System Center Configuration Manager 2007

Deployment Guide

Friday, 26 February 2010
Version 1.0.0.0 Baseline

Prepared by
Microsoft

Microsoft®

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The *System Center Configuration Manager 2007 Deployment Guide* is the first in a series of documents covering the design, deployment and operation of Microsoft® System Center Configuration Manager 2007 (Configuration Manager) Release 2 (R2) Service Pack (SP) 1. The other documents are *System Center Configuration Manager 2007 Software Update Management Guide*[1], *System Center Configuration Manager 2007 Operating System Deployment Guide*[2], and *System Center Configuration Manager 2007 Software Distribution Guide*[3].

The aim of the guidance is to take an IT Professional through the necessary steps in order to design, install and configure a Configuration Manager hierarchy within a healthcare organisation environment and to reduce the time needed to implement Configuration Manager by consolidating the necessary information into a modular documentation set.

The guidance brings together the wealth of information available for Configuration Manager into a concise and easy-to-follow implementation guide. Links to additional information are also provided together with training resources.

[1] *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}:** http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx

[2] *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}:** http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx

[3] *System Center Configuration Manager 2007 Software Distribution Guide* **{R3}:** http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx

2 INTRODUCTION

2.1 Value Proposition

This document provides information on how to design and deploy a Configuration Manager infrastructure within a healthcare organisation. This guidance aims to provide enough information to allow the healthcare IT Administrator to make the right decisions without having to read through the large amount of information available on System Center Configuration Manager. It will allow the healthcare organisation to be confident that the Configuration Manager infrastructure being deployed will fit the needs of the organisation and be designed and deployed using current best practice.

This guidance should not replace the wealth of other information that is available for Configuration Manager; it should simply allow the healthcare organisation to quickly and confidently deploy Configuration Manager. The guidance will also provide details of additional information that the healthcare IT Administrators responsible for Configuration Manager should review once this guidance has been followed. The guidance seeks to cover the most common deployment scenarios that will be used within a healthcare organisation and provides references to further reading should the healthcare organisation require information outside the scope of this document.

2.2 Knowledge Prerequisites

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

2.2.1 Skills and Knowledge

A thorough understanding of certain Configuration Manager key concepts is required to use this Deliverable. These are discussed in the following sections, which should be read before progressing with this document.

2.2.1.1 Configuration Manager Sites

A Configuration Manager Site defines the boundary of administrative control. Configuration Manager can be broken down into one or many sites depending on the underlying network architecture of the healthcare organisation. Multiple Configuration Manager sites allow the healthcare IT Administrator to control the network bandwidth that Configuration Manager will use when traversing slower network links, such as Wide Area Networks (WAN), and can also be used if multiple centres of administration exist within the healthcare organisation.

Table 1 gives high-level information on the types of Configuration Manager site that can be installed:

Site Type	Description
Configuration Manager Primary Site	A Configuration Manager primary site stores data for itself and all the sites beneath it, in a Microsoft® SQL Server® database. This is called the Configuration Manager site database. Primary sites have administrative tools, such as the Configuration Manager Console, that enable the Configuration Manager Administrator to directly manage the site. Configuration Manager Setup creates each primary site as a stand-alone site. They can then be joined as children to other primary sites. Primary sites can have multiple secondary sites, all of which send data to the primary site. When Configuration Manager in configured in a hierarchy, the primary site at the top of the hierarchy is known as the 'central site'.
Configuration Manager Secondary Site	A Configuration Manager secondary site has no site database. It is attached to, and reports to, a primary site. The secondary site is managed by a Configuration Manager Administrator running a Configuration Manager Console that is connected to the primary site. The secondary site forwards the information it gathers from Configuration Manager clients, such as computer inventory data and system status information, to its parent site. The primary site then stores the data of both the primary and secondary sites in the Configuration Manager site database. Secondary sites are particularly useful for locations across Wide Area Network (WAN) links that do not have an onsite administrator to perform management tasks.

Table 1: Description of Configuration Manager Sites

When using this document, it is important to understand the types of Configuration Manager server infrastructure that can be deployed in a location, and the benefits and drawbacks of each. Table 2 lists these from a networking perspective:

Configuration Manager Server Infrastructure Installed	Server Roles That Can Be Deployed Within Location	Strengths	Weaknesses
Configuration Manager Primary Site	All	▪ Can be a parent to other sites in a Configuration Manager hierarchy ▪ All network traffic is contained within this site (apart from scheduled transfers to parent or child sites)	▪ Requires SQL Server database, and is therefore more expensive to license and manage
Configuration Manager Secondary Site	All except Reporting Point (RP) and Server Locator Point (SLP)	▪ Replication of packages to secondary sites can be scheduled and throttled ▪ Configuration Manager clients communicate with the Management Point (MP) at the secondary site, so reducing WAN traffic	▪ Cannot be a parent for another site ▪ MP at secondary site still needs to communicate with SQL Server, so there is some communication with the SQL database across WAN (although very minor)
None	None, Configuration Manager clients perform all communication across WAN	▪ No server infrastructure required ▪ Can use Branch Distribution Point (DP) to reduce network load significantly	▪ All communication is across WAN link

Table 2: Configuration Manager Server Infrastructure Choices

Figure 1 represents a summary of the relationships between primary and secondary sites:

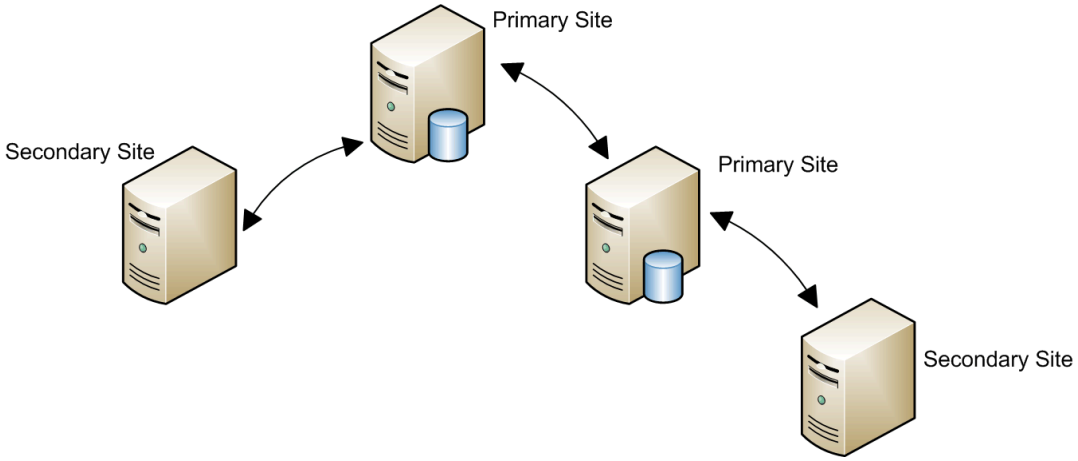


Figure 1: Configuration Manager Primary and Secondary Site Relationships

When Configuration Manager is configured in a hierarchy, all client data, such as inventory data and status information, flows up the hierarchy until it reaches the central site. The central site can therefore be used to view data for all clients in the hierarchy.

Each Configuration Manager site is configured with a three-character alphanumeric site code that must be unique within the hierarchy.

2.2.1.2 Configuration Manager Features

Configuration Manager provides the healthcare organisation with a number of features that provide configuration management of clients and servers. The healthcare organisation can decide to deploy and use any number of these features that are appropriate. When designing the Configuration Manager infrastructure, the healthcare IT Administrator should have an understanding of all the possible features a Configuration Manager hierarchy can provide, even if some of the features will not be used when the system is first implemented. Understanding the features will allow the healthcare IT Administrator to design the Configuration Manager site or site hierarchy so that these features can be easily added in the future if required. The features provided by Configuration Manager are:

- Software and Hardware Inventory
- Software Distribution
- Operating System Deployment
- Software Updates
- Software Metering
- Desired Configuration Management
- Out of Band Management
- Reporting
- Mobile Device Management
- Network Access Protection Integration

2.2.1.2.1 Software and Hardware Inventory

The Configuration Manager Inventory feature allows healthcare IT Administrators to collect a wide range of information from client machines. The feature is broken down into two main components: software inventory, and hardware inventory. Configuration Manager allows the healthcare IT Administrator to configure many aspects of the inventories, such as the kind of information that will be collected and how frequently it will be collected

Software Inventory

By default, the software inventory agent will collect file and product information for all executable files on all client hard disks. These settings can be modified and tuned to the exact requirements of the healthcare organisation using the **Software Inventory Client Agent Properties** shown in Figure 2:

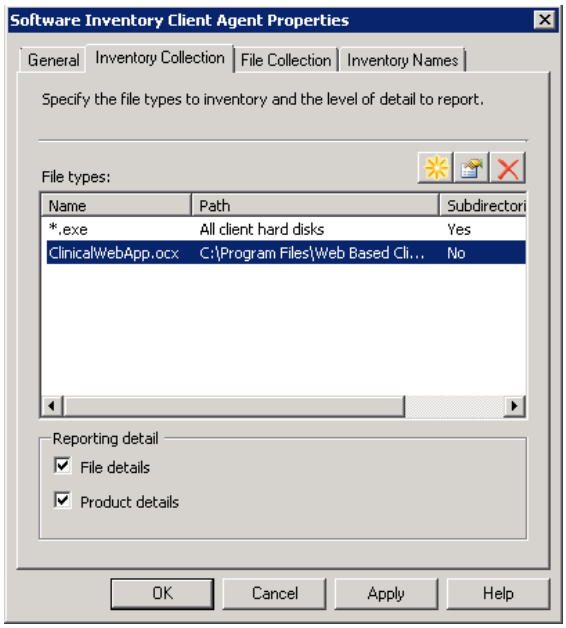


Figure 2: Software Inventory Client Agent Properties

Hardware Inventory

Hardware Inventory in Configuration Manager uses Windows Management Instrumentation (WMI) to gather information relating to a large number of hardware items, such as a client's processor type and speed, available disk space, and so on. It also gathers details on some software items that are stored in the registry; these are the items contained within **Add or Remove Programs** (Windows® XP and earlier) or **Programs and Features** (Windows Vista® or later). The healthcare IT Administrator can configure Configuration Manager hardware inventory to collect any information that is present in WMI by editing the SMS_DEF.mof and Configuration.mof files. This enables collection of custom data such as registry values or user-input data that can then be used to create collections or queries. A good example of this is creating custom registry keys that store healthcare organisation-specific data, such as a machine's location information or department, or the criticality of a machine, such as client machines in operating theatres. Creating collections that are based on this information allows a healthcare IT Administrator to set differing maintenance windows or software distribution schedules for machines in different locations or of differing criticality.

Asset Intelligence

The Asset Intelligence feature of Configuration Manager allows the data collected by the software inventory feature to be categorised into product families and types, providing the healthcare IT Administrator with a much greater level of detail and removing ambiguity from the inventory data. The Asset Intelligence reports provide a wealth of information to the healthcare IT Administrator, such as how many licences are required for a specific product or which client machines have hardware capable of running Windows Vista. There are 70 Asset Intelligence reports included out-of-the-box and these can be used to provide a variety of information. They can also be used as examples to create reports that specifically meet the needs of healthcare organisations.

2.2.1.2.2 Software Distribution

The Configuration Manager software distribution feature automates the distribution of programs to Configuration Manager clients. Using software distribution eliminates the inefficient and costly process of an IT Professional visiting every location where the software is required, and manually installing it. The automated process of software distribution also eliminates the need to travel to the clients' location and removes errors such as entering incorrect values in prompts, running incorrect programs, or entering incorrect arguments. By using software distribution, Configuration Manager clients can successfully run programs and install software without the user needing to know how to run these programs or which setup options are best for them. Software distribution also allows the healthcare organisation to centrally define and control how and when programs run on client computers. The healthcare IT Administrator can choose how little or how much users manage.

Central management of the software distribution in the healthcare organisation allows IT Administrators to monitor the distribution process from beginning to end. Configuration Manager generates detailed status messages that allow the monitoring of individual Configuration Manager clients. This also allows the healthcare IT Administrator to provide assistance to those clients that are having difficulties running a program. The following sections describe the key components that relate to software distribution.

Collections

The healthcare IT Administrator can make software products available to as many computers or users as required. The Configuration Manager clients that need to receive the program must be members of a collection (referred to as the *target collection*). The target collection can, contain a single client, all the clients that are assigned to a specific site, or any subset of clients. When the program is distributed to the target collection, all the clients that are members of that collection receive the program. This allows the healthcare organisation to distribute programs to specific computers, users or user groups, and any group of client computers that share a common set of hardware or software attributes.

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. Configuration Manager client computers that initially did not meet the collection's criteria, but meet the criteria now, automatically become members of the collection. Configuration Manager clients that initially met the collection's criteria, but no longer meet the criteria, are automatically removed from the collection. This does not result in any software that was deployed using the collection being uninstalled. In a dynamic environment, Configuration Manager keeps collections current, thus ensuring that only the appropriate Configuration Manager clients receive distributed programs.

The following scenario illustrates the benefits of this behaviour:

1. Application A is distributed to the ‘All Windows Vista Systems’ collection.
2. Only Configuration Manager client computers running Windows Vista receive the program.
3. A few Configuration Manager client computers running Windows XP upgrade to Windows Vista.
4. The newly upgraded Configuration Manager clients automatically become members of the ‘All Windows Vista Systems’ collection.
5. Application A that was distributed to the ‘All Windows Vista Systems’ collection automatically becomes available to the newly-upgraded Configuration Manager clients (along with all other applications that have previously been made available to the ‘All Windows Vista Systems’ collection).

Programs

The purpose of using the software distribution feature is to automate the process of making a program available to target clients. A program can be a file name (Configuration Manager uses file association to run such programs) or anything else that can run from a command line, such as a batch file or a Windows Installer command line.

Programs have a wide range of configurable options such as security context, supported platforms, and environment requirements. The program's command line can be anything from setup programs to simple batch command lines. Programs often need to download files to the client when they run, for example, installation programs must download installation files. The files that a program requires when it runs are called package source files.

Sometimes, more than one program can be associated with the same set of source files. For example, there can be several variations of a setup program that install the same software by using the same source files. However, each setup program runs differently and provides different setup options, such as running without user intervention or performing an upgrade rather than a full installation. To provide clients with all these setup options, several programs for the same set of source files need to be defined.

A copy of the source files must be distributed to one or more servers, accessible to clients, so that when the program runs on client computers, it can access the files that it requires. The Distribution Point (DP) is a Configuration Manager site system that has that role.

Some programs are not associated with source files. In this case, either the programs use files that are already stored on the client computers, or access to the required files is coordinated outside of the Configuration Manager software distribution. For example, the command line **Defrag.exe c:** might not be associated with source files. In this case, when the program runs on client computers, a local copy of Defrag.exe runs.

Packages

Programs, source files, and source file paths are the main components that make up a software distribution package. A Configuration Manager package is the basic unit of software distribution.

Packages vary widely, depending on their purpose. A package might have source files associated with it. A package typically has at least one program, and can have as many programs as needed.

Advertisements

Another object that is associated with software distribution is the advertisement. Advertisements are the objects that make programs available to clients. The advertisement links the program and package to a collection. A program must be advertised before clients can run it. A variation of an advertisement is an assignment, which is a mandatory advertisement that must run on the client. Advertised programs appear at the Configuration Manager client both in the Configuration Manager user interface and in **Programs and Features** (Windows Vista and above) or **Add or Remove Programs** (Windows XP and Windows 2000) in Control Panel.

How Software Distribution Works

To distribute software to Configuration Manager clients, a software distribution package and programs need to be created and then advertised to the relevant clients. Advertising the program makes a program available to a specified target collection. The advertisement contains the name of the program, the name of the target collection, and the scheduling configuration (such as when to run the program or when the program will expire).

However, the site's Configuration Manager clients will not be able to receive advertised programs until the software distribution client agent is enabled on the site's Configuration Manager clients. This primarily allows Configuration Manager clients to receive and run programs that are advertised.

When the feature is enabled, packages, programs, and advertisements can be created to deliver the programs that Configuration Manager clients need. Figure 3 shows a high-level overview of the software distribution process in Configuration Manager:

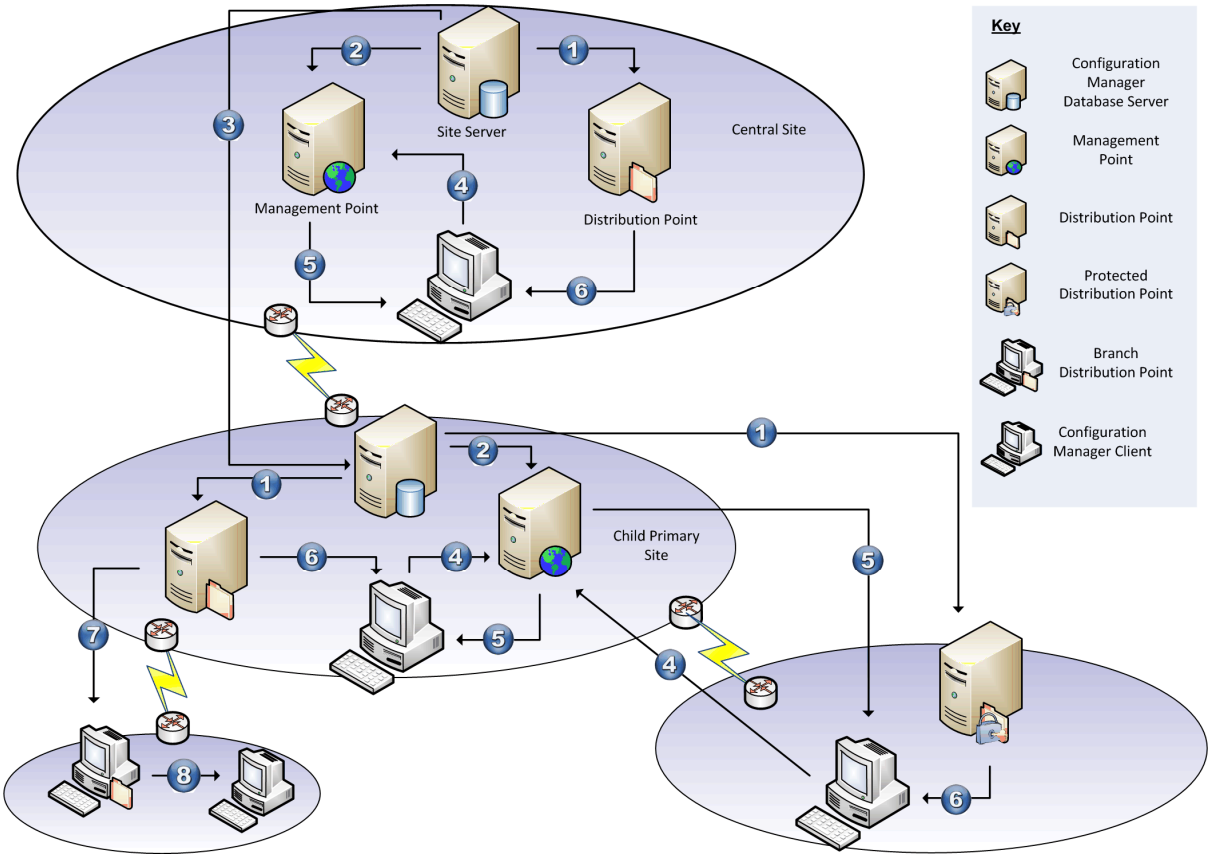


Figure 3: Software Distribution Overview

Table 3 shows the steps involved in the software distribution process:

Step	Description
1.	The Configuration Manager site server copies the package source files to the distribution points according to the package configuration. **Note** If a package has no source files, this step does not take place.
2.	For each advertisement, details of the collection, package and program are made available on the Management Point (MP).
3.	The Configuration Manager site server forwards any package, program and advertisement data to any child sites; this includes the package source files if a DP has been specified for that site or any of its child sites.
4.	The Configuration Manager client will periodically request new policies from the Management Point. The policies contain information about what software is required to be installed, including any scheduling data along with any other Configuration Manager client-side settings.
5.	When software is scheduled to be installed, the Configuration Manager client makes a content location request to the Management Point and waits for a response. The content location request tells the Configuration Manager client which DP to connect to in order to install the software, and if those locations are considered fast or slow, to the Configuration Manager client based on configured boundaries.
6.	If the package has package source files, the source files are either executed from the DP or downloaded to the Configuration Manager client cache and executed locally.
7.	The Configuration Manager Branch Distribution Point downloads the contents of the package to its local cache, which is made available to other local clients.
8.	The Configuration Manager client executes the program using the package source files made available by the Configuration Manager Branch Distribution Point.

Table 3: Software Distribution Overview Steps

2.2.1.2.3 Operating System Deployment

The Operating System Deployment feature of Configuration Manager allows the healthcare IT Administrator to target new or existing client machines with an operating system installation. This can be to a new machine with no existing operating system (referred to as a *bare metal* deployment) or to a client machine that already has a Configuration Manager client deployed. The feature allows for a great deal of flexibility when delivering the new operating system including the use of the User State Migration Tool (USMT) to allow the healthcare IT Administrator to maintain the user's data and settings during the deployment. The following sections describe the key components that relate to operating system deployment.

Boot Images

Boot Images contain a customised version of Windows Pre-Execution Environment (Windows PE) that is used to execute the task sequence that deploys the operating system. Windows PE is used because it is wholly contained in memory on the client machine, allowing for hard disks to be partitioned and formatted prior to the new operating system being installed.

Computer Associations

Computer associations allow the healthcare IT Administrator to generate mappings between two computers (or the same computer) so when the new operating system is deployed and USMT is used to migrate user settings, the Configuration Manager client knows which machines to treat as the source and destination for the user data being migrated.

Operating System Images

Operating system images are the .WIM files that have been created by capturing a reference client machine. The .WIM format provides significant advantages in size and manageability over other imaging formats. These files will be targeted at client machines using task sequences and contain everything required to build the operating system and any additional applications installed on the reference computer.

Operating System Install Packages

Operating System Install Packages contain the Windows source files. This package is typically used to build the reference computer prior to capture.

Task Sequences

A Task Sequence contains a list of actions that are defined by the healthcare IT Administrator to build the client operating system and install any optional software packages required for the healthcare organisation. The task sequence editor contains a number of predefined task sequence actions for performing tasks associated with an operating system deployment.

Drivers

The drivers node of the Configuration Manager console allows the healthcare IT Administrator to add drivers to Configuration Manager that will be evaluated and deployed during operating systems deployment in the healthcare organisation. The drivers can be categorised into different groups, such as mass storage, network, and so on.

Driver Packages

All drivers that can be used by client machines during the operating system deployment process must be part of a driver package. The driver package is similar to a software distribution package and contains the source files for the driver installation. The Import Driver Wizard will populate the source directory for the package with any driver files that are specified. If the healthcare organisation has multiple sites or DPs, they can specify which driver packages will be present on which DPs. This is particularly relevant if different hardware standards or vendors are used between sites.

Unprovisioned Computers

The Unprovisioned Computers node of the Configuration Manager console allows healthcare IT Administrators a single view of all machines that are currently being deployed and have not successfully completed. When a computer starts the provisioning process, and during all stages of the process, status messages are sent back to the Configuration Manager infrastructure providing the healthcare IT Administrator with a detailed, near real time view of any errors that may have occurred.

How Operating System Deployment Works

Operating System Deployment can be targeted at existing Configuration Manager clients or to new client machines that do not have an operating system installed. Targeting an existing Configuration Manager client using a task sequence works in much the same way as software distribution; the task sequence is advertised to a collection and executed by all members of the collection based on the schedule defined. Once the task sequence is received, the operating system, any relevant drivers and any additional software are installed.

There are two ways to deploy an operating system to a client machine that does not yet have an operating system. The first is to create and use boot media, such as a DVD, that contains the boot image. The other is to use a PXE-based server to deploy the boot image directly to the client machine. Figure 4 shows the high-level process for building a client machine using a PXE server:

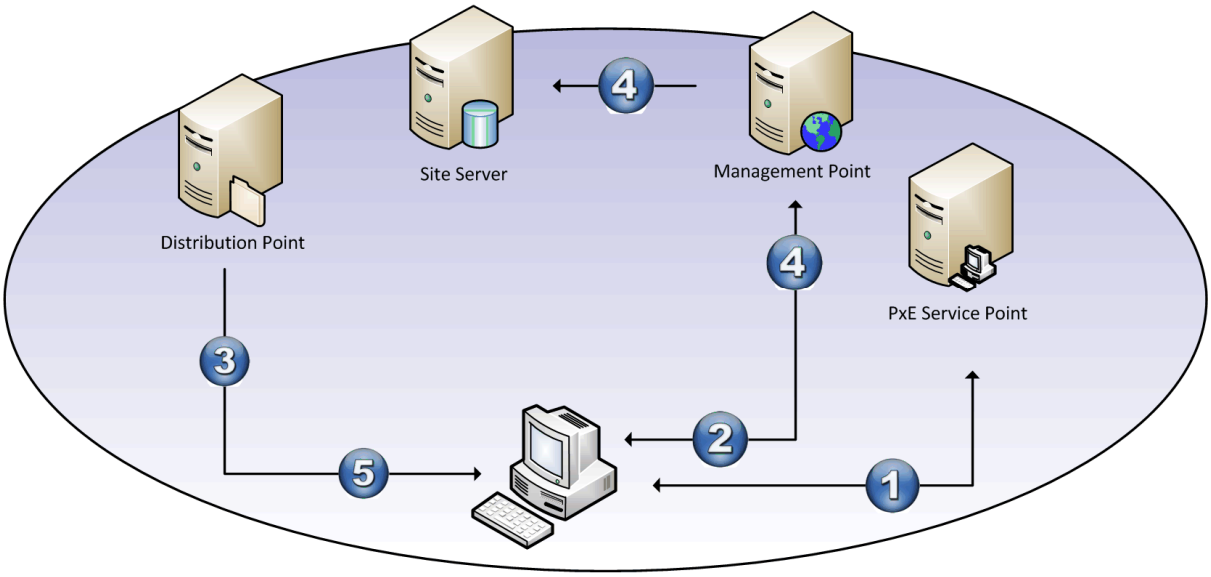


Figure 4: Operating System Deployment Overview

The only difference between this and using boot media is step 1 where the boot image is provided from the DVD, as opposed to being downloaded from the PXE server.

Table 4 describes each step of the PXE-based Operating System Deployment process in more detail:

Step	Description
1.	The client machine is turned on and DHCP address acquired. F12 network service boot is selected and the client downloads the Windows PE boot image from the PXE service point and loads into Windows PE.
2.	Windows PE queries for a Management Point and determines if any task sequences are advertised to the client machine. Task sequences are targeted to machines either by importing the machine prior to the network service boot by adding its Media Access Control (MAC) address, or using the unknown computer object. The task sequence defines which Operating System Install Package or Operating System Image package will be used to build the client machine and which DPs contain the package.
3.	The client contacts the DP and the image is installed using the parameters defined in the task sequence.
4.	The client hardware is scanned and a list of hardware devices is sent to the Management Point. The Management Point queries the database to determine if any matching drivers are available for the client and, if so, returns details of the location of the driver package that contains the required drivers.
5.	The client downloads and installs any drivers that are required and any software packages that are configured to be installed as part of the task sequence.

Table 4: PXE Boot-Based Operating System Deployment Overview Steps

More information on operating system deployment can be found in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.

2.2.1.2.4 Software Update Management

The Software Updates feature of Configuration Manager provides the capability to detect and report on the software update of a healthcare organisation. Combined with the software distribution feature, which allows the healthcare IT Administrators to deploy any 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 following sections describe the key components of the Software Updates feature of Configuration Manager.

Search Folders

Search folders allow the healthcare IT Administrator to create custom views on the 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), and are a useful way to rationalise the very large list of available updates.

Update Lists

An update list provides a mechanism of defining smaller collections of updates that are to be targeted. 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 determine 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.

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 repeatedly entering 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.

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 to which distribution points the package should be deployed. There is no direct link between a deployment and deployment package. If a deployment contains a particular software update, it can be accessed from any deployment package that happens to contain that update. If an update has been downloaded to more than one deployment package, clients will access the update from the most suitable deployment package, regardless of the deployment package that was referenced when running the software update wizard.

How Software Updates Work

Figure 5 shows a high-level overview of the software updates process in Configuration Manager:

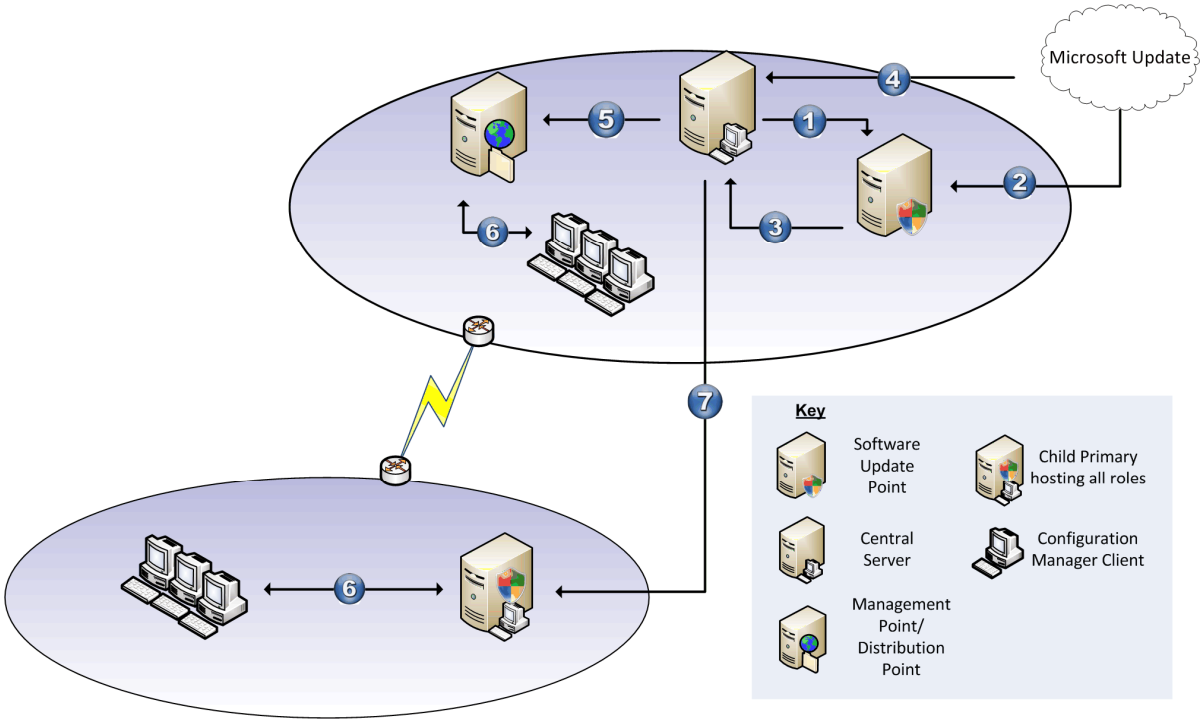


Figure 5: Software Updates Overview

Table 5 describes each step of the Software Update process in more detail:

Step	Description
1.	The Configuration Manager Site Server triggers a synchronisation of the Software Update Point (SUP). This is performed on a schedule or can be manually triggered using the Configuration Manager Console.
2.	This signals Microsoft® Windows Server Update Services (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 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 a healthcare 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 healthcare 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 healthcare IT Administrator can either download the updates from Microsoft Update ready for a future deployment or create the deployment at the same time.
5.	The healthcare 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 Distribution Points. A policy will be created and placed on the Management Point so that clients know the new updates are available and from where they should be installed.
6.	Clients perform a scheduled scan for new updates and retrieve the policy from the Management Point. If any updates are applicable on the client, they will be installed from the closest Distribution Point. As the client scans for required updates and installs updates, State Messages are sent to the Configuration Manager infrastructure so the healthcare IT Administrator has an up-to-date view of the status of the deployment.

Step	Description
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 1-3; the only difference being the lower level SUP will synchronise data with its parent rather than going directly to the Microsoft Update servers.

Table 5: Software Updates Process Overview

More information on Software Update Management in Configuration Manager is available in *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**.

2.2.1.2.5 Software Metering

Software Metering allows the healthcare IT Administrator to collect information on the programs that are being run in a healthcare organisation. The healthcare IT Administrator can configure rules to tell the client to collect usage data on a particular application's executable or an instance of a Microsoft Application Virtualization (App-V) virtual application, such as Microsoft® Office Visio®. This data, combined with the software inventory, provides the healthcare organisation with a view of applications that are actually being run, in addition to applications that are deployed. This can help the healthcare organisation to decide how many licenses are required for a particular application and also if a particular application is being used at all. If an application is no longer used, it can be retired from the healthcare organisation, which can help to reduce the complexity of support.

Configuration Manager will automatically create rules based on data returned by software inventory; these rules are created and are disabled by default. The healthcare IT Administrator can enable these rules to trigger the Configuration Manager client to start to collect data on the application or can create rules manually. The data collected by these rules can be used to create collections, queries or reports. More information on Software Metering in Configuration Manager is available in the TechNet article *Software Metering in Configuration Manager*[4].

2.2.1.2.6 Desired Configuration Management

Desired Configuration Management allows the healthcare IT Administrator to create or import Configuration Baselines that define a specific configuration to which client machines must adhere. This can be for any number of configuration items such as:

- Ensuring the correct operating system is installed and configured correctly
- Ensuring the correct applications are installed and configured correctly
- Ensuring prohibited applications are not installed
- Ensuring the correct security settings are applied

Microsoft and other vendors provide Configuration Packs[5] that contain configuration best practices for a number of applications and these can be imported and applied in the healthcare organisation. These packs can be used as a complete solution, or can be modified to fit the needs of the healthcare organisation. Configuration Packs can also be created by the healthcare IT Administrator using the Configuration Manager Console. More information on Desired Configuration Management in Configuration Manager is available in the TechNet article *Desired Configuration Management in Configuration Manager*[6].

[4] Microsoft TechNet: Software Metering in Configuration Manager **{R6}**: http://technet.microsoft.com/en-gb/library/bb694169.aspx

[5] Microsoft Downloads: Configuration Manager 2007 Configuration Pack Catalog **{R7}**: http://www.microsoft.com/technet/prodtechnol/scp/configmgr07.aspx

[6] Microsoft TechNet: Desired Configuration Management in Configuration Manager **{R8}**: http://technet.microsoft.com/en-gb/library/bb693504.aspx

2.2.1.2.7 Out of Band Management

Out of Band Management allows a healthcare IT Administrator to take advantage of the management controller available on machines that have the Intel® vPro® chipset and Intel Active Management Technology (AMT). This technology allows the healthcare IT Administrator to connect to a machine that is turned off, in a sleep or hibernation state, or if the operating system has become unresponsive, in order to perform the following actions:

- Power on or off one or many computers
- Reconfigure BIOS settings
- Boot to a command prompt to perform diagnostics
- Reimage a non-functioning machine by booting to a PXE server

More information on Out of Band Management in Configuration Manager is available in the TechNet article *Out of Band Management in Configuration Manager 2007 SP1*[7].

2.2.1.2.8 Reporting

The Reporting feature of Configuration Manager allows the healthcare IT Administrator to create and view Web-based reports on any aspect of the information contained in the Configuration Manager site database. A large number of reports containing detailed information on all aspects of Configuration Manager are included with the product. The healthcare IT Administrator can create new reports based on the exact requirements of the healthcare organisation. The queries contained in the existing reports can serve as a good starting point for creating custom reports to retrieve any required information. With Configuration Manager 2007 Release 2 (R2), SQL Server Reporting Services support is included, which allows an even richer toolset to be used to create customised reports for use within the healthcare organisation. Once reports have been created, a dashboard can be used to group together sets of useful reports that can be provided to users and management. This allows users to see multiple useful reports on a single Web site using a single link, and allows the healthcare IT Administrator to easily control who can view the data within the reports. More information on Reporting in Configuration Manager is available in the TechNet article *Reporting in Configuration Manager*[8].

2.2.1.2.9 Mobile Device Management

The Mobile Device Management feature allows the healthcare IT Administrator to manage mobile devices such as Personal Digital Assistants (PDA) and mobile phones running Windows Mobile® and Windows CE® operating systems. Configuring these devices to be Configuration Manager clients allows the healthcare IT Administrator to perform the following functions on the mobile device:

- Hardware inventory
- Software inventory
- File collection
- Software distribution
- Device configuration (such as Internet and e-mail settings, and Wi-Fi policies)

[7] Microsoft TechNet: Out of Band Management in Configuration Manager 2007 SP1 **{R9}**: http://technet.microsoft.com/en-gb/library/cc161989.aspx

[8] Microsoft TechNet: Reporting in Configuration Manager 2007 **{R10}**: http://technet.microsoft.com/en-gb/library/bb632630.aspx

More information on Mobile Device Management in Configuration Manager is available in the TechNet article *Mobile Device Management in Configuration Manager*[9].

2.2.1.2.10 Network Access Protection Integration

Network Access Protection (NAP) is a technology built into Windows Server® 2008 that allows the healthcare IT Administrator to define a policy that states the minimum configuration a client must meet before being allowed access to the healthcare organisation's network. The policy enforces items such as software updates that must be installed on a client machine before they are allowed to connect to the network. This works by placing any client joining the network into a quarantine subnet and requiring the client to provide its current software update status. If the client does not meet the requirements, the software updates are installed from the Configuration Manager Software Update Point. Once the client machine meets the requirements of the policy, it is allowed onto the production network. The policy can be configured to re-evaluate the clients' software update status in accordance with a schedule so the healthcare IT Administrator can ensure that all client machines on the healthcare organisation's network comply with the current NAP policy. More information on NAP integration in Configuration Manager is available in the TechNet article *Network Access Protection in Configuration Manager*[10].

2.2.1.3 Configuration Manager Site Systems

Each Configuration Manager site contains a site server and one or more site systems. A site system is any server running a supported version of Windows® or a shared folder that provides some functionality to the Configuration Manager site. A site system role is a role that a site system performs in a Configuration Manager site. For example, the MP role provides a communication point between the Configuration Manager site and Configuration Manager clients. A computer hosting the MP is a site system.

To decrease the load on primary or secondary site servers, it is possible to perform some server tasks on computers other than the site server.

The Configuration Manager Administrator can assign site system roles to the primary site server or distribute them among several different site systems. Some site system roles are assigned during installation. Other site system roles are assigned through the Configuration Manager Console. Servers are often referred to by their site system role name. For example, a server that performs the Distribution Point role is often called a Distribution Point. This section provides more detailed information about the site system roles that comprise Configuration Manager functionality. These include:

- Site server
- Component server
- Configuration Manager site database server
- Distribution Point (DP)
- Management Point (MP)
- Server Locator Point (SLP)
- Reporting Point (RP)

[9] Microsoft TechNet: Mobile Device Management in Configuration Manager **{R11}**: http://technet.microsoft.com/en-gb/library/bb633175.aspx

[10] Microsoft TechNet: Network Access Protection in Configuration Manager **{R12}**: http://technet.microsoft.com/en-gb/library/bb693725.aspx

- Reporting Services Point (RSP)
- System Health Validator Point (SHVP)
- State Migration Point (SMP)
- PXE service point (PSP)
- Fallback Status Point (FSP)
- Asset Intelligence Synchronization Point (AISP)
- Out of Band Service Point (OOBSP)

Some site system roles can only be installed as part of a primary site. Table 6 provides more information on the site system roles available, along with where they can be installed:

Component	Description	Location
Site Server	The Site Server hosts the Configuration Manager components that are necessary to monitor and manage a Configuration Manager site. When Configuration Manager is installed on a computer, that computer is automatically assigned the Site Server role. The site server computer can host additional roles or these roles can be performed by other servers. By default, the Configuration Manager Console is installed on a primary site server during Configuration Manager setup.	Configuration Manager primary or secondary site
Site Database Server	The Configuration Manager site database server is a computer running SQL Server Standard or Enterprise Edition that stores information such as discovery data, hardware and software inventory data, and configuration and status information for the Configuration Manager site and its lower level sites. Every primary site in the Configuration Manager hierarchy contains a Configuration Manager site database. The Site Database Server role can be installed on the Site Server or on a remote computer. If remote, there must be a fast network connection (100Mbps or greater). The SQL Server installation can also be installed on a Windows Server Cluster to increase resilience.	Configuration Manager primary site only
Configuration Manager Console	The Configuration Manager Console is the primary tool for using Configuration Manager. The console is installed by default on the site server but can also be installed separately on any server or client machine with the required prerequisites. The console allows healthcare IT Administrators access to any objects within Configuration Manager where they have appropriate permissions. The console can also be configured to only show a subset of the nodes in the console to reduce the console's complexity. For example, this can be useful when providing a console to helpdesk staff so they can view information on client machines and use remote control tools, but are not exposed to Configuration Manager site settings or configuration.	Configuration Manager primary site only
Management Point (MP)	The Management Point is the primary point of contact between Configuration Manager clients and the Configuration Manager site server. A Configuration Manager site has only one default Management Point, although multiple Management Points can be configured with Windows Network Load Balancing Service (NLB).	Configuration Manager primary or secondary sites (referred to as a Proxy MP at Secondary Sites)

Component	Description	Location
Distribution Point (DP)	The Distribution Point stores Configuration Manager package source files that Configuration Manager clients use when installing software programs or software updates distributed by Configuration Manager. The Configuration Manager Administrator can enable the Distribution Point to use Background Intelligent Transfer Service (BITS), which enables incremental package file download to Configuration Manager clients. It is also possible to specify a client computer to be a Branch Distribution Point, which allows the Configuration Manager Administrator to reduce the amount of network traffic required when distributing software to clients in remote locations, or over slow network links where no server hardware exists.	Configuration Manager primary or secondary sites
Reporting Point (RP)	A Reporting Point is a server that hosts the code for Report Viewer and any supplemental reports. A Reporting Point communicates only with its Configuration Manager site database server. The reporting point allows the healthcare IT Administrator to view reports on all facets of the Configuration Manager infrastructure, such as software deployment status or inventory data, and make this data available to users without having to provide them with a Configuration Manager Console. It also allows Dashboards to be created, which group together reports into a single page. This can be useful for providing information, such as software update compliance, or reporting asset data to management.	Configuration Manager primary site only
Reporting Services Point (RSP)	A Reporting Services Point provides the same reporting functionality as the Reporting Point but uses SQL Server Reporting Services technology, which allows for much greater flexibility when creating custom reports and can be integrated with technologies such as Microsoft® Office SharePoint® Server.	Configuration Manager primary site only
Server Locator Point (SLP)	The Server Locator Point locates MPs for Configuration Manager clients that are unable to retrieve information from Active Directory® because the client is part of a workgroup or the Active Directory Schema has not been extended.	Configuration Manager primary site only
System Health Validator Point (SHVP)	The System Health Validator Point uses a server with the Network Policy Service (available in Windows Server 2008) and allows the healthcare IT Administrator to integrate Configuration Manager with Microsoft Network Access Protection (NAP). This allows the healthcare IT Administrator to enforce criteria that clients must meet before they are allowed onto the network, such as software update compliance, presence of an anti-malware product and so on. Integrating Configuration Manager with NAP allows Configuration Manager to deploy any required updates or software to the clients while they are in a quarantined network, so they will then be allowed onto the production network.	Configuration Manager primary site only
State Migration Point (SMP)	The State Migration Point is a site system that allows the Configuration Manager client to store any required user data while a computer is migrated to a new operating system. This allows the healthcare IT Administrator to use the User State Migration Tool (USMT) in conjunction with Configuration Manager to capture user data from the target machine, rebuild the machine with the new operating system, and then replace the user data after the upgrade has completed.	Configuration Manager primary or secondary sites

Component	Description	Location
PXE Service Point	The PXE Service Point uses a server that has the Microsoft® Windows® Deployment Service (WDS) running and is used as part of the Operating System Deployment (OSD) feature of Configuration Manager. It responds to operating system deployment requests from client computers that have a PXE-enabled network card. The *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}** contains more information on the OSD features of Configuration Manager.	Configuration Manager central primary site only
Fallback Status Point (FSP)	The Fallback Status Point is a site system role that allows clients to communicate with the Configuration Manager infrastructure if they are unable to communicate via the MP. If a client is unable to install correctly, unable to assign itself to a site or cannot communicate securely with their assigned MP, a status message is sent via the FSP so the healthcare IT Administrator is aware there is an issue with the client.	Configuration Manager primary or secondary sites
Asset Intelligence Synchronization Point	The Asset Intelligence feature of Configuration Manager provides information on installed software that is collected via Hardware and Software Inventory and categorises the information in product types. This site system enables Configuration Manager to contact System Center Online (a service hosted by Microsoft) to update the catalogue of information when updates are made available.	Configuration Manager central primary site only
Out of Band Service Point	An Out of Band Service Point allows Configuration Manager to discover, provision and manage client computers that have management controllers using AMT technology (Such as Intel vPro chipset machines). This allows the healthcare IT Administrator to perform actions, such as startup, shutdown and restart, on client machines that may not have an Operating System (OS) or whose OS may have become corrupted.	Configuration Manager primary site only
Software Update Point	A Software Update Point is a site system that uses WSUS to provide update information to clients and to Configuration Manager allowing healthcare IT Administrators to perform software update management in a controlled manner from the Configuration Manager Console. The *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}** contains more information on the Software Update features of Configuration Manager.	Configuration Manager primary or secondary sites
Client Status Reporting Host System	Although the Client Status Reporting Host System site system role is not actually a site system configured in the Configuration Manager console, it is a role that can be added to a client or server computer to report back to the site server about the client computers it monitors.	Required only if using the client status reporting feature.

Table 6: Configuration Manager Site Systems Overview

2.2.1.4 The Configuration Manager Console

The Configuration Manager Console is the primary interface used to configure, run, and access Configuration Manager features and tools. An administrator installs and uses the Configuration Manager Console to accomplish the day-to-day tasks required to administer a Configuration Manager system. The Configuration Manager Console provides functions used to configure Configuration Manager sites, maintain the Configuration Manager site database, and monitor the status of a Configuration Manager hierarchy.

The Configuration Manager Console can be used to connect to any Configuration Manager primary site, but cannot be connected directly to a secondary site. Once connected to a primary site, it is possible to configure any direct or indirect child sites of that primary site. The only way to configure a secondary site is to connect a console to a primary site that has visibility of that secondary site. For example, Figure 6 shows part of a Configuration Manager Console connected to a central site (with site code **C01**) that has a child primary site (with site code **P01**), which in turn has a child secondary site (with site code **S01**):

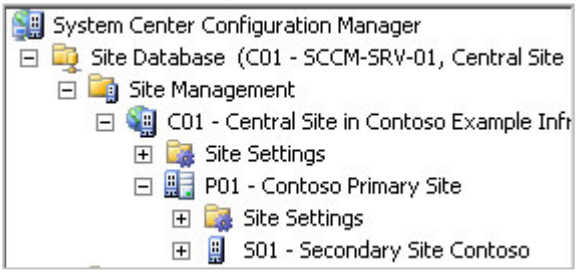


Figure 6: Configuration Manager Console with Visibility of a Secondary Site

As illustrated above, whilst connected to C01, it is possible to navigate to and configure the child sites.

If necessary, it is possible to connect to multiple primary sites from a single administrator console. To connect to another site, simply right-click the **System Center Configuration Manager** node and select **Connect to Site Database**, as shown in Figure 7:

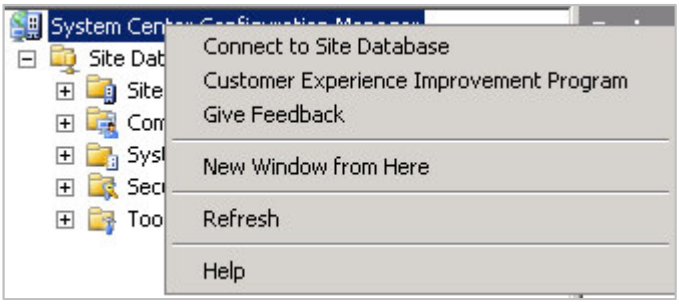


Figure 7: The Systems Management Server Right-Click Menu

This launches a simple wizard that assists in connecting to any other primary site to which the administrator has access.

Figure 8 illustrates the administrator console connected to two primary sites. The individual connections have been highlighted for clarity:

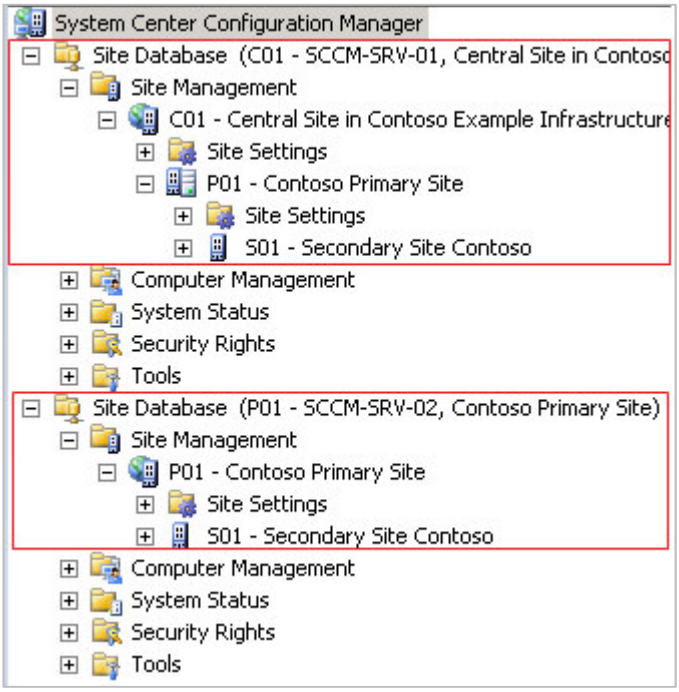


Figure 8: Configuration Manager Console Connected to Two Primary Sites

As shown in Figure 8, the connection to the central site (C01) allows the configuration of all other sites in the hierarchy. The connection to C01's child primary site P01 allows configuration of only P01 and any sites below P01. By connecting to a site, an administrator is connecting directly to the resources on that site server.

To administer a site (for example, modify site settings, create collections, packages, advertisements, and so on), the administrator must connect the console directly to that site. However, any collections, advertisements, packages, and so on, created at a site will flow down to child sites. Using the above example, if the administrator created a new collection whilst connected to C01, this collection would flow down to P01. Site settings, however, do not flow down the hierarchy and must be configured by either connecting directly to the site server or modifying the settings using the Site Settings node under the site object in the Configuration Manager Console. The administrator may wish to connect to P01 to create a collection, for example, if they did not want that collection to exist at C01 (because this information does not flow up, only down). This may be done if a distributed administration model is in place.

When performing site configuration tasks, the healthcare IT Administrator can often choose the most suitable method from a number of alternatives. For example, when navigating to the client agents node for a newly installed primary site, the administrator can achieve this either through the Configuration Console Manager connected to the central site (as this can be used to configure all sites in the hierarchy), or from a console connected directly to that primary site. The exception to this is when the administrator needs to perform administration tasks (as opposed to site configuration tasks). An important example of this is performing the client push installation by right-clicking on a resource or collection and running the Client Push Installation wizard. When this is done, the computers targeted for push installation will copy the client installation files (around 7MB) from the site to which the Configuration Manager Console is connected. Therefore, it is important to perform this from the primary site closest to the computers to which the client is being pushed.

> **Note**
>
> If a site is administered whilst connected to a parent site, any settings changed will need to be replicated down to the site on which the administrator requested those settings to change. Using the example above in Figure 8, if the console was connected to C01 and the administrator configured some changes to the settings on S01, the instructions for this change would first need to be replicated to P01, which would in turn replicate to S01. This replication is performed using Configuration Manager 'senders'.

The administrator console is installed on all site servers by default. To remotely administer a Configuration Manager site, it is also possible to install the console on the Configuration Manager Administrator's computer (or on multiple computers if there are multiple Configuration Manager Administrators). This is recommended, as it allows administration of Configuration Manager without logging on to a server directly. The administrator console can be installed by running the standard Configuration Manager setup program and choosing the relevant installation option.

2.2.2 Training and Assessment

Guidelines on the basic skill sets that are required to make best use of System Center Configuration Manager 2007 R2 are detailed in APPENDIX A. These represent the training courses and other resources available. However, 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 implementing System Center Configuration Manager 2007 R2 in a healthcare organisation:

- Active Directory
- Domain-joined Windows Server® 2003 SP2 or SP3, Windows Server 2008 for server roles
- SQL Server® 2005 (SP2 or SP3), SQL Server® 2008 (SP1)
- Windows® 7, Windows Vista, Windows XP Professional (SP2 or SP3), or Windows 2000 Professional SP4, required for all desktop clients
- Microsoft Windows® 2000 Server SP4, Windows Server 2003 or Windows Server 2008, required for all Server clients

2.4 Audience

The guidance contained in this document is targeted at a variety of roles within a healthcare organisation's IT department. Table 7 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	Develop	Stabilise	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 to meet local requirements	✓	✓	✓	✓	✓	✓

Table 7: Document Audience

2.5 Assumptions

The guidance provided in this document assumes that healthcare organisations that want to share services and resources between sites already have suitable IP Addressing schemes in place to enable successful site-to-site communication; that is, unique IP Addressing schemes assigned to each participating organisation or site with no overlap. Active Directory, and the underlying Domain Name System (DNS), require the use of unique IP Addressing schemes at adjoining sites in order for cross-site communication to function successfully. The use of NAT (Network Address Translation) within an Active Directory environment is neither recommended nor supported by Microsoft.

3 USING THIS DOCUMENT

This document is intended for use by healthcare organisations and healthcare IT Administrators who want to use Configuration Manager to manage servers, desktops or laptops within the healthcare organisation. The document should be used to assist with the planning and implementation 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 five sections that deal with the project lifecycle, as illustrated in Figure 9:

- Plan
- Develop
- Stabilise
- 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*[11] and the *MOF Executive Overview*[12]. 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.

[11] Microsoft Solutions Framework Core White Papers:
http://www.microsoft.com/downloads/details.aspx?FamilyID=e481cb0b-ac05-42a6-bab8-fc886956790e&DisplayLang=en

[12] MOF Executive Overview:
http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofeo.mspx

The five sections of this document are as follows:

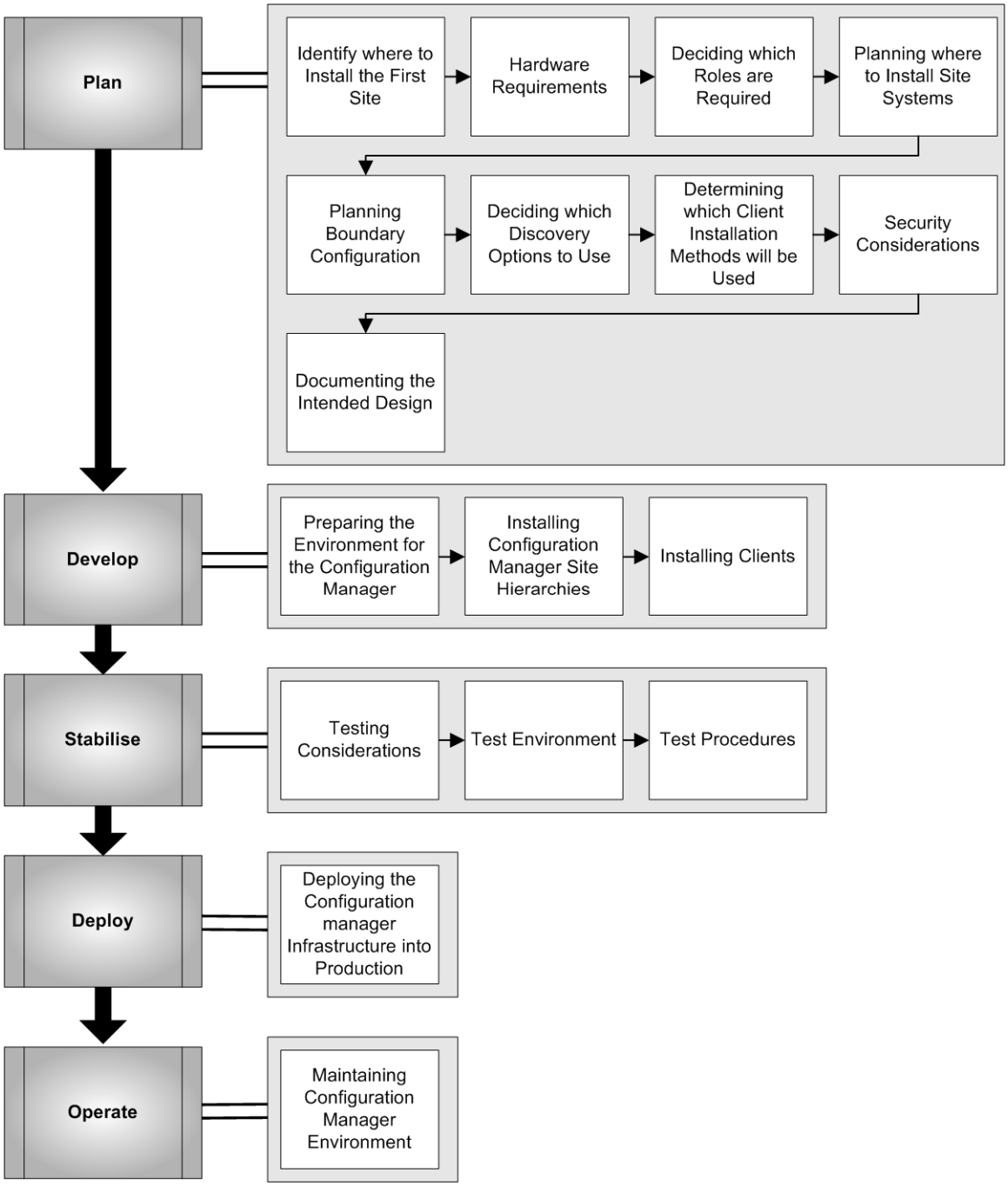


Figure 9: Microsoft Solutions Framework Process Model Phases and Document Structure

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.

