

Proactive Preparation and Hardening to Protect Against Destructive Attacks

V1.0 – JANUARY 14, 2022



Change Log

Version/Date	Notes
1.0: January 14, 2022	Initial Document

Contents

Background	4
Recommendations Summary	4
External Facing Assets.....	6
Identify, Enumerate, and Harden	6
Enforce Multifactor Authentication	6
Critical Asset Protections	8
Domain Controller and Critical Asset Backups	8
IT and OT Segmentation	10
Egress Restrictions.....	11
Virtualization Infrastructure Protections	12
On-Premises Lateral Movement Protections	14
Endpoint Hardening.....	14
Remote Desktop Protocol Hardening.....	17
Disabling Administrative/Hidden Shares.....	20
Hardening Windows Remote Management.....	22
Restricting Common Lateral Movement Tools and Methods	24
Additional Endpoint Hardening	27
Credential Exposure and Account Protections.....	29
Identification of Privileged Accounts and Groups.....	29
Privileged and Service Account Protections	31
Credential Protections When Using RDP.....	39
Restrict Remote Usage of Local Accounts.....	42
Conclusion	45

Background

Threat actors leverage destructive malware to destroy data, eliminate evidence of malicious activity, or manipulate systems in a way that renders them inoperable. Destructive cyber-attacks can be a powerful means to achieve strategic or tactical objectives; however, the risk of reprisal is likely to limit the frequency of use to very select incidents. Destructive cyber-attacks can include destructive malware, wipers, or modified ransomware.

This document provides proactive recommendations for organizations to prioritize for protecting against a destructive attack within an environment. The recommendations include practical and scalable methods that can help protect organizations from not only destructive attacks, but potential incidents where a threat actor is attempting to perform reconnaissance, escalate privileges, laterally move, maintain access, and achieve their mission. The recommendations are focused primarily for on-premises security hardening and defenses, but similar concepts can extend to cloud-based infrastructures.

The detection opportunities outlined in this document are meant to act as supplementary monitoring to existing security tools. Organizations should leverage endpoint and network security tools as additional preventative and detective measures. These tools use a broad spectrum of detective capabilities, including signatures and heuristics, to detect malicious activity with a reasonable degree of fidelity. The custom detection opportunities referenced in this document are correlated to specific threat actor behavior and are meant to trigger on anomalous activity that is identified by its divergence from normal patterns. Effective monitoring is dependent on a thorough understanding of an organization's unique environment and usage of pre-established baselines.

Recommendations Summary

Table 1 provides a high-level overview of guidance in this document with links to the corresponding hardening recommendations and detection opportunities.

Focus Area	Description	Hardening Recommendations	Detection Opportunities
Hardening External Facing Assets	Protect against the risk of threat actors exploiting an externally facing vector or leveraging existing technology for unauthorized remote access.	<ol style="list-style-type: none"> 1. Identify, Enumerate, and Harden Externally Facing Assets 2. Enforce Multifactor Authentication for Externally Facing Services 	<ol style="list-style-type: none"> 1. External Facing Assets and MFA Attempts
Critical Asset Protections	Protect specific high-value infrastructure and prepare for recovery from a destructive attack.	<ol style="list-style-type: none"> 1. Backup AD and other Critical Assets 2. Conduct Targeted Business Continuity Planning 3. Segment IT and OT Environments 4. Implement Egress Restrictions 5. Protect Virtualization Infrastructure 	<ol style="list-style-type: none"> 1. Unauthorized Access to Backups 2. Lateral Movement from IT to OT Networks 3. Unauthorized Egress Traffic 4. Unauthorized Access to Virtualization Infrastructure
On-Premises Lateral Movement Protections	Protect against a threat actor with initial access into an environment from moving laterally to further	<ol style="list-style-type: none"> 1. Restrict Communication To/From Endpoints 2. Harden Remote Desktop Protocol (RDP) 	<ol style="list-style-type: none"> 1. SMB and WMI Communications 2. RDP Usage

	expand their scope of access and persistence.	<ol style="list-style-type: none"> 3. Disable Administrative/Hidden Shares 4. Harden Windows Remote Management (WinRM) 5. Restrict Common Lateral Movement Tools and Methods 6. Implement Malware Protections on Endpoints 	<ol style="list-style-type: none"> 3. Accessing/Enumerating Administrative or Hidden Shares 4. WinRM Usage 5. Common Lateral Movement Tools and Methods 6. Tamper Protection Events
Credential Exposure and Account Protections	Protect against the exposure of privileged credentials to facilitate privilege escalation.	<ol style="list-style-type: none"> 1. Identify and Reduce the Scope of Privileged Accounts 2. Mitigate the Risk of Noncomputer Accounts with SPNs 3. Limit the Logon Rights for Privileged Accounts 4. Limit the Logon Rights for Service Accounts 5. Use Group Managed Service Accounts (gMSAs) 6. Use Protected Users Group 7. Disable WDigest and Enforce GPO Reprocessing 8. Limit Credential Exposure Through Credential Guard 9. Use Restricted Admin Mode for RDP 10. Implement Windows Defender Remote Credential Guard 11. Harden Local Administrator Accounts 	<ol style="list-style-type: none"> 1. Use/Modification of Privileged Accounts/Groups and GPO Modifications 2. Kerberoasting 3. Privileged Account Logons 4. Service Account Logons 5. Managed Service Account Modifications 6. Modification of the Protected Users Security Group 7. WDigest Authentication Conditions 8. Restricted Admin Mode for RDP 9. Modification of Windows Defender Remote Credential Guard Settings 10. Remote Logons with Local Accounts

Table 1: Overview of Hardening Recommendations and Detection Opportunities

External Facing Assets

Identify, Enumerate, and Harden

To protect against a threat actor exploiting vulnerabilities or misconfigurations via an external-facing vector, organizations must determine the scope of applications and organization-managed services that are externally accessible. Externally accessible applications and services are often targeted by threat actors for initial access by exploiting known vulnerabilities, brute-forcing common or default credentials, or authenticating using valid credentials.

To proactively identify and validate external facing applications and services, considerations include:

- Leverage Mandiant Attack Surface Management or a third-party vulnerability scanning technology to identify assets and associated vulnerabilities (e.g., Shodan, Tenable Nessus, Rapid7, Qualys).
- Performing a focused vulnerability assessment or penetration test with the goal of identifying external-facing vectors that could be leveraged for authentication and access.
- Verifying with technology vendors if the products leveraged by an organization for external-facing services require patches or updates to mitigate known vulnerabilities.

Any identified vulnerabilities should be not only be patched and hardened, but the identified technology platforms should also be reviewed to ensure that evidence of suspicious activity or technology/device modifications have not already occurred.

Enforce Multifactor Authentication

External-facing assets that leverage single-factor authentication (SFA) are highly susceptible to brute-forcing attacks, password spraying, or unauthorized remote access using valid (stolen) credentials. External-facing applications and services that currently allow for SFA should be configured to support multifactor authentication (MFA). Additionally, MFA should be leveraged for accessing not only on-premises external-facing managed infrastructure, but also for cloud-based resources (e.g., Software as a Service (SaaS) such as Microsoft 365 (M365)).

When configuring multifactor authentication, the following methods are commonly considered (and ranked from most to least secure):

- Fast Identity Online 2 (FIDO2) security key
- Software/hardware Open Authentication (OATH) token
- Authenticator application (e.g., Duo/Microsoft (MS) Authenticator)
 - Passwordless sign-in
 - Passcode validation
 - Push notification (least preferred option)
- Phone call
- Short Message Service (SMS) verification
- Email-based verification

Risks of Specific MFA Methods

PUSH NOTIFICATIONS

If an organization is leveraging push notifications for MFA (e.g., notification that requires acceptance via an application or automated call to a mobile device), threat actors can exploit this type of MFA configuration for attempted access, as a user may inadvertently accept a push notification on their device without the context of where the authentication was initiated.

PHONE/SMS VERIFICATION

If an organization is leveraging phone calls or SMS-based verification for MFA, these methods are not encrypted and are susceptible to potentially being intercepted by a threat actor. These methods are also vulnerable if a threat actor is able to transfer an employee's phone number to an attacker-controlled subscriber identification module (SIM) card. This would result in the MFA notifications being routed to the threat actor instead of the intended employee.

EMAIL-BASED VERIFICATION

If an organization is leveraging email-based verification for validating access or for retrieving MFA codes and a threat actor has already established the ability to access the email of their target, the actor could potentially also retrieve the email(s) to validate and complete the MFA process.

If any of these MFA methods are leveraged, consider:

- Training remote users to never accept or respond to a logon notification when they are not actively attempting to login.
- Establish a method for users to report suspicious MFA notifications, as this could be indicative of a compromised account.
- Ensure there are messaging policies in place to prevent the auto-forwarding of email messages outside the organization.

Detection Opportunities for External Facing Assets and MFA Attempts

Use Case	MITRE ID	Description
Brute Force	T1110 – Brute Force	Searching for a single user with an excessive number of failed logins from external Internet Protocol addresses (IPs). This risk can be mitigated by enforcing a strong password, MFA, and lockout policy.
Password Spray	T1110.003 – Password Spray	Searching for a high number of accounts with failed logins, typically from the similar origination addresses.
Multiple Failed MFA Same User	T1110 – Brute Force T1078 – Valid Accounts	Searching for multiple failed MFA conditions for the same account. This may be indicative of a previously compromised credential.
Multiple Failed MFA Same Source	T1110.003 – Password Spray T1078 – Valid Accounts	Searching for multiple failed MFA prompts for different users from the same source. This may be indicative of multiple compromised credentials and an attempt to “spray” MFA prompts/tokens for access.
External Authentication from an Account with Elevated Privileges	T1078 – Valid Accounts	Privileged accounts should use internally managed and secured privileged access workstations for access and should not be accessible directly from an external (untrusted) source.

Table 2: Detection Opportunities for External Facing Assets and MFA Attempts

Critical Asset Protections

Domain Controller and Critical Asset Backups

Organizations should verify that backups for domain controllers and critical assets are available and protected against unauthorized access or modification. Backup processes and procedures should be exercised on a continual basis. Backups should be protected and stored within secured enclaves that include both network and identity segmentation.

If an organization's Active Directory (AD) were to become corrupted or unavailable due to ransomware or a potentially destructive attack, restoring Active Directory from domain controller backups may be the only viable option to reconstitute domain services. The following domain controller recovery and reconstitution best practices should be proactively reviewed by organizations:

- Verify that there is a known good backup of domain controllers and SYSVOL shares (e.g., from a domain controller – backup C:\Windows\SYSVOL).
 - For domain controllers, a system state backup is preferred.

Note: For a system state backup to occur, *Windows Server Backup* must be installed as a feature on a domain controller.
 - The following command can be run from an elevated command prompt to initiate a system state backup of a domain controller.

```
wbadmin start systemstatebackup -backuptarget:<targetDrive>:
```

Figure 1: Command to Perform a System State Backup

- The following command can be run from an elevated command prompt to perform a SYSVOL backup (*Manage auditing and security log* permissions must also be configured for the account performing the backup).

```
robocopy c:\windows\sysvol c:\sysvol-backup /copyall /mir /b /r:0 /xd
```

Figure 2: Command to Perform a SYSVOL Backup

- Proactively identify domain controllers that hold flexible single master operation (FSMO) roles, as these domain controllers will need to be prioritized for recovery in the event that a full domain restoration is required.

```
netdom query fsmo
```

Figure 3: Command to Identify Domain Controllers that Hold FSMO roles

- Offline backups: Ensure offline domain controller backups are secured and stored separately from online backups.
- Encryption: Backup data should be encrypted both during transit (over the wire) and when at rest or mirrored for offsite storage.
- DSRM Password validation: Ensure that the Directory Services Restore Mode (DSRM) password is set to a known value for each domain controller. This password is required when performing an authoritative or nonauthoritative domain controller restoration.
- Configure alerting for backup operations: Backup products and technologies should be configured to detect and provide alerting for operations critical to the availability and integrity of backup data (e.g., deletion of backup data, purging of backup metadata, restoration events, media errors).
- Enforce role-based access control (RBAC): Access to backup media and the applications that govern and manage data backups should use RBAC to restrict the scope of accounts that have access to the stored data and configuration parameters.

