Suite 1055, 377 Kent Street Sydney NSW 2000
support@clickitsolutions.com.au
1300 757 505
www.clickitsolutions.com.au

Security Assessment Sample

Resource Compliance Report

View the status and breakdown of compliance policies that are mapped to custom groups.

Custom Group Name : Redacted

Hostname(Target Name) : Redacted

IP Address : Redacted

Operating System : Windows 11 Professional Edition (x64)

OS Platform : Windows

Compliance Status : All

Scan Status : All

Applicable Filter : All

Policy Name	Policy Type	Rules Passed	Percentage
CIS Microsoft Edge Benchmark v2.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)	CIS	2/90 Rules Passed	2%
CIS Google Chrome Benchmark v3.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)	CIS	10/87 Rules Passed	13%
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)	CIS	77/383 Rules Passed	20%

CIS Microsoft Edge Benchmark v2.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)

1 Microsoft Edge	**2/88 passed**
1.13 Password manager and protection	**0/1 passed**
1.13.1. L1 Ensure Enable saving passwords to the password manager is set to Disabled	Failed
1.14 Performance	**0/1 passed**
1.14.1. L1 Ensure Enable startup boost is set to Disabled	Failed
1.17 Private Network Request Settings	**0/1 passed**
1.17.1. L1 Ensure Specifies whether to allow websites to make requests to more-private network endpoints is set to Disabled	Failed
1.20 SmartScreen settings	**0/6 passed**
1.20.3. L1 Ensure Enable Microsoft Defender SmartScreen DNS requests is set to Disabled	Failed
1.20.5. L1 Ensure Prevent bypassing Microsoft Defender SmartScreen prompts for sites is set to Enabled	Failed
1.20.2. L1 Ensure Configure Microsoft Defender SmartScreen to block potentially unwanted apps is set to Enabled	Failed
1.20.6. L1 Ensure Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads is set to Enabled	Failed
1.20.1. L1 Ensure Configure Microsoft Defender SmartScreen is set to Enabled	Failed
1.20.4. L1 Ensure Force Microsoft Defender SmartScreen checks on downloads from trusted sources is set to Enabled	Failed
1.22 TyposquattingChecker settings	**0/1 passed**
1.22.1. L1 Ensure Configure Edge TyposquattingChecker is set to Enabled	Failed
1.2 Cast	**0/1 passed**
1.2.1. L1 Ensure Enable Google Cast is set to Disabled	Failed
1.3 Content Settings	**0/4 passed**
1.3.6. L1 Ensure Control use of the File System API for writing is set to Enabled Dont allow any site to request write access to files and directories	Failed
1.3.3. L1 Ensure Control use of insecure content exceptions is set to Enabled Do not allow any site to load mixed content	Failed
1.3.9. L1 Ensure Default automatic downloads setting is set to Enabled Dont allow any website to perform automatic downloads	Failed
1.3.10. L1 Ensure Default geolocation setting is set to Enabled Dont allow any site to track users physical location	Failed
1.5 Experimentation	**0/1 passed**
1.5.1. L1 Ensure Configure users ability to override feature flags is set to Enabled Prevent users from overriding feature flags	Failed
1.7 HTTP authentication	**0/2 passed**
1.7.2. L1 Ensure Allow cross-origin HTTP Basic Auth prompts is set to Disabled	Failed
1.7.1. L1 Ensure Allow Basic authentication for HTTP is set to Disabled	Failed
1.8 Identity and sign-in	**0/2 passed**
1.8.2. L1 Ensure Guided Switch Enabled is set to Disabled	Failed
1.8.1. L1 Ensure Enable the linked account feature is set to Disabled	Failed

1.110. L1 Ensure Shopping in Microsoft Edge Enabled is set to Disabled	Failed
1.55. L1 Ensure Clear cached images and files when Microsoft Edge closes is set to Disabled	Failed
1.56. L1 Ensure Clear history for IE and IE mode every time you exit is set to Disabled	Failed
1.54. L1 Ensure Clear browsing data when Microsoft Edge closes is set to Disabled	Failed
1.96. L1 Ensure Enable warnings for insecure forms is set to Enabled	Failed
1.95. L1 Ensure Enable use of ephemeral profiles is set to Disabled	Failed
1.62. L1 Ensure Configure the list of names that will bypass the HSTS policy check is set to Disabled	Passed
1.93. L1 Ensure Enable site isolation for every site is set to Enabled	Failed
1.60. L1 Ensure Configure Related Matches in Find on Page is set to Disabled	Failed
1.57. L1 Ensure Configure browser process code integrity guard setting is set to Enabled Enable code integrity guard enforcement in the browser process	Failed
1.58. L1 Ensure Configure InPrivate mode availability is set to Enabled InPrivate mode disabled	Failed
1.102. L1 Ensure In-app support Enabled is set to Disabled	Failed
1.101. L1 Ensure Hide the First-run experience and splash screen is set to Enabled	Failed
1.99. L1 Ensure Enhance the security state in Microsoft Edge is set to Enabled Balanced mode	Failed
1.44. L1 Ensure Allow user feedback is set to Disabled	Failed
1.85. L1 Ensure Enable globally scoped HTTP auth cache is set to Disabled	Failed
1.52. L1 Ensure Block tracking of users web-browsing activity is set to Enabled Balanced Blocks harmful trackers and trackers from sites user has not visited content and ads will be less personalized	Failed
1.50. L1 Ensure Automatically import another browsers data and settings at first run is set to Enabled Disables automatic import and the import section of the first-run experience is skipped	Failed
1.84. L1 Ensure Enable Follow service in Microsoft Edge is set to Disabled	Failed
1.48. L1 Ensure Allow websites to query for available payment methods is set to Disabled	Failed
1.92. L1 Ensure Enable security warnings for command-line flags is set to Enabled	Failed
1.89. L1 Ensure Enable renderer code integrity is set to Enabled	Failed
1.90. L1 Ensure Enable resolution of navigation errors using a web service is set to Disabled	Failed
1.87. L1 Ensure Enable network prediction is set to Enabled Dont predict network actions on any network connection	Failed
1.88. L1 Ensure Enable profile creation from the Identity flyout menu or the Settings page is set to Disabled	Failed
1.77. L1 Ensure Enable AutoFill for payment instructions is set to Disabled	Failed
1.33. L1 Ensure Allow importing of saved passwords is set to Disabled	Failed
1.78. L1 Ensure Enable browser legacy extension point blocking is set to Enabled	Failed
1.34. L1 Ensure Allow importing of search engine settings is set to Disabled	Failed
1.75. L1 Ensure DNS interception checks enabled is set to Enabled	Failed
1.76. L1 Ensure Enable AutoFill for addresses is set to Disabled	Failed
1.73. L1 Ensure Disable saving browser history is set to Disabled	Failed
1.74. L1 Ensure Disable synchronization of data using Microsoft sync services is set to Enabled	Failed
1.118. L1 Ensure Suggest similar pages when a webpage cant be found is set to Disabled	Failed
1.41. L1 Ensure Allow remote debugging is set to Disabled	Failed
1.119. L1 Ensure Suppress the unsupported OS warning is set to Disabled	Failed
1.42. L1 Ensure Allow the audio sandbox to run is set to Enabled	Failed

1.39. L1 Ensure Allow personalization of ads Microsoft Edge search news and other Microsoft services by sending browsing history favorites and collections usage and other browsing data to Microsoft is set to Disabled	Failed
1.117. L1 Ensure Standalone Sidebar Enabled is set to Disabled	Failed
1.40. L1 Ensure Allow queries to a Browser Network Time service is set to Enabled	Failed
1.114. L1 Ensure Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context is set to Disabled	Failed
1.81. L1 Ensure Enable deleting browser and download history is set to Disabled	Failed
1.122. L1 Ensure Wait for Internet Explorer mode tabs to completely unload before ending the browser session is set to Disabled	Failed
1.67. L1 Ensure Control communication with the Experimentation and Configuration Service is set to Enabled Disable communication with the Experimentation and Configuration Service	Failed
1.23. L1 Ensure Ads setting for sites with intrusive ads is set to Enabled Block ads on sites with intrusive ads	Failed
1.64. L1 Ensure Configure the Share experience is set to Enabled Dont allow using the Share experience	Failed
1.65. L1 Ensure Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode is set to Enabled Do not send form data or headers	Failed
1.63. L1 Ensure Configure the list of types that are excluded from synchronization is set to Enabled	Failed
1.107. L1 Ensure Restrict exposure of local IP address by WebRTC is set to Enabled Allow public interface over http default route. This doesnt expose the local IP address	Failed
1.30. L1 Ensure Allow importing of browser settings is set to Disabled	Failed
1.108. L1 Ensure Set disk cache size in bytes is set to Enabled 250609664	Failed
1.31. L1 Ensure Allow importing of home page settings is set to Disabled	Failed
1.105. L1 Ensure Manage exposure of local IP addresses by WebRTC is set to Disabled	Passed
1.72. L1 Ensure Delete old browser data on migration is set to Disabled	Failed
1.28. L1 Ensure Allow import of data from other browsers on each Microsoft Edge launch is set to Disabled	Failed
1.106. L1 Ensure Notify a user that a browser restart is recommended or required for pending updates is set to Enabled Required - Show a recurring prompt to the user indicating that a restart is required	Failed
1.29. L1 Ensure Allow importing of autofill form data is set to Disabled	Failed
1.27. L1 Ensure Allow Google Cast to connect to Cast devices on all IP addresses is set to Disabled	Failed
1.24. L1 Ensure Allow download restrictions is set to Enabled Block malicious downloads	Failed
1.112. L1 Ensure Show Microsoft Rewards experiences is set to Disabled	Failed
1.109. L1 Ensure Set the time period for update notifications is set to Enabled 86400000	Failed
1.32. L1 Ensure Allow importing of payment info is set to Disabled	Failed
1.80. L1 Ensure Enable CryptoWallet feature is set to Disabled	Failed
1.66. L1 Ensure Continue running background apps after Microsoft Edge closes is set to Disabled	Failed
1.82. L1 Ensure Enable Discover access to page contents for AAD profiles is set to Disabled	Failed
1.79. L1 Ensure Enable component updates in Microsoft Edge is set to Enabled	Failed
1.35. L1 Ensure Allow managed extensions to use the Enterprise Hardware Platform API is set to Disabled	Failed
1.113. L1 Ensure Show the Reload in Internet Explorer mode button in the toolbar is set to Disabled	Failed
3 Microsoft Edge Update	**0/2 passed**
3.1 Applications	**0/1 passed**
3.1.1. L1 Ensure Update policy override default is set to Enabled Always allow updates recommended	Failed
3.3 Preferences	**0/1 passed**

3.3.1. L1 Ensure Auto-update check period override is set to any value except 0 Failed

1.13.1. L1 Ensure Enable saving passwords to the password manager is set to Disabled

Rule Status :

Failed

Summary :

This policy setting enables or disables the ability for users to save their passwords in Microsoft Edge.The recommended state for this setting is Disabled.

Rationale :

Saving passwords in Edge could lead to a user"s web passwords being breached if an attacker were to gain access to their web browser especially in the case of an unattended and unlocked workstation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Password manager and protection\Enable saving passwords to the password manager.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template.MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to utilize the Microsoft Edge built-in password manager.

1.14.1. L1 Ensure Enable startup boost is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows Microsoft Edge processes to start at OS sign-in and restart in background after the last browser window is closed.If Microsoft Edge is running in background mode, the browser might not close when the last window is closed, and the browser won ´t be restarted in background when the window closes. See the BackgroundModeEnabled (Continue running background apps after Microsoft Edge closes) policy for information about what happens after configuring Microsoft Edge background mode behavior. Note: The startup boost policy may initially be configured off or on by the user; the user can configure its behavior in edge://settings/system. The recommended state for this setting is: Disabled.

Rationale :

Allowing processes from the browser to run in the background could allow a malicious script or code to continue running once the browser windows has been closed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Performance\Enable startup boost.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will experience normal browser start-up times which may seem slow in comparison to Startup boost.

1.17.1. L1 Ensure Specifies whether to allow websites to make requests to more-private network endpoints is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether insecure websites are allowed to make requests to more private network endpoints.A network endpoint is more private than another if:Its IP address is localhost and the other is not.Its IP address is private and the other is public.In the future, depending on spec evolution, this policy might apply to all cross-origin requests directed at private IPs or localhost.A website is deemed secure if it meets the definition of a secure context in https://developer.mozilla.org/en-US/docs/Web/Security/Secure_Contexts. Otherwise, it will be treated as an insecure context. Note: This policy relates to the Private Network Access specification. See https://wicg.github.io/private-network-access/.or more details. Note #2: If this policy is not configured or set to Disabled , the default behavior for requests from insecure contexts to more-private network endpoints will depend on the user´s personal configuration for the BlockInsecurePrivateNetworkRequests feature, which may be set by a field trial or on the command line. The recommended state for this setting is: Disabled.

Rationale :

Allowing public internet sites to “peek” behind your firewall by using the user’s browser to mix intranet resources into internet-delivered pages represents a dangerous attack surface. The baseline requires enforcement of the new browser restriction that any such intranet requests are blocked if the internet page was delivered over insecure HTTP. Note: If for some reason you need to permit insecure cross-network requests for legacy sites, you can configure temporary exceptions in Allow the listed sites to make requests to more-private network endpoints from insecure contexts .

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Private Network Request Settings\Specifies whether to allow websites to make requests to more-private network endpoints.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to allow non-secure public contexts to request resources from private addresses.

1.20.3. L1 Ensure Enable Microsoft Defender SmartScreen DNS requests is set to Disabled

Rule Status :

Failed

Summary :

This policy setting configures DNS requests made by Microsoft Defender SmartScreen.Note: This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX. The recommended state for this setting is: Disabled.

Rationale :

Whenever SmartScreen is enabled for Edge browser, SmartScreen tries to check if the website is a phishing/malicious URL and does a local DNS query. If the DNS server fails to resolve the website, Web Isolation will not be used to isolate those websites.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\SmartScreen settings\Enable Microsoft Defender SmartScreen DNS requests.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:DNS server might not resolve queries sent to external websites or the website may have no information stored on its local server or cache.Warning: Disabling DNS requests will prevent Microsoft Defender SmartScreen from getting IP addresses, and potentially impact the IP-based protections provided.

1.20.5. L1 Ensure Prevent bypassing Microsoft Defender SmartScreen prompts for sites is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether users may bypass the SmartScreen warning if a site is deemed unsafe.The recommended state for this setting is Enabled.

Rationale :

Windows Defender SmartScreen can provide messages and warnings to users to help thwart phishing and malicious software. However, by default, users may bypass these warnings.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\SmartScreen settings\Prevent bypassing Microsoft Defender SmartScreen prompts for sites.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:SmartScreen will not allow a user to bypass the warning message.

1.20.2. L1 Ensure Configure Microsoft Defender SmartScreen to block potentially unwanted apps is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows configuration of Microsoft Defender SmartScreen and whether potentially unwanted apps are blocked.The recommended state for this setting is Enabled.

Rationale :

Windows Defender SmartScreen can block unwanted apps that will help inform and protect users from vulnerabilities related to adware and low-reputation apps.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen to block potentially unwanted apps.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Microsoft Defender SmartScreen will block potentially dangerous apps. This could stop the user from installing an app that could be potentially harmful to the system.

1.20.6. L1 Ensure Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether users may override Microsoft Defender SmartScreen warnings regarding downloads that are unverified.The recommended state for this setting is Enabled.

Rationale :

Smartscreen checks downloads and verifies whether they are deemed safe or not. Only allowing verified downloads greatly reduces risk of a download containing a virus, spyware, or other unwanted software.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\SmartScreen settings\Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:User will not be able to download software that has not been verified by SmartScreen.

1.20.1. L1 Ensure Configure Microsoft Defender SmartScreen is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows configuration of Microsoft Defender SmartScreen. Microsoft Defender SmartScreen helps to identify phishing and malware websites and to make informed decisions about downloads.The recommended state for this setting is Enabled.

Rationale :
Windows Defender SmartScreen can provide messages and warnings to users to help thwart phishing attempts and malicious software.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\SmartScreen settings\Configure Microsoft Defender SmartScreen.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact:None - this is the default behavior.

1.20.4. L1 Ensure Force Microsoft Defender SmartScreen checks on downloads from trusted sources is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft Defender SmartScreen can check if downloads have been retrieved from a trusted source.The recommended state for this setting is Enabled.

Rationale :

Windows Defender SmartScreen can verify that downloads are from a trusted source can greatly reduce the chances of a user downloading an infected package to their machine.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Force Microsoft Defender SmartScreen checks on downloads from trusted sources.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.22.1. L1 Ensure Configure Edge TyposquattingChecker is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures whether to turn on Edge TyposquattingChecker. The Edge TyposquattingChecker provides warning messages to help protect users from potential typo squatting sites. Typo squatting is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites.The recommended state for this setting is: Enabled.

Rationale :

Edge TyposquattingChecker will provide a warning message and can help protect users from potential typo squatting by alerting the user to the potential of accessing a malicious site.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\TyposquattingChecker settings\Configure Edge TyposquattingChecker.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will receive a warning message if they attempt to access a site deemed (by Microsoft) a typosquatting site.

1.2.1. L1 Ensure Enable Google Cast is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether users may utilize Google Cast. Note that when this setting is set to Disabledthe Show the cast icon in the toolbar setting is ignored as the icon is removed. The recommended state for this setting is: Disabled.

Rationale :

The use of Google Cast could allow users to show potentially sensitive information to non-trusted devices. These devices could be in public areas.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Cast\Enable Google Cast.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to utilize Google Cast and the Google Cast icon will not be displayed in Microsoft Edge.

1.3.6. L1 Ensure Control use of the File System API for writing is set to Enabled Dont allow any site to request write access to files and directories

Rule Status :

Failed

Summary :

This policy setting specifies whether websites can ask for write access to the host operating system ´s filesystem using the File System API. By default websites can ask for access. Users can change this setting. By setting this policy to (2), access is denied.Policy options mapping: BlockFileSystemWrite (2)= Don ´t allow any site to request write access to files and directories AskFileSystemWrite (3)= Allow sites to ask the user to grant write access to files and directories The recommended state for this setting is: Enabled: Don"t allow any site to request write access to files and directories.

Rationale :

There is a large category of attack vectors that are opened up by allowing web applications access to files. By setting this policy to Enabled: Don"t allow any site to request write access to files and directoriesimplements additional protection to safeguard against accidental sharing of sensitive information contained in locals files.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Don"t allow any site to request write access to files and directories.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Content settings\Control use of the File System API for writing.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users with creative roles that require the File System API access permission to write files for photo, video, and text editors or for creating integrated development environments will need additional permissions granted based on their role.

1.3.3. L1 Ensure Control use of insecure content exceptions is set to Enabled Do not allow any site to load mixed content

Rule Status :

Failed

Summary :

This policy setting allows for the configuration for users to add exceptions to allow mixed content for specific sites.The recommended state for this setting is: Enabled: Do not allow any site to load mixed contentNote: This policy can be overridden for specific URL patterns using the insecurecontentAllowedForUrls (Allow insecure content on specified sites) and insecurecontentBlockedForUrls (Block insecure content on specified sites) policies .

Rationale :

Allowing mixed (secure / insecure) content from a site can lead to malicious content being loaded. Mixed content occurs if the initial request is secure over HTTPS, but HTTPS and HTTP content is subsequently loaded to display the web page. HTTPS content is secure. HTTP content is insecure.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to load mixed content.Computer Configuration\Polices\Administrative Templates\Microsoft Edge\Content Settings\Control use of insecure content exceptions.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to add exceptions for mix content webpages.

1.3.9. L1 Ensure Default automatic downloads setting is set to Enabled Dont allow any website to perform automatic downloads

Rule Status :

Failed

Summary :

This policy setting controls whether websites can perform multiple downloads successively without user interaction.The recommended state for this setting is Enabled: Don ´t allow any website to perform automatic downloads.

Rationale :

Allowing websites to perform automatic downloads puts your system at risk as it will be easier to unintentionally download malicious files and executables.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Don ´t allow any website to perform automatic downloads.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Content settings\Default automatic downloads setting.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Websites will be able to perform automatic downloads.

1.3.10. L1 Ensure Default geolocation setting is set to Enabled Dont allow any site to track users physical location

Rule Status :

Failed

Summary :

This policy setting controls whether a users" physical location can be tracked by websites.The recommended state for this setting is: Enabled: Don"t allow any site to track users" physical location.

Rationale :

Geolocation should not be shared with websites to ensure protection of the user"s privacy regarding location. Additionally, location information could lead to clues regarding the user"s network infrastructure surrounding the device they are utilizing.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Don"t allow any site to track users" physical location.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Content settings\Default geolocation setting.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Location information will not be shared with websites in Microsoft Edge. This could have an effect on websites that utilize this information for customized content.

1.5.1. L1 Ensure Configure users ability to override feature flags is set to Enabled Prevent users from overriding feature flags

Rule Status :

Failed

Summary :

This policy setting configures users" ability to override state of feature flags. Feature flags are settings a team can define that indicate whether a given set of features is visible in the user experience and/or invoked within the functionality.The recommended state for this setting is: Enabled: Prevent users from overriding feature flags.

Rationale :

the user"s ability to enter commands and to override programs should be limited at the CLI in order to prevent users from altering systems configurations. Additionally, Feature flags are not necessary for users, as they are used by the DevOps team during the development and experimental process.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Prevent users from overriding feature flags.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Experimentation\Configure users ability to override feature flags.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready features.

1.7.2. L1 Ensure Allow cross-origin HTTP Basic Auth prompts is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether third-party sub-content can open a HTTP Basic Auth dialog and is typically disabled.The recommended state for this setting is Disabled.

Rationale :
This setting is typically disabled to help combat phishing attempts.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\HTTP authentication\Allow cross-origin HTTP Basic Auth prompts.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact:Disabling this setting should have minimal impact to the user as it is typically disabled by default and third-party sub-content can"t open a HTTP Basic Auth dialog box.

1.7.1. L1 Ensure Allow Basic authentication for HTTP is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines if Basic authentication receives challenges over non-secure HTTP. Basic authentication is a non-secure authentication method that relies on sending the username and password to the server in plaintext.Note: This policy setting is ignored (and Basic is always forbidden) if the AuthSchemes (Supported authentication schemes) policy is set and does not include Basic. The recommended state for this setting is Disabled.

Rationale :

Basic authentication is less robust than other authentication methods available because credentials including passwords are transmitted in plain text. An attacker who can capture these credentials in plain text can gain access to the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\HTTP authentication\Allow Basic authentication for HTTP.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Non-secure HTTP requests from the Basic authentication scheme are blocked, and only secure HTTPS is allowed.

1.8.2. L1 Ensure Guided Switch Enabled is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows Microsoft Edge to prompt the user to switch to the appropriate profile when Microsoft Edge detects that a link is a personal or work link.The recommended state for this setting is Disabled.

Rationale :

Linking personal Microsoft Accounts to a company device could inadvertently lead to data being transferred from the environment to a personal device.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Identity and sign-in\Guided Switch Enabled.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users won"t be prompted to switch to another account when there ´s a profile and link mismatch.

1.8.1. L1 Ensure Enable the linked account feature is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines if Microsoft Edge can guide a user to the account management page where they can link a Microsoft Account (MSA) to an Azure Active Directory (Azure AD) account.The recommended state for this setting is: Disabled.

Rationale :
Linking personal Microsoft Accounts to a company device could inadvertently lead to data being transferred from the environment to a personal device.

How to fix :
To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Identity and sign-in\Enable the linked account feature.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:Linked account information will not be shown on a flyout and when the Azure AD profile doesn´t have a linked account it will not show the "Add account" button.

1.110. L1 Ensure Shopping in Microsoft Edge Enabled is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows users to compare the prices of products, get coupons or rebates from the website, auto-apply coupons, and help checkout faster using autofill data. Coupons for the current retailer and prices from other retailers will be fetched from a server.Note: Starting in Microsoft Edge version 90.0.818.56, the behavior of the messaging letting users know that there is a coupon, rebate, price comparison or price history available on shopping domains is also done through a horizontal banner below the address bar. The recommended state for this setting is: Disabled.

Rationale :

Shopping in Microsoft Edge shares a user"s browsing and search history to provide price comparison and coupons, which could inadvertently expose and share sensitive data with a 3rd party.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Shopping in Microsoft Edge Enabled.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users with roles that require this feature will have to perform price comparisons on their own unless exempted from this setting.

1.55. L1 Ensure Clear cached images and files when Microsoft Edge closes is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether cached images and files are deleted each time Microsoft Edge closes.Note: If this policy is disabled, do not enable the ClearBrowsingDataOnExit policy, because it will take precedence over the ClearCachedImagesAndFilesOnExit policy and will delete all browsing data when Microsoft Edge closes, regardless of how the ClearCachedImagesAndFilesOnExit policy is configured. The recommended state for this setting is: Disabled.

Rationale :

Deleting browser data on close will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Clear cached images and files when Microsoft Edge closes.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Cached images and files will not be deleted on closing and the user will be unable to change this setting.

1.56. L1 Ensure Clear history for IE and IE mode every time you exit is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls if history will be cleared for Internet Explorer (IE) and IE mode every time a user exits the browser.The recommended state for this setting is Disabled.

Rationale :

Deleting browser data will delete information that may be important for a computer investigation. Investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Clear history for IE and IE mode every time you exit.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:History will not be cleared for IE and IE mode every time a user exits the browser.

1.54. L1 Ensure Clear browsing data when Microsoft Edge closes is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether web browser data, such as forms, passwords and visited sites is deleted each time Microsoft Edge is closed.Note: If this policy is enabled, do not enable the AllowDeletingBrowserHistory policy, because it will take precedence over the ClearBrowsingDataOnExit policy and all data will be deleted when Microsoft Edge closes, regardless of how AllowDeletingBrowserHistory is configured. The Recommended state for this setting is: Disabled.

