System Center Configuration Manager 2007 Software Distribution Guide

Friday, 26 February 2010 Version 1.0.0.0 Baseline

> Prepared by Microsoft



Copyright

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

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

© Microsoft Corporation 2010. All rights reserved.

Disclaimer

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



System Center Configuration Manager 2007 – Software Distribution Guide Prepared by Microsoft, Version 1.0.0.0 Last modified on 26 February 2010

TABLE OF CONTENTS

1	Exe	ecutive Summary	1
2	Intr	oduction	2
	2.1	Value Proposition	2
	2.2	Knowledge Prerequisites	2
	2.2.	1 Skills and Knowledge	2
	2.2.	2 Training and Assessment	6
	2.3	Infrastructure Prerequisites	6
	2.4	Audience	7
	2.5	Assumptions	7
3	Usi	ng This Document	8
	3.1	Document Structure	8
4	Pla	n	10
	4.1	Understanding Configuration Manager Object Security	10
	4.2	Planning Distribution Targeting	11
	4.2.	1 Hardware and Software Inventory	11
	4.2.	2 Discovering Active Directory Objects	11
	4.3	Planning Maintenance Windows	28
	4.4	Configuring Collections for Software Distribution	28
	4.4.	1 Distributing Software to Computers	28
	4.4.	2 Distributing Software to Users	42
	4.4.	3 Distributing Software to User Groups	51
	4.5	Planning Where to Store Application Source Files	63
5	Dev	/elop	64
	5.1	Configuring Configuration Manager Packages	65
	5.1.	1 Creating Packages Using the Create Package From Definition Wizard	68
	5.1.	2 Creating Packages Without Using the Create Package From Definition Wizard	70
	5.2	Creating Configuration Manager Programs	72
	5.3	Securing Configuration Manager Packages	77
	5.4	Copying Configuration Manager Packages to Distribution Points	79
6	Sta	bilise	81
	6.1	Testing the Deployment on Pilot Computers	81
	6.1.	1 Defining Collections for Pilot Computers	81
	6.1.	2 Creating Configuration Manager Advertisements	82
	6.1.	3 Checking the Status of the Deployment	88
	6.1.	4 Validating Successful Deployment	88

7 Deploy	/	89
7.1 De	ploying an Application to Production Computers	89
7.1.1	Defining Collections for Production Computers	90
7.2 Ad	Ivertising Packages to the Production Environment	91
8 Operat	te	93
8.1 Mo	pnitoring a Deployment	93
8.1.1	Using Configuration Manager Reporting	94
8.1.2	Using the Configuration Manager Status System	97
8.2 Ma	anaging Changes to Packages	98
8.3 Re	moving Packages	99
8.4 So	ftware Distribution Security	101
8.4.1	Enforce Role Separation	101
8.4.2	Ensure Appropriate User Interaction	101
8.4.3	Secure Software at the Package Access Level	102
8.4.4	Set Permissions at Package Creation	102
8.4.5	Secure the Package Source Files	102
8.4.6	Client Cache Considerations	102
APPENDIX	A Skills and Training Resources	103
PART I	Training Resources	103
PART II	Supplemental Training Resources	103
APPENDIX	B Document Information	104
PART I	Terms and Abbreviations	104
PART II	References	105

1 EXECUTIVE SUMMARY

The software distribution feature of System Center Configuration Manager 2007 R2 (Configuration Manager) provides the capability to distribute and install software to any client machines within a healthcare organisation. Combined with the reporting and software inventory features, it represents a complete solution to software distribution and management of the Windows[®] client and server estates in a healthcare organisation.

The System Center Configuration Manager 2007 Software Distribution Guide provides information and guidance to help healthcare IT Administrators to quickly and reliably use the software distribution feature of System Center Configuration Manager. This guide can be used to aid healthcare organisations who have already deployed Configuration Manager, or can be used in conjunction with the System Center Configuration Manager 2007 Deployment Guide¹ to deploy Configuration Manager within the healthcare organisation.

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



2 INTRODUCTION

2.1 Value Proposition

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

- Understand which software distribution strategies are available and how to configure them
- Create collections for software distribution targeting
- Create software distribution packages to target computers, users or user groups

This document provides the information required to quickly become familiar with the software distribution feature and understand the appropriate decisions that need to be made in order to deploy and use the solution. It also provides step-by-step guidance showing how to create the objects required within Configuration Manager to perform the software distribution.

This guidance has been created to reduce the amount of time the healthcare IT Professional needs to implement and use software distribution using an existing Configuration Manager infrastructure. This infrastructure may have been created using the guidance in *System Center Configuration Manager Deployment Guide* **{R1}** or may have been separately installed and configured.

2.2 Knowledge Prerequisites

To effectively implement the recommendations made throughout this document, a number of knowledge-based and environmental infrastructure prerequisites should be in place. This section outlines the knowledge and skills required to use the *System Center Configuration Manager 2007 Software Distribution* guidance, while section 2.3 details the necessary infrastructure prerequisites.

Section 2.2.1 details the prerequisite skills and knowledge, and section 2.2.2 details the information and suggested training resources or skill assessment.

2.2.1 Skills and Knowledge

The technical knowledge and minimum skills required to use the *System Center Configuration Manager 2007 Software Distribution guidance* are discussed in the following sections:

2.2.1.1 Configuration Manager 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 a healthcare IT Professional visiting every location where the software is required, and manually installing it. The automated process of software distribution eliminates the need to travel to the client location and helps prevent 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 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 healthcare 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. Sections 2.2.1.1.1 to 2.2.1.1.7 describe the key components that relate to software distribution.



2.2.1.1.1 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 at a later time, automatically become members of the collection. Configuration Manager clients that initially meet the collection's criteria, but then no longer meet the criteria, are automatically removed from the collection (this does not result in 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. A program 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 Microsoft Windows[®] XP upgrade to Windows Vista.
- 4. The newly-upgraded Configuration Manager clients automatically become members of the 'All Windows Vista Systems' collection.
- 5. The program that was distributed to the 'All Windows Vista Systems' collection automatically becomes available to the newly-upgraded Configuration Manager clients (along with any other programs that are available to the 'All Windows Vista Systems' collection).

2.2.1.1.2 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 prompt, 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. A 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 need to be defined for the same set of source files.

A copy of the source files must be distributed to one or more servers that are 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 performs 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.

2.2.1.1.3 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 also typically has at least one program, and can have as many programs as needed.

2.2.1.1.4 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 Windows[®] 7) or **Add or Remove Programs** (Windows XP and Windows 2000) in Control Panel.

2.2.1.1.5 Understanding Windows Installer Source Location Manager

Windows Installer Source Location Manager allows Configuration Manager clients to dynamically update Windows Installer network locations. It does this on a per-product basis, and only updates source network locations for those Windows Installer products currently installed on the computer. It will support both per-machine and per-user installations. There are three main methods by which the Windows Installer locations are updated:

- Execution of a Configuration Manager program that contains Windows Installer information
- An administrator-defined recurring schedule
- Configuration Manager client roaming to a location supported by a different management point

Maintaining a valid network source path for an installed Windows Installer product is valuable when the user needs to make an addition to their installed components, when a product repair is triggered, or when the original files are required as part of the patching process. If Configuration Manager is aware of the product source locations, when a client roams away from its home site, the Configuration Manager client will update Windows Installer with the local path to the source files. If Windows Installer then requires access to the source files for the application as part of any addition or maintenance, it will contact the local DP rather than connecting to the location from where the application was originally installed. This can prevent Windows Installer from connecting to installation shares across a Wide Area Connection (WAN) connection.

2.2.1.1.6 Software Distribution Security

Configuration Manager software distribution is a powerful feature that can be used as a major point of attack if not secured properly. When installing packages, Configuration Manager can use elevated rights in either the user or the system context, even if the user does not have administrative rights. This allows an attacker to effectively run any attacks that require elevated rights.



Security guidance specific to the software distribution feature of Configuration Manager has been included, where appropriate, throughout this guidance, and is repeated in section 8.4 to provide the healthcare IT Administrator with a single reference point, where all software distribution security considerations can be reviewed.

2.2.1.1.7 How Software Distribution Works

To distribute software to Configuration Manager clients, a software distribution package and program 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 1 shows a high-level overview of the software distribution process in Configuration Manager:



Figure 1: Software Distribution Overview

Step	Description		
1.	The Configuration Manager site server copies the package source files to the Distribution Points (DPs) 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 MP. The policies contain information on which 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 to have fast or slow connections to the DP 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 1: S	oftware Distribution Overview Steps		

Table 1 shows the steps involved in the software distribution process:

2.2.2 Training and Assessment

Guidelines on the basic skill sets that are required in order to make best use of the *System Center Configuration Manager 2007 Software Distribution guidance* are detailed in APPENDIX A. These represent the training courses and other resources available. All courses mentioned are optional and can be provided by a variety of certified training partners.

2.3 Infrastructure Prerequisites

The following are prerequisites for using a Configuration Manager 2007 infrastructure for software distribution.

- An existing System Center Configuration Manager 2007 R2 infrastructure with SP2 or above
- 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 (including R2) required for all server clients
- Configuration Manager client deployed to clients
- 'Configuration Manager Software Updates' feature enabled for Configuration Manager clients

2.4 Audience

The guidance contained in this document is targeted at a variety of roles within the healthcare IT organisations. Table 2 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 2: Document Audience

2.5 Assumptions

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

3 USING THIS DOCUMENT

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

3.1 Document Structure

This document contains five sections that deal with the project lifecycle, as illustrated in Figure 2 and the list below:

- 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 *MSF Process Model White Paper²* and *Microsoft Operations Framework 4.0³*. 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.

² MSF Process Model White Paper:

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

³ Microsoft Operations Framework 4.0:

http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofeo.mspx





The sections of this document are shown in Figure 2:

Figure 2: MSF Process Model Phases and Document Structure

4 PLAN

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

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



Figure 3: Sequence for Planning for Software Distribution

4.1 Understanding Configuration Manager Object Security

Almost all objects within Configuration Manager are controlled by Configuration Manager object security. Configuration Manager object security allows the healthcare IT Administrator to control which users have access to various objects within the Configuration Manager Console. This is especially important when using Configuration Manager software distribution because it allows the administrator to grant access for certain Configuration Manager administrative users to information, such as hardware or software inventory, for a specific collection of machines. However, it does not necessarily grant the ability to distribute software to those machines.

Objects in Configuration Manager are made of classes and instances. A class is the type of object, for example, a collection. An instance is a specific occurrence of a class, for example, the 'All

Systems' collection. These security permissions can either be accessed from the **Security** tab on the **Properties** dialog box of each object, or through the **Security Rights** node in the Configuration Manager Console.

For more information on Configuration Manager Object Security, see the TechNet articles entitled *Overview of Configuration Manager Object Security and WMI*⁴ and *Classes and Instances for Object Security in Configuration Manager*⁵.

4.2 Planning Distribution Targeting

Configuration Manager uses collections to target distributions to Configuration Manager clients. Collections can be made up by using direct membership or dynamic queries, built from any of the available information in the Configuration Manager database. This includes hardware attributes, such as free disk space or processor speed, software attributes, such as file version information, and information from Active Directory[®], such as Organizational Unit (OU), Site or security group membership.

When deciding how to deploy software, the healthcare IT Administrator should first decide how the computers or users are to be targeted. Depending on the requirements for targeting, one or more discovery methods will need to be enabled.

Important

The healthcare IT Administrator should review the information provided in this section in order to fully understand the distribution options available. In addition, section 7.1 contains information on how to decide which method should be used when deploying an application into a production environment. Prior to an application being deployed into production, it should be fully tested in a test or pilot environment.

4.2.1 Hardware and Software Inventory

Hardware inventory data can be used to create collections where members have a common hardware characteristic. Software can then be distributed to these collections. For example, this could allow software to be distributed to those Configuration Manager clients that meet the minimum hardware requirements for that software.

The software inventory feature is useful for software distribution. Software inventory data can be used to create collections that are based on file or product data. Software can then be distributed to these collections. For example, this could allow an antivirus program to be distributed only to those Configuration Manager clients that do not have this program installed. More information on collecting hardware and software inventory can be found in the *System Center Configuration Manager 2007 Deployment Guide* **{R1}**.

4.2.2 Discovering Active Directory Objects

Active Directory 'discovery' is the process that finds Active Directory computers, users, user groups and containers by polling the nearest Active Directory domain controller. 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

⁵ Microsoft TechNet: Classes and Instances for Object Security in Configuration Manager **{R3}**: <u>http://technet.microsoft.com/en-us/library/bb632791.aspx</u>



⁴ Microsoft TechNet: Overview of Configuration Manager Object Security and WMI **{R2}**: <u>http://technet.microsoft.com/en-us/library/bb632332.aspx</u>

Active Directory Security Group Discovery

Plan to specify the containers to be polled, such as specific domains, sites, 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; 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 site server computer account, depending on the security mode that Configuration Manager is running in. When the 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.

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. See the System Center Configuration Manager 2007 Deployment Guide {R1} for information on Configuration Manager client installation and discovery.	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.
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.

Table 3 lists and compares the Active Directory discovery methods used in this guidance:

Table 3: Active Directory Discovery Methods and Comparisons

4.2.2.1 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. Users might have been added, removed, or changed in Active Directory, since the most recent poll.

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 4 shows the Active Directory User Discovery method targets:

Table 4: Active Directory User Discovery Targeting

Table 5 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	System Center Configuration Manager Site Database (C01 - SCCM-SRV-01, Central Site Site Management Site Management Site Management Site Management Site Settings Configuration Site Settings Client Agents Client Installation Methods Component Configuration Certificates Certificates Scoutes Site Maintenance Status Filter Rules Status Summary Site Systems	Discovery Methods 6 items found Look for: Active Directory System Group Discovery Active Directory Security Group Discovery Active Directory User Discovery Active Directory User Discovery Heartbeat Discovery Network Discovery Network Discovery
----	---	---	---

Step	Description	Screenshot
2.	Select Enable Active Directory User Discovery. Click the E button to add a search location.	Active Directory User Discovery Properties General Polling Schedule Active Directory User Discovery Image: Constant Schedule Active Directory User Discovery Active Directory containers: Image: Distinguished Name Recursive Group There are no items to show in this view.
3.	Select Local domain as the location and accept the other default settings. Click OK.	OK Cancel Apply Help New Active Directory Container X Specify an Active Directory container to search during the discovery process. Location • Local domain • Local namespace • Custom LDAP or GC query Path: Path:

Step	Description	Screenshot
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 .	Select New Container
		OK Cancel
5.	Repeat steps 2 to 4 for each container to be searched.	Active Directory User Discovery Properties Image: Constraint of the second

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. Tip Additional attributes can be discovered from Active Directory using the Active Directory attribute tab.	Active Directory User Discovery Properties Image: ConfigMgr can poll Active Directory to discover users and the containers in which they belong. Specify how often to poll Active Directory. Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory to discover users and the containers in which they belong. Specify how often to poll Active Directory. Image: ConfigMgr can poll Active Directory. Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory as soon as poll Active Directory as a poll Active Directory as poll Active Directory as a poll Active Directory as

Table 5: 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.

