



# The Admin's Guide to Preventing SCCM Attacks

Chris Thompson (@\_Mayhem)

Garrett Foster (@unsigned\_sh0rt)





## Garrett Foster

Senior Consultant @ SpecterOps  
Author of SCCMHunter & Misconfiguration Manager  
@unsigned\_sh0rt



## Chris Thompson

Senior Security Researcher @ SpecterOps  
Author of SharpSCCM & Misconfiguration Manager  
 @\_Mayhem



What this talk is not about:

- SCCM fundamentals
- Attack path execution
- Attack path detection

What this talk is about:

- **SCCM attack path prevention**
- Step-by-step reference guide
- Potential pitfalls (and **bypasses**)
- War stories and real-world context

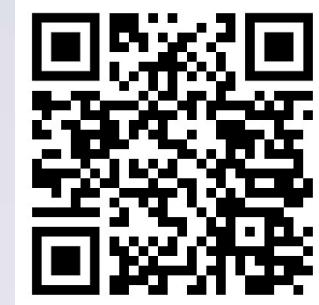
# Who is this talk for?

- Defenders who want to better **understand SCCM attack paths** and which mitigations are best suited for their environments
- System administrators who want to **implement mitigations** for known SCCM attack paths
- Offensive security pros who want to understand misconfigurations, their **potential bypasses**, and how to better report issues to clients



# Misconfiguration Manager

## SCCM Attack Path Management Knowledge Base



- Co-authored with Duane Michael (@subat0mik)
- Step-by-step foundational, offensive, and defensive **write-ups** for known techniques
- A **taxonomy** to simplify and demystify concepts (à la [Certified Pre-Owned](#))
- Based on MITRE ATT&CK
- PowerShell script to identify TAKEOVER and ELEVATE issues



<https://misconfigurationmanager.com>

# Misconfiguration Manager Taxonomy

Because "Hierarchy takeover via NTLM coercion and relay to MSSQL on remote site database" doesn't roll off the tongue...

## Attack Techniques



RECON



CRED



ELEVATE



TAKEOVER



EXEC

## Defense Techniques



PREVENT



DETECT



CANARY

<https://misconfigurationmanager.com>

# Hierarchy TAKEOVER

Gaining complete control of all client devices in the SCCM hierarchy

- How can attackers take over a hierarchy?
  - Obtain the **Full Administrator** role in **ANY** site
  - The site database is replicated to all sites
  - **Own one Primary Site, own them all**
- Why do we care?
  - Allows **arbitrary command execution** on all clients
  - Allows access to features like **CMPivot, Run Script**
  - Allows the ability to impact the availability of software



<https://posts.specterops.io/sccm-hierarchy-takeover-41929c61e087>

# Hierarchy TAKEOVER

## Key concepts

- Each site server's domain computer account must be:
  - Local admin on every site system role (i.e., every SCCM server)
  - Sysadmin in the site database
- Attackers can force this account to authenticate to an arbitrary IP address and use the creds to impersonate the site server to other SCCM servers, then grant themselves the Full Administrator role
- As defenders, if we can **prevent NTLM authentication with relayed credentials**, we prevent most known TAKEOVER and ELEVATE techniques



<https://posts.specterops.io/sccm-hierarchy-takeover-41929c61e087>

# SCCM Hierarchy Takeover Attack Paths



## TAKEOVER-1

NTLM coercion and relay to  
MSSQL on remote site database



## TAKEOVER-2

NTLM coercion and relay to  
SMB on remote site database



## TAKEOVER-3

NTLM coercion and relay  
to HTTP on ADCS



## TAKEOVER-4

NTLM coercion and relay from  
CAS to origin primary site server



## TAKEOVER-5

NTLM coercion and relay to  
AdminService on remote SMS Provider



## TAKEOVER-6

NTLM coercion and relay  
to SMB on remote  
SMS Provider



## TAKEOVER-7

NTLM coercion and relay  
to SMB between primary  
and passive site servers



## TAKEOVER-8

NTLM coercion and relay  
HTTP to LDAP  
on domain controller

SITE-SERVER - Remote Desktop

Microsoft Configuration Manager (Connected to PS1, Aperture Science - SITE-SERVER.APTURE.LOCAL)

Home

Add User or Group | Saved Searches | Create | Search

Administration Overview Updates and Servicing Hierarchy Configuration Cloud Services Site Configuration Client Settings Security Administrative Users

Administration Overview Updates and Servicing Hierarchy Configuration Cloud Services Site Configuration Client Settings Security Administrative Users

Administrative Users 2 items

Search current node

Icon	Account Name	Account Display Name	Security Roles
User icon	APTURE\labadmin	"Full Administrator"	
User icon	SITE-SERVER\labadmin	"Full Administrator"	

Ready

Type here to search

7:21 PM 5/4/2024

# Real World Examples

## TAKEOVER

The screenshot shows the CMPivot interface with the following details:

- Title Bar:** CMPivot (Connected to 123 - Primary Site - All Desktop and Server Clients)
- Entities Sidebar:** A tree view of various entities including DriverVxD, EmbeddedDeviceInformation, Environment, EPStatus, EventLog(), File (with sub-options like Device, FileName, Mode, LastWriteTime, Size, Version, SHA256Hash, MD5Hash, FileContent(), FileShare, Firmware, IDEController, InstalledExecutable, InstalledSoftware, IPCfg, IRQTable, Keyboard), and more.
- Query Bar:** Home, Query, Run Query, Create Collection, Export.
- Query Editor:** File('C:\Users\\*\\*.aws\\*')
- Results Table:** A grid showing file information from 5 clients. The columns are Device, FileName, Mode, LastWriteTime, Size, Version, and SHA256Hash. The data includes multiple entries for config and credentials files across several SCCM hosts.
- Status Bar:** Query completed on 5 of 8 clients (3 clients offline and 0 failures) id(16778562) | All Desktop and Server Clients | 8 objects



# TAKEOVER Prevention

**Just disable NTLM for the domain, it's easy!**

- Just kidding, please don't do this
- This recommendation is common (Chris is guilty of making it) but it isn't feasible to just flip the switch in many organizations
- Careful monitoring must take place beforehand to identify clients that don't support Kerberos
- However, **this fix doesn't account for Kerberos relay attacks**



# TAKEOVER Prevention

## Security Features

- Signing
  - A digital signature of each message is attached to the message, preventing tampering
  - Uses a shared session key to hash message
- Channel binding (e.g., extended protection for authentication, or EPA)
  - Prevents MITM/spoofing attacks by binding authentication to the secure channel
  - Token from secure outer protocol (TLS) is embedded in each authentication message, preventing tampering
- Disable/block connectivity to protocols that don't support these features



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-adcs-3612b773-4043-4aa9-b23d-b87910cd3429>

# TAKEOVER/ELEVATE Prevention

## Prevent Relayed Credentials from Authenticating Successfully

Technique	Codename
Require EPA on AD CS and site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Disable and uninstall WebClient on site servers	PREVENT-11
Block unnecessary connections to site systems	PREVENT-20
Require LDAP channel binding and signing	PREVENT-13

**IMPORTANT:** Implementing these settings **will** impact connectivity and/or performance and we have only personally tested them in a lab environment, so it is crucial to first audit and test these changes in your environment before implementing in production.