- Testing and verification: Both authoritative and nonauthoritative domain controller restoration processes should be documented and tested on a regular basis. The same testing and verification processes should be enforced for critical assets and data.

Business Continuity Planning

Critical asset recovery is dependent upon in-depth planning and preparation, which is often included within an organization's Business Continuity Plan (BCP). Planning and recovery preparation should include the following core competencies:

- A well-defined understanding of crown jewels data and supporting applications that align to backup, failover, and restoration tasks that prioritize mission-critical business operations.
- Clearly defined asset prioritization and recovery sequencing.
- Thoroughly documented recovery processes for critical systems and data.
- Trained personnel to support recovery efforts.
- Validation of recovery processes to ensure successful execution.
- Clear delineation of responsibility for managing and verifying data and application backups.
- Online and offline data backup retention policies, including initiation, frequency, verification, and testing (for both on-premises and cloud-based data).
- Established service-level agreements (SLAs) with vendors to prioritize application and infrastructure-focused support.

Continuity and recovery planning can become stale over time, and processes are often not updated to reflect environment and personnel changes. Prioritizing evaluations, continuous training, and recovery validation exercises will enable an organization to be better prepared in the event of a disaster.

Detection Opportunities for Backups

Use Case	MITRE ID	Description
Volume Shadow Deletion	T1490 – Inhibit System Recovery	Searching for instances where a threat actor will delete volume shadow copies to inhibit system recovery. This can be accomplished using the command line, PowerShell, and other utilities.
Unauthorized Access Attempt	T1078 – Valid Accounts	Searching for unauthorized users attempting to access the media and applications that are used to manage data backups.
Suspicious Usage of the DSRM Password	T1078 – Valid Accounts	Monitoring security event logs on domain controllers for: <ul style="list-style-type: none"> • Event ID 4794 - An attempt was made to set the Directory Services Restore Mode administrator password Monitoring the following registry key on domain controllers: HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior
		<i>Figure 4: DSRM Registry Key for Monitoring</i>
		The possible values for the registry key noted in Figure 4 are: <ul style="list-style-type: none"> • 0 (default): The DSRM Administrator account can only be used if the domain controller is restarted in Directory Services Restore Mode. • 1: The DSRM Administrator account can be used for a console-based log on if the local <i>Active Directory Domain Services</i> service is stopped.

		<ul style="list-style-type: none"> 2: The DSRM Administrator account can be used for console or network access without needing to reboot a domain controller.
--	--	--

Table 3: Detection Opportunities for Backups

IT and OT Segmentation

Organizations should ensure that there is both physical and logical segmentation between corporate information technology (IT) domains, identities, networks, and assets and those used in direct support of operational technology (OT) processes and control. By enforcing IT and OT segmentation, organizations can inhibit a threat actor's ability to pivot from corporate environments to mission-critical OT assets using compromised accounts and existing network access paths.

OT environments should leverage separate identity stores (e.g., dedicated Active Directory domains), which are not trusted or cross-used in support of corporate identity and authentication. **The compromise of a corporate identity or asset should not result in a threat actor's ability to directly pivot to accessing an asset that has the ability to influence an OT process.**

In addition to separate AD forests being leveraged for IT and OT, segmentation should also include technologies that may have a dual use in the IT and OT environments (backup servers, anti-virus (AV), endpoint detection and response (EDR), jump servers, storage, virtual network infrastructure). OT segmentation should be designed such that if there is a disruption in the corporate (IT) environment, the OT process can safely function independently, without a direct dependency (account, asset, network pathway) with the corporate infrastructure. For any dependencies that cannot be readily segmented, organizations should identify potential short-term processes or manual controls to ensure that the OT environment can be effectively isolated if evidence of an IT (corporate)-focused incident were detected.

Segmenting IT and OT environments is a best practice recommended by industry standards such as National Institute of Standards and Technology (NIST) *SP800-82 Rev 2: Guide to Industrial Control Systems Security* (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>) and [IEC 62443](#) (formerly ISA99).

According to these best-practice standards, segmenting IT and OT networks should include the following:

- OT attack surface reduction by restricting the scope of ports, services, and protocols that are directly accessible within the OT network from the corporate (IT) network.
- Incoming access from corporate (IT) into OT must terminate within a segmented OT demilitarized zone (DMZ). The OT DMZ must require that a separate level of authentication and access be granted (outside of leveraging an account or endpoint that resides within the corporate IT domain).
- Explicit firewall rules should restrict both incoming traffic from the corporate environment and outgoing traffic from the OT environment.
- Firewalls should be configured using the principle of deny by default, with only approved and authorized traffic flows permitted. Egress (Internet) traffic flows for all assets that support OT should also follow the deny-by-default model.
- Identity (account) segmentation must be enforced between corporate IT and OT. An account or endpoint within either environment should not have any permissions or access rights assigned outside of the respective environment.
- Remote access to the OT environment should not leverage similar accounts that have remote access permissions assigned within the corporate IT environment. **Multifactor authentication using separate credentials should be enforced for remotely accessing OT assets and resources.**
- Training and verification of manual control processes, including isolation and reliability verification for safety systems.
- Secured enclaves for storing backups, programming logic, and logistical diagrams for systems and devices that comprise the OT infrastructure.

- The default usernames and passwords associated with OT devices should always be changed from the default vendor configuration(s).

Detection Opportunities for IT and OT Segmented Environments

Use Case	MITRE ID	Description
Network Service Scanning	T1046 – Network Service Scanning	Searching for instances where a threat actor is performing internal network discovery to identify open ports and services between segmented environments.
Unauthorized Authentication Attempts Between Segmented Environments	T1078 – Valid Accounts	Searching for failed logins for accounts limited to one environment attempting to login within another environment. This can detect threat actors attempting to reuse credentials for lateral movement between networks.

Table 4: Detection Opportunities for IT and OT Segmented Environments

Egress Restrictions

Servers and assets that are infrequently rebooted are highly targeted by threat actors for establishing backdoors to create persistent beacons to command and control (C2) infrastructure. By blocking or severely limiting Internet access for these types of assets, an organization can effectively reduce the risk of a threat actor compromising servers, extracting data, or installing backdoors that leverage egress communications for maintaining access.

Egress restrictions should be enforced so that servers, internal network devices, critical IT assets, OT assets, and field devices cannot attempt to communicate to external sites and addresses (Internet resources). The concept of deny by default should apply to all servers, network devices, and critical assets (including both IT and OT), with only allow-listed and authorized egress traffic flows explicitly defined and enforced. Where possible, this should include blocking recursive Domain Name System (DNS) resolutions not included in an allow-list to prevent communication via DNS tunneling.

If possible, egress traffic should be routed through an inspection layer (such as a proxy) to monitor external connections and block any connections to malicious domains or IP addresses. Connections to uncategorized network locations (e.g. a domain that has been recently registered) should not be permitted. Ideally DNS requests would be routed through an external service (e.g. Cisco Umbrella, Infoblox DDI) to monitor for lookups to malicious domains.

Threat actors often attempt to harvest credentials (including New Technology Local Area Network (LAN) Manager (NTLM) hashes) based upon outbound Server Message Block (SMB) or Web-based Distributed Authoring and Versioning (WebDAV) communications. Organizations should review and limit the scope of egress protocols that are permissible from **any** endpoint within the environment. While Hypertext Transfer Protocol (HTTP) (Transmission Control Protocol (TCP)/80) and HTTP Secure (HTTPS) (TCP/443) egress communications are likely required for many user-based endpoints, the scope of external sites and addresses can potentially be limited based upon Web traffic-filtering technologies. Ideally, organizations should only permit egress protocols and communications based upon a predefined allow-list. Common high-risk ports for egress restrictions include:

- File Transfer Protocol (FTP)
- Remote Desktop Protocol (RDP)
- Secure Shell (SSH)
- SMB
- Trivial File Transfer Protocol (TFTP)
- WebDAV

Detection Opportunities for Suspicious Egress Traffic Flows

Use Case	MITRE ID	Description
External Connection Attempt to a Known Malicious IP	TA0011 – Command and Control	Leveraging threat feeds to identify attempted connections to known bad IP addresses.
External Communications from Servers, Critical Assets, and Isolated Network Segments	TA0011 – Command and Control	Searching for egress traffic flows from subnets and addresses that correlate to servers, critical assets, OT segments, and field devices.
Outbound Connections Attempted Over SMB	T1212 – Exploitation for Credential Access	Searching for external connection attempts over SMB, as this may be an attempt to harvest credential hashes.

Virtualization Infrastructure Protections

Threat actors often target virtualization infrastructure (e.g., VMware vCenter, Hyper-V) as part of their reconnaissance, lateral movement, data theft, and potential ransomware deployment objectives.

To reduce the attack surface of virtualized infrastructure, a best practice for VMware vCenter and Hyper-V appliances and servers is to isolate and restrict access to the management interfaces, essentially enclaving these interfaces within isolated virtual local area networks (VLANs) (network segments) where connectivity is only permissible from dedicated subnets where administrative actions can be initiated.

To protect management interfaces for VMware ESXi, the VMKernel network interface card (NIC) should **not** be bound to the same virtual network assigned to virtual machines running on the host. Additionally, ESXi servers can be configured in lockdown mode, which will only allow console access from the vCenter server(s). For additional information related to lockdown mode, reference <https://kb.vmware.com/s/article/1008077>.

The SSH protocol (TCP/22) provides a common channel for accessing a physical virtualization server or appliance (vCenter) for administration and troubleshooting. Threat actors commonly leverage SSH for direct access to virtualization infrastructure to conduct destructive attacks. In addition to enclaving access to administrative interfaces, SSH access to virtualization infrastructure should be disabled and only enabled for specific use-cases. If SSH is required, network ACLs should be used to limit where connections can originate.

Identity segmentation should also be configured when accessing administrative interfaces associated with virtualization infrastructure. If Active Directory authentication provides direct integrated access to the physical virtualization stack, a threat actor that has compromised a valid Active Directory account (with permissions to manage the virtualization infrastructure) could potentially use the account to directly access virtualized systems to steal data or perform destructive actions.

Authentication to virtualized infrastructure should rely upon dedicated and unique accounts that are configured with strong passwords and that are **not** co-used for additional access within an environment. Additionally, accessing management interfaces associated with virtualization infrastructure should only be initiated from isolated privileged access workstations, which prevent the storing and caching of passwords used for accessing critical infrastructure components.

For a listing of administrative ports associated with VMWare vCenter (that should be targeted for isolation), reference <https://kb.vmware.com/s/article/1012382>.

For a listing of best practices for securing Hyper-V, reference <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-security-in-windows-server>.

Detection Opportunities for Accessing Virtualization Infrastructure

Use Case	MITRE ID	Description
Unauthorized Access Attempt to Virtualized Infrastructure	T1078 – Valid Accounts	Searching for attempted logins to virtualized infrastructure by unauthorized accounts.
Unauthorized SSH Connection Attempt	T1021.004 – Remote Services: SSH	Searching for instances where an SSH connection is attempted when SSH has not been enabled for an approved purpose or is not expected from a specific origination asset.

