HARRIS COMPUTER SYSTEMS

CONFIGURATION MANAGEMENT POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: ______________________________

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	3/9/2020	Katie Rose	Major	Initial version of policy.	Dwayne Martin
1.1	3/24/2021	Katie Rose	Minor	Annual Policy Review, Added Definitions Document	Dwayne Martin

POLICY

N. Harris Computer Corporation ("Harris" or "Company") is committed to ensuring the security of Company systems and data. This policy establishes configuration management guidelines in order to help with managing risks associated with system or infrastructure changes. The configuration management guidelines are to be followed as closely as possible to ensure the security of Company systems and data. A risk analysis will be conducted for any exceptions to determine the level of risk and the potential for any vulnerabilities exposed. Exceptions and the risk analysis will be formally documented by the System Owner and reviewed by management, an information security Workforce Member, or the Governance, Risk and Compliance Committee (GRCC) as appropriate.

When new systems are introduced or changes are to be made to existing systems or infrastructure, a process of documentation, specification, testing, quality control, configuration guidelines and managed implementation will be followed. This policy provides the minimum requirements and guidance for baseline configuration of systems and resources that are implemented through a change control process per the Corporate Change Control Policy.

Operational Guidelines

1. All systems that are deployed into Company environments must meet the required minimum configuration guidelines.

2. All changes to production systems, network devices, or Company infrastructure must be reviewed to ensure compliance with business and security requirements.
3. All changes to production systems must be tested if at all possible before they are implemented in production.
4. Implementation of approved changes are only performed by authorized personnel.
5. Where possible, frontend functionality (developer dashboards and portals) is separated from backend (database and app servers) systems by being deployed on separate servers or containers and segregated appropriately on the network. If multipurpose is required or intended for a single system, it must meet minimum functional configuration requirements for the services provided by the system (i.e., frontend and backend services).
6. Only vendor supported operating systems and network devices are permitted on Company networks.
7. The Company uses the Center for Internet Security benchmarks and controls for ensuring secure configuration of systems. Refer to the Appendix for samples of the CIS benchmarks.
8. All systems are configured to comply with the least privileged principal in that all unnecessary ports and services are disabled and restricted to only those required and authorized.
9. Clocks are continuously synchronized to an authoritative source across all systems (e.g., NIST time servers) via Network Time Protocols (NTP) or a platform-specific equivalent. Modifying time data on systems is restricted.

Baseline Configuration

1. The Company will develop, document and maintain a current baseline configuration of the information system including communications and connectivity-related aspects of the system.
2. Information systems capable of operating a real-time clock will have the clock configured so that:
   (a) It is synchronized with one primary internal authoritative time source(s) via NTP. An alternate internal authoritative source may be configured for redundancy but should be using the same NTP.
   (b) It is set to an agreed standard received from industry accepted time sources (UTC).
   (c) The correct interpretation of the date\time format will be used to ensure that the timestamp reflects the real date/time (e.g., daylight savings).
3. Information systems will be maintained according to the established baseline configurations. Refer to the detailed security configuration guidelines specific Operating Systems (OS), database systems and various applications systems here.

4. The baseline configuration of information systems will be reviewed and updated at least once a year or when required due to a significant configuration change (e.g., OS upgrade, hardware change).

Control of Operational Software

1. Any new software or application to be introduced into the Company environment must be reviewed and approved prior to implementation.
2. The Company maintains a list of CIT approved software programs.
3. The Company will identify and document unauthorized or blacklisted software.
4. Applications and operating system software will be tested prior to being implemented.
5. A rollback strategy will be developed and documented prior to implementation of any application or software.
6. Vendor supplied software used in information systems will be maintained at a current vendor support and patch level.

