CENTER FOR INTERNET SECURITY

# CIS Microsoft Windows Server 2012 R2

v1.0.0 - 09-15-2014

http://benchmarks.cisecurity.org

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

## *CIS SECURITY BENCHMARKS TERMS OF USE*

### *BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:*

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

### *UNDER THE FOLLOWING TERMS AND CONDITIONS:*

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

***SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS:*** CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

# Table of Contents

# Overview

This document, CIS Microsoft Windows Server 2012 R2 Benchmark v1.0.0, provides prescriptive guidance for establishing a secure configuration posture for CIS Microsoft Windows Server 2012 R2. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Windows Server 2012 R2.

## Consensus Guidance

This benchmark was created using a consensus review process comprised subject matter experts. 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://community.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 |

## Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

**Scored**

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

**Not Scored**

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Domain Controller**

  Items in this profile apply to Domain Controllers 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 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

# 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:

**Editor**
Haemish Edgerton MCSE: Security, MCITP:EA
Hardeep Mehrotara CISSP, CISA, GSEC, ISMSA
Kevin Zhang CISSP, CISA

The Center for Internet Security extends special recognition and thanks to Microsoft's Aaron Margosis, Rick Munck, and the rest of the Security Compliance Manager teams for their collaboration developing the configuration recommendations contained in this document.

# Recommendations

## *1 Account Policies*

This section contains recommendations for account policies.

## *1.1 Password Policy*

Password Policy

### *1.1.1 Set 'Enforce password history' to '24 or more password(s)' (Scored)*

**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 Windows Vista is 0 passwords, but the default setting in 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).`

**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.

**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, set the following Group Policy setting to `24 or more password(s)`.

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

**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.

**Default Value:**

24 passwords remembered

**References:**

1. CCE-37166-6

## *1.1.2 Set 'Maximum password age' to '60 or fewer day(s)' (Scored)*

**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. The default value for this policy setting is 42 days.
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: `60 or fewer day(s).`

**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 is authorized access.

**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, set the following Group Policy setting to `60 fewer day(s).`

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

**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.

**Default Value:**

42 days

**References:**

1. CCE-37167-4

## *1.1.3 Set 'Minimum password age' to '1 or more day(s)' (Scored)*

**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).`

**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.

**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, set the following Group Policy setting to `1 or more day(s).`

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

**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.

**Default Value:**

0 days

**References:**

1. CCE-37073-4

## *1.1.4 Set 'Minimum password length' to '14 or more character(s)' (Scored)*

**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 "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; 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).`

**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.

**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, set the following Group Policy setting to `14 or more character(s)`.

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

**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 pass phrases, 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.

**Default Value:**

0 characters

**References:**

1. CCE-36534-6

## *1.1.5 Set 'Password must meet complexity requirements' to 'Enabled' (Scored)*

**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 four 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`.

**Rationale:**

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

**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, set the following Group Policy setting to `Enabled`.

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

**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 01280159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

**Default Value:**

Disabled

**References:**

1. CCE-37063-5

## *1.1.6 Set 'Store passwords using reversible encryption' to 'Disabled' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Disabled`.

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

**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.

**Default Value:**

Disabled

**References:**

1. CCE-36286-3

## *1.2 Account Lockout Policy*

Account Lockout Policy

### *1.2.1 Set 'Account lockout duration' to '15 or more minute(s)' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.
Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer. The recommended state for this setting is: `15 or more minute(s)`.

**Rationale:**

A denial of service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting to 0, then the account will remain locked out until an administrator unlocks it manually.

**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, set the following Group Policy setting to `15 or more minute(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Account lockout duration
```

**Impact:**

Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

**Default Value:**

Not defined

**References:**

1. CCE-37034-6

## *1.2.2 Set 'Account lockout threshold' to '5 or fewer but not 0 invalid logon attempt(s)' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines the number of failed logon attempts before a lock occurs. Authorized users can lock themselves out of an account by mistyping their password or by remembering it incorrectly, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password will continuously try to authenticate the user, and because the password it uses to authenticate is incorrect, a lock occurs. To avoid accidental lockout of authorized users, set the account lockout threshold to a high number. The default value for this policy setting is 0 invalid logon attempts, which disables the account lockout feature.
Because it is possible for an attacker to use this lockout state as a denial of service (DoS) by triggering a lockout on a large number of accounts, your organization should determine whether to use this policy setting based on identified threats and the risks you want to mitigate. There are two options to consider for this policy setting.
- Configure the value for Account lockout threshold to 0 to ensure that accounts will not be locked out. This setting value will prevent a DoS attack that attempts to lock out accounts in your organization. It will also reduce help desk calls, because users will not be able to lock themselves out of their accounts accidentally. However, this setting value will not prevent a brute force attack. The following defenses should also be considered:
- A password policy that forces all users to have complex passwords made up of 8 or more characters.
- A robust auditing mechanism, which will alert administrators when a series of account

lockouts occurs in the environment. For example, the auditing solution should monitor for security event 539, which is a logon failure. This event identifies that there was a lock on the account at the time of the logon attempt.
The second option is:
- Configure the value for Account lockout threshold to a value that provides users with the ability to mistype their password several times, but locks out the account if a brute force password attack occurs. This configuration will prevent accidental account lockouts and reduce help desk calls, but will not prevent a DoS attack. The recommended state for this setting is: 5 `or fewer but not 0 invalid logon attempt(s).`

**Rationale:**

Password attacks can use automated methods to try millions of password combinations for any user account. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed.
However, a DoS attack could be performed on a domain that has an account lockout threshold configured. An attacker could programmatically attempt a series of password attacks against all users in the organization. If the number of attempts is greater than the account lockout threshold, the attacker might be able to lock out every account.

**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, set the following Group Policy setting to 5 `or fewer but not 0 invalid logon attempt(s).`

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Account lockout threshold
```

**Impact:**

If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting will likely generate a number of additional help desk calls. In fact, locked accounts cause the greatest number of calls to the help desk in many organizations.
If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value such as 15 minutes.
If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's

attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

**Default Value:**

0 invalid logon attempts

**References:**

1. CCE-36008-1

## *1.2.3 Set 'Reset account lockout counter after' to '15 or more minute(s)' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting.
If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: `15 or more minute(s).`

