



BlueFolder.zip

Defensive insights within a compressed format

Responding to Responder Guide 0001

Guide to defend against real world offensive tools of the trade.



CONTENTS

Introduction to Responder	3
Origins and Development	3
Purpose and Functionality	3
Underlying Protocols Targeted	3
Current Maintenance and Evolution	3
Key Developments Over Time	4
Ongoing Relevance	4
Intune Policy Mitigations for Defending Against Responder Attacks	5
Link-Local Multicast Name Resolution (LLMNR).....	5
Context.....	5
Implication.....	5
Solution	5
Impact	6
Technical control/s.....	6
Multicast Domain Name System (mDNS)	7
Context.....	7
Implication.....	7
Solution	7
Impact	7
Technical control/s.....	8
NetBIOS Name Service (NETBios NS)	9
Context.....	9
Implication.....	9
Solution	9
Impact	9
Technical control/s.....	10
Web Proxy Auto-Discovery Protocol (WPAD)	11
Context.....	11
Implication.....	11
Solution	11
Impact	11
Technical control/s.....	12
Additional measures - Intune Policy Mitigations for Defending Against Responder Attacks.....	13
1. Protocol and Name Resolution Hardening	13
2. Authentication and Credential Protection	15



3.Attack Surface Reduction Rule.....	16
Document Credit, Responsible Use & Statement of Legal Intent.....	17

DISCLAIMER

Any actions, configurations, or deployments undertaken based on the information provided in this document are solely the responsibility of the recipient. Jordan Albaladejo and any affiliated entity disclaim all liability for any outcomes resulting from the use or implementation of these solutions.

IT environments vary significantly, and each requires careful customization and a thorough understanding of potential impacts. Before applying any guidance or deploying solutions described herein, it is essential to:

- Assess your organisation's specific requirements and operational context.
- Validate compatibility with existing infrastructure and policies.
- Conduct appropriate testing in a controlled environment prior to production implementation.

By using this document, you acknowledge that all decisions and actions taken are at your own discretion and risk.



RESPONDER: ORIGINS, DEVELOPMENT, AND ONGOING SIGNIFICANCE

INTRODUCTION TO RESPONDER

Responder is an offensive security tool widely used by penetration testers and red teams to uncover and exploit vulnerabilities in network authentication protocols. Through its ability to simulate attacks on name resolution and credential exchange mechanisms, Responder provides practical demonstrations of real-world weaknesses found in both modern and legacy network environments.

ORIGINS AND DEVELOPMENT

The tool was first developed in 2013 by Laurent Gaffié, a French security researcher. Gaffié designed Responder to be a pragmatic solution for exposing authentication flaws, making evident how attackers can intercept and misuse network traffic with relative ease.

PURPOSE AND FUNCTIONALITY

Responder was specifically created to poison network traffic and capture authentication credentials by exploiting the way operating systems process name resolution and authentication requests. It has become a mainstay in penetration testing, particularly valuable for assessing enterprise networks that rely on legacy protocols. The tool helps security professionals evaluate the security posture of their environments and identify potential weaknesses.

UNDERLYING PROTOCOLS TARGETED

Responder exploits several core protocols commonly found in network environments:

- LLMNR (Link-Local Multicast Name Resolution): Used by operating systems for local name resolution when DNS is unavailable, allowing devices to query their neighbours for hostname resolution.
- NBT-NS (NetBIOS Name Service): A legacy protocol used primarily in older Windows networks for name and service resolution, often related to file and printer sharing.
- mDNS (Multicast DNS): Enables device discovery and local hostname resolution via multicast, commonly used with Apple devices and Internet of Things (IoT) equipment.
- NTLMv1/NTLMv2 (NT LAN Manager): Authentication protocols for Windows systems that remain prevalent; Responder leverages these protocols to relay captured credentials, exploiting the challenge-response authentication mechanism.

CURRENT MAINTENANCE AND EVOLUTION

Responder is now maintained by Alessandro Zannoli, also known as lgandx (GitHub username). Under Zannoli's stewardship, the tool has been modernised and its feature set expanded, ensuring it remains effective against evolving protocols and threats.



