

Lappeenranta University of Technology  
School of Industrial Engineering and Management  
Department of Software Engineering and Information Management

Master's thesis

**Jesse Keränen**

**Centralized IT management using SCCM in a large multinational  
company**

Examiners:           Professor Jari Porras  
                          Associate Professor Kari Heikkinen

Supervisors:        Professor Jari Porras  
                          Kasper Salonen

# TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto

Tuotantotalouden tiedekunta

Tietotekniikan koulutusohjelma

Jesse Keränen

Centralized IT management using SCCM in a large multinational company

Diplomityö

2014

91 sivua, 16 kuvaa, 21 taulukkoa.

Työn tarkastajat: Professori Jari Porras, Apulaisprofessori Kari Heikkinen

Hakusanat: SCCM, ConfigMgr, System Center, Configuration Manager, Laittehallinta

Keywords: SCCM, ConfigMgr, System Center, Configuration Manager, Asset Management

Microsoft System Center Configuration Manager on järjestelmänhallintatyökalu suurten tietokone- ja mobiililaittejoukkojen hallintaan. Se tarjoaa hallituille laitteille käyttöjärjestelmä-, ohjelmisto- ja päivitysjakelua, laite- ja ohjelmistoinventaariota, etähallintaominaisuuksia ja monia muita ominaisuuksia.

Tämä diplomityö keskittyy tutkimaan onko tämä kyseisen tuote sopiva suurelle kansainväliselle organisaatiolle, jolla ei ole mitään aikaisempaa keskitettyä työkalua kaikkien tällaisten laitteiden hallintaan, sekä löytämään alueet, joilla järjestelmää voitaisiin muokata paremmin vastaamaan yrityksen tarpeita.

Työn tulokset osoittivat että järjestelmä on kyseiselle organisaatiolle soveltuva oikein konfiguroituna, sekä jos avain-IT-henkilöstön kesken vallitsee selkeä kommunikointimalli.

## **ABSTRACT**

Lappeenranta University of Technology  
School of Industrial Engineering and Management  
Department of Software Engineering and Information Management

Jesse Keränen

Centralized IT management using SCCM in a large multinational company

Master's Thesis

2014

91 pages, 16 figures, 21 tables.

Examiners: Professor Jari Porras, Associate Professor Kari Heikkinen

Keywords: SCCM, ConfigMgr, System Center, Configuration Manager, Asset Management

Microsoft System Center Configuration Manager is a systems management product for managing large groups of computers and/or mobile devices. It provides operating system deployment, software distribution, patch management, hardware & software inventory, remote control and many other features for the managed clients.

This thesis focuses on researching whether this product is suitable for large, international organization with no previous, centralized solution for managing all such networked devices and detecting areas, where the system can be altered to achieve a more optimal management product from the company's perspective.

The results showed that the system is suitable for such organization if properly configured and clear and transparent line of communication between key IT personnel exists.

## **ACKNOWLEDGEMENTS**

I wish to express my gratitude to the Lappeenranta University of Technology and Sulzer Pumps Finland for the possibility of doing this master's thesis.

I would like to thank my former and current supervisors in Sulzer, Matti Outinen and Kasperi Salonen for initially providing me this research subject and trusting in me to carry out the task in a worthwhile manner. Special thanks to Kasperi for providing me the time, tools and access to work on this thesis and ability to continue on this path in the future.

Last, but not least, I'd like to thank my wonderful fiancée Tanja for endless support and enduring me while I was working on this research, possibly neglecting most of my other non-work related responsibilities.

Lappeenranta, November 7<sup>th</sup>, 2014.

Jesse Keränen

# TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	BACKGROUND.....	1
1.2	GOALS AND LIMITATIONS .....	2
1.3	RESEARCH METHODS .....	4
1.4	STRUCTURE OF THE STUDY .....	4
<b>2</b>	<b>SULZER .....</b>	<b>6</b>
2.1	INFRASTRUCTURE .....	6
2.2	CLIENT MANAGEMENT .....	9
<b>3</b>	<b>INTRODUCTION TO CENTRALIZED ASSET MANAGEMENT .....</b>	<b>11</b>
3.1	ACTIVE DIRECTORY.....	11
3.2	HARDWARE MANAGEMENT .....	13
3.3	SOFTWARE MANAGEMENT .....	13
3.3.1	<i>Software Deployment</i> .....	14
3.3.2	<i>Software &amp; License Inventory</i> .....	14
3.4	OPERATING SYSTEM MANAGEMENT.....	15
3.4.1	<i>OS Deployment</i> .....	15
3.4.2	<i>Configuration &amp; compliance management</i> .....	17
3.4.3	<i>Updates and patching</i> .....	18
<b>4</b>	<b>SYSTEM CENTER CONFIGURATION MANAGER .....</b>	<b>20</b>
4.1	HIERARCHY AND ARCHITECTURE.....	24
4.2	OSD .....	26
4.2.1	<i>Tools used in OSD</i> .....	28
4.2.2	<i>Task Sequences</i> .....	29
4.3	APPLICATION MANAGEMENT.....	30
4.4	COLLECTIONS .....	32
4.5	UPDATE DEPLOYMENT .....	33
4.6	INVENTORY & ASSET INTELLIGENCE .....	34
4.7	COMPLIANCY .....	34
4.8	REPORTING .....	35
4.9	ENDPOINT PROTECTION .....	36

4.10	MOBILE DEVICE MANAGEMENT.....	37
<b>5</b>	<b>ANALYSIS OF CURRENT SCCM IMPLEMENTATION.....</b>	<b>41</b>
5.1	SCCM ARCHITECTURE .....	41
5.2	SUPPORTED OPERATING SYSTEMS .....	44
5.2.1	<i>Windows 7.....</i>	<i>44</i>
5.2.2	<i>Windows Server 2003 &amp; 2003 R2.....</i>	<i>45</i>
5.2.3	<i>Windows Server 2008 &amp; 2008 R2.....</i>	<i>46</i>
5.2.4	<i>Windows Server 2012 .....</i>	<i>47</i>
5.3	SUPPORTED HARDWARE .....	47
5.4	OSD PROCESS .....	49
5.5	APPLICATION MANAGEMENT AND DEPLOYMENT.....	51
5.6	ENDPOINT PROTECTION.....	53
5.7	SERVICE DESK .....	54
5.8	BACKUPS .....	55
<b>6</b>	<b>MICROSOFT SCCM BEST PRACTICES.....</b>	<b>56</b>
6.1	APPLICATION MANAGEMENT .....	56
6.2	CLIENT DEPLOYMENT .....	56
6.3	COLLECTIONS .....	58
6.4	CONTENT MANAGEMENT .....	58
6.5	REPORTING .....	59
6.6	SOFTWARE UPDATES .....	60
<b>7</b>	<b>SURVEY RESULTS &amp; CHANGE RECOMMENDATIONS.....</b>	<b>62</b>
7.1	SCCM AS A CENTRALIZED MANAGEMENT TOOL.....	62
7.2	SCCM RECOMMENDATIONS.....	67
7.2.1	<i>Architecture .....</i>	<i>67</i>
7.2.2	<i>OSD.....</i>	<i>67</i>
7.2.3	<i>Application management .....</i>	<i>70</i>
7.2.4	<i>Update management .....</i>	<i>73</i>
7.2.5	<i>Reporting .....</i>	<i>74</i>
7.2.6	<i>System &amp; Sites.....</i>	<i>76</i>
7.2.7	<i>Miscellaneous .....</i>	<i>78</i>
<b>8</b>	<b>IMPLEMENTED CHANGES.....</b>	<b>81</b>
8.1	OSD .....	81
8.1.1	<i>O_01 Core image.....</i>	<i>81</i>

8.1.2	<i>O_04 Bulk asset creation</i> .....	82
8.1.3	<i>O_06 OSD Method</i> .....	82
8.2	APPLICATION MANAGEMENT .....	82
8.2.1	<i>A_01 Application Catalog</i> .....	83
8.2.2	<i>A_02 Application Catalog</i> .....	83
8.2.3	<i>A_04 Application Catalog</i> .....	84
8.2.4	<i>A_07 Application Deployment</i> .....	84
8.2.5	<i>A_08 Application Updates</i> .....	84
8.3	REPORTING .....	85
8.3.1	<i>R_01 Web-Reports</i> .....	85
8.4	SYSTEM & SITES .....	85
8.4.1	<i>S_03 Collections</i> .....	85
8.4.2	<i>S_06 R2 Upgrade</i> .....	86
8.5	MISCELLANEOUS .....	87
8.5.1	<i>M_02 Security</i> .....	87
8.5.2	<i>M_03 Administration</i> .....	87
<b>9</b>	<b>RESULTS</b> .....	<b>88</b>
<b>10</b>	<b>CONCLUSIONS</b> .....	<b>91</b>
	<b>REFERENCES</b> .....	<b>92</b>
	<b>APPENDICES</b>	

## LIST OF FIGURES

Figure 1. Sulzer Pump's users by OU. ....	8
Figure 2. Sulzer's global IT organization.....	9
Figure 3. AD on Windows Network. ....	12
Figure 4. Sample SCCM architecture. ....	25
Figure 5. Bare-metal OSD overview. ....	27
Figure 6. SCCM High-level architecture in Sulzer.....	42
Figure 7. 3-tier SCCM architecture. ....	43
Figure 8. Desktop Operating System Market Share. ....	44
Figure 9. Computer distribution in Sulzer Pumps. ....	48
Figure 10. Computer distribution by OU.....	49
Figure 11. Asset portal.....	50
Figure 12. SCCM Application Catalog.....	52
Figure 13. SCEP Policies in Sulzer. ....	54
Figure 14. Survey answers from all recipients (averages).....	65
Figure 15. Application Catalog before changes.....	83
Figure 16. Application Catalog after changes. ....	83

## LIST OF TABLES

Table 1. Research sub questions .....	3
Table 2. Research structure.....	5
Table 3. System Center family of products .....	20
Table 4. System Center Configuration Manager version history. ....	22
Table 5. System Center 2012 Licenses .....	23
Table 6. System Center Client licenses. ....	24
Table 7. OSD scenarios in SCCM .....	26
Table 8. Basic task sequence steps. ....	29
Table 9. Six basic programs in a .msi package .....	31
Table 10. Mobile device management options in SCCM 2012.....	38
Table 11. Minimum hardware requirements for 64-bit Windows 7.....	45
Table 12. Minimum hardware requirements for Windows Server 2008 & 2008 R2 .....	46
Table 13. Minimum hardware requirements for Windows Server 2012. ....	47
Table 14. Survey Respondents.....	63
Table 15. Support numbers for respondents. ....	63
Table 16. Recommendations for OSD. ....	68
Table 17. Recommendations for Application management.....	71
Table 18. Recommendations for update management.....	74
Table 19. Recommendations for SCCM Reporting.....	74
Table 20. System & site recommendations for SCCM.....	76
Table 21. Miscellaneous recommendations for SCCM .....	79

## **ABBREVIATIONS**

AD	Active Directory
ADR	Automatic Deployment Rules
ADSI	Active Directory Domain Services
BIOS	Basic Input Output System
CAS	Central Administration Site
Client	A computer workstation that is used by an end-user
CMM	Capability Maturity Model
CU	Cumulative Update
DC	Domain Controller
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Services
DP	Distribution Point
DVD	Digital Video Disc
EFI	Extensible Firmware Interface
FEP	Forefront Endpoint Protection
GUI	Graphical User Interface
HP	Hewlett-Packard
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IIS	Internet Information Service
Incident	An unplanned interruption to an IT service
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDT	Microsoft Deployment Toolkit
MP	Management Point
OS	Operating System
OSE	Operating System Environment
OU	Organizational Unit
OSD	Operating System Deployment

PXE	Preboot eXecution Environment
SCCM	System Center Configuration Manager
SCO	System Center Orchestrator
SCSM	System Center Service Manager
SCEP	System Center Endpoint Protection
SMP	State Migration Point
SP	Service Pack
Service Request	A formal request from user for service provision
SQL	Structured Query Language
SSRS	SQL Server Reporting Services
TFTP	Trivial File Transfer Protocol
Ticket	A formal service or change request inputted in the ticketing system
TS	Task Sequence
UI	User Interface
WAN	Wide Area Network
WMI	Windows Management Instrumentation
WQL	WMI Query Language
WSUS	Windows Server Update Service

# 1 INTRODUCTION

This chapter describes the background and context of the thesis; defines the problem and key objectives; discusses the scope and limitations of the study and outlines the structure of this master's thesis.

## 1.1 Background

Computer systems are indispensable components of the modern industry and regardless of the size of the business the profitability of any business operation has critical dependency on the computer systems supporting that business [1]. Modern companies and organizations use more and more technological devices these days that require constant management and support. These devices are usually vital to the organization or its employees and thus need to be kept in working condition and up-to-date by local or external IT (Information Technology) support personnel. When the amount of supported devices grows over a certain point, managing them manually is no longer a cost-effective solution. The answer is automating the management and deployment of those devices (to a degree) without interrupting the end-user.

In an ideal case, the organization could manage all the required devices (computers, smartphones, tablets, networking devices etc.) with a single piece of software; many software manufacturers however, provide their own solution to cover only part of the tasks related to managing these devices. This leads to setting up multiple applications (and usually related servers) to handle hardware and software inventory, application installations, patch management, license information etc. It's also quite common that applications from different manufacturers don't communicate with each other well. Applications or software suites do however exist, that cover all these management tasks, and one of the biggest competitor in that area is Microsoft's SCCM (System Center Configuration Manager). Downsides to these bigger suites are simple: cost and complexity. For their very nature, they require more complex hierarchy for setting up than just a single application – however, implementing the same level of manageability in smaller applications usually leads to incoherent and non-scalable setup. For these reasons, it depends on the size of the organization and the volume

of end-devices what kind of management software is the best choice, since there is no sense in setting up very large-scale setups for several devices nor does it make sense to setup mixed freeware applications for multi-national companies that have tens of thousands of devices to support.

This thesis is done for Sulzer Pumps Finland Oy as a part of their ongoing project for centralized asset and information management in global scale for the Pumps Equipment division, which is one of Sulzer's three main divisions, along with Rotating Equipment Services, and Sulzer Chemtech. The aim of this project was to bring all computing devices into management by Microsoft System Center suite, specifically by the SCCM (System Center Configuration Manager) component, along with migrating all user and computer accounts in AD (Active Directory) within one single domain. This thesis focuses on the SCCM implementation and whether it succeeded in providing expected results in information and asset management.

## **1.2 Goals and limitations**

This thesis is based on an ongoing project at Sulzer Pumps, which's aim is to migrate all users and computers in AD into one single, unified domain (sulzer.com) and implement centralized management tools and processes for all Sulzer Pumps' computers globally. Later on, replacing all possible Windows XP computers with Windows 7 became a part of this project as the deadline for Windows XP's support became imminent and further system support for Windows XP wouldn't be developed in-house. Currently Windows 7 (64bit edition) is the only supported OS (Operating System) for client devices and Windows 2003 and newer for servers, although deploying Server OSs is not yet implemented. Currently only a lite-version of the SCCM agent is deployed to servers for patch-level scanning and inventory.

The aim of this thesis is to analyze the SCCM implementation done in Sulzer Pumps and does it provide adequate tools and level of service for managing all Sulzer's computers globally. The current SCCM system was already set up when this thesis started and the actual implementation of such system is not part of this thesis. The thesis focuses on two main research questions:

1. *Is SCCM a suitable tool for Sulzer to centrally manage all computers in global scale?*
  
2. *What practical improvements can be done to the current system and what benefits can be achieved as a result?*

The main research questions are further divided into sub questions to help answer the main questions described in table 1.

*Table 1. Research sub questions*

<b>#</b>	<b>Question</b>	<b>Method</b>
1a	<i>How well does the SCCM system perform against previous systems locally?</i>	Survey sent to local IT supports at major sites
1b	<i>How well does the SCCM system perform on a global scale?</i>	Analysis of SCCM implementation from global administration viewpoint.
2a	<i>How does the current implementation of SCCM compare against Microsoft's "best practices"?</i>	Literature research
2b	<i>What specific areas in SCCM could benefit from practical changes in order to streamline the current asset management processes?</i>	Combine findings from 2a with company-specific environment and infrastructure for more streamlined solution

Since the area of SCCM and possible configuration options are vast and numerous, this thesis will focus on the most impactful settings taking into account the company-specific environment. Depending on the amount and size of findings from research question 2, one or several suggestions for improvement will be carried out and the potential benefits measured against previous configuration. The current version of SCCM implemented in Sulzer's environment is 2012, and thus this study will focus on that version.

### **1.3 Research methods**

This qualitative research focuses on the implementation at Sulzer Pumps and does not directly produce generalized results. However the findings of this study could be taken into use in similar-sized company, with slight modifications. First, the thesis scope is formed, resulting in the research questions, then a theoretical background is presented on the subject and methods for solving found problems are discussed.

Information is retrieved by literature reviews, interviews with key personnel, surveys to regional local IT-departments and analyzing the system first-hand. Modifications to the system are performed and their impact evaluated. Last, research questions are answered and further development areas for future are provided.

### **1.4 Structure of the study**

The first chapter acts as an introduction, giving background information on the thesis and lists goals and the scope of the study. It also reveals the structure of the thesis which is illustrated in table 2. In the second chapter, centralized asset management and affiliated concepts are explained. Third chapter gives background on the company the thesis is done for. Fourth chapter gives an overview along with detailed description of Microsoft SCCM and its functions. In chapter five, the current SCCM implementation at Sulzer is presented and analyzed.

Results of the study and further development areas are discussed in chapter six and finally, a summary of the research is presented in chapter 7.

Table 2. Research structure.

<b>Chapter #</b>	<b>Theme</b>
Chapter 1 Introduction	Research setting Purpose and scope of the study
Chapter 2 Sulzer	Company background
Chapter 3 Introduction to centralized asset management	Centralized asset management and affiliated concepts explained
Chapter 4 Microsoft System Center Configuration Manager	Microsoft SCCM and its functions explained
Chapter 5 Analysis of current SCCM implementation	Current SCCM implementation presented and analyzed
Chapter 6 Microsoft SCCM Best Practices	Microsoft SCCM Best Practices discussed and compared to current system
Chapter 7 Survey results & change recommendations	Findings of the study and change recommendations for current system
Chapter 8 Implemented changes	Implemented changes, based on recommendations and their impact
Chapter 9 Results	Results of the research
Chapter 10 Conclusions	Conclusion

## **2 SULZER**

Sulzer is an industrial engineering and manufacturing company, founded in 1834 in Winterthur, Switzerland. Its business is divided into three main divisions: Sulzer Chemtech, Rotating Equipment Services and Sulzer Pumps Equipment. Sulzer Chemtec develops solutions to chemical industry and specializes in separation towers, two-component mixing and dispensing systems [2]. Rotating Equipment Services (formerly known as Turbo Services) provides full range of services for turbines, pumps, compressors, motors and generators [3]. The third, and biggest division is Pumps Equipment (formerly known as Sulzer Pumps), which is one of world's leading pump manufacturers and has over 22 manufacturing sites and more than 155 service and sales centers worldwide. It produces pump equipment to key markets such as: oil and gas, hydrocarbon processing, power generation, water (including wastewater), pulp and paper along with other industrial markets [4].

In 2002, through a corporate acquisition, Sulzer acquired Ahlstrom Pumps Oy and its pump business. As a part of Pumps Equipment division, Sulzer Pumps Finland has several different segments it focuses on and is situated mainly in Kotka, but also has minor functions in Espoo, Helsinki, Mänttä and Oulu. In Karhula, Sulzer has a pump factory and a foundry along with a customer support service center. Sulzer Pumps Finland has customer support service centers also in Helsinki (ABS-products only), Mänttä and Oulu. The Finnish headquarters is located in Karhula along with supporting functions such as sales, procurement, HR, finance, documentation, R&D, and local as well as global IT support (two separate departments). Tartek Oy which produces mechanical seals for industrial use [5] is also part of Sulzer, but it's not actually part of Sulzer Pumps Finland, although it is situated in Rauma, Finland.