**Rationale:**

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

**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, set the following Group Policy setting to `15 or more minute(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Reset account lockout counter after
```

**Impact:**

If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user's account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

**Default Value:**

0

**References:**

1. CCE-36883-7

# *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 setting contains recommendations for user rights assignments.

### *2.2.1 Set 'Access Credential Manager as a trusted caller' to 'No One' (Scored)*

**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.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None, this is the default configuration

**Default Value:**

No one

**References:**

1. CCE-37056-9

## *2.2.2 Set 'Access this computer from the network' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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+).

- Level 1 - Domain Controller. The recommended state for this setting is: `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`.
- Level 1 - Member Server. 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 in the group 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.

**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, set the following Group Policy setting:

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

**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, therefor it is recommended that it is assigned to the 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.

**Default Value:**

Everyone, Administrators, Users, Backup Operators

**References:**

1. CCE-35818-4

### *2.2.3 Set 'Act as part of the operating system' to 'No One' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `No One`.

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

**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.

**Default Value:**

No one

**References:**

1. CCE-36876-1

## *2.2.4 Set 'Add workstations to domain' to 'Administrators' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

**Description:**

This policy setting specifies which users can add computer workstations to a specific 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 they have been assigned the Add workstations to a domain user right.
By default, all users in the Authenticated Users group 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.
In Windowsbased 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 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.

**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, set the following Group Policy setting to `Administrators`.

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

**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 computers unless they are removed from and re-added to the domain.

**Default Value:**

Not defined (Authenticated Users for domain controllers)

**References:**

1. CCE-36282-2

## *2.2.5 Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Scored)*

**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`.

**Rationale:**

A user with the Adjust memory quotas for a process privilege 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.

**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, set the following Group Policy setting to `Administrators, LOCAL SERVICE, NETWORK SERVICE`.

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

**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. IIS requires that this privilege be explicitly assigned to the IWAM_<ComputerName>, Network Service, and Service accounts. 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.

**Default Value:**

Administrators, LOCAL SERVICE, NETWORK SERVICE

**References:**

1. CCE-37071-8

## *2.2.6 Set 'Allow log on locally' to 'Administrators' (Scored)*

**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 or IIS also require this user right.
The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability.
The recommended state for this setting is: `Administrators`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. If you have installed optional components such as ASP.NET or Internet Information Services, you may need to assign Allow log on locally user right to additional accounts that are required by those components. For example, IIS 6 requires that this user right be assigned to the IUSR_<ComputerName> account for certain features; see "Default permissions and user rights for IIS 6.0" for more information: http://support.microsoft.com/?id=812614. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

**Default Value:**

Administrators, Users, Backup Operators

**References:**

1. CCE-37659-0

## *2.2.7 Set 'Allow log on through Remote Desktop Services' to 'Administrators' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. 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`.

**Rationale:**

Any account with the Allow log on through Terminal 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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

Removal of the Allow log on through Terminal 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.

**Default Value:**

Administrators, Remote Desktop Users

**References:**

1. CCE-37072-6

## *2.2.8 Set 'Back up files and directories' to 'Administrators' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**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.

**Default Value:**

Administrators, Backup Operators

**References:**

1. CCE-35912-5

## *2.2.9 Set 'Change the system time' to 'Administrators, LOCAL SERVICE' (Scored)*

**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.
When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.
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. The recommended state for this setting is: `Administrators, LOCAL SERVICE`.

**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.

**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, set the following Group Policy setting to `Administrators, LOCAL SERVICE`.

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

**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.

**Default Value:**

Administrators, LOCAL SERVICE

**References:**

1. CCE-37452-0

## *2.2.10 Set 'Change the time zone' to 'Administrators, LOCAL SERVICE' (Scored)*

**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.

**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, set the following Group Policy setting to `Administrators, LOCAL SERVICE`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators, LOCAL SERVICE

**References:**

1. CCE-37700-2

## *2.2.11 Set 'Create a pagefile' to 'Administrators' (Scored)*

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-35821-8

## *2.2.12 Set 'Create a token object' to 'No One' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

No one

**References:**

1. CCE-36861-3

## *2.2.13 Set 'Create global objects' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE

**References:**

1. CCE-37453-8

## *2.2.14 Set 'Create permanent shared objects' to 'No One' (Scored)*

**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.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

No one

**References:**

1. CCE-36532-0

## *2.2.15 Set 'Create symbolic links' to 'Administrators' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**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.

**Default Value:**

Administrators

**References:**

1. CCE-35823-4

## *2.2.16 Set 'Debug programs' to 'Administrators' (Scored)*

**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.
Note Microsoft released several security updates in October 2003 that used a version of Update.exe that required the administrator to have the Debug programs user right. Administrators who did not have this user right were unable to install these security updates until they reconfigured their user rights. This is not typical behavior for operating system updates. For more information, see Knowledge Base article 830846: "Windows Product Updates may stop responding or may use most or all the CPU resources."
The recommended state for this setting is: `Administrators`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**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 privilege; if it does not have it, Windows Clustering will fail. For additional information about how to configure Windows Clustering in conjunction with computer hardening, see article 891597, How to apply more restrictive security settings on a Windows Server 2003based cluster server, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100746).
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.
Also, some older versions of Update.exe (which is used to install Windows product updates) require the account that applies the update to have this user right. If you install one of the patches that uses this version of Update.exe, the computer could become unresponsive. For more information, see article 830846, Windows Product Updates may stop responding or may use most or all the CPU resources, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100747).

**Default Value:**

Administrators

**References:**

1. CCE-37075-9

## *2.2.17 Set 'Deny access to this computer from the network' (Scored)*

**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.

- Level 1 - Domain Controller. The recommended state for this setting is to include: `Guests, Local account`.
- Level 1 - Member Server. The recommended state for this setting is to include: `Guests, Local account and member of Administrators group.`

**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.

**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, set the following Group Policy setting:

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

**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.

**Default Value:**

Guests

**References:**

1. CCE-37954-5

## *2.2.18 Set 'Deny log on as a batch job' to include 'Guests' (Scored)*

**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.
The Deny log on as a batch job user right overrides 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 Deny 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.

**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, set the following Group Policy setting to include `Guests`.

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

**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.

**Default Value:**

No one

**References:**

1. CCE-36923-1

## *2.2.19 Set 'Deny log on as a service' to include 'Guests' (Scored)*

**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 policy setting supersedes the Log on as a service policy setting if an account is subject to both policies.Note: This security setting does not apply to the System, Local Service, or Network Service accounts.
The recommended state for this setting is to include: `Guests`.

**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.

**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, set the following Group Policy setting to include `Guests`.

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

**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.

**Default Value:**

No one

**References:**

1. CCE-36165-9

## *2.2.20 Set 'Deny log on locally' to include 'Guests' (Scored)*

**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.Important:If you apply this security policy to the Everyone group, no one will be able to log on locally.
The recommended state for this setting is to include: `Guests`.

**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.

**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, set the following Group Policy setting to include: `Guests`.

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

**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.

**Default Value:**

Guests

**References:**

1. CCE-37146-8

## *2.2.21 Set 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether users can log on as Terminal Services 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. The recommended state for this setting is to include: `Guests, Local account`.

**Rationale:**

Any account with the right to log on through Terminal 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.

**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, Local account`.

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

**Impact:**

If you assign the Deny log on through Terminal 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 Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

**Default Value:**

No one

**References:**

1. CCE-36867-0

## *2.2.22 Set 'Enable computer and user accounts to be trusted for delegation' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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.

- Level 1 - Domain Controller. The recommended state for this setting is: `Administrators`.
- Level 1 - Member Server. The recommended state for this setting is: `No One`.

**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.

**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, set the following Group Policy setting:

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

**Impact:**

None. This is the default configuration.

**Default Value:**

No one

**References:**

1. CCE-36860-5

## *2.2.23 Set 'Force shutdown from a remote system' to 'Administrators' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting allows users to shut down Windows Vistabased 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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

If you remove the Force shutdown from a remote system user right from the Server Operator 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.

**Default Value:**

Administrators

**References:**

1. CCE-37877-8

## *2.2.24 Set 'Generate security audits' to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `LOCAL SERVICE, NETWORK SERVICE`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

LOCAL SERVICE, NETWORK SERVICE

**References:**

1. CCE-37639-2

## *2.2.25 Set 'Impersonate a client after authentication' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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`.

**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.

**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, set the following Group Policy setting to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

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

**Impact:**

In most cases this configuration will have no impact. If you have installed optional components such as ASP.NET or IIS, you may need to assign the Impersonate a client after authentication user right to additional accounts that are required by those components, such as IUSR_<ComputerName>, IIS_WPG, ASP.NET or IWAM_<ComputerName>.

**Default Value:**

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE

**References:**

1. CCE-37106-2

## *2.2.26 Set 'Increase scheduling priority' to 'Administrators' (Scored)*

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-38326-5

## *2.2.27 Set 'Load and unload device drivers' to 'Administrators' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**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.

**Default Value:**

Administrators

**References:**

1. CCE-36318-4

## *2.2.28 Set 'Lock pages in memory' to 'No One' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

No one

**References:**

1. CCE-36495-0

## *2.2.29 Set 'Manage auditing and security log' to 'Administrators' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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.
The recommended state for this setting is: `Administrators`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-35906-7

## *2.2.30 Set 'Modify an object label' to 'No One' (Scored)*

**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 an other user a malicious user may cause them to execute code at a higher level of privilege than intended.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None, by default the Administrators group has this user right.

**Default Value:**

None

**References:**

1. CCE-36054-5

## *2.2.31 Set 'Modify firmware environment values' to 'Administrators' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-38113-7

## *2.2.32 Set 'Perform volume maintenance tasks' to 'Administrators' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-36143-6

## *2.2.33 Set 'Profile single process' to 'Administrators' (Scored)*

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

If you remove the Profile single process user right from the Power Users 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.

**Default Value:**

Administrators

**References:**

1. CCE-37131-0

## *2.2.34 Set 'Profile system performance' to 'Administrators, NT SERVICE\WdiServiceHost' (Scored)*

**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.

**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, set the following Group Policy setting to `Administrators, NT SERVICE\WdiServiceHost`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators, NT SERVICE\WdiServiceHost

**References:**

1. CCE-36052-9

## *2.2.35 Set 'Replace a process level token' to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)*

**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`.

**Rationale:**

User 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.)

**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, set the following Group Policy setting to `LOCAL SERVICE, NETWORK SERVICE`.

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

**Impact:**

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need

to assign the Replace a process level token privilege to additional accounts. For example, IIS requires that the Service, Network Service, and IWAM_<ComputerName> accounts be explicitly granted this user right.

**Default Value:**

LOCAL SERVICE, NETWORK SERVICE

**References:**

1. CCE-37430-6

## *2.2.36 Set 'Restore files and directories' to 'Administrators' (Scored)*

**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 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`.

**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 are used to back up data.

**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, set the following Group Policy setting to `Administrators`.

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

**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.

**Default Value:**

Administrators, Backup Operators

**References:**

1. CCE-37613-7

## *2.2.37 Set 'Shut down the system' to 'Administrators' (Scored)*

**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`.

**Rationale:**

The ability to shut down domain controllers 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.
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 SingleMaster Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords—the Primary Domain Controller (PDC) Emulator role.

**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, set the following Group Policy setting to `Administrators`.

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

**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.

**Default Value:**

Administrators, Backup Operators

**References:**

1. CCE-38328-1

## *2.2.38 Set 'Synchronize directory service data' to 'No One' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

**Description:**

This security setting determines which users and groups have the authority to synchronize all directory service data. 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.

**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, set the following Group Policy setting to `No One`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Not defined

**References:**

1. CCE-36099-0

## *2.2.39 Set 'Take ownership of files or other objects' to 'Administrators' (Scored)*

**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`.

**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.

**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, set the following Group Policy setting to `Administrators`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Administrators

**References:**

1. CCE-38325-7

## *2.3 Security Options*

This section contains recommendation for security options.

## *2.3.1 Accounts*

### *2.3.1.1 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled' (Scored)*

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Enabled

**References:**

1. CCE-37615-2

### *2.3.1.2 Configure 'Accounts: Rename administrator account' (Scored)*

**Profile Applicability:**

- 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). Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

**Rationale:**

The Administrator account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional 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 thattempt 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.

**Audit:**

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

**Remediation:**

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

**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.)

**Default Value:**

Administrator

### *2.3.1.3 Configure 'Accounts: Rename guest account' (Scored)*

**Profile Applicability:**

- 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.

**Rationale:**

The Guest account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

**Audit:**

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

**Remediation:**

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

**Impact:**

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

**Default Value:**

Guest

**References:**

1. CCE-38027-9

## *2.3.2 Audit*

### *2.3.2.1 Set 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' to 'Enabled' (Scored)*

**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`.

**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.

**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\scenoapplylegacyauditpolicy
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

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

**Impact:**

The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.
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.

**Default Value:**

Not defined

**References:**

1. CCE-37850-5

### *2.3.2.2 Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled' (Scored)*

**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. Therefore, this policy setting is configured to Not Defined for both of the environments that are discussed in this chapter. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

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

**Impact:**

If you enable this policy setting, 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.

**Default Value:**

Disabled

**References:**

1. CCE-35907-5

## *2.3.3 DCOM*

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

## *2.3.4 Devices*

### *2.3.4.1 Set 'Devices: Allowed to format and eject removable media' to 'Administrators' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines who is allowed to format and eject removable media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: `Administrators`.

**Rationale:**

Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

**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\AllocateDASD
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Allowed to format and eject removable media
```

**Impact:**

Only Administrators will be able to format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they will need to be informed of the change in policy.

**Default Value:**

Administrators

**References:**

1. CCE-37701-0

## *2.3.4.2 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

It is feasible for a attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network. To reduce the possibility of such an event, only administrators should be allowed to install printer drivers. However, because laptops are mobile devices, laptop users may occasionally need to install a printer driver from a remote source to continue their work. Therefore, this policy setting should be disabled for laptop users, but always enabled for desktop users. The recommended state for this setting is: `Enabled`.

**Rationale:**

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only Administrators, not users, to do so on servers, because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver.

**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\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Prevent users from installing printer drivers
```

**Impact:**

Only users with Administrative, Power User, or Server Operator privileges will be able to install printers on the servers. If this policy setting is enabled but the driver for a network printer already exists on the local computer, users can still add the network printer.

**Default Value:**

Enabled

**References:**

1. CCE-37942-0

## *2.3.5 Domain controller*

### *2.3.5.1 Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled' (Scored)*

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

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

**Impact:**

The impact 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. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

**Default Value:**

Not defined

**References:**

1. CCE-37848-9

## *2.3.5.2 Set 'Domain controller: LDAP server signing requirements' to 'Require signing' (Scored)*

**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`.

**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.

**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\ldapserverintegrity
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Require signing`.

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

**Impact:**

Clients that do not support LDAP signing will be unable to run LDAP queries against the domain controllers. All Windows 2000based computers in your organization that are managed from Windows Server 2003based or Windows XPbased 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 article 325465, Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100900). 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.

**Default Value:**

Not defined

**References:**

1. CCE-35904-2

## *2.3.5.3 Set 'Domain controller: Refuse machine account password changes' to 'Disabled' (Scored)*

**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. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.
If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password.
Default: This policy is not defined, which means that the system treats it as Disabled. The recommended state for this setting is: `Disabled`.

**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.

**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\RefusePasswor
dChange
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Not defined

**References:**

1. CCE-36921-5

## 2.3.6 Domain member

### 2.3.6.1 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled' (Scored)

**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. If a system is set to always encrypt or sign secure channel data, it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data must be signed and encrypted.
Microsoft recommends to configure the Domain member: Digitally encrypt or sign secure channel data (always) setting to Enabled. 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

**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\requiresignor
seal
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

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

**Impact:**

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. 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 the 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. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.
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. 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 the 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. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

**Default Value:**

Enabled

**References:**

1. CCE-36142-8

## *2.3.6.2 Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled' (Scored)*

**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. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption.
Microsoft recommends to configure the Domain member: Digitally encrypt secure channel

data (when possible) setting to Enabled. The recommended state for this setting is: `Enabled`.

**Rationale:**

When a Windows Server 2003, Windows XP, Windows 2000, or Windows NT 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

**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\sealsecurechannel
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

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

**Impact:**

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. 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 the 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:

**Default Value:**

Enabled

**References:**

1. CCE-37130-2

## *2.3.6.3 Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled' (Scored)*

**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.
Microsoft recommends to configure the Domain member: Digitally sign secure channel data (when possible) setting to Enabled. 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

**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\signsecurecha
nnel
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

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

**Impact:**

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. 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 the 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. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

**Default Value:**

Enabled

**References:**

1. CCE-37222-7

### *2.3.6.4 Set 'Domain member: Disable machine account password changes' to 'Disabled' (Scored)*

**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. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the Domain Member: Maximum machine account password age setting, which by default is every 30 days. 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`.

**Rationale:**

The default configuration for Windows Server 2003based 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.

**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\disablepasswo
rdchange
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

Disabled

**References:**

1. CCE-37508-9

## *2.3.6.5 Set 'Domain member: Maximum machine account password age' to '30 or fewer day(s)' (Scored)*

**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. If you increase this interval significantly or set it to 0 so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: `30 or fewer day(s).`

**Rationale:**

In Active Directorybased 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 password of one or more computer accounts.

**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, set the following Group Policy setting to `30 or fewer day(s)`.

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

**Impact:**

None. This is the default configuration.

**Default Value:**

30 days

**References:**

1. CCE-37431-4

## *2.3.6.6 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.
To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000based domains is required, it is recommended that you disable this policy setting. The recommended state for this setting is: `Enabled`.

**Rationale:**

Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems.
Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks thattempt to hijack network sessions

and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

**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\requirestrong key
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key
```

**Impact:**

Computers that have this policy setting enabled will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, computers that do not support this policy setting will not be able to join domains in which the domain controllers have this policy setting enabled.