Rationale :

Deleting browser data on close will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Clear browsing data when Microsoft Edge closes.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:Browsing data will not be deleted on closing and the user will not be able to change this setting.Note: This setting will preserve browsing history that could contain a user"s personal browsing history. Ensure this setting is in compliance with organizational policies.

1.96. L1 Ensure Enable warnings for insecure forms is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls the handling of insecure forms (forms submitted over HTTP) embedded in secure (HTTPS) sites in the browser.When enabled, a full-page warning will be shown, and autofill will be disabled for those forms. When disabled, warnings will not be shown for insecure forms, and autofill will work normally.The recommended state for this setting is: Enabled.

Rationale :

The default setting of enabled warnings for insecure forms enforces secure connections when domains are capable of HTTPS and prevents auto-filling of data imported from a non-secure source.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable warnings for insecure forms.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.95. L1 Ensure Enable use of ephemeral profiles is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether user profiles are switched to ephemeral mode. In ephemeral mode, profile data is saved on disk for the length of the session and then the data is deleted after the session is over. Therefore, no data is saved to the device.The recommended state for this setting is: Disabled.

Rationale :

Allowing use of ephemeral profiles allows a user to use Microsoft Edge with no data being logged to the system. Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable use of ephemeral profiles.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.62. L1 Ensure Configure the list of names that will bypass the HSTS policy check is set to Disabled

Rule Status :

Passed

Summary :

This policy setting allows a list of names to be specified that will be exempt from HTTP Strict Transport Security (HSTS) policy checks then potentially upgraded from http:// to https://.The recommended state for this setting is: Disabled.

Rationale :
Allowing hostnames to be exempt from HSTS policy checks could allow for protocol downgrade attacks and cookie hijackings .

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled. Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure the list of names that will bypass the HSTS policy check.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:There should be no adverse effect to users.

1.93. L1 Ensure Enable site isolation for every site is set to Enabled

Rule Status :

Failed

Summary :

This policy setting ensures that each website runs in its own process so that a site will not be able to utilize or take data from another running site.The recommended state for this setting is: Enabled.

Rationale :

Enabling site isolation can help stop sites from inadvertently sharing data with other running sites. This will help protect data from untrusted sources.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable site isolation for every site.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.60. L1 Ensure Configure Related Matches in Find on Page is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies how the user receives Related Matches in Find on Page, which provides spellcheck, synonyms, and Q&A results in Microsoft Edge.Note: Disabling this setting still allows users to receive related matches in Find on Page on limited sites . The results are processed on the user´s device instead of a cloud service. The recommended setting for this policy is Disabled.

Rationale :

Sharing a user"s browsing and search history to a cloud service could inadvertently expose data. Due to privacy concerns, data should never be sent to any 3rd party.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure Related Matches in Find on Page.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not see all suggestions for better matches found on page, only from limited sites.

1.57. L1 Ensure Configure browser process code integrity guard setting is set to Enabled Enable code integrity guard enforcement in the browser process

Rule Status :

Failed

Summary :

This policy setting controls the use of code integrity guard in the browser process, which only allows Microsoft signed binaries to load.The recommended state for this setting is Enabled: Enable code integrity guard enforcement in the browser process.

Rationale :

Code Integrity Guard ensures Microsoft"s digital signature is present when loading binaries into a process. Binaries without Microsoft"s digital signature are blocked to protect the system from unknown binaries and prevent the injection of untrustworthy binaries into a process.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Enable code integrity guard enforcement in the browser process.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure browser process code integrity guard setting.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Binaries without Microsoft"s digital signature are blocked from being loaded into a process.

1.58. L1 Ensure Configure InPrivate mode availability is set to Enabled InPrivate mode disabled

Rule Status :

Failed

Summary :

This policy setting controls whether Edge InPrivate mode is available or even forced for the user.The recommended state for this setting is: Enabled: InPrivate mode disabled.

Rationale :

Disabling InPrivate mode for Microsoft Edge will ensure that browsing data is logged on the system which may be important for forensics.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: InPrivate mode disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure InPrivate mode availability.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to initiate the InPrivate browsing mode for Microsoft Edge.

1.102. L1 Ensure In-app support Enabled is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows users to contact in-app Microsoft support agents directly from the Microsoft Edge browser.The recommended state for this setting is: Disabled.

Rationale :

In-app support shares a user"s browsing and search history, which could inadvertently expose and share sensitive data with Microsoft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\In-app support Enabled.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to use or turn on the in-app support feature in the Microsoft Edge browser.

1.101. L1 Ensure Hide the First-run experience and splash screen is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether the First-run experience and splash screen is presented to the user the first time Microsoft Edge is opened. Some of the options presented to the user include the ability to import data from other web browsers on the system.The recommended state for this setting is Enabled.

Rationale :

Allowing the First-run experience and configuration options could potentially allow the user to perform actions that are prohibited such as importing autofill, credit card, and other sensitive data.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Hide the First-run experience and splash screen.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:Users will not be prompted with the First-run experience screens.

1.99. L1 Ensure Enhance the security state in Microsoft Edge is set to Enabled Balanced mode

Rule Status :

Failed

Summary :

This policy setting configures "enhance the security state" in Microsoft Edge. Enhanced security in Microsoft Edge helps safeguard against memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections for the browser. These protections include Hardware-enforced Stack Protection and Arbitrary Code Guard (ACG).Enhanced security provides two levels of browsing security: Balanced and Strict. Balanced mode is an adaptive mode that builds on a user's behavior on a particular device. Strict mode applies added security protections for all the sites a user visits. Users may report some challenges accomplishing their usual tasks when in strict mode.The recommended state for this setting is: Enabled: Balanced mode.

Rationale :

Balance mode will help reduce the risk of an attack by automatically applying stricter security settings on unfamiliar sites while adapting to browsing habits over time.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Balanced mode.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enhance the security state in Microsoft Edge.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will no longer be able to bypass protection for previously visited unfamiliar sites.Edge will apply added security protections to sites that are not visited often or are unknown. Websites that are browsed frequently will be left out.Note: Most sites will work as expected.

1.44. L1 Ensure Allow user feedback is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to utilize the Edge Feedback feature to send feedback, suggestions and surveys to Microsoft as well as issue reports.The recommended state for this setting is: Disabled.

Rationale :

Data should not be shared with 3rd party vendors in an enterprise managed environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow user feedback.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to send feedback to Microsoft.

1.85. L1 Ensure Enable globally scoped HTTP auth cache is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether HTTP auth credentials may be automatically used in the context of another web site visited in Microsoft Edge.Note: This policy is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future. The recommended state for this setting is Disabled.

Rationale :

Allowing HTTP auth credentials to be shared without the user"s consent could lead to a user sharing sensitive information without their knowledge. Enabling this setting could also lead to some types of cross-site attacks, that would allow users to be tracked across sites without the use of cookies.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable globally scoped HTTP auth cache.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.52. L1 Ensure Block tracking of users web-browsing activity is set to Enabled Balanced Blocks harmful trackers and trackers from sites user has not visited content and ads will be less personalized

Rule Status :

Failed

Summary :

This policy setting controls whether websites may track user"s web-browsing activity.The recommended state for this setting is: Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized).

Rationale :

Allowing websites to track user web-browsing activity allows for sites to gather information which could be potentially harmful and used to target users and businesses.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Balanced (Blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized).Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Block tracking of users" web-browsing activity.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Content and ads will have minimal personalization and the website may not function properly.

1.50. L1 Ensure Automatically import another browsers data and settings at first run is set to Enabled Disables automatic import and the import section of the first-run experience is skipped

Rule Status :

Failed

Summary :

This policy setting controls whether settings are imported from another browser into Microsoft Edge.Note: The browser data from Microsoft Edge Legacy will always be silently migrated at the first run, irrespective of the value of this policy. The recommended state for this setting is: Enabled: Disables automatic import, and the import section of the first-run experience is skipped.

Rationale :

Having settings automatically imported from another browser into Microsoft Edge could potentially allow for non-recommended settings to be applied temporarily creating a potential security risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Disables automatic import, and the import section of the first-run experience is skipped.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Automatically import another browser"s data and settings at first run.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.84. L1 Ensure Enable Follow service in Microsoft Edge is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows the Microsoft Edge browser to enable the follow service which allows users to follow an influencer, site, or topic in Microsoft Edge.The recommended state for this setting is: Disabled.

Rationale :

Enabling this feature will create a personalized feed in Edge's Collections section. In order to create a personalized feed, data will be collected from the browser. Due to privacy concerns, data should never be sent to any 3rd party.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable Follow service in Microsoft Edge.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to follow an influencer, site, or topic in Microsoft Edge.

1.48. L1 Ensure Allow websites to query for available payment methods is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to set whether a website can check to see if the user has payment methods saved.The recommended state for this setting is: Disabled.

Rationale :

Saving payment information in Microsoft Edge could lead to the sensitive data being leaked and used for non-legitimate purposes.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow websites to query for available payment methods.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Websites will be unable to query whether payment information within Microsoft Edge is available.

1.92. L1 Ensure Enable security warnings for command-line flags is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevents Microsoft Edge from showing security warnings that potentially dangerous command-line flags are in use at its" launch.The recommended state of this setting is "Enabled".

Rationale :

If Microsoft Edge is being launched with potentially dangerous flags this information should be exposed to the user as a warning, if not the user may unintentionally be using non-secure settings and be exposed to security flaws.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable security warnings for command-line flags.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:None - this is the default behavior.

1.89. L1 Ensure Enable renderer code integrity is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether unknown and potentially hostile code will be allowed to load inside of Microsoft Edge.The recommended state for this setting is: Enabled.

Rationale :

Disabling this setting could have a detrimental effect on Microsoft Edge"s security and stability as unknown, hostile, and/or unstable code will be able to load within the browser"s renderer processes.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable renderer code integrity.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.90. L1 Ensure Enable resolution of navigation errors using a web service is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft Edge can issue a dataless connection to a web service to probe networks, (ex: Hotel and Airport Wi-Fi) for connectivity issues.Note: Except on Windows 8 and later versions of Windows, Microsoft Edge always uses native APIs to resolve connectivity issues. The recommended state for this setting is Disabled.

Rationale :

This setting could potentially allow information about the user"s network to be disclosed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable resolution of navigation errors using a web service.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Microsoft Edge will use native APIs for potential resolution of network connectivity and navigation issues.

1.87. L1 Ensure Enable network prediction is set to Enabled Dont predict network actions on any network connection

Rule Status :

Failed

Summary :

This policy setting controls the network prediction feature which controls DNS prefetching, TCP and SSL pre-connection and pre-rendering of web pages.The recommended state for this setting is Enabled: Don"t predict network actions on any network connection.

Rationale :

Opening connections to resources that may not be used could allow un-needed connections increasing attack surface and, in some cases, could lead to opening connections to resources which the user did not intend to utilize.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Don"t predict network actions on any network connection.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable network prediction.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior, apart from users being able to change the default.

1.88. L1 Ensure Enable profile creation from the Identity flyout menu or the Settings page is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether user profiles can create new profiles in Microsoft Edge.The recommended state for this setting is: Disabled.

Rationale :

Allowing users to create new profiles could allow for such profiles to be removed or switched which may end up in a situation that hides or even removes data which may be important for computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable profile creation from the Identity flyout menu or the Settings page.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to utilize the Add profile option in Microsoft Edge.

1.77. L1 Ensure Enable AutoFill for payment instructions is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users can utilize payment information, such as credit or debit cards in web forms using previously stored information.The recommended state for this setting is: Disabled.

Rationale :

Having payment information stored and auto filled in Microsoft Edge could allow for an attacker to gain access to this sensitive data.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable AutoFill for credit cards.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named AutoFill for credit cards , but it was renamed to Enable AutoFill for payment instructions . Impact:Users will be unable to use and store AutoFill data for credit and debit card information in Microsoft Edge.

1.33. L1 Ensure Allow importing of saved passwords is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to import saved passwords from another browser into Microsoft Edge as well as whether passwords are imported on first use.The recommended state for this setting is Disabled.

Rationale :

Having saved passwords automatically imported or allowing users to import password data from another browser into Microsoft Edge allows for sensitive data to be imported into Edge.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing saved passwords.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to import saved passwords from other browsers into Microsoft Edge.

1.78. L1 Ensure Enable browser legacy extension point blocking is set to Enabled

Rule Status :

Failed

Summary :

This policy setting sets the ProcessExtensionPointDisablePolicy on Microsoft Edge´s browser process to block code injection from legacy third party applications. Note: Per Microsoft, only turn off the policy if there are compatibility issues with third-party software that must run inside Microsoft Edge´s browser process. The recommended state for this setting is: Enabled.

Rationale :

If this policy is set to Disabled, it may have a detrimental effect on Microsoft Edge´s security and stability as unknown and potentially hostile code can load inside Microsoft Edge´s browser process.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable browser legacy extension point blocking.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:Compatibility issues with third-party software can occur.

1.34. L1 Ensure Allow importing of search engine settings is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to import search engine settings from another browser into Microsoft Edge as well as whether said setting is imported on first use.The recommended state for this setting is Disabled.

Rationale :

Having search engine settings automatically imported or allowing users to import the settings from another browser into Microsoft Edge could allow for a malicious search engine to be set.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing search engine settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to perform an import of their search engine settings from other browsers into Microsoft Edge.

1.75. L1 Ensure DNS interception checks enabled is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether a local switch is configured for DNS interception checks. These checks attempt to discover if the browser is behind a proxy that redirects unknown host names.Note: This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on start-up and each DNS configuration change. The recommended state for this setting is: Enabled.

Rationale :

Disabling these checks could potentially allow DNS hijacking and poisoning.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\DNS interception checks enabled.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.76. L1 Ensure Enable AutoFill for addresses is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether the AutoFill feature of Microsoft Edge is enabled for the auto-complete feature for addresses and other information in web forms.The recommended state for this setting is: Disabled.

Rationale :

Allowing autofill data to be saved in Microsoft Edge could potentially allow storage of sensitive data such as personally identifiable information (PII). Considering that storage of sensitive data should be handled with care disabling this setting is recommended.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable AutoFill for addresses.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to store autofill address information in Microsoft Edge and they will also not be prompted to use such information on webforms. Disabling this setting also stops any past activity of autofill.

1.73. L1 Ensure Disable saving browser history is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether browser history is saved and prevents users from changing the policy.The recommended state for this setting is: Disabled.

Rationale :

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Disable saving browser history.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.Note: This setting will preserve browsing history that could contain a user"s personal browsing history. Ensure this setting is in compliance with organizational policies.

1.74. L1 Ensure Disable synchronization of data using Microsoft sync services is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether data synchronization with Microsoft sync services is allowed as well as whether the sync consent prompt appears to users. Examples of synced data include, but are not limited to, history and favorites.The recommended state for this setting is: Enabled.

Rationale :
Data should not be shared with third party vendors in an enterprise-managed environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Disable synchronization of data using Microsoft sync services.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to sync data with Microsoft, the prompt for sync consent will also be hidden from the user.

1.118. L1 Ensure Suggest similar pages when a webpage cant be found is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft Edge may connect to a web service to generate URLs and search suggestions for website connectivity issues. If disabled standard errors will be issued, if enabled errors will be customized with URL suggestions.The recommended state for this setting is Disabled.

Rationale :

This setting could potentially lead to a leak of information regarding the types of websites being visited, it may also open users up to redirection to a malicious site in the event that the service generating information becomes compromised.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Suggest similar pages when a webpage can’t be found.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will still be presented with an error if a website cannot be reached however, the message may be more generic than the user would get in the instance of this service being enabled.

1.41. L1 Ensure Allow remote debugging is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users may use remote debugging. This feature allows remote debugging of live content on a Windows 10 or later device from a Windows or macOS computer.The recommended state for this setting is: Disabled.

Rationale :

Disabling remote debugging enhances security and protects applications from unauthorized access. Some attack tools can exploit this feature to extract information, or to insert malicious code.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow remote debugging.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able access the remote debugging feature in Microsoft Edge.

1.119. L1 Ensure Suppress the unsupported OS warning is set to Disabled

Rule Status :

Failed

Summary :

This policy setting suppresses the warning that appears when Microsoft Edge is running on a computer or operating system that is no longer supported. If this policy is disabled or unset, the warnings will appear on such unsupported computers or operating systems.The recommended state for this setting is: Disabled.

Rationale :

Users will be notified if the Operating System software is no longer supported.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Microsoft Edge\Suppress the unsupported OS warning.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - This is the default behavior.

1.42. L1 Ensure Allow the audio sandbox to run is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether audio processes in Microsoft Edge run in a sandbox.Note: Security software setups within your environment might interfere with the sandbox. The recommended state for this setting is: Enabled.

Rationale :

Having audio processes run in a sandbox ensures that if a website misuses audio processes that data may not be manipulated or exfiltrated from the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow the audio sandbox to run.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

1.39. L1 Ensure Allow personalization of ads Microsoft Edge search news and other Microsoft services by sending browsing history favorites and collections usage and other browsing data to Microsoft is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft is able to collect a user"s browsing history and searches in Microsoft Edge for the purpose of personalizing searches, news, and other Microsoft services.The recommended state for this setting is: Disabled.

Rationale :

Sharing a user"s browsing and search history could inadvertently expose data which should be protected.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow personalization of ads, Microsoft Edge, search, news and other Microsoft services by sending browsing history, favorites and collections, usage and other browsing data to Microsoft.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users" data will not be shared with Microsoft and the personalization of searches, news, etc. will not be available.

1.117. L1 Ensure Standalone Sidebar Enabled is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users will have the ability to activate the standalone sidebar. The standalone sidebar is an optional mode for the sidebar in Microsoft Edge and uses Bing AI. When this mode is activated by a user, the sidebar appears in a fixed position on the Microsoft Windows desktop and is hidden from the browser application frame.The recommended state for this setting is Disabled.

Rationale :

Microsoft Edge determines what data to send to Bing AI based on the user"s query and their consent to share data with Microsoft. This could allow data to be transmitted to a third-party cloud service. This could lead to sensitive data being exposed. Bing AI offers various features, such as summarizing financial reports, comparing financials of different companies, and aiding users in creating and editing content which could also lead to sensitive data being exposed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Standalone Sidebar Enabled.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to access the HubsSidebarEnabled (Show Hubs Sidebar) and it will also prevent them from accessing standalone sidebar and using the Bing AI feature.

1.40. L1 Ensure Allow queries to a Browser Network Time service is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft Edge can send queries to a network time service for accurate timestamps. This check helps in validation of certificates.The recommended state for this setting is: Enabled.

Rationale :

Microsoft Edge uses a network time service to randomly track times from a trusted external service. This allows Microsoft Edge the ability for verification of a certificate"s validity and is important for certificate validation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow queries to a Browser Network Time service.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:None - this is the default behavior.

1.114. L1 Ensure Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether SharedArrayBuffers can be used in a non-cross-origin-isolated context. A SharedArrayBuffer is a binary data buffer that can be used to create views on shared memory. SharedArrayBuffers have a memory access vulnerability in several popular CPUs.The recommended state for this setting is: Disabled.

Rationale :

Disabling this policy prevents attackers from being able to exploit memory access vulnerabilities found in popular CPUs.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users may experience slightly slower loading of webpages.

1.81. L1 Ensure Enable deleting browser and download history is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether users can delete browser and download history for Microsoft Edge.Note: Even when this policy disabled, the browsing and download history aren"t guaranteed to be retained. Users can edit or delete the history database files directly, and the browser itself may remove (based on expiration period) or archive any or all history items at any time. The recommended state for this setting is Disabled.

Rationale :

Deleting browser data will delete information that may be important for a computer investigation. Investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable deleting browser and download history.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.
Impact:Browser data deletion by users will be prohibited.Note: This setting will preserve browsing history that could contain a user"s personal browsing history. Ensure this setting is in compliance with organizational policies.

1.122. L1 Ensure Wait for Internet Explorer mode tabs to completely unload before ending the browser session is set to Disabled

Rule Status :

Failed

Summary :

This policy setting causes Microsoft Edge to continue running until all Internet Explorer tabs have completely finished unloading. This allows Internet Explorer plugins like ActiveX controls to perform additional critical work even after the browser has been closed.The recommended state for this setting is Disabled.

Rationale :

Enabling this policy can cause stability and performance issues, and Microsoft Edge processes may remain active in the background with no visible windows if the webpage or plugin prevents Internet Explorer from unloading. This policy should only be used if your organization depends on a plugin that requires this behavior.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Wait for Internet Explorer mode tabs to completely unload before ending the browser session.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.67. L1 Ensure Control communication with the Experimentation and Configuration Service is set to Enabled Disable communication with the Experimentation and Configuration Service

Rule Status :

Failed

Summary :

This policy setting controls whether Microsoft Edge uses the Experimentation and Configuration Service to deploy the Experimentation and Configuration payload which consists of a list of early in development features that Microsoft is enabling for testing and feedback.The recommended state for this setting is: Enabled: Disable communication with the Experimentation and Configuration Service.

Rationale :

This setting allows feedback (data) to be sent back to a third-party for testing of development features for Microsoft Edge, and can also deliver a payload that contains a list of actions to take on certain domains for compatibility reasons.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Disable communication with the Experimentation and Configuration Service.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Control communication with the Experimentation and Configuration Service.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Data will not be sent back to a third-party and payloads will not be delivered.

1.23. L1 Ensure Ads setting for sites with intrusive ads is set to Enabled Block ads on sites with intrusive ads

Rule Status :

Failed

Summary :

This setting controls whether ads are blocked on sites with intrusive ads. Intrusive ads are typically ads that push invasive, unwelcomed, and irrelevant ads in front of consumers. These ads can pop up unexpectedly, block the host page, open new pages and windows, or play video and audio at inopportune times.The recommended state for this setting is: Enabled: Block ads on sites with intrusive ads.

Rationale :

Intrusive ads are ads found on websites that are invasive or unwelcome. These ads can contain malicious files or can fool an unknowing user into giving away their username and/or password.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Block ads on sites with intrusive ads.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Ads setting for sites with intrusive ads.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Ads that may be non-intrusive can be blocked.

1.64. L1 Ensure Configure the Share experience is set to Enabled Dont allow using the Share experience

Rule Status :

Failed

Summary :

This policy setting allows users to be able to access the Share experience from the Settings and More menu in Microsoft Edge, which can allow information to be shared with other apps on the system. The recommended state for this setting is: Enabled: Don"t allow using the Share experience.

Rationale :

Having this setting enabled could allow malicious content from Microsoft Edge to be exposed to other parts of the operating system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Don"t allow using the Share experience.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure the Share experience.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from Microsoft here. Impact:Users will not be able to view or use the Share button in the toolbar as it will be hidden.

1.65. L1 Ensure Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode is set to Enabled Do not send form data or headers

Rule Status :

Failed

Summary :

This policy setting configures navigations that switch between Internet Explorer mode and Microsoft Edge will include form data. IE Mode in Microsoft Edge allows organizations that still need Internet Explorer 11, (which is not supported) for backward compatibility with existing websites.Available policy options: IncludeNone (0)= Do not send form data or headers IncludeFormDataOnly (1)= Send form data only IncludeHeadersOnly (2)= Send additional headers only IncludeFormDataAndHeaders (3)= Send form data and additional headers The recommended state for this setting is: Enabled: Do not send form data or headers.

Rationale :

Allowing autofill data to be imported could potentially allow sensitive data, such as personally identifiable information (PII) to be exposed. Storage of sensitive data should be handled with care and not stored within the browser.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Do not send form data or headers.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:When entering or exiting IE mode, form data and headers will not be shared between Internet Explorer mode and Microsoft Edge and vice versa.

1.63. L1 Ensure Configure the list of types that are excluded from synchronization is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to specify data types that will be limited/excluded from uploading data to the Microsoft Edge synchronization service.The recommended state for this setting is: Enabledwith the following CASE SENSITIVE datatype passwords. Note: In a High Security/Sensitive Data Environment (L2), this setting should also include the following options: settings, favorites, addressesAndMore, extensionsand collections.

Rationale :

Storing and sharing information could potentially expose sensitive information including but not limited to user passwords and login information. Allowing this synchronization could also potentially allow an end user to pull corporate data that was synchronized into the cloud to a personal machine.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabledwith the following CASE SENSITIVE datatype passwords.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Configure the list of types that are excluded from synchronization.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Password data will not be synchronized with the Azure AD Tenant.

1.107. L1 Ensure Restrict exposure of local IP address by WebRTC is set to Enabled Allow public interface over http default route. This doesnt expose the local IP address

Rule Status :

Failed

Summary :

This policy setting specifies whether the local IP address will be exposed by WebRTC.The recommended state for this setting is Enabled: Allow public interface over http default route. This doesn"t expose the local IP address.

Rationale :

Allowing the exposure of IP addresses allows the attacker to gather information on the internal network that could potentially be utilized to breach and traverse the network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Allow public interface over http default route. This doesn"t expose the local IP address.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Restrict exposure of local IP address by WebRTC.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:The local IP address will not be exposed.

1.30. L1 Ensure Allow importing of browser settings is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to import settings from another browser into Microsoft Edge.The recommended state for this setting is Disabled.

Rationale :

Having settings automatically imported or allowing users to import settings from another browser into Microsoft Edge could potentially allow for non-recommended settings to be applied temporarily creating a potential security risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing of browser settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to perform an import of other browser settings into Microsoft Edge.

1.108. L1 Ensure Set disk cache size in bytes is set to Enabled 250609664

Rule Status :

Failed

Summary :

This setting controls the size of the cache, in bytes, used to store files on the disk.Note: The value specified in this policy isn"t a hard boundary but rather a suggestion to the caching system; any value below a few megabytes is too small and will be rounded up to a reasonable minimum.
Note #2: The recommended disk size for cache is 50 - 250MB, according to Microsoft. The recommended state for this setting is: Enabled: 250609664.