4.2.2.2 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. Computers might have been added, removed, or changed in Active Directory since the most recent poll.

Table 6 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 6: Active Directory System Discovery Targeting

4.2.2.2.1 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 7 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.

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

System Center Configuration Manager 2007 – Software Distribution Guide Prepared by Microsoft, Version 1.0.0.0 Last modified on 26 February 2010

Туре

Attribute

sAMAccountName

Table 7: Custom Attributes for Active Directory System Discovery

Table 8 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.	System Center Configuration Manager Discovery Methods 6 items found Site Database (C01 - SCCM-SRV-01, Central Site Look for: Look for: Site Settings Addresses Addresses Boundaries Client Agents Client Agents Client Installation Methods Component Configuration Active Directory System Group Discovery Consonent Configuration Corponent Configuration Active Directory System Discovery Accounts Discovery Methods Name Stet Maintenance Status Silter Rules Status Systems Site Systems Site Systems
2.	Select Enable Active Directory System Discovery. Click the State button to add a search location.	Active Directory System Discovery Properties Image: Constraint of the system Discovery Image: Constraint of the system Discovery Image: Constraint of the system Discovery Active Directory System Discovery Image: Constraint of the system Discovery Active Directory containers: Image: Constraint of the system Discovery Distinguished Name Recursive Group There are no items to show in this view. Image: Constraint of the system Discovery OK Cancel Apply Help Help

Step	Description	Screenshot
3. Select L the othe Click Ol	Select Local domain as the location and accept the other default settings. Click OK .	New Active Directory Container Specify an Active Directory container to search during the discovery process. Location • Local domain • Local namespace • Custom LDAP or GC query Path;
		Browse Search options Recursive Include groups OK Cancel
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.	Select New Container
		OK Cancel

Step	Description	Screenshot
5.	Repeat steps 2 to 4 for each container to be searched.	Active Directory System Discovery Properties
		General Polling Schedule Active Directory attribute
		Active Directory System Discovery
		Enable Active Directory System Discovery
		Active Directory containers:
		Distinguished Name Recursive Group
		LDAP://OU=Servers,DC=contoso,DC Yes Excluded
		LDAP://CN=Computers,DC=contoso,D Yes Excluded
6.	Click the Polling Schedule tab.	Active Directory System Discovery Properties
	Select Run discovery as soon as possible . Click Schedule to specify an ongoing schedule for the discovery process.	General Polling Schedule Active Directory attribute
		ConfigMgr can poll Active Directory to discover security groups and the
	Click OK .	Directory.
	Тір	· · · · · · · · · · · · · · · · · · ·
	Additional attributes can be discovered from Active Directory using the Active Directory attribute tab.	Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00
	1	Schedule
		Run discovery as soon as possible
		Note: This check box is cleared after the discovery request is made to the site database.
		UN Cancel Apply Help

Table 8: 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**.

4.2.2.3 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 9 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 9: Active Directory System Group Discovery Targeting

Table 10 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 .	System Center Configuration Manager System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, C Site Management Control of the Management Site Settings Clent Agents Clent Agents Clent Installation Methy Clent Installation Methy Component Configuration Active Directory System Group Discovery Active Directory User Discovery Heartbeat Discovery Network Discovery Network Discovery Network Discovery

Step	Description	Screenshot
2.	Select Enable Active Directory System Group Discovery. Click the E button to add a search location.	Active Directory Security Group Discovery Properties General Polling Schedule Image: Active Directory Security Group Discovery Image: Enable Active Directory Security Group Discovery Active Directory containers: Image: Distinguished Name Recursive Group There are no items to show in this view.
2 Salast Level demain as the leveling of	Select Local domain as the location and accent	OK Cancel Apply Help
	the other default settings. Click OK .	Specify an Active Directory location in which to search for the container. If you want to specify a custom LDAP or GC location query, enter the query in the path edit box. Location Local domain Local forest Local forest Local forest Browse Search options Recursive Include groups OK Cancel Help

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 .	Select New Container
		OK Cancel
5.	Repeat steps 2 to 4 for each container to be searched.	Active Directory System Discovery Properties General Polling Schedule Active Directory System Discovery Image: Contract Control Contract Control Contervet

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. 	Active Directory System Discovery Properties Image: ConfigMage Containers in which they belong. Specify how often to poll Active Directory. Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Image: Polling Schedule Schedule Polling schedule Schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Schedule Image: Polling Schedule Schedule Image: Polling Schedule Schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Schedule Image: Polling Schedule Schedu

Table 10: 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**.

4.2.2.4 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 11 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 11: Active Directory Security Group Discovery Targeting

Table 12 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 .	System Center Configuration Manager Discovery Methods 6 items found Site Database (C01 - SCCM-SRV-01, Central Site Look for: Look for: Site Stings Site Stings Addresses Boundaries Clent Agents Addresses Clent Installation Methods Certificates Active Directory System Group Discovery Active Directory System Discovery Active Directory System Discovery Active Directory System Discovery Active Directory Discovery Active Directory System Discovery Active Directory System Discovery Active Directory System Discovery Active Directory System Discovery Active Directory System Discovery Heartbeat Discovery Active Directory System Discovery Heartbeat Discovery Status Filter Rules Status Summary Status Summary Site Systems
2.	Select Enable Active Directory Security Group Discovery. Click the 🕅 button to add a search location.	Active Directory Security Group Discovery Properties General Polling Schedule Image: Active Directory Security Group Discovery Image: Active Directory Security Group Discovery Active Directory containers: Image: Distinguished Name Recursive Group There are no items to show in this view.
		OK Cancel Apply Help

Step	Description	Screenshot
 Select Local domain as the location and accept the other default settings. Click OK. 	Select Local domain as the location and accept the other default settings. Click OK.	New Active Directory Container
		Location Local domain Local namespace Custom LDAP or GC query Path: Browse, Browse,
	OK Cancel Help	
4.	Select the container that contains the user groups that Configuration Manager will discover. Click OK .	Select New Container
		Image: Contoso Image: Computers Image: Computers </td
		OK Cancel

Step	Description	Screenshot
5.	Repeat steps 2 to 4 for each container to be searched.	Active Directory Security Group Discovery Properties Image: Comparison of the security Group Discovery General Polling Schedule Active Directory Security Group Discovery
		Image: Security Group Discovery Active Directory containers: Distinguished Name Recursive Group LDAP://CN=Computers,DC=contoso,D Yes Excluded LDAP://OU=Servers,DC=contoso,DC Yes Excluded IDAP://OU=Servers,DC=contoso,DC Yes Excluded IDAP://OU=Servers,DC=contoso,DC Yes IDAP://OU=Servers,DC=contoso,DC Yes IDAP://OU=Servers,DC=contoso,DC Yes IDAP://OU=Servers,DC=contoso,DC Yes IDAP://IDAP://IDAP IDAP://IDAP IDAP://IDAP IDAP://IDAP IDAP://IDAP IDAP
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 .	Active Directory Security Group Discovery Properties Image: ConfigMgr can poll Active Directory to discover security groups and the containers in which they belong. Specify how often to poll Active Directory. Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Image: ConfigMgr can poll Active Directory to discover security groups and the containers in which they belong. Specify how often to poll Active Directory. Polling schedule Occurs every 1 day(s) effective 01/01/1998 00:00 Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory. Image: Run discovery as soon as possible Image: ConfigMgr can poll Active Directory as soon as possible Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: ConfigMgr can poll Active Directory. Image: Con
		OK Cancel Apply Help

Table 12: 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**.



4.3 Planning Maintenance Windows

Maintenance windows allow the healthcare IT Administrator to define specific times that a Configuration Manager client will perform tasks, such as software distribution and software updates. This can be particularly useful when dealing with critical clinical machines, such as operating theatre equipment and servers. Maintenance windows are configured on a collection, and the settings will apply to all machines within that collection. If a machine is a member of multiple collections that all have maintenance window settings configured, the client will adhere to all maintenance windows. It is important to make sure that a machine is not a member of a number of collections that will enforce too strict a maintenance window policy, as this may prevent any software updates or software distributions from occurring. If this is suspected, the healthcare IT Administrator can use the *Maintenance Windows Available to a Particular Client* report. Section 4.4.1.3 shows the process for configuring maintenance windows for a collection.

4.4 Configuring Collections for Software Distribution

4.4.1 Distributing Software to Computers

When distributing software to computers, there are two different approaches that can be taken, based on requirements. The first approach uses 'direct membership' collections, which involves manually adding all relevant machines into the collection to receive software. This approach is useful when there are no unique system attributes, such as allowing for a dynamic query or for targeting small numbers of computers quickly and easily. See section 4.4.1.1 for the steps to take to configure a direct membership collection.

The second approach is to use 'dynamic query' collections, which are based on hardware or software inventory data. Using this approach, the healthcare IT Administrator can target software to machines based on common attributes that the machines share. For example, a collection to target an update for Microsoft[®] Office could be based on a dynamic query collection containing all machines running an older version than the one being advertised. See section 4.4.1.2 for the steps to take to configure a dynamic query collection.

Caution

For Configuration Manager clients with Windows Terminal Services enabled (Remote Administration mode or Application Server mode), software distribution icons and messages are limited to the console session. On Configuration Manager clients that are remotely controlled using Remote Assistance, Remote Desktop, or Configuration Manager Remote Control, software distribution icons function correctly. It should be noted that software distribution functionality to site systems that have Windows Terminal Services enabled is limited.

4.4.1.1 Direct Membership Collections for Systems

Table 13 shows the process for creating and configuring a direct membership collection for systems:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Computer Management > Collections node. Right-click the Collections node and select New Collection.	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contosc Site Management Computer Management Computer Management Computer Management Sol Export Objects Sol Export Objects Sol Update Collection Membership Sol Update Collection Membership Sol Distribute Sol Transfer Site Settings
2.	In Name, enter an appropriate name for the collection, and if required, enter a Comment and then click Next. Note It is good practice to decide on a collection naming strategy so that collections can be easily identified by their purpose.	New Collection Wizard Image: Constraint of the collection of the collectio
3.	For Direct Membership collections, ensure that the Update this collection on a schedule check box is clear. Click the is button to add a new direct membership rule.	Yew Collection Wizard Image: Security General Collection membership rules determine which resources are included in the collection when it is updated. A membership rules can be a direct assignment or a query. Advettsements Security Security Membership rules: Progress Confirmation Confirmation There are no items to show in this view. Update this collection on a schedule Occurs every 1 day(s) effective 16/10/2009 13:55 Schedule Schedule





Step	Description	Screenshot
10.	Click Next.	New Collection Wizard X Advertisements General Membership Rulas The programs currently being advertised to this collection are listed below. Advertisements Security Progress Confirmation Confirmation There are no Rems to show in this view.
11.	If additional users or groups need to be able to administer this collection, click in the Instance security rights section to modify the rights and add the required users or groups. Click Next .	New Collection Wizard X Security Security General Membership Rules Advertisements Class security rights: Security X Progress Confirmation Confirmation Instance Read, Modify, Delete, Use remote t Instance security rights: X Mane Permissions CONTOSOlyadministrator Read, Modify, Delete, Use remote t Name Permissions CONTOSOlyadministrator Read, Modify, Delete, Use remote t Name Permissions CONTOSOlyadministrator Read, Modify, Delete, Use remote t
12.	Click Close.	New Collection Wizard X Confirmation Confirmation General Details: Membership Rules Bereral Advertisements Security Progress Security Confirmation Security To finish the wizard, click Close. To finish the wizard, click Close.

Table 13: Configuring a Direct Membership Collection for Systems
4.4.1.2 Dynamic Query Collections Based on Hardware or Software Inventory

Table 14 below shows the steps involved in creating an example dynamic query membership collection. In this example, the collection membership is based on a machine running Windows XP SP2. This example is used to demonstrate the flexibility in building collections by dynamic query, because all hardware and software inventory information is available to form the dynamic query. Table 14 shows the process for creating a dynamic query membership collection:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Computer Management > Collections node. Right-click the Collections node and select New Collection.	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contosc Site Management Computer Management Collection Sol Export Objects Sol Export Objects Sol Update Collection Membership Sol Update Collection Membership Sol Distribute Sol Transfer Site Settings
2.	In Name , enter the name for the collection, and if required, enter a Comment . Click Next .	New Collection Wizard 🔀
	Note It is good practice to decide on a collection naming strategy so that collections can be easily identified by their purpose.	General Membership Rules Membership Rules Advertisements Security Progress Confirmation Comment: This is an example collection for dynamic query collections Last update The collection has not been updated yet. Last membership change The collection has not been updated yet. Security Provides Rest Provides Provides Rest Provides Provides Last update The collection has not been updated yet. Contentship change The collection has not been updated yet.
3.	For dynamic query collections, ensure that the Update this collection on a schedule check box	New Collection Wizard
	is selected. Click Schedule to modify the default setting of 1 day, if required. Click the setting button to add a new dynamic query rule.	General Collection membership rules determine which resources are included in the collection when it is updated. A membership rules can be a direct assignment or a query. Advertsementa Security Progress Confirmation Rule Type Undate this collection on a schedule Occurs every 1 day(s) effective 16/10/2009 15:47 Concel

Step	Description	Screenshot
4.	In Name, enter a name for the query rule.	Query Rule Properties
	For this example, ensure that Resource Class is set to System Resource .	General
	Leave Collection limiting set to Not collection limited.	Name: All Windows XP Service Pack 2 Systems
	Note Limiting collections allows the query to be further limited to a group of systems. This allows for more granular control over collection membership. Click Edit Query Statement.	Import Query Statement Resource dass: System Resource Edit Query Statement Collection limiting Not collection limited Limit to collection: Browse
		OK Cancel Help
Э.	Click the $\underbrace{\text{Criteria}}_{\text{Ellock}}$ button to add a new criterion.	Dynamic Query System Collection Query Statement Properties X General Criteria Joins You can specify criteria to narrow the query and limit the results that are
		returned. Criteria:
		Show Query Language OK Cancel Help

