

System Center Configuration Manager Software Update Management Guide

Friday, 26 February 2010
Version 1.0.0.0 Baseline

Prepared by
Microsoft

Microsoft®

Copyright

This document and/or software ("this Content") has been created in partnership with the National Health Service (NHS) in England. Intellectual Property Rights to this Content are jointly owned by Microsoft and the NHS in England, although both Microsoft and the NHS are entitled to independently exercise their rights of ownership. Microsoft acknowledges the contribution of the NHS in England through their Common User Interface programme to this Content. Readers are referred to www.cui.nhs.uk for further information on the NHS CUI Programme.

All trademarks are the property of their respective companies. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

© Microsoft Corporation 2010. All rights reserved.

Disclaimer

At the time of writing this document, Web sites are referenced using active hyperlinks to the correct Web page. Due to the dynamic nature of Web sites, in time, these links may become invalid. Microsoft is not responsible for the content of external Internet sites.

TABLE OF CONTENTS

1	Executive Summary	1
2	Introduction	2
2.1	Value Proposition	2
2.2	Knowledge Prerequisites	2
2.2.1	Skills and Knowledge	2
2.2.2	How Software Updates Work	5
2.2.3	Training and Assessment	6
2.3	Infrastructure Prerequisites	6
2.4	Audience	7
2.5	Assumptions	7
3	Using This Document	8
3.1	Document Structure	8
4	Plan	10
4.1	Planning Software Update Infrastructure	11
4.1.1	Planning Where to Install the Software Update Point	11
4.1.2	Planning for Multiple Sites	11
4.1.3	Planning Group Policy for Configuration Manager Clients	12
4.2	Planning a Software Updates Package Strategy	13
4.2.1	Single Package Strategy	14
4.2.2	Base Package and Semi Annual (Rollup) Strategy	14
4.2.3	Multiple Packages Organised by Product Strategy	15
4.3	Planning Update Selection	16
4.3.1	Products	16
4.3.2	Classifications	17
4.3.3	Languages	17
4.4	Using Custom Catalogues from Third Party Vendors	18
4.5	Planning Software Update Management Collections	18
4.6	Planning Deployment Templates	20
4.7	Planning Maintenance Windows	23
4.8	Planning Pilot Computers for Software Updates	23
4.8.1	Identifying and Categorising Applications	24
4.8.2	Identifying Application Owners	24
4.8.3	Creating Pilot Collections	24
5	Deploy	25
5.1	Preparing a Configuration Manager Infrastructure for Software Update Management	25
5.1.1	Enabling Software Update Agent Settings	25

5.1.2	Installing and Configuring the Software Update Point.....	27
5.1.3	Creating a Package Source Location.....	38
5.1.4	Creating Software Update Collections	38
5.1.5	Creating Deployment Templates.....	48
6	Operate.....	52
6.1	Deploying Software Updates	52
6.1.1	Creating Search Folders.....	52
6.1.2	Creating Update Lists and Deployment Packages.....	53
6.1.3	Creating Deployments	57
6.1.4	Other Methods of Downloading and Deploying.....	61
6.1.5	Creating Compliance Report	61
6.2	Additional Tasks.....	62
APPENDIX A	Skills and Training Resources.....	63
PART I	Training Resources	63
PART II	Supplemental Training Resources	63
APPENDIX B	Document Information.....	64
PART I	Terms and Abbreviations.....	64
PART II	References	65

1 EXECUTIVE SUMMARY

The software updates feature of System Center Configuration Manager 2007 R2 (Configuration Manager) provides the capability to detect and report on the software update or patch state of a healthcare organisation. Combined with the software distribution feature, which allows the healthcare IT Administrators to deploy missing software updates in a controlled manner, it represents a complete solution to software update management of the Windows® client and server estates in a healthcare organisation.

The *System Center Configuration Manager 2007 Software Update Management Guide* provides information and guidance to help healthcare IT Administrators use the software updates feature of Configuration Manager. This guide can be used to aid healthcare organisations who have already deployed Configuration Manager, or can be used in conjunction with the *System Center Configuration Manager 2007 Deployment Guide*¹ to deploy Configuration Manager.

¹ *System Center Configuration Manager 2007 Deployment Guide {R1}*:
<http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx>

2 INTRODUCTION

2.1 Value Proposition

This document provides guidance on implementing and using the software updates feature of Configuration Manager. The guidance will help a healthcare IT Administrator to:

- Decide if any infrastructure changes will be required to support software updates
- Install and configure the software updates feature
- Decide upon a software update management strategy to meet the goals of the healthcare organisation

This document provides the information required to quickly become familiar with the software update feature and understand the appropriate decisions that need to be made in order to deploy and use the solution. It also provides step-by-step guidance showing how to install and configure the required components, and also how to use the most common features.

2.2 Knowledge Prerequisites

To effectively implement the recommendations made throughout this document, a number of knowledge-based and environmental infrastructure prerequisites should be in place. This section outlines the knowledge and skills required to use the Configuration Manager guidance provided in this document, while section 2.3 details the necessary infrastructure prerequisites.

Section 2.2.1 details the prerequisite skills and knowledge, and section 2.2.3 details the information and suggested training resources or skill assessment.

2.2.1 Skills and Knowledge

The technical knowledge and minimum skills required to use this Deliverable are discussed in the following sections. They provide an introduction to the concepts and terminology of the Software Updates feature of Configuration Manager, and describe how the process of detection and updating works.

2.2.1.1 *Software Update Metadata and Software Update Files*

There are two parts to software updates:

- The Software Update Metadata provides information about the software update, including the software that the update supports, the name, description, target operating system, language, and class
- The Software Update Files are the actual binary files which contain the updates themselves. These may be an executable file (.EXE), a Microsoft Installer file (.MSI), or a Windows Installer patch file (.MPS)

As shown in the sections below, the two parts of the update are handled separately.

2.2.1.2 Software Update Point

The Software Update Point (SUP) is a system role required to manage software updates. Each site must have at least one SUP. The SUP must have Windows Server® Update Services (WSUS) 3.0 Service Pack (SP) 1 or above installed on it. The SUP role then manages the communication of information between WSUS and the site server.

While WSUS 3.0 is installed on the SUP, Configuration Manager clients do not install updates from the WSUS server as they would if software updates were being managed by WSUS alone. The WSUS server is responsible only for managing the Update Metadata Catalog. The software update files themselves are downloaded and managed by the site server. This allows much greater control when the patches are deployed and offer the healthcare IT Administrator much greater flexibility when deploying updates. It also allows for detailed reporting and status while the update deployments are being carried out. See section 4.1 for more information on planning SUPs.

2.2.1.3 Deployment Templates

Each time software updates are deployed to Configuration Manager clients, many of the parameters used in the process are the same, or a number of sets of parameters are used across the healthcare organisation, each of which remains consistent for each deployment. To save having to repeatedly enter the same parameters, a number of Deployment Templates can be established, which define many of the parameters required. A Deployment Template can then be applied when a new software update deployment is set up.

A summary of the settings that can be defined in a Deployment Template are shown in Table 1.

Property	Description
Collection	The collection that will be used to target the software update deployment.
Display/Time Settings	Determines whether users will be notified that new updates are available, whether the deployment schedule is evaluated in local time or UTC, and the duration that the deployment is allowed to run for.
Restart Settings	Determines if workstations and/or servers should be automatically restarted, and whether this is allowed outside scheduled maintenance windows.
Event Generation	Controls the generation of events which get reported to System Center Operations Manager. If Operations Manager is in use, alerts can be suppressed during updates in order to prevent false alarms in Operations Manager.
Download Settings	Determines how clients will connect to Distribution Points (DPs).
SMS 2003 Settings	Controls deployment of software updates to SMS 2003 clients. The management of SMS 2003 clients is not in scope of the guidance provided in this document.

Table 1: Summary of Deployment Template Properties

See section 4.6 for more information on planning Deployment Templates.

2.2.1.4 Search Folders

Search Folders allow the healthcare IT Administrator to create custom views on the Software Update Metadata. The Search Folder displays updates that match specific criteria, such as Product or Release Date. This allows the healthcare IT Administrator to quickly find the updates that are required for a particular deployment and create an Update List from the results. Search Folders are dynamic based on the query provided, so are a useful way to rationalise the very large list of possible updates available. See section 6.1.1 for more information on creating Search Folders.

2.2.1.5 Update Lists

An Update List provides a mechanism of defining smaller collections of updates which are to be deployed. Updates can be added to or removed from an Update List, and they remain a static list of updates. A deployment of updates will reference an Update List to say which updates to deploy. This allows Update Lists and the actual deployment process to be separated. Update Lists are also used by some of the key Compliance Reports within Configuration Manager. These reports allow the healthcare IT Administrator to see compliance data based on a particular Update List and collection. See section 6.1.2 for more information on creating Update Lists.

2.2.1.6 Deployment Packages

Deployment Packages are similar to standard Configuration Manager Software Distribution Packages. They contain information such as the source directory for the updates, and which DPs the package should be deployed to. There is no direct link between a deployment and a Deployment Package. If a deployment contains a particular software update, it can be accessed from any Deployment Package which happens to contain that update. If an update has been downloaded to more than one Deployment Package, clients should access the update from the most suitable Deployment Package, regardless of the Deployment Package that was referenced when running the Software Update Wizard.

2.2.1.7 Package Source Folder

A package source folder is the location where all the files for a Deployment Package are downloaded. The files are then copied from this location to the DPs specified in the Deployment Package. Each Deployment Package will have its own package source folder. These are essentially the 'source' files for the package. See section 5.1.3 for more information on creating a package source location.

2.2.1.8 Collections

The healthcare IT Administrator can make software updates available to as many computers as required. The Configuration Manager clients that need to receive the update must be members of a collection (referred to as the target collection). The target collection can, for example, contain a single client, all the clients that are assigned to a specific site, or any subset of clients. When a software update is distributed to the target collection, all the clients that are members of that collection receive the update.

If Active Directory® Domain Services (AD DS) is implemented in the healthcare organisation, a target collection can be created that is based on Active Directory containers. Collections can be created that target systems based on organisational units, domains, site, operating system or any other criteria that is present in the Configuration Manager database. To target systems for software distribution, using Active Directory containers, the Active Directory System and Active Directory System Group discovery methods must be enabled in the site and must have been run at least once. Section 4.5 provides more information on planning collections.

Collections in which membership rules are based on queries are dynamic. After the initial membership list is created, if the collection has been configured with an update schedule, clients are automatically added to, or removed from the collection, as appropriate. Client computers that initially did not meet the collection's criteria, but meet the criteria now, automatically become members of the collection. Clients that initially meet the collection's criteria, but then no longer meet the criteria, are automatically removed from the collection (this does not result in the clients being uninstalled). In a dynamic environment, Configuration Manager keeps collections current, thus ensuring that only the appropriate clients receive the requested software updates.

2.2.2 How Software Updates Work

Figure 1 shows a high level overview of the software updates process in Configuration Manager.

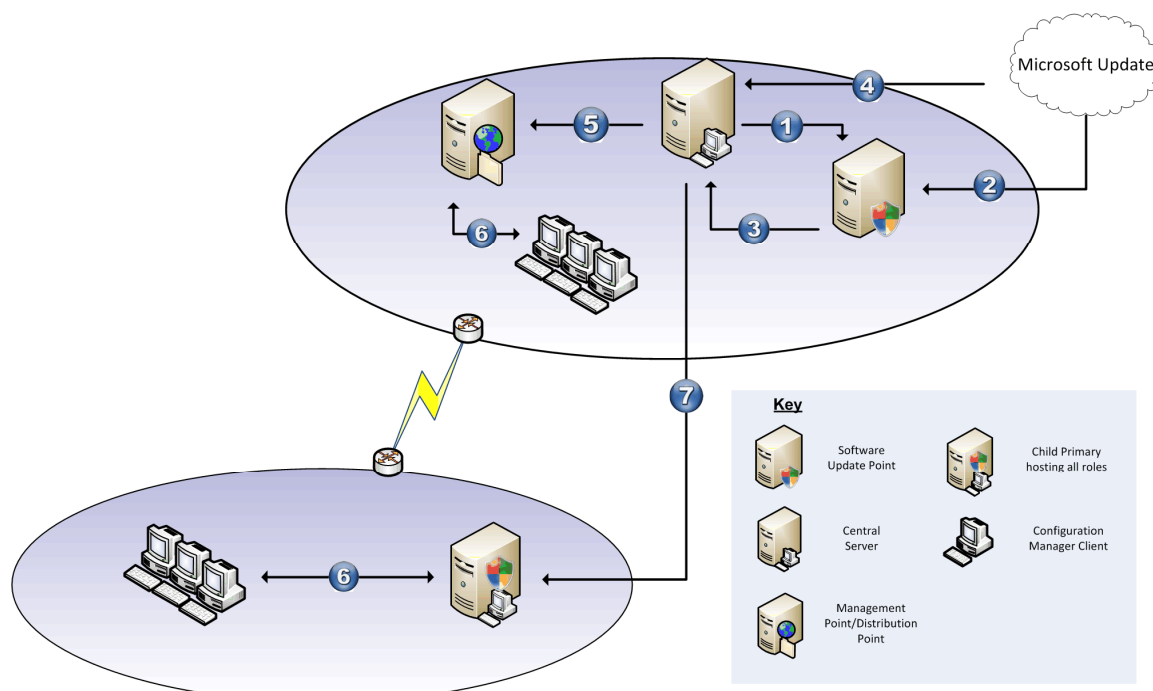


Figure 1: Software Updates Overview

Table 2 describes each step of the Software Update process in more detail.

Step	Description
1.	Configuration Manager Site Server triggers a synchronisation of the SUP. This is performed on a schedule, or can be manually triggered using the Configuration Manager Administrator Console.
2.	This signals WSUS on the SUP to contact the Microsoft Update servers and download Update Metadata on all selected products and categories. No updates are downloaded to the SUP, just metadata describing the updates and how to detect them, and any applicable license information.
3.	The metadata is retrieved by the Configuration Manager site server and stored in the Configuration Manager database. At this stage, clients can start to report information back to the Configuration Manager server on the patch status. The clients contact the SUP in order to retrieve Update Metadata and the Update Agent can perform a scan. This information is sent to Configuration Manager server where an IT Administrator can view the status of software updates across the healthcare organisation's infrastructure.
4.	Having decided which software updates are required for the healthcare organisation, the IT Administrator can now create Search Folders (to allow required updates to be viewed easily), Update Lists (which allow compliance reports to be viewed and updates to be grouped) and Deployment Packages (which contain the binary files necessary to update the clients). At this stage, the IT Administrator can either download the updates from the Microsoft Update, ready for a deployment in the future, or create the deployment at the same time.

Step	Description
5.	The IT Administrator creates the deployment. A deployment is carried out by specifying the Deployment Package that will be deployed, associating that package with a Collection and specifying or creating a Deployment Template. Once the deployment is configured, the Configuration Manager server will place all update files (If not already done) on the required DPs. A policy will be created and placed on the Management Point (MP) so clients know the new updates are available and where they should be installed from.
6.	Clients perform a scheduled scan for new updates and retrieve the policy from the MP. If any updates are applicable on the client, they will be installed from the closest DP. As the client scans for required updates and installs them, State Messages are sent to the Configuration Manager infrastructure so the IT Administrator has an up-to-date view of the status of the deployment.
7.	Once the synchronisation at the Central Site has occurred, a site-to-site replication of a synchronisation request is sent to the child sites. This triggers the same actions as steps 1 to 3, the only difference being that the lower level SUP will synchronise data with its parent, rather than going directly to the Microsoft Update servers.

Table 2: Software Updates Process Overview

More information on the detailed process behind software updates in Configuration Manager is available in the following articles:

- *Software Updates Synchronization Process Flowchart*²
- *Software Update Deployment Process Flowchart*³
- *Deployment Package Process Flowchart*⁴

2.2.3 Training and Assessment

Guidelines on the basic skill sets that are required in order to make best use of this Deliverable are detailed in APPENDIX A. These represent the training courses and other resources available. All courses mentioned are optional and can be provided by a variety of certified training partners.

2.3 Infrastructure Prerequisites

The following are prerequisites for using Configuration Manager for software update management:

- An existing System Center Configuration Manager 2007 infrastructure with SP2 or above
- Windows Server Update Service (WSUS) 3.0 SP 1 or SP2 Server
- Microsoft® Windows® 7, Windows Vista®, Windows XP® Professional (SP2 or SP3), or Windows® 2000 Professional SP4 or above required for all desktop clients
- Microsoft Windows 2000 Server SP4, Windows Server® 2003 or Windows Server® 2008 required for all Server clients
- Configuration Manager client deployed to clients
- Configuration Manager Software Updates feature enabled for Configuration Manager clients

² Microsoft TechNet – Software Updates Synchronization Process Flowchart {R2}:
<http://technet.microsoft.com/en-us/library/bb932170.aspx>

³ Microsoft TechNet – Software Update Deployment Process Flowchart {R3}:
<http://technet.microsoft.com/en-us/library/bb932173.aspx>

⁴ Microsoft TechNet – Deployment Package Process Flowchart {R4}:
<http://technet.microsoft.com/en-us/library/bb932157.aspx>

2.4 Audience

The guidance contained in this document is targeted at a variety of roles within the healthcare organisation's IT department. Table 3 provides a reading guide for this document, illustrating the roles and the sections of the document that are likely to be of most interest. The structure of the sections referred to is described in section 3.1.

Role	Document Usage	Executive Summary	Plan	Deploy	Operate
IT Manager	Review of the entire document to understand the justification and drivers, and to develop an understanding of the implementation requirements	✓			
IT Architect	Review the relevant areas within the document against local architecture strategy and implementation plans	✓	✓	✓	
IT Professional/Administrator	Detailed review and implementation of the guidance provided in this document to meet local requirements	✓	✓	✓	✓

Table 3: Document Audience

2.5 Assumptions

The guidance provided in this document assumes that the healthcare organisation has already deployed, or is planning to deploy, a Configuration Manager Infrastructure in mixed security mode.

3 USING THIS DOCUMENT

This document is intended for use by healthcare organisations and their IT Administrators who wish to use Configuration Manager to perform software updates. The document should be used to assist with the planning and implementation of the Software Update features of Configuration Manager, and as a reference guide for the most common tasks involved with its use.

3.1 Document Structure

This document contains the following three sections that deal with the Project Lifecycle, as illustrated in Figure 2:

- Plan
- Deploy
- Operate

Each section is based on the Microsoft IT Project Lifecycle as defined in the Microsoft Solutions Framework (MSF) Process Model, and the Microsoft Operations Framework (MOF). The IT Project Lifecycle is described in more detail in the *Microsoft Solutions Framework Core White Papers*⁵ and the *MOF Executive Overview*⁶. The MSF Process Model and MOF describe a high-level sequence of activities for building, deploying and managing IT solutions. Rather than prescribing a specific series of procedures, they are flexible enough to accommodate a broad range of IT projects.

The three sections of this document are as follows:

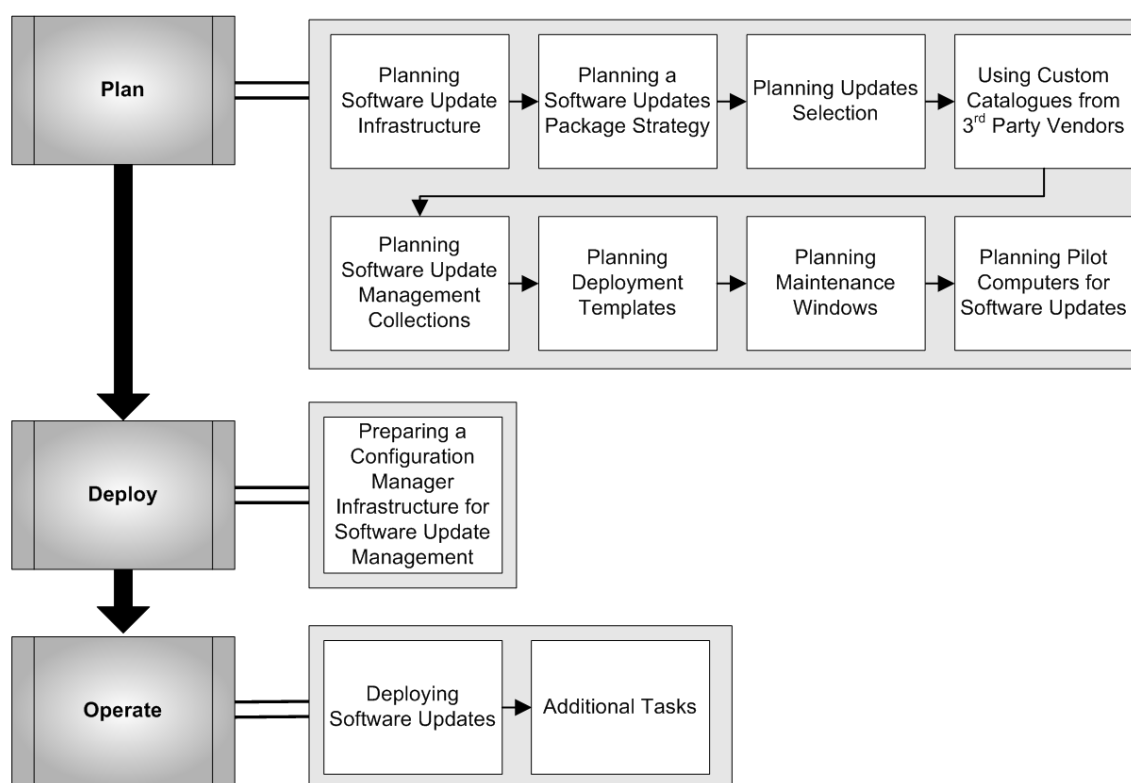


Figure 2: Microsoft Solutions Framework Process Model Phases and Document Structure

⁵ Microsoft Solutions Framework Core White Papers:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e481cb0b-ac05-42a6-bab8-fc886956790e&DisplayLang=en>

⁶ MOF Executive Overview:

<http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofeo.msp>

The key public documentation resources for building a Configuration Manager solution are listed below. Where appropriate, specific chapters or sections from these documents have been referenced throughout this guidance:

- *Microsoft TechNet System Center Configuration Manager TechCenter*⁷
- *Microsoft System Center Configuration Manager Product Homepage*⁸

⁷Microsoft TechNet System Center Configuration Manager TechCenter {R5}:
<http://technet.microsoft.com/en-gb/configmgr/default.aspx>

⁸ Microsoft System Center Configuration Manager Product Homepage {R6}:
www.microsoft.com/sccm

4 PLAN

The Plan phase is where the bulk of the implementation planning is completed. During this phase the areas for further analysis are identified and a design process commences

Figure 3 acts as a high-level checklist, illustrating the sequence of events that the IT Manager and IT Architect need to determine when planning to use the Software Update feature of Configuration Manager within a healthcare organisation:

