case-sensitive).
6. Click **OK** to add it to the list.
7. Now repeat steps 2 – 6 for **PXEClient (UEFI x64)** with **PXEClient:Arch:00007** as the Description and ASCII value.
8. 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.



E:\RemoteInstall\SMSBoot\x64

Name	Date modified
abortpxe.com	8/22/2013 1:28 AM
bootmgfw.efi	8/22/2013 8:45 AM
bootmgr.exe	8/22/2013 8:45 AM
pxeboot.com	8/22/2013 8:45 AM
pxeboot.n12	8/22/2013 8:45 AM
wdsmgfw.efi	8/22/2013 8:45 AM
wdsnbp.com	8/22/2013 8:45 AM



Available classes:

Name	Description
Microsoft Windows 2000 Options	Microsoft vendor-specific option...
Microsoft Windows 98 Options	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...
PXEClient (UEFI x86)	PXEClient:Arch:00006
PXEClient (UEFI x64)	PXEClient:Arch:00007
PXEClient (BIOS x86 & x64)	PXEClient:Arch:00000

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.

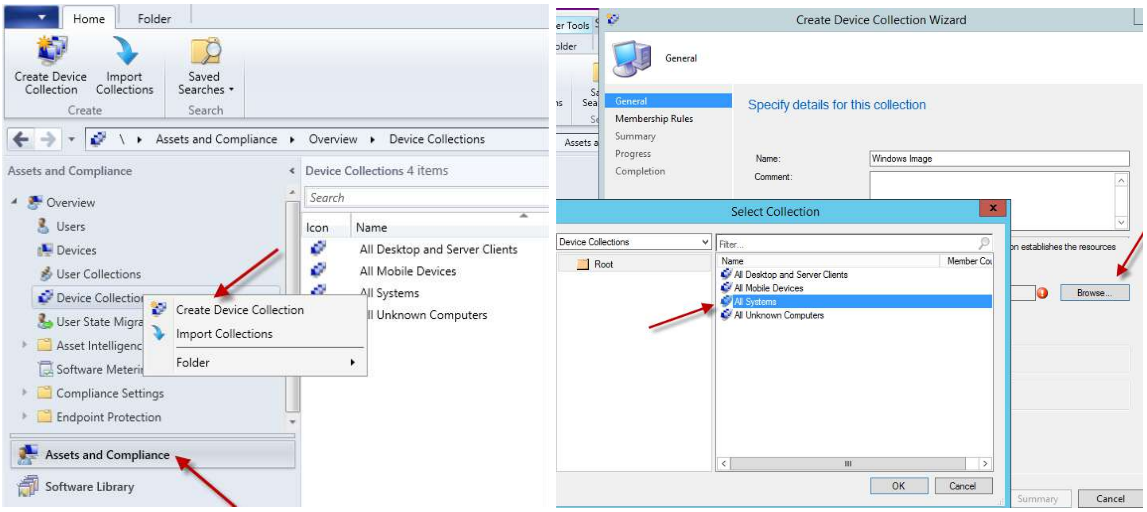
1. Go to **DHCP Console** and expand the scope you wish to create a policy for.
2. Right-click on **Policies** and choose **New Policy**.
3. Enter **PXEClient (UEFI x64)** for the name.
4. Enter a Description if you want. Click **Next**.
5. On the Configure Conditions for the policy screen, click **Add**.
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**.



Name: Windows Image

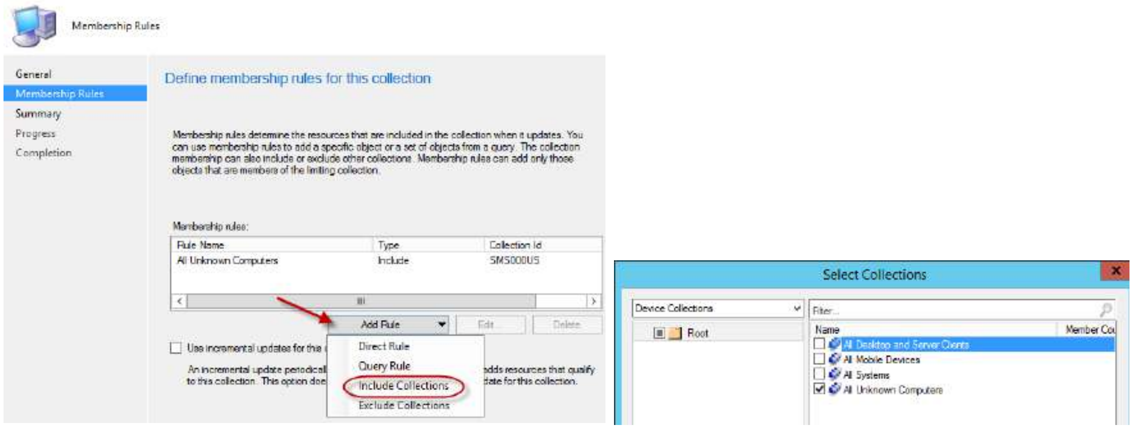
Comment:

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**.



Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.

Membership rules:

Rule Name	Type	Collection Id
All Unknown Computers	Include	SMS000US

□ Use incremental updates for this

An incremental update periodical … adds resources that qualify to this collection. This option doe… date for this collection.

□ All Desktop and Server Clients
□ All Mobile Devices
□ All Systems
☑ All Unknown Computers

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

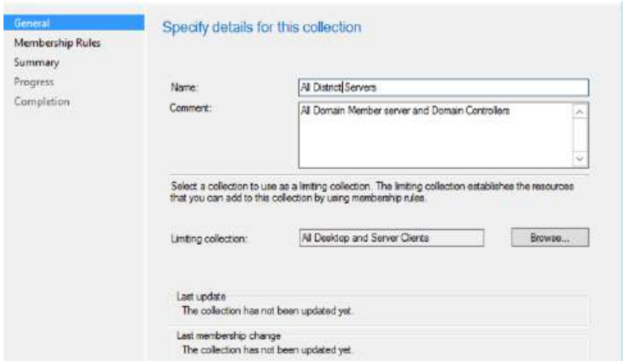
1 In the Configuration Manager console, click **Assets and Compliance**.

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**.



Specify details for this collection

Name: All District Servers

Comment: All Domain Member server and Domain Controllers

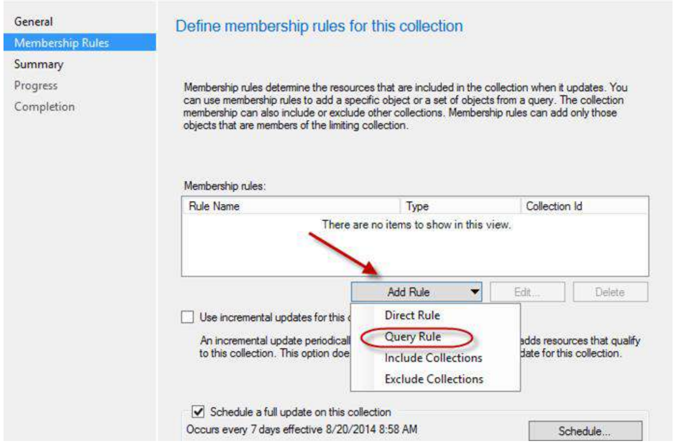
Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Desktop and Server Clients

Last update
The collection has not been updated yet.

Last membership change
The collection has not been updated yet.

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



Define membership rules for this collection

Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.

Membership rules:

Rule Name	Type	Collection Id
There are no items to show in this view.		

□ Use incremental updates for this c

An incremental update periodicall … adds resources that qualify to this collection. This option doe … date for this collection.

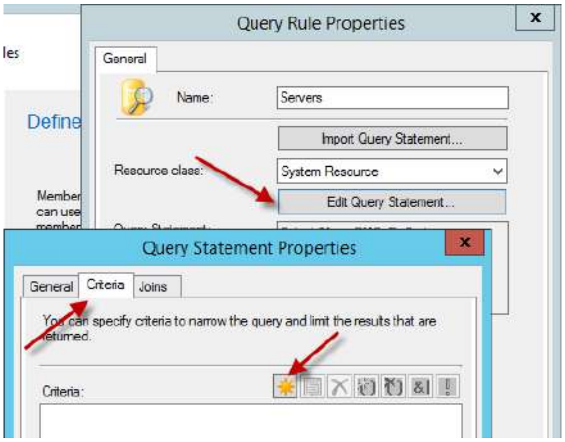
☑ Schedule a full update on this collection
Occurs every 7 days effective 8/20/2014 8:58 AM

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**



Query Rule Properties

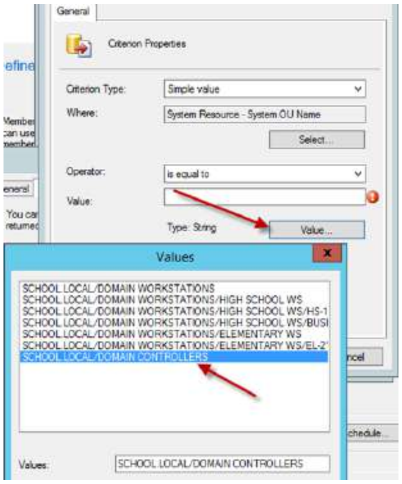
Name: Servers

Resource class: System Resource

Query Statement Properties

You can specify criteria to narrow the query and limit the results that are returned.

Criteria:



Criterion Properties

Criterion Type: Simple value

Where: System Resource - System OU Name

Operator: is equal to

Value:

Type: String

Values

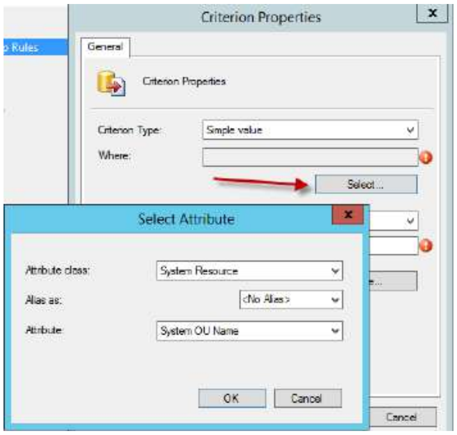
SCHOOL.LOCAL/DOMAIN WORKSTATIONS
SCHOOL.LOCAL/DOMAIN WORKSTATIONS/HIGH SCHOOL WS
SCHOOL.LOCAL/DOMAIN WORKSTATIONS/HIGH SCHOOL WS/HS-1
SCHOOL.LOCAL/DOMAIN WORKSTATIONS/HIGH SCHOOL WS/BUSI
SCHOOL.LOCAL/DOMAIN WORKSTATIONS/ELEMENTARY WS
SCHOOL.LOCAL/DOMAIN WORKSTATIONS/ELEMENTARY WS/EL-2'
SCHOOL.LOCAL/DOMAIN CONTROLLERS

Values: SCHOOL.LOCAL/DOMAIN CONTROLLERS

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

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

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



Criterion Properties

Criterion Type: Simple value

Where:

Select Attribute

Attribute class: System Resource

Alias as: <No Alias>

Attribute: System OU Name

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.

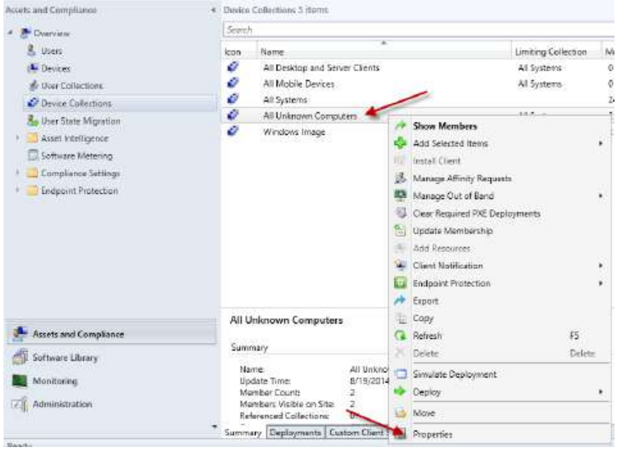
1.e **Value**: Enter a value for which you want to search the selected attribute name. You can use the percent character % as a wildcard. For example, if you wanted to search for computers that have a NetBIOS name beginning with ‘M’, enter M% in this field.

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**.



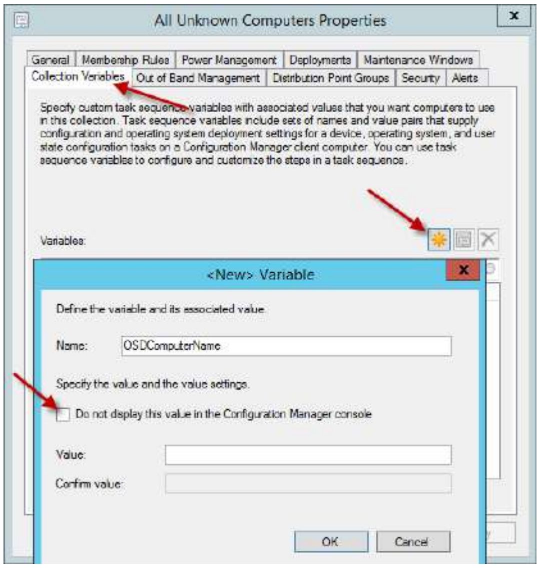
Name	Limiting Collection	M
All Desktop and Server Clients	All Systems	0
All Mobile Devices	All Systems	0
All Systems		2
All Unknown Computers		
Windows Image		

All Unknown Computers

Summary

Name: All Unkno
Update Time: 8/19/2014
Member Count: 2
Members Visible on Site: 2
Referenced Collections:

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



Specify custom task sequence variables with associated values that you want computers to use in this collection. Task sequence variables include sets of names and value pairs that supply configuration and operating system deployment settings for a device, operating system, and user state configuration tasks on a Configuration Manager client computer. You can use task sequence variables to configure and customize the steps in a task sequence.

Define the variable and its associated value.

Name: OSDComputerName

Specify the value and the value settings.

□ Do not display this value in the Configuration Manager console

Value:

Confirm value:

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.

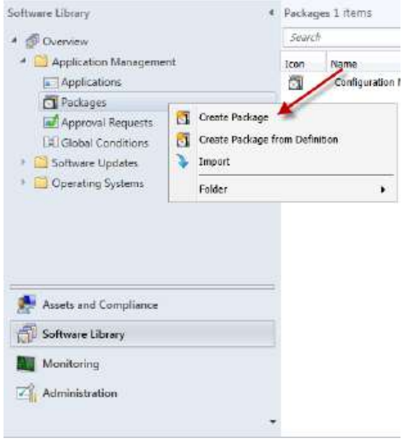
5. In the **Software Distribution** folder, create folders called **Images, Drivers** and **Software**.

5.2 Software Package

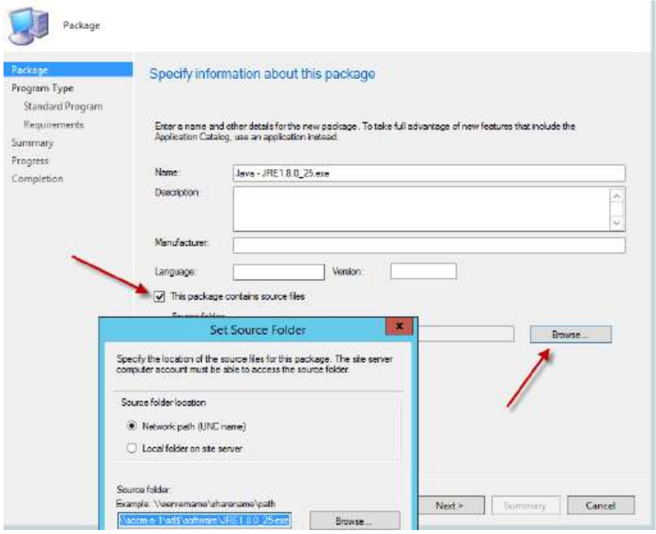
5.2.1 Create Software Package

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:



Enter a name and other details for the new package. To take full advantage of new features that include the Application Catalog, use an application instead.

Name: Java - JRE1.8.0_25.exe

Description:

Manufacturer:

Language: Version:

☑ This package contains source files

Set Source Folder

Specify the location of the source files for this package. The site server computer account must be able to access the source folder.

Source folder location

● Network path (UNC name)

○ Local folder on site server

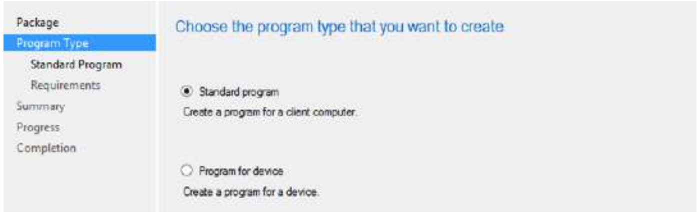
Source folder:

Example: \\servername\sharename\path

\\sccm-s-1\sd$\software\JRE1.8.0_25.exe

Name: **Jre-8u333-windows-i586.exe**
Check This package conatins source files
Source Folder: **Network path (UNC name)**
\\<YOUR_SCCM_SERVER>\sd$\software\JRE8u333-exe

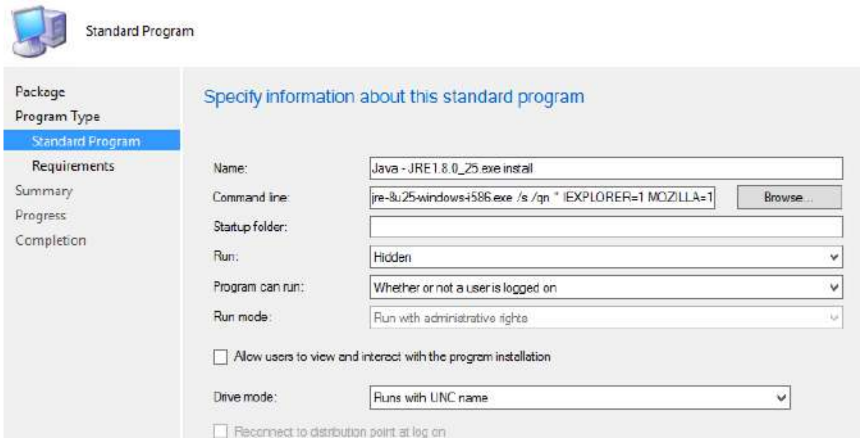
4 On the **Program Type** page of the **Create Package and Program Wizard**, select the type of program you want to create and then click **Next**. You can create a program for a computer, a device or skip this step and create a program later.



● Standard program
Create a program for a client computer.

○ Program for device
Create a program for a device.

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



Standard Program

Specify information about this standard program

Name: Java - JRE1.8.0_25.exe install

Command line: jre-8u25-windows-i586.exe /s /qn " IEXPLORER=1 MOZILLA=1

Startup folder:

Run: Hidden

Program can run: Whether or not a user is logged on

Run mode: Run with administrative rights

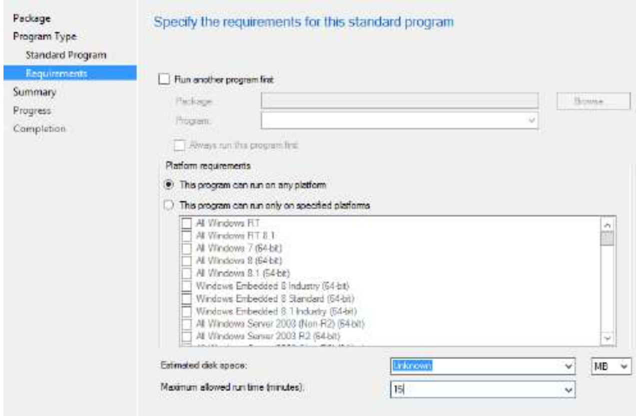
□ Allow users to view and interact with the program installation

Drive mode: Runs with UNC name

□ Reconnect to distribution point at log on

On the **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**

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



Specify the requirements for this standard program

□ Run another program first

Package:

Program:

□ Always run this program first

Platform requirements

● This program can run on any platform

○ This program can run only on specified platforms

□ All Windows RT
□ All Windows RT 8.1
□ All Windows 7 (64-bit)
□ All Windows 8 (64-bit)
□ All Windows 8.1 (64-bit)
□ Windows Embedded 8 Industry (64-bit)
□ Windows Embedded 8 Standard (64-bit)
□ Windows Embedded 8.1 Industry (64-bit)
□ All Windows Server 2003 (Non R2) (64-bit)
□ All Windows Server 2003 R2 (64-bit)

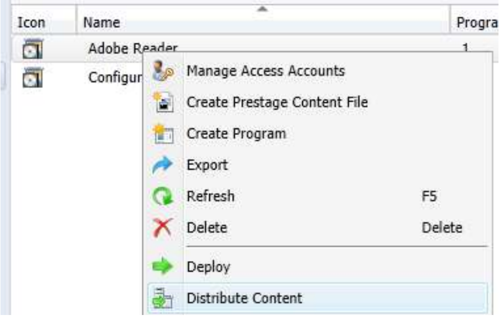
Estimated disk space: Unknown MB

Maximum allowed run time (minutes): 15

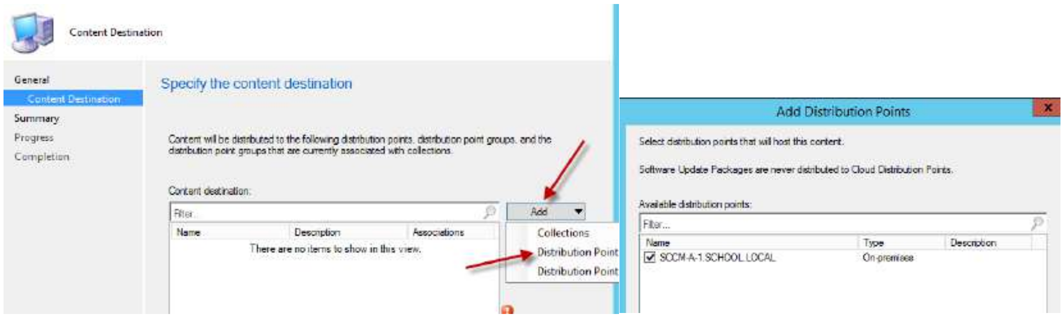
7 Click **Next** and **finish** the wizard.

5.2.2 Distribute Software Package

1 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.



Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

Content destination:

Name	Description	Associations
There are no items to show in this view.		

Select distribution points that will host this content.

Software Update Packages are never distributed to Cloud Distribution Points.

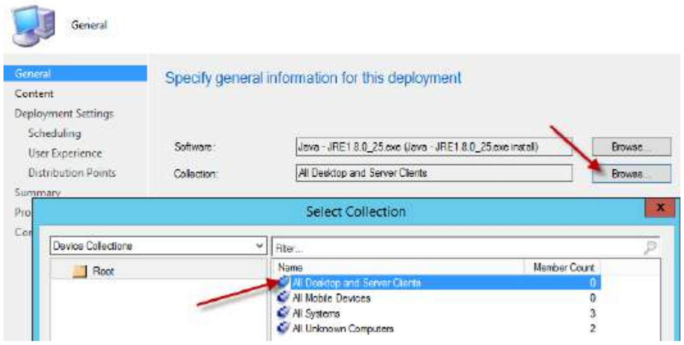
Available distribution points:

Name	Type	Description
☑ SCCM-A-1.SCHOOL.LOCAL	On-premises	

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.