Step	Description	Screenshot
6.	Click Select.	Criterion Properties General Image: Criterion Properties Criterion Type: Simple value Where: Select Operator: Value: Type: String Value
7.	Select Operating System from the Attribute class drop-down list. Select <no alias=""> from the Alias as drop-down list. Select Build Number from the Attribute drop- down list. Click OK.</no>	Select Attribute X Attribute class: Operating System Alias as: <no alias=""> Attribute: Build Number OK Cancel</no>

Step	Description	Screenshot
Step 8.	Description Select Simple value from the Criterion Type drop-down list and select is equal to from the Operator drop-down list. In Value, enter 2600 (this is the build number for Windows XP). Tip Click Values to show all possible values for the attribute. Click OK.	Screenshot Criterion Properties General Image: Criterion Properties Criterion Type: Simple value Where: Operating System - Build Number Select Operator: is equal to Value:
9.	This query will now gather all systems that are running any version of Windows XP. Click the 🔀 button to add a new criterion.	Type: String Value OK Cancel Help Dynamic Query System Collection Query Statement Properties X General Criteria Joins You can specify criteria to narrow the query and limit the results that are
		returned. Criteria: Operating System.Build Number is equal to "2600"
		Show Query Language OK Cancel Help

Step	Description	Screenshot	
10.	Click Select.	Criterion Properties General Image: Criterion Properties Criterion Type: Simple value Where: Select Operator: Value: Type: String Value	
11.	Select Operating System from the Attribute class drop-down list. Select <no alias=""> from the Alias as drop-down list. Select CSD Version from the Attribute drop- down list. Click OK.</no>	OK Cancel Help Select Attribute Attribute class: Operating System Alias as: <no alias=""> Attribute: CSD Version OK Cancel Help</no>	

Step	Description	Screenshot
12.	Select is equal to from the Operator drop-down list. Select Service Pack 2from the Value drop-down list. Tip Click Values to show all possible values for the attribute. Click OK.	Criterion Properties General Image: Criterion Properties Criterion Type: Simple value Where: Operating System - CSD Version Select Operator: is equal to Value: Service Pack 2 Type: String Value
13.	Click OK three times to return to the New Collection Wizard and click Next .	OK Cancel Help New Collection Wizard X Image: State of the sta
		General Collection membership rules determine which resources are included in the collection when it is updated. A membership rule can be a direct assignment or a query. Advertisements Security Progress Membership rules: Confirmation Rule Rule Type If Windows XP Service Pack 2 Systems Query Course every 1 day(s) effective 16/10/2009 15:47 Course Next> Concel
14.	Click Next.	New Collection Wizard
		Advertisements General Membership Rules Advertisements Security Progress Confirmation The programs currently being advertised to this collection are lated below. Advertisements: Program Package Collection There are no items to show in this view. Image: Confirmation There are no items to show in this view.

System Center Configuration Manager 2007 – Software Distribution Guide Prepared by Microsoft, Version 1.0.0.0 Last modified on 26 February 2010



Table 14: Configuring a Dynamic Query Collection for Systems Based on Inventory

4.4.1.3 Configuring Maintenance Windows for a Collection

Maintenance windows allow the healthcare IT Administrator to schedule times that Configuration Manager clients will be allowed to install software updates and software distribution packages. See section 4.3 for more information on maintenance windows. Table 15 shows the process for configuring maintenance windows:

Step	Description	Screenshot
1.	Open the Configuration Manager Console , right-click on the collection for which the maintenance window will be configured, and select Modify Collection Settings .	 Software Updates Collections Test Clients () Conflicting Records Software Distribution Software Updates Software Metering Software Metering Reporting Reporting Serving Mobile Device Manage Clear Last PXE Advertisement Advertise Task Sequence Modify Collection Settings Out of Band Management
2.	On the Maintenance Windows tab, click the 'New maintenance window' button	Test Clients (Monthly Update) Settings X Maintenance Windows Collection Variables Advanced Out of Band Maintenance windows define times during which ConfigMgr can apply advertisements and software update deployments to computers in this collection. Maintenance windows: Image: Collection Provide the provided t
		OK Cancel Help

 3. Enter a Name for the maintenance window. Specify a schedule using the settings in Time and Recurrence pattern. The maintenance window can be configured for a one-off event or on a recurring schedule. Click OK. 4. Click OK. A Click OK. A Note The maintenance window can be turned on and off by selection, if required. A State Schedule apples only to operating system deployment task. sequences windows: Collection Variables Advanced Out of Band Maintenance Windows: Collection Variables Advanced Out of Band Maintenance windows can be configured on a single collection, if required. A State Schedule apples only to operating system deployment task. sequences A State Schedule apples only to operating system deployment task. sequences A State Schedule apples only to operating system deployment task. sequences A State Schedule apples only to operating system deployment task. sequences A State Schedule apples only to operating system deployment task. sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating system deployment task. Sequences A State Schedule apples only to operating syste	Step	Description	Screenshot
4. Click OK. Note The maintenance window can be turned on and off by selecting and clearing the check box. Multiple maintenance windows can be configured on a single collection, if required. Maintenance windows:	3.	Enter a Name for the maintenance window. Specify a schedule using the settings in Time and Recurrence pattern . The maintenance window can be configured for a one-off event or on a recurring schedule. Click OK .	Image: Test Maintenance Windows Time Effective date: 21/09/2009 Start: 01:00:00 Duration: 3 Hour(s) 0 Minute(s) Image: Image: Recurrence pattern Recur every None Recur every Weekly Sunday Monthly Monday Daily Tuesday This schedule applies only to operating system deployment task sequences
	4.	Click OK. Note The maintenance window can be turned on and off by selecting and clearing the check box. Multiple maintenance windows can be configured on a single collection, if required.	Test Clients (Monthly Update) Settings Imaintenance Windows Maintenance Windows Collection Variables Advanced Out of Band Maintenance windows define times during which ConfigMgr can apply advertisements and software update deployments to computers in this collection. Imaintenance windows: Imaintenance windows: Maintenance windows: Imaintenance windows: Imaintenance windows: Imaintenance windows: Name Description Imaintenance windows: Imaintenance windows: Imaintenance windows: Imaintenance windows: Imaintenance windows: Imaintenance windows: Imaintenance windows: <td< td=""></td<>

Table 15: Configuring Maintenance Windows

Microsoft[®]

4.4.2 Distributing Software to Users

Similar to distributing software to computers, there are two different methods available when creating collections to target software at users. The first method is a 'direct membership' collection, which can be used to group together users who have no other common identifying attributes; and the second is a 'dynamic query' collection, which can be used to group users together by common attributes, such as OU, or even name.

Warning

Healthcare IT Administrators should fully understand any software licensing agreements prior to distributing software. This is especially true when distributing software to users or user groups, because a user can potentially log in to several computers, resulting in the software being installed several times within a healthcare organisation.

4.4.2.1 Direct Membership Collections for Users

Table 16 below shows the steps involved in creating a Direct Membership Collection containing users:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Computer Management > Collections node. Right-click on the Collections node and select New Collection.	Image: System Center Configuration Manager Image: Coll Image: Site Database (CEN - SCCM-SRV-01, Contosc Image: Site Management Image: Site Management Image: Computer Management Image: Site Collection Image: Computer Management Image: Sol Update Collection Membership Image: Computer Management Image: Sol Update Collection Image: Co
2.	In Name , enter the name for the collection and, if required, enter a Comment , and then click Next .	New Collection Wizard X
	Note It is good practice to decide on a collection naming strategy so that collections can be easily identified by their purpose.	General Membership Rules Advertsements Security Progress Confirmation Last update The collection has not been updated yet. Last membership change The collection has not been updated yet.

Step	Description	Screenshot
3.	For Direct Membership collections, ensure that the Update this collection on a schedule check box is clear. Click the subtron to add a new direct membership rule.	New Collection Wizard X Wembership Rules General General Collection membership rules determine which resources are included in the collection when R is updated. A membership rules can be a direct assignment or a query. Advertisements Security Progress Confirmation Rule Type There are no Rens to show in this view. Update this collection on a schedule Occurs every 1 day(s) effective 15/10/2009 13:55 Schedule
4.	Click Next.	Create Direct Membership Rule Wizard
		Webcome Search for Resources Collection Limiting Select Resources Finished This weard helps you create direct membership rules for your collection. In contrast to query-based membership rules, which add all resources matching a set of criteria, direct membership rules and a select the resources you want to add as direct membership rules, you locate and select the resources you want to add as direct membership rules, direct membe
5.	Select User Resource from the Resource class drop-down list. Select User Name from the Attribute name drop-down list. In Value, enter the name of the user to be added to the collection. Tip The wildcard '%' can be entered in the Value field to return all systems, or can be used for partial matching. Click Next.	Create Direct Hembership Rule Wizard X Search for Resources Search for Resources Resources Locate the resource that you want to add as direct members of the collections. Select Resources Find all resources that match the following criteria. Findhed Find all resources that match the following criteria. Resource class: User Resource Type: String Exclude resources marked as obsolete Value: Value: % Note: % Note: For values of type string, use the percent character % as a widdard to match multiple strings and allow partial string matching. Previous Next > Findh

Step	Description	Screenshot
6.	In Search in this collection, enter the name of a collection of which the user is already a member, or click Browse. All Users will contain all users that have been discovered by Configuration Manager. Tip Leaving Search in this collection blank will search all collections providing the administrator has Read access to all collections. Click Next.	Create Direct Hembership Rule Wizard X Vielow Collection Limiting Search fix Resources Select a collection to search for resources in. Select Resources You must enter a collection name if you have insufficient privileges to search the entire resource database. Otherwise, you may leave the field blank. Search in this collection: All Users Multicerist Previous Normal Previous Next > Finish
7.	Select the user from the list displayed and click Next. Note If the wildcard '%' was used previously, all matching results will be returned.	Create Direct Hembership Rule Wizard X Vielone Select Resources Select Resources Select Resources you want to add as direct members to the collection. Collection Limiting Select Resources you want to add as direct members to the collection. Betext Resources Resources: Prished CONTOSO/Administrator (Administrator) CONTOSO/Modimistrator (Administrator) Select All CONTOSO/VMSUser (Mass) Clear All CONTOSO/SCOM_Push (SCOM_Push) Clear All CONTOSO/SCOM_Push (SCOM_Push) Clear All
8.	Click Finish.	Create Direct Hembership Rule Wizard
		Welcome Completing the Create Direct Membership Rule Wizard Search for Resources Collection Limiting Select Resources You have successfully completed the Create Direct Membership Rule Wizard. A new rule will be create Direct Membership Rule Wizard. A new rule will be create for each resource you selected.
		Resources: CONTOSO(NHSUser (NHS User) To create the new rules, dick Finish.
		<previous next=""> Cancel</previous>

Step	Description	Screenshot
9.	Repeat steps 4 to 8 for each new system required to become a member of the collection. Click Next .	New Collection Wizard Image: Collection membership Rules General Collection membership rules determine which resources are included in the collection when it is updated. A membership rule can be a direct assignment or a query. Advertisements Security Progress Confirmation Rule Type CONTOSO(VHSUser (VHS User) Direct Not Applicable V Update this collection on a schedule Occurs every 1 day(s) effective 16/10/2009 16:11 Schedule
10.	Circk Next.	Advertisements General Membership Rules Advertisements Security Progress Confirmation The program Package Collection There are no tens to show in this view.
11.	If additional users or groups need to be able to administer this collection, click K in the Instance security rights section to modify the rights and add the required users or groups. Click Next.	New Collection Wizard X Security Security General Speofy the security rights that users have on this object dass or instance. Advertisements Class security rights: Security Progress Confirmation CONTOSO (Administration: Read, Modify, Delete, Use remote t Instance security rights: X Instance security rights: X

Step	Description	Screenshot
12.	Click Close.	New Collection Wizard Image: Confirmation Ceneral Details: Membership Rules Advertisements Security Progress Confirmation Security To fmish the wizard, click Close. Image: Click Close

Table 16: Configuring a Direct Membership Collection for Users

4.4.2.2 Dynamic Query Collection Based on User Attributes

Table 17 below shows the steps involved in creating a Dynamic Query Membership Collection. In the example shown, the collection membership is based on any user that is in the specified OU.

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Computer Management > Collections node. Right-click on the Collections node and select New Collection.	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contosc Site Management Computer Management Computer Management Computer Management Sol Export Objects Sol Export Objects Sol Update Collection Membership Op Import Objects Sol Distribute
2.	In Name, enter the name for the collection, and if required, enter a Comment, and then click Next. Note It is good practice to decide on a collection naming strategy so that collections can be easily identified by their purpose.	Here Collection Wizard Image: Constant of the collection

Step Description

Screenshot New Collection Wiza

3.	For dynamic query collections, ensure that the Update this collection on a schedule check
	box is selected.
	Click Schedule to modify the default setting of 1
	day, if required.
	day, if required.

Click the 🔲 button to add a new dynamic query rule.