Table 5: Detection Opportunities for Virtualization Infrastructure

On-Premises Lateral Movement Protections

Endpoint Hardening

Windows Firewall Configurations

Once initial access to on-premises infrastructure is established, threat actors will conduct lateral movement to attempt to further expand the scope of access and persistence. To protect Windows endpoints from being accessed using common lateral movement techniques, a Windows Firewall policy can be configured to restrict the scope of communications permitted between endpoints within an environment. A Windows Firewall policy can be enforced locally or centrally as part of a Group Policy Object (GPO) configuration. At a minimum, the common ports and protocols leveraged for lateral movement that should be blocked between workstation-to-workstation and workstations to non-domain controllers and non-file servers include:

- SMB (TCP/445, TCP/135, TCP/139)
- Remote Desktop Protocol (TCP/3389)
- Windows Remote Management (WinRM)/Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
- Windows Management Instrumentation (WMI) (dynamic port range assigned through Distributed Component Object Model (DCOM))

Using a GPO (Figure 5), the settings listed in Table 6 can be configured for the Windows Firewall to control **inbound** communications to endpoints in a managed environment. The referenced settings will effectively block all inbound connections for the *Private* and *Public* profiles, and for the *Domain* profile, only allow connections that do not match a predefined block rule.

Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security

Figure 5: GPO Path for Creating Windows Firewall Rules

Profile Setting	Firewall State	Inbound Connections	Log Dropped Packets	Log Successful Connections	Log File Path	Log File Maximum Size (KB)
Domain	On	Allow	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Private	On	Block All Connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Public	On	Block All Connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096

Table 6: Windows Firewall Recommended Configuration State

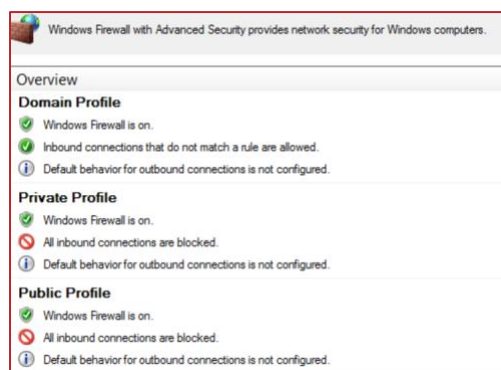


Figure 6: Windows Firewall Recommendation Configurations

Additionally, to ensure that only centrally managed firewall rules are enforced (and cannot be overridden by a threat actor), the settings for *Apply local firewall rules* and *Apply local connection security rules* can be set to *No* for all profiles.

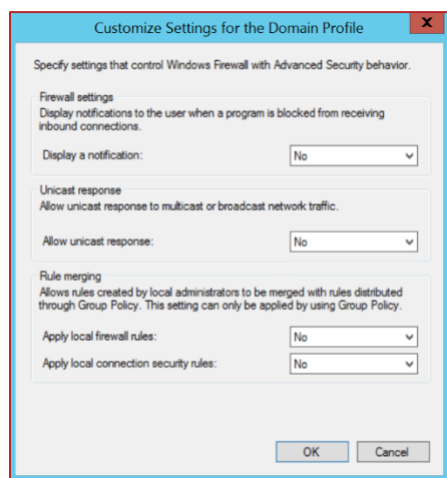


Figure 7: Windows Firewall Domain Profile Customized Settings

To quickly contain and isolate systems, the centralized Windows Firewall setting of *Block all connections* (Figure 8) will prevent any inbound connections from being established to a system. This is a setting that can be enforced on workstations and laptops, but will likely impact operations if enforced for servers, although if there is evidence of an active threat actor lateral pivoting within an environment, it may be a necessary step for rapid containment.

Note: If this control is being used temporarily to facilitate containment as part of an active incident, once the incident has been contained and it has been deemed safe to re-establish connectivity amongst systems within an environment, the *Inbound Connections* setting can be changed back to *Allow* using a GPO.

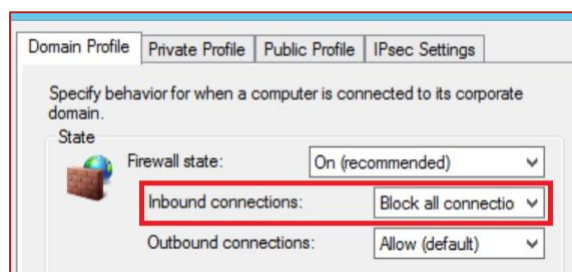


Figure 8: Windows Firewall - Block All Connections Settings

If blocking all inbound connectivity for endpoints during a containment event is not practical, or for the *Domain* profile configurations, at a minimum, the protocols listed in Table 7 should be enforced using either a GPO or via the commands referenced within the table.

For any specific applications that may require inbound connectivity to end-user endpoints, the local firewall policy should be configured with specific IP address exceptions for origination systems that are authorized to initiate inbound connections to such devices.

Protocol/Port	Windows Firewall Rule	Command Line Enforcement
SMB TCP/445, TCP/139, TCP/135	Predefined Rule Name: <ul style="list-style-type: none">File and Print Sharing	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no
Remote Desktop Protocol TCP/3389	Predefined Rule Name: <ul style="list-style-type: none">Remote Desktop	netsh advfirewall firewall set rule group="Remote Desktop" new enable=no
WMI	Predefined Rule Name: <ul style="list-style-type: none">Windows Management Instrumentation (WMI)	netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no
Windows Remote Management/PowerShell Remoting TCP/80, TCP/5985, TCP/5986	Predefined Rule Name: <ul style="list-style-type: none">Windows Remote ManagementWindows Remote Management (Compatibility) Port Rule: <ul style="list-style-type: none">TCP/5986	netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no Via PowerShell: Disable-PSRemoting -Force

Table 7: Windows Firewall Suggested Block Rules




















Name	Group	Profile	Enabled	Action
 Block WINRM SSL Port [5986] - Inbound		All	Yes	Block
 File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (Spooler Service - ...	File and Printer Sharing	All	Yes	Block
 File and Printer Sharing (Spooler Service - ...	File and Printer Sharing	All	Yes	Block
 Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block
 Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block
 Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block
 Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
 Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
 Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
 Windows Remote Management (HTTP-In)	Windows Remote Manage...	All	Yes	Block
 Windows Remote Management (HTTP-In)	Windows Remote Manage...	All	Yes	Block
 Windows Remote Management - Compa...	Windows Remote Manage...	All	Yes	Block

Figure 9: Windows Firewall Suggested Rule Blocks via Group Policy

NTLM Authentication Configurations

Threat actors often attempt to harvest credentials (including Windows NTLMv1 hashes) based upon outbound SMB or WebDAV communications. Organizations should review NTLM settings for Windows-based endpoints, and work to harden, disable, or restrict NTLMv1 authentication requests.

To fully restrict NTLM authentication to remote servers, the following GPO settings can be leveraged:

- *Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers*
 - *Allow all*
 - *Audit all*
 - *Deny all*

Note: If "Deny all" is selected, the client computer cannot authenticate (send credentials) to a remote server using NTLM authentication. Before setting to "Deny all", organizations should configure the GPO setting with the "Audit all" enforcement. With this configuration, audit and block events will be recorded within the Operational event log on endpoints (Applications and Services Log\Microsoft\Windows\NTLM).

If any recorded NTLM authentication events are required, organizations can configure the "Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication" setting to define a listing of remote servers which are required to use NTLM authentication.

Detection Opportunities for SMB, WMI, and NTLM Communications

Use Case	MITRE ID	Description
High Volume of SMB Connections	T1021.002 – SMB/Windows Admin Shares	Searching for a sharp increase in SMB connections that fall outside of a normal pattern.
Outbound Connection Attempted Over SMB	T1212 – Exploitation for Credential Access	Searching for external connection attempts over SMB, as this may be an attempt to harvest credential hashes.
WMI Being Used to Call a Remote Service	T1047 – Windows Management Instrumentation	Searching for WMI being used via a command line or PowerShell to call a remote service for execution.
WMI Being Used for Ingress Tool Transfer	T1105 – Ingress Tool Transfer	Searching for suspicious usage of WMI to download external resources.
Forced NTLM Authentication Using SMB or WebDAV	T1187 – Forced Authentication	Searching for potential NTLM authentication attempts using SMB or WebDAV.

Table 8: Detection Opportunities for SMB, WMI, and NTLM Communications

Remote Desktop Protocol Hardening

Remote Desktop Protocol (RDP) is a common method used by threat actors to remotely connect to systems, laterally move from the perimeter onto a larger scope of internal systems and perform malicious activities (such as data theft or ransomware deployment). External-facing systems with RDP open to the Internet present an elevated risk. Threat

actors may exploit this vector to gain initial access to an organization and then perform lateral movement into the organization to complete their mission objectives.

Proactively, organizations should scan their public IP address ranges to identify systems with RDP (TCP/3389) and other protocols (SMB – TCP/445) open to the Internet. At a minimum, RDP and SMB should not be directly exposed for ingress and egress access to/from the Internet. If required for operational purposes, explicit controls should be implemented to restrict the source IP addresses which can interface with systems using these protocols. The following hardening recommendations should also be implemented.

Enforce Multifactor Authentication

If external-facing RDP must be used for operational purposes, MFA should be enforced when connecting using this method. This can be accomplished either via the integration of a third-party MFA technology or by leveraging a Remote Desktop Gateway and Azure Multifactor Authentication Server using Remote Authentication Dial-In User Service (RADIUS) (<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-nps-rdg>).

Leverage Network-Level Authentication

For external-facing RDP servers, Network-Level Authentication (NLA) provides an extra layer of preauthentication before a connection is established. NLA can also be useful for protecting against brute-force attacks, which often target open Internet-facing RDP servers.

NLA can be configured either via the user interface (UI) (Figure 10) or via Group Policy (Figure 11).

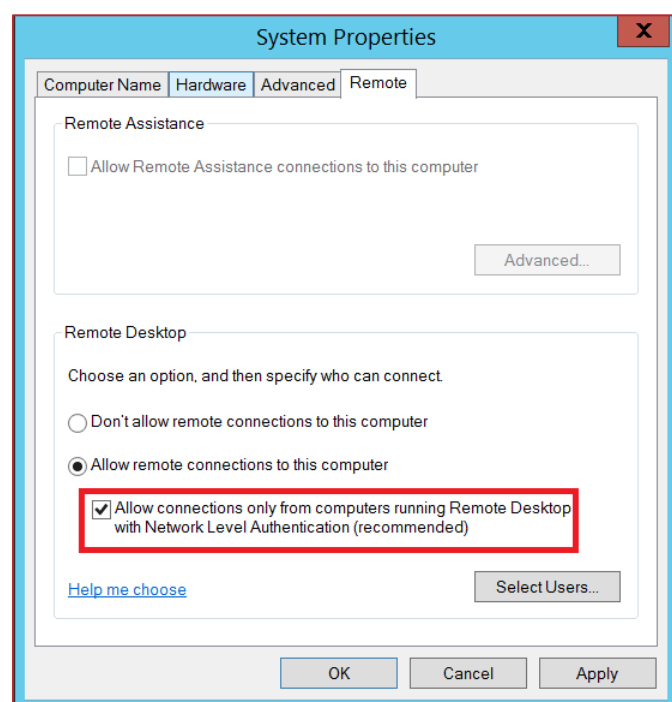


Figure 10: Enabling NLA via the UI

Using a GPO, the setting for NLA can be configured via:

- *Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security > Require user authentication for remote connections by using Network Level Authentication*
 - *Enabled*

Setting	State	Comment
Server authentication certificate template	Not configu...	No
Set client connection encryption level	Not configu...	No
Always prompt for password upon connection	Not configu...	No
Require secure RPC communication	Not configu...	No
Require use of specific security layer for remote (RDP) connections	Not configu...	No
Do not allow local administrators to customize permissions	Not configu...	No
Require user authentication for remote connections by using Network Level Authentication	Enabled	No

Figure 11: Enabling NLA via Group Policy

Some caveats about leveraging NLA for RDP:

- The Remote Desktop client v7.0 (or greater) must be leveraged.
- NLA uses CredSSP to pass authentication requests on the initiating system. CredSSP stores credentials in Local Security Authority (LSA) memory on the initiating system, and these credentials may remain in memory even after a user logs off the system. This provides a potential exposure risk for credentials in memory on the source system.
- On the RDP server, users permitted for remote access using RDP must be assigned the *Access this computer from the network* privilege when NLA is enforced. **This privilege is often explicitly denied for user accounts to protect against lateral movement techniques.**

Restrict Administrative Accounts from Leveraging RDP on Internet-Facing Systems

For external-facing RDP servers, highly privileged domain and local administrative accounts should not be permitted access to authenticate with the external-facing systems using RDP (Figure 12).