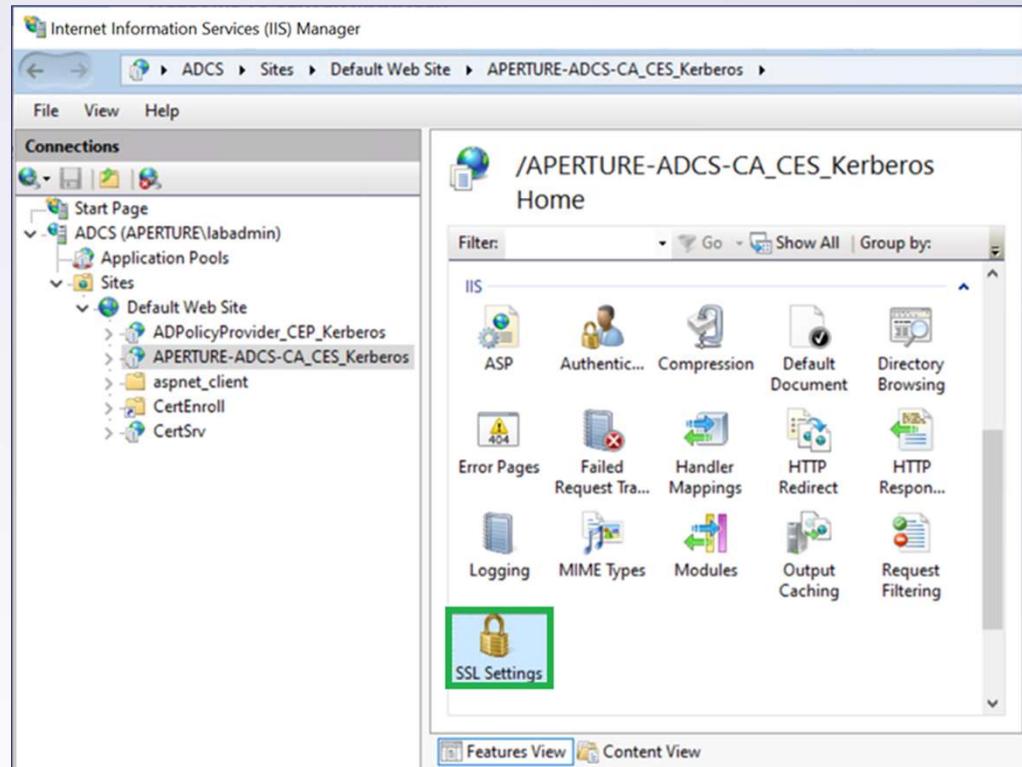
[https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/\\_defense-techniques-list.md](https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/_defense-techniques-list.md)

# Require EPA on AD CS

## PREVENT-14

On AD CS servers:

1. Open IIS Manager
2. Expand the connection, “Sites”, and “Default Web Site”
3. Click on “CertSrv” to configure the Certificate Authority Enrollment Service
4. Double-click “SSL Settings”



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

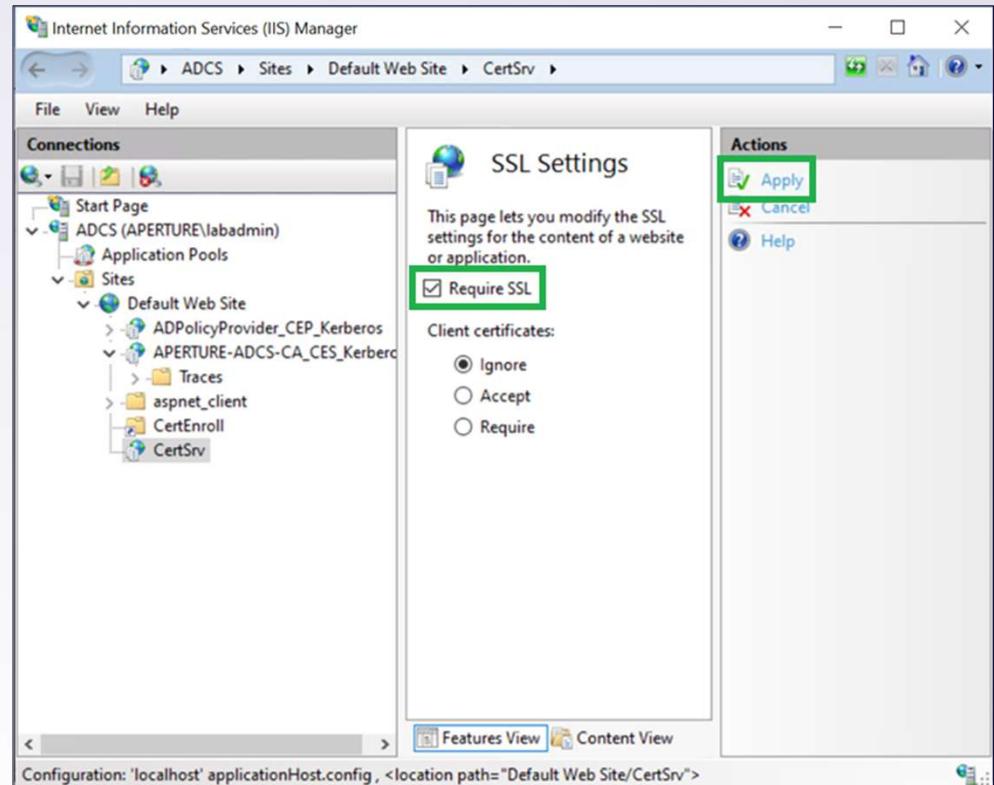


# Require EPA on AD CS

## PREVENT-14

5. Check the box next to “Require SSL”
6. Click “Apply”

If this setting is not applied, relaying to HTTP instead of HTTPS will bypass EPA



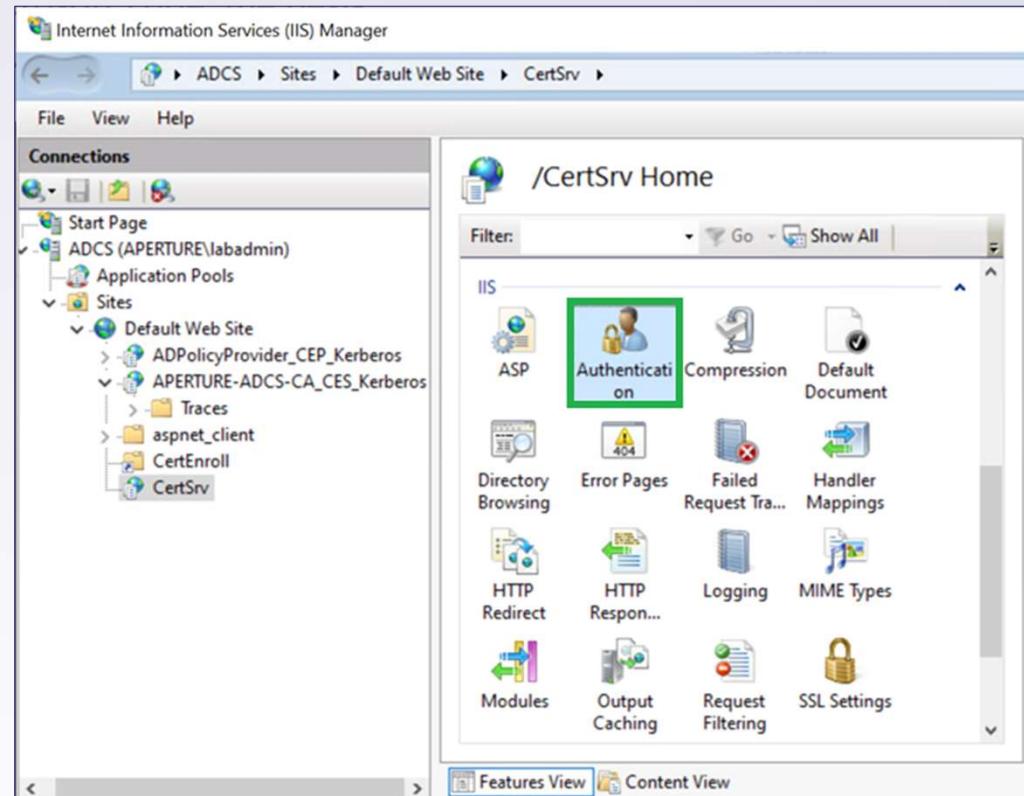
<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>