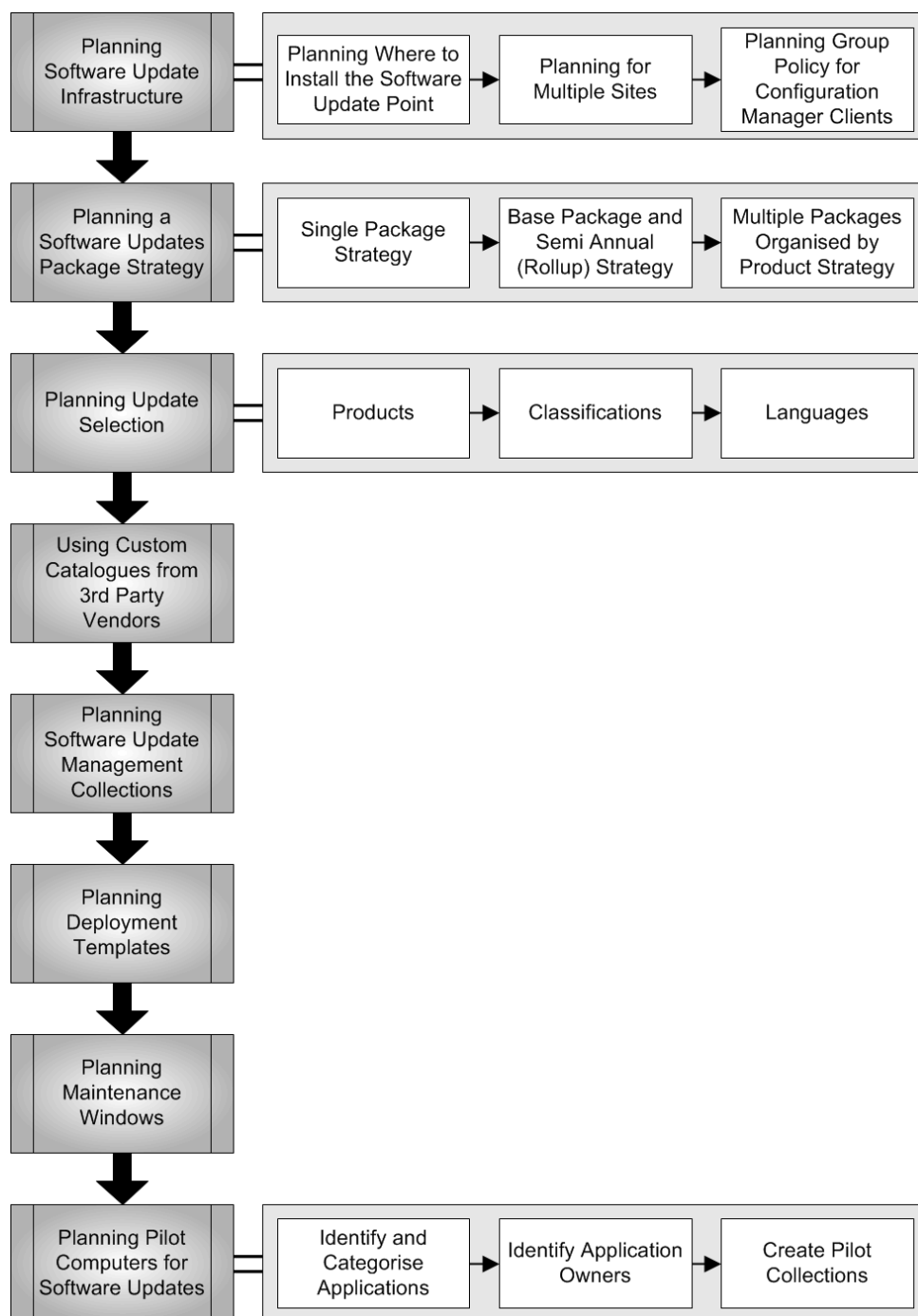


Figure 3: Sequence for Planning the Use of the Software Update Feature in Configuration Manager

4.1 Planning Software Update Infrastructure

There are a number of considerations when planning the deployment of the Software Update infrastructure which can significantly impact the performance of the site and the network. The IT Administrator should decide the best strategy for the healthcare organisation's environment, based on the following key decisions:

- Where to install the SUP role
- How many SUPs will be required in the Configuration Manager Hierarchy
- Will a migration from an existing WSUS infrastructure be required
- Which software Products and Categories are required
- What package strategy will be used

4.1.1 Planning Where to Install the Software Update Point

The SUP role is a WSUS server that Configuration Manager clients contact to gather Update Metadata in order to scan for available software updates. Depending on the number of Configuration Manager clients reporting to the site, it is sometimes necessary to separate this role from the site server. Many factors can affect whether this is necessary, such as server hardware and the features that are enabled on the site. The IT Administrator will need to determine if they should be separated.

Table 4 shows an estimate of the client numbers that may require the SUP role to be separated from the site server.

Number of Clients	Separate SUP Required
0-2,500	No
2,501 – 14,999	Yes, single SUP (can use Network Load Balancing (NLB) for redundancy)
14,999 and above	Network Load Balanced SUPs required

Table 4: Estimated Client Numbers for Separate Software Update Point Role

When installing WSUS to support the SUP role, an Administration website is installed. If the SUP role is installed on the same server as a MP or Background Intelligent Transfer Service (BITS) enabled DP, it should be installed into its own Website. If it is being installed on a dedicated server, then the default Website installation should be used.

4.1.2 Planning for Multiple Sites

If the healthcare organisation has multiple geographic sites and multiple Configuration Manager sites that correspond, it is important to ensure that the SUP architecture follows the same design. WSUS, and therefore the SUP architecture in Configuration Manager, can be designed in a hierarchy to allow for clients to be able to access the information required for scanning from a local source. For example, if the healthcare organisation has a three primary site hierarchy, with slow network connections between each site, the SUP role should be configured at each site to prevent clients traversing the slow network to gather update information.

The following configuration is illustrated in Figure 4:

- The SUP in the Central Site (Site A) is configured to synchronise update data with Microsoft Update
- The SUP in the Child Primary Site (Site B) is configured to synchronise with the SUP in the Central Site. This allows the IT Administrator at the Central Site to define the set of updates that will be available to all sites in the hierarchy, but still allows the Administrators in the Child Primary site to decide if all the updates are applicable to the clients in the child primary site
- The SUP in the Secondary Site (Site C) is configured as a replica of the SUP in the Central Site

As there is no database at a Secondary Site, there is no need to provide the ability to further define applicable updates, so the SUP allows clients to get update information without traversing the slow link.

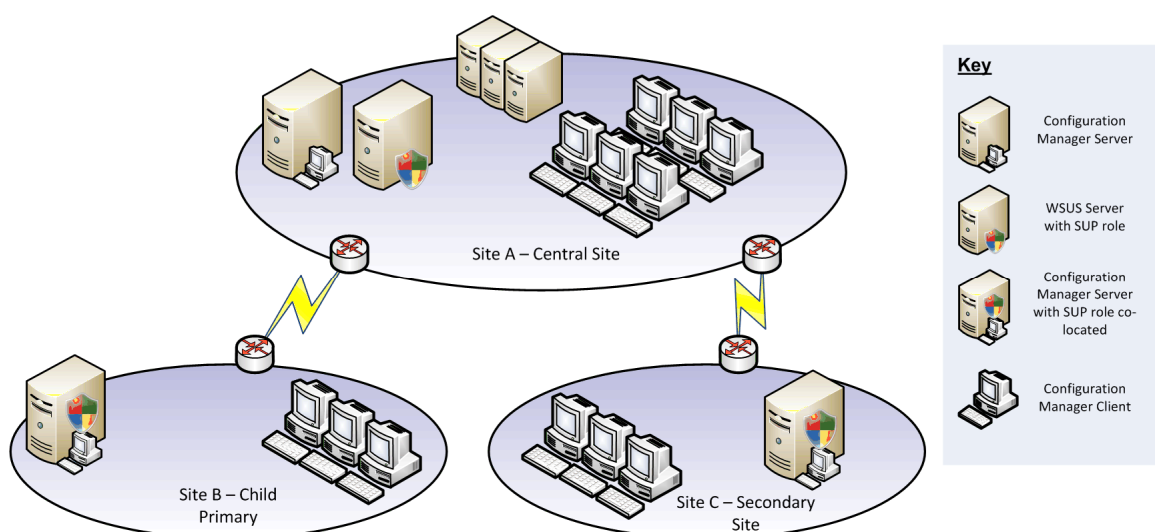


Figure 4: Software Update Points Configured in a Hierarchy

4.1.3 Planning Group Policy for Configuration Manager Clients

When the Software Update client agent is enabled in Configuration Manager, a local machine policy is deployed to the clients in that site. This policy is Specify intranet Microsoft update service location under Administrative Templates/Software Updates. The policy points the Update Agent to the SUP.

Important

It is important that no group policy setting sets the Specify intranet Microsoft update service location otherwise that setting will override the Configuration Manager setting (as it is a local machine policy), and may cause conflicts. This must be considered if WSUS has been used directly to manage software updates in the past.

If multiple SUPs are configured in the hierarchy, the Update Agent will point to the SUP for the local site. It may be necessary to configure the client machine to point to the SUP manually if the Configuration Manager client will be deployed using the SUP Installation method. More information regarding SUP Installation is available in the document *System Center Configuration Manager 2007 Deployment Guide {R1}*.

4.2 Planning a Software Updates Package Strategy

Configuration Manager makes use of packages to distribute software updates for installation on Configuration Manager clients, although the process of running those packages is not the same as for normal Configuration Manager software distribution. Planning a strategy for configuration of these packages will help save time in creating, maintaining and deploying software updates in the healthcare organisation. Package strategies can be considered individually for each SMS site in a hierarchy of SMS sites, or a single strategy can be used for the entire SMS deployment.

The following principles should be considered when planning a Software Updates package strategy:

- Create the packages at the highest level in the SMS hierarchy from which software updates are to be managed. It is then possible to control package deployment at a more granular level by creating deployments for the packages at child sites. In healthcare organisations with a single point of administration for the whole organisation, this should be done at the Central Site
- A single package can contain multiple software updates, and these updates can be for multiple operating systems and versions. At installation, the Software Updates agent determines which software updates are applicable to a given client computer, and installs only those updates
- Existing packages can be modified to add newly authorised software updates, remove authorisation for a software update, or change installation options
- The number of software updates that need to be distributed can be minimised by keeping client computers current with the latest SP. This reduces the package size

Table 5 lists some potential strategies for Software Update packages, and their respective benefits and drawbacks.

Package Strategy	Detail	Benefit	Drawback
Single package containing all authorised software updates	<ul style="list-style-type: none"> ■ Create a single package for all security updates ■ Modify the package periodically by approving newly released software updates to add to the package 	<ul style="list-style-type: none"> ■ Less overhead in creating a single package ■ Can be useful for organisations with standardised environments, such as most Configuration Manager clients running the same operating system versions and SP levels 	<ul style="list-style-type: none"> ■ Cannot easily be used to retire product versions or SP levels ■ Should not exceed 500 updates per package
Base package and Semi Annual (Rollup) package	<ul style="list-style-type: none"> ■ Administer and maintain the base package that contains all authorised updates for update type ■ Rollup package created every six months with all updates added during the six month period 	<ul style="list-style-type: none"> ■ Minimises size of packages in most active use ■ Maintains Definitive Software Library packages for new resources coming online ■ Allows the administrator to phase out older packages once they are no longer needed 	<ul style="list-style-type: none"> ■ Cannot easily be used to retire product versions or SP levels
Multiple packages organised by product	<ul style="list-style-type: none"> ■ Create a package for each product and SP level 	<ul style="list-style-type: none"> ■ Easily accommodates retiring product versions or SP levels ■ Accommodates non-standardised environments with multiple client operating system versions 	<ul style="list-style-type: none"> ■ More administrative overhead in creating and managing packages

Table 5: Software Update Package Strategies: Benefits and Drawbacks

4.2.1 Single Package Strategy

The simplest package configuration is to have a single package that contains all the software updates that are relevant to the healthcare organisation's network environment. In previous versions of the product, any clients that were not in local (fast) boundaries would have to download the entire contents of the Software Updates package before executing the software update, even if only a small percentage of the updates in the package were applicable to the client. This is no longer the case, so maintaining a single package with all updates that are relevant can reduce the administrative overhead. However, there are drawbacks to the configuration as described in Table 5. Maintaining a single package makes it very difficult to reclaim space used by software updates that are no longer required in the healthcare organisation. For example, if a healthcare organisation has migrated from Windows XP to Windows 7, there would no longer be a need to maintain Windows XP software updates in the Software Update package source folder and on all DPs in the Configuration Manager hierarchy. If a single package strategy has been used, the software updates would need to be manually removed from the Deployment Packages. Figure 5 describes the Single Package Strategy in more detail:

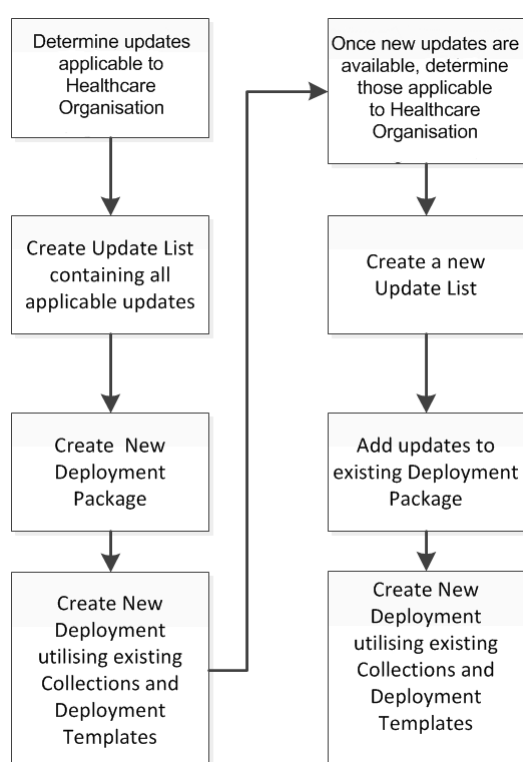


Figure 5: Single Package Strategy Process

4.2.2 Base Package and Semi Annual (Rollup) Strategy

The Base (rollup) package and weekly (or as needed) new updates package strategy works as follows:

- Create one main package that contains all the relevant software updates for the healthcare organisation's Microsoft system infrastructure
- Create a new package on the first month that contains the new updates that are available
- Each month, or as needed, add new updates to the second package until the package contains six months of updates (or however long the healthcare IT Administrator feels appropriate). Once the package is six months old, create a new Deployment Package and start the process again

Figure 6 describes the Base Package and Semi Annual Rollup strategy in more detail:

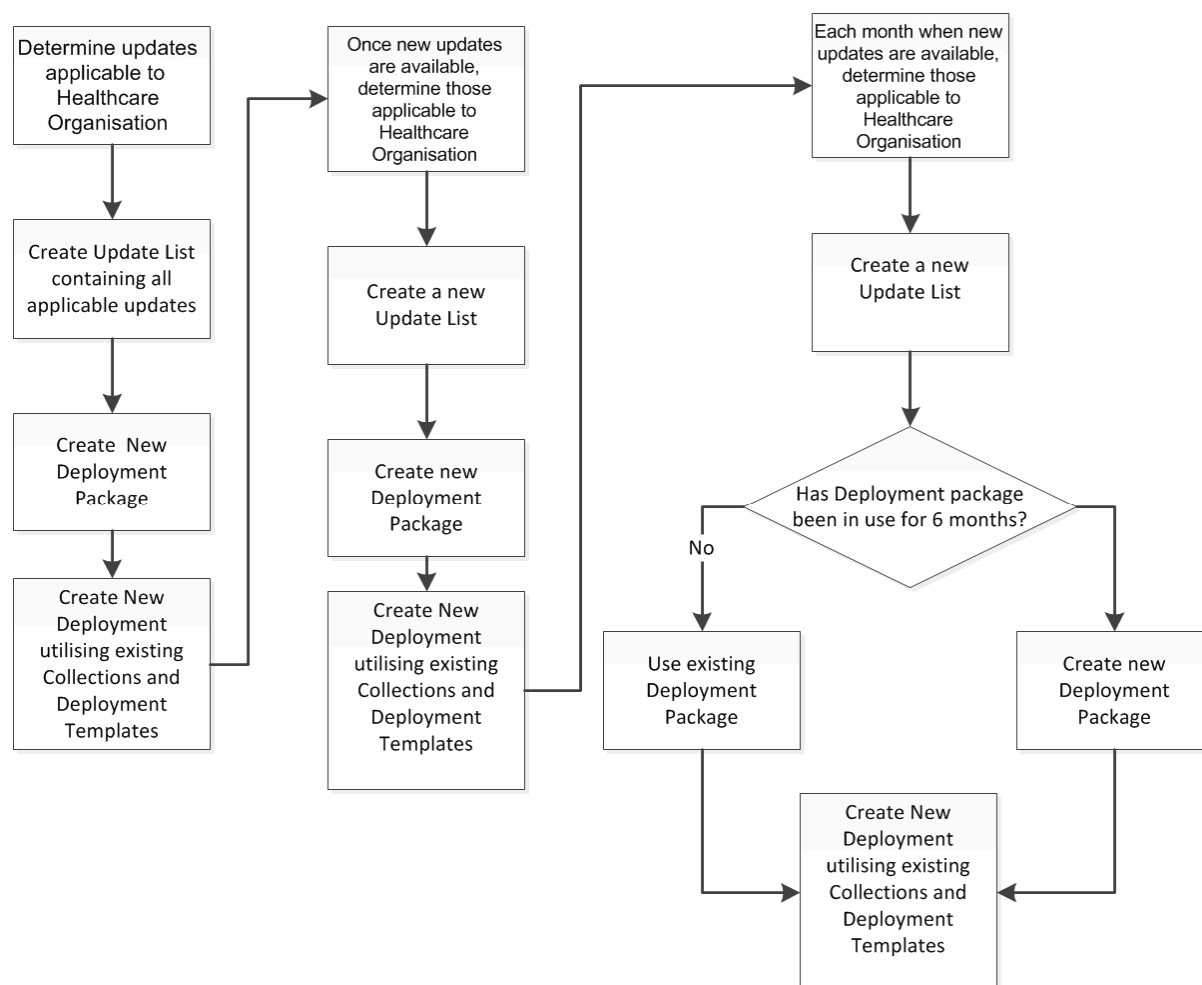


Figure 6: Base Package and Semi Annual Rollup Process

This strategy will allow the IT Administrator to remove old Deployment Packages once the software updates are no longer required in the healthcare organisation.

Caution

Before removing old Deployment Packages the IT Administrator should make sure that there is no possibility that clients will require any of the software updates contained within them. This should be co-ordinated with the healthcare organisation's client and server build strategy to ensure any new machines being added to the network will already have all software updates as part of the build that are contained within the Deployment Packages being retired.

4.2.3 Multiple Packages Organised by Product Strategy

Using multiple Deployment Packages organised by product is the strategy that requires the most administrative effort and works as follows:

- Create a Deployment Package for each Microsoft product that is deployed in the healthcare organisation. For example, a different Deployment Package for Windows XP SP2, Windows XP SP3 and Microsoft Office 2003
- Each month update the existing Deployment Packages with any new applicable updates
- As the healthcare organisation upgrades a product version or SP, the Deployment Package relating to that software can be removed

This strategy is extremely useful for those healthcare organisations that do not have a standardised environment and may not have had an automated means to deploy software updates previously. By using this approach the healthcare organisation can move towards standardising the environment, but still ensuring that existing software is fully up-to-date. As the healthcare organisation moves closer to standardisation, the number of Deployment Packages that will need to be maintained reduces. Using this strategy allows the healthcare organisation to be able to easily maintain only the software updates that are required, and quickly remove any Deployment Packages that are no longer needed. Figure 7 describes the Multiple Packages Organised by Product strategy:

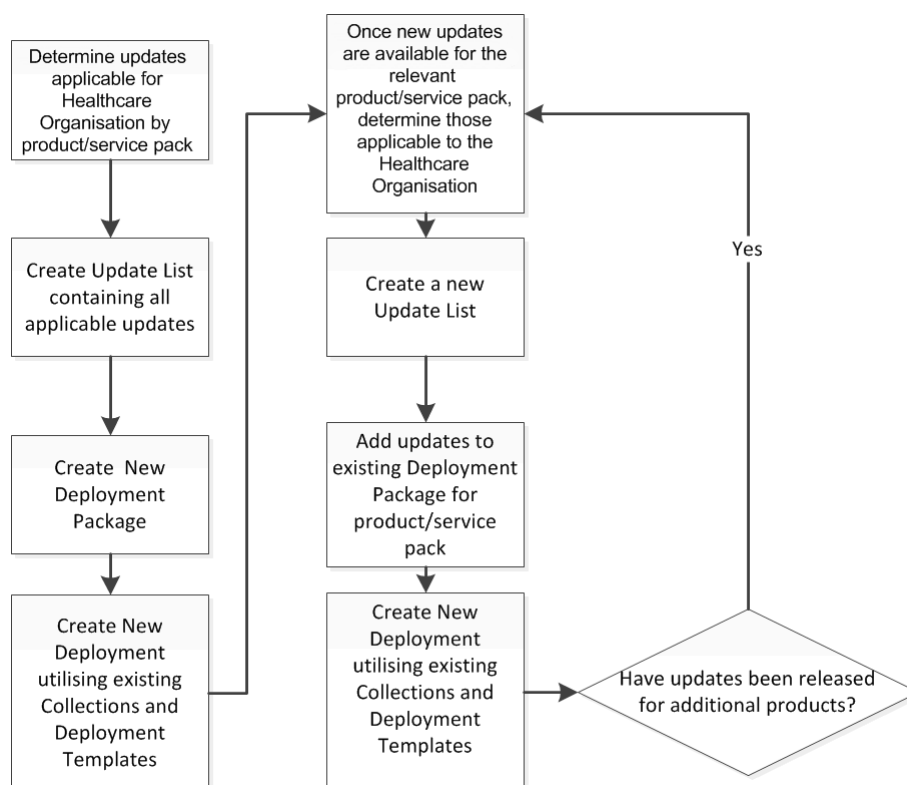


Figure 7: Multiple Packages Organised by Product Strategy

4.3 Planning Update Selection

The healthcare IT Administrator will need to determine which updates are required. The Update Metadata can be very large if all updates are selected, and can make the updates section of the Configuration Manager Administrator Console difficult to manage. Select which updates are required for the healthcare organisation's environment. The updates are broken down into different Products and Classifications.

4.3.1 Products

The healthcare IT Administrator should only choose to synchronise products that are currently available in the healthcare organisation's environment. If a product is upgraded, and therefore no longer available in the healthcare organisation, the product should be removed from the synchronisation list. This will reduce any unnecessary data in the console. The Configuration Manager site server must be synchronised with the SUP at least once before all available products will be presented in the list, as new products are added to the catalogue on a regular basis.

4.3.2 Classifications

The IT Administrator should only choose the classifications that are required to be deployed in the healthcare organisation. This can significantly reduce the amount of data in the Configuration Manager Administrator Console and ease the process of finding and deploying appropriate updates.

Update Classification	Description
Critical Updates	These updates are broadly released and resolve a specific, non-security related bug that could affect system stability. This classification should always be chosen.
Definition Updates	If the healthcare organisation is using any of the Forefront Security products, such as Forefront Client Security or Forefront for Exchange, then this classification should be selected as it contains the anti-malware definition files for those products.
Drivers	This classification will provide metadata on all available drivers. There is no way to specify hardware type prior to synchronisation, so a large amount of data is obtained. Only specify this classification if driver updates are specifically required. An alternative approach would be to download the driver updates for the healthcare organisation's specific hardware, and deploy using the Software Distribution capabilities of Configuration Manager.
Feature Packs	This classification includes updates that provide new product features (usually for server products) which are often included in the next version of the product.
Security Updates	These updates are broadly released and address a specific product related security threat. This classification should always be enabled unless there is a specific reason not to.
Service Packs	These updates contain product SPs. It is often more appropriate to download a SP separately and distribute using the Software Distribution capabilities of Configuration Manager.
Tools	Updates that contain utilities or features required to complete a task. This classification is not regularly used.
Update Rollups	This classification contains updates that are a combination of a number of other updates, for instance Critical, Security and Updates. They are packaged together to ease deployment.
Updates	Contains updates to files applications that are currently installed. If the healthcare organisation is using Forefront Client Security, this classification must be enabled as updated versions of the Forefront Client Security client are deployed using updates of this classification.