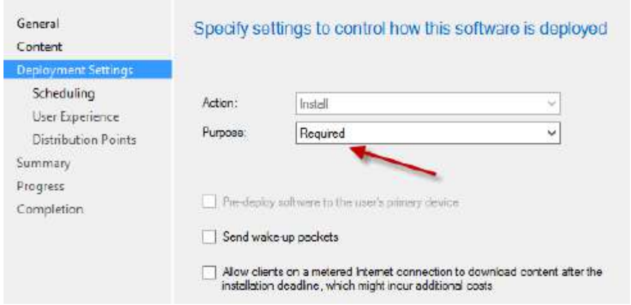
Specify general information for this deployment

Software: Java - JRE1.8.0_25.exe (Java - JRE1.8.0_25.exe install)

Collection: All Desktop and Server Clients

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

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



Specify settings to control how this software is deployed

Action: Install

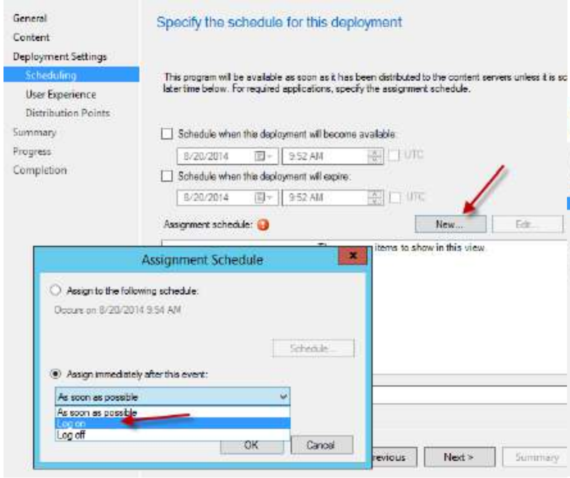
Purpose: Required

□ Pre-deploy software to the user's primary device

□ Send wake-up packets

□ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

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



Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is sc later time below. For required applications, specify the assignment schedule.

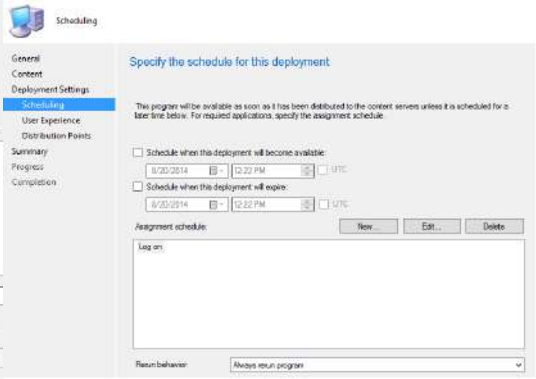
☐ Schedule when this deployment will become available:
8/20/2014 9:52 AM ☐ UTC
☐ Schedule when this deployment will expire:
8/20/2014 9:52 AM ☐ UTC

Assignment schedule:

Assignment Schedule

○ Assign to the following schedule:
Occurs on 8/20/2014 9:54 AM

● Assign immediately after this event:
As soon as possible



Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.

☐ Schedule when this deployment will become available:
8/20/2014 12:22 PM ☐ UTC
☐ Schedule when this deployment will expire:
8/20/2014 12:22 PM ☐ UTC

Assignment schedule:

Log on

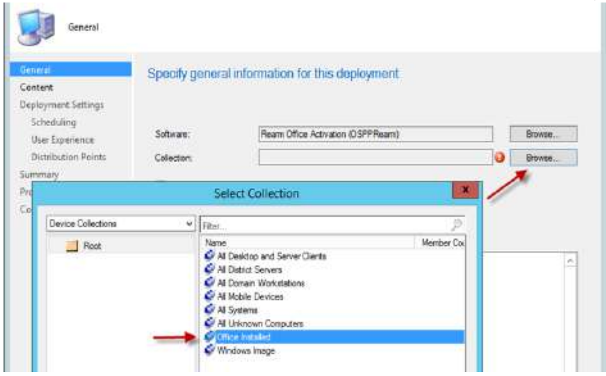
Rerun behavior: Always rerun program

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.

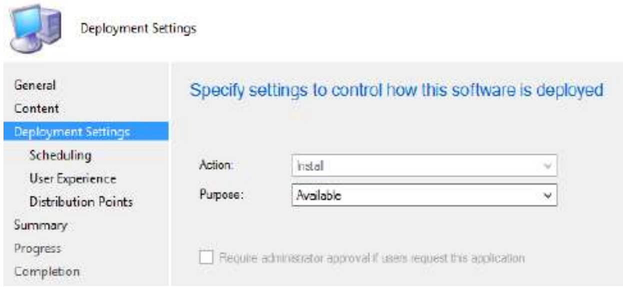


Specify general information for this deployment

Software: Ream Office Activation (OSPPRearm)

Collection:

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



Specify settings to control how this software is deployed

Action: Install

Purpose: Available

□ Require administrator approval if users request this application

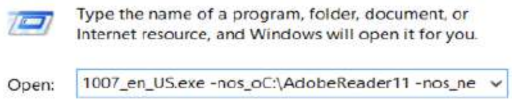
4 On the **Deployment Settings** page, Chose the **Action: Install** and the **Purpose: Available**. Click **Next** through the rest of the wizard.

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.

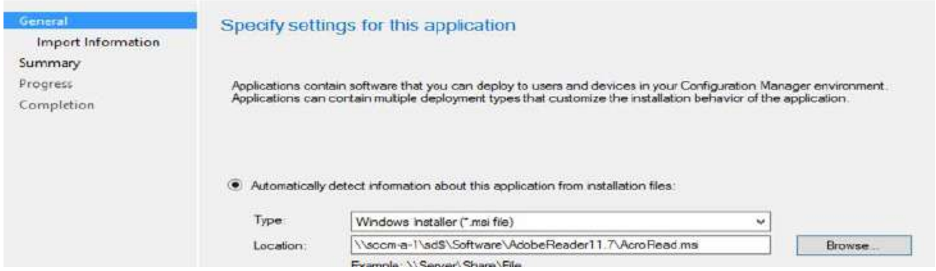
Open: 1007_en_US.exe -nos_oC:\AdobeReader11 -nos_ne

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.**



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

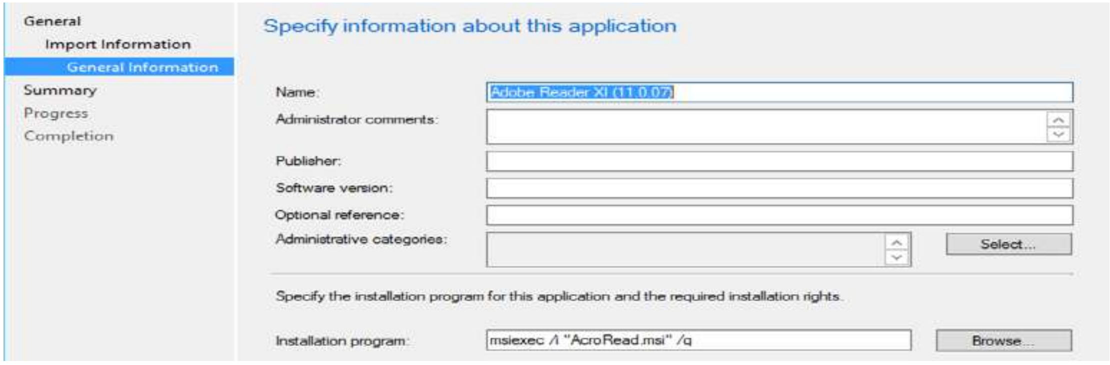
● Automatically detect infomation about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\sccm-a-1\sd$\Software\AdobeReader11.7\AcroRead.ms

Example: \\Server\Share\File

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.



Specify information about this application

Name: Adobe Reader XI (11.0.07)

Administrator comments:

Publisher:

Software version:

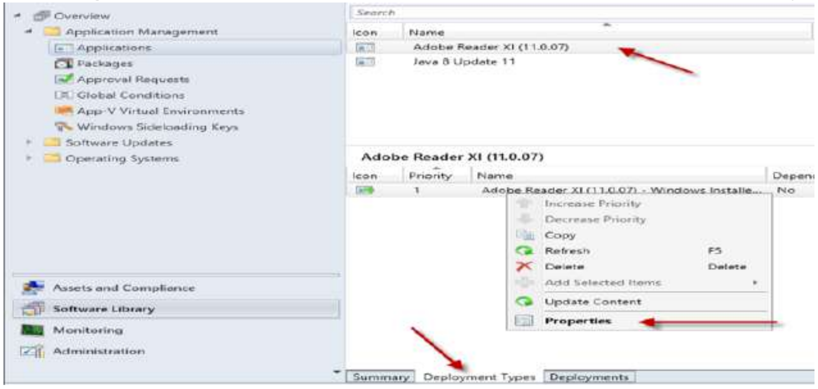
Optional reference:

Administrative categories:

Specify the installation program for this application and the required installation rights.

Installation program: msiexec /i "AcroRead.msi" /q

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

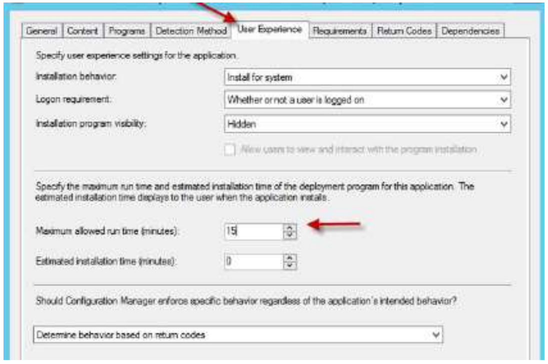


Icon	Name
	Adobe Reader XI (11.0.07)
	Java 8 Update 11

Adobe Reader XI (11.0.07)

Icon	Priority	Name	Depen
	1	Adobe Reader XI (11.0.07) - Windows Installe...	No

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



General | Content | Programs | Detection Method | User Experience | Requirements | Return Codes | Dependencies

Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

Installation program visibility: Hidden

□ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

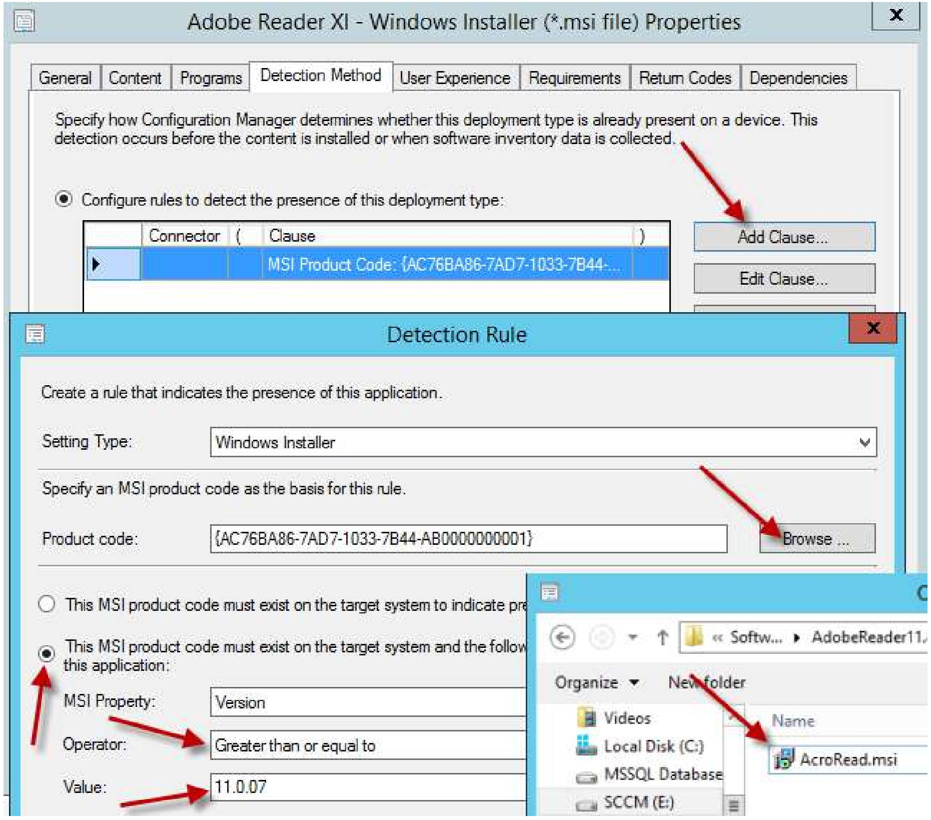
Maximum allowed run time (minutes): 15

Estimated installation time (minutes): 0

Should Configuration Manager enforce specific behavior regardless of the application's intended behavior?

Determine behavior based on return codes

10 Under the Detection Method Tab, Click **Add Clause**. Change Setting Type: **Windows Installer**. Prodect 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 meet to indicate the presence of the application**. Change the Operator: **Greater than or equal to**. Leave the default **Value.**



Adobe Reader XI - Windows Installer (*.msi file) Properties

General | Content | Programs | Detection Method | User Experience | Requirements | Return Codes | Dependencies

Specify how Configuration Manager determines whether this deployment type is already present on a device. This detection occurs before the content is installed or when software inventory data is collected.

● Configure rules to detect the presence of this deployment type:

Connector	(	Clause	)
		MSI Product Code: {AC76BA86-7AD7-1033-7B44-...	

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: Windows Installer

Specify an MSI product code as the basis for this rule.

Product code: {AC76BA86-7AD7-1033-7B44-AB0000000001}

○ This MSI product code must exist on the target system to indicate pre

● This MSI product code must exist on the target system and the follow this application:

MSI Property: Version

Operator: Greater than or equal to

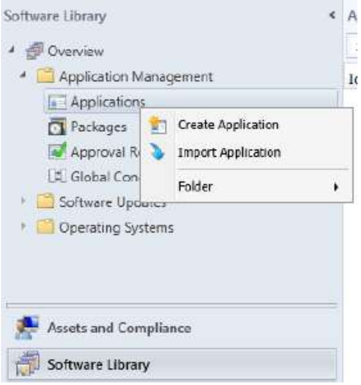
Value: 11.0.07

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

5.3.2 Chrome

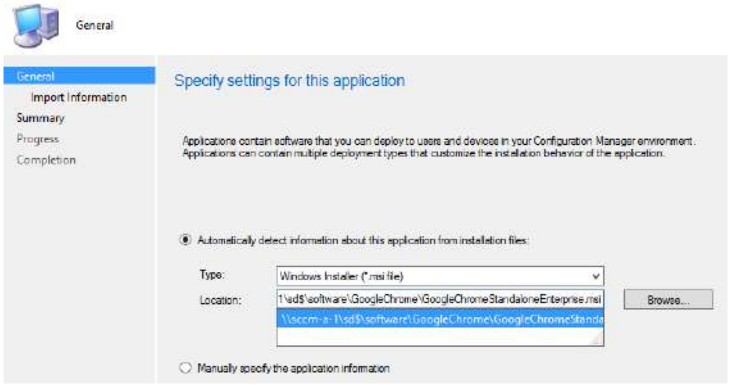
1 In the Configuration Manager console, click **Software Library**

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.**



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

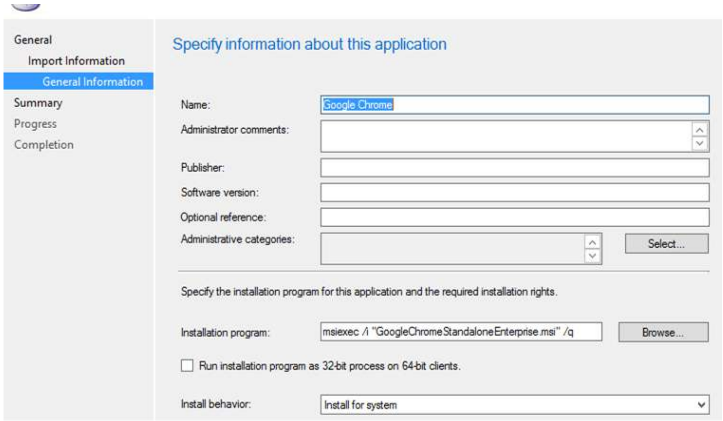
Location: 1\sd$\software\GoogleChrome\GoogleChromeStandaloneEnterprise.msi

\\sccm-a-1\sd$\software\GoogleChrome\GoogleChromeStanda

Browse...

○ Manually specify the application information

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.



Specify information about this application

Name: Google Chrome

Administrator comments:

Publisher:

Software version:

Optional reference:

Administrative categories:

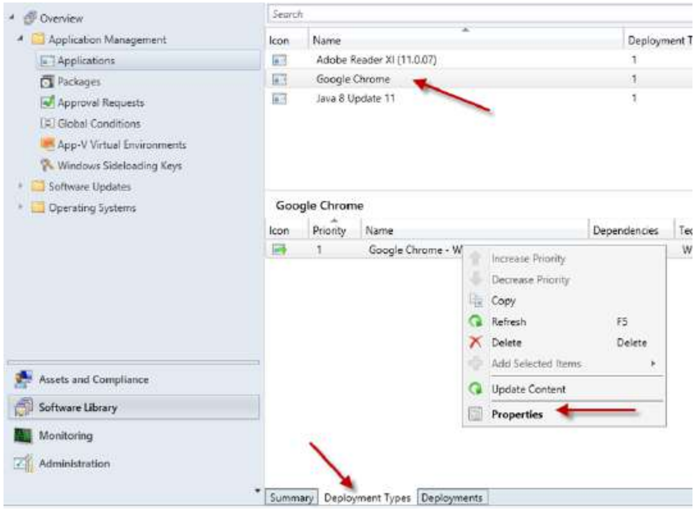
Specify the installation program for this application and the required installation rights.

Installation program: msiexec /i "GoogleChromeStandaloneEnterprise.msi" /q

□ Run installation program as 32-bit process on 64-bit clients.

Install behavior: Install for system

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**

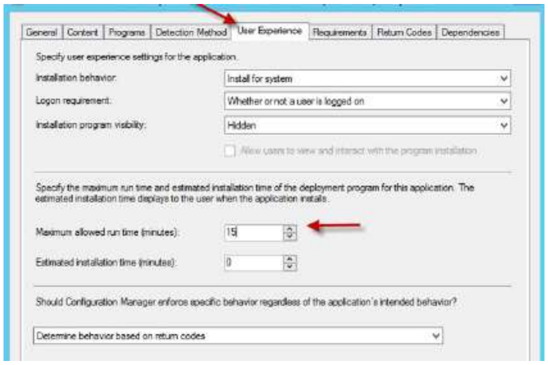


Icon	Name	Deployment T
	Adobe Reader XI (11.0.07)	1
	Google Chrome	1
	Java 8 Update 11	1

Google Chrome

Icon	Priority	Name	Dependencies	Te
	1	Google Chrome - W		W

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



Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

Installation program visibility: Hidden

□ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time deplays to the user when the application installs.

Maximum allowed run time (minutes): 15

Estimated installation time (minutes): 0

Should Configuration Manager enforce specific behavior regardless of the application's intended behavior?

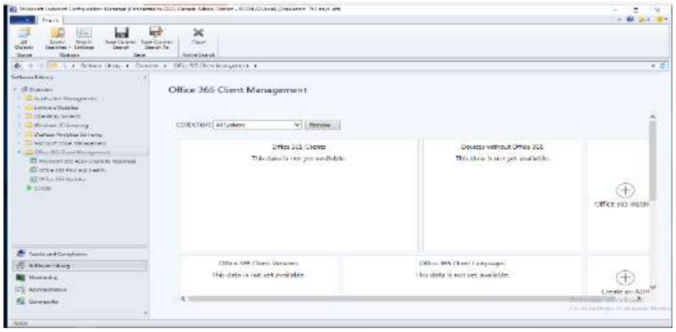
Determine behavior based on return codes

5.3.3 Deploy Office 2019 – Office 365

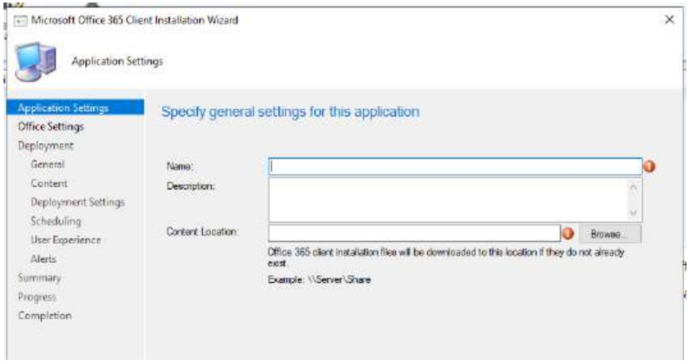
1 In the Configuration Manager console, click **Software Library**.

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.


Office 365 Client Management
Office 365 Clients
This data is not yet available.
Devices without Office 365
This data is not yet available.
Office 365 Installer
Office 365 Client Versions
This data is not yet available.
Office 365 Client Languages
This data is not yet available.
Create an ADR

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.

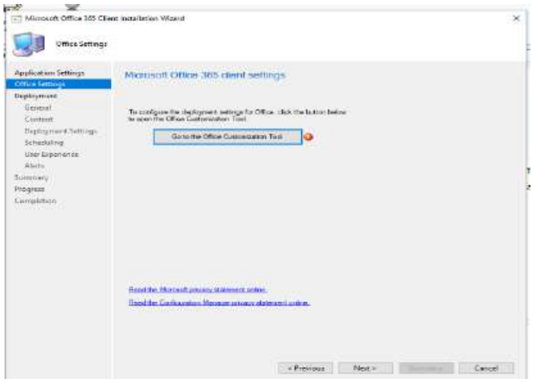


Specify general settings for this application

Office 365 client installation files will be downloaded to this location if they do not already exist.

Example: \\Server\Share

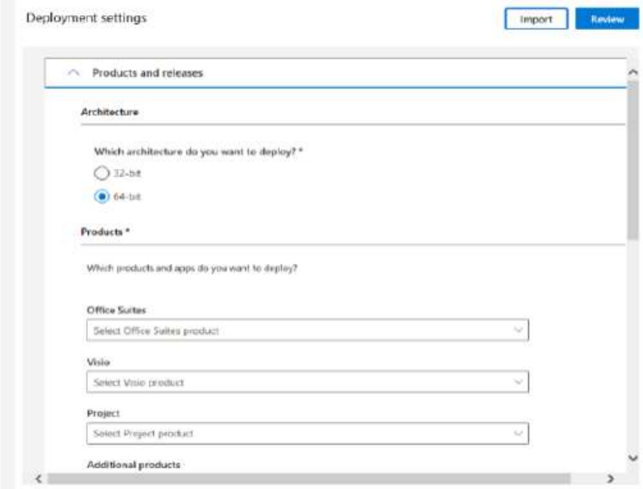
5 Click on the Go to the Office Customization Tool.