New Collection Wizard	les			
General Membership Rules	Collection membership rule updated. A membership ru	s determine which resour le can be a direct assignn	ces are included in th nent or a query.	e collection when it is
Advertisements Security				
Progress	Membership rules:			📃 🚺 🖼 🗙
Confirmation	Rule	Туре	Limit to	1
	Update this collection of Occurs every 1 day(s) e	n a schedule	47	
				Schedule
		< Previous	Next >	Finish Cancel

4.	In Name, enter a name for the query rule.	Query Rule Properties	×
	For this example, ensure that Resource Class is set to User Resource .	General	
	Leave Collection limiting set to Not collection limited.	Name:	User Collection Based on OU Membership
	Note Limiting collections allows the query to be further limited to a group of users. This allows for more granular control over collection membership Click Edit Query Statement.	Resource dass: Collection limiting Not collection limited Limit to collection:	Import Query Statement User Resource Edit Query Statement Browse
			OK Cancel Help

Step	Description	Screenshot
5.	Click the Criteria tab.	Dynamic Query User Collection Query Statement Properties
	Click the 送 button to add new criteria.	General Criteria Joins
		You can specify criteria to narrow the query and limit the results that are returned.
		Citeria:
		Show Query Language OK Cancel Help
6.	Click Select.	Criterion Properties
		General
		Criterion Properties
		Criterion Type: Simple value
		Where:
		Select
		Operator:
		Value:
		Value
		OK Cancel Help

Step	Description	Screenshot
7.	Select User Resource from the Attribute class drop-down list. Select <no alias=""> from the Alias as drop-down list. Select User OU Name from the Attribute drop-down list. Click OK.</no>	Select Attribute X Attribute class: User Resource Image: Comparison of the second
8.	Select is equal to from the Operator drop-down list. In Value , enter the full name of the OU whose members will be targeted, in the format 'Domain/OU Name'. Tip Click Values to show all possible values for the attribute. Click OK .	Criterion Properties General Image: Criterion Properties Criterion Type: Simple value Where: User Resource - User OU Name Select Operator: is equal to Value: CONTOSO.CO.UK/EXAMPLE ORGANISATIONAL Type: String Value
9.	Click OK twice to return to the New Collection Wizard and click Next.	Image: Security Progress Collection membership rules a direct assignment or a query. Confirmation Collection membership rules a direct assignment or a query. Membership Rules Collection membership rules can be a direct assignment or a query. Membership Rules Collection membership rules can be a direct assignment or a query. Progress Confirmation Rule Type User Collection Based on OU Member Query Currs every 1 day(s) effective 16/10/2009 16:24 Concurs every 1 day(s) effective 16/10/2009 16:24 Centred Schedule

Step	Description	Screenshot
10.	Click Next.	New Collection Wizard X Advertsements Advertsements General Membership Rules The programs currently being advertised to this collection are listed below. Advertisements Advertisements: Progress Confirmation Advertisements: Name Program Package Collection There are no items to show in this view.
11.	If additional users or groups need to be able to administer this collection, click Instance security rights section to modify the rights and add the required users or groups. Click Next.	New Collection Wizard X Security Security General Specify the security rights that users have on this object dass or instance. Membership Rules Advertisements Security Class security rights: Progress Confirmation Confirmation Mance Instance security rights: X Name Permissions CONTOSOlydministrator Read, Modify, Delete, Use remote t Name Permissions CONTOSOlydministrator Read, Modify, Delete, Use remote t Name Permissions CONTOSOlydministrator Read, Modify, Delete, Use remote t Name Permissions CONTOSOlydministrator Read, Modify, Delete, Use remote t
12.	Click Close.	New Collection Wizard X Confirmation Confirmation General Details: Membership Rules Advertsements Security Progress Confirmation Security Progress Security To finish the wizard, click Close.

Table 17: Configuring a Dynamic Query Membership Collection for Users

4.4.3 Distributing Software to User Groups

Using the mechanism of targeting software at user groups can have the advantage of removing some of the system administration from the Configuration Manager administrator, allowing them to delegate this authority to junior administrators. By configuring Configuration Manager to target software at user groups, the collections, packages and advertisements only need to be configured once. All further tasks can then be carried out by adding users to security groups using the 'Active Directory User and Computers' Microsoft Management Console (MMC) snap-in.

When targeting software at users or computers, based on Active Directory security group membership, there are two different options that can be used. Each of these options has its own advantages and disadvantages, as shown in Table 18 below.

Warning

Healthcare IT Administrators should fully understand any software licensing agreements that are in place prior to distributing software. This is especially true when distributing software to users or user groups, because a user can potentially log in to many computers, resulting in the software being installed many times within a healthcare organisation.

Software Targeting Option	Advantage	Disadvantage	Usage
Option 1: Using Group Attributes to Create Collections	This option allows the healthcare IT Administrator to target software at users or computers based on their security group membership, without the need for the user to log off and on.	Depending on schedules for discovery and collection evaluation, this option can take a long time to deliver software. When a new user is added to an existing security group, a full discovery and collection update cycle is required.	This option should be used if security group membership is the only targeting method available, and the package should not require a user to log off and on before installation.
Option 2: Using Security Group in Direct Member Collection	This option allows the healthcare IT Administrator to target software without any latency. When a new user is added to an existing security group, Configuration Manager does not need to discover it or update the collection, because it already knows about the group. The group's membership is enumerated by the Configuration Manager client.	Requires users to log off and on. This option cannot be used when distributing software to computers based on security group membership.	This option should be used to deliver packages to users by security group membership when the user can be prompted to log off and back on.

Table 18: Comparison of Software Targeting Options – Based on Security Group Membership





Figure 4: Timeline for Using Group Attributes to Build a Dynamic Collection

Table 19 describes the timeline for using group attributes to build a dynamic collection in more detail:

Step (Figure 4)	Description
1.	The administrator builds the collection based on the user group attribute.
2.	Configuration Manager queries Active Directory to discover the security group membership of all computers and users, according to the configuration of the Active Directory User Discovery and Active Directory System Group Discovery components. See section 4.2.2.1 and section 4.2.2.3 for more detailed information on this.
3.	The collection evaluator component of Configuration Manager reruns the collection query, and populates the collection with any new members that now have the relevant security group attribute associated with the user/computer record.
4.	The Configuration Manager Client will contact the Management Point every 60 minutes by default, to retrieve any new policies. This frequency can be configured to suit the healthcare organisation's specific requirements. Once the Configuration Manager client has received the new policy, the package will be installed.

Table 19: Timeline for Using Group Attributes to Build a Dynamic Collection - Description

Using this software targeting mechanism, the total time it takes for the package to be deployed, once the user is added to the new security group, can vary. This timing depends on the schedules that are configured for each step of the process, and on the current status of Configuration Manager within these schedules. The worst-case deployment time can be calculated by adding together the schedules for Active Directory User/System Group Discovery, the collection update, and Configuration Manager client policy retrieval. The example shown in Figure 4 would have a worst-case deployment time of 2 days and 1 hour.

Table 20 shows the process for configuring collections based on security group attributes:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Computer Management > Collections node. Right-click on the Collections node and select New Collection.	Image: System Center Configuration Manager Image: Site Database (CEN - SCCM-SRV-01, Contosc Image: Site Management Image: Site Management Image: Computer Management
2.	In Name, enter the name for the collection, and if required, enter a Comment, and then click Next. Note It is good practice to decide on a collection naming strategy so that collections can be easily identified by their purpose.	New Collection Wizard X General General Membership Rules Advertisements Security Progress Confirmation Comment: This is an example collection for Dynamic Query membership when it argeting users based on the users security group membership. Last update The collection has not been updated yet. Last collection has not been updated yet. The collection has not been updated yet. Contraction Center Collection has not been updated yet. Collection has not been updated yet. Collection has not been updated yet. Concel
3.	For dynamic query collections, ensure that the Update this collection on a schedule check box is selected. Click Schedule to modify the default setting of 1 day, if required. Click the I button to add a new dynamic query rule.	New Collection Wizard X Image: Security Rembership rules determine which resources are included in the collection when it is updated. A membership rules determine which resources are included in the collection when it is updated. A membership rules determine which resources are included in the collection when it is updated. A membership rules determine which resources are included in the collection when it is updated. A membership rules can be a direct assignment or a query. Advertisements Security Progress Confirmation Rule Type Image: Type Limit to There are no items to show in this view. V Update this collection on a schedule Occurs every 1 day(6) effective 16/10/2009 15:47 Schedule

Step	Description	Screenshot
4.	In Name, enter a name for the query rule. For this example, ensure that the Resource Class is set to User Resource. Leave Collection limiting set to Not collection limited. Note Limiting collections allows the query to be further limited to a group of systems. This allows for more granular control over collection membership. Click Edit Query Statement.	Query Rule Properties Image: Concernation of the security Group General Import Query Statement Import Query Statement Import Query Statement Resource class: User Resource Edit Query Statement Edit Query Statement Collection limiting Not collection limited Import Query Statement Browse
5.	Click the Criteria tab. Click the New Criteria K button.	OK Cancel Help User Collection Based on NHS Security Group Query Statement Pr X General Criteria Joins You can specify criteria to narrow the query and limit the results that are returned. Criteria: Criteria: Image: Imag
		Show Query Language OK Cancel Help

Step	Description	Screenshot		
6. 7.	Click Select.	Criterion Properties General Criterion Pro- Criterion Type: Where: Operator: Value:	Properties Simple value Select Type: String Value	
	Select User Resource from the Attribute class drop-down list. Select <no alias=""></no> from the Alias drop-down list. Select User Group Name from the Attribute	Select Attribute Attribute dass:	OK Cancel Help	
	drop-down list. Click OK .	Alias as: Attribute:	<no alias=""> User Group Name OK Cancel Help </no>	

Step	Description	Screenshot
8.	Select is equal to from the Operator drop-down list. Select the name of the Security Group from the Value drop-down list. (This should include the domain name, in format 'Domain\Group Name'.) Tip	Criterion Properties X General
	Click Values to show all possible values for the attribute.	Where: User Resource - User Group Name
	Click OK .	Operator: is equal to
		Value: CONTOSO\NHS Security Group Type: String Value
		OK Cancel Help
9.	Click OK to return to the New Collection Wizard.	New Collection Wizard X Wendership Rules Collection membership rules determine which resources are included in the collection when it is updated. A membership rules can be a direct assignment or a query. Collection membership rules determine which resources are included in the collection when it is updated. A membership rules can be a direct assignment or a query. Advert stements Security Progress Confirmation Rule Type Member of NHS Security Group Query Vulgdate this collection on a schedule Occurs every 1 day(s) effective 16/10/2009 15:49 Schedule
10.	Click Next.	New Collection Wizard Advertisements General Membership Rules Advertisements Security Progress Confirmation The programs currently being advertised to this collection are lated below. Advertisements Advertisements Confirmation
		< Previous Next > Finish Cancel



Table 20: Configuring Collections Based on Security Group Attributes

4.4.3.2 Option 2 – Using Security Group in Direct Member Collection



Figure 5: Using Security Group Discovery Data Record (DDR) in Direct Member Collection

Table 21 describes the process for using security groups to build a direct member collection in more detail.

Step (Figure 5)	Description
1.	Configuration Manager queries Active Directory to discover the security groups according to the configuration of the Active Directory Security Group Discovery component. See section 4.2.2.4 for more detailed information on this.
	This only needs to occur when new security groups are added to Active Directory for use with Configuration Manager software distribution.
2.	The administrator builds the collection, based on a Direct Membership rule for the User Group Record.
3.	The user logs off and logs back on to the client machine, which allows the Configuration Manager client to enumerate the logged-on user's security token.
4.	When the user logs back on, the Configuration Manager Client queries the Management Point for the new policy and the package is installed.

Table 21: Using Security Group DDR in Direct Member Collection

Using this software targeting mechanism, the total time it takes for the package to be deployed, once the user is added to the new security group, will be controlled by the user. The administrator can discover the security group and configure the collection before the user is added to the security group, which helps save time. Once the user has been added to the security group, they can log off and log back on to the machine and they will receive the new package immediately.

Table 22 below shows the steps involved in creating a direct membership collection containing a security group:







Step	Description	Screenshot
10.	Click Next.	New Collection Wizard X Void Advertisements General The programs currently being advertised to this collection are listed below. Advertisements Advertisements: Security Program Programs Confirmation
		< Previous Next > Finish Cancel
11.	If additional users or groups need to be able to administer this collection, click in the Instance security rights section to modify the rights and add the required users or groups. Click Next .	New Collection Wizard Image: Collection Wizard Security Security General Specify the security rights that users have on this object dass or instance. Membership Rules Advertisements Security Class security rights: Read, Modify, Delete, Use remote t Instance security rights: Instance security rights: Image: Controsoly.udministrator Read, Modify, Delete, Use remote t Instance security rights: Name Permissions Controsoly.administrator Read, Modify, Delete, Use remote t Instance security rights: Image: Controsoly.administrator Name Permissions Controsoly.administrator Read, Modify, Delete, Use remote t
12.	Click Close.	New Collection Wizard Decision Confirmation Details: General Details: Membership Rules Seneral Advertisements Seneral Security Progress Confirmation Security To finish the wizard, click Close. To finish the wizard, click Close.
		< Previous Next > Finish Close

Table 22: Configuring Collections Based on Direct Membership of Security Group

4.5 Planning Where to Store Application Source Files

'Application source files' are pointers to the folders that contain the installation files for the various packages. For example, one such folder could be the folder that contains the Windows Vista SP1 installation files.

Important

It is important to ensure that application source files are always available so that Configuration Manager is able to update and refresh DPs.

The placement of these source files will depend on the available hardware within the healthcare organisation. The *System Center Configuration Manager 2007 Deployment Guide* **{R1}** contains guidance on the recommended levels of hardware for Configuration Manager servers. It is current best practice to store the source files for packages on a separate disk to the Configuration Manager files, or to store them on a different server, if available. The folders should be secured so that only administrators and the Configuration Manager site server can access them.

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 6 acts as a high-level checklist, illustrating the sequence of events that an IT Professional needs to perform when building application packages for software distribution within a healthcare organisation:



Figure 6: Sequence for Building Application Packages for Use with Configuration Manager Software Distribution

5.1 Configuring Configuration Manager 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. As an example, a package might have source files associated with it. A package also typically has at least one program, and can have as many programs as needed. 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.

The Configuration Manager **Package Properties** dialog box contains the options that are available when configuring Configuration Manager packages. The various package properties are arranged by tabs, as shown below in Figure 7 and Figure 8, and detailed in Table 23 and Table 24.