**Default Value:**

Disabled

**References:**

1. CCE-37614-5

## *2.3.7 Interactive logon*

### *2.3.7.1 Set 'Interactive logon: Do not display last user name' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. 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 Terminal 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.

**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\DontDispl
ayLastUserName
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Do not display last user name
```

**Impact:**

Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

**Default Value:**

Disabled

**References:**

1. CCE-36056-0

## *2.3.7.2 Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether users must press CTRL+ALT+DEL before they log on. If you enable this policy setting, users can log on without this key combination. If you disable this policy setting, users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information. The recommended state for this setting is: `Disabled`.

**Rationale:**

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks thattempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path.
An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

**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\DisableCAD
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
```

**Impact:**

Unless they use a smart card to log on, users will have to simultaneously press three keys before the logon dialog box will display.

**Default Value:**

Disabled

**References:**

1. CCE-37637-6

## *2.3.7.3 Set 'Interactive logon: Machine inactivity limit' to '900 or fewer seconds' (Scored)*

**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 of fewer seconds`.

**Rationale:**

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

**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 implement the recommended configuration state, set the following Group Policy setting to `900 or fewer seconds`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
```

**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.

**Default Value:**

Not defined

**References:**

1. CCE-38235-8

## *2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' (Scored)*

**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.

**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\LegalNoti
ceText
```

**Remediation:**

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Message text for users attempting to log on
```

**Impact:**

Users will see a message in a dialog box before they can log on to the server console.
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. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.
Important
If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

**Default Value:**

Not defined

**References:**

1. CCE-37226-8

## *2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting allows text to be specified 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.

**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\LegalNoti
ceCaption
```

**Remediation:**

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Message title for users attempting to log on
```

**Impact:**

Users will see a message in a dialog box before they can log on to the server console.
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. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.
Important
If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

**Default Value:**

Not defined

**References:**

1. CCE-37512-1

## *2.3.7.6 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: `4 or fewer logon(s)`.

**Rationale:**

The number that is assigned to this policy setting indicates the number of users whose logon information the servers will cache locally. If the number is set to 10, then the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session.
Users who access the server console will have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to attempt to determine user passwords.
To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

**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\cachedlogonscount
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `4 or fewer logon(s).`

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Number of previous logons to cache (in case domain
controller is not available)
```

**Impact:**

Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

**Default Value:**

10 logons

**References:**

1. CCE-37439-7

## *2.3.7.7 Set 'Interactive logon: Prompt user to change password before expiration' to 'between 5 and 14 days' (Scored)*

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `between 5 and 14 day(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Prompt user to change password before expiration
```

**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.

**Default Value:**

14 days

**References:**

1. CCE-37622-8

## *2.3.7.8 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: `Lock Workstation`.

**Rationale:**

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

**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\scremoveoption
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Lock Workstation`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Smart card removal behavior
```

**Impact:**

If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

**Default Value:**

No Action

**References:**

1. CCE-38333-1

## *2.3.8 Microsoft network client*

### *2.3.8.1 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled' (Scored)*

**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. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments.
Note When Windows Vistabased 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.

**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\Requ
ireSecuritySignature
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (always)
```

**Impact:**

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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

**Default Value:**

Disabled

**References:**

1. CCE-36325-9

## *2.3.8.2 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled' (Scored)*

**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. The implementation of digital signing in Windowsbased networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network client will use signing only if the server with which it communicates accepts digitally signed communication.
Microsoft recommends to enable The Microsoft network client: Digitally sign communications (if server agrees) setting.
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.

**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\Enab
leSecuritySignature
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (if server agrees)
```

**Impact:**

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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

**Default Value:**

Enabled

**References:**

1. CCE-36269-9

## *2.3.8.3 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

Disable this policy setting to prevent the SMB redirector from sending 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. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

**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\Enab
lePlainTextPassword
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Send unencrypted password to third-party SMB servers
```

**Impact:**

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.

**Default Value:**

Disabled

**References:**

1. CCE-37863-8

## 2.3.9 Microsoft network server

### 2.3.9.1 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15 or fewer minute(s)' (Scored)

**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.
A value of 0 will disconnect an idle session as quickly as possible. The maximum value is 99999, which is 208 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.

**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\autodisco
nnect
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `15 or fewer minute(s).`

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Amount of idle time required before suspending
session
```

**Impact:**

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

**Default Value:**

15 minutes

**References:**

1. CCE-38046-9

## *2.3.9.2 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines if the server side SMB service is required to perform SMB packet signing. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
```

**Impact:**

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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

**Default Value:**

Disabled

**References:**

1. CCE-37864-6

### *2.3.9.3 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Digitally sign communications (if client agrees)
```

**Impact:**

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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

**Default Value:**

Disabled

**References:**

1. CCE-35988-5

## *2.3.9.4 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service will be forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire.
If your organization configures logon hours for users, it makes sense to enable this policy setting. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire
```

**Impact:**

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.

**Default Value:**

Enabled

**References:**

1. CCE-37972-7

## *2.3.9.5 Set 'Microsoft network server: Server SPN target name validation level' to 'Accept if provided by client' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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.
This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: `Accept if provided by client`.

**Rationale:**

The identity of a computer can be spoofed to gain unauthorized access to network 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\LanManServer\Parameters\SMBServer
NameHardeningLevel
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Accept if provided by client`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Server SPN target name validation level
```

**Impact:**

ll 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.

**Default Value:**

Not defined

**References:**

1. CCE-36170-9

## *2.3.10 MSS*

### *2.3.10.1 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

The registry value entry AutoAdminLogon was added to the template file in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ registry key. The entry appears as MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) in the Security Configuration Editor.
This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group.
For additional information, see the Knowledge Base article 315231, "How to turn on automatic logon in Windows XP." The recommended state for this setting is: `Disabled`.

**Rationale:**

If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

**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\AutoAdminLogon
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
```

**Impact:**

None. By default this entry is not enabled.

**Default Value:**

Not defined

**References:**

1. CCE-37067-6

## *2.3.10.2 Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

- Level 1 - Member Server

**Description:**

This entry appears as `MSS: (DisableIPSourceRouting) IPv6 source routing protection level (protects against packet spoofing)` in the SCE. 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: `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.

**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\DisableIPSource Routing
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Highest protection, source routing is completely disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)
```

**Impact:**

If you configure this value to 2, all incoming source routed packets will be dropped.

**Default Value:**

Not defined

**References:**

1. CCE-36871-2

### *2.3.10.3 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

The registry value entry `DisableIPSourceRouting` was added to the template file in the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\` registry key. The entry appears as `MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)` in the SCE. 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: `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.

**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\DisableIPSourceRouting
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Highest protection, source routing is completely disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)
```

**Impact:**

If you configure this value to 2, all incoming source routed packets will be dropped.

**Default Value:**

Not defined

**References:**

1. CCE-36535-3

## *2.3.10.4 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

The registry value entry SafeDllSearchMode was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager\ registry key. The entry appears as MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) in the SCE.
The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:
- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.
When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: `Enabled`.

**Rationale:**

If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

**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\SafeDllSearchMode
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
```

**Impact:**

Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

**Default Value:**

Not defined

**References:**

1. CCE-36351-5

## *2.3.10.5 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' to '5 or fewer seconds' (Scored)*

**Profile Applicability:**

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

**Description:**

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: `5 or fewer seconds`.

**Rationale:**

The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

**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\ScreenSaverGracePeriod
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to 5 or fewer seconds.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver
grace period expires (0 recommended)
```

**Impact:**

Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

**Default Value:**

5 seconds

**References:**

1. CCE-37993-3

## *2.3.10.6 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90% or less' (Scored)*

**Profile Applicability:**

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

**Description:**

The registry value entry WarningLevel was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security\ registry key. The entry appears as MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning in the SCE. This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: `90% or less`.

**Rationale:**

If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

**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\Eventlog\Security\WarningLevel
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `90% or less`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (WarningLevel) Percentage threshold for the security event log at which
the system will generate a warning
```

**Impact:**

This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

**Default Value:**

Not defined

**References:**

1. CCE-36880-3

## 2.3.11 Network access

### 2.3.11.1 Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled' (Scored)

**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. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. 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.

**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, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Allow anonymous SID/Name translation
```

**Impact:**

Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers

is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003based domains. For example, the following computers may not work:
• Windows NT 4.0based Remote Access Service servers.
• Microsoft SQL Servers™ that run on Windows NT 3.xbased or Windows NT 4.0based computers.
• Remote Access Service or Microsoft SQL servers that run on Windows 2000based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

**Default Value:**

Disabled

**References:**

1. CCE-36065-1

## *2.3.11.2 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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 cannot enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: `Enabled`.

**Rationale:**

An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts
```

**Impact:**

It will be impossible to establish trusts with Windows NT 4.0based 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.

**Default Value:**

Enabled

**References:**

1. CCE-36316-8

## *2.3.11.3 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller
- 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 workstations in your environment.
The Network access: Do not allow anonymous enumeration of SAM accounts and shares

setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting is: `Enabled`.

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares
```

**Impact:**

It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. 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.

**Default Value:**

Disabled

**References:**

1. CCE-36316-8

## *2.3.11.4 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (Scored)*

**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. If you enable this policy setting, anonymous Windows users are allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Let Everyone permissions apply to anonymous users
```

**Impact:**

None. This is the default configuration.

**Default Value:**

Disabled

**References:**

1. CCE-36148-5

## *2.3.11.5 Set 'Network access: Remotely accessible registry paths' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines which registry paths will be accessible after referencing the WinReg key to determine access permissions to the paths.
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 subpaths" in Windows Server 2003, Windows Vista, and Windows Server 2008.
Note: 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
```

**Impact:**

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail.
Note: If you want to allow remote access, you must also enable the Remote Registry service.

**Default Value:**

System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion

**References:**

1. CCE-37194-8

## *2.3.11.6 Set 'Network access: Remotely accessible registry paths and sub-paths' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines which registry paths and sub-paths will be accessible when an application or process references the WinReg key to determine access permissions.
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, and Windows Server 2003 does not exist in Windows XP.
Note: 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
```

**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.

**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\AllowedPa
ths\Machine
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting 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\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Remotely accessible registry paths and sub-paths
```

**Impact:**

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail.
Note: If you want to allow remote access, you must also enable the Remote Registry service.

**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

**References:**

1. CCE-36347-3

## *2.3.11.7 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled' (Scored)*

**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 HKLM\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. Null sessions are a weakness that can

be exploited through shares (including the default shares) on computers in your environment. 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.

**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\restrictn
ullsessaccess
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Restrict anonymous access to Named Pipes and Shares
```

**Impact:**

You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries.
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:
- COMNAPSNA session access
- COMNODESNA session access
- SQL\QUERYSQL instance access
- SPOOLSSSpooler service
- LLSRPCLicense Logging service
- NetlogonNet Logon service
- LsarpcLSA access
- SamrRemote access to SAM objects
- browserComputer 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.