# Require EPA on AD CS

## PREVENT-14

7. Click on the “CertSrv” site again
8. Double-click “Authentication”



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

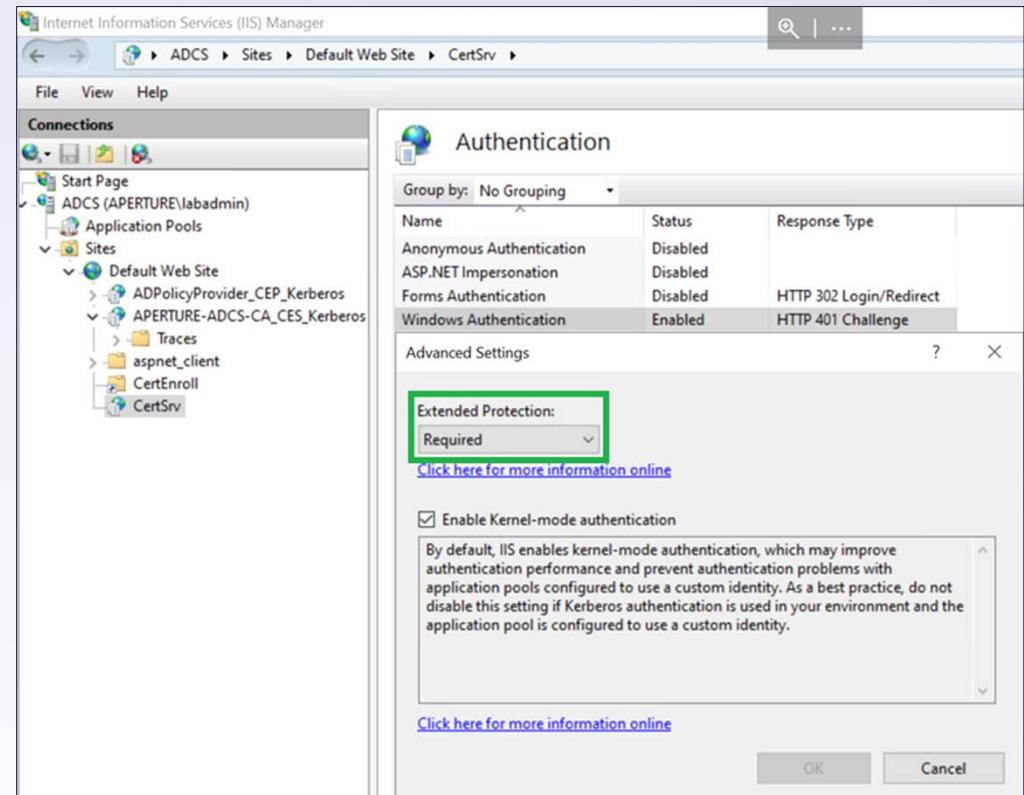


# Require EPA on AD CS

## PREVENT-14

9. Right click “Windows Authentication”
10. Click “Advanced Settings”
11. Set “Extended Protection” to “Required”
12. Click “OK”

Setting to “Accept” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding



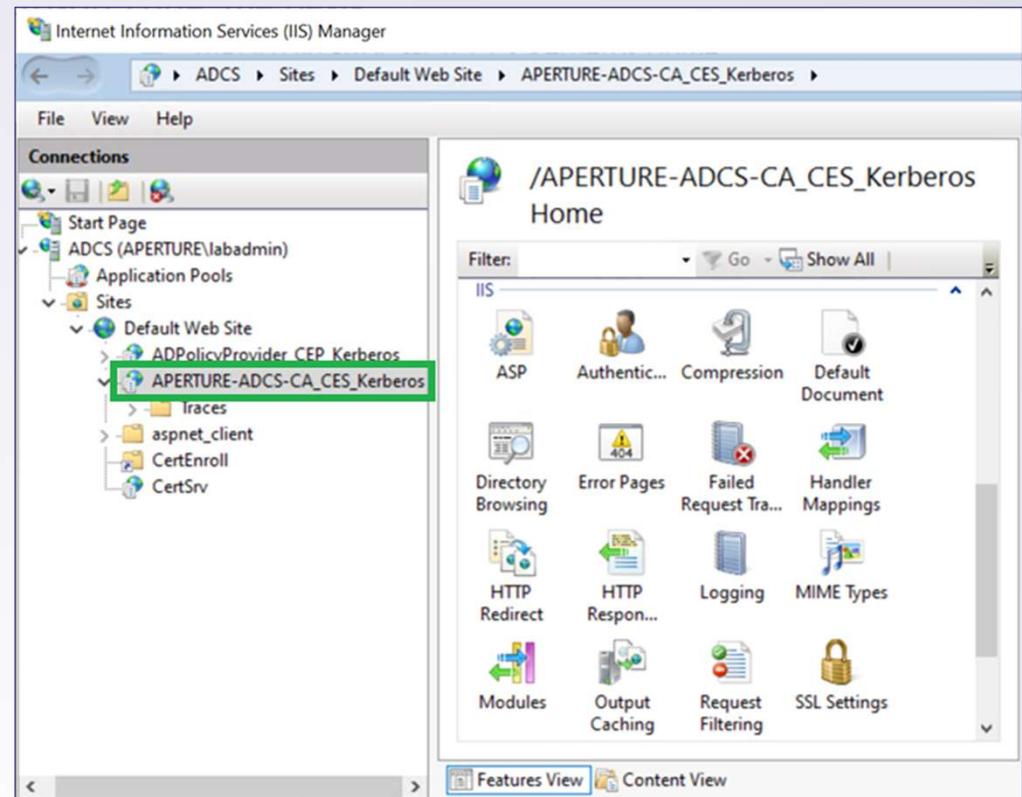
<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>



# Require EPA on AD CS

## PREVENT-14

13. Repeat steps 3-12 for the Certificate Enrollment Web Service (“APERTURE-ADCS-CA\_CES\_Kerberos” in the example)



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>



# Require EPA on AD CS

## PREVENT-14

14. Append "<%windir%>\systemdata\CES\<CA>\_CES\_Kerberos\web.config":

```
<binding name="TransportWithHeaderClientAuth">
  <security mode="Transport">
    <transport clientCredentialType="Windows">
      <extendedProtectionPolicy policyEnforcement="Always" />
    </transport>
    <message clientCredentialType="None" establishSecurityContext="false" negotiateServiceCredential="false" />
  </security>
  <readerQuotas maxStringContentLength="131072" />
</binding>
```

15. Restart the IIS service by issuing the "iisreset /restart" command



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

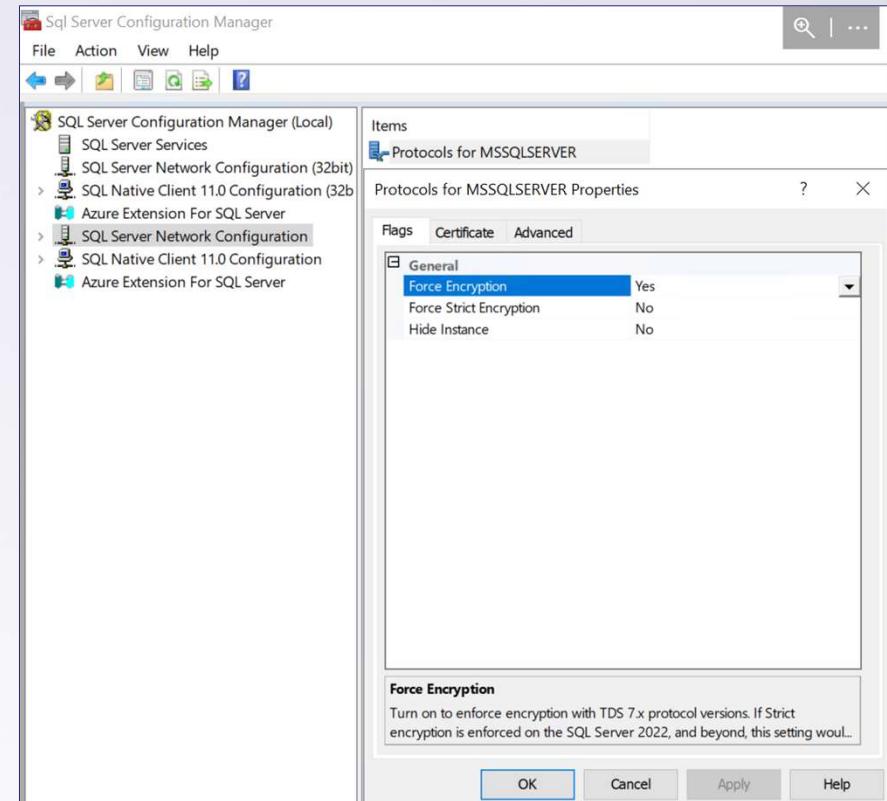
# Require EPA on site databases

## PREVENT-14

On site database servers:

1. Open Sql Server Configuration Manager
2. Click “Sql Server Network Configuration”
3. Right click “Protocols for MSSQLSERVER”, then click “Properties”
4. Set “Force Encryption” to “Yes”

If this setting is not configured, only service binding is enforced (not channel binding)



<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-ver16>

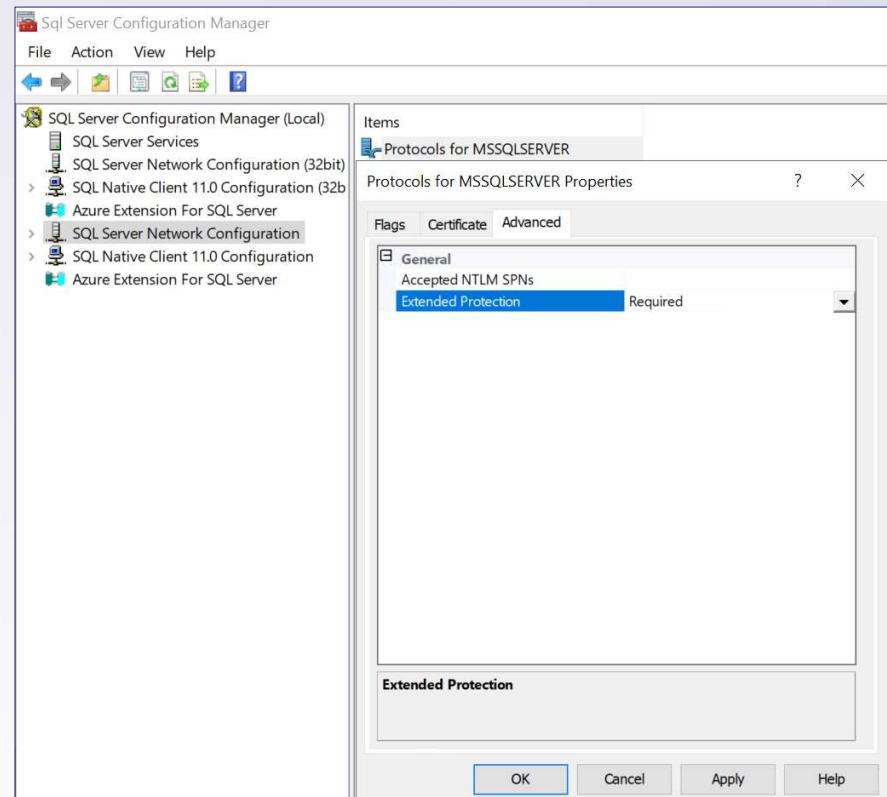


# Require EPA on site databases

## PREVENT-14

5. Navigate to the “Advanced” tab
6. Set “Extended Protection” to “Required”
7. Click “Apply”, then “OK”
8. Restart the “SQL Server (MSSQLSERVER)” service

Setting to “Allowed” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding



<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-ver16>



# Require SMB Signing on Site Systems

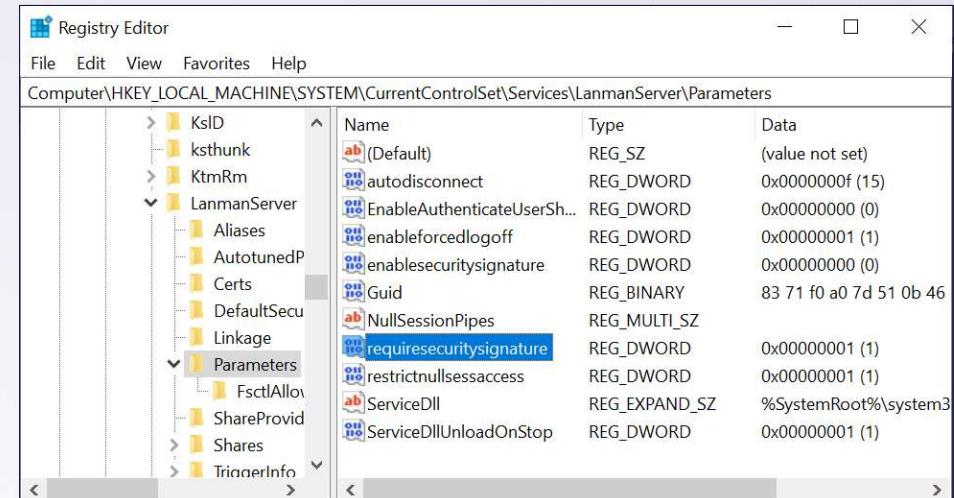
## PREVENT-12

On every site system role:

1. Open regedit
2. Navigate to  
HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\
3. Set “RequireSecuritySignature” to 1

Equivalent GPO: “Microsoft network client:  
Digitally sign communications (always)”

Configuring this setting “if client agrees” or “if server agrees” does not offer relay protection



<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing>

# Disable and Uninstall WebClient on Site Servers

## PREVENT-11

On every primary site server, central administration site server, and passive site server:

1. Open PowerShell (Administrator)
2. Execute the following command:
  - `Uninstall-WindowsFeature -Name WebDAV-Redirector`
3. At the next opportunity, restart the server to complete the change

If WebClient is installed but not running, it can potentially be triggered to start and be abused

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\labadmin.APERTURE> Get-Service WebClient
----- Running WebClient ----- WebClient

PS C:\Users\labadmin.APERTURE> Get-WindowsFeature WebDAV-Redirector
----- Display Name Name Install State -----
[X] WebDAV Redirector WebDAV-Redirector Installed

PS C:\Users\labadmin.APERTURE> Uninstall-WindowsFeature WebDAV-Redirector
----- Success Restart Needed Exit Code Feature Result -----
True Yes SuccessRest... {WebDAV Redirector}
WARNING: You must restart this server to finish the removal process.

