CIS Azure Compute Microsoft Windows Server 2019 Benchmark

v1.0.0 – 09-19-2022

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows.

This secure configuration guide is based on **Server 2019** settings available via built in Microsoft profiles in Azure, and is intended for all versions of the **Server 2019** operating system, including older versions. This secure configuration guide was tested against **Microsoft Windows Server 2019 Datacenter**.

To ensure all new and updated group policy objects (GPOs) are installed on the system, please download the newest version of the `ADMX/ADML` templates for **Windows 11**. This guide is based upon the newest version of the `ADMX/ADML` templates for **Windows 11**. Templates can be downloaded from Microsoft at: Download ADMX Templates for Windows 11 October 2021 Update [21H2] from Official Microsoft Download Center.

To obtain the latest version of this secure configuration guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

The Windows CIS Benchmarks are written for Active Directory **domain-joined** systems using Group Policy, or Azure profiles and not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on a standalone system.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Domain Controller**

  Items in this profile apply to Domain Controllers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Member Server**

  Items in this profile apply to Member Servers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

  Items in this profile also apply to Member Servers that have the following Roles enabled:

  - AD Certificate Services
  - DHCP Server
  - DNS Server
  - File Server
  - Hyper-V
  - Network Policy and Access Services
  - Print Server
  - Remote Access Services
  - Remote Desktop Services
  - Web Server

- **Next Generation Windows Security - Domain Controller**

  This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 or Level 2 profiles.

- **Next Generation Windows Security - Member Server**

  This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 or Level 2 profiles.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Center for Internet Security extends special recognition and thanks to Katy Calbreath, Mike Grimm, Brian Keogh, James Kim, Becky Ochs, Amrita Satapathy, and Ben Schwarz for their collaboration on this benchmark.

Contributor
Haemish Edgerton
Caleb Eifert
Hardeep Mehrotara
Clifford Moten
Rick Munck
Kolbe Stevenson
Guruprasad Venkatesha
Phil White
Matthew Woods
Kevin Zhang

Editor
Jennifer Jarose

Recommendations

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: `24 or more password(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit Enforce password history (Windows 10) - Windows security | Microsoft Docs

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `24 or more password(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Enforce password history
```

Default Value:

24 passwords remembered on domain members. 0 passwords remembered on stand-alone servers.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting defines how long a user can use their password before it expires.

Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

The recommended state for this setting is `365 or fewer days, but not 0`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user has authorized access.

Impact:

If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `365 or fewer days, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Maximum password age
```

Default Value:

42 days.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days.

The recommended state for this setting is: `1 or more day(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Impact:

If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `1 or more day(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Minimum password age
```

Default Value:

1 day on domain members. 0 days on stand-alone servers.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements.

The recommended state for this setting is: `14 or more character(s)`.

Note: In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length.

Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Impact:

Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `14 or more character(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Minimum password length
```

Default Value:

7 characters on domain members. 0 characters on stand-alone servers.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords.

When this policy is enabled, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
    - A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: `Enabled`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

Impact:

If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty.

If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments.

Also, the use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 0128 - 0159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Password must meet complexity requirements
```

Default Value:

Enabled on domain members. Disabled on stand-alone servers.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords.

The recommended state for this setting is: `Disabled`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

Impact:

If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Store passwords using reversible encryption
```

Default Value:

Disabled.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

1.2 Account Lockout Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2 Local Policies

This section contains recommendations for local policies.

2.1 Audit Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.2 User Rights Assignment

This section contains recommendations for user rights assignments.

2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities.

The recommended state for this setting is: `No One`.

Rationale:

If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Access Credential Manager as a trusted caller
```

Default Value:

No one.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The recommended state for this setting is: `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`.

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the **Access this computer from the network** user right is required for users to connect to shared printers and folders. If this user right is assigned to the `Everyone` group, then anyone will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the `Everyone` group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Impact:

If you remove the **Access this computer from the network** user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it is assigned to the `Authenticated Users` group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Access this computer from the network
```

Default Value:

Administrators, Authenticated Users, Enterprise Domain Controllers, Everyone, Pre-Windows 2000 Compatible Access.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.3 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The recommended state for this setting is: `Administrators, Authenticated Users`.

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the **Access this computer from the network** user right is required for users to connect to shared printers and folders. If this user right is assigned to the `Everyone` group, then anyone will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the `Everyone` group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Impact:

If you remove the **Access this computer from the network** user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it is assigned to the `Authenticated Users` group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Access this computer from the network
```

Default Value:

Administrators, Backup Operators, Users, Everyone.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.4 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access.

The recommended state for this setting is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The **Act as part of the operating system** user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.

Impact:

There should be little or no impact because the **Act as part of the operating system** user right is rarely needed by any accounts other than the `Local System` account, which implicitly has this right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Act as part of the operating system
```

Default Value:

No one.

2.2.5 (L1) Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting specifies which users can add computer workstations to the domain. For this policy setting to take effect, it must be assigned to the user as part of the **Default Domain Controller Policy** for the domain. A user who has been assigned this right can add up to 10 workstations to the domain. Users who have been assigned the *Create Computer Objects* permission for an OU or the Computers container in Active Directory can add an unlimited number of computers to the domain, regardless of whether or not they have been assigned the **Add workstations to domain** user right.

In Windows-based networks, the term security principal is defined as a user, group, or computer that is automatically assigned a security identifier to control access to resources. In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. However, some organizations may want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage the computers. If users are allowed to add computers to the domain, tracking and management efforts would be hampered. Also, users could perform activities that are more difficult to trace because of their ability to create additional unauthorized domain computers.

The recommended state for this setting is: `Administrators`.

Rationale:

The **Add workstations to domain** user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could (re-)install Windows on his or her computer and then add the computer to the domain. The user would know the password for the local Administrator account, and could log on with that account and then add his or her domain account to the local Administrators group.

Impact:

For organizations that have never allowed users to set up their own computers and add them to the domain, this countermeasure will have no impact. For those that have allowed some or all users to configure their own computers, this countermeasure will force the organization to establish a formal process for these procedures going forward. It will not affect existing domain computers unless they are removed from and re-added to the domain.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Add workstations to domain
```

Default Value:

Authenticated Users. (All domain users have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.6 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE`.

Note: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #2: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

A user with the **Adjust memory quotas for a process** user right can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Impact:

Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the **Adjust memory quotas for a process** user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Adjust memory quotas for a process
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE.

2.2.7 (L1) Ensure 'Allow log on locally' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services / Remote Desktop Services or IIS also require this user right.

The recommended state for this setting is: `Administrators`.

Note: This user right should generally be restricted to the `Administrators` group. Assign this user right to the `Backup Operators` group if your organization requires that they have this capability.

Rationale:

Any account with the **Allow log on locally** user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the **Allow log on locally** user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Allow log on locally
```

Default Value:

On Member Servers: Administrators, Backup Operators, Users.

On Domain Controllers: Account Operators, Administrators, Backup Operators, Print Operators.

2.2.8 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the `Administrators` group or use the Restricted Groups feature to ensure that no user accounts are part of the `Remote Desktop Users` group.

Restrict this user right to the `Administrators` group, and possibly the `Remote Desktop Users` group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature.

The recommended state for this setting is: `Administrators`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Connection Broker* Role Service will require a special exception to this recommendation, to allow the `Authenticated Users` group to be granted this user right.

Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #3: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the **Allow log on through Remote Desktop Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

Removal of the **Allow log on through Remote Desktop Services** user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Allow log on through Remote Desktop Services
```

Default Value:

Administrators.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.9 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the `Administrators` group or use the Restricted Groups feature to ensure that no user accounts are part of the `Remote Desktop Users` group.

Restrict this user right to the `Administrators` group, and possibly the `Remote Desktop Users` group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature.

The recommended state for this setting is: `Administrators, Remote Desktop Users`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Connection Broker* Role Service will require a special exception to this recommendation, to allow the `Authenticated Users` group to be granted this user right.

Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #3: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the **Allow log on through Remote Desktop Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

Removal of the **Allow log on through Remote Desktop Services** user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Allow log on through Remote Desktop Services
```

Default Value:

Administrators, Remote Desktop Users.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.10 (L1) Ensure 'Back up files and directories' is set to 'Administrators, Backup Operators, Server Operators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as `NTBACKUP`) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply.

The recommended state for this setting is: `Administrators, Backup Operators, Server Operators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Impact:

Changes in the membership of the groups that have the **Back up files and directories** user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, Backup Operators, Server Operators`.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Back up files and directories
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Server Operators.

2.2.11 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred.

The recommended state for this setting is: `Administrators, LOCAL SERVICE`.

Note: Discrepancies between the time on the local computer and on the Domain Controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the Domain Controllers.

Rationale:

Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets.

The risk from these types of events is mitigated on most Domain Controllers, Member Servers, and end-user computers because the Windows Time service automatically synchronizes time with Domain Controllers in the following ways:

- All client desktop computers and Member Servers use the authenticating Domain Controller as their inbound time partner.
- All Domain Controllers in a domain nominate the Primary Domain Controller (PDC) Emulator operations master as their inbound time partner.
- All PDC Emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner.
- The PDC Emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server.

This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

Impact:

There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Change the system time
```

Default Value:

On Member Servers: Administrators, LOCAL SERVICE.

On Domain Controllers: Administrators, Server Operators, LOCAL SERVICE.

2.2.12 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers.

The recommended state for this setting is: `Administrators, LOCAL SERVICE`.

Rationale:

Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with Domain Controllers in different time zones.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Change the time zone
```

Default Value:

Administrators, LOCAL SERVICE.

2.2.13 (L1) Ensure 'Create a pagefile' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer.

The recommended state for this setting is: `Administrators`.

Rationale:

Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create a pagefile
```

Default Value:

Administrators.

2.2.14 (L1) Ensure 'Create a token object' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data.

The recommended state for this setting is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right.

The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create a token object
```

Default Value:

No one.

2.2.15 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right.

Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

Note: A Member Server with Microsoft SQL Server *and* its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users who can create global objects could affect Windows services and processes that run under other user or system accounts. This capability could lead to a variety of problems, such as application failure, data corruption and elevation of privilege.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create global objects
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

2.2.16 (L1) Ensure 'Create permanent shared objects' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right.

The recommended state for this setting is: `No One`.

Rationale:

Users who have the **Create permanent shared objects** user right could create new shared objects and expose sensitive data to the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create permanent shared objects
```

Default Value:

No one.

2.2.17 (L1) Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.

Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only `Administrators` can create symbolic links.

The recommended state for this setting is: `Administrators`.

Rationale:

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.

Impact:

In most cases there will be no impact because this is the default configuration. However, on Windows Servers with the Hyper-V server role installed, this user right should also be granted to the special group `Virtual Machines` - otherwise you will not be able to create new virtual machines.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create symbolic links
```

Default Value:

Administrators.

2.2.18 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.

Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only `Administrators` can create symbolic links.

The recommended state for this setting is: `Administrators` and (when the *Hyper-V* Role is installed) `NT VIRTUAL MACHINE\Virtual Machines`.

Rationale:

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.

Impact:

In most cases there will be no impact because this is the default configuration. However, on Windows Servers with the Hyper-V server role installed, this user right should also be granted to the special group `Virtual Machines` - otherwise you will not be able to create new virtual machines.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create symbolic links
```

Default Value:

Administrators.

2.2.19 (L1) Ensure 'Debug programs' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The **Debug programs** user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to insert rootkit code. By default, the **Debug programs** user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

Impact:

If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the **Debug programs** user right to a separate Group Policy for that OU.

The service account that is used for the cluster service needs the **Debug programs** user right; if it does not have it, Windows Clustering will fail.

Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool `Kill.exe` requires this user right for administrators to terminate processes that they did not start.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Debug programs
```

Default Value:

Administrators.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	18.2 Ensure Explicit Error Checking is Performed for All In-house Developed Software For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.		●	●

2.2.20 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. This user right supersedes the **Access this computer from the network** user right if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Rationale:

Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

Impact:

If you configure the **Deny access to this computer from the network** user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny access to this computer from the network
```

Default Value:

Guest.

2.2.21 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right.

This user right supersedes the **Log on as a batch job** user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk.

The recommended state for this setting is to include: `Guests`.

Rationale:

Accounts that have the **Log on as a batch job** user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Impact:

If you assign the **Deny log on as a batch job** user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.

For example, if you assign this user right to the `IWAM_`*(ComputerName)* account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the `Guests` group, but on a computer that was upgraded from Windows 2000 this account is a member of the `Guests` group. Therefore, it is important that you understand which accounts belong to any groups that you assign the **Deny log on as a batch job** user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on as a batch job
```

Default Value:

No one.

2.2.22 (L1) Ensure 'Deny log on as a service' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which service accounts are prevented from registering a process as a service. This user right supersedes the **Log on as a service** user right if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Note: This security setting does not apply to the `System`, `Local Service`, or `Network Service` accounts.

Rationale:

Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the `System` account.

Impact:

If you assign the **Deny log on as a service** user right to specific accounts, services may not be able to start and a DoS condition could result.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on as a service
```

Default Value:

No one.

2.2.23 (L1) Ensure 'Deny log on locally' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the **Allow log on locally** policy setting if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Important: If you apply this security policy to the `Everyone` group, no one will be able to log on locally.

Rationale:

Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Impact:

If you assign the **Deny log on locally** user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the `ASPNET` account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on locally
```

Default Value:

No one.

2.2.24 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can log on as Remote Desktop clients. After the baseline Member Server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. This user right supersedes the **Allow log on through Remote Desktop Services** user right if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Note: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Impact:

If you assign the **Deny log on through Remote Desktop Services** user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on through Remote Desktop Services
```

Default Value:

No one.

2.2.25 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Enable computer and user accounts to be
trusted for delegation
```

Default Value:

Administrators.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.26 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.

The recommended state for this setting is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Enable computer and user accounts to be
trusted for delegation
```

Default Value:

No one.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.27 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to shut down Windows Vista-based and newer computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right.

The recommended state for this setting is: `Administrators`.

Rationale:

Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

Impact:

If you remove the **Force shutdown from a remote system** user right from the Server Operators group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Force shutdown from a remote system
```

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Server Operators.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.28 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or processes can generate audit records in the Security log.

The recommended state for this setting is: `LOCAL SERVICE, NETWORK SERVICE`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #3: A Member Server that holds the *Active Directory Federation Services* Role will require a special exception to this recommendation, to allow the `NT SERVICE\ADFSSrv` and `NT SERVICE\DRS` services, as well as the associated Active Directory Federation Services service account, to be granted this user right.

Rationale:

An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to allow the IIS application pool(s) to be granted this user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Generate security audits
```

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

2.2.29 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.

Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.

Also, a user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user.
- The user, in this logon session, logged on to the network with explicit credentials to create the access token.
- The requested level is less than Impersonate, such as Anonymous or Identify.

An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server with Microsoft SQL Server *and* its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

Impact:

In most cases this configuration will have no impact. If you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to also assign the user right to `IIS_IUSRS`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Impersonate a client after authentication
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

2.2.30 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.

Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.

Also, a user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user.
- The user, in this logon session, logged on to the network with explicit credentials to create the access token.
- The requested level is less than Impersonate, such as Anonymous or Identify.

An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE` and (when the *Web Server (IIS)* Role with *Web Services* Role Service is installed) `IIS_IUSRS`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server with Microsoft SQL Server *and* its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

Impact:

In most cases this configuration will have no impact. If you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to also assign the user right to `IIS_IUSRS`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Impersonate a client after authentication
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

2.2.31 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools.

The recommended state for this setting is: `Administrators`.

Rationale:

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Increase scheduling priority
```

Default Value:

On Windows Server 2016 or older: Administrators.

On Windows Server 2019 or newer: Administrators, Window Manager\Window Manager Group.

2.2.32 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Device drivers run as highly privileged code. A user who has the **Load and unload device drivers** user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.

Impact:

If you remove the **Load and unload device drivers** user right from the `Print Operators` group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Load and unload device drivers
```

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Print Operators.

2.2.33 (L1) Ensure 'Lock pages in memory' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur.

The recommended state for this setting is: `No One`.

Note: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users with the **Lock pages in memory** user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Lock pages in memory
```

Default Value:

No one.

2.2.34 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users can change the auditing options for files and directories and clear the Security log.

For environments running Microsoft Exchange Server, the `Exchange Servers` group must possess this privilege on Domain Controllers to properly function. Given this, DCs that grant the `Exchange Servers` group this privilege also conform to this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only `Administrators` on DCs.

The recommended state for this setting is: `Administrators` and (when Exchange is running in the environment) `Exchange Servers`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Manage auditing and security log
```

Default Value:

Administrators.

2.2.35 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users can change the auditing options for files and directories and clear the Security log.

For environments running Microsoft Exchange Server, the `Exchange Servers` group must possess this privilege on Domain Controllers to properly function. Given this, DCs that grant the `Exchange Servers` group this privilege also conform to this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only `Administrators` on DCs.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Manage auditing and security log
```

Default Value:

Administrators.

2.2.36 (L1) Ensure 'Modify an object label' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege.

The recommended state for this setting is: `No One`.

Rationale:

By modifying the integrity label of an object owned by another user a malicious user may cause them to execute code at a higher level of privilege than intended.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Modify an object label
```

Default Value:

No one.

2.2.37 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would result in a denial of service condition.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Anyone who is assigned the **Modify firmware environment values** user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Modify firmware environment values
```

Default Value:

Administrators.