This can be enforced using Group Policy, configurable via the following path:

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Deny log on through Terminal Services*

Local Policies/User Rights Assignment	
Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHRT\Domain Admins, MCWHRT\Enterprise Admins, MCWHRT\Schema Admins, MCWHRT\Tier0-DomainAdmins, MCWHRT\Tier0-ExchangeAdmins, MCWHRT\Tier1-ServerAdmins, MCWHRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHRT\Domain Admins, MCWHRT\Enterprise Admins, MCWHRT\Schema Admins, MCWHRT\Tier0-DomainAdmins, MCWHRT\Tier0-ExchangeAdmins, MCWHRT\Tier1-ServerAdmins, MCWHRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHRT\Domain Admins, MCWHRT\Enterprise Admins, MCWHRT\Schema Admins, MCWHRT\Tier0-DomainAdmins, MCWHRT\Tier0-ExchangeAdmins, MCWHRT\Tier1-ServerAdmins, MCWHRT\Tier1-ServiceAccounts
Deny log on locally	Local account and member of Administrators group, MCWHRT\Domain Admins, MCWHRT\Enterprise Admins, MCWHRT\Schema Admins, MCWHRT\Tier0-DomainAdmins, MCWHRT\Tier0-ExchangeAdmins, MCWHRT\Tier1-ServerAdmins, MCWHRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHRT\Domain Admins, MCWHRT\Enterprise Admins, MCWHRT\Schema Admins, MCWHRT\Tier0-DomainAdmins, MCWHRT\Tier0-ExchangeAdmins, MCWHRT\Tier1-ServerAdmins, MCWHRT\Tier1-ServiceAccounts

Figure 12: Group Policy Configuration for Restricting Highly Privileged Domain and Local Administrative Accounts from Leveraging RDP

Detection Opportunities for RDP Usage

Use Case	MITRE ID	Description
RDP Authentication Integration	T1110 – Brute Force T1078 – Valid Accounts T1021.001 – Remote Desktop Protocol	<p>Existing authentication rules should include RDP attempts. This includes use cases for:</p> <ul style="list-style-type: none"> • Brute Force • Password Spraying • MFA Failures Single User • MFA Failures Single Source

		<ul style="list-style-type: none"> External Authentication from an Account with Elevated Privileges
Anomalous Connection Attempts over RDP	T1078 – Valid Accounts T1021.001 – Remote Desktop Protocol	Searching for anomalous RDP connection attempts over known RDP ports such as TCP/3389.

Table 9: Detection Opportunities for RDP Usage

Disabling Administrative/Hidden Shares

To conduct lateral movement, threat actors may attempt to identify administrative or hidden network shares, including those that are not explicitly mapped to a drive letter and use these for remotely binding to endpoints throughout an environment. As a protective or rapid containment measure, organizations may need to quickly disable default administrative or hidden shares from being accessible on endpoints. This can be accomplished by either modifying the registry, stopping a service, or by using the MSS (Legacy) Group Policy template (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>).

Common administrative and hidden shares on endpoints include:

- ADMIN\$
- C\$
- D\$
- IPC\$

Note: Disabling administrative and hidden shares on servers, specifically including domain controllers, may significantly impact the operation and functionality of systems within a domain-based environment.

Additionally, if PsExec is used in an environment, disabling the admin (ADMIN\$) share can restrict the capability for this tool to be used to remotely interface with endpoints.

Registry Method:

Using the registry, administrative and hidden shares can be disabled on endpoints (Figure 13 and Figure 14).

Workstations

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareWks"
Value = "0"
```

Figure 13: Registry Value Disabling Administrative Shares on Workstations

Servers

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareServer"
Value = "0"
```

Figure 14: Registry Value Disabling Administrative Shares on Servers

Service Method:

By stopping the *Server* service on an endpoint, the ability to access any shares hosted on the endpoint will be disabled (Figure 15).

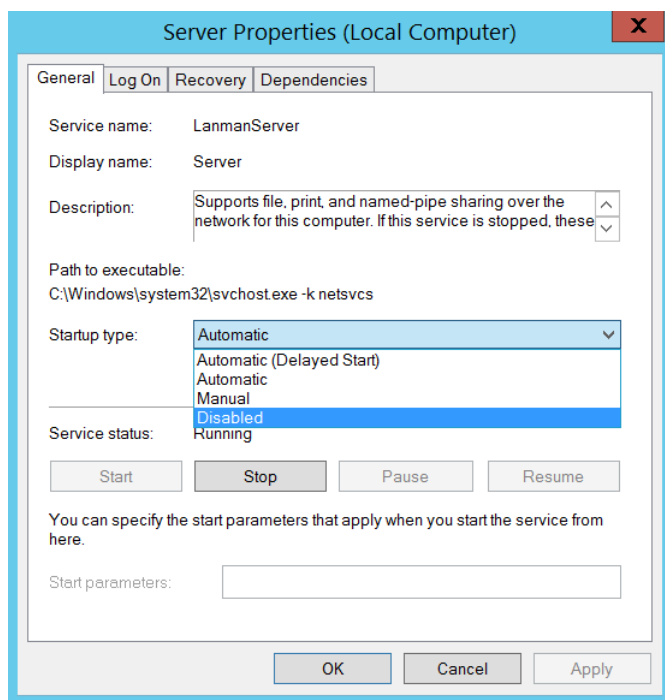


Figure 15: Server Service Properties

Group Policy Method:

Using the MSS (Legacy) Group Policy template, administrative and hidden shares can be disabled on either a server or workstation via a GPO setting (Figure 16).

- *Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)*
 - *Disabled*
- *Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)*
 - *Disabled*

Setting	State	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not configured	No
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended e...	Not configured	No
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure envi...	Disabled	No
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure enviro...	Disabled	No

Figure 16: Disabling Administrative And Hidden Shares via the MSS (Legacy) Group Policy Template

Detection Opportunities for Accessing Administrative or Hidden Shares

Use Case	MITRE ID	Description
Network Discovery: Suspicious Usage of the Net Command	T1049 - System Network Connections Discovery T1135 - Network Share Discovery	Searching for suspicious usage of the net command to enumerate systems such as file shares within an environment.

Table 10: Detection Opportunities for Accessing Administrative or Hidden Shares

Hardening Windows Remote Management

Threat actors may leverage Windows Remote Management (WinRM) to laterally move throughout an environment.

WinRM is enabled by default on all Windows Server operating systems (since Windows Server 2012 and above), but disabled on all client operating systems (Windows 7 and Windows 10) and older server platforms (Windows Server 2008 R2).

PowerShell remoting (PS remoting) is a native Windows remote command execution feature that is built on top of the WinRM protocol.

Windows client (nonservice) operating system platforms where WinRM is disabled indicates that there is:

- No WinRM listener configured
- No Windows firewall exception configured

By default, WinRM uses TCP/5985 and TCP/5986, which can be either disabled using the Windows Firewall or configured so that a specific subset of IP addresses can be authorized for connecting to endpoints using WinRM.

WinRM and PowerShell remoting can be explicitly disabled on endpoint using either a PowerShell command (Figure 17) or specific GPO settings.

PowerShell:

```
Disable-PSRemoting -Force
```

Figure 17: PowerShell Command to Disable WinRM/PowerShell Remoting on an Endpoint

Note: Running `Disable-PSRemoting -Force` does not prevent local users from creating PowerShell sessions on the local computer or for sessions destined for remote computers.

After running the command, the message recorded in Figure 18 will be displayed. These steps provide additional hardening, but after running the `Disable-PSRemoting -Force` command, PowerShell sessions destined for the target endpoint will not be successful.

```
PS C:\WINDOWS\system32> Disable-PSRemoting -Force
WARNING: Disabling the session configurations does not undo all the changes made by the Enable-PSRemoting or
Enable-PSSessionConfiguration cmdlet. You might have to manually undo the changes by following these steps:
1. Stop and disable the WinRM service.
2. Delete the listener that accepts requests on any IP address.
3. Disable the firewall exceptions for WS-Management communications.
4. Restore the value of the LocalAccountTokenFilterPolicy to 0, which restricts remote access to members of the
Administrators group on the computer.
```

Figure 18: Warning Message After Disabling PSRemoting

To enforce the additional steps for disabling WinRM via PowerShell (Figure 19 through Figure 22):

1. Stop and disable the *WinRM* service.

```
Stop-Service WinRM -PassThruSet-Service WinRM -StartupType Disabled
```

Figure 19: PowerShell Command to Stop and Disable the WinRM Service

2. Disable the listener that accepts requests on any IP address.

```
dir wsman:\localhost\listener
```

```
Remove-Item -Path WSMan:\Localhost\listener\<Listener name
```

Figure 20: PowerShell Commands to Delete a WSMan Listener

3. Disable the firewall exceptions for WS-Management communications.

```
Set-NetFirewallRule -DisplayName 'Windows Remote Management (HTTP-In)' -Enabled False
```

Figure 21: PowerShell Command to Disable Firewall Exceptions for WinRM

4. Restore the value of the `LocalAccountTokenFilterPolicy` to 0, which restricts remote access to members of the Administrators group on the computer.