- *System Center Configuration Manager TechCenter* **{R4}**
- *System Center Configuration Manager 2007 TechNet Library* **{R5}**

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 10 acts as a high-level checklist, illustrating the sequence of events that the IT Manager and IT Architect need to determine when planning for Configuration Manager within a healthcare organisation:

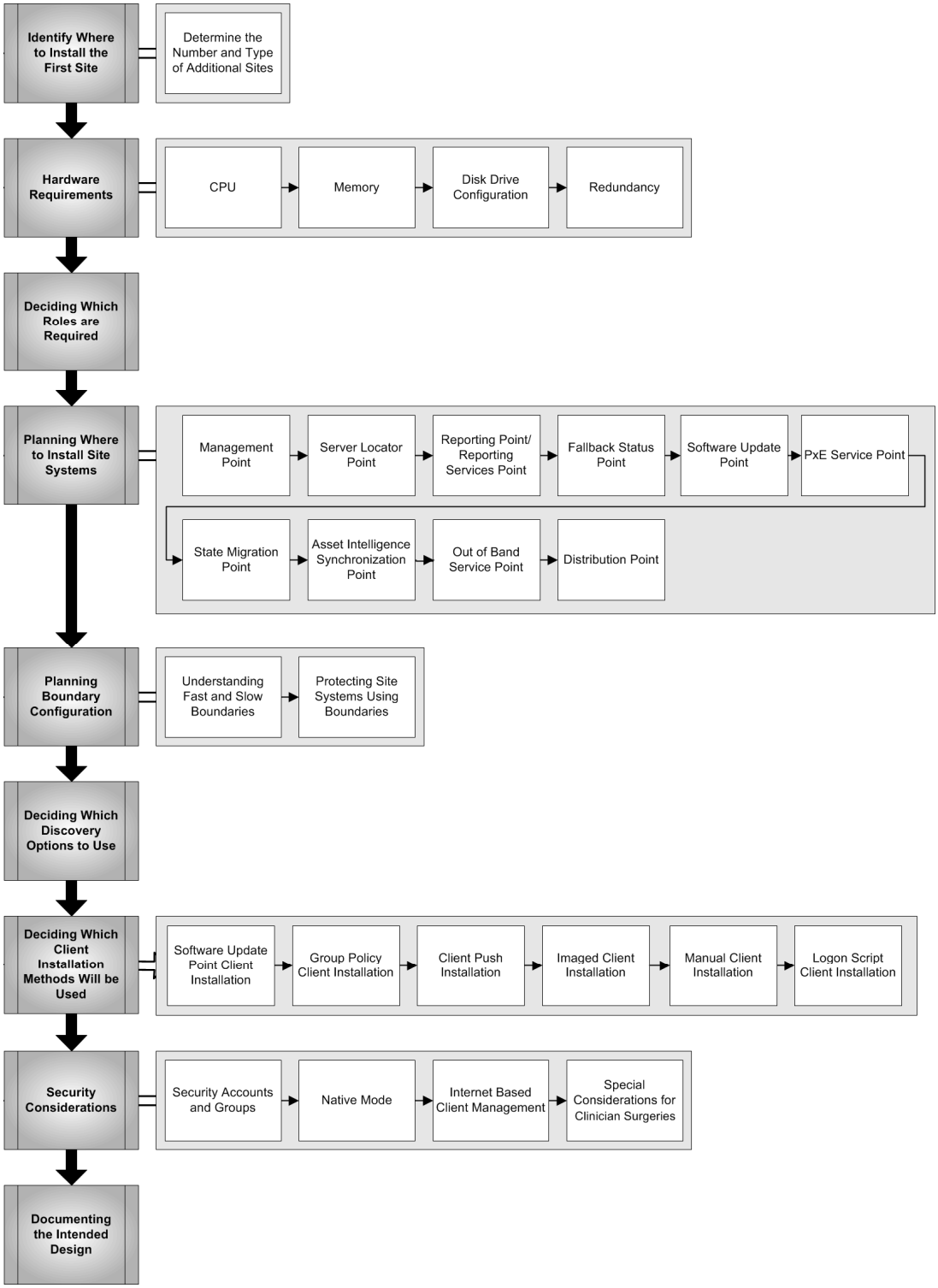


Figure 10: Sequence for Planning Configuration Manager

4.1 Identify Where to Install the First Site

When designing a Configuration Manager infrastructure, the healthcare IT Administrator should first decide where the first (Central) site will be located. This decision can sometimes be dictated by the healthcare organisation's operational structure or can be purely based on the network infrastructure. As discussed previously, the Central site is the top of any Configuration Manager hierarchy and the location where all data collected by Configuration Manager will be stored. It is also the central point of administration and control. If the healthcare organisation uses multiple sites in the hierarchy, administrative control can be delegated to lower sites in the hierarchy but the central site will always act as the central point of administrative control. The Configuration Manager central site should usually be placed at the highest logical point of administration in the healthcare organisation. For example, in an Acute Care organisation that may manage a number of hospitals, the server should be placed in a data center that is in the same physical site as the health organisation's IT Administrators who will manage the whole Configuration Manager hierarchy. In a General Practice provider, the server should be placed in the data center of the General Practice's central administrative office (or the Acute Care organisation that provides IT services to the General Practice, if that is the case).

This may not always be the best design if the underlying network infrastructure does not match the administrative model. For example, Figure 11 shows a network infrastructure for an Acute Care organisation. In this example, the Configuration Manager Central site should be installed into a data center at the Main Hospital site rather than at the Administration Centre site. This will allow all data to flow to highest logical point in the hierarchy. Healthcare IT Administrators can then connect to the Configuration Manager Console across the 100 Mb connection but all client data from the Main Hospital will remain in that site.

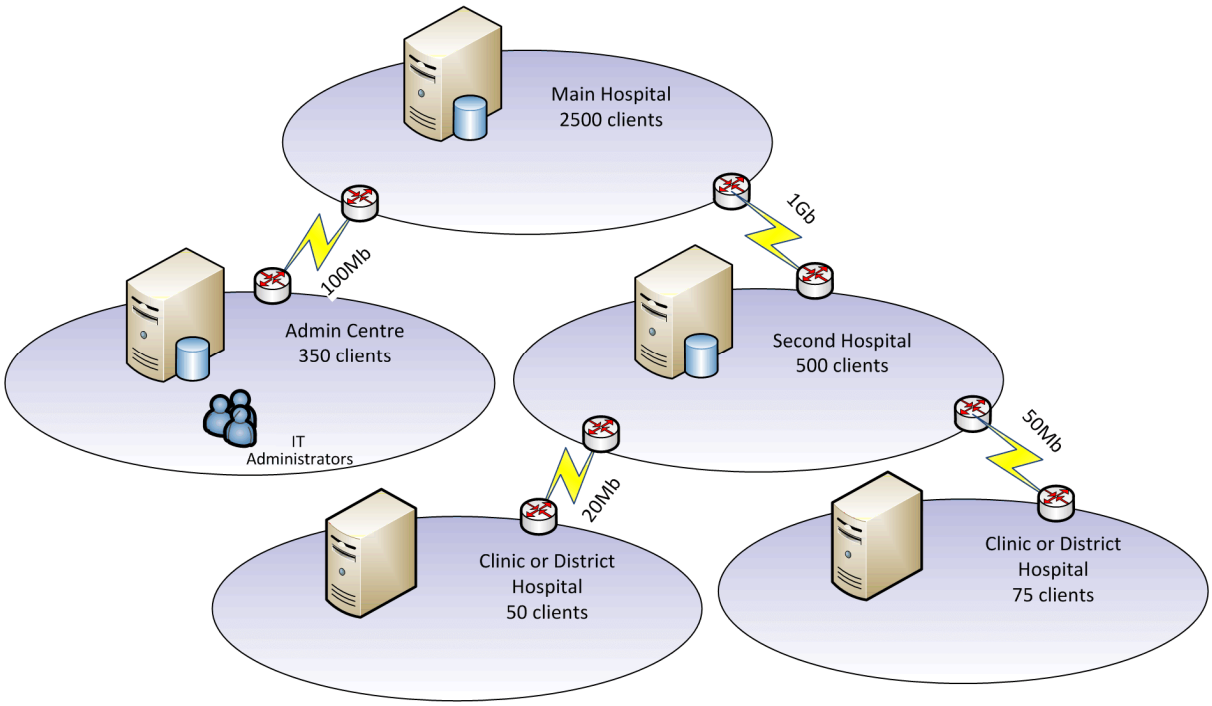


Figure 11: Example Hierarchy Not Aligned With Administrative Model

4.1.1 Determine the Number and Type of Additional Sites

Once the healthcare IT Administrator has decided the location of the Central site, it should be determined if any additional child primary sites need to be deployed in the healthcare organisation. This decision is often based on the number of clients that will be supported at each geographic location of the organisation and the services that will be provided. The main benefit of deploying additional primary sites is to allow the healthcare IT Administrator to strictly control the bandwidth used across network links, such as WANs. The healthcare IT Administrator should aim to deploy the fewest number of sites possible within the healthcare organisation, but in some cases it will be necessary to deploy additional primary sites depending on the underlying network infrastructure. Another reason to deploy a Child Primary site is if the healthcare IT Administrator of the central site needs to delegate administrative control of an entire geographic location to a different set of administrators.

Figure 12 shows the infrastructure of an example healthcare organisation that includes an Acute Care organisation and General Practice provision:

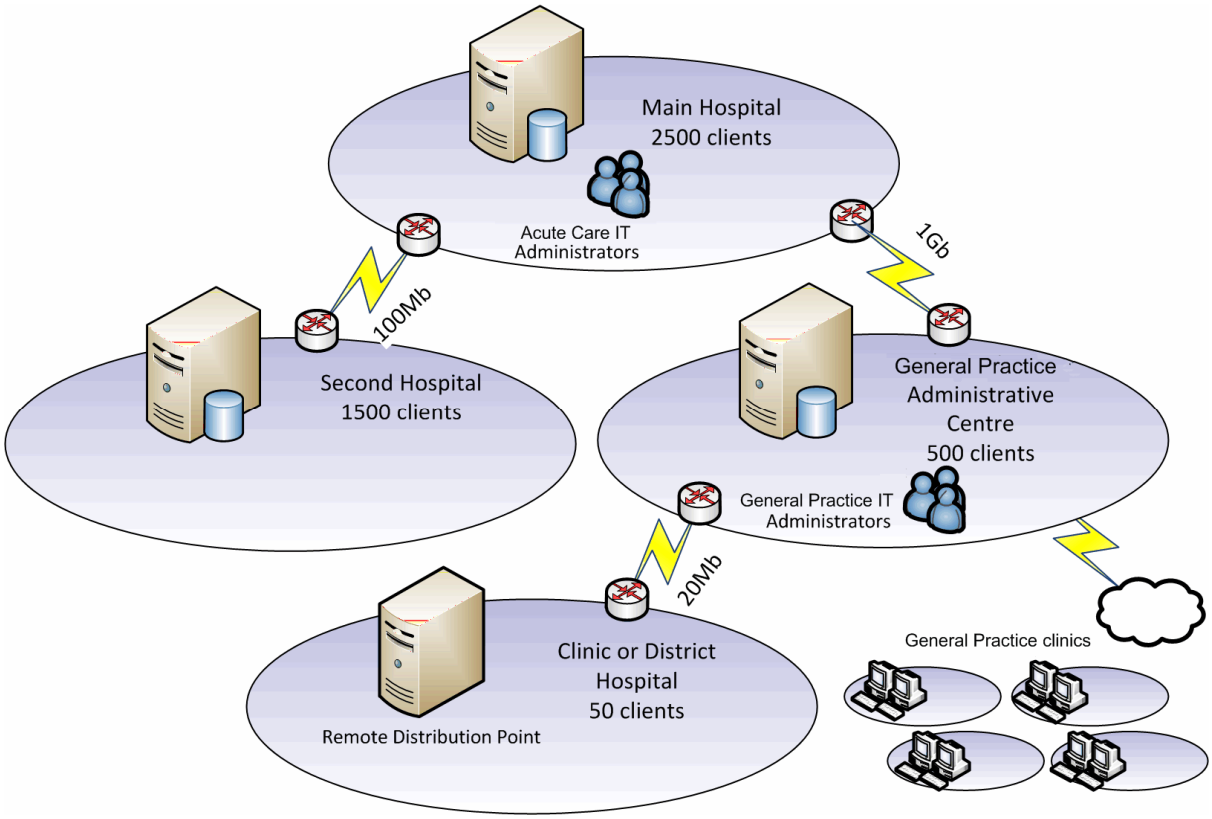


Figure 12: Determining if Additional Sites are Required

In this example, the Central Site has been placed in the Main Hospital because this is where the majority of the clients are located and the healthcare IT Administrators responsible for the whole hierarchy are based. A Child Primary site has been placed in the Second Hospital site because there are a reasonably large number of clients that are supported by a 100 Mb connection. This allows the healthcare IT Administrator to reduce the amount of traffic that Configuration Manager creates over this network connection to a minimum, and to control the times of the day the connection is used to replicate data to the Central Site.

A Child Primary site has been placed in the General Practice Administrative Centre because this will not only allow the traffic to be controlled when replicating data back to the Central site, but also allow the General Practice IT Administrators to have full control over the clients in that site and all locations beneath it in the hierarchy. This will allow for the creation of reports that are specific to General Practice and also allow packages and operating systems to be created and deployed at this level that may not be relevant to the client machines in the Acute Care organisation (packages only flow down the hierarchy). This configuration also means that the healthcare IT Administrators at the Central site can make packages, software updates and operating systems available to the clients in General Practice, if required. Reports that include all the clients in the whole hierarchy can be created at the central site. A remote DP has been used to reduce the network traffic across the 20 Mb link. Section 4.4.2 describes when to use the different types of DPs and Secondary Sites.

4.2 Hardware Requirements

It is important that the hardware to be used for the Configuration Manager site server is adequately specified in terms of performance. Typically, the first Configuration Manager site to be installed becomes the Configuration Manager central site and, as such, will need to receive and process data from child sites within the hierarchy.

In addition to the performance, it is important to provide enough disk space to store the data generated and gathered by Configuration Manager, and to store packages that will be deployed using Configuration Manager.

> **Note**
>
> If the intention is to install Configuration Manager in a test environment, the recommended hardware and disk configurations are not critical. For example, it would be feasible to install the operating system, SQL Server and Configuration Manager on a single partition.

Sections 4.2.1 to 4.2.3 provide the healthcare IT Administrator with estimates of the server hardware that will be required for Configuration Manager site servers. The numbers used should be counted for all clients that will report to the site and any child sites. For example, Figure 13 shows a three-tiered hierarchy with the number of supported clients in each site. In order to calculate the required hardware for each site server, the client numbers need to be rolled up so they are included in the client numbers for all sites above the site in the hierarchy.

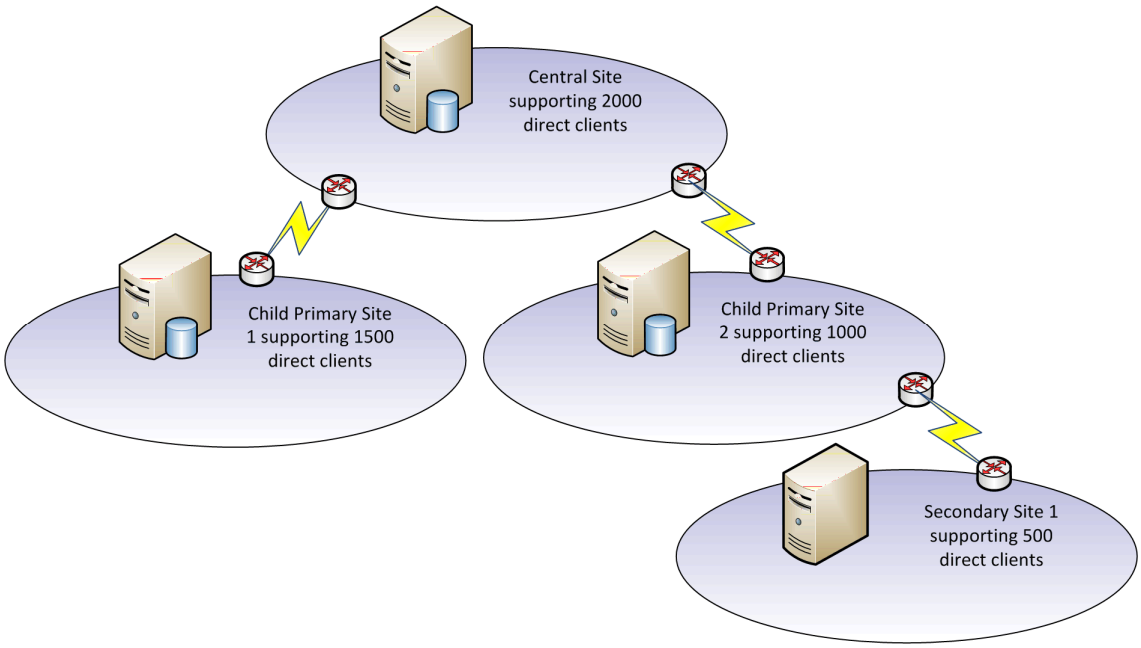


Figure 13: Client Number Rollup for Example Hierarchy

Table 8 shows the total number of clients that should be considered when calculating the hardware for each site server for the example hierarchy shown in Figure 13:

Site	Total Number of Clients Used for Calculating Hardware
Secondary Site 1	500
Child Primary Site 1	1500
Child Primary Site 2	1500
Central Site	5000

Table 8: Client Number Rollup for Calculating Hardware Requirements for Servers

4.2.1 CPU

Table 9 and Table 10 detail a range of CPU speeds and numbers, with average levels of support. There are many factors that will influence the accuracy of the information provided below, and therefore, it should be used as guidance only. Additionally, these values consider average system load and feature settings. Adjusting any or all of the factors discussed earlier can impact the level of support provided by a particular hardware configuration.

CPU Speed	Approximate Number of Clients
1Ghz	1-500
2Ghz	500-2500
3Ghz	2500-15000
3Ghz +	15000-50000

Table 9: Client Support - CPU Speed

CPU Count	Approximate Number of Clients
1 Processor	1-2500
2 Processors	2500-25000
4 Processors	25000-50000
8 Processors	50000+

Table 10: Client Support - CPU Count

Using the tables above, it is possible to identify reasonable processor specifications for a given Configuration Manager primary site server. For example, to support 3,000 clients, a server with dual 3 GHz processors would be acceptable. In another example, if a server is to be used to support 30,000 clients, that server would require four 3 GHz processors for reasonable performance.

> **Note**
>
> Even using these guidelines, the capacity of the Network Interface Card (NIC) and disk configuration will have a significant influence on the performance of the server. Having multiple, fast processors cannot eliminate the bottleneck introduced by these two factors. Therefore, when performance is substandard, it is important to identify and mitigate the performance bottleneck on each server individually as opposed to simply considering an update to common hardware components such as processors and RAM. Tools such as the *Microsoft ® Windows Server ™ 2003 Performance Advisor*[13] and the *Performance Monitor Wizard*[14], *and guidance* such as the *Performance Tuning Guidelines for Windows Server 2008 R2*[15] can help the healthcare IT Administrator to identify performance bottlenecks and modify configuration to improve performance.

4.2.2 Memory

Configuration Manager does not have a high memory requirement. On average, the Configuration Manager core services (SMS_Executive) will only use 50 Mb to 150 Mb of memory during typical operational processes. This is mostly due to the type of tasks performed by the Configuration Manager threads (file parsing and copies).

The significant memory requirement of Configuration Manager comes from the demands of the SQL database. Many Configuration Manager functions consist of rapidly writing and reading a tremendous amount of data from the SQL database. If SQL is not operating efficiently, or it is unable to process transactions in a timely fashion, the performance of Configuration Manager will suffer.

While there is a correlation between client supportability, total server memory, and system performance, there is no defined ratio from which to identify the 'maximum amount of RAM necessary' on a server. It is advisable to configure a server with a reasonable amount of memory, and assess whether that amount is sufficient for the production workload placed on the server. This workload can not only change from organisation to organisation, but also from hour to hour.

The amount of memory required by a primary site server can vary. There is an average workload attributed to the number of managed clients, but if a site is used aggressively with frequent and large software distributions, inventory cycles, and reporting processes, it is possible that the site server will be unable to keep up.

Table 11 lists the System Memory required for a specified number of clients:

System Memory	Approximate Number of Clients
1GB	1-500
2GB	500-3000
3GB	3000-8000
4GB	8000-15000
6GB	15000-25000
8GB +	25000+

Table 11: System Memory – Number of Clients

[13] Microsoft Downloads: Microsoft ® Windows Server ™ 2003 Performance Advisor: http://www.microsoft.com/downloads/details.aspx?familyid=09115420-8C9D-46B9-A9A5-9BFFCD237DA2&displaylang=en

[14] Microsoft Downloads: Performance Monitor Wizard: http://www.microsoft.com/downloads/details.aspx?familyid=31FCCD98-C3A1-4644-9622-FAA046D69214&displaylang=en

[15] Microsoft Downloads: Performance Tuning Guidelines for Windows Server 2008 R2: http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv-R2.mspx

4.2.3 Disk Drive Configuration

Configuration Manager heavily uses the disk drives to store its own configuration and instruction files, and to store data within the SQL database. As such, it is important that the disk drives are configured appropriately. To increase the read/write performance of Configuration Manager, it is recommended that certain types of data are separated onto dedicated drives. These drives should be separate physical drives, which are either configured in an array or as stand-alone disks. However, it is recommended that the drives are configured in an array as this improves the performance considerably and, in some cases, provides resiliency.

As a minimum, it is highly recommended that the operating system, Configuration Manager and SQL Server databases are separated onto different arrays. If possible, the Configuration Manager packages and Configuration Manager database transaction log should be separated to further increase the disk performance.

Table 12 below lists the recommended configuration for the central Configuration Manager site server. Within the 'RAID Level' column, three options are listed. These options are provided for guidance only, as available RAID levels may vary due to different hardware. They are ordered by preference, with the preferred option on the left.

Array	RAID Level	Data
1 (C:)	1	Operating system (including pagefile) and SQL binary files.
2 (D:)	10, 1, 5	Configuration Manager and compressed packages.
3 (E:)	10, 1, 5	Configuration Manager database and SQL tempdb (including transaction logs).
4 (F:)	5	Configuration Manager packages and backup.

Table 12: Central Site Disk Drive Configuration

> **Note**
>
> The drive letters used in the 'Array' column in Table 12 are examples.

It is not always possible (due to hardware restrictions, budget and so on) to achieve the recommended RAID levels. Table 13 below shows an example of a typical server disk configuration with six disks available:

Array	RAID Level	Data	Number of Required Disks
1 (C:)	1	Operating System (including pagefile) and SQL binary files.	2
2 (D:)	1	Configuration Manager, packages and compressed packages.	2
3 (E:)	1	Configuration Manager database, SQL tempdb (including transaction logs) and backup folder.	2

Table 13: Example Central Site Disk Drive Configuration

> **Note**
>
> It is highly recommended that the above components are separated and disk arrays are used; however, it is not a requirement for Configuration Manager.

To determine the amount of disk space that will be required, it is necessary to estimate the eventual number of clients that Configuration Manager will manage.

Use Table 14 below to aid in the estimation of the disk space requirements:

Component	Disk Space	Notes
Operating System (Windows Server 2008)	RAM + 25 GB	RAM refers to the amount of physical memory installed and is specified to allow for the OS pagefile.
Configuration Manager (binaries and inboxes)	20 GB	
SQL (binaries)	5 GB	
Configuration Manager database + transaction log	((Number of machines) * 4 MB) + (30% of DB size)	By default, Configuration Manager will store up to 4MB of data per Configuration Manager client, although this can increase if additional changes are made to the SMS_DEF.MOF file, or if files are collected using software inventory. The Configuration Manager DB transaction log should be sized at 30% of the DB size.
SQL tembdb + transaction log	70% of (Configuration Manager DB and log)	The tempdb database should be sized at 50% of the Configuration Manager database, and the tempdb database transaction log should be sized at 20% of the Configuration Manager database.
Packages	Total size of packages that will be distributed through Configuration Manager	This should include the total size of all software packages and operating system images as well as all drivers that will be used for OS deployment. If the source files for the packages are also stored on the server, this figure should be doubled.
Compressed packages	Same as Packages	The majority of packages are already compressed and, as such, the disk space required will not vary a great deal from the original uncompressed package source files. This is particularly the case with Windows Installer packages (MSI files).
Backup	Configuration Manager Database (no. clients * 4MB) + 20%	The backup is essentially a backup of the Configuration Manager database together with all the necessary configuration files.

Table 14: Central Site Disk Space Requirements

4.2.4 Redundancy

The healthcare IT Administrator can choose to install SQL Server in a clustered configuration, which will provide good resiliency for the data, but the site server can still be a central point of failure for Configuration Manager. The healthcare IT Administrator should ensure that regular backups are taken of Configuration Manager using the built-in backup task, and should also ensure the backup of the source location for any Configuration Manager packages, software updates, and operating system install packages or images. The healthcare IT Administrator should also purchase the most resilient hardware where possible. This should include multiple (redundant) power supplies and multiple (teamed) Network Interface Cards (NIC). Remote component servers, such as MPs, DPs, and so on, can be quickly and easily redeployed in the event of a failure, but if the site server fails, the healthcare IT Administrator will need to restore the site from the last available backup using the Site Recovery Wizard. If the database is also lost, this can result in the loss of data.

4.3 Deciding Which Roles are Required

Each of the features of Configuration Manager will require that certain site systems are deployed to support the feature. If a feature is not being used, the healthcare IT Administrator should not deploy the site system role because this increases the potential attack surface of the product. Table 15 shows the roles that the healthcare IT Administrator must deploy in order to support specific features of the product:

Features	Roles Required
Normal Site Operation	Management Point, Distribution Point, Fallback Status Point, Server Locator Point
Reporting	Reporting Point, SQL Reporting Services Reporting Point
Software Update Management	Software Update Point, Management Point, Distribution Point
Operating System Deployment	PXE Service Point, User State Migration Point, Management Point, Distribution Point
Software Distribution	Management Point, Distribution Point
Hardware and Software Inventory	Management Point, Distribution Point
Software Metering	Management Point, Distribution Point
Desired Configuration Management	Management Point, Distribution Point
NAP Integration	System Health Validator Point, Management Point, Distribution Point
Wake-on-LAN (if using AMT, not magic packet) and Out of Band Management	Out of Band Service Point, Management Point, Distribution Point

Table 15: Features and Role Requirements

4.4 Planning Where to Install Site Systems

When designing the Configuration Manager infrastructure, the healthcare IT Administrator needs to decide where to install site systems. The reasons for distributing site system roles to servers other than the site server include performance and scalability, and also the resiliency of the solution. Sections 4.4.1 to 4.4.10 describe each of the site system roles and should help the healthcare IT Administrator decide if the role should be co-located on the Configuration Manager site server, or if it should be placed on a separate server. Special consideration must be given to DPs when using the software distribution or operating system deployment features of Configuration Manager because the majority of network traffic generated by Configuration Manager clients and the DP.

4.4.1 Management Point

Management Points act as the point of contact between Configuration Manager clients and the Configuration Manager site server. There can only be one management point per site and it can be located on the Configuration Manager site server or a remote component server. If the site supports more than 1500 clients, it is recommended that the management point is located on a different server than the site server to improve performance. A single management point can support up to 25,000 client machines. It is unlikely that any healthcare organisation would need to support more clients than this in a single site, but if this is a requirement Network Load Balancing can be used to support additional clients. The most likely scenario for using an NLB MP in a healthcare organisation is to provide resiliency. Because the MP role can be quickly deployed to a new server in the event of a failure, it is not anticipated that this will be a requirement in most organisations. If there is a specific requirement to provide this functionality, refer to the TechNet article *How to Configure Network Load Balancing for Configuration Manager Site Systems*[16].

4.4.2 Server Locator Point

The Server Locator Point allows Configuration Manager clients to determine to which site they should be assigned in the following situations:

- Clients that are not part of an Active Directory (workgroup clients)
- Clients that are part of a different Active Directory forest than the site server
- Clients in an Active Directory where the schema has not been extended

If no clients in the healthcare organisation meet the above criteria, no SLP needs to be defined. If there are clients that will require an SLP, only one need be defined per Configuration Manager hierarchy and it can be located on the central site's MP server, or any other server that has Internet Information Services (IIS) installed. If resiliency is required for the SLP, it can be configured as part of an NLB cluster, but this is unlikely. If there is a specific requirement to provide this functionality, more information can be found in the TechNet article *How to Configure Network Load Balancing for Configuration Manager Site Systems*[10].

4.4.3 Reporting Point/Reporting Services Point

The Reporting functions in Configuration Manager are provided by either the Reporting Point or the Reporting Services Point. The Reporting Point is the Configuration Manager built-in reporting function and a Reporting Services Point uses SQL Reporting Services (SRS) to provide tools and resources to allow the healthcare IT Administrator to generate advanced reports from the Configuration Manager Console. These roles can be configured to run on the site server; however, if reporting is used heavily within the healthcare organisation it is recommended that these roles are separated onto a different server that has capacity, or a dedicated server.

[16] Microsoft TechNet: How to Configure Network Load Balancing for Configuration Manager Site Systems **{R13}**: http://technet.microsoft.com/en-gb/library/bb633031.aspx

4.4.4 Fallback Status Point

The Fallback Status Point (FSP) gathers status messages from clients that cannot install properly, cannot assign to a Configuration Manager site, or cannot communicate securely with their assigned management points. The healthcare IT Administrator should configure this role on a server other than the server running the MP role (because it provides resiliency when the MP cannot be contacted). All communications with the FSP use unsecured HTTP traffic so, where possible, the role should be installed on a server that does not host any other Configuration Manager functions. The role can be co-located with other servers running Internet Information Services (IIS) but performance should be analysed to ensure the role is not adversely impacting the other services hosted on the server.

4.4.5 Software Update Point

The Software Update Point integrates with Windows Server Update Services (WSUS) 3.0 SP1 or SP2 to provide software update scanning capabilities for clients. Guidance on using the Software Update Management feature of Configuration Manager is contained in the *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**.

4.4.6 PXE Service Point

The PXE Service Point integrates with Windows Deployment Services (WDS) to allow clients to boot from the network and have an operating system deployed to them automatically. Guidance on using the Operating System Deployment feature of Configuration Manager is provided in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.

4.4.7 State Migration Point

The State Migration Point is used when deploying operating systems using Configuration Manager. It allows the healthcare IT Administrator to store data collected by the User State Migration Tool (USMT) when migrating user settings during a deployment. Guidance on using the Operating System Deployment feature of Configuration Manager is provided in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.

4.4.8 Asset Intelligence Synchronization Point

The Asset Intelligence Synchronization Point is used to connect to System Center Online and retrieve update Asset Intelligence catalogues. This site role should be deployed at the central site and can be co-located with the site server.

4.4.9 Out of Band Service Point

The Out of Band Service Point discovers, provisions, and manages desktop computers that have management controllers (such as AMT-based computers). This role needs to be configured on all sites in a hierarchy where AMT-based computers will be managed. The role can be deployed on the site server or any other component server with spare capacity.

4.4.10 Distribution Point

When planning where to install Distribution Points (DPs) in a Configuration Manager deployment, careful consideration needs to be given to ensure that network bandwidth is used as efficiently as possible. There are no rules on the placement of DPs, so the following information should be used to make this decision. The healthcare IT Administrator should also consider the number of clients that will connect to any one distribution point because this can significantly impact the performance of software distribution. Again, there are no rules on the number of DPs that should be used but it is recommended that a DP should support no more than 1000 to 1500 clients. For example, if a health organisation is using a single site to manage 3500 clients, two to three distribution points should be configured. The exact number of required DPs will depend on the volume of software distribution and operating system deployments being performed in the organisation. The healthcare IT Administrator should monitor the performance and add additional DPs once the infrastructure is in full production, if required.

4.4.10.1 Package Placement

Software distribution in Configuration Manager uses a 'top-down' approach, meaning that a software package is imported into Configuration Manager at the point in the hierarchy where the package is most appropriate.

As an example, consider the Configuration Manager hierarchy in Figure 14:

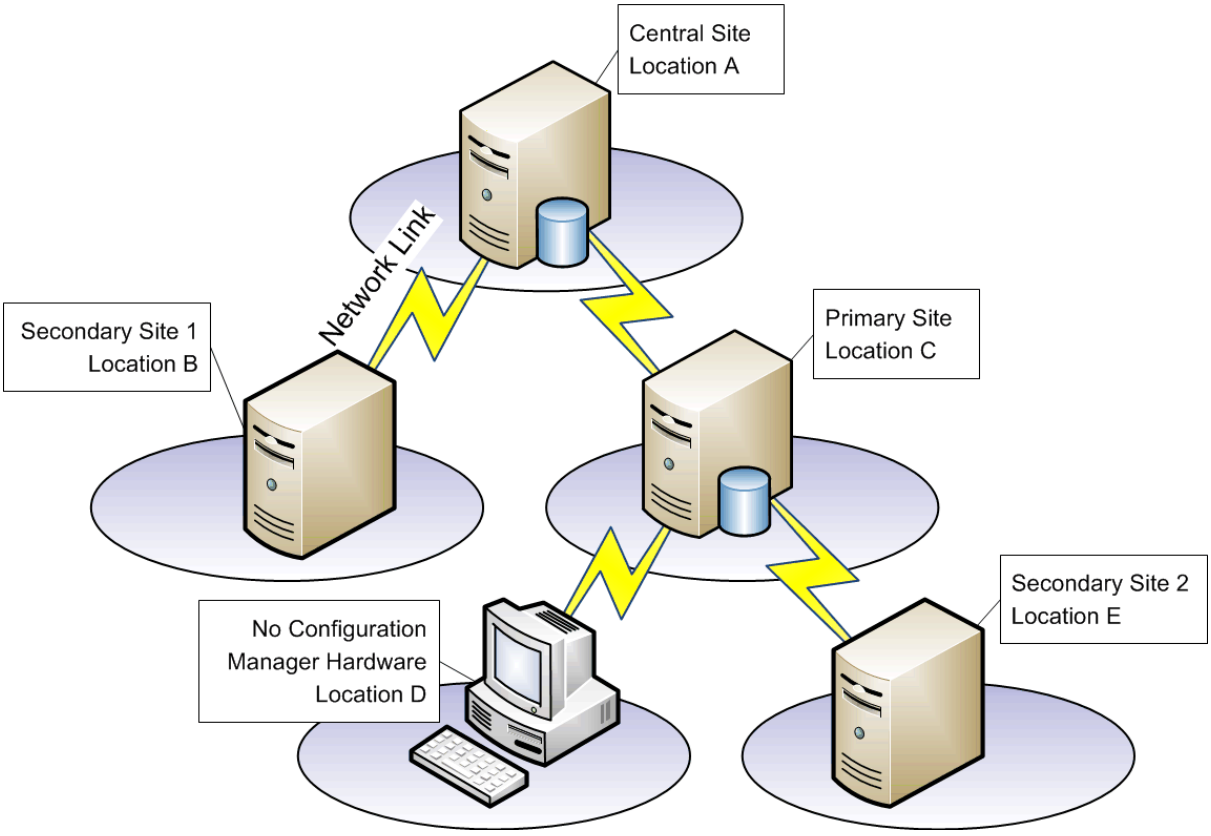


Figure 14: Example Configuration Manager Hierarchy

In this example, if a package is required to be installed on Configuration Manager client machines in all locations in the hierarchy, the Configuration Manager Administrator would need to create the package at the Central Site. This would allow the administrator to select every DP in the hierarchy, and Configuration Manager would move the software installation files (packages) to all of these DPs, according to the rules defined when setting up the site structure. These rules dictate settings like how much bandwidth is available to Configuration Manager during specific time periods, allowing the administrator to have more control over network bandwidth usage.

If the package is only required to be installed on machines in locations C, D and E, the administrator has the option to create the package at the Primary Site in Location C. This will mean that Configuration Manager will not need to copy the package source files across the network from the Central Site to the Primary Site, but will only enable the administrator to place the package source files on the DPs in the Primary Site and Secondary Site 2. Therefore, only Configuration Manager clients in locations C, D and E will be able to install the software. This will also mean that any advertisement status information relating to this package will not be sent to the parent sites, so central reporting will be unavailable for this package. For more information on Configuration Manager reporting, refer to the TechNet article *Reporting in Configuration Manager* **{R10}**.

4.4.10.2 Distribution Point Placement

When a Configuration Manager client receives an advertisement, it sends a request to its Management Point (MP) for the location of the package source files. This is called a Content Location Request. The MP then checks the Configuration Manager database to see which DPs have the content, and in which order the client should try them, based on the client's IP address. This allows the Configuration Manager client to connect to the DP that is best suited to the client.

The decision of where to place the DP may also be influenced by available hardware. If only one server is available for all Configuration Manager functions, the DP would be hosted on the Configuration Manager Server. In sites with fewer than 300 clients, this should not cause any issues, but in larger sites consideration should be given to adding further DPs.

In some circumstances, there may be a requirement to manage Configuration Manager clients in remote locations that have no dedicated hardware. This means that each Configuration Manager client will download a copy of the package from a DP across the WAN link, which could lead to inefficient use of network bandwidth. The impact of this can be limited by implementing Branch Distribution Points. Depending on the number of Configuration Manager clients at the site and the amount and size of any software being distributed, adding hardware to a remote location should be evaluated. Consider the following example.

Example Infrastructure

A healthcare organisation is made up of two geographical locations called Location 1 and Location 2. Both locations are managed by the same Configuration Manager site. The network link between the two sites is usually around 50 percent utilised. All Configuration Manager hardware is in Location 1 and there are approximately 1000 Configuration Manager clients in each location.

Scenario 1

The Configuration Manager Administrator deploys a 100 Mb package to all Configuration Manager clients in the Configuration Manager site and notices that the WAN link between the two sites reaches 100 percent and stays fully utilised for a number of hours.

As there is no Configuration Manager hardware in Location 2, every Configuration Manager client in Location 2 will connect to the DP in Location 1 and copy the 100 Mb package resulting in 100 Gb being copied over the WAN:

100MB × 1000 Configuration Manager clients = 100GB copied over WAN

Scenario 2

A Branch DP, Protected DP or Secondary Site is deployed in Location 2 and the package is copied once across the WAN to that DP. All Configuration Manager clients in Location 1 connect to the existing DP to install the application. All Configuration Manager clients in Location 2 connect to the DP in Location 2 resulting in only 100MB being copied across the WAN:

100MB × 1 copy to DP/Secondary Site = 100MB copied over WAN

4.4.10.3 Protected Distribution Points

A Protected Distribution Point (DP) is a distribution point that only specific Configuration Manager clients can use, based on their location. The Configuration Manager Administrator can configure a Protected DP so that only Configuration Manager clients in a specific subnet, subnet range or Active Directory Site can access it. This allows Configuration Manager administrators to control the network traffic usage of Configuration Manager clients when they contact DPs for software, specifically where Configuration Manager sites cover more than one geographical location.

Figure 15 represents a Configuration Manager site with two remote geographical sites, one with a Protected DP and one with no DP:

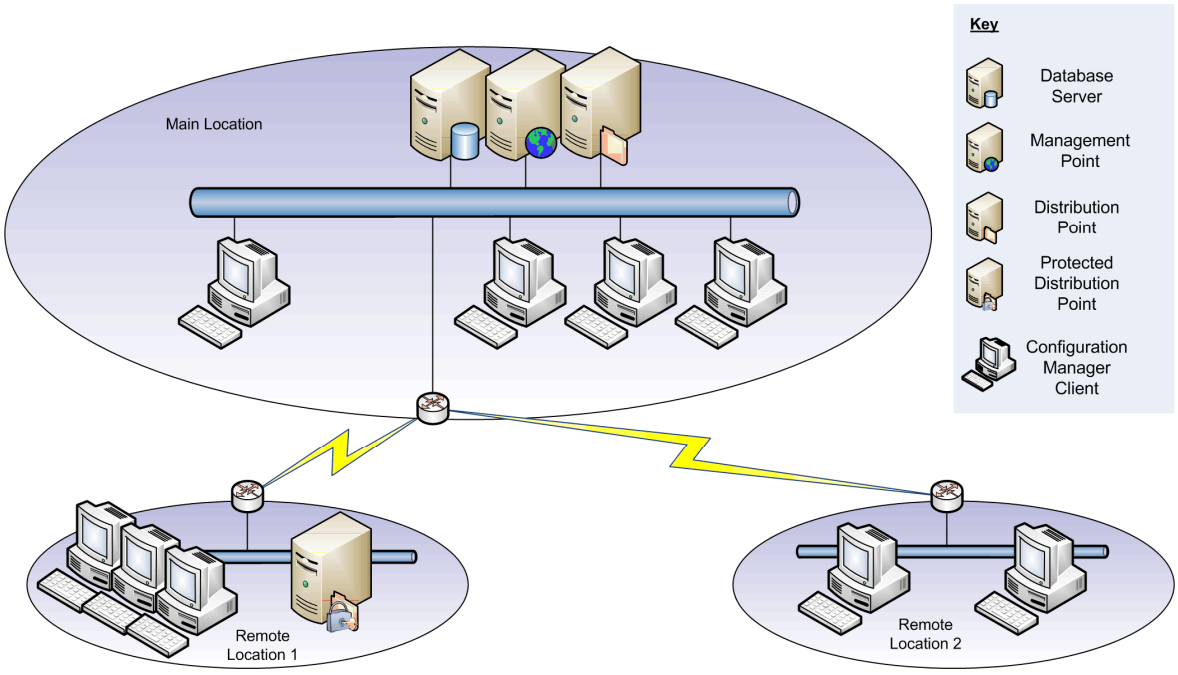


Figure 15: Remote Sites with Protected DP and No DP

In this example, when a Configuration Manager client in Remote Location 1 receives an advertisement, it will contact the MP in Main Location. The MP will check for the availability of the content and return the list of available DPs to the Configuration Manager client. The Configuration Manager client falls within the boundaries of the Protected Distribution Point, so this will take precedence. However, if the content has not been distributed to the DP in Remote Location 1, the Configuration Manager client will connect to the DP in Main Location, if the advertisement is configured to allow it.

If a Configuration Manager client from Remote Location 2 receives the advertisement, it will also contact the MP in Main Location. However, the MP will only return the details of the MP in Main Location. The Configuration Manager client will then connect to the DP in Main Location in order to install the package. Additionally, if a Configuration Manager client from Main Location received the advertisement, the MP will only return the details for the DP in Main Location, preventing the Configuration Manager client from unnecessarily connecting across a potentially slow connection.

> **Note**
>
> If the Configuration Manager client is disconnected from its DP, when it is reconnected, it will continue to download the package from where it left off (byte level). If the Configuration Manager client has moved to another location and connects to a different DP, it will continue the download from the last completed file that was downloaded (file level).

4.4.10.4 Branch Distribution Points

A Branch Distribution Point is a DP that can run on either a server-class computer or a client-class computer. This allows the Configuration Manager Administrator to further control the network bandwidth usage of Configuration Manager for software distribution. If a remote geographical location has a small number of clients, one or more Branch Distribution Points can be deployed, which prevent all clients in a site having to download the package content. Figure 16 shows the same example used in section 4.4.10.3 but with a Branch Distribution Point deployed to Remote Location 2. In this example, when a Configuration Manager client in Remote Location 2 contacts the MP to request content, the Branch DP details will be returned and the client will install the software from the branch DP without having to download the content itself:

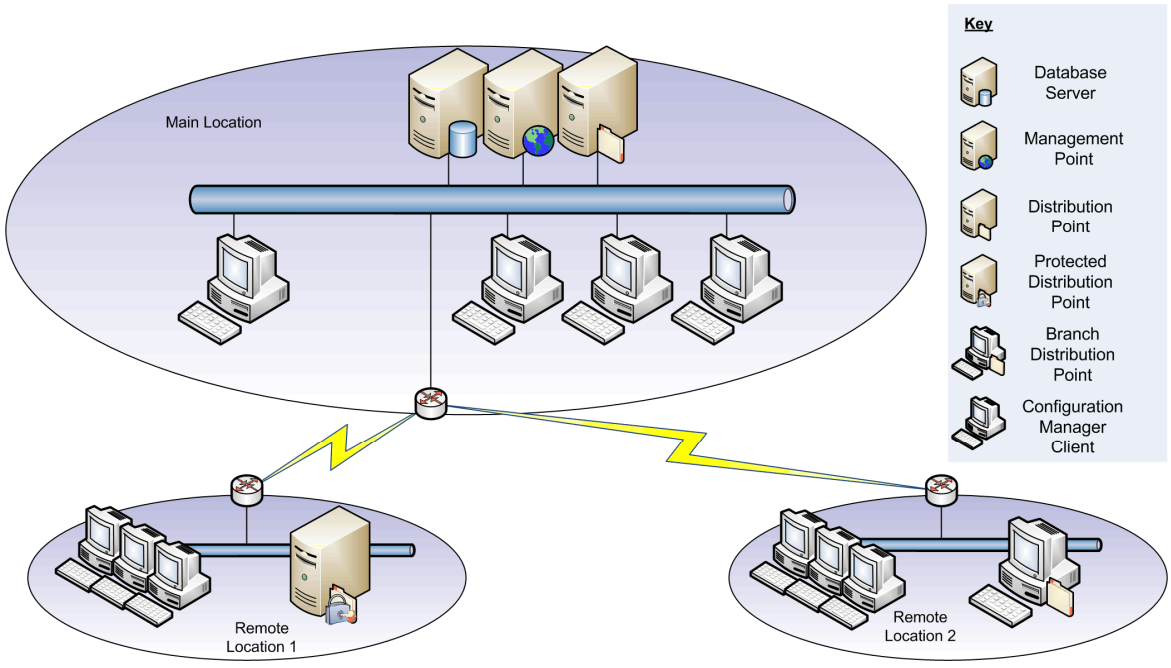


Figure 16: Remote Sites with Protected DP and Branch DP

If the Branch DP is installed on a client operating system, such as Windows Vista, it is limited to a maximum of 10 concurrent connections. When a client attempts to contact the Branch DP, if it already has 10 clients connected to it, the Configuration Manager client will retry after 30 seconds. If this connection also fails, the Configuration Manager client will move on to any other available DP's. Multiple Branch DPs can be deployed to a single location to improve performance.

> **Important**
>
> Because the client will attempt to contact a different DP if the initial connection fails, when deploying Branch DPs to locations that have more than 10 clients, the Branch DP should be configured as a protected Branch DP. This will prevent the Configuration Manager clients from attempting to contact DPs in other locations simply because the Branch DP already has 10 clients connected to it. If the client cannot connect to the Branch DP initially and no other DPs are available, it will continue to retry until the connection is successful.

4.4.10.5 Protected Standard or Branch Distribution Point Versus Secondary Site

When deciding where to place a Configuration Manager DP, consideration should be given to the advantages and disadvantages of a Protected DP over a Secondary Site (see Table 16). Either a Protected Standard or Branch DP, or a Secondary Site, would usually be implemented when the site has a number of Configuration Manager clients in a different geographical location from the main site, connected by a WAN.

Type	Advantages	Disadvantages
Protected Standard Distribution Point	▪ Less configuration required ▪ Lower administrative overhead ▪ Only one copy of the package source has to be copied across the WAN	▪ No control over network bandwidth
Protected Branch Distribution Point	▪ Less configuration required ▪ Lower administrative overhead ▪ Only one copy of the package source has to be copied across the WAN ▪ On-demand Package Distribution Supported (this feature allows the Branch DP to download files only when the program is requested by a client rather than as soon as it becomes available)	▪ Limited to 10 concurrent connections if deployed on a client operating system, which can impact performance during large-scale distribution
Secondary Site	▪ Ability to configure the Configuration Manager Senders to strictly control network bandwidth based on package priorities and working hours ▪ Only one copy of the package source has to be copied across the WAN	▪ Additional configuration required ▪ Additional administrative overhead

Table 16: Protected DP and Secondary Site Advantages and Disadvantages

If a site is connected via a slow link, a Secondary Site or Branch DP would usually be deployed, allowing the administrator to control the network bandwidth. If the link speed is less of a concern, a Protected DP may be deployed but Configuration Manager will start to copy the package source files to all DPs as soon as the package is added to that DP.

4.5 Planning Boundary Configuration

Boundaries in Configuration Manager are used to define if a client will be assigned to a particular site, and also how a client will communicate with DPs when running software updates, software distribution or operating system deployment.

A Configuration Manager boundary can be made up of any of the following:

- Internet Protocol (IP) subnets
- Active Directory site names
- IPv6 Prefix
- IP address range

The healthcare IT Administrator should decide which of the above boundary types will be suitable to ensure that all clients in the healthcare organisation will operate as desired. Any combination of the boundary types above can be used. To be assigned to a site, a client must be included in a boundary of that site.

> **Important**
>
> If the healthcare organisation is deploying multiple Configuration Manager sites, it is crucial to ensure that the boundaries of any sites do not overlap. For example, if both sites operate in the same Active Directory site, this cannot be used as a boundary; IP subnets should be used instead. Similarly, if specifying a subnet as a boundary, the healthcare IT Administrator should ensure that the subnet is not included as part of an Active Directory site that is configured as the boundary for a different Configuration Manager site.

4.5.1 Understanding Fast and Slow Boundaries

Once the healthcare IT Administrator has decided on the boundaries for the site, each one should be evaluated to determine if it will be configured as a fast or slow boundary. When configuring advertisements for software distribution programs, operating system deployment task sequences, or deployments for software updates, the healthcare IT Administrator will be given an option to decide how the client will perform when within a slow boundary as opposed to a fast boundary. Figure 17 shows the **Distribution Points** section of the **New Advertisement Wizard**:

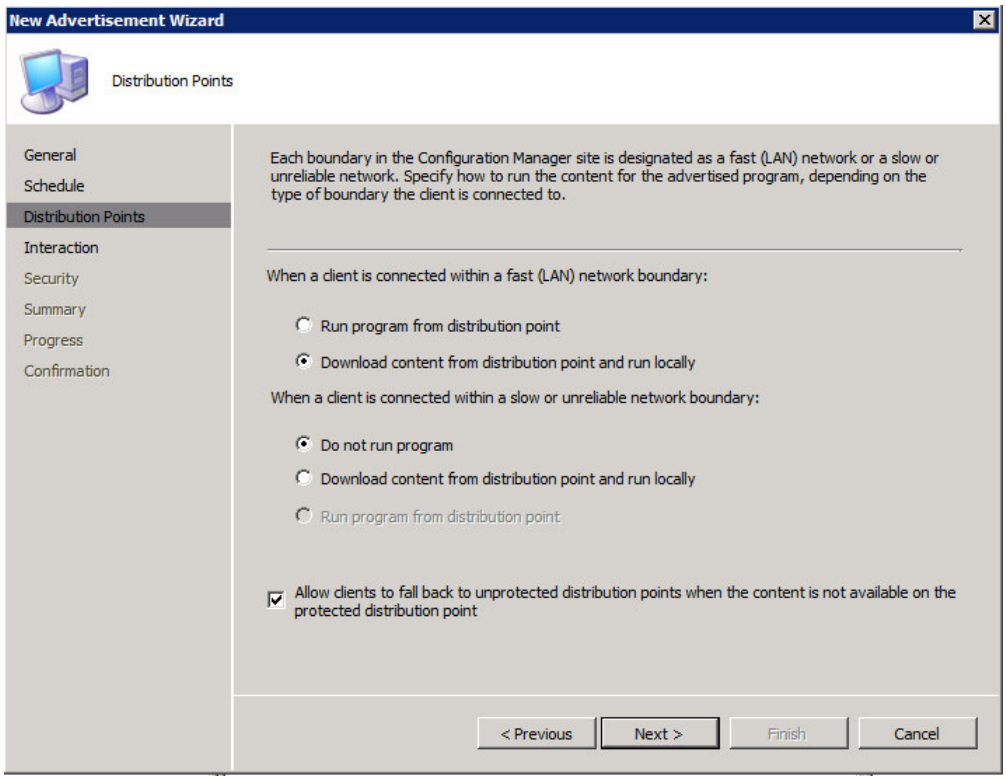


Figure 17: Advertisement Properties for Specifying Boundary-Based Actions

This allows the healthcare IT Administrator to configure an advertisement (software installation) to behave differently depending on from where the client is connecting to the DP. If the client is connected within a fast boundary, it will download the installation files from the DP and execute them. If the client is within a boundary defined as slow, it will not run the program.

For example, if the healthcare IT Administrator wants to deploy the 2007 Microsoft® Office system within the organisation and has configured the advertisement properties as shown in Figure 17, they could configure the boundaries as follows:

- All the subnets within a hospital are configured as a fast boundary because all clients that are connected to those subnets will have a 1 Gb connection to the DP
- An IP address range that is used for clients to connect to the organisation's network using a Virtual Private Network (VPN) has been configured as a slow boundary because clients may be connecting over slow links

These configurations will have the following effects:

- Clients that are physically attached to the network at the hospital will download and install the 2007 Office system from the DP
- Clients that are connected via VPN will not attempt to download the source files for the 2007 Office system until the next time they visit the hospital and connect to the network

4.5.2 Protecting Site Systems Using Boundaries

Another purpose for boundaries is to configure site systems to be protected. A protected site system will only accept connections from clients that are within the specified boundaries. Figure 18 shows an example infrastructure with a Primary site server in one location covering two IP subnets and two different locations, each containing a single subnet. The desired configuration in this example is to specify the following:

- Site Boundaries: All four subnets should be added as fast boundaries because the network connection between the client and its nearest DP is fast. If a Branch DP was not deployed in Location 2, this could be added as a slow boundary to allow the advertisements to be configured so that the clients in this location behave differently.
  - Configure the Distribution Point in Location 1 with a protected boundary of 192.168.3.0/24. This means that when a client in Location 1 requests content for a software distribution, it is directed only to the DP in Location 1. Also, with this configuration, if a client in the Primary Site location requests content for the same package, the DP in Location 1 is not returned as a possible location, preventing the client from connecting across the WAN to the DP in Location 1. If the content is not available on the DP at Location 1, the healthcare IT Administrator can configure the advertisement to either allow the client to contact the DP in the Primary site location across the WAN, or specifically deny it. This following setting will likely differ based on the size and importance of the package: **Allow clients to fall back to unprotected distribution points when the content is not available on the protected distribution point.**
  - Configure the Branch Distribution Point in Location 2 with a protected boundary of 192.168.4.0/24. When the client requests content, only the name of the Branch DP in Location 2 will be returned. Again, if the content is not available on the Branch DP at Location 2, the healthcare IT Administrator can configure the advertisement to either allow the client to contact the DP in the Primary site location across the WAN, or specifically deny it. When using Branch DPs, it is advisable to deny this option because even though the content could be available, all available connections may be taken if the Branch DP is deployed to a non-server operating system.

Figure 18 shows an example infrastructure protected by boundaries:

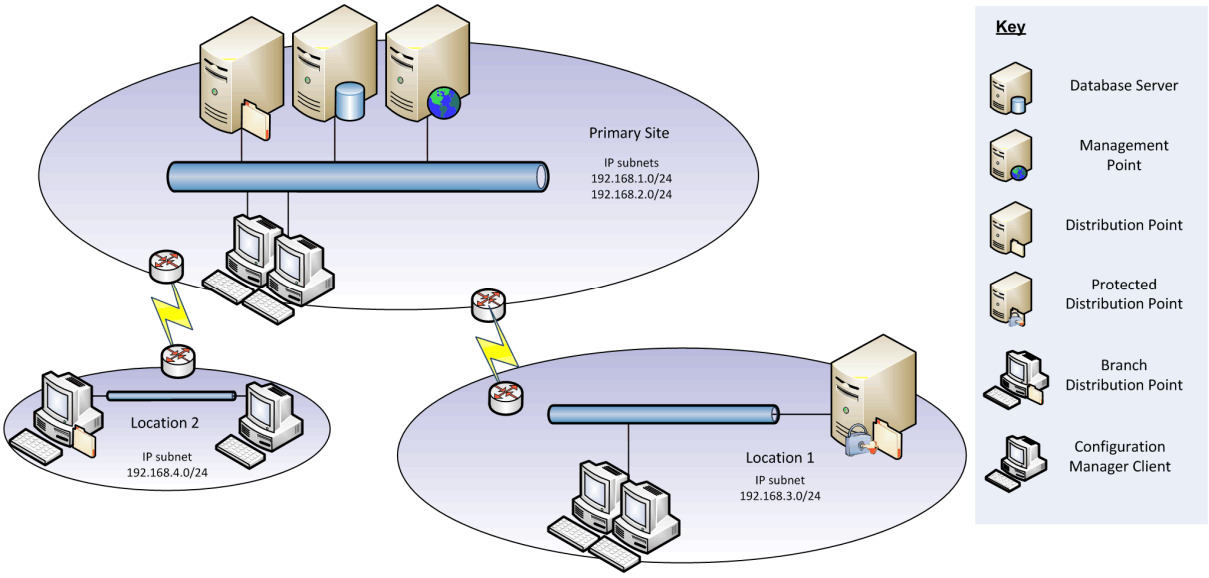


Figure 18: Protecting Site Systems Using Boundaries

The healthcare IT Administrator should decide if any site systems that are deployed should be configured as protected site systems. Protecting a site system only impacts the Distribution Point role and the State Migration Point role. It is not possible to protect any other site system in this way.