Microsoft Office 365 Client Installation Wizard
Office Settings
Application Settings
Office Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Go to the Office Customization Tool
Read the Microsoft privacy statement online.
Read the Configuration Manager privacy statement online.
< Previous
Next >
Cancel

Microsoft Office 365 client settings

To configure the deployment settings for Office, click the button below to open the Office Customization Tool.

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



Deployment settings

Import Review

Products and releases

Architecture

Which architecture do you want to deploy? *

○ 32-bit

● 64-bit

Products *

Which products and apps do you want to deploy?

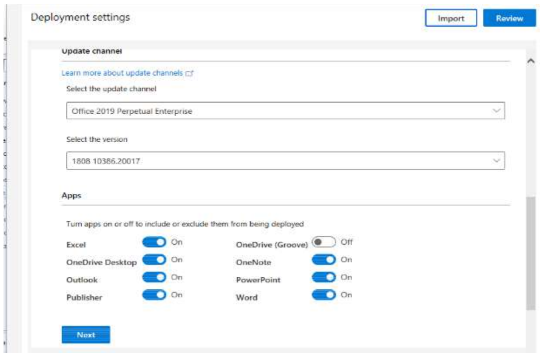
Office Suites: Select Office Suites product

Visio: Select Visio product

Project: Select Project product

Additional products

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



Deployment settings

Import Review

Update channel

Learn more about update channels

Select the update channel: Office 2019 Perpetual Enterprise

Select the version: 1808 10386.20017

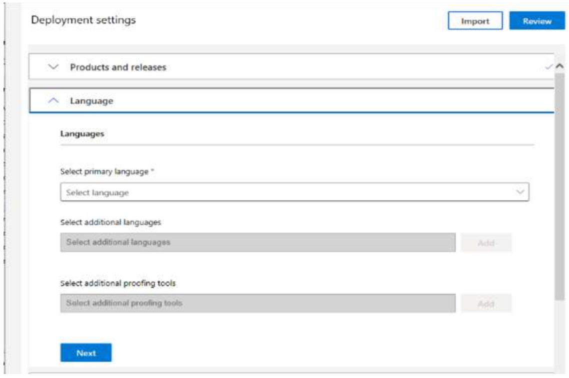
Apps

Turn apps on or off to include or exclude them from being deployed

Excel	On	OneDrive (Groove)	Off
OneDrive Desktop	On	OneNote	On
Outlook	On	PowerPoint	On
Publisher	On	Word	On

Next

8 Set your language after that click next again.



Deployment settings

Import Review

Products and releases

Language

Languages

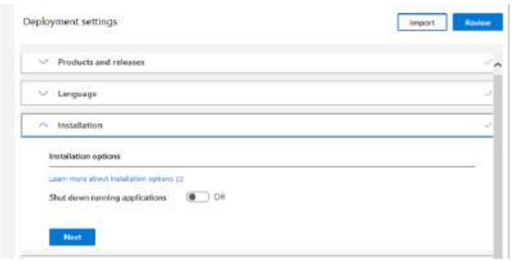
Select primary language *: Select language

Select additional languages: Select additional languages | Add

Select additional proofing tools: Select additional proofing tools | Add

Next

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



Deployment settings

Import Review

Products and releases

Language

Installation

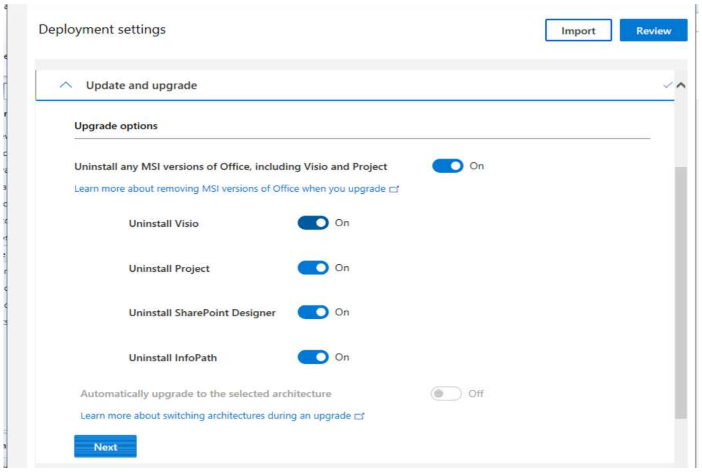
Installation options

Learn more about installation options

Shut down running applications: Off

Next

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



Deployment settings

Update and upgrade

Upgrade options

Uninstall any MSI versions of Office, including Visio and Project — On

Learn more about removing MSI versions of Office when you upgrade

Uninstall Visio — On

Uninstall Project — On

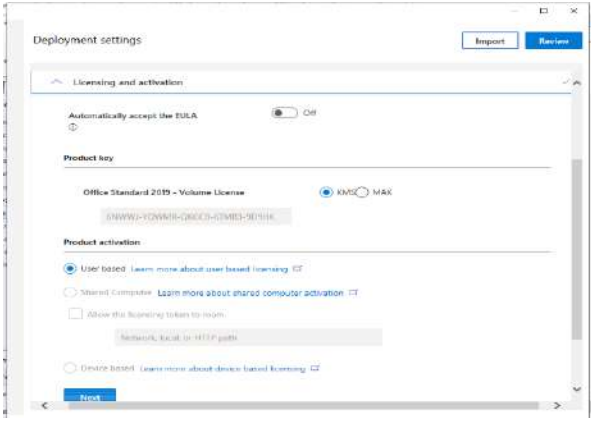
Uninstall SharePoint Designer — On

Uninstall InfoPath — On

Automatically upgrade to the selected architecture — Off

Learn more about switching architectures during an upgrade

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



Deployment settings

Licensing and activation

Automatically accept the EULA — Off

Product key

Office Standard 2019 - Volume License — ● KMS ○ MAK

6NWWJ-YQWMR-QKGCB-6TMB3-9D9HK

Product activation

● User based Learn more about user based licensing

○ Shared Computer Learn more about shared computer activation

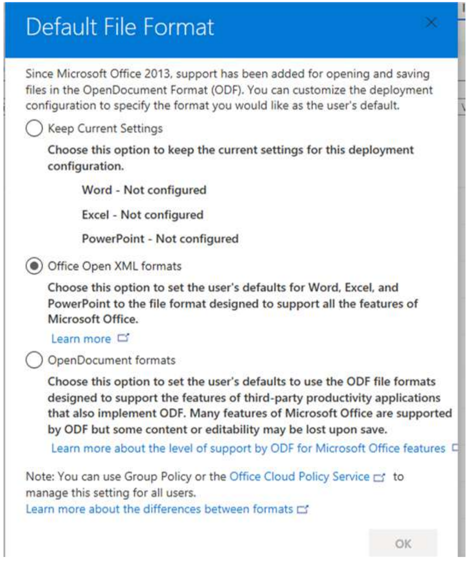
□ Allow the licensing token to roam

Network, local or HTTP path

○ Device based Learn more about device based licensing

12 Next passed the deployment settings.

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



Default File Format

Since Microsoft Office 2013, support has been added for opening and saving files in the OpenDocument Format (ODF). You can customize the deployment configuration to specify the format you would like as the user's default.

○ Keep Current Settings

Choose this option to keep the current settings for this deployment configuration.

Word - Not configured

Excel - Not configured

PowerPoint - Not configured

● Office Open XML formats

Choose this option to set the user's defaults for Word, Excel, and PowerPoint to the file format designed to support all the features of Microsoft Office.

Learn more

○ OpenDocument formats

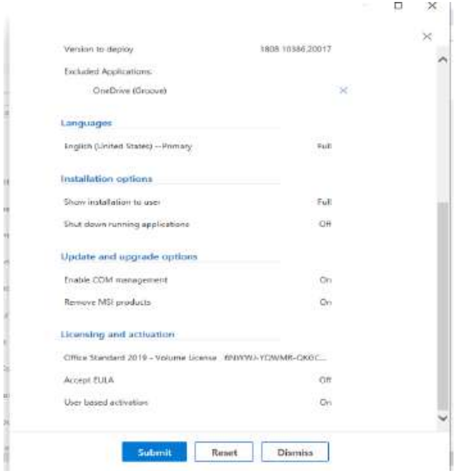
Choose this option to set the user's defaults to use the ODF file formats designed to support the features of third-party productivity applications that also implement ODF. Many features of Microsoft Office are supported by ODF but some content or editability may be lost upon save.

Learn more about the level of support by ODF for Microsoft Office features

Note: You can use Group Policy or the Office Cloud Policy Service to manage this setting for all users.

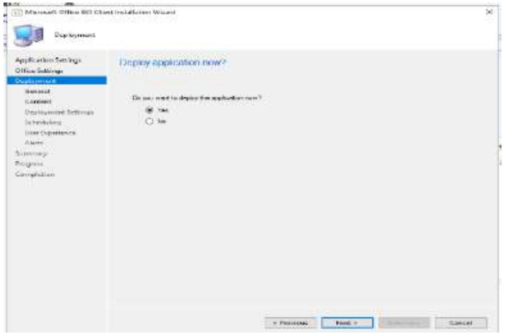
Learn more about the differences between formats

14 Review your settings then click Submit.



Version to deploy	1808 10386.20017
Excluded Applications:	
OneDrive (Groove)	
Languages	
English (United States) --Primary	Full
Installation options	
Show installation to user	Full
Shut down running applications	Off
Update and upgrade options	
Enable COM management	On
Remove MSI products	On
Licensing and activation	
Office Standard 2019 – Volume License	6NWWJ-YQWMR-QKGC...
Accept EULA	Off
User based activation	On

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

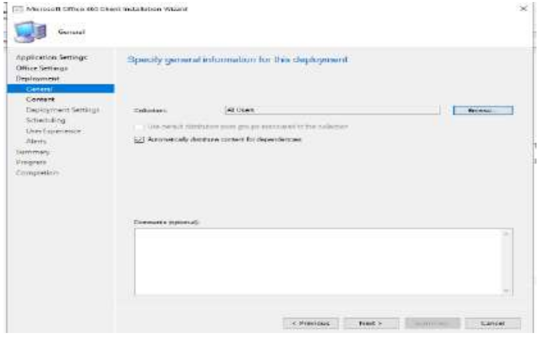


Deploy application now?

Do you want to deploy this application now?

● Yes
○ No

16 Select your collection and click next.



Specify general information for this deployment

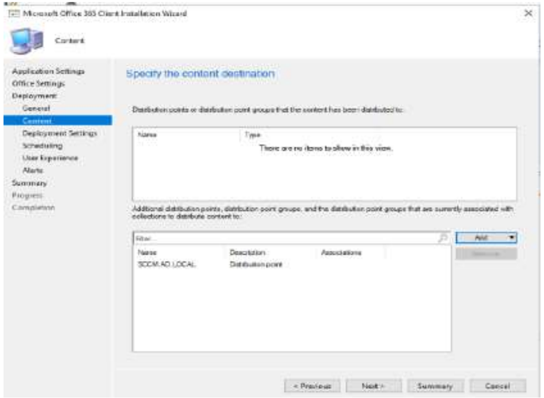
Collection: All Users

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies

Comments (optional):

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



Specify the content destination

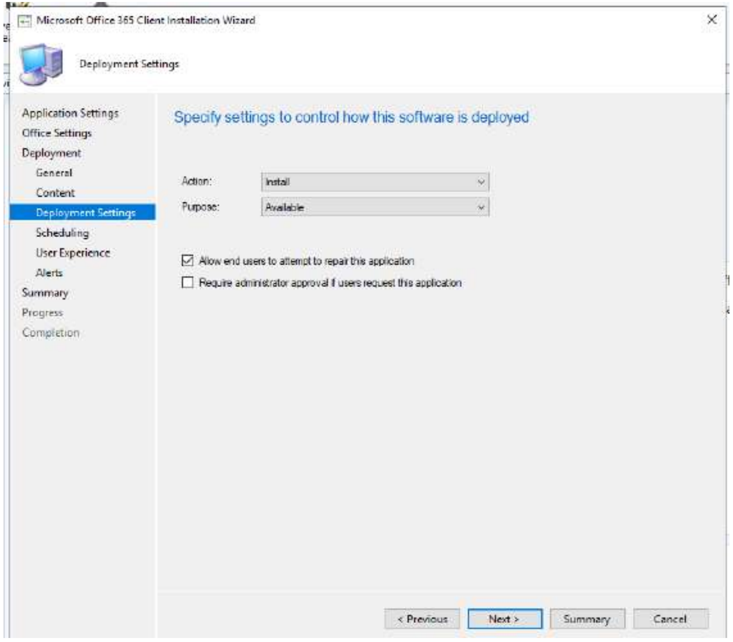
Distribution points or distribution point groups that the content has been distributed to:

Name	Type
There are no items to show in this view.	

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Name	Description	Associations
SCCM.AD.LOCAL	Distribution point	

18 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.



Microsoft Office 365 Client Installation Wizard

Deployment Settings

Specify settings to control how this software is deployed

Action: Install

Purpose: Available

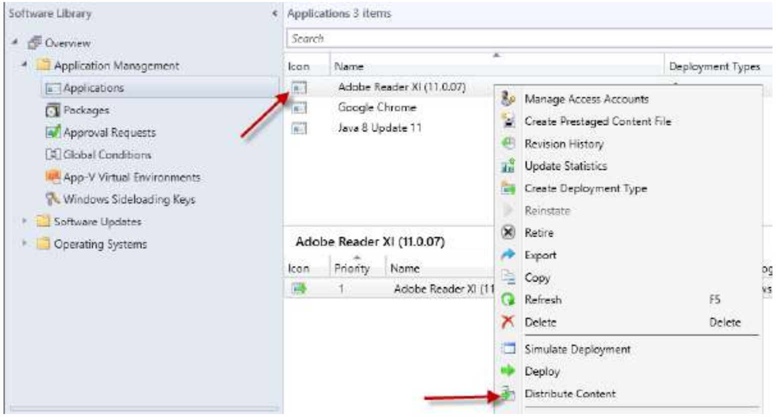
☑ Allow end users to attempt to repair this application

☐ Require administrator approval if users request this application

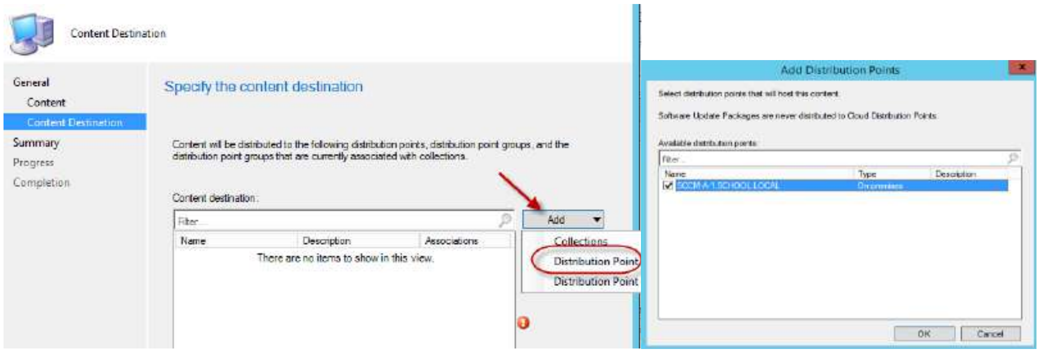
5.4 Distribute Software Application

1 In the Configuration Manager console, click **Software Library**

2 In the **Software Library** workspace, expand **Application Management**, and then Right Click **Adobe Reader Application**, Select **Distribute Content**



3 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



Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

Content destination:

Name	Description	Associations
There are no items to show in this view.		

Select distribution points that will host this content.

Software Update Packages are never distributed to Cloud Distribution Points.

Available distribution points:

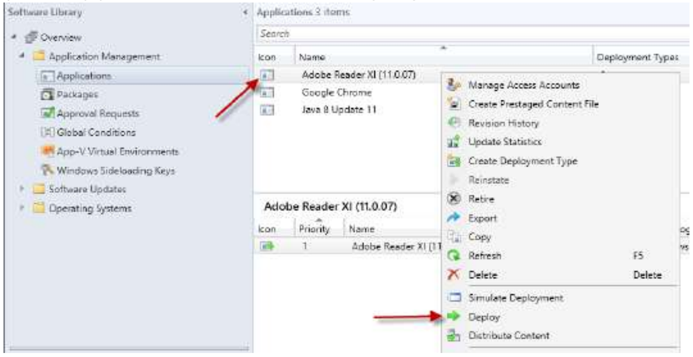
Name	Type	Description
☑ SCCM-A-1.SCHOOL.LOCAL	On-premises	

4 **Next** and **Finish**.

5.5 Deploy Software Application

1 In the Configuration Manager console, click **Software Library**

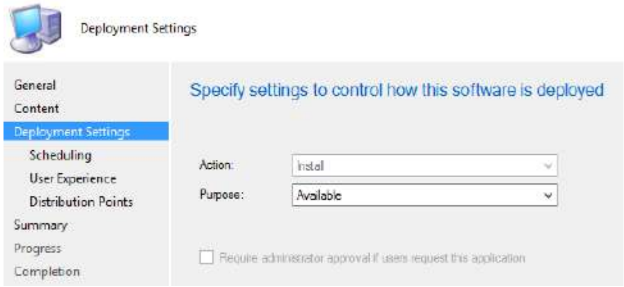
2 In the **Software Library** workspace, expand **Application Management**, and then Right Click your Application and Select **Deploy**



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.



Specify settings to control how this software is deployed

Action: Install

Purpose: Available

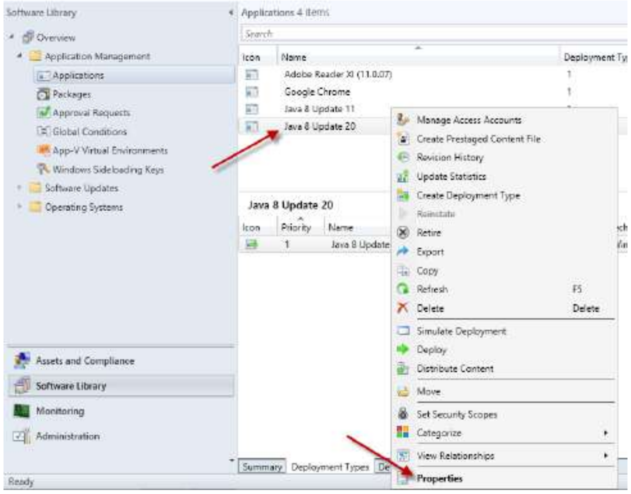
□ Require administrator approval if users request this application

5.6 Update / Supersede Application

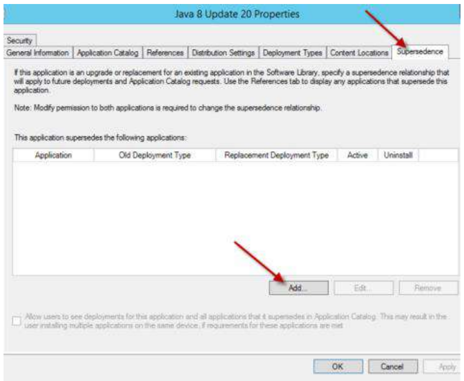
1 Create Software Application (See 5.3.1) for Latest Software Application.

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**.

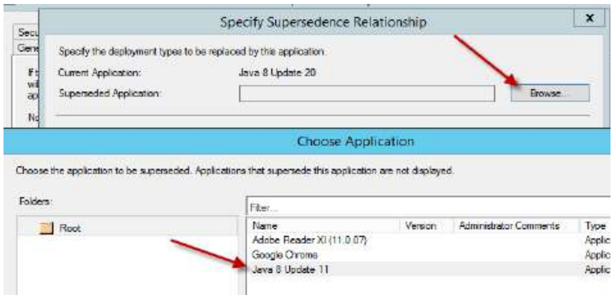


If this application is an upgrade or replacement for an existing application in the Software Library, specify a supersedence relationship that will apply to future deployments and Application Catalog requests. Use the References tab to display any applications that supersede this application.

Note: Modify permission to both applications is required to change the supersedence relationship.

This application supersedes the following applications:

□ Allow users to see deployments for this application and all applications that it supersedes in Application Catalog. This may result in the user installing multiple applications on the same device, if requirements for these applications are met.



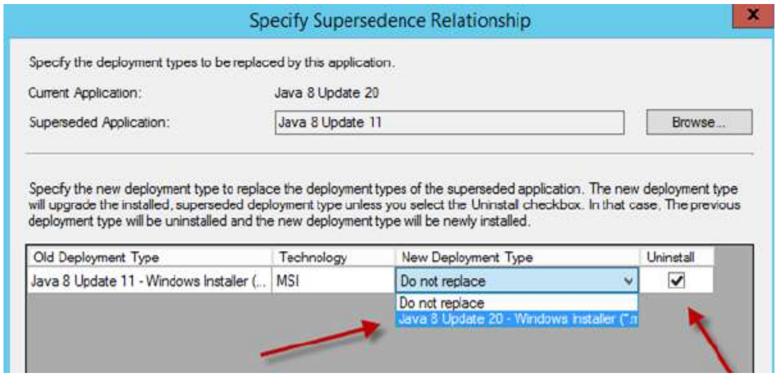
Specify the deployment types to be replaced by this application.

Current Application: Java 8 Update 20

Superseded Application:

Choose the application to be superseded. Applications that supersede this application are not displayed.

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**.


Specify Supersedence Relationship

Specify the deployment types to be replaced by this application.

Current Application: Java 8 Update 20

Superseded Application: Java 8 Update 11

Specify the new deployment type to replace the deployment types of the superseded application. The new deployment type will upgrade the installed, superseded deployment type unless you select the Uninstall checkbox. In that case, The previous deployment type will be uninstalled and the new deployment type will be newly installed.

Old Deployment Type	Technology	New Deployment Type	Uninstall
Java 8 Update 11 - Windows Installer (...	MSI	Do not replace	☑

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.**

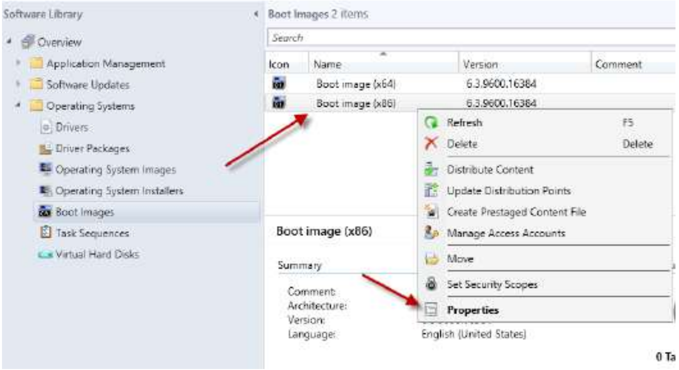
2 Copy **install.wim** file for Windows 10 x64, which is present on the Windows 10 DVD under the **Sources** folder.

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**.