KEY DEVELOPMENTS OVER TIME

Since its initial release, Responder has undergone significant enhancements, including:

- Support for both IPv4 and IPv6, allowing operation in dual-stack networks.
- Improved poisoning modules for LLMNR, NBT-NS, and mDNS, providing greater flexibility and stealth in attacks.
- Advanced NTLMv1/2 relay capabilities, enabling real-time exploitation of captured credentials.
- Refined configuration settings, better logging functionality, and expanded compatibility for complex enterprise environments.

These updates have transformed Responder into a comprehensive toolkit for addressing security challenges in both contemporary and legacy networks.

ONGOING RELEVANCE

Responder remains a fundamental resource for security professionals. Its continued importance is rooted in its ability to reveal misconfigurations and insecure defaults that persist in many operating systems and networks. By exposing vulnerabilities that might otherwise go unnoticed, Responder empowers defenders to proactively remediate risks, helping to protect organisations before real-world attackers can exploit these weaknesses.

However, the question becomes, how do we defend against such tools and the potential for mal actors exploiting enterprise systems. In the following sections, this guide will provide detailed, Intune configurations that can be applied to Windows devices. These recommendations aim to mitigate vulnerabilities and address potential misconfigurations, helping IT teams bolster their security posture.



INTUNE POLICY MITIGATIONS FOR DEFENDING AGAINST RESPONDER ATTACKS

Microsoft Intune provides a powerful platform for IT administrators to implement security controls across managed devices, significantly reducing vulnerabilities to Responder attack techniques within modern enterprise environments. The following strategies outline how Intune's mobile device management (MDM) and endpoint security capabilities can be leveraged to harden name resolution mechanisms and strengthen credential protections.

LINK-LOCAL MULTICAST NAME RESOLUTION (LLMNR)

CONTEXT

Link-Local Multicast Name Resolution (LLMNR) is a protocol used in Windows networks that allows devices on the same local network segment to resolve each other's names without the need for a DNS server. When a device tries to resolve a hostname and DNS fails, it uses LLMNR to broadcast a query to other devices on the local subnet, asking if any of them know the IP address for that name. While LLMNR can be convenient in small or ad-hoc networks, it also introduces security risks, as attackers can respond to these broadcasts with malicious intent, potentially capturing sensitive credentials or redirecting traffic.

IMPLICATION

A critical implication of leaving LLMNR enabled is that it allows attackers equipped with tools like Responder to intercept these unauthenticated broadcasts and impersonate legitimate hosts. When a device receives a reply from a malicious actor, it may attempt to authenticate or exchange credentials, inadvertently exposing password hashes and other sensitive information. This can facilitate credential theft, privilege escalation, and lateral movement across the network. The threat is heightened in environments where DNS reliability is low or users frequently mistype hostnames, as these conditions trigger LLMNR more often, increasing the attack surface. For these reasons, proactively mitigating LLMNR via Intune policies is essential to prevent attackers from exploiting this vulnerability and to reinforce your organisation's overall security posture.

SOLUTION

Disabling LLMNR by applying the 'Turn off multicast name resolution' setting in Intune can significantly reduce the risk of credential theft and network poisoning attacks within your organisation. By preventing devices from broadcasting name resolution queries over the local network, attackers are unable to intercept or spoof responses, thereby safeguarding sensitive information and limiting opportunities for lateral movement. This action also helps ensure that all name resolution relies on more secure, centrally managed DNS infrastructure, promoting a stronger overall security posture.

In addition to this, it is recommended to enable the 'Turn off smart multi-homed name resolution' setting. This further strengthens your organisation's defences by disabling the feature that allows Windows to send out DNS queries across all available network interfaces. By doing so, you reduce the risk of information leakage and prevent attackers from exploiting alternative network paths to intercept or manipulate name resolution traffic. Together, these controls provide a comprehensive approach to minimising exposure to Responder attacks and enhancing network security.



IMPACT

Disabling LLMNR may impact connectivity in environments where DNS is unavailable or unreliable, as devices will no longer be able to resolve local hostnames via LLMNR broadcasts. Organisations should ensure robust DNS availability and educate users about proper hostname usage to mitigate any potential disruption.