### **2.1 Infrastructure**

Currently Sulzer is moving into more unified and centrally managed IT solutions instead of each branch and site managing assets and information locally. One major decision was to move all sites from their own domain in AD into one root domain (Sulzer.com) and differentiate them by just using different OUs (Organizational Units) instead of separating

them by subdomains. Sulzer Pumps (pu.sulzer.com) was the first domain to migrate, followed by Rotating Equipment Services (ts.sulzer.com). Chemtech (ct.sulzer.com) will follow in later. Local IT support will remain to a degree in most of the locations, since physical installations and procedures need to be still done on-site.

Sulzer has a major contract with HP (Hewlett-Packard) to procure mainly their computer devices. In an ideal case, Sulzer would procure all computers from HP to negotiate better deals due to the increased procurement volume, and to keep maintenance and administration as simple as possible. However, Sulzer still has some existing computer base from other manufacturers (such as Dell and Lenovo) but these devices will fall out of the scope according to the normal computer life cycle rotation and afterwards will be replaced with HP machines. Thus, Sulzer has standardized set of models that should be procured by all main locations to make the hardware environment more homogenous and to decrease the diversity of needed drivers and support. The amount of users varies a lot between different regions and countries, and is not always related to the general density of people in the area (although it is related to the size and nature of Sulzer's business functions in that area), as seen in figure 1. The categorization is done by support area, and for example Finland supports also Russia and Sweden, hence the significantly higher amount of users compared to other countries. Also, for the moment being, Wastewater solutions is still a separate OU from the rest, as the users haven't been migrated to the correct support regions' OUs yet. It should also be noted that the amount of users is not the same as amount of workers, since not all workers need a computer account or they use a shared one.

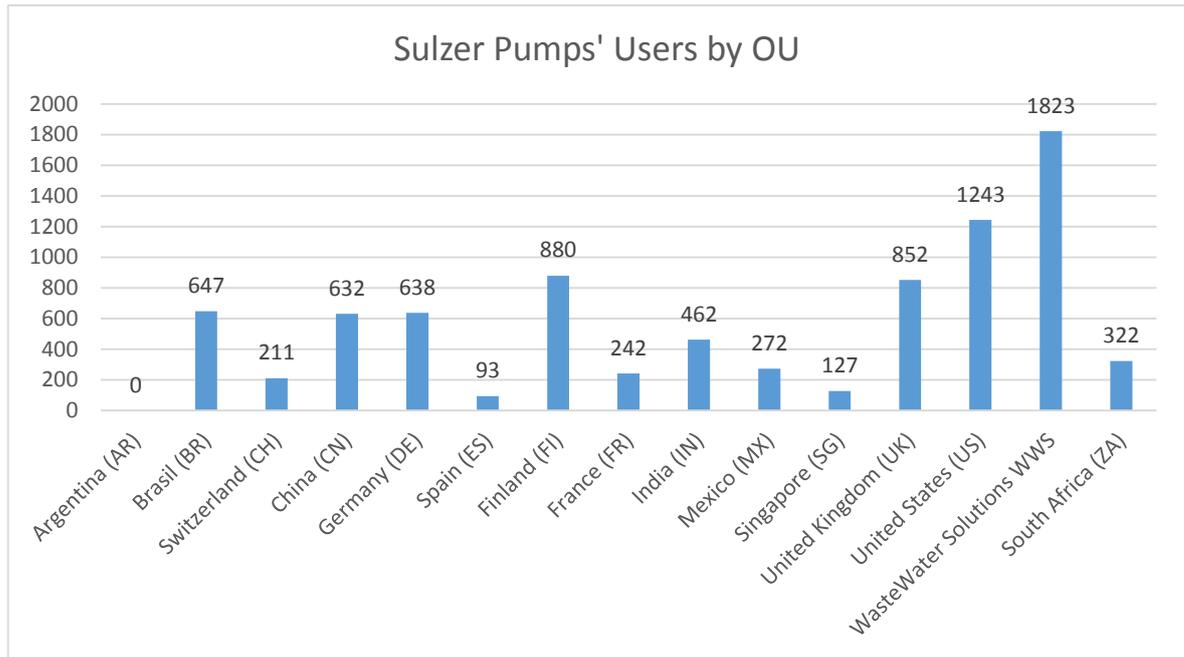


Figure 1. Sulzer Pump's users by OU.

Sulzer also has an enterprise agreement with Microsoft and thus the only supported OS in workstations is Microsoft Windows, and even servers should use Windows Server OSes wherever possible, although Sulzer does have multiple Linux and UNIX servers in place. Microsoft software should also be used whenever possible, in place of other vendors (such as Office products, SharePoint, System Center). This way Sulzer can make the most of the volume licenses and their extended support contract with Microsoft.

Sulzer's top IT level organization is divided into four major branches (depicted in figure 2): Support Service & Demand Management, Business Applications, Infrastructure and Strategy & Planning. The main office and stakeholders remain in Switzerland whereas other heads of branches reside in Finland, US, UK and India. The amount of external IT consultants in Sulzer's global functions is quite high: 161 compared to the 237 internal workers. The current plan is to reduce this number drastically during the autumn 2014 and was one of the main reasons behind building the four different centers of excellence (Data Center, Enterprise Platforms, Clients, and Network and Telecom) – to take over the work from the external workforces. This will significantly reduce costs and also tie internal employees to the core IT processes and their development rather than buying the service on case-by-case basis from consultants.

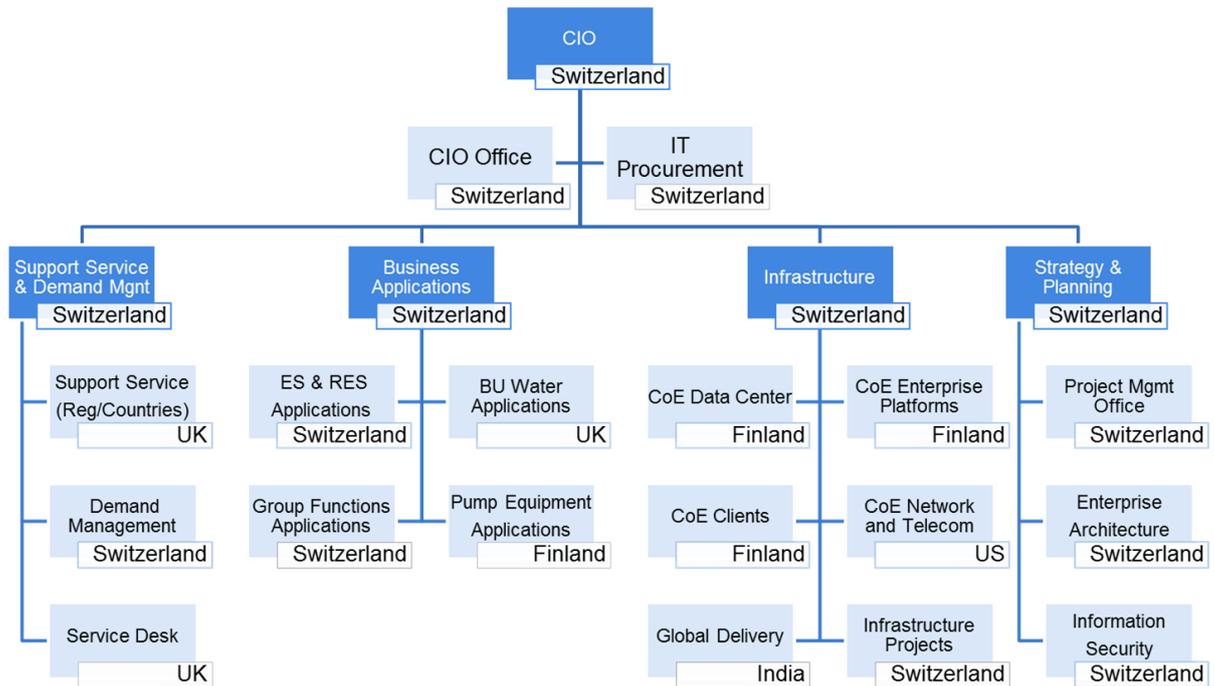


Figure 2. Sulzer's global IT organization.

The future plan is to still outsource the first line of support and utilize in-house knowledge and personnel for second and third level support. The first line of support handles all general IT service request (made via ticketing system or by phone) and forwards them to the correct support group for resolving. Usually the local IT personnel work second level support (if local IT exists) and the global team is the third and final level of support, providing knowledge in the backend-systems running world-wide.

## 2.2 Client management

Originally Sulzer launched project FITS (Future IT Sulzer) to centralize all IT and client management from all divisions by using global Windows 7 build and SCCM 2007, but afterwards the scope was scaled down to division-size (starting with the Pumps division), so they would be integrated and centralized sequentially, leading into the same end-result as FITS originally aimed for, but in a more gracious manner. Eventually, the SCCM version was changed to 2012, as the new version became available. SCCM 2012 environment was created based on the existing work done in SCCM 2007 and the new version of the system

was rolled out world-wide for Sulzer Pumps in late 2013 – early 2014 and is currently *de facto* management method for all computers within Sulzer Pumps (and to be for other divisions as well).

### 3 INTRODUCTION TO CENTRALIZED ASSET MANAGEMENT

The sheer amount of computers and smart devices has risen considerably over the past years and larger organizations have to come up with new and better ways of managing these devices. When the amount of managed devices is low, even manual management is a viable option, but when the amount of devices continues to grow, organizations need a centralized management solution for these devices. A basic computer system consists of *software*, *hardware* and an *operating system* and each of these areas need to be managed continuously. Hardware installations usually cannot be automated and need to be done manually in-person, but software and operating system installation and updating can be managed from afar and carried out without real-life presence. This thesis focuses on environment consisting of Microsoft Windows 7 clients and Microsoft Windows Server (2003 and newer) computers, using mostly Microsoft products. Linux, UNIX or OSX computers are not considered to be part of the environment although they can be partially managed with the same tools.

#### 3.1 Active Directory

Microsoft Active Directory (AD) is a centralized information store used to maintain entity and relationship data for wide array of objects in a networked environment [6]. Information stored in AD can be added, removed, edited and queried through open protocol called LDAP (Lightweight Directory Access Protocol). Based on X.500 protocol, AD can be classified as NOS (Network Operating System) [7] and it works as the network's centralized authentication and authorization service. Even though that AD is a Microsoft product, many other non-Windows based system can be integrated with AD, resulting in much more manageable heterogenic system. In order to achieve this, AD supports technologies such as LDAP and Kerberos. In figure 3, a sample AD relationship model is shown.

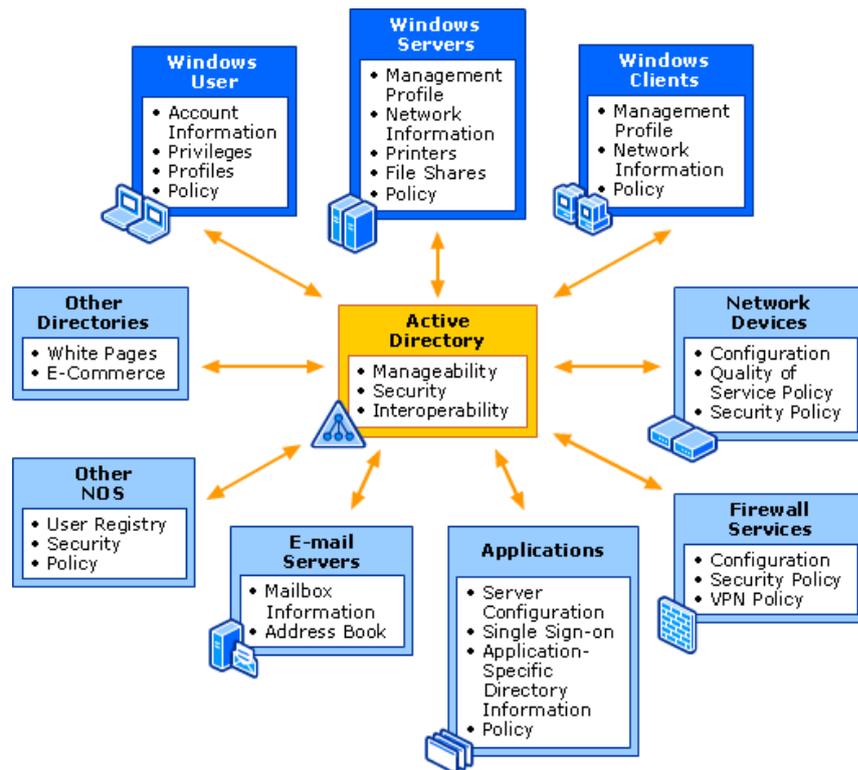


Figure 3. AD on Windows Network [8].

AD groups resources and users (called objects) into administrative units called domains, which each have a distinctive DNS name (such as sulzer.com) [9]. Each domain needs at least one DC (Domain Controller) to store all the information, but usually multiple DCs are set up for fault-tolerance. AD enables organizations to deploy different kind of policies to resources or users connected to the domain via GPOs (Group Policy Objects). GPOs enforce certain settings for users and computers such as password complexity, remote connectivity, firewall and security settings etc. This enables the administrators to target certain settings for specific computers or users, which usually belong to specific security groups.

Most large organizations these days use AD in their environment [10] to manage and administrate their domain-connected resources. Device discovery is usually the basic foundation for all asset management software and it is usually done via AD discovery or network discovery. If all devices are joined in the domain, AD discovery can easily find all the devices, whereas network discovery will be slower, stress the network while it discovers devices and cannot detect offline devices.

AD is the heart of SCCM and there is no non-AD workaround for a SCCM implementation.

### **3.2 Hardware management**

Hardware management can be usually split into three parts, hardware installation, inventory and compliancy. Of these three, the physical installation (such as setting up the computer and peripherals or component installations) cannot be centrally managed into same extent as the latter two; someone has to set up the computer on-location and it has to be done manually. Hardware inventory and compliance management can be, however, done via sophisticated software once the computer is powered on and connected to the network. Hardware inventory management gives detailed information about the hardware that is currently in use by the organization (number of devices, specific components etc.). Hardware compliancy, on the other hand, give information about how well specific devices follow the set compliances, such as device configurations, approved devices etc. This is important especially in bigger, more standardized environments where all devices should be compliant. When a device is non-compliant, depending on the implementation of the compliancy management, administrators can receive automatic notifications and detailed information about the issue. In a practical real-life scenario, a non-compliancy issue could mean a hardware component's failure or malfunction. In modern Windows environments, basic hardware information can be retrieved with the use of WMI (Windows Management Instrumentation) queries.

### **3.3 Software management**

Technical software management (not taking into account procurement or standardization within the environment) consists of methods for deploying (and removing) software to end-users machines, possibly remotely configuring various settings (by e.g. pushing configuration files) and monitoring software and associated license inventory. Some sophisticated methods allow also monitoring the actual usage of the applications through various listeners.

### *3.3.1 Software Deployment*

Software deployment is about realizing the highest value provided by the software and in order to efficiently utilize the IT resources available, software deployment methods should be efficient [11]. In a larger perspective, IT administrators deploying new software in an organization should take careful planning into consideration before choosing and rolling out a product. In this thesis however, software deployment will focus solely on technical aspect of deploying the software to the users' devices; the actual validation or approval process of new software is not included in the scope.

The most basic scenario for installing a single piece of software into user's computer is to take the installation media (optical disk, flash drive or other medium for the installation files) insert it to the device and start the installer for application. Most commonly this would be an .exe (executable) or a MSI (Microsoft Installer) file or in some rare cases a script file (without any additional parameters) to start the actual installer. The person installing the application would then click through the various screens and possibly configuring the installation along the way. If the amount of computers is low in the organization, this is a viable method. If, however, the amount of computers is high as is the case usually in bigger organizations, this process would be very time and resource consuming. A more efficient way would be to use a script file that calls the installer with predefined configuration parameters (if supported), thus the application can be installed by only starting the script on each machine. This is a viable option in small to medium sized organizations. Sophisticated methods for installing software in large and very large organizations usually focus on remote silent installations. The end user won't need to interfere and usually as long as the computer is powered on and connected to the network the installation can be done via third-party tools.

### *3.3.2 Software & License Inventory*

Maintaining an up-to-date picture of deployed and actually used software and licenses in an environment is a constant challenge, due to ever increasing changes. If organization's software and license inventory is not accurate, this can lead to over- or under-purchasing of licenses (where the former will just cost more money and latter breaking signed agreements which usually include costly sanctions). If there is no centralized management software to

handle this, in most common scenario the data is held manually in spreadsheets or similar files. Firstly, there is a problem keeping the license data up-to-date, since licenses are acquired from multiple sources (as there is software used from multiple manufacturers) that are used by different departments and branches. Secondly, keeping track of what licenses are currently in use, by whom, and how many are actually needed is more difficult tasks, since usually without third-party tools, this data cannot be acquired automatically from computers. Many organizations would benefit from better license management, since very large reductions in cost can be acquired by procuring just the correct amount of licenses.

Along with managing software and license inventory, some organizations can find it useful to track software metering as well. This provides information regarding the usage of specific applications, such as how often it is actually used. This way, totally or marginally used applications are possible to be removed, thus leading to lessened amount of administration.

### **3.4 Operating System Management**

OS is the topmost piece of software that control and manages all hardware and other software inside a computing system. In essence, it controls every device, file, section of memory, processing time along with access control that who can use what and when. Therefore, choosing, deploying, maintaining and keeping the OS up-to-date is paramount. Different strategies and tools exist for all of these areas and there is no definite best solution – rather it depends on multitude of factors, such as environment, available resources, and existing infrastructure.

#### *3.4.1 OS Deployment*

Deploying new operating systems in organizations of any size is a large undertaking with vast implications [6]. Improper planning and implementation usually leads to extra costs due to accumulated work and potential data loss. The size of the organization usually defines the deployment method; very small organizations benefit from manual installations since the deployment cost is usually the hourly wage of the person(s) doing the work. In larger organizations, however, it rarely makes sense to install every OS manually per computer,

accompanied by driver and application installations. Installations can be usually speeded up if the hardware base is standardized or homogeneous thus leading to small driver base. Using Microsoft tools, such as WDS (Windows Deployment Services), MDT (Microsoft Deployment Toolkit) and AIK (Automated Installation Kit), Windows OS installations can be speeded up significantly, although considerable amount of time has to be put into preparations. With these tools the installed image can be modified and accompanied by certain configurative tasks, such as hard drive partitioning and driver installations. OS deployment can be also done via multiple sources: optical disks, flash drives or over network.

Microsoft has developed different deployment strategies for different environments. Different factors impact choosing the deployment model: amount of computers to deploy to, network complexity and infrastructure, knowledge and experience of available IT staff. In generalized form, these strategies can be split into four categories: High-touch with retail media, High-touch with standard image, Lite-touch/High volume deployment and Zero touch/High Volume deployment [12].

High-touch with retail media is the most basic form of deployment; by using an unaltered OS image on a DVD (Digital Video Disc), the standard OS is deployed manually to each computer. Configurations must be done by hand or by using XML-answer files (eXtensible Markup Language), which can be edited with Windows System Image Manager. This model is recommended for organizations with less than 100 computers, unmanaged network and no dedicated IT staff.

High-touch with standard image is similar to high-touch with retail, except that the OS image can be customized with additional drivers, applications and settings. The OS still needs to be deployed using flash drives or optical disks to each computer and thus does not scale well. It is however, significantly faster than high-touch with retail media, once the customized image has been created. This is typically recommended for small organizations (100-200 clients) with and IT generalist on staff [13].

