

Abstract

Title: Centralizing security and operations of Windows clients in an emergency care IT infrastructure

Participants: Sondre Breivik, Erik Øhrling Sørli, Gaute Klakegg Dvergsdal

Supervisors: Christian Johansen

Employer Helsetjenestens Driftsorganisasjon for nødnett HF (HDO)

Contact person: Arnt-Helge Nilsen Øyan

Keywords: Configuration Manager, Centralized IT management, Endpoint Security, Windows Management, Emergency Service

Pages: 97

Attachments: 15

Availability: Open

Studypoints: 22,5

Abstract:

HDO is currently in a restructuring process, where they are procuring a new communication solution for the Norwegian emergency network. As part of their new solution, HDO will provide Windows client machines to locations involved in emergency services across Norway. This project group was tasked with creating a system to manage, operate and secure these client machines. The creation of this system involved thorough research into different approaches of managing Windows environments, where both experienced technical professionals and relevant literature were consulted. Specific system requirements like centralization of management abilities, automation of operational tasks and high availability of client machines informed the choice of the management solution. Best practices for security and industry standards for operations have been considered and implemented where it complies with the intended use cases of the system.

Microsoft's Configuration Manager was chosen to be at the center of this system, as it delivers on the required functionality and attributes needed to fulfill the conditions set forth by HDO. As a proof of concept, a domain environment has been created to show how security and operation is accomplished throughout the li-

fecycle of Windows client machines in the proposed environment. The domain environment demonstrates the process of automating the deployment of operating system images, applications and updates, as well as how to secure the clients using Configuration Manager, Active Directory and other security tools. The resulting system has taken all requirements specified by HDO to tailor a solution befitting their use case. A risk analysis focused on client security was completed, detailing the benefits of implementing the proposed system with its added security measures.

Sammendrag

Tittel: Sentralisering av sikkerhet og drift av Windows-klienter i en IT infrastruktur for nødnett

Deltagere: Sondre Breivik, Erik Øhrling Sørli, Gaute Klakegg Dvergsdal

Veileder: Christian Johansen

Oppdragsgiver: Helsetjenestens Driftsorganisasjon for nødnett HF (HDO)

Kontaktperson: Arnt-Helge Nilsen Øyan, arnt-helgenilsen.oyan@hdo.no

Nøkkelord: Configuration Manager, sentralisert IT-styring, Endepunktssikkerhet, Windowsstyring, Kritisk nødnett.

Antall sider: 97

Antall vedlegg: 15

Tilgjengelighet: Åpen

Studiepoeng: 22,5

Sammendrag:

HDO er i dag i en omstillingsprosess der de ønsker å anskaffe en ny kommunikasjonsløsning for det norske nødnettet. Som en del av deres nye løsning, vil HDO sende ut Windows klienter til lokasjoner knyttet til nødnettet, rundt omkring i Norge. Denne prosjektgruppen fikk i oppgave å lage et system til å styre, operere og sikre disse klientene. Opprettelsen av dette systemet har involvert en grundig analyse av vidt forskjellige måter å håndtere Windows-miljø, hvor både erfarne teknikere og relevant litteratur har blitt rådført. Spesifikke systemkrav som sentralisering av styrings-muligheter, automatisering av operasjonelle oppgaver og høy tilgjengelighet hos klientmaskinene, har vært veiledende for valg av styrings-løsningen. Bestepsikiser og industristandarder innen sikkerhet og drift har blitt vurdert og implementert hvor det er hensiktsmessig innenfor det tiltenkte bruksområdet for systemet.

Styringssystemet Configuration Manager fra Microsoft ble valgt som en sentral del av dette systemet, siden det oppfyller kravene for funksjonalitet og egenskaper fremsatt av HDO. Som konseptbevis er det blitt opprettet et domenemiljø for å demonstrere hvordan sikkerhet og drift blir håndtert gjennom livssyklusen til en

Windows klient i den foreslåtte løsningen. Domenemiljøet demonstrerer prosessen av å automatisere utrulling av operativsystem bilde-filer, applikasjoner og oppdateringer, i tillegg til hvordan klienter sikrest ved hjelp av Configuration Manager, Active Directory samt andre sikkerhets-verktøy. Sluttproduktet er et system som har brukt samtlige spesifikasjonskrav fra HDO til å skreddersy en løsning for deres bruksområde. Det er også gjennomført en risikoanalyse med fokus på klient-sikkerhet, hvor fordelene ved å implementere det foreslåtte systemet, med tilhørende sikkerhetstiltak, blir fremhevet.

Preface

This project has benefited from several contributions in a number of areas. We would therefore like to give thanks to those who provided us with useful technical information and advice in writing and structuring the thesis. We would also like to thank our client, HDO, for trusting us with this exciting and challenging assignment, and especially Arnt-Helge, for giving generously of his time to meet with us and discuss the project.

A special thanks goes out to Christian Johansen, for guiding us through the writing process and giving valuable insight along the way. And finally, we thank our fellow students Christian Isnes and Gjert Michael Torp Homb, for providing us with access to their vSphere platform.

Contents

Abstract	iii
Sammendrag	v
Preface	vii
Contents	ix
Figures	xiii
Tables	xv
List of Listings	xvii
Acronyms	xix
Glossary	xxiii
1 Introduction	1
1.1 Background	1
1.2 Project description	2
1.2.1 Project Goals	2
1.2.2 Restrictions and constraints	2
1.2.3 Learning objectives	3
1.3 Target audience	3
1.4 Own background and competence	4
1.4.1 Roles	4
1.5 Project management process	5
1.5.1 Tools	5
1.5.2 Method and approach	5
1.5.3 Source evaluation	6
2 Tools and technologies	8
2.1 Deployment and management environment	8
2.2 System Management	9
2.2.1 Modern vs traditional	9
2.2.2 Choice of System Management	13
2.2.3 Configuration Manager Features	13
2.3 Remote support	15
2.3.1 TeamViewer	16
2.3.2 Microsoft Remote Assistance	17
2.3.3 Remote support choice	17
2.4 Supporting features	17
2.4.1 Virtualization platform	17

2.4.2	DHCP	18
2.4.3	PowerShell	18
2.4.4	BitLocker Drive Encryption	18
2.4.5	Active Directory	18
2.4.6	Group Policy Object	19
2.4.7	Image deployment	19
2.4.8	PXE-booting	20
2.4.9	Windows Deployment Service	20
2.4.10	Caching	21
2.4.11	Caching solution	22
2.5	Technical Obstacles	22
2.5.1	Swap in virtualization platform	22
2.5.2	Misconfiguration within VMware Vsphere	23
3	System implementation and operational concept	24
3.1	Demo Environment	24
3.2	Implementing Configuration Manager	25
3.2.1	Installation	25
3.2.2	Initial Configuration	31
3.2.3	OS deployment	36
3.3	Enable PXE	37
3.4	Deploying client images with SCCM	38
3.4.1	Installing new clients	39
3.4.2	Reimaging clients	44
3.4.3	BitLocker	45
3.4.4	Troubleshooting	45
3.5	Microsoft Remote Assistance	46
3.6	Update Management	47
3.6.1	Preliminary update catalog maintenance	47
3.6.2	Deploying software updates	48
3.6.3	Automatic Deployment Rules	49
3.6.4	Additional Update Features	52
3.6.5	Disable Windows Update	53
3.7	Application management	53
3.7.1	Deploying an application	54
3.7.2	Obstacles	54
3.8	Caching	54
3.8.1	Peer Cache	55
3.8.2	Requirements	56
3.8.3	Multiple peer cache sources	56
3.8.4	BranchCache	57
3.8.5	Caching effectiveness	57
4	Securing the Windows workstation environment	59
4.1	Endpoint Protection	59
4.1.1	BitLocker	59

4.1.2	Antimalware policy	62
4.2	Security Baselines	63
4.2.1	Security Technical Implementation Guides	63
4.2.2	Creating STIG GPOs	65
4.2.3	Windows Security Baselines and Policy Analyzer	66
4.2.4	Configuration Baselines	67
4.3	Local Administrator Password Protection	68
4.4	Password policy	73
4.5	Password Filters	74
4.5.1	Azure AD Password Protection	75
4.5.2	Anixis Password Policy Enforcer	76
4.5.3	Password filter selection	76
4.6	On-premise Azure Active Directory Password Protection	76
4.6.1	Deployment requirements	76
4.6.2	Installation	77
4.6.3	Verification	77
5	Monitoring	79
5.1	Client Health Status	79
5.1.1	Ping client machines	80
5.1.2	CCMeval checking client health	81
6	Risk analysis	84
6.1	Executive summary	84
6.2	Scope	84
6.3	Methodology	85
6.3.1	Probability and consequence matrices	85
6.3.2	Criticality matrix	85
6.4	Assessments	86
6.4.1	Assets	86
6.4.2	Existing controls	86
6.4.3	Vulnerability Assessment	87
6.5	Risk analysis	88
6.5.1	Risk scenarios	88
6.6	Accepted risk	93
7	Conclusion	94
7.1	Results	94
7.1.1	Reflection and evaluation	94
7.2	Further Work	95
7.2.1	MDE	96
7.2.2	Intune with Configuration Manager	96
7.2.3	Enable PKI for configuration manager	96
7.2.4	Windows Defender Credential Guard	96
7.2.5	Fix Reporting services	96
7.2.6	Continue Risk Analysis	97
	Bibliography	98

A	Prosjektplan	106
B	Prosjektavtale	124
C	VB script	128
D	1. SQL script	131
E	2. SQL Script	135
F	Software Update Maintenance - Script	138
G	Read Ccmeval result	139
H	Risk Matrices	142
	H.1 Consequence matrix	144
	H.2 Probability matrix	146
I	Dialog with Erik Hjelmås regarding translation of Matrices	147
J	STIG GPO's overview	148
K	Altered Policies	183
L	Notes from meetings with HDO	185
M	Timeføring med Toggl -Sondre	195
N	Timeføring med Toggl -Erik	197
O	Timeføring med Toggl -Gaute	199

Figures

2.1 PXE booting infrastructure example	20
3.1 Visual representation of lab environment	24
3.2 Required disk partitions	25
3.3 Inbound firewall rule "SQL"	26
3.4 SQL server properties	27
3.5 Windows Server Update Services (WSUS) server role	28
3.6 WSUS IIS change	29
3.7 AD extension logs	30
3.8 System management AD container	30
3.9 Database size toward the end of the project	31
3.10 The roles not highlighted were automatically installed during the installation of Microsoft Endpoint Configuration Manager (Config- uration Manager)	32
3.11 Site system role wizard	33
3.12 Specifying Service account for Client Push	34
3.13 SCCM settings GPO	34
3.14 Boundary with Groups	35
3.15 System Discovery	36
3.16 Open ports for PXE-booting	37
3.17 Choose Task Sequence in WinPE	38
3.18 Task Sequence New client tasks	39
3.19 Task Sequence: Join OU	40
3.20 Task Sequence: Setting site code	41
3.21 Task Sequence: Pass parameters to embedded PowerShell	42
3.22 Task Sequence Migrate settings	44
3.23 Task Sequence Reimaging tasks	45
3.24 Task Sequence BitLocker	45
3.25 Before cleanup	48
3.26 After cleanup	48
3.27 Software Update Group structure example	49
3.28 Workstation Updates ADR	50
3.29 Compliance view of a "Critical Update"-deployment	51

3.30	This notification will show up every 10 minutes after deadline, in the middle of the screen	52
3.31	The highlighted option was removed.	53
3.32	Detection method for Firefox	54
3.33	Creating Custom Client Settings for Peer cache.	55
3.34	Creating Custom Client Settings for Peer cache.	55
3.35	CAS log used to check if peer cache source was used.	56
3.36	Peer cache.	56
3.37	Client content sources last seven days.	58
4.1	BitLocker in Endpoint Protection	60
4.2	MBAM log file	61
4.3	Registry key to enforce BitLocker.	61
4.4	enforced BitLocker on a client machine.	62
4.5	Antimalware file quarantined by Windows Defender	63
4.6	STIG Viewer group policy setting example for Windows 10	64
4.7	STIG GPO Support files	65
4.8	Policy Analyzer	66
4.9	Importing Group Policy Object (GPO)'s as Configuration Items	68
4.10	New computer-objects attributes	70
4.11	Local Administration Password Solution (LAPS) password settings.	71
4.12	Shows the only needed feature of the installation package.	71
4.13	The LAPS Configuration Manager Application-package included in the provisioning Task Sequence (TS)	72
4.14	LAPS User Interface.	73
4.15	Azure Password Protection workflow [78]	75
4.16	Successful enforcement of Azure password policy	78
5.1	Client health dashboard	79
5.2	Output from Read-ccm.ps1	83
6.1	Criticality matrix from Helsetjenestens driftsorganisasjon for nød-net (HDO).	86
H.1	Consequence matrix from HDO.	144
H.2	probability matrix from HDO.	146
I.1	Dialog with Erik Hjelmås.	147
J.1	List of GPOs	149
J.2	172
J.3	176
K.1	184

Tables

4.1	Table displaying excluded GPO's	65
6.1	Existing controls in domain environment.	86
6.2	Vulnerability	87
6.3	Risk matrix before mitigation's.	92
6.4	Risk matrix after mitigation's.	93

List of Listings

3.1	Powershell: Installing prerequisites	26
3.2	Powershell: Create service user	26
3.3	PowerShell: Create .WIM file	37
3.4	Change hostname with embedded PowerShell in TS	42
3.5	Set hostname with package	43
5.1	Part one: Ping Client machine	80
5.2	Part two: Ping Client machine	81
5.3	Send ccm report	82

Acronyms

.WIM Windows Imaging Format. 20, 36, 37

AAD Azure Active Directory. 75–77

AD Active Directory. 17, 18, 26, 29, 30, 35, 41, 43, 68, 69, 74, 76, 77, 85, 86

AD DS Active Directory Domain Services. 15, 39, 41, 74, 76, 85

ADK Assessment and Deployment Kit. 29

ADR Automatic Update Rule. 49, 50, 52

BITS Background Intelligent Transfer Service. 25

BYOD Bring Your Own Device. 12

CLI Command Line Interface. 10

CMC Configuration Manager Client. 14, 15, 33, 34, 96

CMD Command Prompt. 14

Configuration Manager Microsoft Endpoint Configuration Manager. xiii, xiv, 8, 11–15, 19, 21, 22, 24–27, 29–32, 34–37, 39–41, 44–49, 52–57, 59, 63, 65–67, 71, 72, 79–82, 84–86, 88, 94–96

ConOps Concept of Operation. 2, 94

DC Domain Controller. 18, 25, 30, 35, 69, 76, 77, 85

DHCP Dynamic Host Configuration Protocol. 18, 20, 22, 23, 37

DISA Defense Information System Agency. 63

DoD Department of Defence. 63

DOS Denial of Service. 90

DP Distribution point. 15, 21, 37

EP Endpoint Protection. 59, 60, 62

EXE executable. 54

GPO Group Policy Object. xiv, 3, 17–19, 53, 57, 63, 65–68, 70, 86, 87, 94, 96

GUI Graphical User Interface. 10, 14

HDO Helsetjenestens driftsorganisasjon for nødnet. xiv, 1–3, 6, 8, 13, 15–17, 19, 21, 40, 41, 47–49, 52, 54, 68, 84–86, 88, 91, 93–96

IAM Identity and Access Management. 75

ISP Internet Service Provider. 3

IT Information technology. 1–3, 16, 17, 46, 48, 85, 91, 94

LAPS Local Administration Password Solution. xiv, 29, 68, 69, 71–73

LTD lite-touch deployment. 19

MDATP Microsoft Defender Advanced Threat Protection. 59

MDE Microsoft Defender for Endpoint. 59, 96

MDT Microsoft Deployment Toolkit. 12, 14, 19

MVP Microsoft Most Valuable Professional. 7

NBP Network Boot Program. 37

NIC Network Interface Controller. 20

NIST The National Institute of Standards and Technology. 74

OS Operating System. 10, 12, 14, 19, 20, 29, 36, 38, 39, 44, 45, 47, 53, 55, 91

OU Organizational Unit. 15, 18, 35, 39, 44, 57, 70

PP Azure AD Password Protection. 74–77

PXE Preboot Execution Environment. 18, 20, 22, 23, 37, 38

RDP Remote Desktop Protocol. 91

RSAT Remote Server Administrator Tools. 41, 43

SCCM System Center Configuration Manager. 11

- SCT** Security Compliance Toolkit v1. 66
- SID** Security identifier. 68
- SPN** Service Principal Name. 26
- STIG** Security Technical Implementation Guides. 63–66, 74, 94
- SUG** Software Update Group. 49
- SUP** Software Update Point. 32, 47, 52
- TFTP** Trivial File Transfer Protocol. 20, 37
- TS** Task Sequence. xiv, 14, 15, 37–41, 43–46, 71, 72, 92
- WAN** Wide Area Network. 21, 56
- WDS** Windows Deployment Service. 20
- WIP** Work in progress. 5
- WSUS** Windows Server Update Services. xiii, 21, 25, 27–29, 32, 47, 96
- ZTD** zero-touch deployment. 19, 38

Glossary

attack surface All the different points where an attacker can gain unauthorized access to a system and or assets.. 59

Azure Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.. 3, 76

bare-metal provisioning The process of installing an Operating System directly on computer hardware.. 10

integrable Applications that are able to integrate its controls in other software.
8

Microsoft Bitlocker Administration and Monitoring MBAM is an interface that simplifies how to manage and administer BitLocker Drive Encryption. This interface also enables monitoring of client compliance with new BitLocker Drive Encryption policies. 61, 62

OpenStack A cloud computing platform.. 17

Out-of-band A software update, usually a security update, that arrives outside of the "normal" patch-schedule(e.g. Patch Tuesday).. 52

pass-the-hash attack A form of attack where the attacker has gained hold of password-hashes, and uses the hash instead of the password to authenticate against a system. . 88, 96

password manager Encrypted "vault" that stores login information. 68

password spray attack Automatic recording and transmission of data from a remote site to another, for analysis and monitoring. 75

peer-to-peer peer-to-peer networking are a network created when two computers share resources without talking to a server.. 21, 22

SkyHigh An openstack-based cloud solution developed at NTNU.. 18

telemetry Automatic recording and transmission of data from a remote site to another, for analysis and monitoring. 75

WinPE Windows PE (WinPE) for Windows 10 is a small operating system used to install, deploy, and repair Windows 10 for desktop editions, Windows Server, and other Windows operating systems.. 14, 29, 38

Chapter 1

Introduction

1.1 Background

The project owner, i.e., the one defining the requirements for this thesis, is HDO. HDO is an Information technology (IT) operations organization within the Norwegian health sector, which has the primary function of operating and managing the communication solutions used by the Norwegian emergency services. This includes devices ranging from radios used by first responders, to workstations in emergency rooms. Their duty is to ensure a stable communication solution for their customers. HDO's communication solution is used in all municipalities in Norway[1].

As businesses grow they need more IT-equipment, often distributed to multiple geographical locations. This makes management more costly and time consuming, fueling the need for centralized IT management, which are more scalable and cost efficient. Managing and securing IT equipment from a centralized IT department is however a challenge faced by many, including HDO.

Communication equipment used in emergency services has especially high demands of availability and integrity due to the nature of their work, where downtime and incorrect information can lead to serious adverse events. Special consideration is required when performing maintenance on these systems to keep downtime to a minimum, as these systems are in near constant use by health care professionals. Information security in the health sector is also challenging as the health sector has been a target for cyber criminals in recent years [2].

HDO is currently in a restructuring process, in which they are in procurement of a new communication solution. As part of this solution, client machines will be shipped out to customers spread out over 150 locations in Norway. HDO therefore requires a way of deploying these new machines, and a plan for how to secure and support them while they are in operation.

1.2 Project description

This project will result in a Concept of Operation (ConOps)[3] describing a solution on how to maintain and secure Windows 10 clients throughout their lifecycle in HDO's new communications solution. This solution will also be implemented in a lab environment to demonstrate its functionalities. Decentralized IT management has been an issue faced by most larger corporations for some time, and thus there are several solutions on the market catering to solve this in various ways. This project aims to create a scalable solution customized to HDO's needs, and provide a ConOps providing the information needed to implement and use the solution.

1.2.1 Project Goals

The end product will take the form of a functioning Windows Domain environment, complete with hardened workstations. The following features were expected to be implemented in the solution based on the original requirements from HDO:

- A functional Windows Domain Environment.
- Hardened workstations.
- A Centralized Management solution, with added focus on keeping most relevant features in one tool/console.
- Deployment of workstations over the network.
- Efficient handling of Windows patching.
- Automatic deployment of Software.
- Efficient handling of data transfers to branch offices with low bandwidth capacity.
- Security measures specifically for workstations.
- User autonomy regarding workstation maintenance.
- Ability to monitor health and compliance data from workstations.
- Secure and efficient remote assistance solution.
- A focus on high availability.

1.2.2 Restrictions and constraints

HDO has been very liberal on how the project should be solved. Therefore, it is up to the group to make any necessary restrictions for the scope and functionality to meet the requirements set by HDO.

The solution was at one point supposed to be developed in SkyHigh, NTNU's cloud computing platform, but due to technical obstacles with the PXE-booting, this proved to be impossible. At the point where the underlying platform was swapped out, a fair amount of preliminary work had been done in SkyHigh, which resulted

in setting the entire project back roughly one week.

The solution will instead be hosted on a private vSphere cloud. The domain environment created here will simulate a small version of HDOs decentralized environment. When implementing secure solutions, preliminary prepping, roll-out and maintenance of the client, it is important to remember that HDO will not use virtualized setup. Therefore, the solution should not be related to anything that only works with this platform.

During a meeting with the client, the question of securing the backend(e.g. the servers) was brought up. However, given that the security-aspect of this project is specifically about securing client machines, this was considered to be out of scope.

HDO operates with a closed network, so any cloud based services will not be allowed except cloud services offered by Azure, as their Internet Service Provider (ISP) has a secure connection directly to Azure. This was new information that came halfway through the project. Therefore, the majority of the report has not taken the possibility of a cloud-connection into consideration. Instead, where cloud-reliant technology/tools are described as implemented in the report, some form of this disclaimer is included.

HDO has specified that the bandwidth between some remote locations is low. This will have an impact when creating automation of updates and software distribution. If all machines in at a remote location asks for the same update or software directly from the distribution point in the same time frame, it might congest the network.

1.2.3 Learning objectives

- Gain knowledge of different approaches to Windows management, and existing system management-software Section 2.2.
- Understanding how to manage Windows 10 clients in a domain, like in Section 3.2.
- Gain basic knowledge of GPOs and how utilize it in a security setting as in Section 4.2.1.
- Understanding how to use Kanban in practice, like in Section 1.5.2.
- Understanding how to secure Windows client machines, like in Chapter 4.
- Learn to design an operation and security concept for a Windows environment, like in Section 3.2 and Chapter 4.

1.3 Target audience

The intended audience for this project is primarily the IT operations team working at HDO to implement the new communication solution. The project will also be

relevant for other businesses who look to create or expand upon a secure system management-solution. A functional understanding of Windows environments, information security and operations is recommended to get the most out of this report.

1.4 Own background and competence

The group consists of three bachelor students of IT-operations and Information security at NTNU Gjøvik. All members are also currently working as security analysts at mnemonic AS. Gaute also has a certificate of apprenticeship in computer electronics, and has worked with operations in the financial sector.

The group has through the subject ITSM, Security and Risk Management (IMT2008), gained knowledge on how to perform a risk assessment, using standards like ISO27002[4] and NSM grunnprinsipper for IKT 2.0[5]. In the subject Infrastructure as Code (IMT3005) the group learned how to manage devices and infrastructures with the automation tool Puppet. Operativsystemer (IMT2282) gave the group valuable insights into the structure of the Windows OS and powershell-scripting.

1.4.1 Roles

Group Roles

Group leader Sondre Breivik

Secretary Erik Sørli

Meeting Manager Gaute Dvergsdal

Project Roles

Sondre Breivik Overall responsibility for thesis-structure and final presentation.

Erik Sørli General quality assurance for report and technical solution.

Gaute Dvergsdal Overall responsibility for technical choices, implementation and final product.

Administrative responsibilities:

- Book rooms - Sondre Breivik
- Overseeing overleaf structure - Erik Sørli
- Overseeing Trello/Scrumban - Gaute Dvergsdal
- Overseeing Toggl-timekeeping compliance - Sondre Breivik
- Overseeing git-repository structure - Erik Sørli
- Overseeing Gantt-scheme compliance - Gaute Dvergsdal

1.5 Project management process

1.5.1 Tools

GitHub

Two GitHub repository were created, one for backup of the thesis ¹, and one for scripts ². GitHub is used as version control, to track back older versions of the thesis and the scripts. It is also an excellent tool for collaboration and sharing code.

Time tracking with Toggl

Toggl is used to track the time of each individual member on the thesis. This is with Trello, used to keep track of what each member is working on, as well as to see how much time each member of the group are spending on the thesis. This could be a motivator if someone is working hard, or a reminder for a group member to put in some extra time if he is falling behind.

Overleaf

The thesis is written in the collaboration-tool Overleaf. This is a tool that all group members are familiar with, because it has been used in several other projects during the bachelors degree. It also provides a nice structure and interface which makes it effortless for team members to share their ideas.

1.5.2 Method and approach

Trello will be used as a Kanban board, in order to organize our work. The Kanban board is implemented to create a workspace where the workflow is well defined and information is available for every team member. The Kanban board will visualize the whole workflow, which will be divided into 5 columns:

- Backlog
- In progress
- Testing
- Review
- Completed

All columns will have a Work in progress (WIP) [6] number. This is the limit on how many cards can be in that column. WIP helps us from focusing too much on one phase of the project.

Backlog: All tasks the group decides on will be put here. The top 5 on the list will reflect their priority with number one on top.

¹<https://github.com/ErikSorli/Backup>

²<https://github.com/ErikSorli/Send-ccm>

In progress: Group members moves cards from back log into in progress when they start working on it. WIP limit is set to 6 with the intention that each member can work on one practical task and the corresponding part in the report.

Testing: When a coding/practical part is finished it is moved to testing. WIP limit is 3.

Review: All tasks regarding report writing is moved from in progress to review when finished. Another group member will read through it and approve it before it is moved to complete. If it is not satisfactory, it is moved back to in progress. The reviewer will then fix it or notify the person writing it.

Complete: When a task is approved by another member, it is moved to complete.

The functionality in Trello allows assigning cards to group members and track activity related to that card. This lets us easier track who and what has been done, if during a review with the product owner is decided that it is not what they expected.

This workflow will help us to prioritize our work. The board will also help to keep track of older versions, and the work done by each member of the team. This will benefit us when it is approved. Then it will be easy to give feedback to the team member that completed the task.

To ensure that every requirement from HDO is met, a weekly meeting with the client was completed. In this meeting any added functionality was explained, as well as the functionality that would be worked on in the coming week. HDO had the opportunity to provide additional functionality requests, or specify new restrictions during these meetings. The resulting reports can be found in Appendix L. Meetings with the supervisor Christian Johansen, was held sporadically throughout the project, whenever deemed necessary.

1.5.3 Source evaluation

The report below references a myriad of technical articles, scripts and tutorials used by ourselves to understand certain concepts, or to help implement various technologies. References are also placed strategically to give the reader a context for certain descriptions or concepts. When evaluating the quality of the source, we have considered the publisher and the stated background of the author(s). We have preferred to choose resources which originate from the official sites of the developer (e.g. Microsoft docs when discussing Microsoft products). In cases where the specific resource or information is unavailable from the first-party sites, sources published by respected companies/organizations, or written by individu-

als with relevant experience has been used instead. Examples of relevant experience can be previous employment by the developer or commendations from the developer (Such as Microsoft Most Valuable Professional (MVP)).

In sections of the thesis where the installation or configuration of certain central technologies are described, video tutorials are referenced along with written ones. The same qualifications used for all sources were applied when evaluating video tutorials, and practically these sources are referenced by pointing to the accompanying blog post of each video.

In addition to utilizing online resources to find relevant information to be used in the project, several informal discussions with technical professionals were held. These discussion were used both in order to get specific technical answers to questions we had or issues we faced, and to gain needed perspective when making high-impact technological decisions for the project. The individuals interviewed and themes discussed were:

- Joe Richard Muskaug (Mnemonic) - Windows management, hardening and OS deployment
- Øyvind Heggheim (Sparebanken Sogn og Fjordane) - Windows management, hardening and OS deployment
- Lars Erik Pedersen (NTNU) - Virtualization platform and client operation
- Erik Hjelmås (NTNU) - Puppet and OS deployment

Chapter 2

Tools and technologies

In order to make this thesis self contained, this chapter presents argumentation and decisions on what infrastructure, software, tools and methods were chosen to accomplish the goals of this project. To maximize the learning output and the probability of selecting the right tools, several solutions to the problems were considered where applicable, before choosing the ones best suited to solve the issue at hand.

The most impactful choice made, was selecting the right management system, as it is a core feature of the project. The pick fell on Configuration Manager, as it is a leading product with extensive support and integration possibilities. Other solutions and the reasoning behind the choice is discussed in Section 2.2.

2.1 Deployment and management environment

An environment that is able to manage and support client workstations throughout their lifecycle is going to consist of a range of components and moving parts. These functionalities are derived from HDO's requirements, and are comprised of the following features:

- Bare-metal provisioning capability
- Software deployment capabilities
- Patch and update management
- Central security management
- Automation capabilities
- Report and log-generation

Choosing the technologies to realize this is its own challenge, as the solution needs multiple features which again should be integrable with each other. Integration is important to keep the need for different management consoles to a minimum. This reduces the administrative overhead of having to learn several different consoles, and is in line with the goal of gathering all features in one place. In addition, HDO asked for a specific set of functionalities which would be helpful

in their use cases:

- Custom dynamic name generation of new clients
- Workaround for patch and software rollout for low-bandwidth client locations.
- User agency in regards of software update schedules, and restart requirements.

2.2 System Management

The solution is ultimately going to manage 400-500 Windows workstations placed all over the country. As the solution presented here will be demonstrated using a small demo-environment, it is important to ensure that the solution is scalable and will work in the real world scenario. As the clients managed in the solution will be used in mission critical surroundings where continual operation is key, the overall solution must cater to approximate 24/7 operation. As such, the clients will be less fault tolerant which the solution must compensate for.

2.2.1 Modern vs traditional

As stated, finding the right combination of software and tools is a comprehensive job. On one hand there are several "tried and true" methods of deployment and management which has existed and been improved upon in the Windows ecosystem for decades. On the other hand, newer more modern approaches boasting their own set of advantages are constantly being introduced. This section describes the pros and cons of different approaches we have researched, and which solution we ultimately went for.

Puppet (Desired state management tools)

Puppet is becoming increasingly popular in the world of managing Windows environments, and is currently boasting 2,2 million Windows servers managed worldwide with puppet[7]. After Puppet Enterprise(PE), which will be touched upon later, introduced support for Windows in 2011, they have been making strides to improve their windows management capabilities ever since [7].

The strongest aspect of puppet is it's innate drive towards automation. As this project will attempt to automate away manual input as much as possible, this is naturally a big pull.

Puppet is a software configuration management tool, where a declarative language is used to define the desired state of a system or asset in an infrastructure. These definitions are bundled up in modules which manage the intended system[8]. Modules can be self written to cater to specific needs, or be taken from Puppet Forge, which is a catalog containing both community and official puppet

modules[9]. In recent years, Puppet has moved itself towards becoming more catering to managing Windows environments, as it has traditionally been focused on managing Linux distributions. With this shift, several modules targeting specific systems and tools in the Windows server ecosystem have been introduced. Modules for WSUS and Firewall management are good examples of these. Using these modules would mean we could centralize a good amount of all needed settings and security rules in one place, spread over a couple .yaml files. This could potentially improve both security and ease of use. By "locking" down management of a service to one file, changes made anywhere else would be overwritten within minutes, and it would give administrators a single unified point of contact to manage the environment [8].

Puppet comes in two variants. The free open-source option, and Puppet Enterprise. The main difference between the two is that Enterprise includes a versatile Graphical User Interface(GUI) out of the box, and is officially supported by Puppet. For a medium sized infrastructure, such as HDO is planning to deploy, Enterprise would be the better option, as delving into the Ruby-like Command Line Interface (CLI) right away will be challenging, and the free version is generally not used in larger infrastructures. The Graphical User Interface (GUI) included in Enterprise also gives access to dashboards for easy monitoring of clients and deployments, along with extensive reporting capabilities. It makes it easier in general to manage a workstation environment [10].

For Operating System (OS) deployment, and bare-metal provisioning specifically, there are several potential solutions which integrate with Puppet. The ones considered for this project was mainly Foreman and Puppet Razor. Foreman is in itself a complete management tool with numerous capabilities, and is in fact often used together with open-source puppet to provide it a functional GUI, while razor is a provisioning tool developed by Puppet. In this project we are only looking at the Windows provisioning capabilities, leaving system management to Puppet. As stated, both Foreman and Razor provide bare-metal provisioning, but Puppet Razor has two advantages: It comes included with Puppet Enterprise, and can provision a client from bare-metal up to the point where it is fully managed by Puppet Enterprise [11].

In the end it comes down to a couple factors: Open source vs proprietary technology, and whether or not multiple operating systems will be managed. It seems that whenever the question of using Puppet or similar "infrastructure-as-code/desired state automation" solutions to manage a Windows environment comes up, it's usually given that there are also other Operating Systems present, and also that Windows is a minority. What this means for this project, is that it's entirely possible that using Puppet to manage a mixed OS environment might be the better option, but in a "pure" Windows environment it is simply easier and more efficient to stay within the Microsoft ecosystem for management.

First Party Windows Tools

Naturally, Windows has its own set of management, deployment and updating tools in its arsenal. In fact, it has several tools that cater to similar scenarios, and can in some cases be used either interchangeably or in tandem. Therefore, finding the right tool within Windows requires a good deal of research on its own. Here we will highlight some popular tool-combinations and discuss the pros and cons of each scenario:

Configuration Manager

Configuration Manager, better known as System Center Configuration Manager (SCCM) is an on-premise system management tool which has been around in some form since 1994[12]. The current iteration encompasses every functionality needed to operate a Windows client environment through a full lifecycle. This includes software and OS deployment, patch management, client health monitoring, endpoint protection and a host of underlying features and functionalities [13]. It is perhaps best described as a large collection of tools and technologies collected in one console. Configuration Manager is focused on medium to very large Windows environments, ranging from hundreds, to hundreds of thousands of clients and both is, and has been, widely implemented across the globe. As a result of this, the solution is constantly being updated with security and feature patches, and is as well documented as anything.

The fact that Configuration Manager encompasses a range of functionalities and components this wide, makes it particularly attractive for this project. Having access to all requirements "under one roof" relieves some of the administrative overhead of having to incorporate multiple different tools to achieve the same result. In addition, the fact that it is created by Microsoft, for Microsoft products, makes integration with other necessary Microsoft components such as Active Directory and Group Policy Management considerably more seamless than using third-party alternatives. Another benefit that comes out of this, is the inclusion of Windows specific technologies such as Peer-Caching and Delivery Optimization, which can considerably reduce the bandwidth needs of remote workstation locations. In many ways, Configuration Manager sets the "standard" for Windows specific management.