Boot Images 2 items

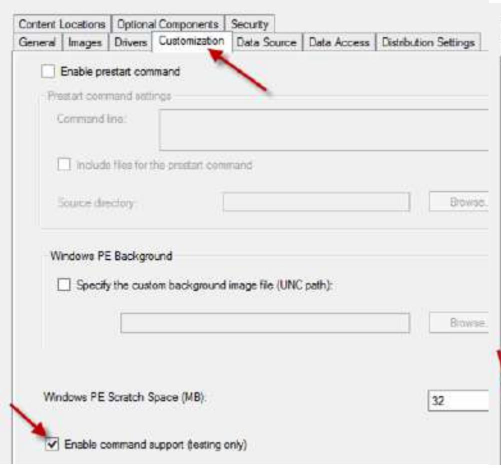
Icon	Name	Version	Comment
	Boot image (x64)	6.3.9600.16384	
	Boot image (x86)	6.3.9600.16384	

Boot image (x86)

Summary

Comment:
Architecture:
Version:
Language: English (United States)

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



☐ Enable prestart command

Prestart command settings

Command line:

☐ Include files for the prestart command

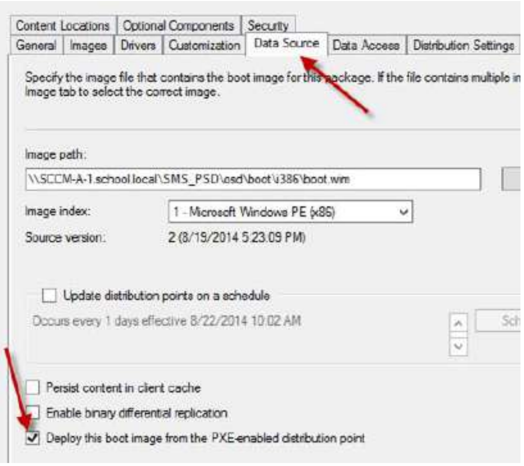
Source directory:

Windows PE Background

☐ Specify the custom background image file (UNC path):

Windows PE Scratch Space (MB): 32

☑ Enable command support (testing only)



Specify the image file that contains the boot image for this package. If the file contains multiple in Image tab to select the correct image.

Image path: \\SCCM-A-1.school.local\SMS_PSD\osd\boot\i386\boot.wim

Image index: 1 - Microsoft Windows PE (x86)

Source version: 2 (8/19/2014 5:23:09 PM)

☐ Update distribution points on a schedule

Occurs every 1 days effective 8/22/2014 10:02 AM

☐ Persist content in client cache

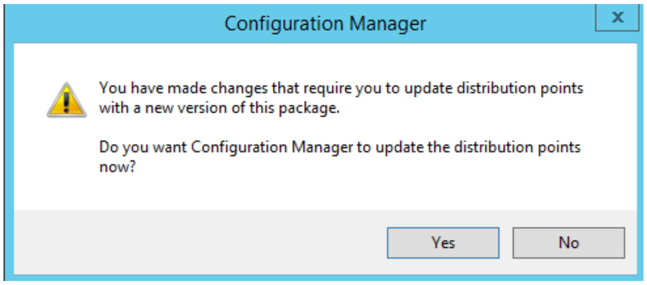
☐ Enable binary differential replication

☑ Deploy this boot image from the PXE-enabled distribution point

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**.

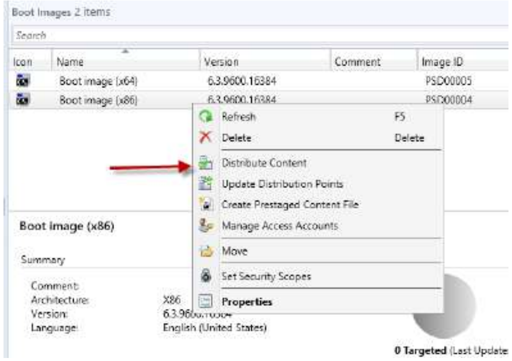
6 When prompted to update the Distribution Points, click **Yes** and then **OK** to close.



You have made changes that require you to update distribution points with a new version of this package.

Do you want Configuration Manager to update the distribution points now?

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



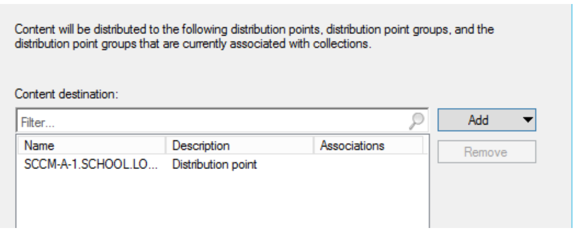
Icon	Name	Version	Comment	Image ID
	Boot image (x64)	6.3.9600.16384		PSD00005
	Boot image (x86)	6.3.9600.16384		PSD00004

Boot image (x86)

Summary

Comment:
Architecture: X86
Version: 6.3.9600.16384
Language: English (United States)

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



Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

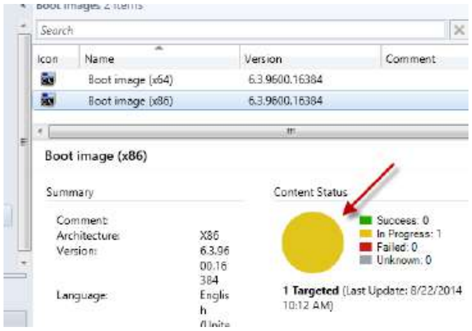
Content destination:

Name	Description	Associations
SCCM-A-1.SCHOOL.LO...	Distribution point	

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

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

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



Boot Images 2 items

Icon	Name	Version	Comment
	Boot image (x64)	6.3.9600.16384	
	Boot image (x86)	6.3.9600.16384	

Boot image (x86)

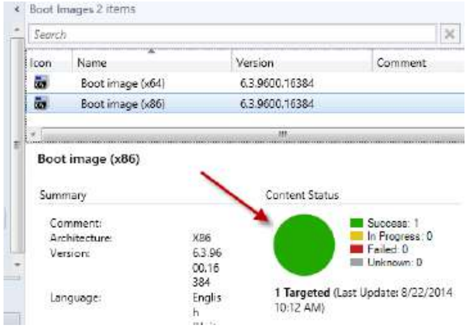
Summary

Comment:
Architecture: X86
Version: 6.3.9600.16384
Language: English (Unite

Content Status

🟩 Success: 0
🟨 In Progress: 1
🟥 Failed: 0
▨ Unknown: 0

1 Targeted (Last Update: 8/22/2014 10:12 AM)



Boot Images 2 items

Icon	Name	Version	Comment
	Boot image (x64)	6.3.9600.16384	
	Boot image (x86)	6.3.9600.16384	

Boot image (x86)

Summary

Comment:
Architecture: X86
Version: 6.3.9600.16384
Language: English

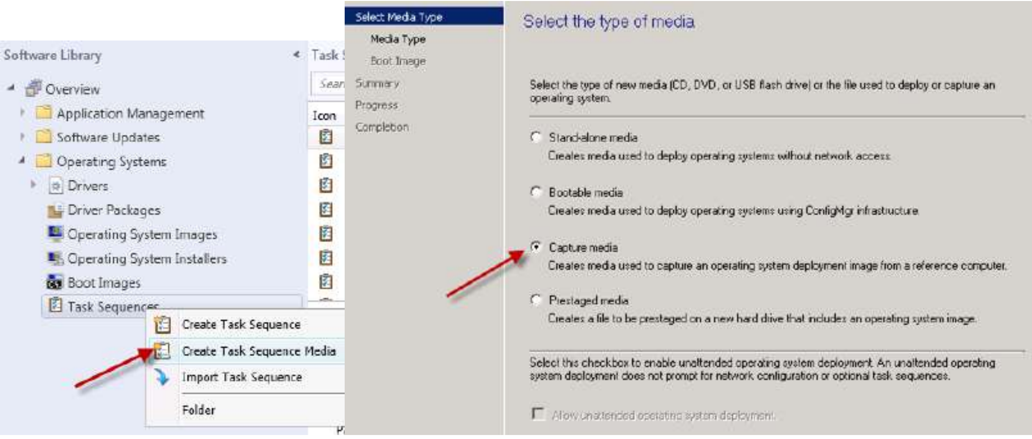
Content Status

🟩 Success: 1
🟨 In Progress: 0
🟥 Failed: 0
▨ Unknown: 0

1 Targeted (Last Update: 8/22/2014 10:12 AM)

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



Select the type of media

Select the type of new media (CD, DVD, or USB flash drive) or the file used to deploy or capture an operating system.

○ Stand-alone media
Creates media used to deploy operating systems without network access.

○ Bootable media
Creates media used to deploy operating systems using ConfigMgr infrastructure.

● Capture media
Creates media used to capture an operating system deployment image from a reference computer.

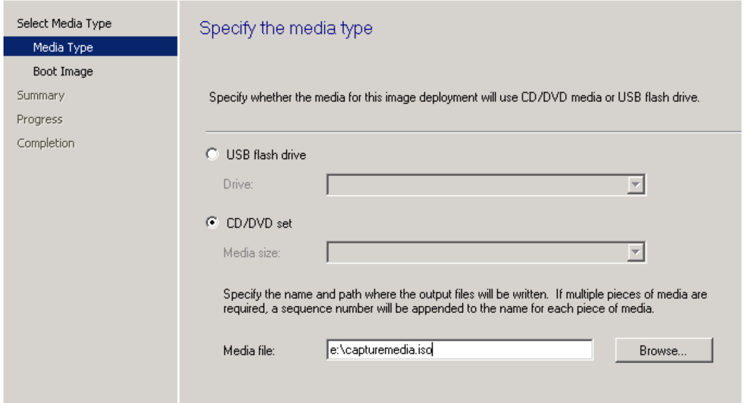
○ Prestaged media
Creates a file to be prestaged on a new hard drive that includes an operating system image.

Select this checkbox to enable unattended operating system deployment. An unattended operating system deployment does not prompt for network configuration or optional task sequences.

□ Allow unattended operating system deployment.

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.



Specify the media type

Specify whether the media for this image deployment will use CD/DVD media or USB flash drive.

○ USB flash drive

Drive:

● CD/DVD set

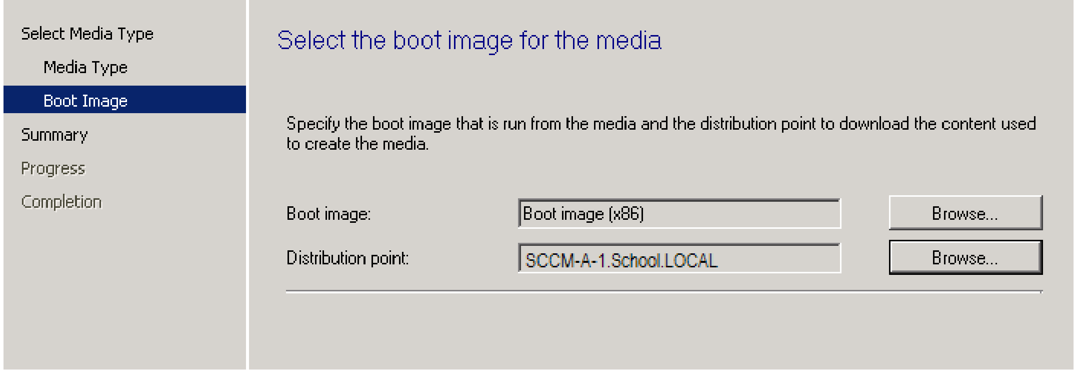
Media size:

Specify the name and path where the output files will be written. If multiple pieces of media are required, a sequence number will be appended to the name for each piece of media.

Media file: e:\capturemedia.iso

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.



Select the boot image for the media

Specify the boot image that is run from the media and the distribution point to download the content used to create the media.

Boot image: Boot image (x86)

Distribution point: SCCM-A-1.School.LOCAL

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

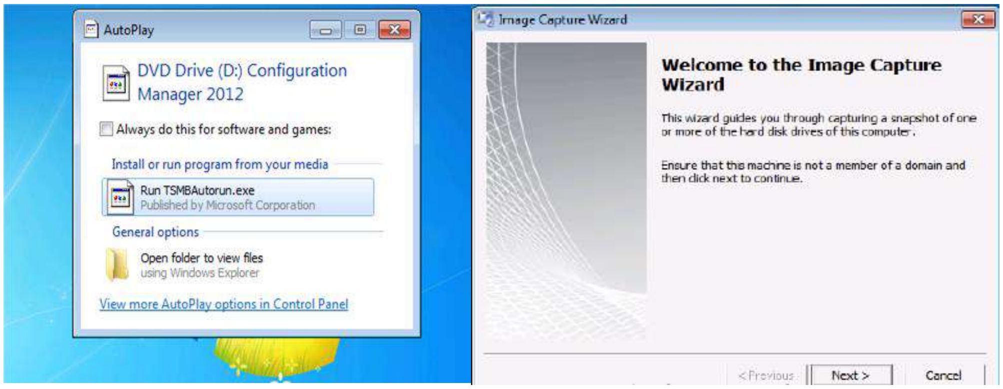
7.b Click on change settings to the right of the Computer Name

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


AutoPlay
DVD Drive (D:) Configuration Manager 2012
Always do this for software and games:
Install or run program from your media
Run TSMBAutorun.exe
Published by Microsoft Corporation
General options
Open folder to view files
using Windows Explorer
View more AutoPlay options in Control Panel
Image Capture Wizard

Welcome to the Image Capture Wizard

This wizard guides you through capturing a snapshot of one or more of the hard disk drives of this computer.

Ensure that this machine is not a member of a domain and then click next to continue.

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

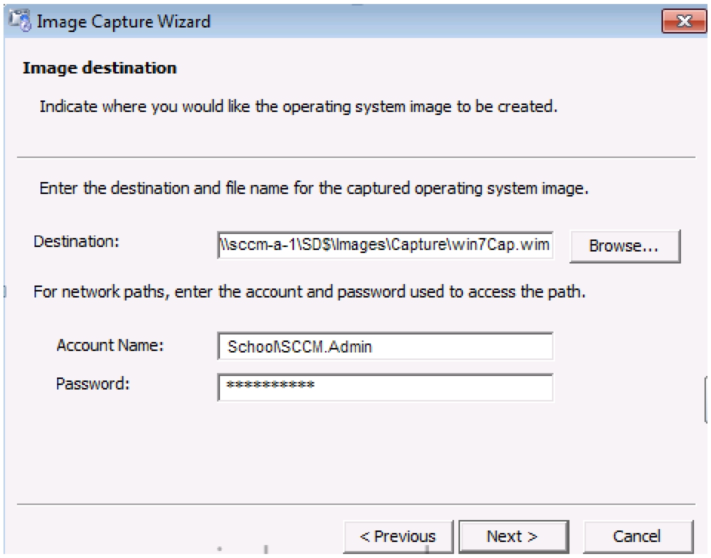


Image Capture Wizard

Image destination

Indicate where you would like the operating system image to be created.

Enter the destination and file name for the captured operating system image.

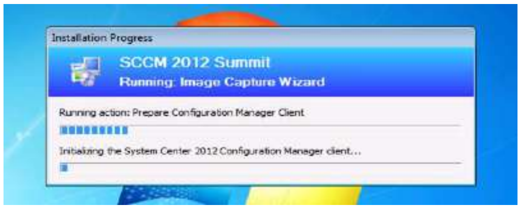
Destination: \\sccm-a-1\SD$\Images\Capture\win7Cap.wim

For network paths, enter the account and password used to access the path.

Account Name: School\SCCM.Admin

Password: ***********

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



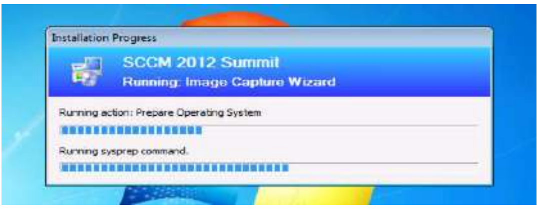
Installation Progress

SCCM 2012 Summit

Running: Image Capture Wizard

Running action: Prepare Configuration Manager Client

Initializing the System Center 2012 Configuration Manager client...



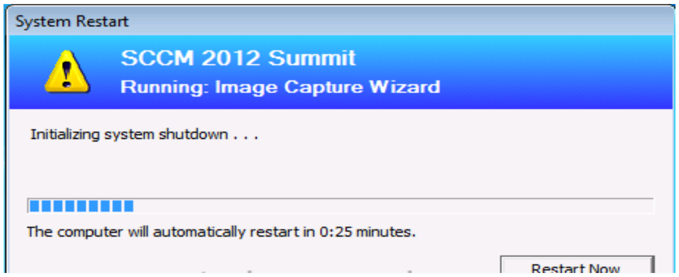
Installation Progress

SCCM 2012 Summit

Running: Image Capture Wizard

Running action: Prepare Operating System

Running sysprep command.



System Restart

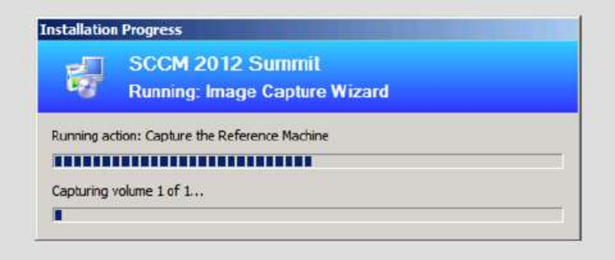
SCCM 2012 Summit

Running: Image Capture Wizard

Initializing system shutdown . . .

The computer will automatically restart in 0:25 minutes.

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.


Installation Progress

SCCM 2012 Summit

Running: Image Capture Wizard

Running action: Capture the Reference Machine

Capturing volume 1 of 1...

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.

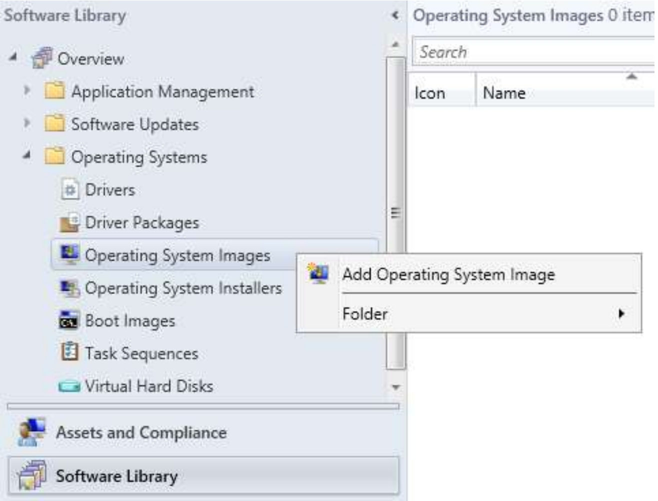
13 Once the workstation has finished the capture process there will be a win10cap.wim file located on the SCCM server that you can Create an Operating System Image and a Task Sequence to be deployed.

6.4 Add Operating System DVD Image (Install.WIM)

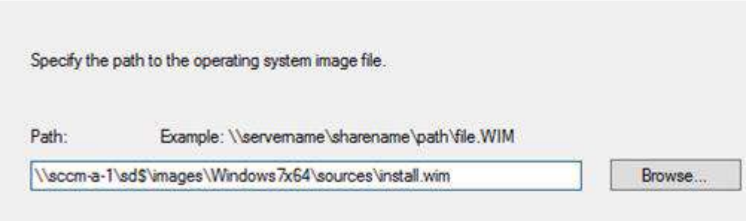
This will be the **install.wim** image file copied from the Windows 7 or Windows 8 DVD.

1 In the SCCM Console, click on **Software Library**.

2 Expand **Operating Systems**, right-click **Operating System Images** and choose **Add Operating System Image**.



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

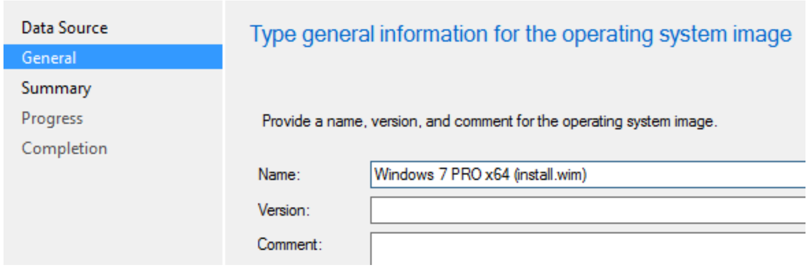


Specify the path to the operating system image file.

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

\\sccm-a-1\sd$\images\Windows7x64\sources\install.wim

4 Enter the **Name**, **Version** number, **Comment** and complete the wizard. Make sure the name is discriptive enough to know what this image contains.
Windows 10 x64 (install.wim)



Type general information for the operating system image

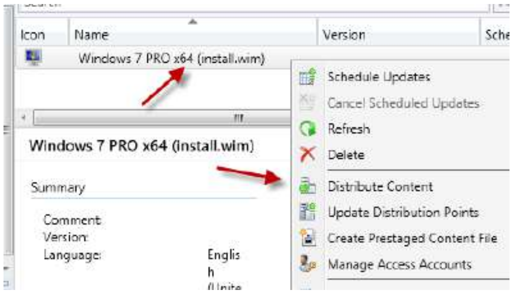
Provide a name, version, and comment for the operating system image.

Name: Windows 7 PRO x64 (install.wim)

Version:

Comment:

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



Icon	Name	Version	Sche
	Windows 7 PRO x64 (install.wim)		

Windows 7 PRO x64 (install.wim)

Summary

Comment:
Version:
Language: English (Unite

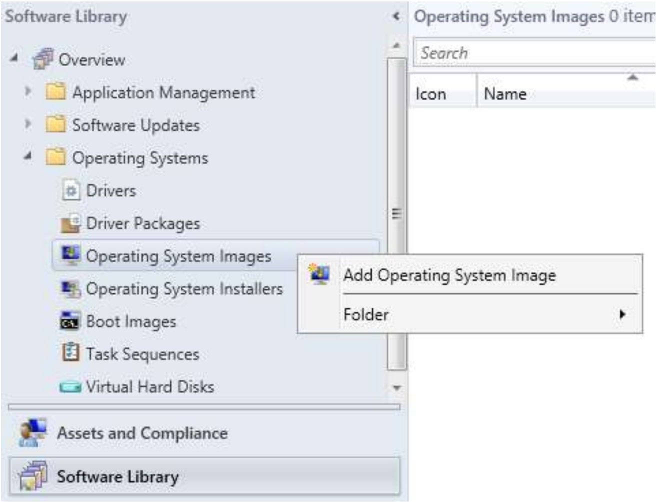
6 **Repeat** steps for each **Version** of Windows you intend to deploy.

6.5 Add Operating System Captured Image (CapturedWindows10.WIM)

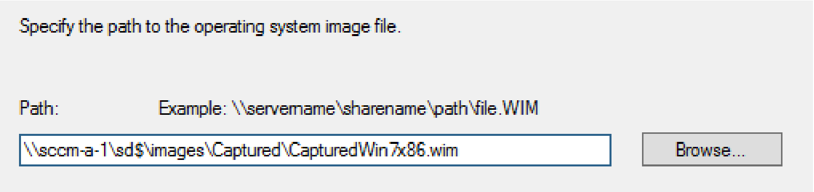
This will be the image file captured from the WDS or SCCM Capture Process.