Rationale :

Having enough disk space for browser cache is important for a computer investigation and investigators such as Computer Forensics Analysts to be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 250609664.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Set disk cache size, in bytes.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact:Browser cache will take up to 250MB in disk space.

1.31. L1 Ensure Allow importing of home page settings is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to import homepage settings from another browser into Microsoft Edge as well as whether homepage settings are imported on first use.The recommended state for this setting is Disabled.

Rationale :

Having settings automatically imported or allowing users to import settings from another browser into Microsoft Edge could potentially allow for non-recommended settings to be applied temporarily creating a potential security risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing of home page settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to import homepage settings from other browsers into Microsoft Edge.

1.105. L1 Ensure Manage exposure of local IP addresses by WebRTC is set to Disabled

Rule Status :

Passed

Summary :

This policy setting specifies a list of URLs or patterns which local IP address will be exposed by WebRTC.Note: If this policy is enabled, disabled, or not configured, and edge://flags/#enable-webrtc-hide-local-ips-with-mdns is Disabled, WebRTC will expose local IP addresses. The recommended state for this setting is: Disabled.

Rationale :

Enabling this setting and allowing exposure of IP addresses can allow an attacker to gather information about the internal network that could potentially be utilized to breach and traverse a network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Manage exposure of local IP addressess by WebRTC.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.72. L1 Ensure Delete old browser data on migration is set to Disabled

Rule Status :

Failed

Summary :

This policy controls whether web browser data is deleted after migration to Microsoft Edge, this data includes forms, passwords, and visited sites.The recommended state for this setting is: Disabled.

Rationale :

Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Delete old browser data on migration.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Browsing data will not be deleted during migration.

1.28. L1 Ensure Allow import of data from other browsers on each Microsoft Edge launch is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls if users will get a prompt following each Microsoft Edge launch to import their data from other browsers. Microsoft Edge will import data such as passwords, bookmarks, cookies, browsing history, and payment information depending on which browser this data is being imported from. At this time Microsoft Edge can only import data from Google Chrome, Mozilla Firefox, Internet Explorer, and some 3rd party Password Managers.The recommended state for this setting is Disabled.

Rationale :

Allowing users to import data from another browser into Microsoft Edge could allow for sensitive data to be imported into Edge.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow import of data from other browsers on each Microsoft Edge launch.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from Microsoft from Download Edge for Business.

Impact:Users will not get a prompt to import their data from other browsers after each Microsoft Edge launch.

1.106. L1 Ensure Notify a user that a browser restart is recommended or required for pending updates is set to Enabled Required - Show a recurring prompt to the user indicating that a restart is required

Rule Status :

Failed

Summary :

This setting determines whether a notification to restart Microsoft Edge due to an update is recommended or required.Note: If this setting is set to Enabled: Required - Show a recurring prompt to the user indicating that a restart is requiredthe browser will be automatically restarted based on the RelaunchNotificationPeriod setting which is recommended to be 24 hours. The recommended state for this setting is: Enabled: Required - Show a recurring prompt to the user indicating that a restart is required.

Rationale :

The end-user will receive a notification informing them that an update has been applied and that the browser must be restarted for the update to be completed. Once updates have been pushed by the organization it is pertinent that the update is applied as soon as possible. Enabling this notification will ensure that users restart their browser in a timely fashion.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Required - Show a recurring prompt to the user indicating that a restart is required.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Notify a user that a browser restart is recommended or required for pending updates.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/adml that can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact: When updates are applied by an organization the end-user will receive a notification after 24 hours that they must restart the browser for updates to complete, after 24 hours the browser will be automatically restarted.

1.29. L1 Ensure Allow importing of autofill form data is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls the user"s ability to import autofill data from other browsers into Microsoft Edge.The recommended state for this setting is Disabled.

Rationale :

Allowing autofill data to be imported could potentially allow sensitive data such as personally identifiable information (PII) from a non-secured source into Microsoft Edge. Storage of sensitive data should be handled with care.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing of autofill form data.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to perform an import of autofill data during Microsoft Edge first run. This will also prevent users from importing data after Microsoft Edge has been set up.

1.27. L1 Ensure Allow Google Cast to connect to Cast devices on all IP addresses is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether Google Cast is able to connect to all IP Addresses or only private IP Addresses as defined in RFC1918 (IPv4) and RFC4193 (IPv6).Note: If the EnabledMediaRouter policy is set to Disabled there is no positive or negative effect for this setting. The recommended state for this setting is Disabled.

Rationale :

Allowing Google Cast to connect to public IP addresses could allow media and other potentially sensitive data to be exposed to the public. Disabling this setting will ensure that Google Cast is only able to connect to private (ie: internal) IP addresses.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow Google Cast to connect to Cast devices on all IP addresses.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact:If this setting is set to Disabled there will be no effect to the user, as the default behavior of Not Configured has the same behavior as disabling the setting.

1.24. L1 Ensure Allow download restrictions is set to Enabled Block malicious downloads

Rule Status :

Failed

Summary :

This policy controls whether Microsoft Edge blocks certain types of downloads, and prevents users from bypassing security warnings, depending on the classification of Safe Browsing.If this policy is not configured the default state of "No special restrictions" will be used, and the downloads will go through the usual security restrictions based on Microsoft Defender SmartScreen analysis results if it is used.Note: These restrictions only apply to downloads from web page content, as well as the "download link..." context menu option. These restrictions don"t apply to saving or downloading the currently displayed page, nor do they apply to the Save as PDF option from the printing options. For more information on Microsoft Defender

SmartScreen, please visit Microsoft Defender SmartScreen Frequently Asked Questions. Note #2: Microsoft Edge relies on the Internet Explorer zones (Local Machine, Local Intranet, Trusted, Internet, Restricted) to determine which sites may bypass this policy setting. Please see Security Zones in Edge – text/plain.or more information. The recommended state for this setting is: Enabled: Block malicious downloads.

Rationale :

Downloads can contain malware that has the potential to exfiltrate sensitive data or encrypt critical systems for ransom.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Block malicious downloads.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow download restrictions.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft.

Impact:Users will be prevented from downloading certain types of files and will not be able to bypass security warnings.

1.112. L1 Ensure Show Microsoft Rewards experiences is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether the Microsoft Reward experience is available to users and if notifications are received. The Microsoft Rewards experience is a free program that allows the user to earn points when searching on Bing.com. With these points, the users can buy merchandise from the Microsoft Store online and in Windows 10.Note: The Bing Rewards experience was merged with the Microsoft Reward experience in 2016. The recommended state for this setting is Disabled.

Rationale :

Due to privacy concerns, data should never be sent to or tracked by any 3rd party since this data could contain sensitive information.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Show Microsoft Rewards experiences.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:The Microsoft Rewards experience will not show in the Microsoft Edge user profile.

1.109. L1 Ensure Set the time period for update notifications is set to Enabled 86400000

Rule Status :

Failed

Summary :

This setting does not determine if updates are applied, the policy setting allows setting a time period in which users are notified that Microsoft Edge has been updated and must be closed and re-opened.The recommended state for this setting is: Enabled: 86400000.

Rationale :

This setting is a notification for the end-user informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that said update takes affect as soon as possible. Enabling this notification will ensure users restart the browser in a timely fashion.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 86400000.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Set the time period for update notifications.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:When updates are applied by an organization the end-user will receive a notification after 24 hours that they must restart the browser for updates to complete.

1.32. L1 Ensure Allow importing of payment info is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users are able to import payment information from another browser into Microsoft Edge as well as whether payment information is imported on first use.The recommended state for this setting is Disabled.

Rationale :

Having payment information automatically imported or allowing users to import payment data from another browser into Microsoft Edge could allow for sensitive data to be imported into Edge.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow importing of payment info.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will be unable to perform a payment information import from other browsers into Microsoft Edge.

1.80. L1 Ensure Enable CryptoWallet feature is set to Disabled

Rule Status :

Failed

Summary :

The CryptoWallet feature allows users to securely store, manage, and transact digital assets such as Bitcoin, Ethereum, and other cryptocurrencies.The recommended state for this setting is Disabled.

Rationale :

In an enterprise organization, users should not be able to manage, buy or sell assets such as Bitcoin, Ethereum, and other cryptocurrencies.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable CryptoWallet feature.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from Microsoft from Download Edge for Business. Impact:The CryptoWallet feature will not be accessible to users.

1.66. L1 Ensure Continue running background apps after Microsoft Edge closes is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether processes from Microsoft Edge may start at Operating System sign-in and continue running once an Edge browser window is closed. This allows background apps and the current browsing session to remain active, including any session cookies. An open background process displays an icon in the system tray and can always be closed from there.The recommended state for this setting is: Disabled.

Rationale :

Allowing processes from the browser to run in the background could allow a malicious script or code to continue running even once the browser windows has been closed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Continue running background apps after Microsoft Edge closes.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:The browser will close its processes and will not continue running as a background process.

1.82. L1 Ensure Enable Discover access to page contents for AAD profiles is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls discover access to page contents for AAD profiles. Discover is an extension that hosts Bing Chat and in order to summarize pages and interact with text selections, it needs to be able to access the page contents. When enabled, page contents will be sent to Bing.The recommended state for this setting is Disabled.

Rationale :

Enabling this policy setting allows data to be transmitted to a third-party (BING), which could lead to sensitive data being exposed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable Discover access to page contents for AAD profiles.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Discover will not be able to access page contents and therefore Bing Chat will not be able to summarize pages and interact with text selections.

1.79. L1 Ensure Enable component updates in Microsoft Edge is set to Enabled

Rule Status :

Failed

Summary :

This policy determines whether updates for Microsoft Edge components are enabled in Microsoft Edge.Note: Updates that are deemed "critical for security" are still applied even if you disable this policy as well as any component that doesn"t contain executable code, that doesn"t significantly alter the behavior of the browser. The recommendation state for this setting is: Enabled.

Rationale :

Component updates should always be up to date to ensure the latest security patches and capabilities are applied.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Enable component updates in Microsoft Edge.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from Microsoft here. Impact:Updates will be automatically downloaded.

1.35. L1 Ensure Allow managed extensions to use the Enterprise Hardware Platform API is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows extensions installed by enterprise policies to be allowed to use the Enterprise Hardware Platform API. This API handles requests from extensions for the manufacturer and model of the hardware platform where the browser is running.The recommended state for this setting is Disabled.

Rationale :

Allowing extensions to access the Enterprise Hardware Platform API could lead to the system being compromised. It is recommended that this setting is disabled unless otherwise directed by Enterprise policies.

How to fix :

To establish the recommended configuration via GP, set the following UI path to DisabledComputer Configuration\Policies\Administrative Templates\Microsoft Edge\Allow managed extensions to use the Enterprise Hardware Platform API.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:None - this is the default behavior.

1.113. L1 Ensure Show the Reload in Internet Explorer mode button in the toolbar is set to Disabled

Rule Status :

Failed

Summary :

This policy setting shows the Reload in Internet Explorer mode button in the toolbar. IE Mode in Microsoft Edge allows organizations that still need Internet Explorer 11, (which is not supported) for backward compatibility with existing websites.Note: The button will only be shown on the toolbar when the InternetExplorerIntegrationReloadInIEModeAllowed (Allow unconfigured sites to be reloaded in Internet Explorer mode) policy is enabled (which is set to disabled in the benchmark). The recommended state for this setting is: Disabled.

Rationale :

Internet Explorer is officially retired and unsupported. Allowing browsers to reconfigure into Internet Explorer mode could open an organization up to malicious sites due to its lack of support for modern security features.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Microsoft Edge\Show the Reload in Internet Explorer mode button in the toolbar.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:Users will not be able to see or use the Internet Explorer Mode toolbar.

3.1.1. L1 Ensure Update policy override default is set to Enabled Always allow updates recommended

Rule Status :

Failed

Summary :

This policy settings sets the default behavior for all channels concerning the way Microsoft Edge Update handles available updates for Microsoft Edge.Note: This setting can be overridden for individual channels by specifying the Update policy override policy for those specific channels. NOTE #2: This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain. The recommended state for this setting is: Enabled: Always allow updates (recommended).

Rationale :

Applying software updates as soon as they become available can ensure that systems will always have the most recent critical updates installed.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Always allow updates (recommended)or Enabled: Automatic silent updates only.Computer Configuration\Polices\Administrative Templates\Microsoft Edge Update\Applications\Update policy override default.Impact:The latest Microsoft Edge updates are automatically installed. Enterprises that use other means of patching systems will need to exclude this recommendation from the benchmark.

3.3.1. L1 Ensure Auto-update check period override is set to any value except 0

Rule Status :

Failed

Summary :

This policy setting configures the minimum number of minutes between automatic update checks.The recommended state for this setting is: any value except 0.

Rationale :

Automatic updates can help ensure that the computers in the environment will always have the most recent critical updates and can decrease the amount of time the system will remain vulnerable between updates and patches.

How to fix :

To establish the recommended configuration via GP, set the following UI path to any value except 0.Computer Configuration\Policies\Administrative Templates\Microsoft Edge Update\Preferences\Auto-update check period override.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MSEdge.admx/admlthat can be downloaded from: Download Microsoft Edge for Business - Microsoft. Impact:If using a third-party for patching, an exception to this recommendation will be needed.

CIS Google Chrome Benchmark v3.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)

1 Enforced Defaults	**8/29 passed**
1.1 HTTP authentication	**0/1 passed**
1.1.1. L1 Ensure Cross-origin HTTP Authentication prompts is set to Disabled	Failed
1.2 Safe Browsing settings	**1/2 passed**
1.2.2. L1 Ensure Safe Browsing Protection Level is set to Enabled Safe Browsing is active in the standard mode. or higher	Unscored
1.2.1. L1 Ensure Configure the list of domains on which Safe Browsing will not trigger warnings is set to Disabled	Passed
1.18. L1 Ensure Enable security warnings for command-line flags is set to Enabled	Failed
1.9. L1 Ensure Determine the availability of variations is set to Enable all variations	Unscored
1.17. L1 Ensure Enable online OCSPCRL checks is set to Disabled	Failed
1.10. L1 Ensure Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities is set to Disabled	Passed
1.11. L1 Ensure Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes is set to Disabled	Passed
1.12. L1 Ensure Disable Certificate Transparency enforcement for a list of URLs is set to Disabled	Passed
1.16. L1 Ensure Enable globally scoped HTTP auth cache is set to Disabled	Failed
1.23. L1 Ensure Import of homepage from default browser on first run is set to Disabled	Failed
1.6. L1 Ensure Ask where to save each file before downloading is set to Enabled	Failed
1.22. L1 Ensure Import autofill form data from default browser on first run is set to Disabled	Failed
1.21. L1 Ensure Ephemeral profile is set to Disabled	Failed
1.7. L1 Ensure Continue running background apps when Google Chrome is closed is set to Disabled	Failed
1.20. L1 Ensure Enables managed extensions to use the Enterprise Hardware Platform API is set to Disabled	Failed
1.29. L1 Ensure URLs for which local IPs are exposed in WebRTC ICE candidates is set to Disabled	Passed
1.28. L1 Ensure Suppress the unsupported OS warning is set to Disabled	Failed
1.13. L1 Ensure Disable saving browser history is set to Disabled	Failed
1.14. L1 Ensure DNS interception checks enabled is set to Enabled	Failed
1.15. L1 Ensure Enable component updates in Google Chrome is set to Enabled	Failed
1.27. L1 Ensure Suppress lookalike domain warnings on domains is set to Disabled	Passed
1.4. L1 Ensure Allow queries to a Google time service is set to Enabled	Failed
1.3. L1 Ensure Allow Google Cast to connect to Cast devices on all IP addresses is set to Disabled	Failed
1.19. L1 Ensure Enable third party software injection blocking is set to Enabled	Failed
1.26. L1 Ensure Origins or hostname patterns for which restrictions on insecure origins should not apply is set to Disabled	Passed
1.25. L1 Ensure List of names that will bypass the HSTS policy check is set to Disabled	Passed
1.24. L1 Ensure Import search engines from default browser on first run is set to Disabled	Failed
1.5. L1 Ensure Allow the audio sandbox to run is set to Enabled	Failed
2 Attack Surface Reduction	**2/37 passed**
2.10 Microsoft Active Directory Management Settings	**0/1 passed**
2.10.1. L1 Ensure Allow automatic sign-in to Microsoft cloud identity providers Is Enabled	Unscored

2.1 Update settings Google section of GPO	**0/1 passed**
2.1.1. L1 Ensure Update policy override is set to Enabled with Always allow updates recommended or Automatic silent updates specified	Failed
2.2 Content settings	**1/2 passed**
2.2.5. L1 Ensure Allow local file access to file URLs on these sites in the PDF Viewer Is Disabled	Passed
2.2.1. L1 Ensure Control use of insecure content exceptions is set to Enabled Do not allow any site to load mixed content	Failed
2.3 Extensions	**0/5 passed**
2.3.7. L1 Ensure Control availability of extensions unpublished on the Chrome Web Store Is Disabled	Failed
2.3.3. L1 Ensure Configure extension installation blocklist is set to Enabled	Failed
2.3.5. L1 Ensure Block third-party storage partitioning for these origins Is Configured	Unscored
2.3.1. L1 Ensure Blocks external extensions from being installed is set to Enabled	Failed
2.3.2. L1 Ensure Configure allowed appextension types is set to Enabled extension hosted app platform app theme	Failed
2.6 Password manager	**0/1 passed**
2.6.1. L1 Ensure Enable saving passwords to the password manager is Explicitly Configured	Unscored
2.7 Printing	**0/1 passed**
2.7.1. L1 Ensure Enable Google Cloud Print Proxy is set to Disabled	Failed
2.8 Remote access Chrome Remote Desktop	**0/7 passed**
2.8.5. L1 Ensure Enable firewall traversal from remote access host is set to Disabled	Failed
2.8.4. L1 Ensure Enable curtaining of remote access hosts is set to Disabled	Failed
2.8.7. L1 Ensure Enable the use of relay servers by the remote access host is set to Disabled.	Failed
2.8.6. L1 Ensure Enable or disable PIN-less authentication for remote access hosts is set to Disabled	Failed
2.8.1. Ensure Allow remote access connections to this machine is set to Disabled	Unscored
2.8.2. L1 Ensure Allow remote users to interact with elevated windows in remote assistance sessions is set to Disabled	Failed
2.8.3. L1 Ensure Configure the required domain names for remote access clients is set to Enabled with a domain defined	Unscored
2.9 First-Party Sets Settings	**0/1 passed**
2.9.1. L1 Ensure Enable First-Party Sets Is Disabled	Unscored
2.24. L1 Ensure Keep browsing data when creating enterprise profile by default Is Enabled	Failed
2.22. L1 Ensure Enable TLS Encrypted ClientHello Is Enabled	Failed
2.16. L1 Ensure Notify a user that a browser relaunch or device restart is recommended or required is set to Enabled Show a recurring prompt to the user indication that a relaunch is required	Failed
2.30. L1 Ensure Enable Renderer App Container Is Enabled	Failed
2.17. L1 Ensure Proxy settings is set to Enabled and does not contain ProxyMode auto detect	Failed
2.31. L1 Ensure Enable strict MIME type checking for worker scripts Is Enabled	Failed
2.27. L1 Ensure Http Allowlist Is Properly Configured	Unscored
2.26. L1 Ensure Enable Google Search Side Panel Is Disabled	Failed
2.11. L1 Ensure Allow download restrictions is set to Enabled Block malicious downloads	Failed
2.13. L1 Ensure Disable proceeding from the Safe Browsing warning page is set to Enabled	Failed

2.14. L1 Ensure Require Site Isolation for every site is set to Enabled	Failed
2.21. L1 Ensure Allow reporting of domain reliability related data Is Disabled	Failed
2.20. L1 Ensure Allow Web Authentication requests on sites with broken TLS certificates Is Disabled	Failed
2.29. L1 Ensure Insecure Hashes in TLS Handshakes Enabled Is Disabled	Failed
2.19. L1 Ensure Set the time period for update notifications is set to Enabled 86400000	Failed
2.25. L1 Ensure Allow file or directory picker APIs to be called without prior user gesture Is Disabled	Passed
2.32. Ensure Allow remote debugging is set to Disabled	Failed
2.28. L1 Ensure Enable automatic HTTPS upgrades Is Enabled	Failed
3 Privacy	**0/13 passed**
3.1 Content settings	**0/1 passed**
3.1.2. L1 Ensure Default geolocation setting is set to Enabled Do not allow any site to track the users physical location	Failed
3.2 Google Cast	**0/1 passed**
3.2.1. L1 Ensure Enable Google Cast is set to Disabled	Failed
3.11. L1 Ensure Enable or disable spell checking web service is set to Disabled	Failed
3.12. L1 Ensure Enable reporting of usage and crash-related data is set to Disabled	Failed
3.16. L1 Ensure Enable URL-keyed anonymized data collection is set to Disabled	Failed
3.6. L1 Ensure Control how Chrome Cleanup reports data to Google is set to Disabled	Failed
3.3. L1 Ensure Allow websites to query for available payment methods is set to Disabled	Failed
3.7. L1 Ensure Disable synchronization of data with Google is set to Enabled	Failed
3.8. L1 Ensure Enable alternate error pages is set to Disabled	Failed
3.4. L1 Ensure Block third party cookies is set to Enabled	Failed
3.13. L1 Ensure Enable Safe Browsing for trusted sources is set to Disabled	Failed
3.9. L1 Ensure Enable deleting browser and download history is set to Disabled	Failed
3.10. L1 Ensure Enable predict network actions is set to Enabled Do not predict actions on any network connection	Failed
4 Data Loss Prevention	**0/7 passed**
4.2 Content settings	**0/3 passed**
4.2.3. L1 Ensure Allow clipboard for these sites Is Configured 4.2.4. L1 Ensure	Unscored
Block clipboard on these sites Is Configured 4.2.5. L1 Ensure Default	Unscored
clipboard setting Is Enabled to Deny Permissions	Failed
4.9. L1 Ensure Enable AutoFill for credit cards is set to Disabled	Failed
4.10. L1 Ensure Import saved passwords from default browser on first run is set to Disabled	Failed
4.11. L1 Ensure List of types that should be excluded from synchronization is set to Enabled passwords	Failed
4.6. L1 Ensure Allow user feedback is set to Disabled	Failed
5 Forensics Post Incident	**0/1 passed**
5.3. L1 Ensure Set disk cache size in bytes is set to Enabled 250609664	Failed

1.1.1. L1 Ensure Cross-origin HTTP Authentication prompts is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether third-party sub-content can open a HTTP Basic Auth dialog and is typically disabled.The recommended state for this setting is: Disabled(0)

Rationale :
This setting is typically disabled to help combat phishing attempts.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\HTTP authentication\Cross-origin HTTP Authentication prompts.Impact:None - This is the default behavior.

1.2.2. L1 Ensure Safe Browsing Protection Level is set to Enabled Safe Browsing is active in the standard mode. or higher

Rule Status :

Unscored

Summary :

Control whether Google Chrome"s Safe Browsing feature is enabled and the mode in which it operates. If you set this setting as mandatory, users cannot change or override the Safe Browsing setting in Google Chrome.If this setting is left not set, Safe Browsing will operate in Standard Protection mode but users can change this setting. No Protection(0): Safe Browsing is never active. Standard Protection(1): Safe Browsing is active in the standard mode. Enhanced Protection(2): Safe Browsing is active in the enhanced mode. This mode provides better security, but requires sharing more browsing information with Google. The recommended state for this setting is: Safe Browsing is active in the standard mode.(1) or higher

Rationale :

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or from downloading dangerous files.NOTE: Google recommends using Enhanced Safe Browsing Mode (2). Turning on Enhanced Safe Browsing will substantially increase protection from dangerous websites and downloads, but will share more data with Google. For more details, please refer to the items in the References section below.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Safe Browsing is active in the standard mode..Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Safe Browsing settings\Safe Browsing Protection Level.Impact:None - This is the default behavior (Standard Protection).

1.2.1. L1 Ensure Configure the list of domains on which Safe Browsing will not trigger warnings is set to Disabled

Rule Status :

Passed

Summary :

The setting determines the functionality of Safe Browsing. Disabled(0): Safe Browsing protection applies to all resources Enabled(1), with a list of 1 or more sites: Means Safe Browsing will trust the domains you designate. It won"t check them for dangerous resources such as phishing, malware, or unwanted software. The recommended state for this setting is: Disabled(0) NOTE: Safe Browsing"s download protection service won"t check downloads hosted on these domains, and its password protection service won"t check for password reuse.

Rationale :

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or download dangerous files.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Safe Browsing settings\Configure the list of domains on which Safe Browsing will not trigger warnings..Impact:None - This is the default behavior.NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

1.18. L1 Ensure Enable security warnings for command-line flags is set to Enabled

Rule Status :

Failed

Summary :

This setting prevents Google Chrome from showing security warnings that potentially dangerous command-line flags are in use at its launch.The recommended state of this setting is: Enabled (0)

Rationale :

If Google Chrome is being launched with potentially dangerous flags, this information should be exposed to the user as a warning. If not, the user may be unintentionally using non-secure settings and be exposed to security flaws.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable security warnings for command-line flags.Impact:None - This is the default behavior.

1.9. L1 Ensure Determine the availability of variations is set to Enable all variations

Rule Status :

Unscored

Summary :

Configuring this setting allows specifying which variations are allowed to be applied in Google Chrome.Variations provide a means for Google to offer modifications to Google Chrome without shipping a new version of the browser by selectively enabling or disabling already existing features. Enable all variations(0): Allows all variations to be applied to the browser (Default value). Enable variations concerning critical fixes only(1): Allows only variations considered critical security or stability fixes to be applied to Google Chrome. Disable all variations(2): Prevent all variations from being applied to the browser. Please note that this mode can potentially prevent the Google Chrome developers from providing critical security fixes in a timely manner and is thus not recommended. The recommended state for this setting is: Enable all variations(0) NOTE: Google strongly believes there is no added security benefit for turning this to critical fixes as leaving it on increases the stability of the browser. Disabling variations can also prevent getting critical security updates in a timely manner.