The biggest strength of Configuration Manager might also be its biggest downside, especially for this project. As the tool itself has such a massive offering of features and technologies, learning to use and master it is its own challenge. The team tasked with operation and maintenance of the system will need to educate themselves thoroughly to grasp the entirety of the ecosystem, and even though comprehensive documentation exists, sifting through it all to find what's relevant

might be difficult in terms of sheer volume of text. The installation and configuration of Configuration Manager will likewise be a major undertaking, as even though one might only wish to use a few of the available functionalities of the system manager, everything is bundled. Therefore overhead in configuration might be unavoidable. Due to its size it is also resource intensive on the server side.

Intune and Autopilot

Perhaps the most modern iteration of Windows management, Microsoft Intune can be described as a cloud based management platform, and is sometimes referred to as Cloud Configuration Manager, although it lacks much of Configuration Manager's functionality [14]. Specifically on company-owned devices it can "enroll" users and devices, and provide full control over settings, security and features by applying policies set within Intune. Examples can be controlling password requirements, creating VPN connections and setting up threat protection. Intune also specializes in managing specific applications, and bringing Bring Your Own Device (BYOD) securely into the company infrastructure [15]. In fact, it is mostly aimed at this more modern Windows eco-system, consisting mostly of both privately and company owned mobile devices like smartphones and laptops.

A common use case with Intune, is to pair it with Microsoft Autopilot for provisioning. Autopilot can be viewed as a deployment tool, depending on cloud infrastructure to "roll out" new clients. It differs from traditional deployment methods by not re-imaging the client, but rather "transforms" the existing OS to be business ready. This way no additional infrastructure is needed to prepare the client for use[16].

For an environment hosting only Windows 10 machines, Intune with Autopilot could in many cases be a viable option for system management. However, by itself it cannot perform actions such as OS deployment without enlisting Microsoft Deployment Toolkit (MDT)[17], and is entirely dependent upon a Cloud connection. It is in general not suited for managing large collections of Windows workstations, and has zero legacy support, meaning it does not support any older OS than Windows 10 [18]. In larger organizations Intune and Autopilot is often used as a supplement to either Configuration Manager or another system management tool, to handle MDM(Mobile Device management).

Microsoft seem to be urging their customers to "evolve" to a more modern version of Windows management where the focus lies on cloud based device management and mobile device operation. This has been evident in their actions, as in 2019, Microsoft unified most of these first-party tools, including Configuration Manager, under one banner: Microsoft Endpoint Manager [19]. This was done to minimize the separation between their cloud and on-premise solutions. This is understand-

able, as Cloud based management offer up powerful tools that either replaces, or improves upon the more rigid features of on-premise system management alternatives that rely on in-house hardware and often complex network infrastructure to function. In some sense it can be viewed as the "future" of system management, but at this point in time, it does not fulfil the requirements of a project such as this.

2.2.2 Choice of System Management

This project will look to a more traditional way of managing Windows, as the overarching needs and required functionality of this project can in fact be described as "Traditional", in that features like bare-metal-provisioning of Windows workstations in a non-cloud environment is characteristic of a highly "traditional" Windows environment. One big pull towards this approach is to be able to lean on the decades of experience and documentation that can be found in these "older" solutions. Another reason is simply that HDO has stated that introducing the cloud into the solution would not work in their scenario, due to the nature of their closed network. Tools such as AutoPilot and Intune also does not inherently support one main aspect of our assignment, which is the ability to do bare-metal provisioning. Also, these more modern approaches tend to focus more on mobile devices such as laptops and phones, which simply does not fit the intended environment.

There are quite a few advantages to the modern way of system management that we forego in choosing Configuration Manager as our solution. Chief among them is the inherent automation possible with the newer solutions, that does not come naturally with Configuration Manager. Puppet is built for automation, and tools such as AutoPilot with Intune does away with a lot of obstacles for automation, such as only needing a connection to the cloud for managing clients.

However, although it might not be as easy to achieve, automation with Configuration Manager is still quite common in the industry. Most, if not all of the functionality this project requires can be automated in some form, whether this being through PowerShell (which is supported throughout Configuration Manager), or using built in options in the console.

Configuration Manager includes every functionality needed and more, to secure and operate a Windows workstation environment throughout it's lifecycle, which is why in the end, the choice fell on this technology.

2.2.3 Configuration Manager Features

In this section, some of the key features and aspects of Configuration Manager are described. Only a select few is written about as it would be impractical to include everything due to the size of the software.

Task Sequence

The TS is one of the pillars for preparing, deploying, and modifying images with Configuration Manager. The TS is a combination of one or more tasks used to create, update or deploy an OS image. Configuration Manager comes with many pre-made tasks that lets you customize the OS, and there are several tools and add-ons that provides even more tasks, like MDT.

Creating a task sequence

When creating a new TS from the Configuration Manager GUI the TS creation wizard has some preset defaults that will guide the user through a basic setup. The usage will be described in more detail in Section 3.4.2. The wizard includes five different types of TS defaults, which are the following:

- Install existing image package.
- Build and capture a reference operating system image.
- Upgrade an operating system from an upgrade package.
- Deploy Windows Autopilot for existing devices.
- Create a new custom task sequence.

Only "Install existing image package" has been actively used and tested in the project. It installs the OS through WinPE, letting the creator customize the installation through different TS tasks. In short, the TS is capable of installing and configuring the OS in almost any thinkable way through the use of Command Prompt (CMD), Powershell, conditions and dynamic variables, along with the rest of the pre-made steps.

Configuration Manager Client

The Configuration Manager Client (CMC) is the piece of software residing on managed Windows workstations responsible for communicating with Configuration Manager. It is through the CMC that actions taken by an administrator on the server side gets enforced on the workstation, along with policy enforcement and the automatic installation of deployed software and updates [20].

The CMC also reports back information about it's hardware and software inventory, which is used by Configuration Manager to determine, among other things, compliance, required software updates and applicable applications. Without the CMC present on the workstation, it is not considered to be "managed" by Configuration Manager [21].

Software Center

Software center can be described as a "storefront" for users to browse downloadable software and updates. It is through Software Center that users gets notified

regarding available updates, installation status and restart requests. It is automatically installed on endpoints together with CMC [22].

Collections

A collection represents a group of users or devices, and is a logical grouping created for tasks like application management, deploying updates and peer cache sources.

To populate collections, one of two types of rules has to be followed, a direct rule or a query rule. The direct rule adds users or computers to a collection manually. This means that if a new device needs to be in a collection, a system administrator has to add it manually to the collection. The query on the other hand, dynamically updates a collection based on i.e. which Active Directory Domain Services (AD DS) Organizational Unit (OU) a user is related to. [23]. After a collection is populated, applications, updates or TS can be deployed directly to it.

Boundaries

A boundary is a location on an intranet, which functions as a division of users and clients, pointing them to the correct Distribution point (DP)[24]. In Configuration Manager, boundaries can be configured based on subnets, active directory sites, IP address ranges or VPN.

Distribution point

A Configuration Manager DP is a server used to host the content files Configuration Manager deploys to the users and devices it manages. Clients connect to the DP and collect the packages it needs. Configuration Manager supports the use of multiple DPs in order to spread out resource utilization[25]. In HDO case, the DP will likely be located at HDO's premises in Gjøvik. Centralizing the DPs in Gjøvik might cause network congestion as there are bandwidth constraints to some locations. Mitigating actions to this consists of, among other measures, different forms of caching, discussed in Section 2.4.10.

2.3 Remote support

Allowing for remote assistance is an important function for HDO, as the users operating the clients are scattered around the country without any local support in place.

It is important to differentiate between Remote Desktop and Remote Assistance. Remote assistance is a connection to a remote host with the intention of providing technical support to the user operating the client. The user must consent to the

connection and can allow different levels of control to the person connecting to the host [26]. The local user will always be able to monitor the activity.

Remote desktop on the other hand, works like accessing you own client. By providing a host address and credentials, the remote user gains full access to the host. Any other connections to the remote host will be locked [26].

The users are mainly health care professionals without any IT-training. Offering remote assistance creates a platform where users can get fast support from HDO, where they can also oversee whats being done, maintaining more control. This helps building confidence and trust in the delivered solution to the users.

Enabling remote assistance in a computer network is an important feature. but it also opens up a new attack surface, meaning security is important. Security considerations must be done beforehand when choosing which solution to go for. Some of the aspects that need to be considered are:

- Who is allowed to initiate a connection.
- What level of control should the remote actor start with.
- What level of control should the remote actor be able to gain.
- How many control levels should there be.

To ensure that the use of remote assistance is as secure as possible without rendering it unusable, the following security settings will be recommended:

- Only authorized support users are allowed to initiate a connection (unsolicited connection).
- The supporter should not have any rights from the start.
- There should be two control levels. First for viewing the remote machine, and second for control.
- The supporter should be able to gain full read/write access.

There are several products on the market offering remote assistance such as Zoho Assist, Solarwinds Take Control and TeamViewer. For this report, only TeamViewer and Microsoft's own Remote Assistance will be discussed in order to not overly focus on this feature.

2.3.1 TeamViewer

QuickSupport

TeamViewer is a well known and widely adopted provider of several products within the remote access part of IT management [27]. For remote assistance, the simplest way is to utilize the QuickSupport app [28]. QuickSupport is a light-weight application that does not require any other TeamViewer software to run on the supported client. QuickSupport supports several platforms such as Windows, iOS and Android devices. QuickSupport does however not support modification

of access rights, meaning that there is no way for IT admins to control the use of it [29]. This provides an attack vector for malicious actors to gain access to the network, and will not be considered.

TeamViewer full licence

The full TeamViewer software with an appropriate licence offers a range of features, including remote assistance. It offers granular control of the security settings, including all the security points mentioned above. The software is well supported if there should be any problems with the product itself. Usage is relatively simple, as the supported user only have to provide its identification number to the supporter for them to be able to connect.

2.3.2 Microsoft Remote Assistance

Remote Assistance is a native tool from Microsoft bundled with Windows 10. It offers both solicited and unsolicited connections to its users. Security settings are managed through GPOs which makes it simple to apply settings to all in Active Directory (AD), and all security points mentioned above are modifiable, including warning texts displayed when the supporter tries to elevate controls. Usage is simple as it utilizes hostnames to connect. HDO already have a suitable naming convention that the users are familiar with, so there are no need for additional training for users.

2.3.3 Remote support choice

TeamViewer comes bundled with many features that are not needed, and requires training, has licensing costs and requires additional software. It covers the requested feature, but the cost outweighs the benefits. Microsoft Remote Assistance on the other hand fits the needs of HDO better, as it is simple to use for both admins and users, is lightweight, and free.

2.4 Supporting features

This subchapter details additional underlying technologies supporting the solution, in addition to containing explanations of certain concepts and technologies which is referred to elsewhere in the report.

2.4.1 Virtualization platform

The final product is a functioning Windows domain lab environment. For practical reasons this was accomplished through virtualization. As stated in "Restrictions" Section 1.2.2, this was supposed to be realized in NTNU's OpenStack-platform,

SkyHigh. Why this turned out to be impossible can be read in Section 2.5. Instead the project was developed and set up on a private vSphere cloud accessible on NTNUs network.

2.4.2 DHCP

A simple Dynamic Host Configuration Protocol (DHCP) server was implemented to automatically provide and assign IP addresses to the client machines in the demo environment. The DHCP server is also in charge of network bootstrap program file, which is in charge of Preboot Execution Environment (PXE) booting is described further in Section 2.4.8.

2.4.3 PowerShell

PowerShell is a command shell used for scripting and automating management of different systems. It is mainly built for Windows platform, but can run on different platforms like Linux and MacOS. Unlike other command shells, PowerShell uses .NET objects to withdraw information [30]. In this thesis, PowerShell was used to run scripts and manage cmdlets from the command line, for example enabling automation of processes and returning information.

2.4.4 BitLocker Drive Encryption

BitLocker Drive Encryption, from here on called BitLocker, is a functionality in Windows 10 which allows for encryption of storage media and tamper proofing. This means that it scrambles your data, so it cant be read without authentication or decryption with a recovery key [31].

2.4.5 Active Directory

AD is a directory-service, or database, created by Microsoft to exists at the center of any Windows based environment. It is, among other responsibilities, responsible for keeping track of users and computers as objects in the database, as well as their accompanying rights, privileges and attributes within the windows environment. Within the hierarchical tree-like structure of AD, objects, like users and computers, can be managed together within groups, and more notably, OUs. OUs are containers of objects that system administrators can apply specific policy for, called GPO.

Services like rights management and login authentication and authorization, are part of the suite of functionality within AD, called Active Directory Domain Services. The server hosting AD and its services, are referred to as the Domain Controller (DC).

2.4.6 Group Policy Object

GPO, is a feature in Microsoft which controls the working environment of computers and user accounts. The GPO's defines how a system will behave and how it will appear. This will be further explained in Section 4.2.1

GPO Baseline

A security baseline in general is a predefined set of security objectives that should/must be implemented to achieve a certain level of security in a system. A GPO baseline a security baseline consisting of GPOs, which must be implemented to satisfy the baseline creator's definition of a secure system.

2.4.7 Image deployment

Deploying new images in a business can be a large task that can cause implications. If the deployment is not planned or deployed properly, it could lead to extra cost and potential loss of data. What method to follow would depend on the size of the company. Smaller companies could benefit from manual installation, but with bigger companies, manual installation would be both time consuming and largely impractical.

In the case of this project, alot of images will be deployed across different locations in Norway. Manual installation is therefore not an option. Configuration Manager which was selected as the System Management tool will be used to create and deploy images to all locations within HDOs network. There are several approaches to OS deployment, but only Lite-touch and Zero-touch deployment has been researched and assessed, as HDO wants as little interaction as possible during the deployment.

Lite-touch deployment

lite-touch deployment (LTD) requires installation of MDT, and is deployment of an OS from a mounted disk, USB stick or any other shared media. This has some requirements with user interaction during the download phase. The Lite-touch deployment requires little infrastructure in order to deploy operating systems, applications and any other pre-configured settings [32].

Zero-touch deployment

zero-touch deployment (ZTD) on the other hand, is a fully automatic deployment schema. ZTD is implemented with configuration management, and does not require any user interaction [32].

Given that HDO will deploy a lot of machines, a ZTD would fit best. This will

require no user interaction during the installation phase, and is more efficient in larger companies.

2.4.8 PXE-booting

PXE is a client-server environment where OS boot files are retrieved over a network connection. A client with a Network Interface Controller (NIC) supporting PXE, utilizes DHCP and Trivial File Transfer Protocol (TFTP) in order to boot an operating system or software.

PXE-booting is enabled on a client machine through the "EFI network" boot option. When the client machine boots, it will receive an IP from the DHCP, and then finds the TFTP/PXE server by either setting DHCP option 66 and 67 or with IP helpers. When the client-server connection is established, the client machine proceeds to download a boot image, which is used to install the OS [33].

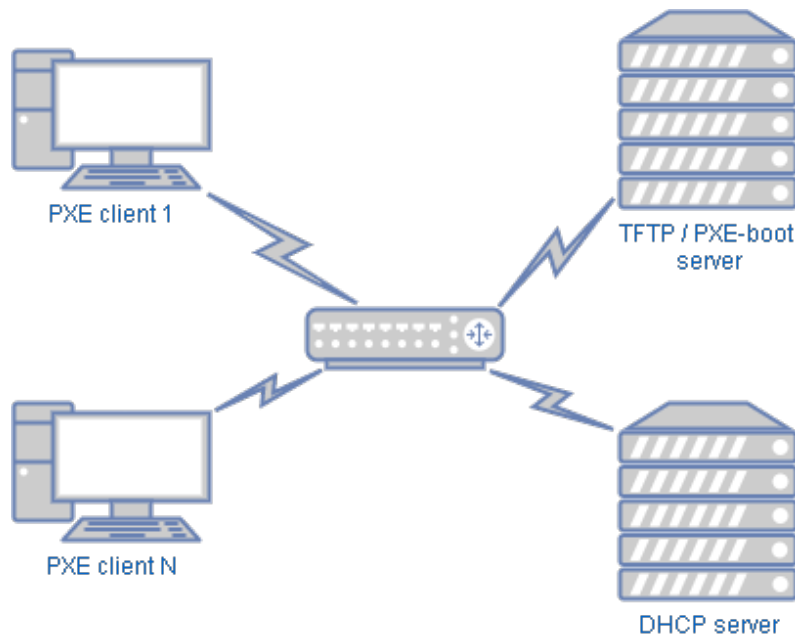


Figure 2.1: PXE booting infrastructure example

2.4.9 Windows Deployment Service

Windows Deployment Service (WDS) is a network-based installation of a Windows OS, using a disk image, in particular a Windows Imaging Format (.WIM) file. WDS can be connected with PXE in order to remotely deploy Windows images to client machines within a company network [34].

2.4.10 Caching

As mentioned in Section 1.2.2, HDO might have low bandwidth between HDO and some of the customer locations. Windows and Configuration Manager has three different mitigating solutions to this problem, which are BranchCache, Peer cache and Delivery Optimization.

BranchCache

BranchCache is an independent Windows OS component integrated with Configuration Manager that allows for bandwidth optimization. BranchCache has two different operating modes, which is Distributed cache and hosted cache mode [35]. In hosted cache mode the content is stored on one or several servers on a branch site, which is not an option as HDO does not have decentralized servers.

Distributed cache on the other hand, can be configured to store the content on client machines in a branch without the need of a server. By enabling distributed cache mode on all clients, all clients will cache parts of the content they download, creating a local peer-to-peer network. This allows the clients to share content between themselves instead of retrieving it from a DP. Using distributed Cache will in turn lower the bandwidth consumption.

Peer cache

Peer cache is a built-in functionality in Configuration Manager that allows for bandwidth optimization. Peer cache sources acts as "miniature" DPs. This works by configuring one or several peer cache sources in each network location or collection. The peer cache sources shares their content by sending a list of its content and the location to the peer cache clients in the same collection [36].

Delivery optimization

Delivery Optimization is a Windows Update feature which enables a peer-to-peer connection to other clients in a network. It breaks down packages into smaller fragments in order to share the content [37]. This allows clients to download Windows Update content locally and distribute it to other clients in the same network.

Delivery Optimization serves the same purpose as the two other options when it comes to save bandwidth on a Wide Area Network (WAN) connection. However, it does not work well when Configuration Manager is distributing updates. This feature is activated through the use of WSUS or Windows Update which is not the case in this project.

2.4.11 Caching solution

BranchCache and Peer cache are two bandwidth optimization technologies with slightly different features. Peer cache is a Configuration Manager tool where a Peer cache source client downloads everything locally, but can only manage Configuration Manager content. Discovery can be done by boundary group, which enables multiple subnets to access the peer, making it suitable for larger locations.

BranchCache resembles a peer-to-peer network where all clients only caches blocks of data. BranchCache clients can only discover other peers on the same subnet, which can be limiting depending on network topology, but is faster than Peer cache.

Both BranchCache and Peer cache was implemented in the project as both are reducing bandwidth usage. Branchcache is enabled on all clients as it has few hardware requirements. Peer cache is implemented as a proof of concept, and should only be implemented on clients with sufficient storage and network capabilities [38].

2.5 Technical Obstacles

In a project such as this where restrictions on technical implementation and use of technologies are nearly non-existent, changes and/or missteps are inevitable. The most notable and impactful of the ones we encountered are described below. Obstacles deemed as less significant are mentioned or described along with the implementation of the tool or technology it occurred in.

2.5.1 Swap in virtualization platform

Early on in the project it was decided that the technical side of things would be hosted on SkyHigh, NTNU's OpenStack platform. A functioning domain was set up, and along with choices in tools and technologies, MDT and Configuration Manager was installed and configured. Shortly thereafter, while configuring the DHCP server on the domain controller, some bigger issues surfaced. Namely, that managing your own DHCP server within OpenStack is problematic, and getting PXE boot, which is a fundamental component in the project, to work would be practically impossible for our use case. This effectively rendered everything done up to that point useless, and another approach was required.

After researching different options, discussing amongst the group members, with HDO and technical personnel at NTNU, a suitable solution was found. A different bachelor-group had already set up a private server on NTNU premises, with ESXI and VMware VSphere configured, which our project were invited to make use

of. After setting up a virtual router isolating the environment, installing a DHCP-server and configuring PXE-boot would not be a problem.

2.5.2 Misconfiguration within VMware Vsphere

After the swap in virtualization platform, there was some issues with performance on the virtual machines. The server was misconfigured, causing the machines to be extremely slow. This led to a setback of the project, as configuration and deployment was extremely time consuming.

After discussing the issue with the bachelor-group hosting the server, a cloud specialist helped reconfigure the server, solving all issues.

Chapter 3

System implementation and operational concept

This chapter shows the work done in order to reach the operational goals in the project. It contains information regarding the installation and configuration phase of Configuration Manager and other necessary components. It also demonstrates how new applications, operating systems and updates can be deployed in our domain environment.

3.1 Demo Environment

The demo environment is hosted on a private vSphere cloud on the NTNU network created by fellow bachelor students, Christian Isnes and Gjert Michael Torp Homb. VMware ESXi was used as a bare-metal hypervisor with VMware vSphere as virtualization platform.

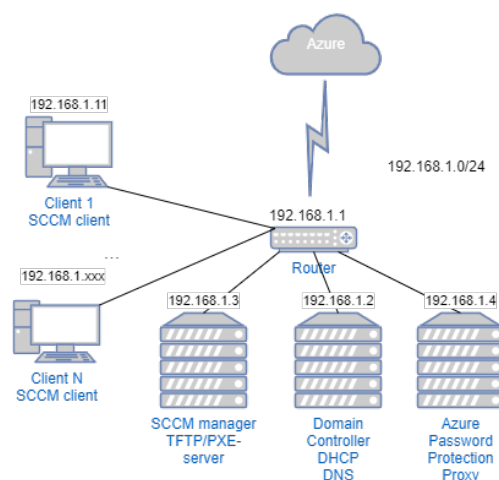


Figure 3.1: Visual representation of lab environment

As seen in the figure 3.16, the environment consists of the bare minimum needed to have a functioning network. A DC, a Configuration Manager server, a router, and client machines.

3.2 Implementing Configuration Manager

3.2.1 Installation

The installation of Configuration Manager is a comprehensive and time-consuming undertaking, where each step could be explained and written about for several pages. To avoid making this description into a detailed manual, only the most impactful choices and deviations from the norm will be described. As such, this section will serve as an overview of the many steps in the installation process, without delving to deeply into any one aspect.

Configuration Manager was installed on a separate server from the Domain Controller, called "Manager". Before starting the actual installation process, prerequisites and initial configuration had to take place on the server, starting with mounting and creating partitions for separate drives, conforming to the specifications recommended by Microsoft, with slight changes due to the size of the demo environment [39]. In addition, three drives were created to contain WSUS SQL database-files, along with Application Sources (for deploying applications) and Configuration Manager Content library.

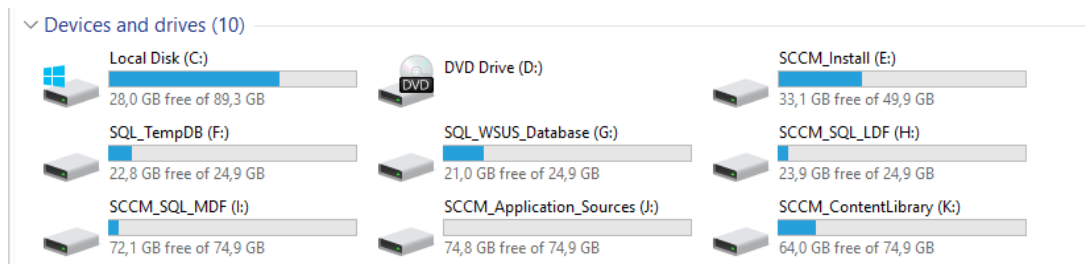


Figure 3.2: Required disk partitions

Additional prerequisites such as Microsoft IIS and Background Intelligent Transfer Service (BITS) was installed using this helpful Powershell script [40]:

```

1 Install-WindowsFeature Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,
2 Web-Http-Redirect,Web-Net-Ext,Web-ISAPI-Ext,Web-Http-Logging,
3 Web-Log-Libraries,Web-Request-Monitor,Web-Http-Tracing,
4 Web-Windows-Auth,Web-Filtering,Web-Stat-Compression,Web-Mgmt-Tools,
5 Web-Mgmt-Compat,Web-Metabase,Web-WMI,BITS,RDC

```

Listing 3.1: Powershell: Installing prerequisites

Some service accounts have been created as it is recommended not to use regular local admin or user accounts for various services related to Configuration Manager. In AD this is just a regular account without the need to change its password. For SQL-specific tasks the service user "SQL_SERVICE", was set up with a Service Principal Name (SPN) on the MANAGER using this command:

```

1 setspn -A MSSQLSvc/MANAGER.HD0.local:1433 HD0/SQL_SERVICE

```

Listing 3.2: Powershell: Create service user

An inbound firewall rule named "SQL" has been created, opening up port 1433 and 4022 to be used by the SQL service.

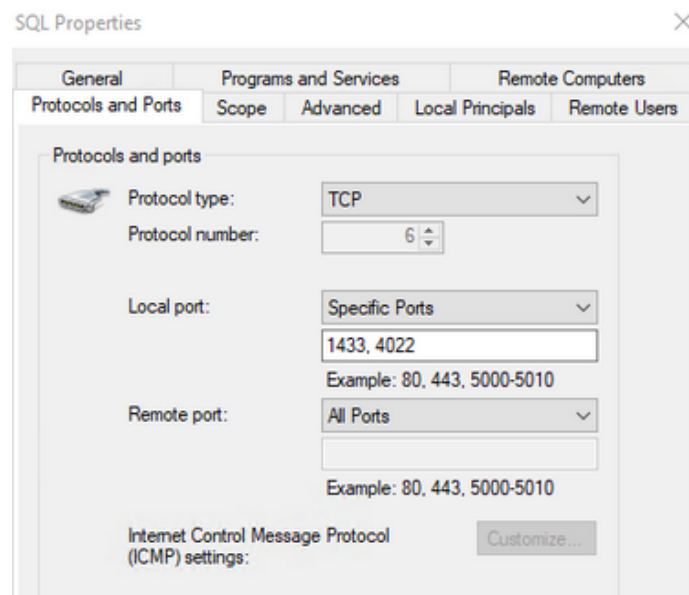


Figure 3.3: Inbound firewall rule "SQL"

Microsoft SQL Server 2019 was downloaded and installed, as this is the latest

version supported [41] by the current branch of Configuration Manager (at the time of installation this was version 2002, although Configuration Manager was updated to version 2103 later in the project). Cumulative update 5 for the SQL server was also installed as per recommendations. SQL was installed as a stand-alone installation (As it does not exist in a clustered environment). Microsoft SQL Server 2019 Reporting services was installed separately, as this is no longer included in the main SQL Server installation [42]. The same goes for SQL Server Management Studio, which is needed to interact graphically with the SQL Server. From Management Studio, the server properties was changed to comply with Microsoft's recommendations [40]. Specifically, memory allocation for a stand-alone primary site server such as ours, the recommended amount is 80% of available memory, which in our case is rounded up to 25600MB (of 32GB available).

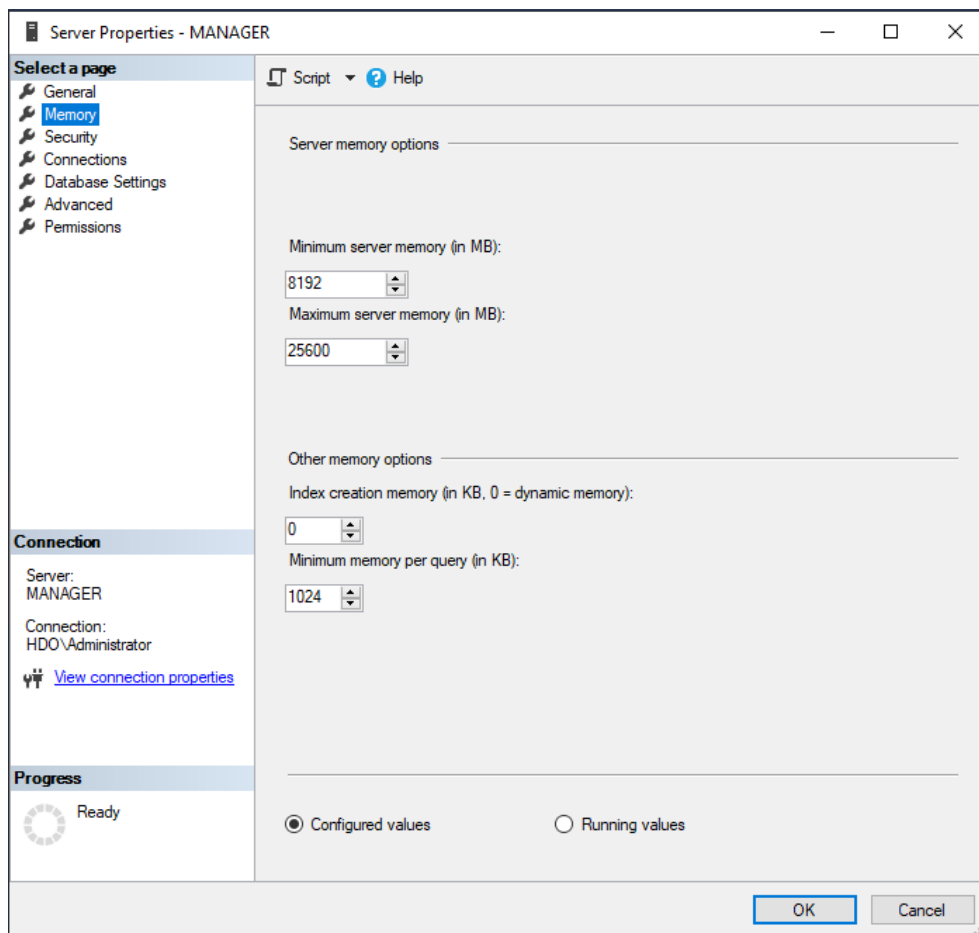


Figure 3.4: SQL server properties

WSUS was installed, as it is needed to use the software update feature of Configuration Manager (Software Update Point). As per the recommended configurations by Microsoft [40], the IIS application pool for WSUS has been altered. Specific-

ally "WsusPool Queue Length" has been doubled to 2000, and "WsusPool Private Memory Limit" quadrupled to 7372800.

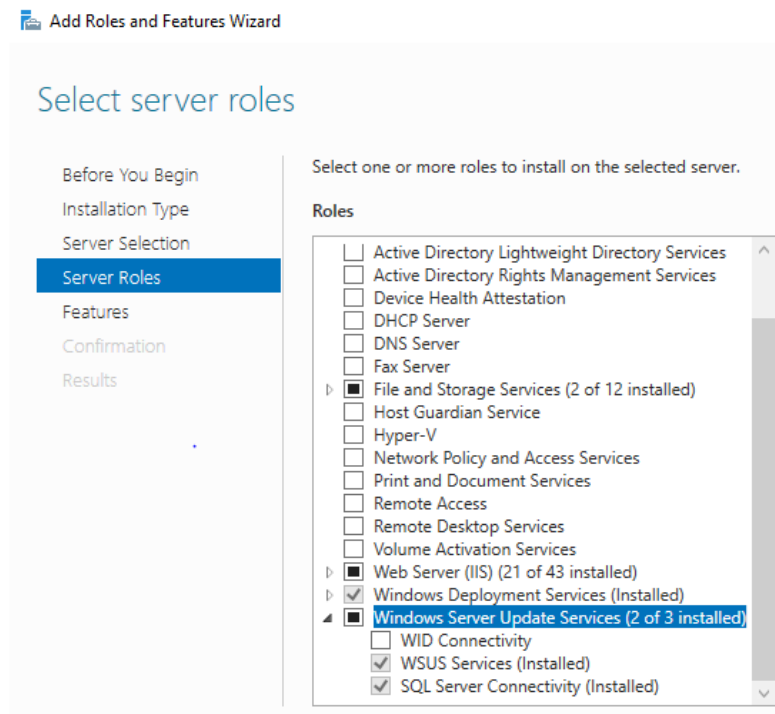


Figure 3.5: WSUS server role

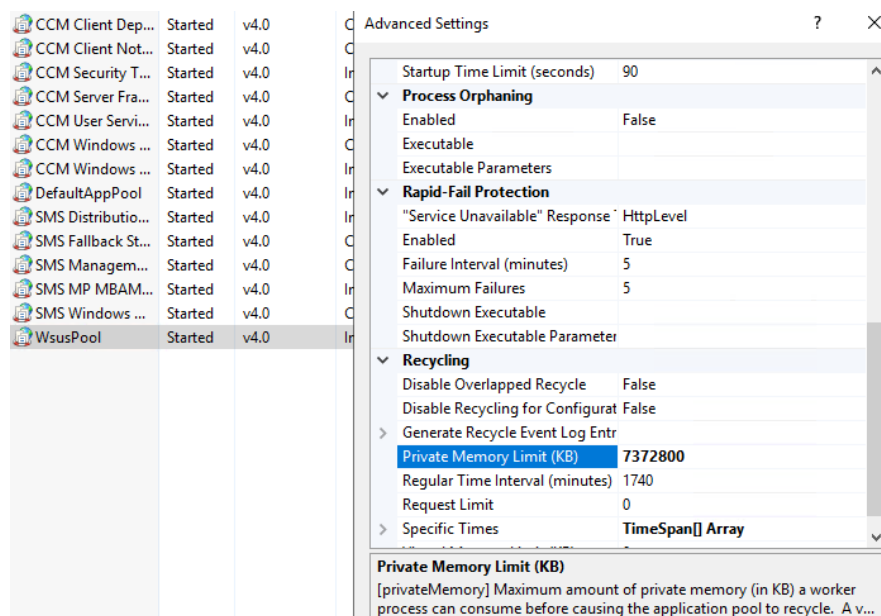


Figure 3.6: WSUS IIS change

Assessment and Deployment Kit (ADK) is another prerequisite needed before starting the Configuration Manager install. The latest release of this software was downloaded and installed, with the features "Deployment Tools" and "User State Migration Tool", which are needed to perform imaging of client operating systems, as well as OS deployment. WinPE is also installed, although separately, as it is no longer included in the ADK install[43].

Next, an extension of the AD schema is needed for Configuration Manager related attributes. A brief demonstration of how AD schema extensions work can be found in the LAPS section of this report in Section 4.3. In the source files of the actual Configuration Manager installation, specifically at this location in our setup: C:\Software\MEM_Configmgr_2002\SMSETUP\BIN\X64, there is a file called "extadsch.exe", which automatically performs this action. This also creates a log file, called "ExtADSch.log", which will confirm that the action was successful:

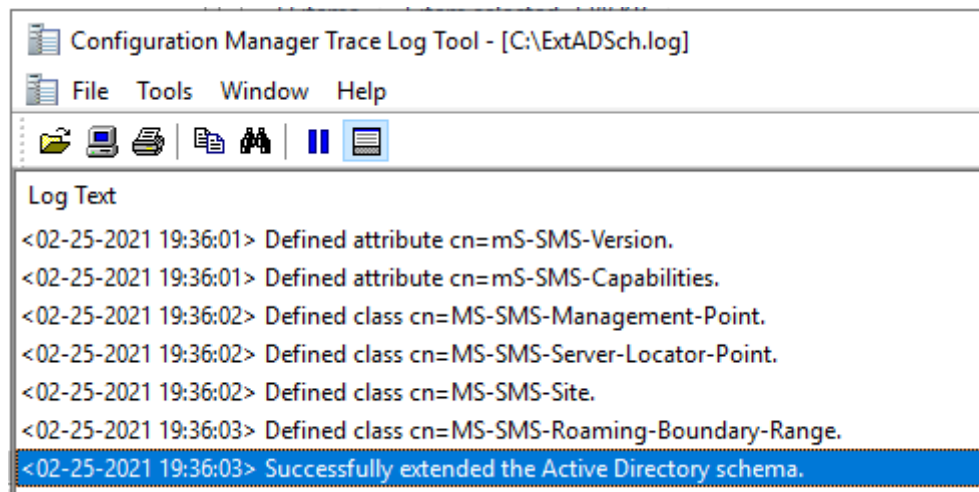


Figure 3.7: AD extension logs

A new container within the "System" container in AD on the DC, called "System Management", was created. This container is used by Configuration Manager to publish information about which sites and boundaries domain joined workstations are supposed to connect to. In essence giving them information about which Configuration Manager-server to connect to (there is only one in this environment), and where to search for content like updates and applications.