Table 6: Software Update Classifications

4.3.3 Languages

If there is not the requirement for languages other than English in the healthcare organisation, the IT Administrator should deselect the other default languages. This will significantly reduce the amount of disk space required to store the downloaded update files. If there is a requirement for additional languages, the healthcare IT Administrator should consider using different Deployment Packages for these languages. Separating the languages into different Deployment Packages allows the IT Administrator greater control over where these language updates are stored. For example, if the requirement for different language updates only exists in a small subsection of the healthcare organisation, such as a clinic, the updates can be deployed to a DP that clients in the clinic connect to and no other DPs. This will reduce the amount of space required to store the updates in the Configuration Manager infrastructure.

4.4 Using Custom Catalogues from Third Party Vendors

With Software Updates in Configuration Manager, it is possible to create update catalogues that can be used by Configuration Manager and operate in exactly the same way as updates provided by Microsoft. The System Center Updates Publisher (SCUP) allows third party software vendors and customers to create catalogues for their own applications. The SCUP is beyond the scope of this documentation, but further information is available in the following articles:

- *System Center Updates Publisher*⁹
- *System Center Updates Publisher 4.5*¹⁰

4.5 Planning Software Update Management Collections

Collections are used by the Software Update feature in Configuration Manager for targeting the updates. Deployment Templates can be created for each collection that will reduce the complexity of deploying the updates, and ensure that software updates are always deployed in a consistent way. It is recommended to use criteria that are unlikely to change regularly to create collections for Software Update distribution. This will help to simplify all of the stages of the Software Update Management process. Stable criteria can include the installed client operating system version and SP level, system role, or target organisation. There should also be different collections to allow for different types of software update criticality. For example, one collection for servers that is used for the standard monthly patch cycle, and a separate collection for the same servers that can be used for an emergency patch deployment. Table 7 lists a suggested starting point for the creation of collections to handle the Software Update process in a healthcare organisation. It is likely that the healthcare IT Administrator will need to adapt these recommendations to suit the exact needs of the organisation, but this will provide a good starting point.

Collection Name	Description	Query
Software Update Collections	Parent collection for organizational purposes. This prevents the console becoming too cluttered and is a good practice for all types of collection.	None.
Test Clients (Monthly Update)	This collection contains a number of machines that are used for the healthcare IT Administrator to perform early testing on. Each software update should be deployed to the test machines before any other machine to ensure the update applies successfully and doesn't cause the machine to fail.	Direct membership collection containing all test systems. These would usually be a number of machines in the IM&T department.
Test Clients (Emergency)	This collection duplicates the standard collection for test machines, but allows a Deployment Template to be created that will target this collection and may have different settings, such as Deadline and Restart Configuration.	Direct membership collection containing all test systems. These would usually be a number of machines in the IM&T department.

⁹ Microsoft TechNet – System Center Updates Publisher {R7}:
<http://technet.microsoft.com/en-us/library/bb531022.aspx>

¹⁰ Microsoft Download Center – System Center Updates Publisher 4.5 {R8}:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0446cce9-94a4-4fb0-b335-e7516044063d&displaylang=en>

Collection Name	Description	Query
Pilot Group (Monthly Update)	This collection contains all machines that have been identified as early adopters. See section 4.8 for information on selecting Pilot computers.	Direct membership collection containing all machines identified as early adopters.
Pilot Group (Emergency)	This collection duplicates the standard collection for pilot machines, but allows a Deployment Template to be created that will target this collection and may have different settings, such as Deadline and Restart Configuration.	Direct membership collection containing all machines identified as early adopters.
Servers (Monthly Update)	This collection contains all servers in the healthcare organisation and its purpose is to target the standard monthly deployment. It is likely that this collection will need to be broken down further in practice and separated based on, for example, service criticality.	Select * from SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like '%Server%'
Servers (Emergency)	This collection duplicates the standard collection for servers, but allows a Deployment Template to be created that will target this collection and may have different settings, such as Deadline and Restart Configuration.	Select * from SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like '%Server%'
Clients (Monthly Update)	This collection represents the client estate in the healthcare organisation. It is likely that this collection would need to be broken down further to separate non-clinical and clinical machines. Additional consideration should be given to machines that reside in critical areas, such as operating theatres.	<p>select SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from SMS_R_System where (SMS_R_System.OperatingSystemNameandVersion = "Microsoft Windows NT Workstation 5.1" or SMS_R_System.OperatingSystemNameandVersion = "Microsoft Windows NT Workstation 6.0") and not SMS_R_System.NetbiosName = "WINXP1" or SMS_R_System.NetbiosName = "Vista1"</p> <p>This query will select all Windows XP and Windows Vista client machines except those called WINXP1 and Vista1. This query can be expanded to select all machines with a certain operating system except those named after the 'and not' section of the query. For example, the machines that are part of the test group of clients</p>

Collection Name	Description	Query
Clients (Emergency)	This collection duplicates the standard collection for clients, but allows a Deployment Template to be created that will target this collection and may have different settings, such as Deadline and Restart Configuration.	<pre>select SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from SMS_R_System where (SMS_R_System.OperatingSystemNameandVersion = "Microsoft Windows NT Workstation 5.1" or SMS_R_System.OperatingSystemNameandVersion = "Microsoft Windows NT Workstation 6.0") and not SMS_R_System.NetbiosName = "WINXP1" or SMS_R_System.NetbiosName = "Vista1"</pre> <p>This query will select all Windows XP and Windows Vista client machines except those called WINXP1 and Vista1. This query can be expanded to select all machines with a certain operating system except those named after the 'and not' section of the query. For example, the machines that are part of the test group of clients</p>

Table 7: Suggested Starting Point for Collection Creation

For information on creating collections, see section 5.1.4.

4.6 Planning Deployment Templates

Deployment Templates allow the healthcare IT Administrator to ensure that software updates are deployed using common settings, and that the administrative overheads of deploying software updates each month are reduced. By configuring Deployment Templates that represent all of the common deployment scenarios, the healthcare IT Administrator can rapidly deploy software updates and ensure they are delivered in a consistent manner. Table 8 contains a recommended starting point for creating Deployment Templates. For information on how to create Deployment Templates, see section 5.1.5.

Deployment Template	Suggested Settings
Test Clients (Monthly Update)	<p>Name: Test Clients (Monthly Update)</p> <p>Collection: Test Clients (Monthly Update)</p> <p>Display/Time Settings: Allow display notifications / UTC / 1 days</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are Microsoft Operations Manager 2005 (MOM) or System Center Operations Manager 2007 (Operations Manager) agents</p> <p>Download Settings: Download from DP and install / Download from unprotected SP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks, or in locations with protected DP's.</p>

Deployment Template	Suggested Settings
Test Clients (Emergency)	<p>Name: Test Clients (Emergency)</p> <p>Collection: Test Clients (Emergency)</p> <p>Display/Time Settings: Allow display notifications / UTC / 1 Hours</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are MOM or Operations Manager agents</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks, or in locations with protected DP's.</p>
Pilot Group (Monthly Update)	<p>Name: Pilot Group (Monthly Update)</p> <p>Collection: Pilot Group (Monthly Update)</p> <p>Display/Time Settings: Allow display notifications / UTC / 3 Days</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are MOM or Operations Manager agents</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks, or in locations with protected DP's.</p>
Pilot Group (Emergency)	<p>Name: Pilot Group (Emergency)</p> <p>Collection: Pilot Group (Emergency)</p> <p>Display/Time Settings: Allow display notifications / UTC / 4 Hours</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>Note</p> <p>If maintenance windows are enforced on clients and a reboot is immediately required, the <i>Allow system restart outside of maintenance window</i> setting should also be applied.</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are MOM or Operations Manager agents</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks, or in locations with protected DP's.</p>

Deployment Template	Suggested Settings
Servers (Monthly Update)	<p>Name: Servers (Monthly Update)</p> <p>Collection: Servers (Monthly Update)</p> <p>Display/Time Settings: Suppress display notifications / UTC / 7 days</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Disable Operations Manager Alerts / Generate Operations Manager Alert if update fails. Only need to be set if server is an Operations Manager Agent</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p>
Servers (Emergency)	<p>Name: Servers (Emergency)</p> <p>Collection: Servers (Emergency)</p> <p>Display/Time Settings: Suppress display notifications / UTC / 1 days</p> <p>Restart Settings: Suppress system restart : None</p> <p>Note</p> <p>The healthcare IT Administrator should exercise caution when applying this setting. This template should only be used if encountering an emergency 'zero-day' threat. A zero day threat means that exploit code is available for a security related threat before the patch has been released by the software vendor. If maintenance windows are enforced on servers, and a reboot is immediately required, the <i>Allow system restart outside of maintenance window</i> setting should also be applied.</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Disable Operations Manager Alerts / Generate Operations Manager Alert if update fails. Only need to be set if server is an Operations Manager Agent</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p>
Clients (Monthly Update)	<p>Name: Clients (Monthly Update)</p> <p>Collection: Clients (Monthly Update)</p> <p>Display/Time Settings: Allow display notifications / UTC / 7 Days</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>Note</p> <p>It may be necessary to suppress restarts on client machines, as well as servers. This is particularly relevant for clinical machines, for example, in operating theatres. For information on maintenance windows as an alternative to suppressing restarts on client machines, see section 4.7.</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are MOM or Operations Manager agents</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks, or in locations with protected DPs.</p>

Deployment Template	Suggested Settings
Clients (Emergency)	<p>Name: Clients (Emergency)</p> <p>Collection: Clients (Emergency)</p> <p>Display/Time Settings: Allow display notifications / UTC / 1 Days</p> <p>Restart Settings: Suppress system restart : Servers</p> <p>Note</p> <p>It may be necessary to suppress restarts on client machines, as well as servers. This is particularly relevant for clinical machines, for example, in operating theatres. For information on maintenance windows as an alternative to suppressing restarts on client machines, see section 4.7. If maintenance windows are enforced on clients and a reboot is immediately required, the <i>Allow system restart outside of maintenance window</i> setting should also be applied.</p> <p>SMS 2003 Settings: Not required unless running SMS 2003 clients</p> <p>Event Generation: Not required unless target clients are MOM or Operations Manager agents</p> <p>Download Settings: Download from DP and install / Download from unprotected DP</p> <p>Note</p> <p>The Download Settings may differ if the healthcare organisation has test clients that are on remote networks or in locations with protected DP's.</p>

Table 8: Suggested Deployment Template Settings

4.7 Planning Maintenance Windows

Maintenance windows allow the healthcare IT Administrator to define specific times that a Configuration Manager client will perform tasks, such as software distribution and software updates. This can be particularly useful when dealing with critical clinical machines, such as operating theatre equipment and servers or during specific times such as year-end in a General Practice organisation. Maintenance windows are configured on a collection, and the settings will apply to all machines within that collection. If a machine is a member of multiple collections that all have maintenance window settings configured, the client will adhere to all maintenance windows. It is important to make sure that a machine is not a member of a number of collections that will enforce too strict a maintenance window policy, as this may prevent any software updates or software distributions from occurring. The healthcare IT Administrator can use the *Maintenance Windows Available to a Particular Client* report if this situation is suspected. Section 5.1.4.1 shows the process for configuring maintenance windows on a collection.

4.8 Planning Pilot Computers for Software Updates

Any software update carries with it a certain amount of risk, although this risk may be small, the nature of software update releases means that they are not fully regression tested and could cause issues with applications deployed in the healthcare organisation. There is no way to completely remove this risk and maintain a fully patched environment, but there are steps the healthcare IT Administrator should take to mitigate the risk:

- Identify and categorise the application in terms of risk
- Identify the application business owners and recruit early adopters
- Create pilot collections

4.8.1 Identifying and Categorising Applications

Maintaining an accurate record of the applications that are installed in the healthcare organisation is an important part of reducing the risk of software updates. Once all applications have been recorded, each should be scored in terms of potential risk. The following is an example scoring system that should be adapted to fit the needs of the healthcare organisation's environment:

1. Clinical Application – High Risk
2. Line of Business Application (for example, accounting) – High Risk
3. Productivity Application – Medium Risk
4. Personal Application (for example, Music Player) – Low Risk

4.8.2 Identifying Application Owners

Once the applications have been identified, the healthcare IT Administrators should identify a key contact with the healthcare organisation that is responsible for the application. This may be a clinician for a clinical application, or a member of the IT team for, for example, a productivity application. These owners are the key contacts for the software update process and the people who should receive first communication when a software update is going to be deployed. It is important that the client machines identified represent a good sample of all client machines within the healthcare organisation and not just machines from the IT Department. Once the owners have been identified, a small subset of around ten percent of the client machines that run the applications (and server machines if the application is client/server) should be identified. Where possible, the machines that are identified should be chosen specifically because if they were to fail due to a software update installation, they would not prevent users performing their day-to-day tasks, but they should also preferably be used as much as any other machine performing that role.

In some circumstances, such as in a high risk environment, consideration should be given to providing an additional client computer that will run the same clinical software, and be used in the same way as an existing machine, solely for the purposes of ensuring the service can continue if a software update causes the clinical application to fail. This should not be necessary in most scenarios.

4.8.3 Creating Pilot Collections

Once the client machines have been identified that will act as early adopters, they should be added to a dedicated pilot collection as described in section 4.5. This will allow the healthcare IT Administrator to install the software updates that are going to be deployed across the whole healthcare organisation to a cross section of the machines that represent the majority of the applications prior to installing to the rest of the estate. The period of time between the pilot deployment and the production deployment is likely to vary depending on the criticality of the update being applied. Deploying software updates in this way allows the group of pilot users to report any issues that have been identified on the early adopter machines without it impacting the service. This allows the healthcare IT Administrators to investigate and correct any issues prior to full production deployment of the software update, and significantly reduces the risk of service interruption. For information on creating collections, see section 5.1.4.

5 DEPLOY

The Deploy phase is used to manage the deployment of core solution components for widespread adoption in a controlled environment. During the managed deployment, the solution is tested and validated through ongoing monitoring and evaluation. A well-planned deployment of solution components as an end-to-end system will enable the delivery of a quality service that meets or exceeds customer expectations.

Figure 8 acts as a high-level checklist, illustrating the critical tasks that an IT Professional responsible for deploying software updates using Configuration Manager needs to perform:

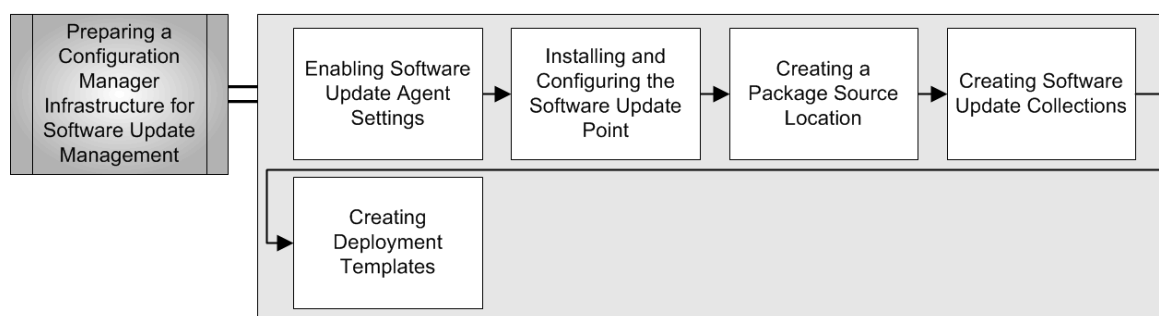


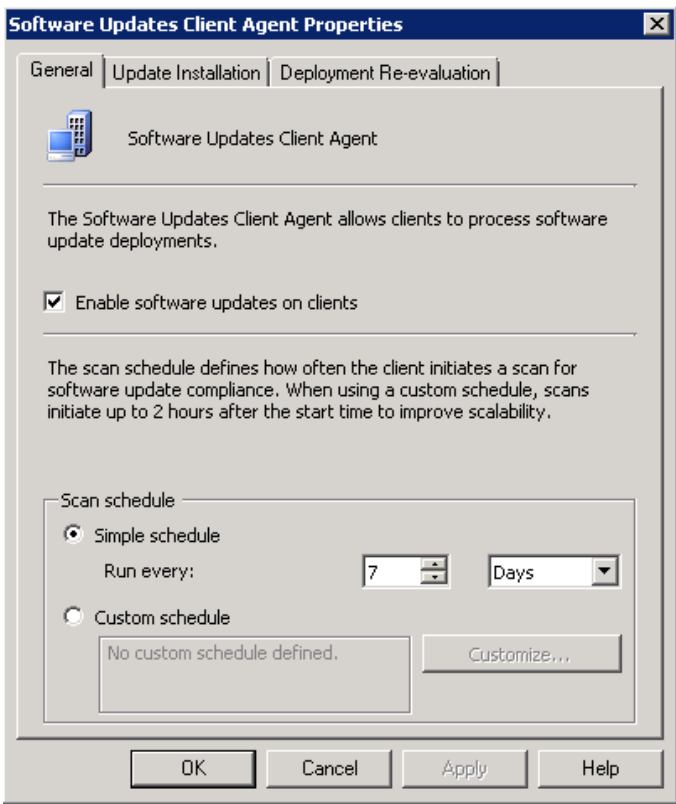
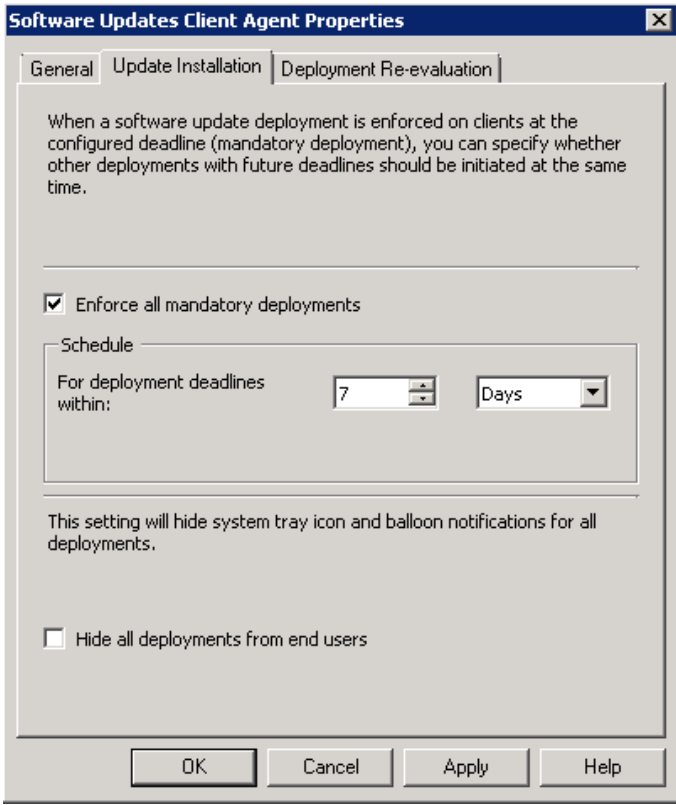
Figure 8: Sequence for Deploying Software Updates Using Configuration Manager

5.1 Preparing a Configuration Manager Infrastructure for Software Update Management

5.1.1 Enabling Software Update Agent Settings

Table 9 shows the steps for enabling the Software Update Agent on Configuration Manager clients. Depending on the schedule configured for the Machine Policy Refresh Cycle, either under the Computer Client Agent settings or on a collection that the client is a member of, this setting can take time to be applied to the client. The healthcare IT Administrator should ensure the agent is enabled prior to deploying software updates.

Step	Description	Screenshot
1.	<p>Open the Configuration Manager Administrator Console and click Client Agents.</p> <p>Click Software Updates Client Agent in the details pane and select Properties.</p>	

Step	Description	Screenshot
2.	<p>In the General tab, select Enable software updates on clients and configure the schedule at which client will scan for software update compliance. The default value is 7 Days, but this can be altered if necessary. Click OK.</p>	
3.	<p>On the Update Installation tab, select Enforce all mandatory deployments. This setting is disabled by default. With the setting enabled, when a software update reaches its deadline for installation, the client will check to see if any other mandatory software updates have a deadline within the specified time period and install them if there are. This can increase security, decrease display notifications, and decrease system restarts. Click Apply and then OK.</p>	

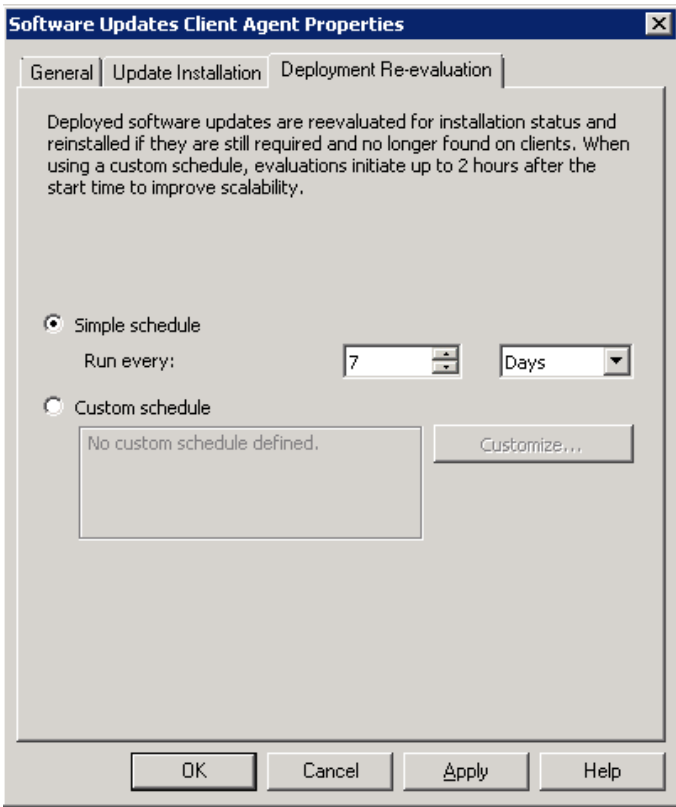
Step	Description	Screenshot
4.	<p>On the Deployment Re-evaluation tab, specify a schedule. The default is 7 Days. This setting configures the client to ensure all applicable software updates are still present, and if they are found to be missing, they are reinstalled.</p> <p>Click OK.</p>	

Table 9: Configuring the Software Update Agent Settings

5.1.2 Installing and Configuring the Software Update Point

If the healthcare organisation is installing the SUP role on a server other than the Configuration Manager site server, ensure that server meets the minimum requirements for the version of WSUS 3.0 that is being installed. At the time of writing, WSUS 3.0 SP2 is the latest version available. The pre-requisite requirements for installing WSUS 3.0 SP2 are listed in the *Microsoft Windows Server Update Services 3.0 SP2 Release Notes*¹¹.


