the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Microsoft Windows Server 2008

Version 1.1.0
July 30th, 2010

http://cisecurity.org
feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Microsoft Windows Server 2008*, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows Server 2008 RTM and R2. This guide was tested against Microsoft Windows Server 2008 RTM and R2. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract 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.

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 2008.

Acknowledgements

The following individuals and organizations have demonstrated a commitment to the IT security community by contributing greatly to the consensus review of this configuration guide:

Maintainers
Susan Bradley
Jaime Castells, CISSP, CSSLP
Richard Manion
Phoram Mehta

Contributors and Reviewers
Phil Bassil
Sandya Boompelly, *CA, Inc.*
Jaime Castells, CISSP, CSSLP
Ron Colvin, *NASA*
Alan Carter Covell
Mike de Libero, *MDE Development, LLC*
Kurt Dillard
Dean Farrington, *Wells Fargo*
Blake Frantz, *Center for Internet Security*
Andre Gironda
Tanmoy Hazra, *CA, Inc.*
Jose F. Maldonado, *Microsoft Corporation*
Richard Manion
Adam W. Montville, CISA, CISSP, *Tripwire, Inc.*
Marco Shaw
Stephen Smoogen, *Red Hat Inc.*
Utkarsh Srivastava, CISSP, CISA, *Symantec*

Nguyen Tuan Trung, *FPT Software*
Martin White, *Smithsonian Institution*

CIS also extends special recognition to the authors of CIS Windows Server 2003 Benchmarks for setting the foundation for this Benchmark – Jeff Shawgo, Sidney Faber, and Collin Greene.

Additionally, Microsoft's Security Compliance Management Toolkit was an excellent resource in the development of this Benchmark. CIS also extends special recognition to development team of those resources. Readers are encouraged to download the toolkit to access many great resources, including tools such as GPOAccelerator and DCM Configuration Packs, which aid in the rapid deployment of security configuration policies.

Typographic 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

Security Profiles

This section defines the profiles used throughout the Benchmark.

Enterprise

Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 of later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.

Specialized Security – Limited Functionality (SSLF)

Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Scoring

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Not Defined

These items do not impact a system's score as the Benchmark does not recommend a specific value for this setting and profile combination.

Not Configured

The default behavior of Windows is commonly a secure behavior. For several settings, Windows allows the administrator to reinforce the default behavior by enabling or disabling a setting. Given this, for the Enterprise profiles, several settings are recommended `Not Configured` as the default behavior is secure. For the SSLF profiles, the Benchmark recommends that the default behavior be reinforced via GPO. An Enterprise profile system that is configured in accordance with the SSLF profile recommendation is not deemed out of conformance with this Benchmark.

1. Recommendations

1.1 Account Policies

1.1.1 Enforce password history

Description:
This control defines the number of unique passwords a user must leverage before a previously used password can be reused. For all profiles, the recommended state for this setting is `24 or more passwords remembered`.

Rationale:
Enforcing a sufficiently long password history will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential. For example, if an attacker compromises a given credential that is then expired, this control prevents the user from reusing that same compromised credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`24 passwords remembered`

References:
CCE-2237-6

1.1.2 Maximum password age

Description:
This control defines how many days a user can use the same password before it expires. For all profiles, the recommended state for this setting is `90 days or less`.

Rationale:
Enforcing a reasonably short password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`42 days`

References:
CCE-2200-4

1.1.3 Minimum password age

Description:
This control defines how many days a user must use the same password before it can be changed. For all profiles, the recommended state for this setting is `1 or more days`.

Rationale:
Enforcing a minimum password age prevents a user from quickly cycling through passwords in an attempt to reuse a familiar password. Preventing this increases the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:

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

Default Value:
`0 days`

References:
CCE-1861-4

1.1.4 Minimum password length

Description:
This control defines the minimum number of characters a user password must contain. It is recommended that this setting be configured as described below:

- For the Enterprise profile(s), the recommended value is `8 or more characters`.
- For the SSLF profile(s), the recommended value is `12 or more character`.

Rationale:
Enforcing a minimum password length helps protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`0 characters`

References:
CCE-2240-0

1.1.5 Password must meet complexity requirements

Description:
This control determines if new passwords are required to satisfy a certain level of complexity. This is accomplished by requiring the composition of all new passwords to be such that they are longer than six characters, are not comprised or the principal's username or real name, and contain characters from at least three distinct character classes (uppercase, lowercase, integer, non-alphanumeric). For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enforcing password complexity requirements reduces the probability of an attacker determining a valid credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Disabled`

References:
CCE-2126-1

1.1.6 Store passwords using reversible encryption

Description:
The Windows authentication model allows storage of a password hash rather than the actual password. A password hash cannot be decoded to regain the original password. Rather, to authenticate, the password must be hashed exactly the same way and compared with the original stored hash. If the values match, the correct password was presented, and access is granted.

In order to support some applications and their authentication, Windows can store passwords using reversible encryption. If at all possible, this should be avoided. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
If the system becomes compromised or the system hard disk is insecurely discarded, the confidentiality of passwords stored using reversible encryption is at a higher risk of compromise. Additionally, in the event of such a compromise, all systems, services, and applications accessible via the compromised credentials may realize an increased exposure to attacks via those credentials.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Disabled`

References:
CCE-2289-7

1.1.7 Account lockout duration

Description:
This control defines the minimum number of minutes a user must wait before a locked account is unlocked. Once the criteria for a lockout are met, the account becomes locked. However, the account will automatically become re-enabled once again after the duration specified in the "Account Lockout Duration." Specify 0 minutes to have the account remain locked out until an administrator manually unlocks the account. For all profiles, the recommended state for this setting is `15 or more minutes`.

Rationale:
Establishing a reasonable length of time a user must wait before attempting to reauthenticate after lockout reduces the number of authentication attempts an attacker may conduct in a given period of time against a single account. This in turn reduces the probability of an attacker successfully determining a valid credential. Additionally, establishing a reasonable time out period will prevent attackers from intentionally locking out all accounts until help desk manually resets them.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Not defined`

References:
CCE-1317-7

1.1.8 Account lockout threshold

Description:
This control defines the number of failed logon attempts before a user is locked out of an account. It is recommended that this setting be configured as described below:

- For the SSLF profile(s), the recommended value is `10 invalid logon attempts`.
- For the Enterprise profile(s), the recommended value is `15 invalid logon attempts`.

Rationale:
Enforcing an account lockout threshold will almost eliminated the effectiveness of automated brute force password attacks and improves the security of a system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`0 invalid logon attempts`

References:
CCE-1872-1

1.1.9 Reset account lockout counter after

Description:
Following an unsuccessful logon, the system increments the count of invalid attempts for this account. This counter continues to increment until the lockout threshold is reached, or the counter is reset. The "Reset Account Lockout After" setting defines how often the counter is reset. For all profiles, the recommended state for this setting is `15 or more minutes`.

Rationale:
Resetting the account lockout counter after a reasonable amount of time will reduce the probability of a user accidently locking themselves out over extended periods of time.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`0`

References:
CCE-2311-9

1.1.10 Enforce user logon restrictions

Description:

This control defines Kerberos-related attributes of domain user accounts, such as the Maximum lifetime for user ticket and Enforce user logon restrictions settings. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Disabling this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on, so this policy setting should be enabled.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Kerberos Policy\Enforce user logon restrictions
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Enabled`

References:
CCE-8594-4

1.1.11 Microsoft network server: Disconnect clients when logon hours expire

Description:
This control defines whether to disconnect a session when the user's valid logon hours expire. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Unless this setting is enabled, the benefits of imposing logon hours will not be realized.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
enableforcedlogoff
```

Default Value:

`Enabled`

References:
CCE-2029-7

1.1.12 Maximum tolerance for computer clock synchronization

Description:
This control defines maximum tolerance for computer clock synchronization. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `5`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Applicable`.

Rationale:
Kerberos leverages timestamps as a mitigation for defending against ticket replay attacks. For this mechanism to be effective, the clocks of Kerberos participants must be closely synchronized.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Kerberos Policy\Maximum tolerance for computer clock synchronization
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`5`

References:
CCE-8268-5

1.1.13 Maximum lifetime for service ticket

Description:
This control defines the maximum number of minutes that a granted session ticket can be used to access a service. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `600`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Applicable`.

Rationale:

Establishing a low ticket lifetime will ensure that user accounts that have been disabled or are restricted by logon hours are unable to access Kerberized resources with a ticket that was granted prior to the account being disabled or logon hours taking effect.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Kerberos Policy\Maximum lifetime for service ticket
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`600`

References:
CCE-8585-2

1.1.14 Maximum lifetime for user ticket renewal

Description:
This control defines the number of days during which a user`s ticket-grating ticket (TGT) can be renewed. It is recommended that this setting be configured as described below:

- For the SSLF Domain Controller profile(s), the recommended value is `7 days`.
- For the Enterprise Domain Controller profile(s), the recommended value is `6 days`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Applicable`.

Rationale:
Establishing a low ticket lifetime will ensure that user accounts that have been disabled or are restricted by logon hours are unable to access Kerberized resources with a ticket that was granted prior to the account being disabled or logon hours taking effect.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Kerberos Policy\Maximum lifetime for user ticket renewal
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

`7 days`

References:
CCE-8000-2

1.1.15 Maximum lifetime for user ticket

Description:
This control defines the maximum number of hours a user`s ticket-grating ticket (TGT) may be used. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `10`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Applicable`.

Rationale:
Establishing a low ticket lifetime will ensure that user accounts that have been disabled or are restricted by logon hours are unable to access Kerberized resources with a ticket that was granted prior to the account being disabled or logon hours taking effect.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Account
Policies\Kerberos Policy\Maximum lifetime for user ticket
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`10`

References:
CCE-8409-5

1.2 Audit Policy

Windows Server 2008 has detailed audit facilities that allow administrators to tune their audit policy with greater specificity. By enabling the legacy audit facilities outlined in this section, it is probable that the performance of the system may be reduced and that the security event log will realize high event volumes. Given this, it is recommended that Detailed Audit Policies in the subsequent section be leveraged in favor over the policies represented below. Additionally, the "Force audit policy subcategory settings", which is recommended to be enabled, causes Windows to favor the audit subcategories over the legacy audit policies. For the above reasons, this Benchmark does not prescribe specific values for legacy audit policies.

1.2.1 Audit account logon events

Description:
Audit account logon events will create an entry in the Security Event Log when a local interactive logon, network logon, batch process, or service logon occurs. Failed account logons may show a trend for password attacks; successful logon events are important to identify which user was logged on to the computer at a given time. "Account Logon" events are generated from the use of domain accounts; this differs from "Logon Events" which are generated by the use of local accounts. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit account logon events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2251-7
CCE-1779-8

1.2.2 Audit account management

Description:
This setting can be used to create an entry in the Security Event log when account management activities occur. Examples of account management activities include create or deleting a user or group, disabling or enabling a user, and renaming a user or group. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit account management
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2211-1
CCE-2538-7

1.2.3 Audit directory service access

Description:
Auditing Directory service access will create an entry in the Security Event log when objects within Active Directory that been accessed. Enabling this control has no effect unless a given object's SACL contains an ACE with audit flags. Enabling directory service access auditing may generate a large amount of log entries, and must be implemented with care. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit directory service access
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2215-2
CCE-2582-5

1.2.4 Audit logon events

Description:
Logon Events will identify which accounts are accessing resources on the local computer. These events are generated only when local machine credentials are used. Even if a

machine is a domain member, it is still possible to log on to the computer using a local account. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit logon events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2242-6
CCE-2574-2

1.2.5 Audit object access

Description:
This control provides auditing capabilities at the object level. This is most commonly used for file system objects. Enabling this control has no effect unless a given object's SACL contains an ACE with audit flags. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit object access
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2136-0
CCE-2217-8

1.2.6 Audit policy change

Description:
This control defines whether the audit for each policy change event is activated. Changes to User Rights, Audit Policies, or Trust Policies will produce events in the Security Event Log if this is enabled. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit policy change
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2433-1
CCE-2512-2

1.2.7 Audit privilege use

Description:
Auditing privilege use enables auditing for any operation that requires a specific privilege grant. If this is enabled, events will be generated in the security event log when a user or process attempts to bypass traverse checking, debug programs, create a token object, replace a process level token, or generate security audits.

If security credentials are used to backup or restore files or directories using the "Backup or Restore" user right, and if this setting is set, security events will be generated.

Privilege Use is used by all user accounts on a regular basis. If success and failure events are audited, there will be a great many events in the event log reflecting such use.
For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:

It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit privilege use
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2035-4
CCE-2265-7

1.2.8 Audit process tracking

Description:
When this option is enabled, an event is generated each time an application or a user starts, stops, or otherwise changes a process. This creates a very large event log very quickly, and the information is not normally exceptionally useful, unless you are tracking a very specific behavior. Auditing process tracking is not required, and is only recommended when absolutely necessary.

Caution: Enabling this setting may generate an excessive amount of log entries. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit process tracking
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-2295-4
CCE-1895-2

1.2.9 Audit system events

Description:
Auditing System events is very important. System events include starting or shutting down the computer, full event logs, and other items which impact the computer, but may not be directly related to security. System events are particularly useful when reviewing a system during or after an incident. For all profiles, the recommended state for this setting is `Not Defined`.

Rationale:
It is recommended that audit subcategories be leveraged instead of legacy audit policies. A system is not considered less secure if this policy is set to Success and/or Failure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Audit Policy\Audit system events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No auditing`

References:
CCE-1837-4
CCE-1939-8

1.2.10Audit: Shut down system immediately if unable to log security audits

Description:
This setting causes the system to shut down if it is unable to log a security event to the Security Event log. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
The risk of causing irreparable damage to the operating system, applications, or data coupled with the unavailability of services provided by the system due to it being immediately shut down typically greatly outweigh the risk of being unable to log a Security event.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v crashonauditfail
```