4.6 Deciding Which Discovery Options to Use

Configuration Manager 'discovery' is the process that finds computers, users, user groups, and containers, by polling the nearest Active Directory domain controller, or querying Dynamic Host Control Protocol (DHCP) Server or Simple Network Management Protocol (SNMP) Communities. Within Configuration Manager, there are several discovery methods available. The discovery methods that will be used within this guidance are:

- Active Directory User Discovery
- Active Directory System Discovery
- Active Directory System Group Discovery
- Active Directory Security Group Discovery
- Network Discovery

To use an Active Directory method of discovery, the Active Directory domain can be in either mixed mode or native mode. Plan to specify the containers to be polled, such as specific domains, sites, Organisational Units (OUs), or user groups. Also, plan to specify the polling schedule.

Configuration Manager polls Active Directory when it is using one of the Active Directory discovery methods. The Configuration Manager resources that are obtained from Active Directory do not necessarily reflect the current Active Directory resources at all times; objects might have been added, removed, or changed in Active Directory since the most recent poll.

Configuration Manager must have read access to the containers configured for the Active Directory discovery methods, by using the Configuration Manager Service account or the site server computer account, depending on the security mode that Configuration Manager is running in. When the Configuration Manager Service account, or site server computer account, is used by these discovery methods in domains other than the site server domain, the account must have domain user credentials on those domains. As a minimum, the account must be a member of the Domain Users group or the local Users group on the domains.

Table 17 lists and compares the Active Directory discovery methods used in this guidance:

Discovery Method	Usage	Advantages	Disadvantages
Active Directory User Discovery	Enable when the targeting of specific users is required. Can also be used to target users based on group membership.	If a user is targeted using a collection based on their group membership, the user can receive the new advertisement without logging off and on.	When a user's group membership changes, a number of steps have to be completed by Configuration Manager before the collection is updated to reflect this information. This can lead to a large latency.
Active Directory System Discovery	Used mainly for Configuration Manager client installation; once Configuration Manager clients have been installed, Heartbeat Discovery will maintain the system's discovery record.	This discovery method is mainly used for Configuration Manager client installation and is included here for completeness. Therefore, advantages are not relevant.	This discovery method is mainly used for Configuration Manager client installation and is included here for completeness. Therefore, disadvantages are not relevant.

Discovery Method	Usage	Advantages	Disadvantages
Active Directory System Group Discovery	Enable when the targeting of machines using OU membership or group membership is required.	Can assist with targeting systems that are based on geographic location according to Active Directory OU or site membership.	Similar to the Active Directory User Discovery method, this information requires Active Directory to be polled and a collection to be updated, so it can take time to deploy packages.
Active Directory Security Group Discovery	Enable if targeting of users based on group membership is required.	This requires little intervention from Configuration Manager administrators and reduces the latency involved in polling the Active Directory.	Package installation requires users to log off and back on, once group membership changes.
Network Discovery	Used to discover resources that are not part of Active Directory. This can include equipment such as routers.	Can use methods other than Active Directory for discovery, such as DHCP or SNMP Communities.	This discovery method is mainly used for Configuration Manager client installation and is included here for completeness. Therefore, disadvantages are not relevant.

Table 17: Active Directory Discovery Methods and Comparisons

4.7 Deciding Which Client Installation Methods Will Be Used

During the Plan phase of the Configuration Manager infrastructure, the healthcare IT Administrator should decide which client installation methods will best suit the needs of the healthcare organisation. Sections 4.7.1 to 4.7.6 briefly describe each of the available methods. It is common practice to use more than one method to achieve the desired results. For example, the healthcare IT Administrator may use Remote Client installation in the following instances:

- When installing the initial clients for testing a pilot
- To enable software update point installation when the infrastructure moves into full production
- To install the client into a master image to be used for operating system deployment

More detailed information to help the healthcare IT Administrator decide which method will best suit the healthcare organisation's needs is available in the TechNet article *Planning and Deploying Clients for Configuration Manager 2007*[17].

4.7.1 Software Update Point Client Installation

The Configuration Manager client can be installed when a computer that is configured to obtain software updates from a WSUS 3.0 SP1 server scans for new updates. This method has the following prerequisites:

- WSUS 3.0 SP1 or SP2 configured as a Configuration Manager site system role
- Clients configured to use the WSUS 3.0 SP1 or SP2 server

If the healthcare organisation has not extended the Active Directory Schema, there may be a requirement to provision Configuration Manager installation properties prior to deploying the client using this method. For more information, see the TechNet article *How to Provision Configuration Manager Client Installation Properties using Group Policy*[18].

[17] Microsoft TechNet: Planning and Deploying Clients for Configuration Manager 2007 **{R14}**: http://technet.microsoft.com/en-gb/library/bb680373.aspx

[18] Microsoft TechNet: How to Provision Configuration Manager Client Installation Properties using Group Policy **{R15}**: http://technet.microsoft.com/en-us/library/bb632469.aspx

4.7.2 Group Policy Client Installation

The Configuration Manager client can be deployed via Group Policy using the Ccmsetup.msi installer. As with Software Update Point Client installation, the healthcare IT Administrator may need to provision installation properties to the client prior to installation.

4.7.3 Client Push Installation

Configuration Manager allows the administrator to install the Configuration Manager client on a computer remotely via a client push from the Configuration Manager site server. The client push can be configured to be triggered automatically after a computer is discovered or it can be initiated manually by an administrator using the Configuration Manager Console. Client push has the following requirements:

- The Configuration Manager site server's computer account, or a designated client push account, is in the target computer's Administrators local group
- The Server service is running on the target computer
- No firewall on the target computer blocks incoming Server Message Blocks (SMB) connections to local file shares
- The administrative (hidden) share on the target computer is available

More information on configuring the Windows Firewall to work with Configuration Manager is available in the TechNet article *Firewall Settings for Configuration Manager Clients*[19].

4.7.4 Imaged Client Installation

The Configuration Manager client supports installation as part of the Windows operating system image. Information on how to install the Configuration Manager client into a computer image is contained in the TechNet article *How to Install Configuration Manager Clients Using Computer Imaging*[20].

4.7.5 Manual Client Installation

It is not possible to run the Client.msi file in order to install the Configuration Manager client, as it was in Microsoft® Systems Management Server (SMS) 2003. CCMSetup.exe must be used to install the client and is located in the '<Site Server Name>\SMS_<Site Code>\Client' share. Information on how to install the Configuration Manager client manually is contained in the TechNet article *How to Install Configuration Manager Clients Manually*[21], and is also described in section 5.3.3 when relating to manual installation of clients for General Practice clinics.

4.7.6 Logon Script Client Installation

Configuration Manager supports the use of logon scripts for installation of the Configuration Manager client. This method uses Ccmsetup.exe to install the client and supports all command-line options for Ccmsetup.exe. The **/logon** switch can be specified to avoid installation of the Configuration Manager client if one is already installed. This installation method requires that the user has local administrative permissions on the computer.

---

[19] Microsoft TechNet: Firewall Settings for Configuration Manager Clients **{R16}**: http://technet.microsoft.com/en-us/library/bb694088.aspx

[20] Microsoft TechNet: How to Install Configuration Manager Clients Using Computer Imaging **{R17}**: http://technet.microsoft.com/en-us/library/bb694095.aspx

[21] Microsoft TechNet: How to Install Configuration Manager Clients Manually **{R18}**: http://technet.microsoft.com/en-us/library/bb693546.aspx

4.8 Security Considerations

The Security of a Configuration Manager hierarchy is extremely important because the Configuration Manager Administrator can make any number of changes to client machines. These client machines can include desktop-class or laptop-class computers, as well as server-class computers and even handheld devices, such as phones and PDAs. The healthcare IT Administrator should fully understand the security considerations that relate to Configuration Manager prior to starting the Plan phase of the project. The information described in this guidance is for the purposes of deployment. To gain a full understanding of Configuration Manager security, the healthcare IT Administrator should review the information contained in the TechNet article *Security and Privacy for Configuration Manager 2007*[22].

4.8.1 Security Accounts and Groups

Table 18 lists the accounts and groups that the healthcare IT Administrator needs to be familiar with prior to installing and configuring Configuration Manager:

Account/Group Name	Type	Description	Requirements
Logged on account during installation	Domain Account	User must be logged on to the domain, and not locally on the server, when installing Configuration Manager.	Account must have administrative permissions on the site server, SQL Server and SMS Provider computer (selected during setup) and be a member of sysadmins on the SQL Server (remote or local).
Client Push Installation Account	Domain Account	Must be created manually and added using the Configuration Manager Admin Console.	Requires administrative access to any clients that will be installed using Remote Client Installation.
Network Access Account	Domain Account	Must be created manually and added using the Configuration Manager Admin Console.	Requires read access to any Software Distribution or Operating System Deployment (OSD) Packages. This account will be used if the client's machine account (advertised to computer) or the user's account (advertised to user or user group) fails. This account must be specified if using OSD or if clients reside in workgroups or untrusted forests.
SMS Admins	Local Group	This group is created by setup and resides on the site server (and the server running the SMS provider, if separate).	Any users of the Configuration Manager Admin Console must be added to this group. It is recommended that a domain group is created and added to the SMS Admins group, and then that users are added to the domain group, because this reduces administrative effort and maintains the group centrally.
SMS Reporting Users	Local Group	This group is created by setup and resides on the reporting point server.	Users that require access to Configuration Manager reporting should be added to this group.

[22] Microsoft TechNet: Security and Privacy for Configuration Manager 2007 **{R19}**: http://technet.microsoft.com/en-gb/library/bb680768.aspx

Account/Group Name	Type	Description	Requirements
Site System to Site Server Connection	Local Group	This group is created by setup and resides on the site server. The group is called SMS_SiteSystemToSiteServerConnection _ <sitecode> where sitecode is the three-character site code reference of the site hosted by the site server.	The machine accounts of any servers that will act as a remote site system should be added to this group on the site server prior to installing the server as a site system. The site server's machine account should also be added to the local administrators group on the remote site system prior to installation.
Site-to-Site Connection Group	Local Group	This group is created by setup and resides on every site server.	When a site is configured to report to another site to form a hierarchy, the machine account of each site server should be added to this group on the other site server. This allows the servers to communicate.

Table 18: Security Groups and Accounts Required for Configuration

These accounts represent the minimum accounts and groups the healthcare IT Administrator will need to understand in order to deploy Configuration Manager. For a full list and description of all accounts and groups used by Configuration Manager, see the TechNet article *Accounts and Groups in Configuration Manager*[23].

4.8.2 Native Mode

Configuration Manager can be configured either in mixed mode security (synonymous to advanced security in SMS 2003), or in native mode security. Native mode security is the recommended site configuration for a new Configuration Manager site as it provides a greater level of data security. Native mode uses industry standard Private Key Infrastructure (PKI) and Secure Sockets Layer (SSL) encryption to secure data that is transferred between clients and servers. This guidance will not cover the additional steps required for implementing native mode security because many healthcare organisations will not require the level of security provided by this solution, and it can significantly increase the administrative overhead of the solution. For those healthcare organisations that have already deployed a PKI, native mode should be considered. For those that have not, consideration should be given to deploying a PKI to support the Configuration Manager native mode deployment. It is current best practice to deploy the sites using mixed mode security and then migrate the sites to native mode, once the deployment has been completed successfully. Implementing native mode security during installation can make troubleshooting issues very complex. More information on Configuration Manager Site modes can be found in the TechNet article *Configuration Manager Site Modes*[24].

[23] Microsoft TechNet: Accounts and Groups in Configuration Manager **{R20}**: http://technet.microsoft.com/en-gb/library/bb693732.aspx

[24] Microsoft TechNet: Configuration Manager Site Modes **{R21}**: http://technet.microsoft.com/en-gb/library/bb680658.aspx

4.8.3 Internet-Based Client Management

Internet-Based Client Management (IBCM) allows the healthcare IT Administrator to provide support for Configuration Manager clients to communicate with the Configuration Manager site, directly over the Internet, without establishing a VPN. This works in a similar way to Microsoft® Office Outlook® communicating with a Microsoft® Exchange Server using RPC over HTTPS. IBCM supports the following Configuration Manager features:

- Hardware and software Inventory
- Software Updates
- Software Distribution
- Software Metering

In order for a site to support IBCM, it must be a primary site and operating in native mode. Full details on the IBCM solution have not been provided in this guidance because it is not felt that the solution will be widely adopted in the healthcare industry. The reason for this is that the majority of healthcare organisations do not have a means of directly publishing infrastructure servers to the Internet. The IBCM solution works by adding additional site server roles that specifically deal with Internet-based clients into a perimeter network and publishing them to the Internet. These servers are then published in a public DNS server. For more information on deploying Configuration Manager to support Internet-Based Clients, see the TechNet article *Deploying Configuration Manager Sites to Support Internet-Based Clients*[25].

4.8.4 Special Considerations for General Practice Clinics

General Practice clinics often represent the most difficult deployment scenario for healthcare organisations because there is limited network connectivity or speed, and the client machines are often part of a separate Active Directory forest, or even part of a workgroup. The healthcare organisation should consider the advantages of bringing the General Practice clinics into the same trusted forest as the Administrative Centre that manages the General Practice clinics, but this is not always practical or possible. There are two methods for managing General Practice clinics using Configuration Manager:

- Using IBCM, as described in section 4.8.3 However, this may be problematic if the healthcare organisation does not have a direct Internet connection hosted from their own data center
- Manually configuring the clients so that they can resolve the name of the MP, SLP, FSP and SUP (if using software update management) using a LMHOSTS file. This will require that the MP, SLP and SUP are accessible to the clients

4.9 Documenting the Intended Design

Once the Plan stage has been completed, it is essential that the intended design is documented in a comprehensive detailed design document. This document should detail the proposed infrastructure, proposed hardware and proposed configuration settings. Once this document has been completed, it must be distributed amongst all business and operational stakeholders for agreement, before any implementation can commence.

A detailed design document should be treated as a living document in that any proposed design or configuration changes can be recorded, either during implementation, or even after the infrastructure has been signed off and implemented. Any design changes must be agreed by all business and operational stakeholders before they are implemented.

[25] Microsoft TechNet: Deploying Configuration Manager Sites to Support Internet-Based Clients **{R22}**: http://technet.microsoft.com/en-us/library/bb680388.aspx

5 DEVELOP

During the Develop phase the solution components are built based on the planning completed during the earlier phases. Further refinement of these components will continue into the stabilisation phase.

Figure 19 acts as a high-level checklist, illustrating the tasks that an IT Professional needs to perform when developing Configuration Manager for a healthcare organisation:

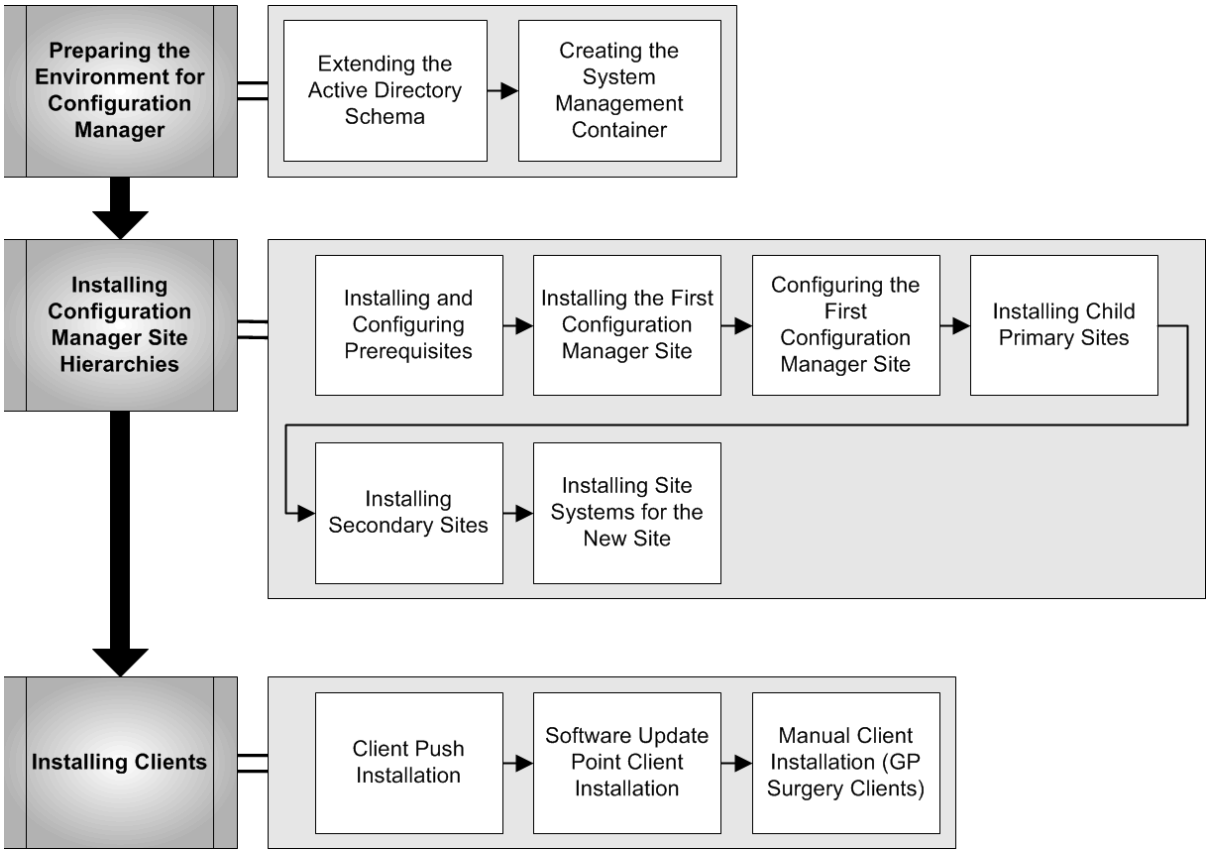


Figure 19: Sequence for Developing Configuration Manager

5.1 Preparing the Environment for Configuration Manager

Sections 5.1 to 5.3 describe the process for installing and configuring a Configuration Manager hierarchy. These procedures should be followed by the healthcare IT Administrator to assist them in building Configuration Manager in a test environment. It is only by building the proposed infrastructure in a test environment that the healthcare IT Administrator can be confident that the proposed design will function as expected and that there are no unique infrastructure or other issues specific to the health organisation's environment that need to be investigated or worked around. During the process of building the test environment, the healthcare IT Administrator should create a record of any issues that are experienced and the resolutions to these issues. This record should be used to create a production implementation plan that can be followed by any healthcare IT Administrator when the service is implemented into a production environment.

5.1.1 Extending the Active Directory Schema

Extending the Active Directory schema allows Configuration Manager functions, such as client assignment and location awareness, to operate correctly. It is possible to install Configuration Manager without extending the schema, but it is not recommended because some features will not work as expected. To extend the Active Directory schema for Configuration Manager, log in to the domain with an account that is a member of the 'Schema Admins' group.

To apply the extensions to Active Directory, the Extadsch.exe utility must be executed. This utility can be found on the Configuration Manager 2007 SP1 CD located under the SMSSETUP\BIN\i386 folder.

The utility should be run from within a command prompt window so that any output can be viewed. There are no command-line parameters to apply to the program; it just needs to be executed. If there were any problems when extending the schema, the errors will be reported on screen. The tool must be executed using an account that is a member of the 'Schema Admins' group.

> **Warning**
>
> Extending the Active Directory schema in a Windows 2000 Active Directory environment will result in a full schema replication. Ensure that the health organisation's Active Directory administrators are consulted when making this change.

5.1.2 Creating the System Management Container

The System Management container allows Configuration Manager to replicate information within Active Directory and should be created before the first Configuration Manager site is installed. To create the system management container, it is necessary to use a the ADSIEdit utility, which is available in the Windows support tools, if using Windows Server 2003, or installed by default on Windows Server 2008 Domain Controller. The support tools are available on the Windows Server 2003 CDs, but are not installed by default. ADSIEdit is an MMC snap-in.

5.1.2.1 Creating the Container

To create the container:

Step	Description
1.	Start ADSIEdit.msc using the **Run** dialog box and connect to the domain partition (select 'Domain' or 'Default naming context' as the well known naming context). **Note** This step must be performed using an account that has the **Create all Child Objects** permission on the **System** container (for example, a member of the 'Domain Admins' group).
2.	In the console pane, expand **Domain or Default naming context [<*computer fully qualified domain name* >]**.
3.	Expand the domain container.
4.	Right-click **CN=System** and select **New > Object** from the menu.
5.	In the **Create Object** dialog box, select **Container** and click **Next**.
6.	In the **Value** field, type 'System Management' and click **Next**. **Caution** Note that the container is named **System Management** and not **Systems Management**.
7.	Click **Finish**.

Table 19: Creating the System Management Container

5.1.2.2 Securing the Container

When publishing data to Active Directory, Configuration Manager uses its machine account as the security context. If it is likely that, over time, a hierarchy of Configuration Manager servers will be installed to support the environment, each Configuration Manager site server will need security permissions to publish to the 'System Management' container. To make this task easier, create a domain local group that contains the machine accounts of all Configuration Manager site servers. This group can then be granted permissions to the container within Active Directory.

To apply the permissions using ADSIEdit:

Step	Description
1.	Start ADSIEdit.msc using the **Run** dialog box and connect to the domain partition (select 'Domain' or 'Default naming context' as the well known naming context). **Note** This step must be performed using an account that has the "Modify" permissions on the **System Management** container (for example, a member of the "Domain Admins" group or the account used to create the **System Management** container).
2.	In the console pane, expand **Domain or Default naming context <*computer fully qualified domain name*>**.
3.	Expand the domain container.
4.	Expand the **CN=System** container.
5.	Right-click **CN=System Management** and select **Properties** from the menu.
6.	In the **CN=System Management Properties** dialog box, select the **Security** tab and add the **<*domain local group name*>** domain local group and grant the group **Full Control** permissions.
7.	Click **Advanced**.
8.	Select **<*domain local group name*>**.
9.	Click **Edit** and select **This object and all descendant objects** from the **Apply to:** drop-down list. **Note** If using Windows Server 2008, the **Apply to** option **This object and all child objects** must be selected.
10.	Keep clicking **OK** until returned to the MMC.

Table 20: Securing the System Management Container Using ADSIEdit

To apply permissions using 'Active Directory Users and Computers':

Step	Description
1.	Open the Active Directory Users and Computers console, click **View**, and then click **Advanced Features**. **Note** This step must be performed using an account that has the 'Modify' permissions on the **System Management** container (for example, a member of the 'Domain Admins' group or the account used to create the **System Management** container).
2.	Expand the **<*domain*>** node.
3.	Expand the **System** node.
4.	Right-click the **System Management** container and select **Delegate Control**. The Delegation of Control Wizard displays.
5.	On the **Welcome** page, click **Next**.
6.	Click **Add**.
7.	In the **Select Users, Computers, or Groups** dialog box, type the <***domain local group***>.
8.	Click **OK** to return to the wizard.
9.	Click **Next**.
10.	Select **Create a custom task to delegate** and click **Next**. The **Active Directory Object Type** page displays.
11.	On the **Active Directory Object Type** page, select **This folder, existing objects in this folder**, and **creation of new objects in this folder**, then click **Next.** The **Permissions** page displays.
12.	Select the check box for **Full Control**, and click **Next**. The **Completing the Delegation of Control** page displays.
13.	Verify the information and click **Finish** to exit the wizard and complete the process.

Table 21: Securing the System Management Container Using 'Active Directory Users and Computers'

Once the group has been created using the above steps, the Configuration Manager server's machine account needs to be added to the group. When doing this, ensure that the 'Computers' object type is enabled in the **Select Users, Contacts, Computers or Groups** dialog box, as shown in Figure 20 below:

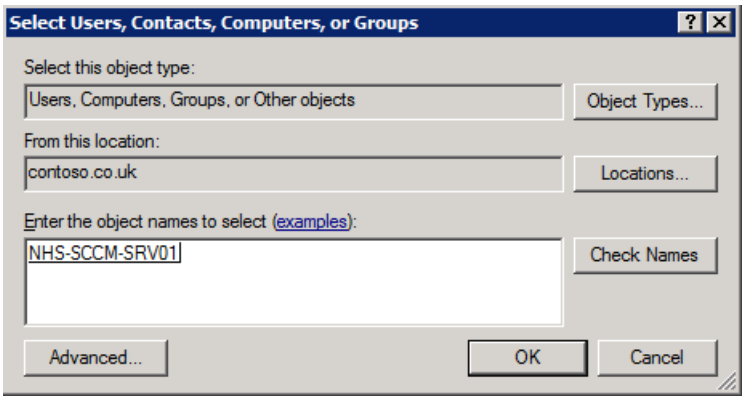


Figure 20: Select Users, Contacts, Computers or Groups Dialog Box

> **Note**
>
> If the server's machine account has been added to a group, and the group granted permissions to the System Management container (as opposed to granting permissions to the server's machine account directly), as shown above, the server will need to be rebooted in order for the group membership to apply.

5.2 Installing Configuration Manager Site Hierarchies

The healthcare IT Administrator can now deploy the infrastructure according to the design that was created during the planning phase.

> **Note**
>
> During installation and operation of Configuration Manager it is often useful to review log files to verify successful installation or troubleshoot problematic installation. The *System Center Configuration Manager 2007 Toolkit*[26] should be installed on all machines that will host Configuration Manager site systems as well as the healthcare IT Administrators client computers. Among other useful tools , the toolkit contains a log file reading tool (Trace32) that can assist when reviewing log files.

5.2.1 Installing and Configuring Prerequisites

Table 22 shows the prerequisite software that is required before installing any of the following Configuration Manager server roles. The healthcare IT Administrator should follow the procedures described on each of the servers before attempting to install Configuration Manager.

Role	Prerequisite Requirements	Section
Site Database Server	▪ SQL Server 2005/2008	Section 5.2.1.5
Site Server	▪ WSUS 3.0 SDK ▪ Remote Differential Compression	Section 5.2.1.4 Section 5.2.1.2
Management Point	▪ IIS 7.0 (including BITS) ▪ WebDAV	Section 5.2.1.1 Section 5.2.1.3
Distribution Point	▪ IIS 7.0 (including BITS) ▪ WebDAV	Section 5.2.1.1 Section 5.2.1.3
Fallback Status Point	▪ IIS 7.0 (including BITS)	Section 5.2.1.1
Reporting Point	▪ IIS 7.0	Section 5.2.1.1
Software Update Point	Not covered in this guidance	See *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**.
PXE Service Point/State Migration Point	Not covered in this guidance	See *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.

Table 22: Prerequisite Requirements for Component Servers

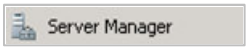
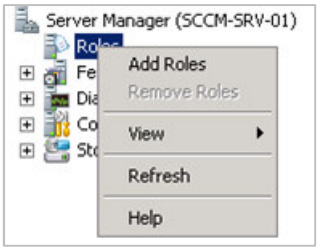
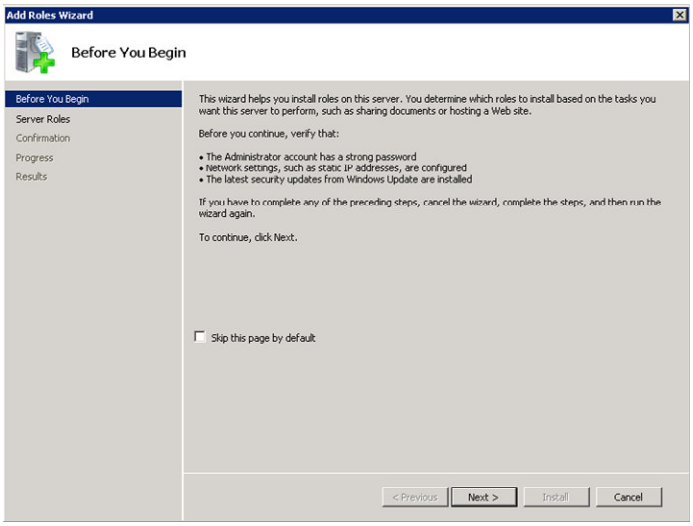
[26] Microsoft Downloads: System Center Configuration Manager 2007 Toolkit: http://www.microsoft.com/downloads/details.aspx?FamilyID=948e477e-fd3b-4a09-9015-141683c7ad5f&DisplayLang=en

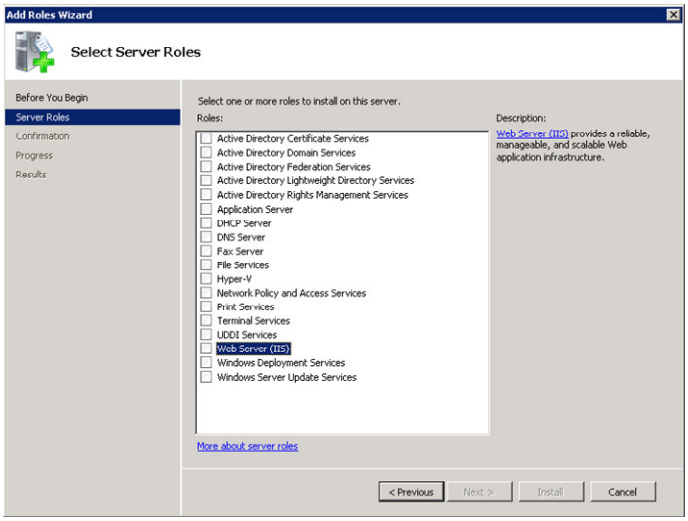
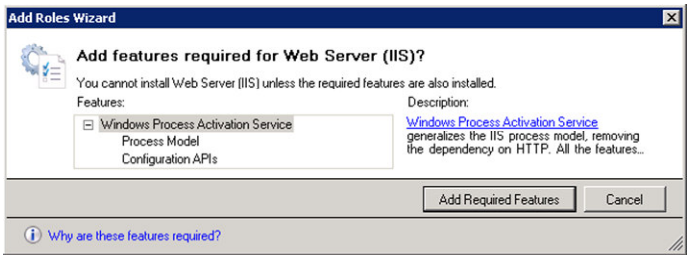
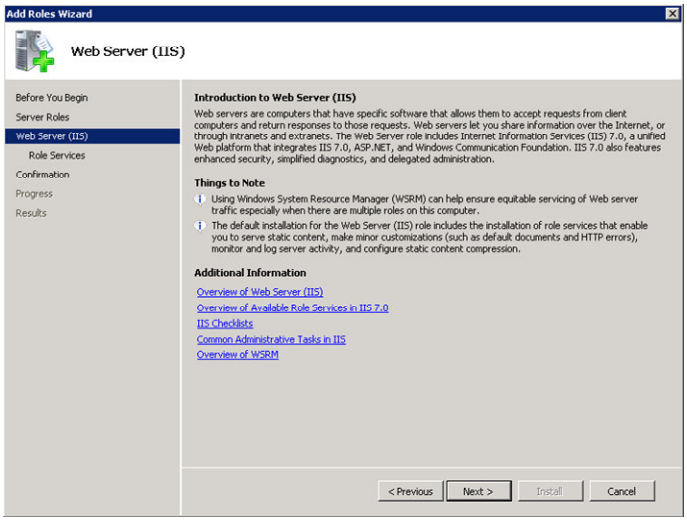
5.2.1.1 Installing Internet Information Server 7.0

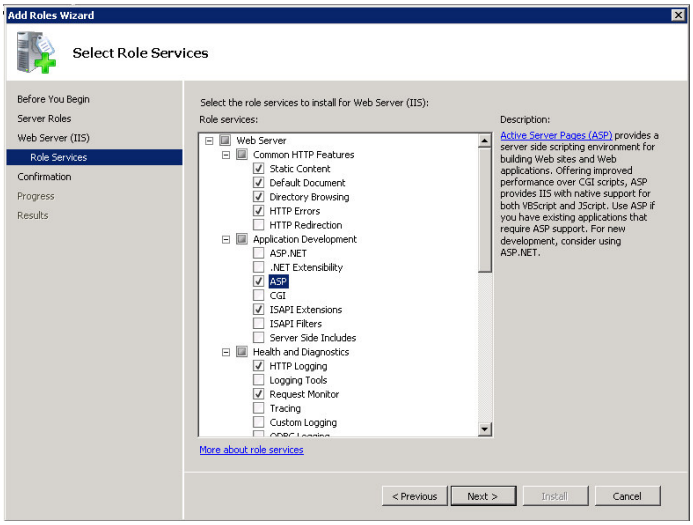
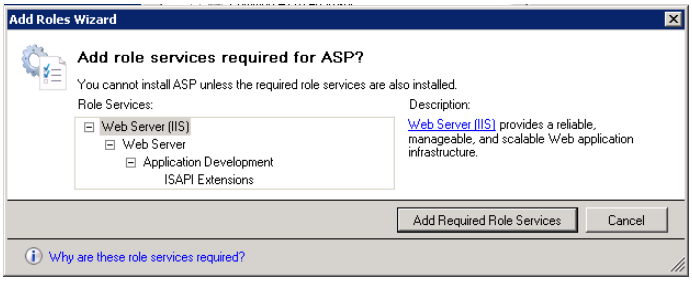
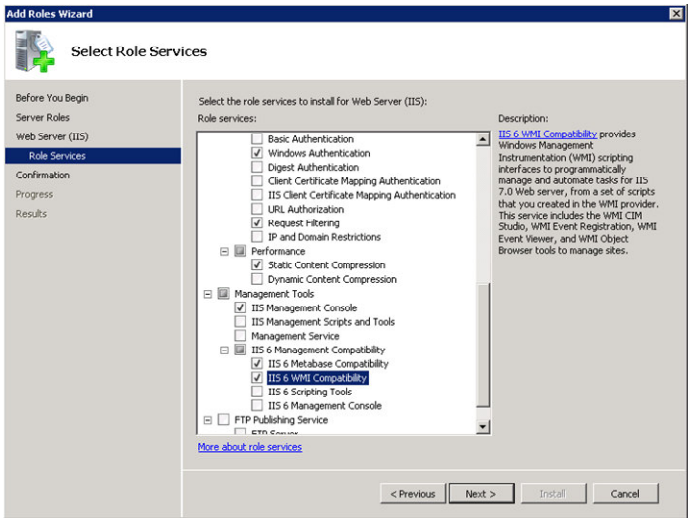
Internet Information Services (IIS) version 7.0 is only required for the following site system roles:

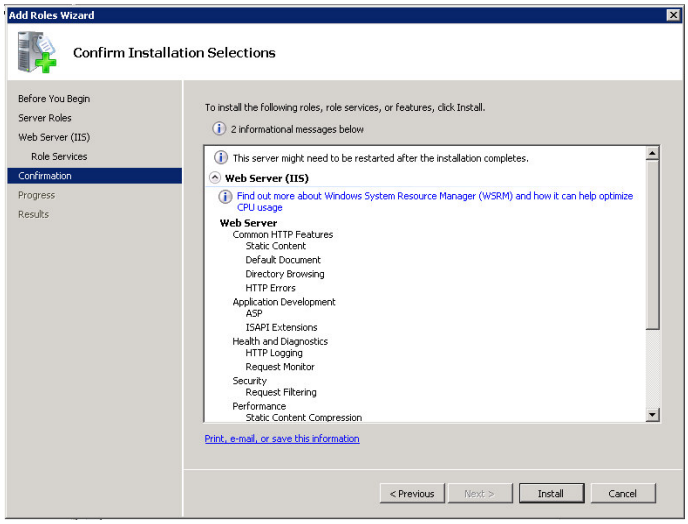
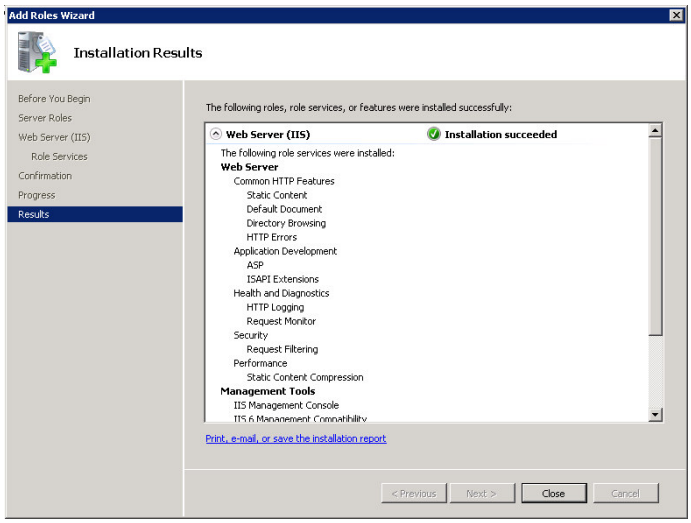
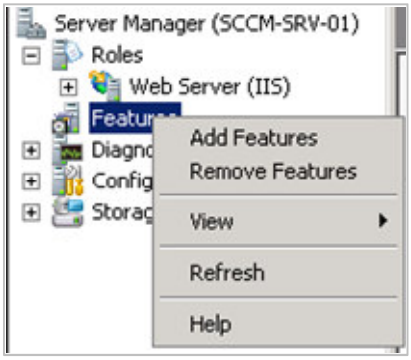
- Management Point (including proxy management points installed on secondary site servers)
- Fallback Status Points
- Server Locator Points
- Reporting Points/ SRS Reporting Points
- BITS-enabled Distribution Points
- State Migration Points
- Software Update Points

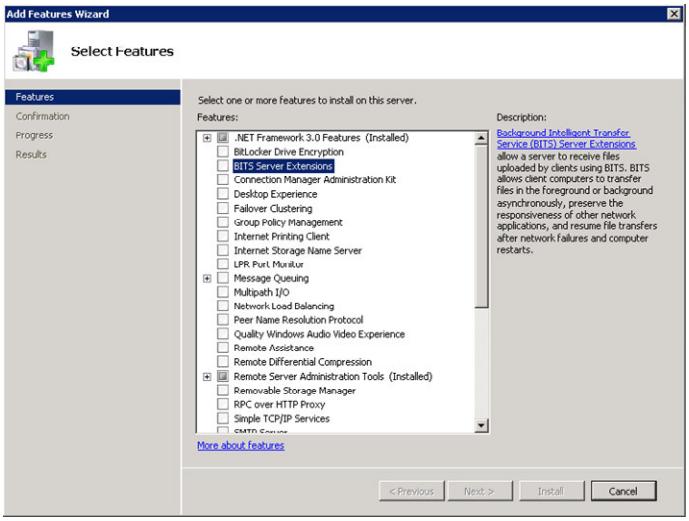
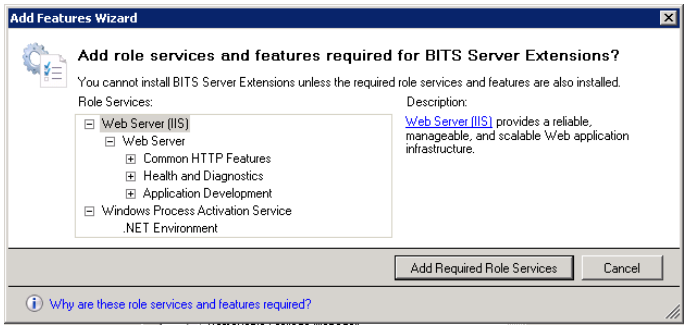
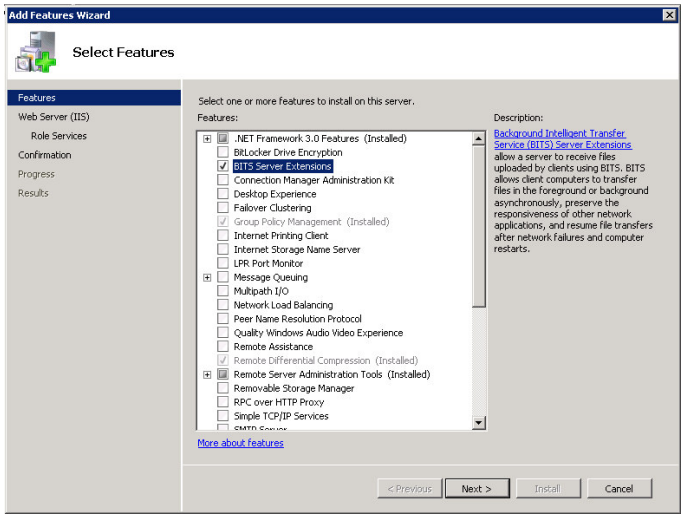
The healthcare IT Administrator must only install IIS 7.0 onto servers hosting these site system roles. Table 23 shows the process for installing IIS 7.0:

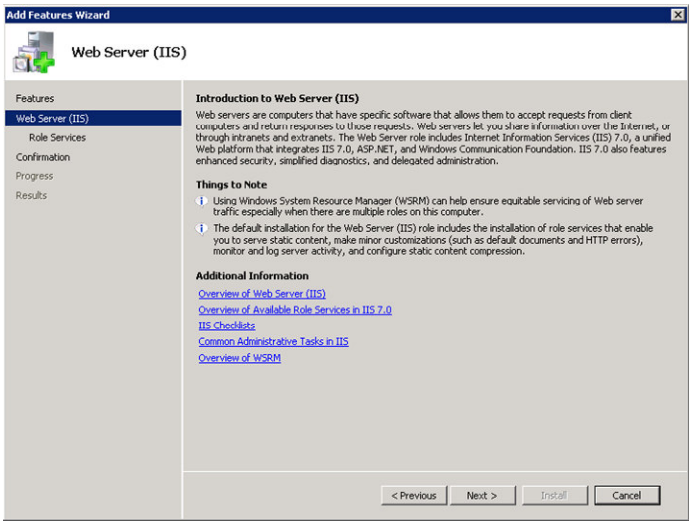
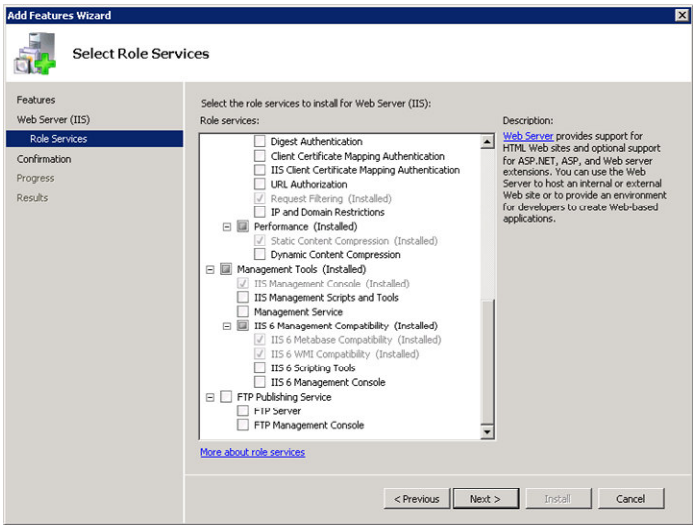
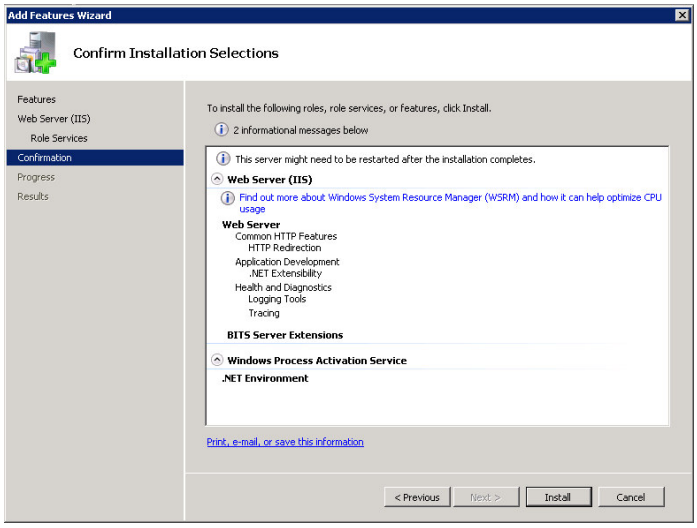
Step	Description	Screenshot
1.	Open **Administrative Tools > Server Manager**.	
2.	Right-click **Roles** and select **Add Roles**.	
3.	Click **Next**.	

Step	Description	Screenshot
4.	On the **Select Server Roles** page, select **Web Server (IIS)**.	
5.	Click **Add Required Features**, and then click **Next**.	
6.	Click **Next**.	

Step	Description	Screenshot
7.	Select **ASP** if the Reporting Point role will be installed on the server.	
8.	Click **Add Required Role Services**.	
9.	Ensure **Windows Authentication, IIS 6 Metabase Compatibility** and **IIS 6 WMI Compatibility** are selected, and click **Next**.	

Step	Description	Screenshot
10.	Click **Install**.	
11.	Click **Close**.	
12.	**Note** If the site system will only be used as a reporting point, the remaining steps in this table are not necessary. Right-click **Features** and select **Add Features**.	

Step	Description	Screenshot
13.	Select **BITS Server Extensions**.	
14.	Click **Add Required Role Services**.	
15.	Click **Next**.	

Step	Description	Screenshot
16.	On the **Web Server (IIS)** page, click **Next**.	
17.	Click **Next**.	
18.	On the **Confirm Installation Selections** page, click **Install**.	

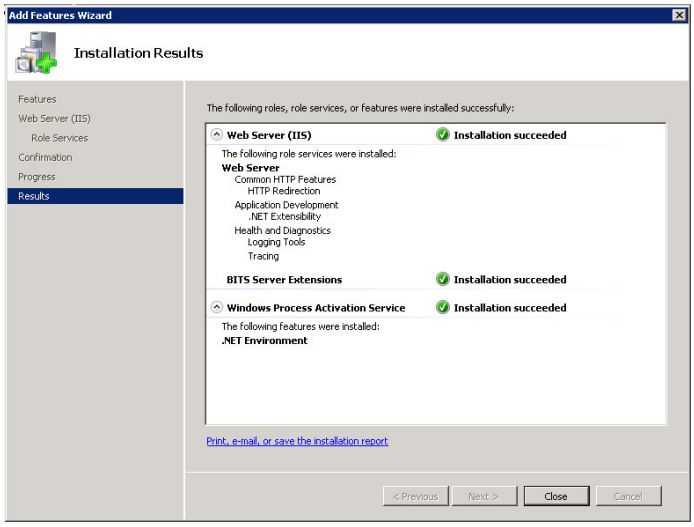
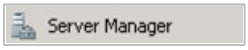
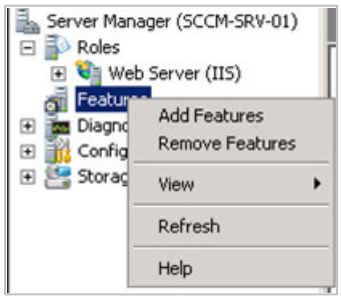
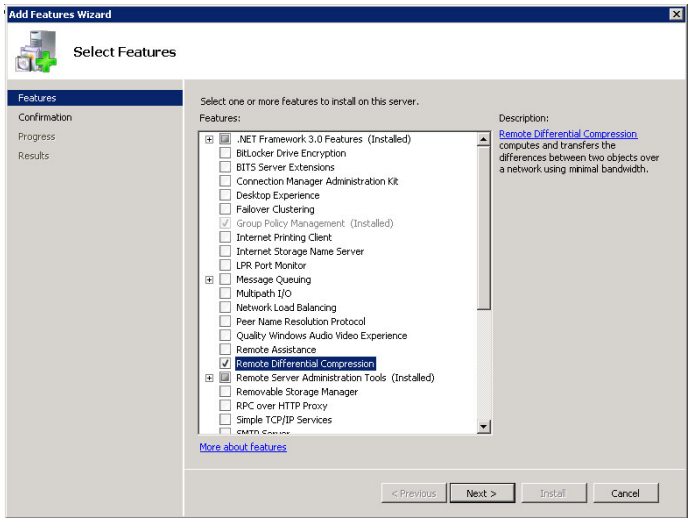
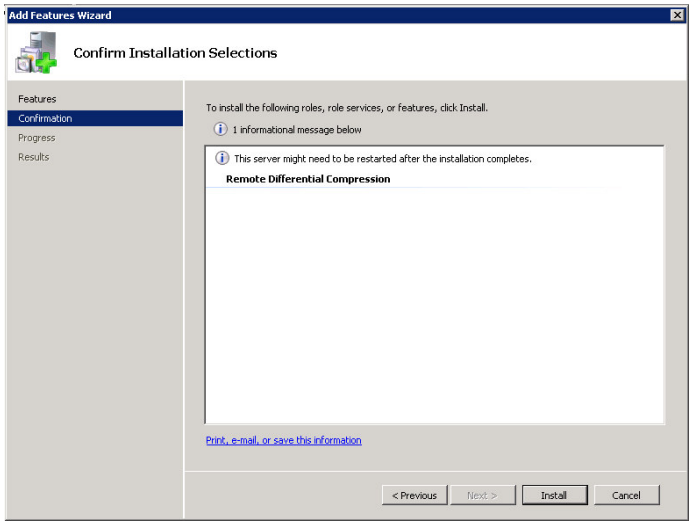
Step	Description	Screenshot
19.	Click **Close**.	

Table 23: Installing IIS 7.0

5.2.1.2 *Enabling Remote Differential Compression*

Table 24 shows the process for installing Remote Differential Compression:

Step	Description	Screenshot
1.	Open **Administrative Tools > Server Manager**.	
2.	Right-click **Features** and select **Add Features**.	
3.	Select **Remote Differential Compression** and click **Next**.	
4.	Click **Install**.	

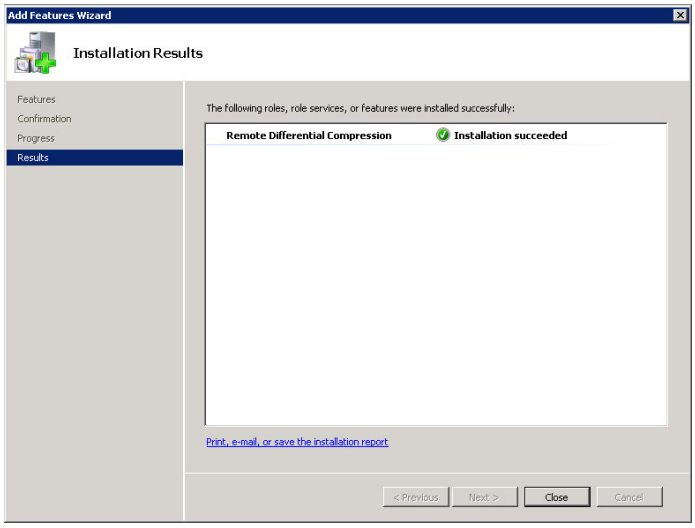
Step	Description	Screenshot
5.	Click **Close**.	

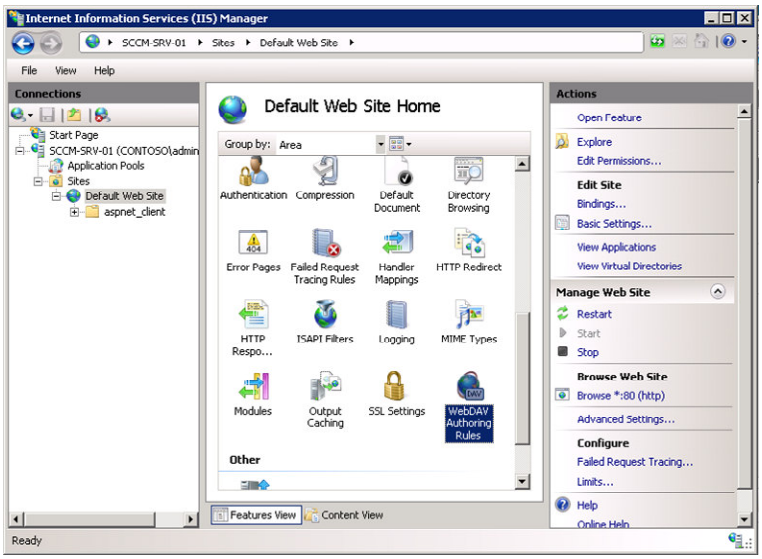
Table 24: Installing Remote Differential Compression

5.2.1.3 Installing WebDAV for IIS 7.0

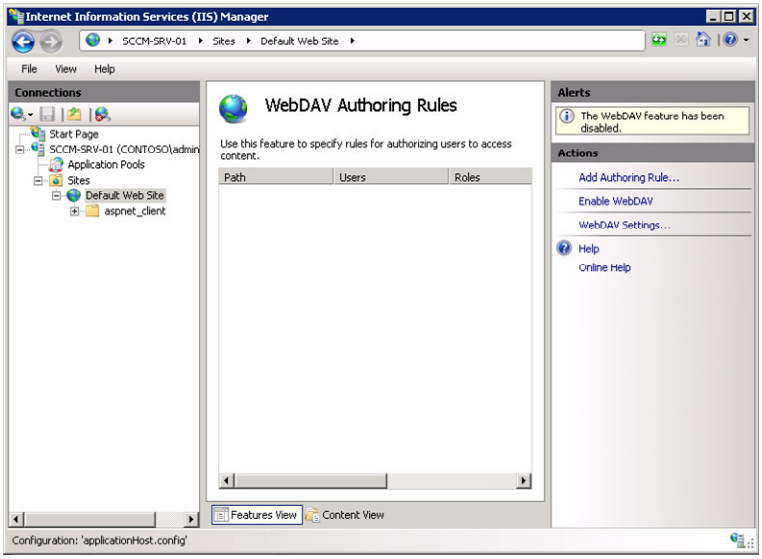
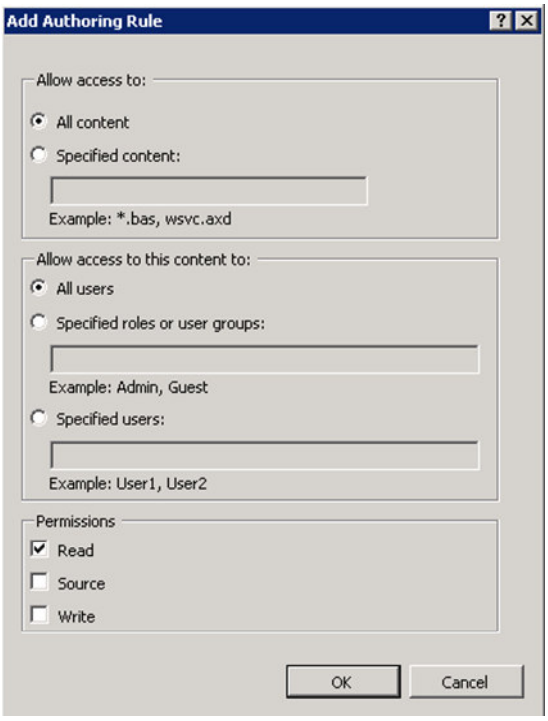
Web-based Distributed Authoring and Versioning (WebDAV) is not included with Windows Server 2008, so it must be downloaded and installed. Detailed steps for downloading and installing WebDAV are available in the article *Installing and Configuring WebDAV on IIS 7.0*[27].

> **Note**
>
> If using Windows Server 2008 R2, WebDAV publishing is included as part of the operating system and can be added as a role service of Web Server (IIS).

Once WebDAV is installed, the steps in Table 25 show how WebDAV should be configured to support Configuration Manager:

Step	Description	Screenshot
1.	Open **Administrative Tools > Internet Information Services (IIS) Manager** and select **Default Web Site.** Double-click **WebDAV Authoring Rules**.	

[27] Installing and Configuring WebDAV on IIS 7.0 **{R23}**: http://go.microsoft.com/fwlink/?LinkId=108052

Step	Description	Screenshot
2.	Click the **Enable WebDAV link** and then click **Add Authoring Rule**.	
3.	Select **All content**, **All users** and **Read**, and then click **OK**.	