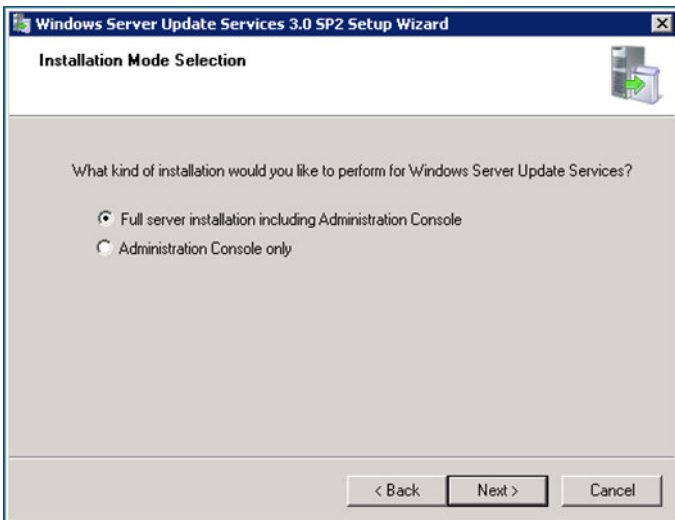
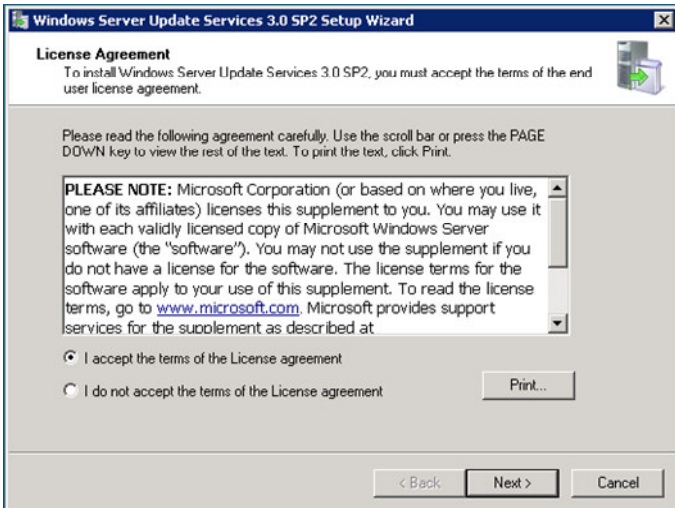
5.1.2.1 Installing WSUS

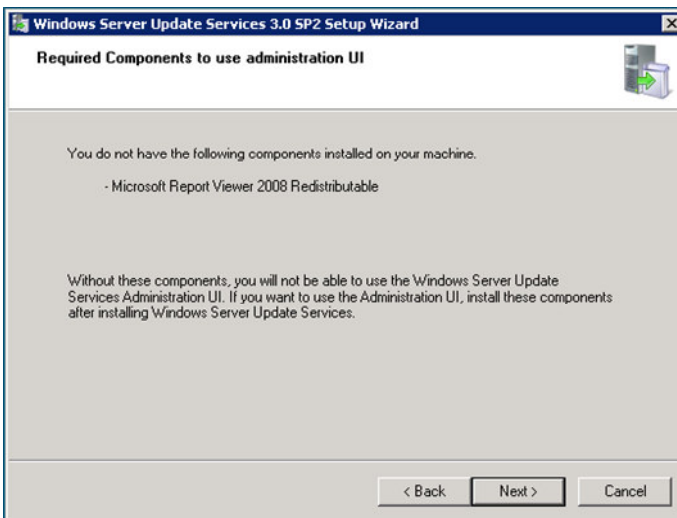
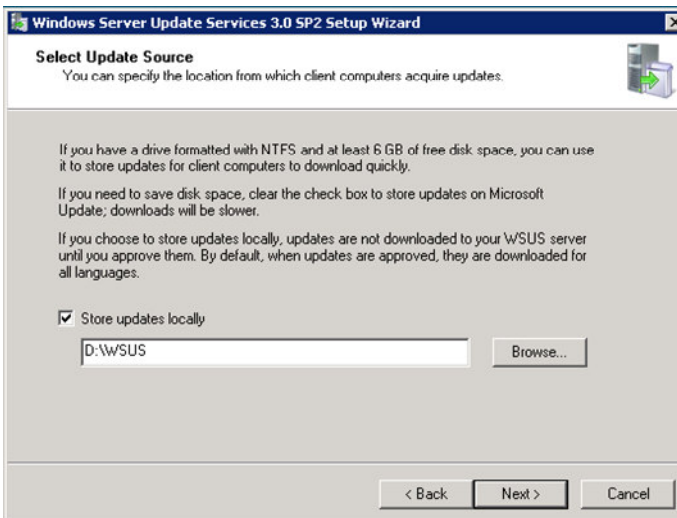
WSUS 3.0 SP1 or higher is required to install a SUP. The SUP can be installed either on the site server or on a remote server computer, depending on the needs of the healthcare organisation. Section 4.1 contains more detail on deciding if the SUP should be local or remote, and how many SUPs will be required if the healthcare organisation's Configuration Manager infrastructure has more than one site. If installing the SUP on a server other than the site server, the WSUS Administration Console must also be installed on the site server to allow the site server to communicate with WSUS on the remote server.

Downloads of the latest version of WSUS 3.0, and links to related information, can be found in the article entitled *Windows Server Update Services*¹².

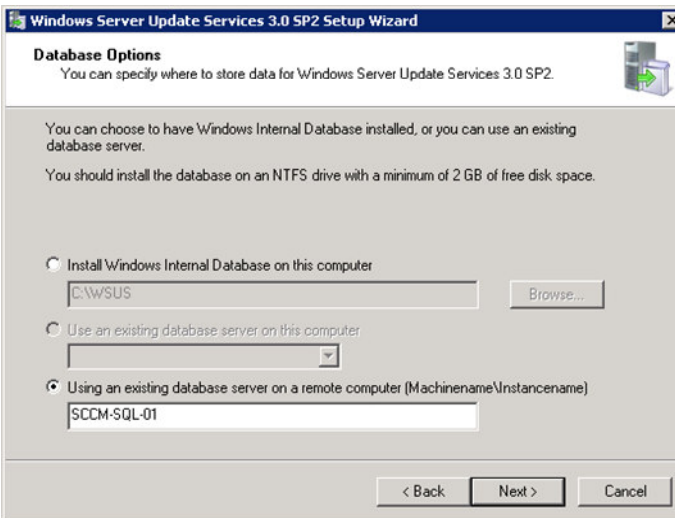
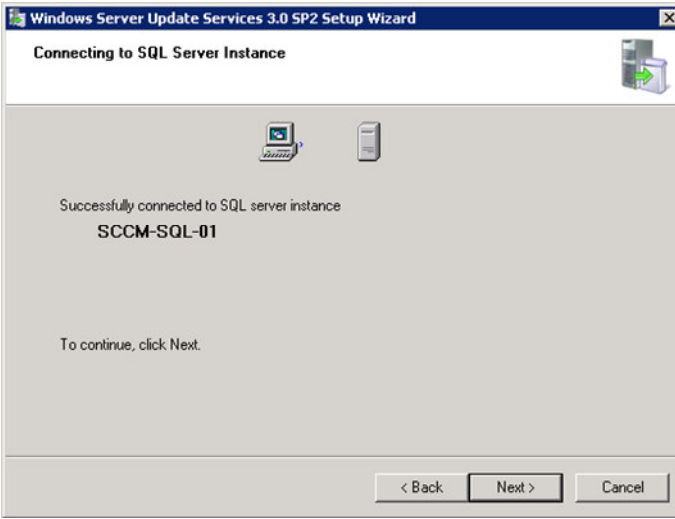
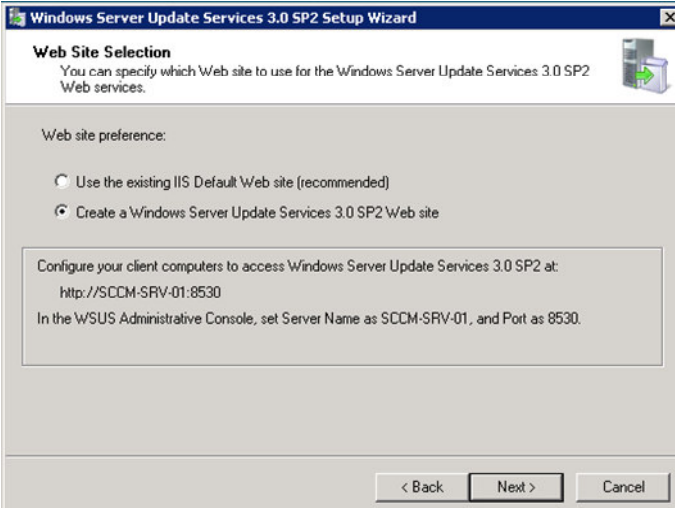
¹¹ Microsoft Download Center – Microsoft Windows Server Update Services 3.0 SP2 Release Notes {R9}:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=ba94a0d3-f22a-4e24-877e-6be6ce5da6d7&displaylang=en#filelist>

¹² Microsoft TechNet – Windows Server Update Services {R10}:
<http://technet.microsoft.com/en-us/wsus/default.aspx>

Step	Description	Screenshot
1.	<p>Run the Windows Server Update Services 3.0 SP2 Setup Wizard (downloaded from the Windows TechNet Website {R10}) that relates to the processor architecture of the server that WSUS will be installed on (for instance, 32 or 64 bit). Click Next.</p>	
2.	<p>Select Full server installation including Administrator Console. Click Next.</p> <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note</p> <p>If the healthcare organisation is installing WSUS on a server other than the Configuration Manager site server, the Administration Console only option should be installed on the site server, in addition to installing the full server on the remote server.</p> </div>	
3.	<p>Read the License Agreement and, if applicable, select I accept the terms of the License agreement. Click Next.</p>	

Step	Description	Screenshot
4.	<p>If the server does not already have the Microsoft Report Viewer Redistributable installed, the Required Components to use administration UI dialog box is displayed. Download the Microsoft Report Viewer Redistributable 2008 executable file from the Microsoft Downloads Website¹³ and install it.</p> <p>Click Next.</p>	
5.	<p>Select Store updates locally and specify a location for the data to be stored.</p> <p>Click Next.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>This location will not store the updates themselves but will store any license or other details relating to the updates. This setting must be enabled for the Configuration Manager SUP to function correctly.</p> </div>	

¹³Microsoft Download Center – Microsoft Report Viewer Redistributable 2008 {R11}:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=CC96C246-61E5-4D9E-BB5F-416D75A1B9EF&displaylang=en>

Step	Description	Screenshot
6.	<p>Specify the Using an existing database server on a remote computer and enter the server name and instance of the SQL server hosting the Configuration Manager database.</p> <p>Click Next.</p> <p>Note</p> <p>If the healthcare organisation is using the Configuration Manager with SQL Technology license for licensing the Configuration Manager server, the WSUS database must be installed into the same instance of SQL server or an additional SQL Server license will be required. If the healthcare organisation wishes to use the Windows Internal Database, or a separately licensed version of SQL, those details should be entered.</p>	
7.	<p>Click Next.</p> <p>Tip</p> <p>If the server cannot be reached at this stage, check the firewall settings on the SQL server and ensure it is reachable from the server where WSUS is being installed.</p>	
8.	<p>Select one of the following:</p> <ul style="list-style-type: none"> ■ If WSUS is being installed on a dedicated server select Use the existing IIS Default Web site. ■ If WSUS is being installed on the same server as the Configuration Manager site server, select Create a Windows Update Services 3.0 SP2 Web site. <p>Click Next.</p>	

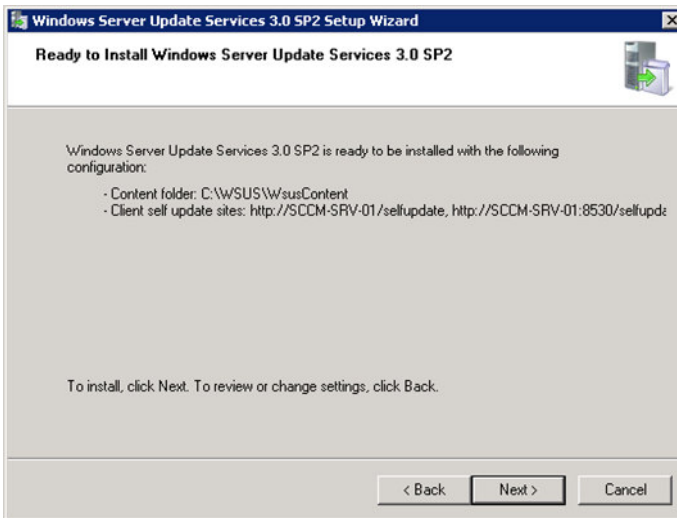
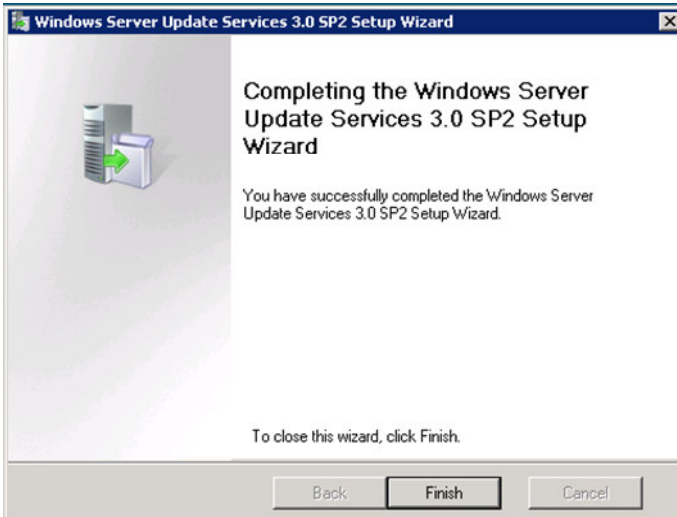
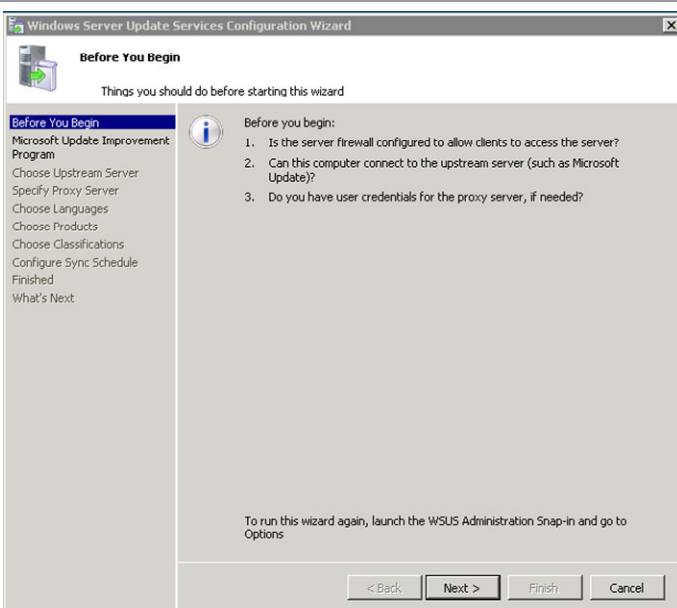
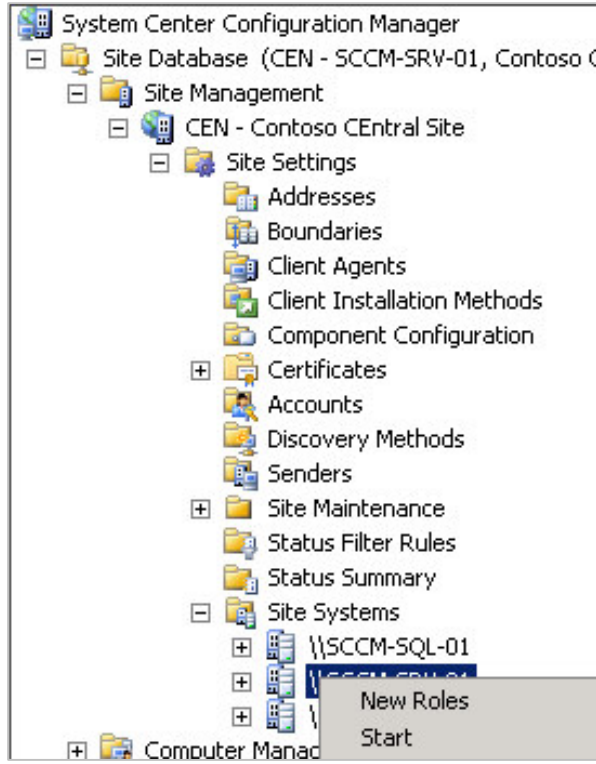
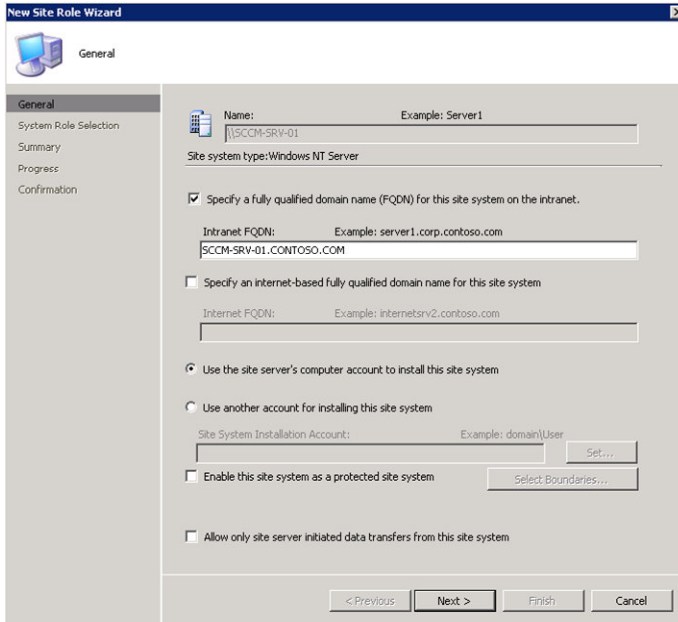
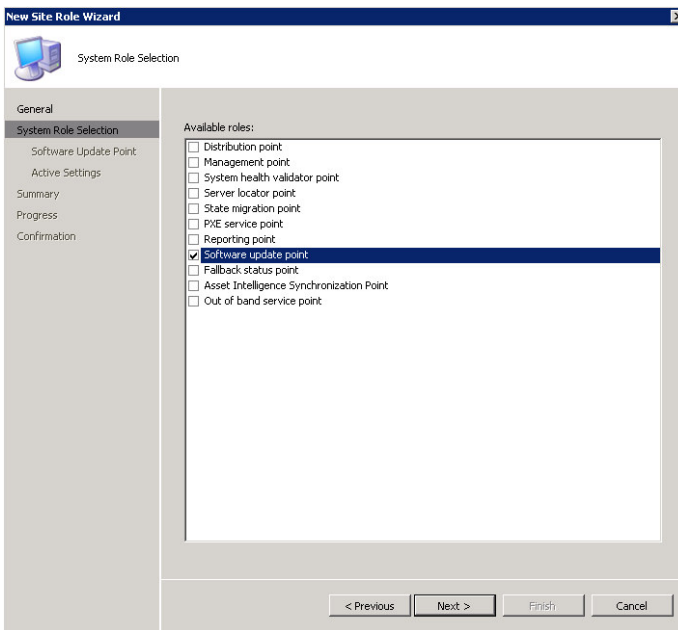
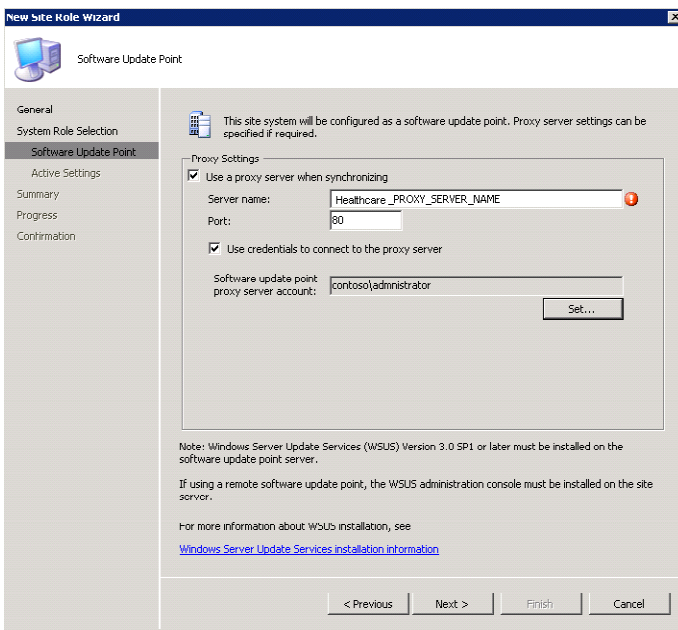
Step	Description	Screenshot
9.	Click Next .	
10.	Click Finish .	
11.	Click Cancel .	<div> <div> <p>Important</p> <p>This step is not required as Configuration Manager will configure WSUS when the SUP is configured so the wizard can be cancelled.</p> </div> <div>  </div> </div>

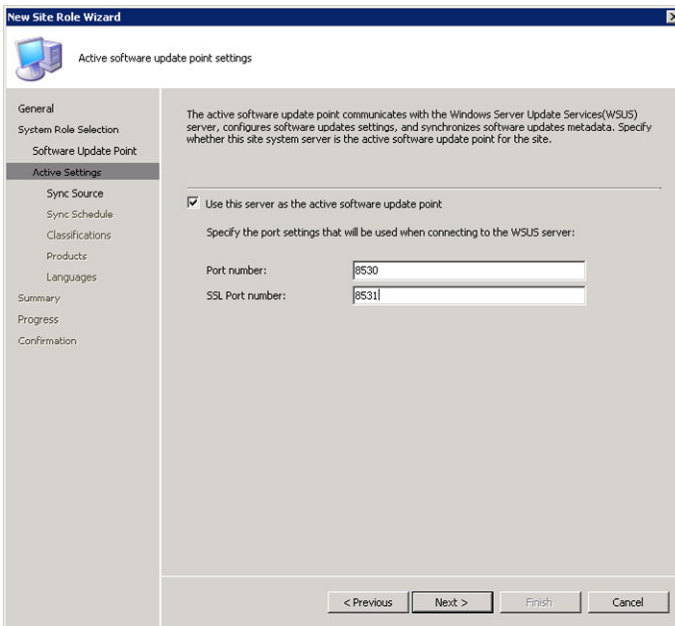
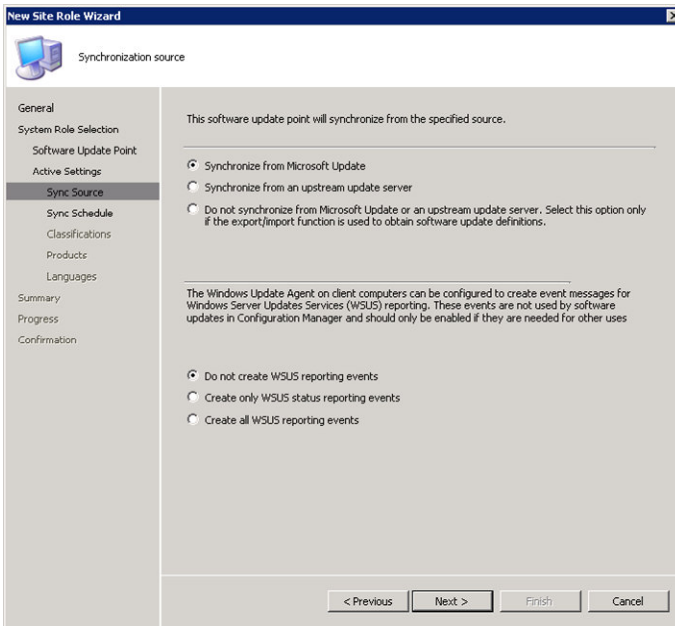
Table 10: Installing WSUS 3.0