Lite-touch, High-volume deployment is recommended for medium-sized organizations which have IT staff present and a managed network. By using MDT, organizations can

deploy thin or thick images either via network or flash memory/optical disk. The deployment is started on each computer separately, but only little input from user is required. Thin images contain only little customization (such as updates and critical applications) whereas thick images contain as much as possible (updates, majority of organization's applications). Downside to using thick images is that keeping all the applications up to date inside the image is usually more tedious than using thin images and deploying the applications afterwards. [14]

Zero-touch, High-volume deployment is recommended for large organizations that have IT staff with expertise in deployment, networking and Microsoft SCCM. Organizations using Zero-touch method usually have over 500 computers and manager networks. Zero-touch deployment doesn't need any interference from the end-user or local technician and can be deployed remotely. Zero-touch, however needs significant infrastructure (SCCM, AD, Volume Licensed media, scalable network, image preparation tools etc.) and costs the most of the four options. [15]. Once the infrastructure is in place and the image created, the Zero-touch method requires the least amount of work to install and thus is the preferred method for high or very high volume environments.

In this thesis, the focus is on Lite-touch and Zero-touch method by utilizing SCCM 2012 OSD (Operating System Deployment) as these methods fit best large standardized environments. There is no point in implementing High-touch strategies in environment with over 10 000 client machines. Zero-Touch strategy would ideally be the best solution for very large environments, but it has some drawbacks also, mainly the prerequisites, planning and setting infrastructure in place, but also depending on the implementation – there exists a great chance for pushing automated installation for unwanted machines if it's not properly configured – and this can lead to disastrous situation where even critical, live machines get installed.

### *3.4.2 Configuration & compliance management*

One of the hot-topics in today's computer management is configuration and compliance management. Many industries have regulatory laws that dictate privacy and corporate responsibilities such as SOX (Sarbanes-Oxley), HIPAA (Health Insurance Portability and

Accountability) and GLBA (Gramm-Leach-Bliley Act) [16]. These kinds of regulations require IT organizations to implement specific privacy and security standards for their IT systems and data. Organizations that must follow these regulations have difficulties in enforcing these policies since the regulations are not technical in nature [6]. In essence: the laws or regulations should be followed and a compliancy plan needs to be made, implemented, enforced and usually compliancy data reported over time. Organizations using Windows OS can use Windows Group Policies, which dictate certain specific configurations and settings and are downloaded from a DC to the client. Problem is, that usually the compliancy is not tracked or automatically reported in any way, except during troubleshooting when the client behaves unexpectedly.

### 3.4.3 *Updates and patching*

One of the largest and most important components in OS maintenance is OS and application updates. Updating or patching systems is a common maintenance task that has been elevated in importance by security concerns [17]. In general, there are three main reasons for OS updates: error fixes, security patches and new features. Security holes are errors in a sense, but since they don't usually manifest in normal day-to-day use, they don't directly hinder the use of the OS. Even though error fixes (also called *bugfixes* or *hotfixes*) and new features are important, the most vital part of the updates are the security patches, since an unpatched machine is vulnerable for viruses, malware and remote breaches. Thus, security updates should be installed preferably as soon as possible, and hotfixes and new features when reviewed and approved.

The key to success in OS patching is proper evaluation, prioritization and testing [17], along with standardized processes that are followed. Turnaround-time for patching is a major issue; if patching a known security hole takes too long, there is a high possibility that it will get exploited – on the other hand, applying patches or updates immediately can break down some systems that rely on a component that was changed in the patch.

In Windows –dominant environments, WSUS (Windows Server Update Services) can be used to manage Windows updates that are deployed to clients. WSUS acts as a gateway for client updates and synchronizes itself with the public Microsoft Windows Update service.

Thus, the clients don't need to download the updates from internet as they download the updates from the WSUS server in the intranet. Along with centrally managed updates, this reduces the amount of required internet bandwidth for OS updates.

Organizations often have one or several computers that are not connected to the internet either at all or seldom. Without WSUS or manual patching, these computers cannot retrieve security updates from internet and pose a security risk if they are still connected to the local intranet, since a virus or other malicious threat could travel through an internet-connected device to the unpatched machine and infect it.

WSUS allows administrators to configure certain updates (usually critical and security updates) to install automatically for all or specific clients and allows administrators to review available updates in order to approve and install those that the organization wants to implement in their environment. Updates can be pushed to clients manually from the WSUS-server or at certain times, such as *Patch Tuesdays* [18] allowing for automatic monthly or weekly updates.

It should be noted that WSUS can offer updates for some other Microsoft products as well, such as Office and Visual Studio.

Along with WSUS, bigger organizations can use Microsoft SCCM for more granular and complete control over update management and deployment. SCCM however requires WSUS server to download and push these updates.

## 4 SYSTEM CENTER CONFIGURATION MANAGER

SCCM is Microsoft’s own software for managing large, Windows-based environments (although some other OSEs are partially supported). SCCM is part of a bigger software suite, called Microsoft System Center, which include other server products among SCCM, displayed in table 3. SCCM allows remote management of clients (not limited to Remote Desktop Protocol), software management and updates, OS deployment and patching, configuration management and compliancy, and comprehensive inventorying (hardware, software and licensing).

*Table 3. System Center family of products [19]*

<b>Product</b>	<b>Function</b>
System Center Advisor	Free cloud service that can be used to analyze installations of Microsoft server workloads in local environments to identify potential misconfiguration issues.
System Center App Controller	Self-service experience for deploying and managing virtual machines and services.
System Center Configuration Manager	Configuration & hardware/software asset management, OS and patch deployment tools
System Center Data Protection Manager	Continuous data protection and recovery
System Center End Point Protection	Anti-malware and security solutions
System Center Essentials	Combined features of Operations Manager and WSUS (aimed at small-medium organizations)
System Center Mobile Device Manager	Mobile device management

System Center Orchestrator	Provides end-to-end automation, coordination and management as well as provides tools for building, testing and managing custom IT solution that can streamline datacenter management.
System Center Operations Manager	Monitoring for hardware, virtual machines, OSES, services and applications.
System Center Service Manager	Integrated platform for delivering IT as a service through automation, self-service, standardization and compliance.
System Center Virtual Machine Manager	Virtual machine management and datacenter virtualization

The first version of Microsoft's system management tool was from 1994 called *Systems Management Server*, which 13 years later changed its name to *System Center Configuration Manager*. The major revisions, including SPs (Service Packs) and CUs (Cumulative Updates) of SCCM can be seen in table 4. The first versions of SMS (Systems Management Server) (1.0-1.2) didn't include AD integration. Since Windows NT domains were clustered by nature, they weren't that common in hierarchical systems and thus SMS 1 had its own site for discovering the structure and devices. The first versions mainly offered application and update packaging. The second major version 2.0 offered the same functionality as the first one, but it also was able to utilize subnets in device discovery. Version 2003 introduced the advanced client and AD discovery methods for managed devices. The advanced client connects to a MP (Management Point) and was implemented as a solution to the problem where laptop users would connect to the network from multiple locations, making it inefficient to download content always from same location. If advanced client is introduced to another SMS site, it may use that site's local DP for downloading content instead of connecting to the original site's DP, which might reside behind long or slow WAN (Wide Area Network) links. In 2007, Microsoft abandoned the traditional site-concept and moved their system management solutions under System Center-suite leading to SCCM version 2007. The new version was designed with AD in mind, (as opposed to the NT-oriented SMS). Drastic changes in management and packaging had been done, and SCCM proved to be much efficient and easier to use than its predecessor, SMS. SCCM included patching and updating using WSUS and later updates made it possible to manage Windows Vista and 7

and possibility to remotely wake up powered off devices if they supported Intel's vPro technology. SCCM included multitude of management changes, such as configuring BIOS (Basic Input Output System) settings or updating the BIOS without physically touching the managed device as well as supporting Microsoft App-V application virtualization. Later, SCCM 2007 supported also OS imaging which made OS installations much easier. The current version of SCCM is 2012 and supports now Windows 8 and several mobile OSes (iOS, Android, Windows Phone and Symbian). The new version also includes Microsoft Endpoint Protection by default (although enabling it in one's environment isn't mandatory, so other 3<sup>rd</sup>-party antivirus solutions are still supported).

*Table 4. System Center Configuration Manager version history.*

<b>Product</b>	<b>Revision</b>	<b>Published</b>
Systems Management Server (SMS)	1.0	1994
Systems Management Server (SMS)	1.1	1995
Systems Management Server (SMS)	1.2	1996
Systems Management Server (SMS)	2.0	1999
Systems Management Server (SMS)	2003	2003
Systems Management Server (SMS)	2003 R2	2006
System Center Configuration Manager (SCCM)	2007	2007
System Center Configuration Manager (SCCM)	2007 SP1	2008
System Center Configuration Manager (SCCM)	2007 R2	2008
System Center Configuration Manager (SCCM)	2007 SP2	2009
System Center Configuration Manager (SCCM)	2007 R3	2010
System Center Configuration Manager (SCCM)	2012	2012/03
System Center Configuration Manager (SCCM)	2012 CU1	2012/08
System Center Configuration Manager (SCCM)	2012 CU2	2012/11
System Center Configuration Manager (SCCM)	2012 SP1	2012/12
System Center Configuration Manager (SCCM)	2012 SP1 CU1	2013/03
System Center Configuration Manager (SCCM)	2012 SP1 CU2	2013/06
System Center Configuration Manager (SCCM)	2012 SP1 CU3	2013/09
System Center Configuration Manager (SCCM)	2012 R2	2013/10
System Center Configuration Manager (SCCM)	2012 SP1 CU4	2014/01

System Center Configuration Manager (SCCM)	2012 R2 CU1	2014/03
System Center Configuration Manager (SCCM)	2012 R2 CU2	2014/06
System Center Configuration Manager (SCCM)	2012 SP1 CU5	2014/07
System Center Configuration Manager (SCCM)	2012 R2 CU3	2014/09

There are currently two different versions of System Center 2012: Datacenter and standard. Comparison between these two versions can be seen in table 5 (license costs are Microsoft reference prices and actual prices may vary greatly). Because the price difference between standard and datacenter is steep, careful planning should be undergone before procuring licenses. Generally, the Datacenter editions are designed for highly virtualized environments, whereas the standards edition is for lightly virtualized or nonvirtualized environments [6]. The publicly announced licensing fees are usually in the correct price range, but the final fees will be case-specific, factoring in amount of devices, license-tied components such as processors, users and wanted features.

*Table 5. System Center 2012 Licenses [20]*

	Standard	Datacenter
# of physical processors per license	2	2
# of managed OSEs per license	2	Unlimited
System Center server management components	All	All
Right to run management server software and supporting SQL Server Runtime	Yes	Yes
Manage any type of supported workload	Yes	Yes
Open No Level License and Software Assurance 2-year price	\$1,323	\$3,607

For managed devices that run non-server OSEs (Operating System Environment), Client Management Licenses are needed. In system center 2012, these are divided into three categories, as shown in table 6 (license costs are Microsoft reference prices and actual prices may vary greatly). These licenses are available on per-OSE or per-user basis. [20]. From this data it can clearly be seen that implementing SCCM will cost quite a lot of money for the

organization, even from purely licensing perspective. Adding the cost of planning, implementation and operation will increase the price significantly. Thus, the decision for implementation should be done carefully and only if the benefits outweigh the price in the long run.

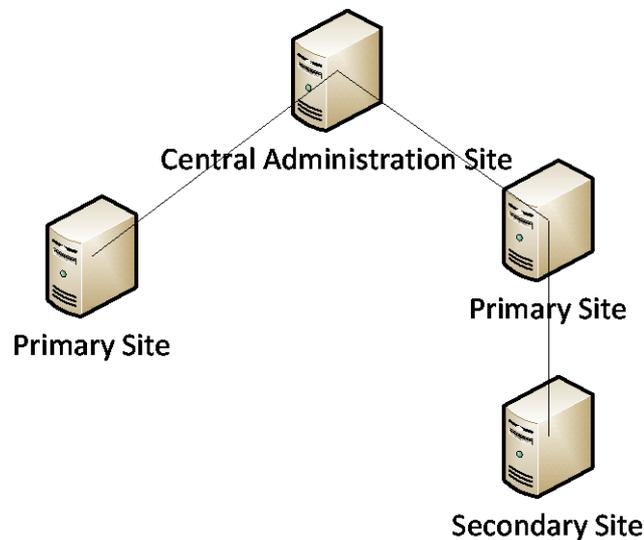
Table 6. System Center Client licenses.

	SCCM Client	Endpoint protection client	Client Management Suite Client
Components	<ul style="list-style-type: none"> <li>• SCCM</li> <li>• Virtual Machine Manager</li> </ul>	<ul style="list-style-type: none"> <li>• Endpoint Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Service Manager</li> <li>• Operations Manager</li> <li>• Data Protection Manager</li> <li>• Orchestrator</li> </ul>
2-year license	\$62	\$22	\$121

#### 4.1 Hierarchy and architecture

SCCM has three main server types (known as *sites*): CAS (Central Administration Site), primary site and secondary site. Of these three, at least one primary site is always required for SCCM implementation and if there are more than one primary sites, one CAS is needed. All primary sites communicate with one CAS (and there can never be more than one CAS in the same environment) and they never directly communicate with each other. Each primary site can have secondary sites, and secondary sites always have exactly one primary site and cannot have secondary sites of their own. SCCM architecture with one CAS can be seen in figure 4. A single primary site can service up to 100 000 clients but usually environments with less than 100 000 clients might be inclined to set up multiple primary sites for redundancy, load balancing and supporting geographically distant branches. The decision for multiple primary sites should be made early, since if primary site has been

initially created without CAS, any additional primary sites cannot be added to the hierarchy later. If additional primary sites are later desired, a new environment has to be created [6].



*Figure 4. Sample SCCM architecture.*

Secondary sites are secondary servers, as the name implies. They cannot provide services to clients by themselves as they always require one primary site. Each secondary site can service up to 2500 clients and they are usually implemented for servicing clients in another network (e.g. in a different city/country). Secondary sites don't have their own management console as they are managed directly through their primary site. Another option for using secondary sites is using DPs (distribution points). Each DP can service up to 4000 clients and they simplify the hierarchy as opposed to deploying whole secondary sites. Main difference between the two is that DP generates more network load between itself and primary site, but secondary site needs its own database. In the end the number of serviced clients and the infrastructure of network dictate which one is more efficient way to go. Microsoft itself recommends secondary sites should be used over slow network links [21].

SCCM is based on three major services that create the base foundation for the SCCM software: AD, Microsoft SQL server and WSUS. AD and Microsoft SQL server are mandatory and WSUS is optional, but required for updates and patches. The SQL server plays a major, albeit on the surface, quite invisible role in SCCM: Almost all data in SCCM is saved into SQL servers' databases. This data can also be queried using WQL (WMI Query Language), but using these queries is not required for SCCM operation. Depending on the

hierarchy implementation of SCCM, the SQL-server can reside in a separate server than SCCM or both instances can be installed on the same server (virtual or physical). Usually in smaller environments it's simpler to implement them on the same server, but on larger environments it's advisable to separate them to different physical hosts due to performance issues.

In order to be managed by SCCM, client devices will need the SCCM client software installed. This can be done during OS deployment, manual installation, or by push-installation from SCCM. If the SCCM client is pushed to the devices, some form of device discovery needs to take place (such as AD- or network discovery, where the former is the preferred method due to smaller network load).

## 4.2 OSD

OSD (Operating System Deployment) is an automated procedure for deploying operating system images. It includes the whole process from creating the OS image to its installation (including disk operations such as partitioning and formatting) along with initial driver, software and update installations. All parts of the OSD process can be further defined with different set of rules (e.g. installing certain set of drivers for specific devices) [6]. SCCM 2012 uses both SCCM and Windows components to deliver OS images to client devices. The OS images customization can be done either prior to image capturing and/or post-deployment via SCCM TSs (Task Sequences). In essence, OSD process includes: OS system image capture (with or without customization), creating a TS, OS deployment and user state migration (optional). Different scenarios for OSD exist: Bare-metal installation, operating system refresh, in-place upgrade and side-by-side migration. In this thesis the main focus will be in bare-metal installations via network using PXE (Preboot eXecution Environment). Summary of each method is described in table 7.

*Table 7. OSD scenarios in SCCM*

Scenario	Description	Method of initiation
----------	-------------	----------------------

Bare-metal installation	Install OS on a client device with no existing OS.	PXE, Bootable and prestaged media.
OS Refresh	Install OS on a client device with an existing OS	SCCM deployment, PXE, Stand-alone and prestaged media.
In-place upgrade	Perform OS refresh and migrate user data	SCCM deployment
Side-by-side migration	Install OS on a new client device and migrate user data from the old device	SCCM deployment, PXE, Bootable media

All deployment scenarios use DP, MP and Primary site server during the OSD. Bare-metal installation overview is shown in figure 5. Even though the MP and the DP are shown as separate servers, these services can also be installed directly to the primary site server. In either case, the communication model between these services remains the same.

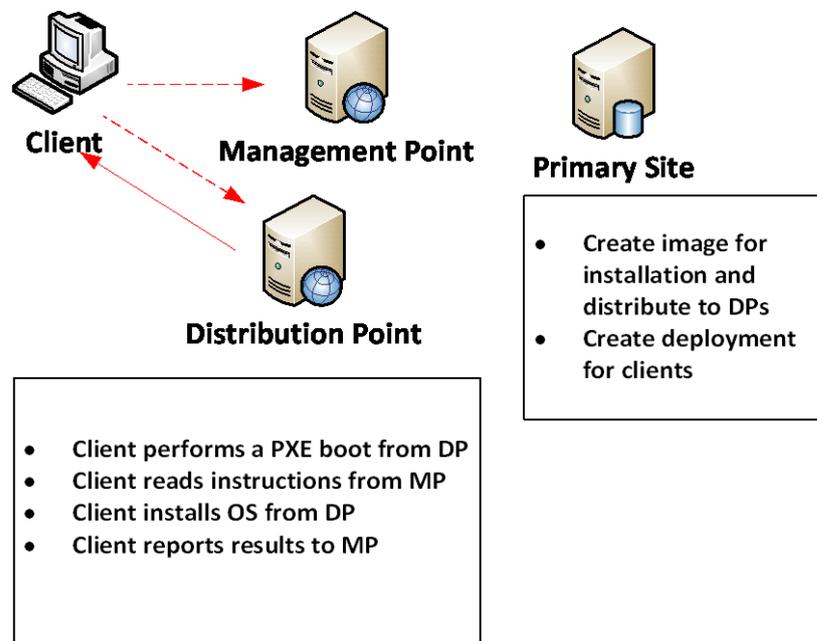


Figure 5. Bare-metal OSD overview.

#### *4.2.1 Tools used in OSD*

Even though that OSD is integrated fully into SCCM, it uses multiple separate tools to achieve this. The major tools used in the OSD process are Sysprep, WAIK (Windows Automated Installation Toolkit) and PXE.

Sysprep is a common tool that is used for automatic OS installation preparations. While creating OS images, sysprep removes many unique identifiers and during the first startup after OS installation, light installation procedures are performed to create these missing identifiers. Normally these can be set manually, but SCCM is able to utilize configuration files to automate the process.

WAIK is a set of tools that are designed for Windows OS installations and is specifically useful for highly-customized environments. SCCM by design uses some of these tools (such as ImageX and Deployment Image Servicing and Management).

PXE allows for the client to boot the computer from network, using a special bootstrap program. The client then contacts the DHCP (Dynamic Host Configuration Protocol) server to fetch an IP (Internet Protocol) address and Network Bootstrap Program file name. If successful, the client downloads the Network Bootstrap Program from the TFTP (Trivial File Transfer Protocol) service and executes it.