Example Package 1.0 EN Properties			Example Package 1.0 EN Properties		Example Package 1.0 EN Properties	
Distribution Setti General	ngs Reporting Security Data Source Data Access		Distribution Settings Reporting Security General Data Source Data Access		Distribution Settings Reporting Security General Data Source Data Access	
Healtho	rg Example Package 1.0 EN	2	Specify whether the package contains source files. If it does, specify the initial location of the files and set additional source file options.		Specify where this package is stored on distribution points. These settings apply to all distribution points receiving the package.	
Version:	1.0	Ì	Source version: 1 (06/11/2009 11:21:19)	5	Access the distribution folder through common ConfigMgr package share	
Manufacturer:	Healthcare Org		<pre><directory on="" server="" site="">C:\PKGSource\i</directory></pre>		C Share the distribution folder	
Language: Comment:	EN This is an example packabe		C Use a compressed copy of the source directory		Share name:	
		6	Always obtain riles from the source airectory Update distribution points on a schedule		Package update settings	
			Occurs every 1 day(s) effective 06/11/2009 Schedule		Number of retries before disconnecting users: 2	
		4	Persist content in the client cache Enable binary differential replication		Interval between user notification and disconnection (minutes):	
OK	Cancel Apply Help		OK Cancel Apply Help		OK Cancel Apply Help	

Figure 7: Configuration Manager Package Properties Dialog Box (Part 1)

Tab Number Description		Description	Recommended Setting	
General	1.	Fields used to enter name and other package information.	N/A	
Data Source	2.	This package contains source files specifies whether or not the package contains source files. When enabled, additional options on the Data Source tab become active.	Enabled if package contains source files.	
		The Source directory field specifies the path to the source files; this can be a directory path for the site server or a network location.	Specify path to source files.	
		Used compressed copy of the source directory and Always obtain files from the source directory specify if Configuration Manager should take a compressed copy of the source folder. Selecting the Use a compressed copy of the source directory option requires additional disk space on the site server.	Always obtain files from source directory	
	3.	Update distribution points on a schedule allows Configuration Manager to check for updated files in the package source directory and deploy the changes to DPs automatically.	Only specify if the package source will change. Do not specify for static source files.	
	4.	The Persist content in the client cache setting will override the default cache behaviour of the Configuration Manager client and always keep the package files in the client cache, even after the program has been run. This can be useful if a package will be run recurrently but will reduce the available size of the client cache for other distributions	Not enabled unless specifically required.	

Tab	Number	Description	Recommended Setting
		The Enable binary differential replication setting allows Configuration Manager to only transfer the differences when replicating large package files. This setting can reduce the overall bandwidth required, if large package files are updated.	Enabled.
Data Access	5.	Settings that allow the administrator to specify a directory other than the default SMSPKG folder on the DP. This can allow Configuration Manager to integrate into existing folder naming standards, if required.	Access the distribution folder through common ConfigMgr package share
	6.	Package update settings allow the administrator to configure Configuration Manager to disconnect users from DPs after a configured time period.	Leave check box clear.

Table 23: Configuration Manager Package Properties Settings (Part 1)

Example Package 1.0 EN Properties	Example Package 1.0 EN Properties	Example Package 1.0 EN Properties
General Data Source Data Access Distribution Settings Reporting Security	General Data Source Data Access Distribution Settings Reporting Security	General Data Source Data Access Distribution Settings Reporting Security
Specify the sending priority and the preferred sender to use when sending the package to child sites.	Specify how Management Information Format (MIF) files generated b clients apply to this package.	9 Specify the security rights that users have on this object class or instance.
Sending priority: Medium	Use package properties for status MIF matching	Class security rights:
Branch distribution point content settings	C Use these fields for status MIF matching:	Name Permissions CONTOSO\administrator Read, Modify, Delete, Distribute, Ad
branch distribution points	MIF file name:	NT AUTHORITY\SYSTEM Read, Modify, Delete, Distribute, Ad
Make this package available on protected distribution points when requested by clients inside the protected boundaries	Version:	
 Administrator manually copies this package to branch distribution points 	Publisher:	Instance security rights:
Operating system deployment settings These settings apply only during the WinPE phase of a run command line task sequence step.		Name Permissions CONTOSO\administrator Read, Modify, Delete, Distribute
Allow this package to be transferred via multicast (WinPE only)		
 Encrypt multicast packages Transfer this package only via multicast 		
OK Cancel Apply Help	OK Cancel Apply He	elp OK Cancel Apply Help

Figure 8: Configuration Manager Package Properties Dialog Box (Part 2)

Tab	Number	Description	Recommended Setting
Distribution Settings	1.	The Sending Priority setting allows the Configuration Manager administrator to specify how quickly the package moves through the Configuration Manager hierarchy, according to rules configured on Configuration Manager Senders.	Medium.
		The Preferred sender setting specifies which Configuration Manager sender this package uses. This can be modified for use with the Configuration Manager courier sender, and so on.	No Preference.

Tab	Number	Description	Recommended Setting	
	2.	The Automatically download content when packages are assigned to branch distribution points setting specifies that the package will be immediately downloaded to branch DPs that have the package assigned.	Enabled.	
		The Make this package available on protected distribution points when requested by clients inside the protected boundaries setting, when selected with Automatically download content when packages are assigned to branch distribution points, will trigger Configuration Manager to distribute the package to the protected branch DP of a client that requests the content, even if the DP is not specifically assigned the package. This only occurs if the branch DP is protected.	Enabled if all clients need to receive packages. Useful if the environment contains a large number of protected branch DPs, because the package will not need to be specifically assigned to every DP.	
		The Administrator manually copies this package to branch distribution point setting allows the healthcare IT Administrator to control the distribution of files to branch DPs that are connected using slow links. The source files can be manually copied outside of peak hours, or copied to a DVD or USB drive, and sent to the location where the branch DP resides.	Only used if very low bandwidth connections exist.	
	3.	The Allow this package to be transferred via multicast (WinPE only) can be used when deploying Windows PE as part of an operating system deployment, and can reduce the network bandwidth required. This setting only applies when running command-line actions that are part of a task sequence during the Windows PE phase of an operating system deployment and will not affect normal software distribution packages.	Disabled unless specifically required during Operating System Deployment.	
Reporting	4.	Specify if additional error reporting is required.	Use package properties for status MIF matching	
Security	5.	The Class security rights settings configure Configuration Manager object security for this Package Class, or for the specific package instance.	Specify the required instance security rights. See section 4.1 for more information on Configuration Manager object security.	

Table 24: Configuration Manager Package Properties Settings (Part 2)

When creating packages in Configuration Manager, the healthcare IT Administrator has the option to either use the Create Package from Definition Wizard or to create the package manually. Many software providers will include a package definition (.sms) file with the software, which can be used to automatically create programs and packages for the application. Any Windows Installer (.msi) file can be imported using the Create Package from Definition Wizard. When imported, six default programs will be created that reflect all the available default runtime options of a Windows Installer program, as follows:

- Per-system attended
- Per-system unattended
- Per-system uninstall
- Per-user attended
- Per-user unattended
- Per-user uninstall

5.1.1 Creating Packages Using the Create Package From Definition Wizard

Table 25 below shows the steps required to create a package using the Create Package from Definition Wizard. A package definition file can be an .sms file provided by an application vendor, or an .msi file:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Packages node. Right-click on the Packages node and select New > Package From Definition .	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Site Management Computer Management Collections Conflicting Records Software Distribution Software Distribute Software Distribute Software Distribute Software Site Settings Software
2.	Click Next.	Create Package from Definition Wizard X Welcome Welcome Package Definition Surce Files Summary I'his wizard helps you create a new package from a previously defined package definition file. A package definition file is a template that specifies all the information needed to create a package except the location of its source files (the package's executables and data files). To create a new package from a package definition file, dick Next.
3.	Click Browse to browse to the directory that contains the .sms or .msi file. In this example, the msi from the <i>System Center</i> <i>Configuration Manager Toolkit</i> ⁶ is being used. Click Next .	Create Package from Definition Wizard X Package Definition Package Definition Source Files Select the publisher and definition for your new package. If the package definition you need is not listed and you have an installation disk, dick Browse. Publisher: Publisher: Microsoft Corporation Image: The package definition you need is not listed and you have an installation disk, dick Browse. Publisher: Microsoft Corporation Image: The package definition Package definition: Name Version Language COM Framework Tools 4.00.5931 English (Mri) Version Language Concel

⁶ Microsoft Downloads: System Center Configuration Manager 2007 Toolkit **{R4}**:

 $[\]underline{http://www.microsoft.com/downloads/details.aspx?FamilyID=948e477e-fd3b-4a09-9015-141683c7ad5f\&DisplayLang=entranslowerstates and the second secon$


Step	Description	Screenshot	
4. 5.	Click Always obtain files from a source directory.	Freate Package from Definition Source Files Velcome Package Definition Source Directory Summary Freate Package from Definition Source Directory Source Directory Velcome Package Definition Source Directory Summary	on Wizerd Specify how your package source files should be managed. Source files are data files or executables that must be made available to clents. If this package contains source files, specify whether they should be obtained from a source files or executables that must be made available to clents. If this package contains source files, specify whether they should be stored as compressed data for distribution. If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If the package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this package does not contain any source files If this directory containing the source files for this package. Package exists. Package exists. Package exists. Package exists. Package exists. Package e
6.	Click Finish.	Create Package from Definiti	on Wizerd
		Wekome Padage Definition Source Files Source Directory Summary	You have successfully completed the Create Package from Definition Wizard. Details: "ackage: CCM Framework. Tools Confightgr will obtain the package data from the source directory whenever the package is Source Directory: C:YNESSource(ConfigMgr2007Toolkit To create the package, click Finish.

Step	Description	Screenshot	
7.	The package and required programs have been automatically configured. The healthcare IT Administrator can now secure any packages that have been created with this method, using the guidance in section 5.3.	System Center Configuration Manager Site Database (CBH - SCM-SW-01, Contoso CEntral Ste) Site Database (CBH - SCM-SW-01, Contoso CEntral Ste) Computer Management Com	Programs 6 Here Found Look for: Look for: Look for: Delicone State State State Terre cystem attended Unicoren Strife Per-cystem utmittal Unicoren Unitaren

Table 25: Creating Packages Using the Create Package from Definition Wizard

5.1.2 Creating Packages Without Using the Create Package From Definition Wizard

Table 26 shows the steps required to create a package manually, without using the Create Package from Definition Wizard:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the Packages node. Right-click on the Packages node and select New > Package. Tip Package Folders or Search Folders can be created to make it easier to find and organise packages within the Configuration Manager Console. To create a new folder, select New > Folder or Search Folder.	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Site Management Computer Management Collections Conflicting Records Software Distribution Software Distribute Distribute Distribute Software Site Settings Software Distribute Software Site Settings Software Site Settings Software Distribute Software Site Settings Software Site Settings Software Distribute Software Site Settings Software Site Settings
2.	In Name , enter the name of the package, then enter any additional details required and click Next .	New Package Wizard X General General Data Source Data Access Data Source Example Package 1.0 EN Data Access Example Package Detring Kample Package Reporting Version: Security I.0 Sourmary Monufacturer: Progress Comment: Confirmation This is an example package



Table 26: Creating Packages Without Using the Create Package from Definition Wizard



5.2 Creating Configuration Manager Programs

The purpose of using the software distribution feature is to automatically make a program available to target Configuration Manager 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 prompt, such as a batch file or a Windows Installer command line. The Configuration Manager **Program Properties** dialog box contains the options that are available when configuring a Configuration Manager program. The various package properties are arranged by tabs, as shown below in Figure 9 and Figure 10, and as detailed in Table 27 and Table 28.



Figure 9: Configuration Manager Program Properties Dialog Box (Part 1)

Tab	Number	Description	Recommended Setting
General	1.	Command Line is a required field and should contain the full command line to execute the program. It should also contain any command-line switches required for execution. This would normally exactly match any command line used to install the application, while interactively logged on to the computer.	Specify the full command line.
	2.	The Start in field is optional, and is used to specify the executable path for the program, if the .exe or .msi file is not in the root folder.	Specify if required.
	3.	Contains settings for run-time behaviour. Options include:	Specify as required.
		Run: Hidden, Maximised or Minimised	
		 After Running: No action required, Program restarts computer, Configuration Manager restarts computer or Configuration Manager logs user off 	
		Category: Optional	
Requirements	4.	The Estimated disk space and Maximum allowed run time (minutes) settings allow the administrator to provide estimated disk usage and run-time information to the user. The Configuration Manager Advanced Client will terminate any running program once the Maximum allowed run time setting is reached. If None is specified, the run time will expire after 72 hours.	Specify the amount of disk space required, and leave Maximum allowed run time as default.
	5.	The This program can be run on any platform and This program can run only on specified program settings allow the administrator to specify the target operating systems on which the package will be executed.	Only specify if the package should only be run on specific operating system versions.

Tab	Number	Description	Recommended Setting
Environment	6.	The Program can run settings specify the circumstances under which the program can run. Options include:	Specify as required. It is current best practice to use the
		 Only when a user is logged on: Can run either with logged-on user rights or with administrative rights. 	lowest possible privilege so if a program is able to run under the
		Whether or not a user is logged on: Can only run with administrative rights because there may be no logged-on user.	logged-on users context, configure it as such.
		 Only when no user is logged on: Can only run with administrative rights because there may be no logged-on user. 	
	7.	The Run mode settings specify as which security context the program should be executed; these options will change according to how the drop-down list (in Number 6) is configured.	Allowing users to interact with programs that are running under administrative context should only be
		The Allow users to interact with this program check box sets the program to be visible to the user. Programs set to run with administrative rights that do not have this option set, must not require any user interaction, otherwise they will fail.	enabled if user interaction is required. Always try to make administrative installations non-interactive, as there is potential for users to elevate privileges if they are able to interact with a program running in administrative context.
	8.	If a program requires a drive to be mapped, or requires a specific drive letter to operate properly, these options are defined here. The Drive mode setting allows the administrator to configure this behaviour for this program.	This usually only applies to old custom-written applications, and should be left as default unless a specific requirement has been identified

Table 27: Configuration Manager Program Properties Settings (Part 1)

Ехап	mple Program Properties		×	Example Program Properties	×	Example Progr	ram Properties		X
	Windows Installer	MOM Maintenance Mod		General Requirements Environment Advanced	1	General	Requirements	Environment	Advanced
	General Requirements	Environment Adva	nced	Windows Installer MOM Maintenance Mode	4	Windo	ows Installer	MOM Mainter	nance Mode
Ŷ	/ou can specify additional criteria /ou can also temporarily disable th	for installing and running this pro ne program.	gram.	If you enable installation source management for this program, the .msi file will automatically return to the package files on an available distribution point to reinstall or repair the installation. Specify the Windows Installer product information to enable installation source		Microsoft Op program run: you can disa	perations Manager (M s. To avoid receiving able the alerts for the	OM) might generate a alerts for this planned duration of the progra	lerts when this maintenance, am.
	Run another program first:			management.	Y				
	Package: Program:	Browse	-	Click Import to specify the product code and the Windows Installer file.		Disable C	Operations Manager a	lerts while this progra	m runs
	🔲 Always run this program firs	t		Click Clear to clear these fields and disable installation source		_			
(2)	When this program is assigned to	a computer:		management or this product.		Generate	e Operations Manage	r alert if this program f	ails
	Run once for the computer		•	Windows Installer product code:					
(3)	Suppress program notifications	;		J					
ŕ	A disabled program is not displaye	d or run on clients.		Windows Installer file:					
4	Disable this program on compu	ters where it is advertised.		Import Clear					
5	Allow this program to be install sequence without being adver	ed from the Install Software task tised.							
	OK C.	ancel Apply	Help	OK Cancel Apply Help			ОК С	ancel Apply	Help

Figure 10: Configuration Manager Program Properties Dialog Box (Part 2)

Tab	Number	Description	Recommended Setting
Advanced	1.	The Run another program first setting allows the administrator to configure another program to run first. This will force the Configuration Manager client to install packages in a specific order. For example, Microsoft Office 2007 is always installed prior to Microsoft Office 2007 Service Pack 2.	Only specify if a specific package installation order is required.