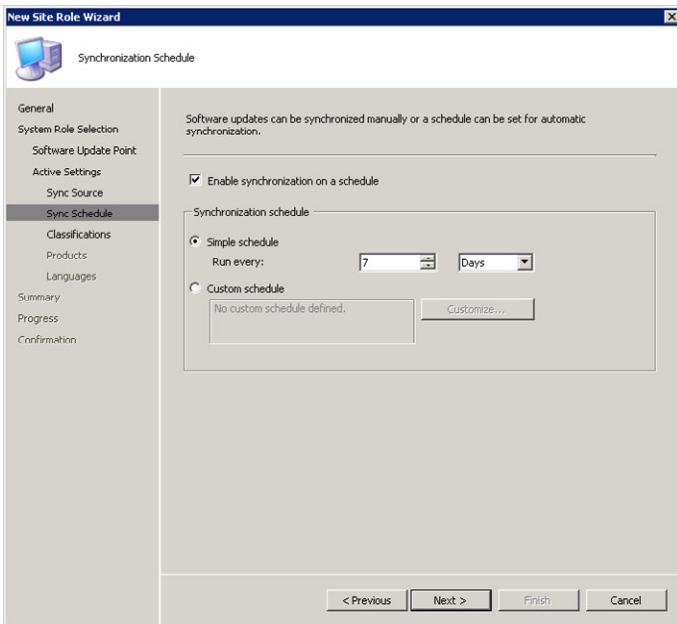
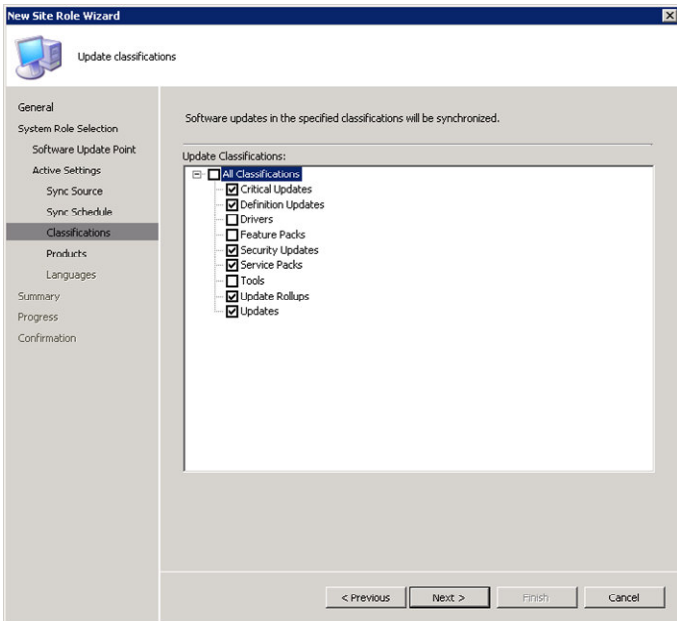
5.1.2.2 Configuring the Software Update Point

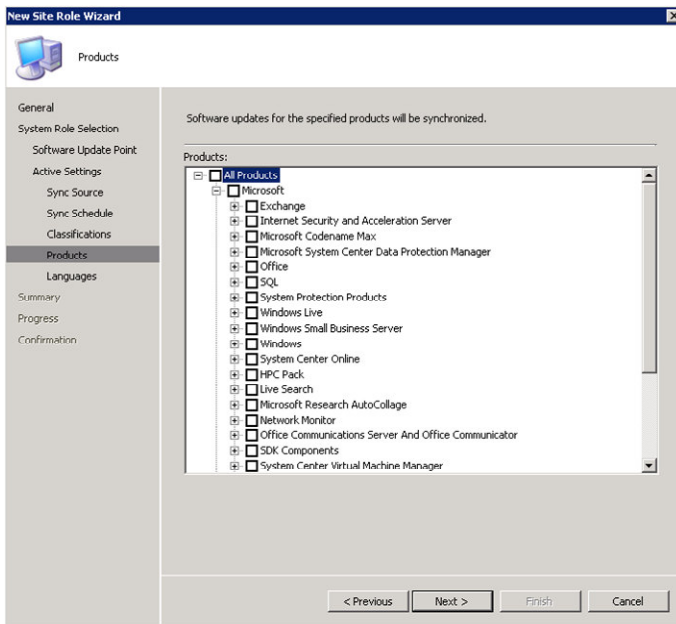
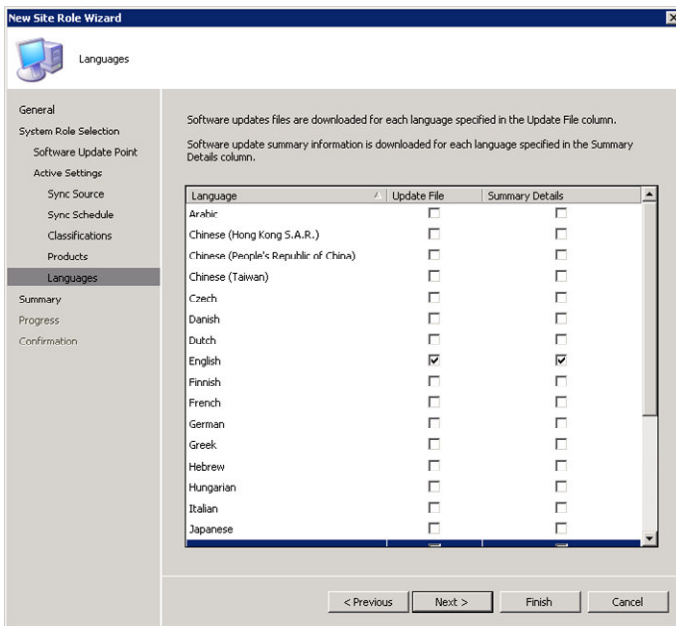
Table 11 shows the steps required to configure the WSUS server to become a Configuration Manager SUP.

Step	Description	Screenshot
1.	<p>Open the Configuration Manager Administrator Console and right click the server object that will host the SUP role under Site Systems.</p> <p>Select New Roles.</p>	
2.	<p>Select Specify a fully qualified domain name (FQDN) for this site system on the intranet and enter the Intranet FQDN that client will use to access the SUP from the healthcare organisation internal network (for example, SUPSERVER.HCODOMAIN.HCO.UK).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>Ensure the site server's computer account is added to the Local Administrators group of the remote server if not installing the SUP role on the Configuration Manager site server.</p> </div> <p>Click Next.</p>	

Step	Description	Screenshot
3.	Select Software update point . Click Next .	 <p>The screenshot shows the 'New Site Role Wizard' window with the 'System Role Selection' tab active. In the 'Available roles' list, 'Software update point' is selected. Other roles include Distribution point, Management point, System health validator point, Server locator point, State migration point, PXE service point, Reporting point, Fallback status point, Asset Intelligence Synchronization Point, and Out of band service point. Navigation buttons at the bottom include '< Previous', 'Next >', 'Finish', and 'Cancel'.</p>
4.	<p>If the healthcare organisation uses a proxy server, select Use a proxy server when synchronizing and specify the Server name and Port. If the proxy server requires user authentication, enter the account details of a user that has access to the internet.</p> <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Important</p> <p>If the user account specified requires a password change periodically, the healthcare IT Administrator can modify the password by right clicking the ConfigMgr software update point object under Site Systems in the Configuration Manager Administrator Console.</p> </div> <p>Click Next.</p>	 <p>The screenshot shows the 'New Site Role Wizard' window with the 'Software Update Point' tab active. The 'Proxy Settings' section is expanded, showing 'Use a proxy server when synchronizing' checked. The 'Server name' is 'Healthcare_PROXY_SERVER_NAME' and the 'Port' is '80'. 'Use credentials to connect to the proxy server' is also checked, with the 'Software update point proxy server account' set to 'contoso/administrator'. A 'Set...' button is next to the account field. A note at the bottom states: 'Note: Windows Server Update Services (WSUS) Version 3.0 SP1 or later must be installed on the software update point server. If using a remote software update point, the WSUS administration console must be installed on the site server. For more information about WSUS installation, see Windows Server Update Services installation information.' Navigation buttons at the bottom include '< Previous', 'Next >', 'Finish', and 'Cancel'.</p>

Step	Description	Screenshot
5.	<p>Select Use this server as the active software update point and specify the Port number and SSL Port number.</p> <p>If WSUS was installed using the Default Web site option, these values will be 80 and 443. If WSUS was installed using the Create a WSUS Web site option, the values will be 8530 and 8531.</p> <p>Click Next.</p>	
6.	<p>Specify Synchronize from Microsoft Update and Do not create WSUS reporting events.</p> <p>Click Next.</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 10px;"> <p>Note</p> <p>If the healthcare IT Administrator is installing a SUP at a child primary site, the Synchronize from an upstream update server option must be selected.</p> </div>	

Step	Description	Screenshot
7.	<p>Select Enable synchronization on a schedule and select the schedule. The default setting is 7 Days. This should meet the needs of most healthcare organisations but can be modified if required.</p> <p>Click Next.</p>	
8.	<p>Select the check boxes for the Update Classifications required within the healthcare organisation. See section 4.3.2 for more information on Classifications.</p> <p>Click Next.</p>	

Step	Description	Screenshot
9.	<p>Select the check boxes for the Products required within the healthcare organisation. See section 4.3.1 for more information on Classifications.</p> <p>Click Next.</p> <div> <p>Important</p> <p>During the SUP setup, the list of products may not be complete as synchronisation has not yet occurred. If products are required that are not on the list, wait until the first synchronisation has occurred and modify the list using the Software Update Point Component dialogue under Site Settings > Component Configuration in the Configuration Manager Administrator Console.</p> </div>	
10.	<p>Deselect all languages except English unless there is a specific reason why the healthcare organisation needs to provide language support other than English.</p> <p>Click Next.</p>	

Step	Description	Screenshot
11.	Click Next .	
12.	Click Close .	<div> <div> <p>Tip</p> <p>Check the wsyncmgr.log on the site server to check the progress of the first synchronization. Depending on the categories and products chosen, and the speed of the internet connection, it can take a number of hours to complete. The SUP will synchronise automatically when first set up. If the healthcare IT Administrator needs to force a synchronisation, right click on Update Repository under Computer Management > Software Updates and choose Run Synchronization. This can be useful on during the monthly Microsoft patch release cycle to force a synchronisation outside the normal schedule.</p> </div> <div> </div> </div>

Table 11: Configuring the Software Update Point

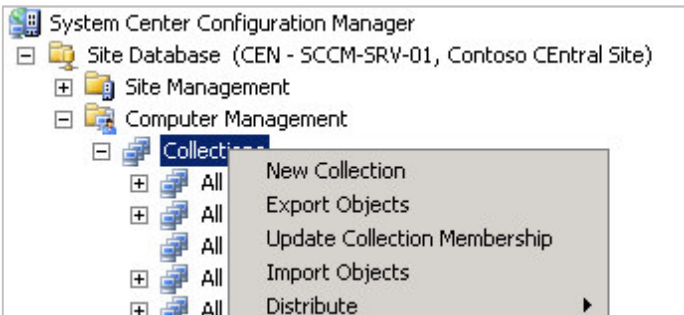
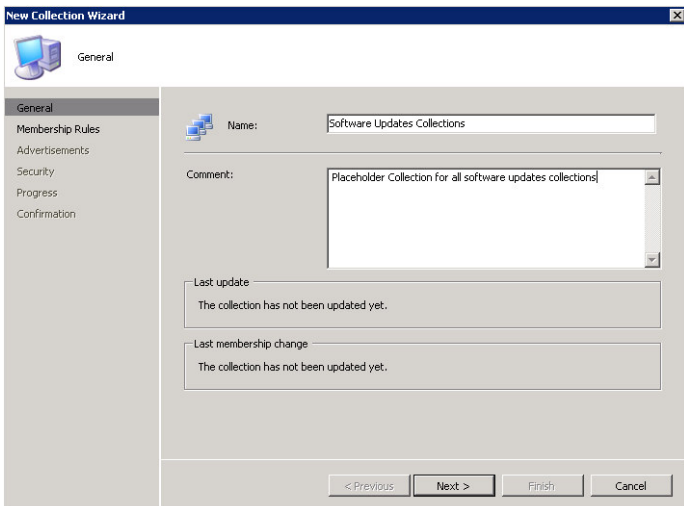
5.1.3 Creating a Package Source Location

The package source location is where all downloaded updates will be stored. It is important to ensure that enough free disk space is available for all potential updates that may be applicable at one time. It is also good practice to make the Access Control Lists (ACL) on this share as restrictive as possible. Users will not require access to this share as the updates will be deployed from the DPs. Only the site server computer account, and any administrators that will create Deployment Packages, should have access to the folder. When Deployment Packages are formed, they should be created as subfolders of the folder. Depending on the deployment strategy decided upon, the folders should be named and arranged logically to make it easy to remove folders for updates that are no longer required in the healthcare organisation and reclaim the associated disk space. Deleting the Deployment Package will not delete the contents held in the package source location.

5.1.4 Creating Software Update Collections

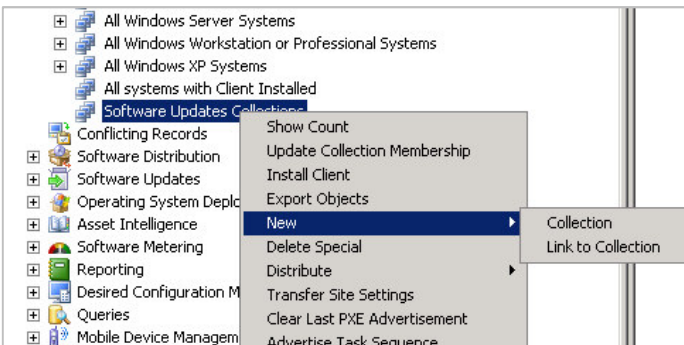
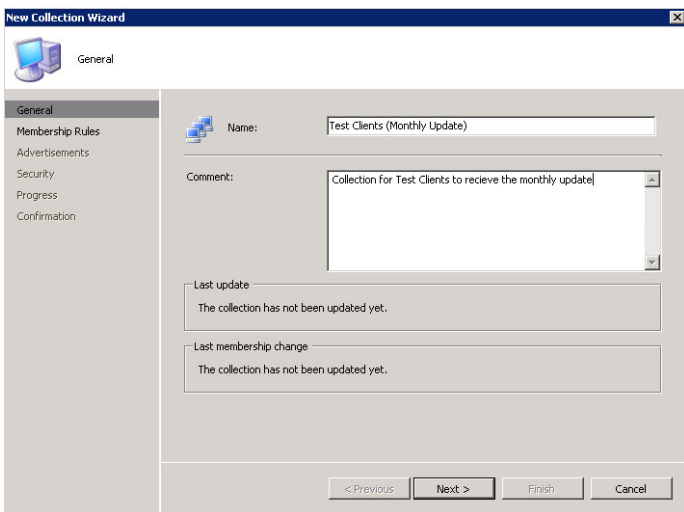

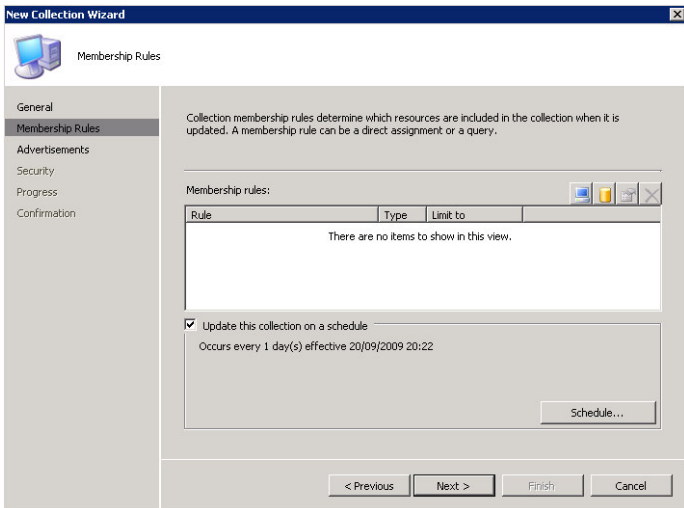
Collections are created to group together machines that will receive the software updates. Section 4.5 lists a recommended starting point for creating Software Update Management collections. Table 12 shows the process for creating the collections.

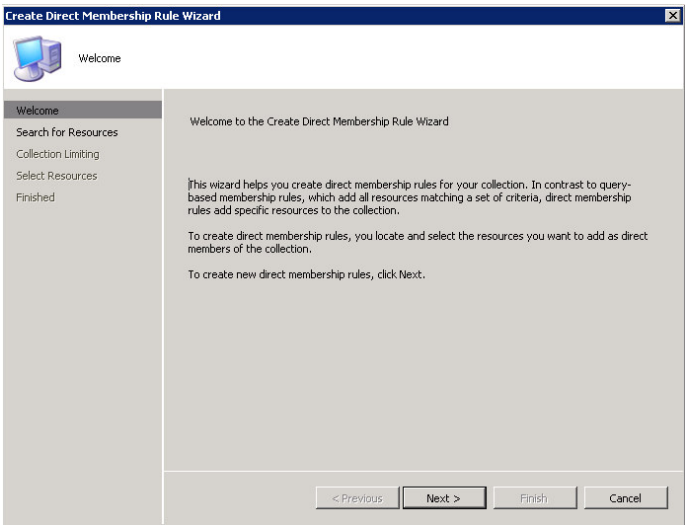
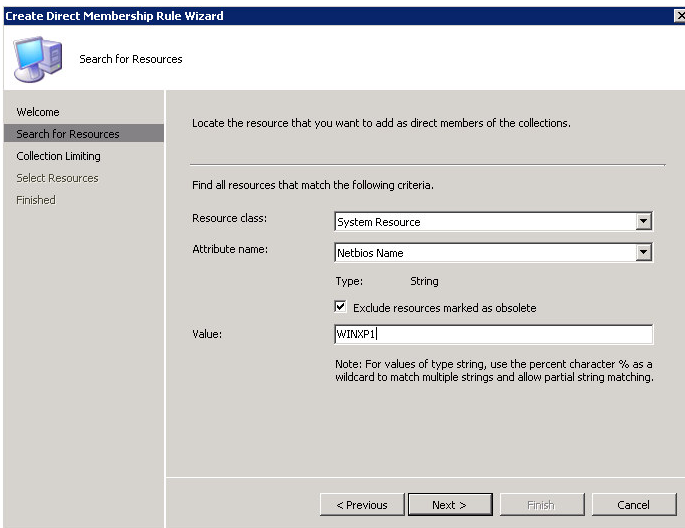
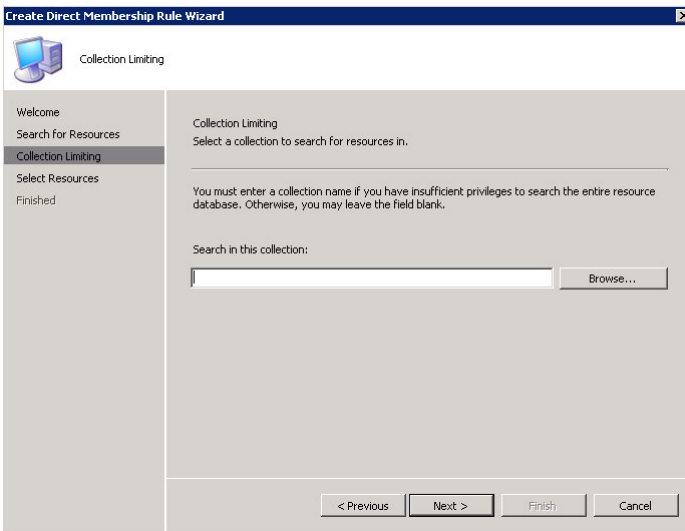
At least the recommended starting collections should be created prior to any software update deployment. It is strongly recommended to maintain a standard naming convention and process for creating the software update collections, as this will significantly reduce the complexity of managing the on-going software updates deployment process.

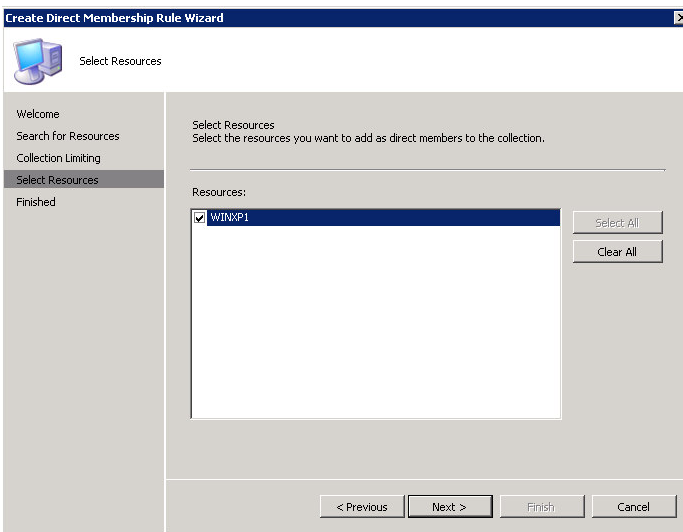
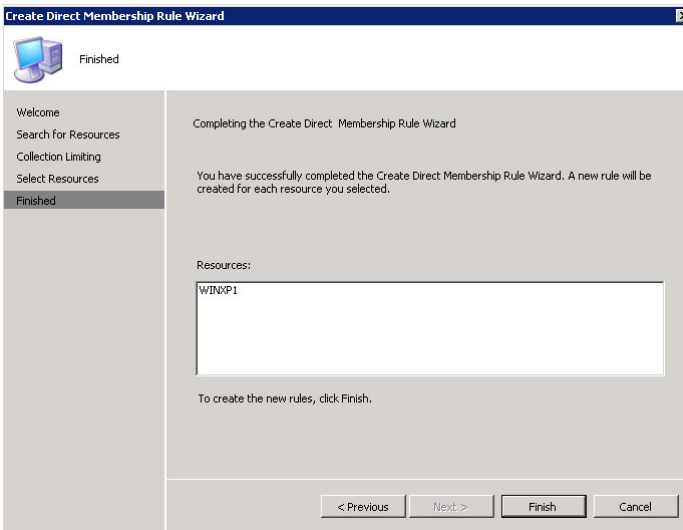

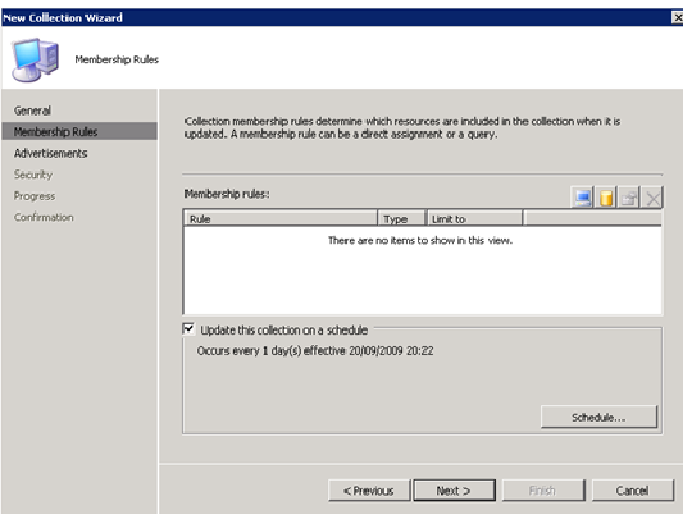
Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , right click Collections , and then select New Collection .	
2.	Enter the name Software Updates Collections and a description. Click Next , Next , Next and then Finish .	