One more important area in OSD is boot images – they include the WinPE-images (Windows Preinstallation Environment) from which the clients are booted during OSD. WinPE is a miniature OS in itself and is currently based on Windows 8.1 (version 5). It supports basic features such as WMI, VBScript, batch files and database access and many things that can be run on regular Windows can also be run in WinPE. Major advantage of WinPE is its reduced size over regular Windows OS (approx. 150MB) and it can be run in system memory rather than directly from disk. SCCM 2012 requires the clients to have at least 512MB memory to be able to run WinPE.

#### 4.2.2 Task Sequences

TSs are the heart of OSD. They form a set of highly customizable tasks that are sequentially performed. Many of these tasks are already built in SCCM but they can be further expanded by MDT (Microsoft Deployment Toolkit).

The basic overview of TS steps can be seen in table 8.

*Table 8. Basic task sequence steps.*

<b>Step</b>	<b>Action</b>
Startup	Runs on existing OS before overwriting it. Mainly used for user data capture or BIOS updates before OS installation.
WinPE	Execute WinPE and prepare the system for the OS installation. Can include hard-drive partitioning and formatting.
Windows setup	Install the OS, exit from WinPE and boot into the new OS.
Post-Windows	All other configurations and customizations are run. Includes application installations, updates and applying drivers. If user data was captured in startup-step, it can be restored during this step.
Capture Image	Special Step that is only run if SCCM agent was prepared for imaging and sysprepping Windows. The unique identifiers are removed, system is rebooted back into WinPE and installed OS is captured into .wim file

Any regular OS configurations that wasn't done during core-image build and capture can be done during TS, and even the ones that were done can be overwritten (in case of using the same core image in more heterogeneous user and/or device environment). Common tasks are hard-drive re-partitioning and formatting, domain joining, applying drivers based on device model and installing applications and updates. Even OS updates can be added in the TS, as core-image is usually updated less frequently than the TS itself. Multiple TSs can coexist in SCCM and be available for OSD at the same time (e.g. regional or departmental TSs / test or production).

In bare-metal installation user data cannot be migrated since it doesn't exist, but when doing a in-place upgrade or side-by-side migration the user data migration can be included in the TS. The data can be stored in the server side in SMP (State Migration Point), or in the case of in-place upgrade it can even reside in the client device even during OSD by hard-linking the data to the harddrive. In this case the drive can be wiped, but not formatted, so the pointers to the files can be restored later. Hard-linking is especially useful in locations with poor network connectivity to the SMP.

### **4.3 Application Management**

One of the challenges IT organizations face today, is the abundance of applications needed in their environment and how to manage and deploy them. SCCM 2012 has the ability to deploy applications (and application updates) to end devices via network and limit the target group if necessary (thus everyone doesn't get the same applications). SCCM also has the capability to show comprehensive inventory of installed application packages and information about their usage. Along with installing applications remotely, SCCM can also uninstall software from devices where it doesn't belong (prohibited and/or old applications).

The software distribution feature has been a core component of SCCM and SMS from the very beginning [6]. Before SCCM is able to deploy a certain application it usually needs to be packaged one way or another. SCCM identifies two different terms for applications: packages and programs. A package consists of general information about the deployed application (e.g. version information, manufacturer, language, source file location etc.) and they are created either from a package definition file, such as .msi files or manually. Packages can also be created without any definition files and for example executables and batch files can be used for deployment.

A single package contains one or more programs which specify what should occur on the target client when it receives the package. Usually an .msi file contains six basic programs that are described in table 9, stating whether the package should be installed unattended or attended and whether it should be installed per-user or per-system. Along with these options,

the package can be defined to be installed as full installation or as a virtualized App-V version. SCCM 2012 now has the ability to check if the deployment has already taken place by another mechanism, thus preventing reinstallation of the same deployment by a different mechanism. It also has a mechanism for checking necessary requirements before installing the deployment. Requirements can include a multitude of criteria and filters, such as hardware & software configurations, OS type etc.

*Table 9. Six basic programs in an .msi package*

<b>Type</b>	<b>Action</b>
Per-system attended	Install system-wide, requires user interaction
Per-system unattended	Install system-wide, no user interaction
Per-system uninstall	Uninstall system-wide
Per-user attended	Install for specified user, requires user interaction
Per-user unattended	Install for specified user, no user interaction
Per-user uninstall	Uninstall for specified user

Now in SCCM 2012, the application and software deployment has switched to more user-centric approach with Software Center. Software Center is a central location where end-users are available to view available and already installed software, pending updates and configure certain personalized settings, such as working hours and power management settings (if allowed by administrators). From within Software Center, end-users can also launch the web-based Application Catalog (which can also be accessed directly from browser) where users can view deployments that are targeted to their user account. Through Application Catalog, users can request software available to them and depending on how a specific application is configured (requiring an approval or not) the user is able to install the software without the need for administrator or elevated privileges. If an application is configured to require approval, then an administrator will need to approve the pending request before the user is able to install it. With the aid of SCSM the approval workflow can be automated further, enabling automated emails to the administrators and users, and allowing administrators or managers to approve software directly from web-based service rather than need to use the SCCM console itself.

Applications also have reference options called dependency and supersedence. If an application has dependencies configured, SCCM will check if they are pre-installed in the target environment and if not, it will either install them before continuing with the actual application install or stop the application installation, depending on how the application installation was configured. Common dependencies are .NET frameworks and Java run-time environments. Supersedence defines a relationship between two applications and establishes a path for replacing one application with another, either by upgrading or uninstalling the superseded one [22].

Note should be made that also other than standard .msi applications and scripts can be deployed, such as previously mentioned App-V packages, Windows 8/RT Modern applications, mobile apps and even Mac OS X applications [22].

#### **4.4 Collections**

A single collection represents a group of resources within SCCM. A collection can consist of computers, users or security groups but in SCCM 2012, a single collection can only contain devices or users, not both. Collections are a logical grouping that can be targeted with SCCM functions such as software distribution, OSD, client settings etc.

Generally, collections can be either static (defined explicitly) or dynamic (queries based on certain criteria). Collections are used as target groups when *deployments* are used. Deployments are distributed to specified DPs and are identified either as available (can be installed) or required (available before deadline, installed silently at deadline). Collections can be scheduled for full updates with customized intervals (hourly/daily/weekly/etc.) or/and using incremental updates. By default, the incremental update looks every 5 minutes (site-specific default, can be configured for shorter or longer time period) if the query within the membership rules includes new members. Incremental updates has no effect on direct membership rules. In theory, the incremental update uses less resources, as it looks only for new members, but as it is usually ran on much frequent cycles it can become a more taxing option than the full update. Since the incremental update (by default) is run every 5 minutes,

in an environment with multitude of collections with frequent new members, the update might not finish within 5 minutes, which means the next update will start before the previous is done, resulting in overlapping incremental updates. Thus incremental updates should be used sparingly and with careful planning.

The general flow when using packages, programs, collections and deployments is as following: A package is created, consisting of one or more programs (usually consisting at least installation and uninstallation programs), a target collection is defined, files are distributed to the necessary DPs and the deployment for the package, targeting the collecting is executed.

## **4.5 Update Deployment**

Microsoft released Software Update Services in 2002 and SMS 2.0 had some patch-management features with the help of an add-on feature pack, but a native patch-management solution came in SMS 2003 that could be used in corporate environment [22]. Originally, SMS 2003 used Microsoft Update technology to detect and install the required updates, but as more and more patches were released for Microsoft OSes and applications the abundance of required files and resources became overly taxing for both server and client sides. In SCCM 2007, the Software Updates feature was rewritten and it now used WSUS for patch management and lightened the load on client side. WSUS is still used in SCCM 2012 and some new features were introduced, such as ADR (Automatic Deployment Rules), Software Update Filtering and Software Update Groups. With ADR, administrators can automatically approve and deploy all or certain updates. Multiple criteria can be used for filtering which updates are allowed to be deployed automatically, such as critical or security updates, or updates for certain OS type.

Since WSUS is used for software updates in SCCM 2012, setting up a WSUS server is a mandatory prerequisite for using software updates. If WSUS doesn't reside in the same server as SCCM, a WSUS administrator console is required for communication with a remote WSUS server. Along with a WSUS server, a Software Update Point role needs to be configured on the same server.

## **4.6 Inventory & Asset Intelligence**

It's crucial for organizations to know what kind of hardware, software and licenses they have in use and how they are actually utilized. SCCM can scan and report on these issues through the use of the SCCM agent. In inventory collection, clients gather data about their hardware and software through WMI and use policies sent from SCCM to define what to include in those scans. This data is then stored temporarily in an XML file and later sent to MP. The Asset Intelligence is used for reporting software licensing information and compliancy for both Microsoft and non-Microsoft software. The Asset Intelligence component has dependencies on both hardware inventory and software metering in order to fully work. By using Asset Intelligence, organizations can import licensing data into SCCM and then compare it against actual field reports through SCCM and see if they are currently under/over licensed and how these licenses are used.

The Asset Intelligence Catalog is used to properly identify software in SCCM. It's a set of tables stored in SCCM database and it contains identification data for over 300 000 software titles [22]. These same tables are used to manage hardware requirements for specific software. Additional items can be imported or created to the catalog through SCCM, but the catalog is also regularly updated by Microsoft and organizations which have Microsoft Software Assurance and are using the Asset Intelligence synchronization point site system role can utilize this dynamic content.

## **4.7 Compliancy**

The compliancy Settings allow the assessment of compliancy in client devices in regards to vast amount of configuration options such as OS version and configuration, whether all required applications are installed and none of the prohibited exist in the client (either installed or just as files). Compliancy also covers aspects such as security and power settings, software update status and even registry settings. Some of the noncompliant settings can be immediately remedied through the use of WMI, Windows registry and scripts in SCCM [22]. In practice, the compliance settings are evaluated against a defined baseline that includes the desired monitoring items and rules. Microsoft also provides SCCM configuration packs that

contain baselines for best practices and they can be directly imported to SCCM. Multiple baselines within clients can coexist, since clients report their compliancy per baseline. This provides administrators with higher level of control over the compliancy. When the clients evaluate their compliancy against the baseline, they immediately report it back to the site, or if they are not currently connected to the network, they will send the data upon reconnection.

In SCCM 2012, the compliancy settings can be divided into four categories: Regulatory compliance, pre- and post-change verification, configuration drift, and time to resolution [6]. Regulatory compliance is very important to some organizations such as those working in the health care industry and with the aid of SCCM regulatory standards can be enforced and reported. Pre- and post-change verification takes into account verifying the configuration of the system before and after planned changes in order to verify that the changes actually took place. Typical IT organizations usually don't take configuration drift into account on their network [6], but when a system goes live into production and multiple administrators/users start to configure it, it gradually starts to drift away from the original configuration state. Lastly, the time to resolution category focuses on identifying problems in the system and correcting them in a timely manner. SCCM does not remove these problem areas altogether, but it makes them more manageable through compliancy features.

## **4.8 Reporting**

SCCM reports are fully enabled for role-based administration and thus the contents of the reports are filtered based on permissions of the user who runs the report. Reports can be created from multitude of different type of information such as inventory, migration and audit information, client health, compliance and settings, OSD, virtual apps, Endpoint protection (antivirus) and administrative security. By default, SCCM 2012 hold over 469 premade reports that are added during installation, although customized reports can be created through SCCM console. The reports themselves can be run either from the SCCM console or the web-based Report Manager. Reports also allow subscriptions, so administrators can get reports automatically delivered via email or as file on a network share.

Reporting in SCCM 2012 uses SSRS (SQL Server Reporting Services) for reporting and thus the SSRS role needs to be installed before the reporting functionality in SCCM can be used. The SRSS can be installed on any primary site or CAS, but if CAS exists in the environment, it's considered best practice to install the role there [22].

## **4.9 Endpoint Protection**

Previously, SCCM 2007 allowed the ability to integrate Microsoft FEP (Forefront Endpoint Protection) 2010 into the system which allowed the administrators to manage and configure it through SCCM. In SCCM 2012, the FEP has been upgraded to SCEP (System Center Endpoint Protection) and the integration between SCCM and Endpoint protection is further enhanced. SCEP no longer uses two different databases to store data, but rather uses the SCCM site database to store all the data. SCEP agent is also included with the SCCM agent and no longer requires a separate deployment for its own agent. By default SCEP includes several customizable policy templates for providing recommended antimalware configurations for standard workload [22].

SCEP protects the underlying computer infrastructure by employing two policies: antimalware and firewall. The antimalware policy defines the antimalware settings that SCEP uses to block any malware and virus definitions, which include scanning schedules and types (quick vs. full), default actions when detecting malware, real-time protection, exclusions and multiple other more advanced configurations. The firewall policy is used to control and manage the Windows Firewall settings within the managed devices. Different policies can be applied for different profile types (domain/public/private). SCEP also allows for joining MAPS (Microsoft Active Protection Service), which is a cloud-based service that allows Endpoint clients to report data about programs exhibiting suspicious behavior to the Microsoft Malware Protection Center. Once the data has been analyzed and reviewed by Microsoft professional it can be later included in the new definition files that are downloaded to the clients.

In order to take advantage of SCEP, the Endpoint Protection Site System Role must be installed and configured. Along with the site server, the role must also be installed to the

CAS, if it exists in the hierarchy. If CAS is not present, the role has to be installed on the standalone primary site. Once the role has been configured the SCEP agent needs to be enabled. Even though the SCEP agent is distributed with the SCCM agent, it isn't actually installed nor activated before Endpoint Protection client is enabled in client settings policy.

SCEP is able to download new definition files automatically by using ADR and since SCEP definition files are updated several times a day [22], an automated solution will streamline the process for system administrators and reduce the time the clients are vulnerable to new threats

#### **4.10 Mobile device management**

The amount of computing power in mobile devices has steadily risen over the past years and this has led to an increasing amount of mobile devices even replacing traditional computers for users who don't need full-featured desktop applications but rather use mobile or web-based applications instead. Since the users are accustomed to using these devices in their personal time, they are starting to seek ability to bring their own devices to work environment. Thus, having a way to manage these mobile devices is crucial; be they user owned or not. Even corporate owned mobile devices are most of the time used for personal tasks outside work hours, so balancing between corporate security and user flexibility is a hard task. Even further challenge is the sheer number of platforms to support: different hardware manufacturers and form-factors, different Oses (Windows Phone, Windows RT, Android, iOS, Blackberry OS, Symbian, etc.) Each platform allows for different capabilities for management and they change and evolve constantly.

SCCM 2012, with the aid of Microsoft cloud-service *Intune*, is designed for bringing these mobile devices under a single management console. SCCM 2012 employs two types of management strategies for mobile devices: lite and depth management. Lite management doesn't install any client software and can be used with devices capable with Exchange Activesync connection (requires Exchange Server 2010 or 2013). Lite management is used for e.g. Windows Phone 7/7.5, iOS, Android and Blackberry OS devices. Depth management is used in traditional Windows Phone platforms, Windows CE, Windows Mobile and

Symbian devices. In depth management, client software is installed on the mobile device and this provides more capabilities than lite management. For older devices, a client application can be downloaded, but for newer devices (Windows Phone 8, newer iOS and Android) depth management can be achieved through Windows Intune connector [22]. So in essence, depth management can be achieved both through using client software or using Windows Intune. Support for different mobile platforms in SCCM 2012 is shown in table 10.

*Table 10. Mobile device management options in SCCM 2012 [22]*

<b>Platform</b>	<b>Management options</b>	<b>Features</b>
Android	<ul style="list-style-type: none"> <li>• Windows Intune connector</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Apple iOS	<ul style="list-style-type: none"> <li>• Windows Intune connector</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Nokia Belle Symbian	<ul style="list-style-type: none"> <li>• Direct via client</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>

Windows 8x / RT	<ul style="list-style-type: none"> <li>• Windows Intune connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Windows CE 5/6/7	<ul style="list-style-type: none"> <li>• Direct via client</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Windows Mobile 6.0/6.1/6.5	<ul style="list-style-type: none"> <li>• Direct via client</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Windows Phone 7.x	<ul style="list-style-type: none"> <li>• Direct via client</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>
Windows Phone 8.x	<ul style="list-style-type: none"> <li>• Windows Intune connector</li> <li>• Exchange connector</li> </ul>	<ul style="list-style-type: none"> <li>• Settings management</li> <li>• Software Distribution</li> <li>• Hardware Inventory</li> <li>• Remote Wipe/retire</li> </ul>

For Lite management, three prerequisites are needed: a device capable of establishing an ActiveSync connection with Exchange server, an Exchange Server 2010/2013 (on-premises or cloud-based), ActiveSync connector in SCCM 2012. The first requirement is quite self-explanatory; since Lite management relies on exchange ActiveSync, devices that can't establish such a connection out of management scope. Second requirement is solely and Exchange server issue, if the server can establish ActiveSync connections it is ready for SCCM purposes and doesn't require further configuration for integration. Configuring the ActiveSync connector, however, is an SCCM issue, but this can be easily configured from the Administration node in SCCM console (labeled as Exchange Server Connectors). It's also possible to configure multiple connectors per site.

For depth management, you can either install a client on a legacy mobile device or use depth management via Windows Intune connector. Depth management via client requires at least four roles: Enrollment proxy point site system role, Enrollment service point site system role, Management point configured for HTTPS (Hypertext Transfer Protocol Secure) and Microsoft enterprise certification authority. Depth management via Windows Intune has its own set of prerequisites: a Windows Intune subscription, configuring Windows Intune with organization's domain name, Synchronizing AD users with Windows Azure AD. Once the prerequisites are done, the users need to enroll the devices and the enrollment process differs for each mobile OS. Quite naturally, since SCCM is a Microsoft product, the broadest set of management features is available for mobile devices with Microsoft's OS (Windows Phone 8.x).

## **5 ANALYSIS OF CURRENT SCCM IMPLEMENTATION**

This chapter objectively analyses and presents the current SCCM implementation in Sulzer. Whether an area is designed good or bad is not taken into consideration here, but rather the system is presented “as is”. Detailed suggestions and improvement ideas are presented later on in chapter 7.

### **5.1 SCCM architecture**

Since Sulzer’s environment is quite large and in initial requirements, support for at least 25 000 clients and 160 locations worldwide was set, while designing the system for further scalability. This resulted in the SCCM architecture/hierarchy design including the CAS and placing primary site servers into main support locations: NSA (North and South America), EMEA (Europe, the Middle East and Africa) and APAC (Asia Pacific). The hierarchy is depicted in figure 6. The CAS is located in EMEA (Switzerland) and is used for central management, central reporting, application management and update synchronization. With this design, it is possible to control the communication between CAS and primary sites to avoid unnecessary replication traffic for DPs and client inventory data, by defining hours of communication.

A general blueprint of the 3-tier architecture can be seen in figure 7. On top-level is the CAS which also includes the reporting services, endpoint protection point, asset intelligence point (download asset intelligence catalog information from Microsoft) and the software update point that downloads the updates from Microsoft via internet. All the site servers also have software update point installed, but they download new updates from CAS rather than from Microsoft to limit the required WAN bandwidth. Each site server also act as a management point and hosts their own application catalog, although the content is same in each. This way clients always contact the application catalog from their parent site.