Default Value:
`Disabled`

References:
CCE-2315-0

1.2.11 Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

Description:
This setting causes Windows to respect audit subcategories in favor of the legacy audit policies. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Before Windows Server 2008 R2, no GPOs existed for configuring audit subcategories. As a result, subcategory audit policies established with auditpol.exe were trumped in favor of the legacy audit policy pushed over GPO. Enabling this setting causes the local system to favor the audit subcategories over the legacy audit policy.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
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
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v
scenoapplylegacyauditpolicy
```

Default Value:
`Not defined`

References:

CCE-2276-4

1.3 Detailed Security Auditing

This section articulates the detailed audit policies introduced in Windows Vista and later. Prior to Windows Server 2008 R2, these settings could only be established via the `auditpol.exe` utility. However, in Server 2008 R2, GPOs exist for managing these items. Guidance is provided for establishing the recommended state using via GPO and `auditpol.exe`. The values prescribed in this section represent the minimum recommended level of auditing.

1.3.1 Audit Policy: System: IPsec Driver

Description:
This control defines whether Internet Protocol security (IPsec) driver activity is audited. For all profiles, the recommended state for this setting is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\System\Audit IPSec Driver\Audit Policy: System: IPsec Driver
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"IPsec Driver" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"IPsec Driver"
```

Default Value:
`No auditing`

References:
CCE-2608-8
CCE-2351-5

1.3.2 Audit Policy: System: Security State Change

Description:

This control defines whether the audit is activated for changes in the security state of the system. For all profiles, the recommended state for this setting is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\System\Audit Security State Change\Audit Policy: System: Security
State Change
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Security State Change" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Security State Change"
```

Default Value:
`Success`

References:
CCE-2414-1
CCE-2448-9

1.3.3 Audit Policy: System: Security System Extension

Description:
This control defines whether the audit is activated for the loading of extension code such as authentication packages by the security subsystem. For all profiles, the recommended state for this setting is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\System\Audit Security System Extension\Audit Policy: System: Security
System Extension
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Security System Extension"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Security System Extension"
```

Default Value:
`No auditing`

References:
CCE-1841-6
CCE-2545-2

1.3.4 Audit Policy: System: System Integrity

Description:
This control defines whether the audit is activated for violations of integrity of the security subsystem. For all profiles, the recommended state for this setting is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\System\Audit System Integrity\Audit Policy: System: System Integrity
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"System Integrity" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"System Integrity"
```

Default Value:
`Success and Failure`

References:
CCE-2348-1
CCE-2440-6

1.3.5 Audit Policy: Logon-Logoff: Logoff

Description:
This control defines whether the audit is activated for when a user logs off from the system. For all profiles, the recommended state for this setting is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Logon/Logoff\Audit Logoff\Audit Policy: Logon-Logoff: Logoff
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Logoff" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Logoff"
```

Default Value:
`Success and Failure`

References:
CCE-2569-2
CCE-2616-1

1.3.6 Audit Policy: Logon-Logoff: Logon

Description:
This control defines whether the audit is activated for when a user attempts to log on to the system. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Logon/Logoff\Audit Logon\Audit Policy: Logon-Logoff: Logon
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Logon" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Logon"
```

Default Value:
`Success`

References:
CCE-2441-4
CCE-2470-3

1.3.7 Audit Policy: Logon-Logoff: Special Logon

Description:
This control defines whether the audit is activated when a special logon is used. For all profiles, the recommended state for this setting is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Logon/Logoff\Audit Special Logon\Audit Policy: Logon-Logoff: Special
Logon
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Special Logon" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Special Logon"
```

Default Value:
`Success`

References:
CCE-2610-4
CCE-2558-5

1.3.8 Audit Policy: Object Access: File System

Description:
This control defines whether the audit is activated when file objects are accessed. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `No auditing`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\Object
Access\Audit File System\Audit Policy: Object Access: File System
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"File System" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"File System"
```

Default Value:
`No auditing`

References:
CCE-2531-2
CCE-2488-5

1.3.9 Audit Policy: Object Access: Registry

Description:
This control defines whether the audit is activated when registry objects are accessed. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `No auditing`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\Object
Access\Audit Registry\Audit Policy: Object Access: Registry
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Registry" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Registry"
```

Default Value:
`No auditing`

References:

CCE-2553-6
CCE-2505-6

1.3.10 Audit Policy: Privilege Use: Sensitive Privilege Use

Description:
This control defines whether the audit is activated when a user account or service uses a sensitive privilege. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `No auditing`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Privilege Use\Audit Sensitive Privilege Use\Audit Policy: Privilege
Use: Sensitive Privilege Use
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Sensitive Privilege Use"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Sensitive Privilege Use"
```

Default Value:
`No auditing`

References:
CCE-2205-3
CCE-2349-9

1.3.11 Audit Policy: Detailed Tracking: Process Creation

Description:

This control defines whether the audit is activated when a process is created and the name of the program that created it. For all profiles, the recommended state for this setting is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Detailed Tracking\Audit Process Creation\Audit Policy: Detailed
Tracking: Process Creation
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Process Creation" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Process Creation"
```

Default Value:
`No auditing`

References:
CCE-2002-4
CCE-2375-4

1.3.12 Audit Policy: Policy Change: Audit Policy Change

Description:
This control defines whether the audit is activated when change in audit policy including SACL changes occur. For all profiles, the recommended state for this setting is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\Policy
Change\Audit Audit Policy Change\Audit Policy: Policy Change: Audit Policy
Change
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Audit Policy Change" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Audit Policy Change"
```

Default Value:
`Success`

References:
CCE-2433-1
CCE-2269-9
CCE-2268-1
CCE-2512-2

1.3.13 Audit Policy: Policy Change: Authentication Policy Change

Description:
This control defines whether the audit is activated when changes in authentication policy occur. For all profiles, the recommended state for this setting is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\Policy
Change\Audit Authentication Policy Change\Audit Policy: Policy Change:
Authentication Policy Change
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Authentication Policy Change"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Authentication Policy Change"
```

Default Value:
Success

References:
CCE-2566-8
CCE-2151-9

1.3.14 Audit Policy: Account Management: Computer Account Management

Description:
This control defines whether the audit is activated when a computer account management event, such as a create, change, rename, delete, disable or enable event occurs. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Management\Audit Computer Account Management\Audit Policy:
Account Management: Computer Account Management
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Computer Account Management"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Computer Account Management"
```

Default Value:
Success

References:
CCE-2288-9
CCE-2415-8

1.3.15 Audit Policy: Account Management: Other Account Management Events

Description:
This control defines whether the audit is activated when an account management event occurs. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Management\Audit Other Account Management Events\Audit Policy:
Account Management: Other Account Management Events
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Other Account Management Events"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Other Account Management Events"
```

Default Value:
`No auditing`

References:
CCE-2485-1
CCE-2062-8

1.3.16 Audit Policy: Account Management: Security Group Management

Description:

This control defines whether the audit is activated when a security group management event, such as a create, change or delete event occurs. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Management\Audit Security Group Management\Audit Policy:
Account Management: Security Group Management
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Security Group Management"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Security Group Management"
```

Default Value:
`Success`

References:
CCE-2443-0
CCE-2560-1

1.3.17 Audit Policy: Account Management: User Account Management

Description:
This control defines whether the audit is activated when a user account management event, such as a create, change, rename, delete, disable or enable event occurs. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Management\Audit User Account Management\Audit Policy: Account
Management: User Account Management
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"User Account Management"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"User Account Management"
```

Default Value:
`Success`

References:
CCE-2394-5
CCE-2411-7

1.3.18Audit Policy: DS Access: Directory Service Access

Description:
This control defines whether the audit is activated when an AD DS object is accessed. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `No auditing`.
- For the SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:

Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\DS
Access\Audit Directory Service Access\Audit Policy: DS Access: Directory
Service Access
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Directory Service Access"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Directory Service Access"
```

Default Value:
`No auditing`

References:
CCE-2367-1
CCE-1926-5

1.3.19 Audit Policy: DS Access: Directory Service Changes

Description:
This control defines whether the audit is activated when changes in Active Directory Domain Services (AD DS) occur. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `No auditing`.
- For the SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy Object\DS
Access\Audit Directory Service Changes\Audit Policy: DS Access: Directory
Service Changes
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Directory Service Changes"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Directory Service Changes"
```

Default Value:
`No auditing`

References:
CCE-2635-1
CCE-2445-5

1.3.20 Audit Policy: Account Logon: Credential Validation

Description:
This control defines whether the audit is activated to report the results of validation tests on credentials submitted by a user account logon request. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Success`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Account Logon\Audit Credential Validation\Audit Policy: Account Logon:
Credential Validation
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Credential Validation" [/success:<enable|disable>
/failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Credential Validation"
```

Default Value:
`Success`

References:
CCE-2463-8
CCE-2516-3

1.4 Event Log

1.4.1 Application: Maximum Log Size (KB)

Description:
This controls the maximum size of the log file in kilobytes. For all profiles, the recommended state for this setting is `32768 KB or greater`.

Rationale:
The recommended log size is sufficient for capturing over 2000 events per month.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Application\Application: Maximum Log Size (KB)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\Application /v
MaxSize
```

Default Value:
`20480 KB`

1.4.2 Application: Retain old events

Description:

This control determines Event Log behavior when the log file reaches its maximum size. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Setting this value to Disabled will cause Windows to overwrite the oldest events in the log to continue logging new events.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Application: Retain old events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\Application /v Retention
```

Default Value:
`Disabled`

1.4.3 Security: Maximum Log Size (KB)

Description:
This controls the maximum size of the log file in kilobytes. For all profiles, the recommended state for this setting is `81920 KB or greater`.

Rationale:
The recommended log size is sufficient for capturing over 5000 events per month.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Security: Maximum Log Size (KB)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\Security /v MaxSize
```

Default Value:
`20480 KB`

1.4.4 Security: Retain old events

Description:
This control determines Event Log behavior when the log file reaches its maximum size. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Setting this value to Disabled will cause Windows to overwrite the oldest events in the log to continue logging new events.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Security: Retain old events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\Security /v Retention
```

Default Value:
`Disabled`

1.4.5 System: Maximum Log Size (KB)

Description:
This controls the maximum size of the log file in kilobytes. For all profiles, the recommended state for this setting is `32768 KB or greater`.

Rationale:
The recommended log size is sufficient for capturing over 2000 events per month.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\System: Maximum Log Size (KB)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\System /v MaxSize
```