2.2.38 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition.

The recommended state for this setting is: `Administrators`.

Note: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for the account that runs the SQL Server service to be granted this user right.

Rationale:

A user who is assigned the **Perform volume maintenance tasks** user right could delete a volume, which could result in the loss of data or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Perform volume maintenance tasks
```

Default Value:

Administrators.

2.2.39 (L1) Ensure 'Profile single process' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the **Profile single process** user right prevents intruders from gaining additional information that could be used to mount an attack on the system.

The recommended state for this setting is: `Administrators`.

Rationale:

The **Profile single process** user right presents a moderate vulnerability. An attacker with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Profile single process
```

Default Value:

Administrators.

2.2.40 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer.

The recommended state for this setting is: `Administrators, NT SERVICE\WdiServiceHost`.

Rationale:

The **Profile system performance** user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers may also be able to determine what processes are active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, NT SERVICE\WdiServiceHost`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Profile system performance
```

Default Value:

Windows Server 2008 (non-R2): Administrators.

Windows Server 2008 R2 and newer: Administrators, NT SERVICE\WdiServiceHost.

2.2.41 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges.

The recommended state for this setting is: `LOCAL SERVICE, NETWORK SERVICE`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #3: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users with the **Replace a process level token** privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the **Replace a process level token** user right also requires the user to have the **Adjust memory quotas for a process** user right that is discussed earlier in this section.)

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Replace a process level token
```

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

2.2.42 (L1) Ensure 'Restore files and directories' is set to 'Administrators, Backup Operators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista (or newer) in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the **Back up files and directories** user right.

The recommended state for this setting is: `Administrators, Backup Operators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

An attacker with the **Restore files and directories** user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that is used to back up data.

Impact:

If you remove the **Restore files and directories** user right from the `Backup Operators` group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, Backup Operators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Restore files and directories
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Server Operators.

2.2.43 (L1) Ensure 'Shut down the system' is set to 'Administrators, Backup Operators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition.

The recommended state for this setting is: `Administrators, Backup Operators`.

Rationale:

The ability to shut down Domain Controllers and Member Servers should be limited to a very small number of trusted Administrators. Although the **Shut down the system** user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a Domain Controller or Member Server.

When a Domain Controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down Domain Controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords — one of the functions of the Primary Domain Controller (PDC) Emulator role.

Impact:

The impact of removing these default groups from the **Shut down the system** user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, Backup Operators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Shut down the system
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Server Operators, Print Operators.

2.2.44 (L1) Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines which users and groups have the authority to synchronize all directory service data. This is also known as Active Directory synchronization.

The recommended state for this setting is: `No One`.

Rationale:

The **Synchronize directory service data** user right affects Domain Controllers; only Domain Controllers should be able to synchronize directory service data. Domain Controllers have this user right inherently, because the synchronization process runs in the context of the `System` account on Domain Controllers. Attackers who have this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Synchronize directory service data
```

Default Value:

No one.

2.2.45 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.

The recommended state for this setting is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Any users with the **Take ownership of files or other objects** user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Take ownership of files or other objects
```

Default Value:

Administrators.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents users from adding new Microsoft accounts on this computer.

The recommended state for this setting is: `Users can't add or log on with Microsoft accounts`.

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Impact:

Users will not be able to log onto the computer with their Microsoft account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
NoConnectedUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Users can't add or log on with Microsoft accounts`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Block Microsoft accounts
```

Default Value:

Users are able to use Microsoft accounts with Windows.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system.

The recommended state for this setting is: `Disabled`.

Note: This setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Rationale:

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Impact:

All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server™ 2003.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Guest account status
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

2.3.1.3 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Limit local account use of blank
passwords to console logon only
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Administrator account that was established when the domain was first created.

Rationale:

The Administrator account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Impact:

You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Rename administrator account
```

Default Value:

Administrator.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

2.3.1.5 (L1) Configure 'Accounts: Rename guest account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Guest account that was established when the domain was first created.

Rationale:

The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Impact:

There should be little impact, because the Guest account is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Rename guest account
```

Default Value:

Guest.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

2.3.2 Audit

This section contains recommendations related to auditing controls.

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista.

The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled.

The recommended state for this setting is: `Enabled`.

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Rationale:

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAudit
Policy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Audit: Force audit policy subcategory settings
(Windows Vista or later) to override audit policy category settings
```

Default Value:

Enabled. (Advanced Audit Policy Configuration settings will be used for auditing configuration, and legacy Audit Policy configuration settings will be ignored.)

References:

1. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing#to-ensure-that-advanced-audit-policy-configuration-settings-are-not-overwritten

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason.

If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. The administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

The recommended state for this setting is: `Disabled`.

Rationale:

If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:CrashOnAuditFail
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Audit: Shut down system immediately if unable to
log security audits
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

2.3.3 DCOM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.4 Devices

This section contains recommendations related to managing devices.

2.3.5 Domain controller

This section contains recommendations related to Domain Controllers.

2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu.

The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Impact:

None - this is the default behavior. Note that users (including those in the Server Operators group) are still able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:SubmitControl
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Allow server operators to
schedule tasks
```

Default Value:

Disabled. (Server Operators are not allowed to submit jobs by means of the AT schedule facility.)

2.3.5.2 (L1) Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether the domain controller bypasses secure RPC for Netlogon secure channel connections for specified machine accounts.

When deployed, this policy should be applied to all domain controllers in a forest by enabling the policy on the domain controllers OU.

When the `Create Vulnerable Connections` list (allow list) is configured:

- Given allow permission, the domain controller will allow accounts to use a Netlogon secure channel without secure RPC.
- Given deny permission, the domain controller will require accounts to use a Netlogon secure channel with secure RPC which is the same as the default (not necessary).

Note: Warning from Microsoft - enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to risk. This policy should be used as a temporary measure for 3rd-party devices as you deploy updates. Once a 3rd-party device is updated to support using secure RPC with Netlogon secure channels, the account should be removed from the Create Vulnerable Connections list. To better understand the risk of configuring accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472.

The recommended state for this setting is: `Not Configured`.

Rationale:

Enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to security risks. It is highly recommended that this setting not be used (i.e. be left completely unconfigured) so as not to add risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Vuln
erableChannelAllowList
```

Note: If this policy is set as prescribed, the registry key `vulnerablechannelallowlist`, will not be present in the above registry location.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Not Configured`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Allow vulnerable Netlogon secure
channel connections
```

Default Value:

Not Configured. (No machines or trust accounts are explicitly exempt from secure RPC with Netlogon secure channel connections enforcement.)

References:

1. https://go.microsoft.com/fwlink/?linkid=2133485

2.3.5.3 (L1) Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This setting determines whether the LDAP server (Domain Controller) enforces validation of Channel Binding Tokens (CBT) received in LDAP bind requests that are sent over SSL/TLS (i.e. LDAPS).

The recommended state for this setting is: `Always`.

Note: All LDAP clients must have the CVC-2017-8563 security update to be compatible with Domain Controllers that have this setting enabled. More information on this setting is available at: MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows

Rationale:

Requiring Channel Binding Tokens (CBT) can prevent an attacker who is able to capture users' authentication credentials (e.g. OAuth tokens, session identifiers, etc.) from reusing those credentials in another TLS session. This also helps to increase protection against "man-in-the-middle" attacks using LDAP authentication over SSL/TLS (LDAPS).

Impact:

All LDAP clients must provide channel binding information over SSL/TLS (i.e. LDAPS). The LDAP server (Domain Controller) rejects authentication requests from clients that do not do so. Clients must have the [CVC-2017-8563]() security update to support this feature, and may have compatibility issues with this setting without the security update. This may also mean that LDAP authentication requests over SSL/TLS that previously worked may stop working until the security update is installed.

When first deploying this setting, you may **initially** want to only set it to the alternate setting of `When supported` (instead of `Always`) on all Domain Controllers. This alternate, **interim** setting enables support for LDAP client channel binding but does not *require* it. Then set one DC that is not currently being targeted by LDAP clients to `Always`, and test each of the critical LDAP clients against that DC (and remediating as necessary), before deploying `Always` to the rest of the DCs.

We also recommend using the new Event ID 3039 on your Domain Controllers (added with the March 2020 security update) to help locate clients that do not use Channel Binding Tokens (CBT) in their LDAPS connections. This new Event ID requires increasing the logging level of the `16 LDAP Interface Events` portion of the NTDS service diagnostics to a value of `2` (Basic). For more information, please see *Table 2: CBT events* at this link: [MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows]()

Older OSes such as Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008 (non-R2), will first require patches for [Microsoft Security Advisory 973811](), as well as all associated fixes, in order to be compatible with domain controllers that have this setting deployed.

Note: Only `Always` is actually considered compliant to the CIS benchmark.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LdapEnfo
rceChannelBinding
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Always`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: LDAP server channel binding
token requirements
```

Note: This Group Policy path requires the installation of the March 2020 (or later) Windows security update. With that update, Microsoft added this setting to the built-in OS security template.

Default Value:

Never. (No LDAP channel binding validation is performed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

2.3.5.4 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing.

The recommended state for this setting is: `Require signing`.

Note: Domain member computers must have *Network security: LDAP signing requirements* (Rule 2.3.11.8) set to `Negotiate signing` or higher. If not, they will fail to authenticate once the above `Require signing` value is configured on the Domain Controllers. Fortunately, `Negotiate signing` is the default in the client configuration.

Note #2: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are shipped with Windows XP Professional use LDAP simple bind or LDAP simple bind through SSL to talk to a Domain Controller.

Note #3: Before enabling this setting, you should first ensure that there are no clients (including server-based applications) that are configured to authenticate with Active Directory via unsigned LDAP, because changing this setting will break those applications. Such applications should first be reconfigured to use signed LDAP, Secure LDAP (LDAPS), or IPsec-protected connections. For more information on how to identify whether your DCs are being accessed via unsigned LDAP (and where those accesses are coming from), see this Microsoft TechNet blog article: Identifying Clear Text LDAP binds to your DC's – Practical Windows Security

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Additionally, allowing the use of regular, unsigned LDAP permits credentials to be received over the network in clear text, which could very easily result in the interception of account passwords by other systems on the network.

Impact:

Unless TLS/SSL is being used, the LDAP data signing option must be negotiated. Clients that do not support LDAP signing will be unable to run LDAP queries against the Domain Controllers. All Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see Microsoft Knowledge Base article 325465: Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools. Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LDAPServ
erIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require signing`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: LDAP server signing requirements
```

Default Value:

None. (Data signing is not required in order to bind with the server. If the client requests data signing, the server supports it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.5.5 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether Domain Controllers will refuse requests from member computers to change computer account passwords.

The recommended state for this setting is: `Disabled`.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

If you enable this policy setting on all Domain Controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Refu
sePasswordChange
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Refuse machine account password
changes
```

Default Value:

Disabled. (By default, member computers change their computer account passwords as specified by the *Domain member: Maximum machine account password age* setting (Rule 2.3.6.5), which is by default every 30 days.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.6 Domain member

This section contains recommendations related to domain membership.

2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted.

The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on Domain Controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

- The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- The ability to authenticate other domains' users from a Domain Controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.

You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and Domain Controllers from trusted/trusting domains to Windows NT 4.0 with SP6a.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Requ
ireSignOrSeal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally encrypt or sign secure
channel data (always)
```

Default Value:

Enabled. (All secure channel data must be signed or encrypted.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates.

The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Seal
SecureChannel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally encrypt secure channel
data (when possible)
```

Default Value:

Enabled. (The domain member will request encryption of all secure channel traffic.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.

The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Sign
SecureChannel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally sign secure channel data
(when possible)
```

Default Value:

Enabled. (The domain member will request digital signing of all secure channel traffic.)

2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member can periodically change its computer account password. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account.

The recommended state for this setting is: `Disabled`.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

The default configuration for Windows Server 2003-based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Disa
blePasswordChange
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Disable machine account password
changes
```

Default Value:

Disabled. (The domain member can change its computer account password as specified by the recommendation *Domain Member: Maximum machine account password age*, which by default is every 30 days.)

2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days.

The recommended state for this setting is: `30 or fewer days, but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables maximum password age.

Note #2: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the passwords of computer accounts.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:Maxi
mumPasswordAge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `30 or fewer days, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Maximum machine account password age
```

Default Value:

30 days.

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

2.3.7.1 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

The recommended state for this setting is: `900 or fewer second(s), but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables the machine inactivity limit.

Rationale:

If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Impact:

The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
InactivityTimeoutSecs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `900 or fewer seconds, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Machine inactivity limit
```

Default Value:

0 seconds. (There is no inactivity limit).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.7.2 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Impact:

Users will have to acknowledge a dialog box containing the configured text before they can log on to the computer.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeText
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Message text for users
attempting to log on
```

Default Value:

No message.

2.3.7.3 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Impact:

Users will have to acknowledge a dialog box with the configured title before they can log on to the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeCaption
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Message title for users
attempting to log on
```

Default Value:

No message.

2.3.7.4 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire.

The recommended state for this setting is: `between 5 and 14 days`.

Rationale:

It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Impact:

Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:PasswordExpiryWarning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to a value `between 5 and 14 days`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Prompt user to change password
before expiration
```

Default Value:

5 days.

2.3.8 Microsoft network client

This section contains recommendations related to configuring the Microsoft network client.

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether packet signing is required by the SMB client component.

Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, **Microsoft network server: Digitally sign communications (always)**, on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.

The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network client will not communicate with a Microsoft network server unless that server agrees to perform SMB packet signing.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network client: Digitally sign
communications (always)
```

Default Value:

Disabled. (SMB packet signing is negotiated between the client and server.)

2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing.

Note: Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

None - this is the default behavior.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parame
ters:EnableSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network client: Digitally sign
communications (if server agrees)
```

Default Value:

Enabled. (The Microsoft network client will ask the server to perform SMB packet signing upon session setup. If packet signing has been enabled on the server, packet signing will be negotiated.)

2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption.

It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.

The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services, which is a significant security risk. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

Impact:

None - this is the default behavior.

Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parame
ters:EnablePlainTextPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network client: Send unencrypted password
to third-party SMB servers
```

Default Value:

Disabled. (Plaintext passwords will not be sent during authentication to third-party SMB servers that do not support password encryption.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

2.3.9 Microsoft network server

This section contains recommendations related to configuring the Microsoft network server.

2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The maximum value is 99999, which is over 69 days; in effect, this value disables the setting.

The recommended state for this setting is: `15 or fewer minute(s)`.

Rationale:

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Impact:

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
AutoDisconnect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `15 or fewer minute(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Amount of idle time
required before suspending session
```

Default Value:

15 minutes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.

The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Digitally sign
communications (always)
```

Default Value:

On Member Servers: Disabled. (SMB packet signing is negotiated between the client and server.)

On Domain Controllers: Enabled. (The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.)

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the **Microsoft network server: Digitally sign communications (always)** setting is not enabled.

Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
EnableSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Digitally sign
communications (if client agrees)
```

Default Value:

On Member Servers: Disabled. (The SMB client will never negotiate SMB packet signing.)

On Domain Controllers: Enabled. (The Microsoft network server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated.)

2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Network security: Force logoff when logon hours expire* (Rule 2.3.11.6).

If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective.

The recommended state for this setting is: `Enabled`.

Rationale:

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Impact:

None - this is the default behavior. If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
enableforcedlogoff
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Disconnect clients when
logon hours expire
```

Default Value:

Enabled. (Client sessions with the SMB service are forcibly disconnected when the client's logon hours expire.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol.

The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2.

The recommended state for this setting is: `Accept if provided by client`. Configuring this setting to `Required from client` also conforms to the benchmark.

Note: Since the release of the MS KB3161561 security patch, this setting can cause significant issues (such as replication problems, group policy editing issues and blue screen crashes) on Domain Controllers when used *simultaneously* with UNC path hardening (i.e. Rule 18.5.14.1). **CIS therefore recommends against deploying this setting on Domain Controllers.**

Rationale:

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Impact:

All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

If configured to `Accept if provided by client`, the SMB server will accept and validate the SPN provided by the SMB client and allow a session to be established if it matches the SMB server’s list of SPN’s for itself. If the SPN does NOT match, the session request for that SMB client will be denied.

If configured to `Required from client`, the SMB client MUST send a SPN name in session setup, and the SPN name provided MUST match the SMB server that is being requested to establish a connection. If no SPN is provided by client, or the SPN provided does not match, the session is denied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
SMBServerNameHardeningLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Accept if provided by client` (configuring to `Required from client` also conforms to the benchmark):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Server SPN target name
validation level
```

Default Value:

Off. (The SPN is not required or validated by the SMB server from a SMB client.)

2.3.10 Network access

This section contains recommendations related to network access.

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name.

The recommended state for this setting is: `Disabled`.

Rationale:

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:TurnOffAnonymousBlock
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Allow anonymous SID/Name
translation
```

Default Value:

Disabled. (An anonymous user cannot request the SID attribute for another user.)

2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections.

The recommended state for this setting is: `Enabled`.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow anonymous enumeration
of SAM accounts
```

Default Value:

Enabled. (Do not allow anonymous enumeration of SAM accounts. This option replaces Everyone with Authenticated Users in the security permissions for resources.)

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment.

The recommended state for this setting is: `Enabled`.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, `ANONYMOUS LOGON`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow anonymous enumeration
of SAM accounts and shares
```

Default Value:

Disabled. (Allow anonymous enumeration of SAM accounts and shares. No additional permissions can be assigned by the administrator for anonymous connections to the computer. Anonymous connections will rely on default permissions.)

