

# 1. SCCM

Short for **System Center Configuration Manager**, **SCCM** is a software management suite allowing users to manage a large number of Windows computers. SCCM is designed and provided by Microsoft and allows for remote control, patch management, operating system deployment, network protection and other various services.

SCCM was formerly known as Systems Management Server (SMS), originally released in 1994. In November 2007, SMS was renamed to SCCM. The most current version is 2012, originally called v.Next, but it is still considered a release candidate product, with an expected final release date of April 2012. The latest stable release is version 2007 R3, originally released in 2010.

**System Center Configuration Manager** (officially referred to as ConfigMgr 2012 or ConfigMgr 2007 or simply ConfigMgr), formerly **Systems Management Server** (SMS), is a systems management software product by Microsoft for managing large groups of computers running Windows, Windows Embedded, Mac OS X, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android.<sup>[1]</sup> Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory.

There have been three major iterations of SMS. The 1.x versions of the product defined the scope of control of the management server (the site) in terms of the NT domain being managed. Since the 2.x versions, that site paradigm has switched to a group of subnets that will be managed together. Since SMS 2003, the site could also be defined as one or more Active Directory sites. The most frequently used feature is inventory management which provides both hardware and software inventory across a business enterprise.

The major difference between the 2.x product and SMS 2003 is the introduction of the Advanced Client. The Advanced Client communicates with a more scalable management infrastructure, namely the Management Point. A Management Point (MP) can manage up to 25000 Advanced Clients.

The Advanced Client was introduced to provide a solution to the problem where a managed laptop might connect to a corporate network from multiple locations and thus should not always download content from the same place within the enterprise (though it should always receive policy from its own site). When an Advanced Client is within another location (SMS Site), it may use a local distribution point to download or run a program which can conserve bandwidth across a WAN.

The current generation of the product, System Center 2012 Configuration Manager, was released in March 2012

## 2. Comparison of SMS 2003 vs SCCM 2007 vs SCCM 2012

Features	SMS 2003	ConfigMgr 2007	ConfigMgr 2012
----------	----------	----------------	----------------

Hardware & Software Inventory	✓	✓	✓
Define Inventory Collection	✓ Using SMS_def.mof file	✓ Using SMS_def.mof file	✓ GUI
Software Distribution	✓	✓	✓
Computer-based Targeting	✓	✓	✓
Self-service Portal			✓
User Only Collection			✓
Device Only Collection			✓
User-Device Affinity			✓
State-based Application Management			✓
App-V Package Distribution		✓	✓
Windows Store Package Distribution			✓
Windows Phone Application Distribution			✓
Windows Mobile Cabinet Package Distribution		✓	✓
iOS .ipa Package Distribution			✓
iOS Application from AppStore			✓
Android .apk Package Distribution			✓
Android Application from Google Play			✓
Auto-install Dependant Application	✓*P Cannot check existence of dependant app before installing	✓*P Cannot check existence of dependant app before installing	✓
Application Requirement Rules			✓
Shared Cache			✓
User-Triggered Un-installation			✓

Hierarchy			
Boundary Groups			✓
Software Updates Management	ITMU	WSUS	WSUS
3rd Party Application		✓	✓
Automatic Deployment Rules			✓
Automatic clean-up of Superseded and Expired Updates			✓
Software Metering	✓	✓	✓
Policy Targeting	Site	Site	Collection
Remote Control	✓	✓	✓Ctrl-Alt-Del
Reporting	✓Web	✓Web + SQL Reporting Services	✓SQL Reporting Services
Agent-based Management	✓	✓	✓
Active Directory Integration	✓	✓	✓
Automatic Site Boundary Discovery			✓
Cross-forest Management			✓
User Discovery		✓	✓
Computer Discovery	✓	✓	✓
AD Group Discovery		✓	✓
Operating System Deployment		✓	✓
Offline Image Servicing			✓
Task Sequence		✓	✓
Automatic Driver Injection		✓	✓
Integration with MDT		✓	✓
Automatic Detection of Configurations and Settings		✓known as Desired Configuration Management	✓known as Settings Management
Automatic Remediation			✓
Internet-based Client Management	✓	✓	✓

Maintenance Window		✓	✓
Intel vPro Integration		✓ SP1	✓
Role-based Access Control			✓
Define User Scope			✓
Power Management		✓ R3	✓
Ability for Users to Opt-out			✓
Device Management		✓	✓
Windows Mobile		✓	✓
Windows Phone			✓
Apple iOS			✓
Google Android			

### 3. SCCM / SMS Interview Questions

*Can you distribute a package to a computer without making it a member of a collection?*

No. To distribute software you must have a package, a program and an advertisement. Advertisements can only be sent to collections, not to computers. If you want to distribute a package to a single computer, you must create a collection for that computer.

**What is Secondary Site?**

Four Main characteristics:

- A Secondary Site does not have access to a Microsoft SQL Database
- Secondary Sites are ALWAYS a Child Site of a Primary Site and can only be administered via a Primary Site
- Secondary Sites cannot have Child Sites of their own
- Clients cannot be assigned directly to the Site

**What is CENTRAL SITE?**

A Central Site is a Configuration Manager Primary Site that resides at the top of the Configuration Manager hierarchy. All Database information rolls from the child to the parent and is collected by the Central Site's Configuration Manager Database. The Central Site can administer any site below it in the hierarchy and can send data down to those sites as well.

**What is PRIMARY SITE?**

Four main characteristics:

- The Site has access to a Microsoft SQL Server Database
- Can administer or be administered via the Configuration Manager Console
- It can be a child of other Primary Sites and can have Child Sites of its own
- Clients can be assigned directly to the Site

**How do you install and configure Secondary site server**

<http://exchangeserverinfo.com/2008/05/02/installation-and-configuration-of-secondary-site-server.aspx>

### **How do you create a package for Adobe?**

the command line `msiexec.exe /q ALLUSERS=2 /m MSIHPSJR /i "AcroRead.msi"`

`TRANSFORMS=mytransform.mst`

How do you distribute a package?

- create a package in SCCM, pointing it to the installation sources, and in the package create an install program (you may have already done this?)
- assign Distribution Points to your package so the contents get synched.
- create a Collection containing the objects (users/computers) that are allowed to receive the package.
- create an Advertisement for the distribution, linking the package you created to the collection, decide whether the Advertisement is mandatory (installation enforced) or not (users have to go to the "Run Advertised Programs" dialog in Windows and select to install the program)

### **How SCCM download the patches?**

You need to add the Software Update Point site role to the site, configure the software update point as active, configure the products, classifications, sync settings, etc. in the Software Update Point properties. THEN, you can go to the Update Repository node and run the Run Synchronization action from the central primary site. Once synchronization completes, you will see the metadata in the Configuration Manager console.

### **How do you configure the SUP?**

In the Configuration Manager console, navigate to **System Center Configuration Manager / Site Database / Site Management / &lt;site code> – <site name> / Site Settings / Site Systems**

Right-click the site system server name, and then click **New Roles**.

Select **Software update point**, and then click **Next**.

Specify whether the site server will use a proxy server when connecting to the software update point, and then click **Next**.

Select **Use this server as the active software update point**, and then specify the port settings configured for the WSUS Web site on this site system.

Specify the synchronization source for the active software update point using one of the following settings: like **Synchronize from Microsoft Update or Synchronize from an upstream update server**

Keep the default setting **Do not create WSUS reporting events**, and then click **Next**

Specify whether to synchronize software updates on a schedule by selecting **Enable synchronization on a schedule**

Specify the update classifications for which the software updates will be synchronized, and then click **Next**.

Specify the products for which the software updates will be synchronized, and then click **Next**.

Open **SUPSetup.log** in `<InstallationPath>Logs` to monitor the installation progress for the software update point.

When the installation completes, `Installation was successful` is written to the log file.

Open **WCM.log** in `<InstallationPath>Logs` to verify that the connection to the WSUS server was successful.

How do you Backup SCCM Server?

To create a scheduled backup task, expand the Site Settings node and expand the Site Maintenance node, click on Tasks.

For Manual backup – Start `SMS_SITE_BACKUP` service

### **What are the client deployments methods?**

Client Push Installation, Software update point based installation, Group Policy Installation, Logon Script Installation, Manual Installation, Upgrade Installation(software Distribution)

### **Can you discover clients those are in different AD forest?**

yes.

Internet-based client management, which supports the following site systems installed in a separate forest to the site server:

Management point

Distribution point

Software update point

Fallback status point

### **What are the prerequisite for Software Update Point?**

Windows Server Update Services (WSUS) 3.0, WSUS 3.0 Administration Console, Windows Update Agent (WUA) 3.0, Site server communication to the active software update point, Network Load Balancing (NLB), Background Intelligent Transfer Server (BITS) 2.5, Windows Installer

What is SMS Provider?

The SMS Provider is a WMI provider that allows both read and write access to the Configuration Manager 2007 site database. The SMS Provider is used by the Configuration Manager console

The SMS Provider can be installed on the site database server computer, site server computer or another server class third computer during Configuration Manager 2007 Setup. After setup has completed, the current installed location of the SMS Provider is displayed on the site properties general tab

### **What is ITMU?**

SMS 2003 Inventory Tool for Microsoft Updates

What is the use of WSUS (Windows Server Update Service)?

It enables administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system.

### **Difference between SMS 2003 and SCCM 2007**

What is WMI (Windows Management Instrumentation)?