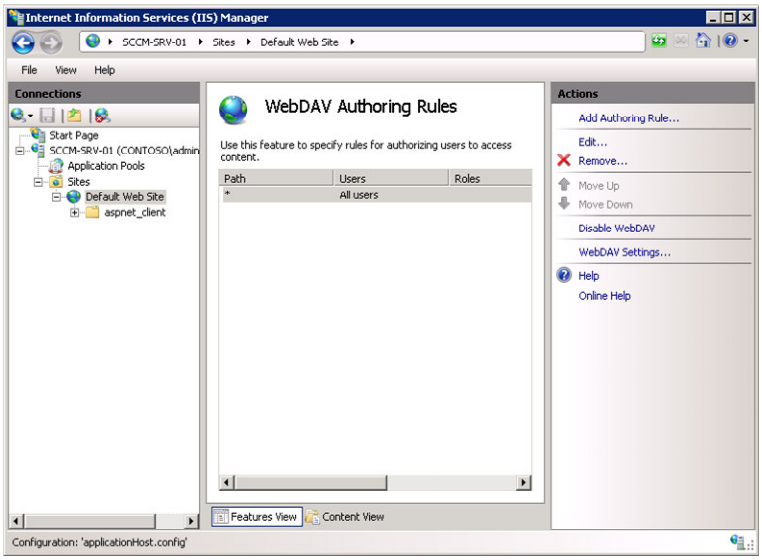
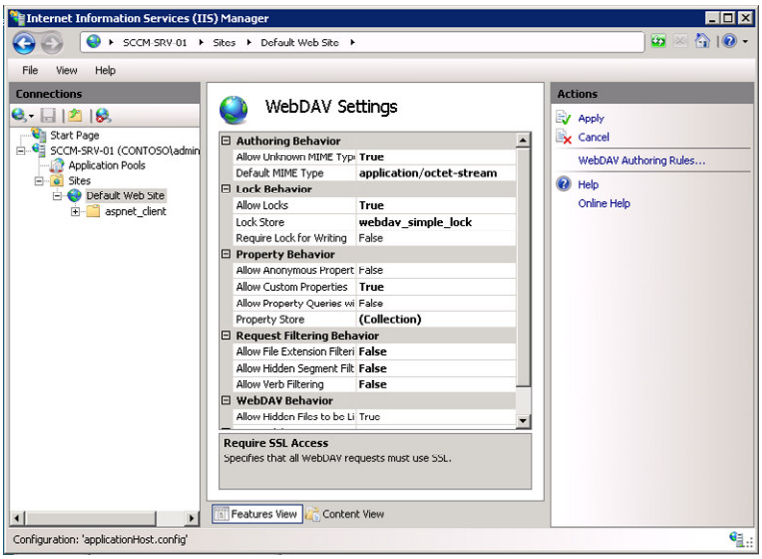
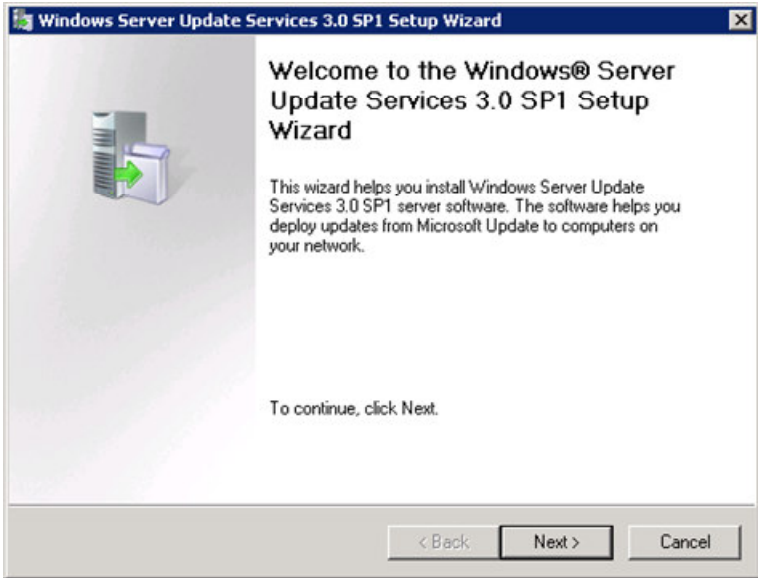
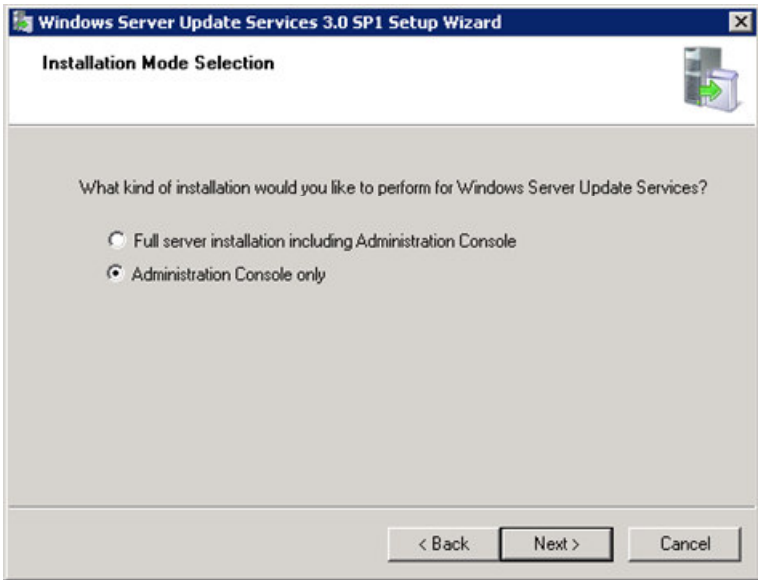
Step	Description	Screenshot
4.	Click **WebDAV Settings**.	
5.	Modify the following settings: ▪ **Allow Anonymous Property Queries –** Set as **True.** ▪ **Allow Custom Properties –** Set as **False.** ▪ **Allow Property Queries with Infinite Depth –** Set as **True** If the server will host a DP, also modify the following setting: ▪ **Allow Hidden Files to be Listed –** Set as **True.** Then click **Apply**.	

Table 25: Configuring WebDAV for Configuration Manager

5.2.1.4 Installing Windows Server Update Services 3.0 SDK

The WSUS 3.0 SDK is installed as part of the WSUS Administrator Console installation. It is not possible to install the SDK separately. Table 26 shows the steps required to install the WSUS Administrator Console, which can be downloaded from:
http://go.microsoft.com/fwlink/?linkid=93750

Step	Description	Screenshot
1.	Run WSUSSetup_30SP1_x<64, or 32>.exe, and click **Next**.	
2.	Select **Administrator Console only** and click **Next**.	

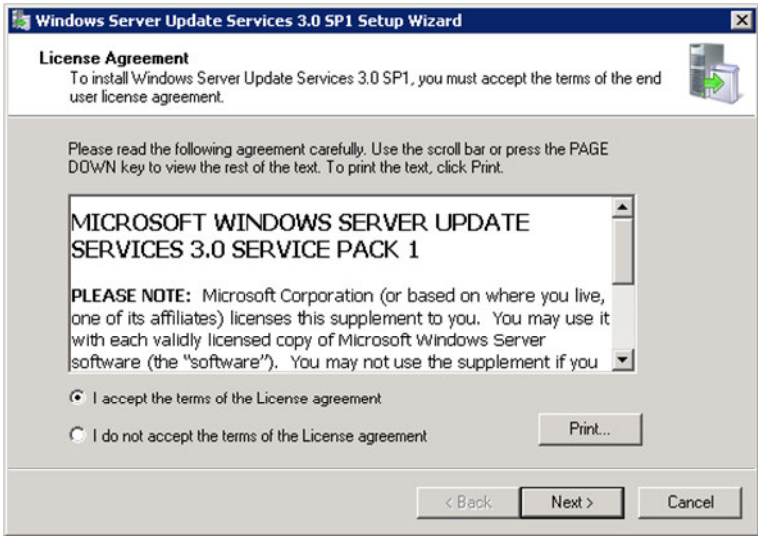
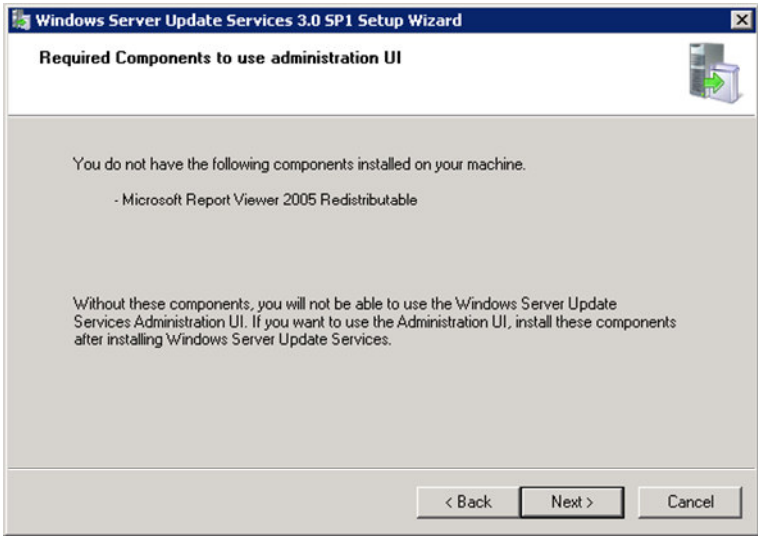
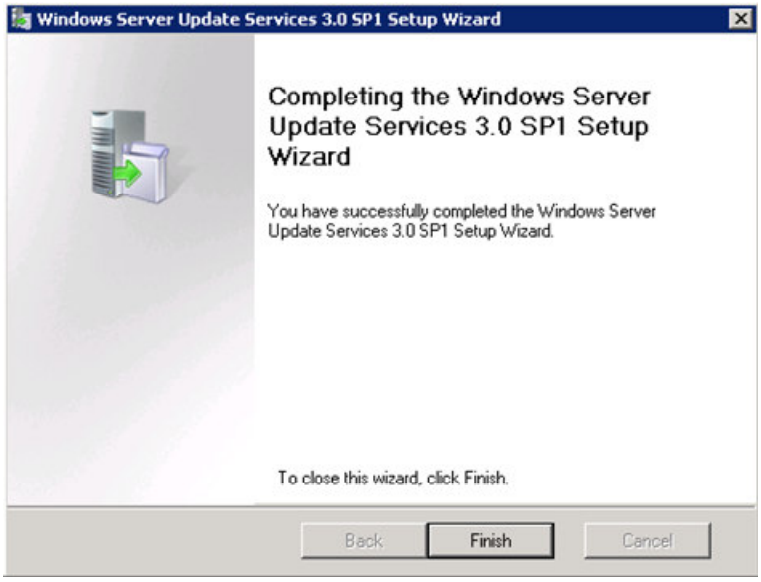
Step	Description	Screenshot
3.	Read the License Agreement and, if applicable, select **I accept the terms of the license agreement** and click **Next**.	
4.	Click **Next**.	
5.	Click **Finish**.	

Table 26: Installing Windows Server Update Services 3.0 SDK

5.2.1.5 Installing Microsoft SQL Server

Microsoft SQL Server (2005 or 2008) needs to be installed either locally on the site server(s) or on a server remote from the site server, if the site database is going to be hosted remotely. If the healthcare organisation is deploying a new SQL server for use with Configuration Manager, and it is being licensed separately (not using the 'System Center Configuration Manager w/ SQL Technology' license), SQL Server 2008 should be used.

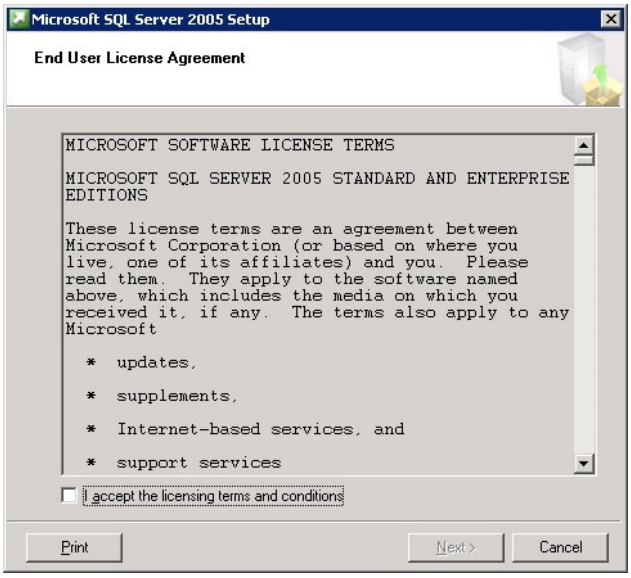
Section 5.2.1.5.1 describes the process to install SQL Server 2005 and section 5.2.1.5.2 describes the process to install SQL Server 2008. Follow the instructions for the version of SQL Server that will be implemented.

These instructions describe the process to install SQL Server in a stand-alone configuration. To install and configure SQL Server 2005 in a failover cluster configuration, see the MSDN article *How to: Create a New SQL Server 2005 Failover Cluster (Setup)*[28]. To configure SQL Server 2008 in a failover cluster configuration see the MSDN article *How to: Create a New SQL Server Failover Cluster (Setup)*[29].

> **Important**
>
> If the SQL Server will be hosted on a different computer to the site server, the site server's computer account must be added to the local Administrators group on each remote site system before running setup.

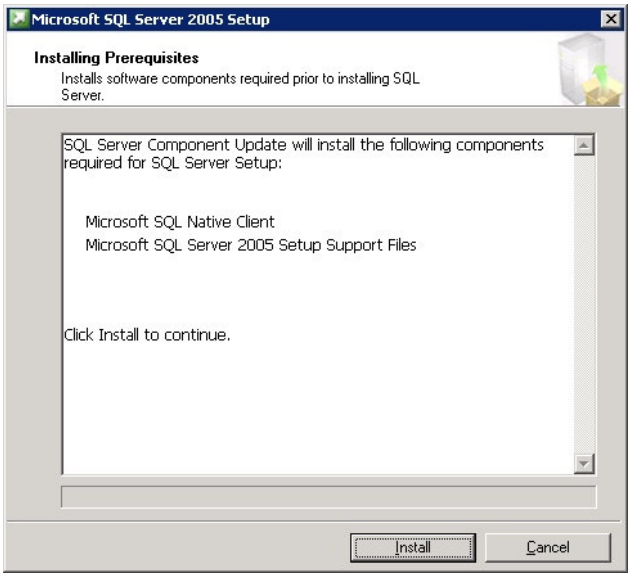
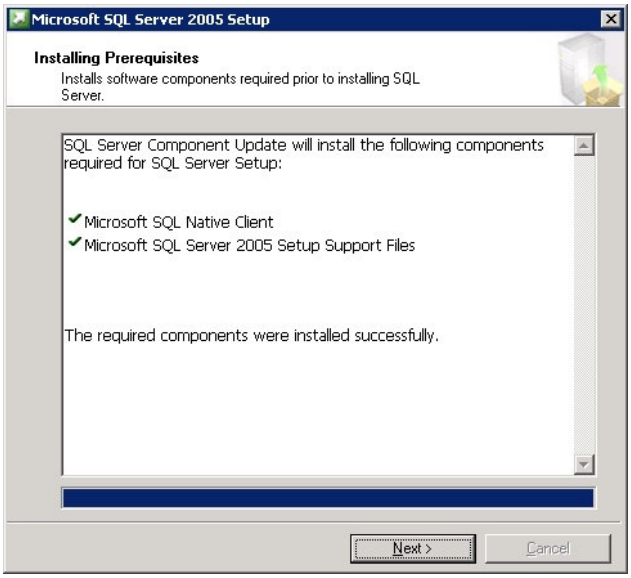
5.2.1.5.1 Install and Configure SQL Server 2005 (Stand-Alone)

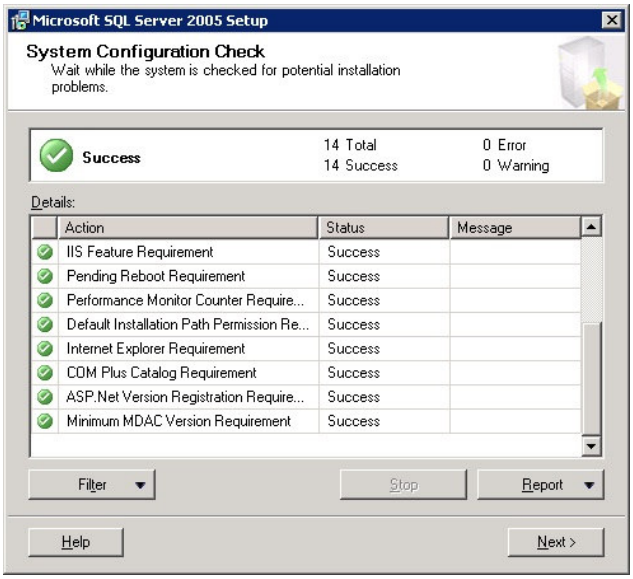
Table 27 shows the process for installing Microsoft SQL Server 2005:

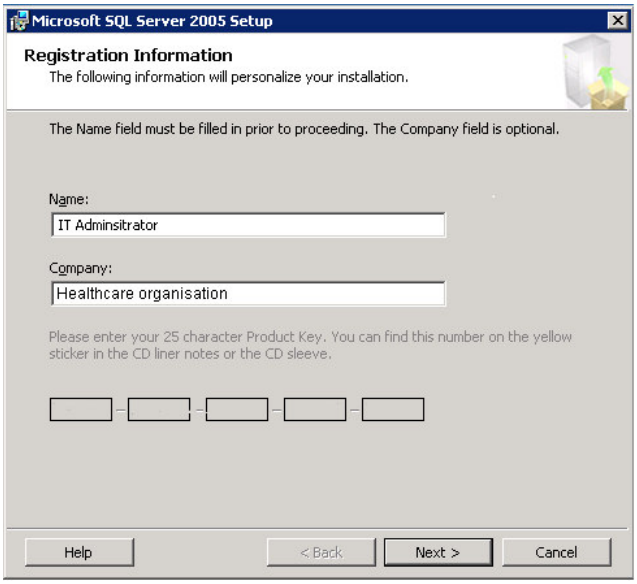
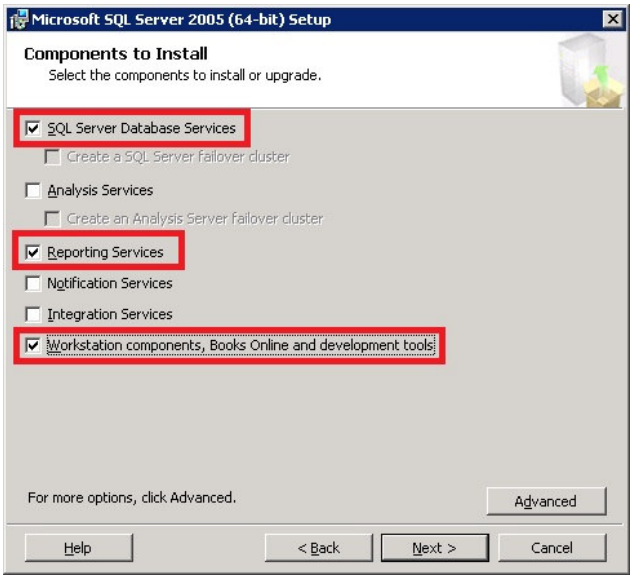
Step	Description	Screenshot
1.	From the SQL Server 2005 source files, select **...Servers\Setup.exe** to launch the Microsoft SQL Server Setup Wizard. Review the **End User Licence Agreement**, and if applicable, select **I accept the licensing terms and conditions**, and then click **Next**.	

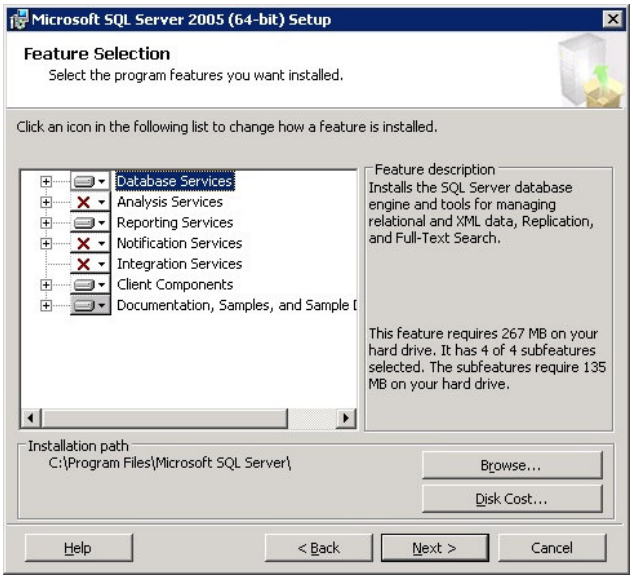
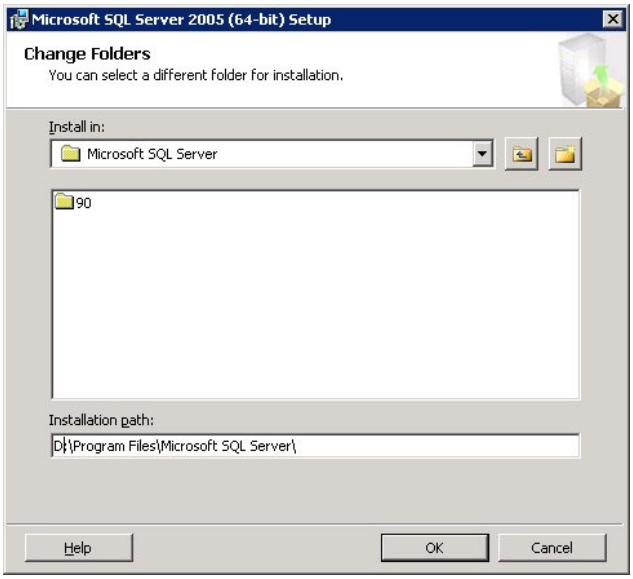
[28] MSDN: How to: Create a New SQL Server 2005 Failover Cluster (Setup) **{R24}**: http://msdn.microsoft.com/en-us/library/ms179530(SQL.90).aspx

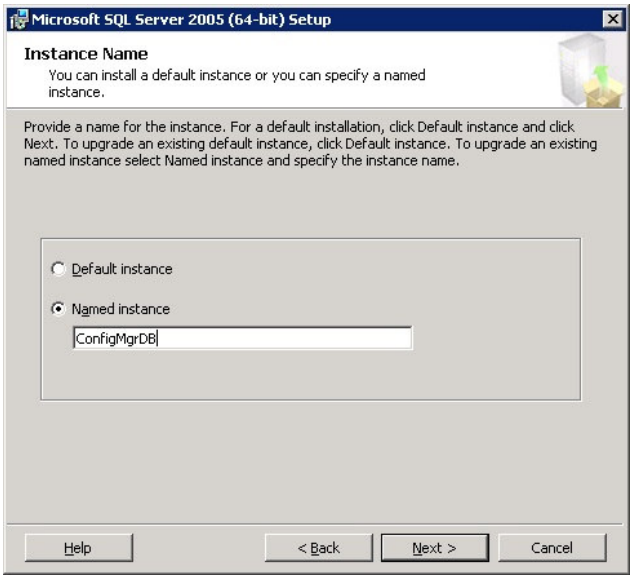
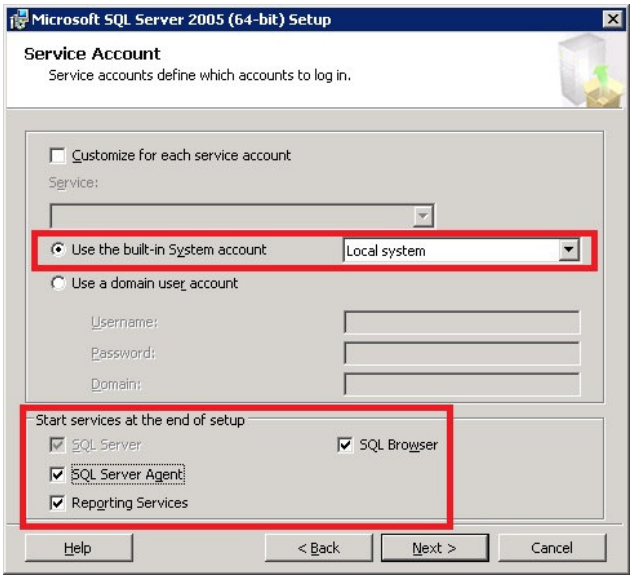
[29] MSDN: How to: Create a New SQL Server Failover Cluster (Setup) **{R25}**: http://msdn.microsoft.com/en-us/library/ms179530.aspx

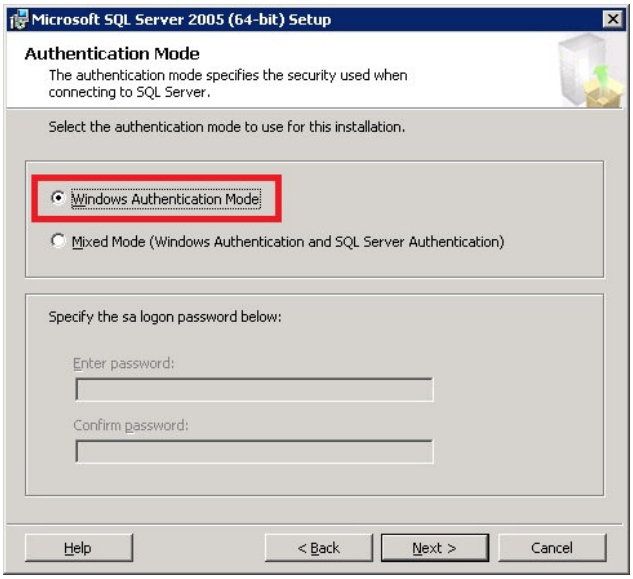
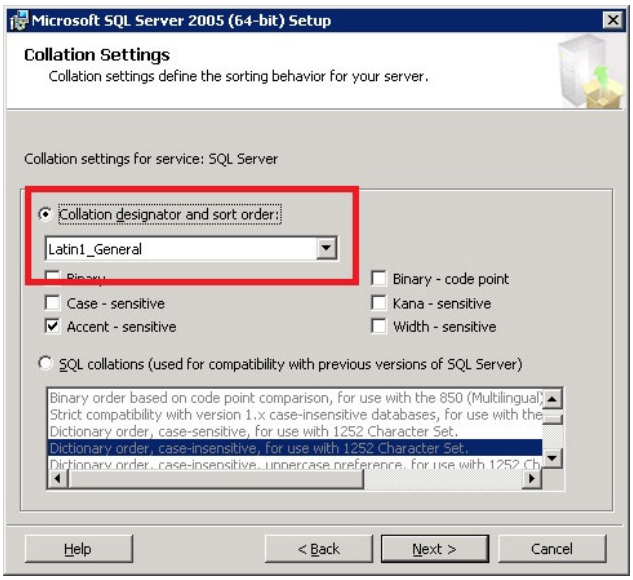
Step	Description	Screenshot
2.	Before SQL Server 2005 installation can proceed, a number of prerequisites need to be installed. On the **Installing Prerequisites** page, click **Install** to begin the prerequisite installation.	
3.	When the installation has completed successfully, the wizard will confirm success as shown. Click **Next**.	

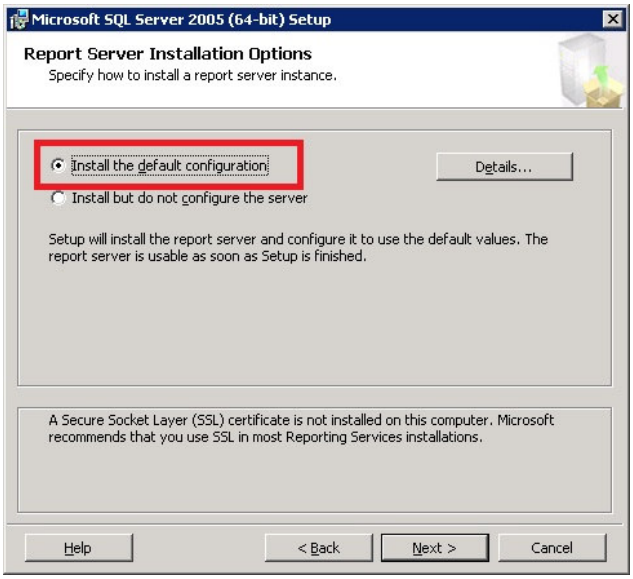
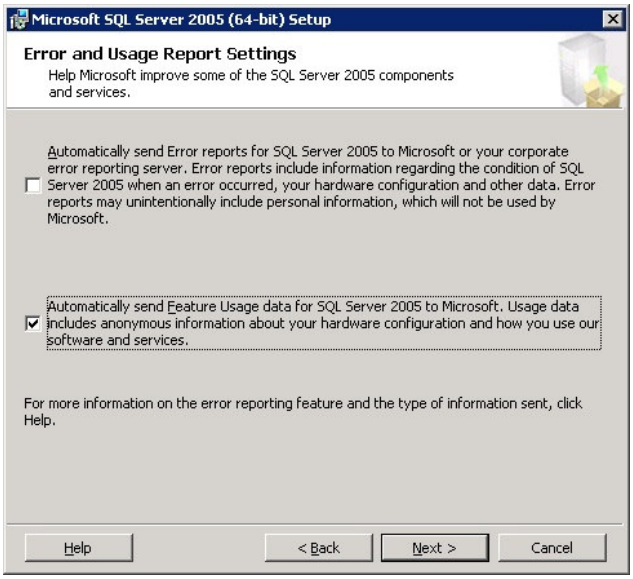
Step	Description	Screenshot
4.	On the Microsoft SQL Server Installation Welcome page, click **Next**.	
5.	On the **System Configuration Check** page, Microsoft SQL Server will evaluate the computer for hardware and software requirements prior to installation, as shown. Ensure that all prerequisite checks complete successfully and click **Next**.	

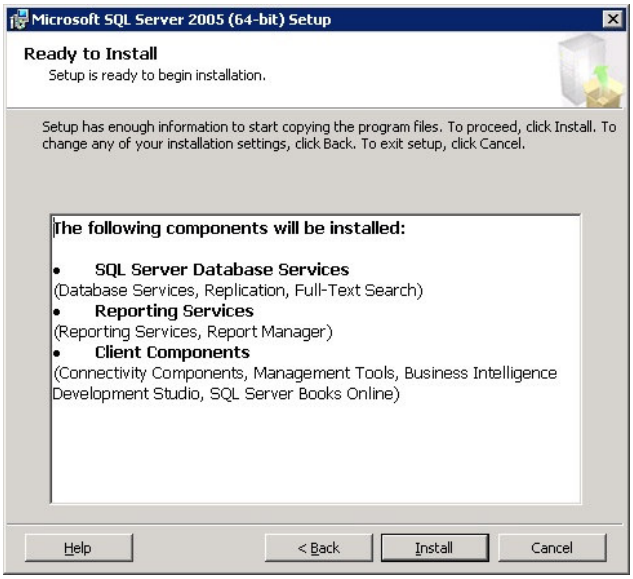
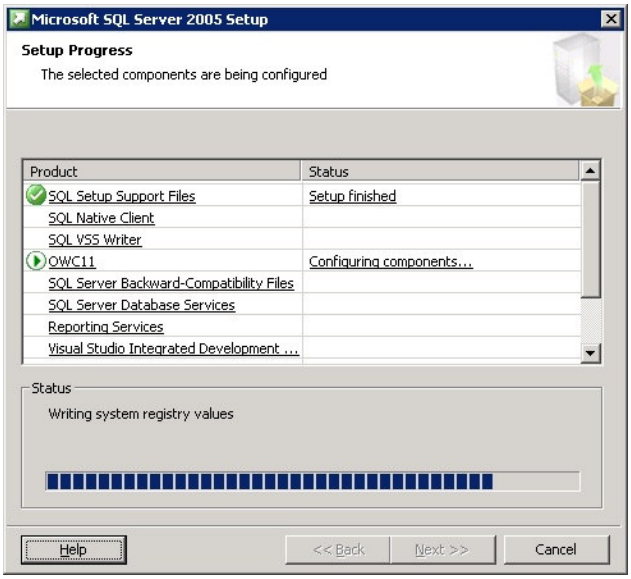
Step	Description	Screenshot
6.	Enter the relevant **Name** and **Company** details and click **Next**.	
7.	Select the following options: ▪ **SQL Server Database Services** ▪ **Reporting Services** ▪ **Workstation components, Books Online and development tools** Then click the **Advanced** button.	

Step	Description	Screenshot
8.	Click the **Browse** button.	
9.	On the **Change Folders** page, select the installation path for each feature. Click **OK** once the correct installation paths have been selected.	

Step	Description	Screenshot
10.	On the **Instance Name** page, select **Named Instance** and specify a name. Click **Next**.	
11.	Ensure the Customize for each service account check box is clear. Click **Use the built-in System account**. **Note** If security is a concern, it is recommended that you create a domain-based account to run SQL Services. If this has been done, click **Use a domain user account** and enter the **Username**, **Password** and **Domain** details of the server-specific SQL service account that has been created. In the **Start services at the end of setup** section, select **SQL Server Agent**, **Reporting Services** and **SQL Browser.** Click **Next**.	

Step	Description	Screenshot
12.	Ensure **Windows Authentication mode** is selected, as shown. Click **Next**.	
13.	Ensure that **Collation designator and sort order** is selected. Ensure that the following options are **clear**: ▪ **Binary** ▪ **Case-sensitive** ▪ **Binary-code point** ▪ **Kana - sensitive** ▪ **Width - sensitive** Ensure that **Accent - sensitive** is selected. Click **Next**.	

Step	Description	Screenshot
14.	Click **Install the default configuration**. Click **Next**.	
15.	Select the **Error and Usage Report Settings** that are required. Click **Next**.	

Step	Description	Screenshot
16.	Click **Install** to begin the installation.	
17.	The setup process will provide status information of all the installation steps, as shown.	

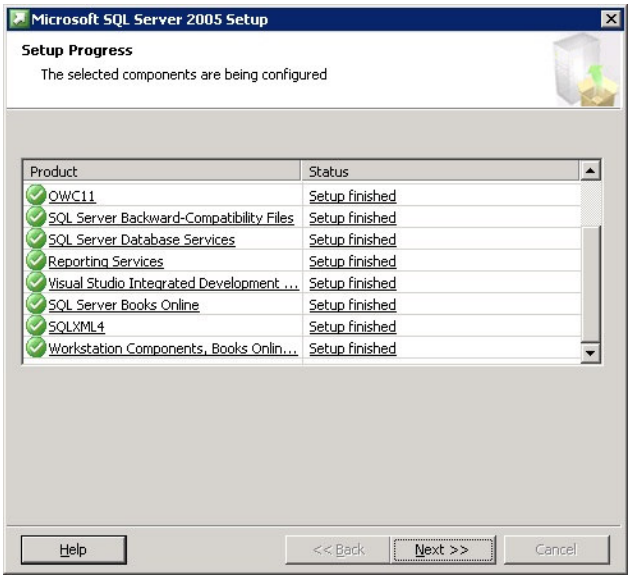
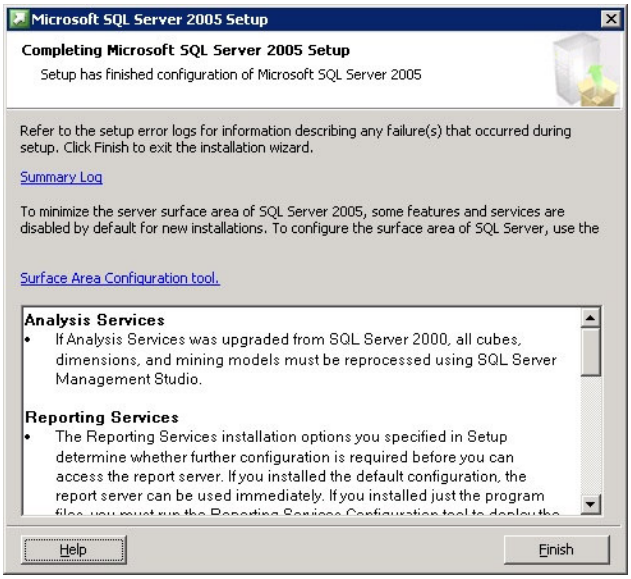
Step	Description	Screenshot
18.	When the installation process has completed, the **Setup Progress** page shows each stage as having completed successfully, as shown. Ensure all steps have completed successfully and then click **Next**.	
19.	Click **Finish**.	

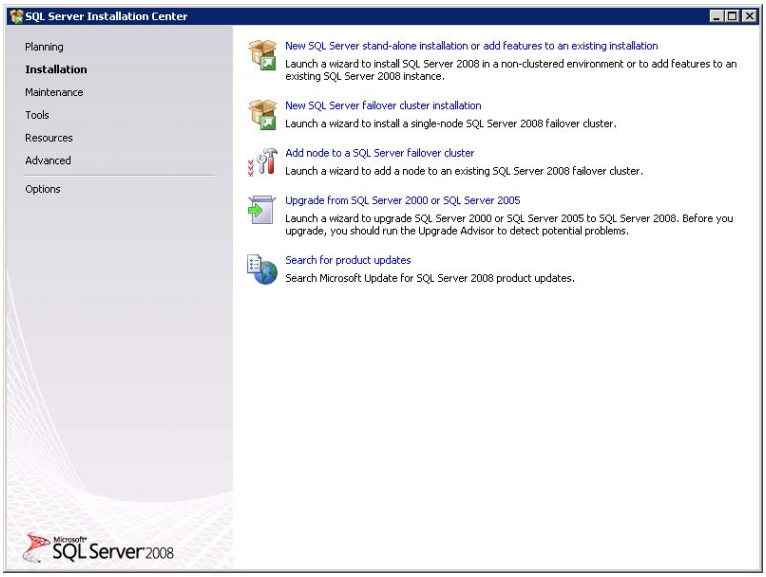
Table 27: Installing and Configuring SQL Server 2005 RTM

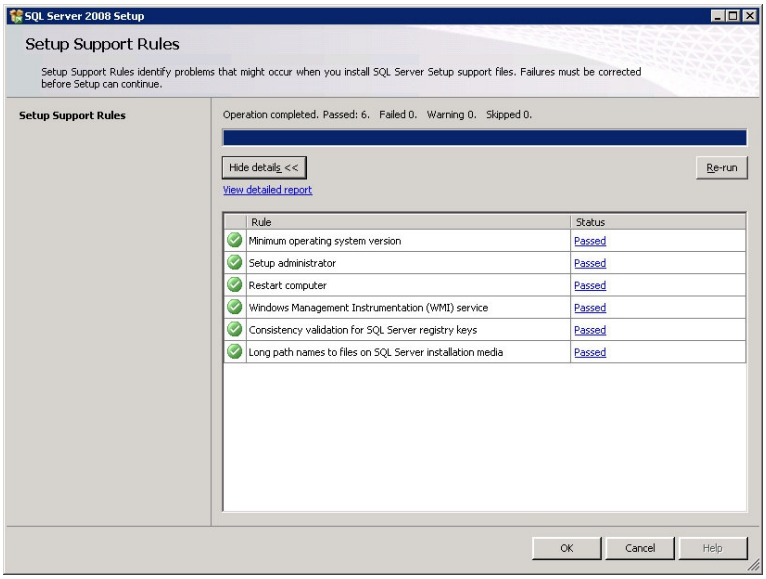
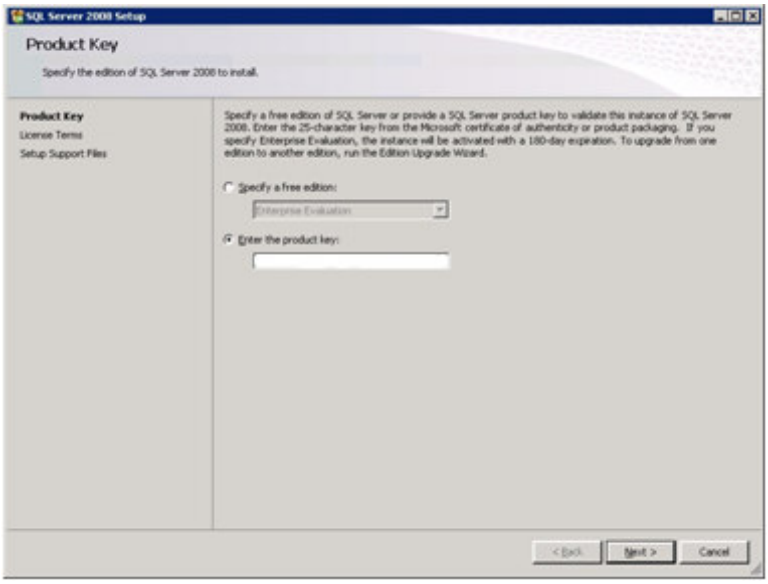
Once the base version of SQL Server 2005 has been installed, the latest service pack needs to be applied. At the time of writing, the latest service pack for SQL Server 2005 was Service Pack 3. The healthcare IT Administrator should check the Knowledge Base article *How to obtain the latest service pack for SQL Server 2005*[30] to verify the latest service pack.

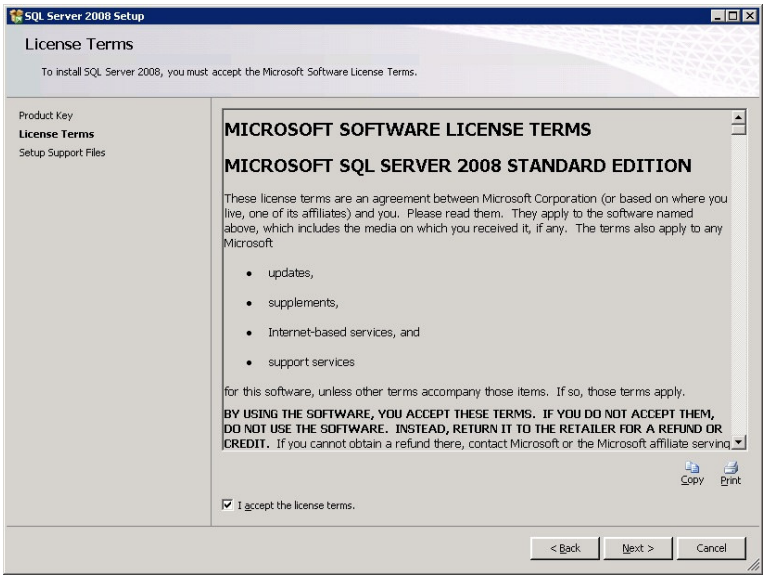
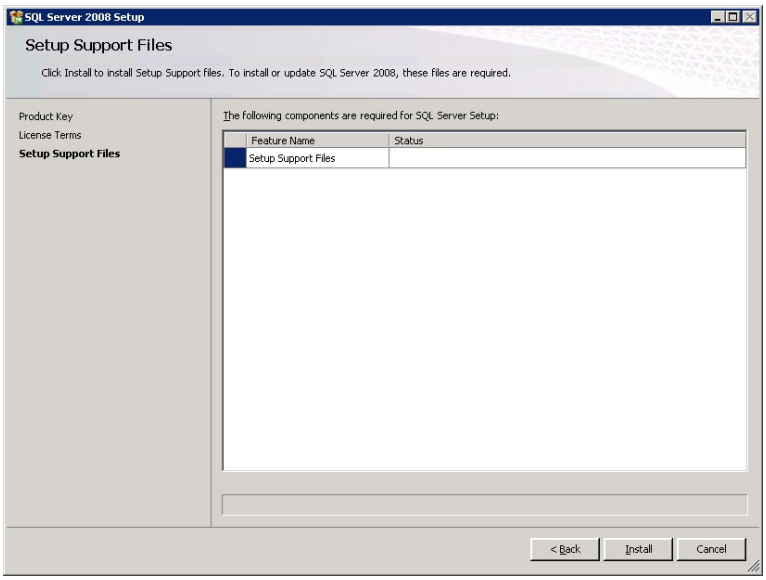
[30] Microsoft Help and Support: How to obtain the latest service pack for SQL Server 2005 **{R26}**: http://support.microsoft.com/kb/913089

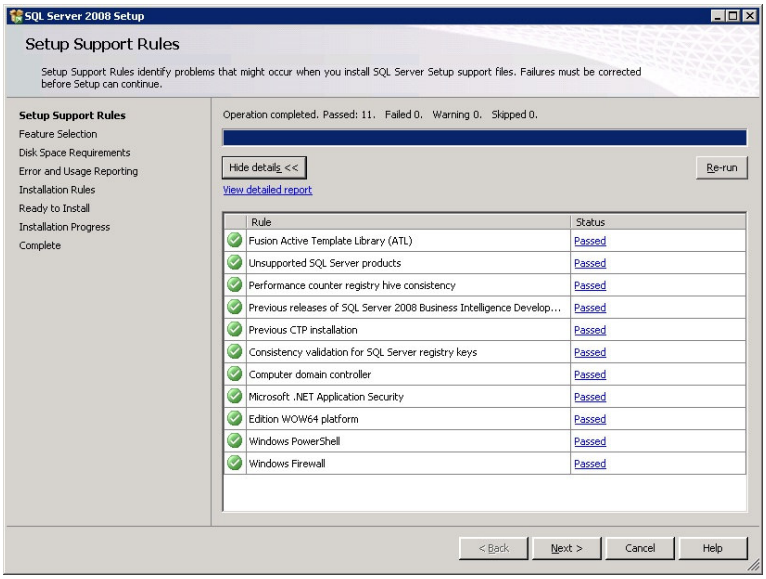
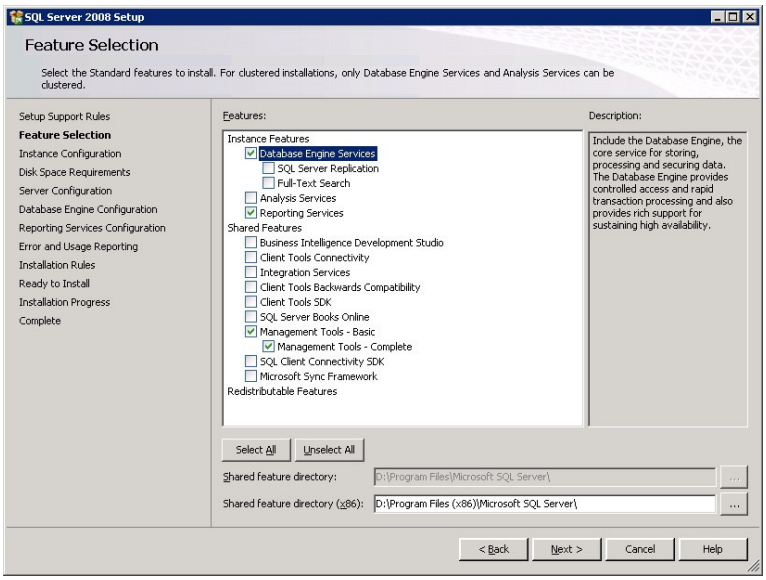
5.2.1.5.2 Install and Configure SQL Server 2008 (Stand-Alone)

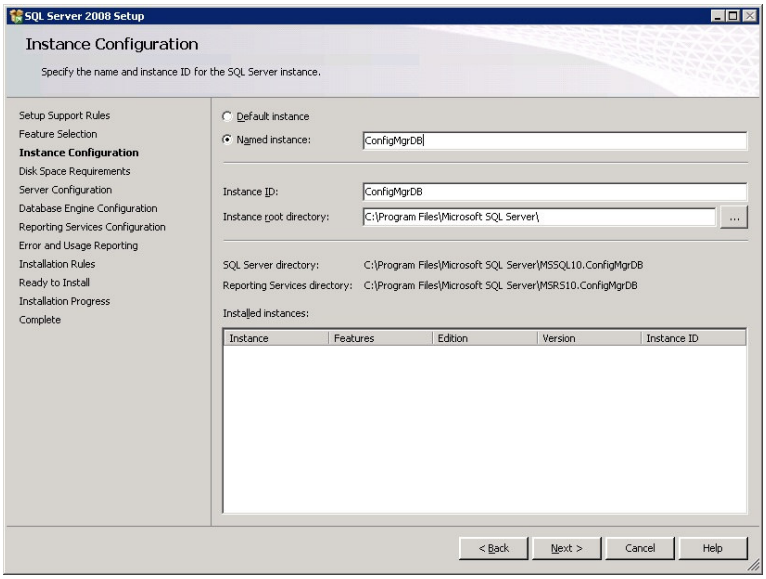
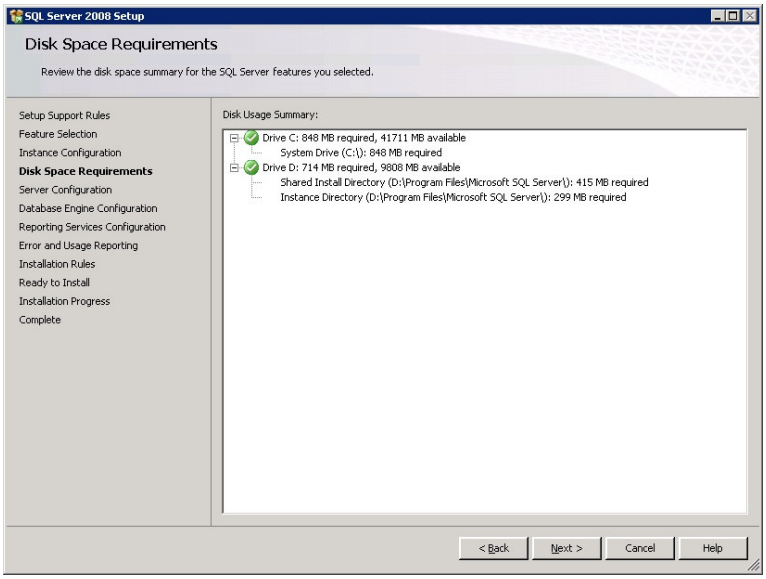
Table 28 shows the process for installing Microsoft SQL Server 2008:

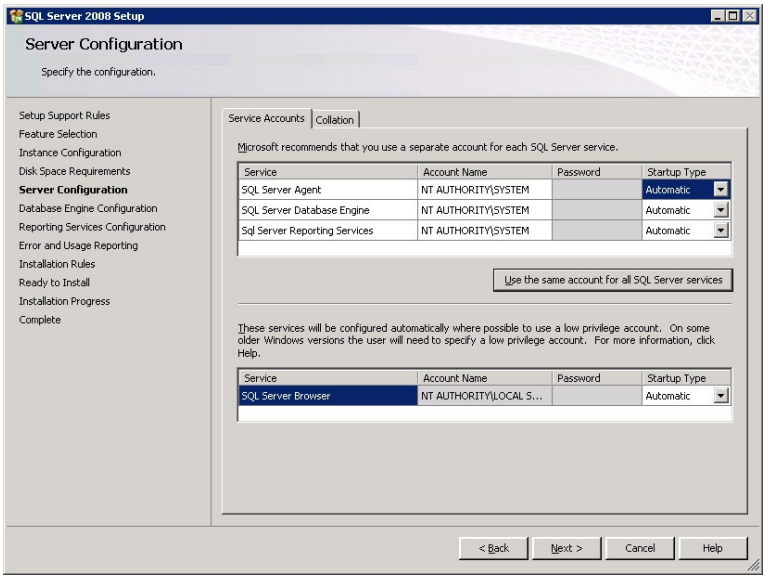
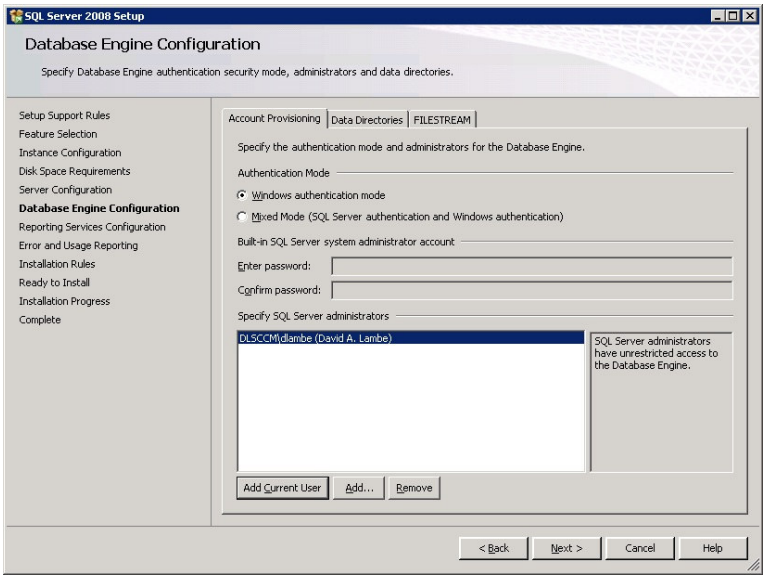
Step	Description	Screenshot
1.	Insert the SQL Server 2008 media and follow the prompts to verify the prerequisites. If Microsoft® NET Framework version 3.5 SP1 has not been installed, a prompt will be displayed to install it. If SQL Server is being installed on Windows Server 2003, Hotfix KB942288-v4 will also be required and a prompt will be displayed. This update requires a restart. Begin the installation of SQL 2008 after the restart (if necessary) by clicking on Setup.exe from the SQL Server 2008 media. The SQL Server Installation Center will open. Run through the System Configuration Checker, Install Upgrade Advisor, or any other prerequisite tools to ensure that the system is ready for an installation. Click on **Installation** below **Planning** on the left side of the window.	
2.	Click on **New SQL Server stand-alone installation or add features to an existing installation**.	

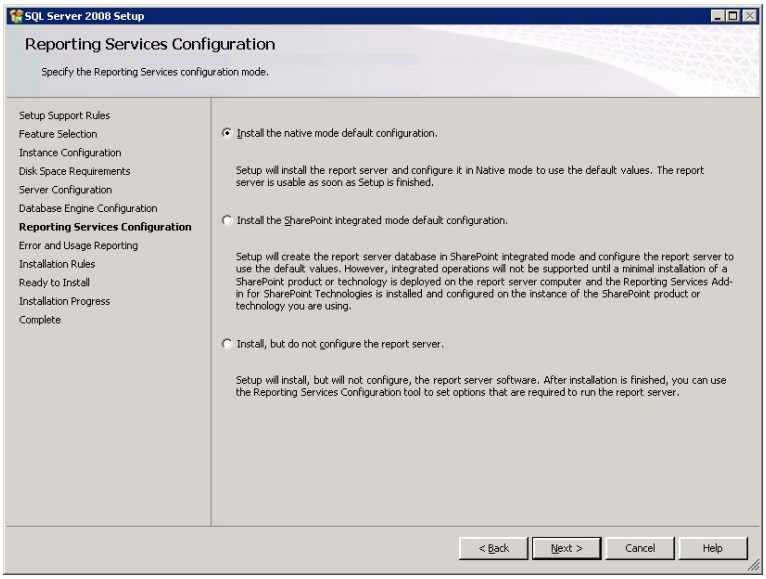
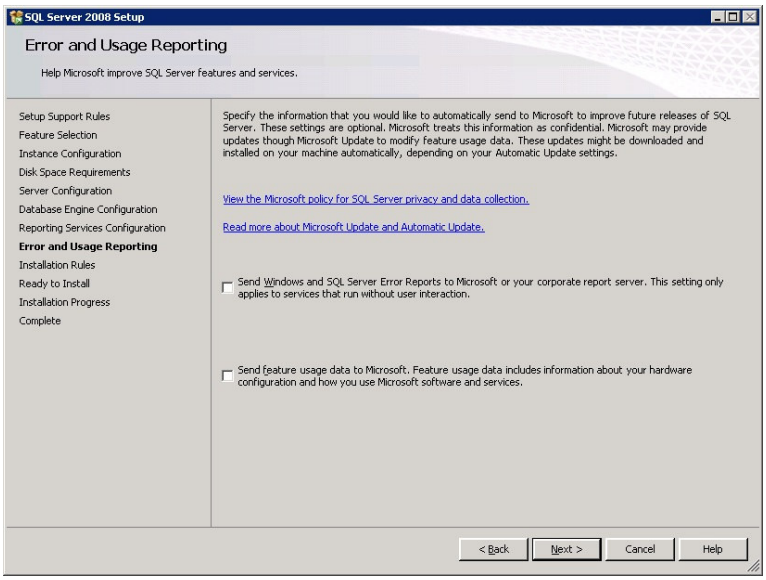
Step	Description	Screenshot
3.	The **Setup Support Rules** page will be displayed. If any warnings or failures are displayed, address these issues before proceeding. Click **OK**.	
4.	Enter the Product Key (if required). Click **Next**.	

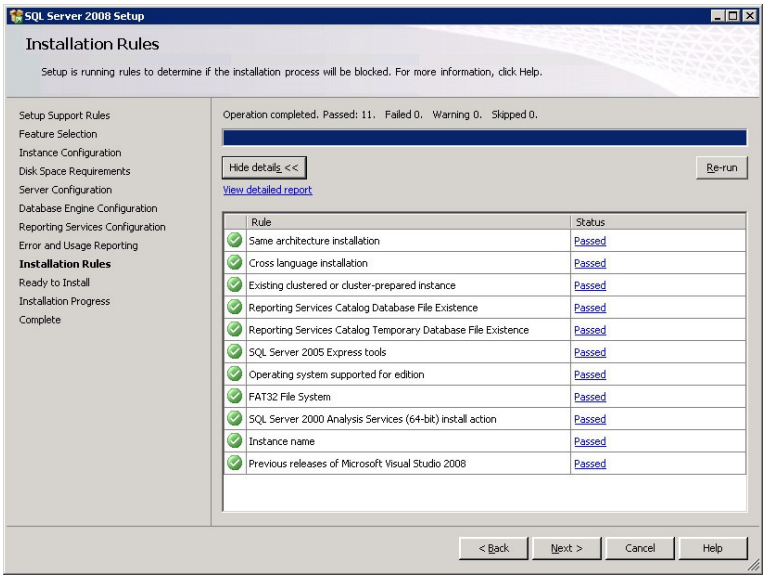
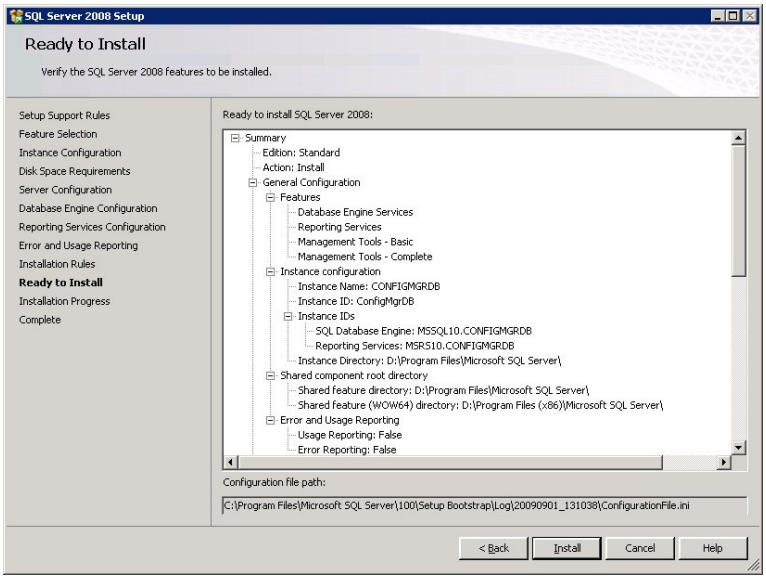
Step	Description	Screenshot
5.	Read the License Terms and, if applicable, select **I accept the license terms**. Click **Next**.	
6.	Click **Install** to install the SQL 2008 Setup Support Components. After the Support Components are installed, click **Next**.	