Access Restrictions for Change

1. Defined, documented, approved, and enforced physical and logical access restrictions associated with changes to the information system will meet the minimum configuration requirements including but not limited to:
   (a) Only qualified and authorized personnel are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.
   (b) Local administrative rights will be granted only with authorized approval.
   (c) Access records will be maintained in order to ensure that configuration change control is being implemented and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system.
   (d) Logical and physical access control lists that authorize vendors, suppliers or other authorized support personnel to make changes to an information system or component must be created and maintained.
2. Authorization will be approved by management, provided on a least privilege basis and monitored.
   (a) Lists will be reviewed on a periodic basis and no less than once per year.

PROCEDURE

Operational Guidelines

1. The Corporate Change Management Policy and Protocol must be followed for all changes to systems or infrastructure.
2. Testing of configuration changes, patches, upgrades, etc. must be conducted on a non-production system or environment when possible. If non-production testing isn't possible, testing must be done within a small group of systems and/or users.

3. All frontend applications are implemented on a designated server that is configured with the recommended baseline configurations. All access to these systems and applications will be limited to least privilege including account access as well as network access. Ports and services are configured for only the approved backend systems and appropriate users. Unnecessary ports and/or services will be disabled.
4. All backend databases and applications are implemented on a separate designated server to the extent possible and are configured with the recommended baseline configurations All access to these systems, databases and applications will be limited to least privilege including account access as well as network access. Ports and services are configured for only the approved frontend systems and appropriate users. Unnecessary ports and/or services will be disabled.
5. Where appropriate frontend systems and backend systems will be segregated in a Demilitarized Zone (DMZ). Where possible the frontend system will be placed in the frontend DMZ and the backend system in the backend DMZ. If this is not possible, the two systems will have appropriate communications controls such as port and IP address restrictions.
6. Benchmarks for various vendor supported operating systems can be found on the CIS website or Windows-based systems use a baseline Active Directory group policy configuration in conjunction with the CIS benchmarks.
7. Benchmarks for various vendor supported operating systems and control recommendations for network devices can be located on the CIT SharePoint site or CIS website.
8. The System Owner will adhere to these benchmarks and control recommendations when implementing changes on systems or the Company network.
9. Firewalls are configured with default deny and only allowing required ports for specified IP addresses.
10. One or more internal time sources will be designated as the definitive time source for all information systems clock synchronizations
    a. The designated time source will be synchronized to an approved, known external time source (e.g., NIST time servers) via network time protocols (NTP)
    b. The designated time source will be synced within 30 seconds of the external time source
    c. The designated time source will synchronize at least on a daily basis and at system boot
11. Information systems capable of operating a real-time clock will have the clock configured so that:
    a. It is synchronized with one or more internal authoritative time source(s) via network time protocol (NTP)
    b. It is set to an agreed standard received from industry accepted time sources (UTC)
    c. The correct interpretation of the date\time format shall be used to ensure that the timestamp reflects the real date/time (e.g., daylight savings)

Baseline Configuration

1. It is the responsibility of the System Owner to ensure that each server within the environment at a minimum have the following aspects of the baseline configuration installed and functioning as stated within the associated policies prior to being placed into a production state:

(a) Standard vendor supported operating system/installed applications with current version numbers and patches.

(b) Standard system security measures:

(i) Anti-virus\host-based firewall

(ii) Event logging enabled

(iii) An up-to-date patch or hot-fix revision level

(c) IP network configuration and connectivity dependent upon prior risk assessment and design phase.

(i) Proper DNS (domain name resolution) configuration

(ii) Proper port and rule configuration applying the least privilege principle

(d) Logical placement of the component within the system and enterprise architecture

(i) Including assignment to the proper Active Directory domain, organizational unit, container, etc.

(1) If applicable, the appropriate group policies shall be applied

(ii) Appropriate placement and configuration in the network infrastructure including:

(1) Access controls by IP where appropriate (i.e., Whitelist)

(2) Placement in the DMZ where appropriate

(3) Disabling Remote Desktop Protocol (RDP) or other ports/protocols where appropriate to secure the system

(4) Restricting External Port access into the production LAN environment.