Default Value:
`20480 KB`

1.4.6 System: Retain old events

Description:
This control determines Event Log behavior when the log file reaches its maximum size. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Setting this value to Disabled will cause Windows to overwrite the oldest events in the log to continue logging new events.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\System\System: Retain old events
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\EventLog\System /v
Retention
```

Default Value:
`Disabled`

1.5 Windows Firewall

1.5.1 Windows Firewall: Allow ICMP exceptions (Domain)

Description:
This control defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling this setting to in conjunction with window firewall prevents attackers to take advantage of computers that accept ICMP message types.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow ICMP
exceptions (Domain)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings
/v
AllowInboundEchoRequest,AllowInboundMaskRequest,AllowInboundRouterRequest,All
owInboundTimestampRequest,AllowOutboundDestinationUnreachable,AllowOutboundPa
cketTooBig,AllowOutboundParameterProblem,AllowOutboundSourceQuench,AllowOutbo
undTimeExceeded,AllowRedirect
```

1.5.2 Windows Firewall: Allow ICMP exceptions (Standard)

Description:
This control defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling this setting to in conjunction with window firewall prevents attackers to take advantage of computers that accept ICMP message types.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall \Standard Profile\Windows Firewall: Allow ICMP
exceptions (Standard)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSettings
/v
AllowInboundEchoRequest,AllowInboundMaskRequest,AllowInboundRouterRequest,All
owInboundTimestampRequest,AllowOutboundDestinationUnreachable,AllowOutboundPa
cketTooBig,AllowOutboundParameterProblem,AllowOutboundSourceQuench,AllowOutbo
undTimeExceeded,AllowRedirect
```

1.5.3 Windows Firewall: Apply local connection security rules (Domain)

Description:
This control defines whether a local administrator is allowed to create local connection security rules that apply together with connection security rules configured by Group policy. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No`.

Rationale:
Enforcing and restricting access to this control will limit the potential for user with administrative privileges to create connection security rules that expose the system to remote attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile /v
AllowLocalIPsecPolicyMerge
```

Default Value:
`No`

1.5.4 Windows Firewall: Apply local connection security rules (Private)

Description:
This control defines whether a local administrator is allowed to create local connection security rules that apply together with connection security rules configured by Group policy. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No`.

Rationale:
Configuring the system as recommended will limit the potential for a user with administrative privileges to create a connection security rule that exposes the system to remote attacks. When this control is set to 'No' only firewalls rules defined in Group Policy are respected.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile /v
AllowLocalIPsecPolicyMerge
```

Default Value:
No

1.5.5 Windows Firewall: Apply local connection security rules (Public)

Description:
This control defines whether a local administrator is allowed to create local connection security rules that apply together with connection security rules configured by Group policy. For all profiles, the recommended state for this setting is No.

Rationale:
Configuring the system as recommended will limit the potential for a user with administrative privileges to create a connection security rule that exposes the system to remote attacks. When this control is set to 'No' only firewalls rules defined in Group Policy are respected.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile /v
AllowLocalIPsecPolicyMerge
```

Default Value:
No

1.5.6 Windows Firewall: Apply local firewall rules (Domain)

Description:
This control defines whether a local administrator is allowed to create local firewall rules that apply together with firewall rules configured by Group policy. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No`.

Rationale:
Configuring the system as recommended will limit the potential for a user with administrative privileges to create a firewall rule that exposes the system to remote attacks. When this control is set to 'No' only firewalls rules defined in Group Policy are respected.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile /v
AllowLocalPolicyMerge
```

Default Value:
`Yes`

1.5.7 Windows Firewall: Apply local firewall rules (Private)

Description:
This control defines whether a local administrator is allowed to create local firewall rules that apply together with firewall rules configured by Group policy. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No`.

Rationale:

Configuring the system as recommended will limit the potential for a user with administrative privileges to create a firewall rule that exposes the system to remote attacks. When this control is set to 'No' only firewalls rules defined in Group Policy are respected.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile /v
AllowLocalPolicyMerge
```

Default Value:
`Yes`

1.5.8 Windows Firewall: Apply local firewall rules (Public)

Description:
This control defines whether a local administrator is allowed to create local firewall rules that apply together with firewall rules configured by Group policy. For all profiles, the recommended state for this setting is `No`.

Rationale:
Configuring the system as recommended will limit the potential for a user with administrative privileges to create a firewall rule that exposes the system to remote attacks. When this control is set to 'No' only firewalls rules defined in Group Policy are respected.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile /v
AllowLocalPolicyMerge
```

Default Value:
`Yes`

1.5.9 Windows Firewall: Display a notification (Domain)

Description:
This control defines whether Windows Firewall displays notifications when a program is blocked from receiving inbound connections. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Yes`.

Rationale:
Notifying the user that an application is attempting to add a firewall exception may alert the user of unexpected application behavior that will increase the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile /v
DisableNotifications
```

Default Value:
`Yes`

1.5.10 Windows Firewall: Display a notification (Private)

Description:
This control defines whether Windows Firewall displays notifications when a program is blocked from receiving inbound connections. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Yes`.

Rationale:
Notifying the user that an application is attempting to add a firewall exception may alert the user of unexpected application behavior that will increase the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile /v
DisableNotifications
```

Default Value:
`Yes`

1.5.11 Windows Firewall: Display a notification (Public)

Description:
This control defines whether Windows Firewall displays notifications when a program is blocked from receiving inbound connections. For all profiles, the recommended state for this setting is `No`.

Rationale:
For the public profile, this benchmark recommends against processing local firewall exceptions. Therefore, if a user is provided with a notification to create an exception their action will be ignored.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile /v
DisableNotifications
```

Default Value:
`Yes`

1.5.12 Windows Firewall: Firewall state (Domain)

Description:
This control defines if the Windows Firewall will use the settings for this profile to filter network traffic. If set to off, the Windows Firewall will not use any of the firewall rules or connection security rules for this profile. For all profiles, the recommended state for this setting is `On`.

Rationale:
Enabling the Windows Firewall for this profile will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile /v
EnableFirewall
```

Default Value:
`On`

1.5.13 Windows Firewall: Firewall state (Private)

Description:
This control defines if the Windows Firewall will use the settings for this profile to filter network traffic. If set to off, the Windows Firewall will not use any of the firewall rules or connection security rules for this profile. For all profiles, the recommended state for this setting is `On`.

Rationale:

Enabling the Windows Firewall for this profile will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile /v
EnableFirewall
```

Default Value:
`On`

1.5.14 Windows Firewall: Firewall state (Public)

Description:
This control defines if the Windows Firewall will use the settings for this profile to filter network traffic. If set to off, the Windows Firewall will not use any of the firewall rules or connection security rules for this profile. For all profiles, the recommended state for this setting is `On`.

Rationale:
Enabling the Windows Firewall for this profile will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile /v
EnableFirewall
```

Default Value:
`On`

1.5.15 Windows Firewall: Inbound connections (Domain)

Description:
This control defines whether inbound connections are blocked or allowed to connect to the system for this profile. For all profiles, the recommended state for this setting is `Block`.

Rationale:
Configuring the system as recommended will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall
with Advanced Security\Windows Firewall with Advanced Security\Windows
Firewall Properties\Domain Profile Tab\Windows Firewall: Inbound connections
(Domain)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile /v
DefaultInboundAction
```

Default Value:
`Block`

1.5.16 Windows Firewall: Inbound connections (Private)

Description:
This control defines whether inbound connections are blocked or allowed to connect to the system. For all profiles, the recommended state for this setting is `Block`.

Rationale:
Configuring the system as recommended will greatly reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall
with Advanced Security\Windows Firewall with Advanced Security\Windows
Firewall Properties\Private Profile Tab\Windows Firewall: Inbound connections
(Private)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile /v
DefaultInboundAction
```

Default Value:
`Block`

1.5.17 Windows Firewall: Inbound connections (Public)

Description:
This control defines whether inbound connections are blocked or allowed to connect to the system for this profile. For all profiles, the recommended state for this setting is `Block`.

Rationale:
Configuring the system as recommended will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall
with Advanced Security\Windows Firewall with Advanced Security\Windows
Firewall Properties\Public Profile Tab\Windows Firewall: Inbound connections
(Public)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile /v
DefaultInboundAction
```

Default Value:
`Block`

1.5.18 Windows Firewall: Prohibit notifications (Domain)

Description:
This control defines whether Windows Firewall will display notifications to users when a program requests an exception be added to the Windows Firewall. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:

Notifying the user that an application is attempting to add a firewall exception may alert the user of unexpected application behavior that will increase the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall\Domain Profile\Windows Firewall: Prohibit
notifications (Domain)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile /v
DisableNotifications
```

Default Value:
`Disabled`

1.5.19 Windows Firewall: Prohibit notifications (Standard)

Description:
This control defines whether Windows Firewall will display notifications to users when a program requests an exception be added to the Windows Firewall. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Notifying the user that an application is attempting to add a firewall exception may alert the user of unexpected application behavior that will increase the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall \Standard Profile\Windows Firewall: Prohibit
notifications (Standard)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile /v
DisableNotifications
```

Default Value:
`Disabled`

1.5.20 Windows Firewall: Protect all network connections (Domain)

Description:
This control defines whether the Windows Firewall is enabled for this profile. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended is important in protecting the computers from potential network-based attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall\Domain Profile\Windows Firewall: Protect all
network connections (Domain)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile /v
EnableFirewall
```

1.5.21 Windows Firewall: Protect all network connections (Standard)

Description:
This control defines whether the Windows Firewall is enabled for this profile. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended is important in protecting the computers from potential network-based attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Network\Network
Connections\Windows Firewall \Standard Profile\Windows Firewall: Protect all
network connections (Standard)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile /v
EnableFirewall
```

1.6 Windows Update

1.6.1 Configure Automatic Updates

Description:
This control defines whether Windows will receive security updates from Windows Update or WSUS. For all profiles, the recommended state for this setting is `Enabled: 3 - Auto download and notify for install`.

Rationale:
Establishing automated means to deploy and apply system updates will help ensure the system always has the most recent critical operating system updates and service packs installed. It is recommended that organizations align this option with their patch policy. For more information on patch management, see http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\Configure Automatic Updates
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v
AUOptions
```

Default Value:

```
Download the updates automatically and notify when they are ready to be
installed
```

References:
CCE-8478-0

1.6.2 Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box

Description:
This control defines whether the Install Updates and Shut Down option is displayed in the Shut Down Windows dialog box. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:

Ensuring that the 'Install Updates and Shut Down' option is visible in the shut down Windows dialog will reinforce the positive behavior of installing security updates.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in  Shut Down Windows dialog box
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v NoAUShutdownOption
```

Default Value:
`Disabled`

1.6.3 Reschedule Automatic Updates scheduled installations

Description:
This control defines whether to delay automatic updates installation that would otherwise normally occur on computer start up. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will help ensure that system updates do not fail to install or impact system startup by avoiding conflict with system startup procedures.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v RescheduleWaitTimeEnabled
```

Default Value:
`Disabled`

References:
CCE-7646-3

1.7 User Account Control

1.7.1 User Account Control: Admin Approval Mode for the Built-in Administrator account

Description:
This control defines whether the built-in Administrator account runs in Admin Approval Mode. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will extend the security benefits of UAC to the Built-in Administrator account.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
FilterAdministratorToken
```

Default Value:
`Disabled`

References:
CCE-2302-8

1.7.2 User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode

Description:
This control defines the behavior of Windows when a logged on administrator attempts to complete a task requiring raised privileges. For all profiles, the recommended state for this setting is `Prompt for credentials`.