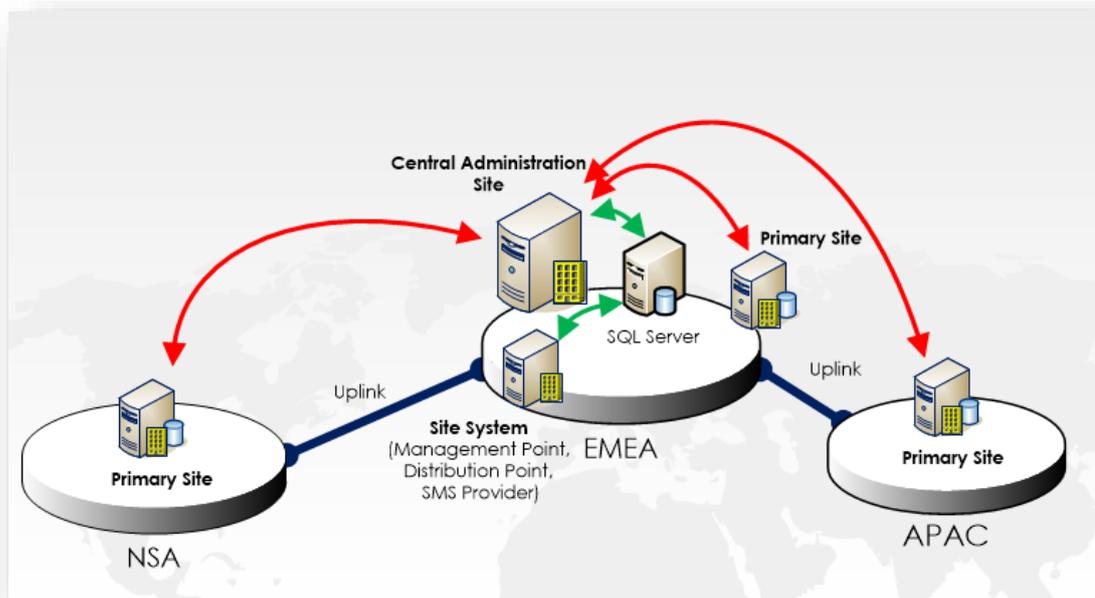


Figure 6. SCCM High-level architecture in Sulzer.

The architecture holds no secondary sites and instead DPs are used. Most major sites and offices have their fixed server-grade distribution points, but smaller offices connect to the closest fixed DP for all content. During the Windows 7 rollout, when massive amounts of machines are staged within a short period of time, mobile DPs (a standard desktop/laptop with Server 2008R2 and DP role) are used in remote locations for OSD and afterwards the location is configured to use the nearby DP. After rollout the mobile DP is moved to the next location or decommissioned. From SCCM perspective there is no difference between a standard fixed DP or a mobile DP, but in practice the difference is mostly in hardware, backups and reliability. Old, existing workstations are used for mobile DPs and no backups are configured for them.

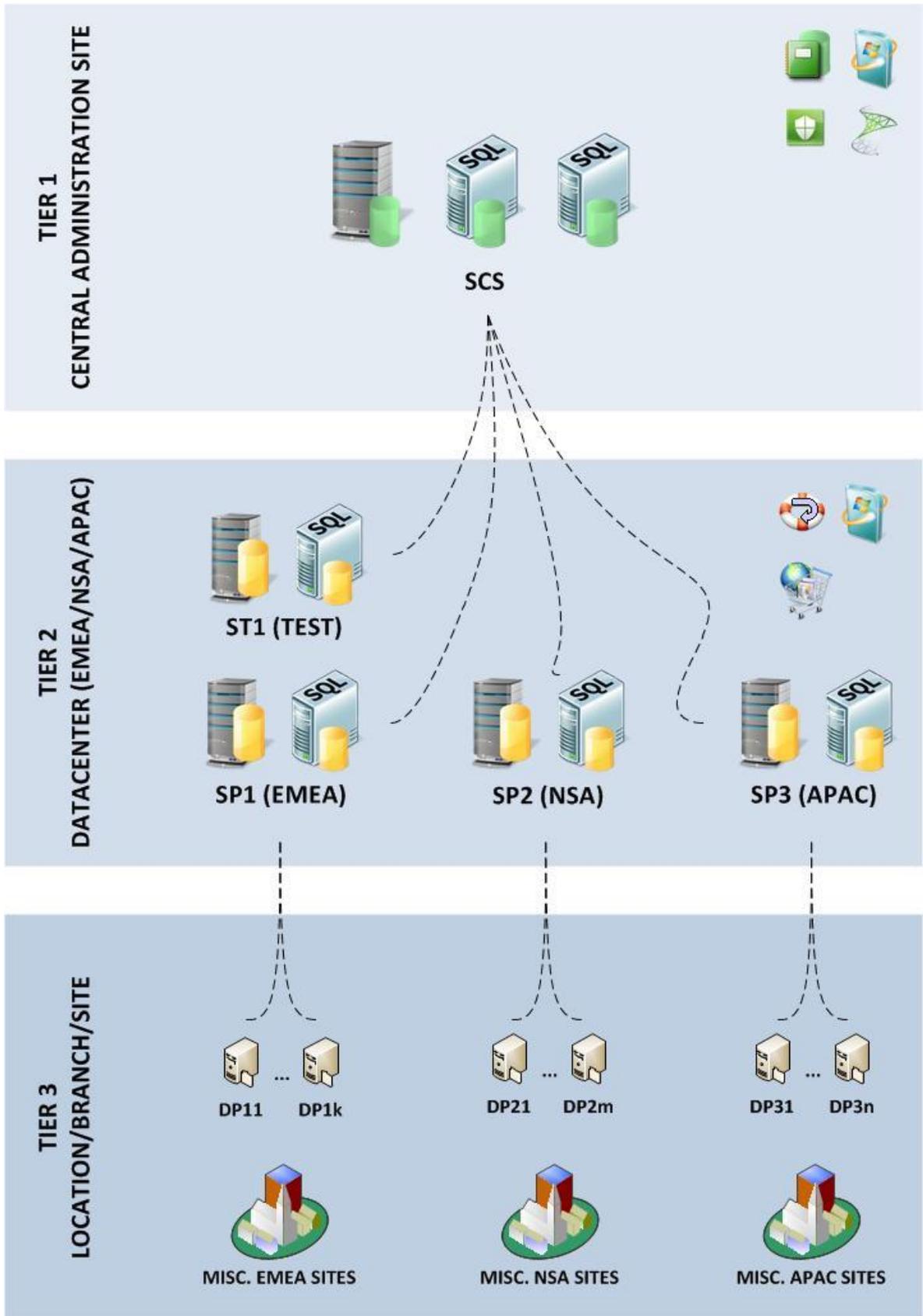


Figure 7. 3-tier SCCM architecture.

## 5.2 Supported Operating Systems

### 5.2.1 Windows 7

Currently, the only available OS for end-user computers is 64-bit Enterprise version of Windows 7. 32-bit version was considered as a parallel option, but was discarded due to management complexity of both 32-bit and 64-bit versions. Since almost all modern applications support 64-bit environment the only major downside is that 16-bit legacy applications do not work in 64-bit environment and this will prohibit those machines from migrating to Windows 7, until an update or workaround for a given application is found.

Since Microsoft dropped support for Windows XP in April 8<sup>th</sup>, 2014 [23] and will no longer provide any security updates nor technical support it is critical that computers will be updated with a newer OS. Windows 7 currently holds the market share when it comes to the desktop OSs, as shown in figure 8. Since Sulzer never planned to use Windows Vista and currently has no plans for migrating to Windows 8/8.1 yet, in practice this means either upgrading the machine to Windows 7 or replacing the machine with newer one, equipped with Windows 7. If the computer is upgraded, the OS is still installed as a “clean” install (meaning that the hard drive will be re-partitioned and formatted) instead of in-place upgrade. This is to ensure standard working environment for all computers across the domain.

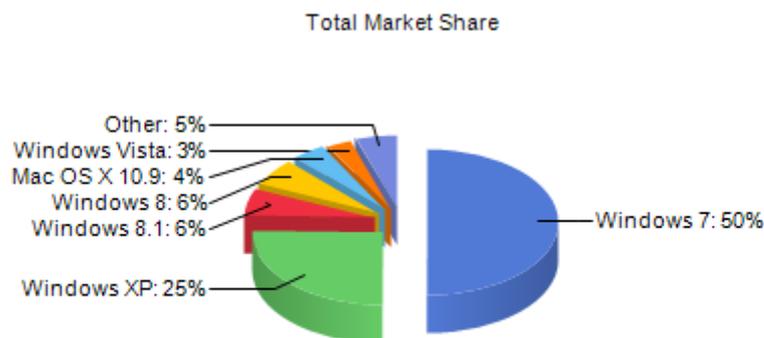


Figure 8. Desktop Operating System Market Share [24].

Windows 7 is a big step from Windows XP, both from a technical and user-experience perspective. Windows 7 came generally available already on 2009 [25] and is based on the Windows Vista core. Although they share the same core, Windows 7 has more streamlined interface and new features such as (but not limited to) libraries, file sharing system called HomeGroup [26] and virtual hard disk support [27]. User Account Control system was also modified in order to make it less intrusive, compared to Vista. Minimum hardware requirements for Windows 7 (64-bit edition) can be seen in table 11.

*Table 11. Minimum hardware requirements for 64-bit Windows 7 [28].*

Component	Minimum requirement
Processor	1 GHz x86-64 processor
Memory	2 GB
Graphics card	DirectX 9 graphics device with WDDM driver 1.0 (required for Aero)
Free Disk Space	20GB

### 5.2.2 Windows Server 2003 & 2003 R2

Windows Server 2003 is a server OS released back in 2003 and it is based on Windows XP but acted more as a follow-up to Server 2000. Server 2003 brought a better, enhanced AD compatibility to help migrating from Windows NT 4.0 to Server 2003 domain. The R2 version was released in 2005 which brought changes such as new features to branch office server management, identity and access management and storage management.

On July 2010 Windows Server 2003 (and related OS systems in the same family) were moved from mainstream support to extended support as per Microsoft Support Lifecycle Policy. During this phase, new security updates will still be rolled out but any free technical support, warranty claims and design changes are no offered any more. On July 2015, all support (including security updates) will be terminated. Since Server 2003 and 2003 R2 are end-of-life, no new installations are done in Sulzer and migration plans to newer server platforms are ongoing.

### 5.2.3 Windows Server 2008 & 2008 R2

Windows Server 2008 is the successor to Windows Server 2003 and is built based on the same code base used in Windows Vista and such it shares many of the same architectures and functionalities. Server 2008 also introduced a new variation of the installation, called *Server Core*, which is a scaled down version without any Windows Explorer shell installed, and it is managed either from the command line or by using remote management console. Primary benefit of using the Server Core is the reduced attack surface of the OS.

Server 2008 R2 is the server counterpart to Windows 7 and was released at the same time. It uses the same kernel as Windows 7 but unlike Windows 7, Server 2008 R2 is only available as 64-bit version and it is the first OS from Microsoft that is released as 64-bit only (later on followed by Server 2012 and 2012 R2). Server 2008 R2 has many new features such as Hyper-V, AD improvements (such as recycle bin for deleted AD objects), IIS 7.5 (Internet Information Service), many security enhancements and new Server Manager for role-based management tool. Core OS improvements include hot patching (allowing non-kernel patches to be applied without restarting the computer), dynamic hardware partitioning, support for hot-addition or replacement of memory and processors and being booted from EFI (Extensible Firmware Interface)-compliant firmware. Minimum system requirements for Windows Server 2008 & server 2008 R2 can be seen in table 12.

Table 12. Minimum hardware requirements for Windows Server 2008 & 2008 R2 [29].

Component	Minimum requirement
Processor	1,4 GHz x86-64 or Itanium 2 processor
Memory	512 MB (May limit some features), Recommended 2GB
Display	800x600 screen resolution or higher
Free Disk Space	32 GB

AD now supports Read-only DCs which hold non-writeable copy of AD and redirects all write actions to a full DC. These can be used in low security environments or branch offices.

The ADDS is implemented as Domain Controller Service and can now also be stopped and started without the need to restart the whole underlying OS.

#### 5.2.4 Windows Server 2012

Windows Server 2012 is the sixth release of Windows Server and is the server version of Windows 8 and became generally available to customers on late 2012 [30]. Like Windows 8, Server 2012 also includes the *modern UI* (User Interface), although it still includes the regular desktop UI as well. Windows Server 2012, unlike previous server editions, can be installed (or later switched) as Server Core or Server with a GUI (Graphical User Interface). Server Core includes a command-line interface only and can be used if no direct graphical access to the server is needed. This reduces the attack and patching surface of the server as well as the resource footprint.

Server 2012 includes a new version of Hyper-V, and come with new features such as network virtualization, multi-tenancy, storage resource pools, cross-premise connectivity and cloud backups. Many guest-related resource restrictions have also been lifted, and each virtual machine can now access up to 64 virtual processors, 1 TB of memory and 64 TB of virtual disk space per hard disk [31]. Minimum hardware requirements for Server 2012 can be seen in table 13.

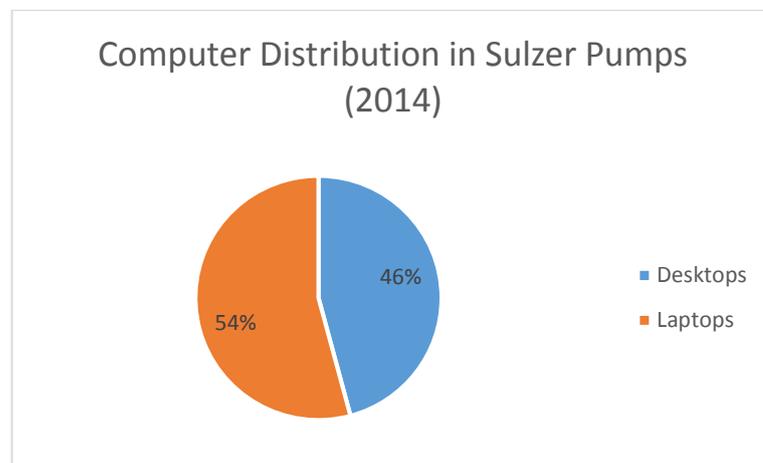
Table 13. Minimum hardware requirements for Windows Server 2012 [32].

Component	Minimum requirement
Processor	1,4 GHz x64
Memory	512 MB
Display	800x600 screen resolution or higher
Free Disk Space	32 GB

### 5.3 Supported Hardware

Currently Sulzer has a major deal with HP and thus HP is the standard manufacturer for computers used by Sulzer. Currently, regular meetings with HP are held to discuss

upcoming models and to form new internal standards for desktop, laptop and high-performance models. The use of laptops instead of desktops has become more common world-wide, and Sulzer is no different; currently Sulzer Pump's has more laptops in use than it has desktop computers, as seen in figure 9. The ratio of laptops vs. desktops also varies between support regions as depicted in figure 10 (data from Sulzer's AD, where each support region is located in its own OU). It should be noted that Finland's support region also covers Russia, Austria and partially Sweden and that WWS OU holds users from an integrated company that have not been yet fused into the existing regional structure (thus forming the biggest OU since it contains user and computers from multiple countries).



*Figure 9. Computer distribution in Sulzer Pumps.*

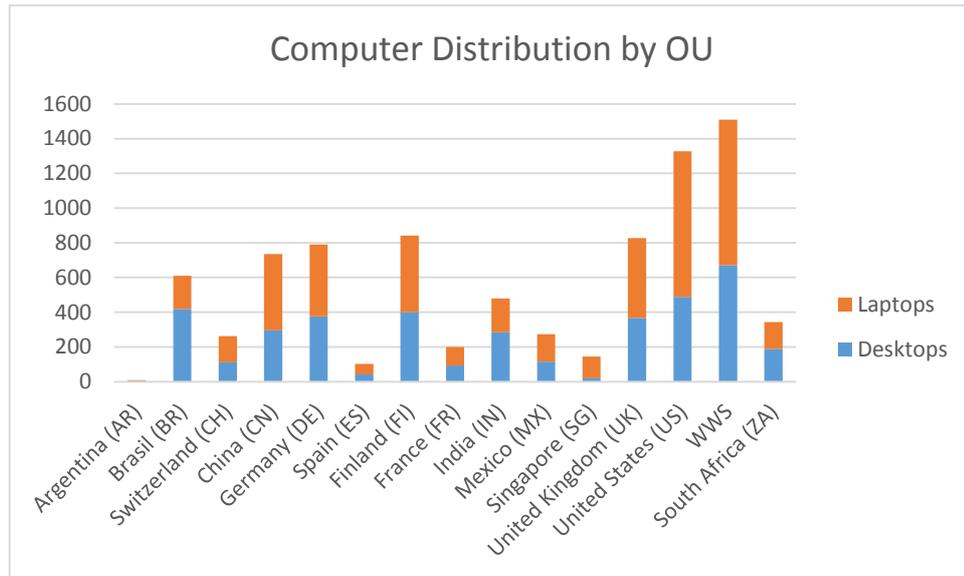


Figure 10. Computer distribution by OU.

## 5.4 OSD Process

Since Sulzer Pumps moved in to centralized management strategy, all OSDs are done through SCCM and currently only PXE-boot is supported (although using flash memory sticks and prestaged media are currently under consideration as parallel options). Previously regional offices had the freedom of choice for OSD (and for example in Finland, OSD was done by using PXE-boot but without SCCM). In its current implementation, assets are ordered through a web-portal, seen in figure 11, which sends the orders to SCSM (System Center Service Manager), where additional data is collected before the actual OS installation. At the web-portal, users select the model and amount they are about to install, and this creates the assets in SCSM, using running hardware IDs and computer names for the machines (desktop workstation names start with W and notebook names start with N). After this, the administrator will use the SCSM console to enter additional mandatory data to the assets; the minimum requirements are MAC (Media Access Control) address and primary user of the machine. After the required information is in place, the machine can be sent to staging and at that point, SCSM will retrieve additional AD attributes (such as preferred software profile, keyboard layout, OS language etc.) for the user account and send these the SCCM.

## Create Staging Assets for Stock

Display Name	Description	Status	Cost	Cost Currency
<input type="checkbox"/> <a href="#">HP Elitebook 9470m</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8570w</a>		Active	0.00	CHF
<input checked="" type="checkbox"/> <a href="#">HP EliteBook 8570p</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8560w</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8560p</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8540w</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8540p</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8530p</a>		Active	0.00	
<input type="checkbox"/> <a href="#">HP EliteBook 8470p</a>		Active	0.00	CHF
<input type="checkbox"/> <a href="#">HP EliteBook 8460p</a>		Active	0.00	CHF

↓

1 object selected (out of 70). HP EliteBook 8570p

Amount

*Figure 11. Asset portal.*

After the asset has been sent from SCSM to SCCM, the administrator will receive several emails into a shared mailbox: first message (start) informs that a staging process for a certain asset has started, second message will be either (ready) a message stating that the asset is now ready for installation and can be PXE-booted to start the OS installation or (failed) and error message, stating that there was something wrong with the asset (usually missing ad-attributes from the user account or faulty/duplicate MAC-address). Last, after the OSD has been completed and the TS has completed, a final (success) message will be sent to the mailbox, informing the administrator that the OSD is now completed and the machine can now be logged into. Any premature logging in will interrupt the TS and can lead to faulty configurations or missing applications on the machine.

Currently virtual machines have to be created manually in SCCM and then installed via PXE-boot. There is no automation in asset creation or getting the running numbers for new clients. Virtual machines can be only created by SCCM admins and they have to manually

check the next available computer name by checking current machine names starting with “V” from both SCCM and AD. Currently the number of SCCM-created virtual machines is quite low (less than 20) and they are all used for testing purposes.

During OSD, the hard-drive is re-partitioned and formatted, the core OS image applied (consisting of base Windows 7-installation with quarter-yearly updates applied, Adobe Acrobat reader X, Software Center, 3-Heights PDF assembler and Producer, 7-Zip, Java 7, Greenshot, Internet Explorer 9, KSOL ProjectReader and Windchill Creo View) and last the TS is run. The TS consists of multiple configuration options and installs the correct drivers (currently supported manufacturers are HP, IBM/Lenovo and Dell), based on the machine model and does OS and application tailoring based on the primary user. During the TS the computer’s BIOS will be updated, the computer joined to Sulzer domain and if it’s a laptop, Bitlocker will be enabled for extra security.