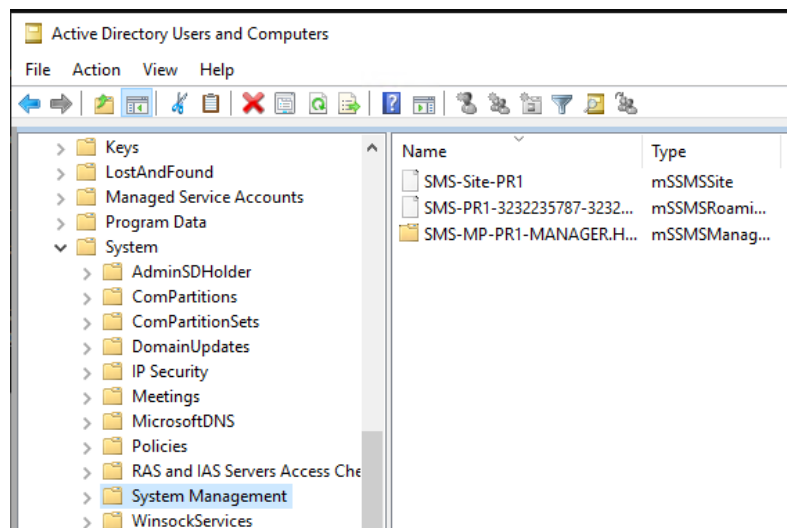


Figure 3.8: System management AD container

The main database used by Configuration Manager, called "CM_PR1" was also created before the Configuration Manager installation. This was configured to be spread out over four traditional database-files (.mdf) which will hold client information, in addition to one log-file. The initial size set for our purposes was

1024MB (256MB per file), with autogrowth kept at default 128MB, and maxsize unlimited. For a larger environment this size would naturally be too small. A rule of thumb in sizing the database is to estimate 5MB per client [40]. However, this estimate did not reflect the reality of our environment, as the files grew noticeably above that value, as can be seen in the image below. This did not cause us any issues, but it might be a good idea to generously provision disk space when deploying a large environment.

Logical Name	File Type	Filegroup	Size (MB)	Autogrowth / Maxsize	Path
CM_PR1_1	ROWS Data	PRIMARY	896	By 128 MB, Unlimited	I:\Database
CM_PR1_2	ROWS Data	PRIMARY	384	By 128 MB, Unlimited	I:\Database
CM_PR1_3	ROWS Data	PRIMARY	768	By 128 MB, Unlimited	I:\Database
CM_PR1_4	ROWS Data	PRIMARY	768	By 128 MB, Unlimited	I:\Database
CM_PR1_log	LOG	Not Applicable	1024	By 256 MB, Limited to ...	H:\Database

Figure 3.9: Database size toward the end of the project

At this point in the installation process the actual installation of Configuration Manager could begin. The current version at the time of download was version 2002. It was installed as a stand-alone Primary Site, including the Configuration Manager Console. Additional required files were automatically downloaded to the same drive as the Configuration Manager installation (drive E:). The "site code" which will identify the Configuration Manager site in the hierarchy (not too important when only installing one site) was set to be "PR1" with the site name "HDO". When asked to connect to a SQL-server, the name of the same machine, MANAGER.HDO.local, was typed in, and under Database Name, "CM_PR1" was added, as per the previous database creation. The rest of the options were kept at default values.

3.2.2 Initial Configuration

After installing Configuration Manager along with all prerequisites, there still remained a lot of preliminary configuration before the site was ready for use. As with the "Installation" section, this will be a general overview and not a thorough deep dive into each step of the configuration.

To enable specific functionality within Configuration Manager, such as software update, client reporting capabilities or content distribution, one must first install

and configure the "site system role" which governs that respective functionality [44]. Reporting Services, which was installed earlier, first had to be configured using the "Report Server Configuration Manager", before its site system role could be installed. Here, the report database "ReportServer" was created, and the URL for report viewing in a web browser (<http://MANAGER:80/reportserver>) was specified.

At this point the roles could be installed:

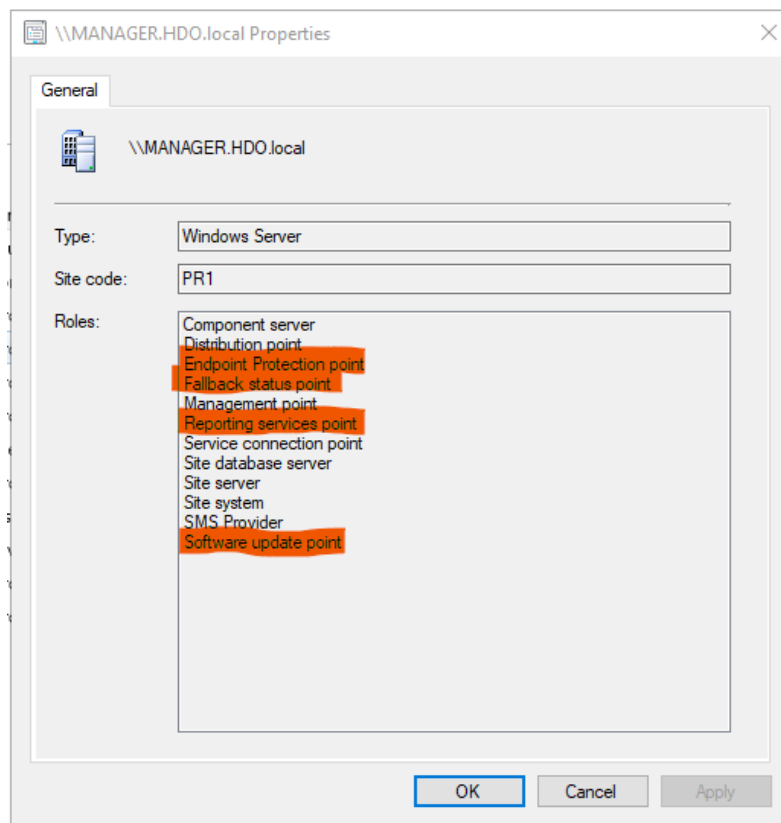


Figure 3.10: The roles not highlighted were automatically installed during the installation of Configuration Manager

In the installation wizard that followed, WSUS was set to use ports 8530 and 8531 to communicate with Configuration Manager, specifically with the Software Update Point (SUP). The SUP was also set up to synchronize with Windows Update each day at 23.00, and the option to "Immediately expire a superseded software update", was also enabled. What that means and why it was done is explained briefly in Section 3.6. In addition, download of "Express Installation files" was enabled for the SUP, which in essence reduces time and bandwidth consumption for workstations when receiving updates, because they only need to download and install the necessary files, without downloading the entire update. The trade-off

being that "express installation files" are more resource intensive on the server side [45].

For the Reporting Services Point a connection to the previously created "ReportingServer" was set up, and a service account (SCCM_SQL) was specified to handle the uploading of reports.

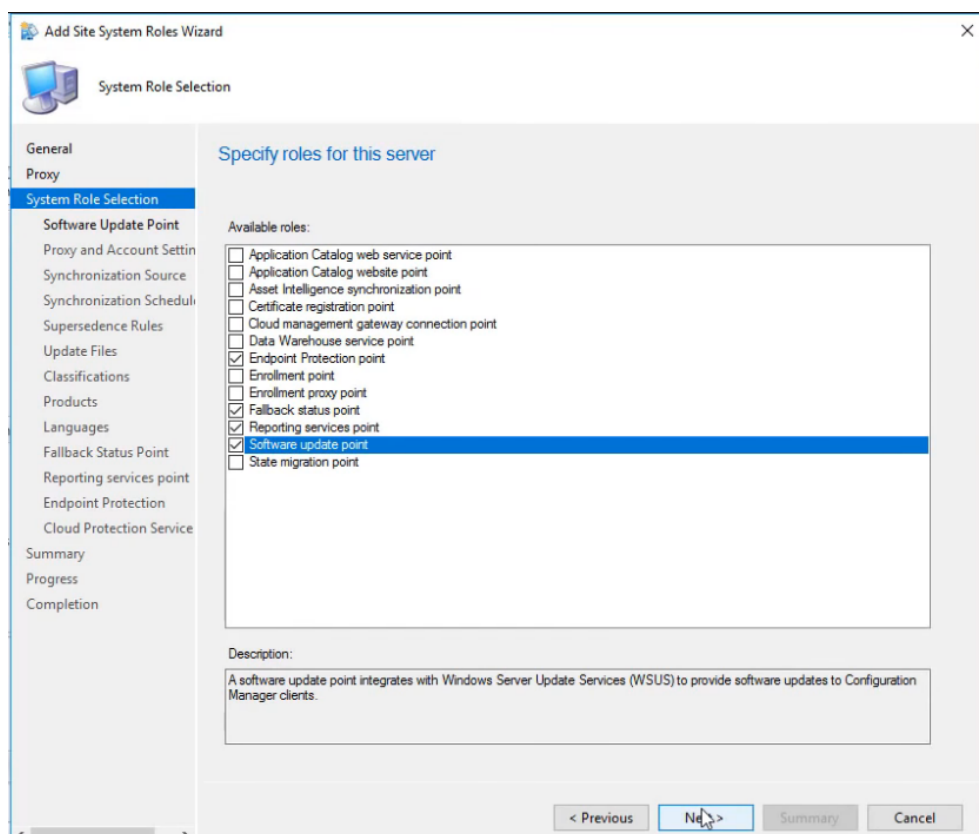


Figure 3.11: Site system role wizard

To enable a workstation to request content and policy from the distribution site (the "MANAGER"-server), a network access account, "SCCM_NAA" was created. During OS-deployment, before the machine is domain joined, this account is used to authenticate against the site server.

To install the CMC on all managed workstations, a service account called "SCCM_PUSH" was created.

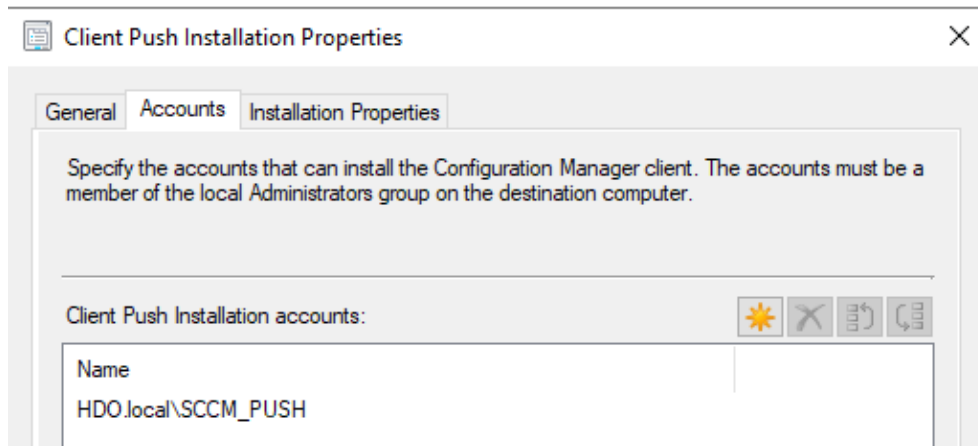


Figure 3.12: Specifying Service account for Client Push

To install the CMC, this account needs local administrative privileges on the workstation where the install takes place. This was granted by the Group Policy "SCCM settings" which is applied to the OU "SCCM_Site_PR1_Workstations". This GPO also creates two inbound firewall rules to enable "SCCM_PUSH" to retrieve the needed installation files from the site server [46].

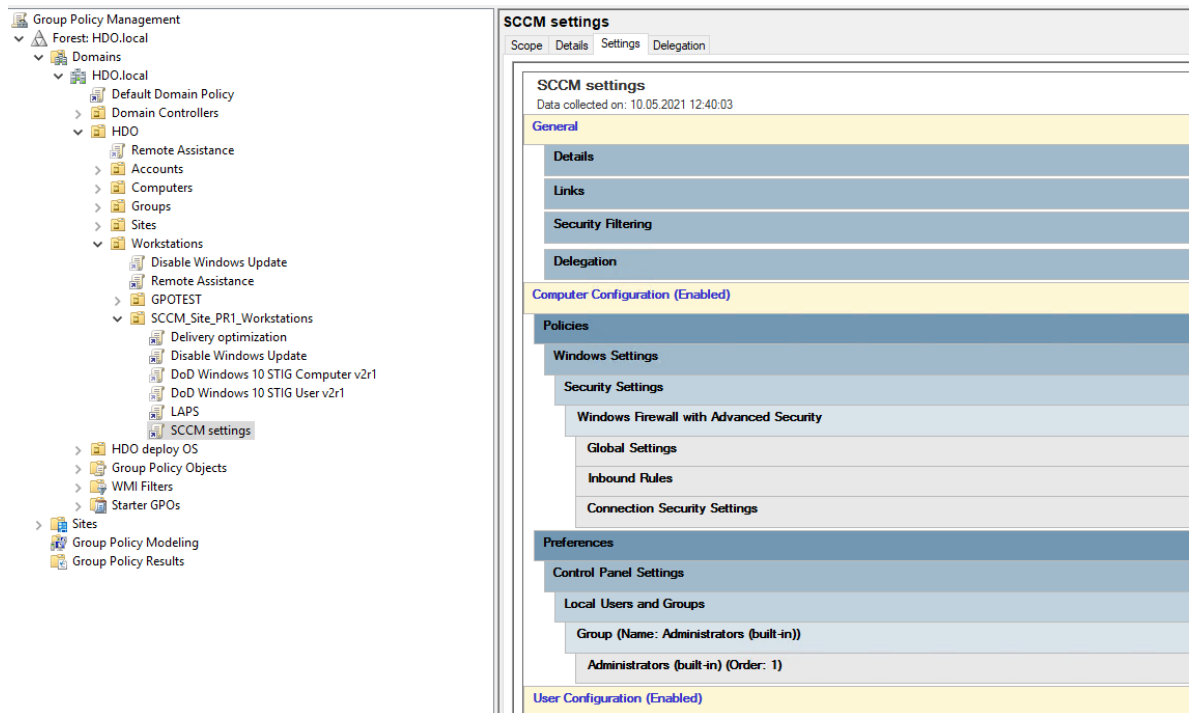


Figure 3.13: SCCM settings GPO

Next, a Boundary had to be created. Description of what a boundary is within Con-

figuration Manager is described in Section 2.2.3. The boundary was configured to encompass the entire subnet used in this environment (192.168.1.11-255), excluding IPs reserved for servers. Two Boundary Groups were configured and added to the Boundary, effectively telling workstations which Site (PR1) and Distribution Point (MANAGER) to assign to [47].

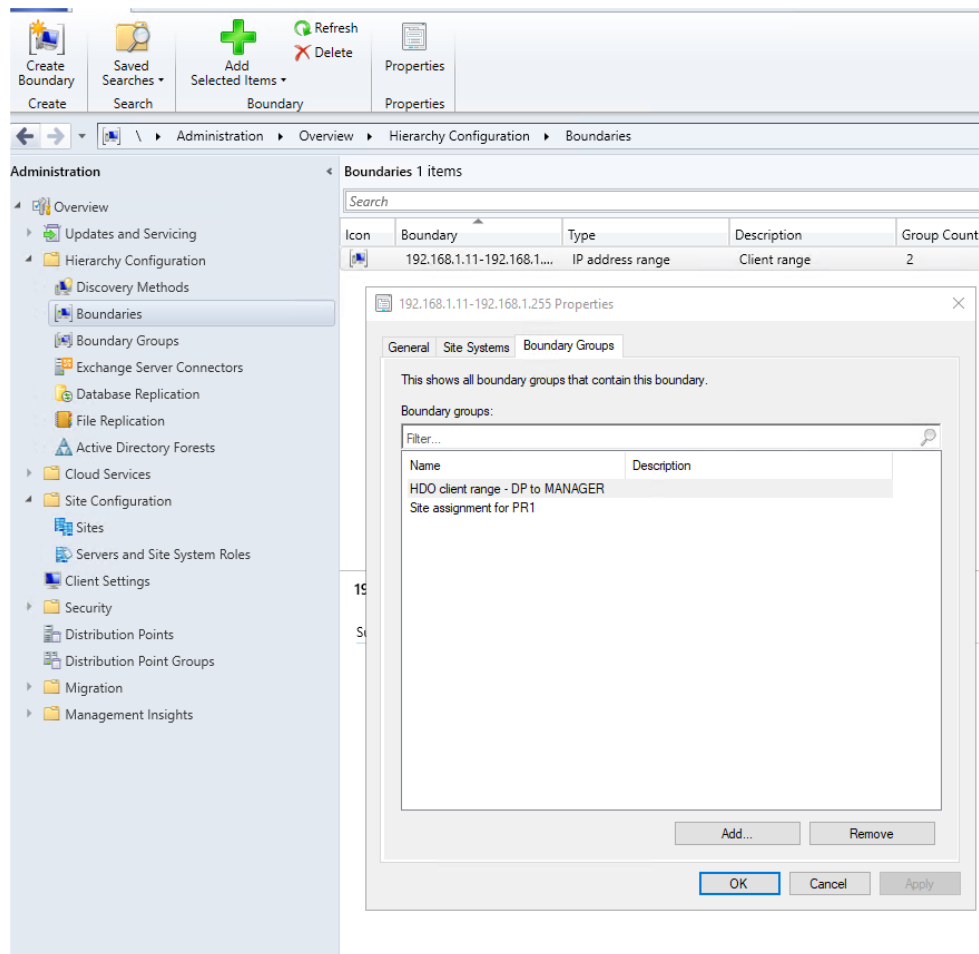


Figure 3.14: Boundary with Groups

Lastly, a Discovery Method for bringing workstations into Configuration Manager was specified. This is configured to discover AD computer objects from the DC in the OU "SCCM_Site_PR1_Workstations" once per day at 00.00 [48].

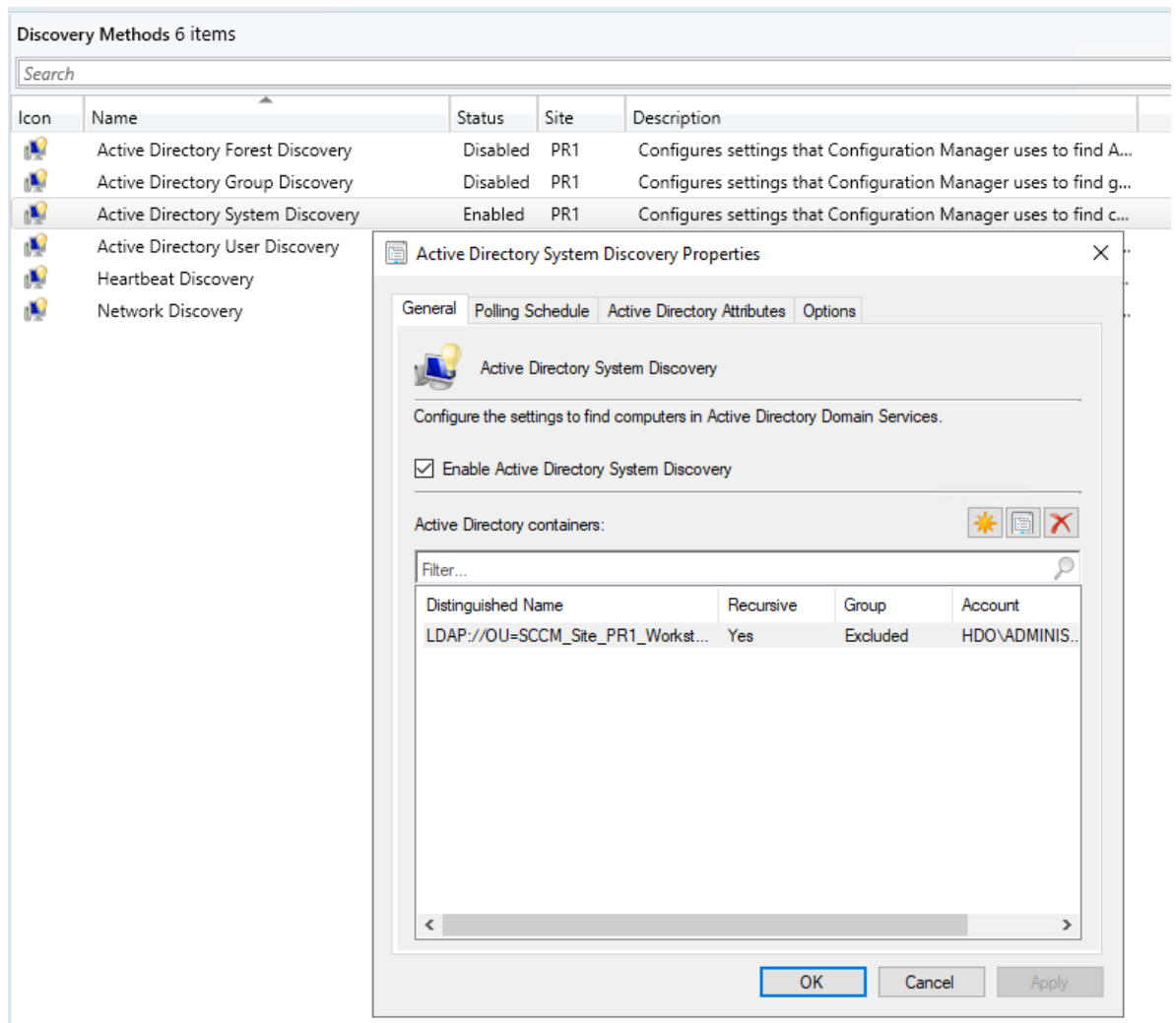


Figure 3.15: System Discovery

3.2.3 OS deployment

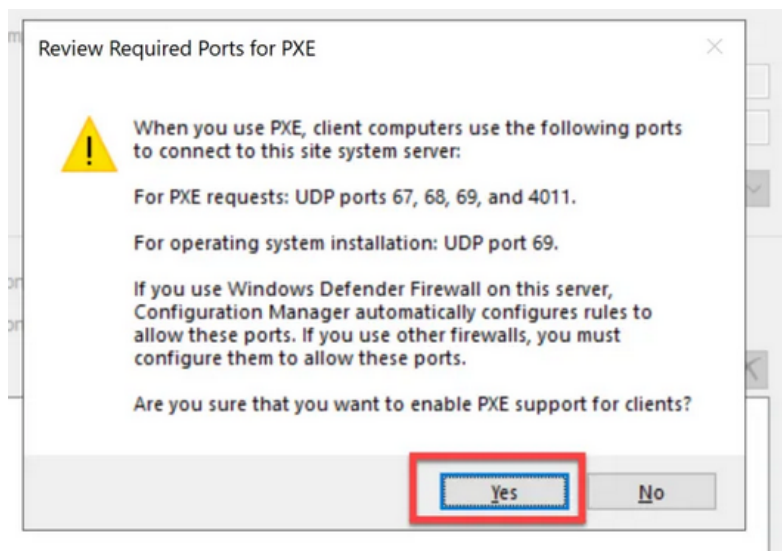
For Configuration Manager to be able to deploy Windows images, it needs a base image file to deploy. In this project Windows 10 Enterprise was chosen. For this to work with Configuration Manager the image needs a .WIM file. The .WIM file allows implementation of multiple copies and replaces them with a single shared copy, this will eliminate data duplication. If another OS should be implemented, a .WIM file needs to replace the .ESD file of the disk image. This is done by using the following commands in Powershell:

```
1 DISM /image:C:\ /optimize-image /boot
2
3 Dism /Capture-Image /ImageFile:"D:\Images\example.wim" /CaptureDir:C:\ /Name:'example'
```

Listing 3.3: PowerShell: Create .WIM file

3.3 Enable PXE

PXE was enabled in Configuration Manager to deploy TSs to the client machines. This was done by enabling PXE booting through the DP in Configuration Manager. When PXE was enabled, the Configuration Manager launched a pop up window requesting port 67, 68, 69 and 4011 to be configured in the firewall. In the case of this thesis, Windows Defender Firewall automatically configured these rules.

**Figure 3.16:** Open ports for PXE-booting

To allow for PXE booting, the DHCP server has configured with the right options. DHCP options 66 and 67 were enabled in this project. These two options are boot server host name, which is the name of the distribution point and the path name of the Network Boot Program (NBP). The boot server host name is defined to tell a client machine where the TFTP server is, and the NBP is defined to give the client machine access to the bootfile. When the machine has acquired the bootfile, it will then choose the corresponding .WIM file. In the case of this demo, the DHCP options are sufficient to deploy new images. However, if the clients being deployed are not in the same subnet, a dhcp-relay or ip-helper is needed to forward the information to other subnets.

3.4 Deploying client images with SCCM

Client deployment is done as a ZTD. This is in order to have as little human interaction with the installation phase as possible. PXE-booting is used to launch WinPE. A suitable TS is then selected in WinPE to deploy and configure the new image.

There are two different scenarios to cover when deploying new images to client machines. One where an already operational client is being reinstalled, and the other when a new client is being connected to the network. Both will be accomplished through the use of a TS, which can be read more about in Section 2.2.3.

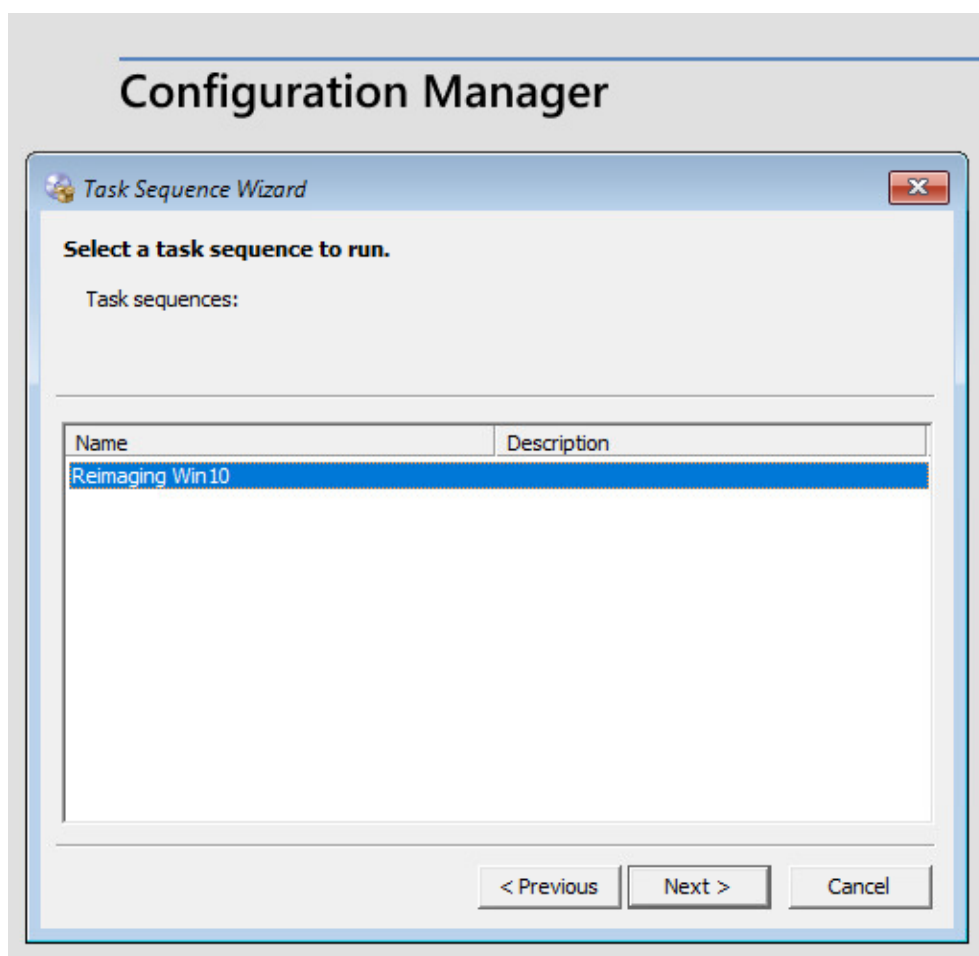


Figure 3.17: Choose Task Sequence in WinPE

Two Task Sequences were created for OS deployment, one for new clients, and one for reimaging clients. Both were created with the TS Wizard. Only steps which require modification will be described in the following sections. Most steps are

self-explanatory and will not be delved into further.

The TS needs to be deployed to a collection in order to install it on clients. When deploying to a computer that is not in the Configuration Manager database, the TS must be deployed to the pre-made collection "All unknown computers". All other Task Sequences can be deployed to any collection that contains the selected computer. In this project the TS for reimaging clients were deployed to a custom collection called "Windows 10".

3.4.1 Installing new clients

When an OS is installed there are multiple settings that needs to be configured before the client is operational, such as language, time, and formatting drives. These configurations are often the same across all clients, with slight deviations based on different factors, such as location or intended usage.

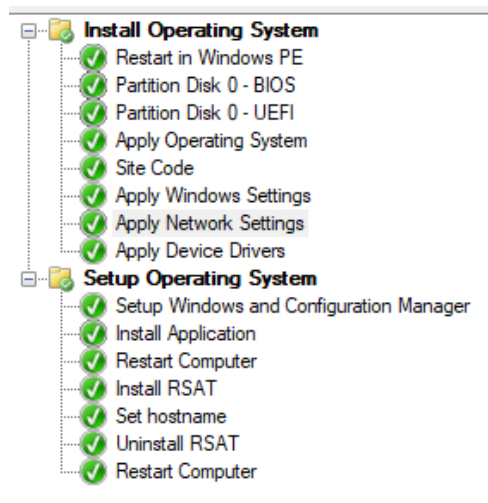


Figure 3.18: Task Sequence New client tasks

Domain joining

In this project there are two major areas where the TS needs to dynamically set some values depending on location, which is hostnames and joining the right OU in AD DS. When installing an OS through a TS one would normally set the hostname first, because the TS Variables used to set the hostname is being deployed before the "Apply Operating System" task seen in Figure 3.18, while domain joining happens in "Apply Network Settings". This is not possible in this case, due to the hostname's dependence on being domain joined before it is set.

Joining the right OU is possible in multiple ways. The simplest way we could see is to use dynamic variables as shown in Figure 3.20. These variables are then

injected into the "Domain OU" field in "Apply Network Settings". See Figure 3.19 for an example.

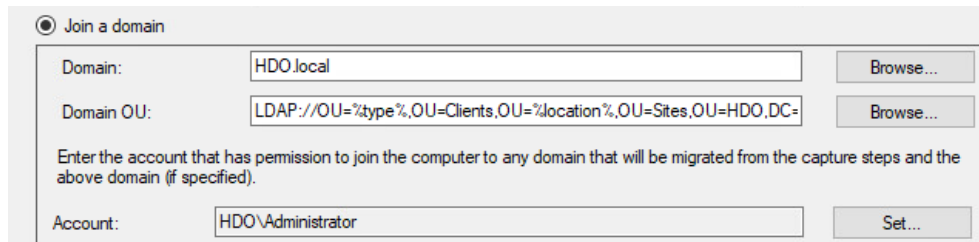


Figure 3.19: Task Sequence: Join OU

Hostnames

Dynamically created hostnames based on certain rules is explicitly requested by HDO.

The hostname structure follows a pattern as described here:

Character position (Highlighted)	Rule
RWP-GJOG360-1	Type of computer
RWP-GJOG360-1	Geographical location
RWP-GJOG360-1	What service is provided at that location (e.g. Emergency room)
RWP-GJOG360-1	Room number
RWP-GJOG360-1	Client number

Finding the correct site code¹ (all characters up until the client number) were solved using the Set Dynamic Variables task. That task can be used to change values in pre-made Configuration Manager TS Variables or custom ones based on a set of rules. In this scenario the site code was determined by the new clients default gateway as shown in Figure 3.20.

¹Site code in this context should not be confused with the Configuration Manager-site code(PR1)

Type: Set Dynamic Variables

Name: Site Code

Description:

Dynamic rules and variables:

The following rules and variables will be evaluated in order:

- IF Default gateway equals "192.168.1.1" THEN
 - SET type = "RWP"
 - SET location = "GJOG360"

Buttons: Add Rule, Add Variable, Move Up

Figure 3.20: Task Sequence: Setting site code

An additional request from HDO was that the client number should represent the "station number" on site, meaning that the client number should increment by one when an additional client is being installed at a location.

It proved difficult to come up with a solution for this, as finding the correct number involves querying other parts of the system which is not directly supported through the TS to count the number of existing clients with the same site code. The first solution was to run a series of client and server side PowerShell scripts to find the correct site code, and then count the number of clients in AD DS that contained that code.

This did not work because Configuration Manager does not support server side PowerShell during a TS. There are third party Configuration Manager add-ons such as Onevinn TSCommander which supports this, but it does not support returning values to the TS which was needed in this scenario[49]. We recommend looking into it either way as it might prove useful in other settings.

A working solution was to install the AD module in Remote Server Administrator Tools (RSAT) on the new client with PowerShell, use the dynamic variables obtained in Figure 3.20 to enumerate the number of clients with that site code in AD and rename the client accordingly, using the script in Code listing 3.4. An important thing to remember is the syntax used when passing a parameter to the PowerShell script. The syntax is as follows: `-<VARIABLE 1> 'value1' -<VARIABLE 2> 'value2'`. An example is shown in Figure 3.21. This example is from the "Set hostname" task. Another notable setting here is that the script is set to run as another user than the one chosen in the TS setup wizard. This is because AD did not accept the original admin user to perform the "Rename-computer" command in Code listing 3.4.

Properties Options

Type: Run PowerShell Script

Name: Set hostname

Description:

☐ Select a package with a PowerShell script:

Package: Browse...

Script name:

☒ Enter a PowerShell script:

Edit Script... Script status: Script is entered.

Parameters: %loc %' -Client Type %type%'

PowerShell execution policy: Bypass Output to task sequence variable:

Start in: Browse...

☐ Time-out (minutes): 15

☒ Run this step as the following account

Account: HDO\Sondre_adm Set...

Figure 3.21: Task Sequence: Pass parameters to embedded PowerShell

```

1  # Import dynamic variables from Task Sequence
2  param(
3      [string]$loc,
4      [string]$ClientType)
5  #Concat type and location
6  $SiteCode = $ClientType + "-" + $loc
7  # Find and count all computers in AD with that site code.
8  # Increment by one and rename
9  $computers = get-adcomputer -Server <DC> -filter "name -like '$SiteCode*' "
10 [int]$count = $($computers | measure).Count
11 $count++
12 $hostname = $SiteCode + "-" + $count
13 Rename-Computer -NewName $hostname -force

```

Listing 3.4: Change hostname with embedded PowerShell in TS

Important: Do not trigger a reboot in a TS while running a script with Restart-Computer. This might corrupt the TS. Use the task "Restart Computer".

