Organisational requirements gathering

- Is there a requirement to encrypt traffic between clients and server, keeping in mind this will add considerable complexity to the deployment? (eg status messages, policy, content)
- Is there a requirement to encrypt server to server traffic?
- Are their many roaming clients or are they fairly static?
- Is there a requirement to run the SCCM reporting website from a dedicated virtual website on a separate dedicated server? (Reduce attack surface)
- What are the Disaster Recovery (fault tolerance) requirements? (Acceptable downtime for each SCCM feature?)
- Any internet-based machines or home users etc?
- Which SCCM features are required? Can these be prioritised?

Feature	Description	Required?	Priority
Internet-based client management	Internet-based client management allows you to manage Configuration Manager 2007 clients when they are not connected to your company network but have a standard Internet connection. For more information about Internet-based client management in Configuration Manager 2007, see Overview of Internet-Based Client Management.		
Inventory	Hardware inventory provides system information (such as available disk space, processor type, and operating system) about each computer. Software inventory provides information such as file types and versions present on client computers. For more information about inventory, see Overview of Inventory.		
Reporting	Reporting helps you to gather, organize, and present information about client computers and devices, site status, and other Configuration Manager operations in your organization. For more information about reporting, see Reporting in Configuration Manager.		
SQL Reporting Services	Applies only to Configuration Manager 2007 R2 or later. SQL Reporting Services provides a set of tools and resources that help you use the advanced reporting capabilities of SQL		

	Reporting Services from the Configuration Manager console. For more information about SQL Reporting Services, see Overview of SQL Reporting Services.		
Software distribution	Software distribution allows you to create packages and programs to install software and run scripts on clients. For more information about software distribution, see Software Distribution Overview.		
Software updates	Software updates provide a set of tools and resources that can help manage the complex task of tracking and applying software updates to client computers in an enterprise. For more information about software updates in Configuration Manager 2007, see Overview of Software Updates.		
Software metering	Software metering allows you to collect detailed information about the programs that you choose to monitor. This includes program and usage information, such as user name, file description, start time, and end time. For more information about software metering, see Software Metering in Configuration Manager.		
Device management	Device management enables mobile device discovery and management for mobile devices running Windows Mobile software for Pocket PC and Smartphone platforms and Windows CE. For more information about device management in Configuration Manager 2007, see Overview of Mobile Device Management.		
Operating system deployment	Operating system deployment enables you to create images that can be deployed to computers using bootable media such as CD set or DVD. The image, in a WIM format file, contains the desired version of a Windows operating system and can also include any line-of-business applications that need to be installed on the computer. For more information about operating system deployment in Configuration Manager 2007, see Overview of Operating System Deployment.		
Asset Intelligence	Asset Intelligence enhances the inventory capabilities of Configuration Manager to help manage software in use and software license management in the enterprise. For more information about Asset Intelligence, see Overview of Asset Intelligence.		
Desired configuration management	Desired configuration management allows you to assess the compliance of computers with regard to a number of configurations, such as whether the correct Windows operating system versions are installed and configured		

	appropriately, whether all required applications are installed and configured correctly, whether optional applications are configured appropriately, and whether prohibited applications are installed. Additionally, you can check for compliance with software updates and security settings. For more information about desired configuration management in Configuration Manager 2007, see Overview of Desired Configuration Management.		
Network Access Protection	Network Access Protection (NAP) works with health policies and network policies on a Network Policy Server, allowing you to select which software updates will be evaluated for compliance. The policies on the Network Policy Server then determine whether clients are granted full or limited network access and whether non-compliant clients are made compliant (remediated). For more information about Network Access Protection in Configuration Manager 2007, see Overview of Network Access Protection.		
Wake On LAN	Wake On LAN can send wake-up transmissions prior to the configured deadline for a software update deployment or at the configured schedule of a mandatory advertisement (which can be for software distribution or a task sequence). For more information about Wake On LAN in Configuration Manager 2007, see Overview of Wake On LAN.		
Remote tools	Remote tools allow you to remotely access and operate client computers that have the remote tools client agent components installed. For more information about remote tools in Configuration Manager 2007, see Overview of Remote Tools.		
Out of band management	Applies only to Configuration Manager 2007 SP1 and later. Out of band management allows you to manage desktop computers independently from the Configuration Manager client or the computer operating system. It requires computers that have the Intel vPro chip set and a version of Intel Active Management Technology (Intel AMT) that is supported by Configuration Manager. For more information about out of band management in Configuration Manager 2007 SP1, see Overview of Out of Band Management.		

- How many applications (roughly) do we want to automatically distribute?
- Do power management policies need to be defined and implemented as part of the scope?