TECHNICAL CONTROL/S

Control	Action Location	Setting Location and State
Turn off multicast name resolution = Enabled	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\DNS Client Turn off multicast name resolution = Enabled
Turn off smart multi-homed name resolution = Enabled	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\DNS Client Turn off smart multi-homed name resolution = Enabled



MULTICAST DOMAIN NAME SYSTEM (mDNS)

CONTEXT

Multicast Domain Name System (mDNS) is a protocol utilised in Windows networks that enables devices within the same local network segment to resolve each other's names without relying on a central DNS server. When a device attempts to resolve a hostname and DNS is unavailable, it leverages mDNS to broadcast a query across the local subnet, seeking a response from any device that knows the IP address for that name. While mDNS can be handy in smaller or temporary networks, it does present security vulnerabilities, as malicious actors can intercept these broadcasts and reply with deceptive information, potentially capturing sensitive data or redirecting network traffic.

IMPLICATION

A critical implication of leaving mDNS enabled is that it allows attackers equipped with tools like Responder to intercept these unauthenticated broadcasts and impersonate legitimate hosts. When a device receives a reply from a malicious actor, it may attempt to authenticate or exchange credentials, inadvertently exposing password hashes and other sensitive information. This can facilitate credential theft, privilege escalation, and lateral movement across the network. The threat is heightened in environments where DNS reliability is low or users frequently mistype hostnames, as these conditions trigger mDNS more often, increasing the attack surface. For these reasons, proactively mitigating mDNS via Intune policies is essential to prevent attackers from exploiting this vulnerability and to reinforce your organisation's overall security posture.

SOLUTION

By employing a platform script at user login, organisations can consistently enforce the control against unauthorised multicast name resolution broadcasts, regardless of manual user changes or inconsistent device configurations. This measure significantly reduces the risk of credential theft and network poisoning, as it prevents mDNS queries from being broadcast and intercepted by potential attackers. Further, this approach complements other security controls by ensuring all network name resolutions are channelled through trusted, centrally managed DNS services.

IMPACT

Disabling mDNS may impact connectivity in environments where DNS is unavailable or unreliable, as devices will no longer be able to resolve local hostnames via mDNS broadcasts. Organisations should ensure robust DNS availability and educate users about proper hostname usage to mitigate any potential disruption.



TECHNICAL CONTROL/S**Action Location:**

Scripts and remediations → Platform scripts

RAW script to disable mDNS using PowerShell:

```
$regPath = "HKLM:\SOFTWARE\ Policies\Microsoft\Windows NT\DNSClient"

$regName = "EnableMDNS"

$regValue = 0

# Ensure the registry path exists

if (-not (Test-Path $regPath)) {

    New-Item -Path $regPath -Force | Out-Null

}

# Check and create or update the registry value

$currentValue = Get-ItemProperty -Path $regPath -Name $regName -ErrorAction

SilentlyContinue

if ($null -eq $currentValue) {

    New-ItemProperty -Path $regPath -Name $regName -Value $regValue -PropertyType DWORD -Force | Out-Null

} elseif ($currentTime.$regName -ne $regValue) {

    Set-ItemProperty -Path $regPath -Name $regName -Value $regValue

}
```



NETBIOS NAME SERVICE (NETBIOS NS)

CONTEXT

NetBIOS Name Service (NetBIOS-NS) is a legacy protocol used in Windows networks to enable devices on the same local network segment to resolve NetBIOS names to IP addresses. When a device tries to locate another using a NetBIOS name, it sends a broadcast query over the network, asking if any device can respond with the relevant IP address. While this functionality was essential in older or mixed environments lacking centralised name resolution, it now poses significant security risks. Attackers can exploit these broadcasts, responding with malicious information to impersonate hosts, intercept credentials, or redirect network traffic.