You can write WMI scripts or applications to automate administrative tasks on remote computers

### **What is SUP ( Software Update Point)?**

This is required component of software updates, and after it is installed, the SUP is displayed as a site system role in the Configuration Manager console. The software update point site system role must be created on a site system server that has Windows Server Update Services (WSUS) 3.0

### **You want specific users/groups to run specific custom reports. What should you do?**

Navigate to “System Center Configuration Manager – Site Database – Security Rights – Users”

Right click on “Users” and select “Manage ConfigMgr Users”

Navigate to the “SCCM Support” group you created earlier

1. For “Collection” – “(All Instances)” add the following:
  - “Delete resource”

- “Modify resource”
  - “Read”
  - “Read resource”
  - “Use remote tools”
2. For “Report” – “(All Instances)” add the following:
    - “Read”
  3. For “Computer association” – “(All Instances)” add the following:
    - “Create”
    - “Delete”
    - “Read”
    - “Recover user state”
  4. Click “Next”
  5. Click “Next”
  6. Click “Close”

*You have been provided with permissions on the SCCM console to create, distribute, modify and delete packages? However, when distributing a package there is no Distribution points listed in the Distribution Point Wizard. What should you do?*

*To designate a distribution point on a new server or server share*

1. In the Configuration Manager console, navigate to **System Center Configuration Manager / Site Database / Site Management / <site name> / Site Settings**.
2. Right-click **Site Systems**, point to New, and then click Server or Server Share, depending on which you want to create.
3. If you are creating a new server, use the **New Site System Server Wizard** to create the site system server, and select the **Distribution Point** check box from the **Available Roles** on the **System Role Selection** page to designate this server as a distribution point.

#### **4. Difference Between SMS 2003, SCCM 2007 & SCCM 2012**

<b>Features</b>	<b>SMS2003</b>	<b>SCCM2007</b>	<b>SCCM 2012</b>
Hardware & Software Inventory	✓	✓	✓
Automatic Client Health Remediation			✓
Software Distribution	✓	✓	✓
Computer based targeting	✓	✓	✓
User based targeting		✓*P	✓
State-based Application Distribution			✓
Self-service portal			✓
App-V Package Deployment		✓	✓
Xen-App Package Deployment			✓
Uninstallation via Software Center			✓
User-Device Affinity			✓
Distribution Point Groups			✓
Boundary Groups			✓
Application Revision History			✓

Content Management			✓
Software Updates	ITMU	Via WSUS	Via WSUS
3 <sup>rd</sup> party application		✓	✓
Automatic Software Updates Deployment Rules			✓
Automatic clean-up of Superseded and Expired Updates			✓
Software Metering	✓	✓	✓
Collection-based Policies			✓
Remote Administration	Remote Tools	Remote Tools & Remote Desktop	Remote Tools + Ctrl-Alt-Del
Reporting	Basic	Basic & SQL Reporting	SQL Reporting Services
Administrator Console	✓	✓	✓
User-friendly ribbon			✓
Status reporting		✓*P	✓
Agent Managed	✓	✓	✓
Integrate with Active Directory	✓	✓	✓
Automatic Boundary Discovery			✓
Forest Discovery			✓
Discovery of Computers	✓	✓	✓
Operating System Deployment		✓	✓
Offline Servicing of OS Image			✓
Task Sequence		✓	✓
Maintenance Windows		✓	✓
Desired Configuration Management		✓	✓
Automatic Remediation of Configuration Drift			✓
Internet Based Client Management		✓	✓
Integration with Windows Server 2008 Network Access Protection		✓	✓
Intel vPro Intergration		✓ SP1	✓
Role-based Access Control			✓
Power Management		✓ R3	✓
User Power Management Opt-out			✓
Windows Mobile Device Management		✓	✓
Non-Windows Mobile Device Management			✓

## 5. System Center Operations Manager (SCOM)

is a cross-platform data center management system for operating systems and hypervisors. It uses a single interface that shows state, health and performance information of computer systems. It also provides alerts generated according to some availability, performance, configuration or security situation being identified. It works with Microsoft Windows Server and Unix-based hosts.

System Center Configuration Manager helps find everything, inventory it and then distribute new software and patches to those systems. While this tool ensures that systems throughout the enterprise are properly accounted for and installed with the right software, Configuration Manager's work ends when the machine is ready for use. After that, the system becomes just another device in a field of devices that may or may not be functioning properly.



Manually monitoring systems is feasible in a small enough environment. An admin can check the logs of his servers each morning, users can report issues with their computers when they happen, and a help desk guy on his way to lunch can notice the blinking light on the printer that says it's almost out of toner.

Running an enterprise-size computing environment takes a lot of work. The bigger the environment gets, the less possible this type of monitoring becomes. Eventually, there are too many servers to actually check logs on each day. Printer lights go unnoticed as more and more users send print jobs that pile up in the queue, before being printed elsewhere (usually without cancelling the original print jobs). For the typical growing business, there comes a point where the only monitoring tool is a help desk phone. If a user's machine is slow, the help desk ticket is the first indicator of trouble. If a server is slowing down, reports of sluggish file access is the first symptom of a bigger problem.

This method can actually work for a while if administrators respond quickly to issues before they blow up into bigger problems. Eventually, however, a user suddenly runs out of disk space while running a critical report, or the second hard drive in an array fails and takes the whole server down and so on. When too many things blossom into big issues because smaller, easier to fix problems went undetected for too long, that's when IT finally budgets for a monitoring solution.

Microsoft System Center Operations Manager (SCOM) is a robust, enterprise-level monitoring solution that offers a way to monitor, detect and react to trouble before it gets out of hand, sometimes without any administrator intervention at all.

A central component of the **Microsoft System Center suite, Operations Manager (SCOM) 2007** is a third-generation product, formerly dubbed Microsoft Operations Manager (MOM). SCOM is used to monitor the health and performance of everything from servers to individual applications in Microsoft Windows environments.

Like Configuration Manager, Microsoft designed SCOM 2007 to help administrators gain better control over their IT environments through different management services working simultaneously for maximum system efficiency.

The company incorporated significant features with SCOM 2007 in order to meet customer needs. For instance, visibility has become one of the defining features of the product in the form of end-to-end service monitoring. To that effect, it allows administrators to screen the state of services known as distributed applications. End-to-end service monitoring also presents mock transactions to give administrators an understanding of the service from the viewpoint of an end user for more proficient troubleshooting.

With SCOM 2007 management packs, administrators can extend Operations Manager capabilities to a wide variety of technologies, including operating systems and applications. In fact, numerous management packs are available for more than 60 Microsoft and third-party products, such as Windows Vista, SQL Server and Exchange Server.

Moreover, SCOM 2007 uses role-based security or custom user roles to allow access to Operations Manager beyond operators and administrators. It also links to Active Directory for simpler deployments and access management controlled by custom user roles.

"What this feature does is allow us to fully automate agent deployment for Operations Manager-based environments," said Pete Zerger, a Microsoft MVP and co-owner of AKOS Technology Services. "As the agent is started up, it will actually query its local Active Directory domain to see if configuration information has been published for an Operations Manager management group."

Each of these features carries over to System Center Operations Manager 2007 R2, released in the spring of 2009 and outfitted with advanced functionality. Upgrading is simple for administrators already working with Operations Manager 2007 SP1.

Those who do decide to upgrade will notice improvements in everything from the user interface to the core product itself, including extended cloud support.

## NEW FEATURES

- **Cross-platform monitoring** – Operations Manager 2007 R2 features enhanced interoperability through Unix and Linux support via a single Windows-based interface. Several management packs have also been developed to extend support.
- 
- **Management pack companion** – R2's Management Pack Wizard provides an inside look at all there is to know about SCOM 2007 MPs, including package updates and the management pack catalog. Administrators can also download and deploy management packs straight from the wizard and keep up with the newest releases.
- 
- **Service-level monitoring** – The service tracking functionality allows administrators to customize service-level objectives, such as distributed applications. Custom settings include when the applications are accessible and when and how they perform.

## FEATURED CONTENT

- **Ops Manager 2007 feature allows for automated agent deployments**  
Microsoft MVP Pete Zerger takes a closer look at the integration of Active Directory with System Center Operations Manager 2007 and how it might simplify administrative tasks.
- **Microsoft server manager adds Linux, Unix support**  
This may be the end of cross-platform criticisms as Microsoft leaps outside the company bubble and adds Unix and Linux support to its System Center Operations Manager product.

- **Updated management pack monitors DFS namespaces**  
Admins can track the health of their machines with an updated management pack that works with System Center Operations Manager to create a centralized monitoring hub.

## **6 Why we require to extend schema ?**

Extending the Active Directory schema for Configuration Manager 2007 allows clients to retrieve many types of information related to Configuration Manager from a trusted source. In some cases, there are workarounds for retrieving the necessary information if the Active Directory schema is not extended, but they are all less secure than querying Active Directory Domain Services.

Additionally, not extending the schema might incur significant workload on other administrators who might need to create and maintain the workaround solutions such as logon scripts and Group Policy objects (GPO) for computers and users in your organization.

The Active Directory schema can be extended before or after running Configuration Manager 2007 Setup. However, as a best practice, extend the schema before you run Configuration Manager 2007 Setup. You have to extend the Active Directory schema only once for the forest that contains site servers; you do not have to extend the schema again if you upgrade the operating systems on the domain controllers or after you raise the domain or forest functional levels. If new versions of Configuration Manager provide new schema extensions that require you to extend the schema again, this requirement will be documented in [Configuration Manager Supported Configurations](#).

### **Using SMS 2003 Active Directory Schema Extensions for Configuration Manager Sites**

It is supported to deploy Configuration Manager 2007 sites using SMS 2003 Active Directory schema extensions. There are important considerations when deciding whether or not to extend the Active Directory schema for Configuration Manager 2007. Even if the Configuration Manager 2007 site is publishing site data to Active Directory Domain Services, the required Active Directory schema attributes to store the published data will not exist in some cases if the Active Directory schema has only been extended for SMS 2003.

If the Active Directory schema has been extended for SMS 2003, but not for Configuration Manager, the following limitations apply:

- A Configuration Manager 2007 server locator point must be used to allow clients to verify assigned site compatibility to complete client assignment. Clients can automatically locate a server locator point through Active Directory Domain Services if the schema is extended for SMS 2003.
- Because Network Access Protection for Configuration Manager requires Configuration Manager 2007 Active Directory schema extensions, this feature is unsupported for sites using SMS 2003 Active Directory schema extensions.