Rationale :

Google strongly recommends leaving this setting at the default (0 = Enable all variations), so fixes are gradually enabled (or if necessary, rapidly disabled) via the Chrome Variations framework.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Enable all variations.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Determine the availability of variations.Impact:None - This is the default behavior.

1.17. L1 Ensure Enable online OCSPCRL checks is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome can reactivate soft-fail, online revocation checks although they can provide some benefit in most cases.If this setting is disabled, unsecure online OCSP/CRL checks are no longer performed.The recommended state for this setting is: Disabled(0)

Rationale :

CRLSets are primarily a means by which Chrome can quickly block certificates in emergency situations. As a secondary function they can also contain some number of non-emergency revocations. These latter revocations are obtained by crawling CRLs published by CAs.Online (i.e. OCSP and CRL) checks are not, by default, performed by Chrome. The underlying system certificate library always performs these checks no matter what Chrome does, so enabling it here is redundant.An attacker may block OCSP traffic and cause revocation checks to pass in order to cause usage of soft-fail behavior. Furthermore, the browser may leak what website is being accessed and who accesses it to CA servers.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable online OCSP/CRL checks.Impact:None - This is the default behavior.

1.10. L1 Ensure Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities is set to Disabled

Rule Status :

Passed

Summary :

Google Chrome can disable the enforcing of Certificate Transparency requirements for a list of Legacy Certificate Authorities.If this setting is disabled, certificates not properly publicly disclosed as required by Certificate Transparency are untrusted.The recommended state for this setting is: Disabled(0)

Rationale :

Legacy Certificate Authorities shall follow the Certificate Transparency policy.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities.Impact:None - This is the default behavior.

1.11. L1 Ensure Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes is set to Disabled

Rule Status :

Passed

Summary :

Google Chrome can exclude certificates by their subjectPublicKeyInfo hashes from enforcing Certificate Transparency requirements. If this setting is disabled, no certificates are excluded from Certificate Transparency requirements.The recommended state for this setting is: Disabled(0)

Rationale :
Certificate Transparency requirements shall be enforced for all certificates.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes.Impact:None - This is the default behavior.

1.12. L1 Ensure Disable Certificate Transparency enforcement for a list of URLs is set to Disabled

Rule Status :

Passed

Summary :

Google Chrome can specify URLs/hostnames for which Certificate Transparency will not be enforced. If this setting is disabled, no URLs are excluded from Certificate Transparency requirements.The recommended state for this setting is: Disabled(0)

Rationale :

Certificates that are required to be disclosed via Certificate Transparency shall be treated for all URLs as untrusted if they are not disclosed according to the Certificate Transparency policy.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of URLs.Impact:None - This is the default behavior.

1.16. L1 Ensure Enable globally scoped HTTP auth cache is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether HTTP auth credentials may be automatically used in the context of another web site visited in Google Chrome.The recommended state for this setting is: Disabled(0) NOTE: This setting is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future.

Rationale :

Allowing HTTP auth credentials to be shared without the user"s consent could lead to a user sharing sensitive information without their knowledge. Enabling this setting could also lead to some types of cross-site attacks that would allow users to be tracked across sites without the use of cookies.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable globally scoped HTTP auth cache.Impact:None - This is the default behavior.

1.23. L1 Ensure Import of homepage from default browser on first run is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether users are able to import homepage settings from another browser into Google Chrome as well as whether homepage settings are imported on first use.If you set this setting to Disabledusers will be unable to perform an import homepage settings from other browsers into Google Chrome. The recommended state for this setting is: Disabled(0)

Rationale :

Having the homepage setting automatically imported or allowing users to import this setting from another browser into Google Chrome allows for the potential of compromised settings being imported into Google Chrome.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Import of homepage from default browser on first run.Impact:None - This is the default behavior.

1.6. L1 Ensure Ask where to save each file before downloading is set to Enabled

Rule Status :

Failed

Summary :

Google Chrome offers to download files automatically to the default download directory without prompting.If this setting is enabled, users are always asked where to save each file before downloading.The recommended state for this setting is: Enabled(1)

Rationale :

Users shall be prevented from the drive-by-downloads threat.

How to fix :

To establish the recommended configuration via Group Policy, set thefollowing UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Ask where to save each file before downloading.Impact:None - This is the default behavior.

1.22. L1 Ensure Import autofill form data from default browser on first run is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether users are allowed to import autofill data from other browsers into Google Chrome.If you set this setting to Disabled, users will be unable to perform an import of autofill data during Google Chrome run. This will also prevent users from importing data after Google Chrome has been set up. The recommended state for this setting is: Disabled(0)

Rationale :

Allowing autofill data to be imported could potentially allow sensitive data such as personally identifiable information (PII) from a non-secured source into Google Chrome. Considering that storage of sensitive data should be handled with care, disabling this setting is recommended.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Import autofill form data from default browser on first run.Impact:None - This is the default behavior.

1.21. L1 Ensure Ephemeral profile is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether user profiles are switched to ephemeral mode. In ephemeral mode, profile data is saved on disk for the length of the session and then the data is deleted after the session is over. Therefore, no data is saved to the device.The recommended state for this setting is: Disabled(0)

Rationale :

Allowing use of ephemeral profiles allows a user to use Google Chrome with no data being logged to the system. Deleting browser data will delete information that may be important for a computer investigation and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Ephemeral profile.Impact:None - This is the default behavior.

1.7. L1 Ensure Continue running background apps when Google Chrome is closed is set to Disabled

Rule Status :

Failed

Summary :

Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed.With this setting Disabled, the browser will close its processes and will stop running background apps.The recommended state for this setting is: Disabled(0)

Rationale :

If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Continue running background apps when Google Chrome is closed.Impact:None - This is the default behavior.

1.20. L1 Ensure Enables managed extensions to use the Enterprise Hardware Platform API is set to Disabled

Rule Status :

Failed

Summary :

This setting allows extensions installed by enterprise policies to be allowed to use the Enterprise Hardware Platform API.The recommended state for this setting is: Disabled(0)

Rationale :
It is recommended that this setting is disabled unless otherwise directed by Enterprise policies.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enables managed extensions to use the Enterprise Hardware Platform API.Impact:None - This is the default behavior.

1.29. L1 Ensure URLs for which local IPs are exposed in WebRTC ICE candidates is set to Disabled

Rule Status :

Passed

Summary :

This setting specifies a list of URLs or patterns for which local IP addresses will be exposed by WebRTC.The recommended state for this setting is: Disabled(0) NOTE: This setting, if Enabled, weakens the protection of local IPs if needed by administrators.

Rationale :

Enabling this setting and allowing exposure of IP addresses can allow an attacker to gather information about the internal network that could potentially be utilized to breach and traverse a network.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\URLs for which local IPs are exposed in WebRTC ICE candidates.Impact:None - This is the default behavior.

1.28. L1 Ensure Suppress the unsupported OS warning is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome will show a warning that appears when Google Chrome is running on a computer or operating system that is no longer supported.The recommended state for this setting is: Disabled(0)

Rationale :

The user shall be informed if the used software is no longer supported.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Suppress the unsupported OS warning.Impact:None - This is the default behavior.

1.13. L1 Ensure Disable saving browser history is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome is configured to save the browser history.The recommended state for this setting is: Disabled(0) NOTE: This setting will preserve browsing history that could contain a user"s personal browsing history. Please make sure that this setting is in compliance with organizational policies.

Rationale :

Browser history shall be saved as it may contain indicators of compromise.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Disable saving browser history.Impact:None - This is the default behavior.

1.14. L1 Ensure DNS interception checks enabled is set to Enabled

Rule Status :

Failed

Summary :

This setting determines whether a local switch is configured for DNS interception checks. These checks attempt to discover if the browser is behind a proxy that redirects unknown host names.The recommended state for this setting is: Enabled(1) NOTE: This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on startup and each DNS configuration change.

Rationale :

Disabling these checks could potentially allow DNS hijacking and poisoning.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\DNS interception checks enabled.Impact:None - This is the default behavior.

1.15. L1 Ensure Enable component updates in Google Chrome is set to Enabled

Rule Status :

Failed

Summary :

Google Chrome"s Component Updater updates several components of Google Chrome on a regular basis (applies only to Chrome browser components).The recommended state for this setting is: Enabled(1) NOTE: Updates to any component that does not contain executable code, does not significantly alter the behavior of the browser, or is critical for its security will not be disabled (E.g. certificate revocation lists and Safe Browsing data is updated regardless of this setting). FYI chrome://componentslists all components, but not if they are affected by this setting. NOTE: Some Google provided components controlled by this setting: Recovery componentPnaclFlocOptimization hintsSSL error assistantCRL setOrigin trialsSW reporterPKI metadata

Rationale :

Google Chrome Updater shall be used to keep the components bundled to Chrome up-to-date.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable component updates in Google Chrome.Impact:None - This is the default behavior.

1.27. L1 Ensure Suppress lookalike domain warnings on domains is set to Disabled

Rule Status :

Passed

Summary :

This setting prevents the display of lookalike URL warnings on the sites listed. These warnings are typically shown on sites that Google Chrome believes might be trying to spoof another site with which the user is familiar. Disabled(0) or set to an empty list: Warnings may appear on any site the user visits. Enabled (1) and set to one or more domains: No lookalike warnings pages will be shown when the user visits pages on that domain. The recommended state for this setting is: Disabled(0)

Rationale :

Look-alike domains are intentionally misleading to give users the false impression that they’re interacting with trusted brands, leading to significant reputation damage, financial losses, and data compromise for established enterprises.In addition, this technique is commonly used to host phishing sites, and often leads to account takeover attacks. Users are prompted to enter their credentials on a fake website, and scammers take control of their online accounts with little effort to engage in fraudulent activity.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Suppress lookalike domain warnings on domains.Impact:None - This is the default behavior.NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

1.4. L1 Ensure Allow queries to a Google time service is set to Enabled

Rule Status :

Failed

Summary :

This setting controls whether Google Chrome can send queries to a Google time service for accurate timestamps. This check helps in validation of certificates.The recommended state for this setting is: Enabled(1)

Rationale :

Google Chrome uses a network time service to randomly track times from a trusted external service. This allows Google Chrome the ability for verification of a certificate"s validity and is important for certificate validation.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow queries to a Google time service.Impact:None - This is the default behavior.

1.3. L1 Ensure Allow Google Cast to connect to Cast devices on all IP addresses is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether Google Cast is able to connect to all IP Addresses or only private IP Addresses as defined in RFC1918 (IPv4) and RFC4193 (IPv6). Note that if the EnabledMediaRouter setting is set to Disabledthere is no positive or negative effect for this setting. The recommended state for this setting is: Disabled(0)

Rationale :

Allowing Google Cast to connect to public IP addresses could allow media and other potentially sensitive data to be exposed to the public. Disabling this setting will ensure that Google Cast is only able to connect to private (ie: internal) IP addresses.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Google Cast\Allow Google Cast to connect to Cast devices on all IP addresses..Impact:None - This is the default behavior.

1.19. L1 Ensure Enable third party software injection blocking is set to Enabled

Rule Status :

Failed

Summary :

Google Chrome can prevent third party software from injecting executable code into Chrome"s processes.The recommended state for this setting is: Enabled(1)

Rationale :

Third party software shall not be able to inject executable code into Chrome"s processes.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable third party software injection blocking.Impact:None - This is the default behavior.

1.26. L1 Ensure Origins or hostname patterns for which restrictions on insecure origins should not apply is set to Disabled

Rule Status :

Passed

Summary :

Google Chrome can use a list of origins (URLs) or hostname patterns (such as "*.example.com") for which security restrictions on insecure origins will not apply and are prevented from being labeled as "Not Secure" in the omnibox.The recommended state for this setting is: Disabled(0)

Rationale :

Insecure contexts shall always be labeled as insecure.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Origins or hostname patterns for which restrictions on insecure origins should not apply. Note: The UI path defined in the chrome.admlincludes a line break between the onand the insecure. In some views, the line break is correctly rendered, in others not. Impact:None - This is the default behavior.

1.25. L1 Ensure List of names that will bypass the HSTS policy check is set to Disabled

Rule Status :

Passed

Summary :

This setting allows a list of names to be specified that will be exempt from HTTP Strict Transport Security (HSTS) policy checks, then potentially upgraded from http:// to https://.The recommended state for this setting is: Disabled(0)

Rationale :
Allowing hostnames to be exempt from HSTS checks could allow for protocol downgrade attacks and cookie hijackings.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\List of names that will bypass the HSTS policy check.Impact:None - This is the default behavior.

1.24. L1 Ensure Import search engines from default browser on first run is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether users are able to import search engine settings from another browser into Google Chrome as well as whether said setting is imported on first use.If you set this setting to Disabledusers will be unable to perform an import of their search engine settings from other browsers into Google Chrome. The recommended state for this setting is: Disabled(0)

Rationale :

Having search engine settings automatically imported or allowing users to import the settings from another browser into Google Chrome could allow for a malicious search engine to be set.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Import search engines from default browser on first run.Impact:None - This is the default behavior.

1.5. L1 Ensure Allow the audio sandbox to run is set to Enabled

Rule Status :

Failed

Summary :

This setting controls whether audio processes in Google Chrome run in a sandbox.NOTE: Security software setups within your environment might interfere with the sandbox. The recommended state for this setting is: Enabled(1)

Rationale :

Having audio processes run in a sandbox ensures that if a website misuses audio processes that data may not be manipulated or exfiltrated from the system.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow the audio sandbox to run.Impact:None - This is the default behavior.

2.10.1. L1 Ensure Allow automatic sign-in to Microsoft cloud identity providers Is Enabled

Rule Status :

Unscored

Summary :

This policy setting allows accounts backed by a Microsoft® cloud identity provider (i.e., Microsoft Azure Active Directory or the consumer Microsoft account identity provider) can be signed into web properties using that identity automatically. It can be configured to either:Disabled (0): Disable Microsoft® cloud authenticationEnabled (1): Enable Microsoft® cloud authenticationIf the value for CloudAPAuthEnabledis not changed from the default, it will behave as it is disabled.

Rationale :

Enabling this policy setting allows users to use Microsoft Cloud Authentication for any site that requires CA (Cloud Authentication) and does not require an extension.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Enable Microsoft® cloud authentication.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Microsoft® Active Directory® management settings\Allow automatic sign-in to Microsoft® cloud identity providers.Impact:There should be no impact to the user.

2.1.1. L1 Ensure Update policy override is set to Enabled with Always allow updates recommended or Automatic silent updates specified

Rule Status :

Failed

Summary :

Google Update manages installation of available Google Chrome updates from Google. This setting allows users to define whether updates are to be applied automatically. Depending on the business scenario, updates shall be applied periodically or also if the user seeks for updates. Updates disabled: Never apply updates (0) Always allow updates: Updates are always applied when found, either by periodic update check or by a manual update check (1) Manual updates only: Updates are only applied when the user does a manual update check (2) Automatic silent updates only: Updates are only applied when they are found via the periodic update check (3) Disabled(0): Google Update handles available updates as specified by "Update policy override default". The recommended state for this setting is: Enabledwith a value of Always allow updates(1) or Automatic silent updates(3) NOTE: This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Rationale :

Software updates shall be applied as soon as they are available since they may include latest security patches.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Always allow updates (recommended).Computer Configuration\Polices\Administrative Templates\Google\Google Update\Applications\Google Chrome\Update policy override.Impact:Latest updates are automatically applied at least periodically.

2.2.5. L1 Ensure Allow local file access to file URLs on these sites in the PDF Viewer Is Disabled

Rule Status :

Passed

Summary :

This setting will allow specified URLs to access file://URLs in the PDF Viewer. By default all domains are blocked from accessing file://URLs in the PDF Viewer

Rationale :

Blocking all domains, or a restricted list of domains, from opening a downloaded PDF file blocks the possibility of a malicious file being masked as a PDF. It could also block unknown or malicious code contained within the PDF that would run on the immediate opening within a browser tab.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Allow local file access to file:// URLs on these sites in the PDF Viewer.Impact:Users will be required to open PDF files manually in the PDF Viewer or in the organization"s PDF viewing application.

2.2.1. L1 Ensure Control use of insecure content exceptions is set to Enabled Do not allow any site to load mixed content

Rule Status :

Failed

Summary :

Setting controls whether users can add exceptions to allow mixed content for specific sites. Do not allow any site to load mixed content(2) Allow users to add exceptions to allow mixed content(3) The recommended state for this setting is: Enabledwith the value of Do not allow any site to load mixed content(2) NOTE: This policy can be overridden for specific URL patterns using the InsecureContentAllowedForUrls and InsecureContentBlockedForUrls policies.

Rationale :

Allowing mixed (secure / insecure) content from a site can lead to malicious content being loaded. Mixed content occurs if the initial request is secure over HTTPS, but HTTPS and HTTP content is subsequently loaded to display the web page. HTTPS content is secure. HTTP content is insecure.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to load mixed content.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Content Settings\Control use of insecure content exceptions.Impact:Users will not be able to mix content.

2.3.7. L1 Ensure Control availability of extensions unpublished on the Chrome Web Store Is Disabled

Rule Status :

Failed

Summary :

This policy disables any extensions in Google Chrome that were downloaded from the Chrome Web Store and are now unpublished. The policy can be configured to either:Enabled (0): Allow unpublished extensionsDisabled (1): Disable unpublished extensionsIf the value for ExtensionInstallBlocklist is unchanged from the default, it will behave as it is enabled.
Note: Only unpublished extensions installed using developer mode and extensions installed using the command-line switch are ignored. Force-installed extensions that are self-hosted are ignored. All version-pinned extensions are also ignored.

Rationale :

Disabling unpublished extensions will remove the ability to run any extensions that are no longer being updated or patched.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Disable unpublished extensions.Computer Configuration\Policies\Administrative Templates\Google Chrome\Extensions\Control availability of extensions unpublished on the Chrome Web Store..Impact:This may disable extensions commonly used by users in your organization.

2.3.3. L1 Ensure Configure extension installation blocklist is set to Enabled

Rule Status :

Failed

Summary :

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blocklisted. Disabled(0): then the user can install any extension in Google Chrome. The recommended state for this setting is: Enabledwith a value of *NOTE: Chrome does offer a more granular permission-based configuration called Extension management settingsif blocklisting all extensions is too aggressive, which allows an organization to drill down to the exact permissions that they want to lock down. The extensions management settings require more coordination and effort to understand what the security requirements are to block site and device permissions globally as well as more IT management to deploy. The benefit would be allowing access to more extensions to their end-users. See link in reference section NOTE: If Chrome Cleanup is Disabled, users may want to configure the extension blocklist instead of using the Extension Management option. Chrome Cleanup can help protect against malicious extensions when paired with the Extension Management setting.

Rationale :

This can be used to block extensions that could potentially allow remote control of the system through the browser. If there are extensions needed for securing the browser or for enterprise use, these can be enabled by configuring either the setting Configure extension installation allowlistor the setting Extension management settings.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand a value of *for Extension IDs the user should be prevented from installing: Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Extensions\Configure extension installation blocklist.Impact:Any installed extension will be removed unless it is specified on the extension allowlist. If an organization is using any approved password managers, ensure that the extension is added to the allowlist.

2.3.5. L1 Ensure Block third-party storage partitioning for these origins Is Configured

Rule Status :

Unscored

Summary :

This setting will block specific sites your organization selects from accessing the storage session from any other site. This will allow an organization to block third party trackers that are embedded on multiple sites from tracking a user across the sites they visit. It will also allow blocking third party access to the user agent and to infer data about the user from the data from another site.Setting the Level 2 recommendation DefaultThirdPartyStoragePartitioningSettingwill block all sites, not just this set list in ThirdPartyStoragePartitioningBlockedForOrigins

Rationale :

If your organization does not want to block all third-party sites from accessing the user agent, you can configure a curated list of sites to block.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand set Showto the approved URLs: Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Block third-party storage partitioning for these origins.Impact:This might cause the user experience to vary from allowed sites to blocked sites.

2.3.1. L1 Ensure Blocks external extensions from being installed is set to Enabled

Rule Status :

Failed

Summary :

Enabling this setting blocks external extensions (an extension that is not installed from the Chrome Web Store) from being installed.The recommended state for this setting is: Enabled(1)

Rationale :
Allowing users to install extensions from other locations (not the Chrome Web Store) can lead to malicious extensions being installed.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Extensions\Blocks external extensions from being installed.Impact:User will only be allowed to install extension for the Chrome web store.

2.3.2. L1 Ensure Configure allowed appextension types is set to Enabled extension hosted app platform app theme

Rule Status :

Failed

Summary :

Enabling this setting allows you to specify which app/extension types are allowed. Disabled(0): Results in no restrictions on the acceptable extension and app types. The recommended state for this setting is: Enabledwith the values of extension, hosted_app, platform_app, theme.

Rationale :

App or extension types that could be misused or are deprecated shall no longer be installed.NOTE: Google has removed support for Chrome Apps which includes the types hosted_app and platform_app. The blog post indicates that these types will require a setting to be enabled for continued use through June 2022.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: extension, hosted_app, platform_app, theme.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Extensions\Configure allowed app/extension types.Impact:Extensions already installed will be removed if its type is denylisted and the extension itself is not allowlisted.

2.6.1. L1 Ensure Enable saving passwords to the password manager is Explicitly Configured

Rule Status :

Unscored

Summary :

Google Chrome has a built-in password manager to store passwords for users. Chrome will use local authentication to allow users to gain access to these passwords.The recommended state for this setting is: Explicitly set to Enabled(1) or Disabled(0) based on the organization"s needs.
NOTE: If you choose to Enable this setting, please review Disable synchronization of data with Googleand ensure this setting is configured to meet organizational requirements.

Rationale :
The Google Chrome password manager is Enabledby default and each organization should review and determine if they want to allow users to store passwords in the Browser. If another solution is used instead of the built in Chrome option then an organization should configure the setting to Disabled.

How to fix :
To establish the recommended configuration via Group Policy, configure the following setting to meet organizational requirements:Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Password manager\Enable saving passwords to the password manager.Impact:Organizationally dependent.

2.7.1. L1 Ensure Enable Google Cloud Print Proxy is set to Disabled

Rule Status :

Failed

Summary :

This setting enables Google Chrome to act as a proxy between Google Cloud Print and legacy printers connected to the machine.The recommended state for this setting is: Disabled(0)

Rationale :
Disabling this option will prevent users from printing documents from unmanaged devices to an organization"s printer.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Printing\Enable Google Cloud Print Proxy.Impact:If this setting is disabled, users cannot enable the proxy, and the machine will not be allowed to share its local printers with Google Cloud Print.

2.8.5. L1 Ensure Enable firewall traversal from remote access host is set to Disabled

Rule Status :

Failed

Summary :

Chrome enables the usage of STUN servers which allows remote clients to discover and connect to a machine even if they are separated by a firewall. By disabling this feature, in conjunction with filtering outgoing UDP connections, the machine will only allow connections from machines within the local network.The recommended state for this setting is: Disabled(0)

Rationale :

If this setting is enabled, remote clients can discover and connect to these machines even if they are separated by a firewall.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Enable firewall traversal from remote access host.Impact:If this setting is disabled and outgoing UDP connections are filtered by the firewall, this machine will only allow connections from client machines within the local network.

2.8.4. L1 Ensure Enable curtaining of remote access hosts is set to Disabled

Rule Status :

Failed

Summary :

This setting allows someone physically present at the host machine to see what a user is doing while a remote connection is in progress.If this setting is disabled, a host"s physical input and output devices are enabled while a remote connection is in progress.The recommended state for this setting is: Disabled(0)

Rationale :
If a remote session is in progress, the user physically present at the host machine shall be able to see what a remote user is doing.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Enable curtaining of remote access hosts.Impact:None - This is the default behavior.

2.8.7. L1 Ensure Enable the use of relay servers by the remote access host is set to Disabled.

Rule Status :

Failed

Summary :

Google Chrome allows the use of relay servers when clients are trying to connect to this machine and a direct connection is not available. Disable(0): The use of relay servers by the remote access host is not allowed Enabled(1): The use of relay servers by the remote access host is allowed The recommended state for this setting is: Disabled(0)

Rationale :
Relay servers shall not be used to circumvent firewall restrictions.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Enable the use of relay servers by the remote access host.Impact:If this setting is disabled, remote clients can not use relay servers to connect to this machine.NOTE: Setting this to Disabled doesn"t turn remote access off, but only allows connections from the same network (not NAT traversal or relay).

2.8.6. L1 Ensure Enable or disable PIN-less authentication for remote access hosts is set to Disabled

Rule Status :

Failed

Summary :

Chrome allows a user to opt-out of using user-specified PIN authentication and instead pair clients and hosts during connection time.The recommended state for this setting is: Disabled(0)

Rationale :
If this setting is enabled, users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Enable or disable PIN-less authentication for remote access hosts.Impact:If this setting is disabled, users will be required to enter PIN every time.

2.8.1. Ensure Allow remote access connections to this machine is set to Disabled

Rule Status :

Unscored

Summary :

This is a setting for Chrome Remote desktop. If this setting is Disabled, the remote access host service cannot be started or configured to accept incoming connections. Disabled(0): Prevent remote access connections to this machine Enabled(1): Allow remote access connections to this machine The recommended state for this setting is: Disabled(0)

Rationale :

Only approved remote access systems should be used.NOTE: If Chrome Remote Desktop is approved and required for use, then this setting can be ignored.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Remote Access\Allow remote access connections to this machine.Impact:This setting will disable Chrome Remote Desktop. In general, Chrome Remote Desktop is not used by most businesses, so disabling it should have no impact.

2.8.2. L1 Ensure Allow remote users to interact with elevated windows in remote assistance sessions is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome can be set to run the remote assistance host in a process with uiAccess permissions. This allows remote users to interact with elevated windows on the local user"s desktop.If this setting is disabled, the remote assistance host will run in the user"s context. Furthermore, remote users cannot interact with elevated windows on the desktop.The recommended state for this setting is: Disabled(0)

Rationale :

Remote users shall not be able to escalate privileges.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Allow remote users to interact with elevated windows in remote assistance sessions.Impact:None - This is the default behavior.