PS C:\Users\labadmin.APERTURE> -
```



<https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-interception-defense?tabs=group-policy#disable-the-webdav-protocol>

# Block Unnecessary Connections to Site Systems

## PREVENT-20

Site servers (including primary site, central administration site, and passive site servers):

- TCP/445 (SMB) - inbound **and outbound**

Site database servers:

- TCP/445 (SMB) - inbound
- TCP/1433 (MSSQL) - inbound



<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/ports>

# Block Unnecessary Connections to Site Systems

## PREVENT-20

**There is no support for relay protection on the SMS Provider AdminService!**

It is imperative to restrict the following ports on SMS Providers (including site servers):

- TCP/443 (HTTPS) - inbound
- TCP/445 (SMB/WMI) - inbound

If necessary, move SMS Providers to a system without client-facing roles

Restricting connections to TCP/443 and TCP/445 isn't feasible when the server also hosts client-facing roles (e.g., management point, distribution point), so these ports are often open



<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/ports>

# Require LDAP Channel Binding and Signing

## PREVENT-13

1. Configure Windows clients and domain controllers to negotiate channel binding **and** signing via GPO **when supported**
2. **Monitor events** to identify clients that may not comply with signing or channel binding requirements
3. **After handling outliers**, require LDAP channel binding **and** signing

If only channel binding is required, relay to LDAP with StartTLS is possible because TLS is established after NTLM authentication is complete

If only signing is required, relay to LDAPS is possible (pre-Windows Server 2025) because TLS traffic is signed



# Client Push Installation

## Overview

- Deploys the client software remotely from the site server
- Copies files to the ADMIN\$ share and executes the installer
- Uses configured credentials and the **site server's domain computer account**, which must be a **local admin** to install the client software
- Can be initiated manually or automatically when new devices are discovered (e.g., in a certain domain/subnet)



<https://medium.com/specter-ops-posts/coercing-ntlm-authentication-from-sccm-e6e23ea8260a>

# Automatic Site-wide Client Push Installation Abuse

## ELEVATE-2

- Attackers can register a fake device record in SCCM by sending requests to a management point
- This will **cause the site server to authenticate to an arbitrary IP address specified for the fake device**
- Incoming NTLM authentication can be **cracked or relayed** to other workstations or SCCM servers (where the site server has admin privileges by default)



<https://medium.com/specter-ops-posts/coercing-ntlm-authentication-from-sccm-e6e23ea8260a>

# ELEVATE-2 Prevention

## Disable Automatic Client Push Installation and Fallback to NTLM

Technique	Codename
Disable automatic site-wide client push installation	PREVENT-3
Patch site server with KB15599094	PREVENT-1
Disable Fallback to NTLM	PREVENT-2
Require PKI certificates for client authentication	PREVENT-8

None of these prevent Kerberos relay if an SCCM admin initiates a manual client push installation

**Use another method of client installation instead of client push installation.** Choose an option that "pulls" the client installer from a server hosting the files instead of using a privileged account to "push" the client installer to the device, for example software update or GPO-based installation.



[https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/\\_defense-techniques-list.md](https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/_defense-techniques-list.md)

# Other Potential Solutions to Prevent TAKEOVER

**Don't try this at home!... or do, and tell us what happened**

Microsoft hasn't provided an official response supporting any of these ideas:

- Add all site servers to the “Protected Users” group
  - Prevents site servers from using NTLM for authentication
- Restrict outbound NTLM from site servers to only necessary systems
- Restrict inbound NTLM to site databases and SMS Providers to only necessary systems

**These solutions do not prevent Kerberos relay**

To their credit, Microsoft did add official support for EPA to the site database, so hopefully we'll make progress on these as well!



# CRED Attacks



# Machine Policy Secrets

Downloaded from Management Points

- Network Access Accounts (NAA)
  - Domain accounts used by systems that are not joined to AD to download content from software distribution points
- Task Sequences
  - Step-by-step instructions executed by clients, often for operating system deployment or complicated software installations/setup
- Collection Variables
  - Environment variables defined for a device collection to access



<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts>

# Machine Policy Secrets

## Downloaded from Management Points

- May contain obfuscated domain join credentials, local admin credentials, RunAs credentials
- Can be requested from a management point and deobfuscated
- Credentials are stored on clients as DPAPI blobs protected by the system's masterkey
- Retrievable via WMI as a privileged user
- Remain in CIM repository after client is uninstalled or account rotation
  - C:\Windows\System32\Wbem\Repository\OBJECTS.DATA



<https://subat0mik.medium.com/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9>

sphere1

alms2408-desktop.specterops.training/#/client/MTQAYwBwb3N0Z3Jlc3Fs

Applications Terminal - testsubject1...

Terminal - testsubject1@sphere1: ~/tools/pxethiefy

File Edit View Terminal Tabs Help