- Site mode changes require manual workarounds on clients.
- Client communication port changes require manual workarounds.
- The management point dNSHostName attribute is no longer published to Active Directory Domain Services.

## Feature and Function Considerations for Extending the Active Directory Schema for Configuration Manager

The following table lists the specific Configuration Manager 2007 features or functions that use Active Directory schema extensions, and any related workarounds if the schema is not extended for Configuration Manager 2007.

Feature or function	Schema extension requirement	Requirement details
Client installation and site assignment	Recommended	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, client installation using Ccmsetup.exe will not be able to automatically retrieve client deployment parameters from Active Directory Domain Services.</p> <p><b>Workaround:</b> Provide client installation properties by using CCMSsetup installation command-line options. For more information, see <a href="#">About Configuration Manager Client Installation Properties</a>.</p> <p><b>Workaround:</b> A Configuration Manager 2007 server locator point that is published to Active Directory Domain Services by using SMS 2003 schema extensions can be automatically located by Configuration Manager 2007 clients if they belong to the same Active Directory forest.</p> <p><b>Workaround:</b> Provide server locator point information by using the client.msi property SMSSLP=&lt;server locator point name&gt; on the CCMSsetup command line during client installation. For more information, see <a href="#">About Configuration Manager Client Installation Properties</a>.</p> <p><b>Workaround:</b> Publish the management point in</p>

		DNS, and publish the server locator point in WINS. For more information, see <a href="#">Configuration Manager and Service Location (Site Information and Management Points)</a> .
Site mode setting and related settings such as client certificate selection and CRL checking	Recommended	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, site mode information and client settings related to native mode configuration cannot be published to Active Directory Domain Services.</p> <p><b>Workaround:</b> Use CCMSSetup.exe client installation command-line properties or client push installation.</p>
Port configuration for client-to-server communication.	Recommended	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, clients will not be able to communicate with site systems if the default communication port is changed after client installation.</p> <p><b>Workaround:</b> Reinstall all affected clients, or deploy a script to manually change the ports used by clients to communicate with site systems within the site.</p>
Global roaming	Required	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager or SMS 2003, a roaming client cannot request content for advertisements and software updates from resident management points. This scenario produces additional network traffic to request content location from the client's default management point, and the client will not be able to locate content from sibling sites in the hierarchy or from sites that are higher in the hierarchy than the client's assigned site. For more information about client behavior when roaming, see <a href="#">About Client Roaming in Configuration Manager</a>.</p> <p><b>Workaround:</b> None.</p>
Network Access Protection (NAP) for Configuration Manager	Required	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, sites enabled for Network Access Protection will be unable to publish Configuration Manager health state references to Active Directory Domain Services. If health state references are not published to Active Directory Domain Servers, the System Health Validator point is unable to validate client</p>

		<p>statements of health.</p> <p><b>Workaround:</b> None.</p>
Secure key exchange between sites <sup>1</sup>	Recommended	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, sites configured to require secure key exchange will be unable to automatically exchange public keys to enable site-to-site communication.</p> <p><b>Note</b> Secure key exchange between Configuration Manager sites is enabled by default.<sup>1</sup></p> <p><b>Workaround:</b> Manually exchange the parent and child site's public keys before attaching a child site by using the hierarchy maintenance tool (Preinst.exe). For more information, see <a href="#">How to Manually Exchange Public Keys Between Sites</a>.</p>
Verifying a trusted management point	Recommended	<p><b>Requirement:</b> If the Active Directory schema has not been extended for Configuration Manager, clients must use the trusted root key to establish trust with a site. Unless clients have been pre-provisioned with the trusted root key, they will trust the first management point they communicate with.</p> <p><b>Workaround:</b> Pre-provision the clients with the trusted root key. For more information, see <a href="#">How to Manage the Trusted Root Key in Configuration Manager</a>.</p> <p><b>Workaround:</b> Use native mode. In native mode, the management point certificate must still be signed by the trusted root key at the central site, but the management point uses a PKI-issued certificate. As long as the PKI has not been compromised, the client can trust the first management point it contacts that has a valid server authentication certificate. For more information about the PKI certificate requirements for native mode, see <a href="#">Certificate Requirements for Native Mode</a>.</p>
Recovering from the failure of a central site server hosting the management point role	Recommended	<p><b>Requirement:</b> If Active Directory schema has not been extended for Configuration Manager, and if clients report to a central site server that also functions as the management point for the site,</p>

		<p>clients have no way to automatically establish trust with the site after a new central site server and management point is restored.</p> <p><b>Workaround:</b> Remove the trusted root key from every client in the site and re-provision it. For more information, see <a href="#">How to Manage the Trusted Root Key in Configuration Manager</a>.</p> <p><b>Workaround:</b> Move the management point role to a different server. As long as the clients in the central site lose only the management point or only the central site server, they can re-establish the trust relationship. For more information, see <a href="#">About the Trusted Root Key</a>.</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 7. What are the protocols supported for streaming?

# Basics of streaming protocols

Streaming of audio and video is a confusing subject. This page is aimed at providing some of the basic concepts.

**Streaming** means sending data, usually audio or video, in a way that allows it to start being processed before it's completely received. Video clips on Web pages are a familiar example.

**Progressive streaming**, aka progressive downloading, means receiving an ordinary file and starting to process it before it's completely downloaded. It requires no special protocols, but it requires a format that can be processed based on partial content. This has been around for a long time; interleaved images, where the odd-numbered pixel rows are received and displayed before any of the even ones, are a familiar example. They're displayed at half resolution before the remaining rows fill in the full resolution.

Progressive streaming doesn't have the flexibility of true streaming, since the data rate can't be adjusted on the fly and the transmission can't be separated into multiple streams. If it delivers a whole file quickly and the user listens to or watches just the beginning, it wastes bandwidth. The user is given the whole file and can copy it without any effort.

"True" streaming uses a streaming protocol to control the transfer. The packets received don't add up to a file. Don't mistake streaming for copy protection, though; unless there's server-to-application encryption, it's not hard to reconstruct a file from the data.

True streaming may be **adaptive**. This means that the rate of transfer will automatically change in response to the transfer conditions. If the receiver isn't able to keep up with a higher data rate, the sender will drop to a lower data rate and quality. This may be done by changes within the stream, or by switching the client to a different stream, possibly from another server. Streamingmedia.com has a [discussion of adaptive streaming](#).

Streaming can be broadly divided into **on-demand** and **real-time** categories. With on-demand streaming, the client requests a recording or movie and receives it; normally no one else will receive the same recording at the same time. With real-time streaming, the sender determines what to send, and the receiver plays it back as it's sent, with a slight and consistent delay.

"On-demand" doesn't necessarily imply a request by a human; if a Web page starts playing a movie or song when it's opened, that's on-demand even if it's annoying and unwanted. If it picks up a broadcast in progress, that's real time. "Real-time" doesn't mean "simultaneous with the source"; at a minimum, there's always a speed-of-light delay. Buffering helps to keep a real-time transmission from skipping, and a delay of a significant fraction of a minute may be an acceptable price for this.

Each category has its own complications. With on-demand streaming, the service has to open files as they're requested and keep streams going to each client. If the system load is heavy, it may have to juggle a lot of separate streams. It may fall behind, so that the clients are sometimes forced to pause. This is annoying but acceptable, as long as it doesn't happen too much. With real-time streaming, the service is usually managing a known number of channels, but it has to keep them going at the speed at which they're played back. If it can't keep up, it's usually better to skip rather than pause. Real-time streaming can be point-to-point (one sender, one receiver) or broadcast (one sender, many receivers). A VOIP conversation is an example of two-way point-to-point streaming.

Streaming servers commonly support more than one protocol, falling back on alternatives if the first choice doesn't work.

There's a [general discussion of streaming protocols](#) on Streamingmedia.com.

Streaming and encoding are two separate issues. Streaming deals with how bytes get from one place to another; encoding deals with how sounds and images are converted to bytes and back.

## **The protocol stack**

Streaming involves protocols at several different layers of the OSI Reference Model. The lower levels (physical, data link, and network) are generally taken as given. Streaming protocols involve:

- The **transport layer**, which is responsible for getting data from one end to the other.
- The **session layer**, which organizes streaming activity into ongoing units such as movies and broadcasts.
- The **presentation layer**, which manages the bridge between information as seen by the application and information as sent over the network.
- The **application layer**, which is the level at which an application talks to the network.



Most Internet activity takes place using the TCP transport protocol. TCP is designed to provide reliable transmission. This means that if a packet isn't received, it will make further efforts to get it through. Reliability is a good thing, but it can come at the expense of timeliness. Real-time streaming puts a premium on timely delivery, so it often uses UDP (User Datagram Protocol). UDP is lightweight compared with TCP and will keep delivering information rather than put extra effort into re-sending lost packets. Some firewalls may block UDP because they're tailored only for TCP communications.

Support for the right streaming protocol doesn't necessarily mean that software will play a particular stream. You need software that supports both the appropriate streaming protocol and the appropriate encoding.

## **The RTP family**

The Real Time Transport Protocol (RTP) has been around for a long time and is often used for streaming. It's defined by [IETF RFC 3550](#). It's a transport protocol which is built on UDP and designed specifically for real-time transfers. It's possible but unusual to use RTP with TCP. Although it sits on top of UDP (or TCP), it's still considered part of the transport layer. It's closely associated with the Real Time Control Protocol (RTCP), which operates at the session layer. The primary function of RTCP is "to provide feedback on the quality of the data distribution," allowing actions such as adjusting the data rate.

Some other protocols are typically used with RTP but aren't tightly coupled to it. The Real Time Streaming Protocol (RTSP), defined by [IETF RFC 2326](#), is a presentation-layer protocol that is described as a "network remote control." It resembles HTTP in some ways, and it carries requests to initiate activities such as playing, pausing, and recording. The Resource Reservation Protocol, with the strained abbreviation RSVP and a spec at [RFC 2205](#), operates at the transport level though it's used in setting up sessions. The protocol stack of RTP, RTCP, and RTSP is sometimes referred to as "RTSP."