2.8.3. L1 Ensure Configure the required domain names for remote access clients is set to Enabled with a domain defined

Rule Status :

Unscored

Summary :

Chrome allows the configuration of a list of domains that are allowed to access the user"s system. When enabled, remote systems can only connect if they are one of the specified domains listed.Setting this to an empty list (Disabled) allows remote systems from any domain to connect to this user"s system.The recommended state for this setting is: Enabled(1) and at least one domain set NOTE: The list of domains is organization specific.

Rationale :

Remote assistance connections shall be restricted.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand enter an organizational specific domain(s) (e.g. nodomain.local): Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Remote access\Configure the required domain names for remote access clients.Impact:If this setting is enabled, only systems from the specified domains can connect to the user"s system.

2.9.1. L1 Ensure Enable First-Party Sets Is Disabled

Rule Status :

Unscored

Summary :

This policy controls access to the First-Party Sets. First-party Sets are a way for sites to declare relationships with each other and enable limited cross-site cookie access for specific, user-facing purposes. It can configured to either:Disabled (0): Disable First-Party Sets for all affected usersEnabled (1): Enable First-Party Sets for all affected users

Rationale :

Setting this policy will not allow sites to declare the relationships that allow them to access the cross-site cookies.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Enable Firty-Party Sets.Impact:This may cause unexpected behavior as a user moves between affiliated sites.

2.24. L1 Ensure Keep browsing data when creating enterprise profile by default Is Enabled

Rule Status :

Failed

Summary :

This setting controls keeping existing browser data when an enterprise profile is created. It can be configured to either:Disabled (0): Do not check the option to keep existing browsing data by defaultEnabled (1): Check the option to keep existing browsing data by defaultIf the value for EnterpriseProfileCreationKeepBrowsingDatais not changed from the default, it will behave as if it is enabled. Note: Unlike other policy settings, the user does get to decide whether or not to keep any existing browsing data when creating an enterprise profile.

Rationale :

Setting this policy gives the user the option to keep any previous browsing data after setting up an enterprise profile.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Keep browsing data when creating enterprise profile by default.Impact:This should have no effect on the user.

2.22. L1 Ensure Enable TLS Encrypted ClientHello Is Enabled

Rule Status :

Failed

Summary :

This setting controls the defaults for using Encrypted ClientHello (ECH). ECH is an extension to TLS and encrypts the initial handshake with a website that can only be decrypted by that website. Google Chrome may, or may not, use ECH based on 3 factors: sever support, HTTPS DNS record availability, or rollout status. It can be configured to either:Disabled (0): Disable the TLS Encrypted ClientHello experimentEnabled (1): Enable the TLS Encrypted ClientHello experimentIf the value for EncryptedClientHelloEnabledis not changed from the default, it will behave as it is enabled.

Rationale :

Previously all handshakes were in the open and could expose sensitive information like the name of the website that you are connecting to. Setting this policy will allow Google Chrome to use an encrypted hello, or handshake, with a website where it is supported, thus not exposing sensitive information.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable TLS Encrypted ClientHello.Impact:There should be no impact on the user.

2.16. L1 Ensure Notify a user that a browser relaunch or device restart is recommended or required is set to Enabled Show a recurring prompt to the user indication that a relaunch is required

Rule Status :

Failed

Summary :

Google Chrome can notify users that it must be restarted to apply a pending update once the notification period defined by the recommendation Set the time period for update notifications is passed. Show a recurring prompt to the user indicating that a relaunch is recommended(1) Show a recurring prompt to the user indicating that a relaunch is required(2) Disabled: Google Chrome indicates to the user that a relaunch is needed via subtle changes to its menu. The recommended state for this setting is: Enabledwith a value of Show a recurring prompt to the user indicating that a relaunch is required(2)

Rationale :

The end-user will receive a notification informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that the update is applied as soon as possible. Enabling this notification will ensure that users restart their browser in a timely fashion.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Show a recurring prompt to the user indicating that a relaunch is required.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Notify a user that a browser relaunch or device restart is recommended or required.Impact:A recurring warning will be shown to the user indicating that a browser relaunch will be forced once the notification period passes. The user"s session is restored after the relaunch of Google Chrome.

2.30. L1 Ensure Enable Renderer App Container Is Enabled

Rule Status :

Failed

Summary :

This setting controls the ability for Google Chrome to allow the Render App Container sandbox to be used while navigating to certain sites. It can be configured to either:Disabled (0): Disable the Renderer App Container sandboxEnabled (1): Enable the Renderer App Container sandboxIf the value for RendererAppContainerEnabledis not changed from the default, it will behave as if it is enabled.

Rationale :

Disabling this policy would weaken the sandbox that Google Chrome uses for the renderer process, and will have a detrimental effect on the security and stability of the browser. This policy needs to be enabled to maintain security and stability.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable Renderer App Container.Impact:This would only impact users if there is third-party software that must run inside renderer processes.

2.17. L1 Ensure Proxy settings is set to Enabled and does not contain ProxyMode auto detect

Rule Status :

Failed

Summary :

Google Chrome offers the functionality to configure the proxy settings by automatic discovery using WPAD (Web Proxy Auto-Discovery Protocol). Setting this configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified from the command line. Disabled(0): Lets users choose their proxy settings. The recommended state for this setting is: Enabledand the value of ProxyModeis not set to auto_detect

Rationale :

Attackers may abuse the WPAD auto-config functionality to supply computers with a PAC file that specifies a rogue web proxy under their control.

How to fix :

To establish the recommended configuration via Group Policy, make sure the following UI path is set to "Enabled" and the value of ProxyModeis not set to auto_detect.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Proxy settings.Impact:If the policy is enabled, the proxy configuration will no longer be discovered using WPAD.

2.31. L1 Ensure Enable strict MIME type checking for worker scripts Is Enabled

Rule Status :

Failed

Summary :

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:Disabled (0): Scripts for workers (Web Workers, Service Workers, etc.) use lax MIME type checking. Worker scripts with legacy MIME types, like text/ascii, will work.Enabled (1): Scripts for workers (Web Workers, Service Workers, etc.) require a JavaScript MIME type, like text/javascript. Worker scripts with legacy MIME types, like text/ascii, will be rejected.If the value for StrictMimetypeCheckForWorkerScriptsEnabledis not changed from the default, it will behave as if it is enabled.

Rationale :

Setting this policy will require worker scripts to use more secure and strict JavaScript MIME types and ones with legacy MIME Types will be rejected.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable strict MIME type checking for worker scripts.Impact:This should have no impact on users.

2.27. L1 Ensure Http Allowlist Is Properly Configured

Rule Status :

Unscored

Summary :

This setting allows administrators to list specific sites that will not be upgraded to HTTPS and will not show an error interstitial if HTTPS-First Modeis enabled. Note: Wildcards (*, [*], etc.) are not allowed in the URL listings.

Rationale :

Setting this policy allows organizations to maintain access to servers that do not support HTTPS without having to disable HTTPS-First mode or HTTPS Upgrades.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand set Showto the approved URLs: Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\HTTP Allowlist.Impact:This should not have an impact on the user.

2.26. L1 Ensure Enable Google Search Side Panel Is Disabled

Rule Status :

Failed

Summary :

This setting controls the Google Search Side Panel. It can be configured to either:Disabled (0): Disable Google Search Side Panel on all web pagesEnabled (1): Enable Google Search Side Panel on all web pages

Rationale :

Setting this policy will not allow the Google Search Side Panel on any webpages.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable Google Search Side Panel.Impact:This should have no user impact.

2.11. L1 Ensure Allow download restrictions is set to Enabled Block malicious downloads

Rule Status :

Failed

Summary :

Google Chrome can block certain types of downloads, and won"t let users bypass the security warnings, depending on the classification of Safe Browsing. No special restrictions. Default.(0, Disabled) (Default) Block malicious downloads and dangerous file types.(1) Block malicious downloads, uncommon or unwanted downloads and dangerous file types.(2) Block all downloads.(3) Block malicious downloads. Recommended.(4) The recommended state for this setting is: Enabledwith a value of Block malicious downloads. Recommended.(4) NOTE: These restrictions apply to downloads triggered from webpage content, as well as the Download link... menu option. They don"t apply to the download of the currently displayed page or to saving as PDF from the printing options.

Rationale :

Users shall be prevented from downloading malicious file types, and shall not be able to bypass security warnings.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Block malicious downloads. Recommended..Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Allow download restrictions.Impact:If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings. These are downloads that have been identified as risky or from a risky source by the Google Safe Browsing Global intelligence engine./xhtml:strong>.

2.13. L1 Ensure Disable proceeding from the Safe Browsing warning page is set to Enabled

Rule Status :

Failed

Summary :

Google provides the Safe Browsing service. It shows a warning page when users navigate to sites that are flagged as potentially malicious. Disabled(0): Users can choose to proceed to the flagged site after the warning appears. The recommended state for this setting is: Enabled(1)

Rationale :

Malicious web pages are widely spread on the internet and pose the most significant threat to the user today. Users shall be prevented from navigating to potentially malicious web content.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Safe Browsing settings\Disable proceeding from the Safe Browsing warning page.Impact:Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. In some cases legitimate sites could be blocked and users would be prevented from accessing.

2.14. L1 Ensure Require Site Isolation for every site is set to Enabled

Rule Status :

Failed

Summary :

This setting controls if every website will load into its own process. Disabled(0): Doesn"t turn off site isolation, but it lets users opt out. The recommended state for this setting is: Enabled(1)

Rationale :
Chrome will load each website in its own process. Even if a site bypasses the same-origin policy, the extra security will help stop the site from stealing your data from another website.

How to fix :
To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Require Site Isolation for every site.Impact:If the policy is enabled, each site will run in its own process which will cause the system to use more memory. You might want to look at the Enable Site Isolation for specified originspolicy setting to get the best of both worlds – isolation and limited impact for users – by using Enable Site Isolation for specified originswith a list of the sites you want to isolate.

2.21. L1 Ensure Allow reporting of domain reliability related data Is Disabled

Rule Status :

Failed

Summary :

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:Disabled (0): Never send domain reliability data to GoogleEnabled (1): Domain Reliability data may be sent to Google depending on Chrome User Metrics (UMA) policyIf the value for DomainReliabilityAllowedis not changed from the default, it will behave as it is enabled.

Rationale :

Setting this policy to disabled can stop any accidental data leakage.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google Chrome\Allow reporting of domain reliability related data.Impact:There should be no impact on the user.

2.20. L1 Ensure Allow Web Authentication requests on sites with broken TLS certificates Is Disabled

Rule Status :

Failed

Summary :

This policy setting controls the WebAuthn API and its interaction with sites that have a broken TLS certificate. It can be configured to either:Disabled (0): Do not allow WebAuthn API requests on sites with broken TLS certificates.Enabled (1): Allow WebAuthn API requests on sites with broken TLS certificates.If the value for AllowWebAuthnWithBrokenTlsCertsis not changed from the default, it will behave as it is disabled.xempt.

Rationale :

Setting this policy will block the ability to authenticate to any website that does not have a valid TLS certificate since the identity of the site cannot be verified.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow Web Authentication requests on sites with broken TLS certificates..Impact:There should be no user impact.

2.29. L1 Ensure Insecure Hashes in TLS Handshakes Enabled Is Disabled

Rule Status :

Failed

Summary :

This setting controls the ability for Google Chrome to allow legacy or insecure hashes during the TLS handshake. It can be configured to either:Disabled (0): Do Not Allow Insecure Hashes in TLS HandshakesEnabled (1): Allow Insecure Hashes in TLS HandshakesIf the value for InsecureHashesInTLSHandshakesEnabledis not changed from the default, it will behave as if it is enabled.

Rationale :

Setting this policy to disabled will block Google Chrome from using insecure hashes. Using insecure, or legacy, hashes could allow sensitive data to be exposed.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Insecure Hashes in TLS Handshakes Enabled.Impact:Users would be blocked from visiting sites that do not support more secure hashes.

2.19. L1 Ensure Set the time period for update notifications is set to Enabled 86400000

Rule Status :

Failed

Summary :

Google Chrome allows to set the time period, in milliseconds, over which users are notified that it must be relaunched to apply a pending update.If not set, or Disabled, the default period of 604800000 milliseconds (7 days) is used. The recommended state for this setting is: Enabledwith value 86400000(1 day)

Rationale :

This setting is a notification for the end-user informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that said update takes effect as soon as possible. Enabling this notification will ensure users restart the browser in a timely fashion.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: 5265C00(86400000 in Hexadecimal): Computer Configuration\Polices\Administrative Templates\Google\Google Chrome\Set the time period for update notifications.Impact:After this time period, the user will be repeatedly informed of the need for an update until a Browser restart is completed.

2.25. L1 Ensure Allow file or directory picker APIs to be called without prior user gesture Is Disabled

Rule Status :

Passed

Summary :

This setting controls the ability for showOpenFilePicker(), showSaveFilePicker(), and showDirectoryPicker()web APIs to be called without user interaction. If the value for FileOrDirectoryPickerWithoutGestureAllowedForOriginsis not changed from the default, it will behave as if it is disabled.

Rationale :

Setting this policy would allow the URLs selected to call the showOpenFilePicker(), showSaveFilePicker(), and showDirectoryPicker()web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow file or directory picker APIs to be called without prior user gesture.Impact:Disabling this policy should have no impact on the user.

2.32. Ensure Allow remote debugging is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users may use remote debugging. This feature allows remote debugging of live content on a Windows 10 or later device from a Windows or macOS computer.The recommended state for this setting is: Disabled.

Rationale :

Disabling remote debugging enhances security and protects applications from unauthorized access. Some attack tools can exploit this feature to extract information, or to insert malicious code.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow remote debugging.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template google.admx/admlthat can be downloaded from: Download Chrome Browser for Your Business - Chrome Enterprise.
Impact:Users will not be able access the remote debugging feature in Google Chrome.

2.28. L1 Ensure Enable automatic HTTPS upgrades Is Enabled

Rule Status :

Failed

Summary :

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:Disabled (0): Disable HTTPS UpgradesEnabled (1): HTTPS Upgrades may be applied depending on feature launch statusIf the value for HttpsUpgradesEnabledis not changed from the default, it will behave as if it is enabled.

Rationale :

Enabling this setting will upgrade the connection to a site from HTTP to HTTPS where available, verifying the identity of the site visited.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Enable automatic HTTPS upgrades.Impact:This should have no impact on the user.Note: If there are internal sites/servers that use HTTP only, set those in the policy HttpAllowlist

3.1.2. L1 Ensure Default geolocation setting is set to Enabled Do not allow any site to track the users physical location

Rule Status :

Failed

Summary :

Google Chrome supports tracking a user"s physical location using GPS, data about nearby Wi-Fi access points or cellular signal sites/towers (even

if you’re not using them), and your computer’s IP. Disabled(0, same as 3) Allow sites to track the users" physical location(1) Do not allow any site to track the users" physical location(2) Ask whenever a site wants to track the users" physical location(3) The recommended state for this setting is: Enabledwith a value Do not allow any site to track the users" physical location(2)

Rationale :

From a privacy point of view it is not desirable to submit indicators regarding the location of the device, since the processing of this information cannot be determined. Furthermore, this may leak information about the network infrastructure around the device.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to track the users" physical location.Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Default geolocation setting.Impact:If this setting is disabled, chrome will no longer send data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address to Google.

3.2.1. L1 Ensure Enable Google Cast is set to Disabled

Rule Status :

Failed

Summary :

Google Cast can send the contents of tabs, sites, or the desktop from the browser to a remote display and sound system.The recommended state for this setting is: Disabled(0)

Rationale :
Google Cast may send the contents of tabs, sites, or the desktop from the browser to non-trusted devices on the local network segment.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Google Cast\Enable Google Cast.Impact:If this is disabled, Google Cast is not activated and the toolbar icon is not shown.

3.11. L1 Ensure Enable or disable spell checking web service is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome can use Google web service to help resolve spelling errors.The recommended state for this setting is: Disabled(0)

Rationale :

Information typed in may be leaked to Google"s spellcheck web service.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable or disable spell checking web service.Impact:After disabling this feature, Chrome no longer sends the entire contents of text fields to Google as you type them. Spell checking can still be performed using a downloaded dictionary. This setting only controls the usage of the online service.

3.12. L1 Ensure Enable reporting of usage and crash-related data is set to Disabled

Rule Status :

Failed

Summary :

This setting controls anonymous reporting of usage and crash-related data about Google Chrome to Google.The recommended state for this setting is: Disabled(0) NOTE: This setting is not available on Windows instances that are not joined to a Microsoft® Active Directory® domain.

Rationale :
Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data ex-filtration from company systems.

How to fix :
To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable reporting of usage and crash-related data.Impact:If this setting is disabled, this information is not sent to Google.

3.16. L1 Ensure Enable URL-keyed anonymized data collection is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome offers the feature URL-keyed anonymized data collection. This sends URLs of pages the user visits to Google to optimize its services.The recommended state for this setting is: Disabled(0)

Rationale :

Anonymized data collection shall be disabled, since it is unclear which information exactly is sent to Google.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable URL-keyed anonymized data collection.Impact:Anonymized data will not be sent to Google to help optimize its services

3.6. L1 Ensure Control how Chrome Cleanup reports data to Google is set to Disabled

Rule Status :

Failed

Summary :

Chrome provides a Cleanup feature to detect unwanted software. If this setting is Enabled, the results of the cleanup may be shared with Google (based on the setting of SafeBrowsingExtendedReportingEnabled) to assist with future unwanted software detection. These results will contain file metadata, automatically installed extensions, and registry keys. If the setting is Disabled, the results of the cleanup will not be shared with Google regardless of the value of SafeBrowsingExtendedReportingEnabled . The recommended state for this setting is: Disabled(0)
NOTE: This setting is not available on Windows instances that are not joined to a Microsoft® Active Directory® domain.

Rationale :

Anonymous crash/usage data can be used to identify people, companies, and information, which can be considered data ex-filtration from company systems.

How to fix :

To establish the recommended configuration via Group Policy, set thefollowing UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Control how Chrome Cleanup reports data to Google.Impact:Chrome Cleanup detected unwanted software and will no longer report metadata about the scan to Google.

3.3. L1 Ensure Allow websites to query for available payment methods is set to Disabled

Rule Status :

Failed

Summary :

This setting allows you to set whether a website can check to see if the user has payment methods saved.The recommended state for this setting is: Disabled(0)

Rationale :
Saving payment information in Google Chrome could lead to sensitive data being leaked and used for non-legitimate purposes.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow websites to query for available payment methods..Impact:Websites will be unable to query whether payment information within Google Chrome is available.

3.7. L1 Ensure Disable synchronization of data with Google is set to Enabled

Rule Status :

Failed

Summary :

Google Chrome can synchronize browser data using Google-hosted synchronization services. Examples of synced data include, but are not limited to, history and favorites.The recommended state for this setting is: Enabled(1) NOTE: if your organization allows synchronization of data with Google, then disabling this setting will synchronize saved passwords with Google.

Rationale :

Browser data shall not be synchronized into the Google Cloud.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Disable synchronization of data with Google.Impact:If this setting is enabled, browser data will no longer sync with Google across devices/platforms, allowing users to pick up where they left off.

3.8. L1 Ensure Enable alternate error pages is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome offers to show suggestions for the page you were trying to reach when it is unable to connect to a web address such as "Page Not Found".The recommended state for this setting is: Disabled(0)

Rationale :

Using navigation suggestions may leak information about the web site intended to be visited.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable alternate error pages.Impact:If this setting is disabled, Chrome will no longer use a web service to help resolve navigation errors.

3.4. L1 Ensure Block third party cookies is set to Enabled

Rule Status :

Failed

Summary :

Chrome allows cookies to be set by web page elements that are not from the domain in the user"s address bar. Enabling this feature prevents third party cookies from being set.The recommended state for this setting is: Enabled(1)

Rationale :

Blocking third-party cookies can help protect a user"s privacy by eliminating a number of website tracking cookies.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Block third party cookies.Impact:Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser"s address bar.NOTE : Third Party Cookies and Tracking Protection are required for many business critical websites, including Microsoft 365 web apps (Office 365), SalesForce, and SAP Analytics Cloud. If these, or similar services, are needed by the organization, then this setting can be Disabled.

3.13. L1 Ensure Enable Safe Browsing for trusted sources is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome can be adjusted to allow downloads without Safe Browsing checks when the requested file is from a trusted source. Trusted sources can be defined using recommendation "Configure the list of domains on which Safe Browsing will not trigger warnings".The recommended state for this setting is: Disabled(0) NOTE: On Microsoft® Windows®, this functionality is only available on instances that are joined to a Microsoft® Active Directory® domain, running on Windows 10 Pro, or enrolled in Chrome Browser Cloud Management.

Rationale :

Information requested from trusted sources shall not be sent to Google"s safe browsing servers.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Safe Browsing for trusted sources.Impact:If this setting is disabled, files downloaded from intranet resources will not be checked by Google Services.

3.9. L1 Ensure Enable deleting browser and download history is set to Disabled

Rule Status :

Failed

Summary :

Google Chrome can delete the browser and download history using the clear browsing data menu.The recommended state for this setting is: Disabled(0) NOTE: Even when this setting is disabled, the browsing and download history aren"t guaranteed to be retained. Users can edit or delete the history database files directly, and the browser itself may remove (based on expiration period) or archive any or all history items at any time

Rationale :

If users can delete websites they have visited or files they have downloaded it will be easier for them to hide evidence that they have visited unauthorized or malicious sites.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable deleting browser and download history.Impact:If this setting is disabled, browsing and download history cannot be deleted by using the clear browsing data menu.

3.10. L1 Ensure Enable predict network actions is set to Enabled Do not predict actions on any network connection

Rule Status :

Failed

Summary :

Google Chrome comes with the network prediction feature which provides DNS prefetching, TCP and SSL preconnection, and prerendering of web pages. Predict network actions on any network connection(0) or (1) Do not predict network actions on any network connection(2) The recommended state for this setting is: Enabledwith a value of Do not predict network actions on any network connection(2)

Rationale :

Opening connections to resources that may not be used could allow unneeded connections increasing attack surface and in some cases could lead to opening connections to resources which the user did not intend to utilize.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not predict network actions on any network connection.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable network prediction.Impact:Users will not be presented with web page predictions.

4.2.3. L1 Ensure Allow clipboard for these sites Is Configured

Rule Status :

Unscored

Summary :

This setting allows administrators to list specific sites that have access to the clipboard site permissions.Note: This does not include using keyboard shortcuts. Those are not gated by the clipboard site permission.

Rationale :

Setting this policy allows specified URLs to have access to the clipboard site permissions. This will allow the specified sites to have access to data on the clipboard that other sites do not. DefaultClipboardSettingis recommended to be set to disabled, so this list would be the only sites that would have access to the clipboard data.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand set Showto the approved URLs: Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Allow clipboard on these sites.Impact:Enforcing this recommendation can cause the clipboard functionality to not work identically for every site.

4.2.4. L1 Ensure Block clipboard on these sites Is Configured

Rule Status :

Unscored

Summary :

This setting allows administrators to list specific sites that do not have access to the clipboard site permissions.Note: This does not include using keyboard shortcuts. Those are not gated by the clipboard site permission.

Rationale :

Specifying URLs that do not have access to the clipboard site permissions limits data for sites that have access to data on the clipboard, and allows for more sites to have access.Setting this policy denies specified URLs to have access to the clipboard site permissions. This will limit the specified sites to access the data on the clipboard that other sites do. DefaultClipboardSettingis recommended to be set to disabled, so this list would be a backup to that policy in case it was enabled, left as the default, or removed.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabledand set Showto the blocked URLs: Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Block clipboard on these sites.Impact:Enforcing this recommendation can cause the clipboard functionality to not work identically for every site.

4.2.5. L1 Ensure Default clipboard setting Is Enabled to Deny Permissions

Rule Status :

Failed

Summary :

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:Disabled (2): Does not allow access to the clipboard site permission by any siteEnabled (3): Sites ask the user to allow access to the clipboard site permissionIf the value for DefaultClipboardSettingis not changed from the default, it will behave as if it is enabled. ClipboardAllowedForUrlsor ClipboardBlockedForUrlswill override this setting for any site that matches the configured URL patterns. With the setting disabled, organizations will need to set ClipboardAllowedForUrlsfor any URLs they want to make exempt.

Rationale :

The clipboard stores data, text, and images that are shared between all applications. An organization would disable clipboard access to restrict sites from reading the contents of the clipboard when visiting.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: Do not allow any site to use the clipboard site permission.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Content settings\Default clipboard setting.Impact:Not allowing sites to have access to the clipboard permission can cause issues with formatting or access to needed images on the clipboard.

4.9. L1 Ensure Enable AutoFill for credit cards is set to Disabled

Rule Status :

Failed

Summary :

Chrome allows users to auto-complete web forms with saved credit card information. Disabling this feature will prompt a user to enter all information manually.The recommended state for this setting is: Disabled(0)

Rationale :

If an attacker gains access to a user"s machine where the user has stored credit card AutoFill data, information could be harvested.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Enable AutoFill for credit cards.Impact:If this setting is disabled, credit card AutoFill will be inaccessible to users.

4.10. L1 Ensure Import saved passwords from default browser on first run is set to Disabled

Rule Status :

Failed

Summary :

This setting controls if saved passwords from the default browser can be imported (on first run and later manually).The recommended state for this setting is: Disabled(0)

Rationale :

In Chrome, passwords can be stored in plain-text and revealed by clicking the “show” button next to the password field by going to chrome://settings/passwords/.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Administrative Templates\Google\Google Chrome\Import saved passwords from default browser on first run.Impact:If this setting is disabled, saved passwords from other browsers are not imported.