IMPLICATION

Leaving NetBIOS-NS enabled exposes networks to attacks such as NetBIOS Name Poisoning, where adversaries use tools like Responder to reply to broadcast queries with spoofed responses. When a device receives a reply from an attacker, it may attempt to authenticate or exchange sensitive information, inadvertently disclosing password hashes or other credentials. This can lead to credential theft, privilege escalation, and lateral movement within the network. The risk is heightened in environments where DNS is unreliable or users frequently enter incorrect hostnames, as these conditions trigger NetBIOS-NS broadcasts more often and widen the attack surface. Therefore, mitigating NetBIOS-NS through Intune policies and platform scripts is crucial for preventing exploitation and strengthening your organisation's security posture.

SOLUTION

Disabling NetBIOS-NS by configuring the appropriate group policy settings and applying a platform script through Intune significantly reduces the risk of credential interception and poisoning attacks. By preventing devices from broadcasting NetBIOS name queries, attackers lose the opportunity to intercept or spoof responses, thereby protecting sensitive credentials and blocking lateral movement. This also ensures that name resolution relies on secure, centrally managed DNS infrastructure, supporting a robust security strategy.

IMPACT

Disabling NetBIOS-NS may affect connectivity in environments where legacy applications or systems rely on NetBIOS name resolution. Organisations should ensure all critical applications support DNS and educate users about best practices for accessing network resources. Maintaining a reliable DNS infrastructure minimises any potential disruption resulting from this hardening step.



TECHNICAL CONTROL/S**Action Location:**

Scripts and remediations → Platform scripts

RAW script to disable NetBIOS NS using PowerShell:

```
$regPath = "HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces"

$regName = "NetbiosOptions"

$regValue = 2

# Loop through all interface subkeys under NetBT Parameters

Get-ChildItem -Path $regPath | ForEach-Object {

    $interfaceKey = $_.PSPATH

    $currentValue = Get-ItemProperty -Path $interfaceKey -Name $regName -ErrorAction
    SilentlyContinue

    if ($null -eq $currentValue) {

        New-ItemProperty -Path $interfaceKey -Name $regName -Value $regValue -PropertyType
        DWORD -Force | Out-Null

    } elseif ($currentValue.$regName -ne $regValue) {

        Set-ItemProperty -Path $interfaceKey -Name $regName -Value $regValue

    }

}
```



WEB PROXY AUTO-DISCOVERY PROTOCOL (WPAD)

CONTEXT

WPAD is a protocol designed to help devices on a network automatically discover the appropriate web proxy configuration without user intervention. When a device connects to a network, it attempts to locate a WPAD configuration file, usually via DHCP or DNS queries, which instructs the system on how to route web traffic through a proxy server. While WPAD was valuable for managing proxy settings in large or dynamic environments, it introduces significant security vulnerabilities. Attackers can exploit WPAD by setting up rogue proxy servers or responding to configuration requests with malicious settings, potentially intercepting or redirecting web traffic.

IMPLICATION

Leaving WPAD enabled exposes networks to attacks such as WPAD hijacking, where adversaries respond to WPAD discovery requests with malicious proxy configuration files. If a device accepts a rogue WPAD file, all its web traffic may be transparently routed through an attacker-controlled proxy. This can result in credential theft, data interception, malware injection, and loss of privacy. The risk is especially high in environments where DNS or DHCP is not tightly controlled, as attackers can easily spoof WPAD records or respond to requests. Therefore, disabling WPAD through Intune policies and platform scripts is essential for reducing exposure and securing organisational web traffic.

SOLUTION

Disabling WPAD by configuring the correct group policy settings and deploying a platform script via Intune significantly reduces the risk of proxy-based attacks. By preventing devices from automatically discovering and trusting WPAD configuration files, attackers lose the opportunity to redirect or intercept web traffic. This ensures browsing activity remains confidential and under the control of trusted network infrastructure, reinforcing a strong security posture.

IMPACT

Disabling WPAD may affect connectivity in networks that rely on automatic proxy configuration for internet access. Organisations should confirm that all critical applications and systems are explicitly configured with the necessary proxy settings, and provide guidance to users on accessing web resources securely. Ensuring a robust and well-documented proxy configuration process will minimise any potential disruptions caused by this hardening measure.