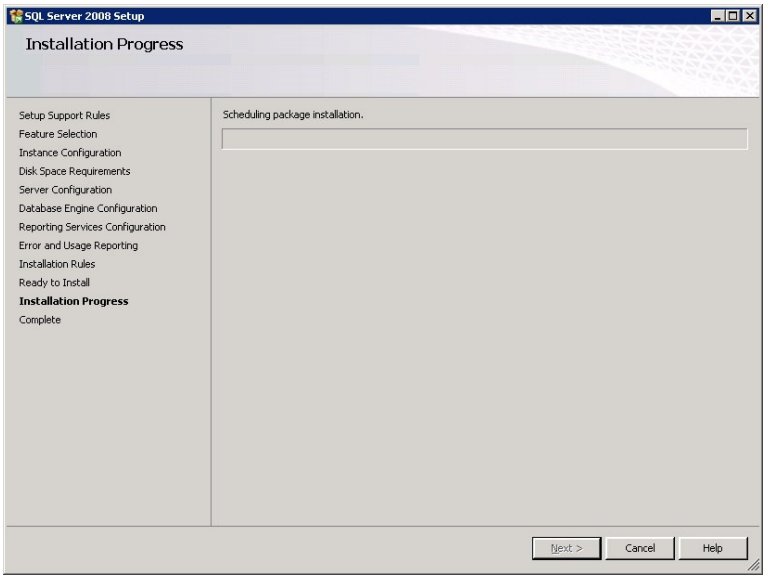
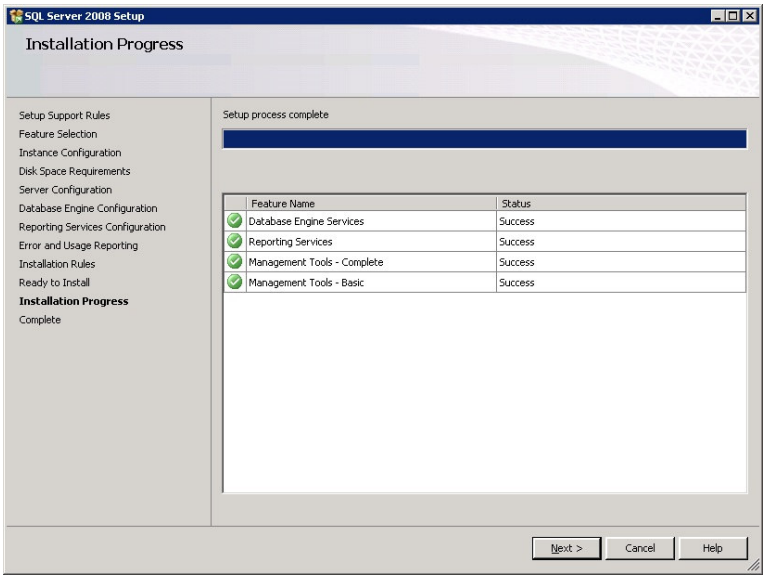
Step	Description	Screenshot
7.	The **Setup Support Rules** page will be displayed. If any warnings or failures appear, address these issues before proceeding. Click **Next**.	
8.	Select these features for the SQL installation: ■ Database Engine Services ■ Reporting Services ■ Management Tools – Complete Then specify the Shared Feature Directory locations. Click **Next**.	

Step	Description	Screenshot
9.	Click **Named Instance** and in the text box, enter **ConfigMgrDB.** Accept the **Instance ID** but change the **Instance root directory** to a drive other than drive C. Click **Next**.	
10.	Verify that enough disk space exists and click **Next**.	

Step	Description	Screenshot
11.	Click on the value under **Account Name** for each **Service** and use the drop-down to select **NT Authority\System** as the Service Account. For SQL Server Agent, click the **Startup Type** drop-down arrow to change the startup type to **Automatic**. Click **Next**.	
12.	Click on the **Data Directories** tab and specify the target directory for each of the following: ■ Data root directory ■ User database directory ■ User database log directory ■ Temp database directory ■ Temp database log directory ■ Backup directory On the **Account Provisioning** tab, click the **Add Current User** button (more users and user groups can be added using the **Add** button). **Important** The users or user groups added here will be the only people able to access the SQL Server Management studio, once SQL Server has been installed. Click **Next**.	

Step	Description	Screenshot
13.	Click **Install the native mode default configuration** and click **Next**.	
14.	Select the **Error and Usage Reporting** settings that are required. Click **Next**.	

Step	Description	Screenshot
15.	Verify that no installation Rules show failures or warnings and click **Next.** **Note** If any issues are experienced during setup, they must be resolved before completing SQL Server installation and installing Configuration Manager. More information will be provided if any errors are experienced and these should be researched to find a resolution, or the healthcare organisation's support provider should be contacted.	
16.	Verify that the installation components summary is correct and click **Install**. **Tip** If multiple servers will be deployed using the same configuration, make a note of the location of the **ConfigurationFile.ini,** because this file can be used to perform an unattended installation of SQL Server, if required.	

Step	Description	Screenshot
17.	The **Installation Progress** page will be displayed.	
18.	When the setup process is complete, verify that all the required features have been installed successfully, and then click **Next**.	

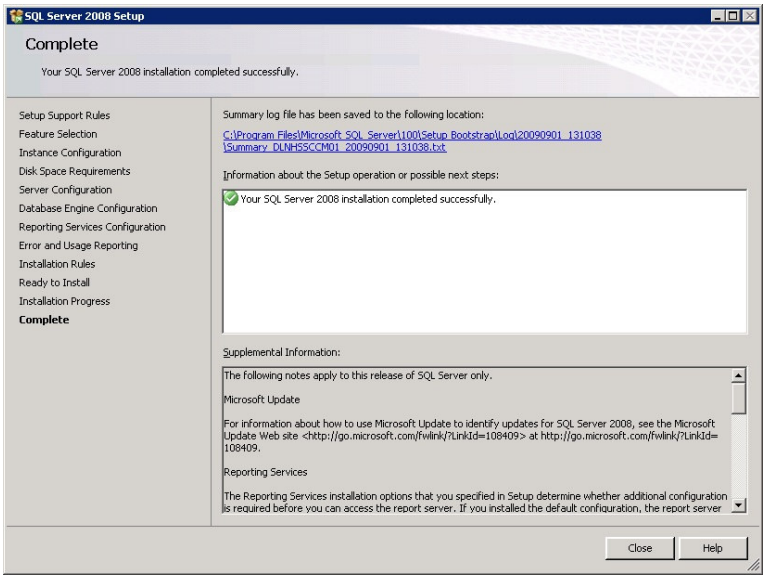
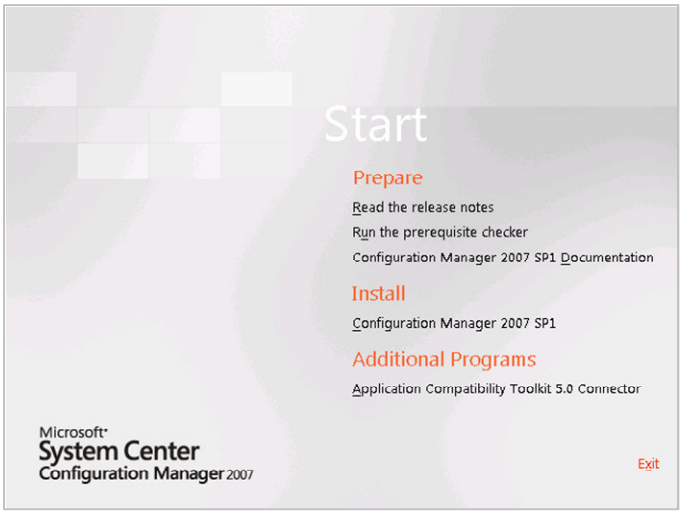
Step	Description	Screenshot
19.	Click **Close**.	

Table 28: Installing and Configuring SQL Server 2008

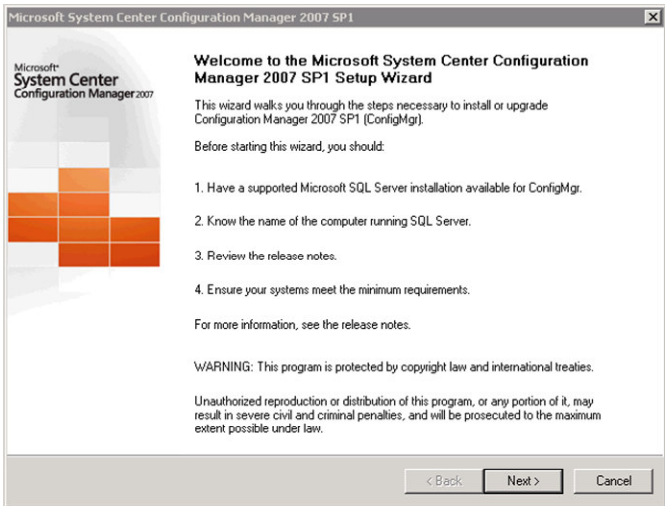
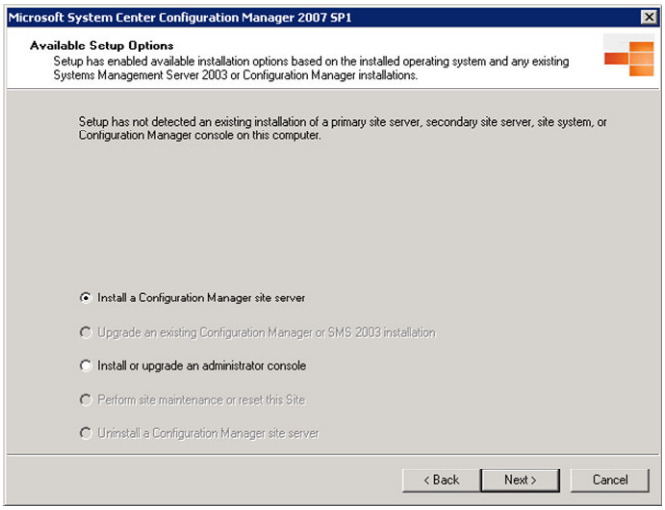
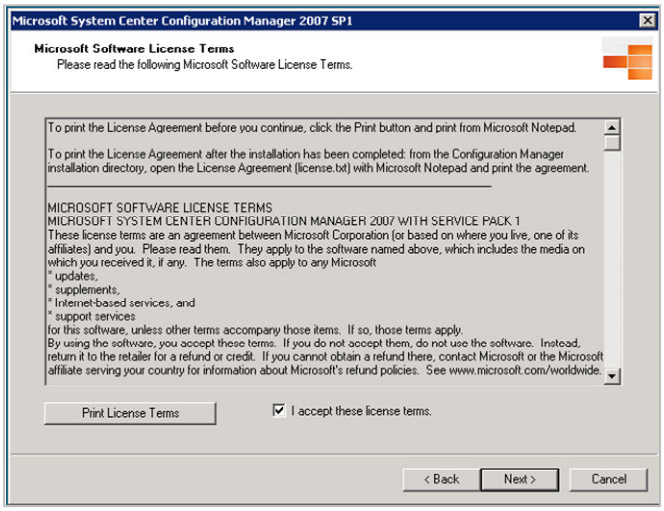
Once the base version of SQL Server 2008 has been installed, the healthcare IT Administrator needs to install the latest service pack (at the time of writing, the latest service pack for SQL Server 2008 was Service Pack 1). Check for the latest version on the *SQL Server 2008 Homepage*[31].

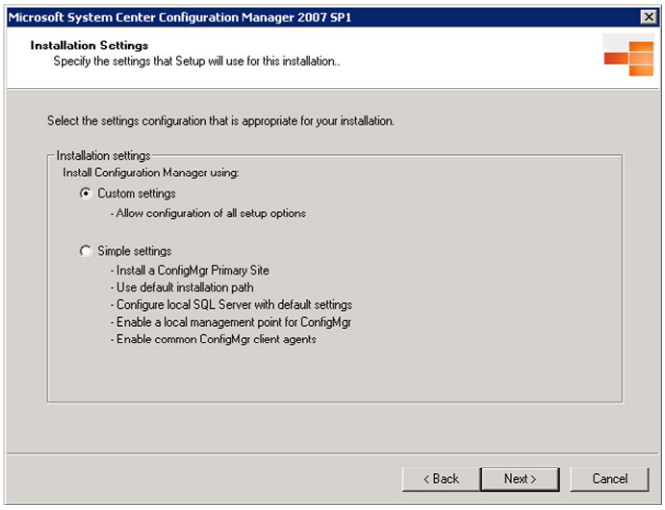
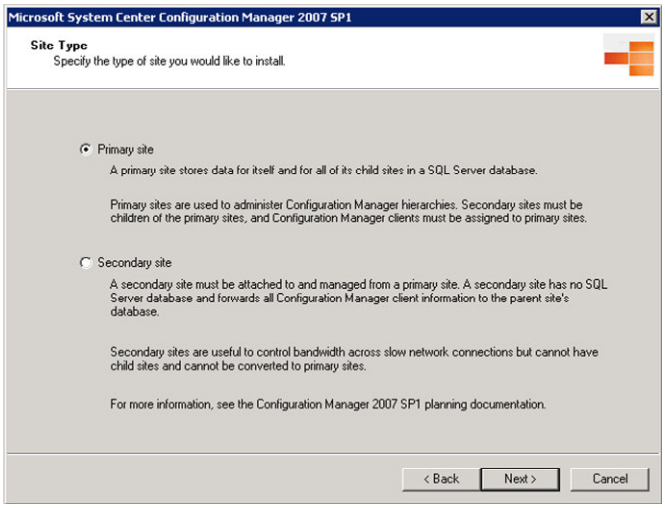
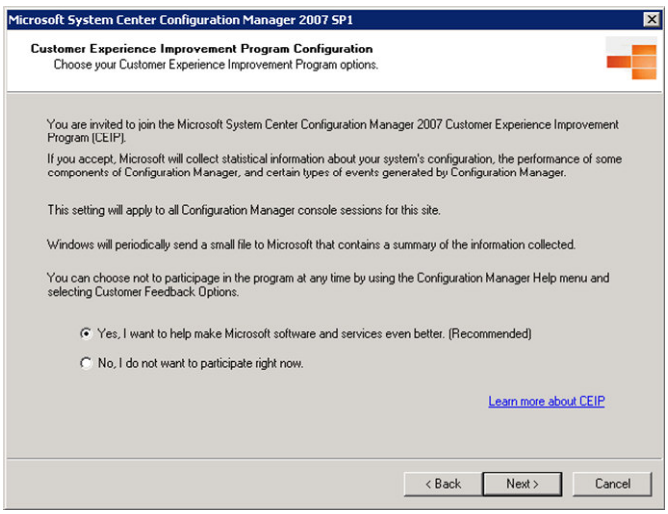
5.2.2 Installing the First Configuration Manager Site

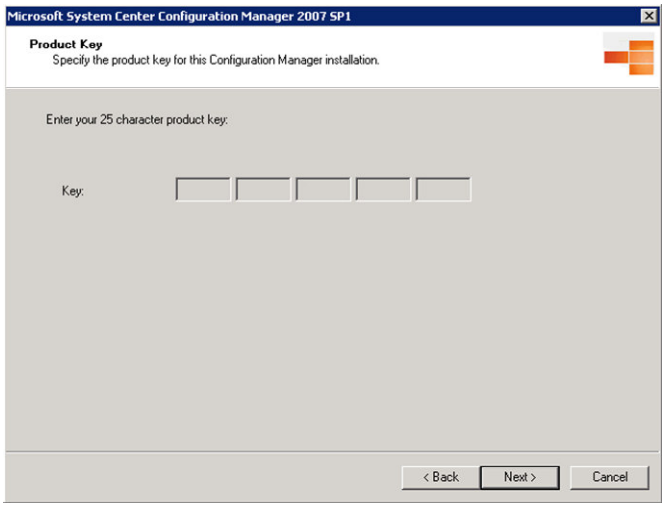
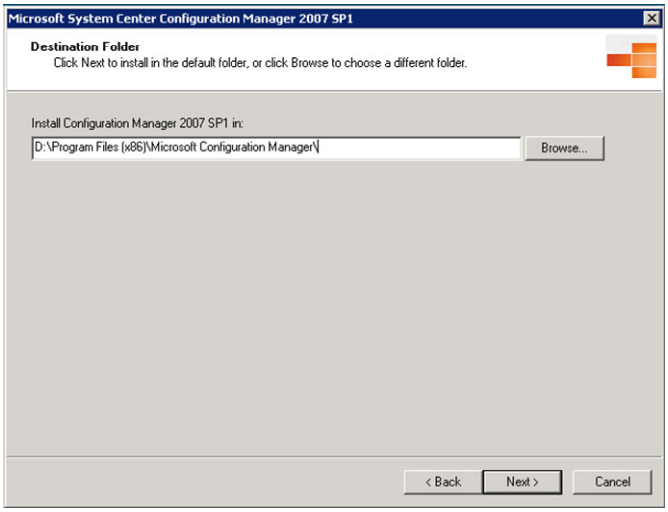
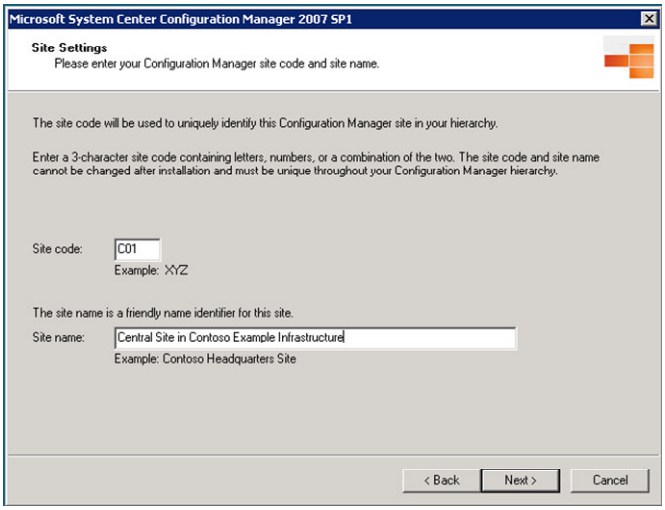
Table 29 below shows the steps to install the first Configuration Manager site. These steps can also be used to install a child primary site; however, a child primary site will need additional configuration once the steps are complete, as shown in section 5.2.4.

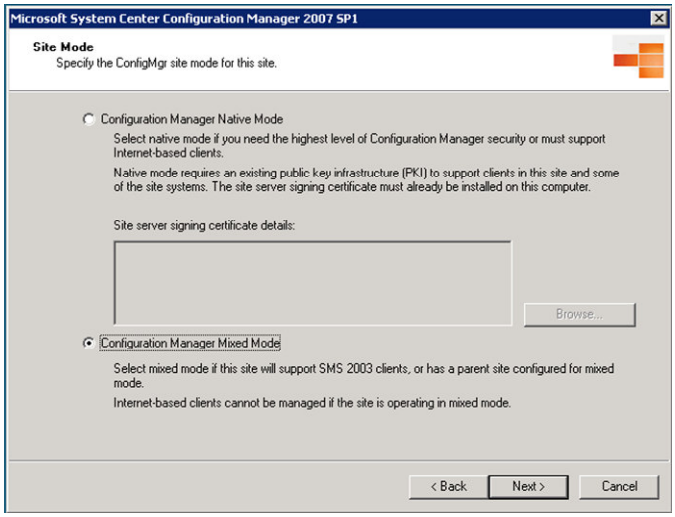
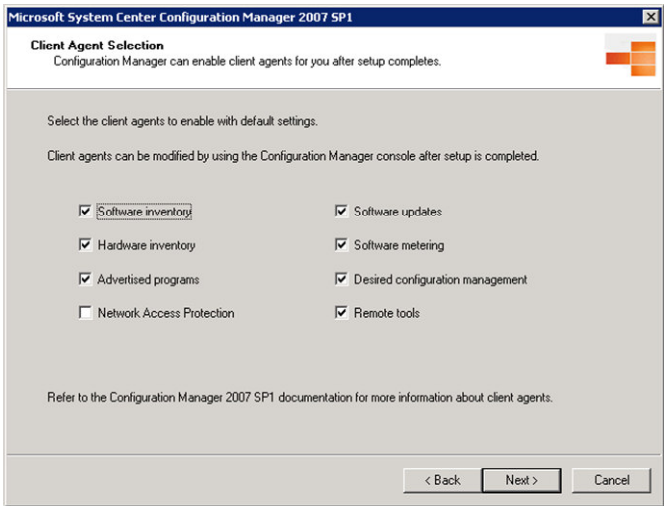
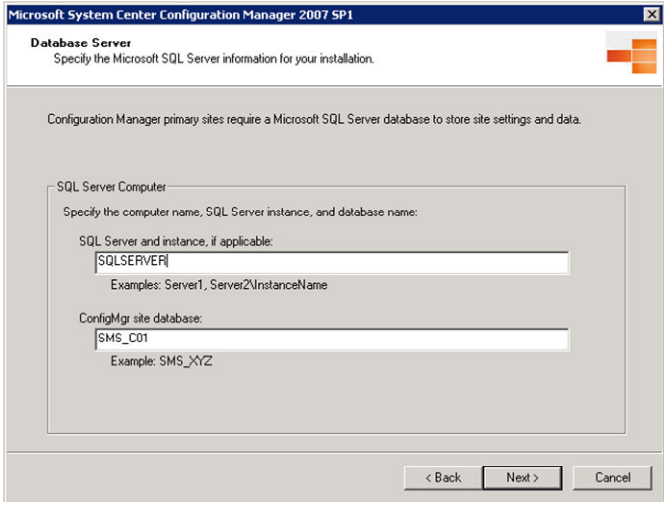
Step	Description	Screenshot
1.	Run Splash.hta from the Configuration Manager product CD. In the **Start** screen, click **Configuration Manager 2007 SP1** under **Install**.	

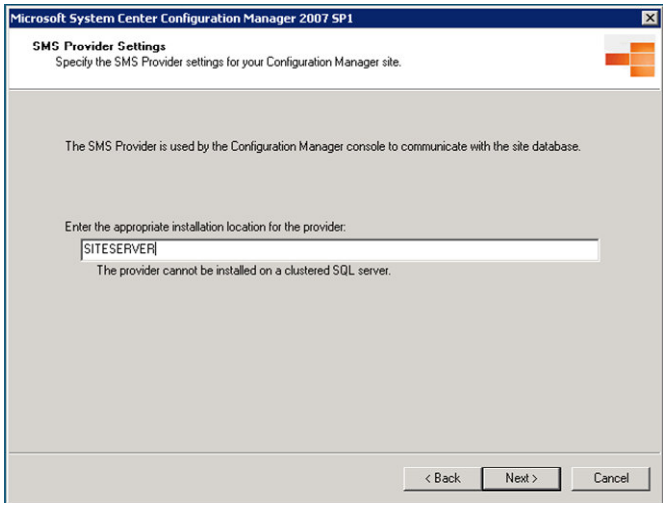
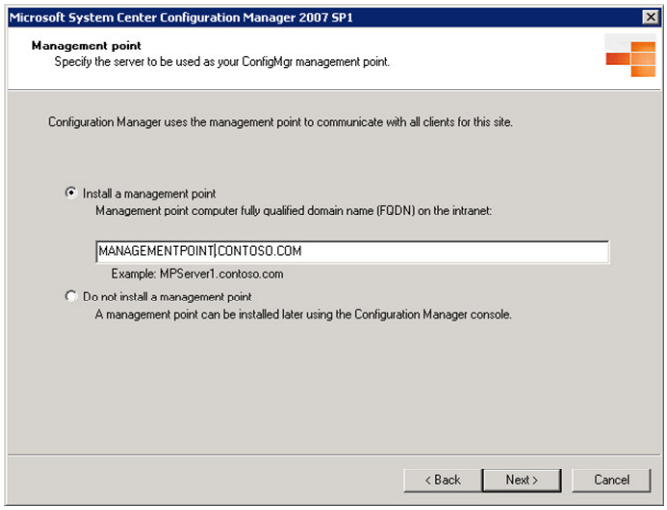
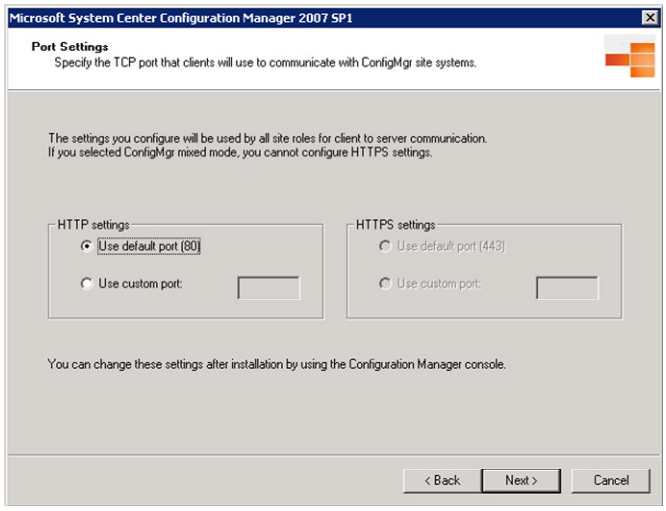
[31] Microsoft Web Site: SQL Server 2008 Homepage **{R27}**: http://www.microsoft.com/sqlserver/2008/en/us/default.aspx

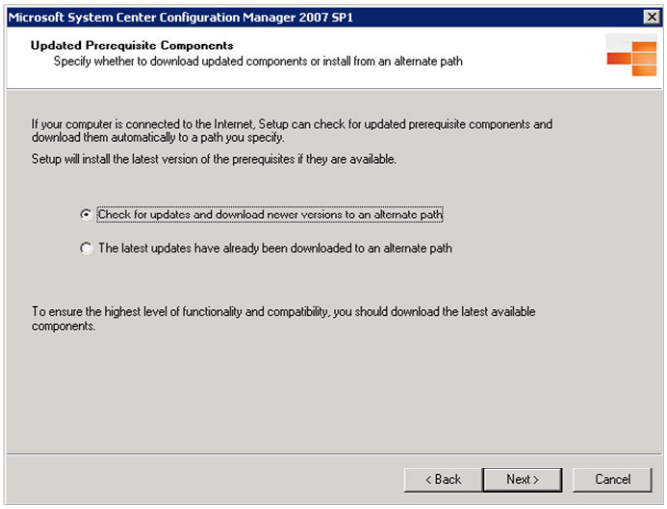
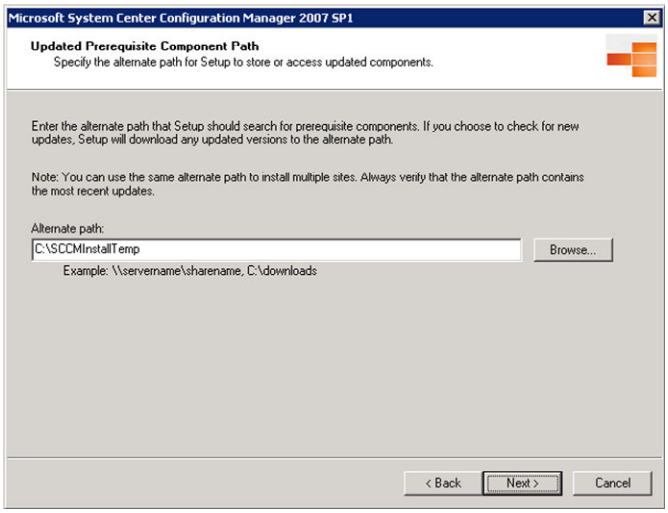
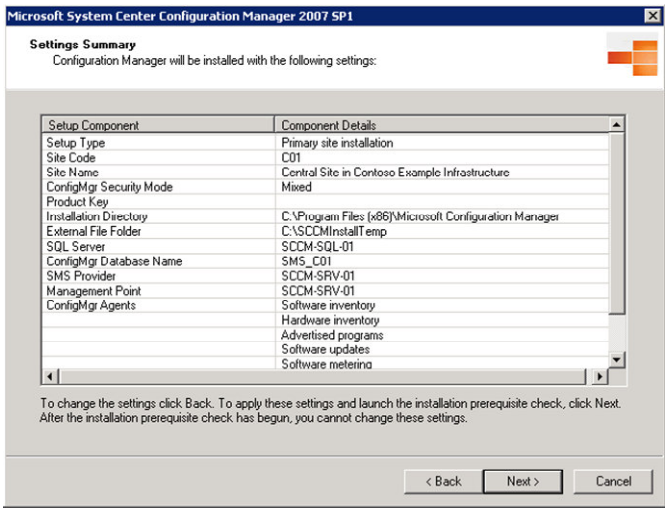
Step	Description	Screenshot
2.	Click **Next**.	
3.	Click **Install a Configuration Manager site server** and click **Next**.	
4.	Read the Microsoft Software License Terms and, if applicable, select **I accept these license terms** and click **Next**.	

Step	Description	Screenshot
5.	Click **Custom settings** and click **Next**.	
6.	Click **Primary site** and click **Next**.	
7.	Select the required option for involvement in the Customer Experience Improvement Program and click **Next**.	

Step	Description	Screenshot
8.	Enter the Product Key, if required.	
9.	Enter the location to install the Configuration Manager binaries. **Note** Recommendations for installation paths can be found in section 4.2.	
10.	Enter a **Site code** and **Site name**. Click **Next**.	

Step	Description	Screenshot
11.	Click **Configuration Manager Mixed Mode**. **Note** Information on Configuration Manager Native Mode can be found in section 4.8.2.	
12.	If any client agents will not be used in the Configuration Manager deployment, clear the relevant check boxes, and click **Next**.	
13.	In the top text box, enter the name of the SQL Server computer that will host the Configuration Manager Database and click **Next**. **Note** If the SQL Server is installed using a non-default instance, the instance name must also be provided in the top text box in the format <ServerName>\<InstanceName>.	

Step	Description	Screenshot
14.	Enter the name of the site server computer and click **Next**.	
15.	Ensure that **Install a management point** is selected and enter the name of the server that will be the default management point and click **Next**.	
16.	If using the default port, click **Next**.	

Step	Description	Screenshot
17.	Click **Check for updates and download newer versions to an alternate path** and click **Next**.	
18.	Specify the path and folder where setup can store updated files, and click **Next**. **Note** Setup will download a number of updated files to the temporary directory, which can take some time. If downloads fail due to Internet connectivity issues, start the download again and setup will continue from the last file attempted.	
19.	Click **Next**.	

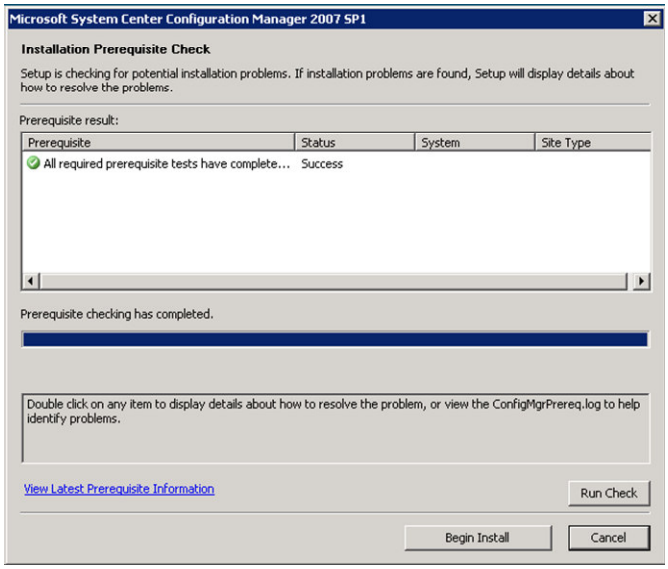
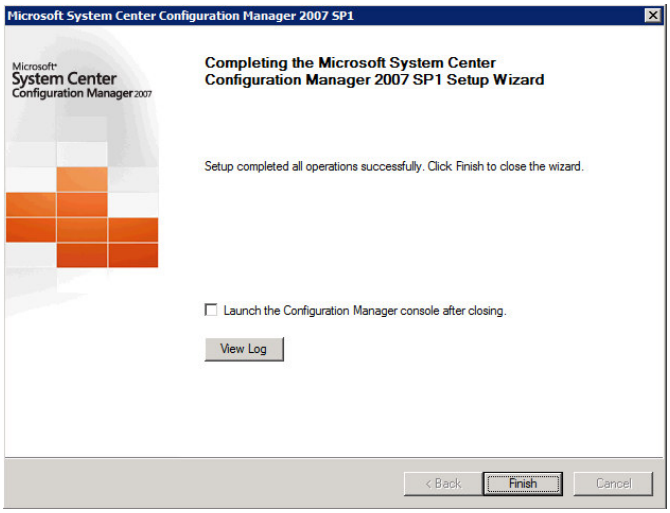
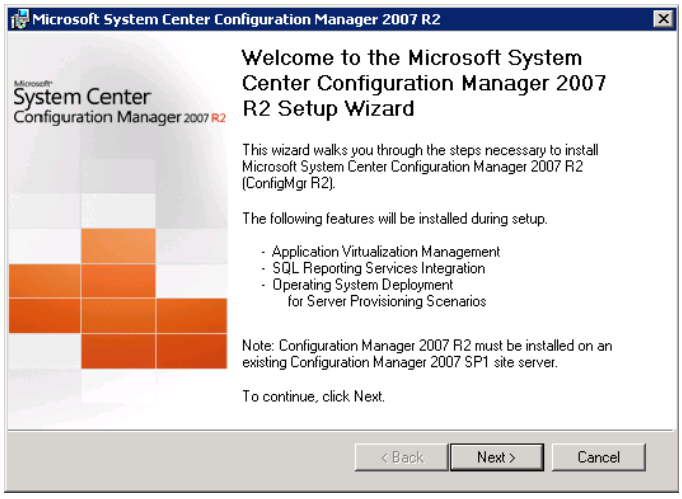
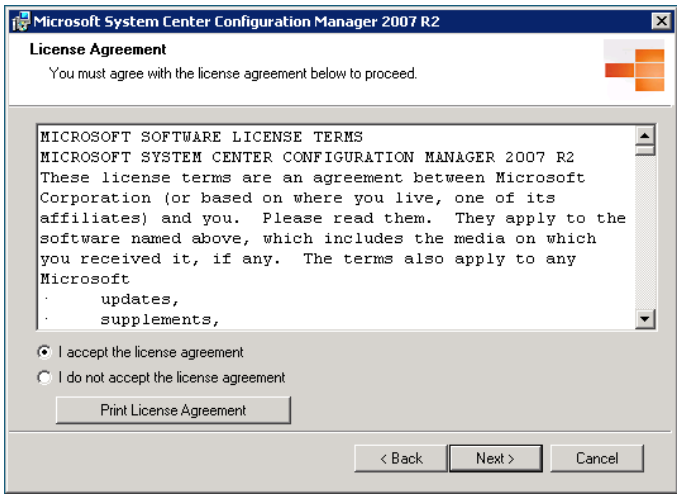
Step	Description	Screenshot
20.	Click **Begin Install**.	
21.	Click **Finish**.	

Table 29: Installing the First Configuration Manager Site

5.2.2.1 Installing Configuration Manager 2007 R2

Once the Configuration Manager 2007 SP1 installation is complete, the healthcare IT Administrator needs to install Configuration Manager 2007 R2. Table 30 shows the steps required to install Configuration Manager 2007 R2:

Step	Description	Screenshot
1.	Run Splash.hta from the Configuration Manager R2 product CD. In the **Start** screen, click **Configuration Manager 2007 R2** under **Install**.	
2.	Click **Next**.	
3.	Read the License Agreement and, if applicable, select **I accept these license terms** and click **Next**.	

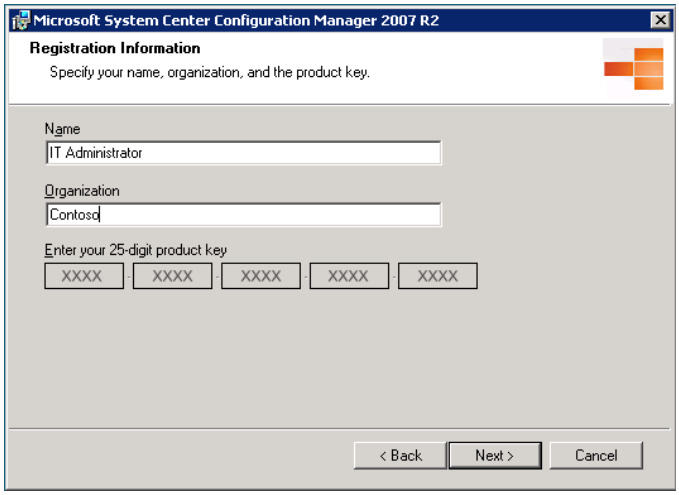
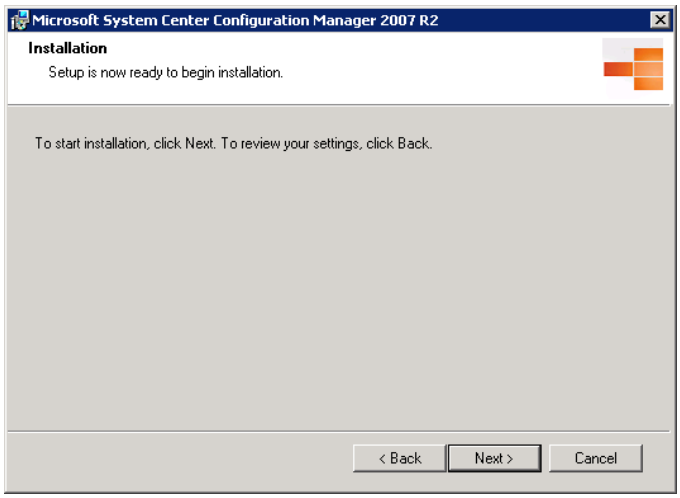
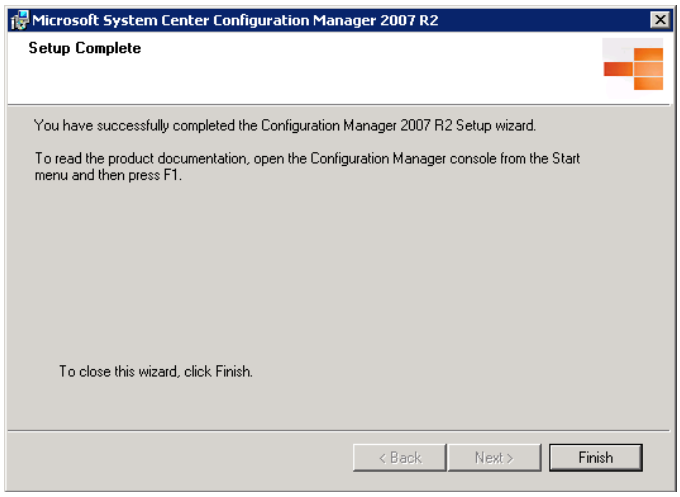
Step	Description	Screenshot
4.	Enter **Name** and **Organization** details and click **Next**.	
5.	Click **Next**.	
6.	Click **Finish**.	

Table 30: Installing Configuration Manager 2007 R2

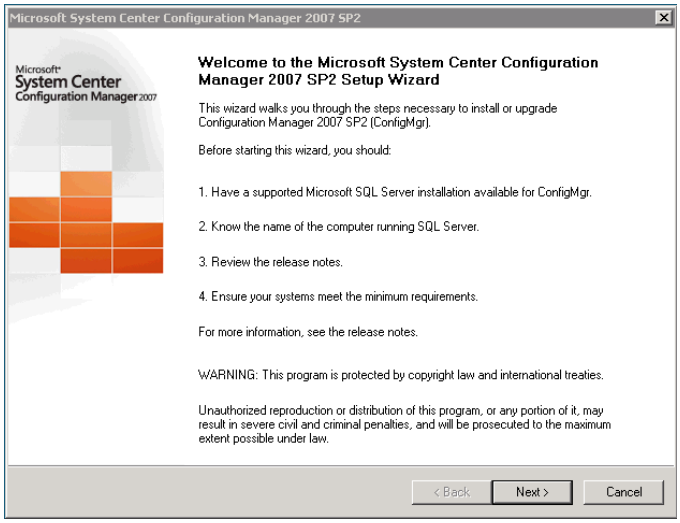
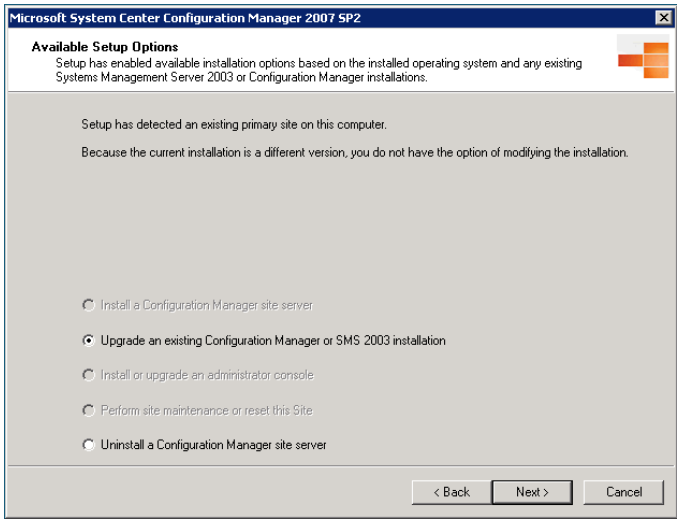
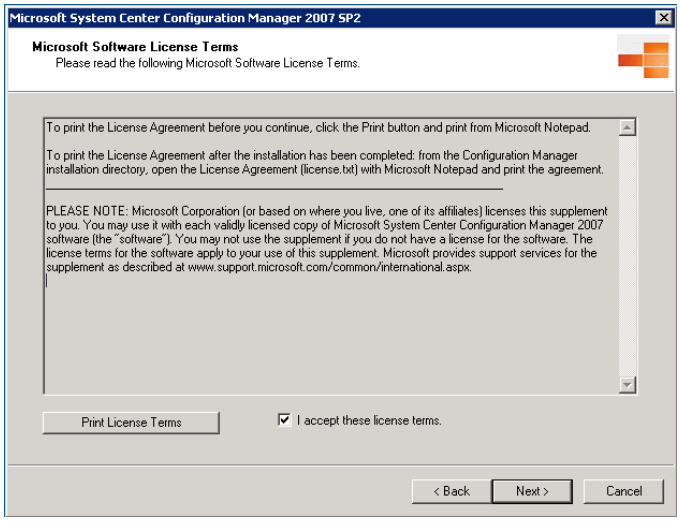
5.2.2.2 Installing Configuration Manager 2007 Service Pack 2

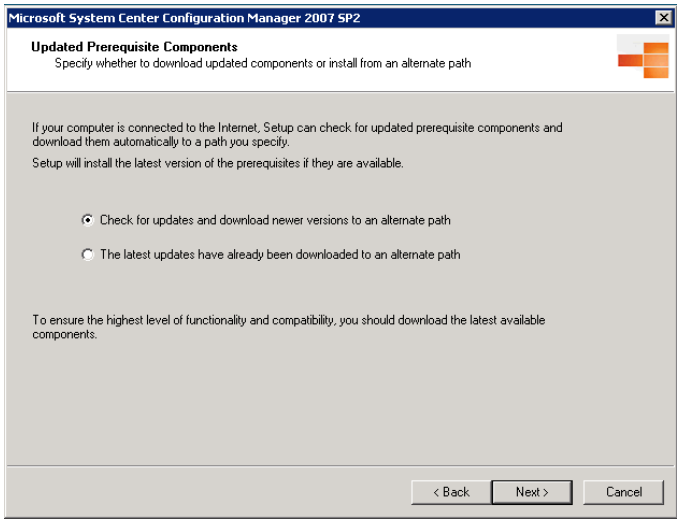
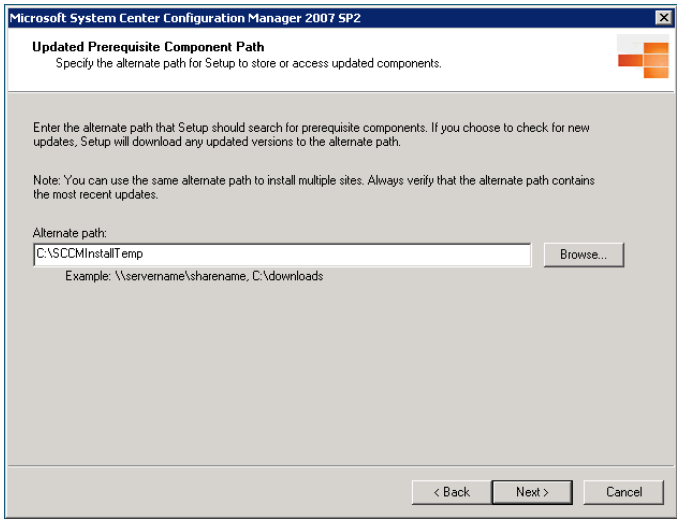
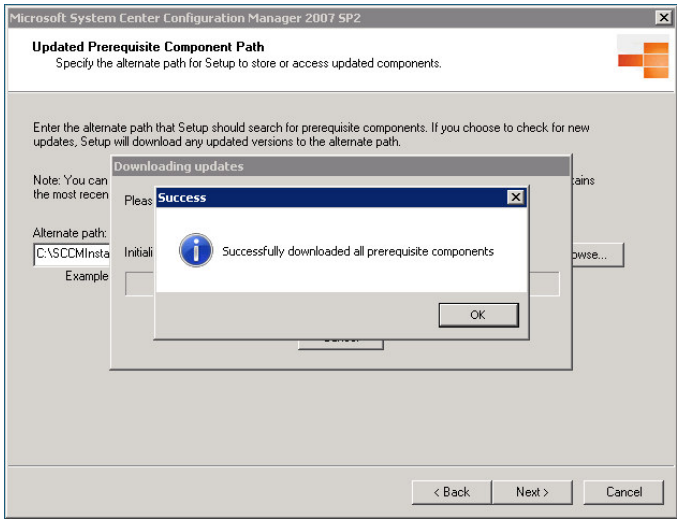
Once the Configuration Manager 2007 R2 setup has completed, the healthcare IT Administrator needs to install the latest Configuration Manager Service Pack. At the time of writing, this was SP2. SP2 can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?FamilyID=3318741a-c038-4ab1-852a-e9c13f8a8140&displaylang=en

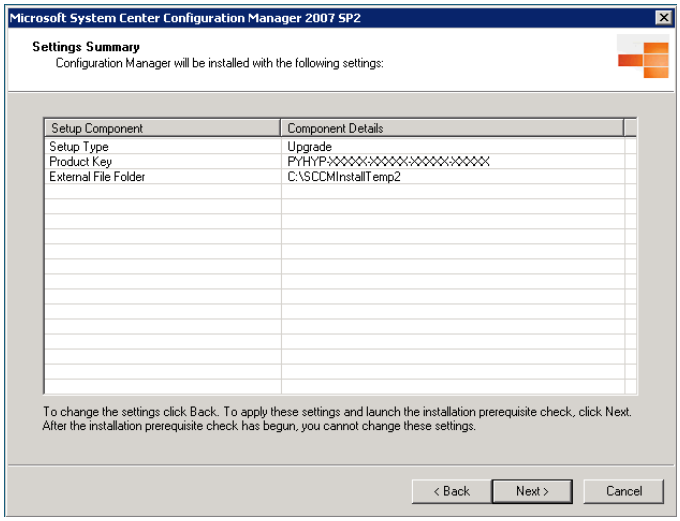
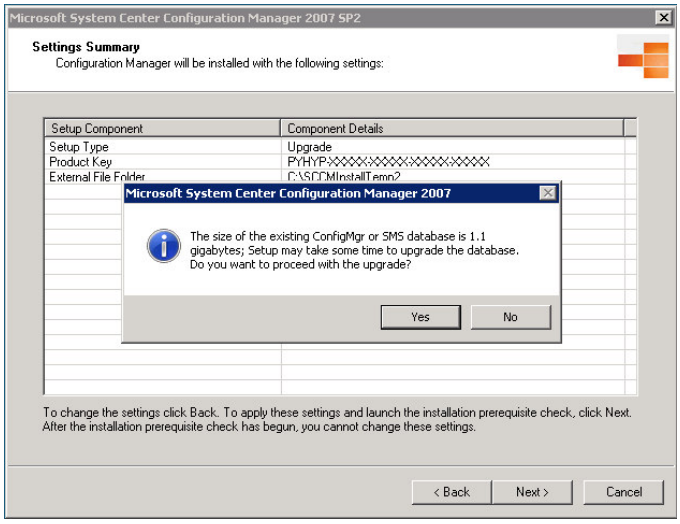
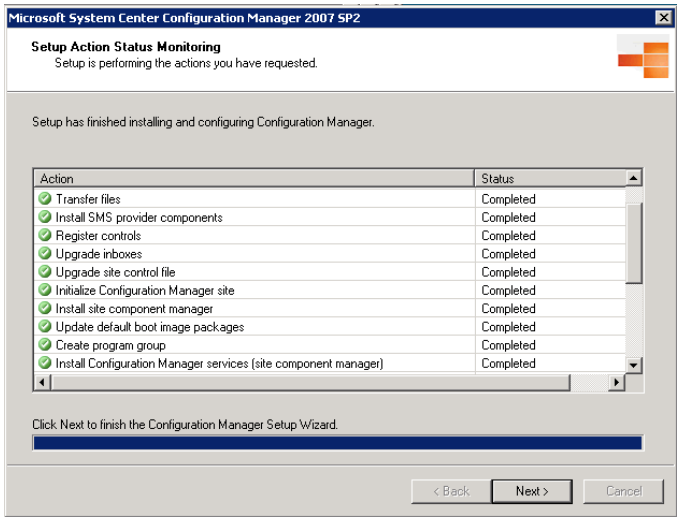
> **Important**
>
> If the Configuration Manager site server is running on the following operating systems, the hotfix detailed in the Knowledge Base article *960037* [32] must be installed prior to the service pack:
>
> - Windows Server 2003 SP1 or SP2 X64
> - Windows Server 2008 SP1 X64
>
> Windows Server 2008 SP2 includes this hotfix, so it is not necessary to install the hotfix if the server already has Windows Server 2008 SP2 installed.

Step	Description	Screenshot
1.	Run Splash.hta from the Configuration Manager SP2 installation folder. In the **Start** screen, click **Configuration Manager 2007 SP2** under **Install**.	

[32] Microsoft Help and Support: When a 32-bit process tries to update a string value with a new value that contains the %ProgramFiles% string, the %ProgramFiles% string is converted to the %ProgramFiles(x86)% string in a 64-bit environment **{R28}**:
http://support.microsoft.com/kb/960037

Step	Description	Screenshot
2.	Click **Next**.	
3.	Click **Upgrade an existing Configuration Manager or SMS 2003 installation** and click **Next**.	
4.	Read the Microsoft Software License Terms and, if applicable, select **I accept these license terms** and then click **Next**.	

Step	Description	Screenshot
5.	Click **Check for updates and download newer versions to an alternate path** and click **Next**.	
6.	Specify the path and folder where setup can store updated files, and click **Next**. **Note** Setup will download a number of updated files to the temporary directory, which can take some time. If downloads fail due to Internet connectivity issues, start the download again and setup will continue from the last file attempted. This must be an empty folder.	
7.	Click **OK** when the download is complete and click **Next**.	

Step	Description	Screenshot
8.	Click **Next**.	
9.	Click **Yes**, and then click **Next**.	
10.	Click **Next**.	

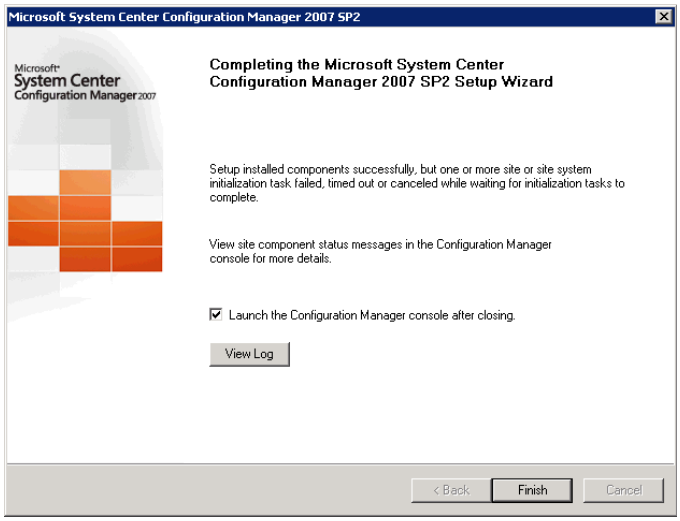
Step	Description	Screenshot
11.	Click **Finish**.	

Table 31: Installing Configuration Manager 2007 SP2

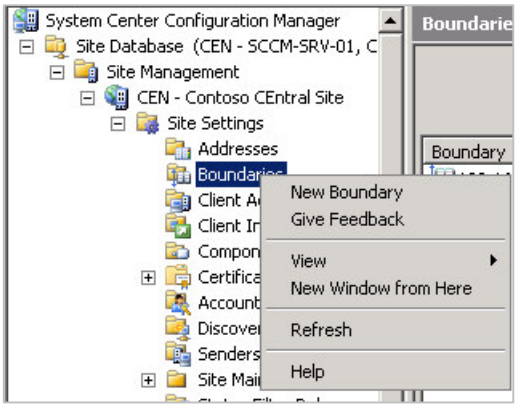
The steps in Table 31 should be followed on every site server. If the healthcare organisation has multiple sites, the service pack needs to be applied first at the central site, then at any child primary sites and finally at any secondary sites.

5.2.3 Configuring the First Configuration Manager Site

There are a large number of configuration settings that healthcare IT Administrators should familiarise themselves with once the product has been installed. Sections 5.2.3.1 to 5.2.3.3 describe the minimum configuration steps required to make Configuration Manager work correctly.

5.2.3.1 Configuring Site Boundaries

As discussed in section 4.5, site boundaries must be configured prior to any clients being installed in the Configuration Manager site. The healthcare IT Administrator should regularly review the boundaries of all sites in the hierarchy to ensure they continue to accurately reflect the healthcare organisation's network. Table 32 shows the process of configuring a boundary for any site in the hierarchy:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** from **Start > Programs > System Center**, right-click on **Boundaries** and select **New Boundary** from the menu displayed.	

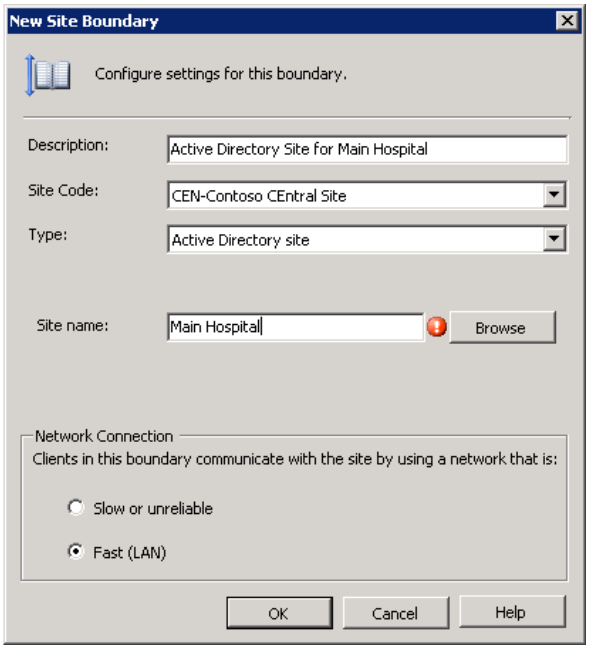
Step	Description	Screenshot
2.	Enter a **Description** for the boundary and specify the **Site Code** to which the boundary will apply. Select the **Type** of boundary (**Active Directory Site, IP Subnet, IPv6 prefix or IP address range**). In the **Network Connection** section, specify if clients within the boundary have fast or slow access to any DPs in the site. Click **OK**.	