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -
Name LocalAccountTokenFilterPolicy -Value 0
```

Figure 22: PowerShell Command to Configure the Registry Key for LocalAccountTokenFilterPolicy

Group Policy:

- *Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM*
 - *Disabled*

If this setting is configured as *Disabled*, the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.

- *Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Shell > Allow Remote Shell Access*
 - *Disabled*

This policy setting will manage the configuration of remote access to all supported shells to execute scripts and commands.

Detection Opportunities for WinRM Usage

Use Case	MITRE ID	Description
Unauthorized WinRM Execution Attempt	T1021.006 - Remote Services: Windows Remote Management	Searching for command execution attempts for WinRM on a system where WinRM has been disabled.
Suspicious Process Creation Using WinRM	T1021.006 - Remote Services: Windows Remote Management	Searching for anomalous process creation events using WinRM that deviate from an established baseline.
Suspicious Network Connection Using WinRM	T1021.006 - Remote Services: Windows Remote Management	Searching for network activity over known WinRM ports, such as TCP/5985 and TCP/5986, to identify anomalous connections that deviate from an established baseline.
Remote WMI Connection Using WinRM	T1021.006 - Remote Services: Windows Remote Management	Searching for remote WMI connection attempts using WinRM.

Table 11: Detection Opportunities for WinRM Usage

Restricting Common Lateral Movement Tools and Methods

Table 12 provides a consolidated summary of security configurations that can be leveraged to combat against common remote access tools and methods used for lateral movement within environments.

Tool/Tactic	Mitigating Security Configurations (Target Endpoints)
<p>PSEXEC (using the current logged-on user account, without the -u switch)</p> <p>If the -u switch is not leveraged, authentication will use Kerberos or NTLM for the current logged-on user of the source endpoint and will register as a Type 3 (network) logon on the destination endpoint.</p> <p>PSEXEC high-level functionality:</p> <ul style="list-style-type: none"> Connects to the hidden ADMIN\$ share (mapping to the C:\Windows folder) on a remote endpoint via SMB (TCP/445). Uses the Service Control Manager (SCM) to start the PSEXESVC service and enable a named pipe on a remote endpoint. Input/output redirection for the console is achieved via the created named pipe. 	<p>Option 1:</p> <p>GPO configuration:</p> <ul style="list-style-type: none"> Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment <ul style="list-style-type: none"> Deny access to this computer from the network <p>Option 2:</p> <p>Windows Firewall rule:</p> <pre>netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no</pre> <p><i>Figure 23: PowerShell Command to Disable Inbound File and Print Sharing (SMB) for an Endpoint Using a Local Windows Firewall Rule</i></p> <p>Option 3:</p> <p>Disable administrative and hidden shares.</p>
<p>PSEXEC (with Alternative Credentials, via the -u switch)</p> <p>If the -u switch is leveraged, authentication will use the alternate supplied credentials and will register as a Type 3 (network) and Type 2 (interactive) logon on the destination endpoint.</p>	<p>Option 1:</p> <p>GPO configuration:</p> <ul style="list-style-type: none"> Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment <ul style="list-style-type: none"> Deny access to this computer from the network Deny log on locally <p>Option 2:</p> <p>Windows Firewall rule:</p> <pre>netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no</pre> <p><i>Figure 24: PowerShell Command to Disable Inbound File and Print Sharing (SMB) for an Endpoint Using a Local Windows Firewall Rule</i></p>
Remote Desktop Protocol (RDP)	<p>Option 1:</p> <p>GPO configuration:</p> <ul style="list-style-type: none"> Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment <ul style="list-style-type: none"> Deny log on through Terminal Services <p>Option 2:</p> <p>Windows Firewall rule:</p>

Tool/Tactic	Mitigating Security Configurations (Target Endpoints)
	<pre>netsh advfirewall firewall set rule group="Remote Desktop" new enable=no</pre> <p><i>Figure 25: PowerShell Command to Disable Inbound Remote Desktop (RDP) for an Endpoint Using a local Windows Firewall Rule</i></p>
PS remoting and WinRM	<p>Option 1: PowerShell command:</p> <pre>Disable-PSRemoting -Force</pre> <p><i>Figure 26: PowerShell Command to Disable PowerShell Remoting for an Endpoint</i></p> <p>Option 2: GPO configuration:</p> <ul style="list-style-type: none"> Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM <ul style="list-style-type: none"> Disabled <p>Option 3: Windows Firewall rule:</p> <pre>netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no</pre> <p><i>Figure 27: PowerShell Command to Disable Inbound WinRM for an Endpoint Using a Local Windows Firewall Rule</i></p>
Distributed Component Object Model (DCOM)	<p>Option 1: GPO configuration:</p> <ul style="list-style-type: none"> Computer Configuration > Policies > Windows Settings > Local Policies > Security Options <ul style="list-style-type: none"> DCOM:Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) Syntax Computer Configuration > Policies > Windows Settings > Local Policies > Security Options <ul style="list-style-type: none"> DCOM:Machine Access Restrictions in Security Descriptor Definition Language (SDDL) Syntax <p>Both of these settings allow an organization to define additional computer-wide controls that govern access to all DCOM-based applications on an endpoint.</p> <p>When users or groups that are provided permissions are specified, the security descriptor field is populated with the SDDL representation of those groups and privileges. Users and groups can be given explicit <i>Allow</i> or <i>Deny</i> privileges for both local and remote access using DCOM.</p>

Tool/Tactic	Mitigating Security Configurations (Target Endpoints)
	Option 2: Windows Firewall rules:
	netsh advfirewall firewall set rule group="COM+ Network Access" new enable=no netsh advfirewall firewall set rule group="COM+ Remote Administration" new enable=no
	<i>Figure 28: PowerShell Commands to Disable Inbound DCOM for an Endpoint Using a Local Windows Firewall Rule</i>
Third-party remote access applications (e.g., VNC/DameWare/ScreenConnect) that rely upon specific interactive and remote logon permissions being configured on an endpoint.	GPO configuration: <ul style="list-style-type: none"> • <i>Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment</i> <ul style="list-style-type: none"> ○ <i>Deny access to this computer from the network</i> ○ <i>Deny log on locally</i>

Table 12: Common Lateral Movement Tools/Methods and Mitigating Security Controls

Detection Opportunities for Common Lateral Movement Tools and Methods

Use Case	MITRE	Description
Anomalous PsExec Usage	T1569.002 – System Services: Service Execution T1021.002 – Remote Services: SMB/Windows Admin Shares T1570 – Lateral Tool Transfer	Searching for attempted execution of PsExec on systems where PsExec is disabled or where it deviates from normal activity.
Process Creation Event Involving a COM Object by Different User	T1021.003 – Remote Services: Distributed Component Object Model T1078 – Valid Accounts	Searching for process creation events including COM objects that are initiated by an account that is not currently the logged-in user for the system.
High Volume of DCOM-Related Activity	T1021.003 – Remote Services:	Searching for a sharp increase in volume of DCOM-related activity.

	Distributed Component Object Model	
Third-Party Remote Access Applications	T1219 – Remote Access Software	Searching for anomalous usage of third-party remote access applications. This type of activity could indicate a threat actor is attempting to use third-party remote access applications as an alternate communication channel or for creating remote interactive sessions.

Table 13: Detection Opportunities for Common Lateral Movement Tools and Methods

Additional Endpoint Hardening

To help protect against malicious binaries, malware, and encryptors being invoked on endpoints, additional security hardening technologies and controls should be considered. Examples of additional security controls for consideration for Windows-based endpoints are provided as follows.

Windows Defender Application Control

Windows Defender Application Control is a set of inherent configuration settings within Active Directory that provide lockdown and control mechanisms for controlling which applications and files users can run on endpoints. With this functionality, the following types of rules can be configured within GPOs:

- Publisher rules: Can be leveraged to allow or restrict execution of files based upon digital signatures and other attributes.
- Path rules: Can be leveraged to allow or restrict file execution or access based upon files residing in specific path.
- File hash rules: Can be leveraged to allow or restrict file execution based on a file's hash.

For additional information related to Windows Defender Application Control, reference <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>.

Microsoft Defender Attack Surface Reduction

Microsoft Defender Attack Surface Reduction (ASR) rules can help protect against various threats, including:

- A threat actor launching executable files and scripts that attempt to download or run files.
- A threat actor running obfuscated or suspicious scripts.
- A threat actor invoking credential theft tools that interface with Local Security Authority Subsystem Service (LSASS).
- A threat actor invoking PsExec or WMI commands.
- Normalizing and blocking behaviors that applications do not usually initiate as part of standardized activity.
- Blocking executable content from email clients and Web mail (phishing).

ASR requires a Windows E3 license or above. A Windows E5 license provides advanced management capabilities for ASR.

For additional information related to Microsoft Defender Attack Surface Reduction functionality, reference <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction>.

Controlled Folder Access

Controlled folder access can help protect data from being encrypted by ransomware. Beginning with Windows 10 version 1709+ and Windows Server 2019+, controlled folder access was introduced within Windows Defender Antivirus (as part of Windows Defender Exploit Guard).

Once controlled folder access is enabled, applications and executable files are assessed by Windows Defender Antivirus, which then determines if an application is malicious or safe. If an application is determined to be malicious or suspicious, it will be blocked from making changes to any files in a protected folder.

Once enabled, controlled folder access will apply to a number of system folders and default locations, including:

- Documents
 - C:\users\\Documents
 - C:\users\Public\Documents
- Pictures
 - C:\users\\Pictures
 - C:\users\Public\Pictures
- Videos
 - C:\users\\Videos
 - C:\users\Public\Videos
- Music
 - C:\users\\Music
 - C:\users\Public\Music
- Desktop
 - C:\users\\Desktop
 - C:\users\Public\Desktop
- Favorites
 - C:\users\\Favorites

Additional folders can be added using the Windows Security application, Group Policy, PowerShell, or mobile device management (MDM) configuration service providers (CSPs). Additionally, applications can be allow-listed for access to protected folders.

Note: For controlled folder access to fully function, Windows Defender's *Real Time Protection* setting must be enabled.

For additional information related to controlled folder access, reference <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders>.

Tamper Protection

Threat actors will often attempt to disable security features on endpoints. Tamper protection either in Windows (via Microsoft Defender for Endpoint) or integrated within third-party AV/EDR platforms can help protect security tools from being modified or stopped by a threat actor. Organizations should review the configuration of security technologies that are deployed to endpoints and verify if tamper protection is (or can be) enabled to protect against unauthorized modification. Once implemented, organizations should test and validate that the tamper protection controls behave as expected as different products offer different levels of protection.

For additional information related to tamper protection for Windows Defender for Endpoint, reference <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection>.

Detection Opportunities for Tamper Protection Events

Use Case	MITRE	Description
Threat Actor Attempting to Disable Security Tooling on an Endpoint	T1562.001 - Disable or Modify Tools	Monitoring for evidence of processes or command-line arguments correlating to security tools/services being stopped.

Table 14: Detection Opportunities for Tamper Protection Events

Credential Exposure and Account Protections

Identification of Privileged Accounts and Groups

Threat actors will prioritize identifying privileged accounts as part of reconnaissance efforts. Once identified, threat actors will attempt to obtain credentials for these accounts for lateral movement, persistence, and mission fulfillment.

Organizations should proactively focus on identifying and reviewing the scope of accounts and groups within Active Directory that have an elevated level of privilege. An elevated level of privilege can be determined by the following criteria:

- Accounts or nested groups that are assigned membership into default domain and Exchange-based privileged groups (Figure 29).
- Accounts or nested groups that are assigned membership into security groups protected by AdminSDHolder.
- Accounts or groups assigned permissions for organizational units (OUs) housing privileged accounts, groups, or endpoints.
- Accounts or groups assigned specific extended right permissions either directly at the root of the domain or for OUs where permissions are inherited by child objects. Example include:
 - DS-Replication-Get-Changes-All
 - Administer Exchange Information Store
 - View Exchange Information Store Status
 - Create-Inbound-Forest-Trust
 - Migrate-SID-History
 - Reanimate-Tombstones
 - View Exchange Information Store Status
 - User-Force-Change-Password
- Accounts or groups assigned permissions for modifying or linking GPOs.
- Accounts or groups assigned explicit permissions on domain controllers or Tier 0 endpoints.
- Accounts or groups assigned directory service replication permissions.
- Accounts or groups with local administrative access on all endpoints (or a large scope of critical assets) in a domain.

To identify accounts that are provided membership into default domain-based privileged groups or are protected by AdminSDHolder, the following PowerShell cmdlets can be run from a domain controller.