_ .

. . .

Tab	Number	Description	Recommended Setting
	2.	The When this program is assigned to a computer setting allows the program to execute either once for the computer, or for every new user that logs on to the computer.	Run once for the computer, unless the package is for specific user components of an application that need to be separately installed for each user.
	3.	The Suppress program notifications setting stops any program notification icons being presented to the user.	Use with software update packages or other packages where the user should be informed. Use caution if the package will restart the computer after the installation.
	4.	If the Disable this program on computers where it is advertised option is selected, all advertisements that contain this program are temporarily disabled. The program is removed from the list available for Configuration Manager clients to run, and will not be run through assignment until it is re-enabled.	Only use when required. Possible uses for enabling this setting include if an issue has been identified with the program, so that no further Configuration Manager clients can run the advertisement until the issue has been resolved.
	5.	The Allow this program to be installed from the Install Software task sequence without being advertised setting must be selected if the program is part of a package that will be deployed during an operating system deployment task sequence execution. Even if the program has been previously advertised, this option must be checked or the task sequence action will fail.	Selected if the program will be installed as part of an operating system deployment task sequence.
Windows Installer	6.	The Windows Installer product code and Windows Installer file fields allow the administrator to import the product code of a Windows Installer application. This allows the Configuration Manager clients to take advantage of the Windows Installer Source Location Manager feature of Configuration Manager. See section 2.2.1.1.5 for more information on this feature.	Specify for any Windows Installer (.msi) application.
MOM Maintenance Mode	7.	The Disable Operations Manager alerts while the program runs and Generate Operations Manager alert if this program fails settings allow for integration with some features of Microsoft [®] Operations Manager. If the program is being deployed to servers that are monitored by Microsoft Operations Manager 2005 or Microsoft [®] System Center Operations Manager 2007, this will prevent unnecessary alerts being raised.	Leave unselected unless required.

Table 28: Configuration Manager Program Properties Settings (Part 2)

Program Program For Device

sh (Unite X

-

•

-

Cancel

Give Feedback

Example Program

deployed by ConfigMgr may be subject to lice ns prior to deploying software.

Next >

'his is an example program

ExampleApp.exe /s

No action required Example Software Category

🖃 🆀 Microse

Comment

and line Start in:

Table 29 below shows the steps required to create a new program:



Genera

Advanced

Summary Progress

Confirmation

Windows Install

MOM Maintenance

- 2. In Name, enter a name for the program. Complete the remaining dialog box settings as follows:
 - Comment: This field is optional.
 - Command Line: This should be the full command line to execute the package including any options (for example, /s for silent install).
 - Start in: Leave as blank. н.
 - Run: Select Normal. .
 - After Running: No Action required.
 - Category: Categories can be added, and will appear on the client in Add or Remove Programs in Control Panel (Windows 2000/XP) or Programs and features (Windows Vista/Windows 7), when the Configuration Manager client receives the advertisement.
- 3. In Requirements, accept the default settings unless the program has specific operating systems dependencies and the program may be deployed to clients on operating systems that are not supported.

Click Next.



Step	Description	Screenshot	
4.	In Program can run , select Only when a user is logged on for programs that require user interaction and can be executed by the user's context. If the program will require additional rights to install, Run with administrative rights needs to be selected. If user input is also required, Allow users to interact with the program must also be selected. This should be used with caution if the installation program runs command lines or batch files, because these processes will have elevated permissions. Click Next .	New Program Wizard Environment General Advanced Windows Installer MOM Maintenance Summary Progress Confirmation Progress Confirmation Run Model Run	In may require certain conditions to be true before it can run. Specify the conditions that met for the program to run. Can run: Conly when a user is logged on Conly when a user is logged on Conly when no Conly when no u
5.	Click Next.	New Program Wizard	X
		General Requirements Environment Advanced Windows Installer MOM Maintenance Summary Progress Confirmation Confirmation	specify additional orienta for installing and running this program. You can also temporarily the program. You can also temporarily another program first: ge:
6.	Click Import to import the product code for any .msi applications. Note This is not required for the example program, but should be configured for any program that executes a Windows Installer package. Click Next.	New Program Wizard Windows Instaler General If you ef Requirements Environment Advanced Undows Instaler Windows Instaler Click Ling Summary Click Cle Progress Confirmation Windows Windows	Adde installation source management for this program, the .msi file will automatically return to age files on an available distribution port to reinstal or repair the installation. Specify the Installer product information to enable installation source management. ar to specify the product code and the Windows Installer file. ar to clear these fields and disable installation source management of this product. Installer product code: Import (Lear (Previous Next> Frich) Cancel



Table 29: Creating Programs

5.3 Securing Configuration Manager Packages

Configuration Manager package access accounts allow for specific permissions to be applied to the Distribution Point folders that contain the Configuration Manager packages. By default, Configuration Manager will grant full control permissions to members of the Administrators local group on the Distribution Point, and read permissions to members of the Users group. It is current best practice to make these permissions the most restrictive possible, without preventing access to required users. Table 30 shows the steps involved in adding a user or a group to the Access Accounts list. Ensure that these permissions are set correctly at the time of package creation because if the access accounts are modified after the package has been deployed, the package will need to be refreshed. This can have a significant impact on network utilisation. Section 8.2 details the steps involved in updating the package, if this is required.

Table 30 below shows the steps required to create new package access accounts for a package:

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the package to which an access account is to be added. Right-click the Access Accounts node and select New > Windows User Access Account .	System Center Configuration Manager Ste Database (CEN - SCCM-SRY-01, Contoso CEntral Site) Ste Database (CEN - SCCM-SRY-01, Contoso CEntral Site) Ste Management Collections Collecti
2.	In Permissions , select the required level of access. Click Set .	New Windows User Access Account Package access account: Package access account: Image: Set Account type: Windows User Access Account Permissions: Read Change Full Control No Access If you add an account or modify the permissions on an existing account, you will need to refresh all distribution points. OK Cancel
3.	In User name , enter the name of the user or user group. Under Account type , specify whether it is a user or a group. Click OK twice to add the user or the group to the Access Accounts list.	Windows User Account X User name: CONTOSO\ Healthcare Org Security Group Syntax: Domain\User Account type Output Group OK Cancel

Table 30: Securing Configuration Manager Packages

5.4 Copying Configuration Manager Packages to Distribution Points

If a Configuration Manager Package contains source files, it cannot be run by Configuration Manager clients until the package source files are copied to the relevant DP. Typically, it is best to copy the package to all available DPs, to allow access for any Configuration Manager clients that are roaming away from their usual home site to packages they may require. This may be especially relevant when programs are configured to use the Source Location Manager feature, because this feature makes the installation source for the installed Windows Installer applications available if the client needs to repair or update the application.

Important

Copying packages to DPs can have a significant impact on the network. The healthcare IT Administrator should always ensure that this task is performed at times when this network traffic does not adversely affect network use. Special consideration should be given when deploying packages to Configuration Manager sites or DPs that are connected using a slow network link.

Step	Description	Screenshot
1.	Open the Configuration Manager Console and navigate to the package to which the Distribution Point is to be added. Right-click the Distribution Points node and select New Distribution Point .	System Center Configuration Manager Ste Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Site Management Computer Management Conflicting Records Microsoft Hyper-V Integration Manager Client Upgrade 4.0 ALL Microsoft Hyper-V Integration Services X64 Microsoft Wolf Va6age 1.0 Microsoft (X86) 3.01 Heathorg Example Package 1.0 EN Access Accounts Distribution New Distribution Points Programs Programs Programs Programs
2.	Click Next.	New Distribution Points Wizard X Welcome Welcome to the New Distribution Points Wizard Copy Package Progress Confirmation This wizard helps you copy a package to new distribution points. To continue, click Next. To continue, click Next.

Table 31 shows the steps required to copy packages to DPs:





Table 31: Copying Configuration Manager Packages to Distribution Points

Note

If changes are required to the package source or settings, the package must be updated on all relevant DP's. See section 8.2 for information on managing changes to packages.

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.

During this phase, testing and acceptance of the Configuration Manager infrastructure and its associated network components will take place. The aim is to minimise the impact on normal business operations by testing the design assumptions and verifying the deployment process in a pilot program. It is important that this phase of testing and verifying should begin during the Build phase and continue through the Deploy and Operate phases.

Figure 11 acts as a high-level checklist, illustrating the areas of the Configuration Manager processes for software distribution that an IT Professional is responsible for stabilising:



Figure 11: Sequence for Stabilising Software Distribution

6.1 Testing the Deployment on Pilot Computers

6.1.1 Defining Collections for Pilot Computers

Before advertising software to any machines, it is current best practice to deploy the software to a collection of pilot computers. The pilot collection should consist of computers that are representative of the computers that will receive the advertisement in the production environment. Usually this would be a direct membership collection defining one or more computers or users in the IT department. This allows the administrator to ensure that the program operates as expected, so that users are not adversely affected when the software is deployed into production. Depending on the scale of the deployment, it is recommended that the deployment is staged as follows:

- 1. Deploy the advertisement to a limited pilot collection to ensure that the installation behaviour is correct and that the application installs successfully.
- Deploy to a larger group of 'trusted users'. This can consist of members of the IT staff, or preferably, users within the production environment who have given agreement for this to take place. This allows the administrator to identify any potential issues that may occur when the advertisement is targeted at the production environment.
- 3. Finally deploy the application to the production target collection.

6.1.2 Creating Configuration Manager Advertisements

Advertisements are the objects that make programs available to Configuration Manager clients. The advertisement links the program and the package to a collection. A program must be advertised before Configuration Manager clients can run it.

The **Advertisement Properties** dialog box contains the options that are available when configuring Configuration Manager advertisements. The various advertisement properties are arranged by tabs, as shown below in Figure 12 and Figure 13, and as detailed in Table 32 and Table 33.

Advertisement to Te	st Collection Properties	Advertisement to Test Collection Properties	×
General Schedule	Distribution Points Interaction Security	General Schedule Distribution Points Interaction Security	
Name:	Advertisement to Test Collection	Specify when the program will be advertised to members of the target collection. You can also create an assignment to make the program mandatory.	
		Advertisement start time:	7
Comment:	This advertisement is targeted to a collection	р6/11/2009 🔽 16:40 📑 🗆 итс	
		Advertisement expires:	
	_	р7/05/2010 🔄 16:40 🗮 🗖 итс	
Package:	Healthorg Example Package Browse	Mandatory assignments:	
Program:	Example Program	As soon as possible	
Collection:	Direct Memeber Sysem Colle Browse	6 Enable Wake On LAN	
2 🗹 Include mem	bers of subcollections	Ignore maintenance windows when running program	
		💙 🗖 Allow system restart outside maintenance windows	
		Priority: Medium	1
		Program rerun behavior: Rerun if failed previous]
OK	Cancel Apply Help	OK Cancel Apply Help	

Figure 12: Advertisement Properties Dialog Box (Part 1)

Tab	Number	Description	Recommended Setting
General	1.	The Package and Program drop-down lists allow the administrator to select from all available packages, then all programs for the selected package. The Collection field allows the administrator to select the required collection. Target collections can be specified, either by typing the name directly into the Collection box or by selecting the required collection using the Browse button.	Select the required package, program and collection.
	2.	When creating collections, they can be configured as child collections to other collections. For example, the administrator can configure a top-level collection for Windows 7, and then configure numerous subcollections for each geographic location in the healthcare organisation. The Include members of subcollections setting specifies that the advertisement will apply to the target collection and all sub-collections.	Enable if required.
Schedule	3.	Advertisements can be preconfigured before they are required to be run on Configuration Manager clients. The Advertisement start time setting allows the administrator to set advertisements that will not apply to the Configuration Manager clients until required.	Leave as default, unless required.

Tab	Number	Description	Recommended Setting		
	4. The Advertisement expires setting can be configured if a program is only relevant for a defined period of time. The advertisement can then be scheduled to expire at a specified date and time.		Leave as default.		
	5. The Mandatory Assignments field allows administrators to Define create, modify or delete mandatory assignments. To ensure users cannot choose <i>not</i> to run the advertised program, define one or more mandatory assignments.		Define as required.		
	6.	The Enable Wake on LAN check box triggers the site server to send a wake up packet to the client machine before the advertised program is scheduled to run.	Leave as default, unless required.		
	7. The Ignore maintenance windows when running program and Allow system restart outside maintenance windows settings allow the healthcare IT Administrator to override any maintenance window configuration, and force the advertisement to run, even if the computer is part of a collection that has maintenance windows configured and the advert is scheduled to run outside of that window.		Enable only when required, and with caution.		
	8.	The Priority setting specifies the advertisement's priority when sent to child sites. This is based on rules defined when configuring Configuration Manager.	Medium.		