2. Information system installations are to be tracked using Company configuration management tools.

(a) Upon the completion of information system baseline configurations proper documentation and sign-off will be produced and archived

Control of Operational Software

1. It is the responsibility of CIT to maintain a list of approved software

(a) Using Harris configuration management tools, approved system software is to be documented and reviewed on a periodic basis and no less than once a year.

(b) The list of approved system software will include at a minimum the following information

(i) ...... Vendor

(ii) ..... Version
(iii) .... Justification\Usage
(iv) .... Approved By
(v) ..... Approved For

2. It is the responsibility of CIT to maintain a list of unauthorized software or blacklisted software
    - (a) Using CIT configuration management tools, unauthorized or blacklisted software is to be documented and reviewed on a periodic basis and no less than once a year
    - (b) Utilizing automated tools if available or manual checks, CIT is responsible for ensuring that blacklisted software does not exist on managed information systems.
        - (i) ...... If found, the information system is to be isolated immediately from the network
            - (1) Found software is to be removed or the system is be re-imaged\replaced where deemed necessary per risk associated with installed software
            - (2) Once verified that the situation has been resolved the system will be removed from isolation
            - (3) The removal, remediation and investigation around the software is to be tracked and documented using the proper tools
3. For new software requests, prior to acquiring the software, all Company employees must first seek proper approval.
    - (a) The employee must submit a request to CIT for review and approval for the software. Email must include:
        - (i) ...... Software name and vendor
        - (ii) ..... Version requested
        - (iii) .... Justification for the use of the software
4. CIT will approve or deny the request via email or ticketing systems when proper vetting has been accomplished
    - (a) If approved the manager must include the security and compliance officer within the approval email
    - (b) Once approved the security and compliance officer must work with the CIT to ensure the software is added to the approved software list.
5. Where possible it is the responsibility of the System Owner ensure that updated versions of applications/operating system software are tested prior to implementation within the production environment
    - (a) Testing should be performed on staging or QA (non-production) level systems and include tests of:
        - (i) ...... Usability
        - (ii) ..... Security
        - (iii) .... Impact on other systems

(b) Results of tests along with any required tasks performed to remediate issues will be documented and published within the proper configuration management tools for future reference if needed.

6. System Owners are also responsible for the development and documentation of a roll-back strategy prior to the changes being implemented within a production environment.

(a) This includes ensuring that the previous version of the software (if applicable) is archived along with any required configuration or documentation if the roll-back strategy requires it.

Access Restrictions for Change

1. Changes to information systems and system components including software/application changes and upgrades are restricted to only authorized personnel.

2. Prior to being granted change access to information systems, employees must submit a formal request either via email or other appropriate tools to management.

(a) Upon authorization from management a formal request via the CIT ticketing system is to be submitted requesting the access and containing the following information:

(i) ...... User requesting access

(ii) ..... Systems\components\software requesting access to

(iii) .... Duration of requested access

(iv) .... Justification for requested access

(b) Using tools such as access-lists and local administrative rights and permissions, the operations team will grant access to the user on a least privilege basis.

(c) All access will be monitored via access control records specific to the information systems accessed and records are to be archived and retained per Company policies.

(d) It is the responsibility of CIT and the System Owner to periodically review user access to information systems and modify where necessary.

(i) ...... Reviews are to be documented and tracked via the appropriate tools including any changes\modifications made as a result of the reviews

DEFINITIONS

See attached policy definitions or click here.