Table 32: Configuring Boundaries

5.2.3.2 Configuring Accounts

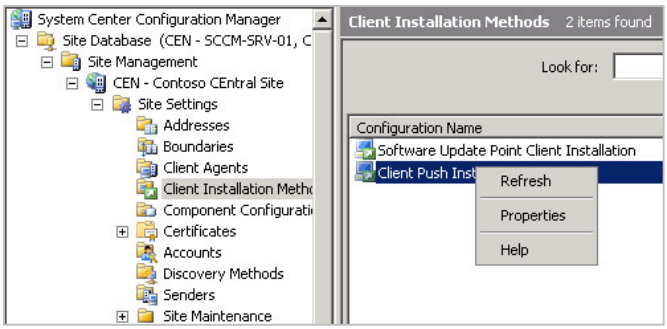
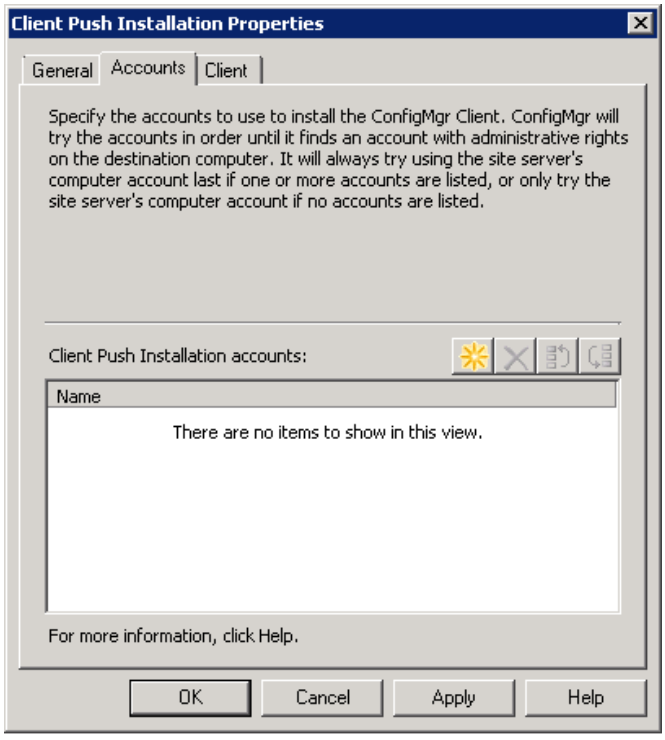
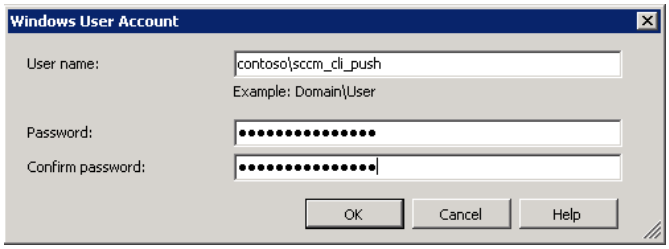
Depending on the features that will be implemented by the healthcare organisation, user accounts may need to be specified, using the Configuration Manager Console, to allow these features to perform as expected. Section 4.8.1 describes the accounts that are required. In order to complete the deployment in a test environment, the following accounts must be configured:

- Client Push Account
- Network Access Account

5.2.3.2.1 Configuring the Client Push Account

If the healthcare IT Administrator intends to use Remote Client Installation, a Client Push Account must be specified. The account must have administrative privileges on machines that will have a client installed using Remote Client Installation. The healthcare IT Administrator can specify multiple accounts that have administrative rights to different sets of machines; Configuration Manager will try each of the accounts in turn until the account can successfully connect to the target machine. If no connection can be made, a status message will be raised. The healthcare IT Administrator can view these messages to determine if any clients did not install to machines because an account has not been specified with appropriate permissions.

Table 33 shows the process for configuring the Client Push Account:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Client Installation Methods** node. In the pane on the right, right-click on **Client Push Installation** and select **Properties**.	
2.	Select the **Accounts** tab. Click the  button to add a Client Push Account.	
3.	Enter the details of the Client Push Account and click **OK**.	

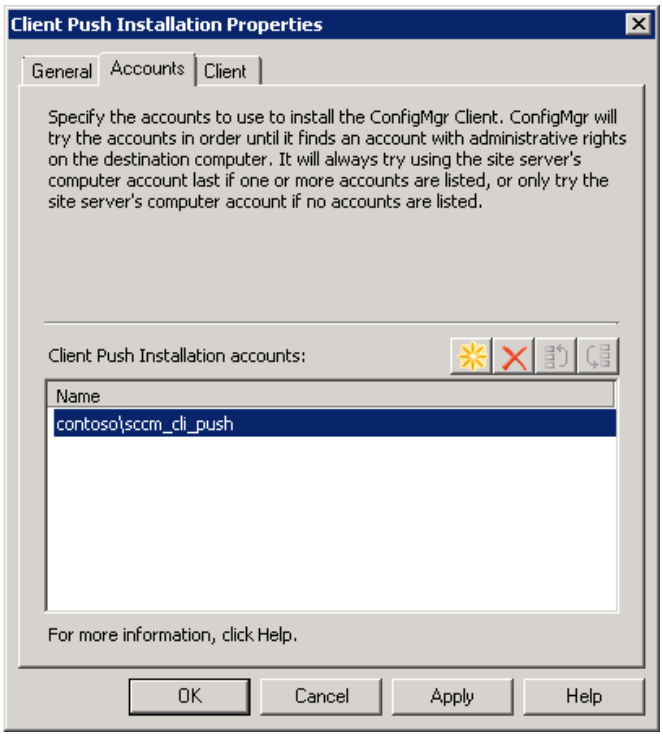
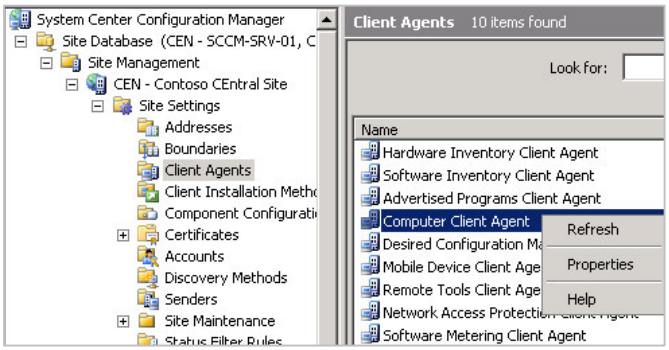
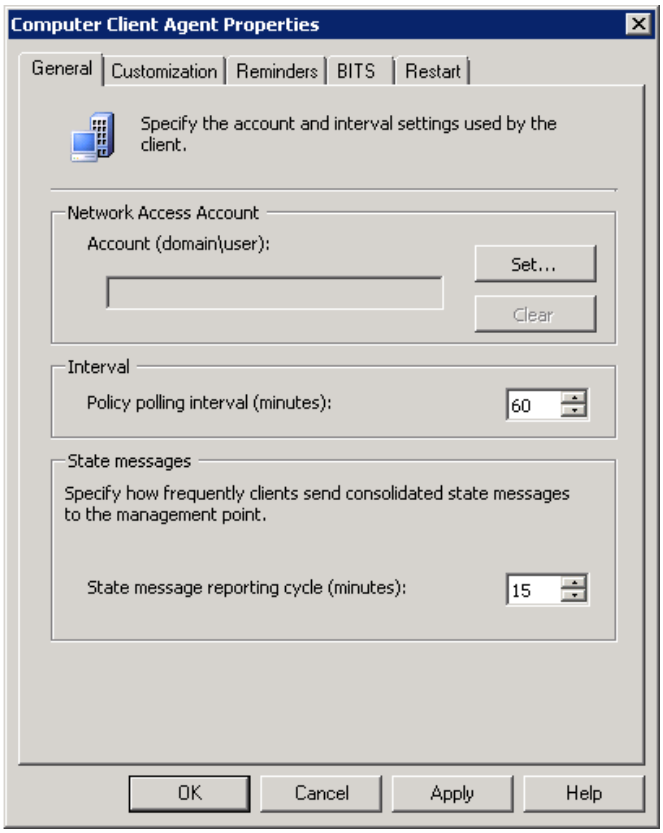
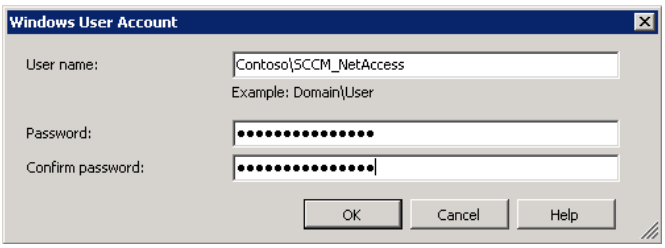
Step	Description	Screenshot
4.	Repeat steps 2 and 3 for any additional accounts that need to be added. Click **OK**.	

Table 33: Configuring the Client Push Account

5.2.3.2.2 *Configuring the Network Access Account*

The Network Access Account is required if the healthcare organisation intends to use the Operating System Deployment feature of Configuration Manager, or if any clients to be managed by the infrastructure are part of an un-trusted Active Directory forest or Workgroup. Table 34 shows the process for configuring the Network Access account:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Client Agents** node. In the right pane, right-click on **Computer Client Agent** and select **Properties**.	

Step	Description	Screenshot
2.	In the **Network Access Account** section, click **Set**.	
3.	Enter the details of the Network Access Account and click **OK**.	

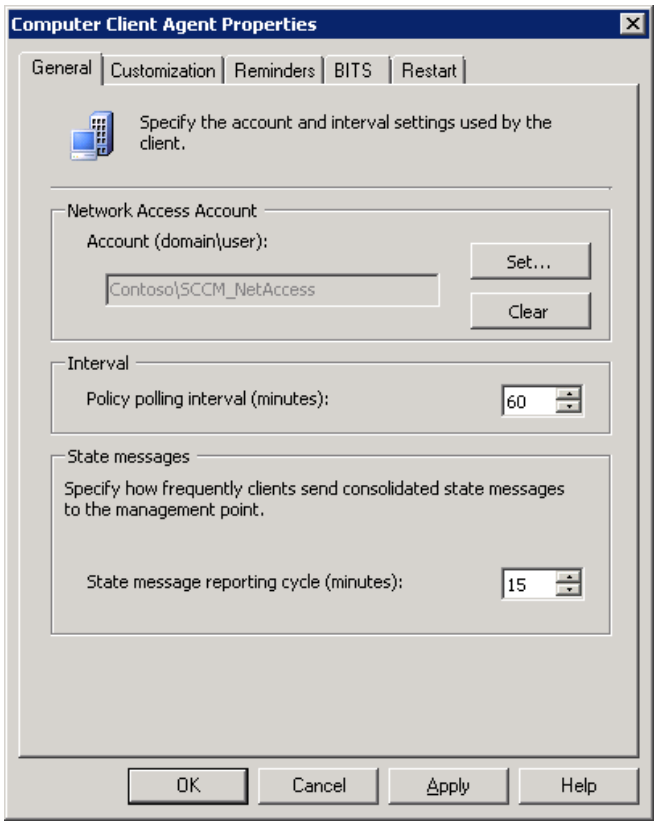
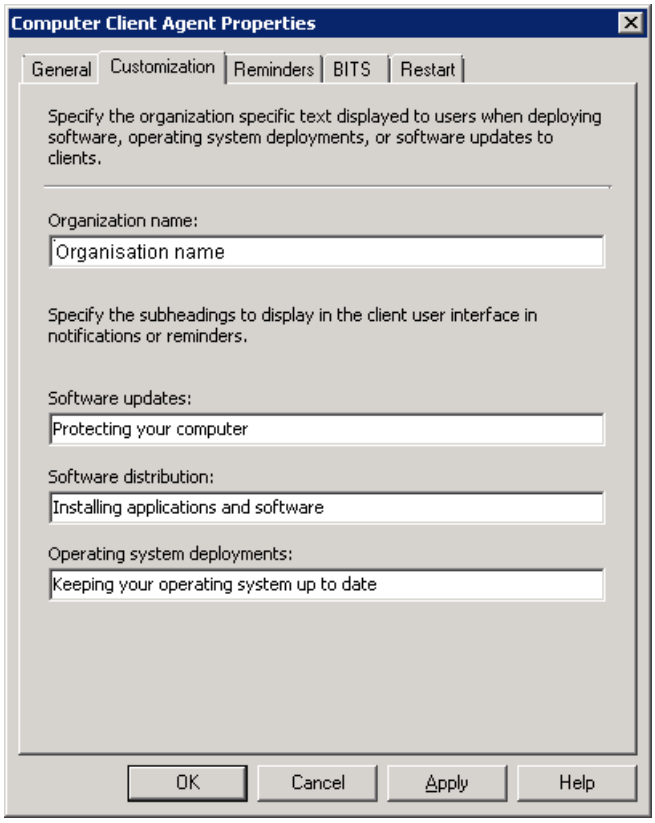
Step	Description	Screenshot
4.	Click **OK** again.	
5.	**Tip** This is not a required step. The healthcare IT Administrator can customise the messages that are presented to users when software updates, software distribution tasks or operating system deployment tasks run, by modifying the text in the **Customization** tab. Click **OK**.	

Table 34: Configuring the Network Access Account

5.2.3.3 Configuring Discovery Methods

As described in section 4.6, Configuration Manager provides a number of different discovery options to allow the healthcare IT Administrator to automate the discovery of client computers, users and user groups within the healthcare organisation. Sections 5.2.3.3.1 to 5.2.3.3.6 describe how to enable the various discovery methods for use in the healthcare organisation.

5.2.3.3.1 Active Directory Security Group Discovery

This discovery method allows the healthcare IT Administrator to create discovery information for:

- Local groups
- Global Groups
- Universal Groups
- Nested Groups

Use Active Directory Security Group Discovery to discover user groups that need to be categorised into Configuration Manager collections. For example, if there is a need to distribute software to users in a specific security group, the security group can be added to a collection. Software packages can then be advertised to only that collection, so that only the appropriate users receive it.

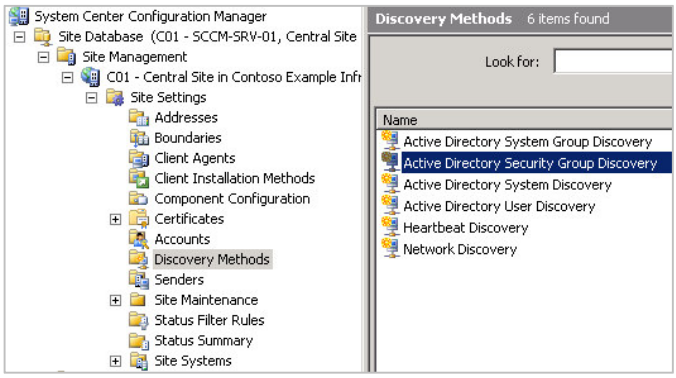
Polling performed by Active Directory Security Group Discovery can generate significant network traffic; therefore, discovery should be scheduled to occur at times when this network traffic does not adversely affect network use.

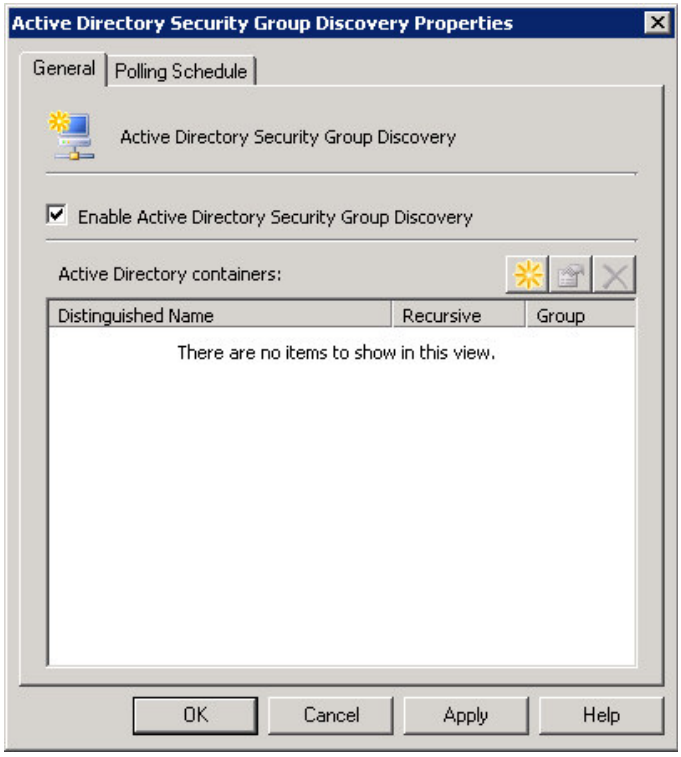
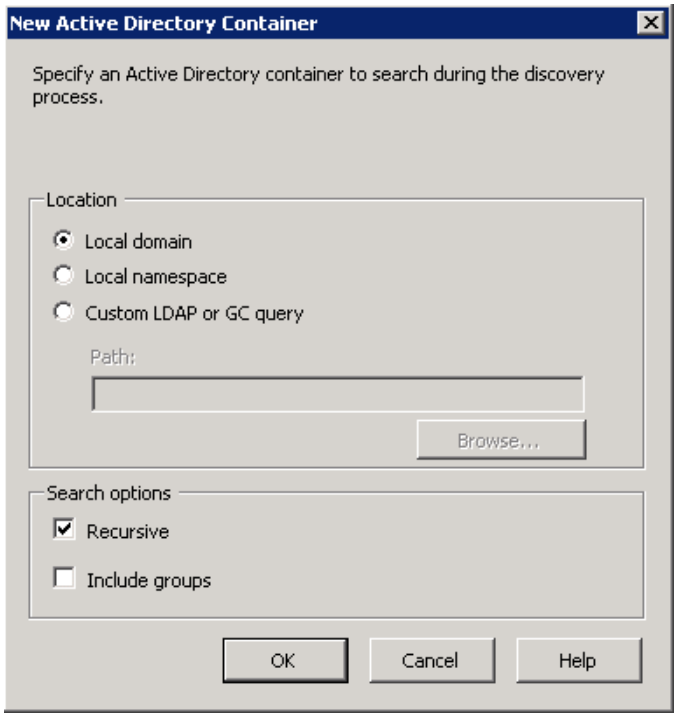
Table 35 shows the Active Directory Security Group Discovery method targets:

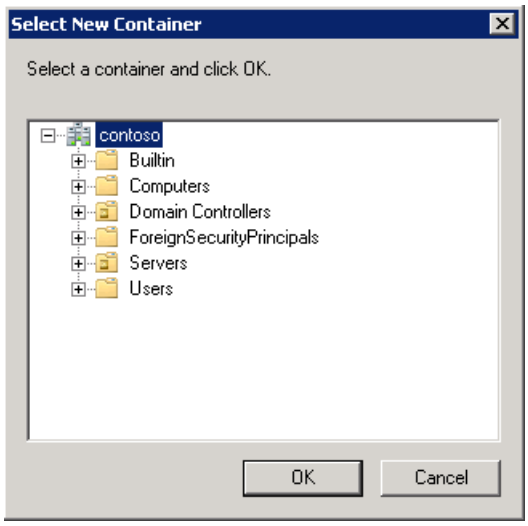
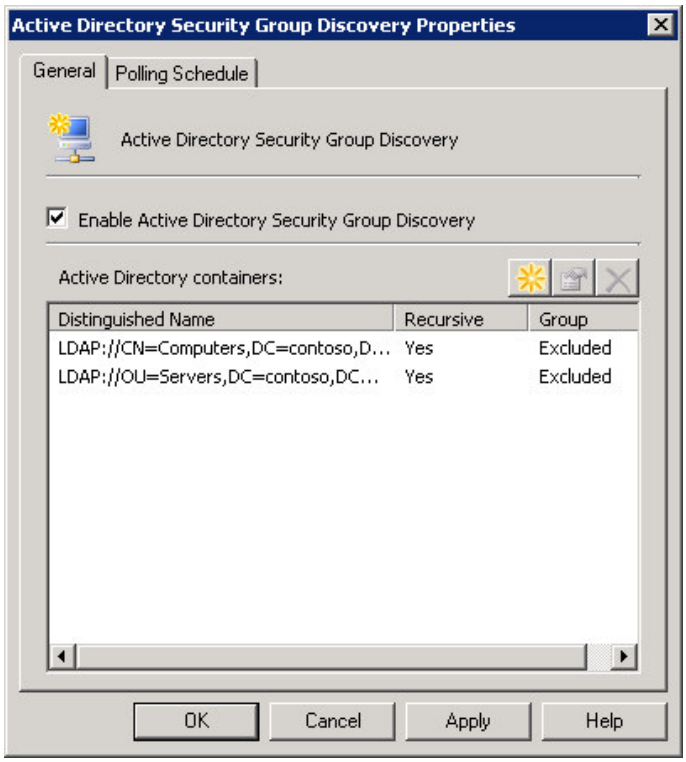
Target Directory Location	Target Site to Run Discovery	Recommended Setting
Configure so that only required objects are returned, by targeting the closest level to the user group objects, for example, the OU or container that contains the user groups required. More than one query can be added, if required.	Active Directory Security Group Discovery must only be enabled on the lowest level Primary sites in the hierarchy.	Enable only if there is a requirement to target software based on user group membership.

Table 35: Active Directory Security Group Discovery Targeting

Table 36 shows the steps involved in enabling the Active Directory Security Group Discovery method:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Discovery Methods** node. In the right pane, right-click on the **Active Directory Security Group Discovery** component and select **Properties**.	

Step	Description	Screenshot
2.	Select **Enable Active Directory Security Group Discovery**. Click the  button to add a search location.	
3.	Select **Local domain** as the location and accept the other default settings. Click **OK**.	

Step	Description	Screenshot
4.	Select the container that contains the user groups that Configuration Manager will discover. Click **OK**.	
5.	Repeat steps 2 to 4 for each container to be searched.	

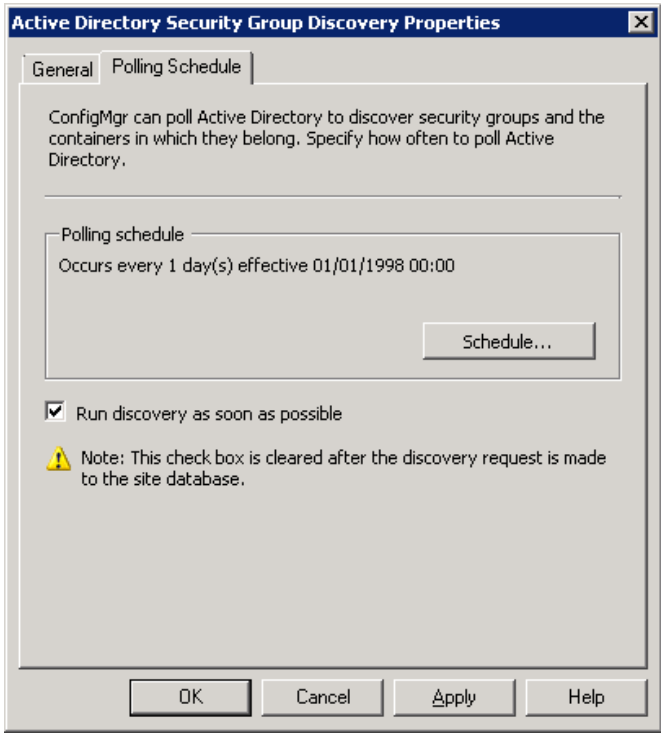
Step	Description	Screenshot
6.	Click the **Polling Schedule** tab. Select **Run discovery as soon as possible**. Click **Schedule** to specify an ongoing schedule for the discovery process. Click **OK**.	

Table 36: Configuring Active Directory Security Group Discovery

The progress of the discovery process can be monitored by looking at the log file <Configuration Manager installation folder>\Logs\Adsgdis.log. Once the discovery records have been processed by Configuration Manager, they will be shown in the Configuration Manager Console within the 'All User Groups' collection, and any other collection that is appropriate for the type of resource.

To view the discovery information that has been gathered for a computer, either double-click the computer from within the Configuration Manager Console or right-click on the computer in the Console and select **Properties**.

5.2.3.3.2 Active Directory System Discovery

Use the Active Directory System Discovery method to discover the following:

- Computer name
- Active Directory container name
- IP address
- Assigned Active Directory site

Do not plan to use Active Directory System Discovery to discover the client operating system. There are other discovery methods, such as Network Discovery, that will do this.

> **Caution**
>
> Polling performed by Active Directory System Discovery can generate significant network traffic (approximately 5 KB per client computer). For this reason, plan to schedule the discovery to occur at a time when this network traffic does not adversely affect network use.

Active Directory System Discovery is used mainly for Configuration Manager client installation. Once the Configuration Manager client is installed, all information provided by Active Directory System Discovery is provided directly by Heartbeat Discovery.

Because Configuration Manager polls Active Directory, instead of being notified of Active Directory changes, the Configuration Manager resources obtained from Active Directory do not necessarily reflect the current Active Directory resources at all times. Computers might have been added, removed, or changed in Active Directory since the most recent poll.

Table 37 shows the Active Directory System Discovery method targets:

Target Directory Location	Target Site to Run Discovery	Recommended Setting
Configure so that only required objects are returned, by targeting the closest level to the computer objects, for example, the OU or container that contains the computers required. More than one query can be added if required.	Active Directory System Discovery must only be enabled on the lowest level Primary sites in the hierarchy.	Enabled. This should be enabled, and scheduled according to the frequency with which new systems are added to the domain.

Table 37: Active Directory System Discovery Targeting

Discovering Custom Active Directory Attributes

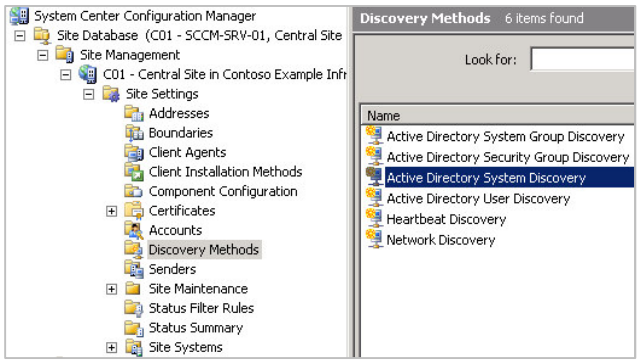
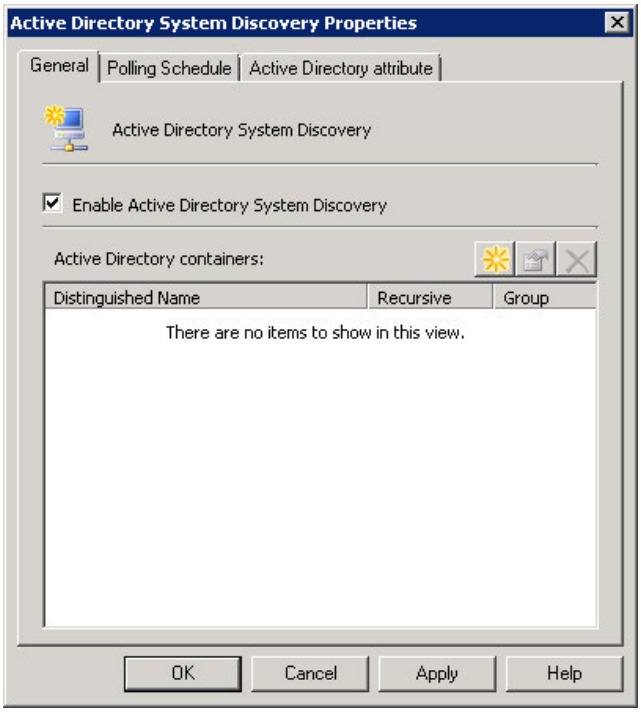
The set of Active Directory attributes that Configuration Manager discovers during an Active Directory System Discovery can be extended to include additional attributes. Table 38 below lists the default attributes that are discovered.

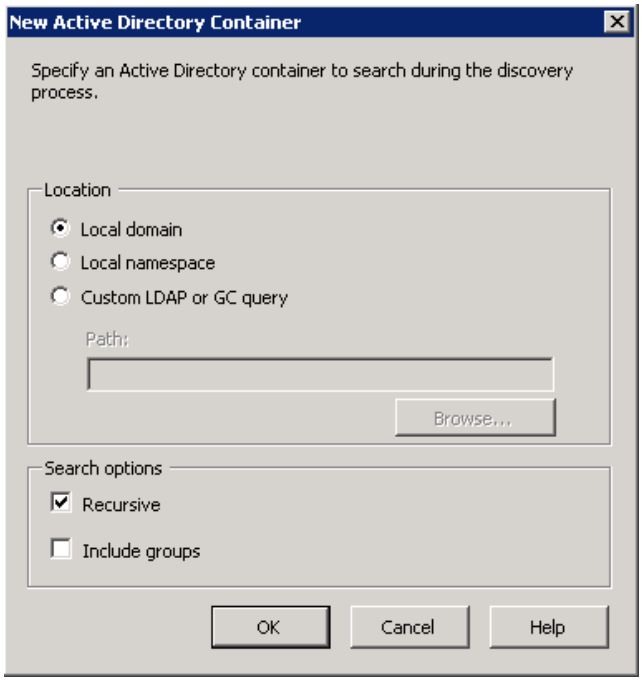
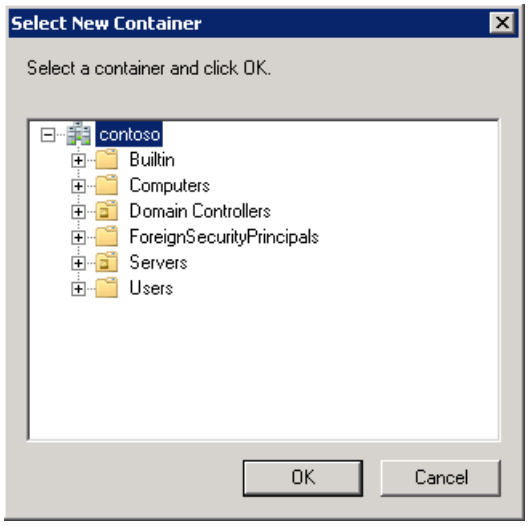
> **Note**
>
> An attribute has to be associated with the *computer* class in Active Directory in order to be available for this discovery method.

Type	Attribute
Default (non-configurable)	ADsPath
	canonicalName
	dNSHostName
	Domain
	memberOf
	Name
	objectClass
	objectGUID
	objectSID
	operatingSystem
	primaryGroupID
	sAMAccountName

Table 38: Custom Attributes for Active Directory System Discovery

Table 39 shows the steps involved in enabling the Active Directory System Discovery method:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Discovery Methods** node. In the right pane, right-click on the **Active Directory System Discovery** component and select **Properties.**	
2.	Select **Enable Active Directory System Discovery**. Click the  button to add a search location.	

Step	Description	Screenshot
3.	Select **Local domain** as the location and accept the other default settings. Click **OK**.	
4.	Select the container that contains the computers that Configuration Manager will discover. **Note** It is good practice to be as specific as possible when specifying the container. It is possible to specify more than one location and, by default, any sub-containers are also searched. Click **OK**.	

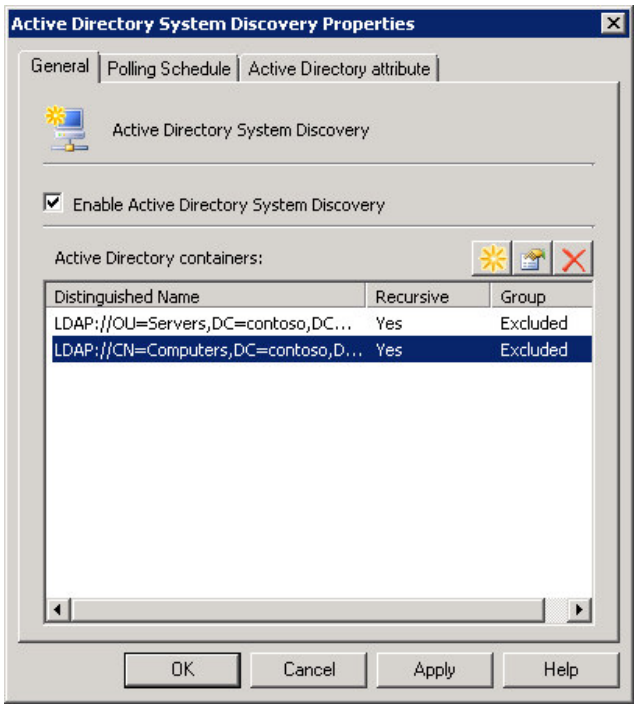
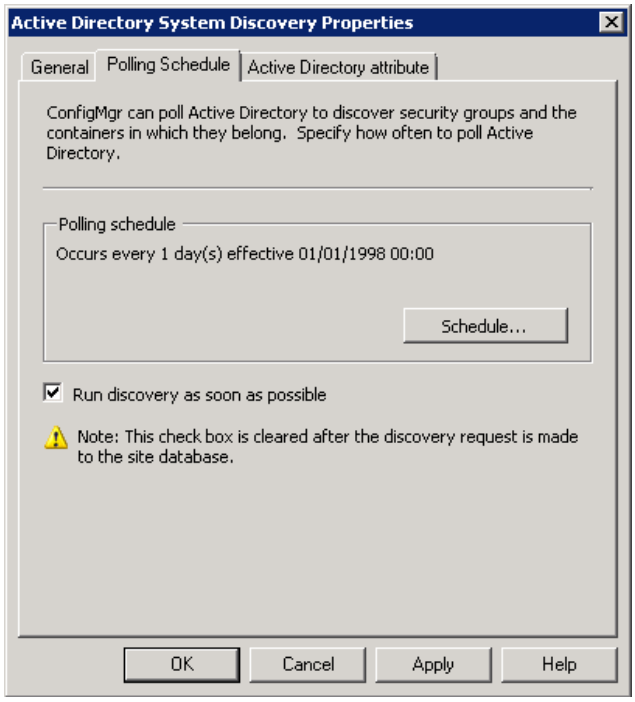
Step	Description	Screenshot
5.	Repeat steps 2 to 4 for each container to be searched.	
6.	Click the **Polling Schedule** tab. Select **Run discovery as soon as possible**. Click **Schedule** to specify an ongoing schedule for the discovery process. Click **OK**. **Tip** Additional attributes can be discovered from Active Directory using the **Active Directory attribute** tab.	

Table 39: Configuring Active Directory System Discovery

The progress of the discovery process can be monitored by looking at the log file <Configuration Manager installation folder>\Logs\Adsysdis.log. Once the discovery records have been processed by Configuration Manager, they will be shown in the Configuration Manager Console within the 'All System' collection, and any other collection that is appropriate for the type of resource. Only very basic information is gathered as part of the discovery process and, as such, machines may not appear within the appropriate collections until the Configuration Manager client is installed and the inventory information has been processed by the Configuration Manager site server.

To view the discovery information that has been gathered for a computer, either double-click the computer from within the Configuration Manager Console or right-click on the computer in the Console and select **Properties**.

5.2.3.3.3 Active Directory System Group Discovery

Use the Active Directory System Group Discovery method to discover the following:

- Organizational units
- Global groups
- Universal groups
- Nested groups
- Non-security groups (Distribution Groups)

Active Directory System Group Discovery can be run only on primary sites. It polls Active Directory for all system resources in the Configuration Manager database, including those discovered at child sites, and including secondary sites. Because Active Directory System Group Discovery does not contact the computers directly, the computers do not have to be turned on to be discovered.

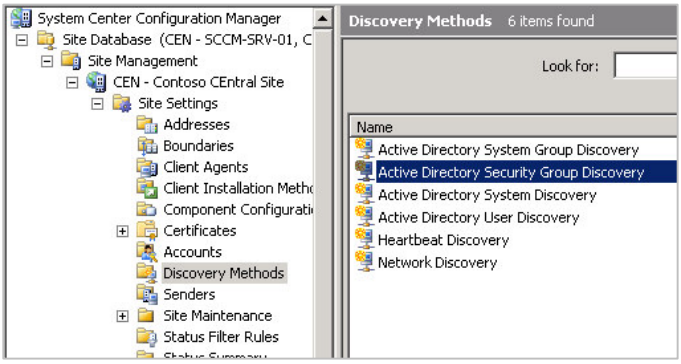
Polling performed by Active Directory System Group Discovery can generate significant network traffic; schedule the discovery to occur at times when this network traffic does not adversely affect network use.

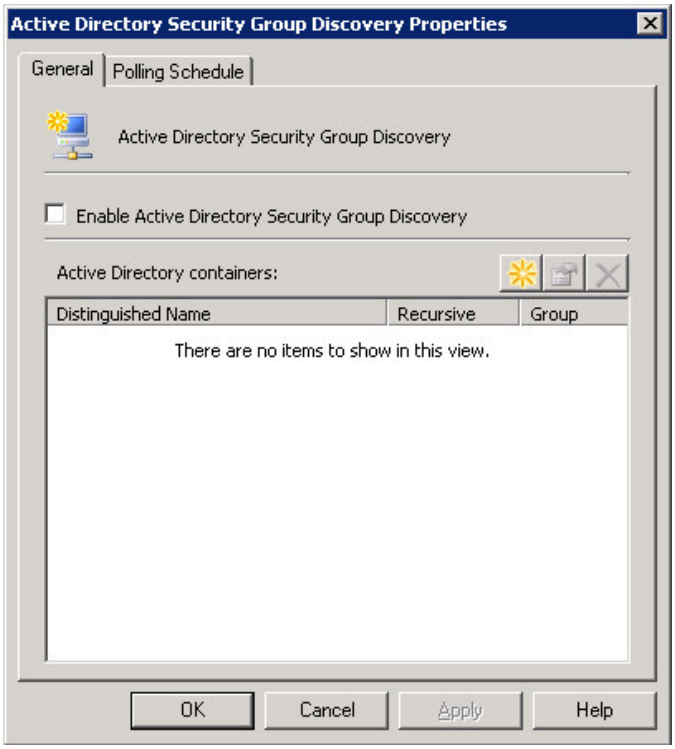
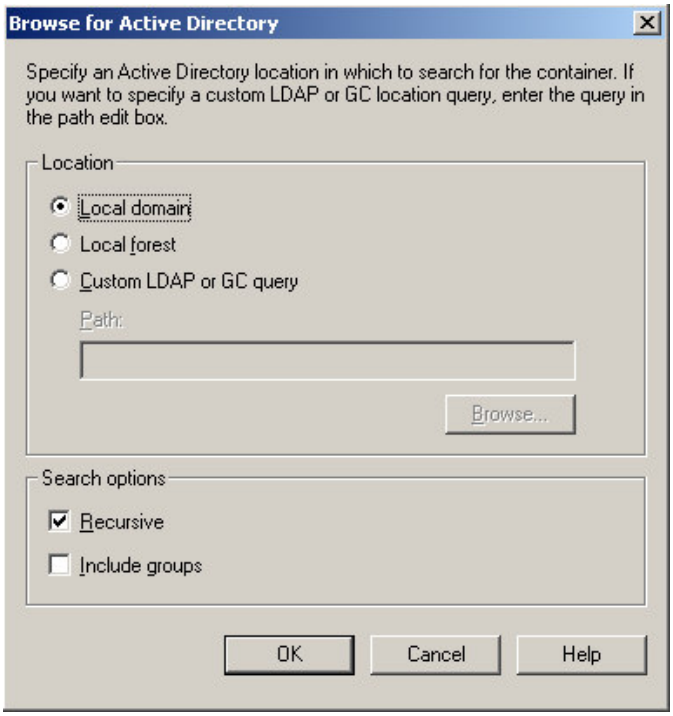
Table 40 shows the Active Directory System Group Discovery method targets:

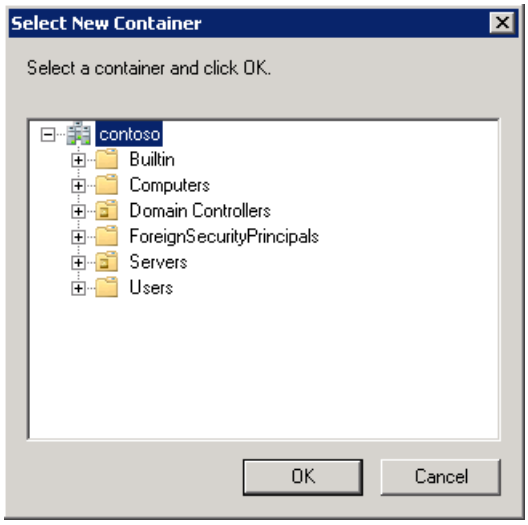
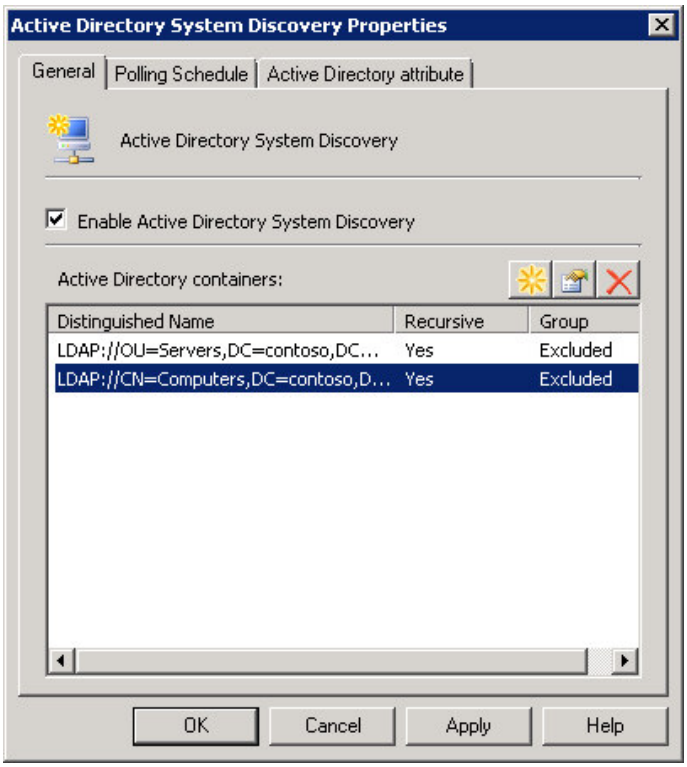
Target Directory Location	Target Site to Run Discovery	Recommended Setting
Configure the container(s) that contain the computers that have already been discovered by the Active Directory System Discovery method. More than one query can be added, if required.	Active Directory System Group Discovery must be enabled on all Primary Sites that have any Configuration Manager clients assigned.	Only enabled if targeting of systems based on OU or security group is required.

Table 40: Active Directory System Group Discovery Targeting

Table 41 shows the steps involved in enabling the Active Directory System Group Discovery method:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Discovery Methods** node. In the right pane, right-click on the **Active Directory System Group Discovery** component and select **Properties**.	

Step	Description	Screenshot
2.	Select **Enable Active Directory System Group Discovery**. Click the  button to add a search location.	
3.	Select **Local domain** as the location and accept the other default settings. Click **OK**.	

Step	Description	Screenshot
4.	Select the container that contains the computers that Configuration Manager will discover. **Note** Ensure that the container(s) that contain the computers that have already been discovered by the Active Directory System Discovery method are specified. Click **OK**.	
5.	Repeat steps 2 to 4 for each container to be searched.	

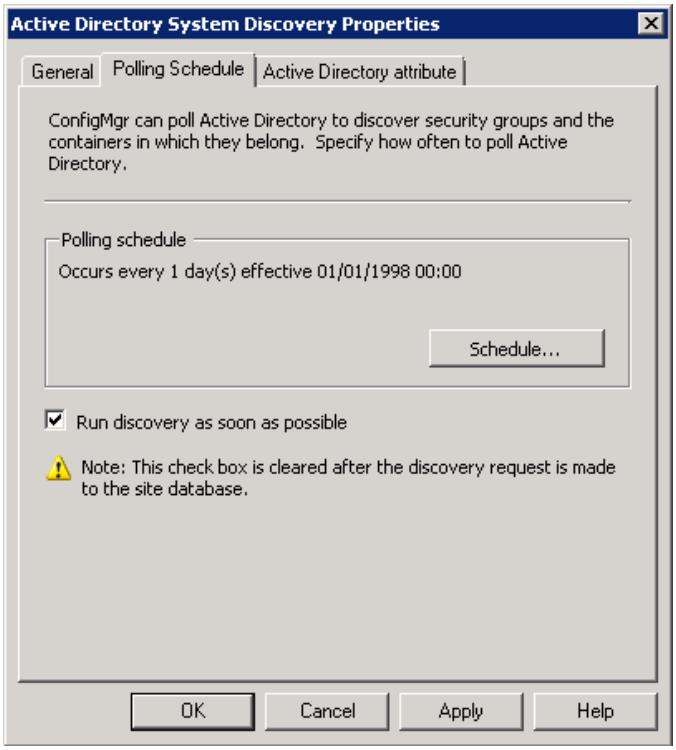
Step	Description	Screenshot
6.	Click the **Polling Schedule** tab. Select **Run discovery as soon as possible**. Click **Schedule** to specify an ongoing schedule for the discovery process. Click **OK**.	

Table 41: Configuring Active Directory System Group Discovery

To monitor the progress of the discovery, or to verify that the discovery process ran successfully, review the log file <Configuration Manager installation folder>\Logs\Adsysgrp.log. Also, look at the individual records from the administrator console to verify that the additional discovery information has been appended. To view the discovery details, either double-click a resource from within the All Systems collection in the Configuration Manager Console, or right-click on the computer in the Console and select **Properties**.

5.2.3.3.4 Active Directory User Discovery

Use the Active Directory User Discovery method to discover the following:

- User name
- Unique user name (includes domain name)
- Active Directory domain
- Active Directory container name
- User groups (except empty groups)

Use this discovery method to discover accounts that are required to be categorised into Configuration Manager collections. For example, if there is a need to distribute software to collections of users, use this discovery method to determine which users are in the Active Directory domains. If the healthcare organisation has users that require a specific software package, those user accounts can be discovered, and a collection can be created containing those accounts. Software packages can then be advertised to that collection exclusively, so that only the appropriate users receive it.

Polling performed by Active Directory User Discovery can generate significant network traffic, although it generates less traffic per resource than Active Directory System Discovery. Plan to schedule the discovery to occur at times when this network traffic does not adversely affect network use.

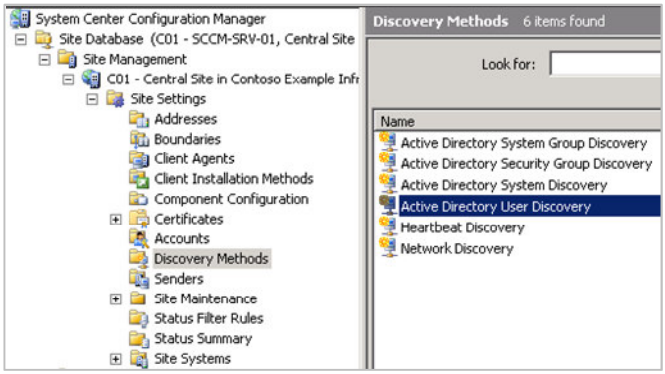
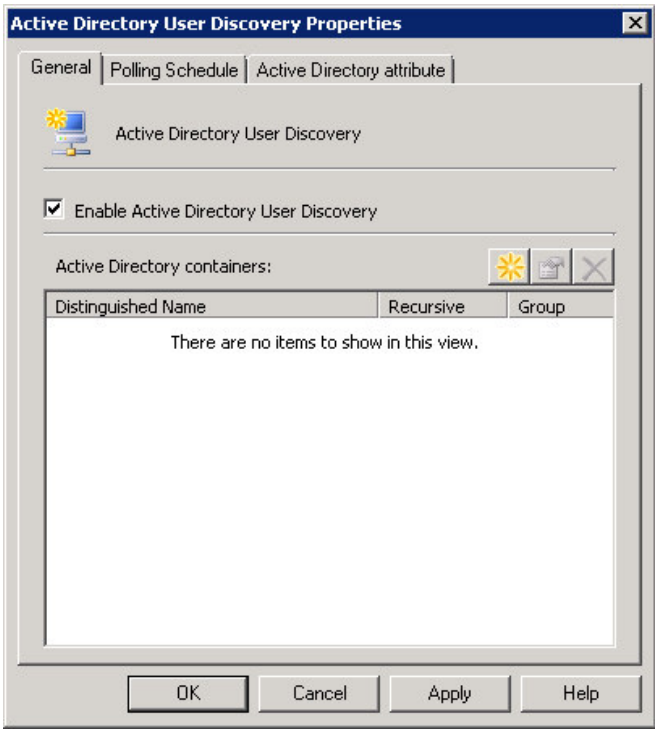
Also, because Configuration Manager polls Active Directory, the Configuration Manager resources that are obtained from Active Directory do not necessarily reflect the current Active Directory resources at all times. Users might have been added, removed, or changed in Active Directory, since the most recent poll.

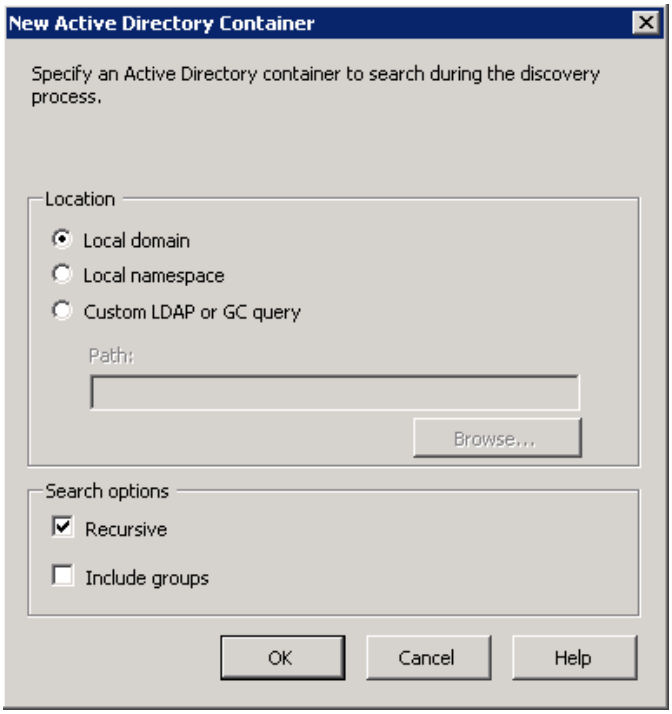
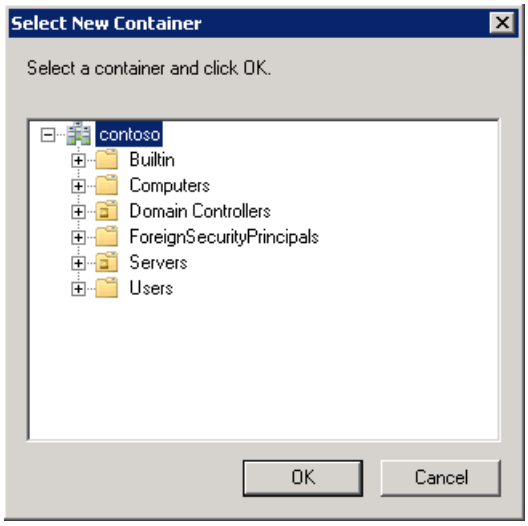
Table 42 shows the Active Directory User Discovery method targets:

Target Directory Location	Target Site to Run Discovery	Recommended Setting
Configure so that only required objects are returned, by targeting the closest level to the user objects, for example, the OU or container that contains the users required. More than one query can be added, if required.	Active Directory Security Group Discovery must only be enabled on the lowest level Primary sites in the hierarchy.	Disabled. This should be disabled unless specifically required.

Table 42: Active Directory User Discovery Targeting

Table 43 shows the steps involved in enabling the Active Directory User Discovery method:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Discovery Methods** node. In the right pane, right-click on the **Active Directory User Discovery** component and select **Properties**.	
2.	Select **Enable Active Directory User Discovery**. Click the  button to add a search location.	

Step	Description	Screenshot
3.	Select **Local domain** as the location and accept the other default settings. Click **OK**.	
4.	Select the container that contains the users that Configuration Manager will discover. **Note** It is good practice to be as specific as possible when specifying the container. It is possible to specify more than one location, and, by default, any sub-containers are also searched. Click **OK**.	

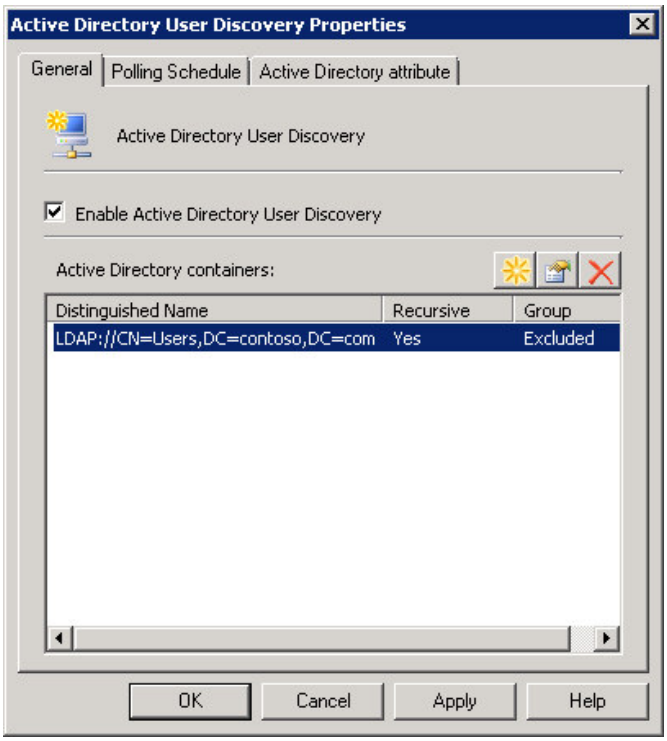
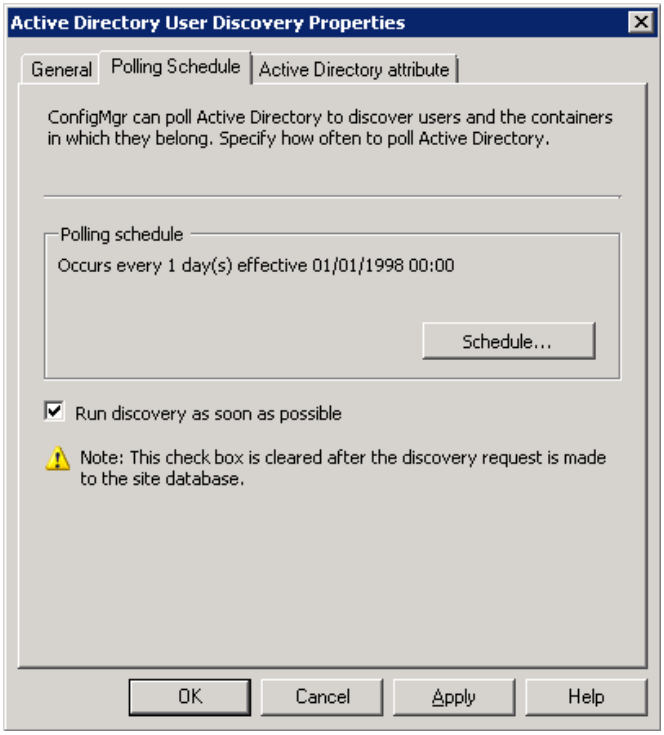
Step	Description	Screenshot
5.	Repeat steps 2 to 4 for each container to be searched.	
6.	Click the **Polling Schedule** tab. Select **Run discovery as soon as possible**. Click **Schedule** to specify an ongoing schedule for the discovery process. Click **OK**. **Tip** Additional attributes can be discovered from Active Directory using the **Active Directory attribute** tab.	

Table 43: Configuring Active Directory User Discovery

The progress of the discovery process can be monitored by looking at the log file <Configuration Manager installation folder>\Logs\Adusrdis.log. Once the discovery records have been processed by Configuration Manager, they will be shown in the Configuration Manager Console within the 'All Users' collection, and any other collection that is appropriate for the type of resource.

To view the discovery information that has been gathered for a computer, either double-click the computer from within the Configuration Manager Console, or right-click on the computer in the Console and select **Properties**.

> **Note**
>
> Collections will only update their contents according to the update schedule specified for the collection. Therefore, it may be necessary to right-click on the collection and select **Update Collection Membership** to populate the collection members.

5.2.3.3.5 Heartbeat Discovery

This method is used to refresh Configuration Manager client computer discovery data in the Configuration Manager site database. If Heartbeat Discovery is disabled, the discovery data is refreshed only when another discovery method is invoked or run on a schedule. Heartbeat Discovery is useful for maintaining current discovery data on clients that are not usually affected by one of the other discovery methods, such as a server that users seldom log on to. By default, this discovery method is enabled and set to run every week.

> **Note**
>
> It is recommended that this method is kept enabled. There is no scheduling for a particular day and time: the Configuration Manager client will invoke a Heartbeat Discovery if it determines that the time since the method was last run is greater than the configured rediscovery period (1 week by default).