TECHNICAL CONTROL/S**Action Location:**

Scripts and remediations → Platform scripts

RAW script to disable WPAD using PowerShell:

```
$regPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp"

$regName = "DisableWpad"

$regValue = 1

# Ensure the registry path exists

if (-not (Test-Path $regPath)) {

    New-Item -Path $regPath -Force | Out-Null

}

# Check and create or update the registry value

$currentValue = Get-ItemProperty -Path $regPath -Name $regName -ErrorAction

SilentlyContinue

if ($null -eq $currentValue) {

    New-ItemProperty -Path $regPath -Name $regName -Value $regValue -PropertyType DWORD -Force | Out-Null

} elseif ($currentValue.$regName -ne $regValue) {

    Set-ItemProperty -Path $regPath -Name $regName -Value $regValue

}
```



ADDITIONAL MEASURES - INTUNE POLICY MITIGATIONS FOR DEFENDING AGAINST RESPONDER ATTACKS

Building upon the previous recommendations, the following advanced security measures are designed to further strengthen your defences under an 'assume breach' mindset. These additional configurations take into account the possibility of existing compromise or exploitation and use least privilege principles to limit potential attacker movement and impact. Microsoft Intune can be leveraged to deploy these extra controls, enabling IT administrators to proactively circumvent common lateral movement techniques and reduce the attack surface associated with name resolution and credential exposure.

1. PROTOCOL AND NAME RESOLUTION HARDENING

Intune configuration profiles and endpoint security policies offer granular control over network protocols and name resolution behaviours, which are essential in minimising exposure to network poisoning attacks. The following controls are recommended:

Control	Action Location	Setting Location and State	Purpose
Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers = Enabled	Prevents unwanted NetBIOS name release that can be exploited for poisoning.
Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Microsoft network client: Digitally sign communications (always) = Enabled	Ensures integrity of client communications to prevent tampering.
Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Microsoft network client: Digitally sign communications (if server agrees) = Enabled	Strengthens communication security if supported by server.
Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Microsoft network server: Digitally sign communications (always) = Enabled	Guarantees server message integrity and authenticity.
Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Microsoft network server: Digitally sign communications (if client agrees) = Enabled	Improves server security when supported by the client.
Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\Link-Layer Topology Discovery: Turn on Responder = Disabled	Disables unsolicited network responses that can be abused.



Allow NetBT Queries to FQDNs	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\DNS Client: Allow NetBT queries for fully qualified domain names = Disabled	Prevents NetBIOS from handling DNS queries, stopping fallback attacks.
Prefer link local over DNS	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\DNS Client: Prefer link local responses over DNS when received over a network with higher precedence = Disabled	Ensures DNS is prioritised over less secure local responses.
Turn off smart protocol reordering	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\DNS Client: Turn off smart protocol reordering = Enabled	Forces DNS precedence to reduce exploitation risk.
Do not process incoming mailslot for DC if based on NetBIOS	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\Net Logon\DC Locator DNS Records: Do not process incoming mailslot messages used for domain controller location based on NetBIOS domain names = Enabled	Limits DC exposure to NetBIOS-based attacks.
Do not use NetBIOS for DC discovery	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\Net Logon\DC Locator DNS Records: Do not use NetBIOS-based discovery for domain controller location when DNS-based discovery fails = Enabled	Eliminates fallback to NetBIOS, reducing attack vectors.
Use DNS for name resolution for single-label domain instead of NetBIOS to locate DC	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\Network\Net Logon\DC Locator DNS Records: Use DNS name resolution with a single-label domain name instead of NetBIOS name resolution to locate the DC = Enabled	Ensures DNS-based DC location, improving security.