RSAT is also uninstalled in the task "Uninstall RSAT" as a security action. RSAT is a tool that can provide much information to an attacker even on an account with few privileges, making it a security concern.

Possible solution without dynamic variables

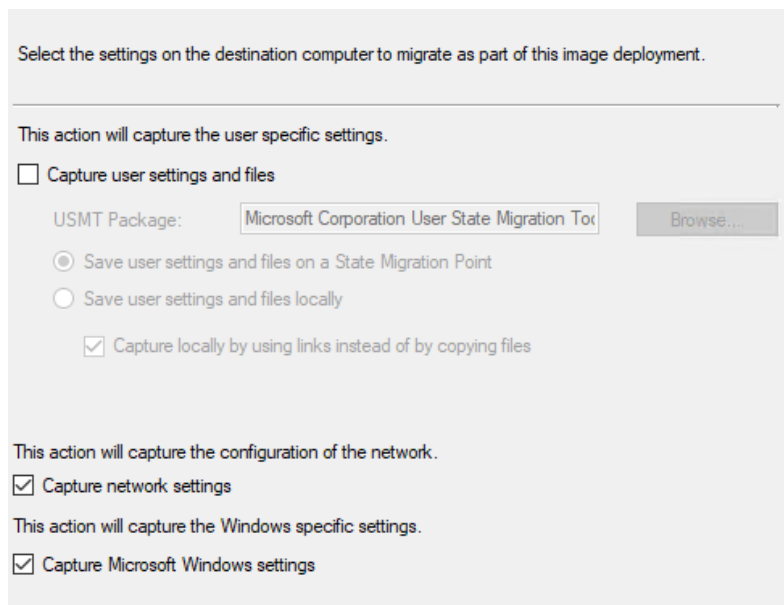
Creating a set of two variables in the TS for each site might be time consuming and hard to maintain properly. Another solution that has not been tested is creating a deployment package with a PowerShell script and a list of all default gateways and the site code it is associated with. The list is formatted as <SITE CODE>:<GATEWAY> with one on each line. The script will then find the clients default gateway and search the list for a match. When a match is found it will strip away the gateway and use the site code to count the entries in AD with that site code, and rename the computer accordingly. An example of the script is in Code listing 3.5

```
1  # Find Default Gateway. -InterfaceAlias might have to be changed, depending on which
2  # network adapter is in use.
3
4  $DG = (Get-NetIPConfiguration -InterfaceAlias Ethernet0).IPv4DefaultGateway.NextHop
5  # Import site codes and default gateways from the list
6  # gateways.txt and find the one that matches this computers gateway.
7
8  $list = Get-Content -Path .\gateways.txt
9  $DGandSite = ($list -match $DG)
10 # Strip away the gateway
11
12 $SiteCode = ($DGandSite -Split ':' ,2)[1]
13
14 # Find and count all computers in ad with that site code.
15 # Increment by one and rename
16 $computers = get-adcomputer -Server <DC> -filter "name -like '$SiteCode*'"
17 [int]$count = $($computers | measure).Count
18 $count++
19 $hostname = "$SiteCode-$count"
20 Rename-Computer -NewName $hostname -force
```

Listing 3.5: Set hostname with package

3.4.2 Reimaging clients

Configuration Manager is able to capture all necessary Windows and network information of existing clients when the TS is running, and copies it over to the new OS installation. This means among other things that the client will remain in the same OU and be given the same hostname as it had before. This is achieved by using the "Capture OS settings" and "Capture network settings". This is possible to configure with the Create TS Wizard.



Select the settings on the destination computer to migrate as part of this image deployment.

This action will capture the user specific settings.

☐ Capture user settings and files

USMT Package:

☒ Save user settings and files on a State Migration Point

☐ Save user settings and files locally

☒ Capture locally by using links instead of by copying files

This action will capture the configuration of the network.

☒ Capture network settings

This action will capture the Windows specific settings.

☒ Capture Microsoft Windows settings

Figure 3.22: Task Sequence Migrate settings

Beyond that there are not much that needs to be done to successfully reimage a client. A step that is not covered in whole through the Wizard is installing drivers. There is a step that tries to install appropriate generic drivers, but it is likely that it would be beneficial to install proprietary drivers for the client equipment, especially if all equipment are the same across multiple sites.

This is achieved through creating "Driver packages" that are deployed to the distribution points. By utilizing dynamic TS variables, conditions or Configuration Manager's own pre-made variables, it is possible to retrieve different Driver Packages based on the hardware without creating multiple TS's.

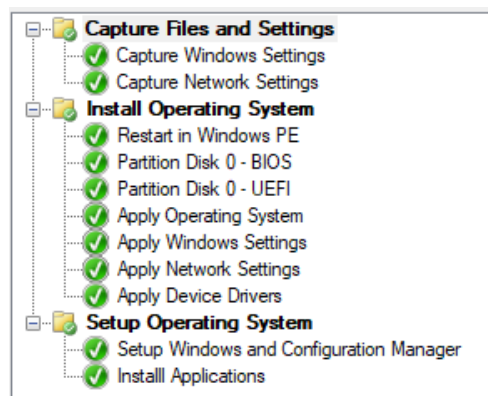


Figure 3.23: Task Sequence Reimaging tasks

3.4.3 BitLocker

There are pre-made tasks in Configuration Manager for configuring BitLocker, which are created and populated by the TS Wizard if Bitlocker is selected. It is not possible to enable this in our vSphere environment, so it has not been tested. It is also possible to configure this through policy which offers more granular configuration, which is described in Section 4.1.1

Figure 3.24: Task Sequence BitLocker

3.4.4 Troubleshooting

When creating and installing a new OS with a TS, many things can go wrong during the installation. All the actions done by the TS is logged in a file called smsts.log which can be found locally on the client, and is the place to start if a deployment fails. The location of the file varies depending on where the deployment stopped:

- Before the disk is formatted and partitioned
 - x:\windows\temp\smstslog\smsts.log
- After the disk is formatted and partitioned
 - C:_SMSTaskSequence\Logs\Smstslog\smsts.log
- After OS is installed

- `c:_SMSTaskSequence\Logs\Smstslog\smsts.log`
- After Configuration Manager client is installed
 - `c:\windows\syswow64\ccm\logs\Smstslog\smsts.log`
- When TS is finished
 - `c:\windows\syswow64\ccm\logs\smsts.log`

Microsoft has released a debugging tool for this, called TS Debugger. Note that this tool is still a pre-release feature, meaning that it is still in an early phase of development[50]. This tool has not been used in this project.

3.5 Microsoft Remote Assistance

MS Remote Assistance is fairly easy to set up as it is bundled with Windows 10. There are several ways to utilize the service, but to minimize the attack surface, the use will be restricted to only allow users with the proper rights to initialize Remote Assistance. This means that a regular user cannot invite others to help, it can only accept an offer from an authorized user, most likely an IT admin. This is achieved by only enabling the "Configure Offer Remote Assistance" policy. This policy requires a list of authorized users that can offer unsolicited remote assistance.

By only enabling unsolicited offers by authorized users, the risk of security breaches by social engineering and typos are greatly reduced, by restricting regular users from inviting others. The end user can also be fairly confident that the user offering assistance is legitimate as the assistance offer can only come from an authorized user, and is unlikely to appear without any communication from the end user to the IT department. The end user must agree to the connection, and must also agree to let the remote user take action on the client.

To utilize this service, the user offering assistance can open the "Run" box by pressing the Windows key + 'r' and type "msra /offerra". From here type the host name or IP address of the client that needs assistance. It is also accessible from the Remote Assistance application and navigating to "Help someone who has invited you" and clicking on "Advanced connection option for help desk".

It is also possible to use Remote Assistance from the Configuration Manager console by navigating to the right computer in "Assets and Compliance" - "Device", and select "Start" - "Remote Assistance".

3.6 Update Management

Update Management is a major part of a healthy Windows domain environment, but it can also be a major headache to configure and maintain. Therefore, our goal when setting up Configuration Manager SUP(Software Update Point) together with WSUS, is to make it as efficient and manageable as possible. Another requirement to take into consideration is the limited bandwidth available to certain branch offices in the infrastructure. Minimizing the amount of data transferred from server to client should therefore be a priority. Lastly, by request from HDO, a feature to give users a certain degree of control over when updates can take place must be implemented. This is to ensure no unnecessary and untimely downtime occurs in high intensity work situations.

3.6.1 Preliminary update catalog maintenance

Before getting into the update plan, or how and when updates will get pushed out, steps to optimize WSUS and the SUP were taken. Whenever a workstation requests updates via its Configuration Manager-client, from its site server, a scanning operation takes place. The entire update catalogue is scanned to find which updates might apply to the specific client. If the update catalogue is not properly maintained, this process will be both time-consuming and resource-intensive [51]. Within an "unclean" catalogue, most of the updates are going to be superseded (meaning newer updates have taken their place). Seldom, if ever, is there any point in scanning or rolling out these superseded updates, so removing them will get rid of some major overhead.

First off, re-indexing the WSUS database helps staving off performance loss over time. This is not specifically needed in a new environment such as this one, but by setting up the method for how to do it, it will be easier to re-index at a later date. This was done by running a script developed by Microsoft, as a query in SQL [52]. To keep high performance over time, it is recommended to run this script periodically, either as a maintenance plan within SQL, or as a scheduled task. A different script creating two separate indexes within the WSUS database, to make the process of declining useless updates up to 30 times quicker, was also executed [53]. Both scripts can be inspected in Appendix D and Appendix E respectively.

Now to decline excessive updates. For this, a update maintenance PowerShell script (located in Appendix F) was used [54]. This script allows for a lot of customization, and describing every possibility will take up to much space. The most impactful changes made for our environment were to specify unsupported Windows 10 versions (every version prior to 20H2), and limiting Windows editions to only include Windows 10 Enterprise. Another change made was to decline all other language specific updates except English. This script is set to run as a scheduled task once a week since we will mainly only push out OS updates, but in a

scenario where a lot of software updates should be included, it might be better to run it more often. Before the first run of the task there were 3908 viable updates. After, there were 651. At that point there were a good deal of updates in Configuration Manager which showed up as "expired". Windows deletes these once a week by default, but by running the VBScript found in Appendix C, expired updates are set to be deleted immediately [51].

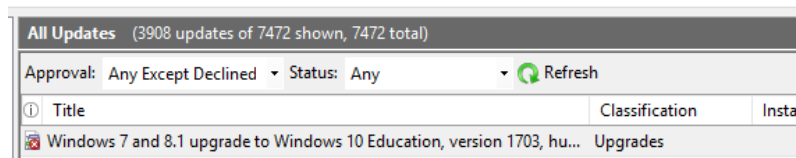


Figure 3.25: Before cleanup

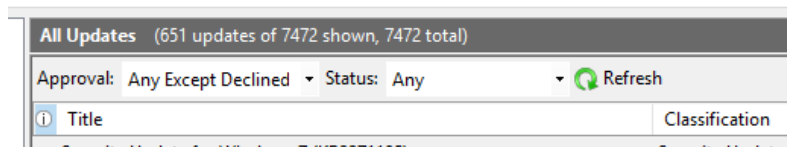


Figure 3.26: After cleanup

3.6.2 Deploying software updates

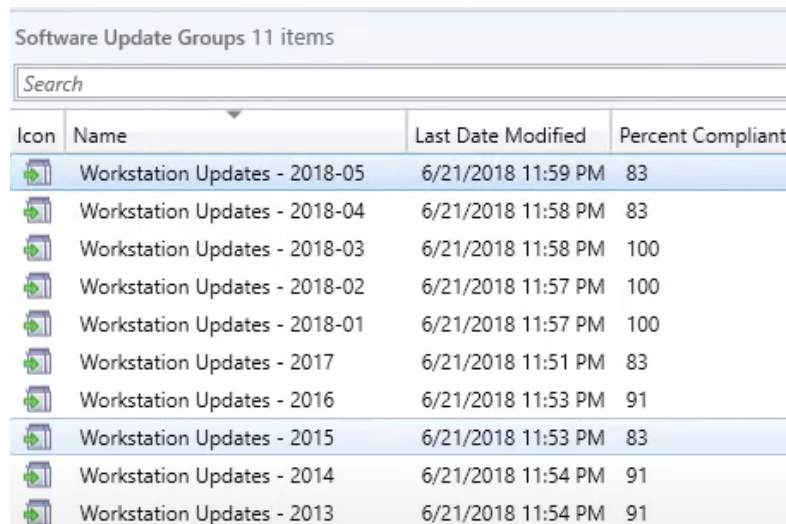
The following deployment scenario is a suggestion based on popular lab environments, but can obviously be altered to fit different needs. Our setup works by specifying three device collections containing workstations (servers are not included as that falls out of scope). The collections are divided into one Pilot collection, where for instance the IT-department could place their own workstations in order to test and verify the newest updates. The second, "Tidlig Utrulling", contain a larger set of workstations where again the update deployment can be tested and verified, before the last collection, "Full Utrulling", which contains the rest of the clients, receives its deployment.

For the intended client environment that HDO will potentially manage with this solution, three distinct collections will not be strictly necessary, as for instance the IT-department will not be present within the same network. The three collections will be kept in the solution anyway, for reference and to display the functionality. There is also a fourth collection named "Maintenance Window". This collection includes all workstations, except for those placed in the "Pilot" or "Early adapters" collection. This collection simply defines a daily time frame where the clients can download and install updates. In our environment this windows lasts from 00.00 to 06.00, Monday through Thursday, as this time period statistically is the least hectic, according to HDO. As for the remaining clients in the other two collections, a custom client policy has been set increasing the default restart deadline from 90

minutes to 8 hours. This is done to give the users here some extra time since the maintenance windows does not apply to their workstations. However, after HDO specified that no forced restarts should occur, this policy was altered. Section 3.6.4 describes how clients are kept compliant with software updates, without having forced reboots enforced.

3.6.3 Automatic Deployment Rules

To deploy software updates in Configuration Manager, the "cleanest" way is to gather relevant updates together into Software Update Group (SUG). For a new environment such as this one, a good way of grouping updates when first starting out, is to utilize the search function for updates, filtering by "Required update" and "Windows Version", and group together all older updates first by year, then by month until the current month is reached. An example Software Update Group structure might look like this [55]:



Icon	Name	Last Date Modified	Percent Compliant
	Workstation Updates - 2018-05	6/21/2018 11:59 PM	83
	Workstation Updates - 2018-04	6/21/2018 11:58 PM	83
	Workstation Updates - 2018-03	6/21/2018 11:58 PM	100
	Workstation Updates - 2018-02	6/21/2018 11:57 PM	100
	Workstation Updates - 2018-01	6/21/2018 11:57 PM	100
	Workstation Updates - 2017	6/21/2018 11:51 PM	83
	Workstation Updates - 2016	6/21/2018 11:53 PM	91
	Workstation Updates - 2015	6/21/2018 11:53 PM	83
	Workstation Updates - 2014	6/21/2018 11:54 PM	91
	Workstation Updates - 2013	6/21/2018 11:54 PM	91

Figure 3.27: Software Update Group structure example

By doing this it becomes easier to know exactly which updates have been deployed to which Device Collections, and if a new unpatched machine is added, it is easy to get it up to date with previous updates. At this point one can go through and deploy each SUG for the "Broad Deployment"-collection to get all clients up to date. As these are older updates, they should be revised and cause no issues when deploying directly to all clients [55].

New updates are handled through the use of Automatic Update Rules (ADRs). ADR is a feature of Configuration Manager in which one can approve and deploy software updates automatically based on a set of rules. For workstation updates two ADRs have configured, based on HDOs wishes. The first, named "Workstation

updates *Critical*” handles more pressing security updates. It includes patches classified by Microsoft as ”Critical Updates”. The second, ”Workstation updates”, is a larger deployment which handles the bulk of new updates. It includes the updates classifications ”Updates”, ”Update rollup”, ”Definition Updates”, and ”Security Updates”.

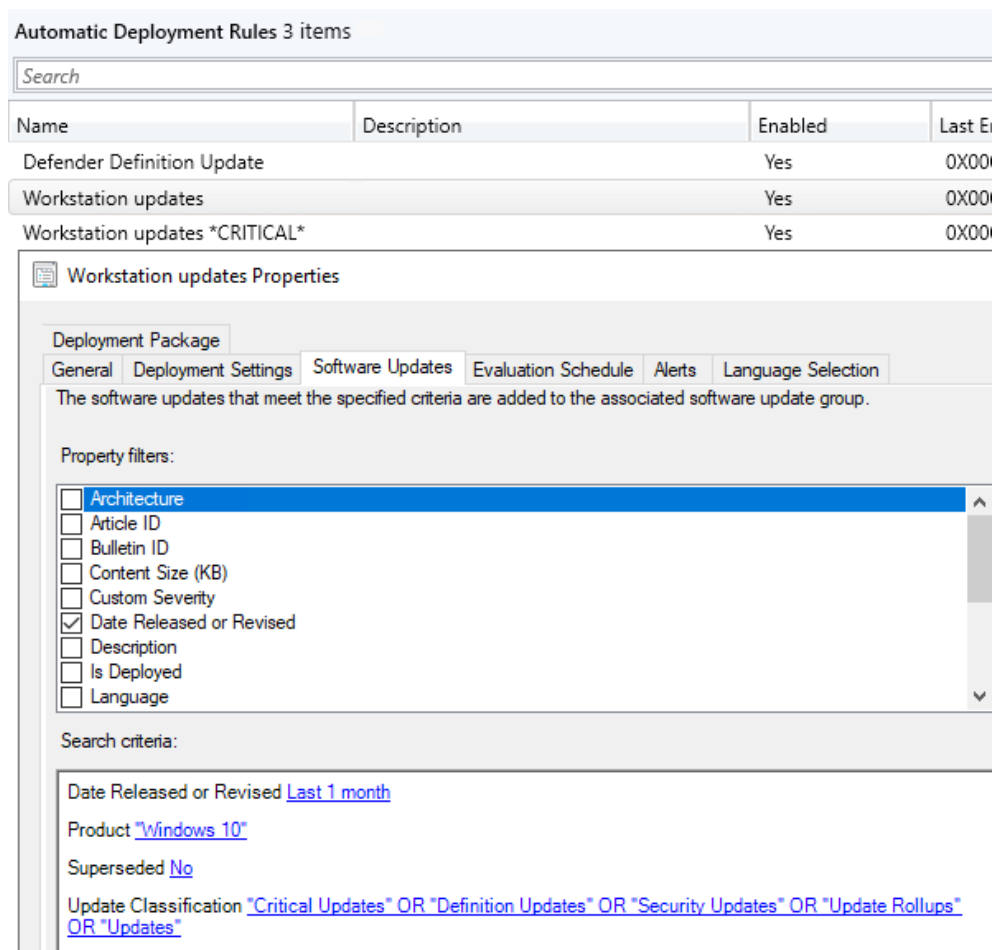


Figure 3.28: Workstation Updates ADR

These two ADRs conform to a modified Patch Tuesday-template, meaning that they run on the second Wednesday of each month. Patch Tuesday is usually when Microsoft drops their monthly security and feature patches [56], and to be sure that all updates are available at the time of rollout, evaluation and deployment of the ADRs wait until after midnight to run, which also coincides with the configured maintenance window. The ADR containing updates classified as ”Critical” runs at 01.00, two hours before the larger ADR, to ensure that patching of potential security holes are prioritized, and to give a separate compliance view to administrators where they can monitor progression of the rollout.

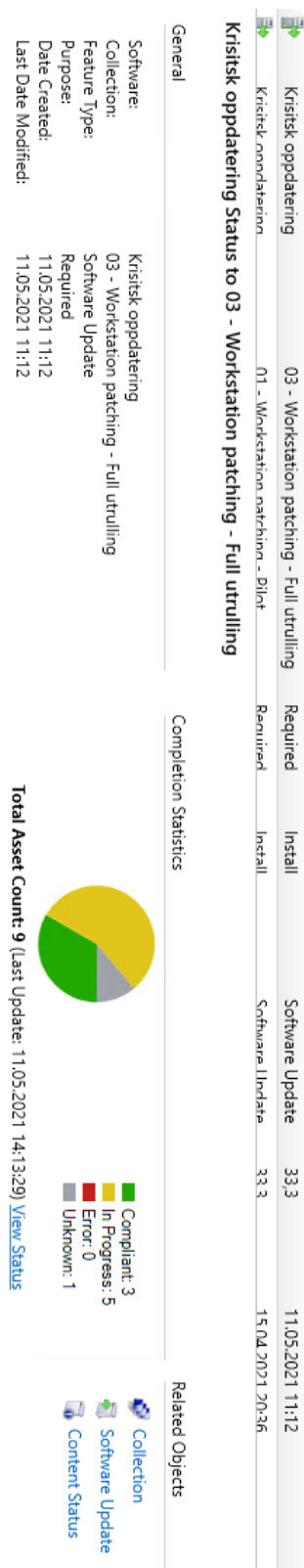


Figure 3.29: Compliance view of a "Critical Update"-deployment

A third ADR, "Defender Definition Update" is in place to cover definition updates for Windows Defender. This rule is scheduled to run each day after SUP synchronizes (at 23.00). Microsoft drops definition updates up to three times per day, so a daily deployment will keep Defender up to date [55].

3.6.4 Additional Update Features

As requested by HDO, forced reboots will not occur on the clients. At first, this was accomplished by toggling the option "Supress restart - Workstations" for each deployment. However, after updating Configuration Manager to the latest stable version (v.2103) the option to disable forced restart by Configuration Manager was made available in Client Settings. This setting is applied to every client in the environment. Now, the applicable patches will be installed at a specified deadline, and notifications stating that a restart is required is shown to the user. HDO requested that these notifications be "Anoying" while not explicitly forcing reboots, so now they appear every 10 minutes after the deadline. Administrators can monitor each deployment to see if clients are compliant with the rollout, and if necessary, contact the user and request a manual restart.

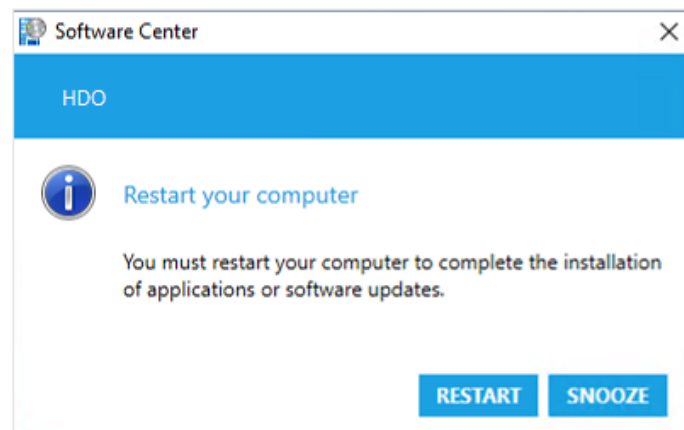


Figure 3.30: This notification will show up every 10 minutes after deadline, in the middle of the screen

Another request made by HDO was to include some functionality to address the low bandwidth connections that exists their remote offices. Microsoft has two viable technologies, BranchCache and Peer cache, which addresses this exact issue and is implemented in Section 3.8.

Lastly, to handle Out-of-band, or particularly critical patches in need of immediate deployment, a specific software update group has been created called "Kritisk Oppdatering". By adding the specific update from "All Software Updates" to this

software update group, and choosing to Deploy using the "Kritisk Oppdatering"-template, the patch will be rolled out with an immediate deadline.

3.6.5 Disable Windows Update

To ensure that clients only receive updates from Configuration Manager, a GPO has been configured to both disable automatic updates, and disable all contact with Windows Update. This is recommended to let the patching of clients happen in a controlled manner. In effect, this change hides the option users have to "Check online for updates from Microsoft Update" in the Windows Update menu, and disables automatic checks against Windows Update [57].

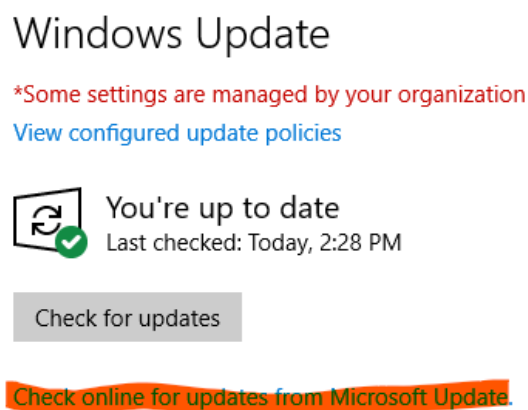


Figure 3.31: The highlighted option was removed.

3.7 Application management

Since manually installing each application needed on every machine would be costly and time consuming, application management through Configuration Manager has been implemented. Configuration Manager has a way to both download, delete and update applications automatically for a whole collection of client machines.

An application in Configuration Manager is a set of installation files and instructions on how the app will be installed on a client machine. This is defined within the application wizard. When the new application is created, there are two ways to install the application to a client machine:

- Deploying the application with the OS image.
- Adding an application to Software Center.

3.7.1 Deploying an application

When adding a new application to Configuration Manager, an executable (EXE) or MSI file can be used. When the application is added, it needs to be deployed to a collection. In the case of testing, Firefox has been deployed to the "all systems collection". This deployment has also been set to "required", which means it is installed automatically to all clients in the collection it is deployed to. If the software should be added to the software center, the deployment can be added as available rather than required. This has not been done, given that HDO would like no user interaction on deployment of new machines.

3.7.2 Obstacles

When a new application is deployed to a collection, the Configuration Manager needs a detection method to check if the installation of an application is done correctly. This detection method can either be a defined script, or a configured rule to detect the presence of the application.

First of, the detection method used was the product code of the program. This quickly failed, when Configuration Manager was holding on the production code of the .msi file, and firefox.exe was installed on each client. All of the client machines therefore constantly responded with a "new software requirements", even though Firefox already was installed. This was fixed by changing the detection method to be to the folder where Firefox is installed, and detecting whether or not firefox.exe is installed.

The screenshot shows a configuration window titled "Specify the file or folder to detect this application." It contains the following fields and controls:

- Type:** A dropdown menu set to "File".
- Path:** A text box containing "C:\Program Files\Mozilla Firefox". To the right of this box is a "Browse..." button.
- File or folder name:** A text box containing "Firefox.exe".
- Checkboxes:** A checked checkbox with the label "This file or folder is associated with a 32-bit application on 64-bit systems."

Figure 3.32: Detection method for Firefox

3.8 Caching

Peer cache and BranchCache were enabled as a proof of concept. It is not possible to recreate HDO's infrastructure to see how it would behave, so it is hard to tell how effective it would be.

3.8.1 Peer Cache

Peer cache was enabled by creating a new Client Settings item in Configuration Manager, selecting "Client Cache settings", and enabling Peer cache. Configuration Manager then automatically opens the necessary ports in Defender Firewall on the Peer cache sources as seen in Figure 3.34.

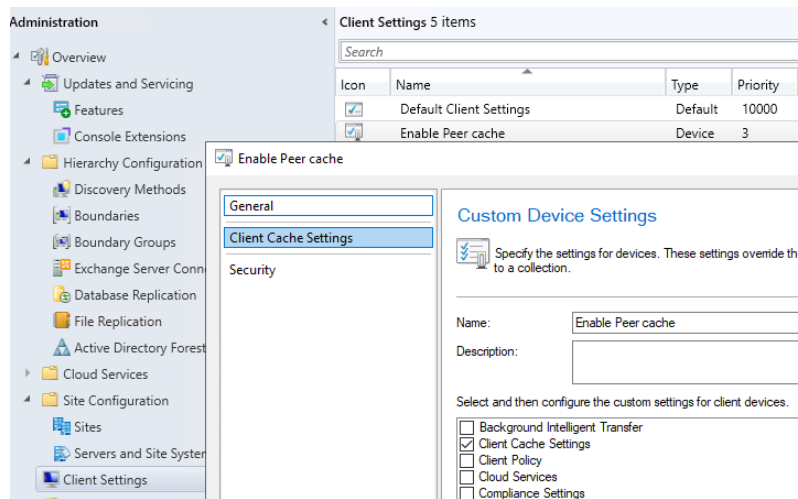


Figure 3.33: Creating Custom Client Settings for Peer cache.

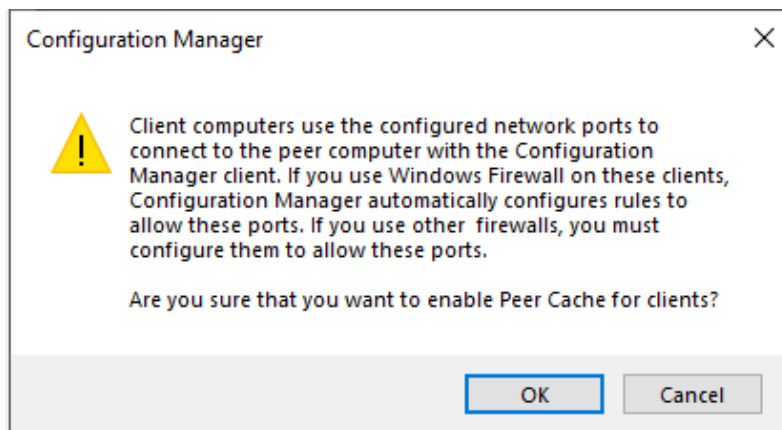


Figure 3.34: Creating Custom Client Settings for Peer cache.

Peer cache sources were selected by creating a device collection called "Peer Cache Sources" and adding the chosen clients to this collection. Lastly, the "Enable Peer cache" Client Settings were deployed to "Peer cache sources". Now, whenever a new device queries for an OS image, update or application, the Peer cache sources will return a list of all its cached content, and sending the package if it is in the same boundary and all requirements are met.

Peer cache utilizes port 8003 and 8004 to send their packages to other machines. And if the packages has actually been sent from the Peer cache source can be seen in the CAS log of the client machine.

```
Httpport:8003, Broadcastport:8004]LOG]!
... 110611...+time="10.25.20 272 120"
```

Figure 3.35: CAS log used to check if peer cache source was used.

3.8.2 Requirements

For Peer cache to work properly, the client Peer sources has to be a part of a domain. The clients asking for packages do not have to be part of the domain, but have to be in the same collection group.

It is also worth mentioning that non-Windows images cannot use Peer cache. A Linux or MacOS can neither be a Peer source or a client.

3.8.3 Multiple peer cache sources

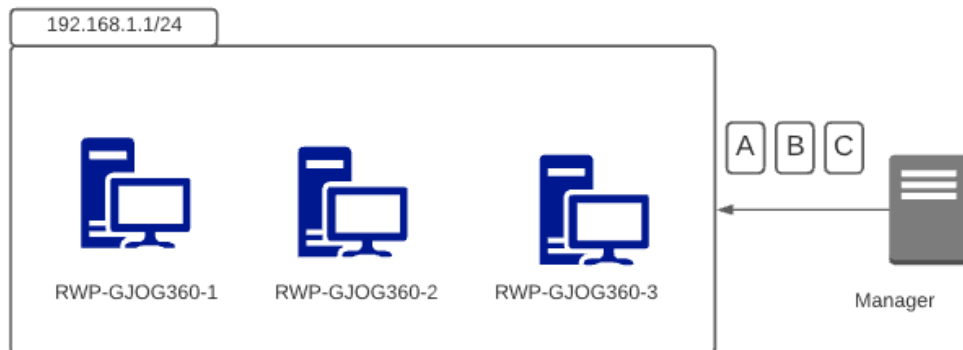


Figure 3.36: Peer cache.

In figure 3.36 a simple example of a branch is added. In this environment, the RWP-GJOG360-1 and RWP-GJOG360-2 are peer cache sources. If there are any new content is distributed, the packages can be split into one or more parts. This is enabled by adding a hierarchy setting in the site, which enables packages to be split to decrease the load of a WAN connection. The first machine will be installing part A telling the second machine, which will immediately begin downloading the second package, B. When the first machine has installed part A, Configuration Manager will tell it to install C, as machine 2 is downloading part B. The last machine, RWP-GJOGG360-3 will wait for a declared set of time before installing

the packages. If this time is set to 1 hour, and the client 3 has not received anything from the two peer sources, it will ask the configuration manager for the packages.

3.8.4 BranchCache

BranchCache is a Windows native feature which is enabled through GPOs. It is possible to do it along with Peer cache in Client settings, but Windows Defender Firewall rules will not be set automatically like Peer cache, so it is tidier to do all in one place.

BranchCache was configured to be in "Distributed cache" mode as there are no servers to configure "Hosted cache" on. The differences are explained in Section 2.4.10. Detailed instructions on how to enable BranchCache can be found ². One setting that was enabled that is not mentioned in the instructions was "Set percentage of disc space used for client computer cache". It was set to 15%. The default value is 5%.

Once the GPO settings are set and the GPO is linked to suitable OUs, BranchCache will be self sustaining and need no further maintenance.

3.8.5 Caching effectiveness

Figure 3.37 shows a donut chart from Configuration Manager's "Client Data Sources" monitoring feature. It shows the distribution of how much content clients have retrieved from the different sources the last week. It shows that 20% of requested content has been retrieved from other clients instead of the distribution point. Considering that BranchCache and Peer cache had not been enabled for more than a couple of days when the data was collected, 20% is a considerable amount.

²<https://docs.microsoft.com/en-us/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers>

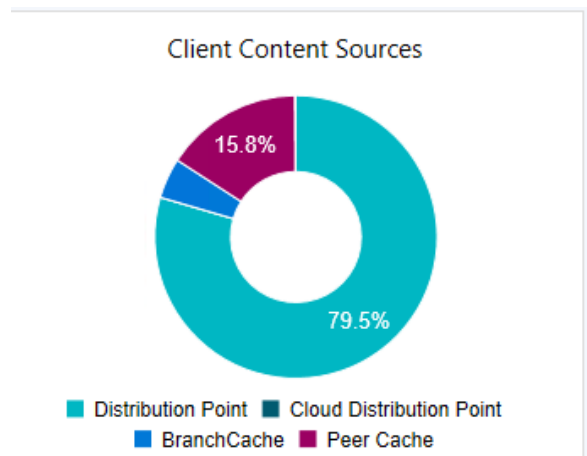


Figure 3.37: Client content sources last seven days.

Chapter 4

Securing the Windows workstation environment

The securing a Information Technology-system is a perpetual process, and is never finished, which is also the case in this project. The security focus in this project has been on reducing the attack surface on the Windows clients. This was done by researching best practices and security controls for Windows domains and Windows client hardening. Implementing best practice security for the entire system, including the backend and underlying infrastructure, is too big of a task to be included in this project. This is why only securing the clients, and some systems directly affecting client security, have been prioritized.

4.1 Endpoint Protection

Configuration Manager has built-in features for managing security on client machines, called Endpoint Protection (EP). EP manages anti-malware policies, BitLocker, and Windows Defender Firewall on clients managed by Configuration Manager [58]. EP policy distribution is managed through device collections, making it easier to manage client with different needs. Microsoft Defender for Endpoint (MDE) earlier known as Microsoft Defender Advanced Threat Protection (MDATP) is also supported through this software, but has its own separate licensing from Configuration Manager, and must be purchased separately or through the office 365 E5 package. The anti-malware policy and Microsoft Defender Firewall comes with the licensing of Configuration Manager.