RTP, RTCP, and RTSP all operate on different ports. Usually when RTP is on port N, RTCP is on port N+1.

An RTP session may contain multiple streams to be combined at the receiver's end; for example, audio and video may be on separate channels.

UDP URLs aren't widely supported by browsers, so a plug-in is needed to do RTP/UDP streaming to a browser. Flash is the one that's most commonly used. RTP is also used by standalone players such as RealPlayer, Windows Media Player, and QuickTime Player.

Android and iOS devices don't have RTP-compatible players as delivered. There are various third-party applications, including RealPlayer for Android.

## **RTMP**

Real Time Messaging Protocol (RTMP) is a proprietary protocol used primarily by Flash, but implemented by some other software as well. Adobe has released a [specification](#) for it, but it's incomplete in some important respects. It's usually used over TCP, though this isn't a requirement. It operates in the application through session layers. Its importance is a direct result of the ubiquity of Flash, and it will decline as the use of Flash does. Apple's iOS doesn't support RTMP or Flash, so iPhones, iPods, and iPads won't accept RTMP streams except through third-party code. Some RTMP implementations (e.g., JW Player) rely on the availability of the Flash plugin.

Although Flash is commonly associated with proprietary file formats, RTMP works with all media formats.

RTMP can be tunneled through HTTP (RTMPT), which may allow it to be used behind firewalls where straight RTMP is blocked. Other variants are RTMPE (with lightweight encryption), RTMPTE (tunneling and lightweight encryption), and RTMPS (encrypted over SSL).

## **HTTP Live Streaming**

The new trend in streaming is the use of HTTP with protocols that support adaptive bitrates. This is theoretically a bad fit, as HTTP with TCP/IP is designed for reliable delivery rather than keeping up a steady flow, but with the prevalence of high-speed connections these days it doesn't matter so much. Apple's entry is HTTP Live Streaming, aka HLS or Cupertino streaming. It was developed by Apple for iOS and isn't widely supported outside of Apple's products. Long Tail Video provides a [testing page](#) to determine whether a browser supports HLS. Its specification is available as an [Internet Draft](#). The draft contains proprietary material, and publishing derivative works is prohibited.

The only playlist format allowed is M3U Extended (.m3u or .m3u8), but the format of the streams is restricted only by the implementation.

## **Adobe HTTP Dynamic Streaming**

Adobe HTTP Dynamic Streaming (HDS) is also known as San Jose streaming. Like Apple's HLS, it operates over HTTP. Like RTMP, it's associated with Flash. HTTP is more likely to be allowed through than other protocols, and HDS is less of a kludge than RTMP over HTTP. The [technical specs](#) say that Flash is required for playback, so its use is mainly in desktop environments.

## **Microsoft Smooth Streaming**

Smooth Streaming is Microsoft's piece of the very fragmented world of HTTP streaming. It's used with Silverlight and IIS.

## Dynamic Streaming over HTTP

DASH, for Dynamic Streaming over HTTP, is MPEG's offering in the HTTP streaming Babel. DASH's creators insist it's not a protocol but an "enabler," but that claim violates the "looks like a duck" principle. It's specified by ISO/IEC 23009-1:2012.

## Shoutcast

The Shoutcast server is a popular way to deliver broadcast streaming. It uses its own protocols, and finding any decent documentation is difficult. Shoutcast's protocol was originally known as ICY; the name Ultravox is currently used for Shoutcast 2. A superset of HTTP is used, with additional headers that don't follow the "X-" convention. Shoutcast's protocols can be used over either TCP or UDP. Metadata and streaming content are mixed in the same stream. The ICY scheme ("icy://") was used in some early versions of the protocol and is still sometimes found. I've also encountered the schema "icyxp://", which seems to be proprietary to one software creator; a search for information about it turns up nothing.

The Icecast server uses a protocol similar to Shoutcast, but there are some compatibility issues.

Shoutcast protocols are used only for broadcasting, not for on-demand delivery.

## BitTorrent Live Streaming

BitTorrent Live Streaming is a newcomer among streaming protocols, currently (May 2013) in open beta. It's a peer-to-peer protocol that can scale to very large numbers of users; "each user becomes a miniature broadcaster and amplifies your broadcast across the Web." This relieves the original sender of the burden of talking to large numbers of clients. I can't find any technical information on it.

## HTML5

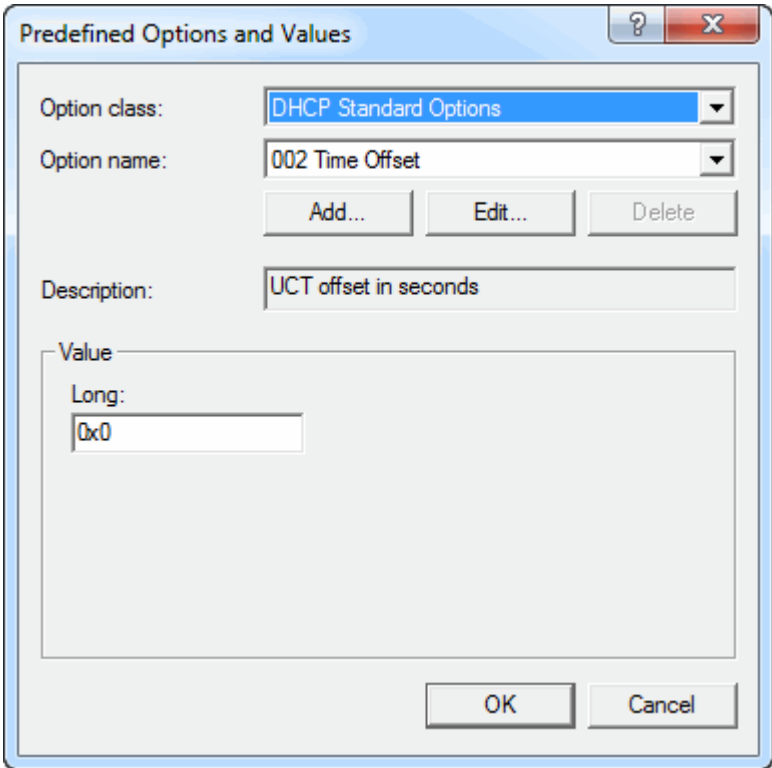
HTML5 needs to be mentioned here, mostly for what it isn't. HTML5 provides the <audio> and <video> tags, along with DOM properties that allow JavaScript to control the playing of the content that these elements specify. This is an application-layer protocol only, with no definition of the lower layers. HTML5 implementations can specify formats which they process. The server is expected to download the content progressively, and it will keep downloading it completely even if paused, unless the browser completely eliminates the element. The Web Audio API allows detailed programmatic control of playback.

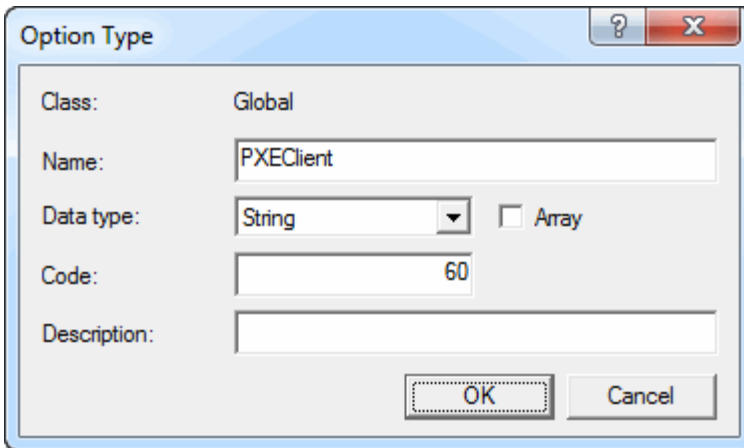
## 8. Configure DHCP to support OSD

Introduction	The following information is the description of how to configure DHCP to support OS Deployment
--------------	------------------------------------------------------------------------------------------------

Element	Description
Settings for ciBoot	<p>If the ciBoot service is running on the machine providing DHCP services, the following options must be set under Scope Options on the DHCP Server.</p> <p>Option 60 Must specify the value PXEClient (the value is case-sensitive)</p> <p>Microsoft does not provide option 60 by default in the DHCP setup, see below for instructions to create the value on a Microsoft DHCP server.</p>
Settings TFTP service	<p>To boot a client via PXE successfully, the following options must be set under Scope Options on the DHCP Server.</p> <p><b>Option 66</b> Must point to a server having a TFTP service available</p> <p><b>Option 67</b> Must point to the boot image to load, in most cases this would point to <code>\cipcc.0</code></p>
Additional options used by OSD	<p><b>Options 5 and 6</b> should also be specified to ensure functional DNS service in WinPE, otherwise the client can experience problems with locating the server. If <b>option 15</b> is not defined a dns suffix may be required for the network access credentials to work correctly.</p> <p><b>Username=installuser@domain.local</b> Using the oldschool syntax <code>domain\installuser</code> will mostly not work in WinPE unless a running WINS service is available. Use <b>option 44</b> to add a WINS server to the DHCP options.</p>
DHCP/PXE models supported by OSD	<p>Depending on the infrastructure provided and the availability and placement of DHCP servers, there are a number of scenarios to use when building DHCP/PXE environments.</p> <p><b>One DHCP one PXE</b> The simple model where the DHCP doubles as the PXE server or simply refers to the PXE server by using 66</p> <p><b>Many DHCP one PXE</b> Point all DHCP servers to the IP of the server, OSD will automatically use the server address provided by DHCP</p> <p><b>One DHCP many PXE</b> To use one PXE server from different DHCP servers or scopes, use option 66 to refer client to the server.</p> <p>*Select PXE server manually from a list*</p> <p>To manually select from a list of available PXE servers, build a number of copies of boot.wim and add additional menu lines to the cipcc.cfg file, each boot.wim should point to a specific servername in OSDLoader.ini.</p>