7 In the SCCM Console, click on **Software Library**.

8 Expand **Operating Systems**, right-click **Operating System Images** and choose **Add Operating System Image**.



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

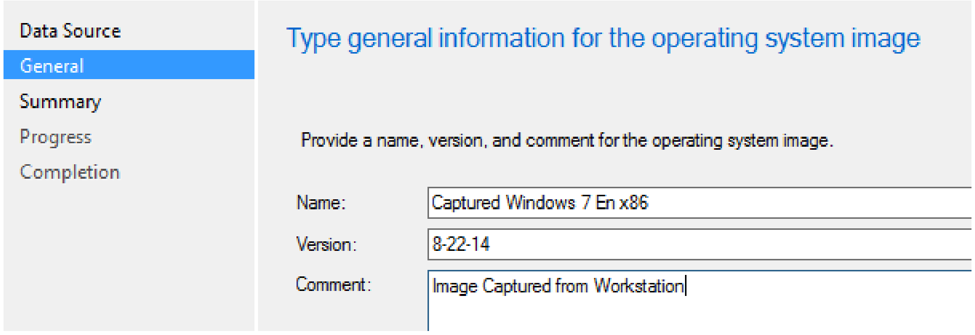


Specify the path to the operating system image file.

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

\\sccm-a-1\sd$\images\Captured\CapturedWin7x86.wim

10 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 discriptive enough to know what this image contains. You will need these comment to know what imgaes are what in the future. Recommend that you put the date the image was captured.



Type general information for the operating system image

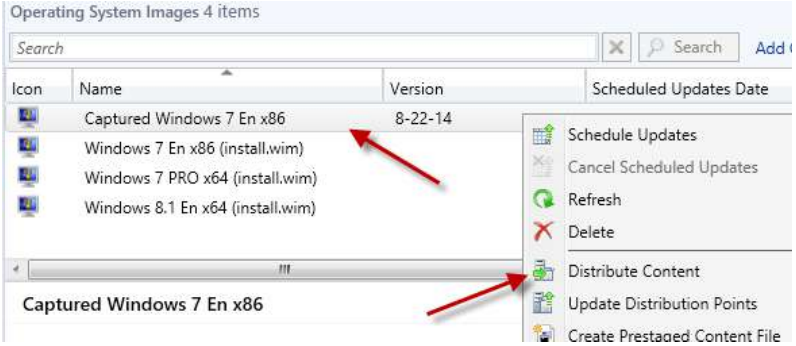
Provide a name, version, and comment for the operating system image.

Name: Captured Windows 7 En x86

Version: 8-22-14

Comment: Image Captured from Workstation

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



Operating System Images 4 items

Icon	Name	Version	Scheduled Updates Date
	Captured Windows 7 En x86	8-22-14	
	Windows 7 En x86 (install.wim)		
	Windows 7 PRO x64 (install.wim)		
	Windows 8.1 En x64 (install.wim)		

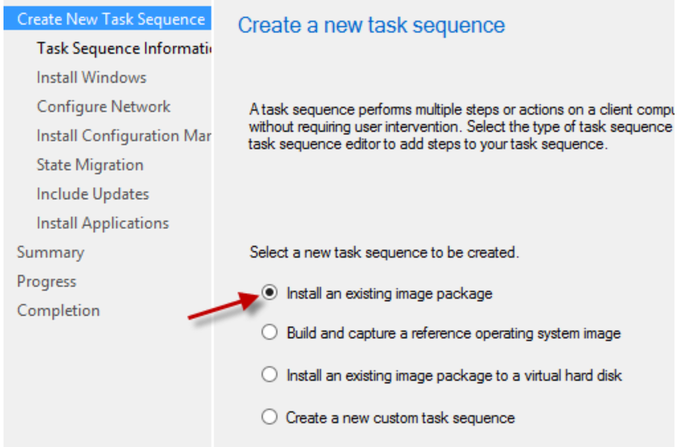
Captured Windows 7 En x86

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**



Create a new task sequence

A task sequence performs multiple steps or actions on a client compu
without requiring user intervention. Select the type of task sequence
task sequence editor to add steps to your task sequence.

Select a new task sequence to be created.

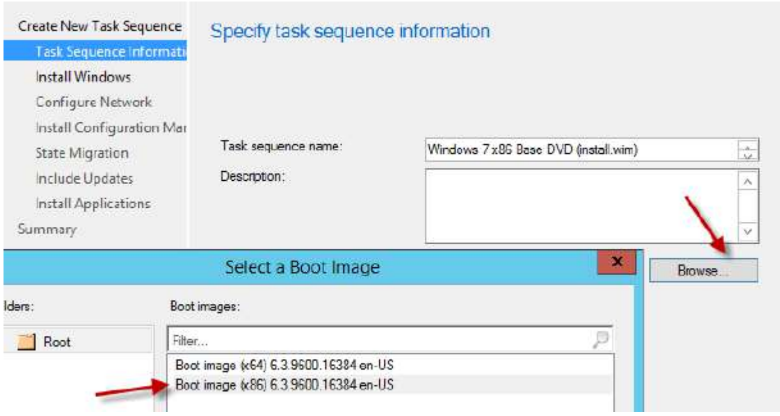
● Install an existing image package

○ Build and capture a reference operating system image

○ Install an existing image package to a virtual hard disk

○ Create a new custom task sequence

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



Specify task sequence information

Task sequence name: Windows 7x86 Base DVD (install.wim)

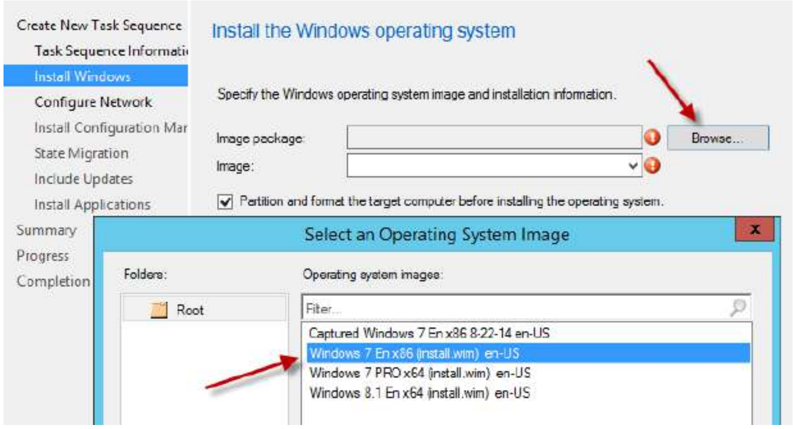
Description:

Boot images:

Boot image (x64) 6.3.9600.16384 en-US

Boot image (x86) 6.3.9600.16384 en-US

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



Install the Windows operating system

Specify the Windows operating system image and installation information.

Image package:

Image:

☑ Partition and format the target computer before installing the operating system.

Select an Operating System Image

Folders:

Operating system images:

Filter...

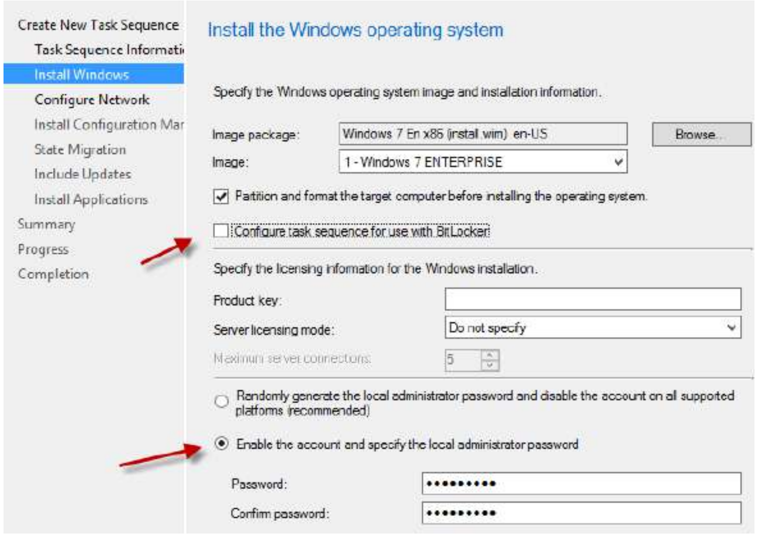
Captured Windows 7 En x86 8-22-14 en-US

Windows 7 En x86 (install.wim) en-US

Windows 7 PRO x64 (install.wim) en-US

Windows 8.1 En x64 (install.wim) en-US

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**.



Install the Windows operating system

Specify the Windows operating system image and installation information.

Image package: Windows 7 En x86 (install.wim) en-US

Image: 1 - Windows 7 ENTERPRISE

☑ Partition and format the target computer before installing the operating system.

□ Configure task sequence for use with BitLocker

Specify the licensing information for the Windows installation.

Product key:

Server licensing mode: Do not specify

Maximum server connections: 5

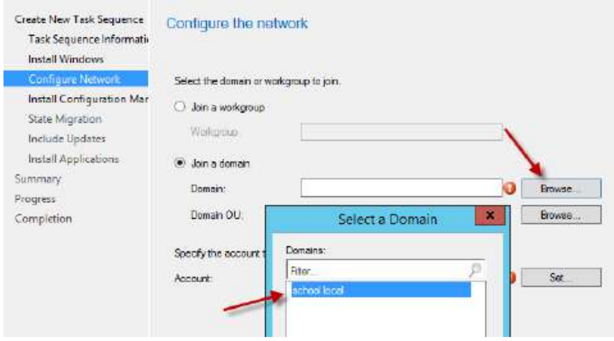
○ Randomly generate the local administrator password and disable the account on all supported platforms (recommended)

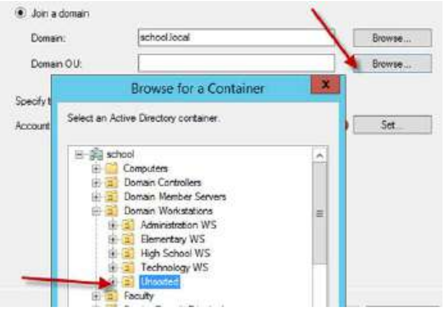
● Enable the account and specify the local administrator password

Password: •••••••••

Confirm password: •••••••••

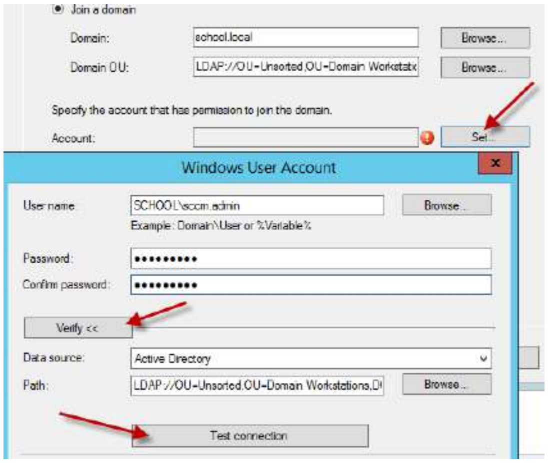
7 On the **Configure Network** screen, select **Join a Domain** and click **Browse** for **Domain** and select **<YOUR_DOMAIN>.local**, click **OK**. Select Browse for Domain OU and select Domain Workstations\Unsorted and Click OK.





Domain: school.local

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



Domain: school.local

Domain OU: LDAP://OU=Unsorted,OU=Domain Workstatic

User name: SCHOOL\sccm.admin

Password: •••••••••

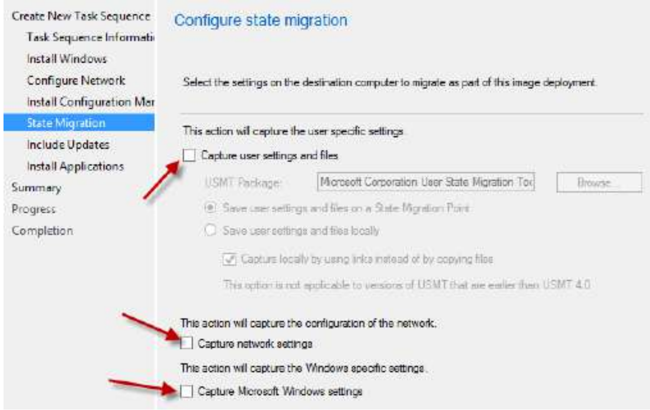
Confirm password: •••••••••

Data source: Active Directory

Path: LDAP://OU=Unsorted,OU=Domain Workstations,D

*****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**.



Select the settings on the destination computer to migrate as part of this image deployment.

This action will capture the user specific settings

☐ Capture user settings and files

USMT Package: Microsoft Corporation User State Migration Too

● Save user settings and files on a State Migration Point

○ Save user settings and files locally

☑ Capture locally by using links instead of by copying files

This option is not applicable to versions of USMT that are earlier than USMT 4.0

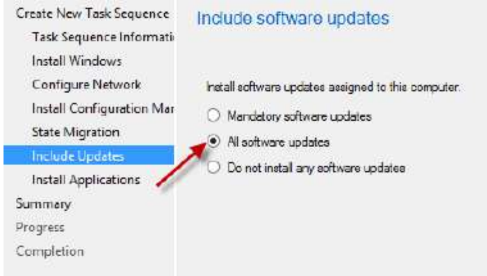
This action will capture the configuration of the network.

☐ Capture network settings

This action will capture the Windows specific settings.

☐ Capture Microsoft Windows settings

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



Include software updates

Install software updates assigned to this computer.

○ Mandatory software updates

● All software updates

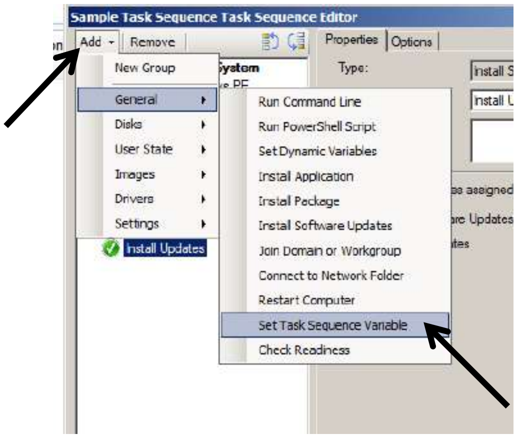
○ Do not install any software updates

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

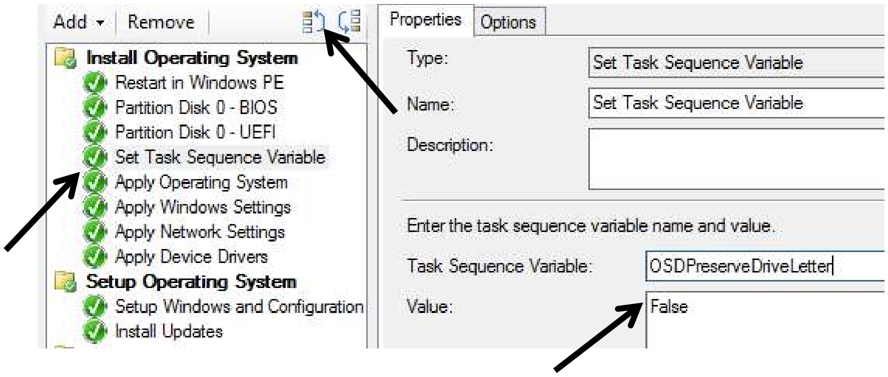
12 Right-click the newly created Task Sequence and select **Edit.**

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**.**



Type: Set Task Sequence Variable

Name: Set Task Sequence Variable

Description:

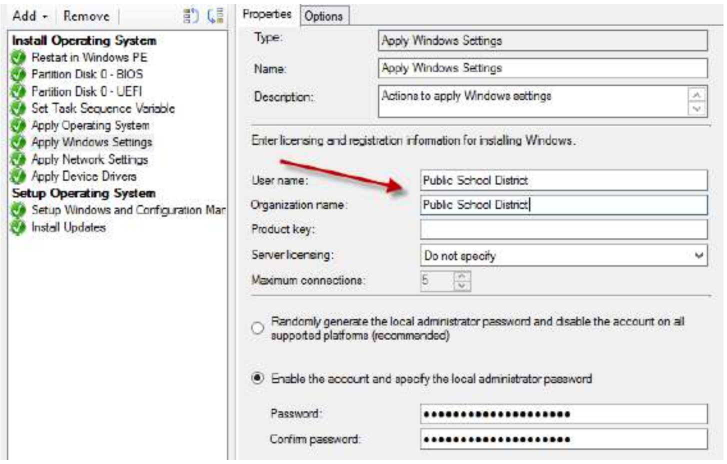
Enter the task sequence variable name and value.

Task Sequence Variable: OSDPreserveDriveLetter

Value: False

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

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



Type: Apply Windows Settings

Name: Apply Windows Settings

Description: Actions to apply Windows settings

Enter licensing and registration information for installing Windows.

User name: Public School District

Organization name: Public School District

Product key:

Server licensing: Do not specify

Maximum connections: 5

○ Randomly generate the local administrator password and disable the account on all supported platforms (recommended)

● Enable the account and specify the local administrator password

Password: ••••••••••••••••••••

Confirm password: ••••••••••••••••••••

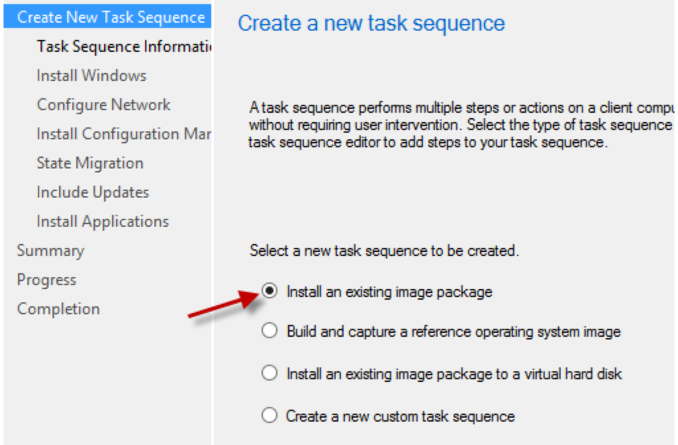
16 Click **Apply** and **OK** to save and close

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**



Create a new task sequence

A task sequence performs multiple steps or actions on a client compu without requiring user intervention. Select the type of task sequence task sequence editor to add steps to your task sequence.

Select a new task sequence to be created.

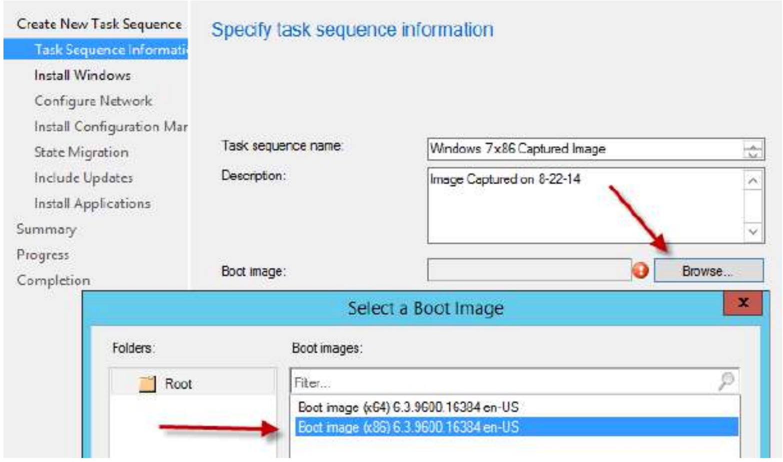
● Install an existing image package

○ Build and capture a reference operating system image

○ Install an existing image package to a virtual hard disk

○ Create a new custom task sequence

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



Specify task sequence information

Task sequence name: Windows 7x86 Captured Image

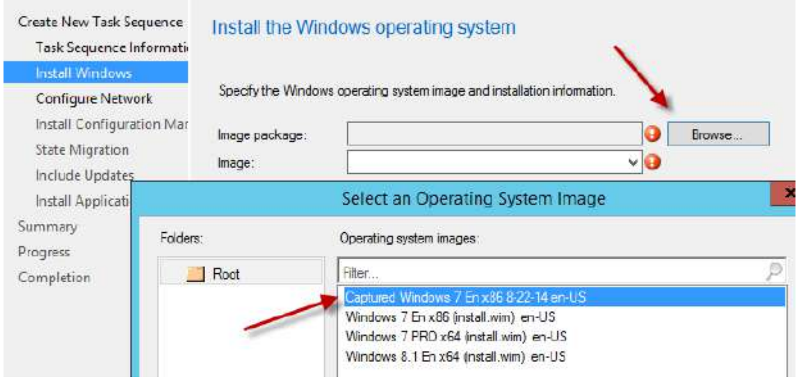
Description: Image Captured on 8-22-14

Boot image:

Boot image (x64) 6.3.9600.16384 en-US

Boot image (x86) 6.3.9600.16384 en-US

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



Install the Windows operating system

Specify the Windows operating system image and installation information.

Image package:

Image:

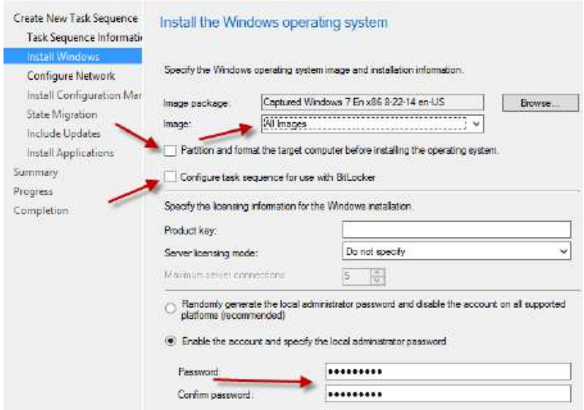
Captured Windows 7 En x86 8-22-14 en-US

Windows 7 En x86 (install.wim) en-US

Windows 7 PRO x64 (install.wim) en-US

Windows 8.1 En x64 (install.wim) en-US

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**.



Install the Windows operating system

Specify the Windows operating system image and installation information.

Image package: Captured Windows 7 En x86 8-22-14 en-US

Image: All Images

□ Partition and format the target computer before installing the operating system.

□ Configure task sequence for use with BitLocker

Specify the licensing information for the Windows installation.

Product key:

Server licensing mode: Do not specify

Maximum server connections: 5

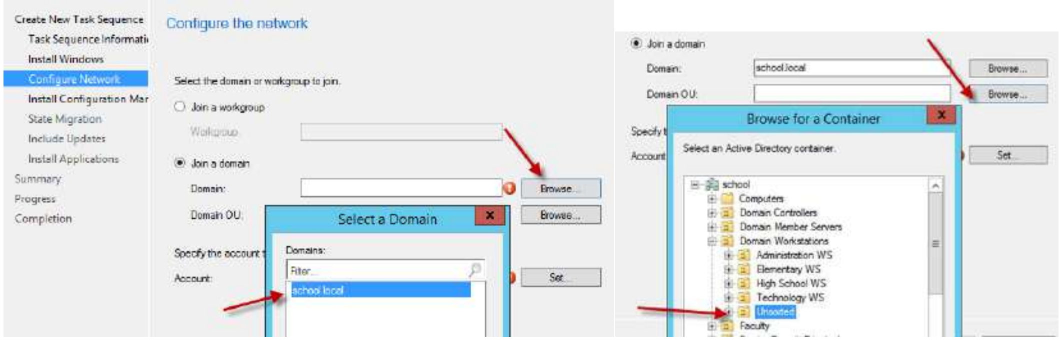
○ Randomly generate the local administrator password and disable the account on all supported platforms (recommended)

● Enable the account and specify the local administrator password

Password: •••••••••

Confirm password: •••••••••

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**.