```
get-ADGroupMember -Identity "Domain Admins" -Recursive | export-csv -path <output
directory>\DomainAdmins.csv -NoTypeInfoInformation
```

```
get-ADGroupMember -Identity "Enterprise Admins" -Recursive | export-csv -path <output
directory>\EnterpriseAdmins.csv -NoTypeInfoInformation
```

```
get-ADGroupMember -Identity "Schema Admins" -Recursive | export-csv -path <output
directory>\SchemaAdmins.csv -NoTypeInfoInformation
```

```
get-ADGroupMember -Identity "Administrators" -Recursive | export-csv -path <output
directory>\Administrators.csv -NoTypeInfoInformation
```

```
get-ADGroupMember -Identity "Account Operators" -Recursive | export-csv -path <output
directory>\AccountOperators.csv -NoTypeInfoInformation
```

```

get-ADGroupMember -Identity "Backup Operators" -Recursive | export-csv -path <output
directory>\BackupOperators.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Cert Publishers" -Recursive | export-csv -path <output
directory>\CertPublishers.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Print Operators" -Recursive | export-csv -path <output
directory>\PrintOperators.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Server Operators" -Recursive | export-csv -path <output
directory>\ServerOperators.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "DNSAdmins" -Recursive | export-csv -path <output
directory>\DNSAdmins.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "DNSAdmins" -Recursive | export-csv -path <output
directory>\DNSAdmins.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Group Policy Creator Owners" -Recursive | export-csv -path
<output directory>\Group-Policy-Creator-Owners.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Exchange Trusted Subsystem" -Recursive | export-csv -path
<output directory>\Exchange-Trusted-Subsystem.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Exchange Windows Permissions" -Recursive | export-csv -path
<output directory>\Exchange-Windows-Permissions.csv -NoTypeInfoInformation

get-ADGroupMember -Identity "Exchange Recipient Administrators" -Recursive | export-csv
-path <output directory>\Exchange-Recipient-Admins.csv -NoTypeInfoInformation

get-ADUser -Filter {(AdminCount -eq 1) -And (Enabled -eq $True)} | Select-Object Name,
DistinguishedName | export-csv -path <output directory>\AdminSDHolder_Enabled.csv

```

Figure 29: Commands to Identify Domain and Exchange-Based Privileged Accounts

Any privileged accounts granted membership into additional security groups can provide a threat actor with a potential path to domain administration-level permissions based upon endpoints where the accounts have permissions to log on or remotely access systems.

Ideally, only a small scope of accounts should be provided with highly privileged access within a domain. Accounts with highly privileged permissions should **not** be leveraged for daily use, used for interactive or remote logons to workstations, laptops, or common servers, or used for performing functions on non-domain controller (Tier 0) assets. For additional recommendations for restricting access for privileged accounts, reference the [Privileged Account Logon Restrictions](#) section of this document.

Detection Opportunities for Privileged Accounts, Groups, and GPO Modifications

Use Case	MITRE	Description
Interactive or Remote Logon of a Highly Privileged Account to an Unauthorized System	T1078 – Valid Accounts	Searching for logon attempts correlating to highly privileged accounts authenticating to systems that reside outside of the Tier 0 layer.

Privileged Account and Group Discovery	T1069 – Permission Groups Discovery Groups Discovery T1078 – Valid Accounts	Searching for command-line events where a user is attempting to enumerate privileged accounts and groups.
Account Added to Highly Privileged Group	T1078 – Valid Accounts T1098 – Account Manipulation	Identifying when accounts are added to highly privileged groups. While this can occur as part of normal activity, it should be infrequent and limited to specific accounts.
Modification of Group Policy Objects	T1484.001 – Domain Policy Modification: Group Policy Modification	<p>Identifying when group policy objects (GPOs) are created or modified. GPOs can also be exported and reviewed to identify last modification timestamps.</p> <pre>get-gpo -all export-csv -path "c:\temp\gpo-listing-all.csv" -NoTypeInfo</pre> <p><i>Figure 30: PowerShell cmdlet to Export and Review GPO Creation and Modification Timestamps</i></p>

Table 15: Detection Opportunities for Privileged Accounts, Groups, and GPO Modifications

Privileged and Service Account Protections

Identify and Review Noncomputer Accounts Configured with a SPN

Accounts with service principal names (SPNs) are commonly targeted by threat actors for privilege escalation. Using Kerberos, any domain user can request a Kerberos service ticket (TGS) from a domain controller for any account configured with an SPN. Noncomputer accounts likely are configured with guessable (nonrandom) passwords. Regardless of the domain function level or the host's Windows version, SPNs that are registered under a noncomputer account will use the legacy RC4-HMAC encryption suite rather than Advanced Encryption Standard (AES). The key used for encryption and decryption of the RC4-HMAC encryption type represents an unsalted NTLM hash version of the account's password, which could be derived via cracking the ticket.

Organizations should review Active Directory to identify noncomputer accounts configured with an SPN. Noncomputer accounts correlated to registered SPNs are likely service accounts and provide a method for a threat actor (without administrative privileges) to potentially derive (crack) the plain-text password for the account (Kerberoasting). To identify noncomputer accounts configured with an SPN, the PowerShell cmdlet referenced in Figure 31 can be ran from a domain controller.

```
Get-ADUser -Filter {(ServicePrincipalName -like "*")} | Select-Object name,samaccountname,sid,enabled,DistinguishedName
```

Figure 31: PowerShell cmdlet to Identify Noncomputer Accounts Configured with an SPN

Where possible, organizations should deregister noncomputer accounts with SPNs configured. Where SPNs are needed, organizations should mitigate the risk associated with Kerberoasting attacks. Accounts with SPNs should be configured with strong, unique passwords (e.g., minimum 25+ characters) with the passwords rotated on periodic basis for the accounts. Furthermore, privileges should be reviewed and reduced for these accounts to ensure that each account has the minimum required privileges needed for the intended function.

Accounts with SPNs should be considered in-scope for the proactive hardening measures detailed throughout this document.

Note: SPNs should never be associated with regular interactive user accounts.

Detection Opportunities for Noncomputer Accounts Configured with an SPN

Use Case	MITRE ID	Description
Potential Kerberoasting Attempt Using RC4	T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting	Searching for a Kerberos request using downgraded RC4 encryption.

Table 16: Detection Opportunities for Noncomputer Accounts Configured with an SPN

Privileged Account Logon Restrictions

Privileged and service accounts credentials are commonly used for lateral movement and establishing persistence.

For any accounts that have privileged access throughout an environment, the accounts should not be used on standard workstations and laptops, but rather from designated systems (e.g., privileged access workstations (PAWs)) that reside in restricted and protected VLANs and tiers. Dedicated privileged accounts should be defined for each tier, with controls that enforce that the accounts can only be used within the designated tier. Guardrail enforcement for privileged accounts can be defined within GPOs or by using authentication policy silos (Windows Server 2012 R2 domain-functional level or above).

The recommendations for restricting the scope of access for privileged accounts are based upon Microsoft's guidance for securing privileged access. For additional information, reference:

- <https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model>
- <https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos>

User Rights Assignments

As a proactive hardening or quick containment measure, consider blocking any accounts with privileged AD access from being able to log in (remotely or locally) to standard workstations, laptops, and common access servers (e.g., virtualized desktop infrastructure).

The settings referenced as follows are configurable using user rights assignments defined within GPOs via the path of:

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*

Accounts delegated with domain-based privileged access should be explicitly denied access to standard workstations and laptop systems within the context of the following settings (which can be configured using GPO settings similar to what are depicted in Figure 32):

- Deny access to this computer from the network (also include S-1-5-114: NT AUTHORITY\Local account and member of Administrators group) (SeDenyNetworkLogonRight)
- Deny logon as a batch job (SeDenyBatchLogonRight)
- Deny logon as a service (SeDenyServiceLogonRight)
- Deny logon locally (SeDenyInteractiveLogonRight)
- Deny logon through Terminal Services (SeDenyRemoteInteractiveLogonRight)

Local Policies/User Rights Assignment	
Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

Figure 32: Example of Privileged Account Access Restrictions for a Standard Workstation Using GPO Settings

Additionally, using GPOs, permissions can be restricted on endpoints to protect against privilege escalation and potential data theft by reducing the scope of accounts that have the following user rights assignments:

- Debug programs (SeDebugPrivilege)
- Back up files and directories (SeBackupPrivilege)
- Restore files and directories (SeRestorePrivilege)
- Take ownership of files or other objects (SeTakeOwnershipPrivilege)

Detection Opportunities for Privileged Account Logons

Use Case	MITRE ID	Description
Attempted Logon of a Privileged Account from a Nonprivileged Access Workstation	T1078 – Valid Accounts	Searching for logon attempts correlating to highly privileged accounts authenticating to systems that reside outside of the Tier 0 layer.

Table 17: Detection Opportunities for Privileged Account Logons

Service Account Logon Restrictions

Organizations should also consider enhancing the security of domain-based service accounts to restrict the capability for the accounts to be used for interactive, remote desktop, and, where possible, network-based logons.

Minimum recommended logon hardening for service accounts (on endpoints where the service account is not required for interactive or remote logon purposes):

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*
 - *Deny logon locally* (SeDenyInteractiveLogonRight)
 - *Deny logon through Terminal Services* (SeDenyRemoteInteractiveLogonRight)

Additional recommended logon hardening for service accounts (on endpoints where the service accounts is not required for network-based logon purposes):

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*
 - *Deny access to this computer from the network* (SeDenyNetworkLogonRight)

If a service account is only required to be leveraged on a single endpoint to run a specific service, the service account can be further restricted to only permit the account's usage on a predefined listing of endpoints (Figure 33).

- *Active Directory Users and Computers > Select the account*

- *Account tab*
 - *Log On To button* > Select the proper scope of computers for access

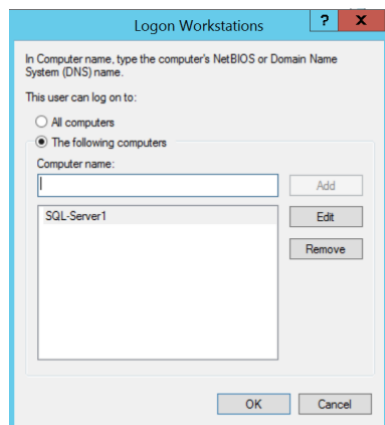


Figure 33: Option to Restrict an Account to Log Onto Specific Endpoints

Detection Opportunities for Service Account Logons

Use Case	MITRE ID	Description
Anomalous Logon from a Service Account	T1078 – Valid Accounts	Searching for login attempts for a service account on a new (unexpected) endpoint. This will require baselining service accounts to expected (approved) systems.

Table 18: Detection Opportunities for Service Account Logons

Managed/Group Managed Service Accounts

Organizations with static service accounts should review the feasibility of migrating the service accounts to be managed service accounts (MSAs) or group managed service accounts (gMSAs).

MSAs were first introduced with the Windows Server 2008 R2 Active Directory schema (domain-functional level) and provide automatic password management (30-day rotation) for dedicated service accounts that are associated with running services on specific endpoints.

- **Standard MSA:** The account is associated with a single endpoint and the complex password for the account is automatically managed and changed on a predefined frequency (30 days by default). While an MSA can only be associated with a single computer account, multiple services on the same endpoint can leverage the MSA.
- **Group managed service account (gMSA):** First introduced with Windows Server 2012 and are very similar to MSAs, but allow for a single gMSA to be leveraged across *multiple* endpoints.

Common uses for MSAs and gMSAs:

- Scheduled Tasks
- Internet Information Services (IIS) application pools
- Structured Query Language (SQL) services (SQL 2012 and later) – Express editions are **not** supported by MSAs.
- Microsoft Exchange services
- Network Load Balancing (clustering) – gMSAs only
- Third-party applications that support MSAs

Note: Threat actors can potentially discover accounts and groups that have permissions to read/leverage the password for a gMSA for privilege escalation and lateral movement. This can be accomplished by leveraging the `get-adserviceaccount` PowerShell cmdlet and enumerating the `msDS-GroupMSAMembership` (PrincipalsAllowedToRetrieveManagedPassword) configuration for a gMSA, which stores the security principals that can access the gMSA password. It is important that when configuring managed service accounts,

organizations focus on restricting the scope of accounts and groups that have the ability to obtain and leverage the password for the managed service accounts and enforce structured monitoring of these accounts and groups.

For additional information related to MSAs and gMSAs, reference:

- <https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/managed-service-accounts-understanding-implementing-best/ba-p/397009>
- <https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>

Detection Opportunities for Managed/Group Managed Service Accounts

Use Case	MITRE ID	Description
Group Membership Addition	T1069 – Permission Groups Discovery T1098 – Account Manipulation	Searching for MSAs/gMSAs and the associated PrincipalsAllowedToRetrieveManagedPassword or PrincipalsAllowedToDelegateToAccount permissions, which could provide the ability to leverage the MSA/gMSA for malicious purposes.
		Example reconnaissance commands for querying for MSAs/gMSAs and associated attributes:
		<pre>get-adserviceaccount</pre> <pre>get-adserviceaccount -filter {name -eq 'account-name'} -prop * select Name, MemberOf, PrincipalsAllowedToDelegateToAccount, PrincipalsAllowedToRetrieveManagedPassword</pre>

Figure 34: Example Reconnaissance Commands for Querying for MSAs/gMSAs

Table 19: Detection Opportunities for Managed/Group Managed Service Accounts

Protected Users Security Group

By leveraging the Protected Users security group for privileged accounts, an organization can minimize various exposure factors and common exploitation methods by a threat actor or malware variant obtaining credentials for privileged accounts on disk or in memory from endpoints.

Beginning with Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2 (and above), the Protected Users security group was introduced to manage credential exposure within an environment. Members of this group automatically have specific protections applied to accounts, including:

- The Kerberos ticket granting ticket (TGT) expires after four hours, rather than the normal 10-hour default setting.
- No NTLM hash for an account is stored in LSASS, since only Kerberos authentication is used (NTLM authentication is disabled for an account).
- Cached credentials are blocked. A domain controller must be available to authenticate the account.
- WDigest authentication is disabled for an account, regardless of an endpoint's applied policy settings.
- DES and RC4 cannot be used for Kerberos preauthentication (Server 2012 R2 or higher); rather, Kerberos with AES encryption will be enforced.
- Accounts cannot be used for either constrained or unconstrained delegation (equivalent to enforcing the *Account is sensitive and cannot be delegated* setting in Active Directory Users and Computers).

To provide domain controller-side restrictions for members of the Protected Users security group, the domain functional level must be Windows Server 2012 R2 (or higher). Microsoft Security Advisory [KB2871997](#) adds

compatibility support for the protections enforced for members of the Protected Users security group for Windows 7, Windows Server 2008 R2, and Windows Server 2012 systems.

Successful (Event IDs 303, 304) or failed (Event IDs 100, 104) logon events for members of the Protected Users security group can be recorded on domain controllers within the following event logs:

- %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Authentication%4ProtectedUserSuccesses-DomainController.evtx
- %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Authentication%4ProtectedUserFailures-DomainController.evtx

The event logs are disabled by default and must be enabled on each domain controller. The PowerShell cmdlets referenced in Figure 35 can be leveraged to enable the event logs for the Protected Users security group on a domain controller.

