Table of Contents

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Audit:

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

Remediation:

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

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

Impact:

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

Default Value:

On Member Servers: Administrators, Backup Operators, Users.

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

References:

1. CCE-37659-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.1 Maintain Inventory of Administrative Accounts
Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

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

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

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

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

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

Rationale:

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

Audit:

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

Remediation:

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

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

Impact:

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

Default Value:

Administrators, Remote Desktop Users.

References:

1. CCE-37072-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.1 Maintain Inventory of Administrative Accounts
Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

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

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

(L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only) (Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

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

Rationale:

In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Audit:

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

Remediation:

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

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

Impact:

Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the Domain Controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.

If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Default Value:

Disabled.

References:

1. CCE-37953-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

(L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether users must press CTRL+ALT+DEL before they log on.

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

Rationale:

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path.

An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Audit:

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

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

Remediation:

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

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

Impact:

Users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information.

Default Value:

On Windows Server 2008 R2 or older: Disabled.

On Windows Server 2012 (non-R2) or newer: Enabled.

References:

1. CCE-37637-6

CIS Controls:

Version 6

8 Malware Defenses
Malware Defenses

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

(L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider.

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

Rationale:

A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClien
t:Enabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time
Service\Time Providers\Enable Windows NTP Client
```

Note: This Group Policy path is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

You can set the local computer clock to synchronize time with NTP servers.

Default Value:

Disabled. (The local computer clock does not synchronize time with NTP servers.)

References:

1. CCE-37843-0

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

(L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Scored)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting allows you to specify whether the Windows NTP Server is enabled.

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

Note: In most enterprise managed environments, you should *not* disable the Windows NTP Server on Domain Controllers, as it is very important for the operation of NT5DS (domain hierarchy-based) time synchronization.

Rationale:

The configuration of proper time synchronization is critically important in an enterprise managed environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServe
r:Enabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time
Service\Time Providers\Enable Windows NTP Server
```

Note: This Group Policy path is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The computer cannot service NTP requests from other computers.)

References:

1. CCE-37319-1

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.