4.11. L1 Ensure List of types that should be excluded from synchronization is set to Enabled passwords

Rule Status :

Failed

Summary :

This setting allows you to specify data types that will be limited/excluded from uploading data to the Google Chrome synchronization service.The recommended state for this setting is: Enabledwith the following text value passwords(Case Sensitive) NOTE: Other settings in addition to passwordscan be included based on organizational needs.

Rationale :

Storing and sharing information could potentially expose sensitive information including but not limited to user passwords and login information. Allowing this synchronization could also potentially allow an end user to pull corporate data that was synchronized into the cloud to a personal machine.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: passwords(Case Sensitive): Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\List of types that should be excluded from synchronization.Impact:Password data will not be synchronized with the Google Chrome synchronization service.

4.6. L1 Ensure Allow user feedback is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether users are able to utilize the Chrome feedback feature to send feedback, suggestions, and surveys to Google, as well as issue reports.The recommended state for this setting is: Disabled(0)

Rationale :

Data should not be shared with third-party vendors in an enterprise managed environment.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Allow user feedback.Impact:Users will not be able to send feedback to Google.

5.3. L1 Ensure Set disk cache size in bytes is set to Enabled 250609664

Rule Status :

Failed

Summary :

This setting controls the size of the cache, in bytes, used to store files on the disk.The recommended state for this setting is: Enabled: 250609664or greater NOTE The value specified in this setting isn"t a hard boundary but rather a suggestion to the caching system; any value below a few megabytes is too small and will be rounded up to a reasonable minimum.

Rationale :

Having enough disk space for browser cache is important for a computer investigation and for investigators such as Computer Forensics Analysts to be able to retrieve pertinent information to the investigation.

How to fix :

To establish the recommended configuration via Group Policy, set the following UI path to Enabled: 250609664.Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Set disk cache size in bytes.Impact:Browser cache will take up to 250MB in disk space.

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 Level 1 (L1) - Corporate/Enterprise Environment (general use)

1 Account Policies	**2/11 passed**
1.1 Password Policy	**2/7 passed**
1.1.7. L1 Ensure Store passwords using reversible encryption is set to Disabled	Passed
1.1.4. L1 Ensure Minimum password length is set to 14 or more characters	Failed
1.1.1. L1 Ensure Enforce password history is set to 24 or more passwords	Failed
1.1.2. L1 Ensure Maximum password age is set to 365 or fewer days but not 0	Passed
1.1.3. L1 Ensure Minimum password age is set to 1 or more days	Failed
1.1.6. L1 Ensure Relax minimum password length limits is set to Enabled	Failed
1.1.5. L1 Ensure Password must meet complexity requirements is set to Enabled	Failed
1.2 Account Lockout Policy	**0/4 passed**
1.2.2. L1 Ensure Account lockout threshold is set to 5 or fewer invalid logon attempts but not 0	Failed
1.2.4. L1 Ensure Reset account lockout counter after is set to 15 or more minutes 1.2.1. L1 Ensure	Failed
Account lockout duration is set to 15 or more minutes 1.2.3. L1 Ensure Allow Administrator account	Failed
lockout is set to Enabled	Unscored
17 Advanced Audit Policy Configuration	**9/27 passed**
17.1 Account Logon	**0/1 passed**
17.1.1. L1 Ensure Audit Credential Validation is set to Success and Failure	Failed
17.2 Account Management	**1/3 passed**
17.2.2. L1 Ensure Audit Security Group Management is set to include Success	Passed
17.2.1. L1 Ensure Audit Application Group Management is set to Success and Failure	Failed
17.2.3. L1 Ensure Audit User Account Management is set to Success and Failure	Failed
17.3 Detailed Tracking	**0/2 passed**
17.3.2. L1 Ensure Audit Process Creation is set to include Success	Failed
17.3.1. L1 Ensure Audit PNP Activity is set to include Success	Failed
17.5 LogonLogoff	**3/6 passed**
17.5.2. L1 Ensure Audit Group Membership is set to include Success	Failed
17.5.3. L1 Ensure Audit Logoff is set to include Success	Passed
17.5.5. L1 Ensure Audit Other LogonLogoff Events is set to Success and Failure	Failed
17.5.4. L1 Ensure Audit Logon is set to Success and Failure	Passed
17.5.6. L1 Ensure Audit Special Logon is set to include Success	Passed
17.5.1. L1 Ensure Audit Account Lockout is set to include Failure	Failed
17.6 Object Access	**0/4 passed**
17.6.4. L1 Ensure Audit Removable Storage is set to Success and Failure	Failed
17.6.2. L1 Ensure Audit File Share is set to Success and Failure	Failed
17.6.1. L1 Ensure Audit Detailed File Share is set to include Failure	Failed
17.6.3. L1 Ensure Audit Other Object Access Events is set to Success and Failure	Failed

17.7 Policy Change	**2/5 passed**
17.7.5. L1 Ensure Audit Other Policy Change Events is set to include Failure	Failed
17.7.1. L1 Ensure Audit Audit Policy Change is set to include Success	Passed
17.7.3. L1 Ensure Audit Authorization Policy Change is set to include Success	Failed
17.7.4. L1 Ensure Audit MPSSVC Rule-Level Policy Change is set to Success and Failure	Failed
17.7.2. L1 Ensure Audit Authentication Policy Change is set to include Success	Passed
17.8 Privilege Use	**0/1 passed**
17.8.1. L1 Ensure Audit Sensitive Privilege Use is set to Success and Failure	Failed
17.9 System	**3/5 passed**
17.9.1. L1 Ensure Audit IPsec Driver is set to Success and Failure	Failed
17.9.4. L1 Ensure Audit Security System Extension is set to include Success	Failed
17.9.2. L1 Ensure Audit Other System Events is set to Success and Failure	Passed
17.9.3. L1 Ensure Audit Security State Change is set to include Success	Passed
17.9.5. L1 Ensure Audit System Integrity is set to Success and Failure	Passed
18 Administrative Templates Computer	**1/194 passed**
18.1 Control Panel	**0/3 passed**
18.1.1 Personalization	**0/2 passed**
18.1.1.2. L1 Ensure Prevent enabling lock screen slide show is set to Enabled	Failed
18.1.1.1. L1 Ensure Prevent enabling lock screen camera is set to Enabled	Failed
18.1.2 Regional and Language Options	**0/1 passed**
18.1.2.2. L1 Ensure Allow users to enable online speech recognition services is set to Disabled	Failed
18.10 Windows Components	**0/106 passed**
18.10.12 Cloud Content	**0/2 passed**
18.10.12.1. L1 Ensure Turn off cloud consumer account state content is set to Enabled	Failed
18.10.12.3. L1 Ensure Turn off Microsoft consumer experiences is set to Enabled	Failed
18.10.13 Connect	**0/1 passed**
18.10.13.1. L1 Ensure Require pin for pairing is set to Enabled First Time OR Enabled Always	Failed
18.10.14 Credential User Interface	**0/3 passed**
18.10.14.2. L1 Ensure Enumerate administrator accounts on elevation is set to Disabled	Failed
18.10.14.1. L1 Ensure Do not display the password reveal button is set to Enabled	Failed
18.10.14.3. L1 Ensure Prevent the use of security questions for local accounts is set to Enabled	Failed
18.10.15 Data Collection and Preview Builds	**0/7 passed**
18.10.15.4. L1 Ensure Do not show feedback notifications is set to Enabled	Failed
18.10.15.7. L1 Ensure Limit Dump Collection is set to Enabled	Failed
18.10.15.5. L1 Ensure Enable OneSettings Auditing is set to Enabled	Failed
18.10.15.6. L1 Ensure Limit Diagnostic Log Collection is set to Enabled	Failed

18.10.15.8. L1 Ensure Toggle user control over Insider builds is set to Disabled	Failed
18.10.15.3. L1 Ensure Disable OneSettings Downloads is set to Enabled	Failed
18.10.15.1. L1 Ensure Allow Diagnostic Data is set to Enabled Diagnostic data off not recommended or Enabled Send required diagnostic data	Failed
18.10.16 Delivery Optimization	**0/1 passed**
18.10.16.1. L1 Ensure Download Mode is NOT set to Enabled Internet	Failed
18.10.17 Desktop App Installer	**0/4 passed**
18.10.17.4. L1 Ensure Enable App Installer ms-appinstaller protocol is set to Disabled	Failed
18.10.17.2. L1 Ensure Enable App Installer Experimental Features is set to Disabled	Failed
18.10.17.3. L1 Ensure Enable App Installer Hash Override is set to Disabled	Failed
18.10.17.1. L1 Ensure Enable App Installer is set to Disabled	Failed
18.10.25 Event Log Service	**0/8 passed**
18.10.25.1 Application	**0/2 passed**
18.10.25.1.2. L1 Ensure Application Specify the maximum log file size KB is set to Enabled 32768 or greater	Failed
18.10.25.1.1. L1 Ensure Application Control Event Log behavior when the log file reaches its maximum size is set to Disabled	Failed
18.10.25.2 Security	**0/2 passed**
18.10.25.2.1. L1 Ensure Security Control Event Log behavior when the log file reaches its maximum size is set to Disabled	Failed
18.10.25.2.2. L1 Ensure Security Specify the maximum log file size KB is set to Enabled 196608 or greater	Failed
18.10.25.3 Setup	**0/2 passed**
18.10.25.3.2. L1 Ensure Setup Specify the maximum log file size KB is set to Enabled 32768 or greater 18.10.25.3.1.	Failed
L1 Ensure Setup Control Event Log behavior when the log file reaches its maximum size is set to Disabled	Failed
18.10.25.4 System	**0/2 passed**
18.10.25.4.1. L1 Ensure System Control Event Log behavior when the log file reaches its maximum size is set to Disabled	Failed
18.10.25.4.2. L1 Ensure System Specify the maximum log file size KB is set to Enabled 32768 or greater	Failed
18.10.28 File Explorer formerly Windows Explorer	**0/3 passed**
18.10.28.5. L1 Ensure Turn off shell protocol protected mode is set to Disabled	Failed
18.10.28.3. L1 Ensure Turn off Data Execution Prevention for Explorer is set to Disabled	Failed
18.10.28.4. L1 Ensure Turn off heap termination on corruption is set to Disabled	Failed
18.10.3 App Package Deployment	**0/1 passed**
18.10.3.2. L1 Ensure Prevent non-admin users from installing packaged Windows apps is set to Enabled	Failed
18.10.41 Microsoft account	**0/1 passed**
18.10.41.1. L1 Ensure Block all consumer Microsoft account user authentication is set to Enabled	Failed
18.10.42 Microsoft Defender Antivirus formerly Windows Defender and Windows Defender Antivirus	**0/14 passed**

18.10.42.10 Real-time Protection	**0/4 passed**
18.10.42.10.2. L1 Ensure Turn off real-time protection is set to Disabled	Failed
18.10.42.10.1. L1 Ensure Scan all downloaded files and attachments is set to Enabled	Failed
18.10.42.10.4. L1 Ensure Turn on script scanning is set to Enabled	Failed
18.10.42.10.3. L1 Ensure Turn on behavior monitoring is set to Enabled	Failed
18.10.42.13 Scan	**0/3 passed**
18.10.42.13.3. L1 Ensure Turn on e-mail scanning is set to Enabled	Failed
18.10.42.13.1. L1 Ensure Scan packed executables is set to Enabled	Failed
18.10.42.13.2. L1 Ensure Scan removable drives is set to Enabled	Failed
18.10.42.5 MAPS	**0/1 passed**
18.10.42.5.1. L1 Ensure Configure local setting override for reporting to Microsoft MAPS is set to Disabled	Failed
18.10.42.6 Microsoft Defender Exploit Guard formerly Windows Defender Exploit Guard	**0/3 passed**
18.10.42.6.1 Attack Surface Reduction	**0/2 passed**
18.10.42.6.1.1. L1 Ensure Configure Attack Surface Reduction rules is set to Enabled	Failed
18.10.42.6.1.2. L1 Ensure Configure Attack Surface Reduction rules Set the state for each ASR	Failed
18.10.42.6.3 Network Protection	**0/1 passed**
18.10.42.6.3.1. L1 Ensure Prevent users and apps from accessing dangerous websites is set to Enabled Block	Failed
18.10.42.7 MpEngine	**0/1 passed**
18.10.42.7.1. L1 Ensure Enable file hash computation feature is set to Enabled	Failed
18.10.42.16. L1 Ensure Configure detection for potentially unwanted applications is set to Enabled Block	Failed
18.10.42.17. L1 Ensure Turn off Microsoft Defender AntiVirus is set to Disabled	Failed
18.10.43 Microsoft Defender Application Guard formerly Windows Defender Application Guard	**0/6 passed**
18.10.43.5. L1 Ensure Configure Microsoft Defender Application Guard clipboard settings Clipboard behavior setting is set to Enabled Enable clipboard operation from an isolated session to the host	Failed
18.10.43.6. L1 Ensure Turn on Microsoft Defender Application Guard in Managed Mode is set to Enabled 1	Failed
18.10.43.3. L1 Ensure Allow data persistence for Microsoft Defender Application Guard is set to Disabled	Failed
18.10.43.1. L1 Ensure Allow auditing events in Microsoft Defender Application Guard is set to Enabled	Failed
18.10.43.2. L1 Ensure Allow camera and microphone access in Microsoft Defender Application Guard is set to Disabled	Failed
18.10.43.4. L1 Ensure Allow files to download and save to the host operating system from Microsoft Defender Application Guard is set to Disabled	Failed
18.10.4 App Privacy	**0/1 passed**
18.10.4.1. L1 Ensure Let Windows apps activate with voice while the system is locked is set to Enabled Force Deny	Failed
18.10.50 OneDrive formerly SkyDrive	**0/1 passed**
18.10.50.1. L1 Ensure Prevent the usage of OneDrive for file storage is set to Enabled	Failed
18.10.56 Remote Desktop Services formerly Terminal Services	**0/8 passed**

18.10.56.2 Remote Desktop Connection Client	**0/1 passed**
18.10.56.2.3. L1 Ensure Do not allow passwords to be saved is set to Enabled	Failed
18.10.56.3 Remote Desktop Session Host formerly Terminal Server	**0/7 passed**
18.10.56.3.11 Temporary folders	**0/1 passed**
18.10.56.3.11.1. L1 Ensure Do not delete temp folders upon exit is set to Disabled	Failed
18.10.56.3.3 Device and Resource Redirection	**0/1 passed**
18.10.56.3.3.3. L1 Ensure Do not allow drive redirection is set to Enabled	Failed
18.10.56.3.9 Security	**0/5 passed**
18.10.56.3.9.5. L1 Ensure Set client connection encryption level is set to Enabled High Level	Failed
18.10.56.3.9.2. L1 Ensure Require secure RPC communication is set to Enabled	Failed
18.10.56.3.9.1. L1 Ensure Always prompt for password upon connection is set to Enabled	Failed
18.10.56.3.9.4. L1 Ensure Require user authentication for remote connections by using Network Level Authentication is set to Enabled	Failed
18.10.56.3.9.3. L1 Ensure Require use of specific security layer for remote RDP connections is set to Enabled SSL	Failed
18.10.57 RSS Feeds	**0/1 passed**
18.10.57.1. L1 Ensure Prevent downloading of enclosures is set to Enabled	Failed
18.10.58 Search	**0/4 passed**
18.10.58.3. L1 Ensure Allow Cortana is set to Disabled	Failed
18.10.58.5. L1 Ensure Allow indexing of encrypted files is set to Disabled	Failed
18.10.58.6. L1 Ensure Allow search and Cortana to use location is set to Disabled	Failed
18.10.58.4. L1 Ensure Allow Cortana above lock screen is set to Disabled	Failed
18.10.5 App runtime	**0/1 passed**
18.10.5.1. L1 Ensure Allow Microsoft accounts to be optional is set to Enabled	Failed
18.10.65 Store	**0/3 passed**
18.10.65.4. L1 Ensure Turn off the offer to update to the latest version of Windows is set to Enabled	Failed
18.10.65.3. L1 Ensure Turn off Automatic Download and Install of updates is set to Disabled	Failed
18.10.65.2. L1 Ensure Only display the private store within the Microsoft Store is set to Enabled	Failed
18.10.71 Widgets	**0/1 passed**
18.10.71.1. L1 Ensure Allow widgets is set to Disabled	Failed
18.10.75 Windows Defender SmartScreen	**0/6 passed**
18.10.75.1 Enhanced Phishing Protection	**0/5 passed**
18.10.75.1.3. L1 Ensure Notify Password Reuse is set to Enabled	Failed
18.10.75.1.2. L1 Ensure Notify Malicious is set to Enabled	Failed
18.10.75.1.5. L1 Ensure Service Enabled is set to Enabled	Failed
18.10.75.1.4. L1 Ensure Notify Unsafe App is set to Enabled	Failed
18.10.75.1.1. L1 Ensure Automatic Data Collection is set to Enabled	Failed

18.10.75.2 Explorer	**0/1 passed**
18.10.75.2.1. L1 Ensure Configure Windows Defender SmartScreen is set to Enabled Warn and prevent bypass	Failed
18.10.77 Windows Game Recording and Broadcasting	**0/1 passed**
18.10.77.1. L1 Ensure Enables or disables Windows Game Recording and Broadcasting is set to Disabled	Failed
18.10.78 Windows Hello for Business formerly Microsoft Passport for Work	**0/1 passed**
18.10.78.1. L1 Ensure Enable ESS with Supported Peripherals is set to Enabled 1	Failed
18.10.79 Windows Ink Workspace	**0/1 passed**
18.10.79.2. L1 Ensure Allow Windows Ink Workspace is set to Enabled On but disallow access above lock OR Enabled Disabled	Failed
18.10.7 AutoPlay Policies	**0/3 passed**
18.10.7.2. L1 Ensure Set the default behavior for AutoRun is set to Enabled Do not execute any autorun commands	Failed
18.10.7.1. L1 Ensure Disallow Autoplay for non-volume devices is set to Enabled	Failed
18.10.7.3. L1 Ensure Turn off Autoplay is set to Enabled All drives	Failed
18.10.8 Biometrics	**0/1 passed**
18.10.8.1 Facial Features	**0/1 passed**
18.10.8.1.1. L1 Ensure Configure enhanced anti-spoofing is set to Enabled	Failed
18.10.80 Windows Installer	**0/2 passed**
18.10.80.1. L1 Ensure Allow user control over installs is set to Disabled	Failed
18.10.80.2. L1 Ensure Always install with elevated privileges is set to Disabled	Failed
18.10.81 Windows Logon Options	**0/2 passed**
18.10.81.1. L1 Ensure Enable MPR notifications for the system is set to Disabled	Failed
18.10.81.2. L1 Ensure Sign-in and lock last interactive user automatically after a restart is set to Disabled	Failed
18.10.88 Windows Remote Management WinRM	**0/6 passed**
18.10.88.1 WinRM Client	**0/3 passed**
18.10.88.1.2. L1 Ensure Allow unencrypted traffic is set to Disabled	Failed
18.10.88.1.3. L1 Ensure Disallow Digest authentication is set to Enabled	Failed
18.10.88.1.1. L1 Ensure Allow Basic authentication is set to Disabled	Failed
18.10.88.2 WinRM Service	**0/3 passed**
18.10.88.2.1. L1 Ensure Allow Basic authentication is set to Disabled	Failed
18.10.88.2.3. L1 Ensure Allow unencrypted traffic is set to Disabled	Failed
18.10.88.2.4. L1 Ensure Disallow WinRM from storing RunAs credentials is set to Enabled	Failed
18.10.90 Windows Sandbox	**0/2 passed**
18.10.90.2. L1 Ensure Allow networking in Windows Sandbox is set to Disabled	Failed
18.10.90.1. L1 Ensure Allow clipboard sharing with Windows Sandbox is set to Disabled	Failed
18.10.91 Windows Security formerly Windows Defender Security Center	**0/1 passed**

18.10.91.2 App and browser protection	**0/1 passed**
18.10.91.2.1. L1 Ensure Prevent users from modifying settings is set to Enabled	Failed
18.10.92 Windows Update	**0/9 passed**
18.10.92.1 Legacy Policies	**0/1 passed**
18.10.92.1.1. L1 Ensure No auto-restart with logged on users for scheduled automatic updates installations is set to Disabled	Failed
18.10.92.2 Manage end user experience	**0/4 passed**
18.10.92.2.2. L1 Ensure Configure Automatic Updates Scheduled install day is set to 0 - Every day	Failed
18.10.92.2.3. L1 Ensure Enable features introduced via servicing that are off by default is set to Disabled	Failed
18.10.92.2.4. L1 Ensure Remove access to Pause updates feature is set to Enabled	Failed
18.10.92.2.1. L1 Ensure Configure Automatic Updates is set to Enabled	Failed
18.10.92.4 Manage updates offered from Windows Update formerly Defer Windows Updates and Windows Update for Business	**0/4 passed**
18.10.92.4.2. L1 Ensure Select when Preview Builds and Feature Updates are received is set to Enabled 180 or more days	Failed
18.10.92.4.4. L1 Ensure Enable optional updates is set to Disabled	Failed
18.10.92.4.1. L1 Ensure Manage preview builds is set to Disabled	Failed
18.10.92.4.3. L1 Ensure Select when Quality Updates are received is set to Enabled 0 days	Failed
18.4 MS Security Guide	**0/8 passed**
18.4.1. L1 Ensure Apply UAC restrictions to local accounts on network logons is set to Enabled	Failed
18.4.2. L1 Ensure Configure RPC packet level privacy setting for incoming connections is set to Enabled	Failed
18.4.5. L1 Ensure Enable Certificate Padding is set to Enabled	Failed
18.4.4. L1 Ensure Configure SMB v1 server is set to Disabled	Failed
18.4.6. L1 Ensure Enable Structured Exception Handling Overwrite Protection SEHOP is set to Enabled	Failed
18.4.3. L1 Ensure Configure SMB v1 client driver is set to Enabled Disable driver recommended	Failed
18.4.7. L1 Ensure NetBT NodeType configuration is set to Enabled P-node recommended	Failed
18.4.8. L1 Ensure WDigest Authentication is set to Disabled	Failed
18.5 MSS Legacy	**0/8 passed**
18.5.1. L1 Ensure MSS AutoAdminLogon Enable Automatic Logon is set to Disabled	Failed
18.5.13. L1 Ensure MSS WarningLevel Percentage threshold for the security event log at which the system will generate a warning is set to Enabled 90 or less	Failed
18.5.7. L1 Ensure MSS NoNameReleaseOnDemand Allow the computer to ignore NetBIOS name release requests except from WINS servers is set to Enabled	Failed
18.5.10. L1 Ensure MSS ScreenSaverGracePeriod The time in seconds before the screen saver grace period expires is set to Enabled 5 or fewer seconds	Failed
18.5.5. L1 Ensure MSS EnableICMPRedirect Allow ICMP redirects to override OSPF generated routes is set to Disabled	Failed
18.5.9. L1 Ensure MSS SafeDllSearchMode Enable Safe DLL search mode is set to Enabled	Failed
18.5.3. L1 Ensure MSS DisableIPSourceRouting IP source routing protection level is set to Enabled Highest protection source routing is completely disabled	Failed
18.5.2. L1 Ensure MSS DisableIPSourceRouting IPv6 IP source routing protection level is set to Enabled Highest protection source routing is completely disabled	Failed

18.6 Network	**0/11 passed**
18.6.11 Network Connections	**0/3 passed**
18.6.11.2. L1 Ensure Prohibit installation and configuration of Network Bridge on your DNS domain network is set to Enabled	Failed
18.6.11.4. L1 Ensure Require domain users to elevate when setting a networks location is set to Enabled	Failed
18.6.11.3. L1 Ensure Prohibit use of Internet Connection Sharing on your DNS domain network is set to Enabled	Failed
18.6.14 Network Provider	**0/1 passed**
18.6.14.1. L1 Ensure Hardened UNC Paths is set to Enabled with Require Mutual Authentication Require Integrity and Require Privacy set for all NETLOGON and SYSVOL shares	Failed
18.6.21 Windows Connection Manager	**0/2 passed**
18.6.21.2. L1 Ensure Prohibit connection to non-domain networks when connected to domain authenticated network is set to Enabled	Failed
18.6.21.1. L1 Ensure Minimize the number of simultaneous connections to the Internet or a Windows Domain is set to Enabled 3 Prevent Wi-Fi when on Ethernet	Failed
18.6.23 WLAN Service	**0/1 passed**
18.6.23.2 WLAN Settings	**0/1 passed**
18.6.23.2.1. L1 Ensure Allow Windows to automatically connect to suggested open hotspots to networks shared by contacts and to hotspots offering paid services is set to Disabled	Failed
18.6.4 DNS Client	**0/3 passed**
18.6.4.3. L1 Ensure Turn off multicast name resolution is set to Enabled	Failed
18.6.4.1. L1 Ensure Configure DNS over HTTPS DoH name resolution is set to Enabled Allow DoH or higher	Failed
18.6.4.2. L1 Ensure Configure NetBIOS settings is set to Enabled Disable NetBIOS name resolution on public networks	Failed
18.6.8 Lanman Workstation	**0/1 passed**
18.6.8.1. L1 Ensure Enable insecure guest logons is set to Disabled	Failed
18.7 Printers	**0/11 passed**
18.7.10. L1 Ensure Point and Print Restrictions When installing drivers for a new connection is set to Enabled Show warning and elevation prompt	Failed
18.7.11. L1 Ensure Point and Print Restrictions When updating drivers for an existing connection is set to Enabled Show warning and elevation prompt	Failed
18.7.8. L1 Ensure Limits print driver installation to Administrators is set to Enabled	Failed
18.7.9. L1 Ensure Manage processing of Queue-specific files is set to Enabled Limit Queue-specific files to Color profiles	Failed
18.7.6. L1 Ensure Configure RPC listener settings Authentication protocol to use for incoming RPC connections is set to Enabled Negotiate or higher	Failed
18.7.7. L1 Ensure Configure RPC over TCP port is set to Enabled 0	Failed
18.7.5. L1 Ensure Configure RPC listener settings Protocols to allow for incoming RPC connections is set to Enabled RPC over TCP	Failed
18.7.3. L1 Ensure Configure RPC connection settings Protocol to use for outgoing RPC connections is set to Enabled RPC over TCP	Failed
18.7.4. L1 Ensure Configure RPC connection settings Use authentication for outgoing RPC connections is set to Enabled Default	Failed
18.7.1. L1 Ensure Allow Print Spooler to accept client connections is set to Disabled	Failed