4.1.1 BitLocker

Unfortunately, BitLocker is not supported on Virtual machines or in VMWare, as stated in Microsoft documentation

BitLocker management isn't supported on virtual machines (VMs) or on server editions. For example, BitLocker management won't start

the encryption on fixed drives of virtual machines. Additionally fixed drives in virtual machines may show as compliant even though they aren't encrypted [59].

BitLocker has therefore only been added, but testing of this functionality could not be done as the disk will not be encrypted.

Implementing BitLocker

BitLocker was implemented by creating a new policy in the EP folder.

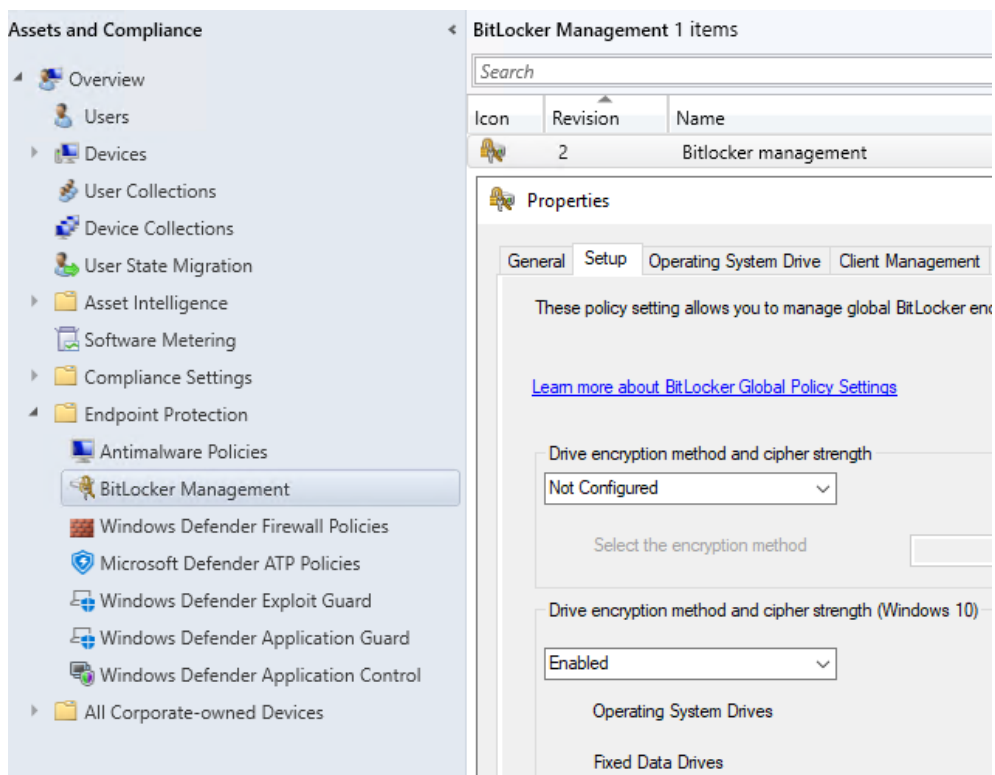


Figure 4.1: BitLocker in Endpoint Protection

In this folder, the prerequisites were defined in the BitLocker wizard. In the wizard, the encrypted components and encryption method is set. The encrypted components is the Operating System Drive and Fixed drives. Drive encryption method for Windows 10 was enabled with the AES-XTS Block Cipher Mode. This block cipher encrypts a block of 256-bit, and uses two EAS keys to perform encryption, with one encrypting the AES block, and the second one encrypting the "Tweak Value". The disk is encrypted with TPM and will now prompt for a password, this could also be changed to a pin with a set length and value. After all properties were defined, the policy was deployed to the "All Windows 10 machines" collection. Verification

can be done by checking the Microsoft Bitlocker Administration and Monitoring (MBAM) Operational log file locally in event viewer, as done in Figure 4.2

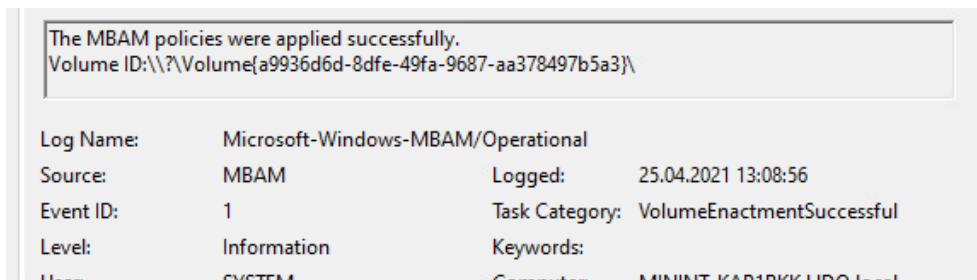


Figure 4.2: MBAM log file

To ensure that the user starts using BitLocker it has to be set to "enforce". If it is not forced it will prompt a user interaction to encrypt the device, and the user has the option to suppress the encryption of the disk. To enforce this, two registry keys has been added through Configuration items. These registry keys has value 0 and 1 and enforces OS policies.

Name	Revision	Last Evaluati...	Complian...
Bitlocker manage...	2	4/29/2021 1...	Compliant
Enforce MBAM En...	2	4/29/2021 1...	Compliant
Windows firewall s...	2	4/29/2021 1...	Compliant

Figure 4.3: Registry key to enforce BitLocker.

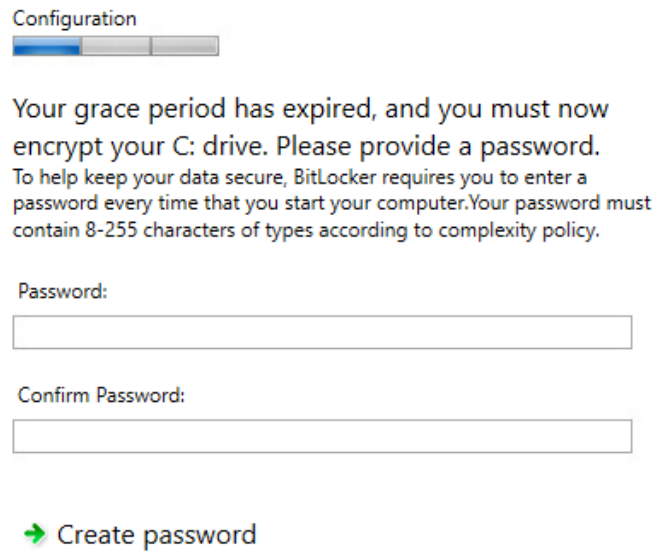


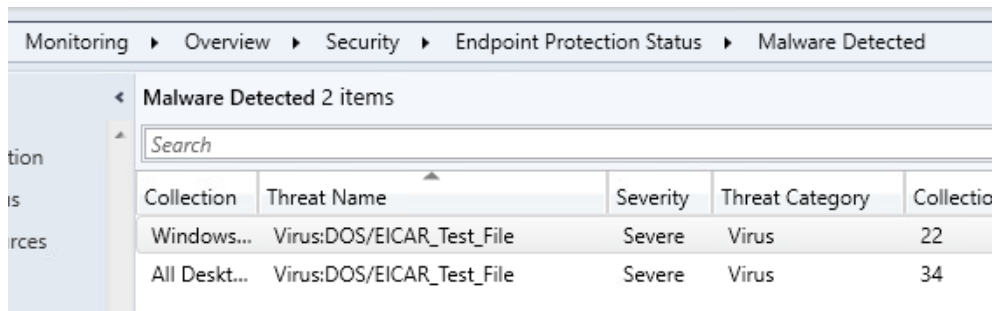
Figure 4.4: enforced BitLocker on a client machine.

As seen in Figure 4.3 the BitLocker policy is compliant with both the registry key enforce Microsoft Bitlocker Administration and Monitoring encryption and BitLocker management. These registry keys enforces the policy to the computer as seen in Figure 4.4,

4.1.2 Antimalware policy

The antimalware policy in EP specifies how computers in a collection are protected from malware and other threats. EP comes with a default template. This template includes information regarding scheduled scans, such as weekly or daily scans, which folders will be scanned, if user interaction will be necessary and what action Windows Defender should take if malware is detected on any of the client machines.

The antimalware policy currently deployed in the domain environment runs a daily quick scan on each client. The scanner runs recursively through the C: drive folder, emails received and removable drives. Files that are identified as malware are displayed in the security monitoring section as seen below (Figure 4.5).



The screenshot shows the Windows Defender 'Malware Detected' window. The breadcrumb trail at the top reads: Monitoring > Overview > Security > Endpoint Protection Status > Malware Detected. Below this, a header bar indicates 'Malware Detected 2 items'. A search bar is present. The main content is a table with the following data:

Collection	Threat Name	Severity	Threat Category	Collection
Windows...	Virus:DOS/EICAR_Test_File	Severe	Virus	22
All Desk...	Virus:DOS/EICAR_Test_File	Severe	Virus	34

Figure 4.5: Antimalware file quarantined by Windows Defender

The detected malware is the EICAR Standard Anti-Virus Test File [60]. This was downloaded on one of the client machines to test the monitoring function from Configuration Manager.

4.2 Security Baselines

Security Baselines are pre-configured GPOs created by security teams aiming to secure Windows clients [61]. Depending on the publisher and intended usage they might vary in both settings and strictness, but are mostly covering the same points.

In this project two baselines have been used to create the security GPO. Security Technical Implementation Guides (STIG) GPO and Windows Security Baselines, where the strictest settings have been used.

4.2.1 Security Technical Implementation Guides

The STIG are best practice controls for installing and supporting government information systems in the United States of America. The STIGs are created by the Defense Information System Agency (DISA), and published by the Department of Defence (DoD) on the DoD Cyber Exchange [62].

As part of the STIGs are a set of baseline GPOs covering Windows 10, Windows Server, Google Chrome among others [63]. To review the settings in a STIG GPO, DISA has developed a tool called STIG Viewer. STIG Viewer imports a STIG benchmark file for appropriate and displays argumentation on why a setting should be set, and how to do it manually if need be.

Windows 10 Security Technical Implementation Guide :: Version 2, Release: 1 Benchmark Date: 13 Nov 2020		
Vul ID: V-220862	Rule ID: SV-220862r569187_rule	STIG ID: WN10-CC-000330
Severity: CAT I	Check Reference: oval:mil.disa.fso.windows:def:4092	Classification: Unclass
Legacy IDs: V-63335; SV-77825		
Rule Title: The Windows Remote Management (WinRM) client must not use Basic authentication.		
Discussion: Basic authentication uses plain text passwords that could be used to compromise a system.		
Fix Text: Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> "Allow Basic authentication" to "Disabled".		

Figure 4.6: STIG Viewer group policy setting example for Windows 10

All settings for the "Windows 10 STIG Benchmark" were manually reviewed before they were set, where the ones that in that for some reason were not usable were written down in Table 4.1.

Stig-ID	Vulnerability	Description	Status
WN10-00-000155	V-220823	Solicited Remote Assistance must not be allowed.	Set in other GPO.
WN10-00-000025	V-220743	The maximum password age must be configured to 60 days or less	Not best practice.
WN10-00-000035	V-220745	Passwords must, at a minimum, be 14 characters long.	Not best practice.
WN10-00-000040	V-220746	The built in Microsoft password complexity filter must be enabled.	Not best practice.

Table 4.1: Table displaying excluded GPO's

4.2.2 Creating STIG GPOs

When the STIG GPOs are downloaded a set of support files are bundled with them as seen in Figure 4.7. The file "DISA_STIG_GPO_Import" contains detailed instructions on how to use the other files to create wanted GPOs. In short the PowerShell script "DISA_GPO_Baseline_Import.ps1" is used to create the required GPOs, by specifying them in one of the CSV files. In this project, only the Windows 10 GPO were used. There are others usable ones, like for Windows Defender and Firewall, but these are managed through Configuration Manager. The unwanted settings in Table 4.1 were manually changed or deleted afterwards.

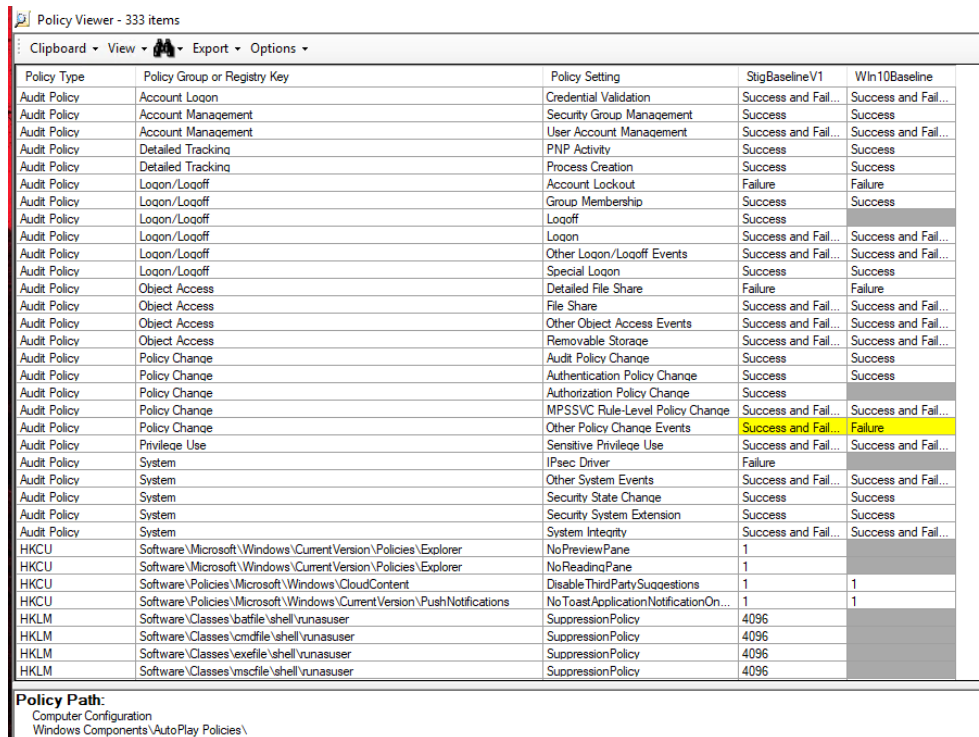
rs > Erik_adm > Downloads > U_STIG_GPO_Package_February_2021 > Support Files >			
Name	Date modified	Type	Si
Local Policies	15.04.2021 13:17	File folder	
DISA_AllGPO_Import_Feb2021	15.04.2021 13:17	CSV File	
DISA_GPO_Baseline_Import	15.04.2021 13:17	Windows PowerS...	
DISA_Quarterly_Import_Feb2021	15.04.2021 13:17	CSV File	
DISA_STIG_GPO_Import	15.04.2021 13:17	Microsoft Word D...	
importtable	15.04.2021 13:17	MIGTABLE File	
Sample_LGPO	15.04.2021 13:17	Windows Batch File	

Figure 4.7: STIG GPO Support files

4.2.3 Windows Security Baselines and Policy Analyzer

Microsoft has released a product called Security Compliance Toolkit v1 (SCT), which in essence is a collection of tools aimed to help system administrators edit and compare their GPO settings to other GPO baselines, specifically, Microsoft-recommended security configuration baselines for Windows [64].

Windows "Policy Analyzer tool" were used to compare the STIG with Windows Security baselines (for version 20H2) [65], to see if there are any discrepancies. The Policy Analyzer tool included in SCT is made for this exact purpose. It takes sets of imported GPOs (in GPO backup-format), and highlights the differences. SCT also includes the relevant Microsoft Security baselines, and in this comparison, all endpoint related Windows 10 Security baselines were used.



Policy Type	Policy Group or Registry Key	Policy Setting	StigBaselineV1	Win10Baseline
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	Success	Success
Audit Policy	Detailed Tracking	Process Creation	Success	Success
Audit Policy	Logon/Logoff	Account Lockout	Failure	Failure
Audit Policy	Logon/Logoff	Group Membership	Success	Success
Audit Policy	Logon/Logoff	Logoff	Success	
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	Failure
Audit Policy	Object Access	File Share	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Removable Storage	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success
Audit Policy	Policy Change	Authorization Policy Change	Success	
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Other Policy Change Events	Success and Fail...	Failure
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	Success and Fail...
Audit Policy	System	IPsec Driver	Failure	
Audit Policy	System	Other System Events	Success and Fail...	Success and Fail...
Audit Policy	System	Security State Change	Success	Success
Audit Policy	System	Security System Extension	Success	Success
Audit Policy	System	System Integrity	Success and Fail...	Success and Fail...
HKCU	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoPreviewPane	1	
HKCU	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoReadingPane	1	
HKCU	Software\Policies\Microsoft\Windows\CloudContent	DisableThirdPartySuggestions	1	1
HKCU	Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications	NoToastApplicationNotificationOn...	1	1
HKLM	Software\Classes\batfile\shell\runasuser	SuppressionPolicy	4096	
HKLM	Software\Classes\cmdfile\shell\runasuser	SuppressionPolicy	4096	
HKLM	Software\Classes\exefile\shell\runasuser	SuppressionPolicy	4096	
HKLM	Software\Classes\mscfile\shell\runasuser	SuppressionPolicy	4096	

Policy Path:
 Computer Configuration
 Windows Components\AutoPlay Policies\

Figure 4.8: Policy Analyzer

Figure 4.8 shows the output of Policy Analyzer, and the column named "Stig-BaselineV1" represents the GPOs already in place, and "Win10Baseline" the GPOs recommended by Microsoft. With a quick overview it is apparent that the STIG-baseline both contain more GPOs, and in instances where the same GPO exists in both baseline, STIG takes the "stricter" stance. A couple notable exceptions are GPOs regarding Windows Defender antivirus and firewall which are configured in the Win10Baseline, but not in the STIG baseline. However, these are settings controlled centrally by Configuration Manager, and it is not advised to have GPOs

governing Windows components controlled by Configuration Manager, as that might lead to malfunction of said components. Some changes were made based on the results of Policy Analyzer, which can be inspected in Appendix K

4.2.4 Configuration Baselines

Configuration Manager includes a feature called "Configuration Baselines" [66] under "Compliance Settings". In a larger environment, ensuring that the correct policy is being applied to every client can be difficult, if not completely infeasible as it often comes down to an IT-administrator having to log on to the client in question and run the "gpresult"-command in the Command Line. When there are hundreds or thousands of clients, checking for compliance might be reduced to either hoping for the best, or taking a few individual sample tests. By establishing a Configuration Baseline in Configuration Manager, you can monitor if specific, or every GPO, is being applied successfully on all workstations in a given collection [66].

A Configuration Baseline based on all endpoint-related GPOs is set in the environment. This was done using a tool called "Microsoft Security Compliance Manager" [67] to convert a backup of all configured GPOs into a DCM-format, and importing the resulting file into Configuration Manager. When importing, the DCM-files gets converted to Configuration Items, which can be organized together into a Configuration Baseline.

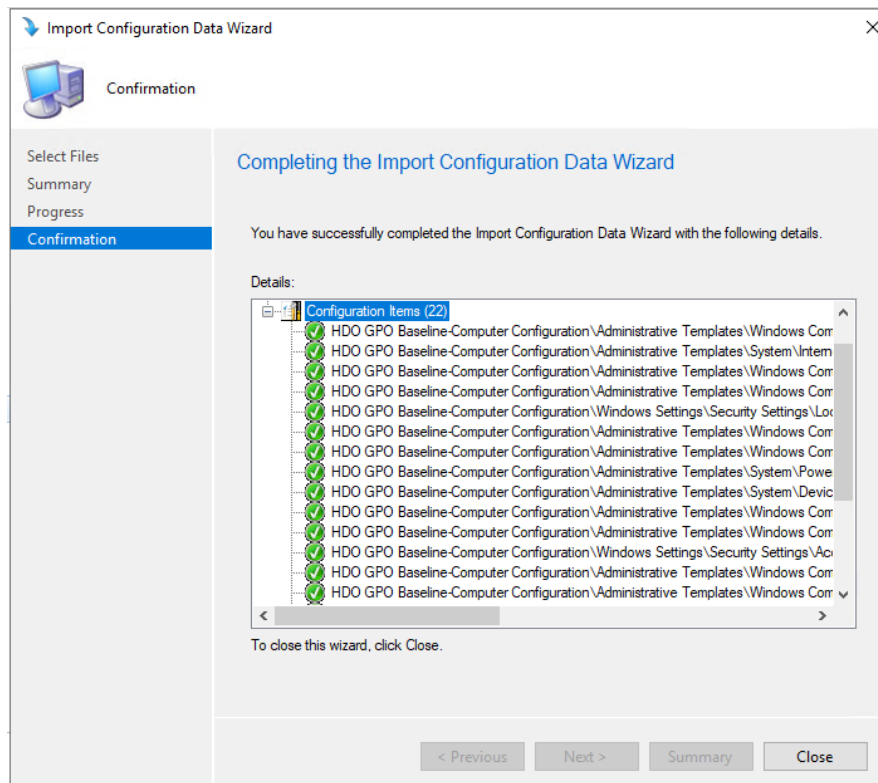


Figure 4.9: Importing GPO's as Configuration Items

The configuration baseline named "HDO GPO Baseline" is deployed to the collection "Full Utrulling", and is set to run every Wednesday at 04.00. When deploying, the option to "Remediate noncompliant rules" is presented. This means that the Configuration Manager-client will alter the registry values of a client to comply with the values set in the configuration baseline, if any discrepancies are found. In effect forcing the change a missing GPO would make. This option is enabled in "HDO GPO Baseline".

4.3 Local Administrator Password Protection

LAPS is Microsoft's solution to secure local admin management [68]. In essence, it functions as a built-in password manager integrated with AD. A common security issue in Windows domains is that the local admin account is set with the same password for every endpoint, making horizontal movement within the organization much simpler for a malicious actor. Microsoft's best practices on local administrator accounts advises to either rename, or disable the account all together [69]. Renaming the account might be a good idea, as the local administrator account is very well known to attackers, and a common target in attacks. However, simply renaming the account does not change the Security identifier (SID), which

will still be discoverable by attackers. Disabling the account might be a good option, as many of the required actions needing local administrator-level privileges are usually accomplishable using workarounds. However, this would introduce a host of manageability issues, and in general increase time spent administrating endpoints.

Introducing LAPS into the environment mitigates many of these issues, simply by setting a unique password for local administrator per endpoint. Instead of disabling or renaming the local admin account, users will have to request the password from a select group of administrators with rights to read the password in Active Directory. By default, the complexity and length of the password is more than what an attacker can hope to "crack" within a reasonable amount of time, and the expiration date is short enough to not give a malicious actor time to even try. Also, the password is unique for each computer, effectively mitigating against "pass-the-hash"-attacks of the local administrator [70].

Implementation of LAPS [71] involves a server and a computer component, as the technology works in a "push" manner, where the computer client sets a new password, and "pushes" this into AD. Setup of LAPS starts by installing the full LAPS package (with all features included) on the DC. This package includes a PowerShell module with a few commands, where three are specifically needed to get LAPS working. The first command, "Update-AdmPwdADSchema" updates the AD schema of computer objects to include two new attributes: The first to hold the actual local administrators password, and the second to hold the expiration date of the password.

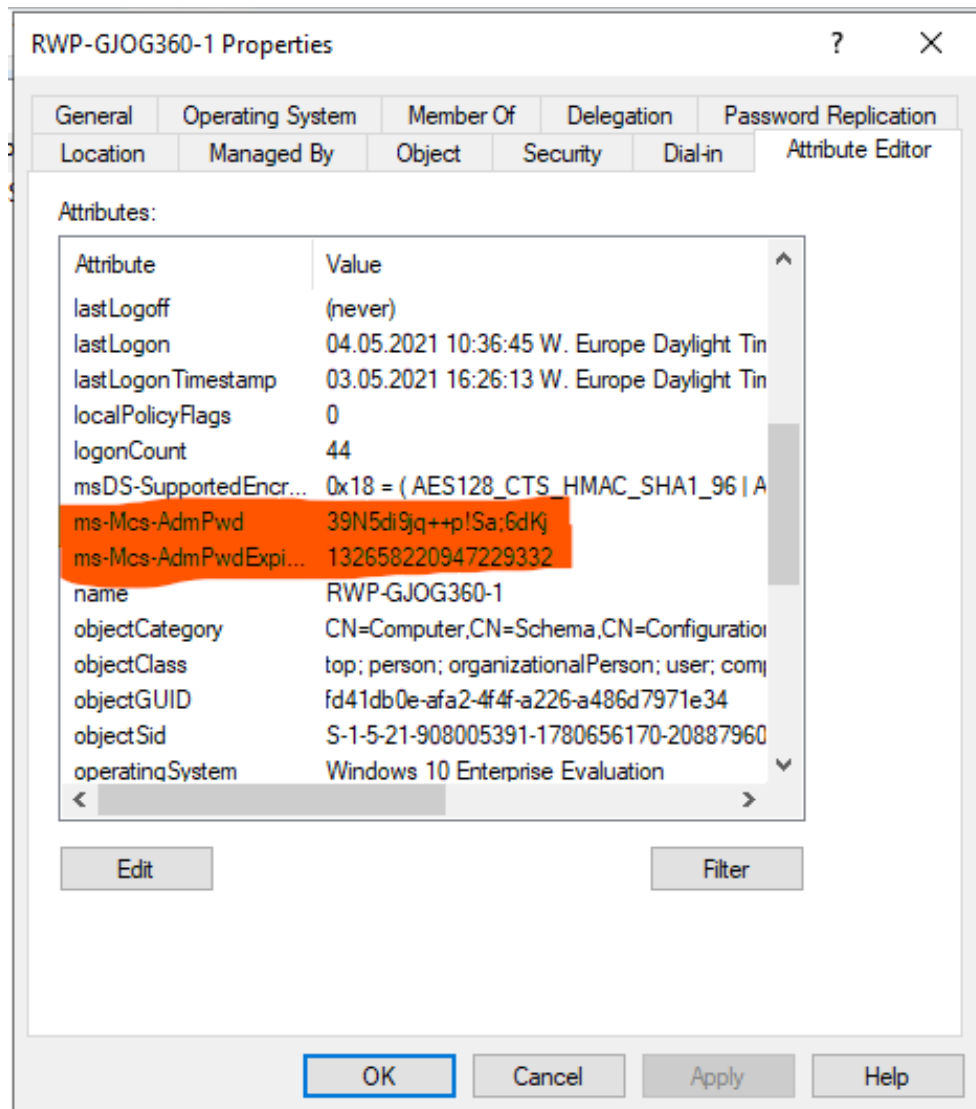


Figure 4.10: New computer-objects attributes

The second command, "Set-AdmPwdComputerSelfPermission -OrgUnit SCCM_Site_PR1_Workstations", gives the computer-objects in the OU "SCCM_Site_PR1_Workstations" the right to alter itself, which is necessary for it to update its own password. The third command, "Set-AdmPwdReadPasswordPermission -OrgUnit SCCM_Site_PR1_Workstations -AllowedPrincipals HDO/LAPS PW Admin", as well as a near identical command "Set-AdmPwdReadPasswordPermission", determines who shall have access to read and reset the local admin password for all computers in the specified OU. This permission is delegated to members of the "LAPS PW Admin"-group.

Next, a GPO which enables management of local admin passwords, and specifies password complexity and password age, must be configured. This setting is found

under "Computer Configuration/Policies/Administrative Templates/LAPS". Password length is set to 20 characters, and password age is set to 15 days.

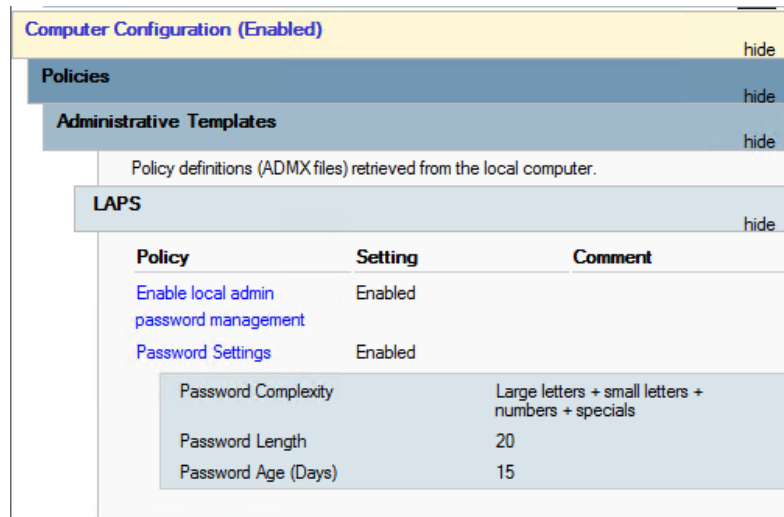


Figure 4.11: LAPS password settings.

To get LAPS working on the computer side, the same LAPS-package installed on the server must be installed here, although only the "AdmPwd GPO extension" feature is needed.

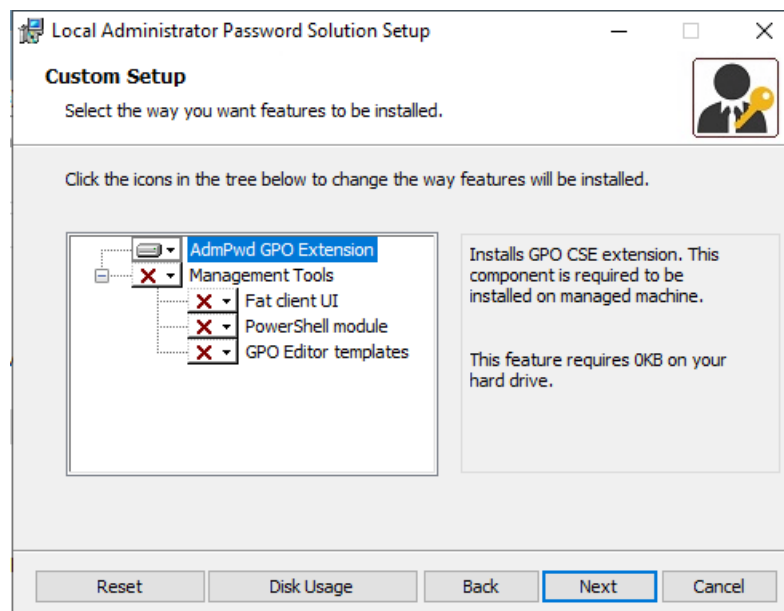


Figure 4.12: Shows the only needed feature of the installation package.

In our environment this package is deployed via the Configuration Manager TS,

meaning the newly provisioned computers will have LAPS functioning from the start.

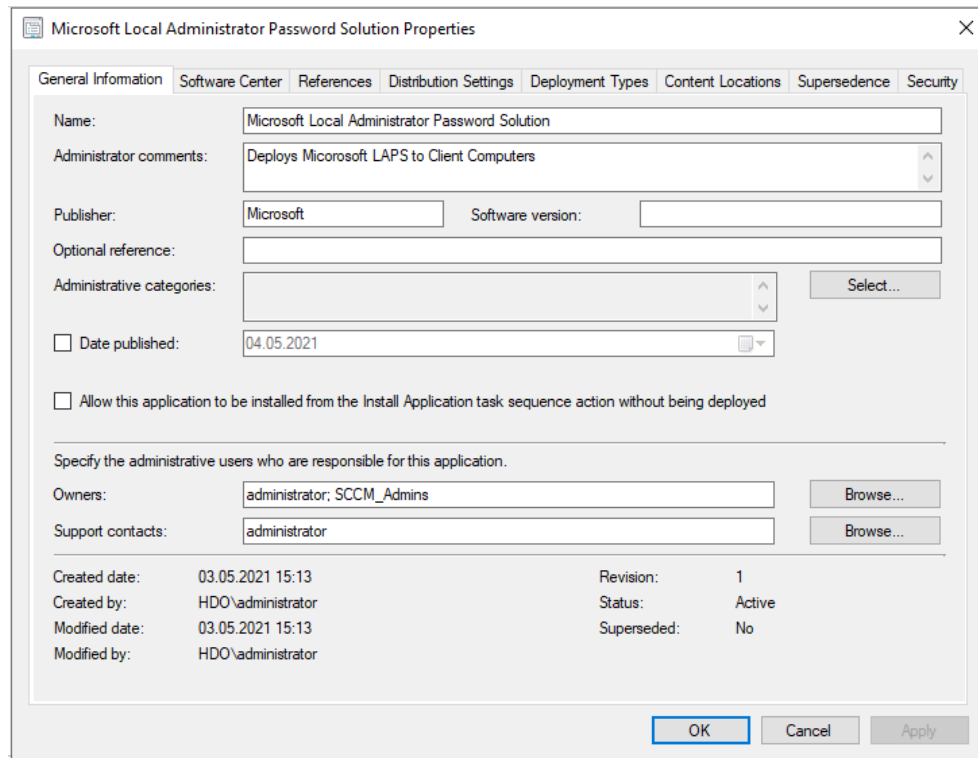


Figure 4.13: The LAPS Configuration Manager Application-package included in the provisioning TS

Finally, whenever a user with legitimate need to use local administrator request the password, a member of the "LAPS PW Admin"-group opens the "LAPS UI" (installed with the initial LAPS package), and enters the hostname of the given computer:

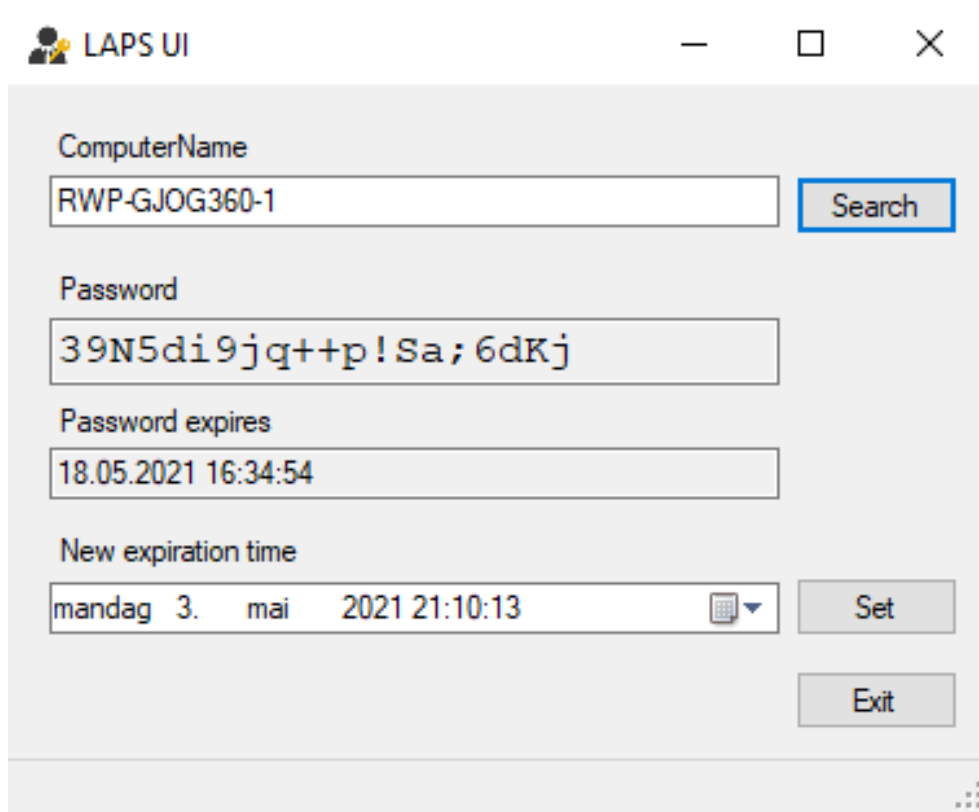


Figure 4.14: LAPS User Interface.