```
testsubject1@sphere1:~/tools/pxethiefy$ sudo python3 ~/tools/pxethiefy/pxethiefy.py
```

CLIENT - Remote Desktop

Administrator: Windows Pow! x + | v

PS C:\Users\labadmin.APERTURE\Desktop> .\SharpSCCM.exe local secrets -m wmi

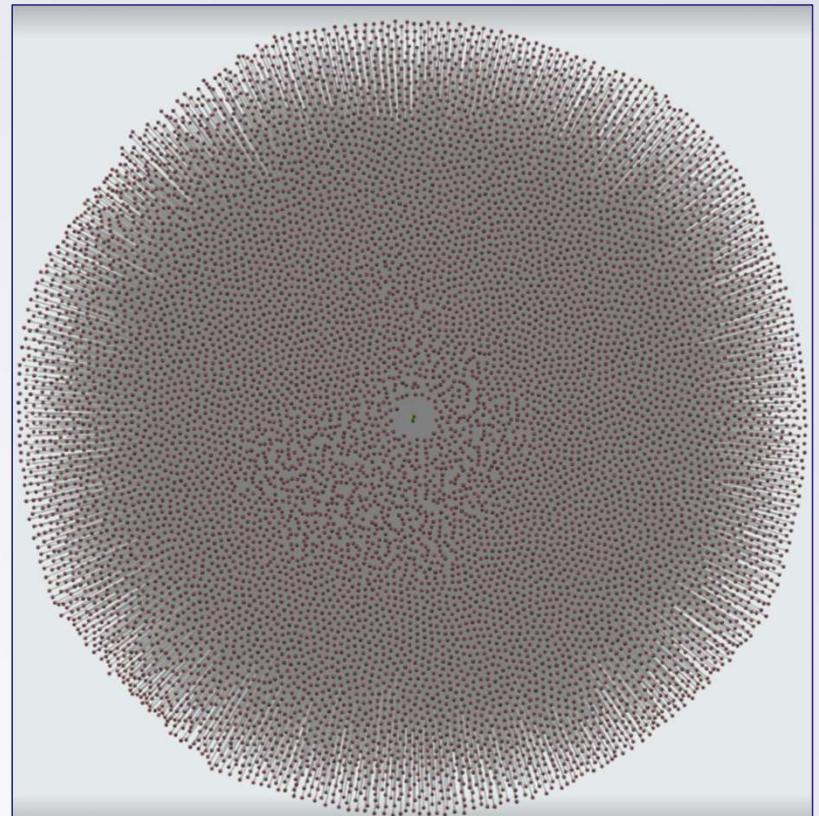
10:29 PM  
6/11/2024

# Real World Examples

## Overprivileged Policy Secrets

- Domain join account in PXE boot task sequence Owns all computers in the domain
- Remember to change ownership and remove rights assignments from accounts that do not require them

Creds in PXE boot task sequences can be retrieved remotely if there is no PXE password or a weak one



[https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/PREVENT/PREVENT-17/prevent-17\\_description.md](https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/PREVENT/PREVENT-17/prevent-17_description.md)

# CRED Prevention

## Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 and PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

\*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

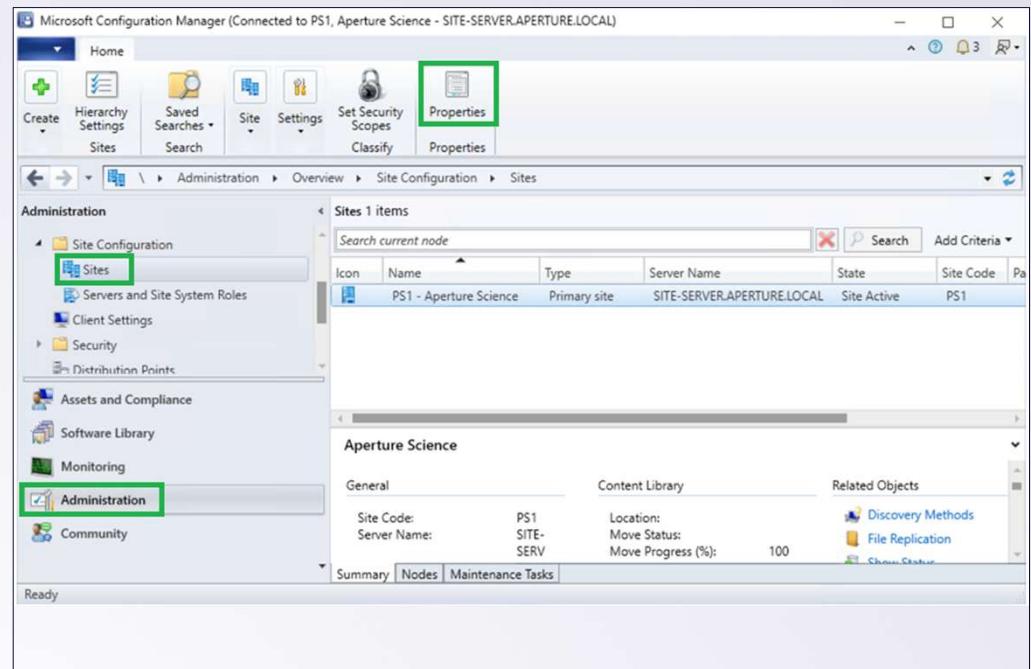
\*\*If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares



# Configure Enhanced HTTP

## PREVENT-4

1. Open the Configuration Manager Console
2. Navigate to Administration > Site Configuration > Sites, then click the site
3. Click “Properties”



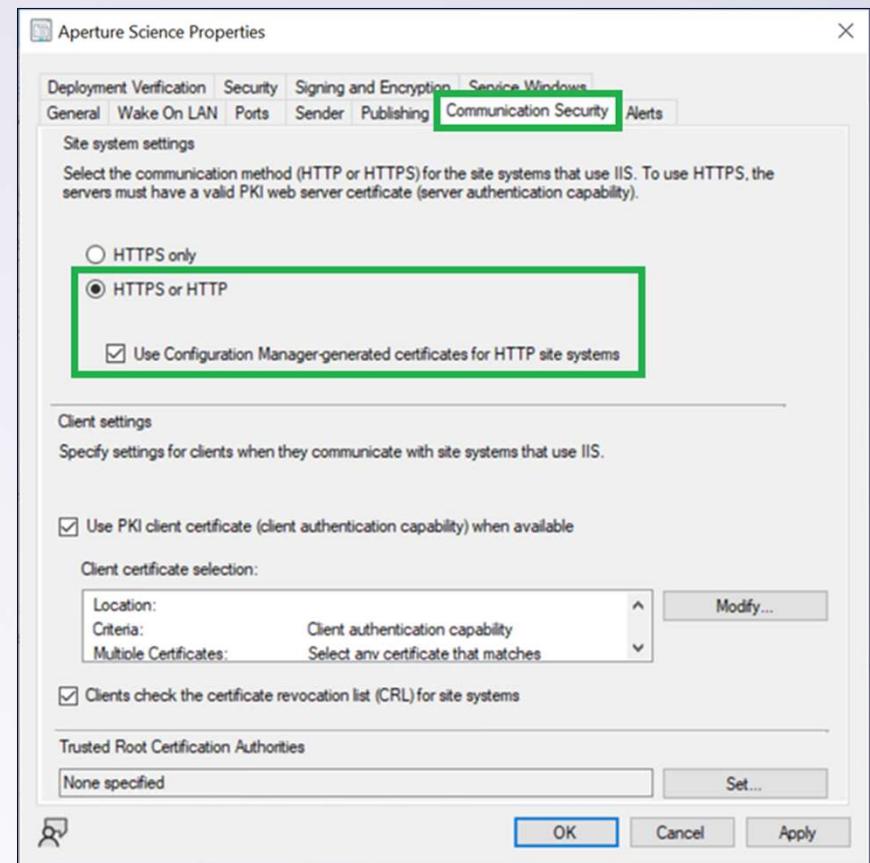
<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/enhanced-http>

# Configure Enhanced HTTP

## PREVENT-4

4. Click the “Communication Security” tab
5. Select “HTTPS or (E)HTTP”
6. Check the box next to “Use Configuration Manager-generated certificates for HTTP site systems”
7. Click “Apply”, then “OK”

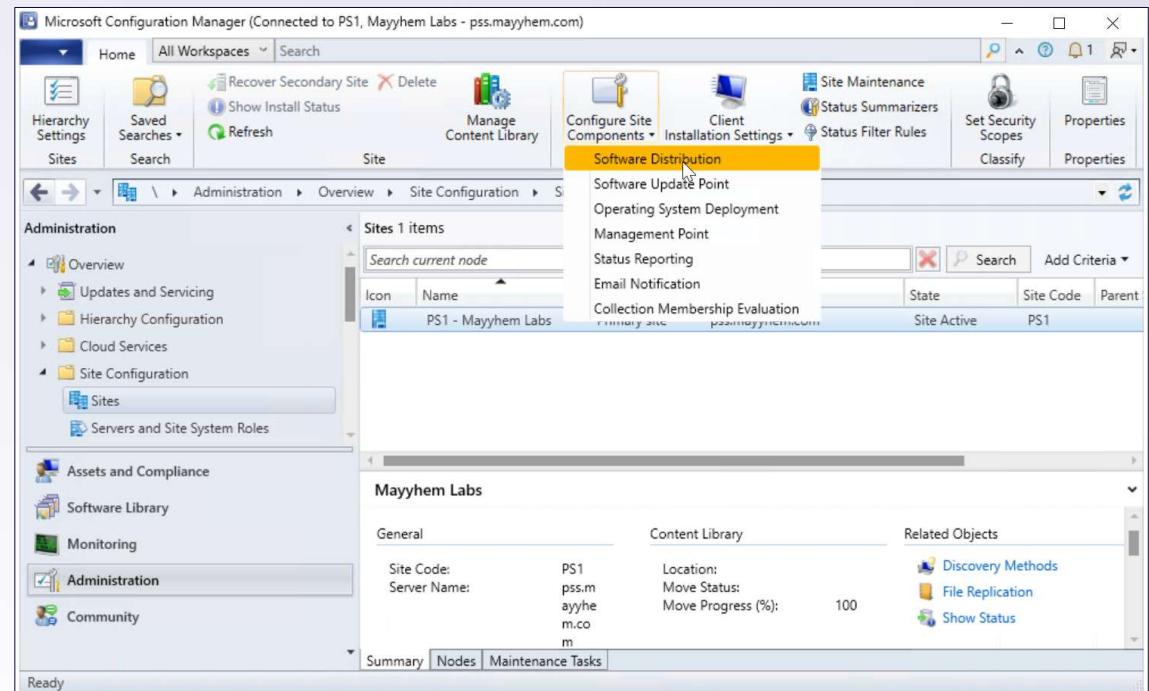
Enhanced HTTP does not prevent registration of fake device records to download machine policy secrets or coerce automatic client push



# Disable Network Access Accounts

## PREVENT-3

1. Open the Configuration Manager Console
2. Navigate to Administration > Site Configuration > Sites, then click the site