**Default Value:**

Enabled

**References:**

1. CCE-36021-4

## *2.3.11.8 Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves' (Scored)*

**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`.

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Classic - local users authenticate as themselves`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Sharing and security model for local accounts
```

**Impact:**

None. This is the default configuration.

**Default Value:**

Classic - local users authenticate as themselves

**References:**

1. CCE-37623-6

## *2.3.12 Network security*

### *2.3.12.1 Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation. 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, 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Allow Local System to use computer identity for NTLM
```

**Impact:**

If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.
If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

**Default Value:**

Not defined

**References:**

1. CCE-38341-4

## *2.3.12.2 Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

Allow NTLM to fall back to NULL session when used with LocalSystem.

**Rationale:**

NULL sessions are less secure because by definition they are unauthenticated.

**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 implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback
```

**Impact:**

Any applications that require NULL sessions for LocalSystem will not work as designed.

**Default Value:**

Not defined

**References:**

1. CCE-37035-3

## *2.3.12.3 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled' (Scored)*

**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. Note Older operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Do not store LAN Manager hash value on next password change
```

**Impact:**

Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

**Default Value:**

Enabled

**References:**

1. CCE-36326-7

### *2.3.12.4 Set 'Network security: Force logoff when logon hours expire' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting, which determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours, affects the SMB component. If you enable this policy setting, client sessions with the SMB server will be disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire.

**Rationale:**

If you disable this policy setting, a user could remain connected to the computer outside of their allotted logon hours.

**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\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Force logoff when logon hours expire
```

**Impact:**

When a user's logon time expires, SMB sessions will terminate. The user will be unable to log on to the computer until their next scheduled access time commences.

**Default Value:**

Disabled

**References:**

1. CCE-36270-7

## *2.3.12.5 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored)*

**Profile Applicability:**

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

**Description:**

LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include 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 possible values for the Network security: LAN Manager authentication level setting are:

- Send LM & NTLM responses
- Send LM & NTLM — use NTLMv2 session security if negotiated
- Send NTLM responses only
- Send NTLMv2 responses only
- Send NTLMv2 responses only\refuse LM
- Send NTLMv2 responses only\refuse LM & NTLM

Not Defined - The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows:

Send LM & NTLM responses - Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

Send LM & NTLM use NTLMv2 session security if negotiated - Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

Send NTLM response only - Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

Send NTLMv2 response only - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

Send NTLMv2 response only\refuse LM - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).

Send NTLMv2 response only\refuse LM & NTLM - 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).

**Rationale:**

In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses—the weakest form of authentication response—are sent over the network, and it is 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 earlier 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 domain controllers.

**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 implement the recommended configuration state, set the following Group Policy setting to `Send NTLMv2 response only. Refuse LM & NTLM`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LAN Manager authentication level
```

**Impact:**

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.
Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see article 305379, Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100907).

**Default Value:**

Send NTLMv2 response only

**References:**

1. CCE-36173-3

## *2.3.12.6 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher (Scored)*

**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, as follows:

- None. The LDAP BIND request is issued with the caller-specified options.
- 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.
- Require signature. This level is the same as Negotiate signing. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed.
Note: This policy setting does not have any impact on ldap_simple_bind or 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 possible values for the Network security: LDAP client signing requirements setting are:
- None
- Negotiate signing
- Require signature
- Not Defined The recommended state for this setting is: `Negotiate signing`.

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Negotiate signing`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LDAP client signing requirements
```

**Impact:**

If you configure the server to require LDAP signatures 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.

**Default Value:**

Negotiate signing

**References:**

1. CCE-36858-9

## *2.3.12.7 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines which behaviors are allowed 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 possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:
- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.
- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.
- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.

- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.
- Not Defined. The recommended state for this setting is: `Require NTLMv2 session security,Require 128-bit encryption`.

**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. In other words, these options help protect against man-in-the-middle attacks.

**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\NTLMMinClientSec
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Require NTLMv2 session security,Require 128-bit encryption`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) clients
```

**Impact:**

Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

**Default Value:**

No minimum

**References:**

1. CCE-37553-5

## *2.3.12.8 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines which behaviors are allowed 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 possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:
- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.
- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.
- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.
- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.
- Not Defined. The recommended state for this setting is: `Require NTLMv2 session security,Require 128-bit encryption`.

**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.

**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\NTLMMinServerSec
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Require NTLMv2 session security,Require 128-bit encryption`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) servers
```

**Impact:**

Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

**Default Value:**

No minimum

**References:**

1. CCE-37835-6

## *2.3.13 Recovery console*

### *2.3.13.1 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

The recovery console is a command-line environment that is used to recover from system problems. If you enable this policy setting, the administrator account is automatically logged on to the recovery console when it is invoked during startup. The recommended state for this setting is: `Disabled`.

**Rationale:**

The Recovery Console can be very useful when you need to troubleshoot and repair computers that do not start. However, it is dangerous to allow automatic logon to the console. Anyone could walk up to the server, disconnect the power to shut it down, restart it, select Recover Console from the Restart menu, and then assume full control of 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\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\securitylevel
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow automatic administrative logon
```

**Impact:**

Users will have to enter a user name and password to access the Recovery Console.

**Default Value:**

Disabled

**References:**

1. CCE-37624-4

## *2.3.13.2 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting makes the Recovery Console SET command available, which allows you to set the following recovery console environment variables:
- AllowWildCards. Enables wildcard support for some commands (such as the DEL command).
- AllowAllPaths. Allows access to all files and folders on the computer.
- AllowRemovableMedia. Allows files to be copied to removable media, such as a floppy disk.
- NoCopyPrompt. Does not prompt when overwriting an existing file. The recommended state for this setting is: `Disabled`.

**Rationale:**

An attacker who can cause the system to restart into the Recovery Console could steal sensitive data and leave no audit or access trail.

**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\Setup\RecoveryConsole\setcommand
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow floppy copy and access to all drives and all folders
```

**Impact:**

Users who have started a server through the Recovery Console and logged in with the built-in Administrator account will not be able to copy files and folders to a floppy disk.

**Default Value:**

Disabled

**References:**

1. CCE-37307-6

## 2.3.14 Shutdown

### 2.3.14.1 Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled' (Scored)

**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`.

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on
```

**Impact:**

Operators will have to log on to servers to shut them down or restart them.

**Default Value:**

Disabled

**References:**

1. CCE-36788-8

## *2.3.14.2 Set 'Shutdown: Clear virtual memory pagefile' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this policy setting is enabled, the system pagefile is cleared each time that the system shuts down properly. If you enable this security setting, the hibernation file (Hiberfil.sys) is zeroed out when hibernation is disabled on a portable computer system. It will take longer to shut down and restart the computer, and will be especially noticeable on computers with large paging files. The recommended state for this setting is: `Disabled`.

**Rationale:**

Important information that is kept in real memory may be written periodically to the page file to help Windows Server 2003 handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file.
Caution
An attacker who has physical access to the server could bypass this countermeasure by simply unplugging the server from its power source.

**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\Memory
Management\ClearPageFileAtShutdown
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Shutdown: Clear virtual memory pagefile
```

**Impact:**

It will take longer to shut down and restart the server, especially on servers with large paging files. For a server with 2 gigabytes (GB) of RAM and a 2-GB paging file, this policy setting could increase the shutdown process by 20 to 30 minutes, or more. For some organizations, this downtime violates their internal service level agreements. Therefore, use caution before you implement this countermeasure in your environment.

**Default Value:**

Disabled

**References:**

1. CCE-38335-6

## *2.3.15 System cryptography*

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

## *2.3.16 System objects*

### *2.3.16.1 Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled' (Scored)*

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Require case insensitivity for non-Windows subsystems
```

**Impact:**

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.

**Default Value:**

Enabled

**References:**

1. CCE-37885-1

## *2.3.16.2 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled' (Scored)*

**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. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create. The recommended state for this setting is: `Enabled`.

**Rationale:**

This setting determines the strength of the default DACL for objects. Windows Server 2003 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. If you enable this setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Strengthen default permissions of internal system objects
(e.g. Symbolic Links)
```

**Impact:**

None. This is the default configuration.

**Default Value:**

Enabled

**References:**

1. CCE-37644-2

## *2.3.17 System settings*

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

## *2.3.18 User Account Control*

### *2.3.18.1 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled' (Scored)*

**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 options are:
- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.
- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. 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 the built-in Administrator account is disabled. 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 Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain 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 location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdm
inistratorToken
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Admin Approval Mode for the Built-in Administrator
account
```

**Impact:**

Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

**Default Value:**

Disabled

**References:**

1. CCE-36494-3

## *2.3.18.2 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.
- Enabled: UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation prompts. If you do not disable the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting, the prompts appear on the interactive user's desktop instead of the secure desktop.
- Disabled: (Default) The secure desktop can be disabled only by the user of the interactive desktop or by disabling the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting. The recommended state for this setting is: `Disabled`.

**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 allows the administrator to perform operations that require elevated privileges while connected via Remote Assistance. This increases security in that organizations can use UAC even when end user support is provided remotely. However, it also reduces security by adding the risk that an administrator might allow an unprivileged user to share elevated privileges for an application that the adminstrator needs to use during the Remote Desktop session.

**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\EnableUIA
DesktopToggle
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Allow UIAccess applications to prompt for elevation
without using the secure desktop
```

**Impact:**

If you enable this setting, ("User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop), requests for elevation are automatically sent to the interactive desktop (not the secure desktop) and also appear on the remote administrator's view of the desktop during a Windows Remote Assistance session, and the remote administrator is able to provide the appropriate credentials for elevation. This setting does not change the behavior of the UAC elevation prompt for administrators.

**Default Value:**

Disabled

**References:**

1. CCE-36863-9

## *2.3.18.3 Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent for non-Windows binaries' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting controls the behavior of the elevation prompt for administrators.
The options are:
- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.
- Prompt for credentials on the secure desktop: When an operation requires elevation of

privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.
- Prompt for consent on the secure desktop: When an operation 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.
- 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.
- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.
- Prompt for consent for non-Windows binaries: (Default) 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. The recommended state for this setting is: `Prompt for consent for non-Windows binaries`.

**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.

**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\ConsentPr
omptBehaviorAdmin
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Prompt for consent for non-Windows binaries`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Behavior of the elevation prompt for administrators in
Admin Approval Mode
```

**Impact:**

This policy setting controls the behavior of the elevation prompt for administrators.

**Default Value:**

Prompt for consent for non-Windows binaries

**References:**

1. CCE-37029-6

## *2.3.18.4 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests' (Scored)*

**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 options are:
- 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.
- Automatically deny elevation requests: 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.
- Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: `Prompt for credentials`.

**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.

**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\ConsentPr
omptBehaviorUser
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to Automatically deny elevation requests:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Behavior of the elevation prompt for standard users
```

**Impact:**

Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

**Default Value:**

Prompt for credentials

**References:**

1. CCE-36864-7

## *2.3.18.5 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled' (Scored)*

**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 options are:
- Enabled: (Default for home) 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.
- Disabled: (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary. 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

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation
```

**Impact:**

Users will need to provide administrative passwords to be able to install programs.