4.4 Password policy

The end goal of any organizational password policy should be a system filled with different, strong passwords. This is what password best practices try to achieve, and the practices changes as more research is done on the matter.

For a time, the best practices for passwords were long, complex passwords with periodic mandatory change [72]. When registering an account online, it's not uncommon to see demands of 14 characters and higher and complexity requirements like including upper/lower case, numbers and characters. These requirements were meant to make the users create strong passwords, but it also makes them hard to remember. Research [73, 74] indicates that most people react in the same predictable way when faced with the aforementioned requirements, like writing them down or use pattern based passwords. This subsequently makes the passwords more similar and easier to guess, ultimately working against achieving the policy goal.

In recent years a new way of thinking passwords has emerged, where focus is

on checking passwords against breached and/or "weak" password lists. Combined with retry limits, it is deemed more secure than its predecessor. Azure AD Password Protection (PP) is used as a password checker in this project and is implemented in Section 4.6.

Multiple credible sources have published their best practices, like Microsoft's "Microsoft Password Guidance" [75], and The National Institute of Standards and Technology (NIST) "Digital Identity Guidelines: *Authentication and Lifecycle Management*" [76]. Microsoft's guide is written in a precise and simple to understand way. It is also written with Active Directory in mind making it easy to look up further if somethings unclear. NIST's document is written in a more technical style, and describes much more detailed scenarios and considerations than is deemed necessary in this project. Considering these factors, and that both outlines the same rules, "Microsoft Password Guidance" will be used as a template for this policy.

The following settings will be implemented in AD to comply with Microsoft Password Guidance:

- Password maximum age: 0
- Password minimum age: 1
- Password minimum length: 8
- Enforce password history: 24
- Complexity requirements: disabled
- Store passwords with reversible encryption: disabled
- Max bad logon attempts: 3
- Bad logon timer: 15 min

The password settings implemented in STIG Baseline, Section 4.2.1 are not in compliance with the settings above and are modified to comply with Microsoft Password Guidance.

Lastly, it is important to note that the rules set in the password policy to conform to best practices require users that have been educated in *why* these rules are set. The requirements set in AD will only get you so far unless the users actively follows the rules managed outside of AD, like writing down passwords etc. People will generally be more compliant if they understand why the rules are in place.

4.5 Password Filters

Active Directory does not include any password filters to check for weak passwords. Best practices regarding password policies are dependant on password checks beyond what AD DS provides. This is discussed further in Section 4.4. There are several products on the market that can be joined with AD DS to provide this

service.

4.5.1 Azure AD Password Protection

Azure Active Directory (AAD) works in similar ways as Active Directory as an Identity and Access Management (IAM) system, only it is used for cloud based systems. With AAD, PP is part of the base solution. PP stops users from choosing known weak passwords and variants of them, using a global block list developed by Microsoft [77]. This list is built by security analysts based on security telemetry from the Azure environment, with no attachments to external data sources, like lists composed of known breached passwords. Microsoft argues that since password spray attacks usually only tries a couple of passwords against each account to avoid detection, their list is more than likely to contain these passwords.

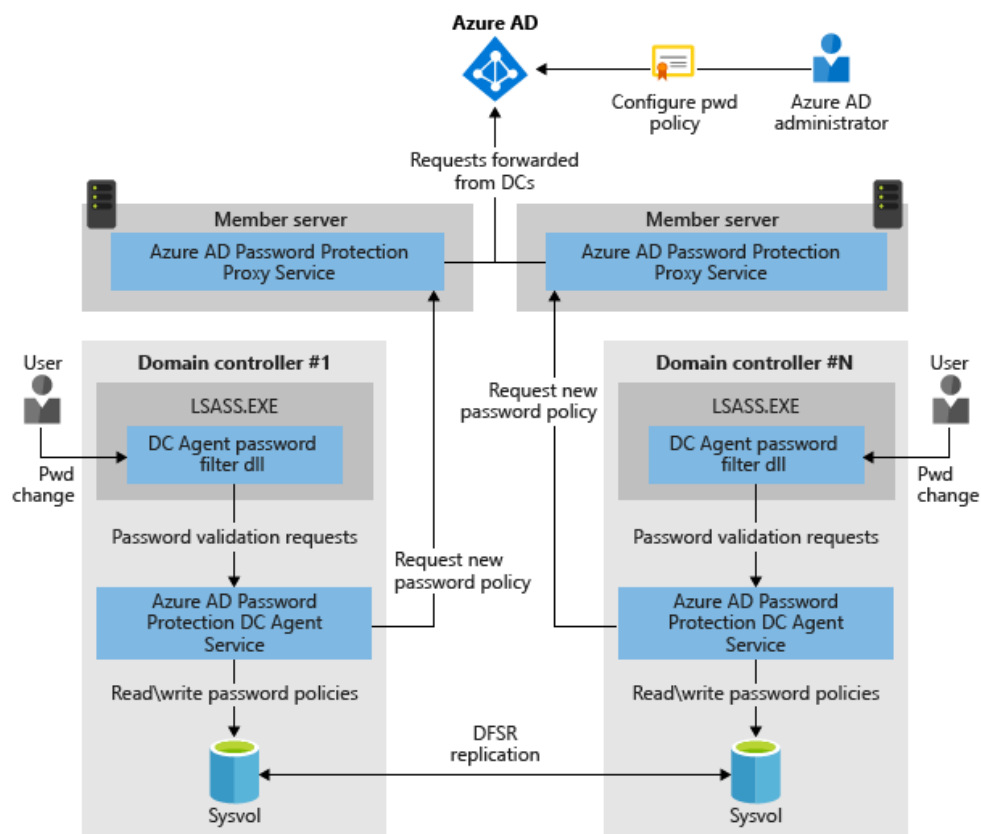


Figure 4.15: Azure Password Protection workflow [78]

PP is also facilitating for improved security through a custom banned password list. This can be used by HDO to prevent users from choosing passwords containing work related terms such as location and system. All terms added to the list will also have other variations of the term blocked. The banned password list is

applied together with the global banned password list.

As PP is an Azure native service, it is not integrated with AD DS. It is however possible to implement it in on-premises AD DS by adding a DC agent and a proxy service.

4.5.2 Anixis Password Policy Enforcer

Password Policy Enforcer [79] provides the same functionality as PP and more, but in a different way. Whereas PP uses a global block list and a "weak password algorithm", Anixis relies their own dictionary rule that detects weak passwords, and a list of leaked passwords. It is hard to tell how it performs against others as there is no data available on that subject. The main difference between PP and Password Policy Enforcer is the enforceable options available. PP and AD DS offers a fairly limited set of rules, only 6. These are the standard ones like min/max password age, length etc. With Anixis, and other third party products such as Specops Password Policy [80], customization is available at a much higher level.

4.5.3 Password filter selection

As these services are installed on DC's and require internet access, the only viable solution is Azure AD PP as cloud services from Azure is the only one permitted, as described in Section 1.2.2.

4.6 On-premise Azure Active Directory Password Protection

PP is a cloud service provided in the Azure Enterprise Mobility + Security E3 and E5 licenses [81]. It was originally meant for AAD, but has been made available for on-premise AD DS as well through the use of a proxy and a DC agent. The proxy is necessary as DC's usually does not have direct access to the internet for security purposes.

4.6.1 Deployment requirements

The following requirements must be met in order for PP to work, as listed by Microsoft [82].

- Azure Enterprise Mobility + Security E3 or E5 license
- At least one DC and one proxy server
- Windows Server 2012 R2 or newer
- .NET 4.5 installed
- Universal C Runtime installed
- Key Distribution Service enabled on all DC's

- Network connectivity between DC and proxies.
- All proxies must have access to the following endpoints:
 - <https://login.microsoftonline.com>
 - <https://enterpriseregistration.windows.net>

4.6.2 Installation

The reason why a cloud-reliant technology such as this has been included, in spite of the "no-cloud"-restriction which has been enforced elsewhere in the thesis, can be found at Section 1.2.2.

The DC and proxy agent can be downloaded from Microsoft ¹. In order for PP to work properly, the DC agent needs to be installed on all DC's that handles password changes. Neither agent needs any installation configuration during setup. The full installation guide can be found here ².

On proxy servers

After installing the proxy agent, the three following commands must be run in a privileged PowerShell session. The user specified after "-AccountUpn" must be a global administrator in Azure.

```
1 Import-Module AzureADPasswordProtection
2 Register-AzureADPasswordProtectionProxy -AccountUpn (Global admin account)
3 Register-AzureADPasswordProtectionForest -AccountUpn (Global admin account)
```

Line one imports the PP PowerShell module, line two enables communication with AAD, and line three registers the on-premise AD forest with the proper credentials for communication with AAD.

4.6.3 Verification

To verify that the DC's have successfully imported any password policies from Azure, one can check the logs in Event Viewer. Following the path Applications and Services-Microsoft-AzureADPasswordProtection-DCAgent/Admin should provide a log like the one in Figure 4.16

¹<https://www.microsoft.com/en-us/download/details.aspx?id=57071>

²<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

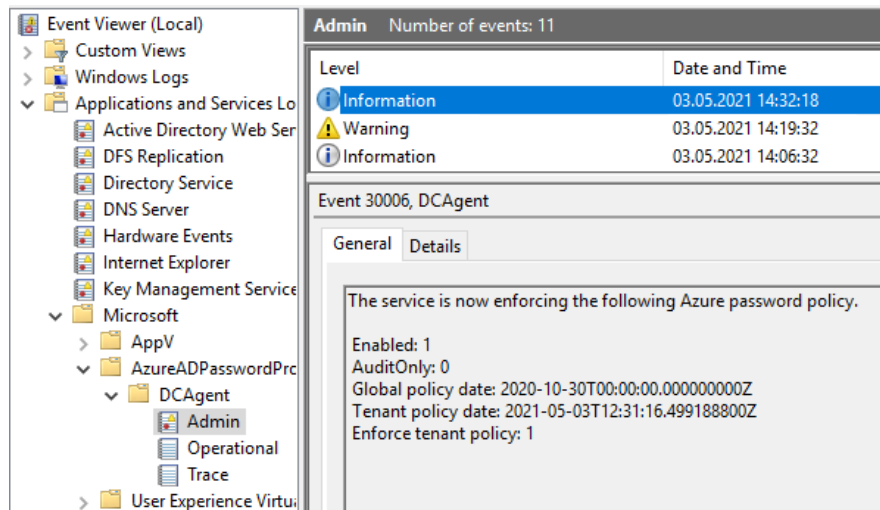


Figure 4.16: Successful enforcement of Azure password policy

A similar verification can be found on a proxy server at Applications and Services-Microsoft-AzureADPasswordProtection-ProxyService/Operational, verifying that everything is communicating correctly.

Chapter 5

Monitoring

The objective of the monitoring section is to explain how performance issues with the client machines is monitored in Configuration Manager. It also includes description of scripts used to monitor specific client machines for this project.

5.1 Client Health Status

The health status of each client machine is monitored through the built in client health dashboard.

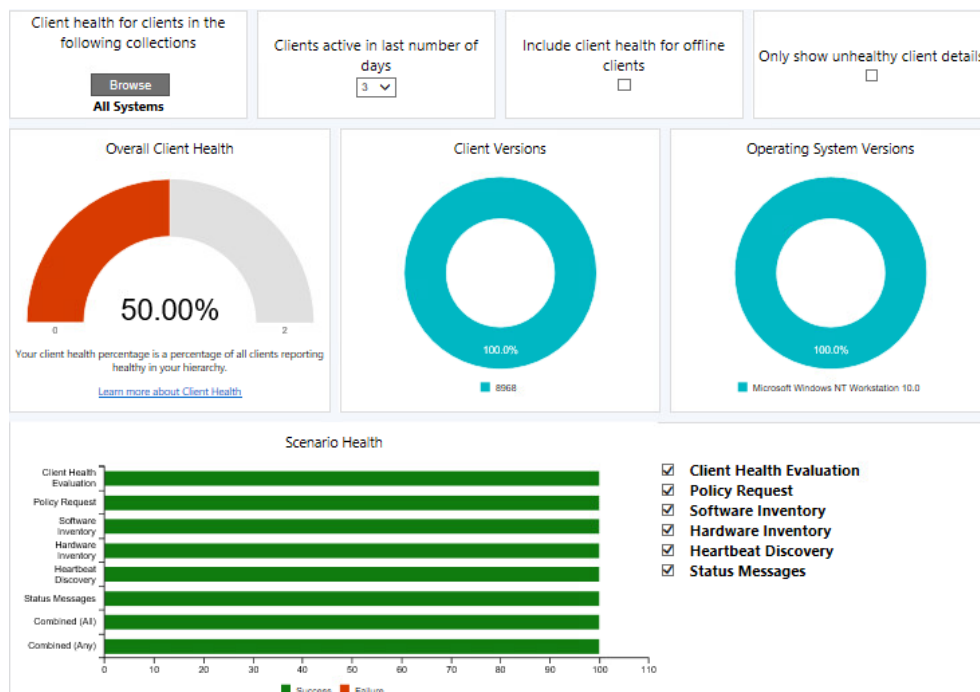


Figure 5.1: Client health dashboard

This dashboard monitors the devices managed Configuration Manager, and displays information regarding a clients health. The health of a client is displayed by the following values, currently online, client activity, client check and decommission. The online status of the clients is checked by sending a ping message to the Configuration Manager. If the client does not send a message within each 5 minutes, it is considered to be offline and it will be pictured on the dashboard.

The client activity tells if the machine has performed a policy update request, sent a list of its hardware inventory and a heartbeat message, which is a message updating the discovery record of the machine within the past seven days. When a policy update request is sent, the client check and decommission responds with a verification if all software or other required programs the client is dependent on are installed and running properly [83].

There were some issues with monitoring clients through the dashboard in Configuration Manager. As displayed in Figure 5.1, there were only two clients being monitored at the time of the screenshot, although 14 machines were currently running in the environment. Since the dashboard was unpredictable, three scripts were created to validate and check the health status of the different machines.

5.1.1 Ping client machines

```
1  #script for pinging all the client machines
2  #path for script
3  Set-Location -Path C:\Users\Administrator\Documents\Testing
4  #Return all the computernames from the domain, printing it to a text file
5  (Get-ADComputer -Filter * -Property *).Name |
6  Out-File -FilePath .\client-machines.txt
7  #Variables
8  $PingClient = Get-Content "client-machines.txt"
9  $date = Get-Content "client-machines.txt"
10 $replies = C:\Users\Administrator\Documents\Testing\replies.log
11 $noreplies = C:\Users\Administrator\Documents\Testing\noreplies.log
12
13 Write-Output "Start log" `r | Out-File -FilePath $replies
14 Write-Output "Start log" `r | Out-File -FilePath $noreplies
```

Listing 5.1: Part one: Ping Client machine

```

1  Foreach($SystemName in $PingClient){
2      $PingStatus = Get-Ciminstance Win32_pingstatus -filter "Address = '$SystemName'"
3      | -erroraction SilentlyContinue | Select-Object address, StatusCode
4
5      If($Pingstatus.StatusCode -eq 0) {
6          Write-output "$SystemName is alive"
7          Write-Output "$SystemName is alive" `r | Out-File -FilePath $replies
8      }
9      else
10     {
11         Write-output "$SystemName is dead"
12         Write-Output "$SystemName is dead" `r | Out-File -FilePath $noreplies
13     }
14 }
15 Write-Output `r "Run on $date" "by env:username at env:ComputerName" `r
16 "End log" `r `r | Out-File -FilePath $replies
17
18 Write-Output `r "Run on $date" "by env:username at env:ComputerName" `r
19 "End log" `r `r | Out-File -FilePath $noreplies
20
21 Foreach($Systemname in $PingClient) {
22     systeminfo.exe /s $Systemname | findstr /i "OS version"
23 }

```

Listing 5.2: Part two: Ping Client machine

The first script is pretty simple, it sends a ping message to all of the clients in the domain, checking whether or not each client machines are alive or dead. It also returns the operating system installed. This was implemented as a client status. Each machine in a working domain is predefined in the client-machine.txt in the beginning of the script. This was done by retrieving each machine in a domain, adding it to the client-machine.txt file.

5.1.2 CCMeval checking client health

The Configuration Manager dashboard displays the current health of any client machine, and it is supposed to get its data from the "CCMeval.exe" which periodically runs checking if all dependencies and functions are running as expected. Given that the dashboard is reporting less data than what was intended, two scripts has taken its place. One is starting the Ccmeval.exe process, and the second one is reading the result from the log file CcmEval.exe creates.

```

1  # Checks if the computer is running on the correct
2  [CmdletBinding()]
3      param(
4          [Parameter(Mandatory=$False)]
5              [String]$ComputerName = $env:COMPUTERNAME)
6  If ($ComputerName -eq $env:COMPUTERNAME)
7  {
8      If (!(([Security.Principal.WindowsPrincipal]
9          [Security.Principal.WindowsIdentity]::GetCurrent()).
10         IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator"))
11      {
12          Write-Warning "Run cmdlet as Admin!"
13          Return
14      }
15      #Starting the process that checks the current health check for the computer
16      WriteOutput "Starting ccm health check for $ComputerName"
17      Start-Process -Filepath "C:\Windows\CCM\CcmEval.exe"
18      do{
19
20      }while (Get-Process -ComputerName $ComputerName
21              -Name CcmEval.exe -ErrorAction SilentlyContinue)
22      #Sending the report to Config Manager
23  }$

```

Listing 5.3: Send ccm report

The first script is starting the CcmEval.exe. This is the program that creates the report that will later be read using a script by Trevor Jonsen, a Microsoft Endpoint Manager and Azure architect [84].

What this script does is starting the CCMEval.exe process. The CCMEval checks with the client agent and sees if all the functions provided are working properly.

CCMEvalreport

When the CCMEval is done running, the read-ccm displays the results from the CCMEvalreport.xml. Xml files tend to be difficult to read, therefore a Powershell script was used. This script can be located in in Appendix G. The script is displaying if the client has received all the latest policies, updates and other information that has been configured by the Configuration Manager. If any of the configuration should fail, this report will display what failed making troubleshooting a bit easier.


```

Microsoft Policy Platform WMI Integrity Test. Passed
Verify BITS exists. Passed
Verify SMS Agent Host service exists. Passed
Verify WMI service exists. Passed
Verify/Remediate Antimalware service startup type for Windows 10 or up. Passed
Verify/Remediate Antimalware service startup type. Not Applicable
Verify/Remediate Antimalware service status for Windows 10 or up. Passed
Verify/Remediate Antimalware service status. Not Applicable
Verify/Remediate BITS startup type. Passed
Verify/Remediate client installation. Passed
Verify/Remediate client prerequisites. Passed
Verify/Remediate client WMI provider. Passed
Verify/Remediate Configuration Manager Proxy service startup type. Not Applicable
Verify/Remediate Configuration Manager Proxy service status. Not Applicable
Verify/Remediate Configuration Manager Remote Control service startup type. Passed
Verify/Remediate Configuration Manager Remote Control service status. Passed
Verify/Remediate Microsoft Policy Platform Service Existence. Passed
Verify/Remediate Microsoft Policy Platform service startup type. Passed
Verify/Remediate Network Inspection service startup type for Windows 10 or up. Passed
Verify/Remediate Network Inspection service startup type. Not Applicable
Verify/Remediate SMS Agent Host service startup type. Passed
Verify/Remediate SMS Agent Host service status. Passed
Verify/Remediate SQL CE database is healthy. Passed
Verify/Remediate Windows Update service startup type on Windows 8. Passed
Verify/Remediate Windows Update service startup type. Not Applicable
Verify/Remediate WMI service startup type. Passed
Verify/Remediate WMI service status. Passed
WMI Event Sink Test. Passed
WMI Repository Integrity Test. Passed

```

Figure 5.2: Output from Read-ccm.ps1

Chapter 6

Risk analysis

As requested a short risk analysis was conducted on the client machines in the domain. This chapter will include threats, vulnerabilities and security controls added in the domain environment. It will only contain the most important parts of a risk analysis as it was not viable to conduct a thorough, by the book analysis within the time frame of this thesis. It is recommended to continue this process later.

6.1 Executive summary

After creating the domain, configuring Configuration Manager to deploy new client machines, and implementing endpoint security, a short risk analysis of the client machines was conducted. In this risk analysis, current threats, existing controls and vulnerabilities that may affect the endpoint nodes of HDO were identified. To uncover these values, as well as finding mitigations, ISO:27002 [4] and NSM's basic principles for ICT 2.0 [5] was used.

The risk scenarios are based on the fact that there where no security implementations in the domain, before they were implemented in this project. The risks before mitigation are therefore affected by this, and are higher than if it had been analyzed after being created in the domain of HDO.

Following the completion of the implementation of basic safety mechanisms, an acceptable risk for HDO has been identified.

6.2 Scope

The security section of this thesis has mainly focused on how to protect the client machines. Given that the task from HDO was securing and operating client machines. This risk assessment will therefore mainly focus on mitigating and defining an acceptable risk for the client machines in HDO's domain.

The scope of the risk assessment follows the same scope as the thesis. The thesis focuses on managing the life cycle of Windows 10 clients in a decentralized AD domain with centralized IT management, and security of these clients. The risk assessment is consequently limited to endpoint security on the clients, and operational availability. This means that AD DS security, network security and monitoring is not a part of the assessment, as this would require a substantial amount of time to complete.

6.3 Methodology

This risk assessment was conducted according to appropriate chapters from "NSM's Grunnprinsipper for IKT-Sikkerhet 2.0" [5] and ISO 27002 [4]. The "NSM's Grunnprinsipper for IKT-sikkerhet 2.0" from NSM is a defined set with principals and measures to secure information systems, and was the main tool used for this risk assessment as it is more clear and concise.

The consequence and probability matrices used to categorize and rank the different risks, are created by HDO and are therefore in Norwegian. These could be found in Appendix H. It was determined that they were not going to be translated to English, after a dialog with Erik Hjelmås found in Appendix I.

The vulnerability assessment were conducted in a "out of the box" domain environment with a DC, Configuration Manager server and Windows 10 clients with no configurations. The domain had the default domain policy linked. No devices had access to the internet to simulate the real environment.

6.3.1 Probability and consequence matrices

The probability and consequence matrices were too big to fit in the report and can be found in Appendix H. These two matrices represent the evaluation of probability and consequence for HDO. Probability is evaluated by the possibility of a risk taking place, with the belonging consequence, as stated in HDO's matrix for Probability found in Appendix H. Consequence is calculated from the different sections in HDO's matrix.

6.3.2 Criticality matrix

The criticality of an event is a result of *probability * consequence*.

Lav	1 til 2
Moderat	3 til 6
Alvorlig	8 til 9
Svært alvorlig	12 til 16

Figure 6.1: Criticality matrix from HDO.

6.4 Assessments

6.4.1 Assets

HDO has not done an asset assessment before and does not plan on doing it, but has said that audio logs are their most valuable asset, meaning any risks involving losing access to audio logs should be prioritized.

6.4.2 Existing controls

The existing controls are restricted to software that is pre-installed on a windows machine, and the default settings in AD and Configuration Manager. These measures are not the most secure, but will defend against some of the more common threats.

Table 6.1: Existing controls in domain environment.

Existing controls	Description	Control-domain	Efficiency
Microsoft defender antivirus.	Microsoft defender antivirus is a software installed on all Windows 10 machines. This software comes with virus and threat protection and automatic backup to cloud.	Technical	Medium
Monitoring through Configuration Manager	Configuration Manager has a built in client health dashboard written about in section 5.1 This does not include any security monitoring, but could give an indication if something is down or not working as expected.	Technical	Low
Default GPO's.	A default GPO is created when a new AD is created. This policy contains some default settings, like a password policy, network access, and accounts like guest and admin.	Technical	Low

Table 6.1 – continued from previous page

Existing controls	Description	Control-domain	Efficiency
Windows Defender Firewall.	Windows Defender firewall is the inbuilt firewall from Microsoft. By default this does not provide the most advanced protection, but blocks every inbound connection.	Technical	Medium

6.4.3 Vulnerability Assessment

The vulnerabilities listed in the vulnerabilities table are the relevant vulnerabilities found

Table 6.2: Vulnerability

Vulnerability	Description
Inadequate encryption in communication	Network traffic does not utilize the highest encryption available by default
Lack of storage media encryption	There are no form of storage media encryption implemented on devices that are left unattended.
Inadequate authentication	Multifactor authentication is not enabled, and passwords requirements are weak, allowing users to set weak and/or breached passwords which may lead to compromised hosts if unauthorized people gains access to the computer.
No centralized anti malware software	The clients have Microsoft Defender enabled, but does not have a centralized management system for detection and prevention of malware.
Inadequate audit logs	Default GPO settings does not provide comprehensive audit logging capabilities, making it hard to track security events.
Unused media ports are not blocked	Media ports such as USB ports are not disabled, leaving it exposed to infect the client through malware on removable media
"Principle of least privilege" not enforced	There are no controls limiting the access for users, applications and processes beyond default settings.
Inadequate limitation of software	There are no controls for downloading of both third and first party software.

Table 6.2 – continued from previous page

Vulnerability	Description
Single point of failure on Configuration Manager	There are no backup server running Configuration Manager, if this machine goes down, there is nothing to fall back to.
No application whitelisting implemented	Clients not configured to only allow whitelisted applications. This might allow end users to run applications or tools only meant for administrators, or run unapproved applications from e.g. removable media, which might compromise the system.
Unnecessary built in features are not deactivated	Several old and unnecessary features are not disabled on the clients, like unused protocols and OneDrive or the application store. This might not be a risk in a closed network, but it is recommended to be disabled nonetheless.

6.5 Risk analysis

6.5.1 Risk scenarios

To further analyze the specific risks facing HDO, the vulnerabilities are presented in scenarios. These scenarios are based on HDO's own matrices and calculates their risks before and after mitigation.

Risk 1

ID: R1

Subject area: Security

Risk description: A Malicious Actor gains access to a workstation, and manages to dump the local password hashes. The Actor uses the hash of local administrator to attempt pass-the-hash attack, thereby gaining horizontal movement within the domain.

Consequence justification: With local admin-privileges an attacker could potentially plant malicious software throughout the environment, and further escalate privileges until the entire system is owned. Stealing sensitive information or making crucial services unavailable for large amounts of time will be achievable.

Consequence: 4

Probability: 1

Probability justification: A planned and targeted attack must underlay such a scenario, with the attacker having already gained access to a workstation.

Risk: 4

Mitigation: Local Administrator Password Protection

Consequence after mitigation: 1

Probability after mitigation: 0

Remaining risk: 0

Risk 2**ID: R2**

Subject area: Security

Risk description: Thief breaks in and steals a client machine. The thief retrieves the storage media, and extracts the data stored on it. The Actor is able to retrieve password or other sensitive information locally stored on the client.

Consequence justification: This might have less serious consequences, depending on what has been written down. Most likely a users own credentials or other info about that user.

Consequence: 2

Probability: 2

Probability justification: Thievery happens from time to time, especially at locations that are closed.

Risk: 4

Mitigation: Encrypt all disks with Bitlocker.

Consequence after mitigation: 1

Probability after mitigation: 2

Remaining risk: 2

Risk 3**ID: R3**

Subject area: Operational

Risk description: Remote office with low available bandwidth receives large quantities of traffic due to updates.

Consequence justification: Low bandwidth will potentially lead to some reduced deliverance of HDO's solution on branches with a lot of machines.

This will generate a lot of traffic to the location, causing Denial of Service (DOS).

Consequence: 2

Probability: 4

Probability justification: Given that Windows sends out updates each month, this will probably happen at least one time a month.

Risk: 8

Mitigation: Implement delivery Optimization.

Consequence after mitigation: 1

Probability after mitigation: 1

Remaining risk: 1

Risk 4

ID: R4

Subject area: Security

Risk description: A careless user places USB stick with unknown content in a client machine. The USB stick contains malware, infecting the computer and spreads to other hosts. **Consequence justification:** A USB stick could potentially lead to Ransomware attacks, or worms spreading through the network. This could potentially lead to loss of data or unavailable services, preventing HDO to deliver their services.

Consequence: 4

Probability: 3

Probability justification: A user with lack of knowledge or competence could plug a USB stick in a computer, unaware of the effects.

Risk: 12

Mitigation: Antimalware policy, scanning all disks, both internal external, quarantining malicious files. Information security awareness training, block removable storage devices in group policy and a warning sticker.

Consequence after mitigation: 1

Probability after mitigation: 1

Remaining risk: 1

Risk 5

ID: R5

Subject area: Operational

Risk description: OS drive on a client gets corrupted after a long operational life. It is the only operational client on that specific location. The location is far from HDO and IT personnel will have to travel to the location to reinstall the client.

Consequence justification: HDO services are down for a longer period of time. Users get annoyed as they cannot do their job properly.

Consequence: 2

Probability: 2

Probability justification: In an environment with a larger number of clients file system corruption and other problems will eventually happen. It is likely that it will happen more than once every five years.

Risk: 4

Mitigation: Implement remote reimaging of clients. Preferably without any required interaction from the user as this can introduce configuration errors.

Consequence after mitigation: 1

Probability after mitigation: 2

Remaining risk: 2

Risk 6

ID: R6

Subject area: Security

Risk description: A domain admin creates a Remote Desktop Protocol (RDP) session to a client machine, accidentally logging in with domain admin credentials. Later, a threat actor launches an attack against the client machine, retrieving the hash of the admin credentials.

Consequence justification: The threat actor now has the password hash of a domain admin, and might gain full access to the entire domain of HDO. This could lead to unavailable services or loss of confidential data.

Consequence: 4

Probability: 1

Probability justification: Given that the domain admin has knowledge and competence to know that this should be avoided, this risk has been given low probability.

Risk: 4

Mitigation: GPO, blocking domain admins from logging into client machines.

Consequence after mitigation: 4

Probability after mitigation: 0

Remaining risk: 0

Risk 7

ID: R7

Subject area: Operation

Risk description: Server admin misconfigures a TS, downloading the wrong application or causes an error when booting a new machine.

Consequence justification: This could cause download of unwanted software or potential downtime at a customer site.

Consequence: 2

Probability: 2

Probability justification: Given that the domain admin has knowledge and competence to now that this should be avoided, this risk has been given low probability.

Risk: 2

Mitigation: Good routines and testing environments. Always testing something before deploying it to production.

Consequence after mitigation: 2

Probability after mitigation: 1

Remaining risk: 2

Consequence → Probability ↓	1	2	3	4
4		3		
3		7		4
2		2,5		
1				1, 6

Table 6.3: Risk matrix before mitigation's.

Consequence → Probability ↓	1	2	3	4
4				
3				
2	2, 5			
1	1, 3, 4, 6	7		

Table 6.4: Risk matrix after mitigation's.

6.6 Accepted risk

After mitigating the risks by creating preventive and reactive controls for HDO, an accepted risk was accomplished. After discussing with HDO and in the group, the residual risk which is on green is considered as acceptable risk. This means that the risk exposure is by HDO deemed as acceptable.

Chapter 7

Conclusion

7.1 Results

The goal of this project was to recommend a ConOps for HDO, illustrating how to manage and secure Windows client machines throughout their lifecycle for HDO's new emergency communication solution. This was delivered in the form of a functioning Windows domain environment, and a ConOps. The report functions as the ConOps, by describing how to implement and use the solution to operate and secure Windows clients in a centralized IT environment.

The solution automates the deployment of new images, updates and applications, provides a centralized console for security management, as well as monitoring and support for the clients in the domain. The solution provides all tools necessary for HDO to manage the Windows clients they provide to their customers, directly from their operation center in Gjøvik.

The Windows clients are secured through the use of GPOs, Endpoint Security and some Microsoft developed security technologies. The GPOs have been put together by combining STIG and Windows security baselines and applied to the domain. Endpoint Security is managed through Configuration Manager and encompasses antimalware policies, Windows Defender Firewall and security monitoring and compliance.

This domain is made specifically for HDO after continuous meetings with the company, discussing the functionality of the solution. The solution delivers on all the goals specified in the Project Description Section 1.2.

7.1.1 Reflection and evaluation

This bachelor's thesis has taken a few turns to get to where it is today, both big and small. The final product is the result of a string of choices made between vastly different approaches to system management (e.g. a desired state manage-

ment solution like Puppet, versus the heavy-duty Windows-centric management of Configuration Manager), and what to include of less significant features, based of both time and scope restrictions.

In the end, the final product evolved to be a comprehensive system tailored to meet the demands of a critical societal function like the emergency services. However, a case can be made on whether or not the ends justify the means. Before starting the work of implementing the various components that would comprise the system, quite some of arguments were made in favor of choosing Configuration Manager as the system management tool, and in general keeping the system as Windows native as possible. As stated, the resulting system is functional and covers all requirements that HDO has specified, but the process of installation, configuration and planning the operation was not as straightforward as one would ideally like it to be.

The sheer size of Configuration Manager with its massive selection of features and corresponding documentation, options in configuration and overabundance of choice in general, pose a major challenge to whomever is tasked with setting it up. It is the experience of this group at the end of this project, that such an endeavor requires a larger team of dedicated professionals to fully grasp all aspects and possibilities of the system, and to keep it operational and effective over time. On the other hand, one could argue that one dedicated person being responsible for implementation, might lead to a "cleaner" result, as being aware of every step of every action taken in the creation of the system, would help in grasping the full picture, and ultimately create a more cohesive system. Finding a balance between these two approaches, where communication and clear division of responsibilities exists as prominent attributes, is likely to give the best result.

There are several ways this assignment could have been accomplished, which became evident after talking to several technical professionals with experience in managing Windows environments. Notably, not one of them had worked with the same exact approach to the issue. This shows that most use cases, even within Windows management, can require very different solutions based on just a few variations in requirements. For this system, the most central requirements were: A closed network without Cloud-connection, stationary workstations and a need of bare-metal deployment. Working out of these restrictions, we feel confident that our system would be a good fit for the real-world environment HDO is planning to deploy, and thus recommend our solution for this use.

7.2 Further Work

This subchapter gives an overview of further actions HDO can take to secure or implement more functionality within Configuration Manager, and the system as a whole.

7.2.1 MDE

As explained in chapter 4.1, MDE is supported through endpoint protection in Configuration Manager with an additional cost. This software adds an extra layer of security to Windows Defender, and the GPO's. We recommend reading about MDE as it will give an extra insight of the application and devices in HDO. It also has automatic remediation, and in the MDE center, all alerts will be displayed with immediate remediation an organization should take if a breach has taken place.

7.2.2 Intune with Configuration Manager

HDO has mentioned that mobile devices might be implemented in the future. This is not deployed in this project, but can be implemented with Intune. Intune is also supported in Configuration Manager by configuring a cloud management Gateway on the "Manager" node. As HDO stated in the latter half of this project that Cloud-connection could be enabled, this would be something to look into.

7.2.3 Enable PKI for configuration manager

Currently, the system uses HTTP when communicating between the Configuration Manager site server and CMC on the workstations. Due to time constraints, the system has not been prepped to use HTTPS (encrypting the communication). The process of enabling this involves installing Microsoft Certificate Authority using Active Directory Certificate Services on the domain controller, and enabling HTTPS on both the site system and WSUS. Enabling TLS (HTTPS) will lead to more data being transferred within the network, so consideration into whether or not it is needed should be taken, especially since the intended network is closed off.