Rationale:
Requiring users to reauthenticate when performing administrative actions will reduce the probability of malicious software or unauthorized users accessing an unlocked console from being able to view or manipulate sensitive Windows settings.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
ConsentPromptBehaviorAdmin
```

Default Value:
`Prompt for consent`

References:
CCE-2474-5

1.7.3 User Account Control: Behavior of the elevation prompt for standard users

Description:
This control defines the behavior of Windows when a standard user attempts to complete a task requiring raised privileges. For all profiles, the recommended state for this setting is `Automatically deny elevation requests`.

Rationale:
Standard users will not have credentials required to approve the elevation request.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
ConsentPromptBehaviorUser
```

Default Value:
`Prompt for credentials`

References:
CCE-2355-6

1.7.4 User Account Control: Detect application installations and prompt for elevation

Description:
This control defines how Windows responds to application installation requests. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will help ensure that users and administrators are aware of and explicitly approve software installations.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableInstallerDetection
```

Default Value:
`Enabled`

References:
CCE-2487-7

1.7.5 User Account Control: Only elevate UIAccess applications that are installed in secure locations

Description:
This control helps protect Windows by only allowing applications installed in a secure location, such as `%ProgramFiles%` and `%SystemRoot%\System32`, to run with elevated privileges. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will help reduce the probability of elevating the privileges of an application that may have been created or altered by a malicious user.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableSecureUIAPaths
```

Default Value:
`Enabled`

References:
CCE-2473-7

1.7.6 User Account Control: Run all administrators in Admin Approval Mode

Description:
This control is the UAC on/off switch and defines whether users and administrators are prompted when they attempt to perform administrative operations. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Leveraging UAC will make it more difficult for a compromised process that is executing under the context of an administrative user to silently change Windows settings.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableLUA
```

Default Value:
`Enabled`

References:
CCE-2478-6

1.7.7 User Account Control: Switch to the secure desktop when prompting for elevation

Description:
This control defines whether the UAC elevation prompt is displayed on the secure desktop. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will limit the potential for malicious software to obtain credentials used for elevation.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
PromptOnSecureDesktop
```

Default Value:
`Enabled`

References:
CCE-2500-7

1.7.8 User Account Control: Virtualize file and registry write failures to per-user locations

Description:
This control defines whether Windows will virtualize file and registry writes to user locations when a non-UAC compliant application attempts to write to protected areas, such as the %SYSTEMROOT%. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Configuring the system as recommended will limit the potential vulnerabilities caused by applications writing data to unpermitted locations on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableVirtualization
```

Default Value:
`Enabled`

References:
CCE-2266-5

1.7.9 User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop

Description:
This control defines whether an application is allowed to prompt for elevation without using the secure desktop. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Configuring the system as recommended will limit the potential for malicious software to obtain credentials used for elevation.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
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
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableUIADesktopToggle
```

Default Value:
`Disabled`

References:
CCE-2434-9

1.8 User Rights

1.8.1 Access this computer from the network

Description:
This control defines whether other users on the network are allowed to connect to this computer. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Administrators, Authenticated Users`.
- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`.

Rationale:
Configuring the system as recommended will ensure only authorized accounts can access the local computer from the network.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Everyone, Administrators, Users, Backup Operators`

References:
CCE-2075-0

1.8.2 Act as part of the operating system

Description:
This control defines whether a process is allowed to assume the identity of a any other user. For all profiles, the recommended state for this setting is `No one`.

Rationale:
This user right is very powerful as it enables grantees to effectively circumvent access controls on the local system by assuming the identity of any other user.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No one`

References:
CCE-2079-2

1.8.3 Adjust memory quotas for a process

Description:
This control allows a user to modify the maximum amount of memory available to a process. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators, LOCAL SERVICE, NETWORK SERVICE`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Limiting the grant of this right will help minimize the chance of a user maliciously or unintentionally impacting system performance, which may result in a denial of service.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`LOCAL SERVICE, NETWORK SERVICE, Administrators`

References:
CCE-2004-0

1.8.4 Back up files and directories

Description:
This control defines whether a user is allowed to backup files and directories on the system. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will reduce the probability of unauthorized disclosure of historic sensitive data. Additionally, restricting the grant of this right will limit the exposure to user maliciously or unintentionally overwriting data that is more recent.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators, Backup Operators`

References:
CCE-1321-9

1.8.5 Bypass traverse checking

Description:
This control defines whether a user with no Traverse Folder access permission is allowed to pass through folders as they browse NTFS or the registry. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server profile(s), the recommended value is `Administrators, Authenticated Users, Backup Operators, Local Service, Network Service`.
- For the Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.
- For the SSLF Domain Controller profile(s), the recommended value is `Authenticated Users, Local Service, Network Service`.
- For the SSLF Member Server profile(s), the recommended value is `Administrators, Authenticated Users, Local Service, Network Service`.

Rationale:
Enforcing or disabling access to this control slightly reduces the potential for unauthorized access to information.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Bypass traverse checking
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
```
Everyone, Administrators, Authenticated Users,  Backup Operators, Local Service, Network Service
```

References:
CCE-2285-5

1.8.6 Change the system time

Description:
This control defines which users and groups are allowed to change the time and date of the system. For all profiles, the recommended state for this setting is `LOCAL SERVICE, Administrators`.

Rationale:
Limiting the grant of this right will help ensure that time stamps on event log entries, file, and folders are correct. Correct time stamps are essential when investigating a security incident.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`LOCAL SERVICE, Administrators`

References:
CCE-2290-5

1.8.7 Create a pagefile

Description:
This control defines whether a user is allowed to modify the size of a pagefile. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.

- For the Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will reduce the probability of a user negatively impacting system performance by modifying the size of the pagefile.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

```
Administrators, SERVICE, Local Service, Network Service
```

References:
CCE-1328-4

1.8.8 Create a token object

Description:
This user right provides the ability to alter the access token object for any process or logged on user. For all profiles, the recommended state for this setting is `No One`.

Rationale:
Users with this right can be used to circumvent the local access control system by altering the grantees own security access token or the tokens of others.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No One`

References:
CCE-1491-0

1.8.9 Create global objects

Description:
This control defines whether a user is allowed to create global objects that are available to all sessions. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators, SERVICE, Local Service, Network Service`.

Rationale:
Enforcing and restricting access to this control will limit the potential for application failure and data corruption.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

```
Administrators, SERVICE, Local Service, Network Service
```

References:
CCE-2226-9

1.8.10 Create permanent shared objects

Description:
This control defines whether a user is allowed to create new shared objects. For all profiles, the recommended state for this setting is `No One`.

Rationale:
This user right is not typically required by standard user accounts. Therefore, from a least privilege perspective, this user right should not be assigned.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No One`

References:
CCE-1341-7

1.8.11 Debug programs

Description:
This control defines whether a user account is allowed to attach a debugger to any process or the kernel. A debugger allows a user to view and manipulate the memory and execution context of any process. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Administrators`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No one`.

Rationale:
Configuring the system as recommended will reduce the probability for a malicious local user to circumvent application or system security control or view sensitive information loaded in memory.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2310-1

1.8.12 Deny access to this computer from the network

Description:
This control defines which accounts are not permitted to connect to the local computer from the network. For all profiles, the recommended state for this setting is `Guests`.

Rationale:

Configuring the system as recommended will ensure only authorized accounts can access the local computer from the network.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Guests`

References:
CCE-2314-3

1.8.13 Enable computer and user accounts to be trusted for delegation

Description:
This control defines whether a user account is allowed to change the Trusted for Delegation setting on a computer object in Active Directory. Delegation provides an impersonating process with the ability to use the impersonated principal's identity when making requests of remote services. For all profiles, the recommended state for this setting is `No One`.

Rationale:
Configuring the system as recommended will reduce the probability of a malicious user or process from accessing network resources as an impersonated client.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No One`

References:
CCE-1481-1

1.8.14 Force shutdown from a remote system

Description:
This control defines whether a user account is allowed to remotely shutdown a computer. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will limit the potential for denial of service (DoS) attack.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-1750-9

1.8.15 Impersonate a client after authentication

Description:
This control defines whether a service or application that executes under a given account context is allowed to impersonate the account of a connecting client after the client has authenticated. This capability is most commonly used by COM or RPC servers. For all profiles, the recommended state for this setting is `Administrators, SERVICE, Local Service, Network Service`.

Rationale:
This user right introduces the risk of an elevation of privileges vulnerability especially if it is granted to a malicious or compromised accounts. A lower privileged service that possess this right can impersonate a higher privileged user, such as the Administrator, if the Administrator connects and authenticates to the service.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
```
Administrators, SERVICE, Local Service, Network Service
```

References:
CCE-1346-6

1.8.16 Increase scheduling priority

Description:
This control defines whether a user is allowed to change the base priority class for a process. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Restricting which users can increase scheduling priorities will reduce the probability of the system performance becoming severely degraded due to unintentional or malicious changes to process priority.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2328-3

1.8.17 Load and unload device drivers

Description:

This control defines whether a user account is allowed to dynamically load a new device driver on the system. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Drivers operate at a very high privilege level. Restricting which principals can load device drivers will help reduce a malicious user's ability to negatively impact the confidentiality, integrity, and availability of information on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-1455-5

1.8.18 Lock pages in memory

Description:
This control defines whether a process is allowed to keep data in physical memory. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No one`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will limit the potential for a application to consume large quantities of memory which may reduce system performance or result in a denial of services (DoS) attack by.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:

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

Default Value:
`No one`

References:
CCE-2332-5

1.8.19 Manage auditing and security log

Description:
This control defines whether a user is allowed to change auditing options for files and directories and clear the Security log. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Enforcing and restricting access to this control will limit the potential for a user to erase evidence of unauthorized activity.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-1843-2

1.8.20 Modify firmware environment values

Description:
This control defines whether a user is allowed to configure the system-wide environment variables that affect hardware configuration. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.

- For the Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will limit the potential for a hardware failure, data corruption or denial of service caused by unauthorized users.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2257-4

1.8.21 Perform volume maintenance tasks

Description:
This control defines whether a user is allowed to manage the system's volume or disk configuration. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will limit the potential for a volume to be deleted or corruption by unauthorized users.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

Administrators

References:
CCE-1383-9

1.8.22 Profile single process

Description:
This control defines whether a user is allowed to use tools to monitor the performance of non-system processes. For all profiles, the recommended state for this setting is Administrators.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users to gain additional information to perform an attack on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
Administrators

References:
CCE-2360-6

1.8.23 Profile system performance

Description:
This control defines whether a user is allowed to use tools to view the performance of system processes. For all profiles, the recommended state for this setting is Administrators.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users to gain additional information to perform an attack on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:

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

Default Value:
`Administrators`

References:
CCE-2113-9

1.8.24 Remove computer from docking station

Description:
This control defines whether a user is allowed to click Eject PC on the Start menu to unlock the computer. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users to remove a computer from its docking station without having to shut it down first.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User
Rights Assignment\Remove computer from docking station
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2382-0

1.8.25 Replace a process level token

Description:
This control defines whether a process is allowed to start another service or process with a different security access token. For all profiles, the recommended state for this setting is `LOCAL SERVICE, NETWORK SERVICE`.

Rationale:
This capability is not typically required by user accounts. Therefore, from a least privilege perspective, this right should not be granted to those principals.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`LOCAL SERVICE, NETWORK SERVICE`

References:
CCE-1527-1

1.8.26 Shut down the system

Description:
This control defines whether a user is allowed to use shut down the operating system when logged on locally on the computer. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Configuring the system as recommended will limit the potential for a unauthorized users to shut down the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators, Backup Operators`

References:
CCE-2078-4

1.8.27 Add workstations to domain

Description:
This control defines whether a user is allowed to add computer workstations to a specific domain. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Defined`.

Rationale:

Configuring the system as recommended will ensure that only authorized workstations are added to the domain.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

```
Not defined (Authenticated Users for domain controllers)
```

References:
CCE-2246-7

1.8.28Allow log on locally

Description:
This control defines whether a user is allowed to interactively log on to computers in another users environment. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users obtaining console access to the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

```
Administrators, Backup Operators, Performance Log Users
```

References:
CCE-2286-3

1.8.29Allow log on through Terminal Services

Description:

This control defines whether a user is allowed to log on as a Terminal Services client. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users obtaining remote access to the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators, Remote Desktop Users`

References:
CCE-2308-5

1.8.30 Change the time zone

Description:
This control defines whether a user is allowed to change the time zone of a computer. For all profiles, the recommended state for this setting is `LOCAL SERVICE, Administrators`.

Rationale:
Altering the time zone does not impact the system time but instead alters the zone the system time is represented in. On servers, none administrative users do not require the need to alter the time zone. Therefore, from a least privilege perspective this right should be reserved for server administrators.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`LOCAL SERVICE, Administrators, Users`

References:
CCE-2171-7

1.8.31 Create symbolic links

Description:
This control defines whether a user is allowed to create symbolic links on the system. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended will limit the potential for users to exploit security vulnerabilities in applications that are not designed to use symbolic links. Symbolic link attacks could be used to change permissions on files, corrupt data, destroy data, or perform denial of service (DoS) attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2305-1

1.8.32 Deny log on locally

Description:
This control defines which accounts are prevented from logging on locally to the computer. For all profiles, the recommended state for this setting is `Guests`.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users accessing the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Guests`

References:
CCE-2296-2

1.8.33 Deny log on through Terminal Services

Description:
This control defines whether a user is allowed to log on as Terminal Service client. For all profiles, the recommended state for this setting is `Guests`.