5.2.3.3.6 Network Discovery

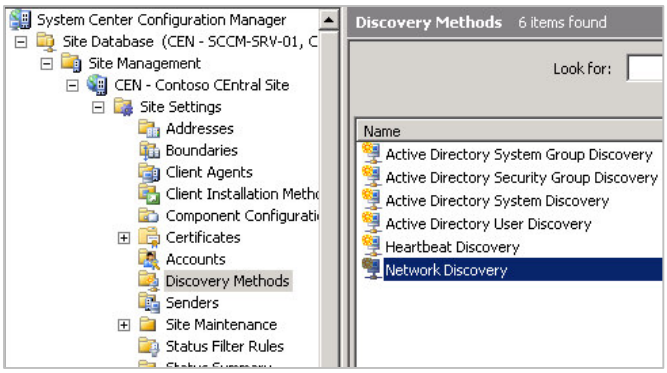
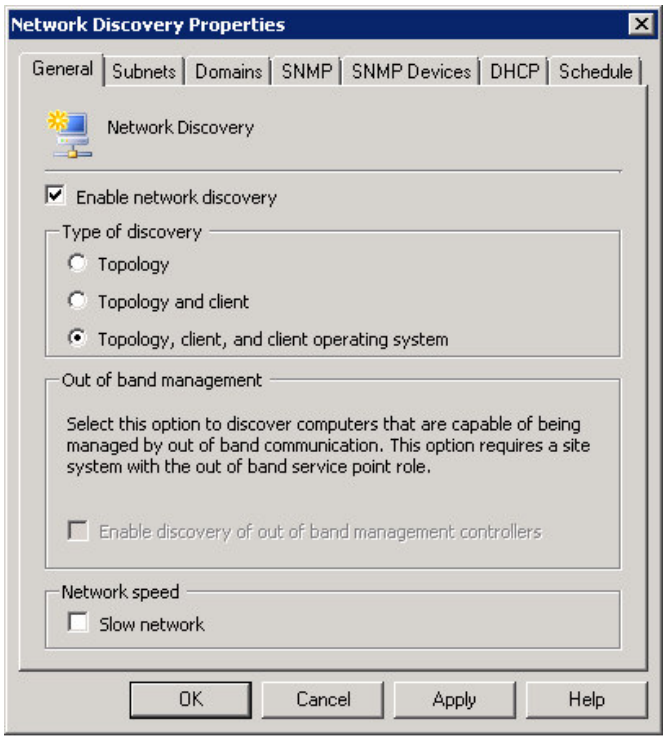
The Configuration Manager Network Discovery method searches for network resources by polling the network for any resources with an IP Address. This means that not only computers, but also printers, routers, bridges, and so on, can be discovered. By default, only the subnet and local domain on which the site server resides are searched, but discovery can be configured to search other subnets and domains throughout the healthcare organisation's network, using DHCP, SNMP or other mechanisms.

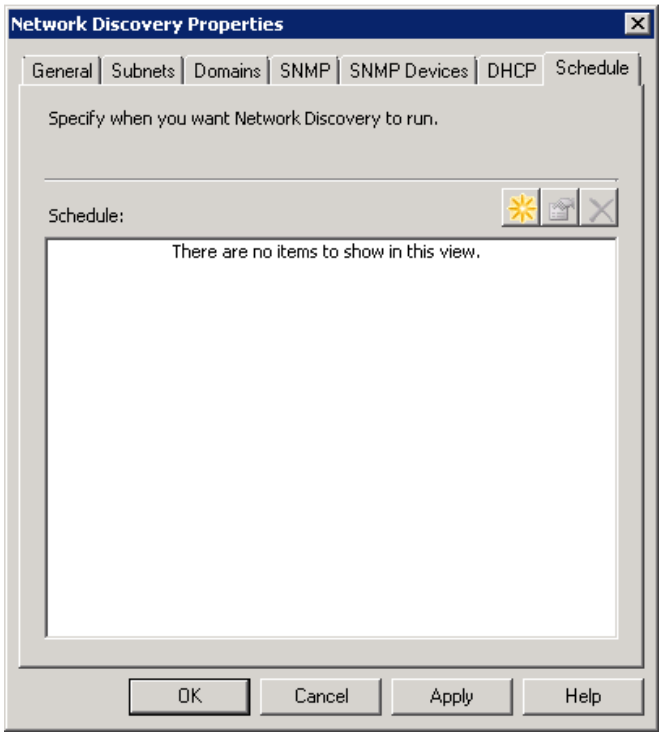
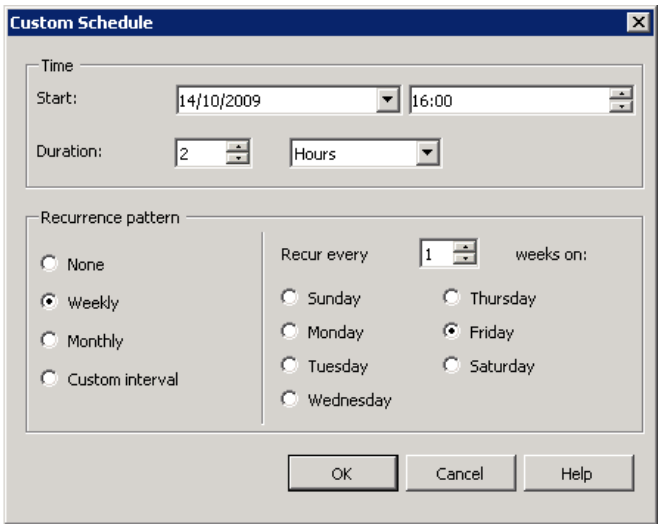
Network Discovery can provide an extensive list of attributes as part of the discovery record, including:

- NetBIOS name
- IP addresses
- Resource domain
- System roles
- SNMP community name
- MAC addresses

Network Discovery is often the most commonly used of the discovery methods, and as such, it has the most flexibility of all configurable discovery methods. It can be used, for instance, to find computers that can become Configuration Manager clients, to identify where they are located on the healthcare organisation's network, and to identify how they are distributed. This enables a more specific plan to be formulated for locating and implementing Configuration Manager sites, site servers, and site systems.

Table 43 shows the steps involved in enabling the Network Discovery method:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Discovery Methods** node. In the right pane, right-click on the **Network Discovery** component and select **Properties**.	
2.	Select **Enable network discovery**. Specify the following as required: ▪ Subnets ▪ Domains ▪ SNMP ▪ SNMP Devices ▪ DHCP	

Step	Description	Screenshot
3.	On the **Schedule** tab, click the new schedule button  .	
4.	Specify the required schedule and click **OK.**	

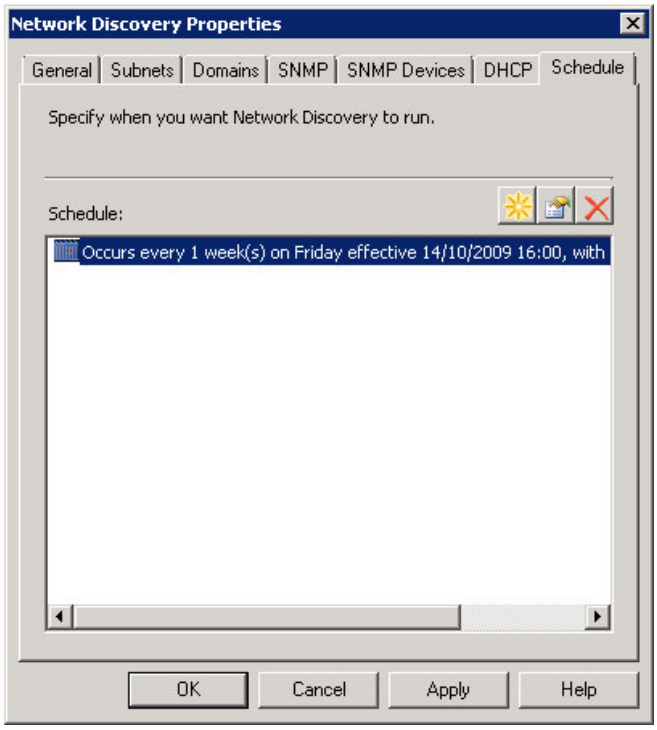
Step	Description	Screenshot
5.	Click **OK**.	

Table 44: Configuring Active Directory User Discovery

The progress of the discovery process can be monitored by looking at the log file <Configuration Manager installation folder>\Logs\Netdisc.log. Once the discovery records have been processed by Configuration Manager, they will be shown in the Configuration Manager Console within the 'All Systems' collection, and any other collection that is appropriate for the type of resource.

To view the discovery information that has been gathered for a computer, either double-click the computer from within the Configuration Manager Console, or right-click on the computer in the Console and select **Properties**.

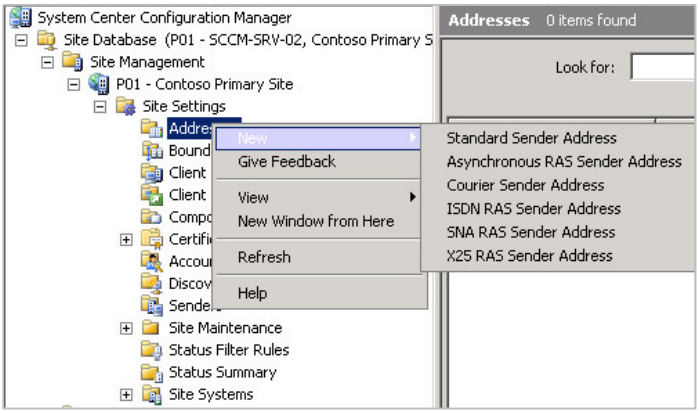
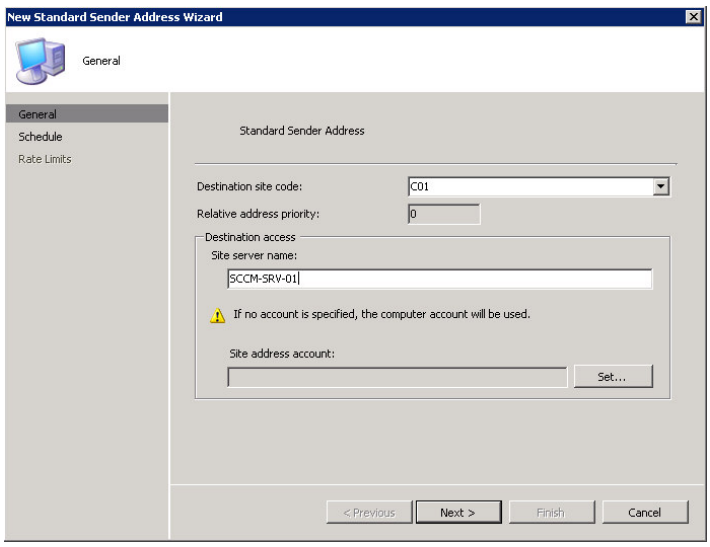
> **Note**
>
> Collections will only update their contents according to the update schedule specified for the collection. Therefore, it may be necessary to right-click on the collection and select **Update Collection Membership** to populate the collection members.

5.2.4 Installing Child Primary Sites

The installation of a child primary site is the same as the installation of the first configuration manager site, but the site must be configured to report to the parent site. Once the steps in Table 29 have been performed to install the site server, the steps in Table 45 must be performed to configure the site to report to the parent site. Prior to configuring the parent-child relationship, each server must be added to the SMS_SiteToSiteConnection_<sitecode> local group on the server of which it will be a parent or child.

5.2.4.1 Creating an Address

In order for Configuration Manager sites to communicate, an address must be configured at both the parent and child sites. The address specifies how Configuration Manager should communicate with the child or parent site and how the network should be utilised. The healthcare IT Administrator can specify schedules to prevent Configuration Manager from using too much network bandwidth during peak hours. Table 45 below shows the process for creating an address in Configuration Manager. This task should be performed at both the parent and child site; however, it is required only for Primary sites. To configure a Secondary site, see section 5.2.5.

Step	Description	Screenshot
1.	Open the **Configuration Manager Console**, right-click **Addresses** and then select **New > Standard Sender Address**.	
2.	Enter the **Destination site code** and **Site server name**. **Note** If the parent or child site is in a different forest, an account with access to the server in that forest must be entered.	

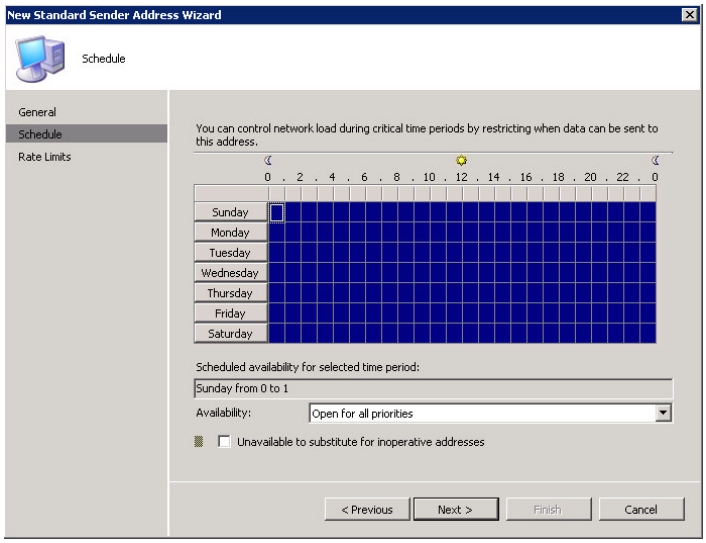
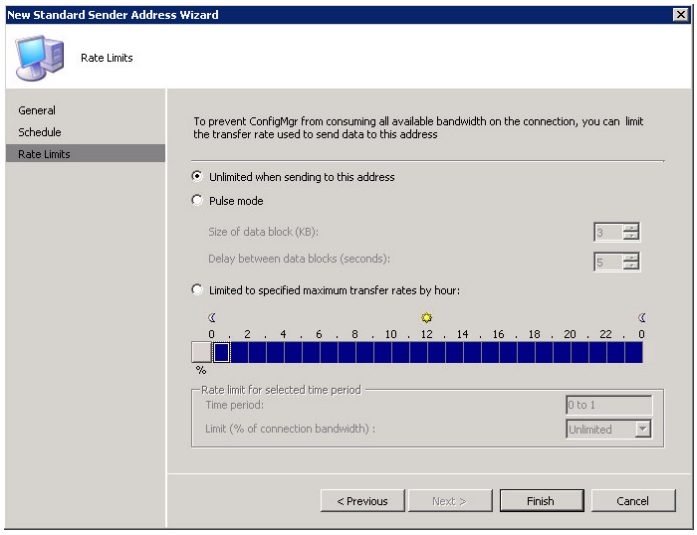
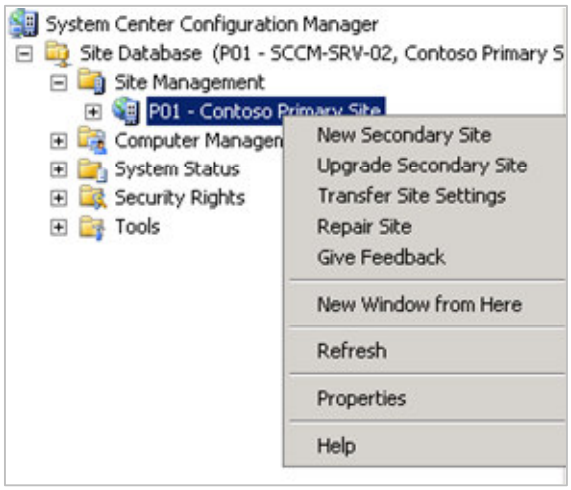
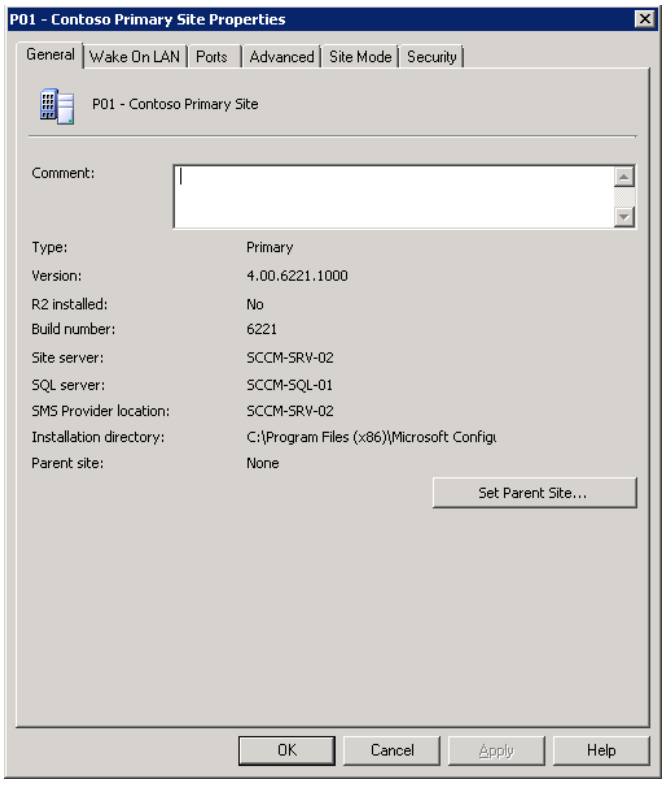
Step	Description	Screenshot
3.	Click **Next**.	
4.	Click **Finish**.	

Table 45: Creating an Address

5.2.4.2 Configuring a Child Primary Site to Report to a Parent Site

Once the addresses have been created on both the parent and child sites, the healthcare IT Administrator can configure the child site to report to the parent. Table 46 shows the process for configuring the parent-child relationship:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console**, then right-click the site node and select **Properties**.	
2.	In the site properties, click **Set Parent Site**.	

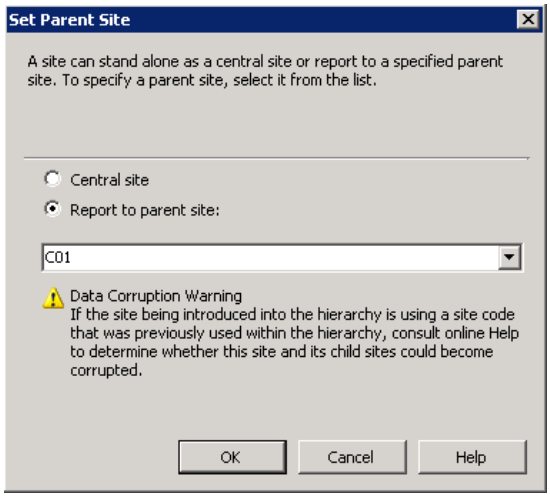
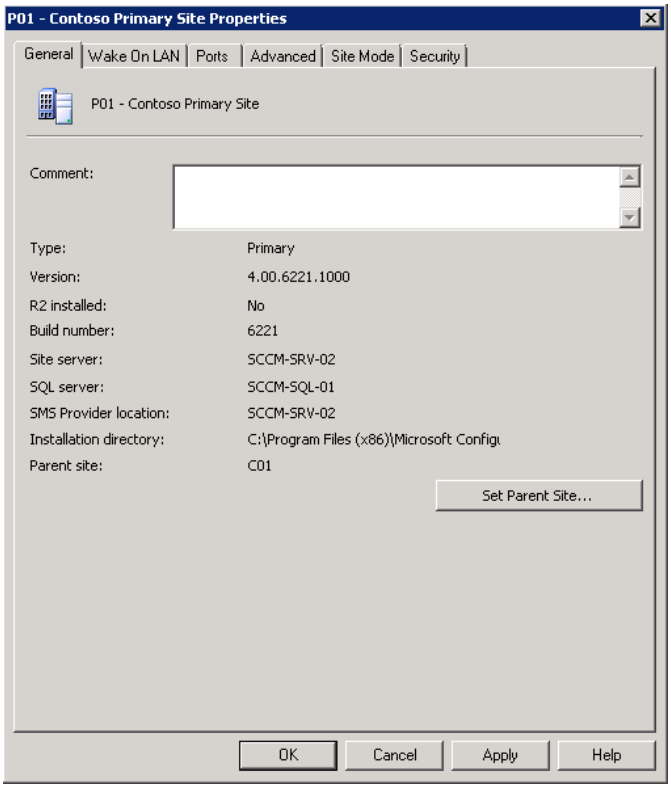
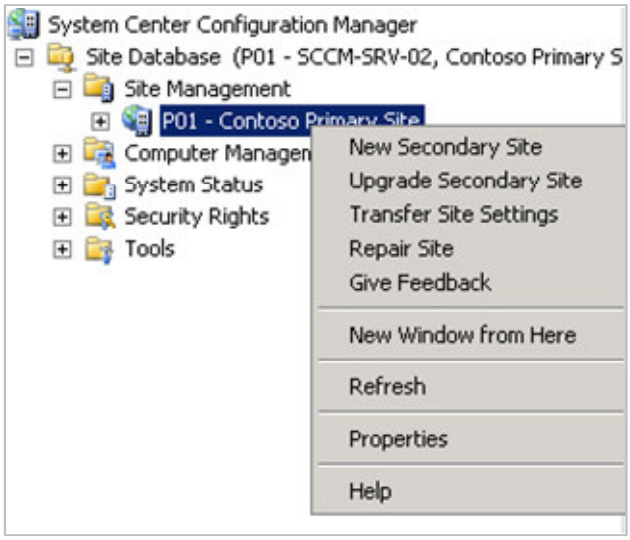
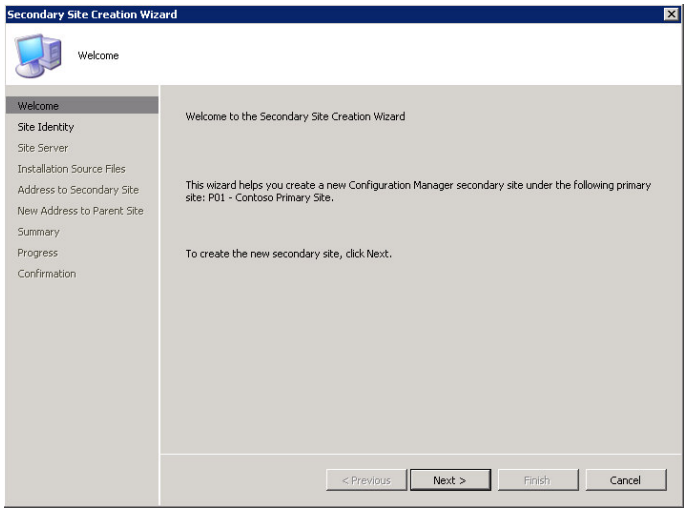
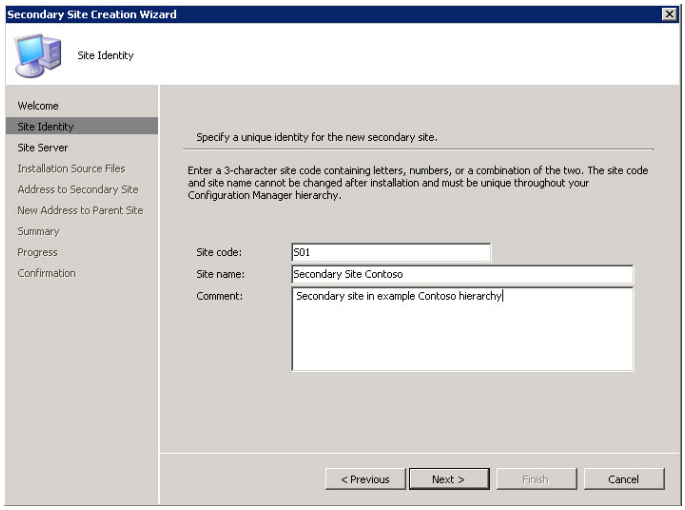
Step	Description	Screenshot
3.	Click **Report to parent site** and choose the central site (C01) from the drop-down list. Click **OK**.	
4.	Click **OK**.	

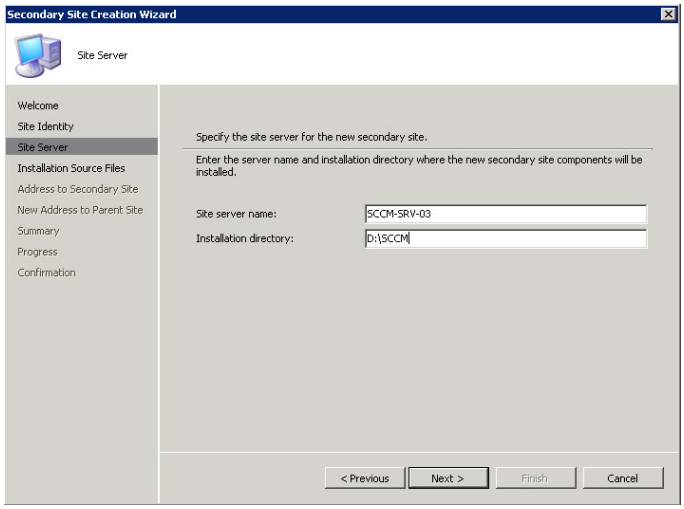
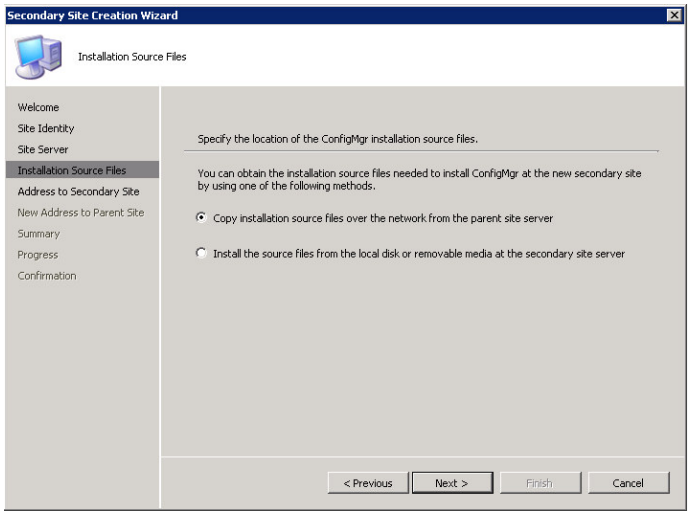
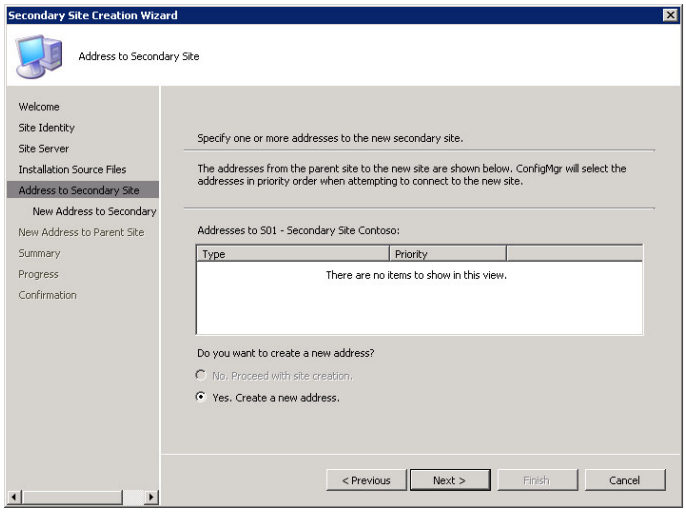
Table 46: Configuring a Child Primary Site to Report to a Parent Site

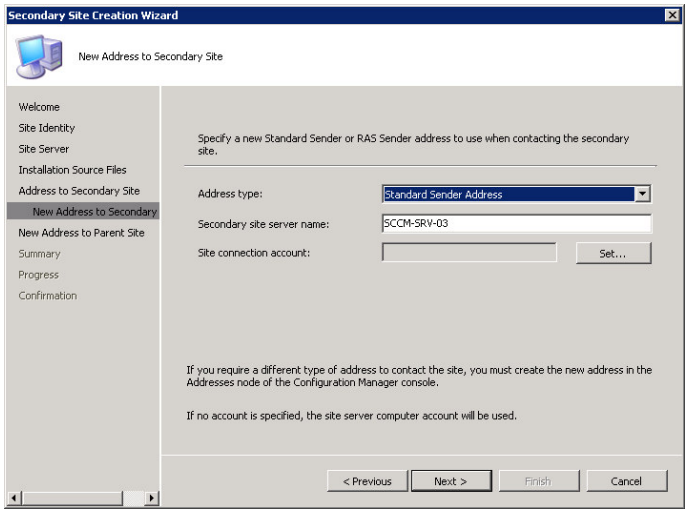
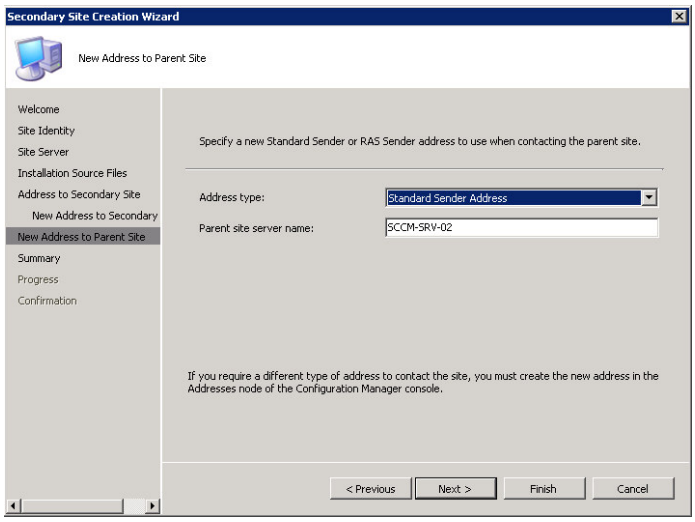
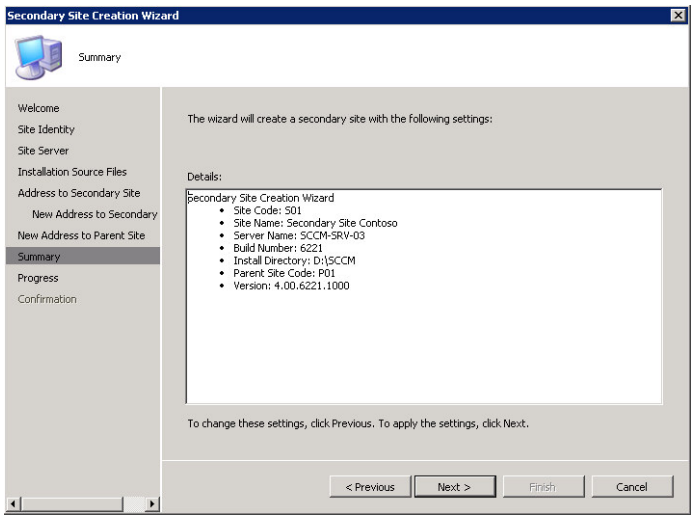
5.2.5 Installing Secondary Sites

Secondary sites can be installed directly from the Configuration Manager Admin Console. Table 47 shows the process for deploying a secondary site over the network from the Configuration Manager Admin Console.

> **Note**
>
> The machine account of the primary site server must be added to the local administrator group on the target server before the secondary site is installed.

Step	Description	Screenshot
1.	Open the **Configuration Manager Console**, right-click the site node of the primary site that will act as the Secondary site's parent, and select **New Secondary Site**.	
2.	On the Secondary Site Creation Wizard **Welcome** page, click **Next**.	
3.	Enter the **Site code**, **Site name** and a **Comment** for the new secondary site, and click **Next**.	

Step	Description	Screenshot
4.	Enter the **Site server name** and **Installation directory** of the new secondary site. Click **Next**.	
5.	Click **Next**.	
6.	On the **Address to Secondary Site** page, click **Next**.	

Step	Description	Screenshot
7.	Click **Next**. **Note** If the new secondary site is in an un-trusted forest, an account with access to the server in that forest must be entered.	
8.	Click **Next**.	
9.	Click **Next**.	

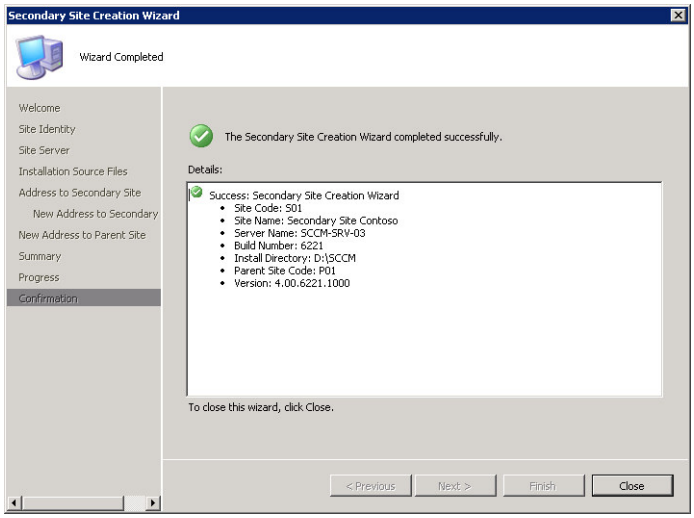
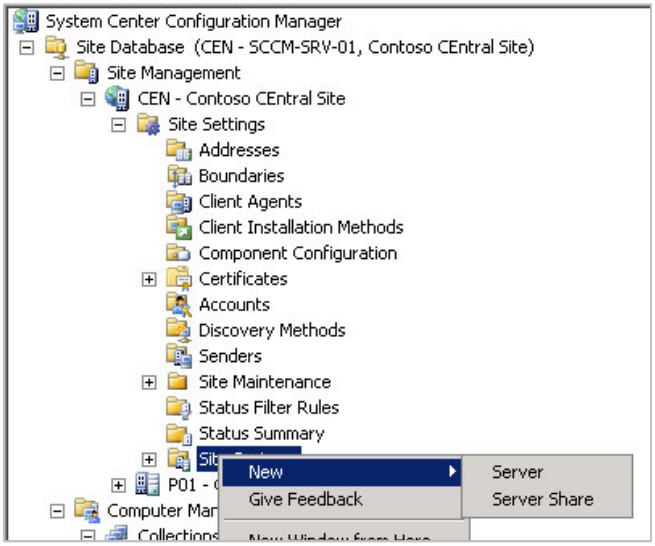
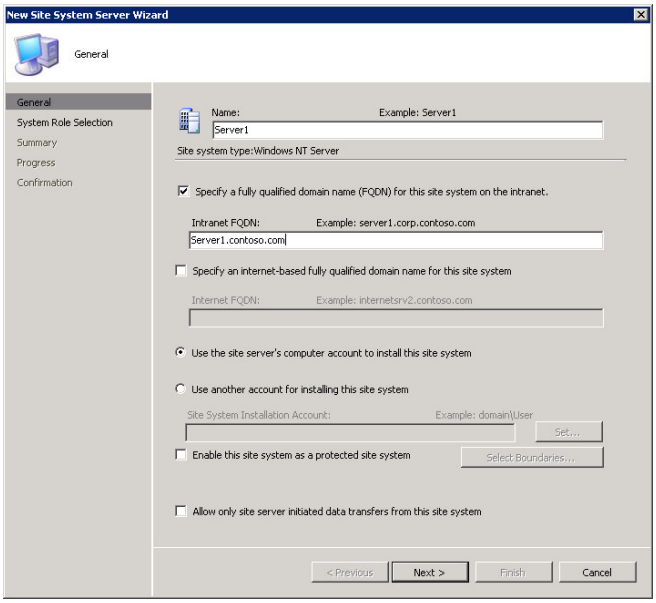
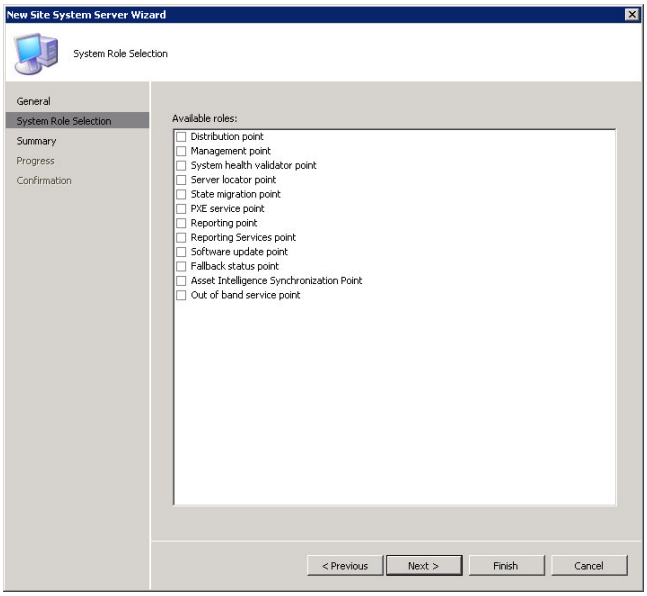
Step	Description	Screenshot
10.	Click **Close**.	

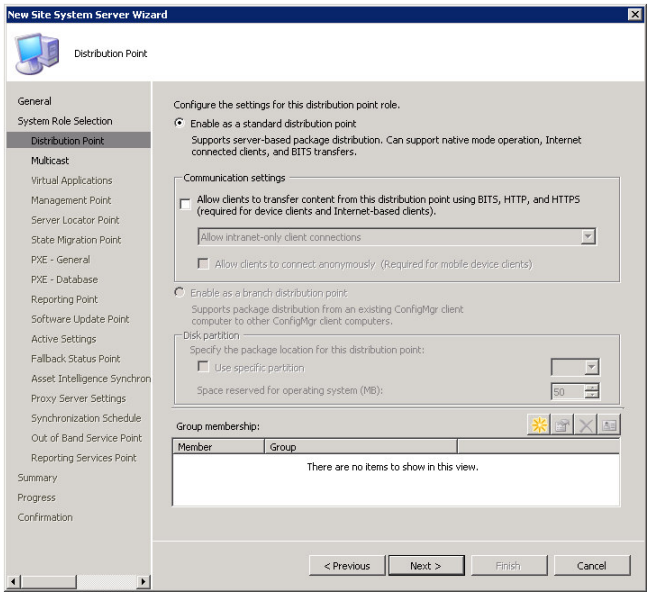
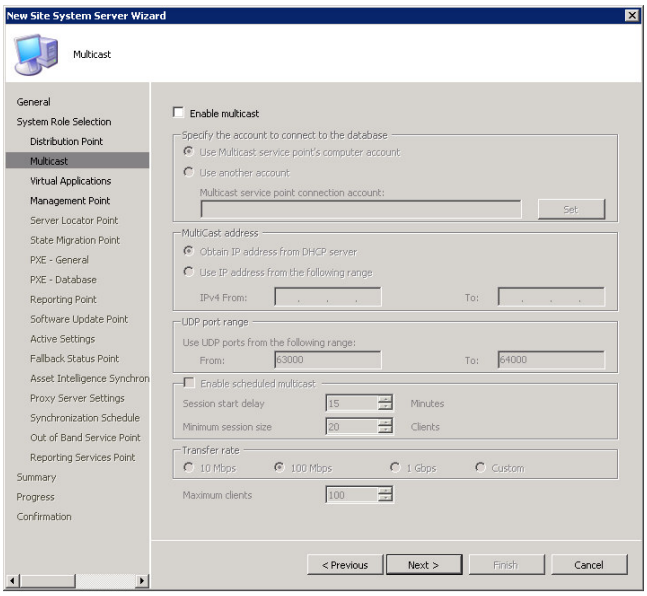
Table 47: Installing Secondary Sites

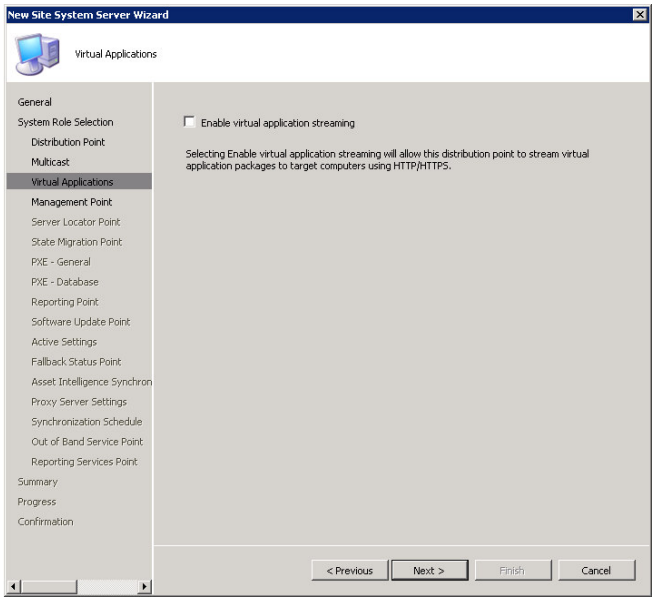
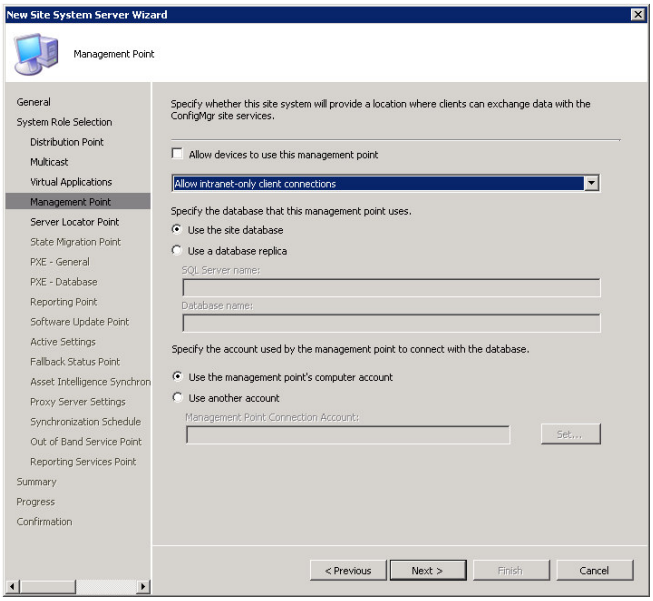
5.2.6 Installing Site Systems for the New Site

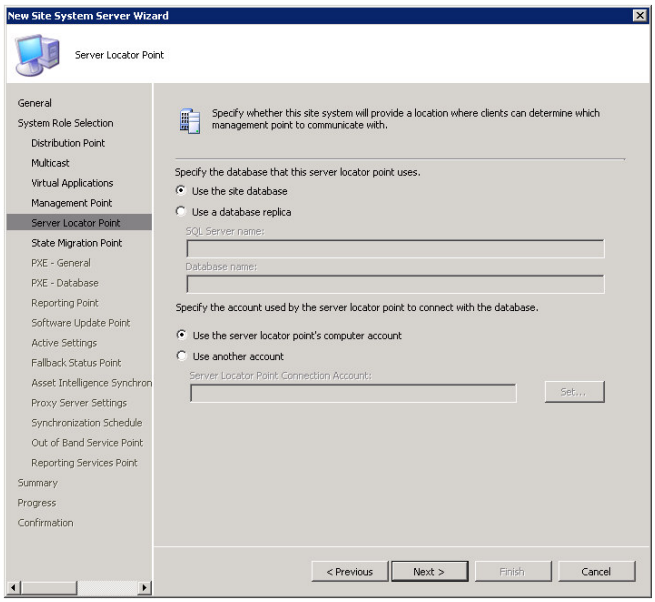
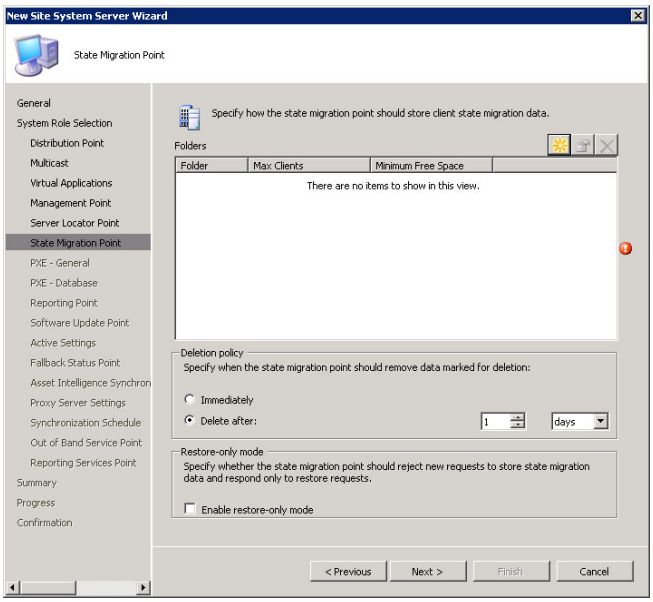
Site systems can be deployed either on the site server or on any other server with the required capacity. During the planning phase, the healthcare IT Administrator should have decided where any site systems will be installed. Table 48 shows the process for installing all site systems, including the dialog boxes for all site systems. The healthcare IT Administrator should only select the site system that needs to be installed.

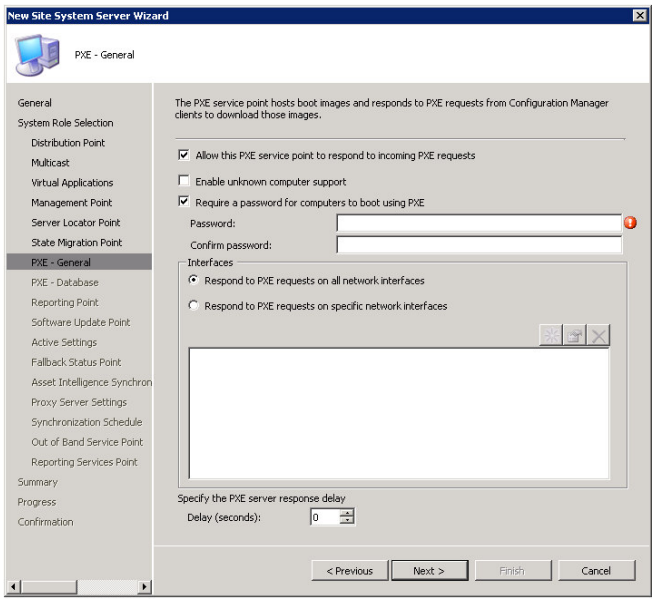
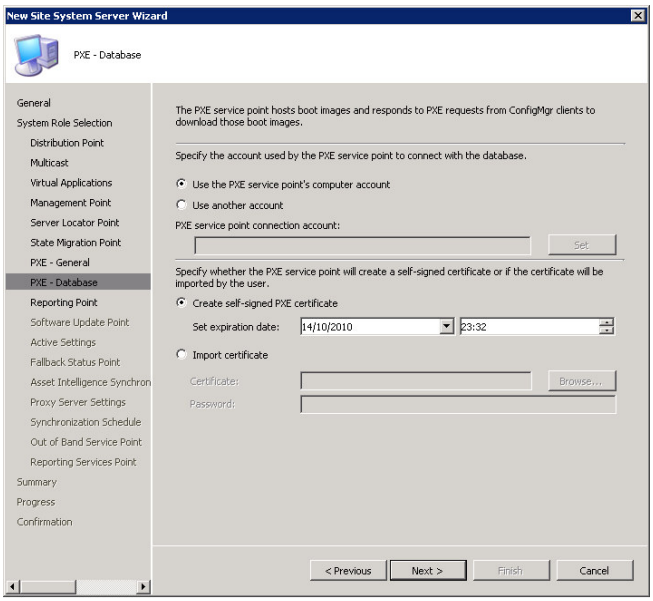
Step	Description	Screenshot
1.	Open the **Configuration Manager Console**, right-click the **Site Systems** node of the site to which the new site system will be added, and then select **New > Server**.	

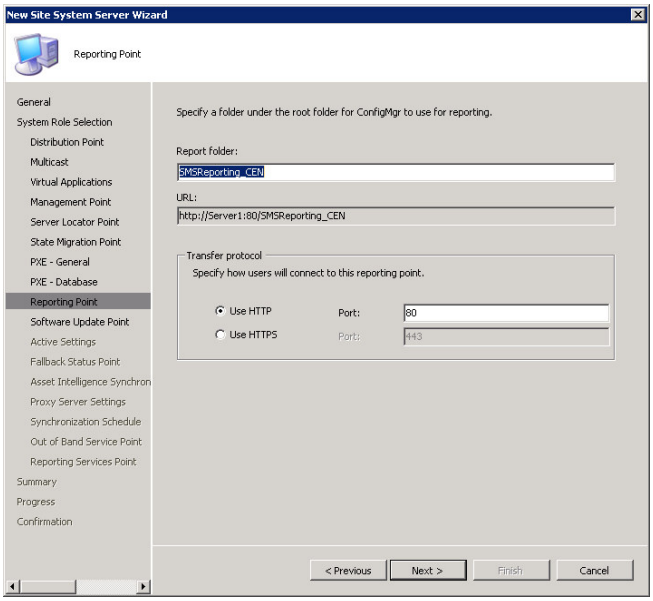
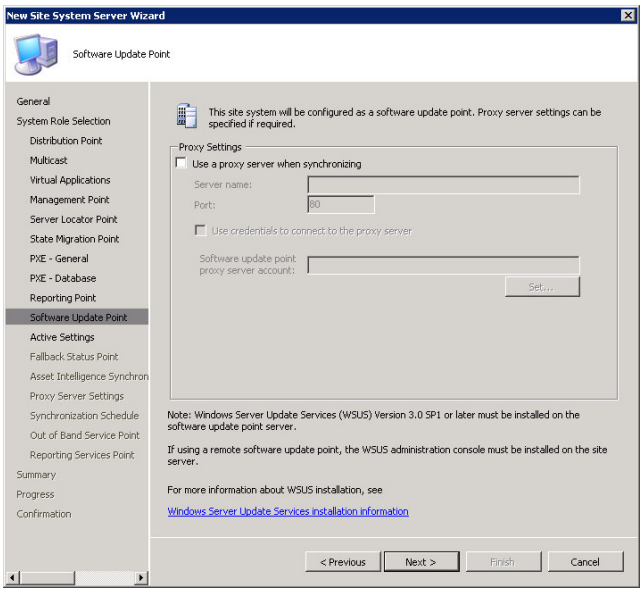
Step	Description	Screenshot
2.	On the **General** page, enter the **Name** for the server and specify an **Intranet FQDN**. **Note** Specify an Internet-based fully qualified domain name, if the site system will serve IBCM clients. Specify a different account for installing the site system, if the site server's machine account does not have administrative privileges on the remote server. Selecting **Enable this site system as a protected site system** allows the healthcare IT Administrator to specify the protected boundaries for this site system. See section 4.5.2 for more information on protecting site systems. Select **Allow only site server initiated data transfers from this site system** if the site system will reside in a perimeter network with no access to the site server. Click **Next.**	
3.	Select the required site system, or systems, from the list and click **Next**.	

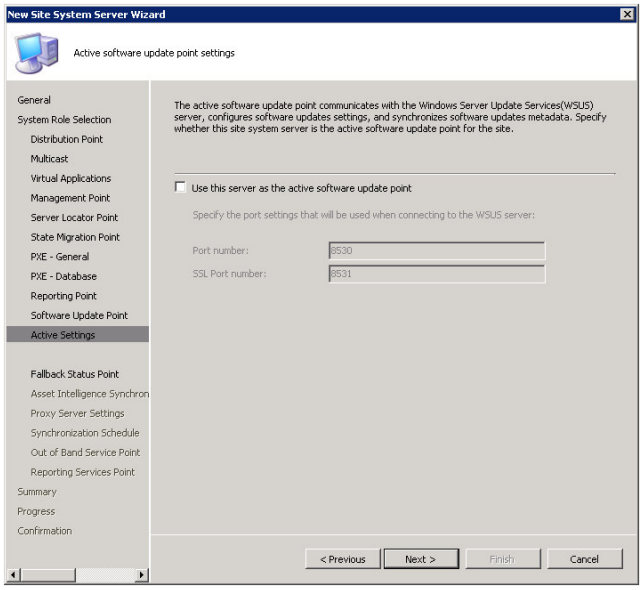
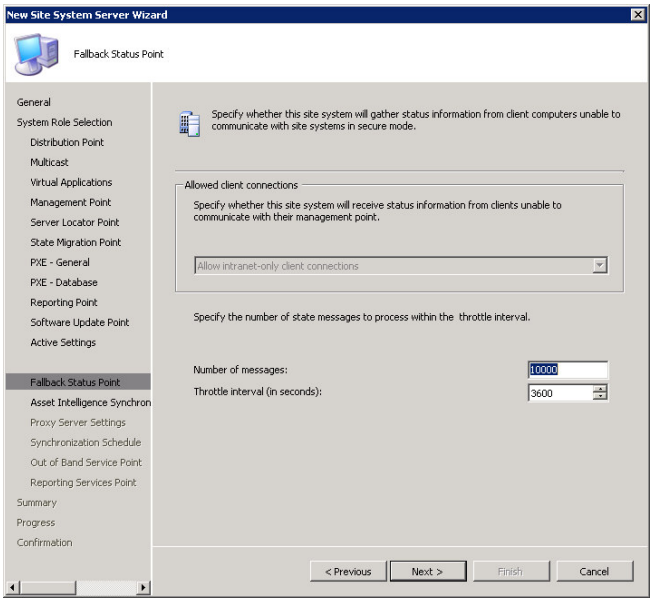
Step	Description	Screenshot
4.	To configure the Distribution Point settings, click **Enable as a standard distribution point**. If the DP will provide content to users via BITS, select **Allow clients to transfer content from this distribution point using BITS, HTTP and HTTPS**.	
5.	If the DP will be used for multicast deployments, select **Enable Multicast** and complete the required details.	

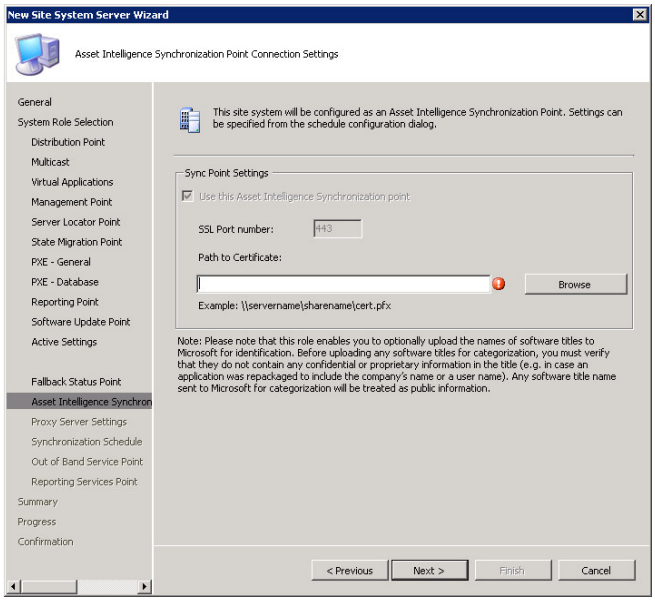
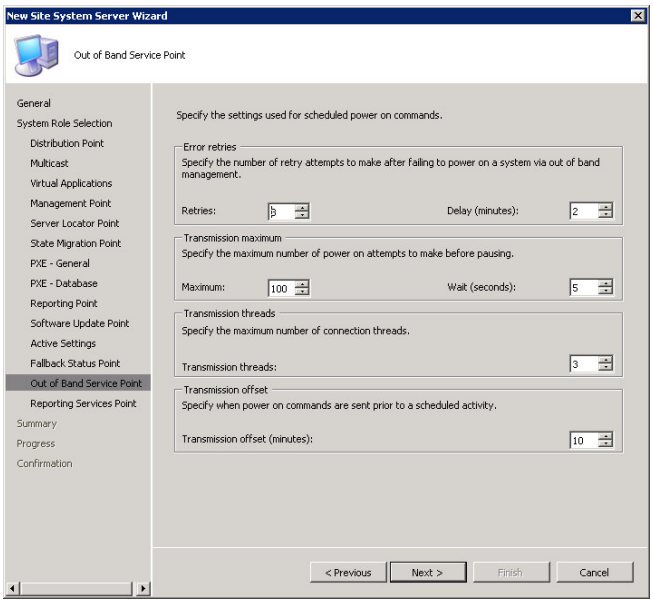
Step	Description	Screenshot
6.	If the DP will be used to stream App-V virtual applications, select **Enable virtual application streaming** and click **Next**.	
7.	If the **Management Point** option was selected in step 3, click **Next**. **Note** Select **Allow devices to use this management point** if the healthcare organisation will be deploying mobile devices to be managed by this site. Only select **Use a database replica** when deploying MPs that will use NLB, or for other high performance scenarios. Using this feature is outside the scope of this guidance. Only select **Use another account** if there are specific security requirements to do so. Otherwise, this option should be left at its default setting.	