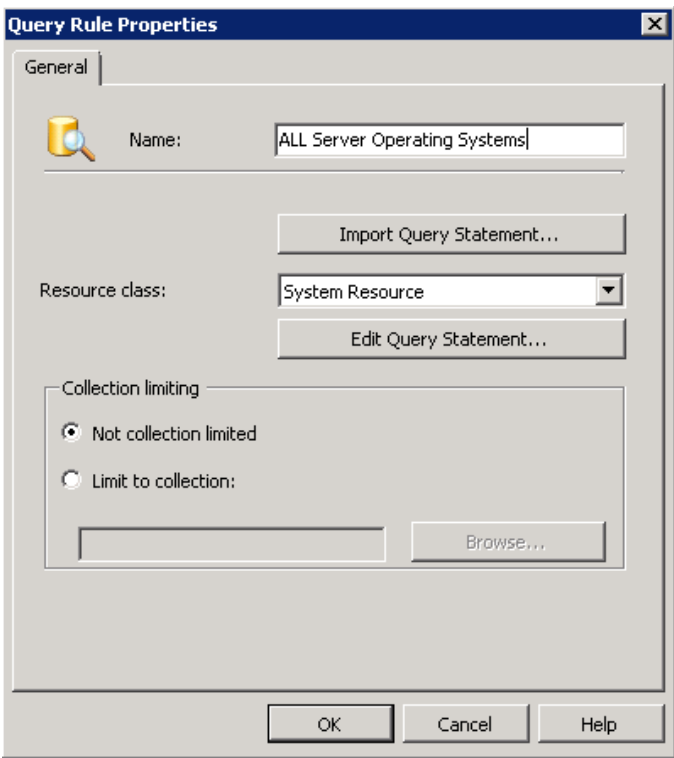

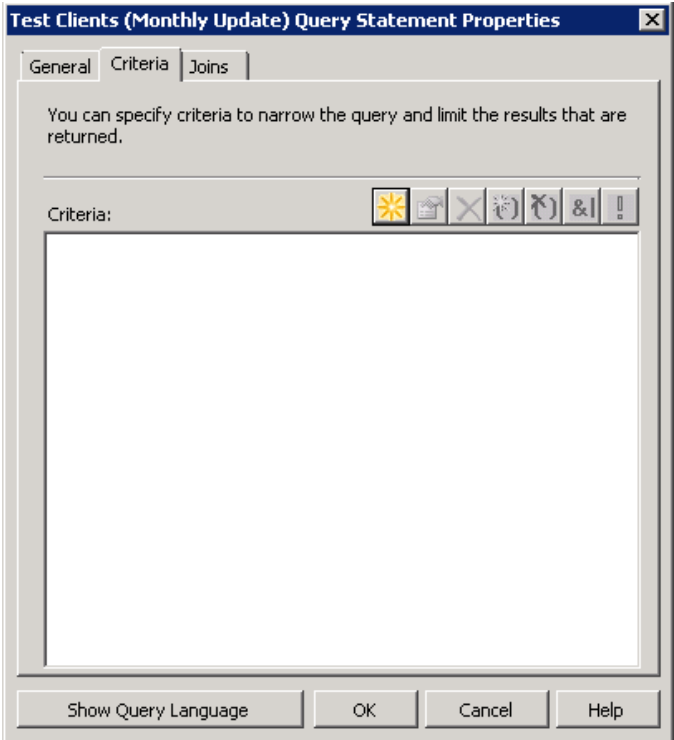
Note

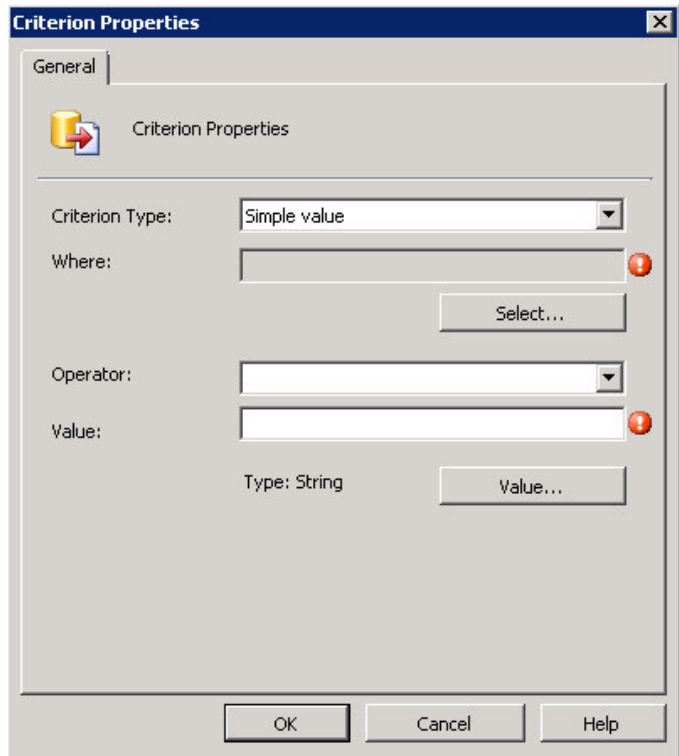
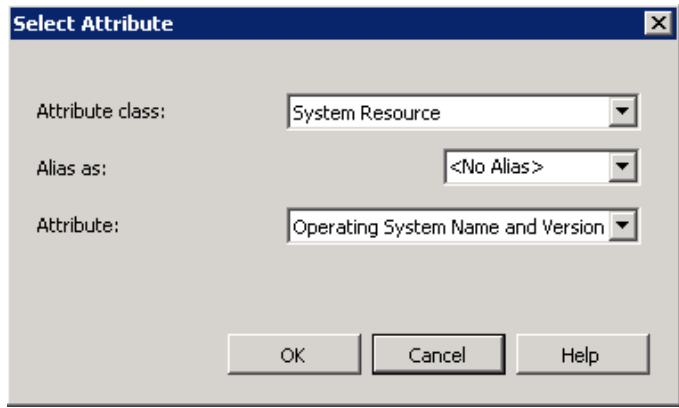
This process creates the placeholder collection for software updates and only needs to be completed once. All subsequent software update collections will be created as a sub-collection.

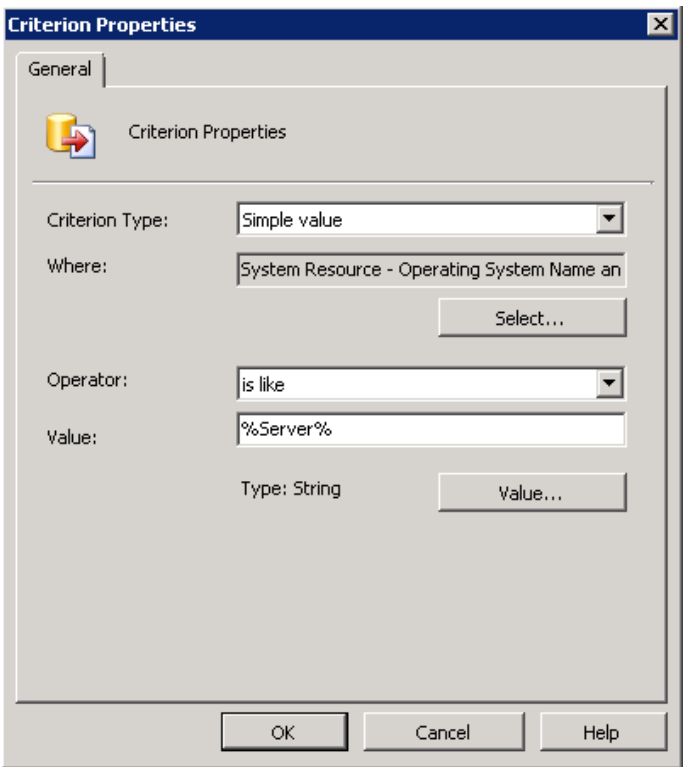
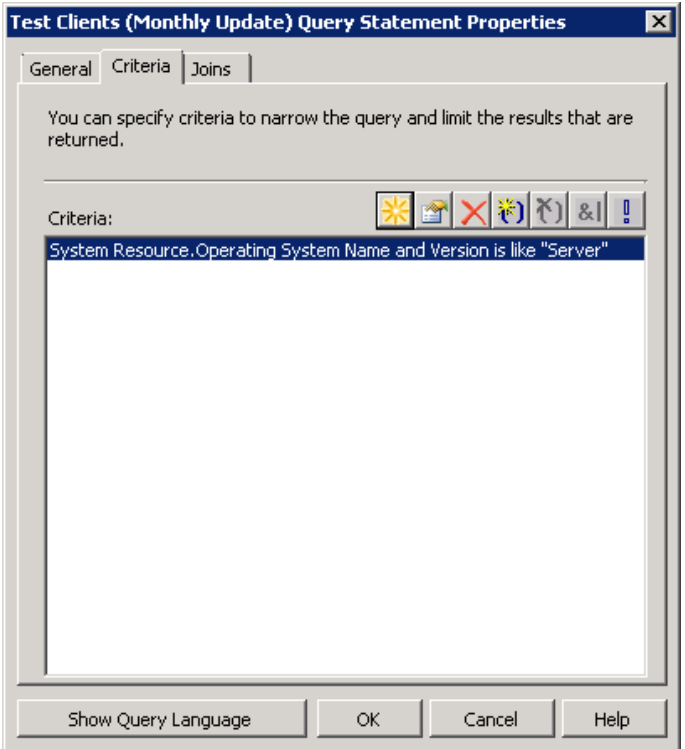
Step	Description	Screenshot
3.	<p>Right click Software Updates Collections collection and select New and then Collection.</p> <p>Note</p> <p>Details of the suggested starting collections are listed in section 4.5.</p>	
4.	<p>Enter the collection Name and a Description.</p> <p>Click Next.</p>	
5.	<p>Note</p> <p>Collections are made up from either Direct Membership rules which allow specific machines to be added, or from query rules which will dynamically add machines based on the query criteria. If creating a Direct Membership Collection, follow steps 5 to 10. If creating a Query based Collection, proceed to step 11.</p> <p>Click the Direct Membership button </p>	

Step	Description	Screenshot
6.	Click Next .	
7.	<p>Click the Resource class drop-down arrow and select System Resource.</p> <p>Click the Attribute name drop-down arrow and select Netbios Name.</p> <p>In the Value box, enter the name of the machine to be added to the collection.</p> <p>Click Next.</p> <div> <p>Tip</p> <p>The % character can be used as a wildcard if multiple machines need to be entered with similar NetBIOS names.</p> </div>	
8.	<p>Click Next.</p> <div> <p>Note</p> <p>There is no need to enter a collection name if the user has full rights to all Configuration Manager collections, such as the site administrator. If the healthcare IT Administrator only has rights to a subset of collections, the collection containing the resource that the healthcare IT Administrator has right to must be selected.</p> </div>	

Step	Description	Screenshot
9.	<p>In the list of Resources, select the check box for the required resource. If a wildcard was used, or only part of the NetBIOS name, multiple machines can be selected from the list.</p> <p>Click Next.</p>	
10.	<p>Click Finish.</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 10px;"> <p>Note</p> <p>If creating a Direct Membership Collection, proceed to step 18.</p> </div>	
11.	<p>Click on the Query Membership rule button </p>	

Step	Description	Screenshot
12.	<p>Enter a Name for the collection and click Edit Query Statement.</p> <p>Note</p> <p>This example will create a collection query for all server operating systems.</p>	
13.	<p>On the Criteria tab, click the New Criteria button .</p>	

Step	Description	Screenshot
14.	Click Select .	
15.	<p>Click the Attribute class drop-down arrow and select System Resource.</p> <p>Click the Attribute drop-down arrow and select Operating System Name and Version for Attribute.</p> <p>Click OK.</p>	

Step	Description	Screenshot
16.	<p>Click the Operator drop-down arrow and select is like.</p> <p>In the Value box, enter %Server%.</p> <p>Click OK.</p>	
17.	Click OK twice.	

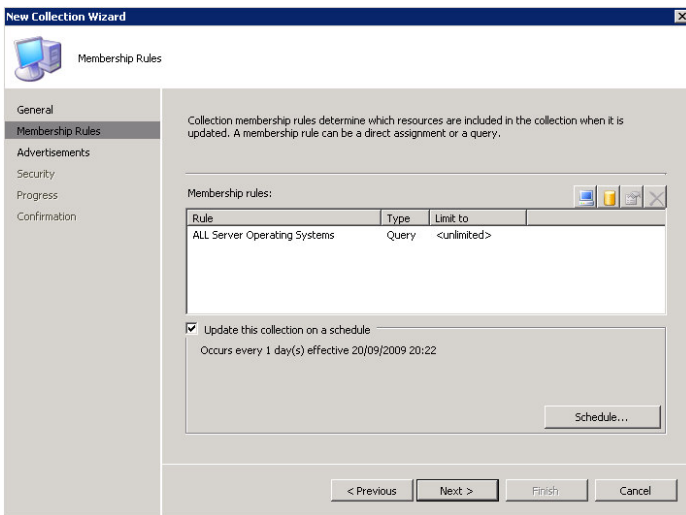
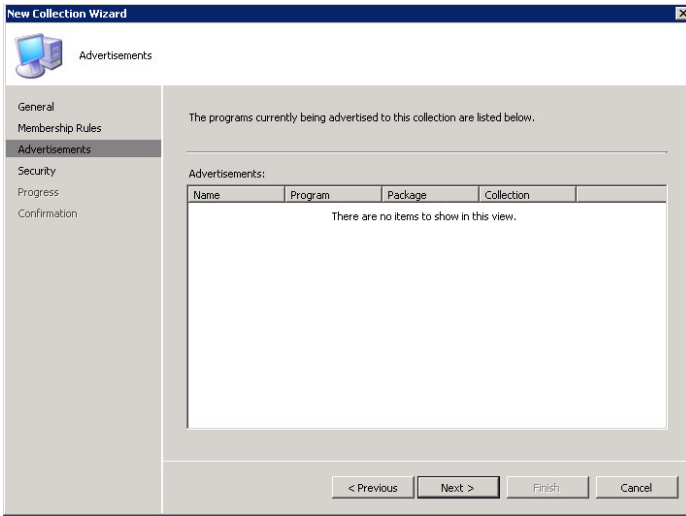
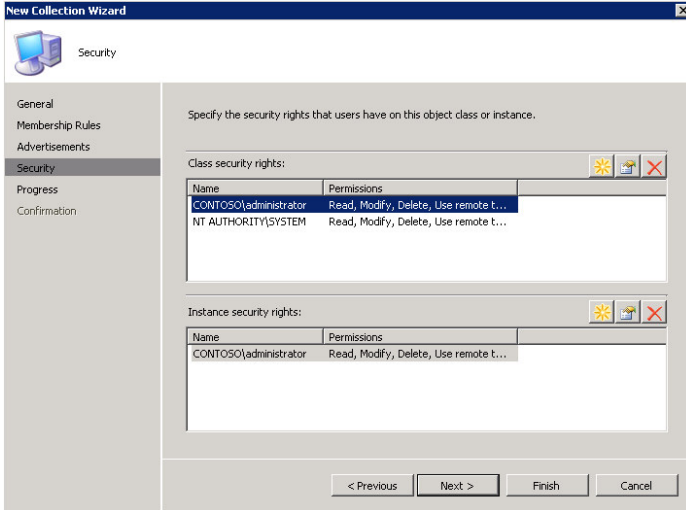
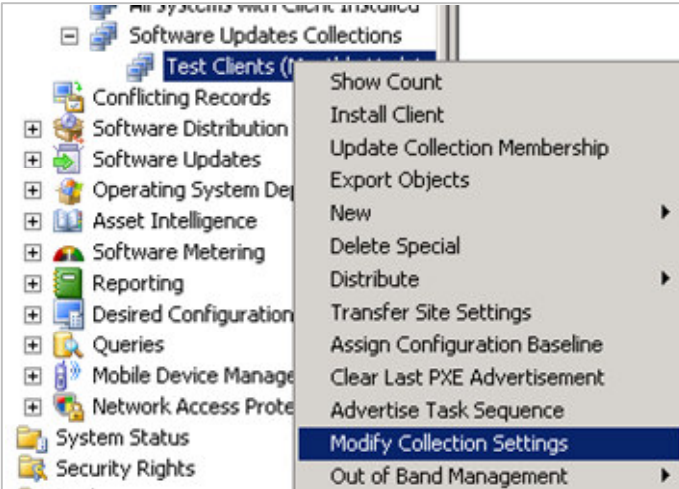

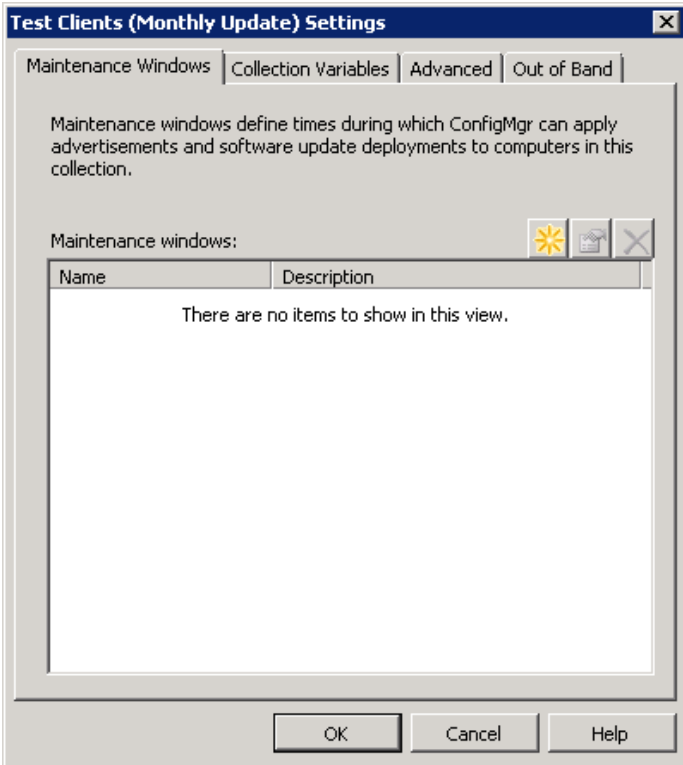
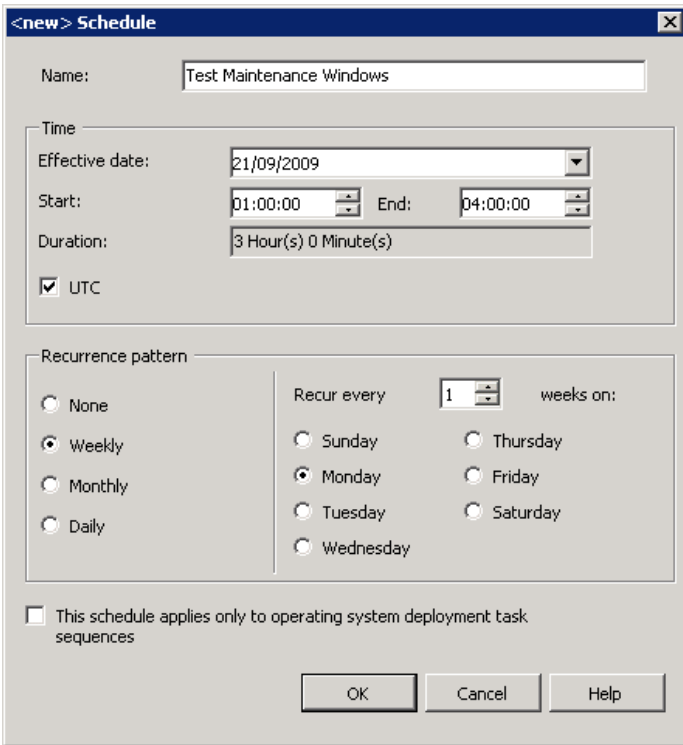
Step	Description	Screenshot
18.	Click Next .	
19.	Click Next .	
20.	Click Next .	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; padding-right: 10px;"> <p>Note</p> <p>If additional healthcare IT Administrators need to be given specific permissions to the collection for delegation purposes those users should be added to the Instance security rights section.</p> </div> <div style="flex: 2;">  </div> </div>

Table 12: Creating Collections

Maintenance windows allow the healthcare IT Administrator to schedule times that Configuration Manager clients will be allowed to install software updates and software distribution packages. See section 4.7 for more information on maintenance windows. Table 13 shows the process for configuring maintenance windows.

Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , right click the collection where the maintenance window should be configured, and select Modify Collection Settings .	

Step	Description	Screenshot
2.	On the Maintenance Windows tab, select the New maintenance windows button 	
3.	Enter a Name for the maintenance window. Specify a schedule. The maintenance window can be configured for a one off window or on a recurring schedule. Click OK .	