Rationale:
Enforcing and restricting access to this control will limit the potential for unauthorized users to download and run malicious software on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No One`

References:
CCE-2102-2

1.8.34 Generate security audits

Description:
This control defines whether a user is allowed to produce audit records in the Security log. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `LOCAL SERVICE, NETWORK SERVICE`.
- For the Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Accounts granted this right could use this capability to create a high volume of security events. This may result in increased difficulty identifying malicious activities in the event

log. Additionally, if the security event log is configured to overwrite entries as needed, this capability may be used to erase evidence of security related events.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Local Service, Network Service`

References:
CCE-2129-5

1.8.35 Increase a process working set

Description:
This control defines whether a user is allowed to increase or decrease the size of a process's working set - the set of memory pages currently visible on the process in the physical RAM memory. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators, Local Service`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
This right is granted to the Users group by default. However, it is possible for a user to increase their process working set to a level that could severely degrade system performance and potentially cause a denial of service on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase a process working set
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Users`

References:
CCE-2306-9

1.8.36 Log on as a batch job

Description:
This control defines whether an account is allowed to log on using the task scheduler service. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `No one`.
- For the Enterprise Member Server profile(s), the recommended value is `Not Defined`.

Rationale:
Granting a user rights introduces little risk. However, this use rights is not typically required by standard user accounts. On system's running IIS or ASP.NET, the IIS_WPG group and the `IUSR_<ComputerName>`, `ASPNET`, and `IWAM_<ComputerName>` accounts require this user right for IIS to function properly.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

```
Administrators, Backup Operators, Performance Log Users
```

References:
CCE-1975-2

1.8.37 Restore files and directories

Description:
This control defines whether a user is allowed to bypass file, directory, registry, and other persistent object permissions when restoring backed up data. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Administrators`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Administrators, Backup Operators`.

Rationale:

Account that possess this user right can gain access to sensitive data, corrupting and overwriting information as well as perform denial of service (DoS) attacks against the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators, Backup Operators`

References:
CCE-2294-7

1.8.38 Take ownership of files or other objects

Description:
This control defines whether a user is allowed to take ownership of files, folders, registry keys, processes, or threads. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Accounts with this user right can take ownership of any resource despite an access control list that would otherwise protect the resource. As such, the confidentiality, integrity, and availability of all data on a system that has this right insecurely configured is at risk

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrators`

References:
CCE-2506-4

1.8.39 Access credential Manager as a trusted caller

Description:
This control defines whether a user is allowed to access user credentials through the Credential Manager. For all profiles, the recommended state for this setting is `No One`.

Rationale:
The Credential Manager is the only entity that should have this right. A user possessing this right can obtain the credentials for other users.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`No One`

References:
CCE-2026-3

1.8.40 Synchronize directory service data

Description:
This control defines whether a process can read all objects and properties in the directory, regardless of the protection on the objects and properties. For all profiles, the recommended state for this setting is `No One`.

Rationale:
The Domain Controller account is the only accounts that require this capability. Due to the capabilities provided by this use right it should not be granted to any users.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Not defined`

References:
CCE-2137-8

1.9 Security Options

1.9.1 Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Description:
This control defines the minimum security requirements for establishing sessions with NTLM SSP servers. For all profiles, the recommended state for this setting is `Require NTLMv2 session security,Require 128-bit encryption`.

Rationale:
Configuring this setting as recommended will reduce the probability of an attacker being able to impact the confidentiality or integrity of session data.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0 /v
NTLMMinServerSec
```

Default Value:
`No minimum`

References:
CCE-2410-9

1.9.2 Network access: Remotely accessible registry paths and sub-paths

Description:
This control defines whether a registry path and sub-paths should be accessible when an application or process references the WinReg key to determine access permissions. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value 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
```

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Restricting the remote accessibility of registry paths reduces the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query
HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths
/v Machine
```

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:
CCE-2357-2

1.9.3 Accounts: Rename administrator account

Description:

This control recommends choosing a name for the built-in local administrator account that is different from the default. Often disabling the Administrator account is not practical. However, simply knowing the name of an account on a machine can be valuable information to an attacker. In an attempt to hide the account, best practices recommend renaming the account to something unique for your implementation.

If the account is renamed, anonymous Security Identifier (SID) / Name translation should also be disabled. This prevents an attacker from locating the renamed account by its SID. For all profiles, the recommended state for this setting is `any value that does not contain the term "admin"`.

Rationale:
Enforcing this recommendation make it more difficult for unauthorized users to guess and gain access to the administrator account and ultimately the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Administrator`

References:
CCE-2227-7

1.9.4 Accounts: Rename guest account

Description:
This control recommends choosing a name for the built-in local guess account that is different from the default. Similar to the Administrator account, the Guest account should be renamed even if it is disabled. The operating system places additional safeguards on the Guest account, and it is less of a target than the Administrator account, but it still deserves significant attention warrant changing the account name. For all profiles, the recommended state for this setting is `any value that does not contain the term "guest"`.

Rationale:
Enforcing this recommendation make it more difficult for unauthorized users to guess and gain access to the guest account and ultimately the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Guest`

References:
CCE-2372-1

1.9.5 Accounts: Guest account status

Description:
The Guest account can provide some regulation to unauthenticated users. Disabling this account will prevent unknown users being authenticated as Guests. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling the Guest account will reduce the system's remote unauthenticated attack surface and ensure that only specific security principals can access resources on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Disabled`

References:
CCE-2342-4

1.9.6 Network access: Allow anonymous SID/Name translation

Description:
This control defines whether an anonymous user is allowed to request security identifier (SID) for another user or use an SID to retrieve the corresponding user name. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Configuring the system as recommended will limit the potential for unauthorized users from initiating password guessing attacks to ultimately gain access to the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:
`Disabled`

References:
CCE-2318-4

1.9.7 Accounts: Limit local account use of blank passwords to console logon only

Description:
Windows divides computer logons into two main types: console or local logons and remote logons. In a console logon, the user physically logs on to the device with the attached keyboard. Remote logons are performed across the network using various protocols such as RPC, telnet, FTP and remote desktop.

When this setting is enabled, the computer refuses remote logons if the user attempts to use a blank password, even if the blank password is valid for that account. This setting should be enabled even though passwords should never be left blank.
For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Refuses remote authentication requests for account with blank passwords helps ensure that only authorized users can access the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v LimitBlankPasswordUse
```

Default Value:
`Enabled`

References:
CCE-2364-8

1.9.8 Devices: Allowed to format and eject removable media

Description:
This setting governs the type of users which have authority to remove NTFS formatted media from the computer. The available choices (listed from most to least restrictive) are Administrators, Administrators and Power Users, or Administrators and Interactive Users. For all profiles, the recommended state for this setting is `Administrators`.

Rationale:
Limiting the users that can remove NTFS media from the system reduces the probability of a malicious user mounting the removing a disk from the local computer to access it on another outside the context of the security restrictions such as DACLs.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
AllocateDASD
```

Default Value:
`Administrators`

References:
CCE-2377-0

1.9.9 Devices: Prevent users from installing printer drivers

Description:
Users typically need the ability to install and configure their own printers. However, printer driver installation loads code directly into the privileged space of the operating system kernel. The malicious user could choose to install a malicious print driver to gain control on the system.

If users must be given the right to install printer drivers, consider requiring that the driver be digitally signed before it can be installed.

Beware of the syntax for this option: Enabled means the users will not be able to install printer drivers and may prevent proper setup of printers; Disabled allows the user to fully manage their own printers.
For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Preventing users from installing printer drivers reduces the probability of a user impacting the stability and security of Windows.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers /v AddPrinterDrivers
```

Default Value:
`Enabled`

References:
CCE-2152-7

1.9.10 Devices: Restrict CD-ROM access to locally logged-on user only

Description:
With sufficient privileges, users can create network shares from any folder on a Windows computer. This extends to sharing a CD-ROM drive externally. This setting would restrict use of the shared CD-ROM drive to the local interactive logon. Since different CDs can be inserted, the user may forget or be unaware that the information on the CD becomes remotely accessible. Also, unlike typical file shares, access control lists cannot be placed on files and directories to control access and auditing. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Enabling this feature will limit the potential for unauthorized users to gain access to sensitive information on a mounted CD remotely.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Devices: Restrict CD-ROM access to locally logged-
on user only
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
AllocateCDRoms
```

Default Value:
`Disabled`

References:
CCE-1390-4

1.9.11 Devices: Restrict floppy access to locally logged-on user only

Description:
This control defines whether the floppy drive is accessible to remote users. Similar to a CD-ROM drive, the floppy drive can be shared to network users. Again, the user may not remember that the information on all inserted floppies becomes exposed.

Beware of the syntax for this option: Enabled means users will not be able to access shared floppy drives. Disabled allows access to shared floppy drives, but share-level access permissions still apply. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Enabling this setting will limit the potential for unauthorized users to gain access to sensitive information on a mounted floppy remotely.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Devices: Restrict floppy access to locally logged-
on user only
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
AllocateFloppies
```

Default Value:
`Disabled`

References:
CCE-2383-8

1.9.12 Domain member: Digitally encrypt or sign secure channel data (always)

Description:
This control defines whether a signature or encryption is required for all secure channel traffic initiated by domain members. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing and encrypting secure channel data will reduce the probability of a successful man in the middle attack while protecting the confidentiality of data traversing the channel.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
requiresignorseal
```

Default Value:
`Enabled`

References:
CCE-2203-8

1.9.13 Domain member: Digitally encrypt secure channel data (when possible)

Description:

This control defines whether a system will try to negotiate encryption for all secure channel traffic initiated by domain members. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally encrypting secure channel data will protect the confidentiality of data traversing the channel.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
sealsecurechannel
```

Default Value:
`Enabled`

References:
CCE-1868-9

1.9.14 Domain member: Digitally sign secure channel data (when possible)

Description:
This control defines whether a system will try to negotiate digital signatures for all secure channel traffic initiated by domain members. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing secure channel data will reduce the probability of a successful man in the middle attack.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
signsecurechannel
```

Default Value:
`Enabled`

References:
CCE-2362-2

1.9.15 Domain member: Disable machine account password changes

Description:
This control defines whether a domain member can periodically change its computer account password. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
By disabling this policy setting on all domain controllers, domain members will be able to periodically change their computer account passwords, which in-turn reduces their susceptibility to attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
disablepasswordchange
```

Default Value:
`Disabled`

References:
CCE-2256-6

1.9.16 Domain member: Maximum machine account password age

Description:
This control defines how many days domain member can use the same password before it expires. For all profiles, the recommended state for this setting is `30 day(s)`.

Rationale:
Enforcing a reasonably short password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
maximumpasswordage
```

Default Value:
`30 days`

References:
CCE-2278-0

1.9.17Domain member: Require strong (Windows 2000 or later) session key

Description:
This control defines whether secure channel communication requires a strong (128-bit) session key. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Utilizing a strong session key will reduce the probability of a success man in the middle attack.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
requirestrongkey
```

Default Value:
`Disabled`

References:
CCE-1802-8

1.9.18 Domain controller: Allow server operators to schedule tasks

Description:
This control defines whether members of the Server Operator group are allowed to use the AT schedule facility to submit jobs. When enabled, server operators can add tasks using the AT command. By default, AT runs under the local system account, which has administrative rights on the machine. When this setting is disabled, server operators can still schedule tasks with the task scheduler; however, these tasks will run under their domain credentials and not under the local system account.

This setting has no effect on computers other than Domain Controllers.
It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `Disabled`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Defined`.