18.7.2. L1 Ensure Configure Redirection Guard is set to Enabled Redirection Guard Enabled	Failed
18.9 System	**1/47 passed**
18.9.13 Early Launch Antimalware	**0/1 passed**
18.9.13.1. L1 Ensure Boot-Start Driver Initialization Policy is set to Enabled Good unknown and bad but critical	Failed
18.9.19 Group Policy	**1/6 passed**
18.9.19.6. L1 Ensure Continue experiences on this device is set to Disabled	Failed
18.9.19.4. L1 Ensure Configure security policy processing Do not apply during periodic background processing is set to Enabled FALSE	Failed
18.9.19.7. L1 Ensure Turn off background refresh of Group Policy is set to Disabled	Passed
18.9.19.2. L1 Ensure Configure registry policy processing Do not apply during periodic background processing is set to Enabled FALSE	Failed
18.9.19.3. L1 Ensure Configure registry policy processing Process even if the Group Policy objects have not changed is set to Enabled TRUE	Failed
18.9.19.5. L1 Ensure Configure security policy processing Process even if the Group Policy objects have not changed is set to Enabled TRUE	Failed
18.9.20 Internet Communication Management	**0/2 passed**
18.9.20.1 Internet Communication settings	**0/2 passed**
18.9.20.1.6. L1 Ensure Turn off Internet download for Web publishing and online ordering wizards is set to Enabled	Failed
18.9.20.1.2. L1 Ensure Turn off downloading of print drivers over HTTP is set to Enabled	Failed
18.9.25 LAPS	**0/8 passed**
18.9.25.4. L1 Ensure Password Settings Password Complexity is set to Enabled Large letters small letters numbers special characters	Failed
18.9.25.7. L1 Ensure Post-authentication actions Grace period hours is set to Enabled 8 or fewer hours but not 0	Failed
18.9.25.5. L1 Ensure Password Settings Password Length is set to Enabled 15 or more	Failed
18.9.25.6. L1 Ensure Password Settings Password Age Days is set to Enabled 30 or fewer	Failed
18.9.25.1. L1 Ensure Configure password backup directory is set to Enabled Active Directory or Enabled Azure Active Directory	Failed
18.9.25.8. L1 Ensure Post-authentication actions Actions is set to Enabled Reset the password and logoff the managed account or higher	Failed
18.9.25.3. L1 Ensure Enable password encryption is set to Enabled	Failed
18.9.25.2. L1 Ensure Do not allow password expiration time longer than required by policy is set to Enabled	Failed
18.9.26 Local Security Authority	**0/2 passed**
18.9.26.2. L1 Ensure Configures LSASS to run as a protected process is set to Enabled Enabled with UEFI Lock	Failed
18.9.26.1. L1 Ensure Allow Custom SSPs and APs to be loaded into LSASS is set to Disabled	Failed
18.9.28 Logon	**0/7 passed**
18.9.28.2. L1 Ensure Do not display network selection UI is set to Enabled 18.9.28.6. L1 Ensure Turn off picture password sign-in is set to Enabled 18.9.28.7. L1 Ensure Turn on convenience PIN sign-in is set to Disabled 18.9.28.1. L1 Ensure Block user from showing account details on sign-in is set to Enabled	Failed Failed Failed Failed

18.9.28.3. L1 Ensure Do not enumerate connected users on domain-joined computers is set to Enabled	Failed
18.9.28.4. L1 Ensure Enumerate local users on domain-joined computers is set to Disabled	Failed
18.9.28.5. L1 Ensure Turn off app notifications on the lock screen is set to Enabled	Failed
18.9.33 Power Management	**0/4 passed**
18.9.33.6 Sleep Settings	**0/4 passed**
18.9.33.6.2. L1 Ensure Allow network connectivity during connected-standby plugged in is set to Disabled	Failed
18.9.33.6.6. L1 Ensure Require a password when a computer wakes plugged in is set to Enabled	Failed
18.9.33.6.5. L1 Ensure Require a password when a computer wakes on battery is set to Enabled	Failed
18.9.33.6.1. L1 Ensure Allow network connectivity during connected-standby on battery is set to Disabled	Failed
18.9.35 Remote Assistance	**0/2 passed**
18.9.35.2. L1 Ensure Configure Solicited Remote Assistance is set to Disabled	Failed
18.9.35.1. L1 Ensure Configure Offer Remote Assistance is set to Disabled	Failed
18.9.36 Remote Procedure Call	**0/2 passed**
18.9.36.1. L1 Ensure Enable RPC Endpoint Mapper Client Authentication is set to Enabled	Failed
18.9.36.2. L1 Ensure Restrict Unauthenticated RPC clients is set to Enabled Authenticated	Failed
18.9.3 Audit Process Creation	**0/1 passed**
18.9.3.1. L1 Ensure Include command line in process creation events is set to Enabled	Failed
18.9.4 Credentials Delegation	**0/2 passed**
18.9.4.1. L1 Ensure Encryption Oracle Remediation is set to Enabled Force Updated Clients	Failed
18.9.4.2. L1 Ensure Remote host allows delegation of non-exportable credentials is set to Enabled	Failed
18.9.51 Windows Time Service	**0/2 passed**
18.9.51.1 Time Providers	**0/2 passed**
18.9.51.1.2. L1 Ensure Enable Windows NTP Server is set to Disabled	Failed
18.9.51.1.1. L1 Ensure Enable Windows NTP Client is set to Enabled	Failed
18.9.5 Device Guard	**0/7 passed**
18.9.5.7. L1 Ensure Turn On Virtualization Based Security Kernel-mode Hardware-enforced Stack Protection is set to Enabled Enabled in enforcement mode	Failed
18.9.5.1. L1 Ensure Turn On Virtualization Based Security is set to Enabled	Failed
18.9.5.4. L1 Ensure Turn On Virtualization Based Security Require UEFI Memory Attributes Table is set to True checked	Failed
18.9.5.5. L1 Ensure Turn On Virtualization Based Security Credential Guard Configuration is set to Enabled with UEFI lock	Failed
18.9.5.2. L1 Ensure Turn On Virtualization Based Security Select Platform Security Level is set to Secure Boot or higher	Failed
18.9.5.3. L1 Ensure Turn On Virtualization Based Security Virtualization Based Protection of Code Integrity is set to Enabled with UEFI lock	Failed
18.9.5.6. L1 Ensure Turn On Virtualization Based Security Secure Launch Configuration is set to Enabled	Failed
18.9.7 Device Installation	**0/1 passed**
18.9.7.2. L1 Ensure Prevent device metadata retrieval from the Internet is set to Enabled	Failed

19 Administrative Templates User	**0/9 passed**
19.5 Start Menu and Taskbar	**0/1 passed**
19.5.1 Notifications	**0/1 passed**
19.5.1.1. L1 Ensure Turn off toast notifications on the lock screen is set to Enabled	Failed
19.7 Windows Components	**0/8 passed**
19.7.26 Network Sharing	**0/1 passed**
19.7.26.1. L1 Ensure Prevent users from sharing files within their profile. is set to Enabled	Failed
19.7.38 Windows Copilot	**0/1 passed**
19.7.38.1. L1 Ensure Turn off Windows Copilot is set to Enabled	Failed
19.7.42 Windows Installer	**0/1 passed**
19.7.42.1. L1 Ensure Always install with elevated privileges is set to Disabled	Failed
19.7.5 Attachment Manager	**0/2 passed**
19.7.5.1. L1 Ensure Do not preserve zone information in file attachments is set to Disabled	Failed
19.7.5.2. L1 Ensure Notify antivirus programs when opening attachments is set to Enabled	Failed
19.7.8 Cloud Content	**0/3 passed**
19.7.8.2. L1 Ensure Do not suggest third-party content in Windows spotlight is set to Enabled	Failed
19.7.8.5. L1 Ensure Turn off Spotlight collection on Desktop is set to Enabled	Failed
19.7.8.1. L1 Ensure Configure Windows spotlight on lock screen is set to Disabled	Failed
2 Local Policies	**55/99 passed**
2.2 User Rights Assignment	**23/37 passed**
2.2.19. L1 Ensure Deny log on locally to include Guests	Failed
2.2.34. L1 Ensure Profile single process is set to Administrators	Passed
2.2.20. L1 Ensure Deny log on through Remote Desktop Services to include Guests Local account	Failed
2.2.4. L1 Ensure Adjust memory quotas for a process is set to Administrators LOCAL SERVICE NETWORK SERVICE	Failed
2.2.18. L1 Ensure Deny log on as a service to include Guests	Failed
2.2.17. L1 Ensure Deny log on as a batch job to include Guests	Failed
2.2.9. L1 Ensure Change the time zone is set to Administrators LOCAL SERVICE Users	Passed
2.2.10. L1 Ensure Create a pagefile is set to Administrators	Passed
2.2.11. L1 Ensure Create a token object is set to No One	Passed
2.2.12. L1 Ensure Create global objects is set to Administrators LOCAL SERVICE NETWORK SERVICE SERVICE	Passed
2.2.5. L1 Ensure Allow log on locally is set to Administrators Users	Failed
2.2.6. L1 Ensure Allow log on through Remote Desktop Services is set to Administrators Remote Desktop Users	Passed
2.2.7. L1 Ensure Back up files and directories is set to Administrators	Failed
2.2.8. L1 Ensure Change the system time is set to Administrators LOCAL SERVICE	Passed
2.2.15. L1 Ensure Debug programs is set to Administrators	Passed

2.2.14. L1 Configure Create symbolic links	Passed
2.2.13. L1 Ensure Create permanent shared objects is set to No One	Passed
2.2.16. L1 Ensure Deny access to this computer from the network to include Guests Local account	Failed
2.2.22. L1 Ensure Force shutdown from a remote system is set to Administrators	Passed
2.2.1. L1 Ensure Access Credential Manager as a trusted caller is set to No One	Passed
2.2.21. L1 Ensure Enable computer and user accounts to be trusted for delegation is set to No One	Passed
2.2.30. L1 Ensure Manage auditing and security log is set to Administrators	Passed
2.2.3. L1 Ensure Act as part of the operating system is set to No One	Passed
2.2.2. L1 Ensure Access this computer from the network is set to Administrators Remote Desktop Users	Failed
2.2.27. L1 Ensure Lock pages in memory is set to No One	Passed
2.2.32. L1 Ensure Modify firmware environment values is set to Administrators	Passed
2.2.31. L1 Ensure Modify an object label is set to No One	Passed
2.2.26. L1 Ensure Load and unload device drivers is set to Administrators	Passed
2.2.25. L1 Ensure Increase scheduling priority is set to Administrators Window ManagerWindow Manager Group	Passed
2.2.24. L1 Ensure Impersonate a client after authentication is set to Administrators LOCAL SERVICE NETWORK SERVICE SERVICE	Failed
2.2.23. L1 Ensure Generate security audits is set to LOCAL SERVICE NETWORK SERVICE	Failed
2.2.39. L1 Ensure Take ownership of files or other objects is set to Administrators	Passed
2.2.38. L1 Ensure Shut down the system is set to Administrators Users	Failed
2.2.33. L1 Ensure Perform volume maintenance tasks is set to Administrators	Passed
2.2.37. L1 Ensure Restore files and directories is set to Administrators	Failed
2.2.36. L1 Ensure Replace a process level token is set to LOCAL SERVICE NETWORK SERVICE	Failed
2.2.35. L1 Ensure Profile system performance is set to Administrators NT SERVICEWdiServiceHost	Passed
2.3 Security Options	**32/62 passed**
2.3.10 Network access	**9/12 passed**
2.3.10.7. L1 Ensure Network access Remotely accessible registry paths is configured	Passed
2.3.10.8. L1 Ensure Network access Remotely accessible registry paths and sub-paths is configured	Passed
2.3.10.12. L1 Ensure Network access Sharing and security model for local accounts is set to Classic - local users authenticate as themselves	Passed
2.3.10.2. L1 Ensure Network access Do not allow anonymous enumeration of SAM accounts is set to Enabled	Passed
2.3.10.6. L1 Ensure Network access Named Pipes that can be accessed anonymously is set to None	Passed
2.3.10.9. L1 Ensure Network access Restrict anonymous access to Named Pipes and Shares is set to Enabled	Passed
2.3.10.5. L1 Ensure Network access Let Everyone permissions apply to anonymous users is set to Disabled	Passed
2.3.10.11. L1 Ensure Network access Shares that can be accessed anonymously is set to None	Passed
2.3.10.4. L1 Ensure Network access Do not allow storage of passwords and credentials for network authentication is set to Enabled	Failed
2.3.10.1. L1 Ensure Network access Allow anonymous SIDName translation is set to Disabled	Passed
2.3.10.10. L1 Ensure Network access Restrict clients allowed to make remote calls to SAM is set to Administrators Remote Access Allow	Failed

2.3.10.3. L1 Ensure Network access Do not allow anonymous enumeration of SAM accounts and shares is set to Enabled	Failed
2.3.11 Network security	**2/12 passed**
2.3.11.10. L1 Ensure Network security Minimum session security for NTLM SSP based including secure RPC servers is set to Require NTLMv2 session security Require 128-bit encryption	Failed
2.3.11.11. L1 Ensure Network security Restrict NTLM Audit Incoming NTLM Traffic is set to Enable auditing for all accounts	Failed
2.3.11.12. L1 Ensure Network security Restrict NTLM Outgoing NTLM traffic to remote servers is set to Audit all or higher	Failed
2.3.11.1. L1 Ensure Network security Allow Local System to use computer identity for NTLM is set to Enabled	Failed
2.3.11.2. L1 Ensure Network security Allow LocalSystem NULL session fallback is set to Disabled	Failed
2.3.11.7. L1 Ensure Network security LAN Manager authentication level is set to Send NTLMv2 response only. Refuse LM NTLM	Failed
2.3.11.8. L1 Ensure Network security LDAP client signing requirements is set to Negotiate signing or higher	Passed
2.3.11.9. L1 Ensure Network security Minimum session security for NTLM SSP based including secure RPC clients is set to Require NTLMv2 session security Require 128-bit encryption	Failed
2.3.11.3. L1 Ensure Network Security Allow PKU2U authentication requests to this computer to use online identities is set to Disabled	Failed
2.3.11.4. L1 Ensure Network security Configure encryption types allowed for Kerberos is set to AES128 HMAC SHA1 AES256 HMAC SHA1 Future encryption types	Failed
2.3.11.5. L1 Ensure Network security Do not store LAN Manager hash value on next password change is set to Enabled	Passed
2.3.11.6. L1 Ensure Network security Force logoff when logon hours expire is set to Enabled	Unscored
2.3.15 System objects	**2/2 passed**
2.3.15.1. L1 Ensure System objects Require case insensitivity for non-Windows subsystems is set to Enabled	Passed
2.3.15.2. L1 Ensure System objects Strengthen default permissions of internal system objects e.g. Symbolic Links is set to Enabled	Passed
2.3.17 User Account Control	**5/8 passed**
2.3.17.4. L1 Ensure User Account Control Detect application installations and prompt for elevation is set to Enabled	Passed
2.3.17.8. L1 Ensure User Account Control Virtualize file and registry write failures to per-user locations is set to Enabled	Passed
2.3.17.5. L1 Ensure User Account Control Only elevate UIAccess applications that are installed in secure locations is set to Enabled	Passed
2.3.17.6. L1 Ensure User Account Control Run all administrators in Admin Approval Mode is set to Enabled	Passed
2.3.17.7. L1 Ensure User Account Control Switch to the secure desktop when prompting for elevation is set to Enabled	Passed
2.3.17.1. L1 Ensure User Account Control Admin Approval Mode for the Built-in Administrator account is set to Enabled	Failed
2.3.17.2. L1 Ensure User Account Control Behavior of the elevation prompt for administrators in Admin Approval Mode is set to Prompt for consent on the secure desktop or higher	Failed
2.3.17.3. L1 Ensure User Account Control Behavior of the elevation prompt for standard users is set to Automatically deny elevation requests	Failed
2.3.1 Accounts	**2/5 passed**
2.3.1.3. L1 Ensure Accounts Limit local account use of blank passwords to console logon only is set to Enabled	Passed

2.3.1.1. L1 Ensure Accounts Block Microsoft accounts is set to Users cant add or log on with Microsoft accounts	Failed
2.3.1.4. L1 Configure Accounts Rename administrator account	Failed
2.3.1.5. L1 Configure Accounts Rename guest account	Failed
2.3.1.2. L1 Ensure Accounts Guest account status is set to Disabled	Passed
2.3.2 Audit	**1/2 passed**
2.3.2.1. L1 Ensure Audit Force audit policy subcategory settings Windows Vista or later to override audit policy category settings is set to Enabled	Failed
2.3.2.2. L1 Ensure Audit Shut down system immediately if unable to log security audits is set to Disabled	Passed
2.3.6 Domain member	**6/6 passed**
2.3.6.1. L1 Ensure Domain member Digitally encrypt or sign secure channel data always is set to Enabled	Passed
2.3.6.5. L1 Ensure Domain member Maximum machine account password age is set to 30 or fewer days but not 0	Passed
2.3.6.2. L1 Ensure Domain member Digitally encrypt secure channel data when possible is set to Enabled	Passed
2.3.6.4. L1 Ensure Domain member Disable machine account password changes is set to Disabled	Passed
2.3.6.3. L1 Ensure Domain member Digitally sign secure channel data when possible is set to Enabled	Passed
2.3.6.6. L1 Ensure Domain member Require strong Windows 2000 or later session key is set to Enabled	Passed
2.3.7 Interactive logon	**1/7 passed**
2.3.7.4. L1 Ensure Interactive logon Machine inactivity limit is set to 900 or fewer seconds but not 0	Failed
2.3.7.2. L1 Ensure Interactive logon Dont display last signed-in is set to Enabled	Failed
2.3.7.9. L1 Ensure Interactive logon Smart card removal behavior is set to Lock Workstation or higher	Failed
2.3.7.8. L1 Ensure Interactive logon Prompt user to change password before expiration is set to between 5 and 14 days	Passed
2.3.7.6. L1 Configure Interactive logon Message title for users attempting to log on	Failed
2.3.7.1. L1 Ensure Interactive logon Do not require CTRLALTDEL is set to Disabled	Failed
2.3.7.5. L1 Configure Interactive logon Message text for users attempting to log on	Failed
2.3.8 Microsoft network client	**2/3 passed**
2.3.8.3. L1 Ensure Microsoft network client Send unencrypted password to third-party SMB servers is set to Disabled	Passed
2.3.8.1. L1 Ensure Microsoft network client Digitally sign communications always is set to Enabled	Failed
2.3.8.2. L1 Ensure Microsoft network client Digitally sign communications if server agrees is set to Enabled	Passed
2.3.9 Microsoft network server	**2/5 passed**
2.3.9.3. L1 Ensure Microsoft network server Digitally sign communications if client agrees is set to Enabled	Failed
2.3.9.1. L1 Ensure Microsoft network server Amount of idle time required before suspending session is set to 15 or fewer minutes	Passed
2.3.9.5. L1 Ensure Microsoft network server Server SPN target name validation level is set to Accept if provided by client or higher	Failed
2.3.9.2. L1 Ensure Microsoft network server Digitally sign communications always is set to Enabled	Failed
2.3.9.4. L1 Ensure Microsoft network server Disconnect clients when logon hours expire is set to Enabled	Passed

5 System Services	10/20 passed
5.12. L1 Ensure OpenSSH SSH Server sshd is set to Disabled or Not Installed	Passed
5.43. L1 Ensure Xbox Live Game Save XblGameSave is set to Disabled	Failed
5.42. L1 Ensure Xbox Live Auth Manager XblAuthManager is set to Disabled	Failed
5.44. L1 Ensure Xbox Live Networking Service XboxNetApiSvc is set to Disabled	Failed
5.29. L1 Ensure Special Administration Console Helper sacsvr is set to Disabled or Not Installed	Passed
5.30. L1 Ensure SSDP Discovery SSDPSRV is set to Disabled	Failed
5.31. L1 Ensure UPnP Device Host upnphost is set to Disabled	Failed
5.32. L1 Ensure Web Management Service WMSvc is set to Disabled or Not Installed	Passed
5.27. L1 Ensure Simple TCPIP Services simptcp is set to Disabled or Not Installed	Passed
5.35. L1 Ensure Windows Media Player Network Sharing Service WMPNetworkSvc is set to Disabled or Not Installed	Failed
5.36. L1 Ensure Windows Mobile Hotspot Service icssvc is set to Disabled	Failed
5.41. L1 Ensure Xbox Accessory Management Service XboxGipSvc is set to Disabled	Failed
5.40. L1 Ensure World Wide Web Publishing Service W3SVC is set to Disabled or Not Installed	Failed
5.23. L1 Ensure Remote Procedure Call RPC Locator RpcLocator is set to Disabled	Failed
5.25. L1 Ensure Routing and Remote Access RemoteAccess is set to Disabled	Passed
5.7. L1 Ensure Infrared monitor service irmon is set to Disabled or Not Installed	Passed
5.9. L1 Ensure LxssManager LxssManager is set to Disabled or Not Installed	Passed
5.10. L1 Ensure Microsoft FTP Service FTPSVC is set to Disabled or Not Installed	Passed
5.3. L1 Ensure Computer Browser Browser is set to Disabled or Not Installed	Passed
5.6. L1 Ensure IIS Admin Service IISADMIN is set to Disabled or Not Installed	Passed
9 Windows Defender Firewall with Advanced Security formerly Windows Firewall with Advanced Security	**0/23 passed**
9.1 Domain Profile	**0/7 passed**
9.1.5. L1 Ensure Windows Firewall Domain Logging Size limit KB is set to 16384 KB or greater	Failed
9.1.1. L1 Ensure Windows Firewall Domain Firewall state is set to On recommended	Failed
9.1.6. L1 Ensure Windows Firewall Domain Logging Log dropped packets is set to Yes	Failed
9.1.2. L1 Ensure Windows Firewall Domain Inbound connections is set to Block default	Failed
9.1.7. L1 Ensure Windows Firewall Domain Logging Log successful connections is set to Yes	Failed
9.1.3. L1 Ensure Windows Firewall Domain Settings Display a notification is set to No	Failed
9.1.4. L1 Ensure Windows Firewall Domain Logging Name is set to SystemRootSystem32logfilesfirewalldomainfw.log	Failed
9.2 Private Profile	**0/7 passed**
9.2.2. L1 Ensure Windows Firewall Private Inbound connections is set to Block default	Failed
9.2.6. L1 Ensure Windows Firewall Private Logging Log dropped packets is set to Yes	Failed
9.2.7. L1 Ensure Windows Firewall Private Logging Log successful connections is set to Yes	Failed
9.2.1. L1 Ensure Windows Firewall Private Firewall state is set to On recommended	Failed
9.2.4. L1 Ensure Windows Firewall Private Logging Name is set to SystemRootSystem32logfilesfirewallprivatefw.log	Failed

9.2.3. L1 Ensure Windows Firewall Private Settings Display a notification is set to No	Failed
9.2.5. L1 Ensure Windows Firewall Private Logging Size limit KB is set to 16384 KB or greater	Failed
9.3 Public Profile	**0/9 passed**
9.3.8. L1 Ensure Windows Firewall Public Logging Log dropped packets is set to Yes	Failed
9.3.2. L1 Ensure Windows Firewall Public Inbound connections is set to Block default	Failed
9.3.3. L1 Ensure Windows Firewall Public Settings Display a notification is set to No	Failed
9.3.4. L1 Ensure Windows Firewall Public Settings Apply local firewall rules is set to No	Failed
9.3.5. L1 Ensure Windows Firewall Public Settings Apply local connection security rules is set to No	Failed
9.3.1. L1 Ensure Windows Firewall Public Firewall state is set to On recommended	Failed
9.3.6. L1 Ensure Windows Firewall Public Logging Name is set to SystemRootSystem32logfilesfirewallpublicfw.log	Failed
9.3.7. L1 Ensure Windows Firewall Public Logging Size limit KB is set to 16384 KB or greater	Failed
9.3.9. L1 Ensure Windows Firewall Public Logging Log successful connections is set to Yes	Failed

1.1.7. L1 Ensure Store passwords using reversible encryption is set to Disabled

Rule Status :

Passed

Summary :

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user"s password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords.The recommended state for this setting is: Disabled. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

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

1.1.4. L1 Ensure Minimum password length is set to 14 or more characters

Rule Status :

Failed

Summary :

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 or newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially around password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization"s business requirements.The recommended state for this setting is: 14 or more character(s). Note: In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length. Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to 14 or more character(s).Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length.Impact:Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

1.1.1. L1 Ensure Enforce password history is set to 24 or more passwords

Rule Status :

Failed

Summary :

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.The recommended state for this setting is: 24 or more password(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center. Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit Enforce password history (Windows 10) - Windows security | Microsoft Docs.

Rationale :

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

How to fix :

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s).Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history.Impact:The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

1.1.2. L1 Ensure Maximum password age is set to 365 or fewer days but not 0

Rule Status :

Passed

Summary :

This policy setting defines how long a user can use their password before it expires.Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.The recommended state for this setting is 365 or fewer days, but not 0. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to 365 or fewer days, but not 0.Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age.Impact:If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

1.1.3. L1 Ensure Minimum password age is set to 1 or more days

Rule Status :

Failed

Summary :

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days.The recommended state for this setting is: 1 or more day(s)). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to 1 or more day(s).Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age.Impact:If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

1.1.6. L1 Ensure Relax minimum password length limits is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information, please see the following Microsoft Security Blog. The recommended state for this setting is: Enabled. Note: This setting only affects local accounts on the computer. Domain accounts are only affected by settings on the Domain Controllers, because that is where domain accounts are stored.