2.3.10.4 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what additional permissions are assigned for anonymous connections to the computer.

The recommended state for this setting is: `Disabled`.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:EveryoneIncludesAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Let Everyone permissions apply to
anonymous users
```

Default Value:

Disabled. (Anonymous users can only access those resources for which the built-in group `ANONYMOUS LOGON` has been explicitly given permission.)

2.3.10.5 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: `LSARPC, NETLOGON, SAMR` and (when the legacy *Computer Browser* service is enabled) `BROWSER`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the `HydraLSPipe` and `TermServLicensing` Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The `BROWSER` named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionPipes
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Named Pipes that can be accessed
anonymously
```

Default Value:

None.

2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: `<blank>` (i.e. None), or (when the legacy *Computer Browser* service is enabled) `BROWSER`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the `HydraLSPipe` and `TermServLicensing` Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The `BROWSER` named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionPipes
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Named Pipes that can be accessed
anonymously
```

Default Value:

None.

2.3.10.7 (L1) Configure 'Network access: Remotely accessible registry paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2).

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
```

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\
AllowedExactPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to:

```
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
```

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Remotely accessible registry paths
```

Default Value:

System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion

2.3.10.8 (L1) Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008 (non-R2), and Windows Server 2003 does not exist in Windows XP.

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

The recommended state for servers that hold the *Active Directory Certificate Services* Role with *Certification Authority* Role Service includes the above list and:

```
System\CurrentControlSet\Services\CertSvc
```

The recommended state for servers that have the *WINS Server* Feature installed includes the above list and:

```
System\CurrentControlSet\Services\WINS
```

Rationale:

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\
AllowedPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Remotely accessible registry paths
and sub-paths
```

When a server holds the *Active Directory Certificate Services* Role with *Certification Authority* Role Service, the above list should also include:

`System\CurrentControlSet\Services\CertSvc`.

When a server has the *WINS Server* Feature installed, the above list should also include:

`System\CurrentControlSet\Services\WINS`

Default Value:

System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog

2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings. This policy setting controls null session access to shares on your computers by adding `RestrictNullSessAccess` with the value `1` in the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
```

registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources.

The recommended state for this setting is: `Enabled`.

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Impact:

None - this is the default behavior. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the **Network access: Named pipes that can be accessed anonymously** list:

- COMNAP: SNA session access
- COMNODE: SNA session access
- SQL\QUERY: SQL instance access
- SPOOLSS: Spooler service
- LLSRPC: License Logging service
- NETLOGON: Net Logon service
- LSARPC: LSA access
- SAMR: Remote access to SAM objects
- BROWSER: Computer Browser service

Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
RestrictNullSessAccess
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Restrict anonymous access to Named
Pipes and Shares
```

Default Value:

Enabled. (Anonymous access is restricted to shares and pipes listed in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings.)

2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows you to restrict remote RPC connections to SAM.

The recommended state for this setting is: `Administrators: Remote Access: Allow`.

Note: A Windows 10 R1607, Server 2016 or newer OS is required to access and set this value in Group Policy.

Note #2: If your organization is using Azure Advanced Threat Protection (APT), the service account, “AATP Service” will need to be added to the recommendation configuration. For more information on adding the “AATP Service” account please see Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity | Microsoft Docs.

Rationale:

To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators: Remote Access: Allow`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Restrict clients allowed to make
remote calls to SAM
```

Default Value:

Administrators: Remote Access: Allow.

2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

The recommended state for this setting is: `<blank>` (i.e. None).

Rationale:

It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionShares
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<blank>` (i.e. None):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Shares that can be accessed
anonymously
```

Default Value:

None. (Only authenticated users will have access to all shared resources on the server.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource.

The recommended state for this setting is: `Classic - local users authenticate as themselves`.

Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale:

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:ForceGuest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Classic - local users authenticate as themselves`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Sharing and security model for
local accounts
```

Default Value:

On domain-joined computers: Classic - local users authenticate as themselves. (Network logons that use local account credentials authenticate by using those credentials.)

On stand-alone computers: Guest only - local users authenticate as Guest. (Network logons that use local accounts are automatically mapped to the Guest account.)

2.3.11 Network security

This section contains recommendations related to network security.

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2.

The recommended state for this setting is: `Enabled`.

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Impact:

Services running as Local System that use Negotiate when reverting to NTLM authentication will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Allow Local System to use
computer identity for NTLM
```

Default Value:

Disabled. (Services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously.)

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem.

The recommended state for this setting is: `Disabled`.

Rationale:

NULL sessions are less secure because by definition they are unauthenticated.

Impact:

Any applications that require NULL sessions for LocalSystem will not work as designed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AllowNullSessionFallback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback
```

Default Value:

On Windows Server 2008 (non-R2): Enabled. (NTLM will be permitted to fall back to a NULL session when used with LocalSystem.)

On Windows Server 2008 R2 and newer: Disabled. (NTLM will not be permitted to fall back to a NULL session when used with LocalSystem.)

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines if online identities are able to authenticate to this computer.

The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called HomeGroup, which permits sharing between computers that are not members of a domain.

With PKU2U, a new extension was introduced to the Negotiate authentication package, `Spnego.dll`. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, `Negoexts.dll`, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U.

When computers are configured to accept authentication requests by using online IDs, `Negoexts.dll` calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes.

The recommended state for this setting is: `Disabled`.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network Security: Allow PKU2U authentication
requests to this computer to use online identities
```

Default Value:

Disabled. (Online identities will not to be allowed to authenticate to a domain-joined machine.)

2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to set the encryption types that Kerberos is allowed to use.

The recommended state for this setting is: `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.`

Note: Some legacy applications and OSes may still require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Rationale:

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Note: Some legacy applications and OSes may still require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Note #2: Windows Server 2008 (non-R2) and below allow DES for Kerberos by default, but later OS versions do not.

Note #3: Some prerequisites might need to be met on Domain Controllers to support Kerberos AES 128 and 256 bit encryption types, as well as enabling support for Kerberos AES 128 and 256 bit on user accounts (in account options) for this recommendation to work correctly.

Note #4: If your organization uses Azure Files, please note that Microsoft did not introduce AES 256 Kerberos encryption support for it until AD DS authentication module v0.2.2. Please see this link for more information:

Azure Files on-premises AD DS Authentication support for AES 256 Kerberos encryption | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
Kerberos\Parameters:SupportedEncryptionTypes
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Configure encryption types
allowed for Kerberos
```

Default Value:

RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Since LM hashes are stored on the local computer in the security database, passwords can then be easily compromised if the database is attacked.

Note: Older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after you enable this setting to gain the proper benefit.

The recommended state for this setting is: `Enabled`.

Rationale:

The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

Impact:

None - this is the default behavior. Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:NoLMHash
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Do not store LAN Manager hash
value on next password change
```

Default Value:

Enabled. (LAN Manager hash values are not stored when passwords are changed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

2.3.11.6 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

LAN Manager (LM) was a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP
- Authenticate to computers that are not in the domain

The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.

The recommended state for this setting is: `Send NTLMv2 response only. Refuse LM & NTLM`.

Rationale:

Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default settings in OSes predating Windows Vista / Windows Server 2008 (non-R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for attackers to sniff that traffic to more easily reproduce the user's password.

The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for older clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or newer Domain Controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

Impact:

Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers refuse LM and NTLM (accept only NTLMv2 authentication). Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Send NTLMv2 response only. Refuse LM & NTLM`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LAN Manager authentication level
```

Default Value:

Send NTLMv2 response only. (Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers accept LM, NTLM & NTLMv2 authentication.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.7 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests.

Note: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are included with Windows XP Professional use `ldap_simple_bind` or `ldap_simple_bind_s` to communicate with a Domain Controller.

The recommended state for this setting is: `Negotiate signing`. Configuring this setting to `Require signing` also conforms to the benchmark.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Impact:

None - this is the default behavior. However, if you choose instead to configure the server to *require* LDAP signatures then you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts, because the caller will be told that the LDAP BIND command request failed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Negotiate signing` (configuring to `Require signing` also conforms to the benchmark):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LDAP client signing requirements
```

Default Value:

Negotiate signing. (If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.8 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: `Require NTLMv2 session security, Require 128-bit encryption`.

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

You can enable both options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClientS
ec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Minimum session security for NTLM
SSP based (including secure RPC) clients
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 and newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: `Require NTLMv2 session security, Require 128-bit encryption`.

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinServerS
ec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Minimum session security for NTLM
SSP based (including secure RPC) servers
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 and newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.12 Recovery console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.13 Shutdown

This section contains recommendations related to the Windows shutdown functionality.

2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system.

The recommended state for this setting is: `Disabled`.

Note: In Server 2008 R2 and older versions, this setting had no impact on Remote Desktop (RDP) / Terminal Services sessions - it only affected the local console. However, Microsoft changed the behavior in Windows Server 2012 (non-R2) and above, where if set to Enabled, RDP sessions are also allowed to shut down or restart the server.

Rationale:

Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable. As noted in the Description above, the Denial of Service (DoS) risk of enabling this setting dramatically increases in Windows Server 2012 (non-R2) and above, as even remote users could then shut down or restart the server from the logon screen of an RDP session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
ShutdownWithoutLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Shutdown: Allow system to be shut down without
having to log on
```

Default Value:

Disabled. (Operators will have to log on to servers to shut them down or restart them.)

2.3.14 System cryptography

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.15 System objects

This section contains recommendations related to system objects.

2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available.

The recommended state for this setting is: `Enabled`.

Rationale:

Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel:ObCaseInsensitive
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Require case insensitivity for non-
Windows subsystems
```

Default Value:

Enabled. (All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.)

2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted.

The recommended state for this setting is: `Enabled`.

Rationale:

This setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager:ProtectionMode
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Strengthen default permissions of
internal system objects (e.g. Symbolic Links)
```

Default Value:

Enabled. (The default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create.)

2.3.16 System settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.17 User Account Control

This section contains recommendations related to User Account Control.

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.

The recommended state for this setting is: `Enabled`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista and newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Impact:

The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
FilterAdministratorToken
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Admin Approval Mode for the
Built-in Administrator account
```

Default Value:

Disabled. (The built-in Administrator account runs all applications with full administrative privilege.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of the elevation prompt for administrators.

The recommended state for this setting is: `Prompt for consent on the secure desktop`.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Impact:

When an operation (including execution of a Windows binary) requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
ConsentPromptBehaviorAdmin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Prompt for consent on the secure desktop`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Behavior of the elevation
prompt for administrators in Admin Approval Mode
```

Default Value:

Prompt for consent for non-Windows binaries. (When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.)

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of the elevation prompt for standard users.

The recommended state for this setting is: `Automatically deny elevation requests`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Impact:

When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.

Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is "*This program will not run. This program is blocked by group policy. For more information, contact your system administrator.*" Some users who are not used to seeing this message may believe that the operation or program they attempted to run is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it *is* already an Administrator account), and they are not doing that.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
ConsentPromptBehaviorUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Automatically deny elevation requests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Behavior of the elevation
prompt for standard users
```

Default Value:

Prompt for credentials. (When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.)

2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of application installation detection for the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

Impact:

When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableInstallerDetection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Detect application
installations and prompt for elevation
```

Default Value:

Disabled. (Default for enterprise. Application installation packages are not detected and prompted for elevation.)

2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- `…\Program Files\`, including subfolders
- `…\Windows\System32\`
- `…\Program Files (x86)\`, including subfolders (for 64-bit versions of Windows)

Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting.

The recommended state for this setting is: `Enabled`.

Rationale:

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities:

- To set the foreground window.
- To drive any application window using SendInput function.
- To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.
- To set journal hooks.
- To uses AttachThreadInput to attach a thread to a higher integrity input queue.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableSecureUIAPaths
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Only elevate UIAccess
applications that are installed in secure locations
```

Default Value:

Enabled. (If an application resides in a secure location in the file system, it runs only with UIAccess integrity.)

2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer.

The recommended state for this setting is: `Enabled`.

Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Rationale:

This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

Impact:

None - this is the default behavior. Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableLUA
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Run all administrators in
Admin Approval Mode
```

Default Value:

Enabled. (Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.)

2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.

The recommended state for this setting is: `Enabled`.

Rationale:

Standard elevation prompt dialog boxes can be spoofed, which may cause users to disclose their passwords to malicious software. The secure desktop presents a very distinct appearance when prompting for elevation, where the user desktop dims, and the elevation prompt UI is more prominent. This increases the likelihood that users who become accustomed to the secure desktop will recognize a spoofed elevation prompt dialog box and not fall for the trick.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
PromptOnSecureDesktop
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Switch to the secure desktop
when prompting for elevation
```

Default Value:

Enabled. (All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.)

2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to:

- `%ProgramFiles%`
- `%windir%`
- `%windir%\System32`
- `HKEY_LOCAL_MACHINE\SOFTWARE`

The recommended state for this setting is: `Enabled`.

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableVirtualization
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Virtualize file and registry
write failures to per-user locations
```

Default Value:

Enabled. (Application write failures are redirected at run time to defined user locations for both the file system and registry.)

3 Event Log

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

4 Restricted Groups

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

5 System Services

This section contains recommendations for system services.

5.1 (L1) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability (CVE-2021-34527) and other attacks against the service.

Impact:

Domain Controllers will not be able to prune published printers from Active Directory. By default, Domain Controllers prune printer objects from Active Directory if the computer that published them doesn't respond to contact requests.

Domain Controllers will not be able to act as a print server, sharing printers for clients.

Applications on and users logged in at Domain Controllers will not be able to print, including printing to files (such as Adobe Portable Document Format (PDF)) which uses the Print Spooler service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\System
Services\Print Spooler
```

Default Value:

Automatic

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

6 Registry

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

7 File System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

8 Wired Network (IEEE 802.3) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

This section contains recommendations for configuring the Windows Firewall.

Note: In older versions of Microsoft Windows, this section was named *Windows Firewall with Advanced Security*, but it was renamed to *Windows Defender Firewall with Advanced Security* starting with the Server 2019 release.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:
EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:
DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SystemRoot%\System32\logfiles\firewall\domainfw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\domainfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size
limit (KB)
```

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log
dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log
successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.2 Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SystemRoot%\System32\logfiles\firewall\privatefw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\privatefw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Size
limit (KB)
```

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Log
dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Log
successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.3 Public Profile

This section contains recommendations for the Public Profile of the Windows Firewall.

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.4 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SystemRoot%\System32\logfiles\firewall\publicfw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\publicfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.3.5 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Size
limit (KB)
```

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Log
dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Log
successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

10 Network List Manager Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

11 Wireless Network (IEEE 802.11) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

12 Public Key Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

13 Software Restriction Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

14 Network Access Protection NAP Client Configuration

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

15 Application Control Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

16 IP Security Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

17 Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

17.1 Account Logon

This section contains recommendations for configuring the Account Logon audit policy.

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the Domain Controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the Domain Controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include:

- 4774: An account was mapped for logon.
- 4775: An account could not be mapped for logon.
- 4776: The Domain Controller attempted to validate the credentials for an account.
- 4777: The Domain Controller failed to validate the credentials for an account.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential
Validation
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.12 Monitor Attempts to Access Deactivated Accounts Monitor attempts to access deactivated accounts through audit logging.		●	●

17.1.2 (L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports the results of events generated after a Kerberos authentication TGT request. Kerberos is a distributed authentication service that allows a client running on behalf of a user to prove its identity to a server without sending data across the network. This helps mitigate an attacker or server from impersonating a user.

- 4768: A Kerberos authentication ticket (TGT) was requested.
- 4771: Kerberos pre-authentication failed.
- 4772: A Kerberos authentication ticket request failed.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos
Authentication Service
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2 Account Management

This section contains recommendations for configuring the Account Management audit policy.

17.2.1 (L1) Ensure 'Audit Computer Account Management' is set to include 'Success and Failure' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include:

- 4741: A computer account was created.
- 4742: A computer account was changed.
- 4743: A computer account was deleted.

The recommended state for this setting is to include: `Success and Failure`.

Rationale:

Auditing events in this category may be useful when investigating an incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Computer
Account Management
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.2 (L1) Ensure 'Audit Distribution Group Management' is set to include 'Success and Failure' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include:

- 4744: A security-disabled local group was created.
- 4745: A security-disabled local group was changed.
- 4746: A member was added to a security-disabled local group.
- 4747: A member was removed from a security-disabled local group.
- 4748: A security-disabled local group was deleted.
- 4749: A security-disabled global group was created.
- 4750: A security-disabled global group was changed.
- 4751: A member was added to a security-disabled global group.
- 4752: A member was removed from a security-disabled global group.
- 4753: A security-disabled global group was deleted.
- 4759: A security-disabled universal group was created.
- 4760: A security-disabled universal group was changed.
- 4761: A member was added to a security-disabled universal group.
- 4762: A member was removed from a security-disabled universal group.
- 4763: A security-disabled universal group was deleted.

The recommended state for this setting is to include: `Success and Failure`.

Rationale:

Auditing these events may provide an organization with insight when investigating an incident. For example, when a given unauthorized user was added to a sensitive distribution group.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit
Distribution Group Management
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.3 (L1) Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports other account management events. Events for this subcategory include:

- 4782: The password hash an account was accessed.
- 4793: The Password Policy Checking API was called.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Other
Account Management Events
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.4 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include:

- 4727: A security-enabled global group was created.
- 4728: A member was added to a security-enabled global group.
- 4729: A member was removed from a security-enabled global group.
- 4730: A security-enabled global group was deleted.
- 4731: A security-enabled local group was created.
- 4732: A member was added to a security-enabled local group.
- 4733: A member was removed from a security-enabled local group.
- 4734: A security-enabled local group was deleted.
- 4735: A security-enabled local group was changed.
- 4737: A security-enabled global group was changed.
- 4754: A security-enabled universal group was created.
- 4755: A security-enabled universal group was changed.
- 4756: A member was added to a security-enabled universal group.
- 4757: A member was removed from a security-enabled universal group.
- 4758: A security-enabled universal group was deleted.
- 4764: A group's type was changed.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Security
Group Management
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

17.2.5 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include:

- 4720: A user account was created.
- 4722: A user account was enabled.
- 4723: An attempt was made to change an account's password.
- 4724: An attempt was made to reset an account's password.
- 4725: A user account was disabled.
- 4726: A user account was deleted.
- 4738: A user account was changed.
- 4740: A user account was locked out.
- 4765: SID History was added to an account.
- 4766: An attempt to add SID History to an account failed.
- 4767: A user account was unlocked.
- 4780: The ACL was set on accounts which are members of administrators groups.
- 4781: The name of an account was changed:
- 4794: An attempt was made to set the Directory Services Restore Mode.
- 5376: Credential Manager credentials were backed up.
- 5377: Credential Manager credentials were restored from a backup.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit User
Account Management
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.3 Detailed Tracking

This section contains recommendations for configuring the Detailed Tracking audit policy.

17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit when plug and play detects an external device.

The recommended state for this setting is to include: `Success`.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

Enabling this setting will allow a user to audit events when a device is plugged into a system. This can help alert IT staff if unapproved devices are plugged in.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP
Activity
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include:

- 4688: A new process has been created.
- 4696: A primary token was assigned to process.

Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process
Creation
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.4 DS Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include:

- 4625: An account failed to log on.

The recommended state for this setting is to include: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy allows you to audit the group membership information in the user’s logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.

The recommended state for this setting is to include: `Success`.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4634: An account was logged off.
- 4647: User initiated logoff.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4624: An account was successfully logged on.
- 4625: An account failed to log on.
- 4648: A logon was attempted using explicit credentials.
- 4675: SIDs were filtered.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
```