Configure the network

Select the domain or workgroup to join.

○ Join a workgroup

Workgroup:

● Join a domain

Domain:

Domain OU:

Specify the account

Account:

Domains:

Filter...

school.local

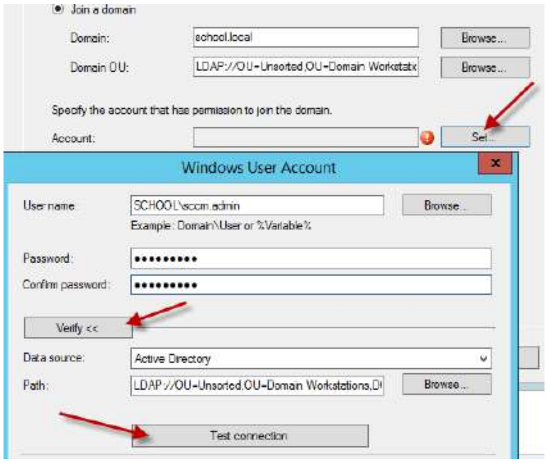
● Join a domain

Domain: school.local

Domain OU:

Select an Active Directory container.

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



● Join a domain

Domain: school.local

Domain OU: LDAP://OU=Unsorted,OU=Domain Workstatio

Specify the account that has permission to join the domain.

Account:

User name: SCHOOL\sccm.admin

Example: Domain\User or %Variable%

Password: •••••••••

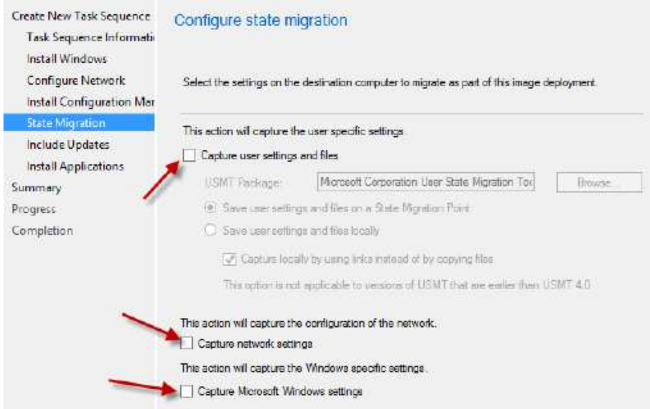
Confirm password: •••••••••

Data source: Active Directory

Path: LDAP://OU=Unsorted,OU=Domain Workstations,D

*****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**.



Configure state migration

Select the settings on the destination computer to migrate as part of this image deployment.

This action will capture the user specific settings.

□ Capture user settings and files

USMT Package: Microsoft Corporation User State Migration Too

● Save user settings and files on a State Migration Point

○ Save user settings and files locally

☑ Capture locally by using links instead of by copying files

This option is not applicable to versions of USMT that are earlier than USMT 4.0

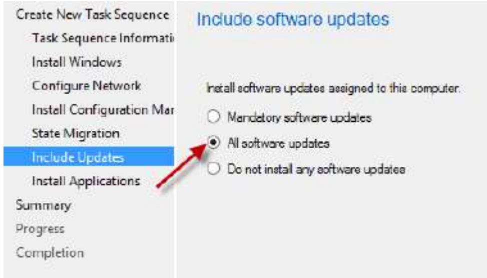
This action will capture the configuration of the network.

□ Capture network settings

This action will capture the Windows specific settings.

□ Capture Microsoft Windows settings

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



Include software updates

Install software updates assigned to this computer.

○ Mandatory software updates

● All software updates

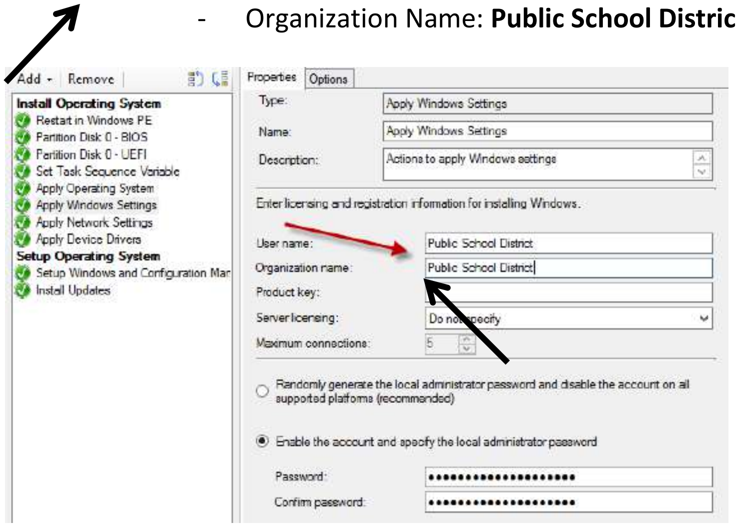
○ Do not install any software updates

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**



Type: Apply Windows Settings

Name: Apply Windows Settings

Description: Actions to apply Windows settings

Enter licensing and registration information for installing Windows.

User name: Public School District

Organization name: Public School District

Product key:

Server licensing: Do not specify

Maximum connections: 5

○ Randomly generate the local administrator password and disable the account on all supported platforms (recommended)

● Enable the account and specify the local administrator password

Password: ••••••••••••••••••••

Confirm password: ••••••••••••••••••••

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.

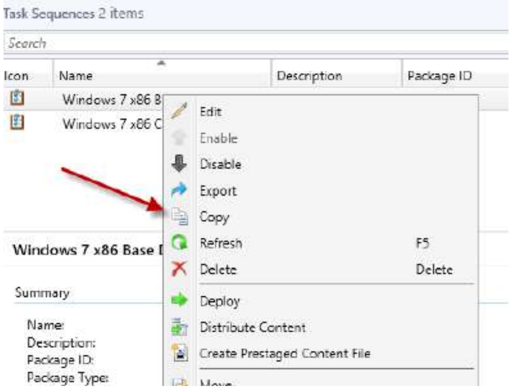
5 On the Deployment Settings screen, check the Make available to boot media and PXE and then click Next.

6 Click Next through the rest of the screens and complete the wizard

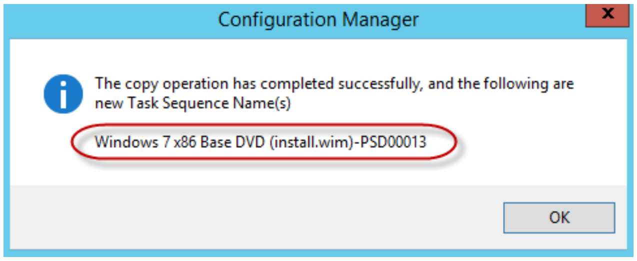
7 Add workstation objects you wish to image to the Windows Image Collection. Make sure the All Unknown Computer Collection is a member of this collection also.

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**.



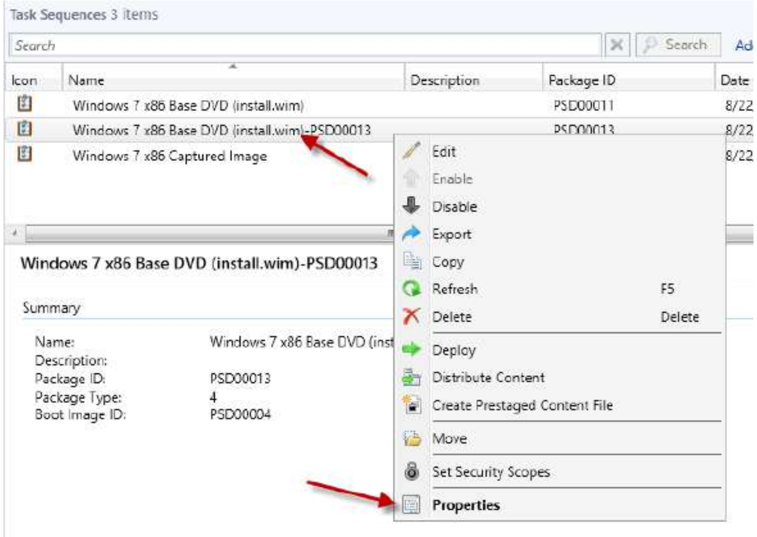
2 Click OK to confirm the copy was successful. Notice the name **Windows 7 x86 Base DVD (install.wim)-PSD00013**. This is the name of the new task sequesnce that was created.


Configuration Manager

The copy operation has completed successfully, and the following are new Task Sequence Name(s)

Windows 7 x86 Base DVD (install.wim)-PSD00013

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



Task Sequences 3 items

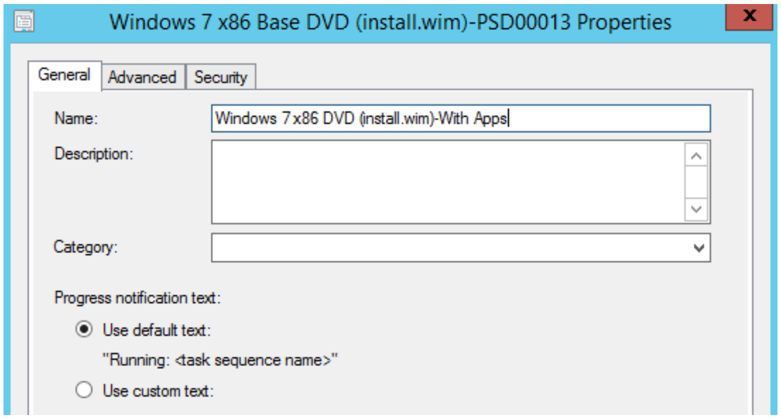
Icon	Name	Description	Package ID	Date
	Windows 7 x86 Base DVD (install.wim)		PSD00011	8/22
	Windows 7 x86 Base DVD (install.wim)-PSD00013		PSD00013	8/22
	Windows 7 x86 Captured Image			8/22

Windows 7 x86 Base DVD (install.wim)-PSD00013

Summary

Name:	Windows 7 x86 Base DVD (inst
Description:	
Package ID:	PSD00013
Package Type:	4
Boot Image ID:	PSD00004

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



Windows 7 x86 Base DVD (install.wim)-PSD00013 Properties

Name: Windows 7 x86 DVD (install.wim)-With Apps

Description:

Category:

Progress notification text:

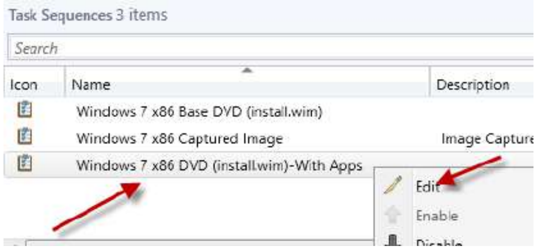
● Use default text:

"Running: <task sequence name>"

○ Use custom text:

5 Click **OK**.

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

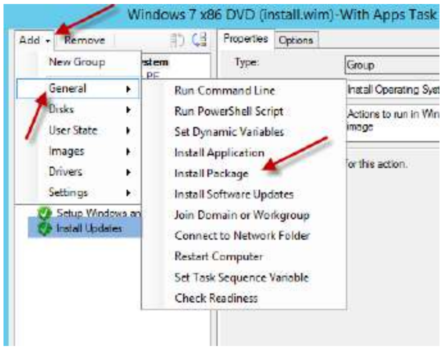


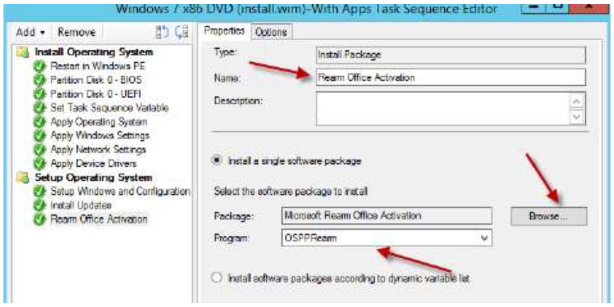
Task Sequences 3 items

Icon	Name	Description
	Windows 7 x86 Base DVD (install.wim)	
	Windows 7 x86 Captured Image	Image Capture
	Windows 7 x86 DVD (install.wim)-With Apps	

7 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





Type: Install Package

Name: Rearm Office Activation

Description:

● Install a single software package

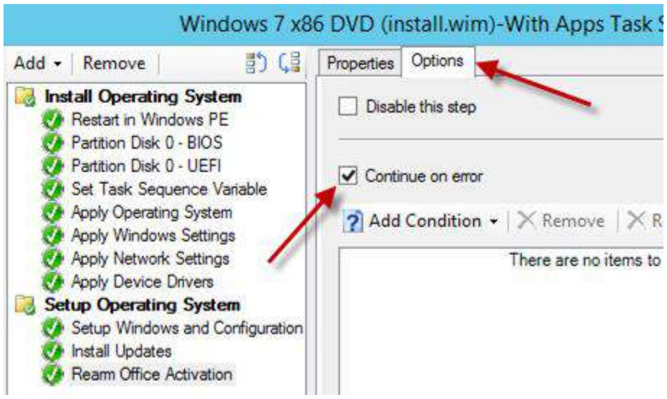
Select the software package to install

Package: Microsoft Rearm Office Activation

Program: OSPPRearm

○ Install software packages according to dynamic variable list

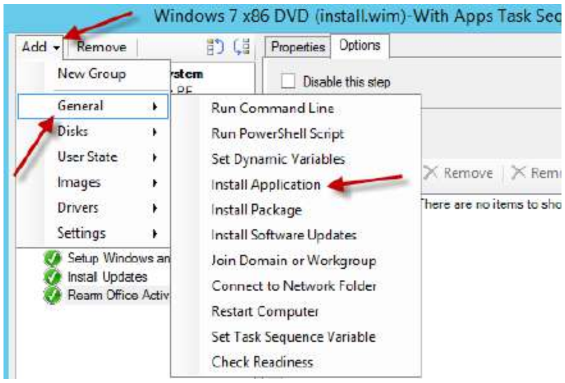
8 Click on the **Options** Tab and Check the box **Continue on error**.

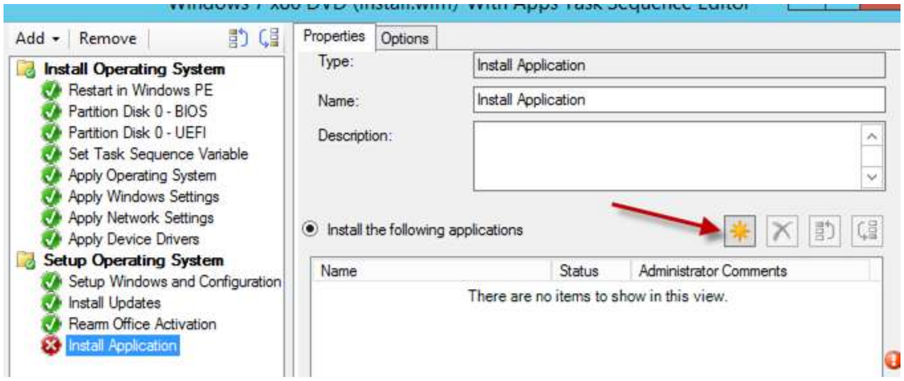


□ Disable this step

☑ Continue on error

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





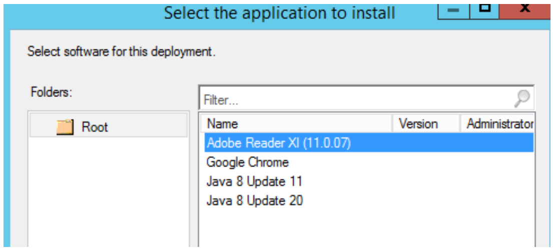
Type: Install Application

Name: Install Application

Description:

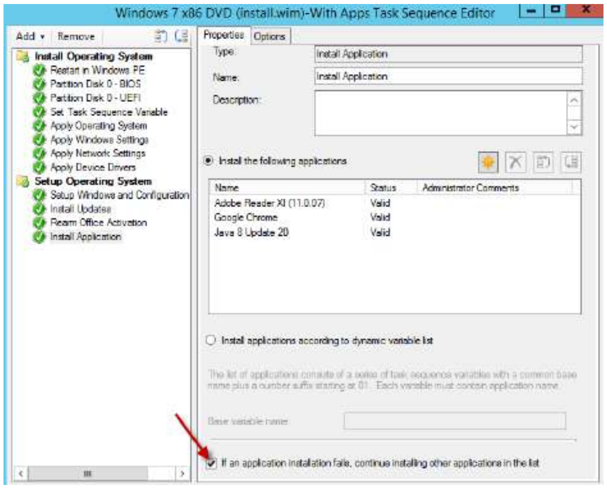
● Install the following applications

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.**



Select software for this deployment.

Name	Version	Administrator
Adobe Reader XI (11.0.07)		
Google Chrome		
Java 8 Update 11		
Java 8 Update 20		



Type: Install Application

Name: Install Application

Description:

● Install the following applications

Name	Status	Administrator Comments
Adobe Reader XI (11.0.07)	Valid	
Google Chrome	Valid	
Java 8 Update 20	Valid	

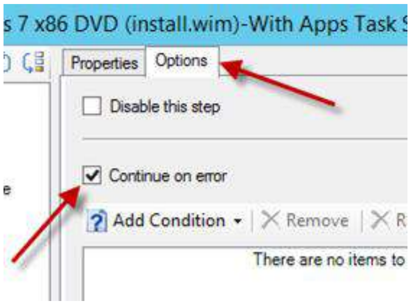
○ Install applications according to dynamic variable list

The list of applications consists of a series of task sequence variables with a common base name plus a number suffix starting at 01. Each variable must contain application name.

Base variable name:

☑ If an application installation fails, continue installing other applications in the list

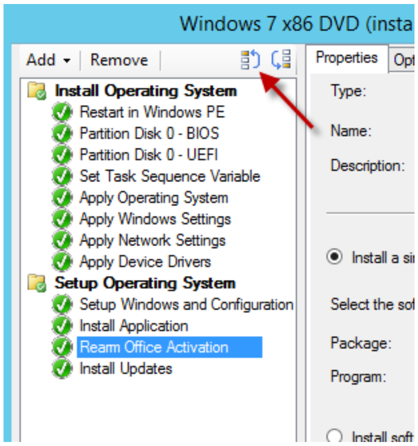
11 Click on the **Options** Tab and Check the box **Continue on error**.



□ Disable this step

☑ Continue on error

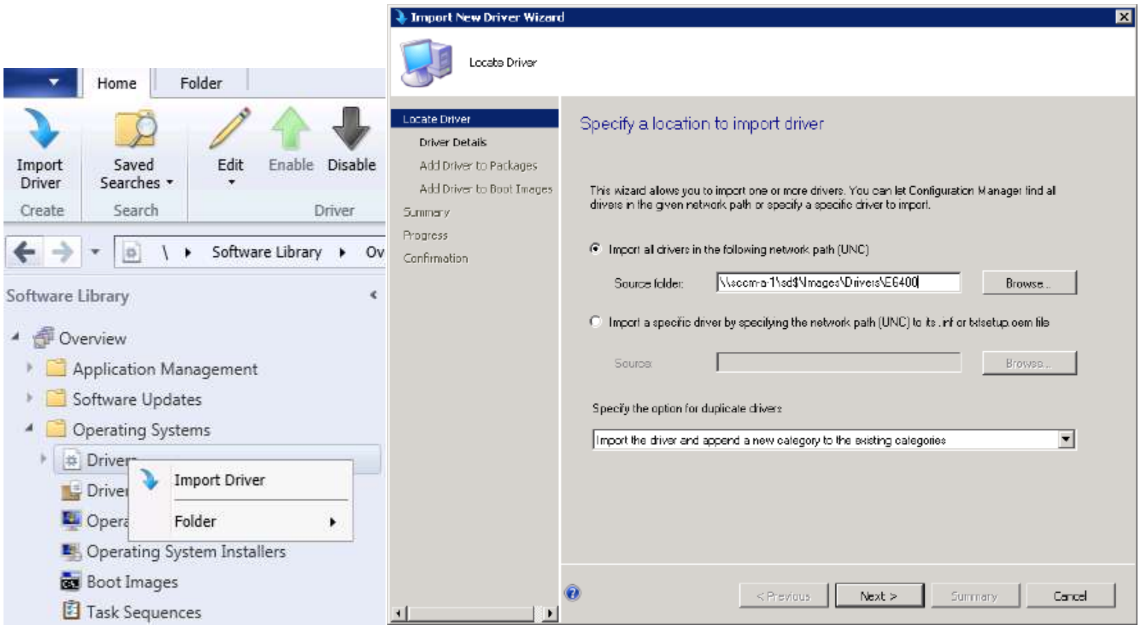
12 Use the button at the top to rearraing the tasks to have the Install Applications above Packages and Updates



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

6.10 Import Device Drivers

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



Specify a location to import driver

This wizard allows you to import one or more drivers. You can let Configuration Manager find all drivers in the given network path or specify a specific driver to import.

● Import all drivers in the following network path (UNC)

Source folder: \\sccm-a-1\sd$\Images\Drivers\E6400 Browse...

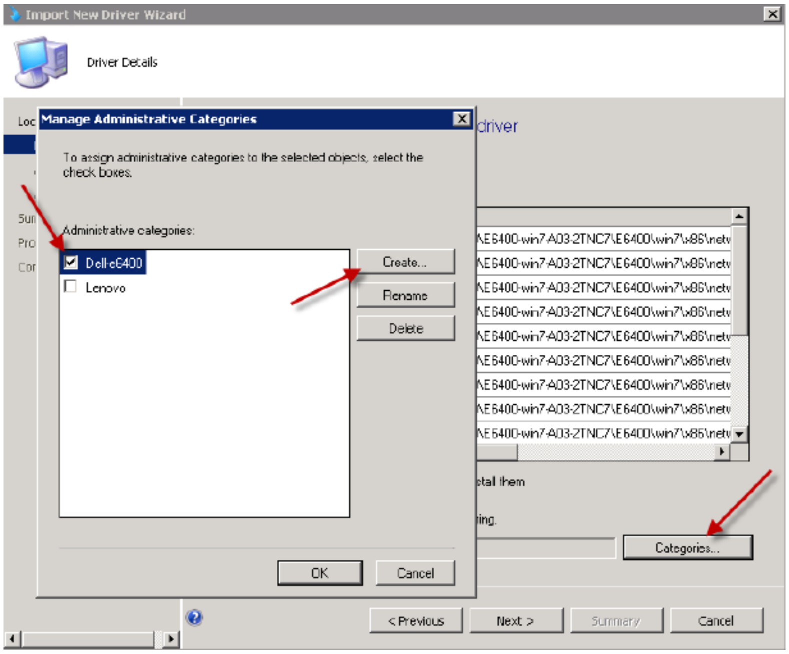
○ Import a specific driver by specifying the network path (UNC) to its .inf or txtsetup.oem file

Source: Browse...