3. Click “Configure Site Components”, then “Software Distribution”

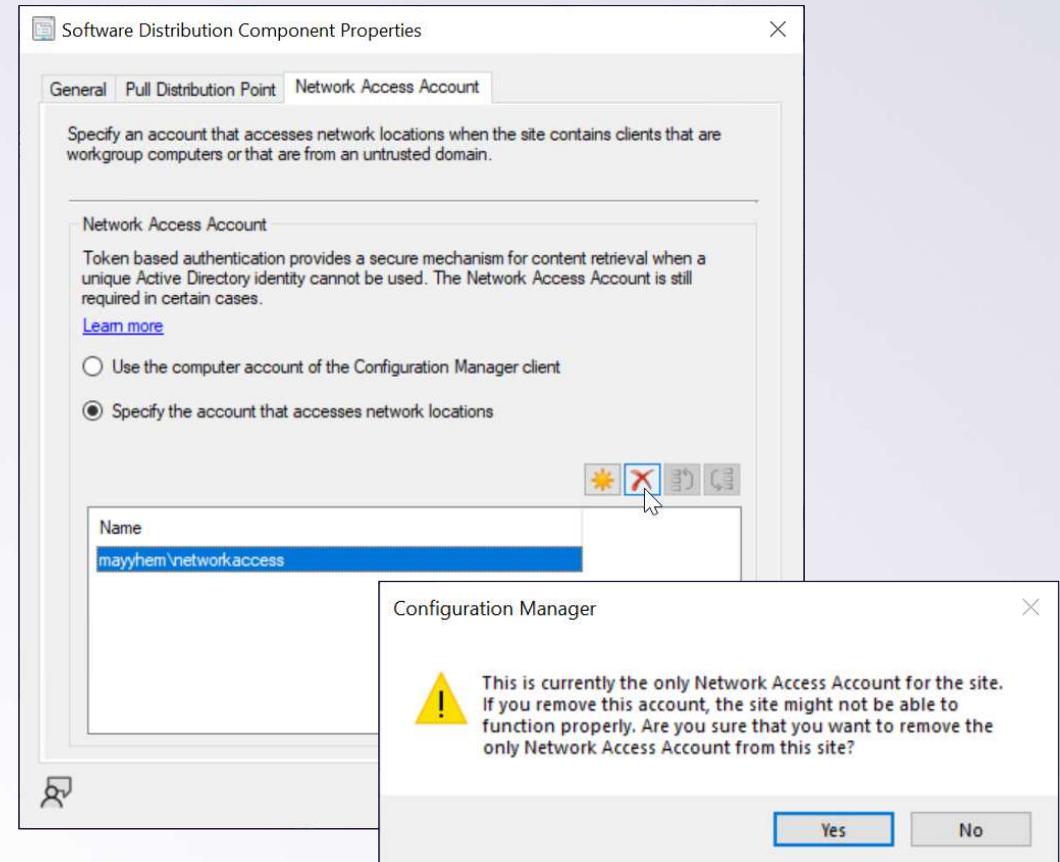


<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

# Disable Network Access Accounts

## PREVENT-3

4. Click the “Network Access Account” tab
5. Select each account and click the big red X
6. When prompted to delete the only NAA, say “Yes”
7. Click “Apply”, then “OK”



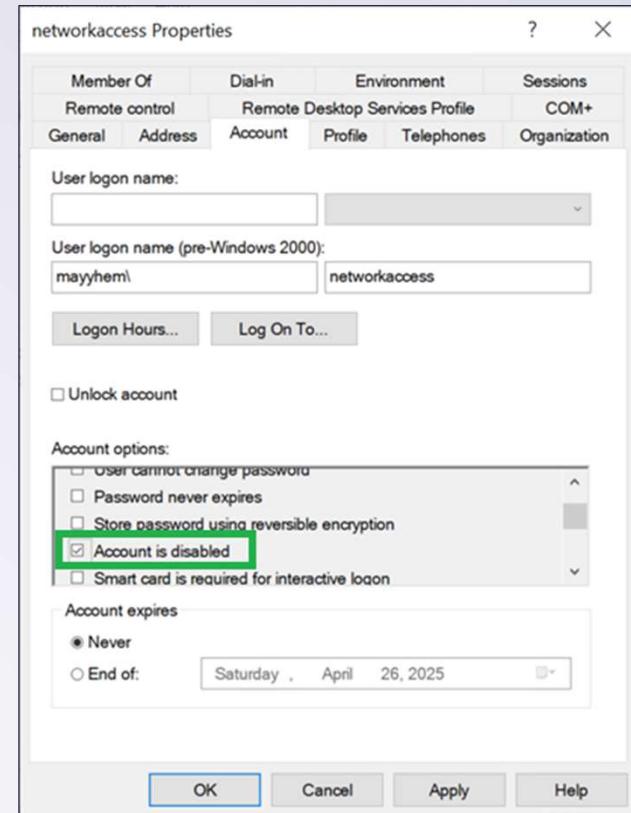
<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>



# Disable Network Access Accounts

## PREVENT-15

8. Open Active Directory Users and Computers
9. Open the “Properties” window for each NAA
10. Click the “Account” tab, check the box next to “Account is disabled”
11. Click “Apply”, then “OK”
12. Rejoice

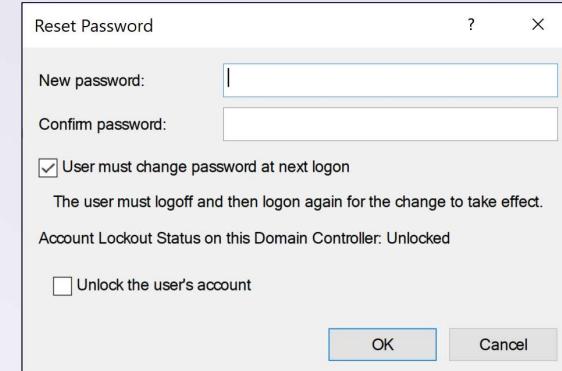


<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

# Disable Network Access Accounts

## PREVENT-15

- Alternatively, rotate the password after removing the NAA from SCCM by selecting “Reset Password” in ADUC **and revoke any issued certificates in Certification Authority.**
- If the NAA is removed from SCCM but not disabled or the password rotated, the WMI repository on client devices will still contain valid credentials.
- If those credentials were at any point used to request a certificate that is still valid, that certificate can still be used for authentication and to get the account’s TGT and NT hash **even after the password has been rotated.**

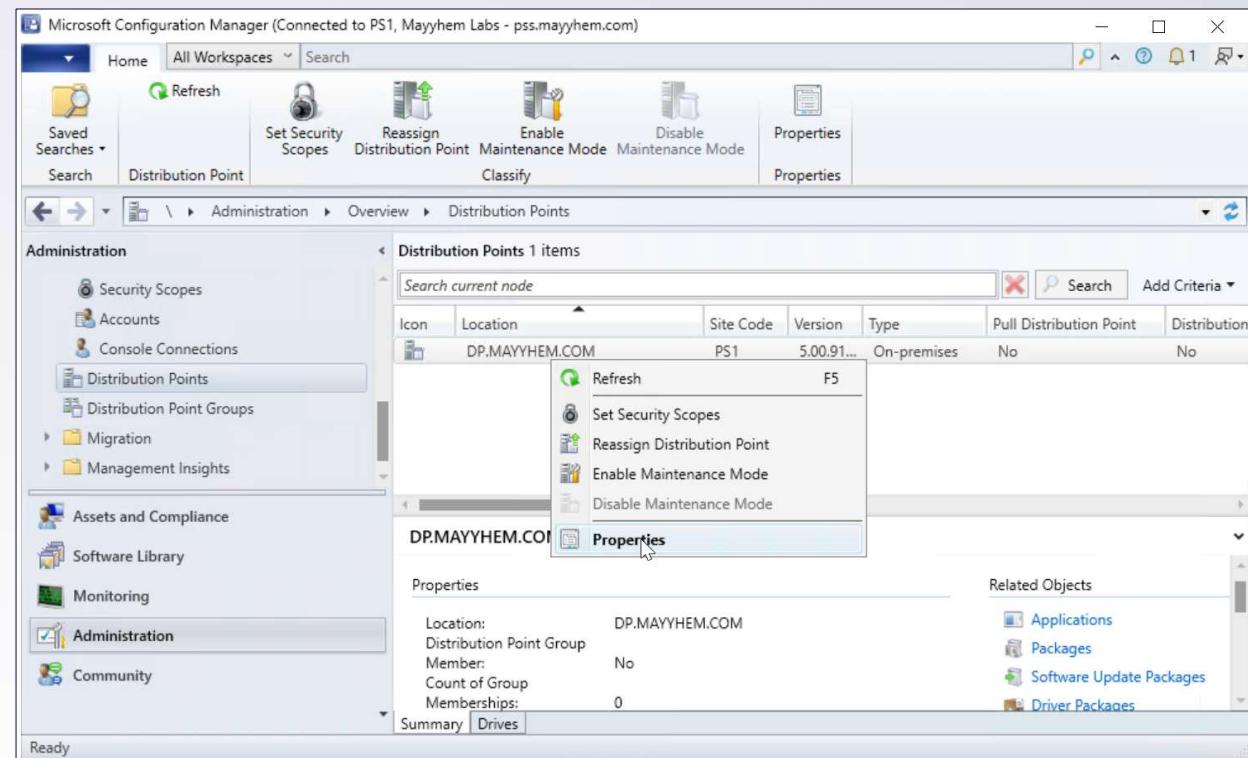


<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

# Configure a Strong PXE Boot Password

## PREVENT-6

1. Open the Configuration Manager Console
2. Navigate to Administration > Distribution Points
3. Right click on each distribution point and select “Properties”



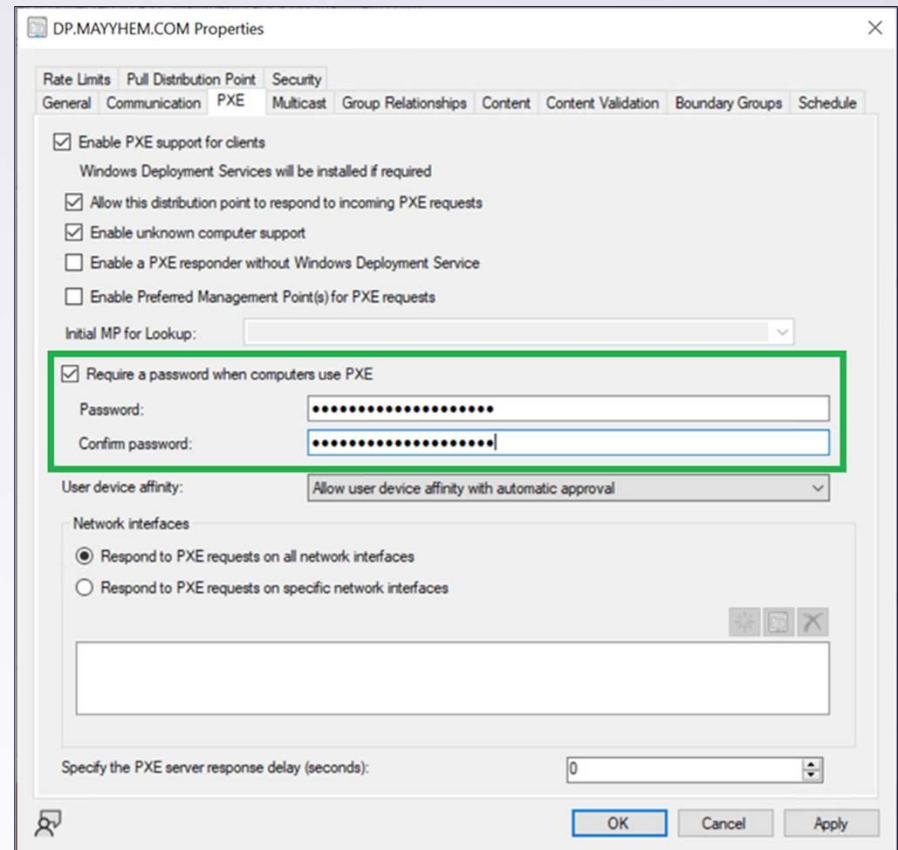
[https://www.mwrcybersec.com/research\\_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences](https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences)

# Configure a Strong PXE Boot Password

## PREVENT-6

4. Click on the “PXE” tab