7.2.4 Windows Defender Credential Guard

To further protect against the threat of pass-the-hash attacks, Windows Defender Credential Guard should be enabled in the system. In essence, this will protect the location where credentials are stored, so as to limit attackers from being able to extract password-hashes in the first place.

7.2.5 Fix Reporting services

Reporting Services has been installed and configured in the system, however, testing and verification was skipped due to time constraints. At last inspection, relevant information seems to be reported by the clients, but the viewing of the generated reports is hindered presumably by a misconfiguration of access rights in the responsible service-account.

7.2.6 Continue Risk Analysis

The Risk Analysis in this thesis only covers a small part of the overall system and should be expanded on. We recommend starting with a high level risk assessment at an organizational level, before starting on the technical parts. By starting at the organizational level you discover what administrative documents that needs to be made or improved on, clearing the way for low level, technical risk assessments later on.

Bibliography

- [1] HDO, 'Om oss,' [Online; accessed 11-February-2021]. [Online]. Available: <https://www.hdo.no/om-oss>.
- [2] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar and R. Ahmad Khan, 'Healthcare data breaches: Insights and implications,' *Healthcare*, vol. 8, no. 2, 2020, ISSN: 2227-9032. DOI: 10.3390/healthcare8020133. [Online]. Available: <https://www.mdpi.com/2227-9032/8/2/133>.
- [3] 'Iso/iec/ieee international standard - systems and software engineering – life cycle processes – requirements engineering,' *ISO/IEC/IEEE 29148:2018(E)*, vol. Annex B, pp. 87–88, 2018. DOI: 10.1109/IEEESTD.2018.8559686.
- [4] I. O. for Standardization, *Information technology — security techniques — code of practice for information security controls*, [Online; accessed 1-May-2021], 2013. [Online]. Available: <https://www.iso.org/standard/54533.html>.
- [5] N. sikkerhetsmyndighet, *Grunnprinsipper for ikt-sikkerhet 2.0*, [Online; accessed 1-May-2021], 2020. [Online]. Available: <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/>.
- [6] *Kanban wip limits*, [Online; accessed 26-Januar-2021]. [Online]. Available: <https://kanbanzone.com/resources/kanban/wip-limits/#:~:text=WIP%5C%20stands%5C%20for%5C%20Work%5C%20In,Kanban%5C%20process%5C%20or%5C%20per%5C%20step.&text=The%5C%20WIP%5C%20limits%5C%20are%5C%20identified%5C%20by%5C%20the%5C%20team%5C%20who%5C%20owns%5C%20the%5C%20workflow..>
- [7] C. Cadman, *Puppet on windows: Top questions (and answers!)* [Online; accessed 9-May-2021]. [Online]. Available: <https://puppet.com/blog/puppet-on-windows-top-questions-and-answers/>.
- [8] Saurabh, *What is puppet ? – configuration management using puppet*, [Online; accessed 5-February-2021]. [Online]. Available: <https://www.edureka.co/blog/what-is-puppet/>.
- [9] Puppet, *Welcome to puppet forge*, [Online; accessed 5-February-2021]. [Online]. Available: <https://forge.puppet.com>.

- [10] U. Team, *Puppet enterprise vs free open source puppet: Which is right for you?* [Online; accessed 7-February-2021]. [Online]. Available: <https://www.upguard.com/blog/open-source-puppet-vs-puppet-enterprise-which-is-right-for-you>.
- [11] U. Team, *Welcome to puppet forge*, [Online; accessed 7-February-2021]. [Online]. Available: <https://www.upguard.com/blog/foreman-vs-puppet>.
- [12] W. Contributors, *Microsoft system center configuration manager*, [Online; accessed 12-March-2021]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Microsoft_System_Center_Configuration_Manager&oldid=1022594121.
- [13] *Features and capabilities of configuration manager*, [Online; accessed 12-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/changes/features-and-capabilities>.
- [14] *Microsoft windows intune vs sccm*, [Online; accessed 14-March-2021]. [Online]. Available: <https://www.communicationsquare.com/news/intune-vs-system-center-configuration-manager/>.
- [15] *Microsoft intune is an mdm and mam provider for your devices*, [Online; accessed 14-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>.
- [16] *Overview of windows autopilot*, [Online; accessed 14-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot>.
- [17] J. B. Roy, *Windows autopilot faq clarifying the general misconceptions part 1*, [Online; accessed 15-March-2021]. [Online]. Available: <https://www.anoopcnaair.com/windows-autopilot-faq-general-misconceptions/>.
- [18] J. B. Roy, *Windows autopilot deployment for existing devices*, [Online; accessed 15-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/autopilot/existing-devices>.
- [19] *Microsoft endpoint configuration manager faq*, [Online; accessed 20-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/understand/microsoft-endpoint-manager-faq>.
- [20] A. Pantos, *Sccm client agents demystified | managing mac with sccm*, [Online; accessed 13-May-2021]. [Online]. Available: <https://www.parallels.com/blogs/sccm-client-agents-demystified-managing-mac-with-sccm/>.
- [21] A. C. Nair, *Sccm software center vs configmgr client applet | differences*, [Online; accessed 13-May-2021]. [Online]. Available: <https://www.anoopcnaair.com/sccm-software-center-vs-configmgr-client-applet/>.

- [22] *Software center user guide*, [Online; accessed 13-May-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/understand/software-center>.
- [23] Microsoft, *How to create collections in configuration manager*, [Online; accessed 9-May-2021], 2021. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/collections/create-collections>.
- [24] Microsoft, *Define network locations as boundaries for configuration manager*, [Online; accessed 10-May-2021], 2020. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/configure/boundaries>.
- [25] *Install and configure distribution points in configuration manager*, [Online; accessed 10-May-2021], 2021. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/configure/install-and-configure-distribution-points>.
- [26] S. Heiney, *Remote assistance vs. remote desktop: Understanding the difference*, [Online; accessed 16-February-2021]. [Online]. Available: <https://blog.netop.com/remote-assistance-vs-remote-desktop>.
- [27] *A brief history of teamviewer*, [Online; accessed 08-April-2021]. [Online]. Available: <https://www.teamviewer.com/en/company/>.
- [28] *Teamviewer quicksupport*, [Online; accessed 08-April-2021]. [Online]. Available: <https://www.teamviewer.com/en/info/quicksupport/>.
- [29] *Teamviewer quicksupport*, [Online; accessed 08-April-2021]. [Online]. Available: <https://dl.teamviewer.com/docs/en/v15/TeamViewer-Manual-Remote-Control-en.pdf>.
- [30] *What is powershell?* [Online; accessed 10-May-2021], 2021. [Online]. Available: <https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.1>.
- [31] Microsoft, *Bitlocker and windows 10 pro protect your data*, [Online; accessed 9-May-2021], 2019. [Online]. Available: <https://community.windows.com/en-us/stories/what-is-bitlocker-windows-10>.
- [32] Lithmee, *What is the difference between lite-touch and zero-touch deployment*, [Online; accessed 8-May-2021], 2019. [Online]. Available: <https://pediaa.com/what-is-the-difference-between-lite-touch-and-zero-touch-deployment/#Lite-Touch%20Deployment>.
- [33] S. Lean, *How does the pxe boot process work?* [Online; accessed 10-May-2021], 2019. [Online]. Available: <https://techcommunity.microsoft.com/t5/itops-talk-blog/how-does-the-pxe-boot-process-work/bap/888557>.

- [34] Microsoft, *Windows deployment services*, [Online; accessed 08-MAY-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/windows/win32/wds/windows-deployment-services-portal>.
- [35] Microsoft, *Branch cache*, [Online; accessed 8-May-2021], 2020. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/networking/branchcache/branchcache>.
- [36] Microsoft, *Peer cache for configuration manager clients*, [Online; accessed 8-May-2021], 2018. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/client-peer-cache>.
- [37] Microsoft, *Optimize windows 10 update delivery with configuration manager*, [Online; accessed 8-May-2021], 2020. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/sum/deploy-use/optimize-windows-10-update-delivery>.
- [38] P Wilcock, *Configmgr peer cache and branchcache – better together!* [Online; accessed 10-May-2021], 2017. [Online]. Available: <https://2pintsoftware.com/configmgr-peer-cache-branchcache/>.
- [39] *Recommended hardware for configuration manager*, [Online; accessed 15-March-2021], Apr. 2021. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/recommended-hardware>.
- [40] *Recommended hardware for configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/recommended-hardware>.
- [41] *Supported sql server versions for configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/support-for-sql-server-versions>.
- [42] R. Gupta, *Installing sql server reporting services 2017*, [Online; accessed 17-March-2021]. [Online]. Available: <https://www.mssqltips.com/sqlservertip/5237/installing-sql-server-reporting-services-2017/>.
- [43] *Windows pe (winpe)*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-intro>.
- [44] *Plan for site system servers and site system roles in configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/plan-for-site-system-servers-and-site-system-roles>.
- [45] *Manage express installation files for windows 10 updates*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/sum/deploy-use/manage-express-installation-files-for-windows-10-updates>.

- [46] *How to deploy clients to windows computers in configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/clients/deploy/deploy-clients-to-windows-computers>.
- [47] *Define site boundaries and boundary groups*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/configure/define-site-boundaries-and-boundary-groups>.
- [48] *About discovery methods for configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/configure/about-discovery-methods>.
- [49] *Onevinn applications*, [Online; accessed 28-April-2021]. [Online]. Available: <https://onevinn.schrewelius.it/Apps01.html>.
- [50] *Debug a task sequence*, [Online; accessed 30-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/osd/deploy-use/debug-task-sequence>.
- [51] *05 – maintaining the wsus catalog by declining updates for better update scanning*, [Online; accessed 13-March-2021]. [Online]. Available: setupconfigmgr.com/maintaining-the-wsus-catalog-by-declining-updates-for-better-sccm-scanning.
- [52] *Re-index the wsus database*, [Online; accessed 13-March-2021]. [Online]. Available: <https://gist.github.com/emnavarro02/0ff6481ce7c9b207f7762732fd73aa8>.
- [53] *Enhancing wsus database cleanup performance sql script*, [Online; accessed 13-March-2021]. [Online]. Available: <https://stevethompsonmvp.wordpress.com/2018/05/01/enhancing-wsus-database-cleanup-performance-sql-script/>.
- [54] *Software update maintenance script updated: All the wsusness*, [Online; accessed 13-March-2021]. [Online]. Available: <https://damgoodadmin.com/2018/04/17/software-update-maintenance-script-updated-all-the-wsusness/>.
- [55] *08 – how to deploy software updates using microsoft sccm*, [Online; accessed 13-March-2021]. [Online]. Available: <https://setupconfigmgr.com/how-to-deploy-software-updates-using-microsoft-sccm>.
- [56] E. Bott, *Insider's guide to managing microsoft patch tuesday*, [Online; accessed 12-May-2021]. [Online]. Available: <https://www.techrepublic.com/article/insiders-guide-to-managing-microsoft-patch-tuesday/>.
- [57] E. Koneti, *Managing windows updates using configuration manager and group policy*, [Online; accessed 15-April-2021]. [Online]. Available: <http://eskonr.com/2020/12/managing-windows-updates-using-configuration-manager-and-group-policy/>.

- [58] *Endpoint protection*, [Online; accessed 10-May-2021], 2020. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/endpoint-protection>.
- [59] *Plan for bitlocker management*, [Online; accessed 16-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/protect/plan-design/bitlocker-management#prerequisites>.
- [60] *Anti malware testfile*, [Online; accessed 25-April-2021]. [Online]. Available: https://www.eicar.org/?page_id=3950.
- [61] *Use security baselines to configure windows 10 devices in intune*, [Online; accessed 10-May-2021], 2021. [Online]. Available: <https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines#:~:text=Security%20baselines%20are%20pre%2Dconfigured,settings%20and%20values%20you%20require..>
- [62] *Security technical implementation guides*, [Online; accessed 10-May-2021], 2020. [Online]. Available: <https://public.cyber.mil/stigs>.
- [63] *Group policy objects*, [Online; accessed 11-May-2021], 2020. [Online]. Available: <https://public.cyber.mil/stigs/gpo/>.
- [64] *Microsoft security compliance toolkit 1.0*, [Online; accessed 25-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10>.
- [65] *Security baseline (final) for windows 10 and windows server, version 20h2*, [Online; accessed 25-April-2021]. [Online]. Available: <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-final-for-windows-10-and-windows-server/ba-p/1999393>.
- [66] *Create configuration baselines in configuration manager*, [Online; accessed 25-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/compliance/deploy-use/create-configuration-baselines>.
- [67] *Security compliance manager now available for download!* [Online; accessed 25-April-2021]. [Online]. Available: <https://techcommunity.microsoft.com/t5/ask-the-performance-team/security-compliance-manager-now-available-for-download/ba-p/374577>.
- [68] *Local administrator password solution (laps)*, [Online; accessed 25-April-2021]. [Online]. Available: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>.
- [69] *Local accounts*, [Online; accessed 25-April-2021]. [Online]. Available: <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>.
- [70] *What is a pass the hash attack?* [Online; accessed 25-April-2021]. [Online]. Available: <https://secureteam.co.uk/articles/information-assurance/what-is-a-pass-the-hash-attack/>.

- [71] *Microsoft local admin password solution (laps) – deployment steps*, [Online; accessed 25-April-2021]. [Online]. Available: <https://cqureacademy.com/blog/hacks/laps-deployment-steps>.
- [72] L. Seltzer, *Password policy recommendations: Here's what you need to know*. [Online; accessed 24-February-2021], Aug. 2019. [Online]. Available: [https://www.hpe.com/us/en/insights/articles/password-policy-recommendations-heres-what-you-need-to-know-1908.html#:~:text=The%20default%20password%20length%20requirement,do%20not%20ban\)%20complexity%20requirements..](https://www.hpe.com/us/en/insights/articles/password-policy-recommendations-heres-what-you-need-to-know-1908.html#:~:text=The%20default%20password%20length%20requirement,do%20not%20ban)%20complexity%20requirements..)
- [73] D. Florencio, C. Herley and B. Coskun, 'Do strong web passwords accomplish anything?' Tech. Rep. MSR-TR-2007-64, Jun. 2007, [Online; accessed 24-February-2021], p. 6. [Online]. Available: <https://www.microsoft.com/en-us/research/publication/do-strong-web-passwords-accomplish-anything/>.
- [74] S. Komanduri, R. Shay, L. Cranor, C. Herley and S. Schechter, 'Telepathwords: Preventing weak passwords by reading users' minds,' in *Proceedings of the 23rd USENIX Security Symposium*, USENIX, Aug. 2014. [Online]. Available: <https://www.microsoft.com/en-us/research/publication/telepathwords-preventing-weak-passwords-by-reading-users-minds/>.
- [75] R. Hicock, 'Password guidance,' [Online; accessed 24-February-2021], May 2016. [Online]. Available: <https://www.microsoft.com/en-us/research/publication/password-guidance/>.
- [76] P. Grassi, E. Newton, J. Fenton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, N. Lefkowitz, J. Danker, Y. Choong, K. Greene and M. Theofanos, 'Digital identity guidelines: Authentication and lifecycle management,' Jun. 2017, [Online; accessed 24-February-2021]. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>.
- [77] *Eliminate bad passwords using azure active directory password protection*. [Online; accessed 11-March-2021], Jul. 2020. [Online]. Available: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>.
- [78] *Enforce on-premises azure ad password protection for active directory domain services*. [Online; accessed 08-March-2021], Jul. 2020. [Online]. Available: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>.
- [79] *Recommended hardware for configuration manager*, [Online; accessed 17-March-2021]. [Online]. Available: <https://www.anixis.com/products/ppe/default.htm>.
- [80] *Specops password policy*, [Online; accessed 17-March-2021]. [Online]. Available: <https://specopssoft.com/product/specops-password-policy/>.

- [81] *Prisalternativer for enterprise mobility + security*, [Online; accessed 03-MAY-2021]. [Online]. Available: <https://www.microsoft.com/nb-no/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing?market=no>.
- [82] *Plan and deploy on-premises azure active directory password protection*, [Online; accessed 3-May-2021], Mar. 2020. [Online]. Available: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>.
- [83] Microsoft, *How to monitor clients in configuration manager*, [Online; accessed 12-May-2021], 2020. [Online]. Available: <https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/monitor-clients>.
- [84] *Reading ccmeval results directly from a configmgr client with powershell*, [Online; accessed 16-April-2021]. [Online]. Available: <https://smsagent.blog/2016/02/12/reading-ccmeval-results-directly-from-a-configmgr-client-with-powershell/>.

Appendix A

Prosjektplan

Appendix C

VB script

```
1 On Error Resume Next
2
3 '*** Define string variables for device, device Resource ID and user of interest
4
5 Class_Name = "SMS_SCI_Component"
6 Class_ItemName = "SMS_WSUS_SYNC_MANAGER|MANAGER.HDO.LOCAL"
7 Class_ItemType = "Component"
8 Property_Name = "Updates Cleanup Age"
9 Property_SiteCode = "PR1"
10 DesiredValue = 0
11
12 '*** Check parameters - we need the provider server name and the site code
13
14 set args=wscript.arguments
15
16 If args.Count = 2 then
17     SMSProviderServer = UCASE(Wscript.Arguments(0))
18     SiteCode = UCASE(Wscript.Arguments(1))
19 Else
20     wscript.Echo "Incorrect command line arguments." & vbCrLf &
21     "Usage: cscript /nologo ModifySCFProperty.vbs
22     <smsproviderserver> <sitecode>" & vbCrLf & "Example: cscript
23     /nologo ModifySCFProperty.vbs SERVER1 S01 >
24     schedules.txt" & vbCrLf
25     WScript.Quit(1)
26 End If
27
28
29 '*** Connect to the provider - report the error and terminate on failure
30
```

```

31 SMSProviderServer = "\\\" + SMSProviderServer + "\"
32 Set ObjSvc = GetObject("winmgmts:" &
33 "{impersonationLevel=Impersonate,authenticationLevel=Pkt}!"
34 & SMSProviderServer & "root\sms\site_" & SiteCode)
35
36 If Err.Number <> 0 Then
37     wscript.Echo "Failed to connect to provider server with code: " & Err.Number & ". Aborting!"
38     WScript.Quit(2)
39 End If
40
41 '*** Get the desired instance of the class
42
43 Set objInst = ObjSvc.Get(Class_Name & ".ItemName='"
44 & Class_ItemName & "',ItemType='" & Class_ItemType & "',SiteCode='" & Property_SiteCode & "'")
45
46 If Err.Number <> 0 Then
47     WScript.Echo "Failed to open desired object with error code "
48     & Err.Number & " (" & Err.Description & "). Aborting!"
49     WScript.Quit(3)
50 End If
51
52 '*** Loop through the Properties until we find a match or run out
53
54 bFoundProperty = False
55
56 For Each objProp in objInst.Props
57     If objProp.PropertyName = Property_Name Then
58         bFoundProperty = True
59         Exit For
60     End If
61 Next
62
63 If bFoundProperty = False Then
64     WScript.Echo "Desired object was found but property was not found.
65     Exiting without making any changes."
66     WScript.Quit(4)
67 End If
68
69 '*** Property found so check to see if existing value matches desired, changing it as appropriate
70
71 If objProp.Value = DesiredValue Then
72     WScript.Echo "Property '" & Property_Name &
73     "' found with desired value '" & DesiredValue & "'. Not making any changes."
74     WScript.Quit(0)
75 Else

```

```
76     OriginalValue = objProp.Value
77     objProp.Value = DesiredValue
78     objProp.Put_
79     objInst.Put_
80
81     If Err.Number <> 0 Then
82         wscript.Echo "Failed to save the desired change with code: " & Err.Number & ". Aborting!"
83         WScript.Quit(5)
84     Else
85         WScript.Echo "Property '" & Property_Name & "' successfully changed from '"
86         & OriginalValue & "' to '" & DesiredValue & "'."
87     End If
88 End If
```

Appendix D

1. SQL script

```
1  /*****
2  This sample T-SQL script performs basic maintenance tasks on SUSDB
3  1. Identifies indexes that are fragmented and defragments them. For certain
4  tables, a fill-factor is set in order to improve insert performance.
5  Based on MSDN sample at http://msdn2.microsoft.com/en-us/library/ms188917.aspx
6  and tailored for SUSDB requirements
7  2. Updates potentially out-of-date table statistics.
8  *****/
9
10 USE SUSDB;
11 GO
12 SET NOCOUNT ON;
13
14 -- Rebuild or reorganize indexes based on their fragmentation levels
15 DECLARE @work_to_do TABLE (
16     objectid int
17     , indexid int
18     , pagedensity float
19     , fragmentation float
20     , numrows int
21 )
22
23 DECLARE @objectid int;
24 DECLARE @indexid int;
25 DECLARE @schemaname nvarchar(130);
26 DECLARE @objectname nvarchar(130);
27 DECLARE @indexname nvarchar(130);
28 DECLARE @numrows int
29 DECLARE @density float;
30 DECLARE @fragmentation float;
```

```

31 DECLARE @command nvarchar(4000);
32 DECLARE @fillfactorset bit
33 DECLARE @numpages int
34
35 -- Select indexes that need to be defragmented based on the following
36 -- * Page density is low
37 -- * External fragmentation is high in relation to index size
38 PRINT 'Estimating fragmentation: Begin. ' + convert(nvarchar, getdate(), 121)
39 INSERT @work_to_do
40 SELECT
41     f.object_id
42     , index_id
43     , avg_page_space_used_in_percent
44     , avg_fragmentation_in_percent
45     , record_count
46 FROM
47     sys.dm_db_index_physical_stats (DB_ID(), NULL, NULL , NULL, 'SAMPLED') AS f
48 WHERE
49     (f.avg_page_space_used_in_percent < 85.0 and f.avg_page_space_used_in_percent/100.0 * page_count < page_
50     or (f.page_count > 50 and f.avg_fragmentation_in_percent > 15.0)
51     or (f.page_count > 10 and f.avg_fragmentation_in_percent > 80.0)
52
53 PRINT 'Number of indexes to rebuild: ' + cast(@@ROWCOUNT as nvarchar(20))
54
55 PRINT 'Estimating fragmentation: End. ' + convert(nvarchar, getdate(), 121)
56
57 SELECT @numpages = sum(ps.used_page_count)
58 FROM
59     @work_to_do AS fi
60     INNER JOIN sys.indexes AS i ON fi.objectid = i.object_id and fi.indexid = i.index_id
61     INNER JOIN sys.dm_db_partition_stats AS ps on i.object_id = ps.object_id and i.index_id = ps.index_id
62
63 -- Declare the cursor for the list of indexes to be processed.
64 DECLARE curIndexes CURSOR FOR SELECT * FROM @work_to_do
65
66 -- Open the cursor.
67 OPEN curIndexes
68
69 -- Loop through the indexes
70 WHILE (1=1)
71 BEGIN
72     FETCH NEXT FROM curIndexes
73     INTO @objectid, @indexid, @density, @fragmentation, @numrows;
74     IF @@FETCH_STATUS < 0 BREAK;
75

```

```

76     SELECT
77         @objectname = QUOTENAME(o.name)
78         , @schemaname = QUOTENAME(s.name)
79     FROM
80         sys.objects AS o
81         INNER JOIN sys.schemas as s ON s.schema_id = o.schema_id
82     WHERE
83         o.object_id = @objectid;
84
85     SELECT
86         @indexname = QUOTENAME(name)
87         , @fillfactorset = CASE fill_factor WHEN 0 THEN 0 ELSE 1 END
88     FROM
89         sys.indexes
90     WHERE
91         object_id = @objectid AND index_id = @indexid;
92
93     IF ((@density BETWEEN 75.0 AND 85.0) AND @fillfactorset = 1) OR (@fragmentation < 30.0)
94         SET @command = N'ALTER INDEX ' + @indexname + N' ON ' + @schemaname + N'.' + @objectname + N' REORGANIZE';
95     ELSE IF @numrows >= 5000 AND @fillfactorset = 0
96         SET @command = N'ALTER INDEX ' + @indexname + N' ON ' + @schemaname + N'.' + @objectname + N' REBUILD';
97     ELSE
98         SET @command = N'ALTER INDEX ' + @indexname + N' ON ' + @schemaname + N'.' + @objectname + N' REBUILD';
99     PRINT convert(nvarchar, getdate(), 121) + N' Executing: ' + @command;
100    EXEC (@command);
101    PRINT convert(nvarchar, getdate(), 121) + N' Done.';
102    END
103
104    -- Close and deallocate the cursor.
105    CLOSE curIndexes;
106    DEALLOCATE curIndexes;
107
108
109    IF EXISTS (SELECT * FROM @work_to_do)
110    BEGIN
111        PRINT 'Estimated number of pages in fragmented indexes: ' + cast(@numpages as nvarchar(20))
112        SELECT @numpages = @numpages - sum(ps.used_page_count)
113        FROM
114            @work_to_do AS fi
115            INNER JOIN sys.indexes AS i ON fi.objectid = i.object_id and fi.indexid = i.index_id
116            INNER JOIN sys.dm_db_partition_stats AS ps on i.object_id = ps.object_id and i.index_id = ps.index_id
117
118        PRINT 'Estimated number of pages freed: ' + cast(@numpages as nvarchar(20))
119    END
120    GO

```

```
121  
122  
123 --Update all statistics  
124 PRINT 'Updating all statistics.' + convert(nvarchar, getdate(), 121)  
125 EXEC sp_updatestats  
126 PRINT 'Done updating statistics.' + convert(nvarchar, getdate(), 121)  
127 GO
```

Appendix E

2. SQL Script

```
1  USE [SUSDB];
2
3  DECLARE @BatchSize int = NULL; -- NULL = do all; <<-- Control batches here
4
5  SET NOCOUNT ON;
6
7  -- Check to see if the delete indexes exist; if not don't try to run the script:
8  DECLARE @IndexRetry bit = 1;
9  IndexRetry:
10 IF INDEXPROPERTY(OBJECT_ID('tbRevisionSupersedesUpdate'),N'IX_tbRevisionSupersedesUpdate',N'IndexID') IS NU
11     OR INDEXPROPERTY(OBJECT_ID('tbLocalizedPropertyForRevision'),N'IX_tbLocalizedPropertyForRevision',N'Inde
12 GOTO NeedIndexes;
13
14 -- Create tables/variables:
15 DROP TABLE IF EXISTS #Results; -- This will only work on newer versions of SQL Server 2016+
16 DECLARE @UpdateId int
17         ,@CurUpdate int
18         ,@TotalToDelete int
19         ,@Msg varchar(2000);
20 CREATE TABLE #Results (RowNum int IDENTITY(1,1) PRIMARY KEY CLUSTERED NOT NULL, UpdateId int NOT NULL);
21 INSERT INTO #Results (UpdateId)
22 EXECUTE dbo.spGetObsoleteUpdatesToCleanup;
23
24 -- If a batch size was provided update the table so we only take care of that many items during this run:
25 IF @BatchSize IS NOT NULL
26 DELETE #Results
27     WHERE RowNum > @BatchSize;
28
29 -- Assign working variables:
30 SELECT @TotalToDelete = MAX(RowNum)
```



```

31     FROM #Results;
32     --
33     SELECT @Msg = 'Total Updates to Delete: ' + CONVERT(varchar(10),@TotalToDelete);
34     RAISERROR (@Msg,0,1) WITH NOWAIT;
35
36     -- Create the loop to delete the updates one at a time:
37     WHILE EXISTS (SELECT * FROM #Results)
38     BEGIN
39         -- Grab the "current" item:
40         SELECT TOP 1 @CurUpdate = RowNum
41             ,@UpdateId = UpdateId
42             FROM #Results
43             ORDER BY RowNum;
44
45         -- Provide some info during the script runtime:
46         SELECT @Msg = CONVERT(varchar(30),GETDATE(),20) + ':' + Deleting ' + CONVERT(varchar(5),@CurUpdate) + '/' +
47         RAISERROR(@Msg,0,1) WITH NOWAIT;
48
49         -- Delete the current update from the DB:
50         EXECUTE dbo.spDeleteUpdate @localUpdateID = @UpdateId;
51
52         -- Delete the current update from the table so we can get the next item:
53         DELETE #Results
54             WHERE RowNum = @CurUpdate;
55     END;
56     GOTO EndScript;
57
58     NeedIndexes:
59     -- If the indexes don't exist we'll try to create them and start over or end if we already tried once:
60     IF @IndexRetry = 0
61     BEGIN
62         PRINT N'Indexes Required to run this script do not exist! Create them and re-run for optimal performance';
63         GOTO EndScript;
64     END;
65     ELSE
66     BEGIN
67         IF INDEXPROPERTY(OBJECT_ID(N'tbRevisionSupersedesUpdate'),N'IX_tbRevisionSupersedesUpdate',N'IndexID') = 0
68         BEGIN
69             SELECT @Msg = CONVERT(varchar(30),GETDATE(),20) + ':' + Index "IX_tbRevisionSupersedesUpdate" does not
70             RAISERROR(@Msg,0,1) WITH NOWAIT;
71             EXECUTE (N'USE [SUSDB]; CREATE NONCLUSTERED INDEX IX_tbRevisionSupersedesUpdate ON dbo.tbRevisionSup
72             SELECT @Msg = CONVERT(varchar(30),GETDATE(),20) + ':' + ..."IX_tbRevisionSupersedesUpdate" created.';
73             RAISERROR(@Msg,0,1) WITH NOWAIT;
74         END;
75         IF INDEXPROPERTY(OBJECT_ID(N'tbLocalizedPropertyForRevision'),N'IX_tbLocalizedPropertyForRevision',N'Ind

```

```
76      BEGIN
77          SELECT @Msg = CONVERT(varchar(30),GETDATE(),20) + ': Index "IX_tbLocalizedPropertyForRevision" does
78          RAISERROR(@Msg,0,1) WITH NOWAIT;
79          EXECUTE (N'USE [SUSDB]; CREATE NONCLUSTERED INDEX IX_tbLocalizedPropertyForRevision ON dbo.tbLocaliz
80          SELECT @Msg = CONVERT(varchar(30),GETDATE(),20) + ': ..."IX_tbLocalizedPropertyForRevision" created.
81          RAISERROR(@Msg,0,1) WITH NOWAIT;
82      END;
83
84      SET @IndexRetry = 0;
85      GOTO IndexRetry;
86  END;
87
88  EndScript:
89  DROP TABLE IF EXISTS #Results;
```

Appendix F

Software Update Maintenance - Script

Due to the structure of this script, it is more appropriate to include it as a link to its location within GitHub. The reason for this is that it is actually a collection of large scripts with accompanying configuration files, and add-on scripts. GitHub location: https://github.com/ErikSorli/Scripts-used-in-bachelor-thesis/tree/main/software_update_Maintainance

Appendix G

Read Ccmeval result

```
1  function Get-CCMEvalResult
2  {
3      <#                .Synopsis
4          Get the results of the most recent client health evaluation on a local or remote computer
5      .DESCRIPTION
6          Parses the ccmevalreport.xml file into a readable format to view the results of the ccmeval task. Can
7      .EXAMPLE
8          Get-CCMEvalResult Returns the ccmeval results from the local machine
9      .EXAMPLE
10         Get-CCMEvalResult -ComputerName PC001 Returns the ccmeval results from a remote machine
11     .EXAMPLE
12         'PC001','PC002' | Get-CCMEvalResult Returns the ccmeval results from a remote machine
13     #>
14
15     #requires -Version 2
16
17     [CmdletBinding()]
18     Param
19     (
20         [Parameter(Mandatory = $false,
21             ValueFromPipeline = $true
22         )]
23         [string[]]$ComputerName = $env:COMPUTERNAME
24     )
25
26     Begin {
27         $Script = {
28             $TargetFile = "C:\Windows\CCM\CcmEvalReport.xml"
29             try
30             {
```

```

31         Start-Process -FilePath powershell.exe -ArgumentList "-Command ""
32         &{Copy-Item C:\Users\Administrator\Documents\CcmEvalReport.xml
33         $TargetFile -Force}"" -Wait -ErrorAction Stop -Verb Runas -WindowStyle Hidden
34     }
35     catch
36     {
37         $_.Exception.Message
38         continue
39     }
40
41     if (!(test-path $TargetFile))
42     {
43         Write-Error -Message "Could not locate the CcmEvalReport.xml"
44         continue
45     }
46
47     $xml = New-Object -TypeName System.Xml.XmlDocument
48     $xml.Load($TargetFile)
49     Remove-Item $TargetFile -Force
50     return $xml
51 }
52 }
53
54 Process {
55     if ($ComputerName -eq $env:COMPUTERNAME)
56     {
57         $xml = Invoke-Command -ScriptBlock $Script
58     }
59     Else
60     {
61         try
62         {
63             $xml = Invoke-Command -ScriptBlock $Script -ComputerName
64             $ComputerName -ErrorAction Stop
65         }
66         catch
67         {
68             if ($Error[0] | Select-String -Pattern 'Access is denied')
69             {
70                 $Credentials = $host.ui.PromptForCredential('Credentials required',
71                 "Access was denied to $Computername. Enter credentials to connect.", '', '')
72                 $xml = Invoke-Command -ScriptBlock $Script -ComputerName $ComputerName
73                 -Credential $Credentials
74             }
75             Else { $_.Exception.Message }

```

```
76         }
77     }
78
79     $Checks = $xml.ClientHealthReport.HealthChecks.HealthCheck |
80     Select-Object -Property @{
81         l = 'Test'
82         e = {
83             $_.Description
84         }
85     }, @{
86         l = 'Result'
87         e = {
88             $_. '#text'
89         }
90     } |
91     Sort-Object -Property Test
92     [array]$Summary = $xml.ClientHealthReport.Summary |
93     Select-Object -Property @{
94         l = 'ComputerName'
95         e = {
96             $ComputerName
97         }
98     }, @{
99         l = 'EvaluationTime'
100        e = {
101            [datetime]($_.EvaluationTime)
102        }
103    }, @{
104        l = 'Result'
105        e = {
106            $_. '#text'
107        }
108    }
109
110     $Summary
111     $Checks | Format-Table
112 }
113 }
```

Appendix H

Risk Matrices

H.1 Consequence matrix

Konsekvensmatrise - områder for vurdering av konsekvens for HDO						
Verdi	Måloppnåelse	Lover og avtaler	Leveranse til kunde	Finans	Omdømme	Personer
4	Svært høy - Ett eller flere av HDOs hovedmål oppnås ikke.	Omfattende og alvorlige brudd på en eller flere lover og/eller avtaler.	Vesentlig redusert leveranse av sentrale tjenester over lengre perioder.	Svært alvorlige konsekvenser for virksomhetens økonomi. Kan ikke løses innenfor virksomhetens økonomiske rammer.	Omfattende og langvarig svekkelse av tillit hos eiere, kunder og ansatte. Betydelig reduksjon av omdømme i samfunnet.	Svært alvorlige konsekvenser for flere menneskers personvern, sosiale, fysiske eller økonomiske forhold.
3	Høy - Betydelig redusert oppnåelse av ett eller flere av HDOs hovedmål.	Alvorlig, men mindre omfattende brudd på lover eller avtaler.	Vesentlig redusert leveranse av sentrale tjenester over kortere perioder.	Alvorlige konsekvenser for virksomhetens økonomi, men kan løses innenfor virksomhetens økonomiske rammer.	Betydelig redusert tillit hos eiere, kunder og ansatte. Mindre reduksjon av omdømme i samfunnet.	Alvorlige konsekvenser for flere menneskers personvern, sosiale, fysiske eller økonomiske forhold.
2	Moderat - Delvis redusert oppnåelse av hovedmål eller delmål.	Mindre alvorlig og mindre omfattende avvik i forhold til lover eller avtaler.	Redusert leveranse av en eller flere deltjenester over kortere perioder.	Mindre alvorlige konsekvenser for virksomhetens økonomi. Kan ofte løses innenfor eksisterende budsjett.	Mindre redusert tillit og omdømme hos eiere, kunder og ansatte. Ikke samfunnsmessige konsekvenser.	Mindre alvorlige konsekvenser for enkelte menneskers personvern, sosiale, fysiske eller økonomiske forhold.
1	Lav - Mindre reduksjon i måloppnåelse.	Mindre alvorlig og mindre omfattende avvik iht. avtaler.	Redusert leveranse av en eller flere mindre tjenester over kortere perioder.	Mindre økonomiske konsekvenser. Eksempel: Tap eller overskridelse < MNOK 2	Mindre redusert tillit hos ansatte. Ikke konsekvenser i forhold til eiere, kunder eller samfunn.	Små konsekvenser for enkelte menneskers personvern, sosiale, fysiske eller økonomiske forhold.
0	Ingen eller ubetydelig konsekvens	Ingen eller ubetydelig konsekvens	Ingen eller ubetydelig konsekvens	Ingen eller ubetydelig konsekvens	Ingen eller ubetydelig konsekvens	Ingen eller ubetydelig konsekvens

Figure H.1: Consequence matrix from HDO.