```
$log1 = New-Object System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-Windows-Authentication/ProtectedUserSuccesses-DomainController
$log1.IsEnabled=$true
$log1.SaveChanges()

$log2 = New-Object System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController
$log2.IsEnabled=$true
$log2.SaveChanges()
```

Figure 35: PowerShell cmdlets for Enabling Event Logging for the Protected Users Security Group on Domain Controllers

Note: Service accounts (including MSAs) should **not** be added to the Protected Users security group, as authentication will fail.

If the Protected Users security group cannot be used, at a minimum, privileged accounts should be protected against delegation by configuring the account with the *Account is Sensitive and Cannot Be Delegated* flag in Active Directory.

Detection Opportunities for the Protected Users Security Group

Use Case	MITRE ID	Description
Removal of Account from Protected User Group	T1098 – Account Manipulation	Searching for an account which has been removed from the Protected Users group.
Attempted Logon of an Account in the Protected User Group from a Nonprivileged Access Workstation	T1078 – Valid Accounts	Searching for logon attempts from accounts in the Protected Users group authenticating from workstations of nonprivileged users.

Table 20: Detection Opportunities for the Protected Users Security Group

Clear-Text Password Protections

In addition to restricting access for privileged accounts, controls should be enforced that minimize the exposure of credentials and tokens in memory on endpoints.

On older Windows versions, clear-text passwords are stored in memory (LSASS) to primarily support WDigest authentication. WDigest should be explicitly disabled on all Windows endpoints where it is not disabled by default.

By default, WDigest authentication is disabled in Windows 8.1+ and in Windows Server 2012 R2+.

Beginning with Windows 7 and Windows Server 2008 R2, after installing KB2871997, WDigest authentication can be configured either by modifying the registry or by using the Microsoft Security Guide GPO template from the Microsoft Security Compliance Toolkit (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>).

Registry Method:

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
REG_DWORD = "0"
```

Figure 36: Registry Key and Value for Disabling WDigest Authentication

Another registry setting that should be explicitly configured is the TokenLeakDetectDelaySecs setting (Figure 37), which will clear credentials in memory of logged-off users after 30 seconds, mimicking the behavior of Windows 8.1 and above.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs
REG_DWORD = "30"
```

Figure 37: Registry Key and Value for Enforcing the TokenLeakDetectDelaySecs Setting

Group Policy Method:

Using the Microsoft Security Guide Group Policy template, WDigest authentication can be disabled via a GPO setting (Figure 38).

- *Computer Configuration > Policies > Administrative Templates > MS Security Guide > WDigest Authentication*
 - *Disabled*

Setting	State	Comment
Configure SMB v1 server	Not configured	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Disabled	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

Figure 38: Disabling WDigest Authentication via the MS Security Guide Group Policy Template

Additionally, an organization should verify that Allow* settings are not specified within the registry keys referenced in Figure 39, as this configuration would permit the tspkgs/CredSSP providers to store clear-text passwords in memory.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\PolicyDefaults
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation
```

Figure 39: Additional Registry Keys for Hardening Against Clear-Text Password Storage

Group Policy Reprocessing

Threat actors can manually enable WDigest authentication on endpoints by directly modifying the registry (UseLogonCredential configured to a value of 1). Even on endpoints where WDigest authentication is automatically disabled by default, it is recommended to enforce the GPO settings noted as follows, which will enforce automatic group policy reprocessing for the configured (expected) settings on an automated basis.

- *Computer Configuration > Policies > Administrative Templates > System > Group Policy > Configure security policy processing*
 - *Enabled - Process even if the Group Policy objects have not changed*
- *Computer Configuration > Policies > Administrative Templates > System > Group Policy > Configure registry policy processing*
 - *Enabled - Process even if the Group Policy objects have not changed*

Note: By default, Group Policy settings are only reprocessed and reapplied if the actual Group Policy was modified prior to the default refresh interval.

As KB2871997 is not applicable for Windows XP, Windows Server 2003, and Windows Server 2008, to disable WDigest authentication on these platforms, prior to a system reboot, WDigest needs to be removed from the listing of LSA security packages within the registry (Figure 40 and Figure 41).

HKLM\System\CurrentControlSet\Control\Lsa\Security Packages

Figure 40: Registry Key to Modify LSA Security Packages

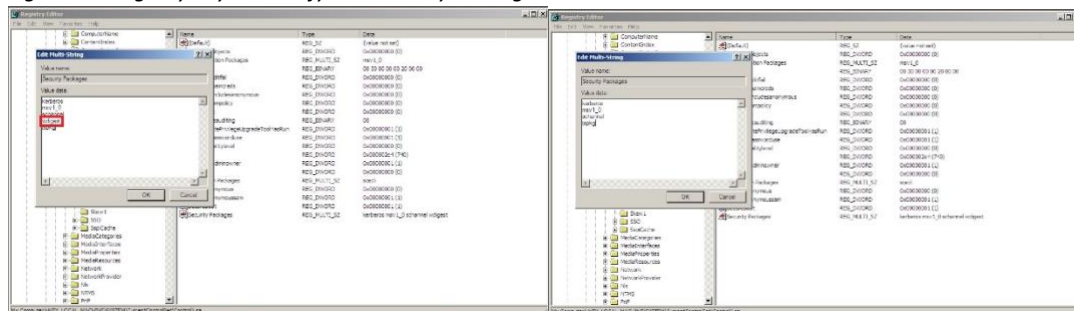


Figure 41: LSA Security Package Registry Key Before and After removal of WDigest Authentication from Listing of Providers

Detection Opportunities for WDigest Authentication Conditions

Use Case	MITRE ID	Description
Enable WDigest Authentication	T1112 – Modify Registry	Searching for evidence of WDigest being enabled in the Windows Registry.
		HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
		REG_DWORD = “1”
		Figure 42: WDigest Windows Registry Modification

Table 21: Detection Opportunities for WDigest Authentication Conditions

Windows Defender Credential Guard

If a threat actor is able to obtain local administrative access on an endpoint, this can allow for hashes and plain-text passwords (even with WDigest being disabled) being accessible for accounts that have previously accessed an endpoint. This tactic is often leveraged by threat actors to obtain clear-text credentials resident in memory (by using the Mimikatz security support provider (SSP) module) via administrative access that was obtained on endpoints. Using [Windows Defender Credential Guard](#) can help minimize the impact and extent of a pass-the-hash or pass-the-ticket-style attack by protecting NLTm password hashes, Kerberos ticket-granting tickets, and credentials stored in memory.

Windows Defender Credential Guard is a feature Microsoft introduced with Windows 10 and Windows Server 2016. This technology uses a combination of both hardware and virtualization-based security to isolate LSA secrets from the operating system, so that only privileged system-based software can access them.

For additional details related to configuring and testing Windows Defender Credential Guard, reference <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage>.

Credential Protections When Using RDP

Restricted Admin Mode for RDP

Restricted Admin Mode for RDP can be enabled for all end-user systems assigned to personnel that perform Remote Desktop connections to servers or workstations with administrative credentials. This feature can limit the in-memory exposure of administrative credentials on a destination endpoint when accessed using RDP.

To leverage restricted admin RDP, the command referenced in Figure 43 can be invoked.

```
mstsc.exe /RestrictedAdmin
```

Figure 43: Command to Invoke Restricted Admin RDP

When an RDP connection uses the Restricted Admin Mode feature, if the authenticating account is an administrator on the destination endpoint, the credentials for the user account are **not** stored in memory; rather, the context of the user account appears as the destination machine account (domain\destination-computer\$).

To leverage Restricted Admin Mode for RDP, settings must be enforced on the originating endpoint in addition to the destination endpoint.

Originating Endpoint (Client Mode - Windows 7 and Windows Server 2008 R2 and above):

A GPO setting must be applied to the originating endpoint initiating the remote desktop session using the *RestrictedAdmin* feature.

- *Computer Configuration > Policies > Administrative Templates > System > Credential Delegation > Restrict delegation of credentials to remote servers*
 - *Require Restricted Admin > set to Enabled*
 - *Use the Following Restricted Mode > Required Restricted Admin*

Configuring this GPO setting will result in the registry keys noted in Figure 44 being configured on an endpoint.

```
HKLM\Software\Policies\Microsoft\Windows\CredentialsDelegation\RestrictedRemoteAdministration
0 = Disabled
1 = Enabled

HKLM\Software\Policies\Microsoft\Windows\CredentialsDelegation\RestrictedRemoteAdministrationType
1 = Require Restricted Admin
2 = Require Remote Credential Guard
3 = Restrict Credential Delegation
```

Figure 44: Registry Settings for Requiring Restricted Admin Mode

Destination Endpoint (Server Mode - Windows 8.1 and Windows Server 2012 R2 and above):

A registry setting will need to be configured (Figure 45):

```
HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin
0 = Enabled
1 = Disabled
```

Figure 45: Registry Setting for Enabling or Disabling RestrictedAdmin RDP

Recommended: Set the registry value to 0 to enable Restricted Admin Mode.