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.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v SubmitControl
```

References:
CCE-2049-5

1.9.19 Domain controller: LDAP server signing requirements

Description:
This control defines whether Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. This option can be set to Require Signature or None (signing is not required unless the client requests it).

This setting has no effect on computers other than Domain Controllers. It is recommended that this setting be configured as described below:

- For the SSLF Domain Controller profile(s), the recommended value is `Require signing`.
- For the Enterprise Member Server, Enterprise Domain Controller and SSLF Member Server profile(s), the recommended value is `Not Defined`.

Rationale:
Data signing protect against man-in-the-middle attacks against data integrity. However, requiring all LDAP clients to sign requests may prevent clients from accessing domain resources.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\NTDS\Parameters /v
ldapserverintegrity
```

References:
CCE-2317-6

1.9.20 Domain controller: Refuse machine account password changes

Description:
This control defines whether domain controllers will refuse requests from member computers to change computer account passwords. It is recommended that this setting be configured as described below:

- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `Disabled`.
- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Not Defined`.

Rationale:
By disabling this policy setting on all domain controllers, domain members will be able to periodically change their computer account passwords, which in-turn reduces their susceptibility to attacks.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v
RefusePasswordChange
```

References:
CCE-1934-9

1.9.21 Interactive logon: Do not display last user name

Description:
Anyone attempting to log into a computer may see the name of the last valid user who logged on to that system. This does not prevent displaying the currently logged on user when unlocking a workstation. This information may seem trivial, but it helps an attacker tie a workstation to a particular individual, or may help an attacker gain access to a stolen mobile device.

Educate users before enabling this setting in a domain environment. Some users may not know their logon, particularly when it differs from the e-mail address or other accounts.

Beware of the syntax for this option: Enabled means the user must type in their user id on every logon; Disabled means the last logged on user appears in the login dialog. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enforcing and restricting this control will limit the potential for unauthorized users to collect account names and gain additional information to perform an attack on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
DontDisplayLastUserName
```

Default Value:
`Disabled`

References:
CCE-2199-8

1.9.22 Interactive logon: Do not require CTRL+ALT+DEL

Description:
This control defines whether a user must press `CTRL+ALT+DEL` before they log on. The Windows operating system treats the `CTRL+ALT+Delete` key sequence different from any other. Operating system design prevents any application from intercepting and responding when these keys are pressed. When you type `CTRL+ALT+Delete`, you are guaranteed that the operating system authentication process will handle the request.

When the console does not require `CTRL+ALT+Delete` to log on, users will not see the dialog "Press CTRL+ALT+Delete to Log On." Rather, the workstation simply presents the standard logon dialog.

Beware of the syntax for this option: Disabled means the user must press `CTRL+ALT+Delete` before every non-smartcard logon; Enabled will present the logon dialog without requiring `CTRL+ALT+Delete`. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
With the CTRL+ALT+Delete requirement lifted, the user could actually be typing their password into a trojaned application, rather than the operating system authentication process. Remember, the trojaned application would not be able to respond had the user pressed CTRL+ALT+Delete.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
DisableCAD
```

Default Value:
`Disabled`

References:
CCE-2331-7

1.9.23 Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Description:
This control defines whether a user can log on to a Windows domain using cached account information. When a workstation belongs to a domain, users can log on to it using domain credentials. The domain credentials can be cached in the local workstation's Security Accounts Manager (SAM) database. On next logon, should no domain controller be available, the user can still log on locally by authenticating against the cached account information.

When logging on using cached credentials, some account properties will not be enforced, since the domain controller maintains responsibility for enforcing account policy. The local SAM database does not "own" the account, so cached account passwords do not expire, and domain accounts cannot be locked out when the domain is unavailable.
When establishing corporate policy for cached accounts, consider the remote user. They commonly log on with cached credentials from a laptop. To access corporate resources, the user establishes a Virtual Private Network (VPN) connection to the corporate network. Since logon occurs before the domain is available—the VPN has not yet been established—the user will never be prompted to change the password on the cached account.

This setting only affects workstations joined to a domain, and only impacts interactive logons with domain accounts. The workstation will not cache non-interactive log on information. Change this setting to zero to disable the caching of domain accounts in the local SAM database.
For all profiles, the recommended state for this setting is `0 logons`.

Rationale:
Setting the number of cached logon to the appropriate level for the system's profile will remove an avenue for an attacker to further compromise the environment by deriving credentials from the cache while allows logons should the domain become unavailable.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
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)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
cachedlogonscount
```

Default Value:
`25 logons`

References:
CCE-2297-0

1.9.24 Interactive logon: Prompt user to change password before expiration

Description:
This control defines how many days in advance a user is notified before their password must be changed. Should a user's password be near its expiration date, the logon process warns the user and asks if they would like to change the password. Once the password has expired, the user will be required to change the password to complete the logon. This setting governs the window of convenience between the time when the system offers the user to change the password, and the time when they are required to change the password. For all profiles, the recommended state for this setting is `14 days`.

Rationale:
Enforcing this control is important in to notify users in advance of the expiry of their password to avoid inadvertently locking them out from the computer when their password expires.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
passwordexpirywarning
```

Default Value:

14 days

References:
CCE-2324-2

1.9.25 Interactive logon: Require Domain Controller authentication to unlock workstation

Description:
This control defines whether a user is requires Domain Controller authentication to unlock a computer. This setting results from a feature in Windows domain authentication; a further understanding of the behavior will help you determine the setting applicable to your organization. This setting does not affect standalone workstations. The typical sequence for failure to unlock a workstation flows like this:

1. The user repeatedly types in the wrong password.

2. For each password attempted, the workstation first compares the password to the cached password hash used for the original logon. If they do not match, it contacts the domain controller and attempts to log on.

3. After a predefined number of attempts, the domain controller locks out the account, and the workstation reports the account lockout.
At this point, most users will contact the system administrator and have the account lockout and perhaps the password reset. However, consider the persistent user that continues attempting to logon:

4. The user continues attempting to logon. Each time a bad password is entered, the workstation still compares it to the local cache; when the comparison fails, it contacts the domain controller, which also denies the logon.

5. Finally, the user enters the correct password. The workstation comparison to the local cache succeeds.

If this setting is disabled, the user then successfully unlocks the workstation. Even with a locked account, the user can then continue to access network resources for connections which were established and authenticated before the machine was locked—mail servers and file servers in particular.

Enabling this setting, however, adds an additional step after every successful workstation comparison with the local cache:

6. The workstation presents the credentials to the domain controller. Only if the domain controller authentication succeeds will the workstation be unlocked.
Enable this setting to protect against brute force password attacks through the screen saver. However, enabling it will hinder the user who locks and hibernates their workstation, and then attempts to resume when the domain controller is unavailable.
Disabling this setting (or leaving it undefined) minimizes domain controller traffic.

For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enforcing this control will limit the potential for unauthorized users with account that have been disabled from being able to unlock a computer on the network.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Require Domain Controller
authentication to unlock workstation
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
ForceUnlockLogon
```

Default Value:
`Disabled`

References:
CCE-2346-5

1.9.26 Interactive logon: Smart card removal behavior

Description:
This control defines what happens when the smart card for a logged on user is removed from the smart card reader. For all profiles, the recommended state for this setting is `Lock Workstation`.

Rationale:
Enforcing this control will limit the potential for unauthorized users from gaining access to perform an attack on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
scremoveoption
```

Default Value:
`No Action`

References:
CCE-1448-0

1.9.27 Interactive logon: Message text for users attempting to log on

Description:
This control defines a text message that displays to users when they log on. For all profiles, the recommended state for this setting is `the text blessed by your organization`.

Rationale:
Enforcing this control may be important in limiting the potential for unauthorized users attempting to gain access to perform an attack on the system by notifying them of the consequences of their misconduct.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
LegalNoticeText
```

References:
CCE-2225-1

1.9.28 Interactive logon: Message title for users attempting to log on

Description:
This control defines the text that appears in the title bar of the windows the user sees when they log on to the system. For all profiles, the recommended state for this setting is `the text blessed by your organization`.

Rationale:
Enforcing this control may be important in limiting the potential for unauthorized users attempting to gain access to perform an attack on the system by notifying them of the consequences of their misconduct.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
LegalNoticeCaption
```

References:
CCE-2037-0

1.9.29 Interactive logon: Require smart card

Description:
This control defines whether a user is required to log on to a computer with a smart card. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Enforcing this control to require a smart card for log on will limit the potential for unauthorized users gaining access to computers containing sensitive data.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Require smart card
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
scforceoption
```

Default Value:
`Disabled`

References:
CCE-2223-6

1.9.30 Microsoft network client: Digitally sign communications (always)

Description:
This control defines whether packet signing is required by the SMB client component. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing SMB communication will reduce the probability of a success man in the middle attack between the SMB client and server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
/v RequireSecuritySignature
```

Default Value:
`Disabled`

References:
CCE-2356-4

1.9.31 Microsoft network client: Digitally sign communications (if server agrees)

Description:
This control defines whether the SMB client will attempt to negotiate SMB packet signing. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing SMB communication will reduce the probability of a success man in the middle attack between the SMB client and server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
/v EnableSecuritySignature
```

Default Value:
`Enabled`

References:
CCE-2378-8

1.9.32 Microsoft network client: Send unencrypted password to third-party SMB servers

Description:
This control defines whether a server can transmit passwords in plaintext across the network to other computers that offer SMB services. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Configuring the system as recommended will prevent Windows for sending unencrypted credentials to SMB servers that lack support for SMB security mechanisms.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
/v EnablePlainTextPassword
```

Default Value:
`Disabled`

References:
CCE-2272-3

1.9.33 Microsoft network server: Amount of idle time required before suspending session

Description:
This control defines the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. For all profiles, the recommended state for this setting is `15 minute(s)`.

Rationale:
Enforcing this control will limit the potential for unauthorized users from repeatedly establishing SMB sessions until the server becomes slow or unresponsive.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
autodisconnect
```

Default Value:
`15 minutes`

References:
CCE-2236-8

1.9.34 Microsoft network server: Digitally sign communications (always)

Description:
This control determines if the server side SMB service is required to perform SMB packet signing. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing SMB communication will reduce the probability of a success man in the middle attack between the SMB client and server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
requiresecuritysignature
```

Default Value:
`Disabled`

References:
CCE-2381-2

1.9.35 Microsoft network server: Digitally sign communications (if client agrees)

Description:
This control defines whether a server side SMB service will sign SMB packets for a client connection. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Digitally signing SMB communication will reduce the probability of a success man in the middle attack between the SMB client and server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
enablesecuritysignature
```

Default Value:
`Disabled`

References:
CCE-2263-2

1.9.36 Microsoft network server: Disconnect clients when logon hours expire

Description:
This control defines whether to disconnect a session when the user's valid logon hours expire. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Unless this setting is enabled, the benefits of imposing logon hours will not be realized.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
enableforcedlogoff
```

Default Value:
`Enabled`

References:
CCE-2029-7

1.9.37 Network access: Do not allow anonymous enumeration of SAM accounts

Description:
This control defines whether an anonymous user is allowed to enumerate the accounts in the Security Accounts Manager (SAM). For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Preventing anonymous enumeration of SAM accounts removes a remote attackers ability to easily determine the list of users on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v RestrictAnonymousSAM
```

Default Value:
`Enabled`

References:
CCE-1962-0

1.9.38 Network access: Do not allow anonymous enumeration of SAM accounts and shares

Description:
This control defines whether an anonymous user is allowed to enumerate the accounts and shares in the Security Accounts Manager (SAM). For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Preventing anonymous enumeration of SAM accounts removes a remote attackers ability to easily determine the list of users on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v RestrictAnonymous
```

Default Value:
`Disabled`

References:
CCE-2340-8

1.9.39 Network access: Do not allow storage of credentials or .NET Passports for network authentication

Description:
This control defines whether the Stored User Names and Passwords feature may save password credentials for later use when domain authentication is achieved. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
The confidentiality of stored credentials, and therefore the systems those credentials access, is at risk if the system is compromised or the hard disk is insecurely discarded.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow storage of credentials
or .NET Passports for network authentication
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v DisableDomainCreds
```

Default Value:
`Disabled`

References:
CCE-2111-3

1.9.40 Network access: Let Everyone permissions apply to anonymous users

Description:
This control defines what additional permissions are assigned for anonymous connections to the computer. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling this setting is important as unauthorized users 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.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v
EveryoneIncludesAnonymous
```

Default Value:
`Disabled`

References:

CCE-1824-2

1.9.41 Network access: Named Pipes that can be accessed anonymously

Description:
This control defines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. It is recommended that this setting be configured as described below:

- For the SSLF Member Server profile(s), the recommended value is `browser`.
- For the SSLF Domain Controller profile(s), the recommended value is:

```
netlogon
lsarpc
samr
browser
```

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Configuring the system as recommended reduces to the system remote attack surface.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Named Pipes that can be accessed
anonymously
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
NullSessionPipes
```

Default Value:
`browser`

References:
CCE-2089-1

1.9.42 Network access: Remotely accessible registry paths

Description:
This control defines which registry paths can be accessed remotely. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is:

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

Rationale:
Restricting the remote accessibility of registry paths reduces the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query
HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPa
ths /v Machine
```

Default Value:

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

References:
CCE-1521-4

1.9.43 Network access: Restrict anonymous access to Named Pipes and Shares

Description:
This control defines restricts anonymous access to only those shares and pipes that are named in the Network access. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Restricting anonymous access to named pipes and shares will ensure that only explicitly security principals have access to these resources.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
restrictnullsessaccess
```

Default Value:
`The registry key does not exist.`

References:
CCE-2361-4

1.9.44 Network access: Shares that can be accessed anonymously

Description:
This control defines which network shares can be accessed by anonymous users. For all profiles, the recommended state for this setting is `None`.