Currently, three windows hotfixes are installed during the TS (KB2775511, KB2732673 and KB2728738). After this, updates for the applications inside the core image are installed along with Teamviewer Quicksupport and for laptops, Cisco Any Connect VPN Client. After these global application installations, the software profiling takes place (based on primary user AD attributes), and depending on them additional software is installed or as in some cases, Java 7 is uninstalled and Java 6 is installed for application compatibility. Any language packs (OS and Office) are also installed if the AD attributes deviate from Standard English settings.

## **5.5 Application management and deployment**

Applications are deployed via SCCM in Sulzer but the approval process for applications or packaging them is not included in the scope of this research as it is done by the packaging team. Currently, there exists three layers of applications in Sulzer’s SCCM environment: core applications, division applications and role/profile applications. Core applications are installed for everyone and include software such as Adobe Reader and Flash, Java, App-V client etc. applications for everyday office use. Some layer 3 and 2 applications are deployed during OSD depending on the AD-attributes of the primary user and the rest have to be requested from Application Catalog. Software available for a given user depends on the

division he belongs to and certain AD-attributes include and exclude some specific applications as well. Some applications are also automatically pushed to client devices by using user and device collections, but the amount is still marginal.

The application catalog (shown in figure 12.) is available for all users. Currently several of the applications are available in English as well as German and they have to be requested even if the application doesn't actually require approval from anyone. This is due to integration implementation with SCSM and the actual requirement option is passed as administrator comment: {0} for no approval required, {1} for approval required and {2} if approval of two different persons are required. In case of no approval requirement, the request will be automatically approved, although it takes some time to complete all necessary steps in SCSM. In practice, getting an application ready for installation takes roughly around 30 minutes, finishing in email notification to user that the request has completed.

The screenshot shows the SCCM Application Catalog interface. At the top, there are navigation tabs: "Application Catalog" (selected), "My Application Requests", and "My Devices". Below the navigation, there is a "BROWSE BY" section with "Category" and "Publisher" options. The "All" category is selected. The main area displays a table of applications with columns for NAME, VERSION, PUBLISHER, and CATEGORY. The table shows four Microsoft Office applications.

NAME	VERSION	PUBLISHER	CATEGORY
Microsoft Office Professional Language Pack 2010 Turkish	14.0	Microsoft	Global Apps
Microsoft Office Visio Premium 2010 ENG	14.0.4763	Microsoft Corporation	Global Apps
Microsoft Office Visio Standard 2010 ENG	14.0.4763	Microsoft Corporation	Global Apps
Microsoft Project Professional 2010 SP1 ENG	14.0.6120	Microsoft	Global Apps

Figure 12. SCCM Application Catalog.

Most of the factory software and other special software are not available globally from the Software Center and they have to be installed traditionally (either manually or scripted) by local IT. Some of these applications are location and machine –specific and cannot be used elsewhere, some are for research purposes and thus won't be distributed – and some are used by only several people so the packaging, storing and distributing cost would not outweigh the benefits.

All applications that have licensing costs are required to have a line manager's approval, but also several free applications also require line managers and/or application owner's

approval. The end-user cannot see the price of the software or even know if it's free or not before requesting, and even after that the only indicator will be the approval process (automatic vs. approval) that is triggered. Even the line manager does not ever receive any indicator what is the price of the software license before approving the request.

Applications are missing descriptions and icons in the catalog and the naming convention on majority of the applications is rather obscure and sometimes even misleading (consider the application "Internet Explorer 9.0 Language Pack Finnish" which in fact is a language pack for Internet Explorer, but due to its requirements, it will install the language pack for Windows 7 (system wide) as well and change the whole OS language). Version numbering is also sometimes given in the name-field even though there is a separate field for version numbering (thus leading to duplicate information).

## **5.6 Endpoint protection**

Endpoint protection is now integrated into SCCM and is the antivirus and malware choice for everyone (previously local differences between regions may have existed). Quick daily and full weekly scans for clients are done and new definitions are downloaded automatically. Different policies exist for clients and servers (servers mainly have exclusions for scans) and they can be seen in figure 13. Default policies scan all drives (except mounted shares) and automatically quarantine any Medium, High and Severe threats found on client systems. Real-time monitoring on client systems is also enabled, and both incoming and outgoing files are scanned. Currently users cannot exclude any additional files or paths nor can they configure quarantine deletions in any way. A basic MAPS membership is used in Endpoint protection.

Icon	Name	Type	Order	Deployments	Description
	Default Client Antimalware Policy	Default	10000	0	Settings that apply to all clients in the hierarchy, and can be modified...
	Endpoint Protection Default Policy for Servers	Custom	2	1	Microsoft Endpoint Protection server role policy for general server wo...
	Exclusion - DPM Agents	Custom	8	1	Exclusion for Servers with DPM Agent
	Exclusion - DPM Servers	Custom	10	1	Exclusions for all Servers with System Center Data Protection Manager
	Exclusion - Exchange 2010 Servers	Custom	13	1	Microsoft Endpoint Protection performance optimized server role polic...
	Exclusion - Hyper-V 2.0 Servers	Custom	7	1	Exclusions for Servers with Hyper-V 2.0 Server Role
	Exclusion - Hyper-V 2.0 Siteservers	Custom	12	1	Exclusions for Siteservers with Hyper-V 2.0 Server Role
	Exclusion - SCCM 2012 Server	Custom	1	1	Exclusion for SCCM 2012 Server
	Exclusion - SCOM Agents	Custom	5	1	Exclusion for Servers with SCOM Agent
	Exclusion - SCOM Servers	Custom	6	1	Exclusions for Servers with SCOM Application
	Exclusion - SCSM Servers	Custom	15	1	Exclusions for Servers with SCSM Server installed
	Exclusion - SharePoint Servers	Custom	14	1	Exclusions for Servers with Sharepoint Server installed
	Exclusion - SQL Server	Custom	4	1	Exclusions for SQL Servers
	Exclusion - Sulzer Domaincontrollers	Custom	11	1	Exclusions for Servers with Domaincontroller and DNS Role
	Exclusion - VMM Servers	Custom	3	1	Exclusions for VMM Servers
	Exclusion - Windows Clustering	Custom	9	1	Exclusions for Servers with Windows Failover Clusters

Figure 13. SCEP Policies in Sulzer.

Automatic emails and reports are generated for found malware and they are sent to people responsible for malware security, although currently proper responsibilities are lacking since nobody is responsible for taking action on found malware threats.

## 5.7 Service Desk

Service Desk is now centralized for all locations and is implemented mainly via SCSM. Users that have a request or incident to file must open the web-portal and submit a ticket to the system with varying degrees of information. Depending on the category of the incident, the 1<sup>st</sup> level support will forward it to the correct solver group (2<sup>nd</sup> level support) and if they are unable to resolve the problem, it will be escalated to 3<sup>rd</sup> level support. Solvers get an email for ticket and they are able to track tickets targeted to them and their whole solver group by using SCSM console (available through Software Center). Sulzer has 3<sup>rd</sup> party support out-of-premises working as 1<sup>st</sup> line support, and internal workers as 2<sup>nd</sup> and 3<sup>rd</sup> level support.

## **5.8 Backups**

Currently, the backup procedures haven't changed from the pre-project state, which means that backups and backup procedures are handled locally (as well as user data migrations). This is due to not having a standard backup and user data protocols in place, since some places use Microsoft DPM (Data Protection Manager) for backups, some use folder redirection and just manage backups for the data storage (leaving clients without backups, since all critical user data should be on servers, and clients are easily re-installed in case of virus outbreak or system failure). Since the backup environment is vastly heterogeneous, analyzing each location becomes cumbersome and time consuming and thus will not be further analyzed until standard protocols and processes are formed for majority of locations. Driving those changes forward is also out of the scope of this research.

## **6 MICROSOFT SCCM BEST PRACTICES**

This chapter compares the current SCCM implementation analyzed in chapter 5 with official Microsoft best practices for SCCM 2012 published in Microsoft TechNet. Only best practices that have practical impact will be reviewed, so e.g. all best practices considering Mac and embedded computers will be left out as these do not exist in the environment on which this thesis focuses.

### **6.1 Application management**

Microsoft best practices for application management are:

- Use application supersedence to update deployed applications

In order to update an application, instead of modifying the existing application (where only the new deployments get the update) or by just deploying a newer version, application supersedence with upgrade or replace option should be used for better control of application updates.

In the current environment, the native supersedence options are not used, but the supersedence is set in the application wrapper (install.vbs) on case-by-case basis. Thus when deploying updates, the old versions' deployments are deleted and the new application is deployed to machines where the old version can be found. In each application, a branding key is inserted into Windows registry during installation, which is used as a detection method on computers. Depending on the application update, the old version is either uninstalled or upgraded (majority of times it is uninstalled).

### **6.2 Client deployment**

Microsoft best practices for client deployment are:

- Use software update-based client installation for AD computers
- Extend the AD schema and publish the site so that you can run CCMSetup without command-line options
- When you have many clients to deploy, plan a phased rollout outside business hours
- Enable automatic upgrade after your main client deployment has finished
- Use SMSMP and FSP if you install the client with client.msi properties
- If you want to use client languages other than English, install the client language packs before you install the clients
- Plan and prepare any required PKI (Public Key Infrastructure) certificates in advance – for Internet-based client management, enrolled mobile devices and Mac computers
- Before you install clients, configure any required client settings and maintenance windows

Microsoft recommends using a software update –based client installation for AD computers since it requires the least amount of configuration and is the most secure way of distributing the client. By extending the AD schema and publishing the site, additional command-line parameters can be omitted from the CCMSetup if the clients can retrieve them from AD. In order to minimize the processing requirements for the site server, the deployment of clients should be phased and in order to save bandwidth for critical business services, it should be done outside working-hours. After the deployment is made, automatic upgrading of clients should be activated. In order to all settings being available as soon as possible, all configurations should be done prior to deployment (but they can be done afterwards).

To remove dependencies on service solutions such as ADDS, DNS and WINS, the *SMSMP* property within client.msi can be used to configure the initial MP for the client. In the same manner the Fallback Status Point can be set via the FSP property to monitor the client installation.

In order to use other languages than English, the language packs should be installed prior to client installations, because otherwise the client needs to be reinstalled for the new languages to be available. In regards to mobile devices, this also means wiping the mobile device and enrolling it again.

In the current environment, the client is installed during OSD for all workstations, and it manually installed on servers. No internet-facing clients, mobile devices or Mac computers exist regarding PKI certificates.

### **6.3 Collections**

Microsoft best practices for collections are:

- Do not use incremental updates for a large number of collections
- Make sure that maintenance windows are large enough to deploy critical software updates

Microsoft recommends not use over 200 collections with incremental updates within the same hierarchy. The limit is not technical and the amount in reality depends on multiple factors such as complexity and size of hierarchy, size of collections, number of clients and the frequency of new resources being added or changed. When using large number of collections with incremental updates, it's possible that the collection evaluator will not be able to finish evaluating all the collections before the next incremental update is initiated (by default every 5 minutes). This will load the collection evaluator even more and increase the latency in collection updates.

If using maintenance windows, they should be long enough for all critical software updates to be able to install. If the maintenance window is always smaller than the critical update, it will never get installed on the system.

In the current environment, over 200 collections with incremental updates exist (most user collections). Maintenance windows are not currently used in application or update deployments.

### **6.4 Content management**

Microsoft best practices for content management are:

- Use source file location for packages that has fast and reliable network connection to the site that owns the package content source

When creating packages with source files, the site where the package is created will become the owner of the content source and the source files (specified for the package) will be copied to the content library on that site. Also when using the *Update Content* or *Update Distribution Point* actions, the files are copied again from the source to the package owner's content library. Thus the connection between the source files and the content owner should be fast and reliable.

In the current environment, all packages are created at the CAS and connection between the file repository and CAS is fast and reliable.

## 6.5 Reporting

Microsoft best practices for reporting are:

- For best performance, install the reporting services point on a remote site system server
- Optimize SQL Server Reporting Services queries
- Schedule report subscription processing to run outside standard office hours

SQL and reporting services is increased when the reporting services point is installed on a separate server rather than on the site server or remote site system. In order to optimize the SQL Server Reporting Services queries, tools such as Query Analyzer and Profiler can be used. If using report subscriptions, they should be scheduled to run outside normal working hours to minimize the resource load on the database server – this will also improve the availability for unpredicted report requests as there will be more resources available for processing them.

In the current environment, the reporting services is separated from other services and is installed as a stand-alone service to a site system (including the default component server and site system roles). Report subscriptions are not currently used.

## 6.6 Software updates

Microsoft best practices for software updates are:

- Use shared WSUS Database for Software Update Points
- When Configuration Manager and WSUS use the same SQL server, configure one of these to use a named instance and the other to use the default instance of SQL server
- Use a custom website for the WSUS installation
- Specify the “Store updates locally” setting for the WSUS installation
- Limit software updates to 1000 in a single software update deployment
- Create a new software update group each time an automatic deployment rule runs for “Patch Tuesday” and for general deployment
- Use an existing software update group for automatic deployment rules for Endpoint Protection definition updates

When using multiple SUPs (Software Update Point) at a primary site, a shared WSUS database should be used. This can drastically mitigate the client and network performance impact when clients switch to new SUP as the used database remains the same and the delta scan will be much smaller than if the WSUS server used a separate database.

When SCCM and WSUS use the same SQL server, one or the other should be configured to use a named instance to differentiate the applications from one another. This will make troubleshooting and diagnosing resource usage easier.

When installing WSUS, it should be configured to use a custom web site so the IIS (Internet Information Services) hosts the WSUS services in a dedicated website rather than sharing the same site with other SCCM site systems. During installation the setting *Store Updates*

*Locally* should be selected to ensure that software updates with license terms get distributed to all clients. Otherwise some clients might fail to scan for software update compliance on these updates.

When deploying software updates, the specified criteria shouldn't exceed 1000 software updates. In the same regard, a new software update group should be created each time automatic deployment rules are ran so the limit won't be surpassed. Contradictorily, Endpoint Protection definition updates should be always configured to use an existing software update group or otherwise, potentially hundreds of software update groups will be created over time due to definition updates getting updated very frequently.

In the current environment, there is only one SUP per site (total of 4) so sharing database between different sites is not an option. WSUS has been created as a custom IIS web site on all sites and thus HTTP (HyperText Transfer Protocol) traffic is configured for port 8530 and HTTPS for port 8351. The reporting services also use different SQL instance than the WSUS.

Per recommendations, no over 1000 software update deployments are made and new groups are made for all new update deployments. Separate, existing group is also used for Endpoint Protection definition updates.

## **7 SURVEY RESULTS & CHANGE RECOMMENDATIONS**

This chapter discusses both main research questions and presents the research's findings to them. RQ1: *“Is SCCM a suitable tool for Sulzer to centrally manage all computers in global scale?”* is answered by utilizing survey results for local management suitability and interviews with SCCM administrators accompanied with practical evaluation of the system for global management suitability. RQ2: *“What practical improvements can be done to the current system and what benefits can be achieved as a result?”* is fulfilled by comparing Microsoft best practices for SCCM with the current implementation and on top of that, finding areas where the system could be improved, taking into account Sulzer's environment and goals.

### **7.1 SCCM as a centralized management tool**

A survey considering the suitability of SCCM from a local IT support point of view was conducted during August 2014. Recipients were selected from major support sites within Sulzer Pump's division (Sulzer Chemtech hasn't started the integration yet, and Rotating Equipment Services is currently in the process of migrating to Sulzer-domain and under SCCM management). Out of 19 recipients, only 7 answered initially and after mid-deadline reminder 9 had answered it when the survey deadline occurred at August 31<sup>st</sup>.

The survey consisted both of scaled, fixed and open questions. The possible answers for scaled questions were fixed and ranged from 1-5 where the lower values represent change for the worse and higher values improvement with 3 being a “no-change” middle ground. Initial questions about the size of the support area were placed also, but no weight factor was put to the answers depending on the size of the answer's support region. Recipients were included from support regions all over the world, including North America, Europe, Asia and Africa (however no recipients from North America responded to the survey).

All responders' local IT teams were from 1-9 people, indicating that currently the local IT teams in any location are not that big, and generally the ratio between support personnel vs. supported client workstations was approximately 1:100. The ratio for supported servers on

the other hand varied quite a lot, from approximately 1:1 ratio to 1:100 ratio. Most of the locations that only have minor functions such as sales have only few servers, such as print & file servers (included in the same server) and SAP server, whereas bigger locations can have close to 100 servers. Respondents and their support locations are described in table 14 and table 15 depicts number of support personnel and supported devices for each respondent.

*Table 14. Survey Respondents*

<b>Respondent #</b>	<b>Region(s)</b>	<b>Cities</b>
1	Germany, Netherlands	(Unspecified)
2	Russia	Moscow, Khimki
3	India, Mumbai	Navi, Mahape
4	UK	Leeds
5	UK	Leeds
6	EMEA	Leeds
7	UAE, KSA	Abu Dhabi, Al Khobar
8	Finland, Russia, Austria, Sweden	(Finland all), St Petersburg, Wels, Malmö, Vadstena, Norrköping
9	UK, Norway, Africa	Leeds, Aberdeen, Glasgow, Bristol, Milton Keynes, Ashford, Sandnes, Nigeria

*Table 15. Support numbers for respondents.*

<b>Respondent</b>	<b>Size of local IT team?</b>	<b># of supported clients?</b>	<b># of supported servers?</b>
<b>1</b>	1-4	500-99	50-99
<b>2</b>	1-4	50-99	1-9
<b>3</b>	5-9	200-499	10-19
<b>4</b>	1-4	500-99	20-49
<b>5</b>	5-9	500-999	50-99
<b>6</b>	5-9	500-999	50-99

<b>7</b>	1-4	1-49	1-9
<b>8</b>	1-4	500-999	50-99
<b>9</b>	5-9	500-999	50-99

All respondents supported areas use HP computers only for clients and most used MDT for OSD before the SCCM rollout. The OSD process as an idea (one image for all, standardized software profiles) was accepted quite well, but in practice the process of installing a new operating system for a device was seen as slow and involving too many steps. The asset creation process was one reason why one location reported needing more resources after SCCM rollout than before, since the steps needed for successful OSD are more numerous and time consuming than before.

Applications were deployed mostly by scripts or manual installations and updates were rolled out using WSUS and GPOs. Most locations were happy with the idea of Application Catalog but the current process was seen as overly complex and hard, and not enough variety in the catalog to meet their needs, which results in manual installations by local IT. Also not controlling licenses is a problem, since licensed software is approved by line managers, but currently even they are not presented with the license/cost information, so most of the time they automatically approve users' request which increase license costs tremendously.

Client remote management was done mostly via Remote Desktop with some additional scripts in some locations. Client inventory was done via wsprop in most locations and by using AD queries in two locations. AD queries are still usable even after the SCCM rollout, but wsprop cannot be used anymore and since local administrators don't have access to the SCCM console or SCCM reports, they're left with less available information than before.

For antivirus, Microsoft Forefront Endpoint protections was used in all locations but also several other products were used as well, including Symantec (Norton) and Microsoft Security Essentials. Positive notes included the ability to limit CPU usage during scanning (although not configurable locally) but negatives included not being able to manage any of the settings (such as scanning time, exclusions, quarantined files etc.) locally.