5. Check the box next to “Require a password when computers use PXE”
6. Enter a strong passphrase
7. Click “Apply”, then “OK”

If an **uncrackable** password is not set, task sequences that may contain creds (and the distribution point's cert, if using PKI) can still be dumped remotely



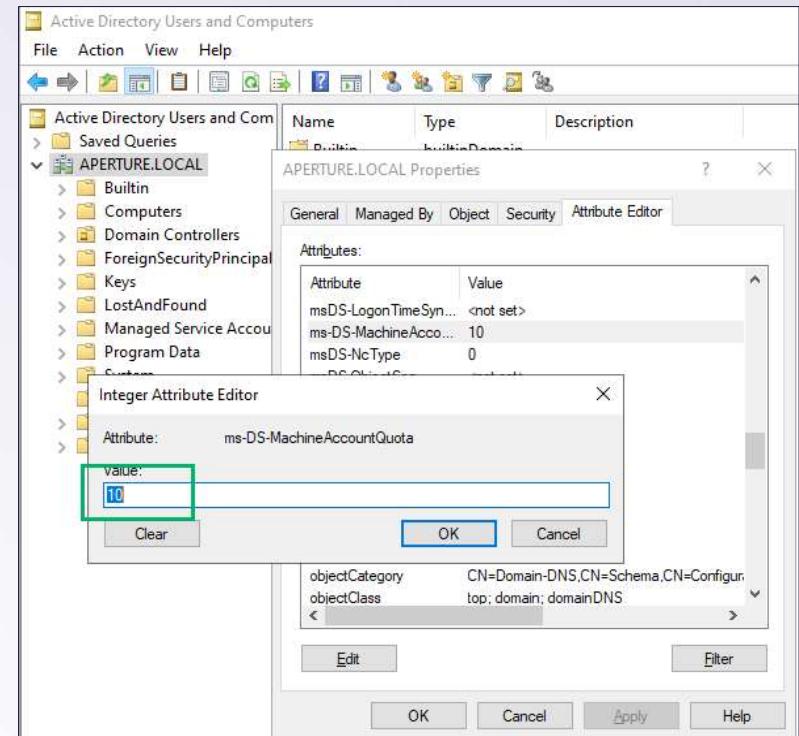
[https://www.mwrcybersec.com/research\\_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences](https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences)



# Restrict Permission to Join Machines to AD

## PREVENT-16: Machine Account Quota

1. Open ADUC on a DC
2. Right click the domain object and select "Properties"
3. Select the "Attribute Editor" tab
4. Find the "ms-DS-MachineAccountQuota" attribute
5. Set the attribute to 0



<https://learn.microsoft.com/en-us/windows/win32/adschema/a-ms-ds-machineaccountquota>

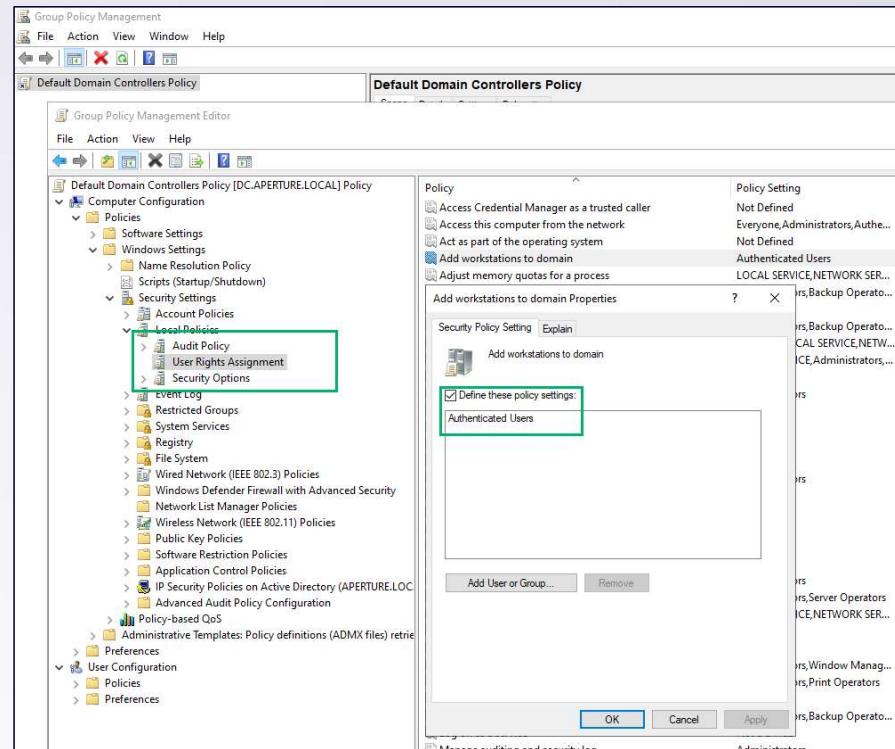


# Restrict Permission to Join Machines to AD

## PREVENT-16: User Rights Assignment

1. Open Group Policy Management
2. Right click “Default Domain Controllers Policy” and select “Edit”
3. Navigate to "User Rights Assignment"
4. Right click "Add workstations to domain" and select "Edit"
5. Remove "Authenticated Users", then click "Apply" and "OK"

Attackers can still impersonate a client device to fetch secret policies from a management point with local admin on any domain-joined computer



<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/add-workstations-to-domain>



# Wrapping It Up

## What should I look at next?

- Misconfiguration Manager repo →
  - **Slides for this talk**
  - MisconfigurationManager.ps1 PowerShell script
  - DETECT and CANARY techniques
  - RESOURCES.md
- New NTLM relay edges in BloodHound
- Josh Prager's detection guidance SO-CON talk,  
**“Detecting Configuration Manager Attack Paths”**
- #sccm channel in BloodHound Slack →  
(<https://ghst.ly/BHSlack>)



<https://misconfigurationmanager.com>





# Thank you!

Any questions?

Chris Thompson (@\_Mayyhem)

Garrett Foster (@unsigned\_sh0rt)