- Is there a current test / pilot environment? Is there a requirement to build this in test and well as production?
- Who will need access to the SCCM reports? (Software inventory, hardware inventory etc)
- At this stage are there any requirements for customized reports that are not provided by SCCM out of the box?
- What are the documentation deliverables? (As-built documents, etc)
- Can we identify a list of clients for a production pilot? Who would handle communication with pilot users?
- What is the requirement for targeting specific groups of machines? Do we want to target machine by location, business unit, company, type, OS, etc and is this reflected in the structure of Active Directory OUs or groups?
- Can we obtain one of each type of hardware model?
- Is there a requirement for maintenance windows for collections?
- Are all software packages required across all sites?
- Have Microsoft licenses only been obtained via the volume licensing (EA) programs or have they also been obtained via retail, Original Equipment Manufacturer (OEM) or other software licensee sales channels?
- Have all Microsoft licenses that have been acquired as part of a merger or takeover been transferred onto the one EA?
- Is there a requirement to use SQL Reporting Services instead of the SCCM reporting method? (Subscription to reports via email, export into a variety of popular formats)
- Is there a requirement for mobile device management? (eg Windows Mobile devices)
- Is there a requirement for Network Access Protection?
- Will the OSD process require backup of data via User State Migration Tool (USMT)?
- Is there a requirement for Wake-on-LAN (WOL) to allow patching and deployments automation during non-business hours?
- Do we want to try and integrate into the current CMDB or start fresh?
- What is the primary reason for implementing SCCM?

- What is the expected timeline for moving to SCCM? Milestones?
- What are the expectations for growth or contraction? Are there significant planned changes in the size or usage patterns of applications or locations?
- Should any particular groups of clients be excluded from our reporting?
- Any regulatory requirements that require total separation of an environment from other environments?
- How should software be deployed? Should it be silent in the background? Should it be silent but give a user notification? Should the user have to go to Add / Remove programs and select to install it?

- From first contact with the Help Desk, what is the organisation's expected software deployment time?
- Is there any requirement for a multilingual environment?
- What is the preference for OS deployment? (PXE network boot, USB stick, CD/DVD boot)
- How often should hardware and software inventories be run?
- Is there a requirement for Out of Band Management (vPro technology)?
- Is server refresh in scope of the project?
- SLAs?
- What is the expectation for Operating System deployment? (Zero touch, lite touch etc)
- What Operating Systems will be deployed? (Workstation and server Oss, 32bit / 64bit)
- Is there a requirement for Application Virtualization (App-V)?
- Are there existing servers that SCCM could utilize (eg DC, F&P servers) on sites with 10+ computers on them?

- Is there a requirement for SCCM to handle firmware and driver updates? (eg Dell and HP)
- What is the current process for deploying an SOE to workstation and servers? Is there an existing WIM file and what version? Ghost file? Reference computer?
- Process for getting quotes on server hardware?
- What training would you like to see as part of the SCCM implementation and who is the audience?
- At what time during the week would you expect most computers to be online?
- What is the typical usage trend? Monday to Friday 9-5? 24/7?
- What operating system versions (including service pack) are potentially in the environment?
- Should I be running this exercise with anyone else?
- Is there a requirement for a self service portal?
- Are both servers and workstation class machines to be targeted?

Technical requirements gathering

- Are there any internet-based clients to be managed? (eg home machines) Will there be any in the foreseeable future?
- What operating system versions (including service pack) are potentially in the environment?
- Any issue with performing AD schema extensions? (Policy or technical roadblocks)
- Understanding of AD sites and comparison to subnets
- Are all potential client IP addresses covered by AD site subnets?
- Are there any workgroup or DMZ clients to be managed?
- Are there any VPN clients? If so, what connection speeds? (Broadband, dialup). Do they have their own AD site?
- Are there multiple Active Directory forests or domains? What are the trust relationships between them?
- Overview of DNS and WINS (if used) configuration (Most server-initiated actions, such as client push installation and remote control, connect to clients by using the short name of the computer instead of the fully qualified domain name (FQDNA). Configuring the site systems with DNS search suffixes for client computers that are in a different forest is one method to ensure that the short name resolves successfully. To discover a computer resource in another forest by using Active Directory System Discovery, there must be a forest trust between the site server forest and the forest where the computer is located.)
- Firewall configuration – is there a firewall between the potential server locations and potential clients?
- Will the server need to be manually configured with the DNS suffixes of potential clients or is this configured automatically?
- Will the potential clients need to be manually configured with the DNS suffixes of the server or is this configured automatically?
- Can you roughly estimate the size of the source installation files for software that will be automatically deployed?
- Is there an existing stable PKI / Certificate Services infrastructure in place?