Rationale:
Preventing anonymous access to shares will ensure that only explicitly security principals have access to shared resources.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Shares that can be accessed
anonymously
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LanManServer\Parameters /v
NullSessionShares
```

Default Value:
`None`

References:
CCE-2507-2

1.9.45 Network access: Sharing and security model for local accounts

Description:
This control defines how network logons that use local accounts are authenticated. For all profiles, the recommended state for this setting is `Classic - local users authenticate as themselves`.

Rationale:
The recommended configuration allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v ForceGuest
```

Default Value:
`Classic - local users authenticate as themselves`

References:
CCE-2406-7

1.9.46 Network security: Do not store LAN Manager hash value on next password change

Description:
This control defines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enabling this setting will increase the difficulty for an attacker to successfully derive credentials by attacking the SAM file.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v NoLMHash
```

Default Value:
`Enabled`

References:
CCE-2304-4

1.9.47 Network security: LAN Manager authentication level

Description:
This control defines LAN Manager authentication level. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Send NTLMv2 response only. Refuse LM`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Send NTLMv2 response only. Refuse LM & NTLM`.

Rationale:
Configuring this setting as recommended will reduce the probability of an attacker being able to derive credentials from authentication responses.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa /v LmCompatibilityLevel
```

Default Value:
`Send NTLMv2 response only`

References:
CCE-2454-7

1.9.48 Network security: LDAP client signing requirements

Description:
This control defines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. For all profiles, the recommended state for this setting is `Negotiate signing`.

Rationale:
Signing client LDAP requests will help ensure the integrity of the query is preserved. In the absence of a signed query, an active network attacker could alter the LDAP query en route to the server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\LDAP /v LDAPClientIntegrity
```

Default Value:
`Negotiate signing`

References:
CCE-2327-5

1.9.49 Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

Description:
This control allows a client computer to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. For all profiles, the recommended state for this setting is `Require NTLMv2 session security,Require 128-bit encryption`.

Rationale:
Enabling all of the options for this policy setting helps to 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.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0 /v
NTLMMinClientSec
```

Default Value:
`No minimum`

References:
CCE-1767-3

1.9.50 Recovery console: Allow automatic administrative logon

Description:
This control defines whether the administrator account is automatically logged on to the recovery console. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
If automatic administrative logon is enabled, a malicious user could walk disconnect the server's power to shut it down, restart it, select Recover Console from the Restart menu, and take full control of the server.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole /v securitylevel
```

Default Value:
`Disabled`

References:
CCE-2309-3

1.9.51 Recovery console: Allow floppy copy and access to all drives and all folders

Description:
This control defines whether the Recovery Console SET command is available. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Disabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Disabling this setting will prevent an attacker who can cause the system to restart into the Recovery Console from stealing sensitive data with no audit or access trail.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole /v setcommand
```

Default Value:
`Disabled`

References:
CCE-1553-7

1.9.52 Shutdown: Clear virtual memory pagefile

Description:
This control defines whether the virtual memory pagefile is cleared when the system is shut down. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Clearing the virtual memory pagefile upon shutdown will cause significant delays in rebooting the system. These delays are considered a higher risk to service availability than the perceived confidentiality benefit of clearing the contents of the pagefile.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Session Manager\Memory
Management /v ClearPageFileAtShutdown
```

Default Value:
`Disabled`

References:
CCE-2416-6

1.9.53 Shutdown: Allow system to be shut down without having to log on

Description:
This control defines whether a computer can be shut down when a user is not logged on. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling this setting is important for high security client systems and for servers as a malicious person may shut down the system in an unauthorized manner.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
ShutdownWithoutLogon
```

Default Value:
`Disabled`

References:
CCE-2403-4

1.9.54 System objects: Require case insensitivity for non-Windows subsystems

Description:
This control defines whether case insensitivity is enforced for all subsystems. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Windows interacts with file system in a case insensitive manner. However, the POSIX subsystem supports case-sensitive filenames. In environments that leverage case-sensitive file systems, enabling this setting with ensure the similarly named files with mixed case are distinguishable via Windows tools.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Session Manager\Kernel /v
ObCaseInsensitive
```

Default Value:
`Not Configured`

References:
CCE-2429-9

1.9.55 System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

Description:
This control defines the strength of the default discretionary access control list (DACL) to help secure shared objects on the system. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
With this setting enabled, non-administrative users will not be able to modify shared objects that they did not create.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Session Manager /v
ProtectionMode
```

Default Value:
`Enabled`

References:
CCE-2451-3

1.9.56 System cryptography: Force strong key protection for user keys stored on the computer

Description:
This control defines whether a user's private key requires a password to be used. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `User must enter a password each time they use a key`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `User is prompted when the key is first used`.

Rationale:
Requiring a password to decrypt stored keys will reduce the probability of an attacker gaining access to those keys even if the attacker takes control of the user's computer.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\System cryptography: Force strong key protection
for user keys stored on the computer
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Cryptography /v ForceKeyProtection
```

Default Value:
`Not Configured`

References:
CCE-2319-2

1.9.57 System settings: Optional subsystems

Description:
This control defines which subsystems are used to support applications in your environment. For all profiles, the recommended state for this setting is `None`.

Rationale:
Configuring this setting to null will prevent possible vulnerabilities of POSIX subsystem.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\System settings: Optional subsystems
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems /v
optional
```

Default Value:
`Posix`

References:
CCE-1598-2

1.9.58 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

Description:
This control defines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:

Enabling this setting configures restriction policies help to protect users and computers because they can prevent the execution of unauthorized code, such as viruses and Trojans horses.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\System settings: Use Certificate Rules on Windows
Executables for Software Restriction Policies
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers /v
AuthenticodeEnabled
```

Default Value:
`Disabled`

References:
CCE-2421-6

1.9.59 MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)

Description:
This control defines whether a user with physical access to a computer is able to automatically log on. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Enforcing this control will limit the potential for unauthorized users with physical access to a computer from gaining access to the computer and any network that the computer is connected to.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
AutoAdminLogon
```

Default Value:
`The registry key does not exist.`

References:
CCE-2307-7

1.9.60 MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

Description:
This control determines if Windows will accept source routed packets. Source Routing allows the packet sender to dictate the route the packet will take to its destination. For all profiles, 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. If multiple routes are available for a given destination, an attacker may leverage source routing to choose the route that contains fewer security safeguards, such as intrusion detection systems or firewalls.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v
DisableIPSourceRouting
```

Default Value:
`The registry key does not exist.`

References:
CCE-1826-7

1.9.61 MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

Description:

This control defines whether the Internet Control Message Protocol (ICMP) redirects to override Open Shortest Path First (OSPF) generated routes. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (EnableICMPRedirect) Allow ICMP redirects to
override OSPF generated routes
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v
EnableICMPRedirect
```

Default Value:
`Enabled`

References:
CCE-1470-4

1.9.62 MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds

Description:
This control defines every how many milliseconds TCP attempts to send a keep-alive packet to verify that an idle connection is still intact. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `5 minutes` .
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Reducing the keep alive timeout will limit the potential for malicious users to establish multiple connections to cause a denial of service (DoS) attack on the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (KeepAliveTime) How often keep-alive packets
are sent in milliseconds
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v
KeepAliveTime
```

Default Value:
`The registry key does not exist.`

References:
CCE-2399-4

1.9.63 MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic

Description:
This control defines whether IPsec exemptions could be configured for various type of network traffic such as Internet Key Exchange (IKE) and Kerberos authentication protocol. For all profiles, the recommended state for this setting is `Only ISAKMP is excempt (recommended for Windows Server 2003).`

Rationale:
With the default exceptions in place, an attacker can bypass filtering rules by sending packets with a source port of 88/UDP.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (NoDefaultExempt) Configure IPSec exemptions
for various types of network traffic
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query    /v NoDefaultExempt
```

Default Value:
`The registry key does not exist.`

References:
CCE-2404-2

1.9.64 MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

Description:
This control defines whether a computer disregards NetBIOS name release requests except those from WINS server in the SCE. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
NetBT is an unauthenticated protocol that operates over the connectionless protocol UDP. Given these characteristics, a malicious user could send a name conflict request to a target computer, which would cause the target computer to relinquish its name. This would result in the target computer being unable to participate with peers over NetBT.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (NoNameReleaseOnDemand) Allow the computer to
ignore NetBIOS name release requests except from WINS servers
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Netbt\Parameters /v
NoNameReleaseOnDemand
```

Default Value:
`Enabled`

References:
CCE-2320-0

1.9.65 MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)

Description:
This control defines whether a computer can stop generating 8.3 style file names. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
If a directory enumeration vulnerability exists in an application, an attacker's odds at successfully guessing unknown filenames is increased by using 8.3 file names. For example, the file "SecretFileWithLongName.doc" can be accessed with the filename "SECRET~1.doc".

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (NtfsDisable8dot3NameCreation) Enable the
computer to stop generating 8.3 style filenames (recommended)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Control\FileSystem /v
NtfsDisable8dot3NameCreation
```

Default Value:
`Disabled`

References:
CCE-2156-8

1.9.66 MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)

Description:
This control defines whether Internet Router Discovery Protocol (IRDP) is used to automatically detect and configure default gateway addresses. For all profiles, the recommended state for this setting is `Disabled`.

Rationale:
Disabling router discovery will limit the potential for malicious network to successfully man-in-the-middle the system's network traffic by impersonating a router.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (PerformRouterDiscovery) Allow IRDP to detect
and configure Default Gateway addresses (could lead to DoS)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v
PerformRouterDiscovery
```

Default Value:

```
Enable only if DHCP sends the Perform Router Discovery option
```

References:

CCE-1800-2

1.9.67 MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)

Description:
This control defines whether an application is forced to begin its DLL search in the system path before searching the current working folder. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enabling this option will help ensure that trusted system DLLs are loaded by an application when it searches for DLLs.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SYSTEM\CurrentControlSet\Control\Session Manager /v
SafeDllSearchMode
```

Default Value:
`The registry key does not exist.`

References:
CCE-2447-1

1.9.68 MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)

Description:
This control defines how many seconds between when the screen saver is launched and when the computer console is actually locked. For all profiles, the recommended state for this setting is `0`.

Rationale:
The grace period may leave the computer vulnerable to a potential attack from someone who could approach the console and attempt to interact with the computer before the lock takes effect.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
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)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v
ScreenSaverGracePeriod
```

Default Value:
5 seconds

References:
CCE-2183-2

1.9.69 MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)

Description:
This control defines the number of times that TCP retransmits an individual data segment before the connection is aborted. For all profiles, the recommended state for this setting is 3.

Rationale:
This will limit the potential for malicious hosts to exhaust a target computer's resources by never sending any acknowledgement messages for data that was transmitted by the target computer.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (TCPMaxDataRetransmissions) How many times
unacknowledged data is retransmitted (3 recommended, 5 is default)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v
TcpMaxDataRetransmissions
```

Default Value:
5

References:
CCE-2424-0

1.9.70 MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning

Description:
This control defines whether an entry is added to the Security event log when the log reaches a user-defined threshold. For all profiles, 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, new events will not be written to the log.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
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
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security /v
WarningLevel
```

Default Value:
`The registry key does not exist.`

References:
CCE-2442-2

1.9.71 MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)

Description:
This control determines if Windows will accept source routed packets. Source Routing allows the packet sender to dictate the route the packet will take to its destination. For all profiles, 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. If multiple routes are available for a given destination, an attacker may leverage source routing to choose the route that contains fewer security safeguards, such as intrusion detection systems or firewalls.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

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

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters /v
DisableIPSourceRouting
```

References:
CCE-5229-0

1.9.72 MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default)

Description:
This control defines the number of times that TCP retransmits an individual data segment before the connection is aborted. For all profiles, the recommended state for this setting is `3`.