With Restricted Admin RDP, another setting that should be configured is the *DisableRestrictedAdminOutboundCreds* registry key (Figure 46).

```
HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdminOutboundCreds
0 = default value (doesn't exist) - Admin Outbound Creds are Enabled
```


1 = Admin Outbound Creds are Disabled

Figure 46: Registry Setting for Disabling Admin Outbound Credentials

Recommended: Set the registry value to 1 to disable admin outbound credentials.

Note: With this setting set to 0, any outbound authentication requests will appear as the system (domain\destination-computer\$) that a user connected to using Restricted Admin Mode. Setting this to 1 disables the ability to authenticate to any downstream network resources when attempting to authenticate outbound from a system that a user connected to using Restricted Admin Mode for RDP.

For additional information regarding Restricted Admin Mode for RDP, reference:

- <https://support.microsoft.com/kb/2973351>
- <https://blogs.technet.microsoft.com/kfalde/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2/>

Detection Opportunities for Restricted Admin Mode for RDP

Use Case	MITRE ID	Description
Disable Restricted Admin Mode for RDP	T1112 – Modify Registry	Searching for an account disabling Restricted Admin Mode for RDP in the Windows Registry.
		HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin REG_DWORD = “1”
		Figure 47: Restricted Admin Mode for RDP Being Disabled in the Windows Registry on a Destination Endpoint
Disable Require Restricted Admin	T1484.001 – Domain Policy Modification: Group Policy Modification	Searching for the <i>Require Restricted Admin</i> option being disabled within a GPO configuration.
		Computer Configuration > Policies > Administrative Templates > System > Credential Delegation > Restrict delegation of credentials to remote servers “Require Restricted Admin” > set to Disabled
		Figure 48: Require Restricted Admin Being Disabled in a GPO

Table 22: Detection Opportunities for Restricted Admin Mode for RDP

Windows Defender Remote Credential Guard

For Windows 10 and Windows Server 2016 endpoints, Windows Defender Remote Credential Guard can be leveraged to reduce the exposure of privileged accounts in memory on destination endpoints when remote desktop is used for connectivity. With Remote Credential Guard, all credentials remain on the client (origination system) and are not directly exposed to the destination endpoint. Instead, the destination endpoint requests service tickets from the source as needed.

When a user logs in via RDP to an endpoint that has Remote Credential Guard enabled, none of the SSPs in memory store the account’s clear-text password or password hash. Note that Kerberos tickets remain in memory to allow interactive (and single sign-on (SSO)) experiences from the destination server.

The Remote Desktop client (origination) host:

- Must be running at least Windows 10 (v1703) to be able to supply credentials.
- Must be running at least Windows 10 (v1607) or Windows Server 2016 to use the user’s signed-in credentials (no prompt for credentials).
- This requires the user’s account be able to sign into both the client (origination) and the remote (destination) endpoint.

- Must be running the Remote Desktop Classic Windows application.
- The Remote Desktop Universal Windows Platform application does not support Windows Defender Remote Credential Guard.
- Must use Kerberos authentication to connect to the remote host.

Note: If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM. Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.

The Remote Desktop remote (destination) host:

- Must be running at least Windows 10 (v1607) or Windows Server 2016.
- Must allow Restricted Admin connections.
- Must allow the client's domain user to access Remote Desktop connections.
- Must allow delegation of nonexportable credentials.

To enable Remote Credential Guard on the client (origination) host using a GPO configuration:

- *Computer Configuration > Administrative Templates > System > Credentials Delegation > Restrict delegation of credentials to remote servers*
 - To require either Restricted Admin mode or Windows Defender Remote Credential Guard, choose *Prefer Windows Defender Remote Credential Guard*.
 - In this configuration, Remote Credential Guard is preferred, but it will use *Restricted Admin Mode* (if supported) when Remote Credential Guard cannot be used.
 - Neither Remote Credential Guard nor Restricted Admin Mode for RDP will send credentials in clear text to the Remote Desktop server.
 - To require Remote Credential Guard, choose *Require Windows Defender Remote Credential Guard*.
 - In this configuration, a Remote Desktop connection will succeed only if the remote computer meets the requirements for Remote Credential Guard.

To enable Remote Credential Guard on the remote (destination) host (Figure 49):

HKLM\System\CurrentControlSet\Control\Lsa

Registry Entry: DisableRestrictedAdmin

Value: 0

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0 /t REG_DWORD
```

Figure 49: Registry Key and Command Options to Enable Remote Credential Guard on a Remote (Destination) Host

To leverage Remote Credential Guard, use the command referenced in Figure 50.

```
mstsc.exe /remoteguard
```

Figure 50: Command to Leverage Remote Credential Guard

Detection Opportunities for Windows Defender Remote Credential Guard

Use Case	MITRE ID	Description
Disable Remote Credential Guard	T1112 – Modify Registry	Searching for an account disabling Remote Credential Guard in the Windows Registry.
		HKLM\System\CurrentControlSet\Control\Lsa Registry Entry: DisableRestrictedAdmin Value: 1
		Figure 51: Remote Credential Guard Being Disabled in the Windows Registry on a Destination Endpoint

Disable Require Remote Credential Guard	T1484.001 – Domain Policy Modification: Group Policy Modification	Searching for the <i>Require Remote Credential Guard</i> option being disabled within a GPO configuration.
		Computer Configuration > Administrative Templates > System > Credentials Delegation > Restrict delegation of credentials to remote servers
		<i>Figure 52: Remote Credential Guard Being Disabled in a GPO</i>

Table 23: Detection Opportunities for Windows Defender Remote Credential Guard

Restrict Remote Usage of Local Accounts

Local accounts that exist on endpoints are often a common avenue leveraged by threat actors to laterally move throughout an environment. This tactic is especially impactful when the password for the built-in local administrator account is configured to the same value across multiple endpoints.

To mitigate the impact of local accounts being leveraged for lateral movement organizations should consider both limiting the ability of local administrator accounts to establish remote connections and creating unique and randomized passwords for local administrator accounts across the environment.

KB2871997 (<https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a>) introduced two well-known SIDs that can be leveraged within GPO settings to restrict the usage of local accounts for lateral movement.

- S-1-5-113: NT AUTHORITY\Local account
- S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

Specifically, the SID S-1-5-114: NT AUTHORITY\Local account and member of Administrators group is added to an account's access token if the local account is a member of the BUILTIN\Administrators group. **This is the most beneficial SID to leverage to help stop a threat actor (or ransomware variant) that propagates using credentials for any local administrative accounts.**

Note: For SID S-1-5-114: NT AUTHORITY\Local account and member of Administrators group, if Failover Clustering is used, this feature should leverage a nonadministrative local account (CLIUSR) for cluster node management. **If this account is a member of the local Administrators group on an endpoint that is part of a cluster, blocking the network logon permissions can cause cluster services to fail.** Be cautious and thoroughly test this configuration on servers where Failover Clustering is used.

Step 1 – Option 1: S-1-5-114 SID

To mitigate the usage of local administrative accounts from being used for lateral movement, use the SID S-1-5-114: NT AUTHORITY\Local account and member of Administrators group within the following settings:

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*
 - Deny access to this computer from the network (SeDenyNetworkLogonRight)
 - Deny logon as a batch job (SeDenyBatchLogonRight)
 - Deny logon as a service (SeDenyServiceLogonRight)
 - Deny logon through Terminal Services (SeDenyRemoteInteractiveLogonRight)
 - Debug programs (SeDebugPrivilege: Permission used for attempted privilege escalation and process injection)

Step 1 – Option 2: UAC Token-Filtering

An additional control that can be enforced via GPO settings pertains to the usage of local accounts for remote administration and connectivity during a network logon. If the full scope of permissions (referenced previously) cannot be implemented in a short timeframe, consider applying the User Account Control (UAC) token-filtering method to local accounts for network-based logons.

To leverage this configuration via a GPO setting:

1. Download the Security Compliance Toolkit (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>) to use the MS Security Guide ADMX file.
2. Once downloaded, the SecGuide.admx and SecGuide.adml files must be copied to the \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.
3. If a centralized GPO store is configured for the domain, copy the PolicyDefinitions folder to the C:\Windows\SYSVOL\sysvol\<domain>\Policies folder.

GPO setting:

- *Computer Configuration > Policies > Administrative Templates > MS Security Guide > Apply UAC restrictions to local accounts on network logons*
 - *Enabled*

Once enabled, the registry value (Figure 53) will be configured on each endpoint:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
REG_DWORD = "0" (Enabled)
```

Figure 53: Registry Key and Value for Enabling UAC Restrictions for Local Accounts

When set to 0, remote connections with high-integrity access tokens are only possible using either the plain-text credential or password hash of the RID 500 local administrator (and only then depending on the setting of FilterAdministratorToken, which is configurable via the GPO setting of *User Account Control: Admin Approval Mode for the built-in Administrator account*).

The FilterAdministratorToken option can either enable (1) or disable (0) (default) *Admin Approval* mode for the RID 500 local administrator. When enabled, the access token for the RID 500 local administrator account is filtered and therefore UAC is enforced for this account (which can ultimately stop attempts to leverage this account for lateral movement across endpoints).

GPO setting:

- *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > User Account Control: Admin Approval Mode for the built-in Administrator account*

Once enabled, the registry value (Figure 54) will be configured on each endpoint:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken
REG_DWORD = "1" (Enabled)
```

Figure 54: Registry Key and Value for Requiring Admin Approval Mode for Local Administrative Accounts

Note: It is also prudent to ensure that the default setting for *User Account Control: Run all administrators in Admin Approval Mode* (EnableLUA option) is **not changed** from *Enabled* (default, as shown in Figure 55) to *Disabled*. If this setting is disabled, **all UAC policies are also disabled**. With this setting disabled, it is possible to perform privileged remote authentication using plain-text credentials or password hashes with any local account that is a member of the local administrators group.

GPO setting:

- *Computer Configuration > Policies > Administrative Templates > MS Security Guide > User Account Control: Run all administrators in Admin Approval Mode*
 - *Enabled*

Once enabled, the registry value (Figure 55) will be configured on each endpoint. This is the default setting.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
REG_DWORD = "1" (Enabled)

Figure 55: Registry Key and Value for Requiring Admin Approval Mode for All Local Administrative Accounts

UAC access token filtering will not affect any domain accounts in the local Administrators group on an endpoint.

Step 2: LAPS

In addition to blocking the usage of local administrator accounts from remote authentication to access endpoints, an organization should align a strategy to enforce password randomization for the built-in local administrator account. For many organizations, the easiest way to accomplish this task is by deploying and leveraging Microsoft's Local Administrator Password Solutions (LAPS).

For additional information regarding LAPS, reference <https://www.microsoft.com/en-us/download/details.aspx?id=46899>.

Detection Opportunities for Local Accounts

Use Case	MITRE ID	Description
Attempted Remote Logon of Local Account	T1078.003 - Valid Accounts: Local Accounts	Searching for remote logon attempts for local accounts on an endpoint.

Table 24: Detection Opportunities for Local Accounts

Conclusion

Destructive attacks, including ransomware, pose a serious threat to organizations. This whitepaper provides practical guidance on protecting against common techniques used by threat actors for initial access, reconnaissance, privilege escalation, and mission objectives. This whitepaper should not be considered as a comprehensive defensive guide for every tactic, but it can serve as a valuable resource for organizations to prepare for such attacks. It is based on front-line expertise with helping organizations prepare, contain, eradicate, and recover from potentially destructive threat actors and incidents.