Table 32: Advertisement Properties Settings (Part 1)

Advertisement to Test Collection Properties	X Advertisement to Test Collection Properties
General Schedule Distribution Points Interaction Security	General Schedule Distribution Points Interaction Security
Each boundary in the Configuration Manager site is designated as a fast (LAN) network or a slow or unreliable network. Specify how to run the content for the advertised program, depending on the type of boundary the client is connected to.	Specify settings that affect how users are notified about and interact with this advertised program.
When a client is connected within a fast (LAN) network boundary:	Allow users to run the program independently of assignments
C Run program from distribution point	5 🗵 Display reminders according to the client agent reminder intervals
$\ensuremath{\mathfrak{O}}$ Download content from distribution point and run locally	
When a client is connected within a slow or unreliable network boundary:	Use custom countdown notification length (minutes):
O Do not run program	
O Download content from distribution point and run locally	
C Run program from distribution point	
Allow clients to fall back to unprotected distribution points when the content is not available on the protected distribution point	
OK Cancel Apply Help	OK Cancel Apply Help

Figure 13: Advertisement Property Settings (Part 2)

Tab	Tab Number Description		Recommended Setting		
Distribution Points	1.	The When a client is connected within a fast (LAN) boundary settings specify the run-time behaviour of the Configuration Manager client, when it falls within the fast boundaries of the site. This is usually when the Configuration Manager client has a fast and reliable connection to the DP.	Define as required.		
	2.	The When a client is connected within a slow or unreliable network boundary settings specify the run-time behaviour of the Configuration Manager client, when it falls within the slow boundaries of the site. This is usually when the Configuration Manager client is separated from the DP by an N3 WAN connection (links to external geographic locations or GP surgeries, and so on).	Define as required.		
	3.	The Allow clients to fall back to unprotected distribution points when the content is not available on the protected distribution point setting allows the healthcare IT Administrator to override the default behaviour of the client for this particular advertisement.	Use with caution because the setting will cause clients to traverse slow network links for content if the content is not available on the local DP		
	4.	The Allow users to run the program independently of assignments setting allows the user to execute the advertisement before the mandatory installation time. For example, if the program is scheduled for mandatory installation on the first day of the following month, and the user knows they will be connected via a slow link, they can run the program in advance while connected to the LAN.	Leave as default.		
	5.	The Display reminders according to the client agent reminder intervals settings specifies that the client will be reminded that the advertisement is going to run, based on the configuration specified in the Computer Client Agent properties under Site Settings > Client Agents in the Configuration Manager Console.	Define as required.		
	6.	The Use custom countdown notification length (minutes) setting allows the user to provide a specific countdown for the advertisement, to warn the user that advertisement will run. This is particularly useful when the installation will restart the client computer or force a user to log off. This time will allow the user to save any work before the advertisement runs.	Specify as required.		

Table 33: Advertisement Properties Settings (Part 2)

By default, Configuration Manager clients do not rerun advertised programs unless the advertisement is on a recurring schedule. Because it is possible for clients to receive multiple advertisements or assignments for the same package or program, it is not recommended that the client installs the same package or program more than once. For this reason, Configuration Manager uses the package/program combination to determine whether or not a package has been previously run. Healthcare IT Administrators may require that advertisements be rerun if they have previously failed; this is especially relevant in a test environment when deployment testing is performed.

Table 34 shows the steps involved in deploying a program from a package to a collection. This example of a Direct Member System collection demonstrates the configuration of an advertisement:

Step	Description	Screenshot			
1.	 Open the Configuration Manager Console and navigate to the Advertisements node. Right-click on the Advertisements node and select New > Advertisement. Tip Advertisement folders and Search folders can be created to make it easier to find and organise packages within the Configuration Manager Console. To create a new folder, select New > Folder or Search Folder. Complete the settings as follows: Name: Enter 'Advertisement to test collection'. Comment: This field is optional. Package: Select a package. Program: Select the collection of pilot computers. Click Next.	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Computer Management Collections Conflicting Records Software Distribution Software Distribution Software Distribute Advertise Task Sequence Software Distribute Conserved Software Distribute Software Distribute Conserved Software Distribute Software Distribute Software Distribute Software Distribute Advertisement to Test Collection Software Distribute Software Distribute Sof			
3.	Click the Schedule tab. Click the button to add a new mandatory assignment. Note If no mandatory assignment is configured, the user can select the application using Add/Remove Programs (Windows 2000 or	New Advertisement Wzard X Schedule General Specfy when the program will be advertised to members of the target collection. You can also create an assignment to make the program mandatory. Distribution Points Interaction Security Summary Progress Distribution Points Distribution Points Madvertisement expires: Distribution Mandatory astronements:			
	Windows XP). Program and Features	There are no items to show in this view.			

(Windows Vista or Windows 7) or Run

Advertised Programs in Control Panel, at

any time after the advertisement start time.

Enable Wake On LAN

Program rerun behavior:

E Aller

Priority:

🔲 Ignore maintenance windows when running program

Medium

Always

< Previous Next > Finish Cancel

•

Step	Description	Screenshot
4.	Select As soon as possible from the Assign immediately after this event drop-down list. Click OK .	Assignment Schedule C Assign to the following schedule: Occurs on 06/11/2009 16:45 C Assign immediately after this event: As soon as possible OK Cancel Help
5.	On the Distribution Points page, configure the settings to match the intended options for the production deployment and click Next .	New Advertisement Wizard X Schulton Points Each boundary in the Configuration Manager site is designated as a fast (LAN) network or a slow or preliable network. Specify how to un the content for the advertised program, depending on the type of boundary the clerk is connected to. Distribution Points Each boundary the clerk is connected to. Distribution Points When a clerk is connected within a fast (LAN) network boundary: Summary • Run program from distribution point. • Download content from distribution point. • Download content from distribution point and run locally. When a clerk is onnected within a slow or unreliable network boundary: • Download content from distribution point. • Download content from distribution point and run locally. • Download content from distribution point. • Provide distribution point.
6.	Specify Interaction options and click Next.	New Advertisement Wizard X Interaction Specify settings that affect how users are notified about and interact with this advertised program. Schedule Specify settings that affect how users are notified about and interact with this advertised program. Distribution Points Interaction Security ✓ Allow users to run the program independently of assignments Summary ✓ Display reminders according to the client agent reminder intervals Confirmation ✓ Use custom countdown notification length (minutes): Image: Previous Next > Propriot Cancel



Table 34: Creating Configuration Manager Advertisements

6.1.3 Checking the Status of the Deployment

The status of the deployment in the pilot environment can be monitored in the same way as in the production environment, by using Configuration Manager reports or Configuration Manager status messages. It is likely that pilot computers will be located close to the administrator so that the deployment can also be monitored by physically logging in to the pilot Configuration Manager clients. Section 8.1 contains step-by-step instructions on using Configuration Manager reporting and Configuration Manager status messages to monitor deployment.

6.1.4 Validating Successful Deployment

Validating the deployment is the most important part of pilot testing. Before the application is rolled out into production, the administrator must be certain that the user experience will be as expected. This can be achieved by logging in to a pilot Configuration Manager client while the deployment happens, to make sure there are no unexpected dialog boxes or user interaction, and to ensure that the program has achieved the desired results, for example, installing new software.

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.

Figure 14 acts as a high-level checklist, illustrating the critical tasks that an IT Professional responsible for deploying an application using Configuration Manager software distribution needs to perform:



Figure 14: Sequence for Deploying Applications to Production Computers

7.1 Deploying an Application to Production Computers

After the package has been tested, and the healthcare IT Administrator is confident that the package and program will function as expected, the same processes can be followed to deploy the application into production. Depending on the scale of the deployment, the administrator can decide to create one, or a number of collections. Creating more than one collection allows the administrator to create different advertisements with different schedules, for different parts of the healthcare organisation. This can also be useful in staging an application deployment so that not all the machines install the package at the same time.

Important

For remote clients that are connected via a network link, such as General Practice clinics, it is important that the healthcare IT Administrator reviews the *Manual Client Installation* section of the *System Center Configuration Manager 2007 Deployment Guide* **{R1}**. This provides information for the healthcare IT Administrator on how to configure Configuration Manager clients that are in disconnected domains, forests or workgroups.

7.1.1 Defining Collections for Production Computers

Once the application has been fully tested in a pilot environment, a collection needs to be created that will target all computers, or users, that require the application. Figure 15 below guides the healthcare IT Administrator through the decision making process involved in creating the collection for production deployment. Once the collection has been created, the package can be advertised to the new collection.





System Center Configuration Manager 2007 – Software Distribution Guide Prepared by Microsoft, Version 1.0.0.0 Last modified on 26 February 2010

7.2 Advertising Packages to the Production Environment

Once the production collections have been created, the healthcare IT Administrator can advertise the package into the production environment.

Note

When scheduling the advertisement, ensure that the application is deployed with the least amount of user impact. Avoid scheduling the advertisement to trigger an installation during busy periods.

The steps in section 6.1.2 can be followed to create the production advertisement, ensuring that production collections are selected and that the schedule timings are set appropriately.

For some applications, it may be required to run them on a recurring basis. This means the Configuration Manager client will rerun the advertisement every time the schedule occurs.

Table 35 shows the additional steps required to configure the advertisement to have a recurring schedule, and should be followed in conjunction with the procedure in Table 34:

Step	Description	Screenshot				
1.	Click the 🙁 button to add a new mandatory	Advertisement to Test Collection Properties				
	assignment.	General Schedule Distribution Points Interaction Security				
		Specify when the program will be advertised to members of the target collection. You can also create an assignment to make the program mandatory.				
		Advertisement start time:				
		06/11/2009 Inc UTC				
		Mandatory assignments:				
		There are no items to show in this view.				
		Enable Wake On LAN				
		□ Ignore maintenance windows when running program				
		Allow system restart outside maintenance windows				
		Priority: Medium				
		Program rerun behavior:				
		OK Cancel Apply Help				
2.	Click Schedule.	Assignment Schedule				
		 Assign to the following schedule: 				
		Occurs on 06/11/2009 18:42				
		Schedule				
		C Assign immediately after this event:				
		As soon as possible				
		OK Cancel Help				

System Center Configuration Manager 2007 – Software Distribution Guide Prepared by Microsoft, Version 1.0.0.0 Last modified on 26 February 2010

Step	Description	Screenshot
3.	Configure the start time and recurrence pattern as required. Click OK three times to save the settings and close the dialog boxes.	Custom Schedule Image: Start: D6/11/2009 18:42 Image: Start: D6/11/2009 Image: Start: D6/11/2009 Image: Start: Image: Start: D6/11/2009 Image: Start: Ima

Table 35: Configuring Recurring Advertisement Schedule

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 16 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 software distribution environment:



Figure 16: Sequence for Operating Configuration Manager Software Distribution

8.1 Monitoring a Deployment

Configuration Manager allows the healthcare IT Administrator to monitor the progress of a software deployment using either Web-based reports or the built-in status message system. By using these tools, the administrator can have a near real-time picture of the number of Configuration Manager clients that have successfully installed the application, and identify any Configuration Manager clients that are experiencing issues with the deployment.

8.1.1 Using Configuration Manager Reporting

Configuration Manager reporting includes over 380 built-in reports, covering a variety of information.

Table 36 contains step-by-step instructions on how to use Configuration Manager reporting to monitor the status of a deployment. This example uses only one of the built-in reports. It is also possible to create custom reports using the SQL views and standard T-SQL queries. More information on creating custom reports can be found in the TechNet article *Creating Custom Reports by Using Configuration Manager 2007 SQL Views*⁷.

Step	Description	Screenshot			
1.	From within the Configuration Manager Console , navigate to the Reporting node. Right-click on the Reporting node and select Run .	System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Site Management Computer Management Conflicting Records Software Distribution Software Updates Software Updates Software Metering			
2.	Internet Explorer is invoked and connects to the Configuration Manager Reporting Web site. Information It is also possible to start Internet Explorer and navigate to the URL http:// <configuration Manager site server>/ SMSReporting <site code="">, from any machine that can connect to the Configuration Manager site server.</site></configuration 	View Confighting Reports - Windows Internet Explorer Image: Subject States - Image: S			
3.	From the tree view, click the report Status of a specific advertisement .	 Software Distribution - Advertisement Status Advertisement status messages for a client being upgraded to the Advanced Client Advertisement status messages for a particular client advertisement All system resource advertisements with status All system resources for a specific advanced client distribution in a specific state All system resources for a specific advertisement in a specific state Chart - Hourly advertisement completion status Status of a specific advertisement 			

⁷ Microsoft TechNet: Creating Custom Reports by Using Configuration Manager 2007 SQL Views **{R5}**: <u>http://technet.microsoft.com/en-us/library/dd334593.aspx</u>

Step	Description	Screenshot		
Step 4.	Description Click Values to display all advertisements. Tip The Advertisement ID can be specified directly, if known. This can be obtained by clicking on the Advertisements node in the Configuration Manager Console.	Screenshot Report Information Report Category Software Distribution - Advertis Report Name Status of an advanced client dis Report Comment This report shows the status su targeted by an advertisement to summary is broken into two par how many resources have rece advertisement. Delivery status run or attempted to run the pro-	ement Status stribution immary of all resources that have to upgrade to the SCCM Client. Th ts. Acceptance status will summa- ived, rejected, or not yet receive will summarize the resources that ogram being advertised. ent installation advertisemer rds: He%lo W_rld%)	been ne Displa d the have
5.	Click the appropriate value in the available Advertisement Id list.	Values Select a value to use when running below, the value in the first column report. Advertisement Id	the report. If more than one column a of the selected row will be used when nt Name Package Name	appears running the Program Name
		CEN20000 Reference Compu- Sequence Vista (Xi CEN20001 CCM Framework 1 system unattende CEN20002 Vista Client Build CEN20003 CCM Tools to all (mandatory) CEN20004 Advertisement to Collection	Iter Task 86) Computer Task Sequence Vista (X86) Tools - Per- d to Vista1 CCM Framework Tools Vista Client Build non CCM Framework Tools Test Example Package	* Per-system unattended * Per-system attended Example Program
6.	Click the Display button .	Report Information Report Category Software Distribution - Advertis Report Name Status of an advanced client dis Beport Comment	ement Status stribution	

This report shows the status summary of all resources that have been targeted by an advertisement to upgrade to the SCCM Client. The summary is broken into two parts. Acceptance status will summarize how many resources have received, rejected, or not yet received the advertisement. Delivery status will summarize the resources that have run or attempted to run the program being advertised.

Advertisement ID for a client installation advertisement (Reduce Values set with wildcards: He%lo W_rld%)

CEN20003
Values...