**Default Value:**

Enabled

**References:**

1. CCE-36533-8

## *2.3.18.6 Set 'User Account Control: Only elevate executables that are signed and validated' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting enforces public key infrastructure (PKI) signature checks for any interactive applications that request elevation of privilege. Enterprise administrators can control which applications are allowed to run by adding certificates to the Trusted Publishers certificate store on local computers.
The options are:
- Enabled: Enforces the PKI certification path validation for a given executable file before it is permitted to run.
- Disabled: (Default) Does not enforce PKI certification path validation before a given executable file is permitted to run. The recommended state for this setting is: `Disabled`.

**Rationale:**

Intellectual property, personally identifiable information, and other confidential data are normally manipulated by applications on the computer and require elevated credentials to get access to the information. Users and administrators inherently trust applications used with these information sources and provide their credentials. If one of these applications is replaced by a rogue application that appears identical to the trusted application the confidential data could be compromised and the user's administrative credentials would also be compromised.

**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\ValidateAdminCodeSignatures
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Only elevate executables that are signed and validated
```

**Impact:**

Enabling this setting requires that you have a PKI infrastructure and that your Enterprise administrators have populated the Trusted Root Store with the certificates for the allowed applications. Some older applications are not signed and will not be able to be used in an environment that is hardened with this setting. You should carefully test your applications in a pre-production environment before implementing this setting. For information about the steps required to test application compatibility, make application compatibility fixes, and sign installer packages to prepare your organization for deployment of Windows Vista User Account Control, see Understanding and Configuring User Account Control in Windows Vista (http://go.microsoft.com/fwlink/?LinkID=79026).
Control over the applications that are installed on the desktops and the hardware that is able to join your domain should provide similar protection from the vulnerability addressed by this setting. Additionally, the level of protection provided by this setting is not an assurance that all rogue applications will be found

**Default Value:**

Disabled

**References:**

1. CCE-36865-4

## *2.3.18.7 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled' (Scored)*

**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 options are:
- Enabled: (Default) If an application resides in a secure location in the file system, it runs only with UIAccess integrity.
- Disabled: An application runs with UIAccess integrity even if it does not reside in a secure location in the file system. 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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations
```

**Impact:**

If the application that requests UIAccess meets the UIAccess setting requirements, Windows Vista starts the application with the ability to bypass most of the UIPI

restrictions. If the application does not meet the security restrictions, the application will be started without UIAccess rights and can interact only with applications at the same or lower privilege level.

**Default Value:**

Enabled

**References:**

1. CCE-37057-7

## *2.3.18.8 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled' (Scored)*

**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 options are:
- Enabled: (Default) 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.
- Disabled: Admin Approval Mode and all related UAC policy settings are disabled. Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced. The recommended state for this setting is: `Enabled`.

**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.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode
```

**Impact:**

Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

**Default Value:**

Enabled

**References:**

1. CCE-36869-6

## *2.3.18.9 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled' (Scored)*

**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 options are:
- Enabled: (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.
- Disabled: All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used. The recommended state for this setting is: `Enabled`.

**Rationale:**

Elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malicious software.

**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 implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation
```

**Impact:**

None. This is the default configuration.

**Default Value:**

Enabled

**References:**

1. CCE-36866-2

## *2.3.18.10 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled' (Scored)*

**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, or HKLM\Software.

The options are:
- Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry.
- Disabled: Applications that write data to protected locations fail. The recommended state for this setting is: `Enabled`.

**Rationale:**

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

**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\EnableVir
tualization
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Virtualize file and registry write failures to per-user
locations
```

**Impact:**

None. This is the default configuration.

**Default Value:**

Enabled

**References:**

1. CCE-37064-3

# *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.

## 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 Firewall With Advanced Security

This section contains recommendations for configuring the Windows Firewall.

## 9.1 Domain Profile

This sections contains recommendations for the Domain Profile of the Windows Firewall.

### 9.1.1 Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)' (Scored)

**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.

**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\EnableFir
ewall
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Firewall state
```

**Impact:**

None, this is the default configuration.

**Default Value:**

On

**References:**

1. CCE-36062-8

## *9.1.2 Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)' (Scored)*

**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 default behavior is to block connections unless there are firewall rules to allow the connection. 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.

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Inbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Block

**References:**

1. CCE-38117-8

## *9.1.3 Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)' (Scored)*

**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. In Windows Vista, the default behavior is to allow connections unless there are firewall rules that block the connection. 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.

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Outbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Allow

**References:**

1. CCE-36146-9

### *9.1.4 Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

**Note:** When the Apply local firewall rules setting is configured to `No`, it's recommended to also configure the `Display a notification setting` to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

**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\DisableNotifications
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Display a notification
```

**Impact:**

If you configure this policy setting to Yes, Windows Firewall will display these notifications.

**Default Value:**

Yes

**References:**

1. CCE-38041-0

## *9.1.5 Set 'Windows Firewall: Domain: Allow unicast response' to 'No' (Scored)*

**Profile Applicability:**

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

**Description:**

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: No.

**Rationale:**

An attacker could respond to broadcast or multicast message with malicious payloads.

**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\DisableUn
icastResponsesToMulticastBroadcast
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to No.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Allow unicast response
```

**Impact:**

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

**Default Value:**

Yes

**References:**

1. CCE-37859-6

## *9.1.6 Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLocalPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Apply local firewall rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-37860-4

## *9.1.7 Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLoca
lIPsecPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Apply local connection security
rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-38040-2

### *9.1.8 Set 'Windows Firewall: Domain: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log' (Scored)*

**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

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Name
```

**Impact:**

The log file will be stored in the specified file.

**Default Value:**

Not configured

**References:**

1. CCE-37482-7

## *9.1.9 Set 'Windows Firewall: Domain: Logging: Size limit (KB)' to '16384 KB or greater ' (Scored)*

**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: `16384 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

**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 `16384 KB or greater`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Size limit (KB)
```

**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

**Default Value:**

Not configured

**References:**

1. CCE-36088-3

## *9.1.10 Set 'Windows Firewall: Domain: Logging: Log dropped packets' to 'Yes' (Scored)*

**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

**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\L
ogDroppedPackets
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Log dropped
packets
```

**Impact:**

Information about dropped packets will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-37523-8

## *9.1.11 Set 'Windows Firewall: Domain: Logging: Log successful connections' to 'Yes' (Scored)*

**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

**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\L
ogSuccessfulConnections
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Log successful
connections
```

**Impact:**

Information about successful connections will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-36393-7

## *9.2 Private Profile*

This sections contains recommendations for the Private Profile of the Windows Firewall.

### *9.2.1 Set 'Windows Firewall: Private: Firewall state' to 'On (recommended)' (Scored)*

**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.

**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\EnableFi
rewall
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `On (recommended).`

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Windows Firewall: Private: Firewall state
```

**Impact:**

None, this is the default configuration.

**Default Value:**

On

**References:**

1. CCE-38239-0

## *9.2.2 Set 'Windows Firewall: Private: Inbound connections' to 'Block (default)' (Scored)*

**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 default behavior is to block connections unless there are firewall rules to allow the connection. 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.

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Inbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Block

**References:**

1. CCE-38042-8

### *9.2.3 Set 'Windows Firewall: Private: Outbound connections' to 'Allow (default)' (Scored)*

**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 default behavior is to allow connections unless there are firewall rules that block the connection.
Important 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. 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.

**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\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Windows Firewall: Private: Outbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Allow

**References:**

1. CCE-38332-3

## *9.2.4 Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

**Note:** When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also also configure the `Display a notification` setting to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

**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\DisableNotifications
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Display a notification
```

**Impact:**

If you configure this policy setting to Yes, Windows Firewall will display these notifications.

**Default Value:**

Yes

**References:**

1. CCE-37621-0

## *9.2.5 Set 'Windows Firewall: Private: Allow unicast response' to 'No' (Scored)*

**Profile Applicability:**

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

**Description:**

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: `No`.

**Rationale:**

An attacker could respond to broadcast or multicast message with malicious payloads.

**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\DisableU
nicastResponsesToMulticastBroadcast
```

**Remediation:**

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

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Windows Firewall: Private: Allow unicast response
```

**Impact:**

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

**Default Value:**

Yes

**References:**

1. CCE-37134-4

## *9.2.6 Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLocalPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Apply local firewall rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-37438-9

## *9.2.7 Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLocalIPsecPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Apply local connection security rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-36063-6

## *9.2.8 Set 'Windows Firewall: Private: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' (Scored)*

**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

**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\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Name
```

**Impact:**

The log file will be stored in the specified file.

**Default Value:**

Not configured

**References:**

1. CCE-37569-1

## *9.2.9 Set 'Windows Firewall: Private: Logging: Size limit (KB)' to '16384 KB or greater' (Scored)*

**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: `16384 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

**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 `16384 KB or greater`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Size limit (KB)
```

**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

**Default Value:**

Not configured

**References:**

1. CCE-38178-0

### *9.2.10 Set 'Windows Firewall: Private: Logging: Log dropped packets' to 'Yes' (Scored)*

**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

**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\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Log dropped
packets
```

**Impact:**

Information about dropped packets will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-35972-9

## *9.2.11 Set 'Windows Firewall: Private: Logging: Log successful connections' to 'Yes' (Scored)*

**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

**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\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Log successful
connections
```

**Impact:**

Information about successful connections will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-37387-8

## *9.3 Public Profile*

This sections contains recommendations for the Public Profile of the Windows Firewall.

### *9.3.1 Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)' (Scored)*

**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.

**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\EnableFir
ewall
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Firewall state
```

**Impact:**

None, this is the default configuration.

**Default Value:**

On

**References:**

1. CCE-37862-0

## *9.3.2 Set 'Windows Firewall: Public: Inbound connections' to 'Block (default)' (Scored)*

**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 default behavior is to block connections unless there are firewall rules to allow the connection. 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.

**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\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Inbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Block

**References:**

1. CCE-36057-8

## *9.3.3 Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)' (Scored)*

**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 default behavior is to allow connections unless there are firewall rules that block the connection.
Important 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. 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.

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Outbound connections
```

**Impact:**

None, this is the default configuration.

**Default Value:**

Allow

**References:**

1. CCE-37434-8

## *9.3.4 Set 'Windows Firewall: Public: Display a notification' to 'Yes' (Scored)*

**Profile Applicability:**

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

**Description:**

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

**Note:** When the `Apply local firewall rules` setting is configured to Yes, it is also recommended to also configure the `Display a notification` setting to `Yes`. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: `Yes`.

**Rationale:**

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

**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\DisableNo
tifications
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to Yes.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Display a notification
```

**Impact:**

If you configure this policy setting to No, Windows Firewall will not display these notifications.

**Default Value:**

Yes

**References:**

1. CCE-38043-6

## *9.3.5 Set 'Windows Firewall: Public: Allow unicast response' to 'No' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

- Level 1 - Member Server

**Description:**

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: No.

**Rationale:**

An attacker could respond to broadcast or multicast message with malicious payloads.

**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\DisableUn
icastResponsesToMulticastBroadcast
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to No.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Allow unicast response
```

**Impact:**

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

**Default Value:**

Yes

**References:**

1. CCE-36324-2

## *9.3.6 Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLocalPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Apply local firewall rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-37861-2

## *9.3.7 Set 'Windows Firewall: Public: Apply local connection security rules' to 'No' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No.

**Rationale:**

Users with administrative privileges might create firewall rules that expose the system to remote attack.

**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\AllowLocalIPsecPolicyMerge
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to No.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Apply local connection security rules
```

**Impact:**

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

**Default Value:**

Yes

**References:**

1. CCE-36268-1

## *9.3.8 Set 'Windows Firewall: Public: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log' (Scored)*

**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

**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\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Name
```

**Impact:**

The log file will be stored in the specified file.