Specify the option for duplicate drivers

Import the driver and append a new category to the existing categories

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



Import New Driver Wizard

Driver Details

Manage Administrative Categories

To assign administrative categories to the selected objects, select the check boxes.

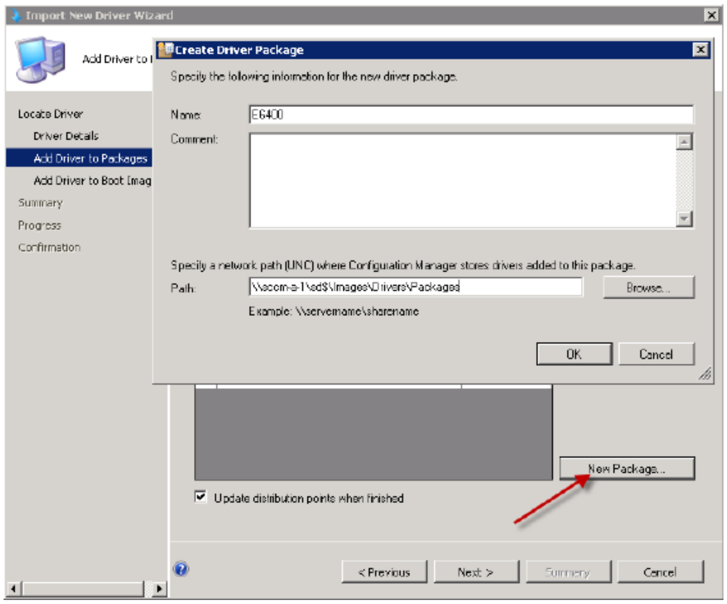
Administrative categories:

☑ Dell e6400

□ Lenovo

\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv
\E6400-win7-A03-2TNC7\E6400\win7\x86\netv

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**.



Import New Driver Wizard

Create Driver Package

Specify the following information for the new driver package.

Name: E6400

Comment:

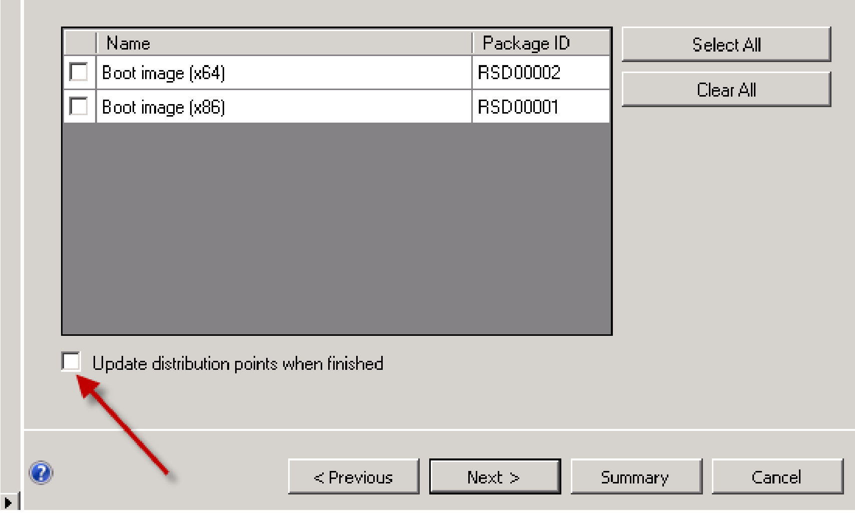
Specify a network path (UNC) where Configuration Manager stores drivers added to this package.

Path: \\sccm-a-1\sd$\Images\Drivers\Packages

Example: \\servername\sharename

☑ Update distribution points when finished

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.**



	Name	Package ID
□	Boot image (x64)	RSD00002
□	Boot image (x86)	RSD00001

□ Update distribution points when finished

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:

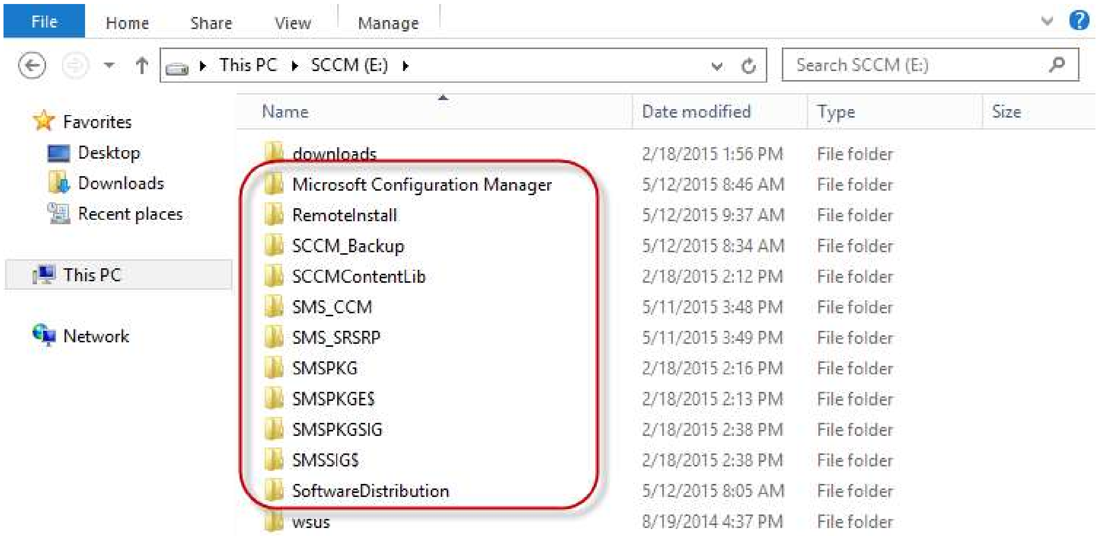
- SMS Writer service must be running for the process to complete successfully
- Backup schedule should be configured for an appropriate time that is outside active working hours to avoid any service disruptions.

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

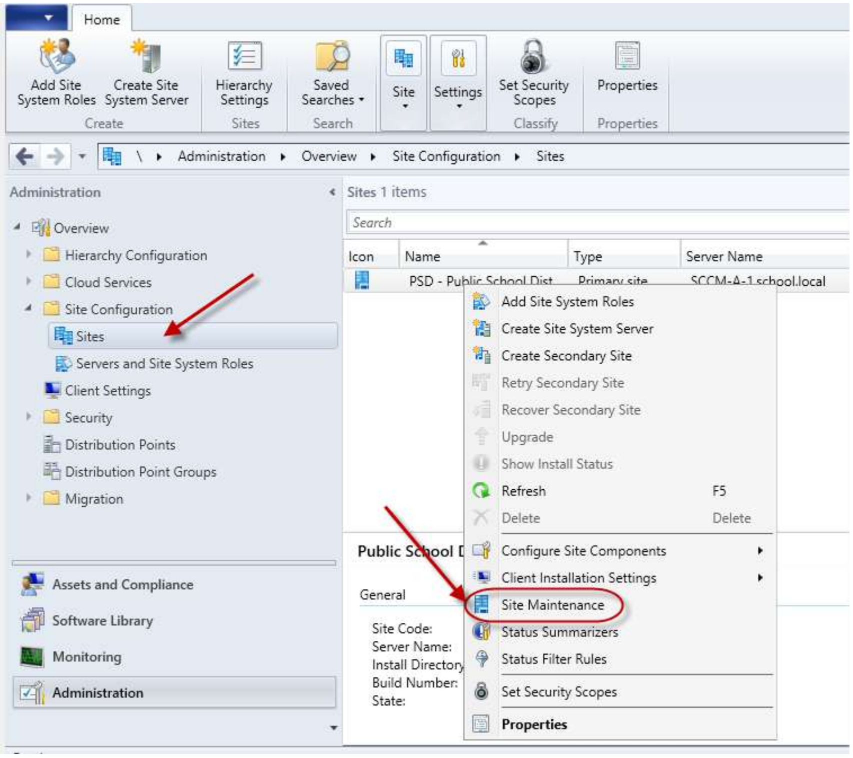


Name	Date modified	Type	Size
downloads	2/18/2015 1:56 PM	File folder	
Microsoft Configuration Manager	5/12/2015 8:46 AM	File folder	
RemoteInstall	5/12/2015 9:37 AM	File folder	
SCCM_Backup	5/12/2015 8:34 AM	File folder	
SCCMContentLib	2/18/2015 2:12 PM	File folder	
SMS_CCM	5/11/2015 3:48 PM	File folder	
SMS_SRSRP	5/11/2015 3:49 PM	File folder	
SMSPKG	2/18/2015 2:16 PM	File folder	
SMSPKGE$	2/18/2015 2:13 PM	File folder	
SMSPKGSIG	2/18/2015 2:38 PM	File folder	
SMSSIG$	2/18/2015 2:38 PM	File folder	
SoftwareDistribution	5/12/2015 8:05 AM	File folder	
wsus	8/19/2014 4:37 PM	File folder	

8.1 Backup SCCM Site Server

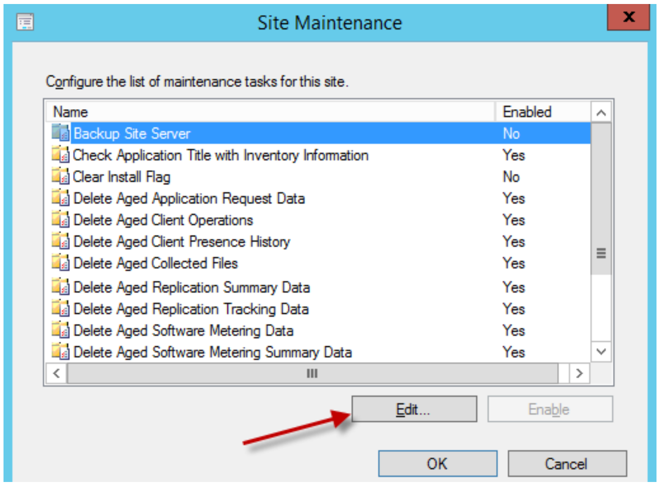
To configure the built-in Backup Site Server maintenance task, launch the SCCM management console. On the bottom left of the screen, select the **Administration** tab and expand **Overview**, if not already expanded. Expand **Site Configuration**, select **Sites** and on the right plane click on the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



Icon	Name	Type	Server Name
	PSD - Public School Dist...	Primary site	SCCM-A-1.school.local

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**.



Site Maintenance

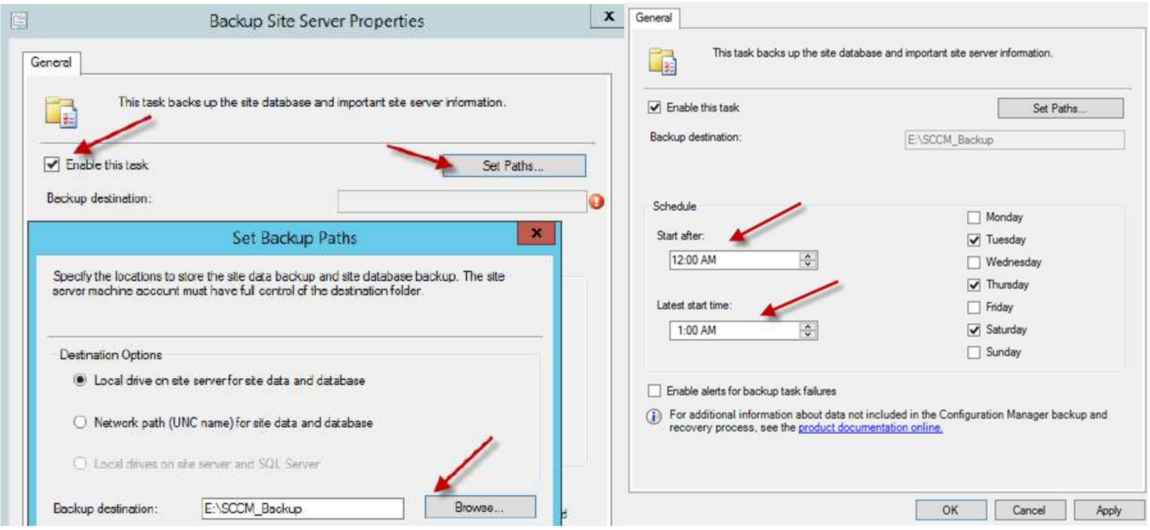
Configure the list of maintenance tasks for this site.

Name	Enabled
Backup Site Server	No
Check Application Title with Inventory Information	Yes
Clear Install Flag	No
Delete Aged Application Request Data	Yes
Delete Aged Client Operations	Yes
Delete Aged Client Presence History	Yes
Delete Aged Collected Files	Yes
Delete Aged Replication Summary Data	Yes
Delete Aged Replication Tracking Data	Yes
Delete Aged Software Metering Data	Yes
Delete Aged Software Metering Summary Data	Yes

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.***



Backup Site Server Properties

General

This task backs up the site database and important site server information.

☑ Enable this task

Backup destination:

Set Backup Paths

Specify the locations to store the site data backup and site database backup. The site server machine account must have full control of the destination folder.

Destination Options

● Local drive on site server for site data and database

○ Network path (UNC name) for site data and database

○ Local drives on site server and SQL Server

Backup destination: E:\SCCM_Backup

General

This task backs up the site database and important site server information.

☑ Enable this task

Backup destination: E:\SCCM_Backup

Schedule

Start after: 12:00 AM

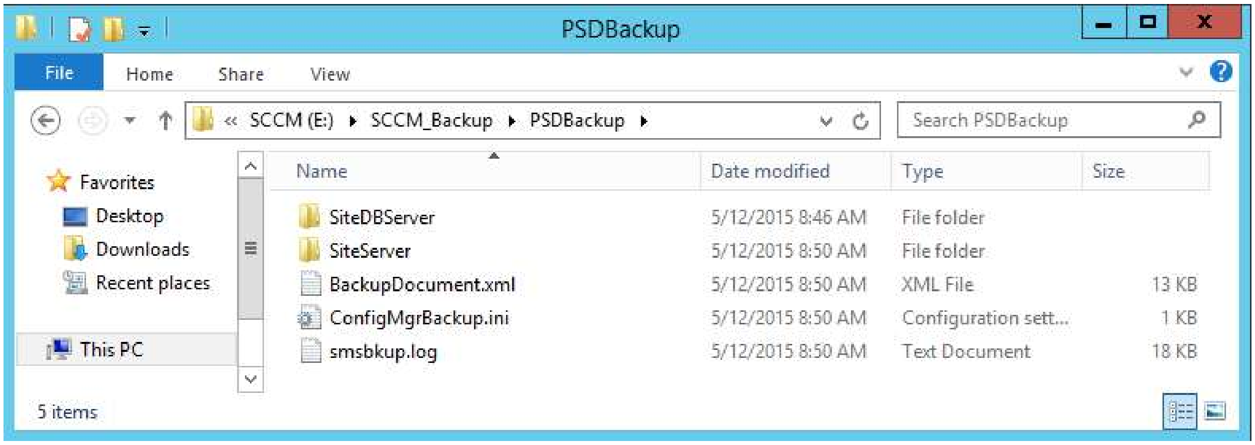
Latest start time: 1:00 AM

□ Monday
☑ Tuesday
□ Wednesday
☑ Thursday
□ Friday
☑ Saturday
□ Sunday

□ Enable alerts for backup task failures

For additional information about data not included in the Configuration Manager backup and recovery process, see the product documentation online.

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.

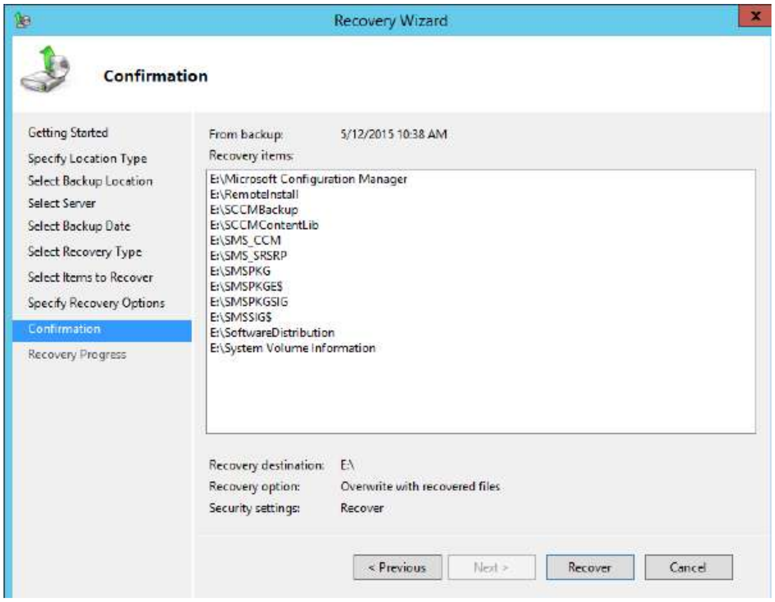


Name	Date modified	Type	Size
SiteDBServer	5/12/2015 8:46 AM	File folder	
SiteServer	5/12/2015 8:50 AM	File folder	
BackupDocument.xml	5/12/2015 8:50 AM	XML File	13 KB
ConfigMgrBackup.ini	5/12/2015 8:50 AM	Configuration sett...	1 KB
smsbkup.log	5/12/2015 8:50 AM	Text Document	18 KB

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



From backup: 5/12/2015 10:38 AM

Recovery items:

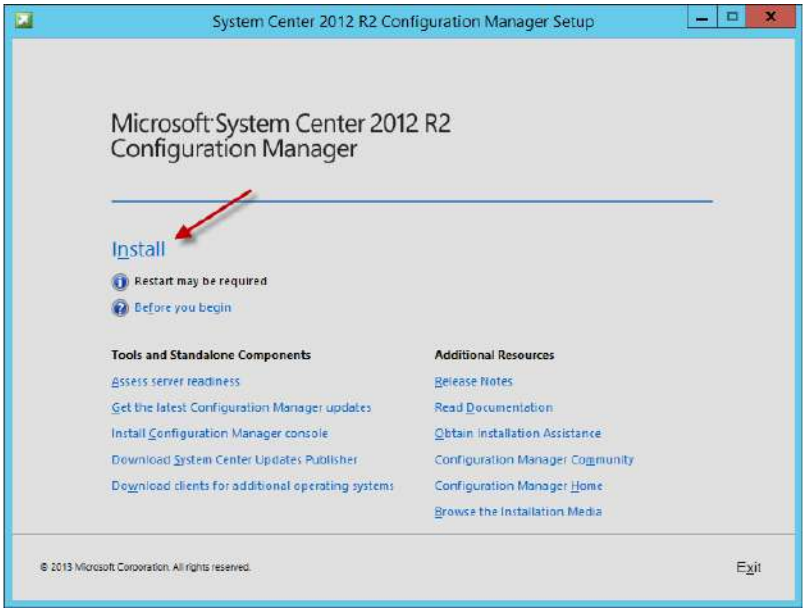
```
E:\Microsoft Configuration Manager
E:\RemoteInstall
E:\SCCMBackup
E:\SCCMContentLib
E:\SMS_CCM
E:\SMS_SRSRP
E:\SMSPKG
E:\SMSPKGE$
E:\SMSPKGSIG
E:\SMSSIG$
E:\SoftwareDistribution
E:\System Volume Information
```

Recovery destination: E:\

Recovery option: Overwrite with recovered files

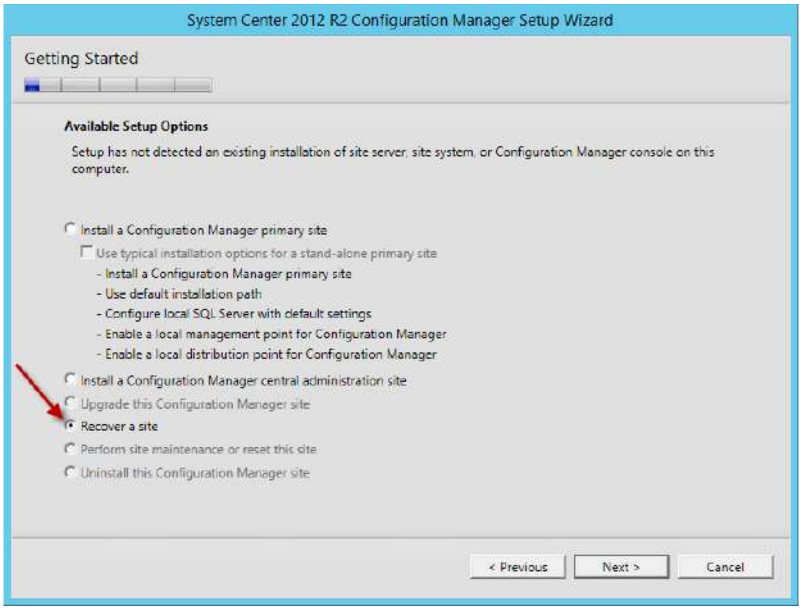
Security settings: Recover

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.



System Center 2012 R2 Configuration Manager Setup
Microsoft System Center 2012 R2
Configuration Manager
Install
Restart may be required
Before you begin
Tools and Standalone Components
Assess server readiness
Get the latest Configuration Manager updates
Install Configuration Manager console
Download System Center Updates Publisher
Download clients for additional operating systems
Additional Resources
Release Notes
Read Documentation
Obtain Installation Assistance
Configuration Manager Community
Configuration Manager Home
Browse the Installation Media
© 2013 Microsoft Corporation. All rights reserved.
Exit

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



Available Setup Options

Setup has not detected an existing installation of site server, site system, or Configuration Manager console on this computer.

○ Install a Configuration Manager primary site

□ Use typical installation options for a stand-alone primary site
- Install a Configuration Manager primary site
- Use default installation path
- Configure local SQL Server with default settings
- Enable a local management point for Configuration Manager
- Enable a local distribution point for Configuration Manager

○ Install a Configuration Manager central administration site

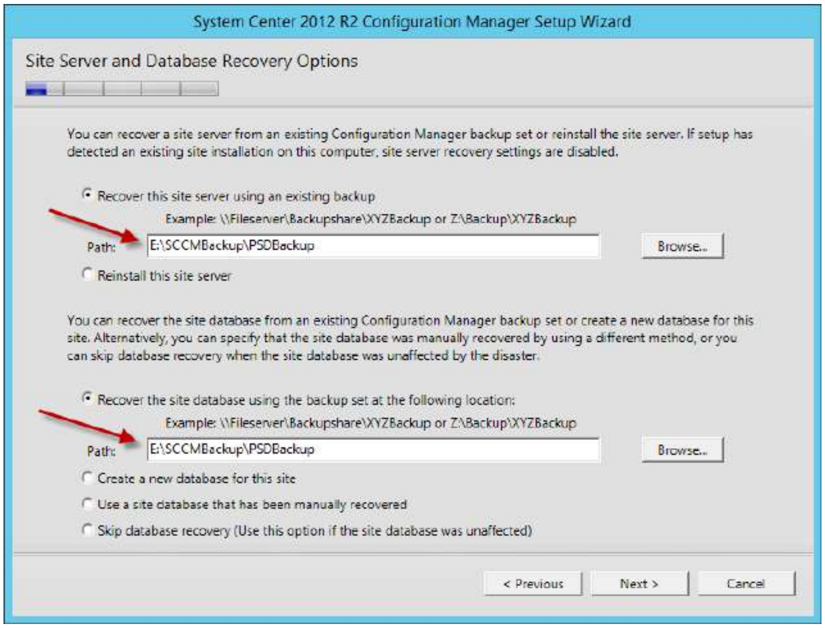
○ Upgrade this Configuration Manager site

● Recover a site

○ Perform site maintenance or reset this site

○ Uninstall this Configuration Manager 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.