Default Value:

Success and Failure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other logon/logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include:

- 4649: A replay attack was detected.
- 4778: A session was reconnected to a Window Station.
- 4779: A session was disconnected from a Window Station.
- 4800: The workstation was locked.
- 4801: The workstation was unlocked.
- 4802: The screen saver was invoked.
- 4803: The screen saver was dismissed.
- 5378: The requested credentials delegation was disallowed by policy.
- 5632: A request was made to authenticate to a wireless network.
- 5633: A request was made to authenticate to a wired network.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other
Logon/Logoff Events
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include:

- 4964 : Special groups have been assigned to a new logon.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.6 Object Access

This section contains recommendations for configuring the Object Access audit policy.

17.6.1 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit events generated by the management of task scheduler jobs or COM+ objects.

For scheduler jobs, the following are audited:

- Job created.
- Job deleted.
- Job enabled.
- Job disabled.
- Job updated.

For COM+ objects, the following are audited:

- Catalog object added.
- Catalog object updated.
- Catalog object deleted.

The recommended state for this setting is: `Success and Failure`.

Rationale:

The unexpected creation of scheduled tasks and COM+ objects could potentially be an indication of malicious activity. Since these types of actions are generally low volume, it may be useful to capture them in the audit logs for use during an investigation.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object
Access Events
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.6.2 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage.

The recommended state for this setting is: `Success and Failure`.

Note: A Windows 8.0, Server 2012 (non-R2) or newer OS is required to access and set this value in Group Policy.

Rationale:

Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Removable
Storage
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7 Policy Change

This section contains recommendations for configuring the Policy Change audit policy.

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include:

- 4715: The audit policy (SACL) on an object was changed.
- 4719: System audit policy was changed.
- 4902: The Per-user audit policy table was created.
- 4904: An attempt was made to register a security event source.
- 4905: An attempt was made to unregister a security event source.
- 4906: The CrashOnAuditFail value has changed.
- 4907: Auditing settings on object were changed.
- 4908: Special Groups Logon table modified.
- 4912: Per User Audit Policy was changed.

The recommended state for this setting is include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy
Change
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in authentication policy. Events for this subcategory include:

- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4713: Kerberos policy was changed.
- 4716: Trusted domain information was modified.
- 4717: System security access was granted to an account.
- 4718: System security access was removed from an account.
- 4739: Domain Policy was changed.
- 4864: A namespace collision was detected.
- 4865: A trusted forest information entry was added.
- 4866: A trusted forest information entry was removed.
- 4867: A trusted forest information entry was modified.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication
Policy Change
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.3 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe). Events for this subcategory include:

- 4944: The following policy was active when the Windows Firewall started.
- 4945: A rule was listed when the Windows Firewall started.
- 4946: A change has been made to Windows Firewall exception list. A rule was added.
- 4947: A change has been made to Windows Firewall exception list. A rule was modified.
- 4948: A change has been made to Windows Firewall exception list. A rule was deleted.
- 4949: Windows Firewall settings were restored to the default values.
- 4950: A Windows Firewall setting has changed.
- 4951: A rule has been ignored because its major version number was not recognized by Windows Firewall.
- 4952: Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
- 4953: A rule has been ignored by Windows Firewall because it could not parse the rule.
- 4954: Windows Firewall Group Policy settings have changed. The new settings have been applied.
- 4956: Windows Firewall has changed the active profile.
- 4957: Windows Firewall did not apply the following rule.
- 4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

The recommended state for this setting is : `Success and Failure`

Rationale:

Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-
Level Policy Change
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

Auditing this subcategory will create a high volume of events. Events for this subcategory include:

- 4672: Special privileges assigned to new logon.
- 4673: A privileged service was called.
- 4674: An operation was attempted on a privileged object.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive
Privilege Use
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9 System

This section contains recommendations for configuring the System audit policy.

17.9.1 (L1) Ensure 'Audit Security State Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include:

- 4608: Windows is starting up.
- 4609: Windows is shutting down.
- 4616: The system time was changed.
- 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security State Change
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.2 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include:

- 4610: An authentication package has been loaded by the Local Security Authority.
- 4611: A trusted logon process has been registered with the Local Security Authority.
- 4614: A notification package has been loaded by the Security Account Manager.
- 4622: A security package has been loaded by the Local Security Authority.
- 4697: A service was installed in the system.

The recommended state for this setting is to include: `Success`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security System
Extension
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.3 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include:

- 4612 : Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- 4615 : Invalid use of LPC port.
- 4618 : A monitored security event pattern has occurred.
- 4816 : RPC detected an integrity violation while decrypting an incoming message.
- 5038 : Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
- 5056: A cryptographic self test was performed.
- 5057: A cryptographic primitive operation failed.
- 5060: Verification operation failed.
- 5061: Cryptographic operation.
- 5062: A kernel-mode cryptographic self test was performed.

The recommended state for this setting is: `Success and Failure`.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure:`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit System Integrity
```

Default Value:

Success and Failure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

18 Administrative Templates (Computer)

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

18.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.1 Personalization

This section contains recommendations for Control Panel personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen.

The recommended state for this setting is: `Enabled`.

Rationale:

Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

Impact:

If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLock
ScreenCamera
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Prevent enabling lock screen camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable invocation of an available camera on the lock screen.)

18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen.

The recommended state for this setting is: `Enabled`.

Rationale:

Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

Impact:

If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLock
ScreenSlideshow
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Prevent enabling lock screen slide show
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable a slide show that will run after they lock the machine.)

18.1.2 Regional and Language Options

This section contains recommendation settings for Regional and Language Options.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.2.1 Handwriting personalization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech.

The recommended state for this setting is: `Disabled`.

Rationale:

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInpu
tPersonalization
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Regional and Language Options\Allow users to enable online speech
recognition services
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow input personalization*, but it was renamed to *Allow users to enable online speech recognition services* starting with the Windows 10 R1809 & Server 2019 Administrative Templates.

Default Value:

Enabled. (Automatic learning of speech, inking and typing is enabled, but users may change this value via PC Settings.)

18.2 LAPS

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AdmPwd.admx/adml` that is included with LAPS.

18.3 MS Security Guide

This section contains settings for configuring additional settings from the MS Security Guide.

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available from Microsoft at this link.

18.3.1 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (`MRxSmb10`), which is recommended to be disabled.

The recommended state for this setting is: `Enabled: Disable driver (recommended)`.

Note: Do not, *under any circumstances*, configure this overall setting as `Disabled`, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable driver (recommended)`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure SMB v1 client driver
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

Windows Server 2008 (non-R2), 2008 R2, and 2012 (non-R2): Enabled: Manual start.

Windows Server 2012 R2 and Server 2016 (up to R1607): Enabled: Automatic start.

Windows Server 2016 R1709 and newer: Enabled: Disable driver.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.3.2 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol.

The recommended state for this setting is: `Disabled`.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:
SMB1
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure SMB v1 server
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

Windows Server 2016 R1607 and older: Enabled.

Windows Server 2016 R1709 and newer: Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.3.3 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). We recommend enabling this feature to improve the security profile of the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

This feature is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. This protection mechanism is provided at run-time. Therefore, it helps protect applications regardless of whether they have been compiled with the latest improvements, such as the /SAFESEH option.

Impact:

After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\kernel:DisableExceptionChainValidation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link. More information is available at MSKB 956607: How to enable Structured Exception Handling Overwrite Protection (SEHOP) in Windows operating systems

Default Value:

Disabled for 32-bit processes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.3.5 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This setting determines which method NetBIOS over TCP/IP (NetBT) uses to register and resolve names. The available methods are:

- The B-node (broadcast) method only uses broadcasts.
- The P-node (point-to-point) method only uses name queries to a name server (WINS).
- The M-node (mixed) method broadcasts first, then queries a name server (WINS) if broadcast failed.
- The H-node (hybrid) method queries a name server (WINS) first, then broadcasts if the query failed.

The recommended state for this setting is: `Enabled: P-node (recommended)` (point-to-point).

Note: Resolution through LMHOSTS or DNS follows these methods. If the `NodeType` registry value is present, it overrides any `DhcpNodeType` registry value. If neither `NodeType` nor `DhcpNodeType` is present, the computer uses B-node (broadcast) if there are no WINS servers configured for the network, or H-node (hybrid) if there is at least one WINS server configured.

Rationale:

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node (point-to-point) will prevent the system from sending out NetBIOS broadcasts.

Impact:

NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NodeType
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: P-node (recommended)`:

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\NetBT NodeType configuration
```

Note: This change does not take effect until the computer has been restarted.

Note #2: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link. Please note that this setting is **only** available in the *Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903* (or newer) release of `SecGuide.admx/adml`, so if you previously downloaded this template, you may need to update it from a newer Microsoft baseline to get this new *NetBT NodeType configuration* setting.

Default Value:

B-node (broadcast only) if a WINS server is not configured in NIC properties.

H-node (hybrid - point-to-point first, then broadcast) if a WINS server is configured in NIC properties.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.3.6 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server.

For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents.

For more information about `UseLogonCredential`, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014.

The recommended state for this setting is: `Disabled`.

Rationale:

Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Impact:

None - this is also the default configuration for Server 2012 R2 and newer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
:UseLogonCredential
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\WDigest Authentication (disabling may require KB2871997)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

On Server 2012 (non-R2) and older: Enabled. (Lsass.exe retains a copy of the user's plaintext password in memory, where it is at risk of theft.)

On Server 2012 R2 and newer: Disabled. (Lsass.exe does not retain a copy of the user's plaintext password in memory.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

18.4 MSS (Legacy)

This section contains recommendations for the Microsoft Solutions for Security (MSS) settings.

This Group Policy section is provided by the Group Policy template `MSS-legacy.admx/adml` that is available that is available from Microsoft at Download Microsoft Security Compliance Toolkit 1.0 from Official Microsoft Download Center.

18.4.1 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network.

The recommended state for this setting is: `Enabled: Highest protection, source routing is completely disabled`.

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters:Disabl
eIPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(DisableIPSourceRouting IPv6) IP source routing protection level (protects
against packet spoofing)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

No additional protection, source routed packets are allowed.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing.

The recommended state for this setting is: `Enabled: Highest protection, source routing is completely disabled`.

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Disable
IPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(DisableIPSourceRouting) IP source routing protection level (protects against
packet spoofing)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Medium, source routed packets ignored when IP forwarding is enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.4.3 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes.

The recommended state for this setting is: `Disabled`.

Rationale:

This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Impact:

When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableI
CMPRedirect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]()

Default Value:

Enabled. (ICMP redirects can override OSPF-generated routes.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.4.4 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request.

The recommended state for this setting is: `Enabled`.

Rationale:

The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries.

An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameR
eleaseOnDemand
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release
requests except from WINS servers
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5 Network

This section contains recommendations for network settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.1 Background Intelligent Transfer Service (BITS)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Bits.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.2 BranchCache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PeerToPeerCaching.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.3 DirectAccess Client Experience Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `nca.admx/adml` that is included with the Microsoft 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.4 DNS Client

This section contains recommendations related to DNS Client.

This Group Policy section is provided by the Group Policy template `DnsClient.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.4.1 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

The recommended state for this setting is: `Enabled`.

Rationale:

An attacker can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, tricking the host into thinking that it knows the location of the requested system.

Note: To completely mitigate local name resolution poisoning, in addition to this setting, the properties of each installed NIC should also be set to `Disable NetBIOS over TCP/IP` (on the WINS tab in the NIC properties). Unfortunately, there is no global setting to achieve this that automatically applies to all NICs - it is a per-NIC setting that varies with different NIC hardware installations.

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\DNSClient:EnableMulticast
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Turn off multicast name resolution
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (LLMNR will be enabled on all available network adapters.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.5 Fonts

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.5.6 Hotspot Authentication

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `hotspotauth.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.7 Lanman Server

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `LanmanServer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.8 Lanman Workstation

This section contains recommendations related to Lanman Workstation.

This Group Policy section is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.

The recommended state for this setting is: `Disabled`.

Rationale:

Insecure guest logons are used by file servers to allow unauthenticated access to shared folders.

Impact:

The SMB client will reject insecure guest logons. This was not originally the default behavior in older versions of Windows, but Microsoft changed the default behavior starting with Windows Server 2016 R1709: Guest access in SMB2 disabled by default in Windows 10 and Windows Server 2016

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:Allo
wInsecureGuestAuth
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman
Workstation\Enable insecure guest logons
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Server 2016 RTM (R1607) and older: Enabled. (The SMB client will allow insecure guest logons.)

Server 2016 R1709, Server 2019 and newer: Disabled. (The SMB client will reject insecure guest logons.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.9 Link-Layer Topology Discovery

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.10 Microsoft Peer-to-Peer Networking Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.11 Network Connections

This section contains recommendations for Network Connections settings.

This Group Policy section is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.11.1 Windows Defender Firewall (formerly Windows Firewall)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsFirewall.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Firewall* but was renamed by Microsoft to *Windows Defender Firewall* starting with the Microsoft Windows 10 Release 1709 Administrative Templates.

18.5.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

You can use this procedure to control a user's ability to install and configure a Network Bridge.

The recommended state for this setting is: `Enabled`.

Rationale:

The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A Network Bridge thus allows a computer that has connections to two different networks to share data between those networks.

In an enterprise managed environment, where there is a need to control network traffic to only authorized paths, allowing users to create a Network Bridge increases the risk and attack surface from the bridged network.

Impact:

Users cannot create or configure a Network Bridge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_AllowNetBridge_NLA
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Connections\Prohibit installation and configuration of Network Bridge on your
DNS domain network
```

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users are able create and modify the configuration of Network Bridges. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

18.5.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Although this "legacy" setting traditionally applied to the use of Internet Connection Sharing (ICS) in Windows 2000, Windows XP & Server 2003, this setting now freshly applies to the Mobile Hotspot feature in Windows 10 & Server 2016.

The recommended state for this setting is: `Enabled`.

Rationale:

Non-administrators should not be able to turn on the Mobile Hotspot feature and open their Internet connectivity up to nearby mobile devices.

Impact:

Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_ShowSharedAccessUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Connections\Prohibit use of Internet Connection Sharing on your DNS domain
network
```

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (All users are allowed to turn on Mobile Hotspot.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.12 Network Connectivity Status Indicator

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.13 Network Isolation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NetworkIsolation.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.14 Network Provider

This section contains recommendations for Network Provider settings.

This Group Policy section is provided by the Group Policy template `NetworkProvider.admx/adml` that is included with the MS15-011 / MSKB 3000483 security update and the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: `Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares`.