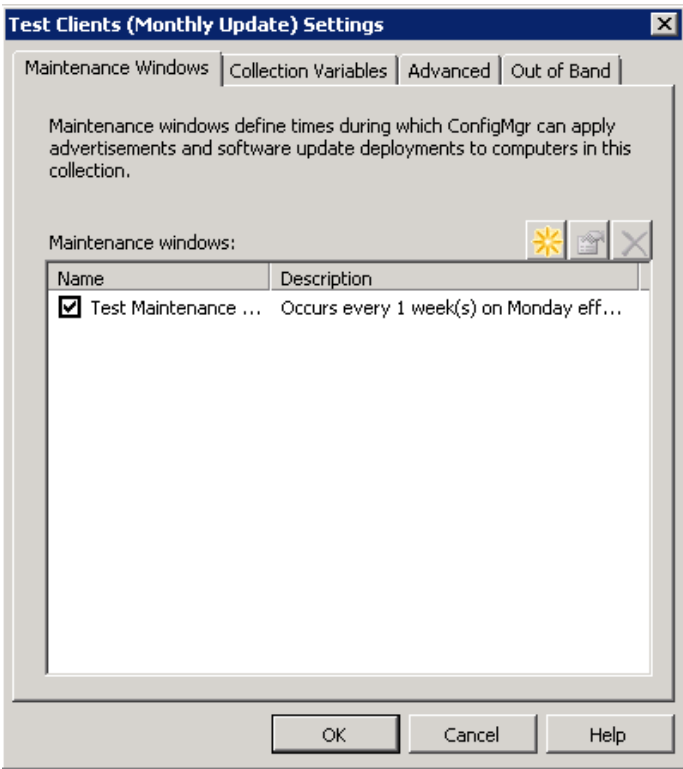
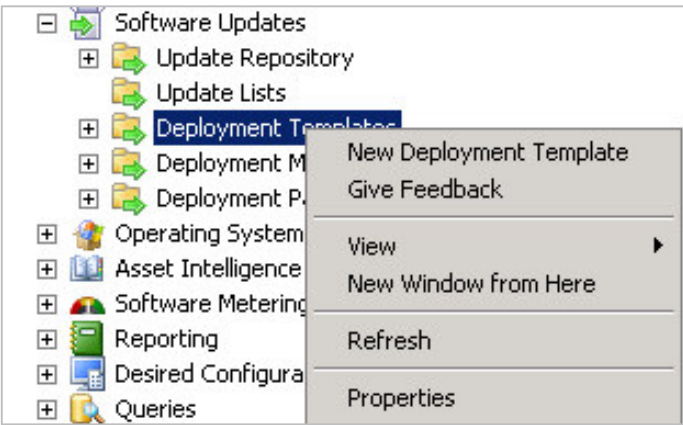
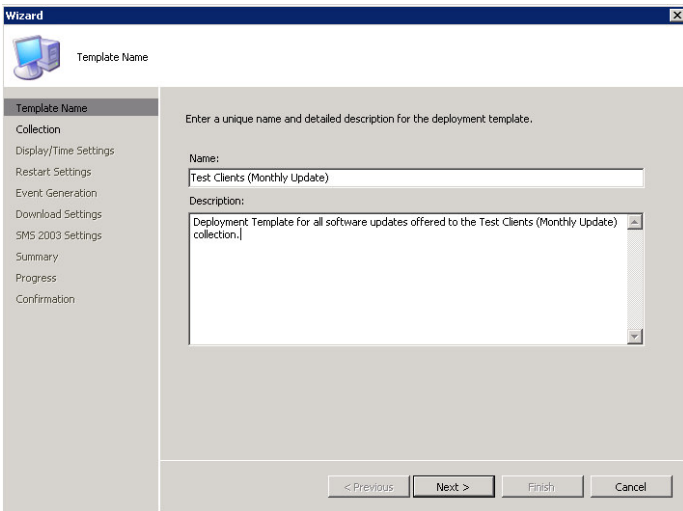
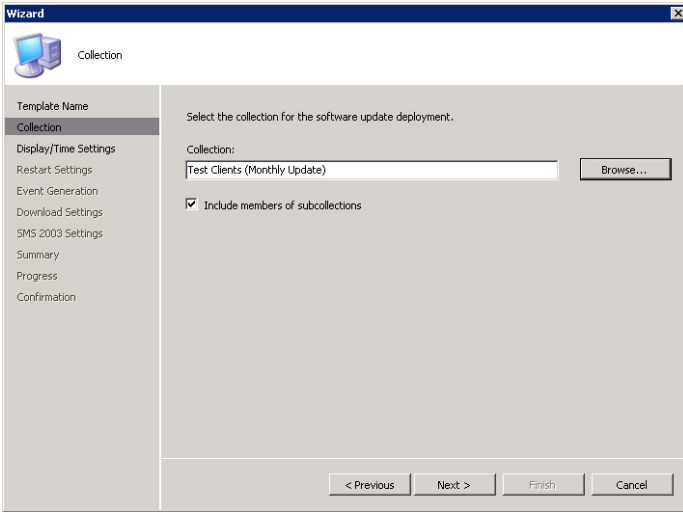
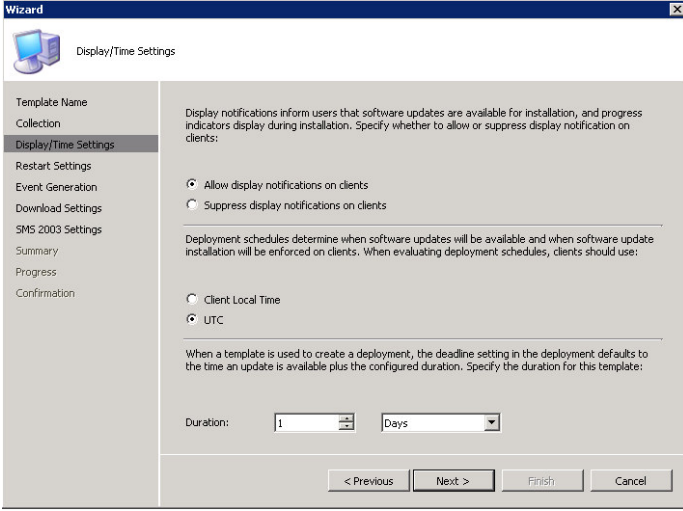
Step	Description	Screenshot
4.	Click OK . Note The maintenance window can be turned on and off by selecting and deselecting the check box. Multiple maintenance windows can be configured on a single collection if required.	

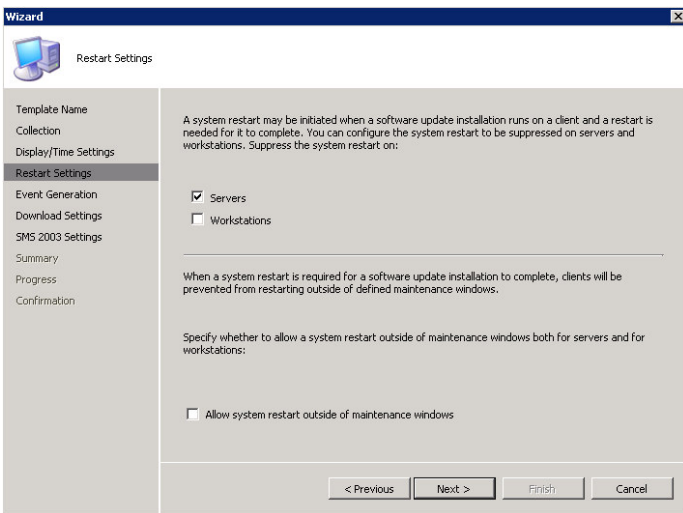
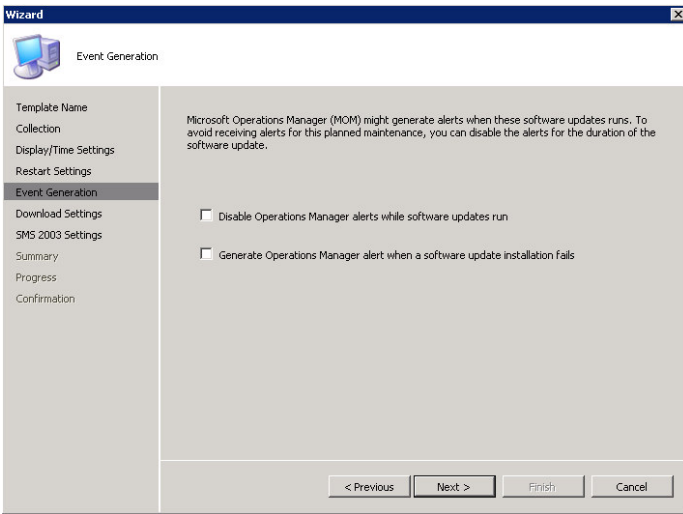
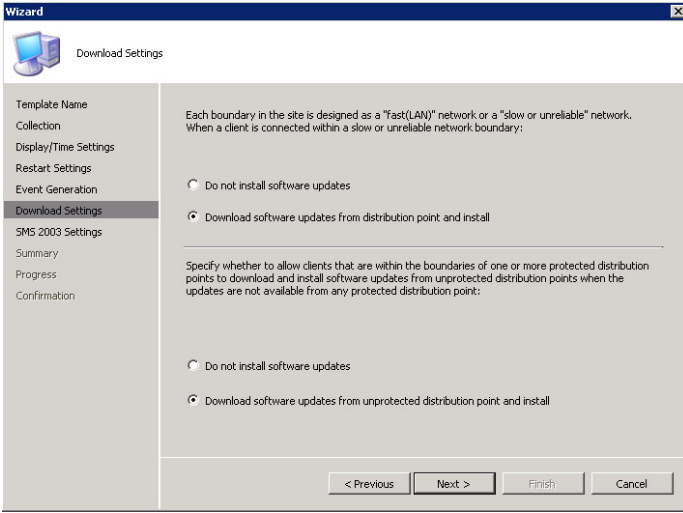
Table 13: Configuring Maintenance Windows

5.1.5 Creating Deployment Templates

Deployment Templates allow the healthcare IT Administrator to easily deploy software updates and ensure that deployment settings, such as restart time and user interaction, are consistent. A Deployment Template should be created for each software update management collection as described in section 4.6. Table 14 shows the process for creating deployment templates.

Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , right click on Software Updates > Deployment Templates , and then select New Deployment Template .	

Step	Description	Screenshot
2.	Enter a Name and Description for the Deployment Template. Click Next .	
3.	Select the Collection that this Deployment Template will be associated with. Click Next .	
4.	Enter the configuration for the relevant Deployment Template, as detailed in Table 8. Click Next .	

Step	Description	Screenshot
5.	Enter the configuration for the relevant Deployment Template, as detailed in Table 8. Click Next .	
6.	Enter the configuration for the relevant Deployment Template, as detailed in Table 8. Click Next .	
7.	Enter the configuration for the relevant Deployment Template, as detailed in Table 8. Click Next .	

Step	Description	Screenshot
8.	Click Next .	
9.	Click Next .	
10.	Click Close . Repeat steps for each Deployment Template listed in Table 8.	

Table 14: Creating Deployment Templates

6 OPERATE

During the Operate phase, solution components are proactively managed as an end-to-end IT Service to ensure the service provides the required levels of solution functionality, reliability, availability, supportability and manageability. Successfully bringing a well-designed service into a production environment takes efficient planning to balance speed, cost and safety, while ensuring minimum disruption to operations and supporting the 'business as usual' delivery of the organisation's IT requirements.

Figure 9 acts as a high-level checklist, illustrating the critical components for which an IT Professional is responsible for maintaining when using Configuration Manager for deploying software updates:

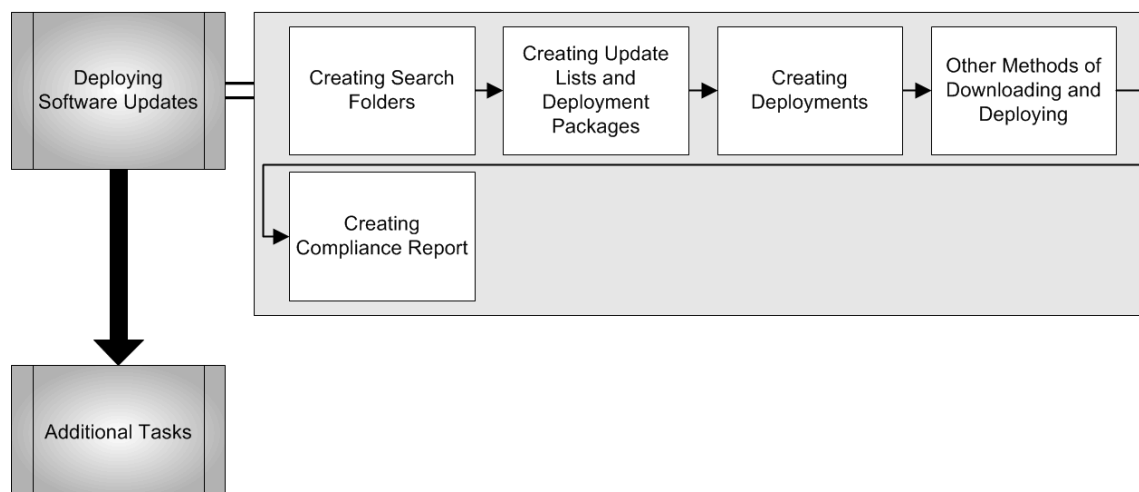


Figure 9: Sequence for Operating Configuration Manager for Deploying Software Updates

6.1 Deploying Software Updates

The process for deploying software updates will vary depending on the update type and criticality. Section 4.2 describes the various strategies a healthcare organisation can employ when deploying software updates. The following sections will take the healthcare IT Administrator through the process of creating a new software update deployment as an example. Once the process is understood, this can be applied to all future software updates.

6.1.1 Creating Search Folders

The first step in the process is creating a Search Folder to select the updates the healthcare IT Administrator needs to review in a single window. Table 15 shows the process for creating an example Search Folder to display all updates for Windows XP.

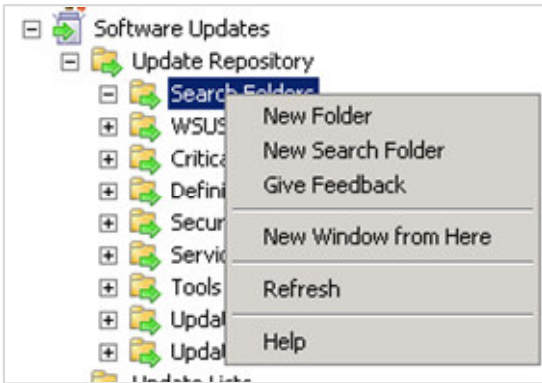
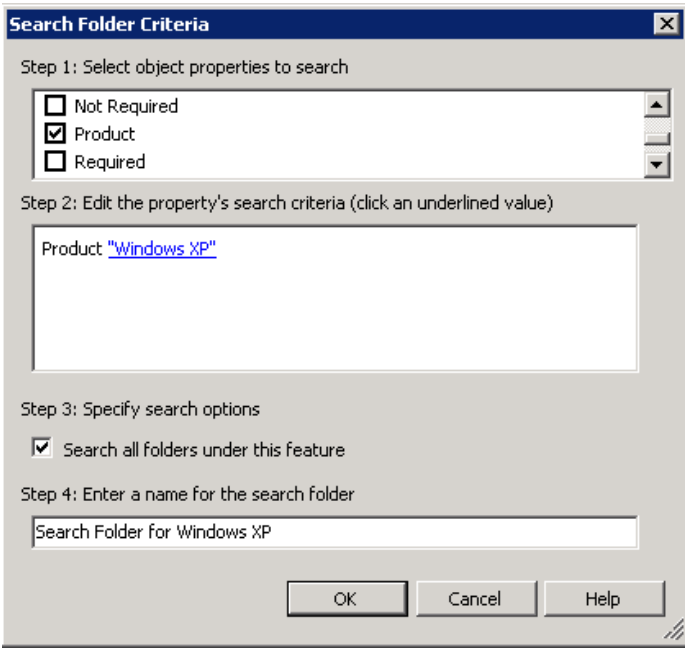
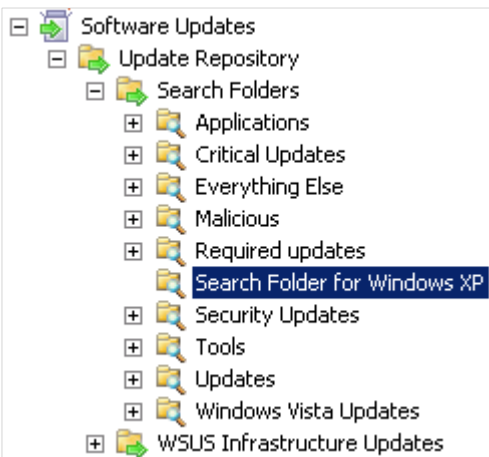
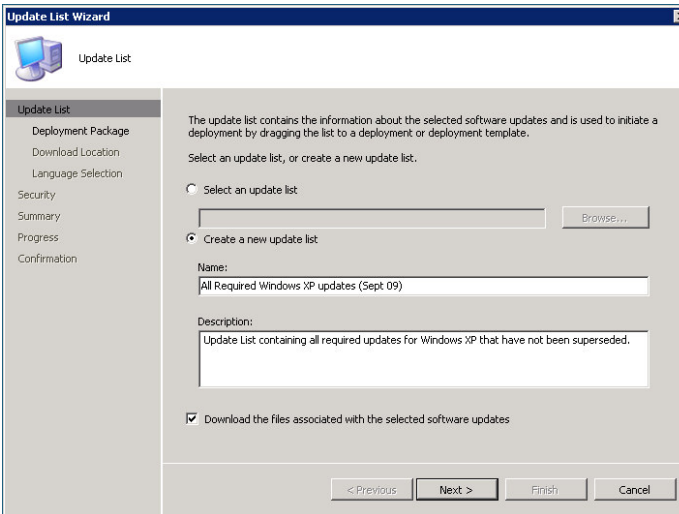
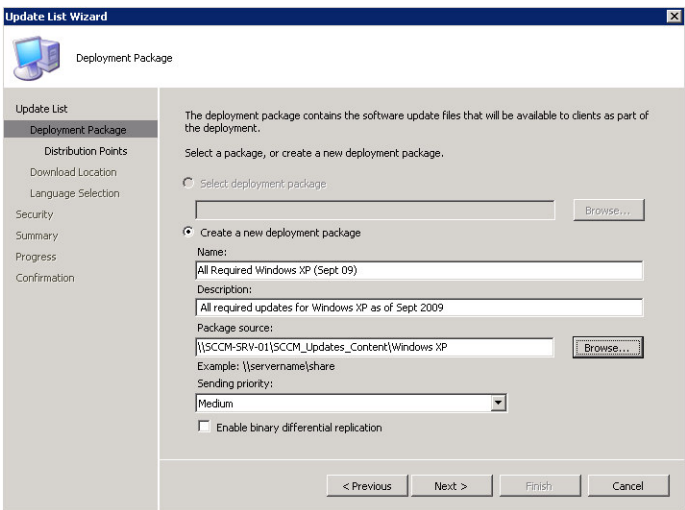
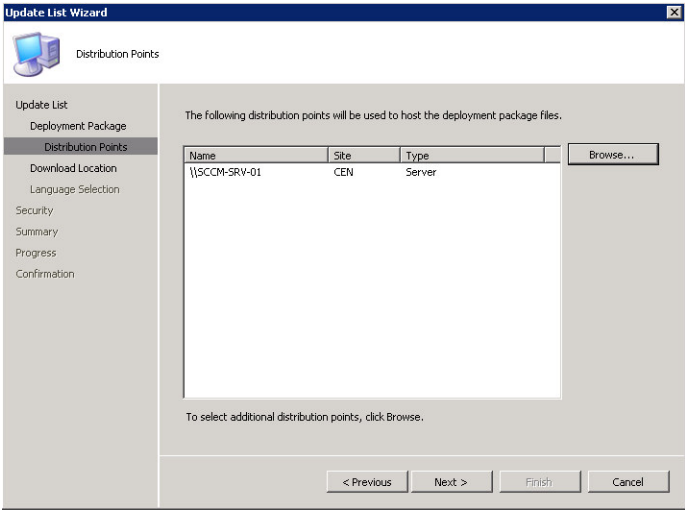
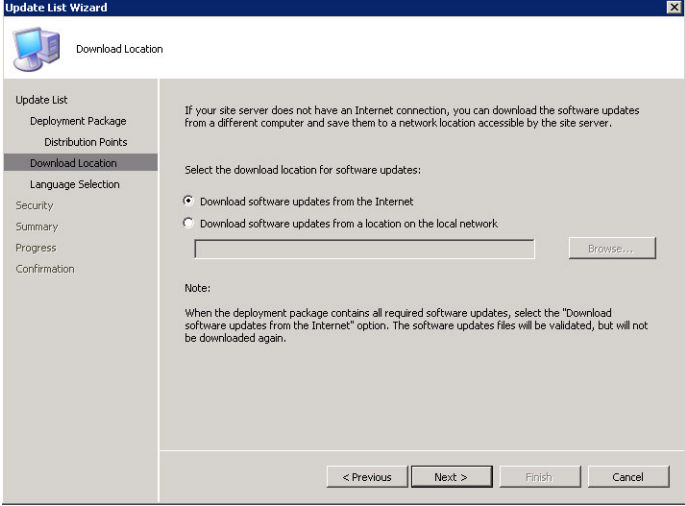
Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , right click on Software Updates > Update Repository > Search Folders , and select New Search Folder .	
2.	<p>In Select object properties to select, select the Product check box.</p> <p>In Edit the property's search criteria, click Windows XP.</p> <p>Select Search all folders under this feature.</p> <p>Enter a name for the search folder in the box provided.</p> <p>Click OK.</p>	

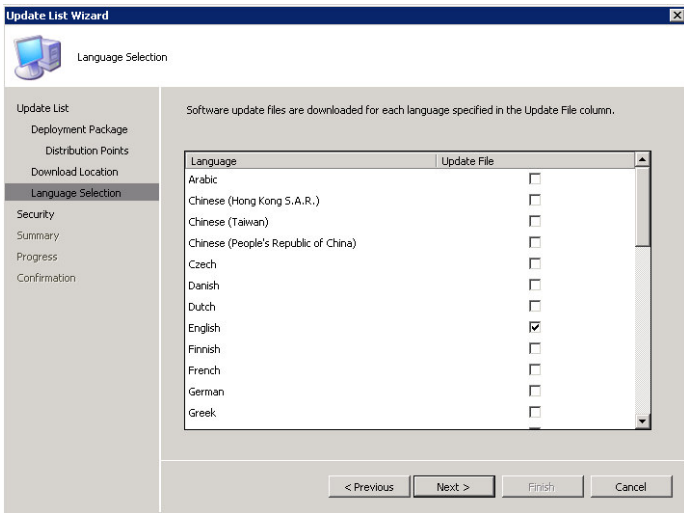
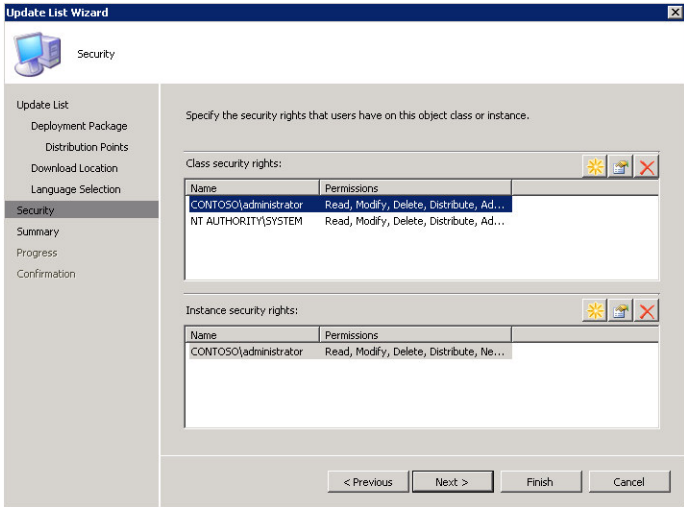
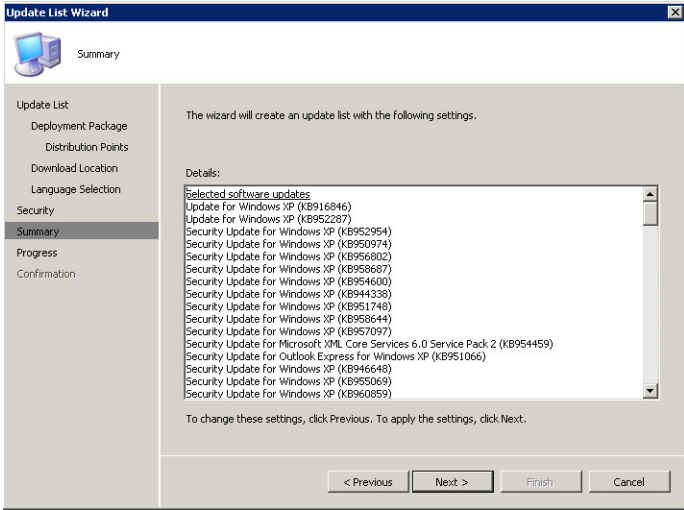
Table 15: Creating Search Folders

6.1.2 Creating Update Lists and Deployment Packages

Table 16 shows the process for creating Update Lists which will allow the healthcare IT Administrator to view compliance reports and keep a record of the updates that are associated with a deployment. It also shows the process of creating Deployment Packages that contain all the downloaded updates. Be aware that these two objects are not linked after the creation of the Deployment Package, so adding or removing updates from either an Update List or a Deployment Package will not affect the other.