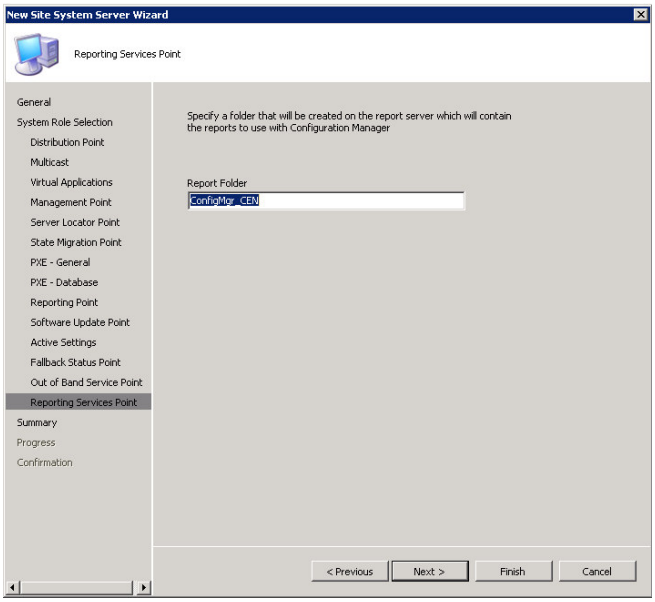
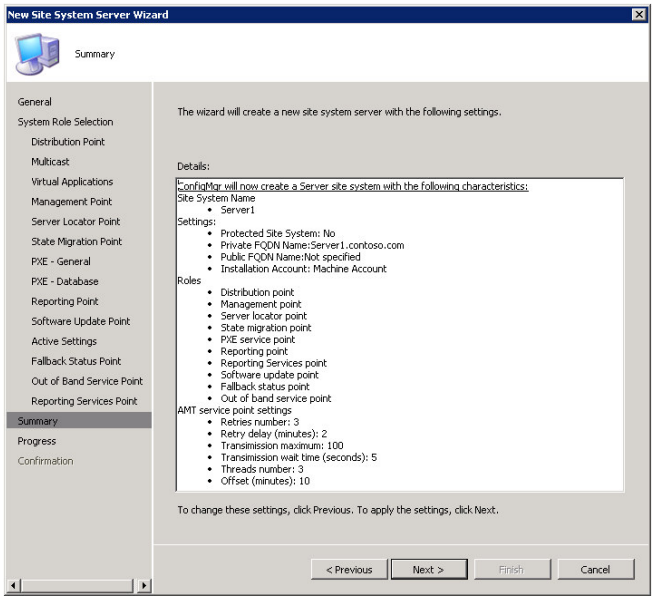
Step	Description	Screenshot
8.	If the **Server Locator Point** option was selected in step 3, click **Next**. **Note** Only select **Use a database replica** when deploying SLPs that will use NLB, or for other high performance scenarios. Using this feature is outside the scope of this guidance. Only select **Use another account** if there are specific security requirements to do so. Otherwise, this option should be left at its default setting.	
9.	If the **State Migration Point** option was selected in step 3, the healthcare IT Administrator can specify a folder on the site system to store users' migration data and can specify how long to maintain the data once it has been marked for deletion. More information on deploying the state migration point is available in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.	

Step	Description	Screenshot
10.	If the **PXE Service Point** option was selected in step 3, the healthcare IT Administrator can specify the following: ■ If the server will respond to incoming PXE requests ■ On which interfaces the server will respond to incoming requests ■ If unknown computer support will be provided ■ Whether the user will need to enter a password More information on deploying the PXE service point is available in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.	
11.	Select which account the PXE service point will use to connect to the Configuration Manager database, and whether the service will create a self-signed PXE certificate or import a certificate to use. More information on deploying the PXE service point is available in the *System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**.	

Step	Description	Screenshot
12.	If the **Reporting Point** option was selected in step 3, click **Next**. **Note** Modify the name of **Reporting folder**, if required. Select **Use HTTPS** if the Web site will use SSL security.	
13.	If the **Software Update Point** option was selected in step 3, click **Next**. **Note** If a proxy server is used to connect to the Internet, the details can be specified here, including any credentials that may be required. More information on deploying the software update point is available in the *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**.	

Step	Description	Screenshot
14.	Select **Use this server as the active software update point** and click **Next**. **Note** Once this option is selected, additional screens will appear in the wizard to specify synchronisation settings. More information on deploying the software update point is available in the *System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**.	
15.	If the **Fallback Status Point** option was selected in step 3, click **Next**. **Note** If the server is co-located with a server performing a different (non-Configuration Manager) function, the healthcare IT Administrator can limit the number of messages the FSP will process to reduce its impact.	

Step	Description	Screenshot
16.	If the **Asset Intelligence Synchronization Point** option was selected in step 3, specify the path to the System Center Online certificate and click **Next**. This certificate can be obtained by contacting the healthcare organisation's Microsoft representative.	
17.	If the **Out of Band Service Point** option was selected in step 3, click **Next**.	

Step	Description	Screenshot
18.	If the **Reporting Services Point** option was selected in step 3, click **Next**. **Note** The healthcare IT Administrator can modify the name of the **Report Folder**, if required.	
19.	Ensure the summary details are correct and click **Next**.	

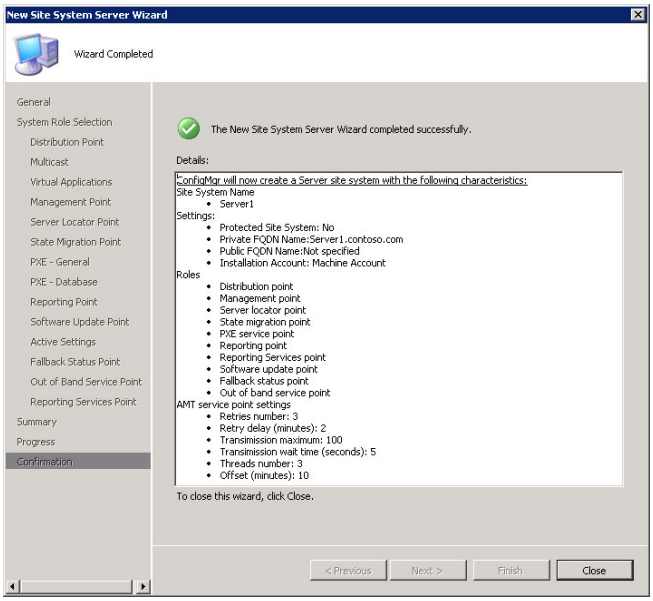
Step	Description	Screenshot
20.	Click **Close**.	

Table 48: Installation Process for Installing All Site Systems

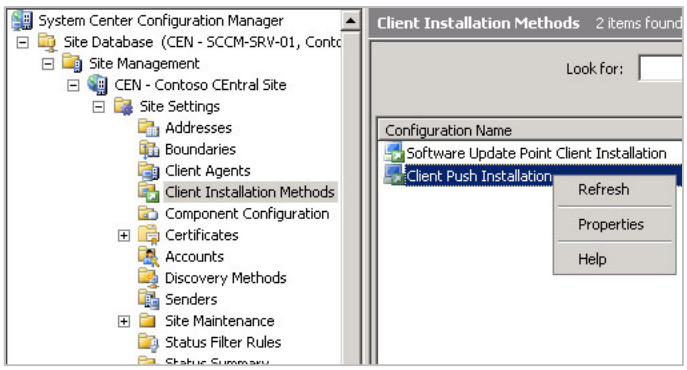
5.3 Installing Clients

Various methods can be used for installing clients using Configuration Manager including:

- Client Push Installation
- Software Update Point Client Installation
- Manual Client Installation

5.3.1 Client Push Installation

Client Push Installation can be performed in two ways. The first requires the healthcare IT Administrator to enable client push on a site-wide basis. This method can be useful once the site is in full production but should not be used during pilot stages. This method will attempt to install a client on any system that is discovered by Configuration Manager. The healthcare IT Administrator can specify whether the client should be automatically installed on client-class computers, server-class computers, domain controllers or any combination of these. Table 49 shows the process for enabling site-wide client push installation:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Client Installation Methods** node. In the right pane, right-click **Client Push Installation** and select **Properties**.	

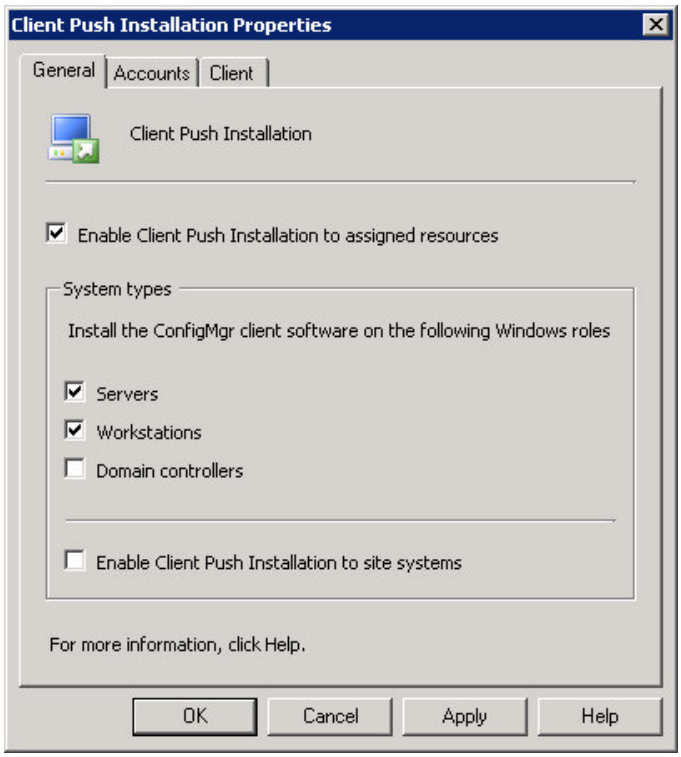
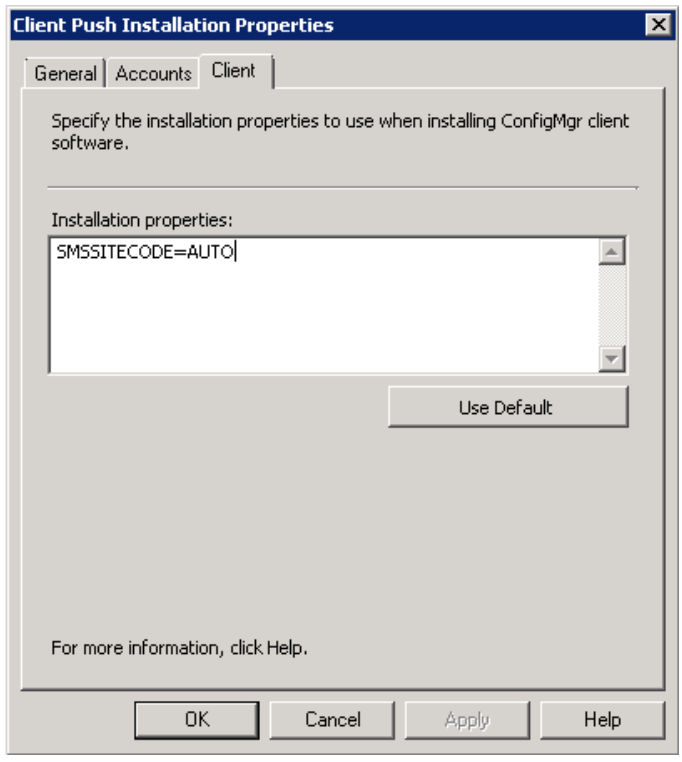
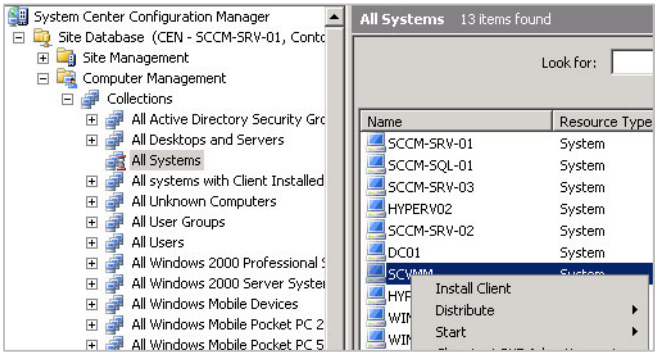
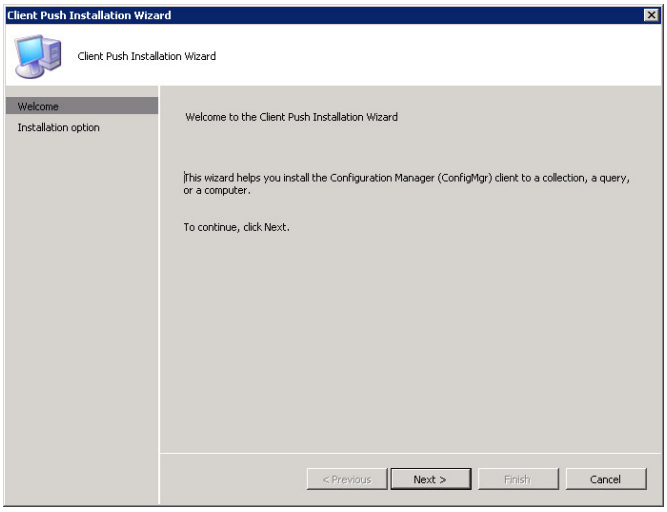
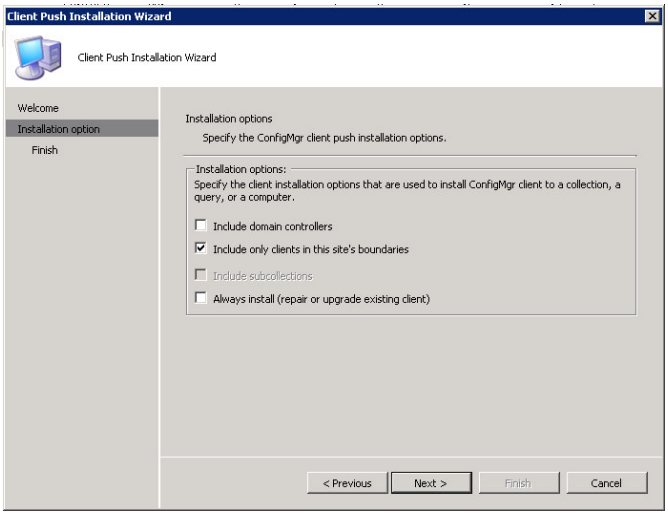
Step	Description	Screenshot
2.	Select **Enable Client Push Installation to assigned resources** and select which **System Types** will be automatically deployed.	
3.	On the **Client** tab, the healthcare IT Administrator can specify additional installation properties to control how the client will be installed. More information on client installation properties is available in the TechNet article *About Configuration Manager Client Installation Properties*[33]. Click **OK** to save your settings and close the **Client Push Installation Properties** dialog box.	

Table 49: Enabling Site-Wide Remote Client Installation

[33] Microsoft TechNet: About Configuration Manager Client Installation Properties **{R29}**: http://technet.microsoft.com/en-us/library/bb680980.aspx

The second option for installing a client using Client Push installation is to use the client Installation Wizard. This allows the healthcare IT Administrator to select a discovered resource, or collection of resources, and trigger the site server to install the Configuration Manager client on the selected system or on all the systems within the selected collection.

> **Important**
>
> In order to use the Client Installation Wizard to install clients, it is not necessary to enable Client Push. The healthcare IT Administrator only needs to specify the Client Push account and any required settings, and not enable the Client Push feature.

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Computer Management > Collections** node. Select the collection that contains the client to be deployed, then in the right pane, right-click on the computer object and select **Install Client**. **Tip** The collection can also be selected if all clients within the collection need to be deployed.	
2.	Click **Next**.	
3.	Click **Next**. **Note** If domain controllers are being targeted, the **Include domain controllers** option must be selected. If clients that are not within the sites boundaries are being targeted, the **Include only clients in this site's boundaries** option must be clear. If the target machine already has a previous version of the Configuration Manager client (or SMS 2003 client), or the healthcare IT Administrator is redeploying the client to try and resolve a technical issue, the **Always install (repair or upgrade existing client)** option must be selected.	

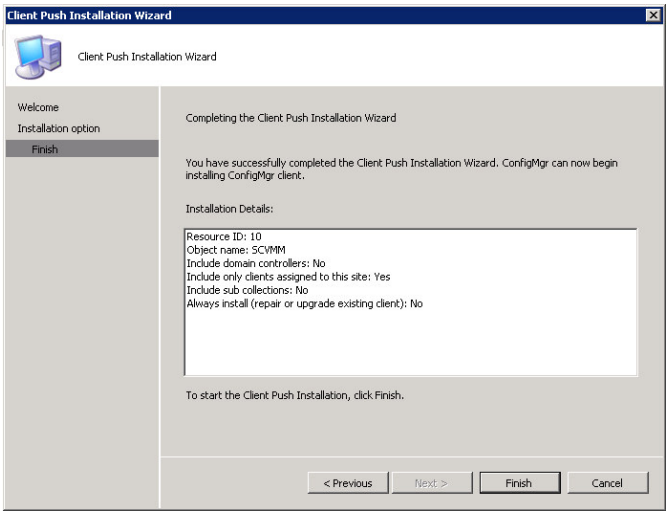
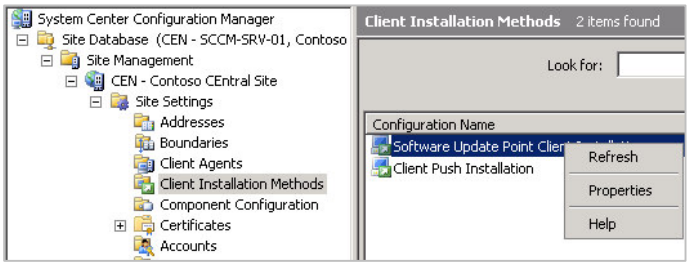
Step	Description	Screenshot
4.	Click **Finish**.	

Table 50: Deploying a Client Using the Client Installation Wizard

The progress of the installation process can be monitored by looking at the log file <Configuration Manager installation folder>\Logs\Ccm.log on the server and the <SystemRoot>\CCMSetup\Ccmsetup.log on the target machine.

5.3.2 Software Update Point Client Installation

Software Update Point Client Installation allows the healthcare IT Administrator to deploy the Configuration Manager client as if it was a software update. The Configuration Manager will appear during the Windows update cycle and be installed just like any other software update. If the healthcare organisation has already deployed and used WSUS for patch management, this client deployment process should fit in with existing processes. In order to use Software Update Point Client Installation, a Configuration Manager SUP must be deployed and operational. Table 51 details how to enable Software Update Point Client Installation:

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Client Installation Methods** node. In the right-pane, right-click on **Software Update Point Client Installation** and select **Properties**.	

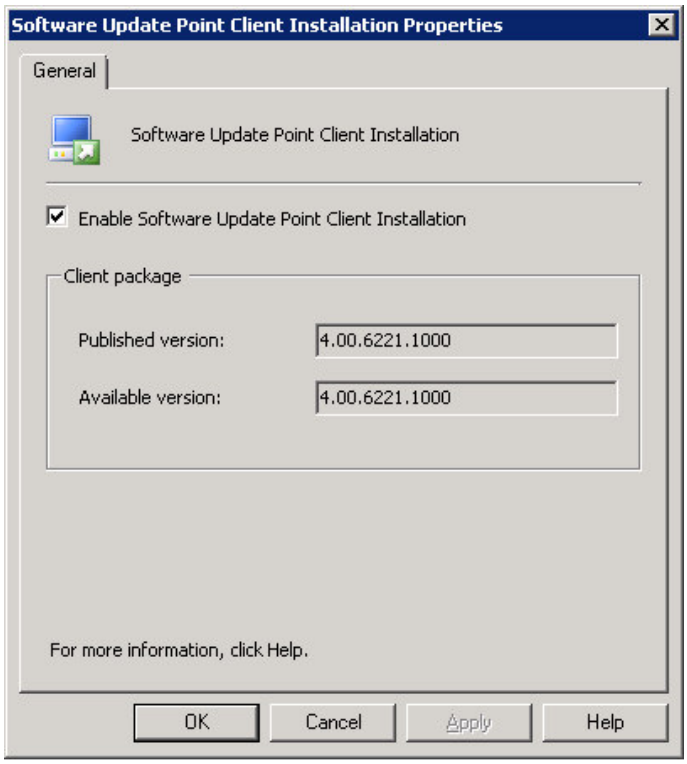
Step	Description	Screenshot
2.	Select **Enable Software Update Point Client Installation** and click **OK**.	

Table 51: Enabling Software Update Point Client Installation

> **Important**
>
> When deploying the client using Software Update Point Client Installation, the client will be installed using default command-line properties, even if custom properties were set in the **Client Push Installation Properties** dialog box. In order to specify custom settings, the healthcare IT Administrator must deploy a group policy to the client prior to installing the client. More information on deploying this group policy is available in the TechNet article *How to Provision Configuration Manager Client Installation Properties using Group Policy* **{R15}**.

5.3.3 Manual Client Installation (General Practice Clients)

In some healthcare organisations, clients that reside in remote locations, for example, General Practice clinics may not be part of the central Active Directory. Because Configuration Manager uses Active Directory to publish information about client assignment, when clients are not part of the Active Directory, additional steps need to be performed to install the Configuration Manager client. In this case, it is not possible to use the automated methods for installing the Configuration Manager client.

5.3.3.1 Configuring the Configuration Manager Site to Manage General Practice Clinics

If possible, the IP subnets of the General Practice clinics should be added as a slow boundary of the Configuration Manager primary or secondary site that has the fastest connection to this location. However, if the IP subnets in use are not known, or are not centrally controlled (for example, they could be changed at any time without the healthcare IT administrators knowing, which may happen if they are managed by a third-party provider), it is still possible to manage the clients without specifying the IP subnet in the boundaries of a site.

If it is not possible to specify the subnets, the client will still become assigned to a primary site as usual because this will be configured at client installation. If the nearest Configuration Manager site is a secondary site, the subnet information must be added as a slow boundary of that secondary site, in order for the client to use that server as a proxy. If the subnet information is not added, the client will never be made aware of the secondary site and will always communicate directly with the primary site.

Follow the steps in section 5.2.3.1 to configure the boundaries of the primary or secondary site respectively.

5.3.3.2 Configuring Name Resolution

Because the computers in this location are not part of the same Active Directory environment as the Configuration Manager servers, it will not be possible to discover the machines in this location using Active Directory discovery methods. This means that client push installation will not be possible for these computers. Instead, the clients will need to be installed manually on the machines and then report to Configuration Manager following the manual client installation.

However, before the client can be installed, ensure that the client will be able to locate and communicate with Configuration Manager servers. In normal circumstances, the client will use Active Directory to locate Configuration Manager server resources, and use standard name resolution methods to then communicate with those servers.

For example, following successful client installation, the following high-level steps occur:

1. The client queries Active Directory to find a Configuration Manager site that manages the IP subnet, IP Range, IPv6 Prefix or Active Directory site in which the client resides. This query would return a site code, for example, P01.
2. Once the client has found the Configuration Manager site, it queries Active Directory again to find the name of the management point for the site. If this fails, the client can use NetBIOS name resolution, assuming that appropriate records are available.
3. Once the client has found the name of the management point, standard name resolution methods will be used to attempt to communicate with the server.

If the computers are in a different forest to the Configuration Manager site servers, or are in a workgroup, they will fail to perform step 1. Depending on the name resolution infrastructure available to the clients, they may then fail steps 2 and 3.

Before installing the client, it is important to ensure that it will be able to locate Configuration Manager resources and communicate with the management point and other site systems. Step 1 will be resolved by specifying the site assignment on the command line during installation, rather than configuring the client to automatically discover the Configuration Manager site. This will remove the need for the client to query Active Directory to find its site assignment.

Steps 2 and 3 will need to be resolved by ensuring that the computer can use NetBIOS name resolution to locate the management point.

If the computers share the same Windows Internet Naming Service (WINS) infrastructure, the computers should be able to locate the management point using records that the management point automatically registers in WINS. Verify this by checking the WINS database that the computers are configured to use for the MP_<site code> record. For example, if the site code is P01, an MP_P01 record should exist in WINS, which maps to the IP address of the management point for P01.

If they do not share the same WINS infrastructure, appropriate records need to be added to the Lmhosts file (located in %windir%\System32\Drivers\Etc) on the client computers. If the Lmhosts file does not exist on the machine, create one in %windir%\System32\Drivers\Etc. It must be a file named **Lmhosts** with no file extension, and can be edited in Notepad. When querying using NetBIOS name resolution, the client will look for these particular records:

- MP_<sitecode>. For example, if the client is assigned to site P01, it will query for MP_P01
- The name of the MP. For example, if the management point is installed on HCO-SMS-SVR02, it will need to be able to resolve this name

An example section of an Lmhosts file is given below:

```
192.168.1.2 "MP_P01         \0x1A"    #PRE

192.168.1.2 MPSERVERNAME              #PRE
```

> **Important**
>
> It is important that the file is formatted correctly or it will not function as expected. In the example above, the space between the IP Address and the opening quote is a single tab and the space between the closing quote and #PRE is also a single tab. All characters in the file must be in upper case except for the 'x' in \0x1A. Additionally, the number of characters specified in the MP record is important. There must be 15 characters prior to the \0x1A portion. Therefore, this is made up of 6 characters for the MP_<site code> portion and then 9 spaces up to the \0x1A portion.

In cases where the client should communicate via a secondary site, add the details for the primary site to which the client will be assigned, and the secondary site that contains the boundaries to manage the General Practice clinics.

Once the file has been created it can be copied to all General Practice clients that will require the same settings. If the healthcare IT Administrator is replacing the Lmhosts file by copying the new file to client machines, the existing Lmhosts file should be checked to ensure it does not contain any custom configuration.

After adding the records, close the Lmhosts file and type the following at the command prompt:

```
C:> Nbtstat -R
```

Use the following command to verify the entries:

```
C:> Nbtstat -c
```

Figure 21 shows the expected output of the **Nbtstat –c** command if the Lmhosts file has been created correctly using the example above:

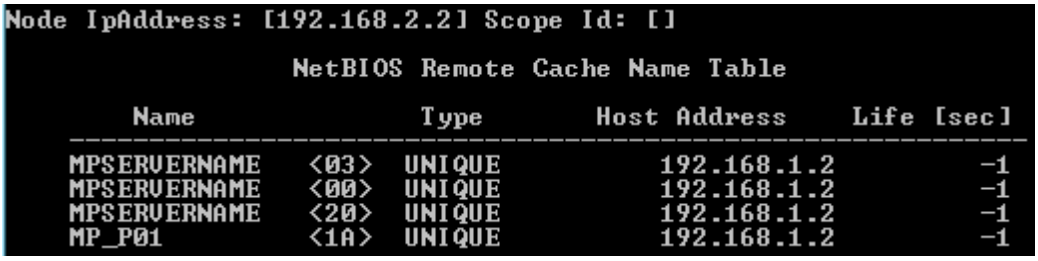


Figure 21: Expected Output from Running Nbtstat –c

The example code fragment below should be copied into Notepad and saved with a .vbs extension once the correct name of the desired management point has been substituted. The example below is for a management point installed on a server called HCO-SCCM-SVR02. The healthcare IT Administrator should replace the bold text below with the NetBIOS name of the management point server, leaving the quotation marks in place.

```
dim oSMSClient
set oSMSClient = CreateObject ("Microsoft.SMS.Client")
oSMSClient.SetCurrentManagementPoint "HCO-SCCM-SVR02",0
set oSMSClient=nothing
```

Once the Configuration Manager client is installed and the Lmhosts file has been configured, double-click on the .vbs file on the client to complete the client installation process.

> **Note**
>
> Executing the .vbs file will not provide any feedback or present any dialog boxes to the user; it will simply execute and exit.

5.3.3.3 Manually Installing the Configuration Manager Client

Table 52 shows the process for manually installing the client for General Practice clinics.

> **Tip**
>
> It is recommended but not essential that the hierarchy's Trusted Root Key is pre-provisioned when deploying to clients in a workgroup or an un-trusted domain. This ensures that the client is communicating with the correct management point and eliminates the risk of the client being assigned to a 'rogue' MP. More information on the reasons for this and details of how to pre-provision the trusted root key are available in the TechNet article *How to Pre-provision the Trusted Root Key on Clients*[34].

Step	Description
1.	The files needed for client installation are located on the Configuration Manager site servers in the <Configuration Manager Installation directory>\Client\ folder. The files required are: ▪ Ccmsetup.exe ▪ Ccmsetup.cab The folders required are: ▪ i386 ▪ ia64 ▪ x64 Copy the above files and folders to a folder on the computer on which the client is to be installed, for example, C:\Temp.

[34] Microsoft TechNet: How to Pre-provision the Trusted Root Key on Clients **{R30}**: http://technet.microsoft.com/en-us/library/bb680504.aspx

Step	Description

2.	Install the client from a command prompt. For example, if the files were copied to C:\Temp\SCCMClientFiles, and the client will be assigned to P01, run the following commands:
	`C:>cd c:\temp\sccmclientfiles`
	`C:\temp\sccmclientfiles>CCMSetup.exe SMSSITECODE=P01`
	The above commands need to be run using an account with administrative rights on the computer.
	Important
	Always specify the site code of a primary site in the above commands, because a client cannot be assigned to a secondary site. If there is a secondary site that the clients will use as a proxy, then assuming that the subnet information was added to the remote roaming boundaries of the secondary site in question, the client will first communicate with the assigned primary site. The assigned primary site will then inform the client that it is within the boundaries of a secondary site, and the client will then use this secondary site as a proxy.

3.	If the client is unable to locate the management point for the site, review the steps in section 5.3.3.2 to ensure that the computer is capable of resolving the appropriate NetBIOS records.

Table 52: Manual Installation of the Configuration Manager Client

6 STABILISE

The Stabilise phase involves testing the solution components whose features are complete, resolving and prioritising any issues that are found. Testing during this phase emphasises usage and operation of the solution components under realistic environmental conditions.

This involves testing and acceptance of the application prior to production deployment.

Figure 22 acts as a high-level checklist, illustrating the areas of the Configuration Manager design that an IT Professional is responsible for stabilising:

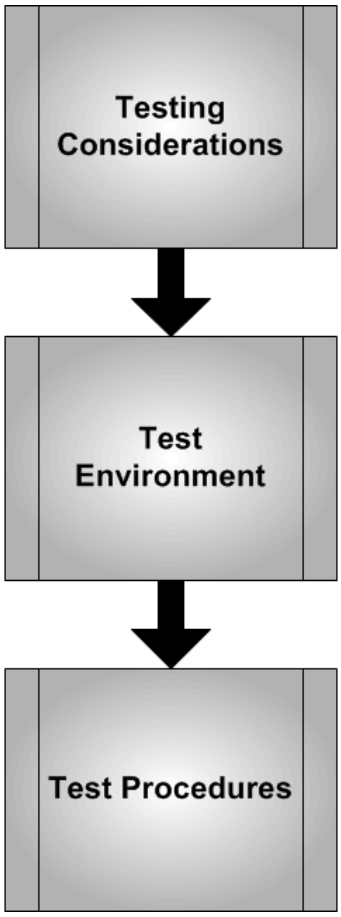


Figure 22: Sequence for Stabilising Configuration Manager

6.1 Testing Considerations

Testing is an important part of any software deployment project and has a number of benefits. Testing allows the healthcare IT Administrator to be comfortable with the infrastructure implementation or configuration changes that are about to be made. It is also important to allow the healthcare IT Administrator to identify any potential issues that could be introduced and to plan for them prior to implementation in a production environment.

6.2 Test Environment

Any test environment should match the production environment as closely as possible to get the best results. It is often not possible to exactly match the production environment in a laboratory setting because this can be quite costly. When considering the design of a test environment, solution components should be prioritised in terms of risk and importance, and included appropriately. The use of virtualisation software can be useful in test environments, and can significantly reduce costs.

6.3 Test Procedures

When testing any new infrastructure platform, it is important to keep an accurate record of what is to be tested. By creating this record, the tests can be easily repeated at each stage of the project as the product moves from lab testing into pilot and then into production. The healthcare IT Administrator should create a detailed test plan to include the following sections of testing:

- Ensure infrastructure installs as expected
- Ensure clients can be deployed
- Ensure all features that will be used in production are functioning as expected
- Test the impact of the new software on existing software (make sure no conflicts exist)
- Ensure all operational staff are familiar with the new toolset and receive appropriate training
- Ensure a Disaster Recovery Plan has been created and all backup and restore procedures have been tested

For each of the items above, the healthcare IT Administrator should decide what will be tested and document how it will be tested. The above areas should only be considered a starting point for creating the test plan. The test plan should include as many of the activities and scenarios that may be experienced in the production environment as possible.

7 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.

7.1 Deploying the Configuration Manager Infrastructure into Production

The healthcare IT Administrator should now have fully deployed the Configuration Manager infrastructure into a test environment and tested that all components work as expected. While performing these tasks, any issues that may have occurred should have been investigated, and where possible, resolved. These issues should have been documented and an implementation plan created. The purpose of creating an implementation plan is to allow the healthcare organisation to deploy the Configuration Manager infrastructure in a consistent way and also to maintain a record of how the implementation was carried out.

Once fully tested in a lab environment, the solution should be deployed based on the design created in the Plan section. The solution should be deployed using a phased approach as shown in Table 53:

Task Description	Section or Link Providing More Information	Additional Notes
Decide on a design for all sites and locations	Section 4 : Plan	The sections described in the Plan section of this document will help the healthcare IT Administrator to design a basic Configuration Manager solution for the healthcare organisation. Additional links have been provided to information for those cases where more advanced scenarios must be covered.
Document the design and gather approval from all stakeholders		This task should be performed in order to maintain a record of the desired configuration of the solution. The design will likely change and be updated during the Test and Validate phase, so the document should be treated as a 'living document' and updated regularly.
Install the desired solution into a test environment	Section 5: Develop	This is an extremely important part of the process and will identify any aspects of the healthcare organisation's infrastructure that may need investigation or modification before Configuration Manager can be deployed into production.
Finalise detailed design document once testing has been completed and create an implementation guide to assist with deployment		The implementation guide created should contain detailed steps to allow any healthcare IT Administrator to deploy the designed solution. It can also act as a reference of the chosen configuration options and as part of a Disaster Recovery process, if backup is not performed or corrupted for some reason.
Implement the first primary site in production	Section 5.2.1: Installing and Configuring Prerequisites Section 5.2.2: Installing the First Configuration Manager Site Section 5.2.3 : Configuring the First Configuration Manager Site	

Task Description	Section or Link Providing More Information	Additional Notes
Configure the required accounts and specify the boundaries for the site	Section 5.2.3 : Configuring the First Configuration Manager Site	
Run the desired discovery tasks to allow for client installation to be performed	Section 5.2.3.3: Configuring Discovery Methods	
Define a group of pilot clients and deploy the client	Section 5.3.1: Client Push Installation	The healthcare IT Administrator should define a pilot group of clients. This group should include users from as many different departments and job roles as possible because this will provide the best pilot results. The group should not only contain computers that are located in the IT department. The purpose of the pilot is to identify if any applications that are deployed in the healthcare organisation, clinical or otherwise, have compatibility issues that were not identified during lab testing.
Implement any additional primary sites or secondary sites into production	Section 5.2.4 : Installing Child Primary Sites Section 5.2.5 : Installing Secondary Sites	This step should be carried out once the initial pilot clients that reside within the boundaries of the Central site have been deployed. Once each new primary or secondary site has been deployed, pilot clients should be defined and deployed within the new sites boundaries.
Gather feedback from all pilot clients to ensure that no issues have been identified		It is also advisable to run through any non-destructive tests that were carried out when the product was tested in a lab environment. This will ensure that all desired features are working as expected in the production environment.
Deploy the Configuration Manager client to all remaining client machines	Section 5.3 : Installing Clients	This can be performed in a number of ways but should ideally be performed using a staged approach. The healthcare IT Administrator should monitor the deployment carefully to ensure that no issues occur. There are a number of built-in reports that can help with the monitoring of client deployments.
Perform Software Updates Using Configuration Manager	*System Center Configuration Manager 2007 Software Update Management Guide* **{R1}**	
Perform Software Distribution Using Configuration Manager	*System Center Configuration Manager Software Distribution Guide* **{R3}**	
Performing Operating System Deployments Using Configuration Manager	*System Center Configuration Manager 2007 Operating System Deployment Guide* **{R2}**	
Managing and viewing reports in Configuration Manager	Reporting in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb632630.aspx	
Using Desired Configuration Management in Configuration Manager	Desired Configuration Management in Configuration Manager http://technet.microsoft.com/en-gb/library/bb693504.aspx	

Task Description	Section or Link Providing More Information	Additional Notes
Migrate to Native Mode	Administrator Checklist: Migrating a Site to Native Mode: http://technet.microsoft.com/en-gb/library/bb632727.aspx	Once the Configuration Manager deployment has been completed successfully, the healthcare IT Administrator should decide if the site will be configured as native mode.

Table 53: Configuration Manager Deployment Approach

8 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 23 acts as a high-level checklist, illustrating the critical components for which an IT Professional is responsible for maintaining in a managed and operational Configuration Manager:

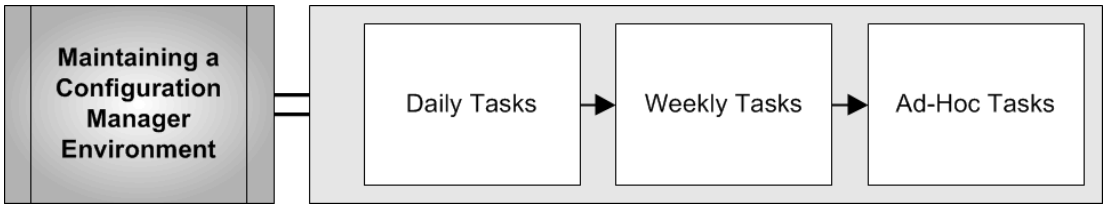


Figure 23: Sequence for Operating Configuration Manager

8.1 Maintaining a Configuration Manager Environment

In order to ensure that Configuration Manager continues to operate effectively, a maintenance plan should be developed. This maintenance plan should include the maintenance tasks and site monitoring tasks that are described in the TechNet article *Maintaining Configuration Manager 2007*[35].

> **Note**
>
> This section describes how to carry out the tasks that are specific to the guidance in this document and should not be considered a complete list of tasks.

After a maintenance plan has been developed for all Configuration Manager sites, the details of the plan should be documented so that it is easy to review and update. Having a maintenance plan document also simplifies the monitoring of maintenance throughout the hierarchy. Documenting the plan is especially important in large hierarchies where there can be many Configuration Manager administrators. You can provide the plan document to the Configuration Manager administrators that are responsible for site maintenance to ensure that sites are maintained as planned.

[35] Microsoft TechNet: Maintaining Configuration Manager 2007 **{R31}**: http://technet.microsoft.com/en-us/library/bb693882.aspx

Table 54 shows the tasks that are specific to this guidance document:

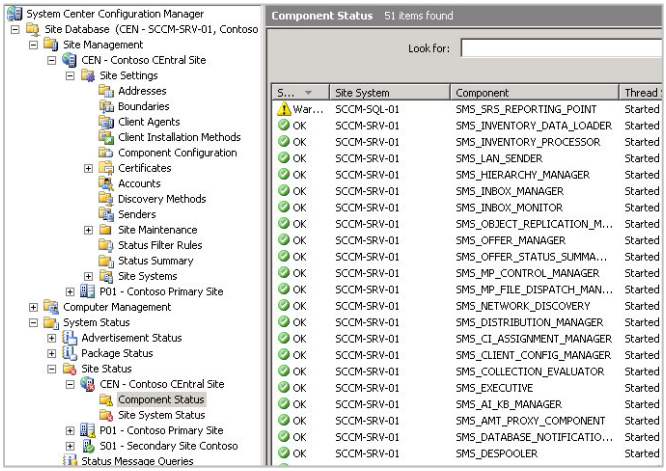
Frequency	Task Description	Further Information
Daily	Check General Configuration Manager State	Section 8.1.1.1
Daily	Check Windows Event Logs	Section 8.1.1.2
Daily	Check Available Disk Space	Section 8.1.1.3
Daily	Ensure Configuration Manager Backup Task is Configured	Section 8.1.1.4
Weekly/Ad hoc	Check Boundary Configuration	This task should be completed frequently if Configuration Manager clients are being added or network changes are occurring, and less frequently if the environment is more static. Section 8.1.2.1
Weekly	Run Disk Defragmentation Tools	Section 8.1.2.2
Ad hoc	Restore Backup into Test Environment	Section 8.1.3.1

Table 54: Configuration Manager Operations Tasks

8.1.1 Daily Tasks

8.1.1.1 Check General Configuration Manager State

The Configuration Manager status system gives the Configuration Manager Administrator the ability to quickly see the overall state of the Configuration Manager environment. The Configuration Manager Status Summariser displays the information to the administrator and summarises the information by either Configuration Manager component or by Site System. This information is forwarded upwards throughout the Configuration Manager hierarchy allowing the administrator to easily check the functional status of a Configuration Manager site, Site System or Site System Component. Table 55 shows the steps for checking the site status messages.

Step	Description	Screenshot
1.	Open the **Configuration Manager Console,** navigate to the **Component Status** node within the console and ensure that there are no errors or warnings in the right pane. If there are any errors or warnings, right-click on the component and select **Show Messages > All**. This will start the status message viewer where it is possible to investigate the cause of the issue.	

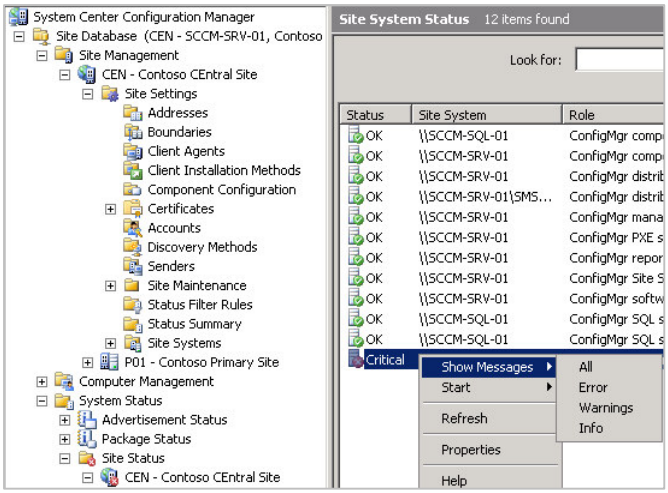
Step	Description	Screenshot
2.	Navigate to the **Site System Status** node within the console and ensure that there are no errors or warnings. If there are any errors or warnings, right-click the site system and select **Show Messages > All**. This will start the status message viewer where the cause of the issue can be investigated.	

Table 55: Viewing Configuration Manager Status Messages

> **Note**
> When a component is experiencing issues, Configuration Manager will set its icon to either Warning ⚠ or Critical ⛔. These icons will be reset after 24 hours providing the issue has been resolved. To accelerate this, it is possible to right-click the component and select **Reset Counts**. This process will take a few minutes to complete and will be reflected in the console.

8.1.1.2 Check Windows Event Logs

The Windows Event Log can be used to determine if any issues are being experienced on the server that may not be immediately obvious, but could be causing performance or other issues that may affect Configuration Manager.

To start the Windows Event Log Viewer, run Eventvwr.msc from the **Start > Run** dialog box.

8.1.1.3 Check Available Disk Space

The Configuration Manager status system also collects data on available disk space for all Configuration Manager Site Systems. Using the Site System Status node allows the administrator to quickly check the levels of free disk space on every server within the hierarchy. Table 56 shows the steps for checking free disk space on Configuration Manager site systems:

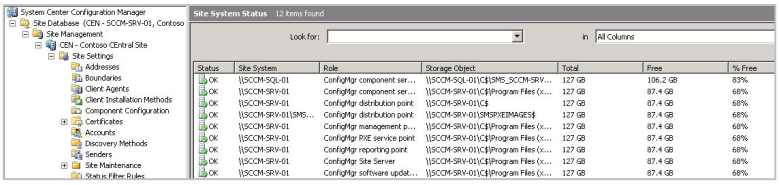
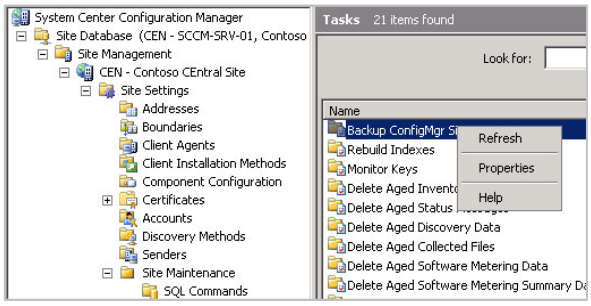
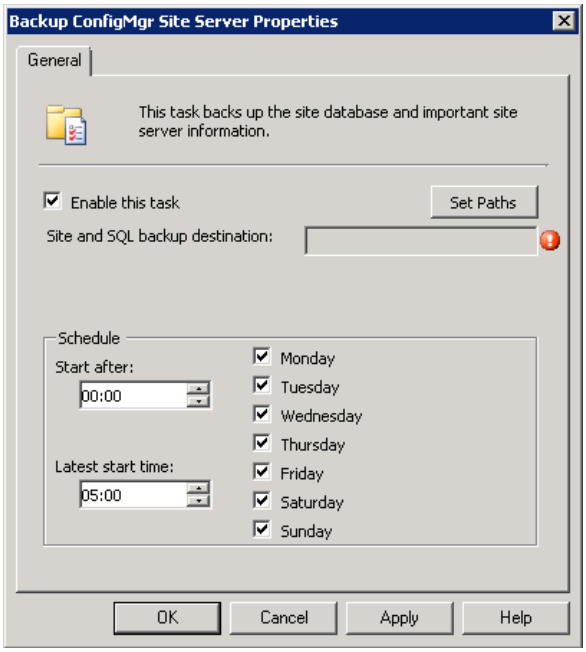
Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Site System Status** node. Each Site System will have **Total**, **Free** and **%Free** columns detailing the free space. This information may be repeated if the server hosts more than one Site System role.	

Table 56: Checking Site System Free Disk Space

8.1.1.4 Ensure Configuration Manager Backup Task is Configured

The Configuration Manager Backup Task is configured via the Administrator Console, and performing this task is the recommended way of ensuring that a successful backup of any Configuration Manager server takes place. Table 57 shows the process for configuring the Configuration Manager backup task.

> **Warning**
>
> If the server is backed up by another means, it is still important that the healthcare IT Administrator ensures that the Configuration Manager Backup task is run. Configuration Manager stores data in the Registry, the Configuration Manager database and the file system, and it is important that this information is backed up simultaneously to ensure a successful restore. The Configuration Manager Backup task takes all the necessary steps to ensure data consistency, so that no further administrative effort is required. The Configuration Manager backup task includes all data from the Registry, Configuration Manager Database and the file system and contains all the data specific to Configuration Manager that is required for a restore.

Step	Description	Screenshot
1.	Open the **Configuration Manager Console** and navigate to the **Tasks** node for the primary site. In the right pane, right-click on the **Backup ConfigMgr Site Server** task and select **Properties**.	
2.	Select **Enable this task**. Configure the **Schedule** to run on a nightly basis. Click **Set Paths**.	

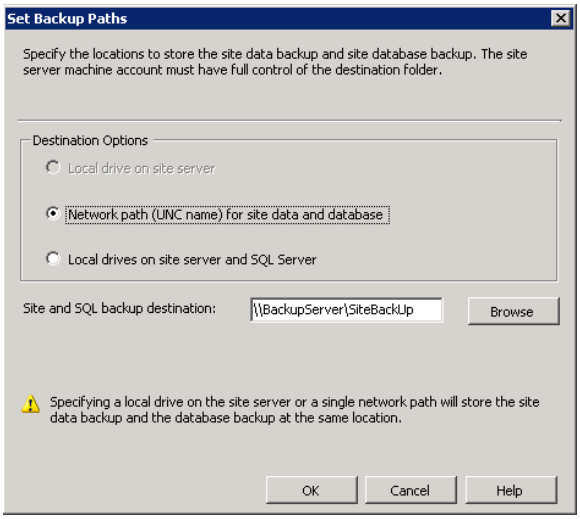
Step	Description	Screenshot
3.	Click **Network path (UNC name) for site data and database** and specify the network share where the data is to be stored. This share must be accessible to the site server machine account. It is also possible to configure the backups to write to the local disk on both the site server and the SQL server, if they are separate.	

Table 57: Configuring the Configuration Manager Backup Task

By following the steps in Table 57, the healthcare IT Administrator ensures that all relevant files and data are backed up to the location specified. Additionally, utilise the health organisation's standard backup methods to back up the files that are created by the Configuration Manager Backup Task, for example, using a tape backup solution. The backup task will overwrite itself each time it is executed, so using the health organisation's backup solution allows the healthcare IT Administrator to create an archive of previous backups, which can be used if there is a need to restore.

For additional information relating to backup for Configuration Manager, refer to the TechNet articles *Backing up Configuration Manager Sites*[36] and *Tasks for Backing Up a Site*[37].

8.1.2 Weekly Tasks

8.1.2.1 Check Boundary Configuration

Boundaries are extremely important in ensuring that Configuration Manager Software Distribution, Software Updates and Operating System Deployment are functioning as effectively as possible. For this reason, the healthcare IT Administrator should regularly verify that the boundaries for all Configuration Manager sites are configured correctly. This task may not need to be performed weekly, but should be performed whenever any of the network configurations are changed or any new sites are added to the environment. Section 5.2.3.1 covers the procedures for performing this task.

[36] Microsoft TechNet: Backing up Configuration Manager Sites **{R32}**: http://technet.microsoft.com/en-us/library/bb694133.aspx

[37] Microsoft TechNet: Tasks for Backing Up a Site **{R33}**: http://technet.microsoft.com/en-us/library/bb680862.aspx

8.1.2.2 Run Disk Defragmentation Tools

Over time, disk volumes on Configuration Manager Sites become fragmented and site operations, such as distributing large software packages, might significantly increase fragmentation on site servers and distribution points. In order to maintain the performance levels of disk operations it is essential to run disk defragmentation tools on a regular basis. Third-party tools can be used for this task, or the built-in Windows tools can be used by running the following command:

```
C:> Defrag <Volume>
```

In the above example, <volume> is the drive letter to defragment, including the colon (:) after the drive letter.

> **Note**
>
> On a Windows Server 2008 server this task can be scheduled using the Defrag task in the built-in Task Scheduler Library. On Windows 2003 servers a custom task scheduler task can be created to perform the defragmentation.

8.1.3 Ad-Hoc Tasks

8.1.3.1 Restore Backup into Test Environment

It is important to ensure that the Configuration Manager healthcare IT Administrator is familiar with the procedures for restoring a Configuration Manager backup. This is the best way to be fully prepared for a site recovery operation, should the need arise. Further information regarding the Configuration Manager site restore process are outlined in the TechNet articles *Recovering Configuration Manager Sites*[38] and *Tasks for Recovering a Site*[39], and should be performed in a test environment, from time to time, to ensure familiarity.

[38] Microsoft TechNet: Recovering Configuration Manager Sites **{R34}**: http://technet.microsoft.com/en-us/library/bb680751.aspx

[39] Microsoft TechNet: Tasks for Recovering a Site **{R35}**: http://technet.microsoft.com/en-us/library/bb680456.aspx

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
SCCM Training	http://www.microsoft.com/systemcenter/configurationmanager/en/us/learning-resources.aspx	Links to Learning resources available from Microsoft and Microsoft Learning Partners
SCCM Product Documentation	http://www.microsoft.com/systemcenter/configurationmanager/en/us/product-documentation.aspx	Links to product documentation and whitepapers

Table 58: 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 SCCM)	http://www.myitforum.com

Table 59: Supplemental Training Resources

APPENDIX B DOCUMENT INFORMATION

PART I TERMS AND ABBREVIATIONS

Abbreviation	Definition
AISP	Asset Intelligence Synchronization Point
AMT	Active Management Technology
App-V	Microsoft Application Virtualization
BITS	Background Intelligent Transfer Service
CUI	Common User Interface
Configuration Manager	System Center Configuration Manager 2007
CPU	Central Processing Unit
DNS	Domain Name System
DP	Distribution Point
FSP	Fallback Status Point
IBCM	Internet-Based Client Management
IIS	Internet Information Services
IP	Internet Protocol
IPv6	Internet Protocol Version 6
MAC	Media Access Control
MP	Management Point
MSI	Windows Installer Package
NAP	Network Access Protection
NAT	Network Address Translation
NIC	Network Interface Card
NLB	Network Load Balancing
OOBSP	Out of Band Service Point
OS	Operating System
OSD	Operating System Deployment
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PSP	PXE service point
R2	Release 2
RP	Reporting Point
RPC	Remote Procedure Call
RSP	Reporting Services Point
SHVP	System Health Validator Point

Abbreviation	Definition
SLP	Server Locator Point
SMB	Server Message Blocks
SMP	State Migration Point
SMS	Systems Management Server
SP	Service Pack
SRS	SQL Reporting Services
SSL	Secure Sockets Layer
USMT	User State Migration Tool
VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Windows Deployment Server
WebDAV	Web-based Distributed Authoring and Versioning
Windows PE	Windows Pre-Execution Environment
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WSUS	Windows Server Update Services

Table 60: Terms and Abbreviations

PART II REFERENCES

Reference	Document	Version
R1.	System Center Configuration Manager 2007 Software Update Management Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx	1.0.0.0
R2.	System Center Configuration Manager 2007 Operating System Deployment Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx	1.0.0.0
R3.	System Center Configuration Manager 2007 Software Distribution Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/serverbuild/sms.aspx	1.0.0.0
R4.	System Center Configuration Manager 2007 TechCenter: http://technet.microsoft.com/en-gb/configmgr/default.aspx	
R5.	System Center Configuration Manager 2007 TechNet Library: http://technet.microsoft.com/en-gb/library/bb735860.aspx	
R6.	Microsoft TechNet: Software Metering in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb694169.aspx	
R7.	Microsoft Downloads: Configuration Manager 2007 Configuration Pack Catalog: http://www.microsoft.com/technet/prodtechnol/scp/configmgr07.aspx	
R8.	Microsoft TechNet: Desired Configuration Management in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb693504.aspx	
R9.	Microsoft TechNet: Out of Band Management in Configuration Manager 2007 SP1: http://technet.microsoft.com/en-gb/library/cc161989.aspx	
R10.	Microsoft TechNet: Reporting in Configuration Manager 2007: http://technet.microsoft.com/en-gb/library/bb632630.aspx	
R11.	Microsoft TechNet: Mobile Device Management in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb633175.aspx	
R12.	Microsoft TechNet: Network Access Protection in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb693725.aspx	
R13.	Microsoft TechNet: How to Configure Network Load Balancing for Configuration Manager Site Systems: http://technet.microsoft.com/en-gb/library/bb633031.aspx	
R14.	Microsoft TechNet: Planning and Deploying Clients for Configuration Manager 2007: http://technet.microsoft.com/en-gb/library/bb680373.aspx	
R15.	Microsoft TechNet: How to Provision Configuration Manager Client Installation Properties using Group Policy: http://technet.microsoft.com/en-us/library/bb632469.aspx	
R16.	Microsoft TechNet: Firewall Settings for Configuration Manager Clients http://technet.microsoft.com/en-us/library/bb694088.aspx	
R17.	Microsoft TechNet: How to Install Configuration Manager Clients Using Computer Imaging: http://technet.microsoft.com/en-us/library/bb694095.aspx	
R18.	Microsoft TechNet: How to Install Configuration Manager Clients Manually: http://technet.microsoft.com/en-us/library/bb693546.aspx	
R19.	Microsoft TechNet: Security and Privacy for Configuration Manager 2007: http://technet.microsoft.com/en-gb/library/bb680768.aspx	
R20.	Microsoft TechNet: Accounts and Groups in Configuration Manager: http://technet.microsoft.com/en-gb/library/bb693732.aspx	

Reference	Document	Version
R21.	Microsoft TechNet: Configuration Manager Site Modes: http://technet.microsoft.com/en-gb/library/bb680658.aspx	
R22.	Microsoft TechNet: Deploying Configuration Manager Sites to Support Internet-Based Clients: http://technet.microsoft.com/en-us/library/bb680388.aspx	
R23.	IIS.NET: Installing and Configuring WebDAV on IIS 7.0: http://go.microsoft.com/fwlink/?LinkId=108052	
R24.	MSDN: How to: Create a New SQL Server 2005 Failover Cluster (Setup): http://msdn.microsoft.com/en-us/library/ms179530(SQL.90).aspx	
R25.	MSDN: How to: Create a New SQL Server Failover Cluster (Setup): http://msdn.microsoft.com/en-us/library/ms179530.aspx	
R26.	Microsoft Help and Support: How to obtain the latest service pack for SQL Server 2005: http://support.microsoft.com/kb/913089	
R27.	Microsoft Web Site: SQL Server 2008 Homepage: http://www.microsoft.com/sqlserver/2008/en/us/default.aspx	
R28.	Microsoft Help and Support: When a 32-bit process tries to update a string value with a new value that contains the %ProgramFiles% string, the %ProgramFiles% string is converted to the %ProgramFiles(x86)% string in a 64-bit environment: http://support.microsoft.com/kb/960037	
R29.	Microsoft TechNet: About Configuration Manager Client Installation Properties: http://technet.microsoft.com/en-us/library/bb680980.aspx	
R30.	Microsoft TechNet: How to Pre-provision the Trusted Root Key on Clients: http://technet.microsoft.com/en-us/library/bb680504.aspx	
R31.	Microsoft TechNet: Maintaining Configuration Manager 2007: http://technet.microsoft.com/en-us/library/bb693882.aspx	
R32.	Microsoft TechNet: Backing up Configuration Manager Sites: http://technet.microsoft.com/en-us/library/bb694133.aspx	
R33.	Microsoft TechNet: Tasks for Backing Up a Site: http://technet.microsoft.com/en-us/library/bb680862.aspx	
R34.	Microsoft TechNet: Recovering Configuration Manager Sites: http://technet.microsoft.com/en-us/library/bb680751.aspx	
R35.	Microsoft TechNet: Tasks for Recovering a Site: http://technet.microsoft.com/en-us/library/bb680456.aspx	

Table 61: References