Note: If the environment exclusively contains Windows 8.0 / Server 2012 (non-R2) or newer systems, then the "`Privacy`" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the MS15-011 / MSKB 3000483 security update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (`NetworkProvider.admx/adml`) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
```

```
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1
```

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden
edPaths:\\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden
edPaths:\\*\SYSVOL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with the following paths configured, at a minimum:
`\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1`
`\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1`

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`NetworkProvider.admx/adml`) is required - it is included with the MS15-011 / MSKB 3000483 security update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (No UNC paths are hardened.)

18.5.15 Offline Files

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OfflineFiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.16 QoS Packet Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `QOS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.17 SNMP

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Snmp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.18 SSL Configuration Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CipherSuiteOrder.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.19 TCPIP Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.20 Windows Connect Now

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

This Group Policy section is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents computers from establishing multiple simultaneous connections to either the Internet or to a Windows domain.

The recommended state for this setting is: `Enabled: 1 = Minimize simultaneous connections'`.

Rationale:

Preventing bridged network connections can help prevent a user unknowingly allowing traffic to route between internal and external networks, which risks exposure to sensitive internal data.

Impact:

While connected to an Ethernet connection, Windows won't allow use of a WLAN (automatically *or* manually) until Ethernet is disconnected. However, if a cellular data connection is available, it will always stay connected for services that require it, but no Internet traffic will be routed over cellular if an Ethernet or WLAN connection is present.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMi
nimizeConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1 = Minimize simultaneous connections'`:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connection Manager\Minimize the number of simultaneous connections to the
Internet or a Windows Domain
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates. It was updated with a new *Minimize Policy Options* sub-setting starting with the Windows 10 Release 1903 Administrative Templates.

Default Value:

Enabled: 1 = Minimize simultaneous connections. (Any new automatic internet connection is blocked when the computer has at least one active internet connection to a preferred type of network. The order of preference (from most preferred to least preferred) is: Ethernet, WLAN, then cellular. Ethernet is always preferred when connected. Users can still manually connect to any network.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

18.6 Printers

This section contains recommendations for printer settings.

This Group Policy section is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting controls whether the Print Spooler service will accept client connections.

The recommended state for this setting is: `Disabled`.

Note: The Print Spooler service must be restarted for changes to this policy to take effect.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Rationale:

Disabling the ability for the Print Spooler service to accept client connections mitigates **remote** attacks against the PrintNightmare vulnerability (CVE-2021-34527) and other **remote** Print Spooler attacks. However, this recommendation *does not* mitigate against **local** attacks on the Print Spooler service.

Impact:

Provided that the Print Spooler service is not disabled, applications on and users logged in to servers will continue to be able to print *from the server*. However, the Print Spooler service will not accept client connections or allow users to share printers. Note that all printers that were already shared will continue to be shared.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows
NT\Printers:RegisterSpoolerRemoteRpcEndPoint
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Printers:Allow Print
Spooler to accept client connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing2.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (The Print Spooler will always accept client connections.)

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

18.7 Start Menu and Taskbar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.8 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.1 Access-Denied Assistance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.2 App-V

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `appv.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.8.3 Audit Process Creation

This section contains settings related to auditing of process creation events.

This Group Policy section is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the process creation command line text is logged in security audit events when a new process has been created.

The recommended state for this setting is: `Enabled`.

Note: This feature that this setting controls was not originally supported in server OSes older than Windows Server 2012 R2. However, in February 2015 Microsoft added support for the feature to Windows Server 2008 R2 and Windows Server 2012 (non-R2) via an update - KB3004375. Therefore, this setting is also important to set on those older OSes.

Rationale:

Capturing process command line information in event logs can be very valuable when performing forensic investigations of attack incidents.

Impact:

Process command line information will be included in the event logs, which can contain sensitive or private information such as passwords or user data.

Warning: There are potential risks of capturing credentials and sensitive information which could be exposed to users who have read-access to event logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: About Logging Windows - PowerShell | Microsoft Docs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
Audit:ProcessCreationIncludeCmdLine_Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Audit Process
Creation\Include command line in process creation events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The process's command line information will not be included in Audit Process Creation events.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

18.8.4 Credentials Delegation

This section contains settings related to Credential Delegation.

This Group Policy section is provided by the Group Policy template `CredSsp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Some versions of the CredSSP protocol that is used by some applications (such as Remote Desktop Connection) are vulnerable to an encryption oracle attack against the client. This policy controls compatibility with vulnerable clients and servers and allows you to set the level of protection desired for the encryption oracle vulnerability.

The recommended state for this setting is: `Enabled: Force Updated Clients`.

Rationale:

This setting is important to mitigate the CredSSP encryption oracle vulnerability, for which information was published by Microsoft on 03/13/2018 in CVE-2018-0886 | CredSSP Remote Code Execution Vulnerability. All versions of Windows Server from Server 2008 (non-R2) onwards are affected by this vulnerability, and will be compatible with this recommendation provided that they have been patched up through May 2018 (or later).

Impact:

Client applications which use CredSSP will not be able to fall back to the insecure versions and services using CredSSP will not accept unpatched clients. This setting should not be deployed until all remote hosts support the newest version, which is achieved by ensuring that all Microsoft security updates at least through May 2018 are installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
CredSSP\Parameters:AllowEncryptionOracle
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Force Updated Clients`:

```
Computer Configuration\Policies\Administrative Templates\System\Credentials
Delegation\Encryption Oracle Remediation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

Default Value:

Without the May 2018 security update: Enabled: Vulnerable (Client applications which use CredSSP will expose the remote servers to attacks by supporting fall back to the insecure versions and services using CredSSP will accept unpatched clients.)

With the May 2018 security update: Enabled: Mitigated (Client applications which use CredSSP will not be able to fall back to the insecure version but services using CredSSP will accept unpatched clients.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Remote host allows delegation of non-exportable credentials. When using credential delegation, devices provide an exportable version of credentials to the remote host. This exposes users to the risk of credential theft from attackers on the remote host. The Restricted Admin Mode and Windows Defender Remote Credential Guard features are two options to help protect against this risk.

The recommended state for this setting is: `Enabled`.

Note: More detailed information on Windows Defender Remote Credential Guard and how it compares to Restricted Admin Mode can be found at this link: Protect Remote Desktop credentials with Windows Defender Remote Credential Guard (Windows 10) | Microsoft Docs

Rationale:

Restricted Admin Mode was designed to help protect administrator accounts by ensuring that reusable credentials are not stored in memory on remote devices that could potentially be compromised. *Windows Defender Remote Credential Guard* helps you protect your credentials over a Remote Desktop connection by redirecting Kerberos requests back to the device that is requesting the connection. Both features should be enabled and supported, as they reduce the chance of credential theft.

Impact:

The host will support the *Restricted Admin Mode* and *Windows Defender Remote Credential Guard* features.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation:
AllowProtectedCreds
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Credentials
Delegation\Remote host allows delegation of non-exportable credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (*Restricted Admin Mode* and *Windows Defender Remote Credential Guard* are not supported. Users will always need to pass their credentials to the host.)

References:

1. https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.8.5 Device Guard

This section contains Device Guard settings.

This Group Policy section is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.8.5.1 (NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This policy setting specifies whether Virtualization Based Security is enabled. Virtualization Based Security uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: `Enabled`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Kerberos, NTLM, and Credential manager isolate secrets by using virtualization-based security. Previous versions of Windows stored secrets in the Local Security Authority (LSA). Prior to Windows 10, the LSA stored secrets used by the operating system in its process memory. With Windows Defender Credential Guard enabled, the LSA process in the operating system talks to a new component called the isolated LSA process that stores and protects those secrets. Data stored by the isolated LSA process is protected using virtualization-based security and is not accessible to the rest of the operating system.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:EnableVirt
ualizationBasedSecurity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.2 (NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This policy setting specifies whether Virtualization Based Security is enabled. Virtualization Based Security uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: `Secure Boot and DMA Protection`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Boot can help reduce the risk of bootloader attacks and in conjunction with DMA protections to help protect data from being scraped from memory.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePla
tformSecurityFeatures
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Secure Boot and DMA Protection`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Select Platform Security Level
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.3 (NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The recommended state for this setting is: `Enabled with UEFI lock`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The `Enabled with UEFI lock` option ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Once this setting is turned on and active, **Virtualization Based Security cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:Hypervisor
EnforcedCodeIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled with UEFI lock`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Virtualization Based Protection
of Code Integrity
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.4 (NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This option will only enable Virtualization Based Protection of Code Integrity on devices with UEFI firmware support for the Memory Attributes Table. Devices without the UEFI Memory Attributes Table may have firmware that is incompatible with Virtualization Based Protection of Code Integrity which in some cases can lead to crashes or data loss or incompatibility with certain plug-in cards. If not setting this option the targeted devices should be tested to ensure compatibility.

The recommended state for this setting is: `True (checked)`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

This setting will help protect this control from being enabled on a system that is not compatible which could lead to a crash or data loss.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HVCIMATReq
uired
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `TRUE`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes
Table
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.5 (NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Member Server

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials. The "Enabled with UEFI lock" option ensures that Credential Guard cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI.

The recommended state for this setting is: `Enabled with UEFI lock`, *but only on Member Servers (not Domain Controllers).*

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The `Enabled with UEFI lock` option ensures that Credential Guard cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Warning #3: Once this setting is turned on and active, **Credential Guard cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled with UEFI lock` (on Member Servers only):

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Credential Guard Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.6 (NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials.

The recommended state for this setting is: `Disabled` *on Domain Controllers*.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Credential Guard is not useful on Domain Controllers and can cause crashes on them.

Impact:

None - this is the default behavior.

Warning: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Credential Guard Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Credential Guard is disabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.5.7 (NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.

The recommended state for this setting is: `Enabled`.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Launch changes the way windows boots to use Intel Trusted Execution Technology (TXT) and Runtime BIOS Resilience features to prevent firmware exploits from being able to impact the security of the Windows Virtualization Based Security environment.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureS
ystemGuardLaunch
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Secure Launch Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Not Configured. (Administrative users can choose whether to enable or disable Secure Launch.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.6 Device Health Attestation Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.7 Device Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.8 Device Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceRedirection.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.9 Disk NV Cache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DiskNVCache.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.10 Disk Quotas

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DiskQuota.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.11 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.8.12 Distributed COM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DCOM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.13 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.14 Early Launch Antimalware

This section contains recommendations for configuring boot-start driver initialization settings.

This Group Policy section is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:

- `Good`: The driver has been signed and has not been tampered with.
- `Bad`: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
- `Bad, but required for boot`: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
- `Unknown`: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.

If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.

The recommended state for this setting is: `Enabled: Good, unknown and bad but critical`.

Rationale:

This policy setting helps reduce the impact of malware that has already infected your system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPo
licy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Good, unknown and bad but critical:`

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch
Antimalware\Boot-Start Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Boot-start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be bad is skipped.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.15 Enhanced Storage Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EnhancedStorage.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.16 File Classification Infrastructure

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.17 File Share Shadow Copy Agent

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileServerVSSAgent.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.18 File Share Shadow Copy Provider

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy templates `FileServerVSSProvider.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.19 Filesystem (formerly NTFS Filesystem)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileSys.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *NTFS Filesystem* but was renamed by Microsoft to *Filesystem* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.8.20 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.21 Group Policy

This section contains recommendations for configuring group policy-related settings.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.21.1 Logging and tracing

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicyPreferences.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart.

The recommended state for this setting is: `Enabled: FALSE` (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Group
Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoBackgroundPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Do not apply during periodic background processing` option to `FALSE` (unchecked):

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Configure registry policy processing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.8.21.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed.

The recommended state for this setting is: `Enabled: TRUE` (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Impact:

Group Policies will be reapplied even if they have not been changed, which could have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Group
Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoGPOListChanges
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Process even if the Group Policy objects have not changed` option to `TRUE` (checked):

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Configure registry policy processing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the Windows device is allowed to participate in cross-device experiences (continue experiences).

The recommended state for this setting is: `Disabled`.

Rationale:

A cross-device experience is when a system can access app and send messages to other devices. In an enterprise managed environment only trusted systems should be communicating within the network. Access to any other system should be prohibited.

Impact:

The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Continue experiences on this device
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

The default behavior depends on the Windows edition.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers.

The recommended state for this setting is: `Disabled`.

Rationale:

This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is in effect when the following registry location does not exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableBkGndGroupPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Turn off background refresh of Group Policy
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Updates can be applied while users are working.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.8.22 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.22.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.22.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.

The recommended state for this setting is: `Enabled`.

Rationale:

Users might download drivers that include malicious code.

Impact:

Print drivers cannot be downloaded over HTTP.

Note: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Printers:DisableWebPnPDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off downloading
of print drivers over HTTP
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can download print drivers over HTTP.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

18.8.23 iSCSI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `iSCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.24 KDC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `KDC.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.8.25 Kerberos

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Kerberos.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.26 Kernel DMA Protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DmaGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

18.8.27 Locale Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.28 Logon

This section contains recommendations related to the logon process and lock screen.

This Group Policy section is provided by the Group Policy template `Logon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy prevents the user from showing account details (email address or user name) on the sign-in screen.

The recommended state for this setting is: `Enabled`.

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

The user cannot choose to show account details on the sign-in screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:BlockUserFromSh
owingAccountDetailsOnSignin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Block
user from showing account details on sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (The user may choose to show account details on the sign-in screen.)

18.8.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.

The recommended state for this setting is: `Enabled`.

Rationale:

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

Impact:

The PC's network connectivity state cannot be changed without signing into Windows.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetw
orkSelectionUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not
display network selection UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.)

18.8.29 Mitigation Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.8.30 Net Logon

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Netlogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.31 OS Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.32 Performance Control Panel

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PerfCenterCPL.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.33 PIN Complexity

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.8.34 Power Management

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.35 Recovery

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ReAgent.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.36 Remote Assistance

This section contains recommendations related to Remote Assistance.

This Group Policy section is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer.

Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

The recommended state for this setting is: `Disabled`.

Rationale:

A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fAllowUnsolicited
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Offer Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.

The recommended state for this setting is: `Disabled`.

Rationale:

There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Impact:

Users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Solicited Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.37 Remote Procedure Call

This section contains recommendations related to Remote Procedure Call.

This Group Policy section is provided by the Group Policy template `RPC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with *1-way* forest trusts if it is applied to the *trusting* domain DCs (see Microsoft KB3073942), so we do not recommend applying it to Domain Controllers.

Note: This policy will not be in effect until the system is rebooted.

The recommended state for this setting is: `Enabled`.

Rationale:

Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Impact:

RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Rpc:EnableAuthEpResolution
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Procedure Call\Enable RPC Endpoint Mapper Client Authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.38 Removable Storage Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `RemovableStorage.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.39 Scripts

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Scripts.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.40 Security Account Manager

This section contains recommendations related to the Security Account Manager.

This Group Policy section is provided by the Group Policy template `SAM.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.8.40.1 (L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows you to configure how Domain Controllers handle Windows Hello for Business (WHfB) keys that are vulnerable to the "Return of Coppersmith´s attack" (ROCA) vulnerability.

If this policy setting is enabled the following options are supported:

`Ignore`: During authentication the Domain Controller will not probe any WHfB keys for the ROCA vulnerability.

`Audit`: During authentication the Domain Controller will emit audit events for WHfB keys that are subject to the ROCA vulnerability (authentications will still succeed).

`Block`: During authentication the Domain Controller will block the use of WHfB keys that are subject to the ROCA vulnerability (vulnerable authentications will fail).

The recommended state for this setting is: `Enabled: Audit`. Configuring this setting to `Enabled: Block` also conforms to the benchmark.

Note: This setting only takes effect on Domain Controllers.

Note #2: A reboot is not required for changes to this setting to take effect.

Rationale:

The "Return of Coppersmith´s attack" or ROCA vulnerability is a cryptographic weakness in a widely used cryptographic library. An attacker can reveal secret keys (offline with no physical access to the affected device) on certified devices using this library.

For more information on this vulnerability, visit ADV170012 - Security Update Guide - Microsoft - Vulnerability in TPM could allow Security Feature Bypass.

Impact:

This setting may affect vulnerable Trusted Platform Module (TPMs). To avoid issues, this setting should not be set to `Block` until appropriate mitigations have been performed, for example patching of vulnerable TPMs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
SAM:SamNGCKeyROCAValidation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Audit` (configuring to `Enabled: Block` also conforms to the benchmark):

```
Computer Configuration\Policies\Administrative Templates\System\Security
Account Manager\Configure validation of ROCA-vulnerable WHfB keys during
authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Sam.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled: Audit. (Domain Controllers will default to using their local configuration. The default local configuration is Audit.)

References:

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361
2. https://nvd.nist.gov/vuln/detail/CVE-2017-15361

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.8.41 Server Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ServerManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.42 Service Control Manager Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ServiceControlManager.admx/adml` that is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer).

18.8.43 Shutdown

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.44 Shutdown Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Winsrv.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.45 Storage Health

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `StorageHealth.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.46 Storage Sense

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `StorageSense.admx/adml` that is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer).

18.8.47 System Restore

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SystemRestore.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.48 Troubleshooting and Diagnostics

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.49 Trusted Platform Module Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.50 User Profiles

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserProfiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.51 Windows File Protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsFileProtection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.52 Windows HotStart

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `HotStart.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.53 Windows Time Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.1 Active Directory Federation Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `adfs.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.2 ActiveX Installer Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ActiveXInstallService.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.4 App Package Deployment

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppxPackageManager.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.5 App Privacy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppPrivacy.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.6 App runtime

This section contains recommendations for App runtime settings.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

Impact:

Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
MSAOptional
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\App runtime\Allow Microsoft accounts to be optional
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users will need to sign in with a Microsoft account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

18.9.7 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.8 AutoPlay Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.9 Backup

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserDataBackup.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1511 Administrative Templates (except for the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates).

18.9.10 Biometrics

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11 BitLocker Drive Encryption

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.12 Camera

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Camera.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.13 Chat

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Taskbar.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.14 Cloud Content

This section contains recommendations related to Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.14.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether cloud consumer account state content is allowed in all Windows experiences.

The recommended state for this setting is: `Enabled`.

Rationale:

The use of consumer accounts in an enterprise managed environment is not good security practice as it could lead to possible data leakage.

Impact:

Users will not be able to use Microsoft consumer accounts on the system, and associated Windows experiences will instead present default fallback content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableCo
nsumerAccountStateContent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Cloud Content\Turn off cloud consumer account state content
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences are able to use cloud consumer accounts.)

18.9.14.2 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account.

The recommended state for this setting is: `Enabled`.

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Having apps silently install in an enterprise managed environment is not good security practice - especially if the apps send data back to a 3rd party.

Impact:

Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableWi
ndowsConsumerFeatures
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Cloud Content\Turn off Microsoft consumer experiences
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Users may see suggestions from Microsoft and notifications about their Microsoft account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.15 Connect

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.16 Credential User Interface

This section contains recommendations related to the Credential User Interface.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.16.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure the display of the password reveal button in password entry user experiences.

The recommended state for this setting is: `Enabled`.

Rationale:

This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Impact:

The password reveal button will not be displayed after a user types a password in the password entry text box.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePassword
Reveal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Do not display the password reveal
button
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The password reveal button is displayed after a user types a password in the password entry text box. If the user clicks on the button, the typed password is displayed on-screen in plain text.)

18.9.16.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application.

The recommended state for this setting is: `Disabled`.

Rationale:

Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:
EnumerateAdministrators
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Enumerate administrator accounts on
elevation
```

Note: This Group Policy path is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be required to always type in a username and password to elevate.)