Step	Description	Screenshot																																																								
1.	<p>Open the Configuration Manager Administrator Console. Click on Software Updates > Update Repository > Search Folders, and then select the Search Folder created in section 6.1.1.</p>																																																									
2.	<p>Select all updates that require deployment using CTRL + select.</p> <div><p>Tip</p><p>Updates that are shown with a yellow arrow have been superseded by another update; therefore these do not need to be included in the deployment.</p></div> <p>Once all the required updates have been selected, drag and drop them on to the Software Updates > Update Lists folder.</p> <div><p>Note</p><p>To add updates to an existing update list drag the updates to the required list under the update lists folder. to remove updates select the update from within the list to be removed and click delete</p></div>	<table><thead><tr><th>Bulletin ID</th><th>Article ID</th><th>Title</th><th>% Compliant</th></tr></thead><tbody><tr><td>MS09-071</td><td>974318</td><td>Security Update for Win...</td><td>30.77 %</td></tr><tr><td>MS09-069</td><td>974392</td><td>Security Update for Win...</td><td>30.77 %</td></tr><tr><td>MS09-073</td><td>973904</td><td>Security Update for Win...</td><td>30.77 %</td></tr><tr><td></td><td>890830</td><td>Windows Malicious Soft...</td><td>100.00 %</td></tr><tr><td>MS09-072</td><td>976325</td><td>Cumulative Security Up...</td><td>30.77 %</td></tr><tr><td>MS08-076</td><td>972187</td><td>Security Update for Win...</td><td>61.54 %</td></tr><tr><td>MS08-076</td><td>972187</td><td>Security Update for Win...</td><td>61.54 %</td></tr><tr><td></td><td>976098</td><td>Update for Windows XP ...</td><td>61.54 %</td></tr><tr><td>MS08-076</td><td>952069</td><td>Security Update for Win...</td><td>61.54 %</td></tr><tr><td>MS08-076</td><td>952069</td><td>Security Update for Win...</td><td>61.54 %</td></tr><tr><td>MS09-065</td><td>969947</td><td>Security Update for Win...</td><td>100.00 %</td></tr><tr><td>MS09-066</td><td>973039</td><td>Security Update for Win...</td><td>100.00 %</td></tr><tr><td></td><td>975364</td><td>Update for Internet Exp...</td><td>100.00 %</td></tr></tbody></table>	Bulletin ID	Article ID	Title	% Compliant	MS09-071	974318	Security Update for Win...	30.77 %	MS09-069	974392	Security Update for Win...	30.77 %	MS09-073	973904	Security Update for Win...	30.77 %		890830	Windows Malicious Soft...	100.00 %	MS09-072	976325	Cumulative Security Up...	30.77 %	MS08-076	972187	Security Update for Win...	61.54 %	MS08-076	972187	Security Update for Win...	61.54 %		976098	Update for Windows XP ...	61.54 %	MS08-076	952069	Security Update for Win...	61.54 %	MS08-076	952069	Security Update for Win...	61.54 %	MS09-065	969947	Security Update for Win...	100.00 %	MS09-066	973039	Security Update for Win...	100.00 %		975364	Update for Internet Exp...	100.00 %
Bulletin ID	Article ID	Title	% Compliant																																																							
MS09-071	974318	Security Update for Win...	30.77 %																																																							
MS09-069	974392	Security Update for Win...	30.77 %																																																							
MS09-073	973904	Security Update for Win...	30.77 %																																																							
	890830	Windows Malicious Soft...	100.00 %																																																							
MS09-072	976325	Cumulative Security Up...	30.77 %																																																							
MS08-076	972187	Security Update for Win...	61.54 %																																																							
MS08-076	972187	Security Update for Win...	61.54 %																																																							
	976098	Update for Windows XP ...	61.54 %																																																							
MS08-076	952069	Security Update for Win...	61.54 %																																																							
MS08-076	952069	Security Update for Win...	61.54 %																																																							
MS09-065	969947	Security Update for Win...	100.00 %																																																							
MS09-066	973039	Security Update for Win...	100.00 %																																																							
	975364	Update for Internet Exp...	100.00 %																																																							
3.	<p>Select Create a new update list and enter a Name and Description.</p> <p>Select Download the files associated with the selected software updates.</p> <p>Click Next.</p> <div><p>Tip</p><p>If the Download the files associated with the selected software updates option is not selected, the Deployment Package can be created later by right clicking the Update List. This can be useful if the healthcare IT Administrator wants to start the download process at the end of the day, to be performed overnight.</p></div>																																																									

Step	Description	Screenshot
4.	<p>Select Create a new deployment package and enter a Name, Description, and specify the Package source.</p> <p>Click Next.</p> <p>Note</p> <p>The Package source location should be a subfolder of the folder described in section 5.1.3</p>	
5.	<p>Select the DPs that the updates should be copied to using the Browse button.</p> <p>Click Next.</p>	
6.	<p>Select Download software updates from the Internet.</p> <p>Click Next.</p>	

Step	Description	Screenshot
7.	Deselect all languages except English . Click Next .	
8.	Click Next . Note If additional users need instance rights to this Update List, they can be specified here.	
9.	Click Next .	

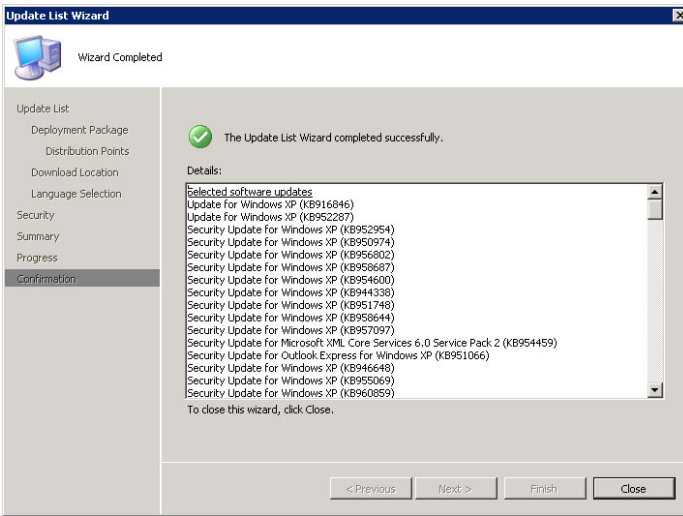
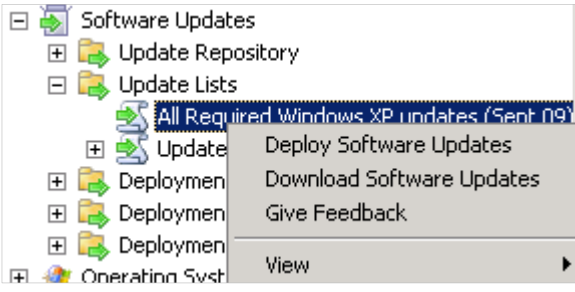
Step	Description	Screenshot
10.	Once the updates have been downloaded, click Close .	

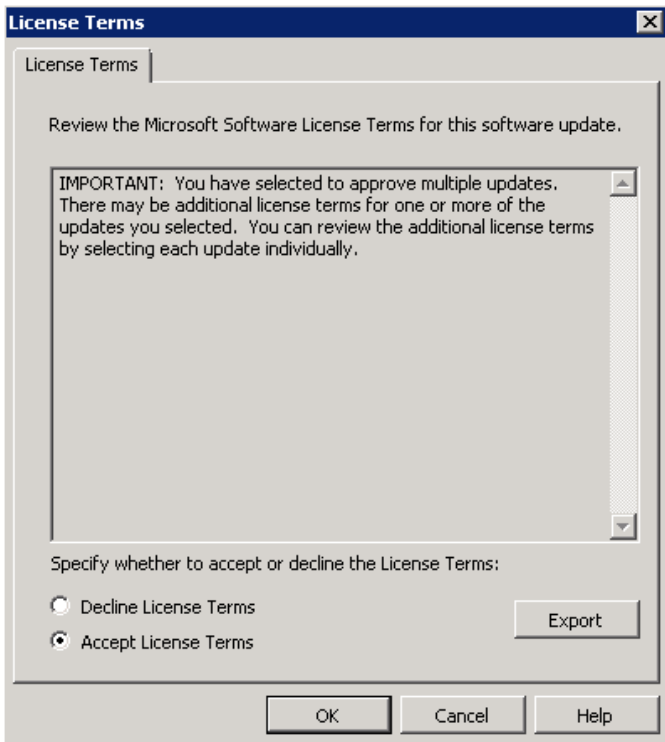
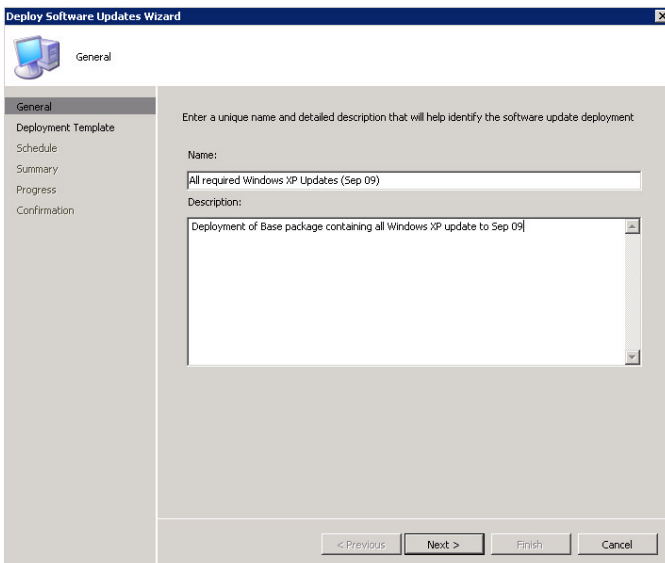
Table 16: Creating Update Lists and Deployment Packages

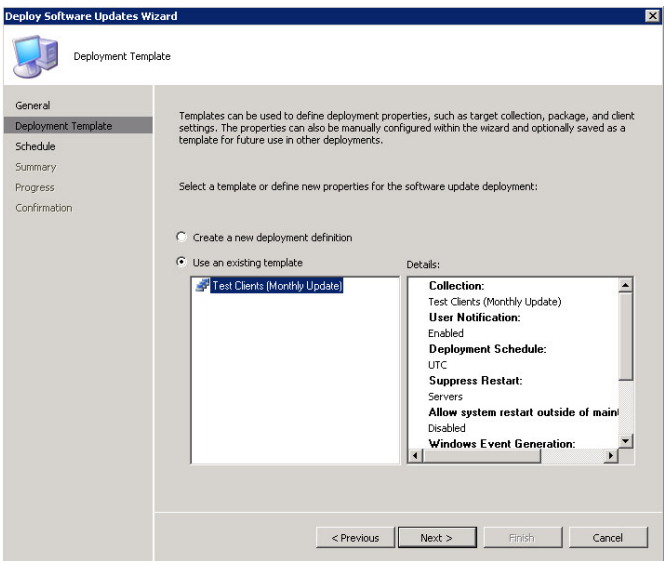
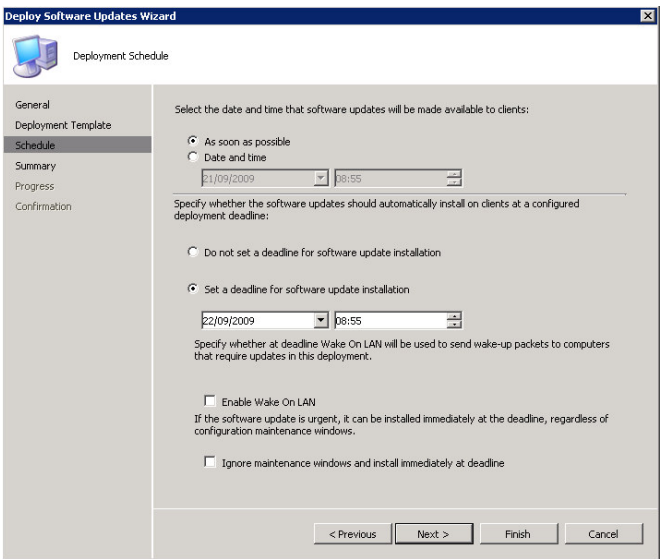
6.1.3 Creating Deployments

Table 17 shows the process for creating Deployments. Deployments allow the healthcare IT Administrator to:

- Make the updates in the Deployment Package available to client machines
- Specify which Deployment Template should be used
- Specify schedule settings, such as when to make the updates available to clients and when the update must be installed by

Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , right click on the Update List to be deployed under Software Updates > Update Lists , and select Deploy Software Updates .	

Step	Description	Screenshot
2.	Select Accept License Terms . Click OK .	
3.	Enter a Name and Description for the deployment. Click Next .	

Step	Description	Screenshot
4.	<p>Select the appropriate Deployment Template from the list of existing templates provided.</p> <p>Click Next.</p> <div data-bbox="362 360 414 387" data-label="Section-Header"> <p>Note</p> </div> <div data-bbox="362 407 695 526" data-label="Text"> <p>If no deployment Template contains the appropriate settings a new one can be created by selecting Create a new deployment definition.</p> </div>	
5.	<p>Select the date and time the software updates will be made available. This can be As soon as possible or a specific Date and time in the future.</p> <p>Decide whether to Set a deadline for software update installation. Enter the Date and time for the deadline or, alternatively, use the default deadline settings of the present time plus the deadline setting in the Deployment Template used.</p> <p>If Wake On LAN has been implemented in the healthcare organisation, selecting Enable Wake On LAN will configure the deployment to remotely turn on any machines targeted in the deployment that have not installed the update before the deadline time.</p> <p>If maintenance windows are configured and the update is urgent, specify Ignore maintenance windows and install immediately at deadline.</p> <div data-bbox="362 1469 414 1496" data-label="Section-Header"> <p>Note</p> </div> <div data-bbox="362 1516 647 1603" data-label="Text"> <p>This option should be used with caution if targeting clinical applications or servers.</p> </div> <p>Click Next.</p>	

Step	Description	Screenshot
6.	Click Next .	

7.	Click Close .	
----	----------------------	--

8.	<p>Note</p> <p>Once the deployment package has been created updates can be removed from the package by selecting the update and clicking delete. Updates can be added by dragging the required update from an update list or search folder and dropping it on the deployment package.</p>	
----	--	--

Table 17: Creating Deployments

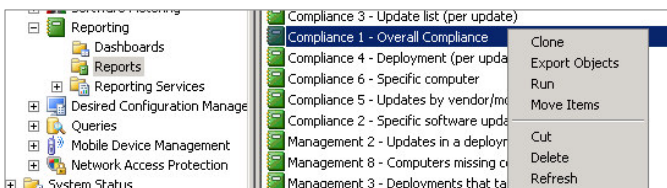
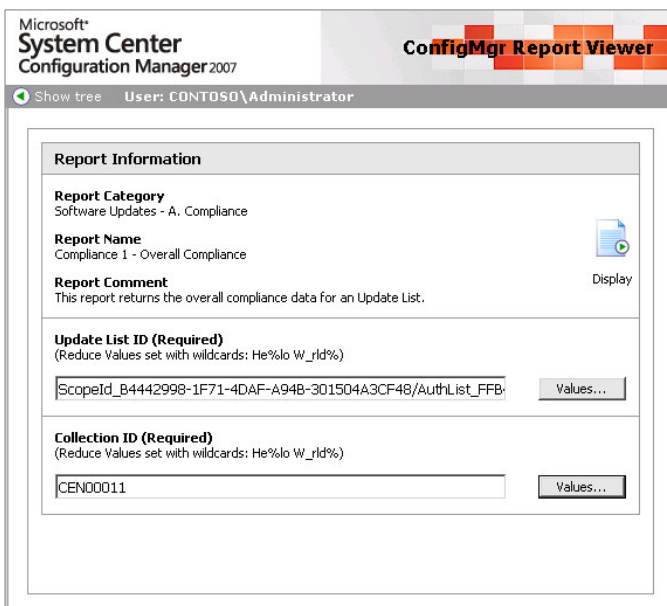
6.1.4 Other Methods of Downloading and Deploying

Sections 6.1.1 to 6.1.3 describe one of the ways it is possible to deploy updates using the Configuration Manager Administrator Console. Using Update Lists and Search Folders ensure that the healthcare IT Administrator is able to access the most complete information regarding the deployment. Other possible ways to deploy software updates via the Configuration Manager Administrator Console include:

- Single or multi-selecting any number of updates from the Update repository, right clicking and selecting **Deploy Software Updates** (this will launch the Software Update Wizard and allow a Deployment Package to be created without the Update List)
- Launching the Software Updates Wizard from the Software Updates home page

6.1.5 Creating Compliance Report

Once the Deployment has been triggered, the healthcare IT Administrator can track the compliance of the client machines using one of the Software Update Compliance Reports that are included with Configuration Manager, or by creating custom reports. Table 18 shows the steps required to run the Overall Compliance report using the Update List created in Table 16.

Step	Description	Screenshot
1.	Open the Configuration Manager Administrator Console , select Reporting > Reports , and right click the report named Compliance 1 – Overall Compliance . Select Run .	
2.	Using the Values buttons, specify the Update List ID and Collection ID . Click Display .	


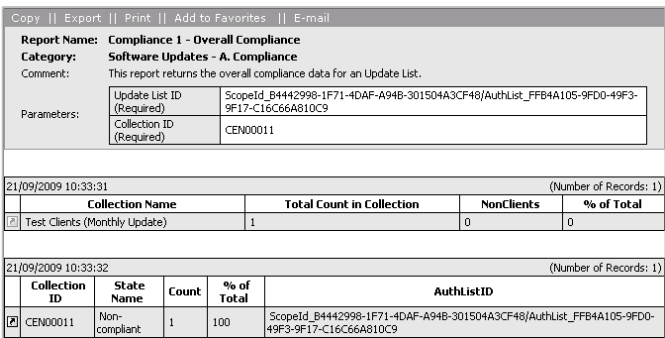
Step	Description	Screenshot
3.	<p>The report shows the number of machines that are compliant or non-compliant in the specified collection. To see more detailed information for each client in the collection. Use the linked report button </p>	 <p>The screenshot displays a report titled 'Compliance 1 - Overall Compliance' under the category 'Software Updates - A. Compliance'. It includes a comment stating 'This report returns the overall compliance data for an Update List.' and parameters for 'Update List ID (Required)' and 'Collection ID (Required)'. Below this, there are two tables. The first table, dated 21/09/2009 10:33:31, shows the overall compliance status for 'Test Clients (Monthly Update)' with a total count of 1, 0 non-compliant clients, and 0% of total. The second table, dated 21/09/2009 10:33:32, shows the compliance status for 'CEN00011' with a total count of 1, 0 non-compliant clients, and 0% of total.</p>

Table 18: Creating Compliance Reports

6.2 Additional Tasks

This document has taken the healthcare IT Administrator through the basic tasks for planning and implementing software updates in Configuration Manager. Table 19 contains links to tasks that were out of scope for this documentation, but may need to be considered if implementing software updates in a more complex environment.

Task	Description	Link to Further Information
Review current best practices	This document contains the latest source for best practices when deploying a Configuration Manager SUP. It should be reviewed prior to performing the installation of the SUP.	http://technet.microsoft.com/en-us/library/bb932162.aspx
How to Add the Web Server Certificate to the Custom WSUS Web Site	If SSL is required on the WSUS SUP, these steps must be followed.	http://technet.microsoft.com/en-us/library/bb680861.aspx
How to Configure the WSUS Web Site to Use SSL	If SSL is required on the WSUS SUP, these steps must be followed.	http://technet.microsoft.com/en-us/library/bb633246.aspx
How to Create and Configure an Active Internet-Based Software Update Point	If the healthcare organisation is using Internet Based Client Management (IBCM), an Internet based software update should be configured to support clients that connect to the site over the Internet.	http://technet.microsoft.com/en-us/library/bb694182.aspx
How to Configure the Active Software Update Point Component to Use an NLB Cluster	If the healthcare organisation requires an additional SUP for scaling or resilience purposes a Network Load Balancing (NLB) Cluster will need to be configured.	http://technet.microsoft.com/en-us/library/bb633165.aspx
How to Install and Configure the Inventory Tool for Microsoft Updates	If the healthcare organisation has any SMS 2003 clients that cannot be upgraded and need to receive software updates an updated version of the Inventory Tool for Microsoft Updates (ITMU) that was previously used in Systems Management Server (SMS) 2003 will need to be used.	http://technet.microsoft.com/en-us/library/bb632814.aspx
Tasks for Software Updates	These articles contain more information on the tasks required for deploying software updates. This guide acts as a shortcut to enable the healthcare IT Administrator to quickly become familiar with the technology but it is recommended that this information is reviewed when possible.	http://technet.microsoft.com/en-us/library/bb693776.aspx

Table 19: Additional Tasks

APPENDIX A SKILLS AND TRAINING RESOURCES

The tables in PART I of this appendix list the suggested training and skill assessment resources available. This list is not exhaustive; there are many third-party providers of such skills. The resources listed are those provided by Microsoft. PART II lists additional training resources that might be useful.

PART I TRAINING RESOURCES

For further information on System Center Configuration Manager, see <http://www.microsoft.com/sccm>

Skill or Technology Area	Resource Location	Description
Configuration Manager Training	http://www.microsoft.com/systemcenter/configurationmanager/en/us/learning-resources.aspx	Links to Learning resources available from Microsoft and Microsoft Learning Partners
Configuration Manager Product Documentation	http://www.microsoft.com/systemcenter/configurationmanager/en/us/product-documentation.aspx	Links to product documentation and whitepapers

Table 20: Microsoft System Center Configuration Manager 2007 Training Resources

PART II SUPPLEMENTAL TRAINING RESOURCES

Title	Link
Microsoft TechNet System Center Configuration Manager TechCenter	http://technet.microsoft.com/en-gb/configmgr/default.aspx
MyITforum.com (forum site focusing on Configuration Manager)	http://www.myitforum.com

Table 21: Supplemental Training Resources

APPENDIX B DOCUMENT INFORMATION

PART I TERMS AND ABBREVIATIONS

Abbreviation	Definition
ACL	Access Control List
BITS	Background Intelligent Transfer Service
CUI	Common User Interface
DP	Distribution Point
EXE	Executable File
FQDN	Fully Qualified Domain Name
IBCM	Internet Based Client Management
IEC	International Electrotechnical Commission
IM&T	Information Management & Technology
ISO	International Organization for Standardization
ITMU	Inventory Tool for Microsoft Updates
LAN	Local Area Network
MP	Management Point
MPS	Windows Installer Patch File
MSI	Microsoft Installer File
NLB	Network Load Balancing
Configuration Manager	System Center Configuration Manager
SCUP	System Center Updates Publisher
SMS	Systems Management Server
SP	Service Pack
SUP	Software Update Point
UTC	Coordinated Universal Time
WSUS	Windows Server Update Services

Table 22: Terms and Abbreviations

PART II REFERENCES

Reference	Document	Version
R1.	System Center Configuration Manager 2007 Deployment Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx	1.0.0.0
R2.	Microsoft TechNet: Software Updates Synchronization Process Flowchart http://technet.microsoft.com/en-us/library/bb932170.aspx	November 2007
R3.	Microsoft TechNet: Software Update Deployment Process Flowchart http://technet.microsoft.com/en-us/library/bb932173.aspx	November 2007
R4.	Microsoft TechNet: Deployment Package Process Flowchart http://technet.microsoft.com/en-us/library/bb932157.aspx	November 2007
R5.	Microsoft TechNet System Center Configuration Manager TechCenter http://technet.microsoft.com/en-gb/configmgr/default.aspx	
R6.	Microsoft System Center Configuration Manager: Product Homepage www.microsoft.com/sccm	
R7.	Microsoft TechNet: System Center Updates Publisher http://technet.microsoft.com/en-us/library/bb531022.aspx	
R8.	Microsoft Download Center: System Center Updates Publisher 4.5 http://www.microsoft.com/downloads/details.aspx?FamilyID=0446cce9-94a4-4fb0-b335-e7516044063d&displaylang=en	4.5
R9.	Microsoft Download Center: Microsoft Windows Server Update Services 3.0 SP2 Release Notes http://www.microsoft.com/downloads/details.aspx?FamilyID=ba94a0d3-f22a-4e24-877e-6be6ce5da6d7&displaylang=en#filelist	3.0 SP2
R10.	Microsoft TechNet: Windows Server Update Services http://technet.microsoft.com/en-us/wsus/default.aspx	
R11.	Microsoft Download Center: Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?FamilyID=CC96C246-61E5-4D9E-BB5F-416D75A1B9EF&displaylang=en	09.00.21022.08

Table 23: References