System Center 2012 R2 Configuration Manager Setup Wizard

Site Server and Database Recovery Options

You can recover a site server from an existing Configuration Manager backup set or reinstall the site server. If setup has detected an existing site installation on this computer, site server recovery settings are disabled.

● Recover this site server using an existing backup

Example: \\Fileserver\Backupshare\XYZBackup or Z:\Backup\XYZBackup

Path: E:\SCCMBackup\PSDBackup

○ Reinstall this site server

You can recover the site database from an existing Configuration Manager backup set or create a new database for this site. Alternatively, you can specify that the site database was manually recovered by using a different method, or you can skip database recovery when the site database was unaffected by the disaster.

● Recover the site database using the backup set at the following location:

Example: \\Fileserver\Backupshare\XYZBackup or Z:\Backup\XYZBackup

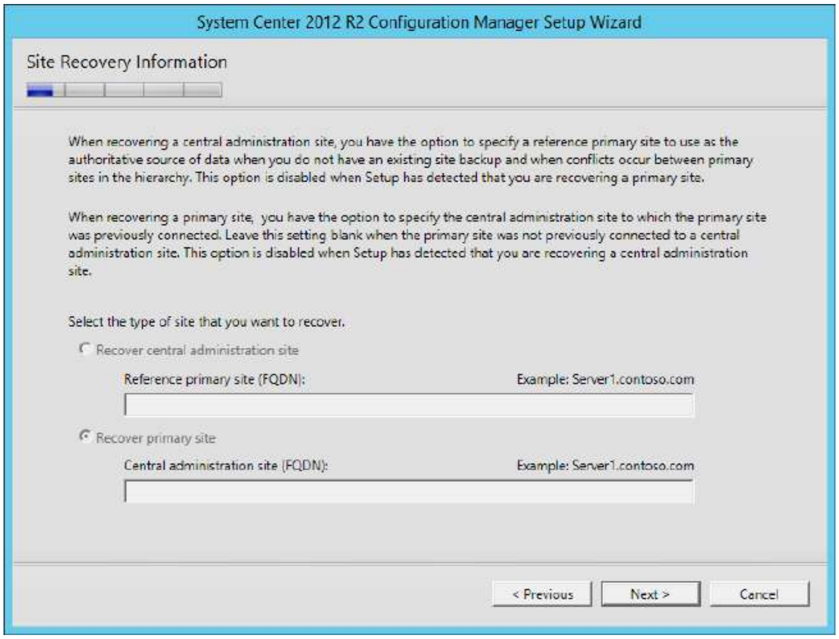
Path: E:\SCCMBackup\PSDBackup

○ Create a new database for this site

○ Use a site database that has been manually recovered

○ Skip database recovery (Use this option if the site database was unaffected)

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


System Center 2012 R2 Configuration Manager Setup Wizard

Site Recovery Information

When recovering a central administration site, you have the option to specify a reference primary site to use as the authoritative source of data when you do not have an existing site backup and when conflicts occur between primary sites in the hierarchy. This option is disabled when Setup has detected that you are recovering a primary site.

When recovering a primary site, you have the option to specify the central administration site to which the primary site was previously connected. Leave this setting blank when the primary site was not previously connected to a central administration site. This option is disabled when Setup has detected that you are recovering a central administration site.

Select the type of site that you want to recover.

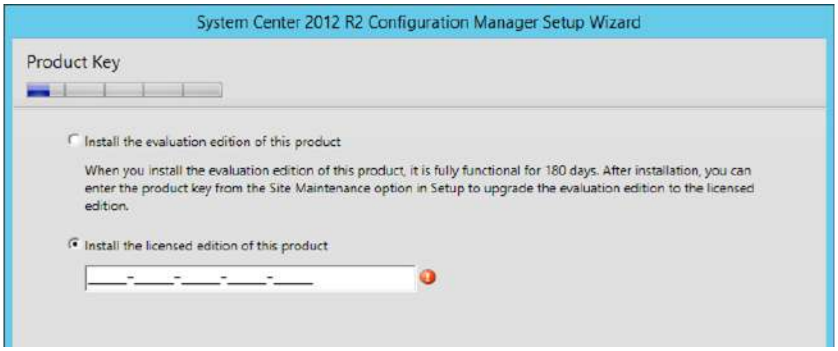
○ Recover central administration site

Reference primary site (FQDN): Example: Server1.contoso.com

● Recover primary site

Central administration site (FQDN): Example: Server1.contoso.com

On the Product Key screen enter your SCCM Product License Key


System Center 2012 R2 Configuration Manager Setup Wizard

Product Key

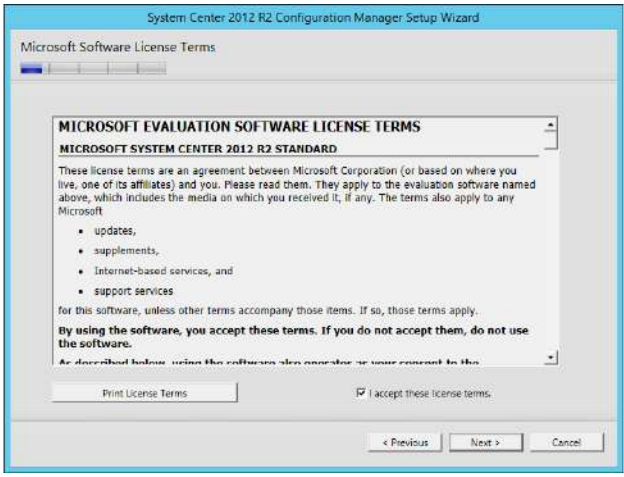
○ Install the evaluation edition of this product

When you install the evaluation edition of this product, it is fully functional for 180 days. After installation, you can enter the product key from the Site Maintenance option in Setup to upgrade the evaluation edition to the licensed edition.

● Install the licensed edition of this product

_____-_____-_____-_____-_____

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


System Center 2012 R2 Configuration Manager Setup Wizard

Microsoft Software License Terms

MICROSOFT EVALUATION SOFTWARE LICENSE TERMS

MICROSOFT SYSTEM CENTER 2012 R2 STANDARD

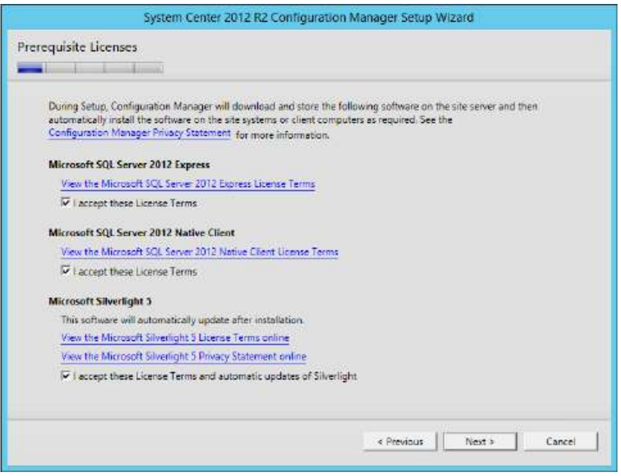
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the evaluation software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software.

☑ I accept these license terms.


System Center 2012 R2 Configuration Manager Setup Wizard

Prerequisite Licenses

During Setup, Configuration Manager will download and store the following software on the site server and then automatically install the software on the site systems or client computers as required. See the Configuration Manager Privacy Statement for more information.

Microsoft SQL Server 2012 Express

View the Microsoft SQL Server 2012 Express License Terms

☑ I accept these License Terms

Microsoft SQL Server 2012 Native Client

View the Microsoft SQL Server 2012 Native Client License Terms

☑ I accept these License Terms

Microsoft Silverlight 5

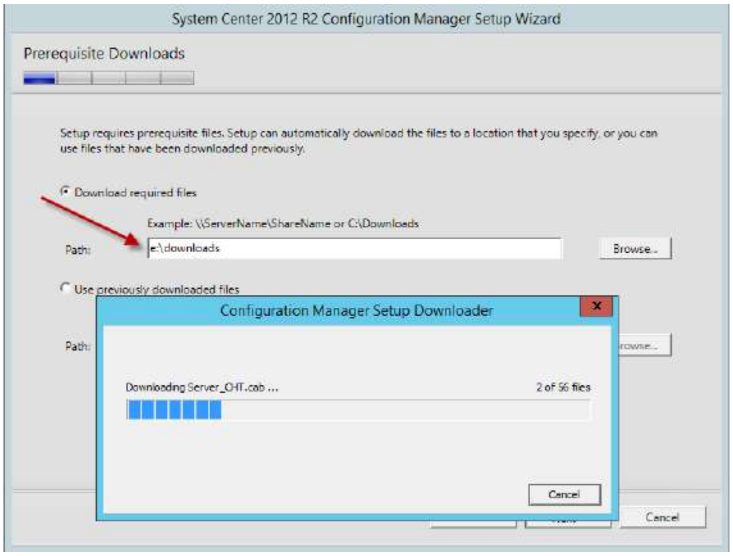
This software will automatically update after installation.

View the Microsoft Silverlight 5 License Terms online

View the Microsoft Silverlight 5 Privacy Statement online

☑ I accept these License Terms and automatic updates of Silverlight

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**


System Center 2012 R2 Configuration Manager Setup Wizard

Prerequisite Downloads

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: e:\downloads

○ Use previously downloaded files

Path:

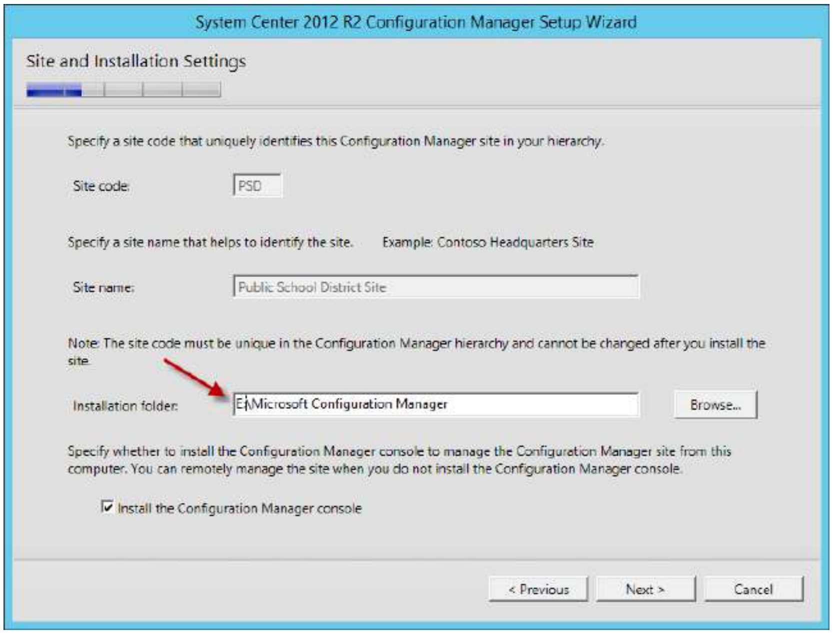
Configuration Manager Setup Downloader

Downloading Server_CHT.cab ...

2 of 56 files

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*



System Center 2012 R2 Configuration Manager Setup Wizard

Site and Installation Settings

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

Site code: PSD

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

Site name: Public School District Site

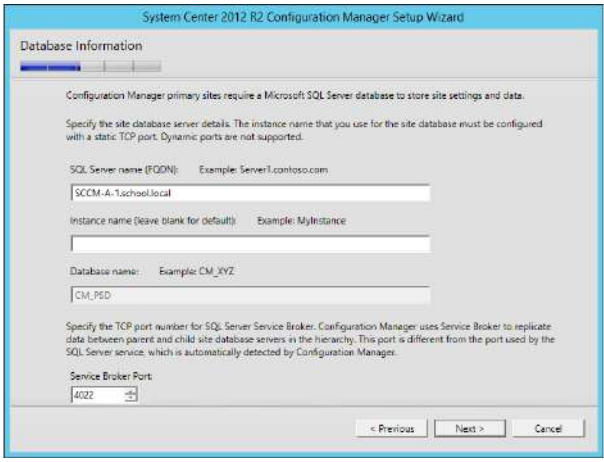
Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.

Installation folder: E:\Microsoft Configuration Manager

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

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.



Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.

Specify the site database server details. The instance name that you use for the site database must be configured with a static TCP port. Dynamic ports are not supported.

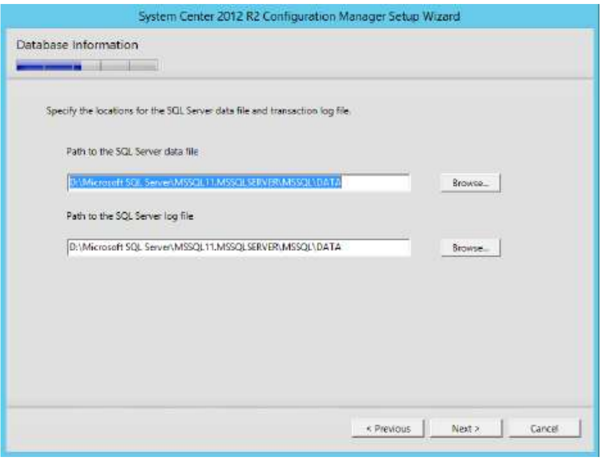
SQL Server name (FQDN): Example: Server1.contoso.com
SCCM-A-1.school.local

Instance name (leave blank for default): Example: MyInstance

Database name: Example: CM_XYZ
CM_PSD

Specify the TCP port number for SQL Server Service Broker. Configuration Manager uses Service Broker to replicate data between parent and child site database servers in the hierarchy. This port is different from the port used by the SQL Server service, which is automatically detected by Configuration Manager.

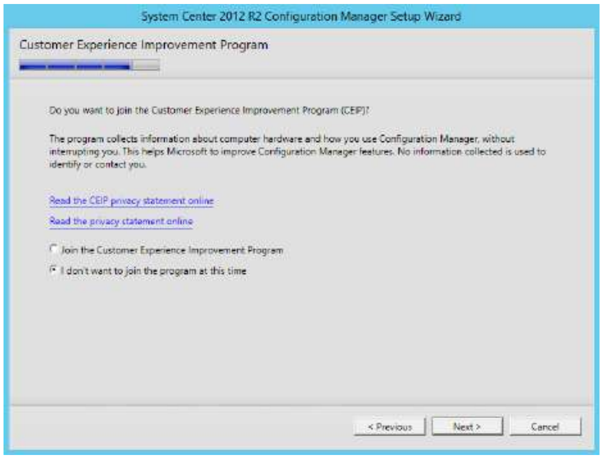
Service Broker Port
4022



Specify the locations for the SQL Server data file and transaction log file.

Path to the SQL Server data file
D:\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA

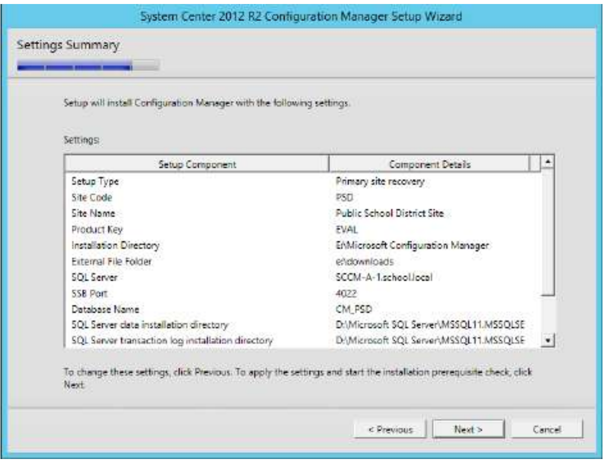
Path to the SQL Server log file
D:\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA


System Center 2012 R2 Configuration Manager Setup Wizard
Customer Experience Improvement Program
Read the CEIP privacy statement online
Read the privacy statement online
< Previous
Next >
Cancel

Do you want to join the Customer Experience Improvement Program (CEIP)?

The program collects information about computer hardware and how you use Configuration Manager, without interrupting you. This helps Microsoft to improve Configuration Manager features. No information collected is used to identify or contact you.

○ Join the Customer Experience Improvement Program
● I don't want to join the program at this time

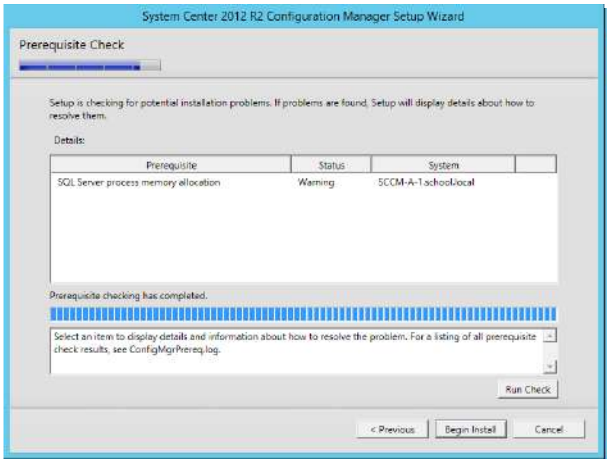


Setup will install Configuration Manager with the following settings.

Settings:

Setup Component	Component Details
Setup Type	Primary site recovery
Site Code	PSD
Site Name	Public School District Site
Product Key	EVAL
Installation Directory	E:\Microsoft Configuration Manager
External File Folder	e:\downloads
SQL Server	SCCM-A-1.school.local
SSB Port	4022
Database Name	CM_PSD
SQL Server data installation directory	D:\Microsoft SQL Server\MSSQL11.MSSQLSE
SQL Server transaction log installation directory	D:\Microsoft SQL Server\MSSQL11.MSSQLSE

To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.



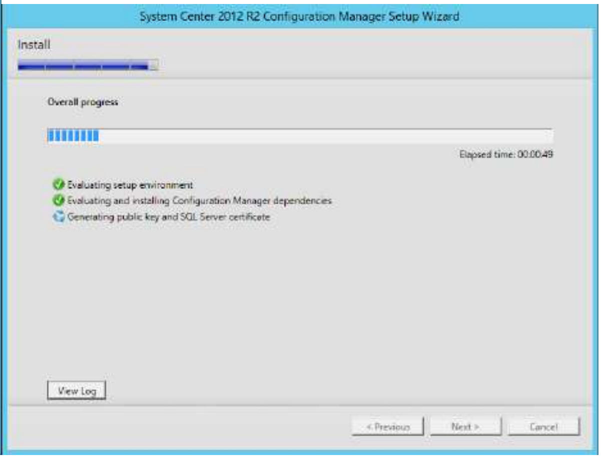
Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.

Details:

Prerequisite	Status	System
SQL Server process memory allocation	Warning	SCCM-A-1.school.local

Prerequisite checking has completed.

Select an item to display details and information about how to resolve the problem. For a listing of all prerequisite check results, see ConfigMgrPrereq.log.

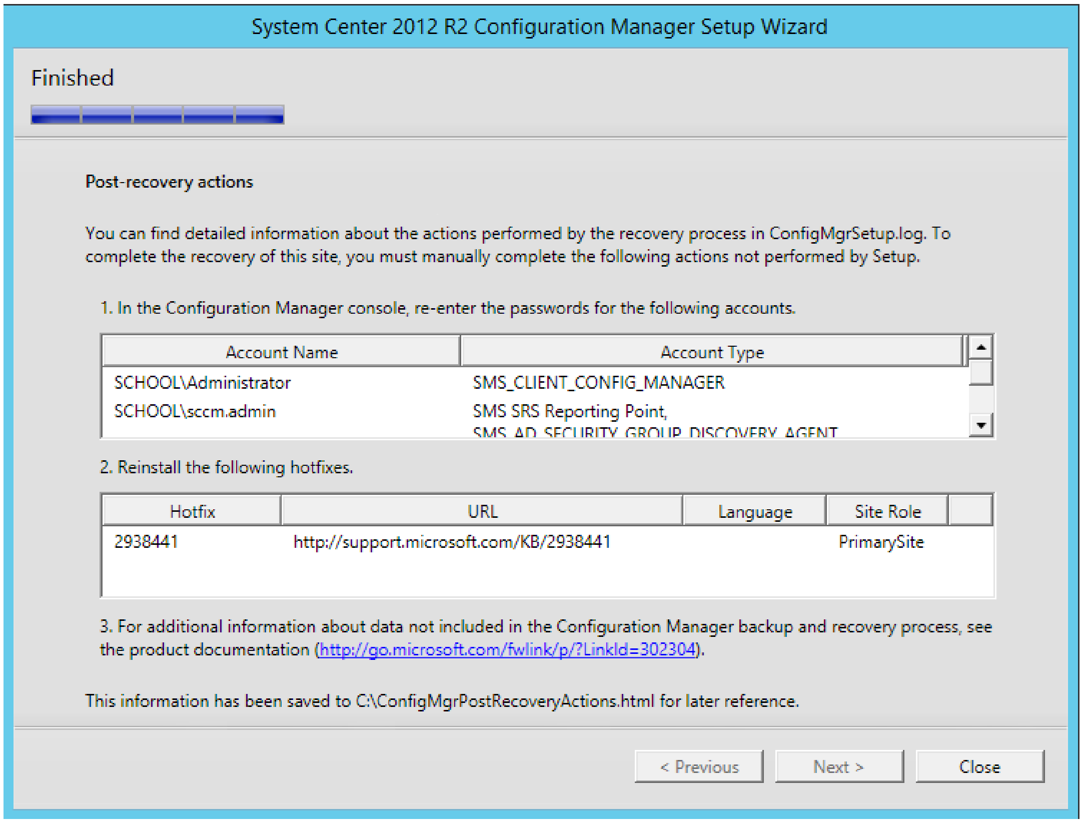


Overall progress

Elapsed time: 00:00:49

✓ Evaluating setup environment
✓ Evaluating and installing Configuration Manager dependencies
Generating public key and SQL Server certificate

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.



Post-recovery actions

You can find detailed information about the actions performed by the recovery process in ConfigMgrSetup.log. To complete the recovery of this site, you must manually complete the following actions not performed by Setup.

1. In the Configuration Manager console, re-enter the passwords for the following accounts.

Account Name	Account Type
SCHOOL\Administrator	SMS_CLIENT_CONFIG_MANAGER
SCHOOL\sccm.admin	SMS SRS Reporting Point, SMS_AD_SECURITY_GROUP_DISCOVERY_AGENT

2. Reinstall the following hotfixes.

Hotfix	URL	Language	Site Role
2938441	http://support.microsoft.com/KB/2938441		PrimarySite

3. For additional information about data not included in the Configuration Manager backup and recovery process, see the product documentation (http://go.microsoft.com/fwlink/p/?LinkId=302304).

This information has been saved to C:\ConfigMgrPostRecoveryActions.html for later reference.