H.2 Probability matrix

Beskrivelse sannsynlighet for HDOs risikoregister			
Sannsynlighet	Frekvens	Letthetsvurdering - Tiltak	Letthetsvurdering - Motivasjon
4 Svært høy sannsynlighet	Inntreffer flere ganger hver måned	Sikkerhetstiltak er ikke etablert, eller kan omgå/brytes av egne medarbeidere og eksternt personell med små til normale ressurser. Det er ikke nødvendig med kjennskap til tiltakene.	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevist eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.
3 Høy sannsynlighet	Inntreffer en gang per år eller oftere	Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten. Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene. Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normalle ressurser. Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten.	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.
2 Moderat sannsynlighet	Inntreffer sjeldnere enn en gang per år	Tiltakene kan likevel omgå/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene. Eksternt personell trenger gode ressurser, og godfullstendig kjennskap til tiltakene for å omgå/bryte disse.	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.
1 Lav sannsynlighet	Inntreffer en gang per 5 år eller sjeldnere	Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgå/brytes av egne medarbeidere med gode ressurser, og godfullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene.	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten
Veiledning: Sannsynlighet vurderes ut ifra muligheten for at en hendelse inntreffer med den tilhørende konsekvensen.			

Figure H.2: probability matrix from HDO.

Appendix J

STIG GPO's overview

Account lockout threshold	<p>This policy setting determines the number of failed logon attempts before a lock occurs. Authorized users can lock themselves out of an account by mistyping their password or by remembering it incorrectly, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password will continuously try to authenticate the user, and because the password it uses to authenticate is incorrect, a lock occurs. To avoid accidental lockout of authorized users, set the account lockout threshold to a high number. The default value for this policy setting is 0 invalid logon attempts, which disables the account lockout feature.</p> <p>Because it is possible for an attacker to use this lockout state as a denial of service (DoS) by triggering a lockout on a large number of accounts, your organization should determine whether to use this policy setting based on identified threats and the risks you want to mitigate. There are two options to consider for this policy setting.</p> <ul style="list-style-type: none"> - Configure the value for Account lockout threshold to 0 to ensure that accounts will not be locked out. This setting value will prevent a DoS attack that attempts to lock out accounts in your organization. It will also reduce help desk calls, because users will not be able to lock themselves out of their accounts accidentally. However, this setting value will not prevent a brute force attack. The following defenses should also be considered: <ul style="list-style-type: none"> - A password policy that forces all users to have complex passwords made up of 8 or more characters. - A robust auditing mechanism, which will alert administrators when a series of account lockouts occurs in the environment. For example, the auditing solution should monitor for security event 539, which is a logon failure. This event identifies that there was a lock on the account at the time of the logon attempt. The second option is:
Reset account lockout counter after	<p>This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting.</p> <p>If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically.</p>
Account lockout duration	<p>This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.</p> <p>Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.</p>

Accounts: Rename guest account	<p>The built-in local guest account is another well-known name to attackers. Microsoft recommends to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.</p> <p>Note This policy setting is not configured in the Security Templates, nor is a new user name for the account suggested here. Suggested user names are omitted to ensure that organizations that implement this guidance will not use the same new user name in their environments.</p>
Network access: Allow anonymous SID/Name translation	<p>This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs.</p>
Accounts: Guest account status	<p>This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.</p>
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	<p>This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords.</p>
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	<p>This policy setting controls the behavior of the elevation prompt for administrators.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments. - Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege. - Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. - Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

User Account Control: Behavior of the elevation prompt for standard users	<p>This policy setting controls the behavior of the elevation prompt for standard users.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls. - Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008.
User Account Control: Detect application installations and prompt for elevation	<p>This policy setting controls the behavior of application installation detection for the computer.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Enabled: (Default for home) When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Disabled: (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary.
User Account Control: Run all administrators in Admin Approval Mode	<p>This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Enabled: (Default) Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode. - Disabled: Admin Approval Mode and all related UAC policy settings are disabled. Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

User Account Control: Only elevate UIAccess applications that are installed in secure locations	<p>This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:</p> <ul style="list-style-type: none"> - %ProgramFiles%, including subfolders - %System32%, including subfolders - %ProgramFiles(x86)%, including subfolders for 64-bit versions of Windows <p>Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Enabled: (Default) If an application resides in a secure location in the file system, it runs only with UIAccess integrity. - Disabled: An application runs with UIAccess integrity even if it does not reside in a secure location in the file system.
User Account Control: Virtualize file and registry write failures to per-user locations	<p>This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry. - Disabled: Applications that write data to protected locations fail.
User Account Control: Admin Approval Mode for the Built-in Administrator account	<p>This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation. - Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege.
Interactive logon: Machine inactivity limit	Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.
Network Security: Configure encryption types allowed for Kerberos	<p>This policy setting allows you to set the encryption types that Kerberos is allowed to use.</p> <p>This policy is supported on at least Windows 7 or Windows Server 2008 R2.</p>

Network access: Let Everyone permissions apply to anonymous users	This policy setting determines what additional permissions are assigned for anonymous connections to the computer. If you enable this policy setting, anonymous Windows users are allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks.
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	<p>This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Although this policy setting increases security, most public Web sites that are secured with TLS or SSL do not support these algorithms. Client computers that have this policy setting enabled will also be unable to connect to Terminal Services on servers that are not configured to use the FIPS compliant algorithms.</p> <p>Note If you enable this policy setting, computer performance will be slower because the 3DES process is performed on each block of data in the file three times. This policy setting should only be enabled if your organization is required to be FIPS compliant.</p> <p>Important: This setting is recorded in different registry locations depending upon the version of Windows being used. For Windows XP and Windows Server 2003 it is stored at HKLM\System\CurrentControlSet\Control\Lsa\FIPSAAlgorithmPolicy, with Windows Vista and later versions of Windows it is stored at HKLM\System\CurrentControlSet\Control\Lsa\FIPSAAlgorithmPolicy\Enabled. This means that you must use Windows XP or Windows Server 2003 to edit group policies and security templates which will be applied to computers running Windows XP or Windows Server 2003. However, when editing group policies or security templates which will be applied to computers running Windows Vista or Windows Server 2008 you must use Windows Vista or Windows Server 2008.</p>
Accounts: Limit local account use of blank passwords to console logon only	This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.

Network security: LAN Manager authentication level	<p>LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2.</p> <p>LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:</p> <ul style="list-style-type: none"> - Join a domain - Authenticate between Active Directory forests - Authenticate to down-level domains - Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP - Authenticate to computers that are not in the domain <p>The possible values for the Network security: LAN Manager authentication level setting are:</p> <ul style="list-style-type: none"> - Send LM & NTLM responses - Send LM & NTLM "use NTLMv2 session security if negotiated" - Send NTLM responses only - Send NTLMv2 responses only - Send NTLMv2 responses only\refuse LM - Send NTLMv2 responses only\refuse LM & NTLM - Not Defined <p>The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons.</p>
Network security: Allow LocalSystem NULL session fallback	<p>Allow NTLM to fall back to NULL session when used with LocalSystem.</p> <p>The default is TRUE up to Windows Vista and FALSE in Windows 7.</p>
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	<p>This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.</p> <p>The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:</p> <ul style="list-style-type: none"> - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	<p>This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.</p> <p>The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:</p> <ul style="list-style-type: none"> - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.
Network security: Do not store LAN Manager hash value on next password change	<p>This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT[®] hash.</p> <p>Note Older operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting.</p>
Network Security: Allow PKU2U authentication requests to this computer to use online identities	<p>Windows 7 and Windows Server 2008 R2 introduce an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. You can also develop or add other SSPs.</p> <p>When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes.</p> <p>This policy will be turned off by default on domain joined machines. This would disallow the online identities to be able to authenticate to the domain joined machine in Windows 7.</p>
Network access: Do not allow anonymous enumeration of SAM accounts and shares	<p>This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment.</p> <p>The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide.</p>

Network access: Do not allow anonymous enumeration of SAM accounts	This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections cannot enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections.
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled.
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	This policy setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create.
Microsoft network server: Digitally sign communications (always)	This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.
Network access: Restrict anonymous access to Named Pipes and Shares	When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccess with the value 1 in the HKLM\System\CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.
Microsoft network client: Send unencrypted password to third-party SMB servers	Disable this policy setting to prevent the SMB redirector from sending plaintext passwords during authentication to third-party SMB servers that do not support password encryption. Microsoft recommends that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.

Microsoft network client: Digitally sign communications (always)	<p>This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments.</p> <p>Note When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.</p>
Network security: LDAP client signing requirements	<p>This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests, as follows:</p> <ul style="list-style-type: none"> - None. The LDAP BIND request is issued with the caller-specified options. - Negotiate signing. If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options. - Require signature. This level is the same as Negotiate signing. However, if the LDAP server's intermediate sasIBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. <p>Note: This policy setting does not have any impact on <code>ldap_simple_bind</code> or <code>ldap_simple_bind_s</code>. No Microsoft LDAP clients that are included with Windows XP Professional use <code>ldap_simple_bind</code> or <code>ldap_simple_bind_s</code> to communicate with a domain controller.</p> <p>The possible values for the Network security: LDAP client signing requirements setting are:</p> <ul style="list-style-type: none"> - None - Negotiate signing - Require signature - Not Defined
Domain member: Disable machine account password changes	<p>This policy setting determines whether a domain member can periodically change its computer account password. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the Domain Member: Maximum machine account password age setting, which by default is every 30 days. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account.</p>

Domain member: Maximum machine account password age	This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly or set it to 0 so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts.
Domain member: Digitally encrypt or sign secure channel data (always)	This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data must be signed and encrypted. Microsoft recommends to configure the Domain member: Digitally encrypt or sign secure channel data (always) setting to Enabled.
Domain member: Require strong (Windows 2000 or later) session key	When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key. To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000-based domains is required, Microsoft recommends that you disable this policy setting.
Domain member: Digitally encrypt secure channel data (when possible)	This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption. Microsoft recommends to configure the Domain member: Digitally encrypt secure channel data (when possible) setting to Enabled.
Domain member: Digitally sign secure channel data (when possible)	This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network. Microsoft recommends to configure the Domain member: Digitally sign secure channel data (when possible) setting to Enabled.
Secondary Logon	Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Access Credential Manager as a trusted caller	This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Access this computer from the network	<p>This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)–based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Act as part of the operating system	<p>This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Allow log on locally	<p>This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, Microsoft recommends that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Back up files and directories	<p>This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Change the system time	<p>This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p> <p>Note: Discrepancies between the time on the local computer and on the domain controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the domain controllers.</p>

Create a pagefile	<p>This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Create a token object	<p>This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Create global objects	<p>This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right.</p> <p>Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Create permanent shared objects	<p>This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Create symbolic links	<p>This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.</p> <p>Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only Administrators can create symbolic links.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>

Debug programs	<p>This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it.</p> <p>Note Microsoft released several security updates in October 2003 that used a version of Update.exe that required the administrator to have the Debug programs user right. Administrators who did not have this user right were unable to install these security updates until they reconfigured their user rights. This is not typical behavior for operating system updates. For more information, see Knowledge Base article 830846: "Windows Product Updates may stop responding or may use most or all the CPU resources."</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Deny access to this computer from the network	<p>This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Deny log on as a batch job	<p>This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right.</p> <p>The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Deny log on as a service	<p>This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. Note: This security setting does not apply to the System, Local Service, or Network Service accounts.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>

Deny log on locally	<p>This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Deny log on through Remote Desktop Services	<p>This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Enable computer and user accounts to be trusted for delegation	<p>This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Force shutdown from a remote system	<p>This policy setting allows users to shut down Windows Vista™-based computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, Microsoft recommends that only highly trusted administrators be assigned this user right.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>

Impersonate a client after authentication	<p>The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.</p> <p>Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.</p> <p>Also, a user can impersonate an access token if any of the following conditions exist:</p> <ul style="list-style-type: none"> - The access token that is being impersonated is for this user. - The user, in this logon session, logged on to the network with explicit credentials to create the access token. - The requested level is less than Impersonate, such as Anonymous or Identify. <p>An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Load and unload device drivers	<p>This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Lock pages in memory	<p>This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Manage auditing and security log	<p>This policy setting determines which users can change the auditing options for files and directories and clear the Security log.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Modify firmware environment values	<p>This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values could lead to a hardware failure that would result in a denial of service condition.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>

Perform volume maintenance tasks	<p>This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Profile single process	<p>This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right prevents intruders from gaining additional information that could be used to mount an attack on the system.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Restore files and directories	<p>This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Take ownership of files or other objects	<p>This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.</p> <p>When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.</p>
Enumerate administrator accounts on elevation	By default, all administrator accounts are displayed when you attempt to elevate a running application.
Turn off Internet download for Web publishing and online ordering wizards	This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards.
Turn off downloading of print drivers over HTTP	This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.
Turn off printing over HTTP	This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.
Turn off access to all Windows Update features	<p>This setting allows you to remove access to Windows Update.</p> <p>If you enable this setting, all Windows Update features are removed. This includes blocking access to the Windows Update Web site at http://windowsupdate.microsoft.com, from the Windows Update hyperlink on the Start menu, and also on the Tools menu in Internet Explorer. Windows automatic updating is also disabled; you will neither be notified about nor will you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site.</p>

	<p>If you disable or do not configure this setting, users will be able to access the Windows Update Web site and enable automatic updating to receive notifications and critical updates from Windows Update.</p>
Default behavior for AutoRun	<p>Sets the default behavior for Autorun commands.</p> <p>Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.</p> <p>Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention.</p> <p>This creates a major security concern as code may be executed without user's knowledge. The default behavior in Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.</p> <p>If you enable this policy, an Administrator can change the default Windows Vista behavior for autorun to:</p> <ul style="list-style-type: none"> A) Completely disable autorun commands, or B) Revert back to Pre-Windows Vista behavior of automatically executing the autorun command. <p>If you disable or not configure this policy, Windows Vista will prompt the user whether autorun command is to be run.</p>
Turn off Autoplay	<p>Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.</p> <p>Note You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives.</p>
Turn off Autoplay for non-volume devices	<p>If this policy is enabled, autoplay will not be enabled for non-volume devices like MTP devices. If you disable or not configure this policy, autoplay will continue to be enabled for non-volume devices.</p>

Require additional authentication at startup	<p>This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.</p> <p>Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.</p> <p>If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode a USB drive is required for start-up and the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable you will need to use one of the BitLocker recovery options to access the drive.</p> <p>On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 4-digit to 20-digit personal identification number (PIN), or both.</p> <p>If you enable this policy setting, users can configure advanced startup options in the BitLocker setup wizard.</p> <p>If you disable or do not configure this policy setting, users can configure only basic options on computers with a TPM.</p>
Configure minimum PIN length for startup	<p>This policy setting allows you to configure a minimum length for a Trusted Platform Module (TPM) startup PIN. This policy setting is applied when you turn on BitLocker. The startup PIN must have a minimum length of 4 digits and can have a maximum length of 20 digits.</p> <p>If you enable this policy setting, you can require a minimum number of digits to be used when setting the startup PIN.</p> <p>If you disable or do not configure this policy setting, users can configure a startup PIN of any length between 4 and 20 digits.</p>

Allow enhanced PINs for startup	<p>This policy setting allows you to configure whether or not enhanced startup PINs are used with BitLocker.</p> <p>Enhanced startup PINs permit the use of characters including uppercase and lowercase letters, symbols, numbers, and spaces. This policy setting is applied when you turn on BitLocker.</p> <p>If you enable this policy setting, all new BitLocker startup PINs set will be enhanced PINs.</p> <p>Note: Not all computers may support enhanced PINs in the pre-boot environment. It is strongly recommended that users perform a system check during BitLocker setup.</p> <p>If you disable or do not configure this policy setting, enhanced PINs will not be used.</p>
Deny write access to removable drives not protected by BitLocker	<p>This policy setting configures whether BitLocker protection is required for a computer to be able to write data to a removable data drive.</p> <p>If you enable this policy setting, all removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.</p> <p>If the "Deny write access to devices configured in another organization" option is selected, only drives with identification fields matching the computer's identification fields will be given write access. When a removable data drive is accessed it will be checked for valid identification field and allowed identification fields. These fields are defined by the "Provide the unique identifiers for your organization" policy setting.</p> <p>If you disable or do not configure this policy setting, all removable data drives on the computer will be mounted with read and write access.</p>
Prevent downloading of enclosures	<p>This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer.</p> <p>If you enable this policy setting, the user cannot set the Feed Sync Engine to download an enclosure through the Feed property page. A developer cannot change the download setting through the Feed APIs.</p> <p>If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.</p>
Require a Password When a Computer Wakes (On Battery)	Specifies whether or not the user is prompted for a password when the system resumes from sleep.
Require a Password When a Computer Wakes (Plugged In)	Specifies whether or not the user is prompted for a password when the system resumes from sleep.
Allow Standby States (S1-S3) When Sleeping (On Battery)	
Allow Standby States (S1-S3) When Sleeping (Plugged In)	

Turn off Program Inventory	<p>This policy controls the state of the Program Inventory collector in the system.</p> <p>The PDU inventories programs and files on the system and sends information about those files to Microsoft. This information is used to help associate files to programs and diagnose application compatibility problems.</p> <p>The PDU is on by default.</p> <p>If you enable this policy setting, inventory collection will be turned off and data will not be sent to Microsoft. Enabling this setting also disables collection of installation data through PCA.</p> <p>If you disable or do not configure this policy setting, inventory collection will be turned on.</p>
Prevent installation of devices using drivers that match these device setup classes	<p>This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.</p> <p>If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.</p> <p>If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.</p>
Maximum Log Size (KB)	<p>This policy requires Windows Vista or later versions of Windows. This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file maximum size will be set to the local configuration value. This value can be changed by the local administrator using the log properties dialog and it defaults to 20 megabytes. For backwards compatibility the same setting can also be configured at Computer Configuration\Windows Settings\Security Settings\Event Log, if set at both locations this one will take precedence.</p>
Maximum Log Size (KB)	<p>This policy requires Windows Vista or later versions of Windows. This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file maximum size will be set to the local configuration value. This value can be changed by the local administrator using the log properties dialog and it defaults to 20 megabytes. For backwards compatibility the same setting can also be configured at Computer Configuration\Windows Settings\Security Settings\Event Log, if set at both locations this one will take precedence.</p>

Configure registry policy processing	<p>This policy setting determines when registry policies are updated.</p> <p>This policy setting affects all policies in the Administrative Templates folder and any other policies that store values in the registry. It overrides customized settings that the program implementing a registry policy set when it was installed.</p> <p>If you enable this policy setting, you can use the check boxes provided to change the options. If you disable or do not configure this policy setting, it has no effect on the system.</p> <p>The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart.</p> <p>The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired policy setting in case a user has changed it.</p>
Enable user control over installs	<p>Permits users to change installation options that typically are available only to system administrators.</p> <p>This setting bypasses some of the security features of Windows Installer. It permits installations to complete that otherwise would be halted due to a security violation.</p> <p>The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.</p> <p>This setting is designed for less restrictive environments. It can be used to circumvent errors in an installation program that prevents software from being installed.</p>

Always install with elevated privileges	<p>Directs Windows Installer to use system permissions when it installs any program on the system.</p> <p>This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.</p> <p>If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.</p> <p>Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.</p> <p>Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.</p>
Enumerate local users on domain-joined computers	<p>This policy setting allows local users to be enumerated on domain-joined computers.</p> <p>If you enable this policy setting, Logon UI will enumerate all local users on domain-joined computers.</p> <p>If you disable or do not configure this policy setting, the Logon UI will not enumerate local users on domain-joined computers.</p>
Turn on PIN sign-in	<p>This policy setting allows you to control whether a domain user can sign in using a PIN.</p> <p>If you enable this policy setting, a domain user can set up and sign in with a PIN.</p> <p>If you disable or don't configure this policy setting, a domain user can't set up and use a PIN.</p> <p>Note that the user's domain password will be cached in the system vault when using this feature.</p>
Configure Windows SmartScreen	This policy setting allows you to manage the behavior of Windows SmartScreen

Configure Windows SmartScreen	<p>This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.</p> <p>If you enable this policy setting, Windows SmartScreen behavior may be controlled by setting one of the following options:</p> <ul style="list-style-type: none"> - Require approval from an administrator before running downloaded unknown software - Give user a warning before running downloaded unknown software - Turn off SmartScreen <p>If you disable or do not configure this policy setting, Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center.</p> <p>Options:</p> <ul style="list-style-type: none"> - Require approval from an administrator before running downloaded unknown software - Give user a warning before running downloaded unknown software - Turn off SmartScreen
Prohibit connection to non-domain networks when connected to domain authenticated network	<p>This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time.</p> <p>If this policy setting is enabled, the computer responds to automatic and manual network connection attempts based on the following circumstances:</p> <p>Automatic connection attempts</p> <ul style="list-style-type: none"> - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked. <p>Manual connection attempts</p> <ul style="list-style-type: none"> - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked. <p>If this policy setting is not configured or is disabled, computers are allowed to connect simultaneously to both domain and non-domain networks.</p>

Allow indexing of encrypted files	<p>This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content.</p> <p>When this setting is enabled or disabled, the index is rebuilt completely.</p> <p>Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.</p>
Allow Basic authentication	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication.</p> <p>If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text.</p> <p>If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication.</p>
Allow unencrypted traffic	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.</p> <p>If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network.</p> <p>If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.</p>
Disallow Digest authentication	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.</p> <p>If you enable this policy setting, the WinRM client will not use Digest authentication.</p> <p>If you disable or do not configure this policy setting, the WinRM client will use Digest authentication.</p>
Allow Basic authentication	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.</p> <p>If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client.</p> <p>If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client.</p>

Figure J.2

Allow unencrypted traffic	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.</p> <p>If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network.</p> <p>If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.</p>
Disallow WinRM from storing RunAs credentials	<p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins.</p> <p>If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer.</p> <p>If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely.</p> <p>If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset.</p>
Restrictions for Unauthenticated RPC clients	<p>This policy setting configures the RPC Runtime on an RPC server to restrict unauthenticated RPC clients from connecting to the RPC server. A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC interfaces that have specifically asked to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy.</p>
Do not allow passwords to be saved	<p>This policy setting helps prevent Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server.</p>
Do not allow drive redirection	<p>This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClnt\<driveletter>\$</p> <p>If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.</p>
Set client connection encryption level	<p>This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session.</p>

<p>Always prompt for password upon connection</p>	<p>This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.</p> <p>The Always prompt client for password upon connection setting is configured to Enabled for both of the environments that are discussed in this guide.</p> <p>Note If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent.</p>
<p>Require secure RPC communication</p>	<p>Specifies whether a Remote Desktop Session Host server requires secure RPC communication with all clients or allows unsecured communication.</p> <p>You can use this setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.</p> <p>If the status is set to Enabled, Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.</p> <p>If the status is set to Disabled, Remote Desktop Services always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request.</p> <p>If the status is set to Not Configured, unsecured communication is allowed.</p> <p>Note: The RPC interface is used for administering and configuring Remote Desktop Services.</p>

Allow users to connect remotely by using Remote Desktop Services	<p>This policy setting allows you to configure remote access to computers by using Remote Desktop Services.</p> <p>If you enable this policy setting, users who are members of the Remote Desktop Users group on the target computer can connect remotely to the target computer by using Remote Desktop Services.</p> <p>If you disable this policy setting, users cannot connect remotely to the target computer by using Remote Desktop Services. The target computer will maintain any current connections, but will not accept any new incoming connections.</p> <p>If you do not configure this policy setting, Remote Desktop Services uses the Remote Desktop setting on the target computer to determine whether the remote connection is allowed. This setting is found on the Remote tab in the System properties sheet. By default, remote connections are not allowed.</p> <p>Note: You can limit which clients are able to connect remotely by using Remote Desktop Services by configuring the policy setting at Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication.</p> <p>You can limit the number of users who can connect simultaneously by configuring the policy setting at Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Limit number of connections, or by configuring the policy setting Maximum Connections by using the Remote Desktop Session</p>
------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Boot-Start Driver Initialization Policy	<p>This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:</p> <ul style="list-style-type: none"> - Good: The driver has been signed and has not been tampered with. - Bad: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized. - Bad, but required for boot: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver. - Unknown: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver. <p>If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.</p> <p>If you disable or do not configure this policy setting, the boot start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be Bad is skipped.</p> <p>If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.</p>
Turn on or off details pane	<p>This policy setting shows or hides the Details Pane in Windows Explorer.</p> <p>If you enable this policy setting and configure it to hide the pane, the Details Pane in Windows Explorer is hidden and cannot be turned on by the user.</p> <p>If you enable this policy setting and configure it to show the pane, the Details Pane is always visible and cannot be hidden by the user. Note: This has a side effect of not being able to toggle to the Preview Pane since the two cannot be displayed at the same time.</p> <p>If you disable, or do not configure this policy setting, the Details Pane is hidden by default and can be displayed by the user. This is the default policy setting.</p>
Turn off Preview Pane	<p>Hides the Preview Pane in Windows Explorer.</p> <p>If you enable this policy setting, the Preview Pane in Windows Explorer is hidden and cannot be turned on by the user.</p> <p>If you disable, or do not configure this setting, the Preview Pane is displayed by default and can be hidden by the user.</p>

Figure J.3

Turn off toast notifications on the lock screen	<p>This policy setting turns off toast notifications on the lock screen.</p> <p>If you enable this policy setting, applications will not be able to raise toast notifications on the lock screen.</p> <p>If you disable or do not configure this policy setting, toast notifications on the lock screen are enabled and can be turned off by the administrator or user.</p> <p>No reboots or service restarts are required for this policy setting to take effect.</p>
Set percentage of disk space used for client computer cache	<p>This policy setting changes the default percentage of total disk space to dedicate to caching retrieved content with BranchCache. This content is made available to other requesting client computers if they are authorized by the server to access the content.</p> <p>If you enable this policy setting, you can configure the percentage of total disk space to allocate for the cache.</p> <p>If you disable or do not configure this policy setting, the cache is set to 5 percent of the total disk space on the client computer.</p>
Set BranchCache Distributed Cache mode	<p>This policy setting specifies whether the client computer should use the Distributed Cache mode. This BranchCache mode enables a client computer to retrieve content that has been downloaded and cached by other client computers in the branch office. To access cached content from other client computers in the branch, the computer must have permissions to access the content on the source server.</p> <p>This policy setting specifies whether the Distributed Cache mode is used. Enable this policy setting when using BranchCache in branch offices for which there is no server acting as a hosted cache.</p> <p>If you enable this policy setting, the Distributed Cache mode is used. For this policy setting to take effect, you also need to enable the "Turn on BranchCache" policy setting.</p> <p>If you disable or do not configure this policy setting, the Distributed Cache mode is turned off.</p>

Turn on BranchCache	<p>This policy setting specifies whether BranchCache is enabled on the client computer. BranchCache reduces the utilization of the wide area network (WAN) links connecting branch offices to the data center or headquarters and increases access speeds for content that has already been downloaded into the branch office. BranchCache does this by enabling computers in a branch office to cache files and HTTP traffic from Intranet servers on which BranchCache is enabled, and then securely share the files with other computers in the branch. Computers in the branch office can retrieve content from a hosted cache server in the branch (when using Hosted Cache mode), or from other client computers in the branch (when using Distributed Cache mode). To access cached content, the computer must have permissions to access the content on the source server.</p> <p>Enable this policy setting on client computers in branch offices where WAN bandwidth is low, latency is high, and there are a number of client computers that need to access the same data from servers in the central office.</p> <p>If you enable this policy setting, BranchCache is turned on. For this policy setting to take effect, you also must install the BranchCache feature on the client computer.</p> <p>If you disable or do not configure this policy setting, BranchCache is turned off.</p>
Configure Automatic Updates	<p>This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.</p> <p>After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:</p> <ul style="list-style-type: none"> - Notify before downloading any updates and notify again before installing them. - Download the updates automatically and notify when they are ready to be installed. (Default setting) - Automatically download updates and install them on the schedule specified below. <p>If you disable this policy setting, you will need to download and manually install any available updates from Windows Update.</p>

Specify settings for optional component installation and component repair	<p>This policy setting specifies the network locations that will be used for the repair of operating system corruption and for enabling optional features that have had their payload files removed.</p> <p>If you enable this policy setting and specify the new location, the files in that location will be used to repair operating system corruption and for enabling optional features that have had their payload files removed. You must enter the fully qualified path to the new location in the "Alternate source file path" text box. Multiple locations can be specified when each path is separated by a semicolon.</p> <p>The network location can be either a folder, or a WIM file. If it is a WIM file, the location should be specified by prefixing the path with "wim:" and include the index of the image to use in the WIM file. For example wim:\server\share\install.wim:3</p> <p>If you disable or do not configure this policy setting, or if the required files cannot be found at the locations specified in this policy setting, the files will be downloaded from Windows Update, if that is allowed by the policy settings for the computer.</p>
Turn on Script Execution	<p>This settings lets you configure the script execution policy, controlling what scripts are allowed to run.</p> <p>If you enable this setting, the scripts selected in the drop down list will be allowed to run.</p> <p>The "Allow only signed scripts" setting allows script to execute only if they are signed by a trusted publisher.</p> <p>The "Allow local scripts and remote signed scripts" setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.</p> <p>The "Allow all scripts" setting allows all scripts to run.</p> <p>If you disable this setting, no scripts are allowed to run.</p> <p>Note: This setting exists under both "Computer Configuration" and "User Configuration" in the group policy editor. The "Computer Configuration" has precedence over "User Configuration."</p> <p>If this policy setting is not configured or disabled, the setting reverts to a per-machine preference setting; the default if that is not configured is "No scripts allowed."</p>

Configure Solicited Remote Assistance	<p>This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.</p> <p>If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings.</p> <p>If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.</p> <p>If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.</p> <p>If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer."</p> <p>The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open.</p> <p>The "Select the method for sending email invitations" setting specifies which email standard to use to send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient</p>
Allow only Vista or later connections	<p>This policy setting enables Remote Assistance invitations to be generated with improved encryption so that only computers running this version (or later versions) of the operating system can connect. This setting does not affect Remote Assistance connections that are initiated by instant messaging contacts or the unsolicited Offer Remote Assistance.</p> <p>If you enable this policy setting, only computers running this version (or later versions) of the operating system can connect to this computer.</p> <p>If you disable this policy setting, computers running this version and a previous version of the operating system can connect to this computer.</p> <p>If you do not configure this setting users can configure the setting in System Properties in the Control Panel.</p>
Turn on session logging	<p>This policy setting allows you to turn logging on or off. Log files are located in the user's Documents folder under Remote Assistance.</p> <p>If you enable this policy setting, log files will be generated.</p> <p>If you disable this policy setting, log files will not be generated.</p> <p>If you do not configure this setting, application-based settings will be used.</p>

Turn on bandwidth optimization	<p>This policy setting allows you to improve performance in low bandwidth scenarios.</p> <p>This setting is incrementally scaled from "No optimization" to "Full optimization". Each incremental setting includes the previous optimization setting.</p> <p>For example:</p> <p>"Turn off background" will include the following optimizations: No full window drag Turn off background</p> <p>"Full optimization" will include the following optimizations: Use 16-bit color (8-bit color in Windows Vista) Turn off font smoothing(not supported in Windows Vista) No full window drag Turn off background</p> <p>If you enable this policy setting, bandwidth optimization will occur at the level specified.</p> <p>If you disable this policy setting, application-based settings will be used.</p> <p>If you do not configure this policy setting, application-based settings will be used.</p>
Customize Warning Messages	<p>The "Display warning message before sharing control" policy setting allows you to specify a custom message to display before a user shares control of his or her computer.</p> <p>The "Display warning message before connecting" policy setting allows you to specify a custom message to display before a user allows a connection to his or her computer.</p> <p>If you enable this policy setting, the warning message you specify will override the default message that is seen by the novice.</p> <p>If you disable this policy setting, the user will see the default warning message.</p> <p>If you do not configure this setting, the user will see the default warning message.</p>

Configure Offer Remote Assistance	<p>This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer.</p> <p>If you enable this policy setting, users on this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.</p> <p>If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.</p> <p>If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.</p> <p>If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance.</p> <p>To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:</p> <p><Domain Name>\<User Name> or</p> <p><Domain Name>\<Group Name></p>
-----------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix K

Altered Policies

Policy Type	Policy Group or Registration Key	Policy Setting	StigBaselineV1	Win10Baseline	StigBaselineV1 new setting
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters	AllowEncryptionOracle	Not configured	0	0
HKLM	Software\Policies\Microsoft\Services\AdmPwd	AdmPwdEnabled	Not configured	1	1(See chapter on LAPS)
HKLM	SOFTWARE\Policies\Microsoft\FVE	DisableExternalDMAUnderLock	Not configured	1	1
HKLM	System\CurrentControlSet\Policies\Microsoft\FVE	RDVDenyWriteAccess	Not configured	1	1
HKLM	SOFTWARE\Policies\Microsoft\FVE	UseEnhancedPin	Not configured	1	1
HKLM	SOFTWARE\Policies\Microsoft\Power\PowerSettings\ab7c2519-3608-4c2a-94ea-171b0ed546ab	ACSettingIndex	Not configured	0	0
HKLM	SOFTWARE\Policies\Microsoft\Power\PowerSettings\ab7c2519-3608-4c2a-94ea-171b0ed546ab	DCSettingIndex	Not configured	0	0
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions	DenyDeviceClasses	Not configured	1	1
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions	DenyDeviceClassesRetroactive	Not configured	1	1
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\DenyDeviceClasses	1	Not configured	{d48179be-e20-11d1-b6b8-00c04fa372a7}	{d48179be-e20-11d1-b6b8-00c04fa372a7}
HKLM	SYSTEM\CurrentControlSet\Services\Wext\Parameters	NodeType	Not configured	2	2

Figure K.1