**Default Value:**

Not configured

**References:**

1. CCE-37266-4

## *9.3.9 Set 'Windows Firewall: Public: Logging: Size limit (KB)' to '16384 KB or greater' (Scored)*

**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: `16384 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

**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 `16384 KB or greater`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Size limit (KB)
```

**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

**Default Value:**

Not configured

**References:**

1. CCE-36395-2

## *9.3.10 Set 'Windows Firewall: Public: Logging: Log dropped packets' to 'Yes' (Scored)*

**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

**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\L
ogDroppedPackets
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
```

```
Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Log dropped
packets
```

**Impact:**

Information about dropped packets will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-37265-6

## *9.3.11 Set 'Windows Firewall: Public: Logging: Log successful connections' to 'Yes' (Scored)*

**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

**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\L
ogSuccessfulConnections
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Log successful
connections
```

**Impact:**

Information about successful connections will be recorded in the firewall log file

**Default Value:**

Not configured

**References:**

1. CCE-36394-5

# 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 AppLocker

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

### 17.1.1 Set 'Audit Policy: Account Logon: Credential Validation' to 'Success and Failure' (Scored)

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential
Validation
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37741-6

## *17.2 Account Management*

### *17.2.1 Set 'Audit Policy: Account Management: Application Group Management' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports each event of application group management on a computer, such as when an application group is created, changed, or deleted or when a member is added to or removed from an application group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of application group accounts. Events for this subcategory include:
4783: A basic application group was created.
4784: A basic application group was changed.
4785: A member was added to a basic application group.
4786: A member was removed from a basic application group.
4787: A non-member was added to a basic application group.
4788: A non-member was removed from a basic application group.
4789: A basic application group was deleted.
4790: An LDAP query group was created.
4791: A basic application group was changed.
4792: An LDAP query group was deleted.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.

If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Application Group Management
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-38329-9

## *17.2.2 Configure 'Audit Policy: Account Management: Computer Account Management' (Scored)*

**Profile Applicability:**

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

**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.

- Level 1 - Domain Controller. The recommended state for this setting is: `Success and Failure`.
- Level 1 - Member Server. The recommended state for this setting is: `Success`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Computer Account Management
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38004-8

## *17.2.3 Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Distribution Group Management
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-36265-7

## *17.2.4 Set 'Audit Policy: Account Management: Other Account Management Events' to 'Success and Failure' (Scored)*

**Profile Applicability:**

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

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an

attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Other Account Management Events
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37855-4

## *17.2.5 Set 'Audit Policy: Account Management: Security Group Management' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If

security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Security Group Management
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38034-5

## *17.2.6 Set 'Audit Policy: Account Management: User Account Management' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their

activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User
Account Management
```

**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.

**Default Value:**

Success

**References:**

1. CCE-37856-2

## *17.3 Detailed Tracking*

### *17.3.1 Set 'Audit Policy: Detailed Tracking: Process Creation' to 'Success' (Scored)*

**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 the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking:
Process Creation
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-36059-4

## *17.4 DS Access*

### *17.4.1 Set 'Audit Policy: DS Access: Directory Service Access' to 'Success and Failure' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

**Description:**

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to domain controllers. Events for this subcategory include:
4662 : An operation was performed on an object. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.

If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service
Access
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37433-0

## *17.4.2 Set 'Audit Policy: DS Access: Directory Service Changes' to 'Success and Failure' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

**Description:**

This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers. Events for this subcategory include:
5136 : A directory service object was modified.
5137 : A directory service object was created.
5138 : A directory service object was undeleted.
5139 : A directory service object was moved.

The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service
Changes
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37616-0

## *17.5 Logon/Logoff*

### *17.5.1 Set 'Audit Policy: Logon-Logoff: Account Lockout' to 'No Auditing' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Account Lockout
```

**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.

**Default Value:**

Success

**References:**

1. CCE-37133-6

## *17.5.2 Set 'Audit Policy: Logon-Logoff: Logoff' to 'Success' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38237-4

## *17.5.3 Set 'Audit Policy: Logon-Logoff: Logon' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logon
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38036-0

## *17.5.4 Set 'Audit Policy: Logon-Logoff: Other Logon/Logoff Events' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports other logon/logoff-related events, such as Terminal 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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other
Logon/Logoff Events
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-36322-6

## *17.5.5 Set 'Audit Policy: Logon-Logoff: Special Logon' to 'Success' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Special Logon
```

**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.

**Default Value:**

Success

**References:**

1. CCE-36266-5

## *17.6 Object Access*

### *17.6.1 Set 'Audit Policy: Object Access: File System' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports when file system objects are accessed. Only file system objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a file system object that has a specified system access control list (SACL), effectively enabling auditing to take place.
A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:
- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.

- A flag to indicate whether to audit failed access events, successful access events, or both.
If you configure the Audit object access setting to Success, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to Failure, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL.
Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the Write and Append Data auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.
Events for this subcategory include:
4664: An attempt was made to create a hard link.
4985: The state of a transaction has changed.
5051: A file was virtualized.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: File System
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37384-5

## *17.6.2 Set 'Audit Policy: Object Access: Handle Manipulation' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports when a handle to an object is opened or closed. Only objects with SACLs cause these events to be generated, and only if the attempted handle operation matches the SACL. Handle Manipulation events are only generated for object types where the corresponding Object Access subcategory is enabled, for example File System or Registry. Events for this subcategory include:
4656: A handle to an object was requested.
4658: The handle to an object was closed.
4690: An attempt was made to duplicate a handle to an object.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Handle
Manipulation
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37511-3

## *17.6.3 Set 'Audit Policy: Object Access: Registry' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports when registry objects are accessed. Only registry objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a registry object that has a specified system access control list (SACL), effectively enabling auditing to take place.
A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:
- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.
- A flag to indicate whether to audit failed access events, successful access events, or both.
If you configure the Audit object access setting to Success, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to Failure, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL.
Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the Write and Append Data auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.
Events for this subcategory include:
4657 : A registry value was modified.
5039: A registry key was virtualized.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Registry
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37193-0

## *17.6.4 Set 'Audit Policy: Object Access: Removable Storage' to 'No Auditing' (Scored)*

**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: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Removable
Storage
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37617-8

## *17.7 Policy Change*

### *17.7.1 Set 'Audit Policy: Policy Change: Audit Policy Change' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Audit Policy Change
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38028-7

## *17.7.2 Set 'Audit Policy: Policy Change: Authentication Policy Change' to 'Success' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer

performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authentication Policy Change
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38327-3

## *17.8 Privilege Use*

### *17.8.1 Set 'Audit Policy: Privilege Use: Sensitive Privilege Use' to 'Success and Failure' (Scored)*

**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, and 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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Sensitive
Privilege Use
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-36267-3

## *17.9 System*

### *17.9.1 Set 'Audit Policy: System: IPsec Driver' to 'Success and Failure' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include:
4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
5478: IPsec Services has started successfully.
5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.
5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: IPsec Driver
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-37853-9

## *17.9.2 Set 'Audit Policy: System: Other System Events' to 'No Auditing' (Scored)*

**Profile Applicability:**

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

**Description:**

This subcategory reports on other system events. Events for this subcategory include:
5024 : The Windows Firewall Service has started successfully.
5025 : The Windows Firewall Service has been stopped.
5027 : The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
5028 : The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
5030: The Windows Firewall Service failed to start.
5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
5033 : The Windows Firewall Driver has started successfully.
5034 : The Windows Firewall Driver has been stopped.
5035 : The Windows Firewall Driver failed to start.
5037 : The Windows Firewall Driver detected critical runtime error. Terminating.
5058: Key file operation.
5059: Key migration operation.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log

security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Other System Events
```

**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.

**Default Value:**

Success and Failure

**References:**

1. CCE-38030-3

## *17.9.3 Set 'Audit Policy: System: Security State Change' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Security State Change
```

**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.

**Default Value:**

Success

**References:**

1. CCE-38114-5

## *17.9.4 Set 'Audit Policy: System: Security System Extension' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events

are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Security System Extension
```

**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.

**Default Value:**

No auditing

**References:**

1. CCE-36144-4

## *17.9.5 Set 'Audit Policy: System: System Integrity' to 'Success and Failure' (Scored)*

**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.
Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

**Rationale:**

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

**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, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: System Integrity
```

**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.

**Default Value:**

Success and Failure

**References:**

1. CCE-37132-8

## *17.10 Global Object Access Auditing*

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

# *18 Administrative Templates (Computer)*

This section contains recommendations for administrative templates.

## *18.1 Control Panel*

This section contains recommendation for the control panel.

## *18.1.1 Personalization*

This section contains recommendations for personalization settings.

### *18.1.1.1 Set 'Prevent enabling lock screen camera' to 'Enabled' (Scored)*

**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.

**Rationale:**

Disabling the lock screen camera extends the protection afforded by the lock screen to camera 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\Personalization:NoLockScreenCam
era
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Control Panel\Personalization\Prevent
enabling lock screen camera
```

**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.

**Default Value:**

By default, users can enable invocation of an available camera on the lock screen.

**References:**

1. CCE-38347-1

## *18.1.1.2 Set 'Prevent enabling lock screen slide show' to 'Enabled' (Scored)*

**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.

**Rationale:**

Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

**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:NoLockScreenSli
deshow
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Control Panel\Personalization\Prevent
enabling lock screen slide show
```

**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.

**Default Value:**

By default, users can enable a slide show that will run after they lock the machine.

**References:**

1. CCE-38348-9

## 18.2 Network

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

## 18.3 Printers

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

## 18.4 SCM: Pass the Hash Mitigations

This section contains recommendations for mitigating pass the hash attacks.

### 18.4.1 Set 'Apply UAC restrictions to local accounts on network logons' to 'Enabled' (Scored)

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.

Enabled (recommended): Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the `LocalAccountTokenFilterPolicy` registry value to `0`. This is the default behavior for Windows.

Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the `LocalAccountTokenFilterPolicy` registry value to `1`.

For more information about local accounts and credential theft, see "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques"

For more information about `LocalAccountTokenFilterPolicy`, see http://support.microsoft.com/kb/951016.

**Rationale:**

Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems.

**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, set the following Group Policy setting to 0.

```
Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations\Apply
UAC restrictions to local accounts on network logons
```

**Impact:**

If you enable this setting, Windows applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the `LocalAccountTokenFilterPolicy` registry value to `0`. This is the default behavior for Windows.

If you disable this setting, Windows allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1.

**Default Value:**

0

**References:**

1. CCE-37069-2

## *18.4.2 Set 'WDigest Authentication' to 'Disabled' (Scored)*

**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.

**Rationale:**

Preventing the plaintext storage of credentials may reduce opportunity for credential theft.