Create option 60 in Microsoft DHCP server console

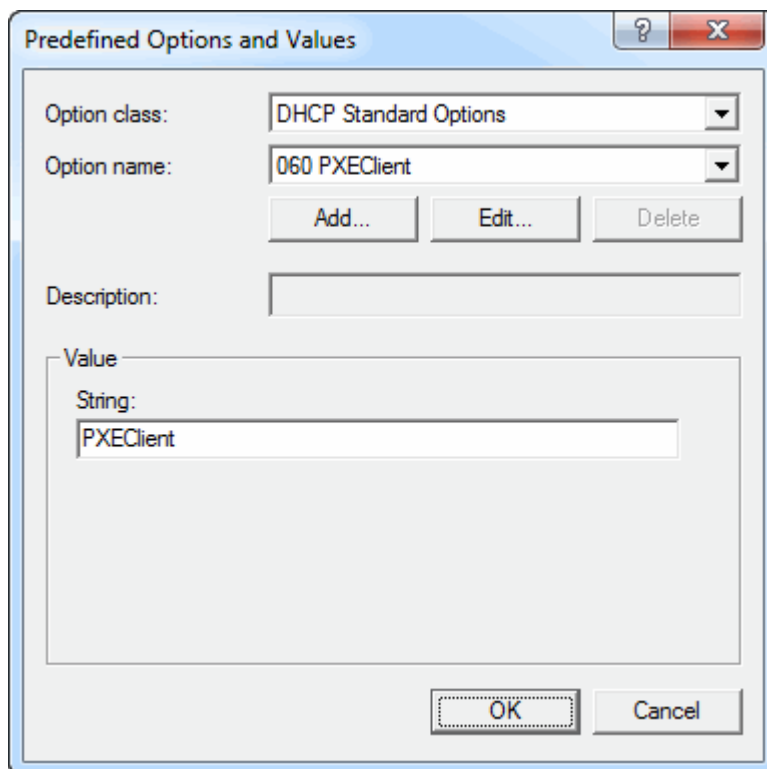
Step	Action
1	Open the DHCP management console
2	Right click the server node and select "Set Predefined Options..." and the follow windows appears. 
3	Click Add... to open the following window



Specify the name, Data type and Code as shown.

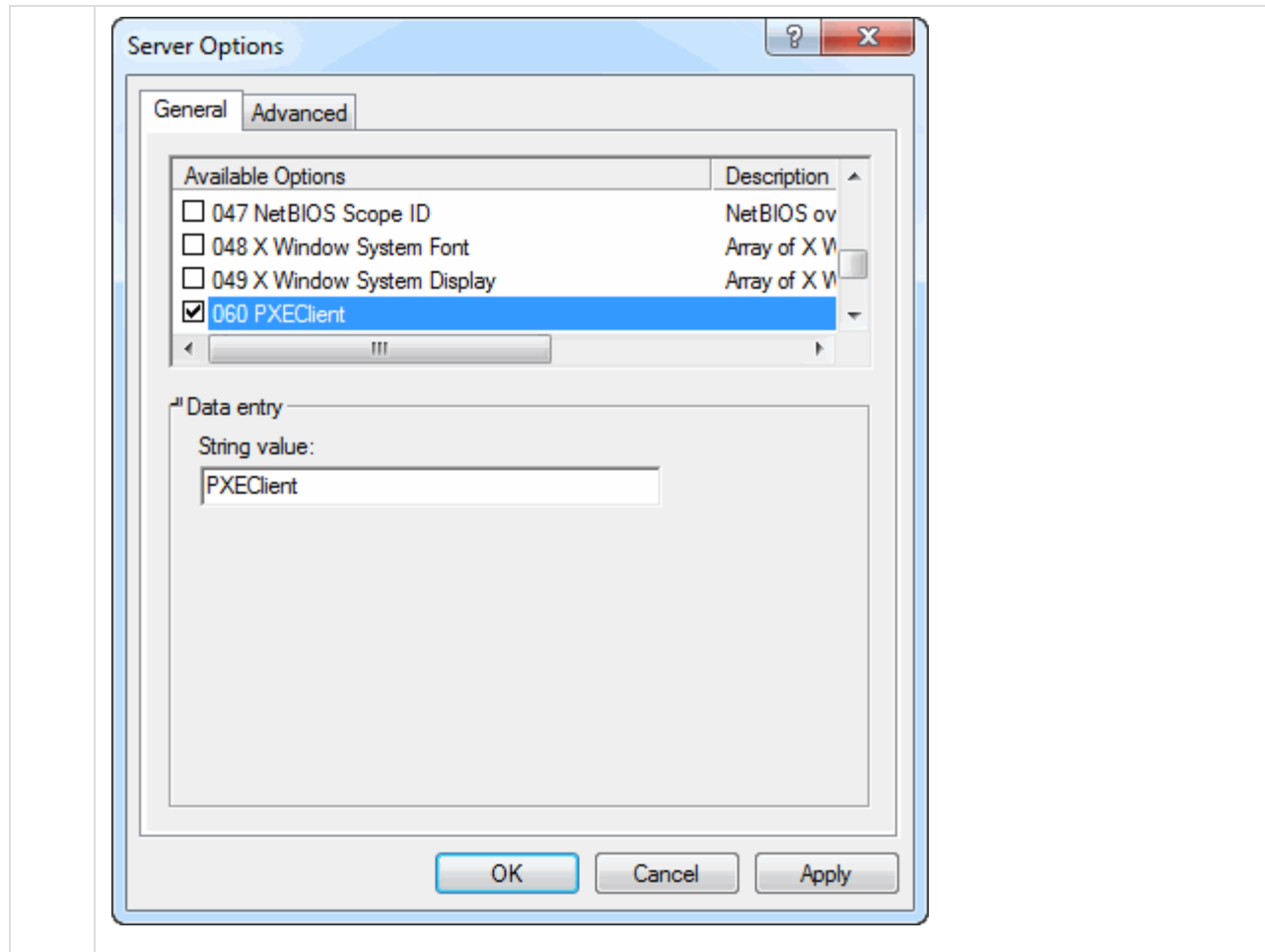
4 Click OK to create the new Option Type.

5 Set the default value of the new Option Type to "PXEClient"



6 Click OK to save new Predefined Option

7 Option 60 is now available as both server option and scope option



## 9. List of Log Files in Configuration Manager 2007

### Client Log Files

The Configuration Manager 2007 client logs are located in one of the following locations:

- On computers that serve as management points, the client logs are located in the *%ProgramFiles%\SMS\_CCM\Logs* folder.
- On all other computers, the client log files are located in the *%Windir%\System32\CCM\Logs* folder or the *%Windir%\SysWOW64\CCM\Logs*.

The following table lists and describes the client log files.

Log File Name	Description
CAS.log	Content Access service. Maintains the local package cache.
CcmExec.log	Records activities of the client and the SMS Agent Host service.
CertificateMaintenance.log	Maintains certificates for Active Directory directory service and management points.
ClientIDManagerStartup.log	Creates and maintains the client GUID.
ClientLocation.log	Site assignment tasks.
ContentTransferManager.log	Schedules the Background Intelligent Transfer Service (BITS) or the Server Message Block (SMB) to download or to access SMS packages.
DataTransferService.log	Records all BITS communication for policy or package access.
Execmgr.log	Records advertisements that run.
FileBITS.log	Records all SMB package access tasks.
Fsinvprovider.log (renamed to FileSystemFile.log in all SMS 2003 Service Packs)	Windows Management Instrumentation (WMI) provider for software inventory and file collection.
InventoryAgent.log	Creates discovery data records (DDRs) and hardware and software inventory records.
LocationServices.log	Finds management points and distribution points.
Mifprovider.log	The WMI provider for .MIF files.
Mtrmgr.log	Monitors all software metering processes.
PolicyAgent.log	Requests policies by using the Data Transfer service.
PolicyAgentProvider.log	Records policy changes.
PolicyEvaluator.log	Records new policy settings.
RemoteControl.log	Logs when the remote control component (WUSER32) starts.
Scheduler.log	Records schedule tasks for all client operations.
Smscliui.log	Records usage of the Systems Management tool in Control Panel.
StatusAgent.log	Logs status messages that are created by the client components.
SWMTRReportGen.log	Generates a usage data report that is collected by the metering agent. (This data is logged in Mtrmgr.log.)



## Site Server Log Files

Most Configuration Manager 2007 site server log files are located in the <InstallationPath>\LOGS folder. Because Configuration Manager 2007 relies heavily on Internet Information Services (IIS), you can review the IIS log file for additional errors that relate to client access to the IIS server. The IIS log file is located in the %Windir%\System32\Logfiles\W3SVC1 folder on the IIS server.

The following table lists and describes the site server log files.