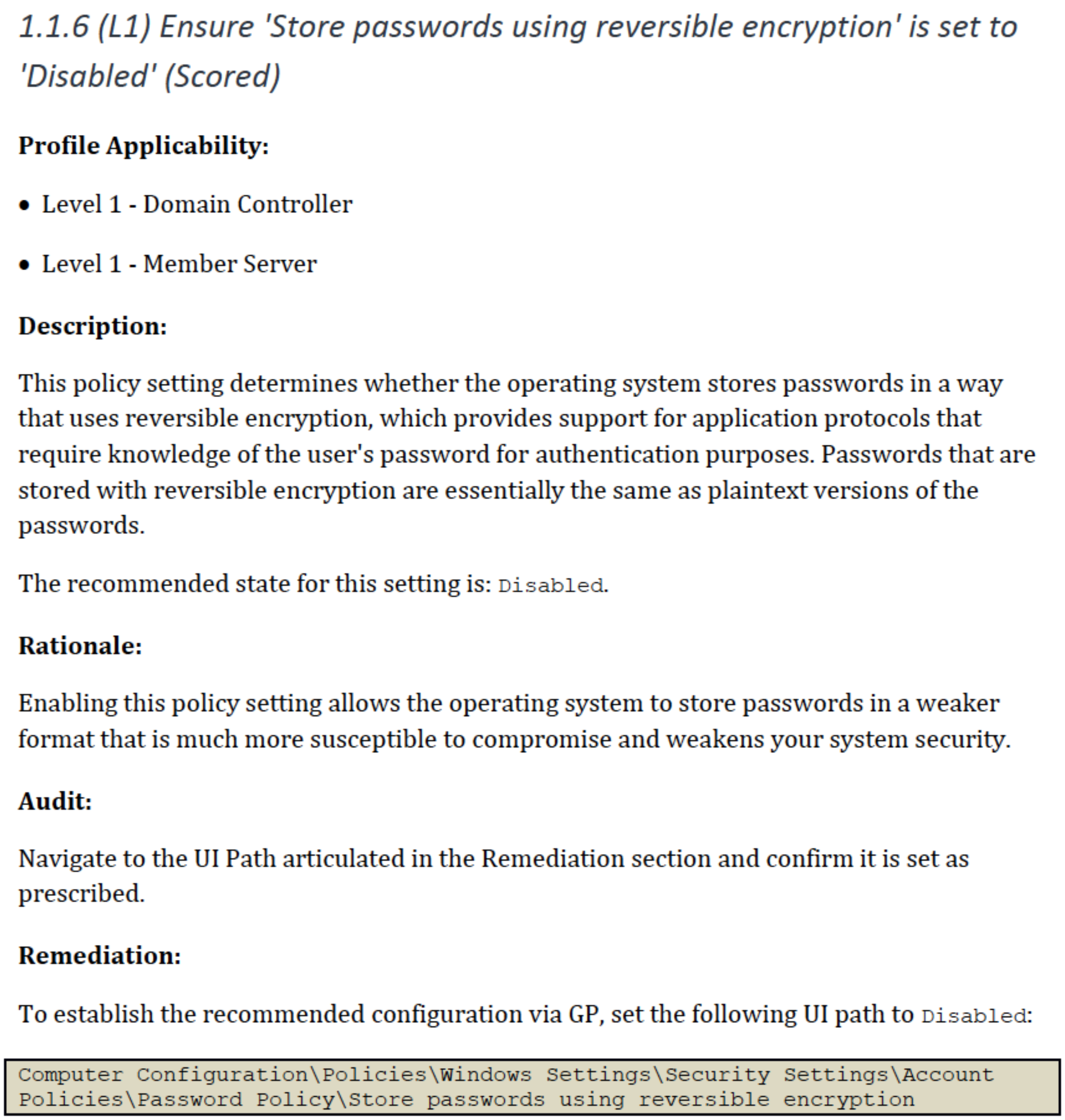
REGULATORY REFERENCES

NIST SP 800-53 R4 CM-2(3)
NIST SP 800-53 R4 CM-3
NIST SP 800-53 R4 CM-3(2)
NIST SP 800-53 R4 CM-4
NIST SP 800-53 R4 CM-6
NIST SP 800-53 R4 CM-6(1)
NIST SP 800-53 R4 CM-6(2)
NIST SP800-53 r4 CM-7(4)

APPENDIX

SAMPLES CIS BENCHMARK

Windows Server 2016



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

Profile Applicability:

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

Description:

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

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

Rationale:

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

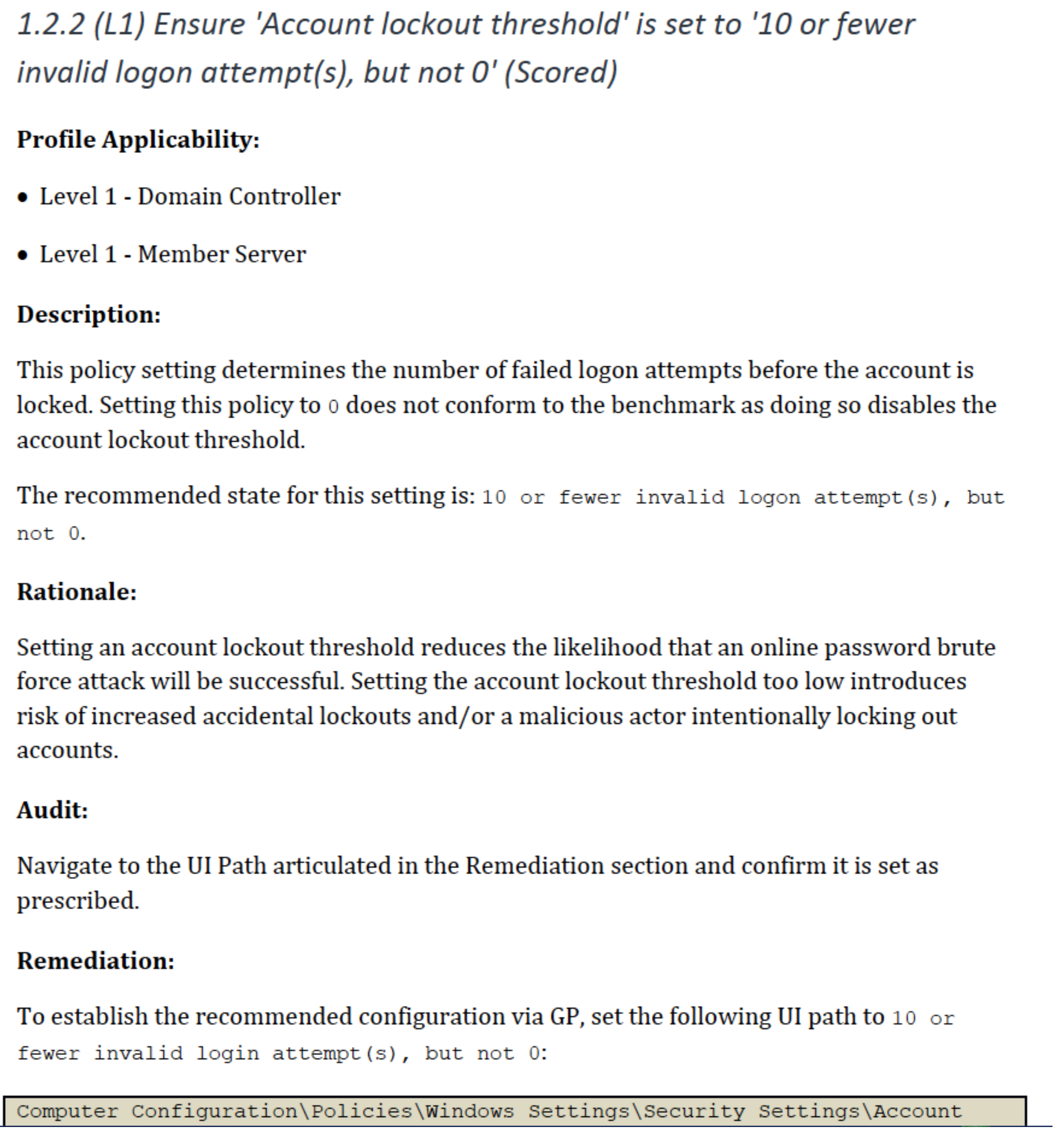
Audit:

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

Remediation:

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

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



1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)

Profile Applicability:

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

Description:

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to `0` does not conform to the benchmark as doing so disables the account lockout threshold.

The recommended state for this setting is: `10 or fewer invalid logon attempt(s), but not 0`.