**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\UseLogon
Credential
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest
Authentication (disabling may require KB2871997)
```

**References:**

1. CCE-38444-6

## *18.5 Server*

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

## *18.6 Start Menu and Taskbar*

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

## 18.7 System

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

## 18.7.1 Access-Denied Assistance

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

## 18.7.2 Audit Process Creation

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

## 18.7.3 Credentials Delegation

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

## 18.7.4 Device Installation

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

## 18.7.5 Device Redirection

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

## 18.7.6 Disk NV Cache

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

## 18.7.7 Disk Quotas

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

## 18.7.8 Distributed COM

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

## *18.7.9 Driver Installation*

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

## *18.7.10 Early Launch Antimalware*

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

## *18.7.11 Enhanced Storage Access*

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

## *18.7.12 File Classification Infrastructure*

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

## *18.7.13 File Share Shadow Copy Agent*

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

## *18.7.14 File Share Shadow Copy Provider*

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

## *18.7.15 Filesystem*

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

## *18.7.16 Folder Redirection*

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

## *18.7.17 Group Policy*

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

## *18.7.18 Internet Communication Management*

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

## *18.7.19 iSCSI*

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

## *18.7.20 KDC*

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

## *18.7.21 Kerberos*

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

## *18.7.22 Locale Services*

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

## *18.7.23 Logon*

This section contains recommendations related to the logon process and lock screen.

### *18.7.23.1 Set 'Do not display network selection UI' to 'Enabled' (Scored)*

**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.

**Rationale:**

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks 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:

```
HKLM\Software\Policies\Microsoft\Windows\System\DontDisplayNetworkSelectionUI
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\System\Logon\Do not display network
selection UI
```

**Impact:**

If you enable this policy setting, the PC's network connectivity state cannot be changed without signing into Windows.

If you disable or don't configure this policy setting, any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

**References:**

1. CCE-38353-9

## *18.8 Windows Components*

## *18.8.1 Active Directory Federation Services*

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

## *18.8.2 ActiveX Installer Service*

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

## *18.8.3 Add features to Windows 8.1*

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

## *18.8.4 App Package Deployment*

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

## *18.8.5 App runtime*

This section contains recommendations for App runtime settings.

### *18.8.5.1 Set 'Allow Microsoft accounts to be optional' to 'Enabled' (Scored)*

**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.

**Rationale:**

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.

**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:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\MSAOptional
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`

```
Computer Configuration\Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional
```

**Impact:**

If you enable this policy setting, Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

If you disable or do not configure this policy setting, users will need to sign in with a Microsoft account.

**References:**

1. CCE-38354-7

## *18.8.6 Application Compatibility*

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

## *18.8.7 AutoPlay Policies*

This section contains recommendation for AutoPlay policies.

### *18.8.7.1 Set 'Turn off Autoplay' to 'Enabled:All drives' (Scored)*

**Profile Applicability:**

- Level 1 - Domain Controller

- Level 1 - Member Server

**Description:**

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.
Note You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: `Enabled:All drives`.

**Rationale:**

An attacker could use this feature to launch a program to damage a client computer or data on 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\Explorer\NoDrive
TypeAutoRun
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\AutoPlay
Policies\Turn off Autoplay\Turn off Autoplay
```

Then set the `Turn off Autoplay on:` option to `All drives`.

**Impact:**

Users will have to manually launch setup or installation programs that are provided on removable media.

**Default Value:**

Not configured

**References:**

1. CCE-36875-3

## 18.8.8 Backup

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

## 18.8.9 Biometrics

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

## 18.8.10 BitLocker Drive Encryption

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

## 18.8.11 Credential User Interface

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

## 18.8.12 Desktop Gadgets

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

## 18.8.13 Desktop Window Manager

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

## 18.8.14 Device and Driver Compatibility

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

## 18.8.15 Digital Locker

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

## 18.8.16 Edge UI

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

## 18.8.17 EMET

This section contains recommendations for configuring the Enhanced Mitigation Experience Toolkit (EMET).

### 18.8.17.1 Ensure EMET is installed (Scored)

**Profile Applicability:**

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

**Description:**

The enhanced mitigation experience toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to to applications that run on Windows.

**Rationale:**

EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows

**Audit:**

Navigate to `Control Panel\Program\Programs and Features` and confirm "EMET 5.0" is listed in the `Name` column

**Remediation:**

Install EMET 5.

### 18.8.17.2 Set 'Default Protections for Internet Explorer' to 'Enabled' (Scored)

**Profile Applicability:**

- Level 1 - Domain Controller

- Level 1 - Member Server

**Description:**

This settings determine if EMET mitigations are applied to Internet Explorer.

**Rationale:**

Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

**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:

HEY_LOCAL_MACHINE\Software\Policies\Microsoft\EMET\Defaults:IE

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\EMET\Default
Protections for Internet Explorer
```

**References:**

1. CCE-38428-9

## *18.8.17.3 Set 'Default Protections for Popular Software' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This settings determine if EMET mitigations are applied to other popular software.

**Rationale:**

Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them.

**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\Administrative Templates\Windows Components\EMET\Default
Protections for Popular Explorer
```

## *18.8.17.4 Set 'Default Protections for Recommended Software' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java.

**Rationale:**

Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

**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\Administrative Templates\Windows Components\EMET\Default
Protections for Recommended Software
```

**References:**

1. CCE-38433-9

## *18.8.17.5 Set 'System ASLR' to 'Enabled:Application Opt-In' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting determines how applications become enrolled in address space layout randomization (ASLR).

**Rationale:**

ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

**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\EMET\SysSettings:ASLR
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled:Application Opt-In`.

```
Computer Configuration\Administrative Templates\Windows Components\EMET\ASLR Setting
```

## *18.8.17.6 Set 'System DEP' to 'Enabled:Application Opt-Out' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting determines how applications become enrolled in data execution protection (DEP).

**Rationale:**

DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

**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\EMET\SysSettings:DEP
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled:Application Opt-Out`.

```
Computer Configuration\Administrative Templates\Windows Components\EMET\DEP Setting
```

## *18.8.17.7 Set 'System SEHOP' to 'Enabled:Application Opt-Out' (Scored)*

**Profile Applicability:**

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

**Description:**

This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP).

**Rationale:**

When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are use to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

**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\EMET\SysSettings:SEHOP
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `Enabled:Application Opt-Out`.

```
Computer Configuration\Administrative Templates\Windows Components\EMET\SEHOP Setting
```

## 18.8.18 Event Forwarding

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

## 18.8.19 Event Log Service

This section contains recommendation for configuring the event log service.

## 18.8.19.1 Application

### 18.8.19.1.1 Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)

**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. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.
**Note:** Old events may or may not be retained according to the "Backup log automatically when full"• policy setting. The recommended state for this setting is: `Disabled`.

**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

**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\Retention
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Application\Control Event Log behavior when the log file reaches its maximum
size
```

**Impact:**

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.
If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

**Default Value:**

Disabled

**References:**

1. CCE-37775-4

## *18.8.19.1.2 Set 'Application: Maximum Log Size (KB)' to 'Enabled:32768 or greater' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies the maximum size of the log file in kilobytes.
If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments.
If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator

using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:32768 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

**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\MaxSize
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Application\Specify the maximum log file size (KB)\Specify the maximum log
file size (KB)
```

Then set the `Maximum Log Size (KB)` option to `32768 or greater`.

**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 Operations Manager (MOM) 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.

**Default Value:**

20480 KB

**References:**

1. CCE-37948-7

## *18.8.19.2 Security*

### *18.8.19.2.1 Set 'Security: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)*

**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. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.
**Note:** Old events may or may not be retained according to the "Backup log automatically when full"• policy setting. The recommended state for this setting is: `Disabled`.

**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

**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\Retention
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Security\Control Event Log behavior when the log file reaches its maximum size
```

**Impact:**

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.
If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

**Default Value:**

Disabled

**References:**

1. CCE-37145-0

## *18.8.19.2.2 Set 'Security: Maximum Log Size (KB)' to 'Enabled:196608 or greater' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:196608 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

**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\MaxSize
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Security\Specify the maximum log file size (KB)\Specify the maximum log file
size (KB)
```

Then set the `Maximum Log Size (KB)` option to `196608 or greater`.

**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 Operations Manager (MOM) 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.

**Default Value:**

20480 KB

**References:**

1. CCE-37695-4

## *18.8.19.3 Setup*

### *18.8.19.3.1 Set 'Setup: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)*

**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. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.
If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.
Note: Old events may or may not be retained according to the "Backup log automatically when full"• policy setting. The recommended state for this setting is: `Disabled`.

**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

**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\Administrative Templates\Windows Components\Event Log
Service\Setup\Control Event Log behavior when the log file reaches its maximum size
```

**Default Value:**

Disabled

**References:**

1. CCE-34170-1

## *18.8.19.3.2 Set 'Setup: Maximum Log Size (KB)' to 'Enabled:32768 or greater' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:32768 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

**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`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Setup\Specify the maximum log file size (KB)
```

Then set the `Maximum Log Size (KB)` option to `32768 or greater`.

**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 Operations Manager (MOM) 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.

**Default Value:**

20480 KB

**References:**

1. CCE-35091-8

## *18.8.19.4 System*

### *18.8.19.4.1 Set 'System: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)*

**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. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.
**Note:** Old events may or may not be retained according to the "Backup log automatically when full"• policy setting. The recommended state for this setting is: `Disabled`.

**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

**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\Retention
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\System\Control Event Log behavior when the log file reaches its maximum size
```

**Impact:**

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.
If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

**Default Value:**

Disabled

**References:**

1. CCE-36160-0

## *18.8.19.4.2 Set 'System: Maximum Log Size (KB)' to 'Enabled:32768 or greater' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies the maximum size of the log file in kilobytes.
If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments.
If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:32768 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

**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\MaxSize
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\System\Specify the maximum log file size (KB)\Specify the maximum log file
size (KB)
```

Then set the `Maximum Log Size (KB)` option to `32768 or greater`.

**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 Operations Manager (MOM) 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.

**Default Value:**

20480 KB

**References:**

1. CCE-36092-5

## *18.8.20 Event Viewer*

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

## 18.8.21 Family Safety

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

## 18.8.22 File Explorer

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

## 18.8.23 File History

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

## 18.8.24 Game Explorer

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

## 18.8.25 HomeGroup

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

## 18.8.26 Import Video

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

## 18.8.27 Internet Explorer

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

## 18.8.28 Internet Information Services

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

## 18.8.29 Location and Sensors

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

## 18.8.30 Maintenance Scheduler

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

## 18.8.31 NetMeeting

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

## 18.8.32 Network Access Protection

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

## 18.8.33 Network Projector

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

## 18.8.34 OneDrive (formerly SkyDrive)

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

## 18.8.35 Online Assistance

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

## 18.8.36 Password Synchronization

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

## 18.8.37 Portable Operating System

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

## 18.8.38 Presentation Settings

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

## 18.8.39 Remote Desktop Services (formerly Terminal Services)

## 18.8.39.1 RD Licensing

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

## 18.8.39.2 Remote Desktop Connection Client

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

## 18.8.39.3 Remote Desktop Session Host

## 18.8.39.3.1 Application Compatibility

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

## 18.8.39.3.2 Connections

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

## 18.8.39.3.3 Device and Resource Redirection

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

## 18.8.39.3.4 Licensing

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

## *18.8.39.3.5 Printer Redirection*

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

## *18.8.39.3.6 Profiles*

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

## *18.8.39.3.7 RD Connection Broker*

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

## *18.8.39.3.8 Remote Session Environment*

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

## *18.8.39.3.9 Security*

### *18.8.39.3.9.1 Set 'Set client connection encryption level: Encryption Level' to 'Enabled: High Level' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

**Rationale:**

If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

**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:**

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Set client connection encryption
level\Set client connection encryption level: Encryption Level
```

**Impact:**

Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

**Default Value:**

Not configured

**References:**

1. CCE-36627-8

## *18.8.40 RSS Feeds*

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

## *18.8.41 Search*

This section contains recommendations for Search settings.

### *18.8.41.1 Set 'Allow indexing of encrypted files' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, 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.