Answers for scaled questions were gathered and calculated average between all regions for each question can be seen in figure 14. Even though that answers between each area varied quite a lot depending on the question (example: SCCM usability was rated 1 in a certain location and 5 in another) the overall theme between all questions is that not a lot has changed better or worse since the averages deviate from the midway (3) approximately by 0,5. Of course, as with all the other questions, it has to be taken into consideration that the sample size is quite small and the questions somewhat generic (which is one reason why the open questions were implemented – to dig deeper into the reasoning behind scaled questions’ answers).

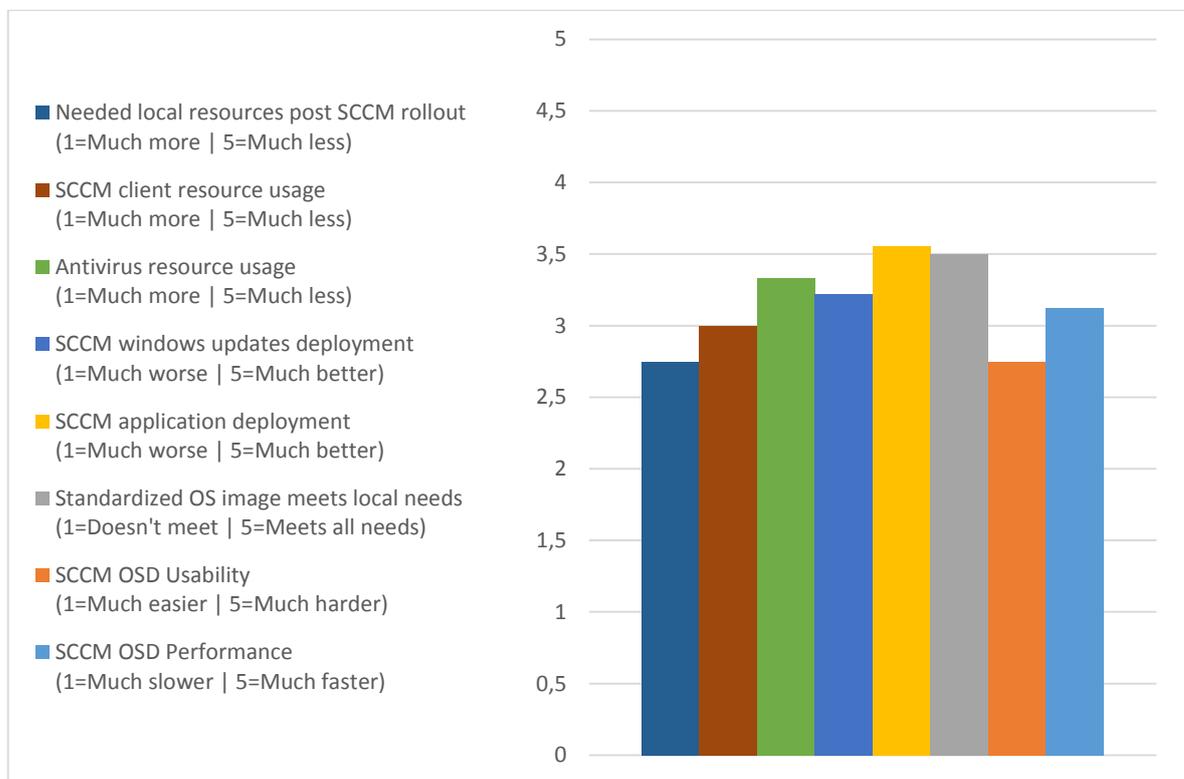


Figure 14. Survey answers from all recipients (averages).

One common problem with local IT departments seems to be the lack of communication from top-down and global IT not taking clear responsibility over the different areas of support regarding SCCM. One the reasons for this was that most of the daily operational tasks were carried out by a group of consultants who did the tasks per request, usually only accomplishing whatever was detailed in the service/change/incident request and nothing

more. From consultants' perspective, this is natural, since they're paid to do the tasks they're assigned and not take part in company politics or taking an initiative make the system better without someone assigning that to them. Steps to alleviate the situation has been taken and number of consultants has been dramatically reduced since and more is to be let go. The global plan is to shift all work done by externals to internal professionals and regarding SCCM the complete shift (100% internal work) is to take place in late September. This allows the organization to pin certain areas for specific people, so there's a clear line between a task or function and the responsible person. Currently the plan is to assign each SCCM area or tasks to one person who is responsible for it, but still have some overlap with other people so operational functions can continue even if the person absent. Main point focusing on the fact that if the person is available, he's the one responsible for making sure everything is running smoothly on the designated areas, whereas when he's away, rest of the people use "best effort" approach (routine functions get done, major changes are tried to be postponed if possible). When the system has been taken into internal hands, the line of communication from global IT to local IT is much clearer and ways to share knowledge and information in most efficient way should be implemented. Once this has been done the local IT departments should be able to make better use of SCCM.

From global administration point of view, SCCM gives a single tool to manage all computers within Sulzer network. The system is quite big, but so is the amount of devices to manage. During multiple workshops between the internal and external SCCM professionals in Sulzer in June-September 2014 it became clear that the system does work for global device management, but in order to be more efficient in doing that, certain changes need to be made. The initial plans and implementations were done for an environment where different divisions still resided in different subdomains and some of the original plans were abandoned mid-project, but the remnants still remain in the SCCM. Some legacy implementations even resided in production environment, such as creating and filtering application packages individually for each division (worst case scenario: having the identical package made and stored multiple times – once for each division).

## 7.2 SCCM Recommendations

### 7.2.1 Architecture

Although the architecture can be a bit overestimated for the environment (a single primary site can directly serve up to 100 000 clients), since it is already in production, it will be hard to change the underlying architecture and the benefits of doing so will be minimal. Additional distribution points can be set up and decommissioned quite easily, but removing existing primary sites would have a large negative impact. Also since there is one primary site per larger region (NSA, EMEA, APAC), it makes sense to distribute the primary sites geographically to avoid any network issues. Thus, recommendation for architecture is to keep the existing CAS and primary sites in place, but to try to simplify it in the future (not setting up additional primary sites). Re-design of the architecture can be reviewed if/when planning for the next major version of SCCM. Mobile distribution points are used in many locations especially during rollouts, but in some cases these have been left in-place – which is not desirable. If a location really needs its own distribution point, the decision should be made to set up a regular, on premise DP in that location, as mobile DPs are not designed for larger client-bases and continuous use. If a location no longer has real need for a MDP or DP, the MDP should be decommissioned.

### 7.2.2 OSD

The current OSD process is quite inefficient. Software is installed in the core image, updated during the TS and possibly again after the SCCM agent contacts the MP. Several Windows updates are also installed during the TS instead of implanted into the core image or pushing them via SCCM later like regular OS updates. Some of the software profiles cause Java 7 to be uninstalled (Java 7 is included in the core image) and Java 6 installed instead, rather than not including it in the core image and either installing the correct version or pushing it via SCCM after the OSD. Many factory and production machines don't even need these included applications and in some cases they even have to be manually removed before the machine can go live. Since the OSD is done on location and many offices don't have a dedicated installation rooms or the space is limited, cutting down the OSD time is highly beneficial (as it frees room for new machines). Switching application installations from

OSD to post-OSD gives an opportunity to ship the computer to a different location (such as us end user’s location) as well as powering it off and cutting it off the network, since a failed application installation will be retried later and it won’t break the system (unlike interrupting OSD). All recommendation regarding the OSD process can be seen in table 17.

Table 16. Recommendations for OSD.

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>O_01</b>	<b>Core image</b>	Bloated core image	Include only OS and OS updates	Streamlined OSD, possibility to use the same core image for factory and office users	Applications have to be installed during TS or after OSD
<b>O_02</b>	<b>Application installs</b>	Multiple software profiles inside TS	Push application installations via SCCM after OSD	Faster OSD process and machine can be shipped to user earlier.	Applications have to be installed after OSD, longer overall time for complete workstation with all required applications.
<b>O_03</b>	<b>Boot image</b>	Command support enabled	Command support enabled for debugging (case-by-case)	Better security during OSD, since currently during WinPE, a	Inability to capture and view logfiles and perform other troubleshooting during OSD from client

				Network Access Account is used to access the .wim file and credentials can be seen with command prompt.	machine until Command support is enabled.
<b>O_04</b>	<b>Bulk asset creation</b>	One-by-one asset creation	Enable mass-creation of assets simultaneously	Saves time to pre-fill the information on client end and importing the data vs. creating them at server-side one-by-one	Easier possibility to flood the system with multiple mass-imports.
<b>O_05</b>	<b>OSD method</b>	No USB-based installation	Locations with bad network connectivity could benefit from USB-based OS installations	Faster OSD in locations where the network connection would be the bottleneck	Increased complexity in OS-version control
<b>O_06</b>	<b>OSD method</b>	No .iso-based installation launch	Locations with bad network connectivity could benefit from bypassing	Higher success rate for OSD in locations with	None

			PXE and using an .iso file to start the OSD.	bad network connectivity	
<b>O_7</b>	<b>OSD Method</b>	No Prestaged media	Get computers from supplier with prestaged media	Reduce internal resources and time used for staging process	Increased cost, supplier needs possible infrastructure changes and up-to date image files.
<b>O_08</b>	<b>32-bit Win7</b>	No 32-bit image (and supporting TS) available	Research the need and possible benefit of creating a limited 32-bit Windows 7 support	Overcome the obstacle of migrating 16-bit XP devices to Windows 7	Need to maintain two productive images. All applications in environment (except for Office) are 64-bit by default
<b>O_09</b>	<b>Windows 8.1 / 10</b>	No plan for future Windows version support	Research and decide when and which future Windows OS is going to be implemented	Inevitable change – at the latest when Windows 7 support ends. Tablet support.	Need to support new and additional OS images and task sequences. Additional driver etc. support

### 7.2.3 Application management

The current application management and deployment process is working, but not nearly as well as it should and could. From end-users perspective, the application catalog can be intimidating and obscure to cipher. The naming convention used in the application names

comes directly from testing and packaging naming standards and conventions and are not that clear to the end-user. There's also no descriptions in any applications (what does it do, what's different in standard/premium versions etc.) nor pricing information. All applications show initially as "request needed", even though most freeware applications are automatically approved (this is due to the current integration method with SCSM, where all requests are converted into service requests in SCSM, where an automated workflow processes all application requests). Most of the time this is confusing for the end-users since they can't know if an application actually requires approval or not. Additionally, even when applications are automatically approved, it usually takes roughly 30 minutes since the user can install that application (and even then it is not automatically installed).

Due to the fact that pricing information is missing from both the application catalog and the application requests (that are send to the line managers), users request expensive software that they necessarily do not need and line managers around the world approve these requests, since they don't know the price and don't have the time to place inquiries about each request. [33]

The application catalog (and the SCCM backend) hold vast amounts of applications, some of which are very marginally used or at all. These eat up storage space, clutter the catalog and still have to be part of regular application life-cycle management. Thus, removing applications that are not really needed should be retired and removed.

Recommendations for Application management can be seen in table 18.

*Table 17. Recommendations for Application management*

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>A_01</b>	<b>Application Catalog</b>	Obscure descriptions	Use consistent, clear naming conventions	Better UI and usability	None

<b>A_02</b>	<b>Application Catalog</b>	Missing descriptions and icons	Include icons where possible and have a short description of the application	Better UI and usability for end-users	None
<b>A_03</b>	<b>Application Catalog</b>	Multiple unused or marginally used applications in the catalog	Remove unnecessary applications	Better UI, saved storage space and administration work	Removed applications are no longer available
<b>A_04</b>	<b>Application Catalog</b>	Freeware software needs to be requested	Make freeware applications available for installation without the approval process	Lighter load on back-end, better user experience, more clear application offerings.	None
<b>A_05</b>	<b>Application Catalog</b>	No pricing information	Include pricing information on applications that have licensing costs	Line managers have better knowledge when they approve/reject an application request. Application requesters can see the actual price of the	Hard to keep costs accurate since some license costs fluctuate or are part of bigger volume deal.

				software they are requesting.	
<b>A_06</b>	<b>Application Deployment</b>	Region- /department wide software have to be requested by all users	Use automatic boundary groups for pushing desired applications to correct groups	Better automation, less user time wasted	
<b>A_07</b>	<b>Application Deployment</b>	App-V not used	Create App-V packages for suitable applications	Isolated environment for running applications, better user experience across multiple devices	
<b>A_08</b>	<b>Application update</b>	Supersedence not used	Use supersedence on application updates	Better control over application updates.	None

#### 7.2.4 Update management

Currently, the client-side updates are rolled out via SCCM, whereas the server updates are still updated via other methods (mainly WSUS). No ADRs are currently used except for SCEP definition updates and monthly updates are reviewed before rolling out.. Recommendations for update management can be seen in table 19.

Table 18. Recommendations for update management

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>U_01</b>	<b>Automatic Deployment rules</b>	Not Used	Use ADR for security and critical updates for Windows 7 clients (excluding servers)	Automatically get the latest critical and security updates patched.	Possibility for installation of bugged or failure-causing updates
<b>U_02</b>	<b>Server Patching</b>	Not Used	Create a plan for patching servers	Standard procedures for patching servers	If poorly planned or implemented, can lead to incorrect patching on some critical servers

### 7.2.5 Reporting

Reporting via SCCM is currently heavily underutilized. There are some customized reports made, but most of the reports are standard reports made by Microsoft. Now that SCCM is rolled out for majority of locations and their old tools (such as wsprop etc.) are no longer in use, they're only good source for information about client devices is SCCM, but they don't have any access to SCCM console nor the web-based reports.

Table 19. Recommendations for SCCM Reporting

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>R_01</b>	<b>Web-Reports</b>	Local IT has no access	Allow local IT personnel access for web-based	Better tools for local IT support personnel	None

			reports to retrieve information on clients, software etc.		
<b>R_02</b>	<b>License reports</b>	Not used	Create license reports that suit the company needs and can be used by IT procurement.	Reports over used / available licenses give IT procurement more accurate data to act on when purchasing licenses.	None
<b>R_03</b>	<b>Custom reports</b>	Local IT doesn't have all required reports	Create custom reports tailored for local IT support	Local IT support gets the information they need from SCCM reports	None
<b>R_04</b>	<b>Reporting Services</b>	Optimization	Get better optimization data by running Query Analyzer and Profiler	Possible that the SQL Server Reporting Services is not properly optimized.	None
<b>R_05</b>	<b>Report subscription</b>	Report subscriptions not used	Plan and implement report subscriptions for desired services (such as malware alerts etc.)	Get automatic reports	More resources used

7.2.6 System & Sites

The current systems have been setup by external consultants and no additional reviews or major changes has been done after the initial setup. Discovery methods are reasonable (no network discovery, heartbeat and AD discoveries enabled), but the inclusion rules of them should be reviewed in order to optimize the results. Maintenance breaks or windows are not used for either site maintenance or client side installations (such as updates).

A vast amount of collections (mainly user collections) with incremental updates enabled were found and even the internal standard operating procedures instruct to enable these on all new user collections that are used for publishing applications to the application catalog.

No cloud based solutions are used, such as cloud-based DPs. Proof of concept was run previously but the results were inconclusive.

Recommendations for system and sites can be seen in table 20.

Table 20. System & site recommendations for SCCM.

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>S_01</b>	<b>Discovery methods</b>	Current discovery methods haven't been reviewed since creation	Review current discovery methods (AD)	Better, more thorough, or less resource consuming discovery methods might be available	Time used for reviewing
<b>S_02</b>	<b>Maintenance breaks</b>	No clear maintenance windows from system side have	Implement a maintenance schedule so end-users and local IT	Clearer communication between backend and users, less	None

		been declared	personnel know when the system service might be temporarily reduced or unavailable	service requests for downtime that was planned but poorly communicated.	
<b>S_03</b>	<b>Cloud services</b>	No could services (such as cloud based DPs) are used	Research the pros and cons of using cloud services in addition to current infrastructure	Saving infrastructure costs for small remote locations. Can reach clients outside company network.	Cost and moving data outside of company to 3 <sup>rd</sup> party.
<b>S_04</b>	<b>Collections</b>	Incremental updates are used in over 200 collections	Reduce the number of collections that use incremental updates	Better performance in SCCM.	Some collections might get less frequent updates
<b>S_05</b>	<b>Wake On Lan</b>	Wake On Lan not utilized	Enable WOL on each site and client machine	Better compliancy for all deployments when machines are within the network but turned off/sleep	Time consuming and complex to set up in global environment where currently each location manages their

					own networks.
<b>S_06</b>	<b>R2 Upgrade</b>	SCCM has not been updated to version R2	Upgrade from SP1 to R2	New features and fixes for existing bugs in current version.	Need to upgrade SCO, SCSM and SCOM to similar level. The current Application Approval Workflow is not supported in SCCM R2.
<b>S_07</b>	<b>Client installation</b>	CCMSetup requires command-line options	Publish client installation properties to ADDS	By locating the client installation properties from ADDS the command-line parameters can be omitted from CCMSetup installation.	None

### 7.2.7 *Miscellaneous*

Recommendations not fitting any specific category or when there was only a few items per category are grouped under *miscellaneous recommendations*, which can be seen in table 21. These include plan and research for mobile device management (currently doesn't exist in the environment).

Table 21. Miscellaneous recommendations for SCCM

<b>ID</b>	<b>Area</b>	<b>Problem</b>	<b>Change</b>	<b>Possible benefit</b>	<b>Cons</b>
<b>M_01</b>	<b>Mobile management</b>	No mobile device management implemented	Research the pros and cons of using Microsoft Intune and mobile device management	Increased security and management capabilities on mobile devices.	Cost and moving data outside of company to 3 <sup>rd</sup> party. Introduces another management layer for administrators
<b>M_02</b>	<b>Security</b>	Too many users with full access to SCCM	Remove full-administrator rights to SCCM from everyone except the actual SCCM administrators	Increased security and better traceability of changes made in SCCM.	Users who had full-admin rights can no longer access all the same features
<b>M_03</b>	<b>Administration</b>	Role-based administration is under-utilized	Use more granular role-based groups for users who require access to specific functions within SCCM	Increased security and better traceability of changes made in SCCM.	None
<b>M_04</b>	<b>Remote control</b>	SCCM Remote	Review and decide if the	Alternative tools for	Additional network and

		control features are not utilized	SCCM remote control features should be used or not.	remote management	firewall configurations, role-based permissions need to be set up and service desk needs to be allowed access to SCCM console
--	--	-----------------------------------	---	-------------------	---

## **8 IMPLEMENTED CHANGES**

This chapter discusses the change recommendations hand-picked from chapter 7 to be carried out during this thesis and evaluates their success (or failure) and impact on the system.

### **8.1 OSD**

The impact of OSD changes would've been critical before the Sulzer Pumps and RES divisions' rollout, as all client workstations were re-installed with the standard image within a short period of time, and thus saving even 10 minutes from the OSD process would result in approximately saving over 1600 hours of staging time. This, however cannot be converted into actual man-hours, since the installation is mostly unattended, but it would've still made a significant impact on the time and efficiency of the stagings. Doing the changes after the rollouts have a lesser impact, since in the future the installations will be more random until a new version of Windows needs to be mass deployed, or another division (such as Chemtech) is integrated.

#### *8.1.1 O\_01 Core image*

New core-image was designed to include only the Windows 7 OS, Microsoft office 2010, Management Framework 4.0 (latest that will be available for Windows 7) and updates both for Windows and Office. All application installations excluding Microsoft Office were removed from the core-image. Office was initially to be removed, but since installation of Office during the task sequence takes usually over 20 minutes, it was decided to be included in the core image to drastically cut down the OSD time.

This recommendation was implemented with minor changes. Achieved impact was medium and mostly administrative.