Rationale:
This will limit the potential for malicious hosts to exhaust a target computer's resources by never sending any acknowledgement messages for data that was transmitted by the target computer.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options\MSS: (TCPMaxDataRetransmissions) IPv6 How many
times unacknowledged data is retransmitted (3 recommended, 5 is default)
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters /v
TcpMaxDataRetransmissions
```

Default Value:
`5`

References:
CCE-5263-9

1.10 Terminal Services

1.10.1 Always prompt client for password upon connection

Description:
This control defines whether Terminal Services or Remote Desktop will prompt for a password even if it was already provided in the Remote Desktop Connection client For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer to connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Remote
Desktop Services\Remote Desktop Session Host\Security\Always prompt client
for password upon connection
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services /v
fPromptForPassword
```

Default Value:
`Not Configured`

References:
CCE-7636-4

1.10.2 Set client connection encryption level

Description:
This control defines whether the computer that hosts a remote connection will enforce an encryption level for the connection. For all profiles, the recommended state for this setting is `Enabled:High level`.

Rationale:

Requiring 128-bit encryption for Terminal Services and Remote Desktop communication will help ensure the confidentiality and integrity of data sent and received.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Remote
Desktop Services\Remote Desktop Session Host\Security\Set client connection
encryption level
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services /v
MinEncryptionLevel
```

Default Value:
`Not Configured`

References:
CCE-7667-9

1.10.3 Do not allow drive redirection

Description:
This control defines whether a user is allowed to share the local drives on their client computers to Terminal Servers that they access It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.

Rationale:
Redirecting a local drive to a remote Terminal Services session may expose local drive contents to threats against its confidentiality, integrity, and availability.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Remote
Desktop Services\Remote Desktop Session Host\Device and Resource
Redirection\Do not allow drive redirection
```

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services /v
fDisableCdm
```

Default Value:
`Not Configured`

1.10.4 Do not allow passwords to be saved

Description:
This control defines whether the Terminal Services client will save passwords. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
If the user account that has saved passwords is compromised, an attacker can leverage saved passwords to access other servers.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Remote
Desktop Services\Remote Desktop Connection Client\Do not allow passwords to
be saved
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services /v
DisablePasswordSaving
```

Default Value:
`Not Configured`

1.11 Internet Communication

1.11.1 Turn off downloading of print drivers over HTTP

Description:
This control defines whether the computer can download print driver packages over HTTP. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Preventing users from downloading print drivers over HTTP may reduce the probability of introducing drivers that impact the system's stability and security.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off downloading of print
drivers over HTTP
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows NT\Printers /v
DisableWebPnPDownload
```

1.11.2 Turn off the "Publish to Web" task for files and folders

Description:
This control defines whether to make the tasks for publishing files, folders and selected items to web available from File and Folder Tasks in Window folders. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Disabling Publish to Web capabilities will reduce the probability of a user publishing confidential or sensitive information to a public service.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off the "Publish to Web" task
for files and folders
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
NoPublishingWizard
```

1.11.3 Turn off Internet download for Web publishing and online ordering wizards

Description:
This control defines whether Windows will download a list of providers for the Web publishing and online ordering wizards. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Enabling this control will reduce the possibility of a user unknowingly downloading malicious content.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoWebServices
```

1.11.4 Turn off printing over HTTP

Description:
This control defines whether a client computer is allowed to print over HTTP. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
HTTP is a clear text protocol that provides not confidentiality or integrity guarantees. Given this, the confidentiality and integrity of print data is at risk when printing over HTTP.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows NT\Printers /v DisableHTTPPrinting
```

1.11.5 Turn off Search Companion content file updates

Description:

This control defines whether Search Companion should automatically download content updates during local and Internet searches. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
This control reduces the probability of a user unknowingly revealing sensitive information via the topics they are searching for.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off Search Companion content
file updates
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\SearchCompanion /v
DisableContentFileUpdates
```

1.11.6 Turn off the Windows Messenger Customer Experience Improvement Program

Description:
This control defines whether Windows Messenger will collect and send anonymous information on Windows Messenger usage. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
This feature provides no functional capability to the system. Therefore, it is recommended that this capability be disabled to eliminate any risk of information disclosure.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off the Windows Messenger
Customer Experience Improvement Program
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Messenger\Client /v CEIP
```

1.11.7 Turn off Windows Update device driver searching

Description:
This control defines whether Windows will search Windows Update for device drivers when no local drivers for a device are present. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Enabling this setting prevents users from downloading and installing device drivers that reduces system stability and security.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off Windows Update device
driver searching
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\DriverSearching /v
DontSearchWindowsUpdate
```

1.12 Additional Security Settings

1.12.1 Do not process the legacy run list

Description:
This control defines whether the legacy run list will be ignored. The run list is the list of programs that Windows runs automatically when it starts. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.

Rationale:
The capabilities provided by this list may be leveraged by a malicious user or software to cause Windows to execute arbitrary code upon reboot.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Logon\Do not process
the legacy run list
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
DisableLocalMachineRun
```

Default Value:
`Not Configured`

1.12.2 Do not process the run once list

Description:
This control defines whether the run once list will be ignored. The run once list is the list of programs that Windows runs automatically the next time it starts. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.

Rationale:
The capabilities provided by this list may be leveraged by a malicious user or software to cause Windows to execute arbitrary code upon reboot.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Logon\Do not process
the run once list
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
DisableLocalMachineRunOnce
```

Default Value:

Not Configured

1.12.3 Registry policy processing

Description:
This control defines when and how registry policies are updated. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is `Enabled (Process even if the Group Policy objects have not changed)`.
- For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Updating and reapplying all policies to the system will ensure that any changes to policy made by the local user have are reset as defined in Group Policy.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Group Policy\Registry policy processing
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2} /v NoGPOListChanges,NoBackgroundPolicy
```

Default Value:
Not Configured

References:
CCE-8492-1

1.12.4 Offer Remote Assistance

Description:
This control defines whether Windows will allow unsolicited offers to provide remote assistance to the local user. Remote assistance provides the remote party with the ability to view or control the local system. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Disabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Allowing a remote system to view or control the local system effectively extends the local system's trust boundary to include the remote system. As such, the security status of the remote system may impact the security status of the local system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\Offer Remote Assistance
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\policies\Microsoft\Windows NT\Terminal Services /v
fAllowUnsolicited
```

Default Value:
`Not Configured`

References:
CCE-7643-0

1.12.5 Solicited Remote Assistance

Description:
This control defines whether Windows will allow the local user to request a remote party to view or control their system. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Disabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Allowing a remote system to view or control the local system effectively extends the local system's trust boundary to include the remote system. As such, the security status of the remote system may impact the security status of the local system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\Solicited Remote Assistance
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\policies\Microsoft\Windows NT\Terminal Services /v
fAllowToGetHelp
```

Default Value:
`Not Configured`

1.12.6 Restrictions for Unauthenticated RPC clients

Description:
This control defines the RPC Runtime on an RPC server to restrict unauthenticated RPC clients from connecting to the RPC server. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled:Authenticated`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Requiring the RPC client to authenticate prior to communicating with an RPC server will reduce the remote unauthenticated attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Remote Procedure
Call\Restrictions for Unauthenticated RPC clients
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows NT\Rpc /v
RestrictRemoteClients
```

Default Value:
`Not Configured`

References:
CCE-7658-8

1.12.7 RPC Endpoint Mapper Client Authentication

Description:

This control defines whether an RPC client is required to authenticate prior to communicating with the Endpoint Mapper Service. It is recommended that this setting be configured as described below:

- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Enabled`.
- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Defined`.

Rationale:
Requiring the RPC client to authenticate prior to communicating with the Endpoint Mapper Service will reduce the remote unauthenticated attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\System\Remote Procedure
Call\RPC Endpoint Mapper Client Authentication
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Windows NT\Rpc /v
EnableAuthEpResolution
```

Default Value:
`Not Configured`

References:
CCE-8572-0

1.12.8 Turn off Autoplay

Description:
This control defines whether autoplay is allowed. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. For all profiles, the recommended state for this setting is `Enabled:All drives`.

Rationale:
Configuring the system as recommended will reduce the probability of a user unintentionally executing potentially malicious software when inserting removable media.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\AutoPlay
Policies\Turn off Autoplay
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v
NoDriveTypeAutoRun
```

Default Value:
`Not Configured`

References:
CCE-8634-8

1.12.9 Enumerate administrator accounts on elevation

Description:
This control defines whether a user is allowed to see all administrator accounts displayed when a user attempts to elevate a running application. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `Not Configured`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Disabled`.

Rationale:
Displaying a list of administrator accounts on the system may inadvertently disclose the names of power accounts.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Credential
User Interface\Enumerate administrator accounts on elevation
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\CredUI /v
EnumerateAdministrators
```

Default Value:
`Not Configured`

References:
CCE-8568-8

1.12.10 Require trusted path for credential entry

Description:
When this setting is enabled, instead of displaying the credentials dialog, Windows will first prompt the user to press `Control+Alt+Delete`, then Windows will switch to the secure desktop to accept the users credentials. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Requiring the use of a trusted path helps reduce the probability of an administrator being tricked into divulging credentials to malicious software that is masquerading as the credential dialog.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows Components\Credential
User Interface\Require trusted path for credential entry
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\CredUI /v
EnableSecureCredentialPrompting
```

Default Value:
`Not Configured`

1.12.11 Disable remote Desktop Sharing

Description:
This control defines whether a user is allowed to share their desktop using NetMeeting. For all profiles, the recommended state for this setting is `Enabled`.

Rationale:
Preventing remote Desktop Sharing will reduce the remote attack surface of the system.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Administrative Templates\Windows
Components\NetMeeting\Disable remote Desktop Sharing
```

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

```
reg query HKLM\Software\Policies\Microsoft\Conferencing /v NoRDS
```

Default Value:
Not Configured

References:
CCE-8178-6

Appendix A: References

1. Microsoft, Inc. (2009). *Windows Server 2008 Security Guide*. Available: http://www.microsoft.com/downloads/details.aspx?familyid=FB8B981F-227C-4AF6-A44B-B115696A80AC&displaylang=en. Last accessed 4 February 2010.

2. Microsoft, Inc. (2009). *Security Compliance Management Toolkit Series*. Available: http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displaylang=en. Last accessed 4 February 2010.

3. Defense Information Systems Agency. (2009). *Windows Server 2008 Security Checklist*. Available: http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=228. Last accessed 4 February 2010.

4. Center for Internet Security. (2007). *CIS Windows 2003 Server Domain Controller Benchmark v.2.0.0*. Available: http://cisecurity.org/en-us/?route=permalink.7a30501f056fd924e42a40473a3e9ee8. Last accessed 4 February 2010.

5. Center for Internet Security. (2007). *CIS Windows 2003 Server Member Server Benchmark v.2.0.0*. Available: http://cisecurity.org/en-us/?route=permalink.e5e9b1c5408964e0d438ac41cccc58f2. Last accessed 4 February 2010.

Appendix B: Change History

Date	Version	Changes for this version
November 5th, 2009	1.0.0	Initial Public Release
July 30th, 2010	1.1.0	- Section 1.1.10: Fixed GPO in Remediation section. - Changed 1.3.17: Fixed auditpol command to search for the correct policy - Changed 1.9.10: Set the recommended value to enabled from disabled - Changed 1.5.1: Fixed typos - Changed 1.5.2: Fixed typos - Changed 1.10.1: Fixed GPO path in Remediation section - Changed 1.10.2: Fixed GPO path in Remediation - Changed 1.10.3: Fixed GPO path in Remediation - Changed 1.10.4: Fixed GPO path in Remediation - Changed 1.12.3: Fixed Registry Key in Audit