Log File Name	Description
Adsgdis.log	Records Active Directory Security Group Discovery actions.
Adsysgrp.log	Records Active Directory System Group Discovery actions.
Adsysdis.log	Records Active Directory System Discovery actions.
Adusrdis.log	Records Active Directory User Discovery actions.
Ccm.log	Client Configuration Manager tasks.
Cidm.log	Records changes to the client settings by the Client Install Data Manager (CIDM).
Colleval.log	Logs when collections are created, changed, and deleted by the Collection Evaluator.
Compsumm.log	Records Component Status Summarizer tasks.
Cscnfsvc.log	Records Courier Sender confirmation service tasks.
Dataldr.log	Processes Management Information Format (MIF) files and hardware inventory in the Configuration Manager 2007 database.
Ddm.log	Saves DDR information to the Configuration Manager 2007 database by the Discovery Data Manager.
Despool.log	Records incoming site-to-site communication transfers.
Dismgr.log	Records package creation, compression, delta replication, and information updates.
Hman.log	Records site configuration changes, and publishes site information in Active Directory Domain Services.
Fspmgr.log	Records activities of the fallback status point site system role.
Inboxast.log	Records files that are moved from the management point to the corresponding SMS\INBOXES folder.
Inboxmgr.log	Records file maintenance.
Invproc.log	Records the processing of delta MIF files for the Dataloader component from client inventory files.
Mpcontrol.log	Records the registration of the management point with WINS. Records

	the availability of the management point every 10 minutes.
Mpfdm.log	Management point component that moves client files to the corresponding SMS\INBOXES folder.
MPMSI.log	Management point .msi installation log.
MPSetup.log	Records the management point installation wrapper process.
Netdisc.log	Records Network Discovery actions.
Ntsvrdis.log	Records NT Server Discovery.
Offermgr.log	Records advertisement updates.
Offersum.log	Records summarization of advertisement status messages.
Polycpv.log	Records updates to the client policies to reflect changes to client settings or advertisements.
Replmgr.log	Records the replication of files between the site server components and the Scheduler component.
Rsetup.log	Reporting point setup log.
Schedule.log	Records site-to-site job and package replication.
Sender.log	Records files that are sent to other child and parent sites.
Sinvproc.log	Records client software inventory data processing to the site database in Microsoft SQL Server.
Sitecomp.log	Records maintenance of the installed site components.
Sitectl.log	Records site setting changes to the Sitectl.ct0 file.
Sitestat.log	Records the monitoring process of all site systems.
Smsdbmon.log	Records database changes.
Smsexec.log	Records processing of all site server component threads.
Smsprov.log	Records WMI provider access to the site database.
Smsfspsetup.log	Records messages generated by the installation of a fallback status point.
SMSReportingInstall.log	Records the Reporting Point installation. This component starts the installation tasks and processes configuration changes.
Srvacct.log	Records the maintenance of accounts when the site uses standard security.
Statmgr.log	Writes all status messages to the database.
Swmproc.log	Processes metering files and maintains settings.

The Admin UI log files are located in <InstallationPath>\AdminUI\. The following table lists and describes the Admin UI log files.

**Log File Name**

**Description**

RepairWizard.log	Records errors, warnings, and information about the process of running the Repair Wizard.
ResourceExplorer.log	Records errors, warnings, and information about running the Resource Explorer.
SMSAdminUI.log	Records the local Configuration Manager 2007 console tasks when you connect to Configuration Manager 2007 sites.

## Management Point Log Files

If management points are installed in the site hierarchy, management point log files are stored in the SMS\_CCM\Logs folder on the management point computer. The following table lists and describes the management point log files.

Log File Name	Description
MP_Ddr.log	Records the conversion of XML.ddr records from clients, and copies them to the site server.
MP_GetAuth.log	Records the status of the site management points.
MP_GetPolicy.log	Records policy information.
MP_Hinv.log	Converts XML hardware inventory records from clients and copies the files to the site server.
MP_Location.log	Records location manager tasks.
MP_Policy.log	Records policy communication.
MP_Relay.log	Copies files that are collected from the client.
MP_Retry.log	Records the hardware inventory retry processes.
MP_Sinv.log	Converts XML software inventory records from clients and copies them to the site server.
MP_Status.log	Converts XML.svf status message files from clients and copies them to the site server.

## Fallback Status Point Log Files

If fallback status points are installed in the site hierarchy, fallback status point log files are stored in the SMS\_CCM\Logs folder on the fallback status point computer. The following table lists and describes the fallback status point log files.

Log File Name	Description
fspmsi.log	Records messages generated by the installation of a fallback status point.

fspisapi.log	Records activities of the fallback status point site system role.
--------------	-------------------------------------------------------------------

## Mobile Device Management Log Files

If mobile device management is enabled in the site hierarchy, mobile device management point log files are generally stored in the <ConfigMgrInstallationPath>\Logs folder on the mobile device management point computer. The following table lists and describes the mobile device management point log files.

### Mobile Device Management Point Logs

Log File Name	Description
DmClientHealth.log	Records the GUIDs of all the mobile device clients that are communicating with the Device Management Point.
DmClientRegistration.log	Records registration requests from and responses to the mobile device client in Native mode.
DmpDatastore.log	Records all the site database connections and queries made by the Device Management Point.
DmpDiscovery.log	Records all the discovery data from the mobile device clients on the Device Management Point.
DmpFileCollection.log	Records mobile device file collection data from mobile device clients on the Device Management Point.
DmpHardware.log	Records hardware inventory data from mobile device clients on the Device Management Point.
DmpIsapi.log	Records mobile device communication data from device clients on the Device Management Point.
dmpMSI.log	Records the Windows Installer data for Device Management Point setup.
DMPSetup.log	Records the mobile device management setup process.
DmpSoftware.log	Records mobile device software distribution data from mobile device clients on the Device Management Point.
DmpStatus.log	Records mobile device status messages data from mobile device clients on the Device Management Point.
FspIsapi.log	Records Fallback Status Point communication data from mobile device clients and client computers on the Fallback Status Point.

### Mobile Device Management Client Logs

For the locations of log files on managed mobile devices and on computers that are used to deploy the mobile device client, see [How to Configure Logging for Windows Mobile and](#)

[Windows CE Devices](#). The following table lists and describes the mobile device management client log files.

Log File Name	Description
DmCertEnroll.log	Records certificate enrollment data on mobile device clients.
DMCertResp.htm (in \Temp)	Records HTML response from the certificate server when the mobile device Enroller program requests a client authentication certificate on mobile device clients.
DmClientSetup.log	Records client setup data on mobile device clients.
DmClientXfer.log	Records client transfer data for Windows Mobile Device Center and ActiveSync deployments.
DmCommonInstaller.log	Records client transfer file installation for setting up mobile device client transfer files on client computers.
DmInstaller.log	Records whether DMInstaller correctly calls DmClientSetup, and whether DmClientSetup exits with success or failure on mobile device clients.
DmInvExtension.log	Records Inventory Extension file installation for setting up Inventory Extension files on client computers.
DmSvc.log	Records mobile device management service data on mobile device clients.

## Operating System Deployment Log Files

The following table lists and describes the operating system deployment log files.

Log File Name	Description
CCMSSetup.log	Provides information about client-based operating system actions.
CreateTSMedia.log	Provides information about task sequence media when it is created. This log is generated on the computer running the Configuration Manager 2007 administrator console.  Log file location:  <ConfigMgrInstallationPath>\AdminUI\log
Dism.log	Provides information about drivers installed during operating system deployment.  Configuration Manager 2007 SP2 installs drivers by using the

	<p>Deployment Image Servicing and Management (DISM) tool in Windows Automated Installation Kit (AIK) 2.0.</p> <p>Log file location:</p> <p><i>%Temp%\SMSTSLOG\Dism.log</i></p>
DriverCatalog.log	Provides information about device drivers that have been imported into the driver catalog.
MP_ClientIDManager.log	Provides information about the Configuration Manager 2007 management point when it responds to Configuration Manager 2007 client ID requests from boot media or Pre-Boot Execution Environment (PXE). This log is generated on the Configuration Manager 2007 management point.
MP_DriverManager.log	Provides information about the Configuration Manager 2007 management point when it responds to a request from the <b>Auto Apply Driver</b> task sequence action. This log is generated on the Configuration Manager 2007 management point.
MP_Location.log	Provides information about the Configuration Manager 2007 management point when it responds to request state store or release state store requests from the state migration point. This log is generated on the Configuration Manager 2007 management point.
PkgMgr.log	<p>Provides information about drivers installed during operating system deployment.</p> <p>Configuration Manager 2007 with SP1 installs drivers by using the Package Manager tool.</p> <p>Log file location:</p> <p><i>%Temp%\SMSTSLOG\Pkgmgr.log</i></p>
Pxecontrol.log	Provides information about the PXE Control Manager.
PXEMsi.log	Provides information about the PXE service point and is generated when the PXE service point site server has been created.
PXESetup.log	Provides information about the PXE service point and is generated when the PXE service point site server has been created.
Setupact.log	Provide information about Windows Sysprep and setup logs.
Setupapi.log	
Setuperr.log	
SmpIsapi.log	Provides information about the state migration point Configuration Manager 2007 client request responses.
Smpmgr.log	Provides information about the results of state migration point health

	checks and configuration changes.
SmpMSI.log	Provides information about the state migration point and is generated when the state migration point site server has been created.
Smsprov.log	Provides information about the SMS provider.
Smspxe.log	Provides information about the Configuration Manager 2007 PXE service point.
SMSSMPSetup.log	Provides information about the state migration point and is generated when the state migration point site server has been created.
Smsts.log	<p>General location for all operating system deployment and task sequence log events.</p> <p>Log file location:</p> <ul style="list-style-type: none"> <li>• If task sequence completes when running in the full operating system with a Configuration Manager 2007 client installed on the computer: <i>&lt;CCM Install Dir&gt;\Logs</i></li> <li>• If task sequence completes when running in the full operating system with no Configuration Manager 2007 client installed on the computer: <i>%Temp%\SMSTSLOG</i></li> <li>• If task sequence completes when running in Windows PE: <i>&lt;largest fixed partition&gt;\SMSTSLOG</i></li> </ul> <p><b>Note</b></p> <p><i>&lt;CCM Install Dir&gt;</i> is <i>%Windir%\System32\Ccm\Logs</i> for most Configuration Manager 2007 clients and is <i>&lt;Configuration Manager 2007 installation drive&gt;\SMS_CCM</i> for the Configuration Manager 2007 site server. For 64-bit operating systems, it is <i>%Windir%\SysWOW64\Ccm\Logs</i>.</p>
TaskSequenceProvider.log	Provides information about task sequences when they are imported, exported, or edited.
USMT Log loadstate.log	Provides information about the User State Migration Tool (USMT) regarding the restore of user state data.
USMT Log scanstate.log	Provides information about the USMT regarding the capture of user state data.

## Network Access Protection Log Files

By default, client log files related to Network Access Protection are found in %Windir%\CCM\Logs. For client computers that are also management points, the log files are found in %ProgramFiles%\SMS\_CCM\Logs.