18.9.17 Data Collection and Preview Builds

This section contains settings for Data Collection and Preview Builds.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.17.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Send required diagnostic data' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the amount of diagnostic and usage data reported to Microsoft:

- A value of (0) `Diagnostic data off (not recommended)`. Using this value, no diagnostic data is sent from the device. This value is only supported on Enterprise, Education, and Server editions. If you choose this setting, devices in your organization will still be secure.
- A value of (1) `Send required diagnostic data`. This is the minimum diagnostic data necessary to keep Windows secure, up to date, and performing as expected. Using this value disables the *Optional diagnostic data* control in the Settings app.
- A value of (3)`Send optional diagnostic data`. Additional diagnostic data is collected that helps us to detect, diagnose and fix issues, as well as make product improvements. Required diagnostic data will always be included when you choose to send optional diagnostic data. Optional diagnostic data can also include diagnostic log files and crash dumps. Use the *Limit Dump Collection* and the *Limit Diagnostic Log Collection* policies for more granular control of what optional diagnostic data is sent.

Windows telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10/11.

The recommended state for this setting is: `Enabled: Send required diagnostic data`.

Note: If your organization relies on Windows Update, the minimum recommended setting is `Required diagnostic data`. Because no Windows Update information is collected when diagnostic data is off, important information about update failures is not sent. Microsoft uses this information to fix the causes of those failures and improve the quality of updates.

Note #2: The *Configure diagnostic data opt-in settings user interface* group policy can be used to prevent end users from changing their data collection settings.

Note #3: Enhanced diagnostic data setting is not available on Windows 11 and Windows Server 2022 and has been replaced with policies that can control the amount of optional diagnostic data that is sent. For more information on these settings visit Manage diagnostic data using Group Policy and MDM

Rationale:

Sending any data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

Impact:

Note that setting values of 0 or 1 will degrade certain experiences on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:AllowTe
lemetry
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Send required diagnostic data`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Allow Diagnostic Data
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow Telemetry*, but it was renamed to *Allow Diagnostic Data* starting with the Windows 11 Release 21H2 Administrative Templates.

Default Value:

Disabled. (The device will send required diagnostic data and the end user can choose whether to send optional diagnostic data from the Settings app.)

References:

1. https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.18 Delivery Optimization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.19 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.20 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.21 Device and Driver Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceCompat.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.22 Device Registration (formerly Workplace Join)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WorkplaceJoin.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Workplace Join* but was renamed by Microsoft to *Device Registration* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.9.23 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.24 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.25 EMET

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EMET.admx/adml` that is included with Microsoft EMET.

EMET is free and supported security software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Many of these mitigations were later coded directly into Windows 10 and Server 2016.

Note: Although EMET is quite effective at enhancing exploit protection on Windows server OSes prior to Server 2016, it is highly recommended that compatibility testing is done on typical server configurations (including all CIS-recommended EMET settings) before widespread deployment to your environment.

Note #2: EMET has been reported to be very problematic on 32-bit OSes - we only recommend using it with 64-bit OSes.

Note #3: Microsoft has announced that EMET will be End-Of-Life (EOL) on July 31, 2018. This does not mean the software will stop working, only that Microsoft will not update it any further past that date, nor troubleshoot new problems with it. They are instead recommending that servers be upgraded to Server 2016.

18.9.26 Event Forwarding

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventForwarding.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.27 Event Log Service

This section contains recommendations for configuring the Event Log Service.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.27.1 Application

This section contains recommendations for configuring the Application Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.27.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:R
etention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Application\Control Event Log behavior when the
log file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:M
axSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Application\Specify the maximum log file size
(KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.2 Security

This section contains recommendations for configuring the Security Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.27.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Rete
ntion
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Security\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 196,608 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxS
ize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 196,608 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Security\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.3 Setup

This section contains recommendations for configuring the Setup Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.27.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Setup\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Setup\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.4 System

This section contains recommendations for configuring the System Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.27.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retent
ion
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\System\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.27.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSiz
e
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\System\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.9.28 Event Logging

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventLogging.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.29 Event Viewer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventViewer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.30 Family Safety (formerly Parental Controls)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ParentalControls.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 RTM (Release 1507) Administrative Templates.

Note: This section was initially named *Parental Controls* but was renamed by Microsoft to *Family Safety* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.31 File Explorer (formerly Windows Explorer)

This section contains recommendations to control the availability of options such as menu items and tabs in dialog boxes.

This Group Policy section is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.31.1 Previous Versions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PreviousVersions.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.31.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disabling Data Execution Prevention can allow certain legacy plug-in applications to function without terminating Explorer.

The recommended state for this setting is: `Disabled`.

Note: Some legacy plug-in applications and other software may not function with Data Execution Prevention and will require an exception to be defined for that specific plug-in/software.

Rationale:

Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecuti
onPrevention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off Data Execution Prevention for Explorer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Explorer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Data Execution Prevention will block certain types of malware from exploiting Explorer.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.31.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Without heap termination on corruption, legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Ensuring that heap termination on corruption is active will prevent this.

The recommended state for this setting is: `Disabled`.

Rationale:

Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTermina
tionOnCorruption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off heap termination on corruption
```

Note: This Group Policy path is provided by the Group Policy template `Explorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Heap termination on corruption is enabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.31.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol, applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows.

The recommended state for this setting is: `Disabled`.

Rationale:

Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:PreXPSP2ShellProtocolBehavior
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off shell protocol protected mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The protocol is in the protected mode, allowing applications to only open a limited set of folders.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.32 File History

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileHistory.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.33 Find My Device

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FindMy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.34 Game Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GameExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35 Handwriting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Handwriting.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.36 HomeGroup

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.37 Human Presence

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.38 Import Video

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

18.9.39 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

CIS publishes security guidance for Microsoft Internet Explorer in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community.

18.9.40 Internet Information Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `IIS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.41 Location and Sensors

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.42 Maintenance Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `msched.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.43 Maps

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinMaps.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.44 MDM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MDM.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.45 Messaging

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Messaging.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.46 Microsoft account

This section contains recommendations related to Microsoft Accounts.

This Group Policy section is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.46.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines whether applications and services on the device can utilize new consumer Microsoft account authentication via the Windows `OnlineID` and `WebAccountManager` APIs.

The recommended state for this setting is: `Enabled`.

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used on their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Impact:

All applications and services on the device will be prevented from *new* authentications using consumer Microsoft accounts via the Windows `OnlineID` and `WebAccountManager` APIs. Authentications performed directly by the user in web browsers or in apps that use `OAuth` will remain unaffected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAu
th
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft accounts\Block all consumer Microsoft account user
authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Applications and services on the device will be permitted to authenticate using consumer Microsoft accounts via the Windows `OnlineID` and `WebAccountManager` APIs.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

18.9.47 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)

This section contains recommendations related to Microsoft Defender Antivirus.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 Release 1703 Administrative Templates. It was renamed (again) to *Microsoft Defender Antivirus* starting with the Windows 10 Release 2004 Administrative Templates.

18.9.47.1 Client Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.2 Device Control

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.47.3 Exclusions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.4 MAPS

This section contains recommendations related to Microsoft Active Protection Service (MAPS).

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.4.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft has now renamed to "Microsft Defender Antivirus Cloud Protection Service". This setting can only be set by Group Policy.

The recommended state for this setting is: `Disabled`.

Rationale:

The decision on whether or not to participate in Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:LocalSettingOverrideSpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\MAPS\Configure local setting override
for reporting to Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.47.5 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section contains Microsoft Defender Exploit Guard settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.9.47.5.1 Attack Surface Reduction

This section contains Attack Surface Reduction settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.5.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.

The recommended state for this setting is: `Enabled`.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows
Defender Exploit Guard\ASR:ExploitGuard_ASR_Rules
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.47.5.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting sets the Attack Surface Reduction rules.

The recommended state for this setting is:

`9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1` (Block credential stealing from the Windows local security authority subsystem (lsass.exe))

`e6db77e5-3df2-4cf1-b95a-636979351e5b - 1` (Block persistence through WMI event subscription)

Recommended Optional Values for this setting:

`26190899-1602-49e8-8b27-eb1d0a1ce869 - 1` (Block Office communication application from creating child processes)

`3b576869-a4ec-4529-8536-b80a7769e899 - 1` (Block Office applications from creating executable content)

`5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1` (Block execution of potentially obfuscated scripts)

`75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1` (Block Office applications from injecting code into other processes)

`7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1` (Block Adobe Reader from creating child processes)

`92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1` (Block Win32 API calls from Office macro)

Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows
Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows
Defender Exploit Guard\ASR\Rules:e6db77e5-3df2-4cf1-b95a-636979351e5b
```

Optional Values:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:3b576869-a4ec-4529-8536-b80a7769e899
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:d3e037e1-3eb8-44c8-a917-57927947596d
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender
Exploit Guard\ASR\Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a
```

Remediation:

To establish the recommended configuration via GP, set the following UI path so that: `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2` and `e6db77e5-3df2-4cf1-b95a-636979351e5b` are each set to a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set
the state for each ASR rule
```

Optional Values:

`26190899-1602-49e8-8b27-eb1d0a1ce869`, `3b576869-a4ec-4529-8536-b80a7769e899`, `5beb7efe-fd9a-4556-801d-275e5ffc04cc`, `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84`, `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c`, `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b`, `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4`, `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550`, `d3e037e1-3eb8-44c8-a917-57927947596d`, and `d4f940ab-401b-4efc-aadc-ad5f3c50688a`

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.47.5.2 Controlled Folder Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.5.3 Network Protection

This section contains Windows Network Protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.47.5.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Microsoft Defender Exploit Guard network protection.

The recommended state for this setting is: `Enabled: Block`.

Rationale:

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

Impact:

Users and applications will not be able to access dangerous domains.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows
Defender Exploit Guard\Network Protection:EnableNetworkProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Microsoft Defender Exploit
Guard\Network Protection\Prevent users and apps from accessing dangerous
websites
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users and applications will not be blocked from connecting to dangerous domains.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.47.6 MpEngine

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.47.7 Network Inspection System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.8 Quarantine

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.9 Real-time Protection

This section contains settings related to Real-time Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.9.1 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures scanning for all downloaded files and attachments.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableIOAVProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all
downloaded files and attachments
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (All downloaded files and attachments will be scanned.)

References:

1. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.9.2 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures real-time protection prompts for known malware detection.

Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

The recommended state for this setting is: `Disabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableRealtimeMonitoring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-
time protection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft Defender Antivirus will prompt users to take actions on malware detections.)

References:

1. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.9.3 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure behavior monitoring for Microsoft Defender Antivirus.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default configuration.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableBehaviorMonitoring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on behavior
monitoring
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Behavior monitoring will be enabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.9.4 (L1) Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows script scanning to be turned on/off. Script scanning intercepts scripts then scans them before they are executed on the system.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableScriptScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on script
scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Script scanning will be enabled.)

References:

1. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.10 Remediation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.11 Reporting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.12 Scan

This section contains settings related to Microsoft Defender Antivirus scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.12.1 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

The recommended state for this setting is: `Enabled`.

Rationale:

Incoming e-mails should be scanned by an antivirus solution such as Microsoft Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Impact:

E-mail scanning by Microsoft Defender Antivirus will be enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisableEmailScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (E-mail scanning by Microsoft Defender Antivirus will be disabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.13 Security Intelligence Updates (formerly Signature Updates)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Signature Updates* but was renamed by Microsoft to *Security Intelligence Updates* starting with the Microsoft Windows 10 Release 1903 Administrative Templates.

18.9.47.14 Threats

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.15 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.

The recommended state for this setting is: `Enabled: Block`.

For more information, see this link: Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs

Rationale:

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender:PUAProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Configure detection for potentially
unwanted applications
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Disabled. (Applications that are identified by Microsoft as PUA will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.16 (L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off Microsoft Defender Antivirus. If the setting is configured to Disabled, Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

The recommended state for this setting is: `Disabled`.

Rationale:

It is important to ensure a current, updated antivirus product is scanning each computer for malicious file activity. Microsoft provides a competent solution out of the box in Microsoft Defender Antivirus.

Organizations that choose to purchase a reputable 3rd-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender:DisableAntiSpyware
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Turn off Microsoft Defender AntiVirus
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn off Windows Defender*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates. It was again renamed to *Windows Defender Antivirus* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.48 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Application Guard* but was renamed by Microsoft to *Microsoft Defender Application Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.9.49 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ExploitGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.9.50 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

CIS publishes security guidance for Microsoft Edge in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community.

18.9.51 Microsoft FIDO Authentication

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FidoAuth.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.52 Microsoft Secondary Authentication Factor

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceCredential.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.53 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.54 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.55 Network Access Protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NAPXPQec.admx/adml` that is only included with the Microsoft Windows Server 2008 (non-R2) through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.56 Network Projector

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.57 News and interests

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Feeds.admx/adml` that is included with the Microsoft Windows 10 Release 21H1 Administrative Templates (or newer).

18.9.58 OneDrive (formerly SkyDrive)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

The Group Policy settings contained within this section are provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *SkyDrive* but was renamed by Microsoft to *OneDrive* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.9.59 Online Assistance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.60 OOBE

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

18.9.61 Password Synchronization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PswdSync.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.62 Portable Operating System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ExternalBoot.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.63 Presentation Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.64 Push To Install

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PushToInstall.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.65 Remote Desktop Services (formerly Terminal Services)

This section contains recommendations related to Remote Desktop Services.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.65.1 RD Licensing (formerly TS Licensing)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Licensing* but was renamed by Microsoft to *RD Licensing* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.65.2 Remote Desktop Connection Client

This section contains recommendations for the Remote Desktop Connection Client.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.2.1 RemoteFX USB Device Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.65.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting helps prevent Remote Desktop clients from saving passwords on a computer.

The recommended state for this setting is: `Enabled`.

Note: If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.

Rationale:

An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Impact:

The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DisablePasswordSaving
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Connection Client\Do not
allow passwords to be saved
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be able to save passwords using Remote Desktop Connection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.65.3 Remote Desktop Session Host (formerly Terminal Server)

This section contains recommendations for the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Server* but was renamed by Microsoft to *Remote Desktop Session Host* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.65.3.1 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer-Server.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.65.3.2 Connections

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.3 Device and Resource Redirection

This section contains recommendations related to Remote Desktop Session Host Device and Resource Redirection.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.3.1 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents users from sharing the local drives on their client computers to Remote Desktop Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format:

```
\\TSClient\<driveletter>$
```

If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.

The recommended state for this setting is: `Enabled`.

Rationale:

Data could be forwarded from the user's Remote Desktop Services session to the user's local computer without any direct user interaction. Malicious software already present on a compromised server would have direct and stealthy disk access to the user's local computer during the Remote Desktop session.

Impact:

Drive redirection will not be possible. In most situations, traditional network drive mapping to file shares (including administrative shares) performed manually by the connected user will serve as a capable substitute to still allow file transfers when needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableCdm
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow drive redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (An RD Session Host maps client drives automatically upon connection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.65.3.4 Licensing

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.5 Printer Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.6 Profiles

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.7 RD Connection Broker (formerly TS Connection Broker)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Connection Broker* but was renamed by Microsoft to *RD Connection Broker* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.65.3.8 Remote Session Environment

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.9 Security

This section contains recommendations related to Remote Desktop Session Host Security.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.

The recommended state for this setting is: `Enabled`.

Rationale:

Users have the option to store both their username and password when they create a new Remote Desktop Connection shortcut. If the server that runs Remote Desktop Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Remote Desktop Server through the Remote Desktop Connection shortcut, even though they may not know the user's password.