Step	Description	Screenshot			
7.	The report is then displayed. Configuration Manager clients can return a number of states, depending on how far they are through the installation process. A functioning deployment will show the status in the following order: Accepted Waiting Running	Copy Export Print Add to Favorites Report Name: Status of an advanced client of Software Distribution - Advert This report shows the status summ. Comment: This report shows the status summ. two parts. Acceptance status will su the resources that have run or atter Parameters: 06/11/2009 18:57:18 Resource Receipt Status		E-mail distribution rtisement Status mary of all resources that have be summarize how many resources h tempted to run the program being tallation advertisement CEN2000 Number of Resources	
	Succeeded	 Accepted No Status 06/11/2009 18:57:18 Status of Targete Accepted - No Further Status Advanced Client Installed Failed Succeeded 	d Resources	8	Number of Reso 3 2 1 2
8.	Refreshing the Web page will refresh the data in the report so that the deployment status of all machines can be monitored. Configuration Manager will organise machines of different statuses into groups in the report. If any error statuses are encountered, click the link button I to drill down to linked reports with further detail.	Copy Export Print Report Name: Status of an Category: Software Dis This report she This report she Comment: two parts. Acc Parameters: Advertisement	Add to Favorites advanced client stribution - Adver ows the status sum ceptance status will that have run or att nt ID for a client inst	E distri rtisen mary o summa tempte tallatio	-mail bution hent Status f all resources that have be arize how many resources h ad to run the program being n advertisement CEN2000
		06/11/2009 18:57:18 Resource Receipt Accepted No Status 06/11/2009 18:57:18 06/11/2009 18:57:18 Accepted - No Further Status Advanced Client Installed Failed Succeeded Succeeded	Status	8	Number of Resources Number of Reso 3 2 1 2
9.	The linked reports show status messages for all the relevant statuses that led to the end condition.		Copy Export Report Name: 4 Category: 5 Comment: 5	Prin All sys Softwa This rep	It Add to Favorites tem resources for a speci are Distribution - Advertis ort will show a list of all resou fully run a program being adw



Step	Description	Screenshot		
10.	Click the link button I to drill down to the description of the status message. If an error	Status Message D	Details	
	occurred during installation, the description of the			Message Details
	status massage will provide detail of why the	Timestamp:	04/11/2009 16:09:52	Message Type:
	status message will provide detail of why the	Site Code:	CEN	Message ID:
	error occurred, and will often include possible	System:	HYPERV02	Process ID:
	resolutions	Source:	SMS Client	Thread ID:
		Component:	Software Distribution	Severity:
		The content for "CENOU any distribution servers, boundaries of the site. O distribution points and is from distribution point. S binderies then change th standard distribution point Advertisement ID Client: SMS Unique ID	DOC" - "1" could not be located. This SMS client w or the advertisement may have been marked n content source might not be available because th not available on a standard distribution point. B Solution: Use the Manage Distribution Points wiza ne advertisement to allow running program from nt if you want to use the option Run program fro CEN20003 GUID:580ADFE4-8DDC-488	Description ill no longer attempt to locate this o to run program when no local Disi te advertisement is configured with ranch distribution point do not sup rd to distribute the content to a disi remote Distribution Point. Use the f m distribution point. Properties D-B84B-3F28D3F3818A

Table 36: Using Configuration Manager Reporting

8.1.2 Using the Configuration Manager Status System

Many actions performed within the Configuration Manager hierarchy generate status messages that are passed back through the site systems into the Configuration Manager database. These messages give detailed information on every aspect of Configuration Manager and can be used to monitor or troubleshoot the distribution of software. The Configuration Manager status message viewer allows Configuration Manager Console users to view and query status messages.

Table 37 provides step-by-step instructions on how to view status messages applicable to a specific software advertisement:

Step	Description	Screenshot		
1.	From within the Configuration Manager Console , navigate to the Advertisement Status node and select the advertisement required.	 System Center Configuration Manager Site Database (CEN - SCCM-SRV-01, Contoso CEntral Site) Site Management Collections Collections Conflicting Records Software Distribution Packages Packages Software Updates Operating System Deployment Asset Intelligence Software Undets Masset Intelligence Reporting Reporting Reporting Reporting Metwork Access Protection System Status Advertisement Status Advertisement to Test Collection CCM Trade status (CCM Tools to all (non mandstory)) 	CEM Tools to all (non mandatory) 2 II Look for:	
2.	Right-click on the Configuration Manager Site object to which the Configuration Manager client is assigned and select Show Messages	Look for:		
	> All.	Site Received	Failures Progr	
		CEN - Contosc Show Messages ► Reset Counts ► Refresh Help	All Received Failures Program started Program errors Program success Program errors (MIF)	

Step	Description	Screenshot			
3.	Right-click on the status messages in the Configuration Manager status message viewer and select Detail .	ConfigMgr Status Message Viewer for <cen> <contoso central="" site=""> File Edit View Help</contoso></cen>			
				Date / Time	Sustan
		Milestor	De CEN	04/11/2009 1	System
		 Milestor 	e CEN e CEN e CEN e CEN e CEN e CEN e CEN e CEN	29/10/2009 0 29/10/2009 0 29/10/2009 0 29/10/2009 0 08/10/2009 0 08/10/2009 0 08/10/2009 0 08/10/2009 0	Copy Ctrl+C Delete Delete Detail Ctrl+D Filter Ctrl+L Refresh F5 NOT:05 HYPERV02 k:03:59 HYPERV02
4.	Review the Description field for detailed information. If the status is describing an error, it will typically include information on possible resolutions.	Status Messan	e Details		X
ч.		Date: I	08/10/2009	Туре:	Milestone
		Time:	08:04:05.933	Severity:	Information
		Site code:	CEN	Message ID:	10002
		System: I	HYPERV01	Process ID:	3192
		Source:	6MS Client	Thread ID:	4716
		Component:	Software Distribution		
		Description:			
		Advertisement	"CEN20003" was recei	ved from site "CB	EN".
		The client pas	ses any supported platfo	rm requirements	and the SMS 📃
		Properties:			
		Advertisement Client SMS Un 4429DD023E/	ID : CEN20003 ique ID : GUID:29F02D \5	46-7FAD-4D98-9	3D89-
		<u> </u>	rious <u>V</u> ext	ОК	Help

Table 37: Using Configuration Manager Status System

8.2 Managing Changes to Packages

When making changes to Configuration Manager packages, the package information needs to be replicated to DPs and to any child sites. However, if regular changes are to be made to a package, for example, files changes in the package source files, the package can be configured to update the DPs on a schedule. This configuration procedure is covered in section 5.1.2.

Table 38 shows the procedure for manually updating the package on the DP:



Table 38: Updating Distribution Points

8.3 Removing Packages

Healthcare IT Administrators should monitor the existing packages within Configuration Manager on a regular basis and remove any packages that are no longer required. This will help to reduce the disk space requirements for the Configuration Manager environment as a whole, because packages can be stored in multiple locations within a Configuration Manager hierarchy. Table 39 shows the steps required to remove packages from Configuration Manager:

Step	Description	Screenshot	
1.	Open the Configuration Manager Console and navigate to the Packages node. Right-click on the required package node and select Delete .	 Software Distribution Software Distribution Software Distribution Software CCM Framework Tool Software Operating Microsoft Configuratin Microsoft Hyper-V Int Microsoft MDT Package Microsoft MDT Package Microsoft USMT (X86) Software Updates Microsoft Corporatio Advertisements Software Updates Software Metering Reporting Reporting Desired Configuration Mana Queries Mobile Device Management System Status Security Rights 	s 4.00 on Manager Client Upgrade 4.0 / egration X86 rergration Services X64 ge 1.0 (3.01) Update Distribution Points Manage Distribution Points Distribute Transfer Site Settings Move Items Give Feedback New Window from Here Cut Delete Refresh Pronerties

Step Description	Screenshot
2. Click Next.	Delete Package Wizard Image: Confirmation Welcome Welcome to the Delete Package Wizard Deletion Effects You can use this wizard to delete packages, as well as seeing the results of deleting that package. Package: Example Package To continue, click Next. To continue, click Next.

- 3. Select one of the following information options:
 - Click No. I know that I want to delete this package to prevent the wizard from showing the summary information and proceed straight to Step 4.
 - Click Yes, I want to see more information to show a series of screens listing all of the associated objects that will also be deleted when deleting this package. This information includes programs, advertisements, task sequences, distribution points (this does not delete the DP itself, just the package on the DP), access accounts and security rights. If any of the objects associated with the package must not be deleted, the package should not be deleted.



Click Next.

4. Click Finish.

Completing the De	Nete Package Wizard
Wekome Deletion Effects Confirmation	You have successfully completed the Delete Package Wizard. You have chosen to delete the package listed below. Package: Example Paskage To delete the package, click-Finish.
	< Previous Next > Finish Cancel

Table 39: Removing Packages

8.4 Software Distribution Security

Configuration Manager software distribution is a powerful feature that can be used as a major point of attack if not secured properly. When installing packages, Configuration Manager can use elevated rights in either the user or the system context, even if the user does not have administrative rights. This allows an attacker to effectively run any attacks that elevate rights. The following recommended security current best practices are detailed in this section:

- Enforce Role Separation
- Ensure Appropriate User Interaction
- Secure Software at the Package Access Level
- Set Permissions at Package Creation
- Secure Package Source Files
- Client Cache Considerations

8.4.1 Enforce Role Separation

Not all administrators need full administrative access to Configuration Manager. Consider applying security permissions to collections to limit which administrators can perform which functions on a given collection. For example, if one administrator manages the servers, and another administrator is responsible for desktop computers in a site, create separate collections and assign permissions to the instance accordingly.

Also consider separating the functions of packaging and advertising administrators. If the same person is allowed to create both packages and advertisements, that person can easily distribute malicious software. Permission to advertise software can be controlled on a collection-by-collection basis, or it can be restricted on each advertisement. Section 4.1 has further details on Configuration Manager Object Security.

8.4.2 Ensure Appropriate User Interaction

When configuring a program, the option **Allow users to interact with this program** can be set so that users can respond to any required prompts in the user interface. If the program is also configured to **Run with administrative rights**, a user at the computer that is running the program could use the user interface to form an attack in order to escalate privilege on the client computer.

It is strongly recommended that Windows Installer-based setup programs are used with per-user elevated privileges for installations that require administrative credentials, but they must also be run in the context of a user who does not have administrative credentials. Using Windows Installer per-user elevated privileges provides the most secure way of deploying applications with this requirement.

Note

If an advertised program is set to Run with administrative rights, and Allow users to interact with this program is not selected, the program might fail if it displays a dialog box that requires a user to make a selection or click a button. In such a case, the dialog box that the user is required to interact with is not visible to the user so it can never be responded to. The program waits for user interaction until the program's configured Maximum allowed run time is exceeded. After the Maximum allowed run time is exceeded, the program's process is terminated on the Configuration Manager client. If a Maximum allowed run time program starts to run until the program's process ends after 72 hours. During the period from when the program starts to run until the program's process ends, Configuration Manager will not start any other pending software distribution programs.

If a package is created using the Create Package from Definition Wizard, and the package definition file line **UserInputRequired=False is not specified**, Configuration Manager creates the program for the package with **Allow users to interact with this program** enabled. If user interaction is not required, always include the line **UserInputRequired=False** in the package definition file. If any packages have already been created from definition files, manually disable the setting **Allow users to interact with this program** on any programs within that package, where it is not required.

8.4.3 Secure Software at the Package Access Level

By default, the package files on DPs are fully accessible by administrators and are readable by users. Users with administrative rights can set the Configuration Manager client to join any site, even if the computer is not within the boundaries of the site. When the Configuration Manager clients have joined the site, they can receive any software distributions that are available at that site, and where the computer or user meets the qualifications of the relevant collections. For this reason, software that will be limited to specific users must be secured to those users at the package access level, rather than being limited by site availability or collection criteria. Section 5.3 contains more detail on securing Configuration Manager packages using package access accounts.

8.4.4 Set Permissions at Package Creation

Changes to the access accounts on the package files (as opposed to the DP shared folders), only become effective when the package is refreshed. Therefore, package access permissions need to be set carefully when the package is first created, especially if the package is large, is being distributed to many DPs, or if network capacity for package distributions is limited. To quickly initiate the refresh of all DPs, use the Update Distribution Points task for the package. See section 8.2 for more information.

8.4.5 Secure the Package Source Files

When creating packages, many packages have sources files that are available from either a directory or a shared folder. Configuration Manager uses those source files to update the packages. However, because the source files are not in Configuration Manager directories, they are not being secured by Configuration Manager. If the files have been tampered with, Configuration Manager clients could be compromised. Therefore, ensure that the source files are secured. The only Configuration Manager accounts that need access to the package source files are the Configuration Manager site server computer account and the Configuration Manager administrator logged on when the package is first created.

8.4.6 Client Cache Considerations

When packages are downloaded to Configuration Manager clients, the package source files are stored in the Configuration Manager client's download cache. This means that packages can be run by anyone on the computer by browsing to that directory; or a user could copy the files to a directory or shared folder that can be accessed by other people. If unauthorised people must not be able to access the files, the download option must not be used for those packages.

APPENDIX A Skills and Training Resources

The tables in 8.4.6APPENDIX APART 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. 8.4.6APPENDIX APART II lists additional training resources that might be useful.

PART I TRAINING RESOURCES

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

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

Table 40: Microsoft System Center Configuration Manager 2007 Training Resources

PART II SUPPLEMENTAL TRAINING RESOURCES

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

Table 41: Supplemental Training Resources

APPENDIX B DOCUMENT INFORMATION

PART I TERMS AND ABBREVIATIONS

Abbreviation	Definition
CUI	Common User Interface
DDR	Discovery Data Record
DNS	Domain Name System
DP	Distribution Point
IP	Internet Protocol
MIF	Management Information Format
NAT	Network Address Translation
OSD	Operating system distribution
OU	Organizational Unit
ММС	Microsoft Management Console
MP	Management Point
NAT	Network Address Translation
SP	Service Pack
SQL	Structured Query Language
WAN	Wide Area Network
Windows PE	Windows Pre-Execution Environment
WMI	Windows Management Instrumentation

Table 42: Terms and Abbreviations
PART II REFERENCES

Reference	Document	Version
R1.	System Center Configuration Manager 2007 Deployment Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/systman/scom.aspx	1.0.0.0
R2.	Microsoft TechNet: Overview of Configuration Manager Object Security and WMI: <u>http://technet.microsoft.com/en-us/library/bb632332.aspx</u>	
R3.	Microsoft TechNet: Classes and Instances for Object Security in Configuration Manager: http://technet.microsoft.com/en-us/library/bb632791.aspx	
R4.	Microsoft Downloads: System Center Configuration Manager 2007 Toolkit: <u>http://www.microsoft.com/downloads/details.aspx?FamilyID=948e477e-fd3b-4a09-9015-</u> <u>141683c7ad5f&DisplayLang=en</u>	
R5.	Microsoft TechNet: Creating Custom Reports by Using Configuration Manager 2007 SQL Views: http://technet.microsoft.com/en-us/library/dd334593.aspx	

Table 43: References