2. AUTHENTICATION AND CREDENTIAL PROTECTION

Intune's security baselines and device compliance policies provide essential tools for enforcing authentication safeguards and strengthening protection of user credentials. The following controls are recommended:

Control	Action Location	Setting Location and State	Purpose
Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\MS Security Guide: Configure SMB v1 client driver = Enabled: Disable driver (recommended)	Disables outdated SMB v1 to prevent exploitation.
Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	Windows Configuration → Window 10 and later → Settings catalog	Administrative Templates\MS Security Guide: Configure SMB v1 server = Disabled	Blocks legacy server protocol to close vulnerabilities.
Disable Unencrypted Password to Third Party SMB Servers	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Microsoft Network Client Send Unencrypted Password To Third Party SMB Servers = Disabled	Prevents sending plaintext passwords to external servers.
Disable NTLM Where Possible	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Allow Local System To Use Computer Identity For NTLM = Enabled	Blocks legacy NTLM authentication to thwart credential theft.
Network Security Restrict NTLM Incoming NTLM Traffic	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Restrict NTLM Incoming NTLM Traffic = Deny all accounts	Blocks legacy NTLM authentication to thwart credential theft.
Network Security Restrict NTLM Outgoing NTLM Traffic To Remote Servers	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Restrict NTLM Outgoing NTLM Traffic To Remote Servers = Deny all accounts	Blocks legacy NTLM authentication to thwart credential theft.
Network Security Minimum Session Security For NTLMSSP Based Clients	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Minimum Session Security For NTLMSSP Based Clients = Require NTLMv2 session security	Forces use of secure NTLMv2 to enhance authentication strength.
Network Security Minimum Session Security For NTLMSSP Based Servers	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Minimum Session Security For NTLMSSP Based Servers = Require NTLMv2 session security	Forces use of secure NTLMv2 to enhance authentication strength.



Do not allow storage of network authentication passwords	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Access Do Not Allow Storage Of Passwords and Credentials For Network Authentication = 1	Prevents credential caching, lowering theft risk.
Disable LM Hashing	Windows Configuration → Window 10 and later → Settings catalog	Local Policies Security Options: Network Security Do Not Store LAN Manager Hash Value On Next Password Change = Enabled	Eliminates weak LM hashes, mitigating downgrade attacks.
Enable Credential Guard	Windows Configuration → Window 10 and later → Settings catalog	Device Guard: Credential Guard = (Enabled with UEFI lock)	Secures credentials in memory to prevent hash theft.

3. ATTACK SURFACE REDUCTION RULE

Intune's security baselines and device compliance policies are vital for enforcing robust authentication safeguards and enhancing the protection of user credentials. As part of a comprehensive security strategy, organisations should implement the following attack surface reduction control:

Control	Action Location	Setting Location and State	Purpose
Block credential stealing from the Windows local security authority subsystem	Endpoint Security → Attack surface reduction → Windows → Attack Surface Reduction Rules	Block credential stealing from the Windows local security authority subsystem: Block	Prevents unauthorised access to sensitive credentials in memory

By applying these configurations via Microsoft Intune, organisations can substantially reduce the risk of network poisoning, credential theft, and relay attacks. Regular testing and review of these policies are essential to ensure continued protection against evolving threats and to maintain a robust security posture.



DOCUMENT CREDIT, RESPONSIBLE USE & STATEMENT OF LEGAL INTENT

This document has been created with the support of Microsoft Copilot and OpenAI ChatGPT, reflecting ethical and responsible use of artificial intelligence to provide practical guidance for professionals. It is offered freely as a resource to advance security awareness, foster knowledge sharing, and support the broader community, not as a formal academic publication nor for commercial advantage.

All content herein is shared under an open-access philosophy. Users are encouraged to use, share, and adapt this material in good faith, with the intent to benefit the professional community. While the document strives for accuracy and relevance, users should verify information before implementing it in their specific environments and accept responsibility for its use.

Credit for this document is attributed to the collaborative efforts enabled by Microsoft Copilot, OpenAI ChatGPT and the integration of AI-driven insights. No exclusive claim of authorship or ownership is made, especially where material is derived or adapted from external, AI-generated, or publicly available sources. Where feasible, original sources are acknowledged, but collective knowledge and indirect contributions are not explicitly credited to individuals or entities.

Upholding principles of ethical information exchange, this guide is freely available for lawful use, distribution, modification, and improvement. Users should act in accordance with applicable laws, respect intellectual property rights, and maintain high ethical standards when utilising, sharing, or adapting the content. The material is provided in the spirit of open learning and community advancement, with a commitment to transparency and responsible collaboration.