The following table lists and describes the Network Access Protection log files.

Log File Name	Description
Ccmcca.log	Logs the processing of compliance evaluation based on Configuration Manager NAP policy processing and contains the processing of remediation for each software update required for compliance.
CIAgent.log	Tracks the process of remediation and compliance. However, the software updates log file, Updateshandler.log, provides more informative details about installing the software updates required for compliance.
locationservices.log	Used by other Configuration Manager features (for example, information about the client's assigned site), but also contains information specific to Network Access Protection when the client is in remediation. It records the names of the required remediation servers (management point, software update point, and distribution points that host content required for compliance), which are also sent in the client statement of health.
SDMAgent.log	Shared with the Configuration Manager feature desired configuration management and contains the tracking process of remediation and compliance. However, the software updates log file, Updateshandler.log, provides more informative details about installing the software updates required for compliance.
SMSSha.log	<p>The main log file for the Configuration Manager Network Access Protection client and contains a merged statement of health information from the two Configuration Manager components: location services (LS) and the configuration compliance agent (CCA).</p> <p>This log file also contains information about the interactions between the Configuration Manager System Health Agent and the operating system NAP agent, and also between the Configuration Manager System Health Agent and both the configuration compliance agent and the location services. It provides information about whether the NAP agent successfully initialized, the statement of health data, and the statement of health response.</p>

The System Health Validator point log files are located in %systemdrive%\SMSSHV\SMS\_SHV\Logs, and they are listed and described in the following table.



Log File Name	Description
Ccmperf.log	Contains information about the initialization of the System Health Validator point performance counters.
SmsSHV.log	The main log file for the System Health Validator point; logs the basic operations of the System Health Validator service, such as the initialization progress.
SmsSHVADCacheClient.log	Contains information about retrieving Configuration Manager health state references from Active Directory Domain Services.
SmsSHVCacheStore.log	Contains information about the cache store used to hold the Configuration Manager NAP health state references retrieved from Active Directory Domain Services, such as reading from the store and purging entries from the local cache store file. The cache store is not configurable.
SmsSHVRegistrySettings.log	Records any dynamic changes to the System Health Validator component configuration while the service is running.
SmsSHVQuarValidator.log	Records client statement of health information and processing operations. To obtain full information, change the registry key LogLevel from 1 to 0 in the following location:  HKLM\SOFTWARE\Microsoft\SMSSHV\Logging\@GLOBAL

Setup information for the System Health Validator point can be found in a setup log file, described in the following table, on the computer running the Network Policy Server.

Log File Name	Description
<ConfigMgrInstallationPath>\Logs\SMSSHVSetup.log	Records the success or failure (with failure reason) of installing the System Health Validator point.

### Desired Configuration Management Log Files

By default, the Configuration Manager 2007 client computer log files are found in %Windir%\System32\CCM\Logs or in %Windir%\SysWOW64\CCM\Logs. For client computers that are also management points, the client log files are located in the SMS\_CCM\Logs folder. The following table lists and describes these log files.

Log File Name	Description
---------------	-------------

ciagent.log	Provides information about downloading, storing, and accessing assigned configuration baselines.
dcmagent.log	Provides high-level information about the evaluation of assigned configuration baselines and desired configuration management processes.
discovery.log	Provides detailed information about the Service Modeling Language (SML) processes.
sdmagent.log	Provides information about downloading, storing, and accessing configuration item content.
sdmdiscagent.log	Provides high-level information about the evaluation process for the objects and settings configured in the referenced configuration items.

## Wake On LAN Log Files

The Configuration Manager 2007 site server log files related to Wake On LAN are located in the folder *<ConfigMgrInstallationPath>\Logs* on the site server. There are no client-side log files for Wake On LAN. The following table lists and describes the Wake On LAN log files.

Log File Name	Description
Wolmgr.log	Contains information about wake-up procedures such as when to wake up advertisements or deployments that are configured for Wake On LAN.
WolCmgr.log	Contains information about which clients need to be sent wake-up packets, the number of wake-up packets sent, and the number of wake-up packets retried.

## Software Update Point Log Files

By default, the Configuration Manager 2007 site system log files are found in *<ConfigMgrInstallationPath>\Logs*. The following table lists and describes the software updates site system log files.

Log File Name	Description
ciamgr.log	Provides information about the addition, deletion, and modification of software update configuration items.
distmgr.log	Provides information about the replication of software update deployment packages.
objreplmgr.log	Provides information about the replication of software updates notification files from a parent to child sites.
PatchDownloader.log	Provides information about the process for downloading software updates from the update source specified in the software updates metadata to the

	download destination on the site server.
	<b>Note</b>
	On 64-bit operating systems and on 32-bit operating systems with no Configuration Manager 2007 installed, PatchDownloader.log is created in the server logs directory. On 32-bit operating systems, if the Configuration Manager 2007 client is installed, PatchDownloader.log is created in the client logs directory.
replmgr.log	Provides information about the process for replicating files between sites.
smsdbmon.log	Provides information about when software update configuration items are inserted, updated, or deleted from the site server database and creates notification files for software updates components.
SUPSetup	Provides information about the software update point installation. When the software update point installation completes, <b>Installation was successful</b> is written to this log file.
WCM.log	Provides information about the software update point configuration and connecting to the Windows Server Update Services (WSUS) server for subscribed update categories, classifications, and languages.
WSUSCtrl.log	Provides information about the configuration, database connectivity, and health of the WSUS server for the site.
wsyncmgr.log	Provides information about the software updates synchronization process.

## WSUS Server Log Files

By default, the log files for WSUS running on the software update point site system role are found in %ProgramFiles%\Update Services\LogFiles. The following table lists and describes the WSUS server log files.

Log File Name	Description
Change.log	Provides information about the WSUS server database information that has changed.
SoftwareDistribution.log	Provides information about the software updates that are synchronized from the configured update source to the WSUS server database.

## Software Updates Client Computer Log Files

By default, the Configuration Manager 2007 client computer log files are found in %Windir%\CCM\Logs. For client computers that are also management points, the log files are

found in %ProgramFiles%\SMS\_CCM\Logs. The following table lists and describes the software updates client computer log files.

Log File Name	Description
CIAgent.log	Provides information about processing configuration items, including software updates.
LocationServices.log	Provides information about the location of the WSUS server when a scan is initiated on the client.
PatchDownloader.log	Provides information about the process for downloading software updates from the update source to the download destination on the site server.  This log is only on the client computer configured as the synchronization host for the Inventory Tool for Microsoft Updates.
PolicyAgent.log	Provides information about the process for downloading, compiling, and deleting policies on client computers.
PolicyEvaluator	Provides information about the process for evaluating policies on client computers, including policies from software updates.
RebootCoordinator.log	Provides information about the process for coordinating system restarts on client computers after software update installations.
ScanAgent.log	Provides information about the scan requests for software updates, what tool is requested for the scan, the WSUS location, and so on.
ScanWrapper	Provides information about the prerequisite checks and the scan process initialization for the Inventory Tool for Microsoft Updates on Systems Management Server (SMS) 2003 clients.
SdmAgent.log	Provides information about the process for verifying and decompressing packages that contain configuration item information for software updates.
ServiceWindowManager.log	Provides information about the process for evaluating configured maintenance windows.
smscliUI.log	Provides information about the Configuration Manager Control Panel user interactions, such as initiating a Software Updates Scan Cycle from the <b>Configuration Manager Properties</b> dialog box, opening the Program Download Monitor, and so on.
SmsWusHandler	Provides information about the scan process for the Inventory Tool for Microsoft Updates on SMS 2003 client computers.
StateMessage.log	Provides information about when software updates state messages are created and sent to the management point.
UpdatesDeployment.log	Provides information about the deployment on the client, including software update activation, evaluation, and enforcement. Verbose

	logging shows additional information about the interaction with the client user interface.
UpdatesHandler.log	Provides information about software update compliance scanning and about the download and installation of software updates on the client.
UpdatesStore.log	Provides information about the compliance status for the software updates that were assessed during the compliance scan cycle.
WUAHandler.log	Provides information about when the Windows Update Agent on the client searches for software updates.
WUSSyncXML.log	Provides information about the Inventory Tool for the Microsoft Updates synchronization process.  This log is only on the client computer configured as the synchronization host for the Inventory Tool for Microsoft Updates.

## Windows Update Agent Log File

By default, the Windows Update Agent log file is found on the Configuration Manager Client computer in %Windir%. The following table provides the log file name and description.

Log File Name	Description
WindowsUpdate.log	Provides information about when the Windows Update Agent connects to the WSUS server and retrieves the software updates for compliance assessment and whether there are updates to the agent components.

## Out of Band Management Log Files

Applies only to Configuration Manager 2007 SP1 and later.

These log files are found in the following locations:

- On the out of band service point site system server.
- On any computer that runs the out of band management console from the Configuration Manager console.
- On computers that are running the client for Configuration Manager 2007 SP1 or later and that are managed out of band.

The following sections lists and describes the log files related to out of band management in Configuration Manager 2007 SP1 and later.

## Out of Band Service Point Log Files

The out of band service point log files listed in the following table are located in the folder <ConfigMgrInstallationPath>\Logs on the site system server selected to host the out of band service point role.

Log File Name	More Information
AMTSPSetup.log	Shows the success or failure (with failure reason) of installing the out of band service point.
Amtopmgr.log	Shows the activities of the out of band service point relating to discovery of management controllers, provisioning, and power control commands.
Amtproxmgr.log	<p>Shows the activities of the site server relating to provisioning, which include the following:</p> <ul style="list-style-type: none"><li>• Publishing provisioned computers to Active Directory Domain Services.</li><li>• Registering the service principal name of provisioned computers in Active Directory Domain Services.</li><li>• Requesting the Web server certificate from the issuing certification authority.</li></ul> <p>Shows the activities of sending instruction files to the out of band service point, which include the following:</p> <ul style="list-style-type: none"><li>• Discovery of management controllers.</li><li>• Provisioning.</li><li>• Power control commands.</li></ul> <p>Shows the activities related to out of band management site replication.</p>

## Out of Band Management Console Log Files

The out of band management console log file listed in the following table is located in the folder <ConfigMgrInstallationPath>\AdminUI\AdminUILog on any computer that runs the out of band management console from the Configuration Manager console.