**Rationale:**

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

**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\Administrative Templates\Windows Components\Search\Allow
indexing of encrypted files
```

**References:**

1. CCE-38277-0

## *18.8.42 Security Center*

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

## 18.8.43 Server for NIS

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

## 18.8.44 Shutdown Options

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

## 18.8.45 Smart Card

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

## 18.8.46 Sound Recorder

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

## 18.8.47 Store

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

## 18.8.48 Sync your settings

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

## 18.8.49 Tablet PC

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

## 18.8.50 Task Scheduler

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

## 18.8.51 Windows Calendar

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

## 18.8.52 Windows Color System

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

## 18.8.53 Windows Customer Experience Improvement Program

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

## 18.8.54 Windows Defender

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

## 18.8.55 Windows Error Reporting

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

## 18.8.56 Windows Installer

### *18.8.56.1 Set 'Always install with elevated privileges' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

Directs Windows Installer to use system permissions when it installs any program on the system.
This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop),

assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.
If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.
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: 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.

**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\AlwaysInstallElevated
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Installer\Always install with elevated privileges
```

**Impact:**

Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

**Default Value:**

Not configured

**References:**

1. CCE-36919-9

## *18.8.57 Windows Logon Options*

### *18.8.57.1 Set 'Sign-in last interactive user automatically after a system-initiated restart' to 'Disabled' (Scored)*

**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.

**Rationale:**

The device could be restarted and information disclosure could occur through the lock screen apps configured for the user.

**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:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableAutomaticRestart
SignOn
```

**Remediation:**

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`

```
Computer Configuration\Administrative Templates\Windows Components\Windows Logon
Options\Sign-in last interactive user automatically after a system-initiated restart
```

**Impact:**

If you enable or do not configure this policy setting, 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.

If you disable this policy setting, 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.

**References:**

1. CCE-36977-7

## *18.8.58 Windows Mail*

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

## *18.8.59 Windows Media Center*

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

## *18.8.60 Windows Media Digital Rights Management*

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

## *18.8.61 Windows Media Player*

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

## *18.8.62 Windows Messenger*

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

## 18.8.63 Windows Mobility Center

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

## 18.8.64 Windows Movie Maker

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

## 18.8.65 Windows PowerShell

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

## 18.8.66 Windows Reliability Analysis

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

## 18.8.67 Windows Remote Management (WinRM)

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

## 18.8.68 Windows Remote Shell

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

## 18.8.69 Windows SideShow

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

## 18.8.70 Windows System Resource Manager

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

## *18.8.71 Windows Update*

This section contains recommendations for Windows Update.

### *18.8.71.1 Set 'Configure Automatic Updates' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work: - Notify before downloading any updates and notify again before installing them. - Download the updates automatically and notify when they are ready to be installed. (Default setting) - Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: `Enabled`.

**Rationale:**

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs 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\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\Configure Automatic Updates
```

**Impact:**

Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

**Default Value:**

Download the updates automatically and notify when they are ready to be installed

**References:**

1. CCE-36172-5

## *18.8.71.2 Set 'Configure Automatic Updates: Scheduled install day' to '0 - Every day' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.

After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:
- Notify before downloading any updates and notify again before installing them.
- Download the updates automatically and notify when they are ready to be installed. (Default setting)
- Automatically download updates and install them on the schedule specified below.
If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: `0 - Every day`.

**Rationale:**

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs 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\Policies\Microsoft\Windows\WindowsUpdate\AU\ScheduledInstallDay
```

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `0 - Every day`.

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day
```

**Impact:**

Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

**Default Value:**

Not Defined

**References:**

1. CCE-36172-5

## *18.8.71.3 Set 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. Note that this policy setting has no impact if the Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box policy setting is enabled. The recommended state for this setting is: `Disabled`.

**Rationale:**

Updates are important for maintaining the ongoing security of a computer, therefore this setting should not 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\WindowsUpdate\AU\NoAUAsDefaultShutdownOption
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box
```

**Impact:**

If you enable this policy setting, the user's last shut down choice (Hibernate, Restart, etc.) is the default option in the Shut Down Windows dialog box, regardless of whether the 'Install Updates and Shut Down' option is available in the 'What do you want the computer to do?' list. If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

**Default Value:**

Disabled

**References:**

1. CCE-36508-0

### *18.8.71.4 Set 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting allows you to manage whether the Install Updates and Shut Down option is displayed in the Shut Down Windows dialog box. This policy setting works in conjunction with the following Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows Dialog box setting. The recommended state for this setting is: `Disabled`.

**Rationale:**

Updates are important for maintaining the ongoing security of a computer, therefore this setting should not 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\WindowsUpdate\AU\NoAUShutdownOp
tion
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do
not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box
```

**Impact:**

If you disable this policy setting, the Install Updates and Shut Down option will display in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

**Default Value:**

Disabled

**References:**

1. CCE-37385-2

## *18.8.71.5 Set 'No auto-restart with logged on users for scheduled automatic updates installations' to 'Disabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are: - Enabled - Disabled - Not Configured Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: `Disabled`.

**Rationale:**

Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

**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\WindowsUpdate\AU\NoAutoRebootWithLoggedOnUsers
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\No
auto-restart with logged on users for scheduled automatic updates installations
```

**Impact:**

If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

**Default Value:**

Enabled

**References:**

1. CCE-37027-0

## *18.8.71.6 Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled' (Scored)*

**Profile Applicability:**

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

**Description:**

This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. If you configure this policy setting to Enabled, a previously scheduled installation will begin after a specified number of minutes when you next start the computer. If you configure this policy setting to Disabled or Not configured, previously scheduled installations will occur during the next regularly scheduled installation time. Note: This policy setting only works when Automatic Updates is configured to perform scheduled update installations. If the Configure Automatic Updates setting is Disabled, the Reschedule Automatic Updates scheduled installations setting has no effect. You can enable the latter two settings to ensure that previously missed installations will be scheduled to install each time the computer restarts. The recommended state for this setting is: `Enabled`.

**Rationale:**

If Automatic Updates is not forced to wait a few minutes after a restart, computers in your environment might not have enough time to completely start all of their applications and services. If you specify enough time after a restart, new update installations should not conflict with the computer's startup procedures.

**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\WindowsUpdate\AU\RescheduleWaitTimeEnabled
```

**Remediation:**

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

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations
```

**Impact:**

Automatic Updates will not start until 10 minutes after the computer restarts.

**Default Value:**

Disabled

**References:**

1. CCE-37390-2

# 19 Administrative Templates (User)

## 19.1 Control Panel

## 19.1.1 Add or Remove Programs

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

## 19.1.2 Display

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

## 19.1.3 Personalization

### 19.1.3.1 Set 'Enable screen saver' to 'Enabled' (Scored)

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

This policy setting allows you to manage whether or not screen savers run. If the Screen Saver setting is disabled screen savers do not run and the screen saver section of the Screen Saver tab in Display in Control Panel is disabled. If this setting is enabled a screen saver will run if the following two conditions are met: first, that a valid screen saver is specified on the client via the Screen Saver Executable Name group policy setting or Control Panel on the client. Second, the screensaver timeout is set to a value greater than zero via the Screen Saver Timeout group policy setting or Control Panel on the client. The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**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_USERS\<SID>\Software\Policies\Microsoft\Windows\Control
Panel\Desktop\ScreenSaveActive
```

**Remediation:**

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

```
User Configuration\Administrative Templates\Control Panel\Personalization\Enable
screen saver
```

**Impact:**

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

**Default Value:**

Not Configured

**References:**

1. CCE-37970-1

## *19.1.3.2 Set 'Force specific screen saver: Screen saver executable name' to 'Enabled:scrnsave.scr' (Scored)*

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

This policy setting allows you to manage whether or not screen savers run. If the Screen Saver setting is disabled screen savers do not run and the screen saver section of the Screen Saver tab in Display in Control Panel is disabled. If this setting is enabled a screen saver will run if the following two conditions are met: first, that a valid screen saver is specified on the client via the Screen Saver Executable Name group policy setting or Control Panel on the client. Second, the screensaver timeout is set to a value greater than zero via the Screen Saver Timeout group policy setting or Control Panel on the client. The recommended state for this setting is: `Enabled:scrnsave.scr`.

**Rationale:**

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

**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_USERS\<SID>\Software\Policies\Microsoft\Windows\Control
Panel\Desktop\SCRNSAVE.EXE
```

**Remediation:**

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

```
User Configuration\Administrative Templates\Control Panel\Personalization\Force
specific screen saver
```

Then set the `Screen saver executable name` option to `scrnsave.scr`.

**Impact:**

The screen saver will automatically activate when the computer has been unattended for the amount of time specified by the Screen Saver timeout setting.

**Default Value:**

Not Configured

**References:**

1. CCE-37907-3

## *19.1.3.3 Set 'Password protect the screen saver' to 'Enabled' (Scored)*

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

If the Password protect the screen saver setting is enabled, then all screen savers are password protected, if it is disabled then password protection cannot be set on any screen saver. The recommended state for this setting is: `Enabled`.

**Rationale:**

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

**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_USERS\<SID>\Software\Policies\Microsoft\Windows\Control
Panel\Desktop\ScreenSaverIsSecure
```

**Remediation:**

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

```
User Configuration\Administrative Templates\Control Panel\Personalization\Password
protect the screen saver
```

**Impact:**

Users will have to provide their logon credentials when they want to access their locked desktop session.

**Default Value:**

Not Configured

**References:**

1. CCE-37658-2

## *19.1.3.4 Set 'Screen saver timeout:Seconds' to 'Enabled:900 or fewer seconds' (Scored)*

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

If the Screen Saver Timeout setting is enabled, then the screen saver will be launched when the specified amount of time has passed since the last user action. Valid values range from 1 to 89,400 seconds (24 hours). The setting has no effect if the wait time is set to zero or no screen saver has been specified. The recommended state for this setting is: `Enabled:900 or fewer seconds`.

**Rationale:**

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

**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_USERS\<SID>\Software\Policies\Microsoft\Windows\Control
Panel\Desktop\ScreenSaveTimeOut
```

**Remediation:**

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

```
User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver
timeout
```

Then set the `Seconds` option to `Enabled:900 or fewer seconds`.

**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.

**Default Value:**

Not Configured

**References:**

1. CCE-37908-1

## *19.2 Desktop*

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

## *19.3 Network*

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

## 19.4 Shared Folders

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

## 19.5 Start Menu and Taskbar

## 19.5.1 Notifications

### 19.5.1.1 Set 'Turn off toast notifications on the lock screen' to 'Enabled' (Scored)

**Profile Applicability:**

- Level 1 - Member Server

**Description:**

This policy setting turns off toast notifications on the lock screen. If you enable this policy setting, applications will not be able to raise toast notifications on the lock screen. If you disable or do not configure this policy setting, toast notifications on the lock screen are enabled and can be turned off by the administrator or user. No reboots or service restarts are required for this policy setting to take effect. The recommended state for this setting is `Enabled`.

**Rationale:**

While this feature can be handy for users applications that provide toast notifications might display sensitive personal or business data while the device is unattended.

**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_USERS\<SID>\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications\
NoToastApplicationNotificationOnLockScreen
```

**Remediation:**

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

```
User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn
off toast notifications on the lock screen
```

**Impact:**

By turning off this feature, applications will not be able to raise toast notifications on the lock screen, and user will not be able to access the information.

**References:**

1. CCE-36332-5

## *19.6 System*

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

## *19.7 Windows Components*

### *19.7.1 Add features to Windows 8.1*

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

### *19.7.2 App runtime*

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

### *19.7.3 Application Compatibility*

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

### *19.7.4 Attachment Manager*

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

# Appendix: Change History

| Date | Version | Changes for this version |
|---|---|---|
| 09-15-2014 | 1.0.0 | Initial Public Release |