Impact:

Users cannot automatically log on to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fPromptForPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Always prompt for password upon connection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named *Always prompt client for password upon connection*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.)

18.9.65.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication.

You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Impact:

Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fEncryptRPCTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require secure RPC communication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request.)

18.9.65.3.9.3 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.

The recommended state for this setting is: `Enabled: High Level`.

Rationale:

If Remote Desktop client connections that use low level encryption are allowed, it is more likely that an attacker will be able to decrypt any captured Remote Desktop Services network traffic.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MinEncryptionLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: High Level`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set
client connection encryption level
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled: High Level. (All communications between clients and RD Session Host servers during remote connections using native RDP encryption must be 128-bit strength. Clients that do not support 128-bit encryption will be unable to establish Remote Desktop Server sessions.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.9.65.3.10 Session Time Limits

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.11 Temporary folders

This section contains recommendations related to Remote Desktop Session Host Session Temporary folders.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff.

The recommended state for this setting is: `Disabled`.

Rationale:

Sensitive information could be contained inside the temporary folders and visible to other administrators that log into the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DeleteTempDirsOnExit
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary
Folders\Do not delete temp folders upon exit
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Do not delete temp folder upon exit*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Temporary folders are deleted when a user logs off.)

18.9.65.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the `sessionid`. This temporary folder is used to store individual temporary files.

To reclaim disk space, the temporary folder is deleted when the user logs off from a session.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this setting keeps the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:PerSessionTempDir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary
Folders\Do not use temporary folders per session
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Per-session temporary folders are created.)

18.9.66 RSS Feeds

This section contains recommendations related to RSS feeds.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.66.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents the user from having enclosures (file attachments) downloaded from an RSS feed to the user's computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Impact:

Users cannot set the Feed Sync Engine to download an enclosure through the Feed property page. Developers cannot change the download setting through feed APIs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet
Explorer\Feeds:DisableEnclosureDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\RSS Feeds\Prevent downloading of enclosures
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Turn off downloading of enclosures*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Users can set the Feed Sync Engine to download an enclosure through the Feed property page. Developers can change the download setting through the Feed APIs.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

18.9.67 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.67.1 OCR

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SearchOCR.admx/adml` that is only included with the Microsoft Windows 7 & Server 2008 R2 through the Windows 10 Release 1511 Administrative Templates.

18.9.67.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.

The recommended state for this setting is: `Disabled`.

Rationale:

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows
Search:AllowIndexingEncryptedStoresOrItems
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow indexing of encrypted files
```

Note: This Group Policy path is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

18.9.68 Security Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SecurityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.69 Server for NIS

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Snis.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.70 Shutdown Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.71 Smart Card

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SmartCard.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.72 Software Protection Platform

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.73 Sound Recorder

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.74 Speech

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Speech.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.75 Store

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.76 Sync your settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SettingSync.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.77 Tablet PC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.78 Task Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.79 Tenant Restrictions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TenantRestrictions.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.80 Text Input

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TextInput.admx/adml` that is only included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates and Microsoft Windows 10 Release 1511 Administrative Templates.

18.9.81 Widgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NewsAndInterests.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.82 Windows Calendar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.83 Windows Color System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.84 Windows Customer Experience Improvement Program

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CEIPEnable.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.85 Windows Defender SmartScreen

This section contains Windows Defender SmartScreen settings.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.85.1 Explorer

This section contains recommendations for Explorer-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.85.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.

The recommended state for this setting is: `Enabled: Warn and prevent bypass`.

Rationale:

Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

Impact:

Users will be warned before they are allowed to run unrecognized programs downloaded from the Internet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScre
en
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScree
nLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Warn and prevent bypass`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender
SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Disabled. (Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.86 Windows Error Reporting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.87 Windows Game Recording and Broadcasting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.88 Windows Hello for Business (formerly Microsoft Passport for Work)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates.

18.9.89 Windows Ink Workspace

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.90 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.90.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether users are permitted to change installation options that typically are available only to system administrators. The security features of Windows Installer normally prevent users from changing installation options that are typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.

The recommended state for this setting is: `Disabled`.

Rationale:

In an enterprise managed environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability to have any control over installs can risk unapproved software from being installed or removed from a system, which could cause the system to become vulnerable to compromise.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserCo
ntrol
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Allow user control over installs
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Enable user control over installs*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The security features of Windows Installer will prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●

18.9.90.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.

The recommended state for this setting is: `Disabled`.

Rationale:

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstal
lElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Always install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

18.9.91 Windows Logon Options

This section contains recommendations related to Windows Logon Options.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.91.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this feature will prevent the caching of user's credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

Impact:

The device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts. The user is required to present the logon credentials in order to proceed after restart.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.
This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableAutomaticRestartSignOn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Logon Options\Sign-in and lock last interactive user
automatically after a restart
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinLogon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Sign-in last interactive user automatically after a system-initiated restart*, but it was renamed starting with the Windows 10 Release 1903 Administrative Templates.

Default Value:

Enabled. (The device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.)

Additional Information:

Disable this policy setting so that the device does not store the user's credentials for automatic sign-in after a Windows Update restart and the users' lock screen apps are not restarted after the system restarts.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.92 Windows Mail

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

18.9.93 Windows Media Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

18.9.94 Windows Media Digital Rights Management

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaDRM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.95 Windows Media Player

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.96 Windows Meeting Space

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsCollaboration.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.97 Windows Messenger

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMessenger.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.98 Windows Mobility Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCMobilityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.99 Windows Movie Maker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MovieMaker.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.100 Windows PowerShell

This section contains recommendations related to Windows PowerShell.

This Group Policy section is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.100.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enables logging of all PowerShell script input to the `Applications and Services Logs\Microsoft\Windows\PowerShell\Operational` Event Log channel.

The recommended state for this setting is: `Enabled`.

Note: If logging of *Script Block Invocation Start/Stop Events* is enabled (option box checked), PowerShell will log additional events when invocation of a command, script block, function, or script starts or stops. Enabling this option generates a high volume of event logs. CIS has intentionally chosen not to make a recommendation for this option, since it generates a large volume of events. **If an organization chooses to enable the optional setting (checked), this also conforms to the benchmark.**

Rationale:

Logs of PowerShell script input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell script input will be logged to the `Applications and Services Logs\Microsoft\Windows\PowerShell\Operational` Event Log channel, which can contain credentials and sensitive information.

Warning: There are potential risks of capturing credentials and sensitive information in the PowerShell logs, which could be exposed to users who have read-access to those logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: About Logging Windows - PowerShell | Microsoft Docs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlock
Logging:EnableScriptBlockLogging
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Script Block Logging
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (PowerShell will log script blocks the first time they are used.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

18.9.100.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

The recommended state for this setting is: `Disabled`.

Rationale:

If this setting is enabled there is a risk that passwords could get stored in plain text in the `PowerShell_transcript` output file.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcripti
on:EnableTranscripting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Transcription
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the `Start-Transcript` cmdlet.)

18.9.101 Windows Reliability Analysis

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `RacWmiProv.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.102 Windows Remote Management (WinRM)

This section contains recommendations related to Windows Remote Management (WinRM).

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.102.1 WinRM Client

This section contains recommendations related to the Windows Remote Management (WinRM) client.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.102.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication.

The recommended state for this setting is: `Disabled`.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client does not use Basic authentication.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.9.102.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.

The recommended state for this setting is: `Disabled`.

Rationale:

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnen
cryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client sends or receives only encrypted messages over the network.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.9.102.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.

The recommended state for this setting is: `Enabled`.

Rationale:

Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

The WinRM client will not use Digest authentication.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDige
st
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client will use Digest authentication.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.9.102.2 WinRM Service

This section contains recommendations related to the Windows Remote Management (WinRM) service.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.102.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.

The recommended state for this setting is: `Disabled`.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service will not accept Basic authentication from a remote client.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.9.102.2.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.

The recommended state for this setting is: `Disabled`.

Rationale:

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUne
ncryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service sends or receives only encrypted messages over the network.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.9.102.2.3 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will allow RunAs credentials to be stored for any plug-ins.

The recommended state for this setting is: `Enabled`.

Note: If you enable and then disable this policy setting, any values that were previously configured for `RunAsPassword` will need to be reset.

Rationale:

Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Impact:

The WinRM service will not allow the `RunAsUser` or `RunAsPassword` configuration values to be set for any plug-ins. If a plug-in has already set the `RunAsUser` and `RunAsPassword` configuration values, the `RunAsPassword` configuration value will be erased from the credential store on the computer.

If this setting is later Disabled again, any values that were previously configured for `RunAsPassword` will need to be reset.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableR
unAs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM
from storing RunAs credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The WinRM service will allow the `RunAsUser` and `RunAsPassword` configuration values to be set for plug-ins and the `RunAsPassword` value will be stored securely.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.9.103 Windows Remote Shell

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.104 Windows Sandbox

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsSandbox.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.105 Windows Security (formerly Windows Defender Security Center)

This section contains recommendations related to the Windows Security Center console settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Security Center* but was renamed by Microsoft to *Windows Security* starting with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates.

18.9.105.1 Account protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

18.9.105.2 App and browser protection

This section contains App and browser protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.105.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Security settings.

The recommended state for this setting is: `Enabled`.

Rationale:

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

Impact:

Local users cannot make changes in the Exploit protection settings area.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security
Center\App and Browser protection:DisallowExploitProtectionOverride
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Security\App and browser protection\Prevent users from
modifying settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Local users are allowed to make changes in the Exploit protection settings area.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.106 Windows SideShow

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SideShow.admx/adml` that is only included with the Microsoft Windows Vista Administrative Templates through Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.107 Windows System Resource Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SystemResourceManager.admx/adml` that is only included with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.108 Windows Update

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: Please see the following Microsoft Documentation on Windows Updates in Azure: Manage updates and patches for your VMs in Azure Automation | Microsoft Docs

Appendix: Summary Table

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
1	**Account Policies**		
1.1	**Password Policy**		
1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	□	□
1.1.2	(L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	□	□
1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	□	□
1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	□	□
1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	□	□
1.1.6	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	□	□
1.2	**Account Lockout Policy**		
2	**Local Policies**		
2.1	**Audit Policy**		
2.2	**User Rights Assignment**		
2.2.1	(L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)	□	□
2.2.2	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.3	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)	□	□
2.2.4	(L1) Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	□	□
2.2.5	(L1) Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)	□	□
2.2.6	(L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	□	□
2.2.7	(L1) Ensure 'Allow log on locally' is set to 'Administrators' (Automated)	□	□
2.2.8	(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)	□	□
2.2.9	(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)	□	□
2.2.10	(L1) Ensure 'Back up files and directories' is set to 'Administrators, Backup Operators, Server Operators' (Automated)	□	□
2.2.11	(L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	□	□
2.2.12	(L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Automated)	□	□
2.2.13	(L1) Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	□	□
2.2.14	(L1) Ensure 'Create a token object' is set to 'No One' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.15	(L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	□	□
2.2.16	(L1) Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	□	□
2.2.17	(L1) Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated)	□	□
2.2.18	(L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated)	□	□
2.2.19	(L1) Ensure 'Debug programs' is set to 'Administrators' (Automated)	□	□
2.2.20	(L1) Ensure 'Deny access to this computer from the network' to include 'Guests' (Automated)	□	□
2.2.21	(L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	□	□
2.2.22	(L1) Ensure 'Deny log on as a service' to include 'Guests' (Automated)	□	□
2.2.23	(L1) Ensure 'Deny log on locally' to include 'Guests' (Automated)	□	□
2.2.24	(L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (Automated)	□	□
2.2.25	(L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)	□	□
2.2.26	(L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)	□	□
2.2.27	(L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.28	(L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	□	□
2.2.29	(L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)	□	□
2.2.30	(L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) (Automated)	□	□
2.2.31	(L1) Ensure 'Increase scheduling priority' is set to 'Administrators' (Automated)	□	□
2.2.32	(L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	□	□
2.2.33	(L1) Ensure 'Lock pages in memory' is set to 'No One' (Automated)	□	□
2.2.34	(L1) Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) (Automated)	□	□
2.2.35	(L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)	□	□
2.2.36	(L1) Ensure 'Modify an object label' is set to 'No One' (Automated)	□	□
2.2.37	(L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)	□	□
2.2.38	(L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)	□	□
2.2.39	(L1) Ensure 'Profile single process' is set to 'Administrators' (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
2.2.40	(L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	□	□
2.2.41	(L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	□	□
2.2.42	(L1) Ensure 'Restore files and directories' is set to 'Administrators, Backup Operators' (Automated)	□	□
2.2.43	(L1) Ensure 'Shut down the system' is set to 'Administrators, Backup Operators' (Automated)	□	□
2.2.44	(L1) Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)	□	□
2.2.45	(L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	□	□
2.3	**Security Options**		
2.3.1	**Accounts**		
2.3.1.1	(L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)	□	□
2.3.1.2	(L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)	□	□
2.3.1.3	(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)	□	□
2.3.1.4	(L1) Configure 'Accounts: Rename administrator account' (Automated)	□	□
2.3.1.5	(L1) Configure 'Accounts: Rename guest account' (Automated)	□	□
2.3.2	**Audit**		

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
2.3.2.1	(L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	□	□
2.3.2.2	(L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	□	□
2.3.3	**DCOM**		
2.3.4	**Devices**		
2.3.5	**Domain controller**		
2.3.5.1	(L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)	□	□
2.3.5.2	(L1) Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)	□	□
2.3.5.3	(L1) Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)	□	□
2.3.5.4	(L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)	□	□
2.3.5.5	(L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)	□	□
2.3.6	**Domain member**		
2.3.6.1	(L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
2.3.6.2	(L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)	□	□
2.3.6.3	(L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)	□	□
2.3.6.4	(L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	□	□
2.3.6.5	(L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)	□	□
2.3.7	**Interactive logon**		
2.3.7.1	(L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	□	□
2.3.7.2	(L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	□	□
2.3.7.3	(L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	□	□
2.3.7.4	(L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	□	□
2.3.8	**Microsoft network client**		
2.3.8.1	(L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)	□	□
2.3.8.2	(L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)	□	□
2.3.8.3	(L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.9	**Microsoft network server**		
2.3.9.1	(L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)	□	□
2.3.9.2	(L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)	□	□
2.3.9.3	(L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)	□	□
2.3.9.4	(L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)	□	□
2.3.9.5	(L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)	□	□
2.3.10	**Network access**		
2.3.10.1	(L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)	□	□
2.3.10.2	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)	□	□
2.3.10.3	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)	□	□
2.3.10.4	(L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)	□	□
2.3.10.5	(L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Automated)	□	□
2.3.10.6	(L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
2.3.10.7	(L1) Configure 'Network access: Remotely accessible registry paths' is configured (Automated)	□	□
2.3.10.8	(L1) Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	□	□
2.3.10.9	(L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	□	□
2.3.10.10	(L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)	□	□
2.3.10.11	(L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	□	□
2.3.10.12	(L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	□	□
2.3.11	**Network security**		
2.3.11.1	(L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	□	□
2.3.11.2	(L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	□	□
2.3.11.3	(L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	□	□
2.3.11.4	(L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)	□	□
2.3.11.5	(L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.11.6	(L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	□	□
2.3.11.7	(L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	□	□
2.3.11.8	(L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	□	□
2.3.11.9	(L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	□	□
2.3.12	**Recovery console**		
2.3.13	**Shutdown**		
2.3.13.1	(L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)	□	□
2.3.14	**System cryptography**		
2.3.15	**System objects**		
2.3.15.1	(L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	□	□
2.3.15.2	(L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	□	□
2.3.16	**System settings**		
2.3.17	**User Account Control**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.17.1	(L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	□	□
2.3.17.2	(L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Automated)	□	□
2.3.17.3	(L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	□	□
2.3.17.4	(L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)	□	□
2.3.17.5	(L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	□	□
2.3.17.6	(L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	□	□
2.3.17.7	(L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)	□	□
2.3.17.8	(L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	□	□
3	**Event Log**		
4	**Restricted Groups**		
5	**System Services**		
5.1	(L1) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
6	**Registry**		
7	**File System**		
8	**Wired Network (IEEE 802.3) Policies**		
9	**Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)**		
9.1	**Domain Profile**		
9.1.1	(L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	□	□
9.1.2	(L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)	□	□
9.1.3	(L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Automated)	□	□
9.1.4	(L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)	□	□
9.1.5	(L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	□	□
9.1.6	(L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	□	□
9.1.7	(L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	□	□
9.2	**Private Profile**		
9.2.1	(L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	□	□
9.2.2	(L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.2.3	(L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Automated)	□	□
9.2.4	(L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)	□	□
9.2.5	(L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	□	□
9.2.6	(L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	□	□
9.2.7	(L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	□	□
9.3	**Public Profile**		
9.3.1	(L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	□	□
9.3.2	(L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)	□	□
9.3.3	(L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Automated)	□	□
9.3.4	(L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)	□	□
9.3.5	(L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	□	□
9.3.6	(L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	□	□
9.3.7	(L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
10	**Network List Manager Policies**		
11	**Wireless Network (IEEE 802.11) Policies**		
12	**Public Key Policies**		
13	**Software Restriction Policies**		
14	**Network Access Protection NAP Client Configuration**		
15	**Application Control Policies**		
16	**IP Security Policies**		
17	**Advanced Audit Policy Configuration**		
17.1	**Account Logon**		
17.1.1	(L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	□	□
17.1.2	(L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)	□	□
17.2	**Account Management**		
17.2.1	(L1) Ensure 'Audit Computer Account Management' is set to include 'Success and Failure' (DC only) (Automated)	□	□
17.2.2	(L1) Ensure 'Audit Distribution Group Management' is set to include 'Success and Failure' (DC only) (Automated)	□	□
17.2.3	(L1) Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)	□	□
17.2.4	(L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	□	□
17.2.5	(L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.3	**Detailed Tracking**		
17.3.1	(L1) Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	□	□
17.3.2	(L1) Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	□	□
17.4	**DS Access**		
17.5	**Logon/Logoff**		
17.5.1	(L1) Ensure 'Audit Account Lockout' is set to include 'Success and Failure' (Automated)	□	□
17.5.2	(L1) Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	□	□
17.5.3	(L1) Ensure 'Audit Logoff' is set to include 'Success' (Automated)	□	□
17.5.4	(L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	□	□
17.5.5	(L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)	□	□
17.5.6	(L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	□	□
17.6	**Object Access**		
17.6.1	(L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)	□	□
17.6.2	(L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	□	□
17.7	**Policy Change**		
17.7.1	(L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.7.2	(L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	□	□
17.7.3	(L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	□	□
17.8	**Privilege Use**		
17.8.1	(L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)	□	□
17.9	**System**		
17.9.1	(L1) Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	□	□
17.9.2	(L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	□	□
17.9.3	(L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	□	□
18	**Administrative Templates (Computer)**		
18.1	**Control Panel**		
18.1.1	**Personalization**		
18.1.1.1	(L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	□	□
18.1.1.2	(L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	□	□
18.1.2	**Regional and Language Options**		
18.1.2.1	**Handwriting personalization**		
18.1.2.2	(L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	□	□
18.2	**LAPS**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.3	**MS Security Guide**		
18.3.1	(L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	□	□
18.3.2	(L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	□	□
18.3.3	(L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	□	□
18.3.5	(L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	□	□
18.3.6	(L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)	□	□
18.4	**MSS (Legacy)**		
18.4.1	(L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	□	□
18.4.2	(L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	□	□
18.4.3	(L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	□	□
18.4.4	(L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	□	□
18.5	**Network**		
18.5.1	**Background Intelligent Transfer Service (BITS)**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.5.2	**BranchCache**		
18.5.3	**DirectAccess Client Experience Settings**		
18.5.4	**DNS Client**		
18.5.4.1	(L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	□	□
18.5.5	**Fonts**		
18.5.6	**Hotspot Authentication**		
18.5.7	**Lanman Server**		
18.5.8	**Lanman Workstation**		
18.5.8.1	(L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)	□	□
18.5.9	**Link-Layer Topology Discovery**		
18.5.10	**Microsoft Peer-to-Peer Networking Services**		
18.5.11	**Network Connections**		
18.5.11.1	**Windows Defender Firewall (formerly Windows Firewall)**		
18.5.11.2	(L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)	□	□
18.5.11.3	(L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)	□	□
18.5.12	**Network Connectivity Status Indicator**		
18.5.13	**Network Isolation**		
18.5.14	**Network Provider**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.5.14.1	(L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated)	□	□
18.5.15	**Offline Files**		
18.5.16	**QoS Packet Scheduler**		
18.5.17	**SNMP**		
18.5.18	**SSL Configuration Settings**		
18.5.19	**TCPIP Settings**		
18.5.20	**Windows Connect Now**		
18.5.21	**Windows Connection Manager**		
18.5.21.1	(L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Automated)	□	□
18.6	**Printers**		
18.6.1	(L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	□	□
18.7	**Start Menu and Taskbar**		
18.8	**System**		
18.8.1	**Access-Denied Assistance**		
18.8.2	**App-V**		
18.8.3	**Audit Process Creation**		
18.8.3.1	(L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.8.4	**Credentials Delegation**		
18.8.4.1	(L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	□	□
18.8.4.2	(L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)	□	□
18.8.5	**Device Guard**		
18.8.5.1	(NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	□	□
18.8.5.2	(NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection' (Automated)	□	□
18.8.5.3	(NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	□	□
18.8.5.4	(NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	□	□
18.8.5.5	(NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)	□	□
18.8.5.6	(NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)	□	□
18.8.5.7	(NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	□	□
18.8.6	**Device Health Attestation Service**		
18.8.7	**Device Installation**		
18.8.8	**Device Redirection**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.8.9	**Disk NV Cache**		
18.8.10	**Disk Quotas**		
18.8.11	**Display**		
18.8.12	**Distributed COM**		
18.8.13	**Driver Installation**		
18.8.14	**Early Launch Antimalware**		
18.8.14.1	(L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	□	□
18.8.15	**Enhanced Storage Access**		
18.8.16	**File Classification Infrastructure**		
18.8.17	**File Share Shadow Copy Agent**		
18.8.18	**File Share Shadow Copy Provider**		
18.8.19	**Filesystem (formerly NTFS Filesystem)**		
18.8.20	**Folder Redirection**		
18.8.21	**Group Policy**		
18.8.21.1	**Logging and tracing**		
18.8.21.2	(L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	□	□
18.8.21.3	(L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	□	□
18.8.21.4	(L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.8.21.5	(L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	□	□
18.8.22	**Internet Communication Management**		
18.8.22.1	**Internet Communication settings**		
18.8.22.1.1	(L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	□	□
18.8.23	**iSCSI**		
18.8.24	**KDC**		
18.8.25	**Kerberos**		
18.8.26	**Kernel DMA Protection**		
18.8.27	**Locale Services**		
18.8.28	**Logon**		
18.8.28.1	(L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	□	□
18.8.28.2	(L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	□	□
18.8.29	**Mitigation Options**		
18.8.30	**Net Logon**		
18.8.31	**OS Policies**		
18.8.32	**Performance Control Panel**		
18.8.33	**PIN Complexity**		
18.8.34	**Power Management**		
18.8.35	**Recovery**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.8.36	**Remote Assistance**		
18.8.36.1	(L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	□	□
18.8.36.2	(L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	□	□
18.8.37	**Remote Procedure Call**		
18.8.37.1	(L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)	□	□
18.8.38	**Removable Storage Access**		
18.8.39	**Scripts**		
18.8.40	**Security Account Manager**		
18.8.40.1	(L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) (Automated)	□	□
18.8.41	**Server Manager**		
18.8.42	**Service Control Manager Settings**		
18.8.43	**Shutdown**		
18.8.44	**Shutdown Options**		
18.8.45	**Storage Health**		
18.8.46	**Storage Sense**		
18.8.47	**System Restore**		
18.8.48	**Troubleshooting and Diagnostics**		
18.8.49	**Trusted Platform Module Services**		
18.8.50	**User Profiles**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.8.51	**Windows File Protection**		
18.8.52	**Windows HotStart**		
18.8.53	**Windows Time Service**		
18.9	**Windows Components**		
18.9.1	**Active Directory Federation Services**		
18.9.2	**ActiveX Installer Service**		
18.9.3	**Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)**		
18.9.4	**App Package Deployment**		
18.9.5	**App Privacy**		
18.9.6	**App runtime**		
18.9.6.1	(L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)	□	□
18.9.7	**Application Compatibility**		
18.9.8	**AutoPlay Policies**		
18.9.9	**Backup**		
18.9.10	**Biometrics**		
18.9.11	**BitLocker Drive Encryption**		
18.9.12	**Camera**		
18.9.13	**Chat**		
18.9.14	**Cloud Content**		
18.9.14.1	(L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.14.2	(L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)	□	□
18.9.15	**Connect**		
18.9.16	**Credential User Interface**		
18.9.16.1	(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	□	□
18.9.16.2	(L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	□	□
18.9.17	**Data Collection and Preview Builds**		
18.9.17.1	(L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Send required diagnostic data' (Automated)	□	□
18.9.18	**Delivery Optimization**		
18.9.19	**Desktop Gadgets**		
18.9.20	**Desktop Window Manager**		
18.9.21	**Device and Driver Compatibility**		
18.9.22	**Device Registration (formerly Workplace Join)**		
18.9.23	**Digital Locker**		
18.9.24	**Edge UI**		
18.9.25	**EMET**		
18.9.26	**Event Forwarding**		
18.9.27	**Event Log Service**		
18.9.27.1	**Application**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.27.1.1	(L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	□	□
18.9.27.1.2	(L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	□	□
18.9.27.2	**Security**		
18.9.27.2.1	(L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	□	□
18.9.27.2.2	(L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	□	□
18.9.27.3	**Setup**		
18.9.27.3.1	(L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	□	□
18.9.27.3.2	(L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	□	□
18.9.27.4	**System**		
18.9.27.4.1	(L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	□	□
18.9.27.4.2	(L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	□	□
18.9.28	**Event Logging**		
18.9.29	**Event Viewer**		
18.9.30	**Family Safety (formerly Parental Controls)**		
18.9.31	**File Explorer (formerly Windows Explorer)**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.31.1	**Previous Versions**		
18.9.31.2	(L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	□	□
18.9.31.3	(L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	□	□
18.9.31.4	(L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	□	□
18.9.32	**File History**		
18.9.33	**Find My Device**		
18.9.34	**Game Explorer**		
18.9.35	**Handwriting**		
18.9.36	**HomeGroup**		
18.9.37	**Human Presence**		
18.9.38	**Import Video**		
18.9.39	**Internet Explorer**		
18.9.40	**Internet Information Services**		
18.9.41	**Location and Sensors**		
18.9.42	**Maintenance Scheduler**		
18.9.43	**Maps**		
18.9.44	**MDM**		
18.9.45	**Messaging**		
18.9.46	**Microsoft account**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.46.1	(L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)	□	□
18.9.47	**Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)**		
18.9.47.1	**Client Interface**		
18.9.47.2	**Device Control**		
18.9.47.3	**Exclusions**		
18.9.47.4	**MAPS**		
18.9.47.4.1	(L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	□	□
18.9.47.5	**Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)**		
18.9.47.5.1	**Attack Surface Reduction**		
18.9.47.5.1.1	(L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	□	□
18.9.47.5.1.2	(L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)	□	□
18.9.47.5.2	**Controlled Folder Access**		
18.9.47.5.3	**Network Protection**		
18.9.47.5.3.1	(L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	□	□
18.9.47.6	**MpEngine**		
18.9.47.7	**Network Inspection System**		
18.9.47.8	**Quarantine**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.47.9	**Real-time Protection**		
18.9.47.9.1	(L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	□	□
18.9.47.9.2	(L1) Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	□	□
18.9.47.9.3	(L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	□	□
18.9.47.9.4	(L1) Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	□	□
18.9.47.10	**Remediation**		
18.9.47.11	**Reporting**		
18.9.47.12	**Scan**		
18.9.47.12.1	(L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	□	□
18.9.47.13	**Security Intelligence Updates (formerly Signature Updates)**		
18.9.47.14	**Threats**		
18.9.47.15	(L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	□	□
18.9.47.16	(L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)	□	□
18.9.48	**Microsoft Defender Application Guard (formerly Windows Defender Application Guard)**		
18.9.49	**Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)**		
18.9.50	**Microsoft Edge**		
18.9.51	**Microsoft FIDO Authentication**		

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
18.9.52	**Microsoft Secondary Authentication Factor**		
18.9.53	**Microsoft User Experience Virtualization**		
18.9.54	**NetMeeting**		
18.9.55	**Network Access Protection**		
18.9.56	**Network Projector**		
18.9.57	**News and interests**		
18.9.58	**OneDrive (formerly SkyDrive)**		
18.9.59	**Online Assistance**		
18.9.60	**OOBE**		
18.9.61	**Password Synchronization**		
18.9.62	**Portable Operating System**		
18.9.63	**Presentation Settings**		
18.9.64	**Push To Install**		
18.9.65	**Remote Desktop Services (formerly Terminal Services)**		
18.9.65.1	**RD Licensing (formerly TS Licensing)**		
18.9.65.2	**Remote Desktop Connection Client**		
18.9.65.2.1	**RemoteFX USB Device Redirection**		
18.9.65.2.2	(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	□	□
18.9.65.3	**Remote Desktop Session Host (formerly Terminal Server)**		
18.9.65.3.1	**Application Compatibility**		
18.9.65.3.2	**Connections**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.65.3.3	**Device and Resource Redirection**		
18.9.65.3.3.1	(L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	□	□
18.9.65.3.4	**Licensing**		
18.9.65.3.5	**Printer Redirection**		
18.9.65.3.6	**Profiles**		
18.9.65.3.7	**RD Connection Broker (formerly TS Connection Broker)**		
18.9.65.3.8	**Remote Session Environment**		
18.9.65.3.9	**Security**		
18.9.65.3.9.1	(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	□	□
18.9.65.3.9.2	(L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	□	□
18.9.65.3.9.3	(L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	□	□
18.9.65.3.10	**Session Time Limits**		
18.9.65.3.11	**Temporary folders**		
18.9.65.3.11.1	(L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	□	□
18.9.65.3.11.2	(L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)	□	□
18.9.66	**RSS Feeds**		
18.9.66.1	(L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	□	□
18.9.67	**Search**		

<table>
<tr><th colspan="2" rowspan="2">CIS Benchmark Recommendation</th><th colspan="2">Set Correctly</th></tr>
<tr><th>Yes</th><th>No</th></tr>
<tr><td><b>18.9.67.1</b></td><td colspan="3"><b>OCR</b></td></tr>
<tr><td>18.9.67.2</td><td>(L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)</td><td>□</td><td>□</td></tr>
<tr><td><b>18.9.68</b></td><td colspan="3"><b>Security Center</b></td></tr>
<tr><td><b>18.9.69</b></td><td colspan="3"><b>Server for NIS</b></td></tr>
<tr><td><b>18.9.70</b></td><td colspan="3"><b>Shutdown Options</b></td></tr>
<tr><td><b>18.9.71</b></td><td colspan="3"><b>Smart Card</b></td></tr>
<tr><td><b>18.9.72</b></td><td colspan="3"><b>Software Protection Platform</b></td></tr>
<tr><td><b>18.9.73</b></td><td colspan="3"><b>Sound Recorder</b></td></tr>
<tr><td><b>18.9.74</b></td><td colspan="3"><b>Speech</b></td></tr>
<tr><td><b>18.9.75</b></td><td colspan="3"><b>Store</b></td></tr>
<tr><td><b>18.9.76</b></td><td colspan="3"><b>Sync your settings</b></td></tr>
<tr><td><b>18.9.77</b></td><td colspan="3"><b>Tablet PC</b></td></tr>
<tr><td><b>18.9.78</b></td><td colspan="3"><b>Task Scheduler</b></td></tr>
<tr><td><b>18.9.79</b></td><td colspan="3"><b>Tenant Restrictions</b></td></tr>
<tr><td><b>18.9.80</b></td><td colspan="3"><b>Text Input</b></td></tr>
<tr><td><b>18.9.81</b></td><td colspan="3"><b>Widgets</b></td></tr>
<tr><td><b>18.9.82</b></td><td colspan="3"><b>Windows Calendar</b></td></tr>
<tr><td><b>18.9.83</b></td><td colspan="3"><b>Windows Color System</b></td></tr>
<tr><td><b>18.9.84</b></td><td colspan="3"><b>Windows Customer Experience Improvement Program</b></td></tr>
<tr><td><b>18.9.85</b></td><td colspan="3"><b>Windows Defender SmartScreen</b></td></tr>
<tr><td><b>18.9.85.1</b></td><td colspan="3"><b>Explorer</b></td></tr>
</table>

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
18.9.85.1.1	(L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	□	□
18.9.86	**Windows Error Reporting**		
18.9.87	**Windows Game Recording and Broadcasting**		
18.9.88	**Windows Hello for Business (formerly Microsoft Passport for Work)**		
18.9.89	**Windows Ink Workspace**		
18.9.90	**Windows Installer**		
18.9.90.1	(L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)	□	□
18.9.90.2	(L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	□	□
18.9.91	**Windows Logon Options**		
18.9.91.1	(L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)	□	□
18.9.92	**Windows Mail**		
18.9.93	**Windows Media Center**		
18.9.94	**Windows Media Digital Rights Management**		
18.9.95	**Windows Media Player**		
18.9.96	**Windows Meeting Space**		
18.9.97	**Windows Messenger**		
18.9.98	**Windows Mobility Center**		
18.9.99	**Windows Movie Maker**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.100	**Windows PowerShell**		
18.9.100.1	(L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	□	□
18.9.100.2	(L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Automated)	□	□
18.9.101	**Windows Reliability Analysis**		
18.9.102	**Windows Remote Management (WinRM)**		
18.9.102.1	**WinRM Client**		
18.9.102.1.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	□	□
18.9.102.1.2	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	□	□
18.9.102.1.3	(L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	□	□
18.9.102.2	**WinRM Service**		
18.9.102.2.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	□	□
18.9.102.2.2	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	□	□
18.9.102.2.3	(L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)	□	□
18.9.103	**Windows Remote Shell**		
18.9.104	**Windows Sandbox**		
18.9.105	**Windows Security (formerly Windows Defender Security Center)**		
18.9.105.1	**Account protection**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.105.2	**App and browser protection**		
18.9.105.2.1	(L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	□	□
18.9.106	**Windows SideShow**		
18.9.107	**Windows System Resource Manager**		
18.9.108	**Windows Update**		

Appendix: Change History

Date	Version	Changes for this version
09/19/2022	1.0.0	Initial Public Release