Log File Name	More Information
Oobconsole.log	Shows activities related to running the out of band management console.

## Out of Band Management Client Computer Log Files

The out of band management client log file listed in the following table is located in the folder *%Windir%\System32\CCM\Logs* on workstation computers that are running the client for Configuration Manager 2007 SP1 or later and that are managed out of band.

Log File Name	More Information
Oobmgmt.log	Shows out of band management activities performed on workstation computers, including the provisioning state of the management controller.

## Power Management Log Files

Applies only to Configuration Manager 2007 R3.

The log files listed in the following table are located in the folder *%windir%\System32\CCM\Logs* on 32-bit workstation computers and in the folder *%windir%\SysWOW64\CCM\Logs* on 64-bit workstation computers that have the Power Management Client Agent enabled.

Log File Name	More Information
pwrmgmt.log	Shows power management activities performed on the client computer that include monitoring and enforcement activities performed by the Power Management Client Agent. On computers that are running Windows XP, this log also records power settings to the computer.
PwrProvider.log	Shows the activities of the power management provider (PWRInvProvider) hosted in the Windows Management Instrumentation (WMI) service. On all supported versions of Windows, the provider enumerates the current settings on computers during hardware inventory. On computers that are running Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, the provider is also responsible for applying power plan settings to the computer.

## 10. SCCM Roles applicable for Central, Primary & Secondary Sites

**What is Primary site :**

- It has its own site database
- Primary site can Managed directly through Configuration Manager console installed on site server

- Only a primary site can be a parent
- First site installed must be a primary site

### **What is Secondary site:**

- A secondary site, is a specific site type with limitations compared to a primary site and no demand for a SQL server.
- Secondary site must be a child site, and report to a primary parent site
- No database of its own, data stored in parent's database
- It has No console, managed from parent site
- It doesn't require Configuration Manager server license
- Clients cannot be assigned

### **What is Parent site:**

- It Must be a primary site
- This Can also be a child site
- Site database contains information from child sites

### **What is Child Site:**

- A child site, is simply referring to the site location in the hierarchy. If you have a parent site, then by default you will become a child site.
- Primary site can be child site; secondary site must be child site.
- Child site Can also be parent site, but only if it is a primary site.
- Only one parent (Primary can change parent; secondary cannot)

### **What is Central site:**

- Site at the top of a hierarchy
- Contains information from all sites in hierarchy
- Stand-alone (without parent or child) still considered "central site"



### **Central administration site:**

*The central administration site coordinates intersite data replication across the hierarchy by using Configuration Manager database replication.*

it has the following differences from a central site in Configuration Manager 2007:

- Does not process client data.
- Does not accept client assignments.
- Does not support all site system roles.
- Participates in database replication

### **Primary site :**

*Manages clients in well-connected networks.*

Primary sites in Configuration Manager 2012 have the following differences from primary sites in Configuration Manager 2007:

- Additional primary sites allow the hierarchy to support more clients.
- Cannot be tiered below other primary sites.
- No longer used as a boundary for client agent settings or security.
- Participates in database replication.

### **Secondary site :**

*Controls content distribution for clients in remote locations across links that have limited network bandwidth*

Secondary sites in Configuration Manager 2012 have the following differences from secondary sites in Configuration Manager 2007:

- SQL Server is required and SQL Server Express will be installed during site installation if required.
- A proxy management point and distribution point are automatically deployed during the site installation.
- Secondary sites can be tiered to support content distribution to remote locations.
- Participates in database replication.

## **11. SCCM 2007 Components Threads Use Site-Site Replication**

SCCM 2007 Components are critical to perform its activities and if any of the component is stopped(some components start when they have work to do like Discovery methods are only start

if discovery runs) ,you may see issues respective to that Component(Ex: Distribution Manager stopped,nohing process about packages).

Some of the components that involved in Site-Site Replication and ensure **these components are running** before you Dig more into Site-site replication issues.

I do check these components if I see any replication issues on my Child sites and follow the troubleshooting Steps.

<b>Component</b>	<b>Description</b>
<b>OFFER MANAGER</b>	Offer Manager replicates advertisements to child sites. C:\SMS_\<sitecode>\inboxes\replmgr.box\outbound\<Priority>  Replication Manager then creates a mini-job in SMS\inbox\<sitecode>\replmgr\<sitecode>\<Priority>\<ObjectID>.RPT. Replmgr creates a sequentially numbered job file.
<b>DISTRIBUTION MANAGER</b>	Distribution Manager manages the replication of package definition files from parent to child sites. For package definition file, it creates a package (.pkg) file in SMS_\<sitecode>\Inboxes\Replmgr.box\Outbound\Normal\<ObjectID>.RPT. Replmgr creates a job in SMS\Inboxes\Schedule.box\ by using a sequentially numbered job file.  Distribution Manager also manages package status and creates status messages.
<b>COLLECTION EVALUATOR</b>	Collection Evaluator on child primary sites inputs collection definition or deleted notifications to each child site processes – replmgr, scheduler, sender. On secondary sites, collection data on secondary sites are stored in a *.clf file.
<b>INVENTORY DATALOADER</b>	Hardware Inventory .mif files are forwarded from child sites to parent site through replication processes – replmgr, scheduler, and sender. Sender sends inventory data in its site database to .mif files and this data is replicated to parent site.
<b>DESPOOLER</b>	Despooler processes replication instruction files from the child sites. Despooler reads the file instruction files in order to replicate the files to the parent site.
<b>DISCOVERY DATA MANAGER</b>	All child sites forward discovery data to their parents. Secondary sites send all DDRs to their parent for processing. The parent site replicates a *.pdr file back down to the secondary sites. The secondary site replicates the .pdr to its parent site.
<b>INVENTORY PROCESSOR</b>	All child sites forward inventory data to their parents. Sender sends their parent site by using standard replication processes.
<b>HIERARCHY MANAGER</b>	Hierarchy Manager replicates the heartbeat site control files to the parent site.

	<p>that each parent site's database contains the up-to-date co</p> <p>Site Control files replicated to child sites use normal repli child site.. However, Despooler at the child site bypasses new site control file directly to Hierarchy Manager.</p> <p>Secondary site installation initiated at parent site – Hierar send a Setup package to the secondary site server. When Manager starts a thread to compress the installation files \Inboxes\Hman.box\Sitepkg.p*folder on the parent server (Replication Manager) to replicate this site installation pa replicated back to the back to the parent site. Secondary s</p>
<p><b>SOFTWARE INVENTORY PROCESSOR</b></p>	<p>The Software Inventory Processor (SinvProc) reads inven (full report) and SID (delta report) files from the\inboxes\ \inboxes\sinv.box inbox. It parses the file, and updates the information.</p> <p>The reports may also contain collected files, in which cas \inboxes\sinv.box\FileCol\. If running on a child site, the binary files and replicated to the parent. Secondary sites r site where the data is added to the site database. This inve child to parent sites.</p>
<p><b>SITE CONTROL MANAGER</b></p>	<p>Site Control Manager replicates site control files between are replicated to child sites as .CT1 files. After child sites child site replicates a .CT2 file back to its parent site.</p>
<p><b>OBJECT REPLICATION MANAGER</b></p>	<p>Object Replication Manager (ORM) provides the infrastr replication of various kinds of SMS objects.</p> <ul style="list-style-type: none"> <li>· ORM is responsible for creation of replication objects o register various object types for replication. After it is reg object on the parent site is monitored. If there are changes (depending on object type) get dropped into the \inboxes\ thread processes these objects and serializes them to files makes a call to replication manager to replicate these cha Replication Manager uses transaction based replication (t</li> <li>· On the child site, when replication manager drops inco \inboxes\objmgr\ folder, ORM processes these files and c insert, delete, or update the appropriate object on the chil</li> </ul> <p>The different types of objects that Object Replication Ma Manager 2007 are the following:</p>

	<ul style="list-style-type: none"> <li>· Configuration Items</li> <li>· Update Sources</li> <li>· Software Update Categories</li> <li>· SDM Packages</li> <li>· EULAs (End User License Agreements)</li> <li>· Device Setting Items</li> </ul>
<b>CI ASSIGNMENT MANAGER</b>	<p>CI Assignment Manager runs on every primary site in the hierarchy and replicating them to other sites. It also manages changes to CI Assignment, addition and deletion of CIs and changes to CI Assignment.</p> <p>When a new CI Assignment is added, updated or deleted, it sends a file to all its primary child sites via a database trigger. This causes it to create a new replication file and send it down to all its primary child sites. When the child site receives this file it updates the database of the site accordingly.</p> <p>For more information about Configuration Items see About Configuration Items: <a href="http://msdn.microsoft.com/en-us/lib">http://msdn.microsoft.com/en-us/lib</a></p>
<b>SMS_OFFER_STATUS_SUMMARIZER</b>	Monitors for and gathers offer status data from advertisements. Summarized status is replicated up the site hierarchy to all parent sites.
<b>SMS_SITE_SYSTEM_STATUS_SUMMARIZER</b>	Monitors and gathers data on disk space, network access, and server roles. Summarized status is replicated up the site hierarchy.
<b>SMS_COMPONENT_STATUS_SUMMARIZER</b>	Monitors and gathers component status messages and availability. Summarized status is replicated up the site hierarchy.
<b>SMS_OFFER_STATUS_SUMMARIZER</b>	Monitors for and gathers offer status data from advertisements. Summarized status is replicated up the site hierarchy.
<b>SMS_STATUS_MANAGER</b>	Monitors for status messages and applies all enabled status changes. This includes replication of messages up the site hierarchy.