### *8.1.2 O\_04 Bulk asset creation*

The bulk asset creation feature was implemented partially during this thesis. Now the assets no longer have to be created one-by one, but staging personnel can fill an excel-sheet with correct machine-primary user linking, which can be uploaded to SCSM during the staging process. It is still necessary to send each asset to SCCM one by one from SCSM, but the process is much faster and efficient now. The showstopper for implementing the whole feature with automated asset creation was the current version and implementation of SCO (System Center Orchestrator) where by implementing the automated asset creation could've caused flooding of the runbook queues. The flooding can either halt the system or at least push out the oldest assets in the queue which are not yet staged.

This recommendation was partially implemented with plans for full implementation. Achieved impact of full implementation would be huge.

### *8.1.3 O\_06 OSD Method*

The .iso file used for booting can be easily captured from SCCM and used to bypass the PXE-boot in staging process. In some locations due to switch configurations or other unknown network problems it's easier to start the location by loading the boot-image from an .iso file by using a flash memory stick or CD/DVD. This process only skips the initial boot-image loading and all contents of the task sequence are still fetched from DP.

This recommendation was successfully implemented. Achieved impact was minor, since most locations can use PXE-boot.

## **8.2 Application management**

Changes to application management affect everyday use and the results can be seen both by administrators and end-users. The changes for end-users were refining the user-experience in the application catalog and for administrators better manageability and control was sought out.

### 8.2.1 A\_01 Application Catalog

The naming scheme from Application Catalog was changed for more user-friendly, by removing the version numbers from the name (since they are already in the version-field) and by removing publisher name from all products except Adobe, Autodesk and Microsoft. Also product names that didn't have any spaces between words were corrected and language version was redacted unless it was something else than the default English.

Example of changes can be seen in figure 15 (old catalog) and figure 16 (new catalog).

NAME	VERSION	PUBLISHER
 Autodesk Inventor View 2012 ENG	16.1.19000	Autodesk
 AutodeskInventorView2014 18.0.1660 ENG	18.0.1660	Autodesk
 Banana 6.0.8 ENG	6.0.8	Banana.ch SA
 BravaReader 7.2.0 ENG	7.2.0	Informative Graphics
 Calltime 8.02.2 DEU	8.02.2	Calitime AG, CH-6214 Schenkon
 CES-Selector2013 12.1.30 MUI	12.1.30	Granta Design Ltd. UK

Figure 15. Application Catalog before changes.

NAME	VERSION	PUBLISHER	CATEGORY	REQUIRES APPROVAL
 Autodesk Inventor View 2014	18.0.1660	Autodesk	Freeware	No
 Autodesk Product Design Suite Premium 2012 -Order	1.0.0	Sulzer	Licensed	Yes
 Banana	6.0.8	Banana.ch SA	Licensed	Yes
 Brava Reader	7.2.0	Informative Graphics	Freeware	No
 Calltime DEU	8.02.2	Calitime AG, CH-6214...	Freeware	No
 CES-Selector 2013	12.1.30	Granta Design Ltd. UK	Licensed	Yes

Figure 16. Application Catalog after changes.

This recommendation was successfully implemented. The impact was minor.

### 8.2.2 A\_02 Application Catalog

The missing icons were inserted to vast majority of applications. Some applications don't have any icons at all, since they are shell-extensions or the publisher never created any. The changes can be seen in figure 15 and figure 16. Description for applications are wanted, but currently it is unclear *who* will provide them and ensure they are accurate.

This recommendation was partially implemented with plans for full implementation. The current implementation's impact was minor.

#### 8.2.3 *A\_04 Application Catalog*

All freeware software was made available for users to install directly from application catalog without the need to go through the approval process.

This recommendation was successfully implemented. The impact was major from usability and time usage perspective.

#### 8.2.4 *A\_07 Application Deployment*

App-V was previously not used at all and currently an App-V package of Mozilla Firefox has been successfully deployed to pilot users. Plan is to start utilizing App-V more, especially with application with legacy dependencies in order to use isolated environments for them.

This recommendation was successfully piloted. The actual impact is still unclear, as with the testing no increase or decrease with performance, manageability or usability was noticed.

#### 8.2.5 *A\_08 Application Updates*

Currently supersedence is mostly implemented within the application wrappers (install.vbs) on case-by-case basis (whether to uninstall the previous version or not). For better transparency and management decision to move to using supersedence was made, as the status of applications' supersedence can be seen straight from the SCCM console (unlike the application wrapper).

This recommendation has been set in motion, but no meaningful data can be yet gathered on the impact yet.

## **8.3 Reporting**

Reporting changes focused currently on local IT administrators' issue of having no asset and monitoring data due to not having access to SCCM monitoring & reports after their old tools were decommissioned.

### *8.3.1 R\_01 Web-Reports*

Local regional and local IT-personnel were granted a read-access to web-based reporting services.

This recommendation was successfully implemented. The impact was major.

## **8.4 System & Sites**

Along with OSD changes, the system & site –wide changes will in theory have the biggest impact overall. Clear areas for change were found but rapid changes in large environments are not ideal and thus it is vital to test out the changes preferably in test environment or at minimum, by doing small increments in the system. Steps in the right direction were made, but any dramatic changes haven't been implemented yet.

### *8.4.1 S\_03 Collections*

Incremental updates were discovered to be enabled in over 200 collections which is even against Microsoft's best practices. Vast majority of these collections were user collections used for deploying software as "available" (Visible in the Application Catalog for users to install) and they made a query of "all users" discovered from AD. The queries for all users were changed to include the default "All users" collection, which itself has incremental updates enabled. When the "All users" collection updates itself, it will automatically update every collection that is limited by it and thus the user collections for available application deployments will automatically get updated. As per the recommendation cons, slight negative hit was noticed in the update frequency, as the collections are not updated that was.

However the overall update membership performance has increased (and for example, manually updating a collection is now faster).

This recommendation was successfully implemented, with slight negative impact. Future modification and/or fine-tuning is planned for this. The impact was medium.

#### *8.4.2 S\_06 R2 Upgrade*

A decision was made to move from SCCM 2012 SP1 CU3 (current version in use) to 2012 R2 CU3 (currently newest version available). Due to the high level of integration between SCO, SCSM, SCOM and SCCM, all versions are planned to be upgraded sequentially, following Microsoft's recommendation for System Center products' R2 upgrade [34]. Thus the products will be upgraded in following order: SCO, SCSM, SCOM and last SCCM.

Current showstopper for the R2 upgrade is the Application Approval Workflow Solution Accelerator [35] which doesn't work with R2 upgrade. There is a separate tool for R2, but this has to be tested before trying it out in production, since all application requests will be on hold for the time being.

Current plan is to setup a similar but simplified environment for upgrade testing with AD, SCCM and SQL servers and try out the R2 upgrade process there and the alternative approval tools. A DP and several test clients will be installed also.

This recommendation has been planned, but not yet fully implemented. Hardware has been acquired for the host machine and Server 2012 R2 has been installed with Hyper-V role. Guest OS's are Server 2008 R2 to make the environment similar to the one currently in use. The impact of the upgrade will be major.

## **8.5 Miscellaneous**

The implemented miscellaneous changes focused on security and administration, as mobile management and remote control features weren't something that could realistically be implemented during this research. Both implemented changes were successful.

### *8.5.1 M\_02 Security*

Full administration rights were removed from 13 user accounts and only the current real SCCM administrators were left with the permissions. Old accounts included mostly external consultants that were released after September, but also couple of internal user accounts.

This recommendation was successfully implemented. The impact from security perspective was major.

### *8.5.2 M\_03 Administration*

Role-based administration was increased after removing the full administration rights from all non-essential (from SCCM administration point of view) personnel. Permission groups for maintaining and administration specific areas (such as importing application from test environment to production, creating queries or managing specific collections) were implemented and taken into use. Creating these groups also allowed SCCM administrators to shift their workload to other staff personnel that are responsible for the target area (such as allowing application team to import new applications and packages and Exchange and AD team to manage Exchange and DC –specific collections and exclusions).

This recommendation was successfully implemented. The impact from security and administration perspective was between medium and major.

## 9 RESULTS

The present study was set to the task of systematically analyzing the SCCM system in Sulzer's global environment. As an outcome, the suitability of such system in Sulzer's environment for both local and global device and asset management and change recommendations for further optimization were desired. In order to fulfill the objectives of the first research question, a survey was sent to selected regional IT managers and local IT personnel from multiple countries and varying sizes of organizations. The second research question's objectives were fulfilled by analyzing the current implementation of SCCM in Sulzer and comparing it to the Microsoft's best practices (on areas where these best practices exist and are published by Microsoft) and aggregating new information in the form of change recommendations from these findings.

This chapter is set to not only discuss the findings along the lines with the research questions from presented in section 1.2, but also to prepare the finding for the concluding chapter of the research.

### **How well does the SCCM system perform against previous systems locally?**

Based on the survey results, multiple conversations with key IT personnel from variety of business locations, and from a multitude of service requests in the ticketing system, the SCCM system is something the local and regional IT can work with, but doesn't meet all their needs as well as their previous asset management solutions. Part of the reason is that the new system was mostly pushed in place, without giving any proper training or access for local IT to use the tools provided by the SCCM. From pure performance perspective, the SCCM system is slower when compared to most locations' previous products when it comes to common IT tasks such as OSD or application and update deployment. It was especially noted that the OSD process is now much more complex and slower compared to what the locations used to have (WDS, image cloning, and manual installation from customized media). So in essence, SCCM works on local scale, but not as good as it should or could. Most of the issues that were seen as step for the worse are not technical limitations, but rather the outcome of the processes that have been designed for these areas.

In order to make SCCM perform better on local level, proper training and access to at least reporting tools should be made available support IT personnel. It is also important to increase the level of communication and transparency between global and local functions in regards to SCCM.

### **How well does the SCCM system perform on a global scale?**

The performance and suitability of SCCM as a global asset management tool was analyzed from global administrator's perspective, keeping in mind the company's interest firstly and not just aiming to make administrators' jobs easier. Given that the global environment is mostly overseen by two operational administrators for SCCM it can be said that the system performs and is quite suitable in global scale with over 10 000 computer accounts and close to 20 000 user accounts in SCCM. The system is currently used to manage clients on all continents where Sulzer has business functions (which includes all other continents except Antarctica). In order to increase the performance and optimize the SCCM on global scale, a clear vision needs to be set regarding where the company wants to be in regards to SCCM in next couple of years and *what* (clients, servers, mobile devices, applications, updates, antiviral solutions, etc.) , it wants to manage with the product. This allows focusing on those key areas and not designing and progressing in the areas that are going to be abandoned down the road, as those resources could be directed for sustaining the core functionalities.

### **How does the current implementation of SCCM compare against Microsoft's "best practices"?**

Microsoft didn't have published Best Practices for every area of SCCM, but from those that existed, the ones that overlapped with areas in the current system were discussed and compared against the current implementation. The SCCM system in Sulzer was compliant with most Microsoft Best Practices for SCCM and those that deviated from the best practice were included in chapter 7's change recommendations. It should be noted that in the past Microsoft has reviewed the system and made suggestions to different areas, which were then changed – but the system was originally designed to keep the best practices in mind. Overall the current implementation is adequately compliant with the best practices, major difference being in overusing collections with incremental updates, and even making a standard

operating procedures for creating them in a scenario that happens quite frequently, thus producing ever increasing number of collections with incremental updates enabled.

**What specific areas in SCCM could benefit from practical changes in order to streamline the current asset management processes?**

Drawing from the previous research question, taking the uncompliant Microsoft Best Practice areas and by manually analyzing the system different change recommendations were created which were presented in chapter 7. From these change recommendations, several were hand-picked and implemented and their impact discussed in chapter 8. The recommendations spread over different areas and themes, such as performance, security and user experience. Since the system was analyzed for changes along with other research questions only during the timespan of this research, naturally all possible changes that the company could benefit from were not found, and only areas where beneficial changes were expected to be found were investigated. Naturally, the process for scanning and evaluating the system for beneficial change areas should continue in the future, and with each upgrade the configurations should be reviewed against the changes and/or new features presented with the new version.

## 10 CONCLUSIONS

The purpose of the present study was to analyze whether the Microsoft SCCM 2012 is a suitable tool for large, multinational organization and especially for Sulzer's environment. The study was carried by using literature review for scoping out the ideal environment and best practices, and by conducting a hands-on analysis of the existing system and producing practical change recommendations to optimize the system to better meet the needs of the company.

Based on the findings of the study, a set of conclusions was reached regarding the fitness of the product for local and global asset management and the overall consensus was that the SCCM 2012 as an asset management product is fit for the studied environment. However, several steps and actions should be taken to ensure optimal performance, administration, security and user experience (these steps were covered in chapter 7).

As a product, SCCM also has a future roadmap, since Microsoft has already released technical previews of some System Center products (VMM, SCSM and SCOM) [36] and technical preview for SCCM will be available in 2015. They have also already released information that the next version of SCCM will fully support Windows 10 and associated updates, and that SCCM 2012 R2 and SP1 will be receiving updates to ensure full Windows 10 support. SCCM 2007 SP2, R2 and R3, however, will be receiving updates that will ensure only Windows 10 management support (no deployment) [37].

## REFERENCES

1. Verma, D., Principles of Computer Systems and Network Management, Springer, USA, 2010.
2. Sulzer, Our Businesses, Chemtech, <https://www.sulzer.com/en/About-us/Our-Businesses/Chemtech>, retrieved 08.08.2014
3. Sulzer, Our Businesses, Rotating Equipment Services, <https://www.sulzer.com/en/About-us/Our-Businesses/Rotating-Equipment-Services>, retrieved 08.08.2014
4. Sulzer, Our Businesses, Pumps Equipment, <https://www.sulzer.com/en/About-us/Our-Businesses/Pumps-Equipment>
5. Sulzer, Sulzer Pumps Expand Technology Portfolio with Acquisition of Tartek Oy, Finnish Seal Manufacturer, <http://www.sulzer.com/en/Newsroom/Business-News/2013/131021-Sulzer-Pumps-Expands-Technology-Portfolio-with-Acquisition-of-Tartek-Oy> , retrieved 08.08.2014
6. Meyler, K., Holt, B., Oh, M., Sandys, J., Ramsey, G., System Center 2012 Configuration Manager Unleashed. Sams Publishin, USA, 2012
7. Weider, C., Technical Overview of X.500, RF 1309, <http://www.ietf.org/rfc/rfc1309.txt?number=1309>, retrieved 08.08.2014.
8. Microsoft TechNet, Active Directory Collection, <http://technet.microsoft.com/en-us/library/cc780036%28v=ws.10%29.aspx> retrieved 08.08.2014.
9. McHoes, A., Flynn, I., Understanding Operating Systems, 6<sup>th</sup> edition, Cengage Learning, USA, 2013.
10. Microsoft TechNet, Active Directory Team Blog, <http://blogs.technet.com/b/ad/archive/2013/04/15/welcome-to-the-active-directory-team-blog.aspx> retrieved 08.08.2014.
11. Koojimans, A., Kak, A., Crain, S., Crepinsek, A., Gadepalli, V., Hall, I., Value Realization from Efficient Software Deployment, IBM Redbooks, 2011.
12. Microsoft TechNet, Windows 7, Choosing A Deployment Strategy, <http://technet.microsoft.com/en-us/library/dd919185.aspx>, retrieved 08.08.2014.
13. Microsoft TechNet, Windows 7, High Touch with Standard Image, <http://technet.microsoft.com/en-us/library/dd919184.aspx> retrieved 08.08.2014.

14. Microsoft TechNet, Windows 7, Lite Touch, High-Volume Deployment, <http://technet.microsoft.com/en-us/library/dd919179.aspx> retrieved 08.08.2014.
15. Microsoft TechNet, Windows 7, Zero-Touch, High-Volume Deployment, <http://technet.microsoft.com/en-us/library/dd919178.aspx> retrieved 08.08.2014.
16. Praetorian, Regulatory Compliance, <http://www.praetorian.com/regulatory-compliance>, retrieved 08.08.2014.
17. Stackpole, B., Hanrion, P., Software Deployment, Updating and Patching, CRC Press, 2007, pp. 166-167
18. Microsoft TechNet, Security TechCenter, Microsoft Security Bulletin Advance Notification, <http://technet.microsoft.com/en-US/security/gg309152.aspx> retrieved 08.08.2014.
19. Tulloch, M., Perriman, S., Introducing Microsoft System Center 2012 R2: Technical Overview. Microsoft Press, USA, 2013.
20. Microsoft Licensing Datasheet, retrieved 24.6.2014  
<http://download.microsoft.com/download/1/1/1/11128EC7-2BE7-480C-9D46-4ECECA9E481A/System%20Center%202012%20Licensing%20Datasheet.pdf>
21. Microsoft TechNet, System Center, Choose Between Primary Sites, Secondary Sites and Branch Distribution Points, <http://technet.microsoft.com/en-us/library/bb693570.aspx> retrieved 08.08.2014.
22. Martinez, S., Daalmans, P., Bennett, B., Mastering System Center 2012 R2 Configuration Manager, John Wiley & Sons, USA & Canada, 2014.
23. Microsoft Windows, Enterprise, End of Support, <http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx>, retrieved 08.08.2014.
24. Netmarketshare, Desktop Operating System Market Share, <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>, Generated and retrieved 4.6.2014
25. Microsoft News Center, Windows 7 and Windows Server 2008 R2 Timelines Shared at Computex, <http://www.microsoft.com/en-us/news/features/2009/jun09/06-02steveguggenheimer.aspx>, retrieved 08.08.2014.
26. Microsoft Windows, HomeGroup, <http://windows.microsoft.com/en-us/windows7/products/features/homegroup>, retrieved 08.08.2014.

27. Paul Thurrot's Supersite for windows, Windows 7's support of VHD is all about backwards compatibility, <http://winsupersite.com/news/windows-7s-support-vhd-all-about-backwards-compatibility>, retrieved 08.08.2014
28. Microsoft Windows, Windows 7 system requirements, <http://windows.microsoft.com/en-us/windows7/products/system-requirements>, retrieved 08.08.2014.
29. Microsoft Windows Server, Windows Server 2008 System Requirements, <http://technet.microsoft.com/en-us/windowsserver/bb414778> retrieved 08.08.2014.
30. Microsoft TechNet blogs, Windows Server Blog, Windows Server 2012 released for manufacturing, <http://blogs.technet.com/b/windowsserver/archive/2012/08/01/windows-server-2012-released-to-manufacturing.aspx>, retrieved 08.08.2014.
31. Windows IT Pro, What are Windows Server 2012's scalability numbers?, <http://windowsitpro.com/windows-server-2012/q-what-are-windows-server-2012-s-scalability-numbers> , retrieved 08.08.2014.
32. Microsoft TechNet, Windows Server, Installing Windows Server 2012, [http://technet.microsoft.com/library/jj134246#BKMK\\_sysreq](http://technet.microsoft.com/library/jj134246#BKMK_sysreq) retrieved 08.08.2014.
33. Encompass Project Meeting, 29.8.2014 (Over Lync).
34. Microsoft TechNet, System Center, Upgrade Sequencing for System Center 2012 R2, <http://technet.microsoft.com/en-us/library/dns521010.aspx> , retrieved 30.10.2014
35. Microsoft TechNet, Application Approval Workflow Solution, <http://technet.microsoft.com/fi-fi/solutionaccelerators/hh875160.aspx> , retrieved 30.10.2014.
36. Microsoft TechNet, System Center, Release Notes for System Center Technical Preview, <http://technet.microsoft.com/en-us/library/dn806369.aspx> , retrieved 31.10.2014
37. System Center Configuration Manager Team Blog, Windows 10 enterprise management with System Center Configuration Manager and Intune, <http://blogs.technet.com/b/configmgrteam/archive/2014/09/30/windows-10-enterprise-management-with-sc-configmgr-and-intune.aspx> , retrieved 31.10.2014