Rationale:

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

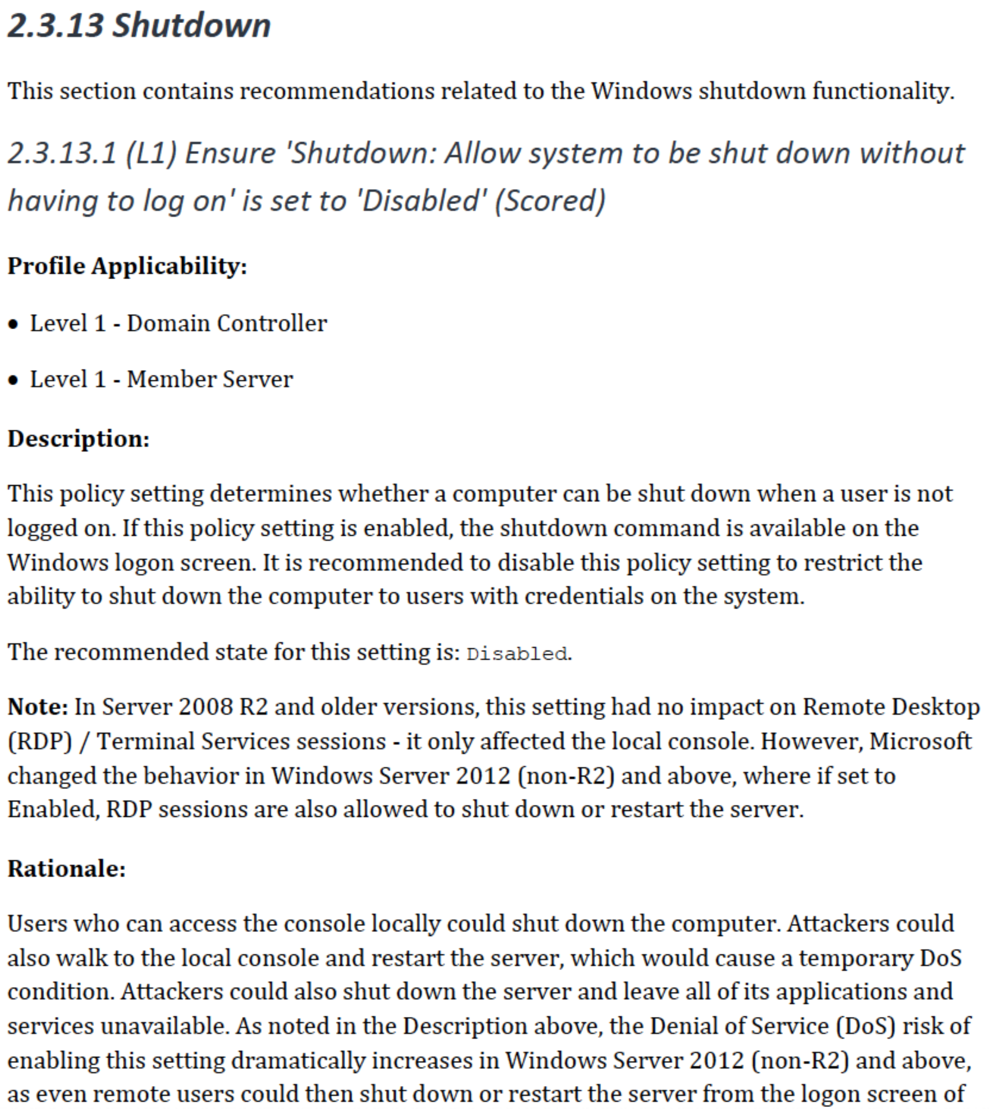
Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `10 or fewer invalid login attempt(s), but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
```



2.3.13 Shutdown

This section contains recommendations related to the Windows shutdown functionality.

2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system.

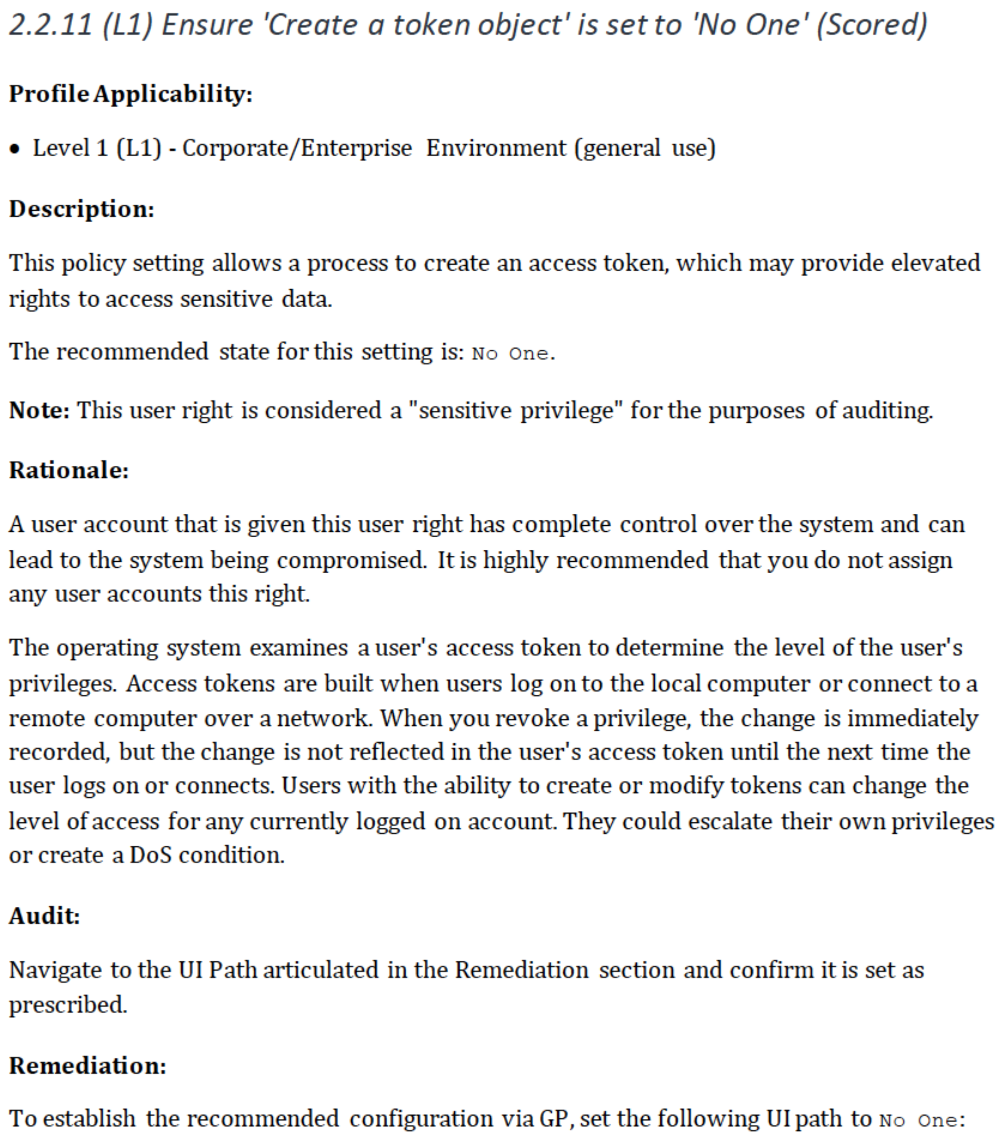
The recommended state for this setting is: `Disabled`.

Note: In Server 2008 R2 and older versions, this setting had no impact on Remote Desktop (RDP) / Terminal Services sessions - it only affected the local console. However, Microsoft changed the behavior in Windows Server 2012 (non-R2) and above, where if set to Enabled, RDP sessions are also allowed to shut down or restart the server.

Rationale:

Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable. As noted in the Description above, the Denial of Service (DoS) risk of enabling this setting dramatically increases in Windows Server 2012 (non-R2) and above, as even remote users could then shut down or restart the server from the logon screen of

Windows 10 Enterprise



2.2.11 (L1) Ensure 'Create a token object' is set to 'No One' (Scored)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

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

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

Rationale:

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

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

Audit:

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

Remediation:

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

2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' (Scored)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

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

Caution: Configuring a standalone (non-domain-joined) workstation as described above may result in an inability to remotely administer the workstation.

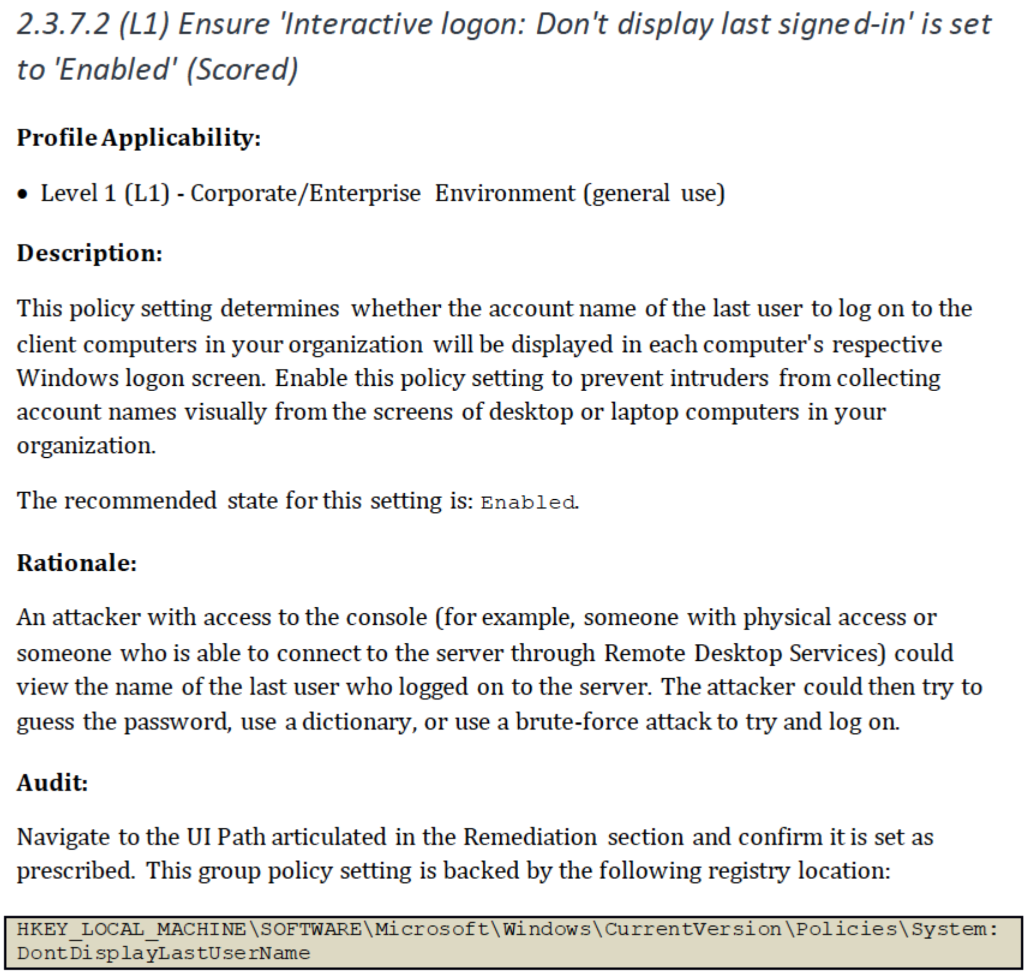
Note: The security identifier `Local account` is not available in Windows 7 and Windows 8.0 unless MSKB 2871997 has been installed.

Rationale:

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

Audit:

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



2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

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

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Audit:

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

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