- How are the server operating systems deployed? Is it ok to run Windows 2008 R2 64-bit?
- Where will SCCM be administered from? (SCCM server, admin workstation, admin servers?)
- Are we using IPv4 or IPv6 in the environment? Network protocols in use? (TCP/IP, IPv6, NetBEUI, IPX/SPX, AppleTalk, DLC)
- Network diagram if available
- Number of physical sites
- Link speed between sites
- Link speed from data centre to remote sites
- Rough number of clients on each site
- Extranet sites (or any sites that are firewalled off from the regular network), any isolated sites?
- Any known capacity issues? (will we need to throttle SCCM communications?)
- Firewall layout (eg are there firewalls between sites or between data centre and potential clients)
- VPN configuration, if any
- IP address schema (all of the IP subnets in use across the network)
- DMZ or perimeter network layout
- Any IPS systems that may impact the SCCM network discovery process
- Any issue with client installation methods? (Client Push Installation, WSUS Based, Group Policy Installation, Logon Script Installation, Manual Installation)
- Is the Windows software firewall (or any other vendor software firewall) enabled / installed on potential clients?
- How many of the above applications need to be repackaged to allow automatic distribution?
- How many different workstation hardware models are there in the environment that we may potential deploy Operating Systems to?

- What is the expectation for Operating System deployment? (Zero touch, lite touch etc)
- What Operating Systems will be deployed? (Workstation and server OSs)
- What tools are currently used for client remote control? Is the plan to continue using existing tools?
- Is there currently a workstation and server SOE?
- Is there a requirement for traffic throttling across network links?
- Is the existing SQL cluster resourced adequately to support the SCCM database?
- Is there an existing server we can use for Fallback Status Point (FSP)?
- Is there a requirement to manually approve clients that are discovered or is it ok to automatically approve all discovered computers?
- Do all potential clients meet the OS minimum requirement levels (http://technet.microsoft.com/en-us/library/ee344146.aspx) and also have a ADMIN$ share? Remote registry service running?
- Any issue with SCCM installation automatically upgrading client software:
    - Microsoft Background Intelligent Transfer Service (BITS) version 2.5
    - Windows Installer version 3.1.4000.2435
    - Windows Update Agent version 7.0.6000.363
    - Microsoft Core XML Services (MSXML) version 6.0.3883.0
    - Windows Management Instrumentation (WMI) Redistributable Components version 5.2.3790.1830
    - Microsoft Remote Differential Compression (RDC)
- Is there going to be enough space on clients for SCCM temporary installation files and then cache?
- Who should be alerted when there are errors within SCCM?
- Is there a requirement for Application Virtualization (App-V)? – App-V reference card available.
- Are there existing servers that SCCM could utilize (eg DC, F&P servers) on sites with 10+ computers on them?
- How is (Microsoft and other vendors) patch management currently handled? (WSUS?) Any challenges with this? Success rate? Automatic approval? Administrator intervention?

- Is there a requirement for SCCM to handle firmware and driver updates? (eg Dell and HP)
- What is the current process for deploying an SOE to workstation and servers? Is there an existing WIM file and what version? Ghost file? Reference computer?
- Is there currently a driver catalogue for use with OS deployment?
- What would be the maximum number of router hops a client device could potentially be from the SCCM server?
- Does internet access from the SCCM server require authenticated access?
- Number of servers and clients at each location
- Network usage and traffic patterns? (Peak times etc)
- Are there any other systems management products in the environment?
- Server naming conventions?
- Process for getting quotes on server hardware?
- Are Group Policy objects needed to be defined for the MOE?
- Can we apply organisation-wide exclusions to antivirus scanning?
- Where / how to download and store volume licensing products?

Technical prerequisites

The following is a list of technical prerequisites that need to be met before SCCM deployment can begin:

- 'Enterprise Admins' permissions
- 'Schema Admins' permissions
- Ability to perform Schema extension
- Ability to use ADSI edit to add 'System Management' container in AD
- SQL instance (default or named), preferably clustered. Named pipes and TCP/IP network protocol communication is required (configured in SQL Server Configuration Manager under Network Configuration). SQL 2005 SP3+. Sql Server Windows Authentication Mode. If clustered, machine account of the primary site server needs to be in the local administrators group of each of the client nodes. The sysadmin SQL server role need to be granted to the user account running the SCCM setup.
- Admin rights to the SQL server computer
- Permissions to create Active Directory groups
- Permissions to add SRV record to DNS
- Required service accounts:
    - Client push installation account - Account or accounts with local administrator permissions to all potential clients (can be new or existing) – can be local accounts or domain accounts or combination of both
        - This account does not require the right to log on locally
    - Network Access account – service account used to provided clients with access to files on distribution points
        - The password for the network access account is limited to 38 characters or less
        - This account does not require interactive logon rights
    - Site Address Account – will be require if we need to connect to a site in a different forest
    - Domain joining account – account with permissions to join a computer to the domain – used when deploying new operating systems
        - Do not assign this account interactive logon permissions
        - Do not use the Network Access account for this account
    - Proxy account – credentials needed for SCCM to connect to the Internet via a proxy server requiring authenticated access
- Internet access from the SCCM primary server (via proxy is fine)
- Ability to create empty file named no_sms_on_drive.sms at the root folder of any drive that you want to prevent SCCM from installing files on
- Availability of all hardware model types for MOE development