Rationale :

This setting will enable the enforcement of longer and generally stronger passwords or passphrases where MFA is not in use.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Relax minimum password length limits.Note: This setting is only available within the built-in OS security template of Windows 10 Release 2004 and Server 2022 (or newer), and is not available via older versions of the OS, or via downloadable Administrative Templates (ADMX/ADML). Therefore, you must use a Windows 10 Release 2004 or Server 2022 system (or newer) to view or edit this setting with the Group Policy Management Console (GPMC) or Group Policy Management Editor (GPME). Impact:The Minimum password length setting may be configured higher than 14 characters. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

1.1.5. L1 Ensure Password must meet complexity requirements is set to Enabled

Rule Status :

Failed

Summary :

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords.When this policy is enabled, passwords must meet the following minimum requirements:Not contain the user"s account name or parts of the user"s full name that exceed two consecutive charactersBe at least six characters in lengthContain characters from three of the following categories:English uppercase characters (A through Z)English lowercase characters (a through z)Base 10 digits (0 through 9)Non-alphabetic characters (for example, !, $, #, %)A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific.Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.The recommended state for this setting is: Enabled. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements.Impact:If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty.If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments.Also, the use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 0128 - 0159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

1.2.2. L1 Ensure Account lockout threshold is set to 5 or fewer invalid logon attempts but not 0

Rule Status :

Failed

Summary :

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0does not conform to the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 5 or fewer invalid logon attempt(s), but not 0. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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.

How to fix :

To establish the recommended configuration via GP, set the following UI path to 5 or fewer invalid login attempt(s), but not 0.Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold.Impact:If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker"s attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

1.2.4. L1 Ensure Reset account lockout counter after is set to 15 or more minutes

Rule Status :

Failed

Summary :

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting.If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically.The recommended state for this setting is: 15 or more minute(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s).Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after.Impact:If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user"s account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

1.2.1. L1 Ensure Account lockout duration is set to 15 or more minutes

Rule Status :

Failed

Summary :

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.The recommended state for this setting is: 15 or more minute(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s).Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration.Impact:Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization"s help desk receives to unlock accounts that were locked by mistake.

1.2.3. L1 Ensure Allow Administrator account lockout is set to Enabled

Rule Status :

Unscored

Summary :

This policy setting determines whether the built-in Administrator account is subject to the following Account Lockout Policy settings: Account lockout duration , Account lockout threshold , and Reset account lockout counter . By default, this account is excluded from the account lockout controls and will never be locked out with repeated bad password attempts. The recommended state for this setting is: Enabled. Note: This setting applies only to OSes patched as of October 11, 2022 (see MS KB5020282..

Rationale :

Enabling account lockout policies for the built-in Administrator account will reduce the likelihood of a successful brute force attack.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policies\Allow Administrator account lockout.Impact:The built-in Administrator account will be subject to the policies in Section 1.2 Account Lockout Policy of this benchmark.

17.1.1. L1 Ensure Audit Credential Validation is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the Domain Controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the Domain Controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include:4774: An account was mapped for logon.4775: An account could not be mapped for logon.4776: The Domain Controller attempted to validate the credentials for an account.4777: The Domain Controller failed to validate the credentials for an account.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.2.2. L1 Ensure Audit Security Group Management is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include:4727: A security-enabled global group was created.4728: A member was added to a security-enabled global group.4729: A member was removed from a security-enabled global group.4730: A security-enabled global group was deleted.4731: A security-enabled local group was created.4732: A member was added to a security-enabled local group.4733: A member was removed from a security-enabled local group.4734: A security-enabled local group was deleted.4735: A security-enabled local group was changed.4737: A security-enabled global group was changed.4754: A security-enabled universal group was created.4755: A security-enabled universal group was changed.4756: A member was added to a security-enabled universal group.4757: A member was removed from a security-enabled universal group.4758: A security-enabled universal group was deleted.4764: A group"s type was changed.The recommended state for this setting is to include: Success.

Rationale :
Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success:Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.2.1. L1 Ensure Audit Application Group Management is set to Success and Failure

Rule Status :

Failed

Summary :

This policy setting allows you to audit events generated by changes to application groups such as the following:Application group is created, changed, or deleted.Member is added or removed from an application group.Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure. Note: Although Microsoft " Deprecated. Windows Authorization Manager (AzMan) in Windows Server 2012 and 2012 R2, this feature still exists in the OS (unimproved), and therefore should still be audited.

Rationale :

Auditing events in this category may be useful when investigating an incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.2.3. L1 Ensure Audit User Account Management is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include:4720: A user account was created.4722: A user account was enabled.4723: An attempt was made to change an account"s password.4724: An attempt was made to reset an account"s password.4725: A user account was disabled.4726: A user account was deleted.4738: A user account was changed.4740: A user account was locked out.4765: SID History was added to an account.4766: An attempt to add SID History to an account failed.4767: A user account was unlocked.4780: The ACL was set on accounts which are members of administrators groups.4781: The name of an account was changed:4794: An attempt was made to set the Directory Services Restore Mode.5376: Credential Manager credentials were backed up.5377: Credential Manager credentials were restored from a backup.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.3.2. L1 Ensure Audit Process Creation is set to include Success

Rule Status :

Failed

Summary :

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include:4688: A new process has been created.4696: A primary token was assigned to process.Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008.or the most recent information about this setting. The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.3.1. L1 Ensure Audit PNP Activity is set to include Success

Rule Status :

Failed

Summary :

This policy setting allows you to audit when plug and play detects an external device.The recommended state for this setting is to include: Success.
Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale :
Enabling this setting will allow a user to audit events when a device is plugged into a system. This can help alert IT staff if unapproved devices are plugged in.

How to fix :
To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.2. L1 Ensure Audit Group Membership is set to include Success

Rule Status :

Failed

Summary :

This policy allows you to audit the group membership information in the users logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.The recommended state for this setting is to include: Success. Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.3. L1 Ensure Audit Logoff is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:4634: An account was logged off.4647: User initiated logoff.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.5. L1 Ensure Audit Other LogonLogoff Events is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory reports other logon/logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include:4649: A replay attack was detected.4778: A session was reconnected to a Window Station.4779: A session was disconnected from a Window Station.4800: The workstation was locked.4801: The workstation was unlocked.4802: The screen saver was invoked.4803: The screen saver was dismissed.5378: The requested credentials delegation was disallowed by policy.5632: A request was made to authenticate to a wireless network.5633: A request was made to authenticate to a wired network.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.4. L1 Ensure Audit Logon is set to Success and Failure

Rule Status :

Passed

Summary :

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:4624: An account was successfully logged on.4625: An account failed to log on.4648: A logon was attempted using explicit credentials.4675: SIDs were filtered.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.6. L1 Ensure Audit Special Logon is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include:4964 : Special groups have been assigned to a new logon.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.5.1. L1 Ensure Audit Account Lockout is set to include Failure

Rule Status :

Failed

Summary :

This subcategory reports when a user"s account is locked out as a result of too many failed logon attempts. Events for this subcategory include:4625: An account failed to log on.The recommended state for this setting is to include: Failure.

Rationale :
Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.6.4. L1 Ensure Audit Removable Storage is set to Success and Failure

Rule Status :

Failed

Summary :

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage.The recommended state for this setting is: Success and Failure. Note: A Windows 8.0, Server 2012 (non-R2) or newer OS is required to access and set this value in Group Policy.

Rationale :

Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Storage.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.6.2. L1 Ensure Audit File Share is set to Success and Failure

Rule Status :

Failed

Summary :

This policy setting allows you to audit attempts to access a shared folder.The recommended state for this setting is: Success and Failure.
Note: There are no system access control lists (SACLs) for shared folders. If this policy setting is enabled, access to all shared folders on the system is audited.

Rationale :

In an enterprise managed environment, workstations should have limited file sharing activity, as file servers would normally handle the overall burden of file sharing activities. Any unusual file sharing activity on workstations may therefore be useful in an investigation of potentially malicious activity.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit File Share.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.6.1. L1 Ensure Audit Detailed File Share is set to include Failure

Rule Status :

Failed

Summary :

This subcategory allows you to audit attempts to access files and folders on a shared folder. Events for this subcategory include:5145: network share object was checked to see whether client can be granted desired access.The recommended state for this setting is to include: Failure

Rationale :

Auditing the Failures will log which unauthorized users attempted (and failed) to get access to a file or folder on a network share on this computer, which could possibly be an indication of malicious intent.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File Share.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.6.3. L1 Ensure Audit Other Object Access Events is set to Success and Failure

Rule Status :

Failed

Summary :

This policy setting allows you to audit events generated by the management of task scheduler jobs or COM+ objects.For scheduler jobs, the following are audited:Job created.Job deleted.Job enabled.Job disabled.Job updated.For COM+ objects, the following are audited:Catalog object added.Catalog object updated.Catalog object deleted.The recommended state for this setting is: Success and Failure.

Rationale :

The unexpected creation of scheduled tasks and COM+ objects could potentially be an indication of malicious activity. Since these types of actions are generally low volume, it may be useful to capture them in the audit logs for use during an investigation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object Access Events.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.7.5. L1 Ensure Audit Other Policy Change Events is set to include Failure

Rule Status :

Failed

Summary :

This subcategory contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.5063: A cryptographic provider operation was attempted.5064: A cryptographic context operation was attempted.5065: A cryptographic context modification was attempted.5066: A cryptographic function operation was attempted.5067: A cryptographic function modification was attempted.5068: A cryptographic function provider operation was attempted.5069: A cryptographic function property operation was attempted.5070: A cryptographic function property modification was attempted.6145: One or more errors occurred while processing security policy in the group policy objects.The recommended state for this setting is to include: Failure.

Rationale :

This setting can help detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Other Policy Change Events.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.7.1. L1 Ensure Audit Audit Policy Change is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include:4715: The audit policy (SACL) on an object was changed.4719: System audit policy was changed.4902: The Per-user audit policy table was created.4904: An attempt was made to register a security event source.4905: An attempt was made to unregister a security event source.4906: The CrashOnAuditFail value has changed.4907: Auditing settings on object were changed.4908: Special Groups Logon table modified.4912: Per User Audit Policy was changed.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.7.3. L1 Ensure Audit Authorization Policy Change is set to include Success

Rule Status :

Failed

Summary :

This subcategory reports changes in authorization policy. Events for this subcategory include:4703: A user right was adjusted.4704: A user right was assigned.4705: A user right was removed.4670: Permissions on an object were changed.4911: Resource attributes of the object were changed.4913: Central Access Policy on the object was changed.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.7.4. L1 Ensure Audit MPSSVC Rule-Level Policy Change is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe). Events for this subcategory include:4944: The following policy was active when the Windows Firewall started.4945: A rule was listed when the Windows Firewall started.4946: A change has been made to Windows Firewall exception list. A rule was added.4947: A change has been made to Windows Firewall exception list. A rule was modified.4948: A change has been made to Windows Firewall exception list. A rule was deleted.4949: Windows Firewall settings were restored to the default values.4950: A Windows Firewall setting has changed.4951: A rule has been ignored because its major version number was not recognized by Windows Firewall.4952: Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.4953: A rule has been ignored by Windows Firewall because it could not parse the rule.4954: Windows Firewall Group Policy settings have changed. The new settings have been applied.4956: Windows Firewall has changed the active profile.4957: Windows Firewall did not apply the following rule.4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.The recommended state for this setting is : Success and Failure

Rationale :

Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-Level Policy Change.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.7.2. L1 Ensure Audit Authentication Policy Change is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports changes in authentication policy. Events for this subcategory include:4706: A new trust was created to a domain.4707: A trust to a domain was removed.4713: Kerberos policy was changed.4716: Trusted domain information was modified.4717: System security access was granted to an account.4718: System security access was removed from an account.4739: Domain Policy was changed.4864: A namespace collision was detected.4865: A trusted forest information entry was added.4866: A trusted forest information entry was removed.4867: A trusted forest information entry was modified.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.8.1. L1 Ensure Audit Sensitive Privilege Use is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:Act as part of the operating systemBack up files and directoriesCreate a token objectDebug programsEnable computer and user accounts to be trusted for delegationGenerate security auditsImpersonate a client after authenticationLoad and unload device driversManage auditing and security logModify firmware environment valuesReplace a process-level tokenRestore files and directoriesTake ownership of files or other objectsAuditing this subcategory will create a high volume of events. Events for this subcategory include:4672: Special privileges assigned to new logon.4673: A privileged service was called.4674: An operation was attempted on a privileged object.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.9.1. L1 Ensure Audit IPsec Driver is set to Success and Failure

Rule Status :

Failed

Summary :

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include:4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.5478: IPsec Services has started successfully.5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.9.4. L1 Ensure Audit Security System Extension is set to include Success

Rule Status :

Failed

Summary :

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include:4610: An authentication package has been loaded by the Local Security Authority.4611: A trusted logon process has been registered with the Local Security Authority.4614: A notification package has been loaded by the Security Account Manager.4622: A security package has been loaded by the Local Security Authority.4697: A service was installed in the system.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.9.2. L1 Ensure Audit Other System Events is set to Success and Failure

Rule Status :

Passed

Summary :

This subcategory reports on other system events. Events for this subcategory include:5024 : The Windows Firewall Service has started successfully.5025 : The Windows Firewall Service has been stopped.5027 : The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.5028 : The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.5030: The Windows Firewall Service failed to start.5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.5033 : The Windows Firewall Driver has started successfully.5034 : The Windows Firewall Driver has been stopped.5035 : The Windows Firewall Driver failed to start.5037 : The Windows Firewall Driver detected critical runtime error. Terminating.5058: Key file operation.5059: Key migration operation.The recommended state for this setting is: Success and Failure.

Rationale :

Capturing these audit events may be useful for identifying when the Windows Firewall is not performing as expected.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Other System Events.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.9.3. L1 Ensure Audit Security State Change is set to include Success

Rule Status :

Passed

Summary :

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include:4608: Windows is starting up.4609: Windows is shutting down.4616: The system time was changed.4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some audit-able activity might not have been recorded.The recommended state for this setting is to include: Success.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Success.Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

17.9.5. L1 Ensure Audit System Integrity is set to Success and Failure

Rule Status :

Passed

Summary :

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include:4612 : Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.4615 : Invalid use of LPC port.4618 : A monitored security event pattern has occurred.4816 : RPC detected an integrity violation while decrypting an incoming message.5038 : Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.5056: A cryptographic self test was performed.5057: A cryptographic primitive operation failed.5060: Verification operation failed.5061: Cryptographic operation.5062: A kernel-mode cryptographic self test was performed.The recommended state for this setting is: Success and Failure.

Rationale :

Auditing these events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Success and Failure:Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity.Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

18.1.1.2. L1 Ensure Prevent enabling lock screen slide show is set to Enabled

Rule Status :

Failed

Summary :

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen.The recommended state for this setting is: Enabled.

Rationale :
Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show.Note: This Group Policy path is provided by the Group Policy template ControlPanelDisplay.admx/admlthat is included with the Microsoft Windows 8.1 & 2012 R2 Administrative Templates (or newer).

Impact:If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

18.1.1.1. L1 Ensure Prevent enabling lock screen camera is set to Enabled

Rule Status :

Failed

Summary :

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen.The recommended state for this setting is: Enabled.

Rationale :
Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera.Note: This Group Policy path is provided by the Group Policy template ControlPanelDisplay.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

18.1.2.2. L1 Ensure Allow users to enable online speech recognition services is set to Disabled

Rule Status :

Failed

Summary :

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user"s OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech.The recommended state for this setting is: Disabled.

Rationale :

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow users to enable online speech recognition services.Note: This Group Policy path is provided by the Group Policy template Globalization.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow input personalization , but it was renamed to Allow users to enable online speech recognition services starting with the Windows 10 R1809 & Server 2019 Administrative Templates. Impact:Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

18.10.12.1. L1 Ensure Turn off cloud consumer account state content is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether cloud consumer account state content is allowed in all Windows experiences.The recommended state for this setting is: Enabled.

Rationale :

The use of consumer accounts in an enterprise managed environment is not good security practice as it could lead to possible data leakage.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off cloud consumer account state content.Note: This Group Policy path is provided by the Group Policy template CloudContent.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Impact:Users will not be able to use Microsoft consumer accounts on the system, and associated Windows experiences will instead present default fallback content.

18.10.12.3. L1 Ensure Turn off Microsoft consumer experiences is set to Enabled

Rule Status :

Failed

Summary :

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account.The recommended state for this setting is: Enabled. Note: Per Microsoft TechNet. this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale :

Having apps silently install in an enterprise managed environment is not good security practice - especially if the apps send data back to a third-party.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Microsoft consumer experiences.Note: This Group Policy path is provided by the Group Policy template CloudContent.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).
Impact:Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

18.10.13.1. L1 Ensure Require pin for pairing is set to Enabled First Time OR Enabled Always

Rule Status :

Failed

Summary :

This policy setting controls whether or not a PIN is required for pairing to a wireless display device.The recommended state for this setting is: Enabled: First TimeOR Enabled: Always.

Rationale :

If this setting is not configured or disabled then a PIN would not be required when pairing wireless display devices to the system, increasing the risk of unauthorized use.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: First TimeOR Enabled: Always.Computer Configuration\Policies\Administrative Templates\Windows Components\Connect\Require pin for pairing.Note: This Group Policy path is provided by the Group Policy template WirelessDisplay.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). The new Choose one of the following actionssub-option was later added as of the Windows 10 Release 1809 Administrative Templates. Choosing Enabledin the older templates is the equivalent of choosing Enabled: First Timein the newer templates. Impact:The pairing ceremony for connecting to new wireless display devices will always require a PIN.

18.10.14.2. L1 Ensure Enumerate administrator accounts on elevation is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application.The recommended state for this setting is: Disabled.

Rationale :

Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation.Note: This Group Policy path is provided by the Group Policy template CredUI.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates.

Impact:None - this is the default behavior.

18.10.14.1. L1 Ensure Do not display the password reveal button is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to configure the display of the password reveal button in password entry user experiences.The recommended state for this setting is: Enabled.

Rationale :

This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button.Note: This Group Policy path is provided by the Group Policy template CredUI.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:The password reveal button will not be displayed after a user types a password in the password entry text box.

18.10.14.3. L1 Ensure Prevent the use of security questions for local accounts is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether security questions can be used to reset local account passwords. The security question feature does not apply to domain accounts, only local accounts on the workstation.The recommended state for this setting is: Enabled.

Rationale :

Users could establish security questions that are easily guessed or sleuthed by observing the users social media accounts, making it easier for a malicious actor to change the local user account password and gain access to the computer as that user account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Prevent the use of security questions for local accounts.Note: This Group Policy path is provided by the Group Policy template CredUI.admx/admlthat is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer). Impact:Local user accounts will not be able to set up and use security questions to reset their passwords.

18.10.15.4. L1 Ensure Do not show feedback notifications is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows an organization to prevent its devices from showing feedback questions from Microsoft.The recommended state for this setting is: Enabled.

Rationale :

Users should not be sending any feedback to third-party vendors in an enterprise managed environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Do not show feedback notifications.Note: This Group Policy path is provided by the Group Policy template FeedbackNotifications.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Impact:Users will no longer see feedback notifications through the Windows Feedback app.

18.10.15.7. L1 Ensure Limit Dump Collection is set to Enabled

Rule Status :

Failed

Summary :

This policy setting limits the type of memory dumps that can be collected when more information is needed to troubleshoot a problem.The recommended state for this setting is: Enabled. Note: Memory dumps are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation Allow Diagnostic Datais set to Enabled: Diagnostic data off (not recommended)or Enabled: Send required diagnostic datato send only basic information.

Rationale :

Memory dumps can contain sensitive information. Sending this data to a third-party vendor is a security concern and should only be done on an as-needed basis.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled. Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Limit Dump Collection.Note: This Group Policy path is provided by the Group Policy template DataCollection.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:Windows Error Reporting is limited to sending kernel mini and user mode triage memory dumps, reducing the risk of sending sensitive information to Microsoft.

18.10.15.5. L1 Ensure Enable OneSettings Auditing is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether Windows records attempts to connect with the OneSettings service to the Event Log.The recommended state for this setting is: Enabled.

Rationale :

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Enable OneSettings Auditing.Note: This Group Policy path is provided by the Group Policy template DataCollection.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:Windows will record attempts to connect with the OneSettings service to the Applications and Services Logs\Microsoft\Windows\Privacy-Auditing\OperationalEvent Log channel.

18.10.15.6. L1 Ensure Limit Diagnostic Log Collection is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether additional diagnostic logs are collected when more information is needed to troubleshoot a problem on the device.The recommended state for this setting is: Enabled. Note: Diagnostic logs are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation Allow Diagnostic Datais set to Enabled: Diagnostic data off (not recommended)or Enabled: Send required diagnostic datato send only basic information.

Rationale :

Sending data to a third-party vendor is a security concern and should only be done on an as-needed basis.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Limit Diagnostic Log Collection.Note: This Group Policy path is provided by the Group Policy template DataCollection.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:Diagnostic logs and information such as crash dumps will not be collected for transmission to Microsoft.

18.10.15.8. L1 Ensure Toggle user control over Insider builds is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software.The recommended state for this setting is: Disabled. Note: This policy setting applies only to devices running Windows 10 Pro or Windows 10 Enterprise, up until Release 1703. For Release 1709 or newer, Microsoft encourages using the Manage preview buildssetting (Section 18.10.92). We have kept this setting in the benchmark to ensure that any older builds of Windows 10 in the environment are still enforced.

Rationale :

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready builds.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Toggle user control over Insider builds.Note: This Group Policy path is provided by the Group Policy template AllowBuildPreview.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:The item "Get Insider builds" will be unavailable.

18.10.15.3. L1 Ensure Disable OneSettings Downloads is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether Windows attempts to connect with the OneSettings service to download configuration settings.The recommended state for this setting is: Enabled.

Rationale :

Sending data to a third-party vendor is a security concern and should only be done on an as-needed basis.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Disable OneSettings Downloads.Note: This Group Policy path is provided by the Group Policy template DataCollection.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:Windows will not connect to the OneSettings service to download configuration settings.

18.10.15.1. L1 Ensure Allow Diagnostic Data is set to Enabled Diagnostic data off not recommended or Enabled Send required diagnostic data

Rule Status :

Failed

Summary :

This policy setting determines the amount of diagnostic and usage data reported to Microsoft:A value of (0) Diagnostic data off (not recommended). Using this value, no diagnostic data is sent from the device. This value is only supported on Enterprise, Education, and Server editions. If you choose this setting, devices in your organization will still be secure. A value of (1) Send required diagnostic data. This is the minimum diagnostic data necessary to keep Windows secure, up to date, and performing as expected.Using this value disables the Optional diagnostic data control in the Settings app. A value of (3) Send optional diagnostic data. Additional diagnostic data is collected that helps us to detect, diagnose and fix issues, as well as make product improvements. Required diagnostic data will always be included when you choose to send optional diagnostic data. Optional diagnostic data can also include diagnostic log files and crash dumps. Use the Limit Dump Collection and the Limit Diagnostic Log Collection policies for more granular control of what optional diagnostic data is sent. Windows telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10/11.The recommended state for this setting is: Enabled: Diagnostic data off (not recommended)or Enabled: Send required diagnostic data. Note: If your organization relies on Windows Update, the minimum recommended setting is Required diagnostic data. Because no Windows Update information is collected when diagnostic data is off, important information about update failures is not sent. Microsoft uses this information to fix the causes of those failures and improve the quality of updates. Note #2: The Configure diagnostic data opt-in settings user interface group policy can be used to prevent end users from changing their data collection settings. Note #3: Enhanced diagnostic data setting is not available on Windows 11 and Windows Server 2022 and has been replaced with policies that can control the amount of optional diagnostic data that is sent. For more information on these settings visit Manage diagnostic data using Group Policy and MDM.

Rationale :

Sending any data to a third-party vendor is a security concern and should only be done on an as needed basis.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Diagnostic data off (not recommended)or Enabled: Send required diagnostic data.Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Allow Diagnostic Data.Note: This Group Policy path is provided by the Group Policy template DataCollection.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow Telemetry , but it was renamed to Allow Diagnostic Data starting with the Windows 11 Release 21H2 Administrative Templates. Impact:Note that setting values of 0 or 1 will degrade certain experiences on the device.

18.10.16.1. L1 Ensure Download Mode is NOT set to Enabled Internet

Rule Status :

Failed

Summary :

This policy setting specifies the download method that Delivery Optimization can use in downloads of Windows Updates, Apps and App updates. The following methods are supported:0 = HTTP only, no peering.1 = HTTP blended with peering behind the same NAT.2 = HTTP blended with peering across a private group. Peering occurs on devices in the same Active Directory Site (if exist) or the same domain by default. When this option is selected, peering will cross NATs. To create a custom group use Group ID in combination with Mode 2.3 = HTTP blended with Internet Peering.99 = Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services.100 = Bypass mode. Do not use Delivery Optimization and use BITS instead.The recommended state for this setting is any value EXCEPT: Enabled: Internet (3). Note: The default on all SKUs other than Enterprise, Enterprise LTSB or Education is Enabled: Internet (3), so on other SKUs, be sure to set this to a different value.

Rationale :

Due to privacy concerns and security risks, updates should only be downloaded directly from Microsoft, or from a trusted machine on the internal network that received its updates from a trusted source and approved by the network administrator.

How to fix :

To establish the recommended configuration via GP, set the following UI path to any value other than Enabled: Internet (3).Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization\Download Mode.Note: This Group Policy path is provided by the Group Policy template DeliveryOptimization.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:Machines will not be able to download updates from peers on the Internet. If set to Enabled: HTTP only (0), Enabled: Simple (99), or Enabled: Bypass (100), machines will not be able to download updates from other machines on the same LAN.

18.10.17.4. L1 Ensure Enable App Installer ms-appinstaller protocol is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users can install packages from a website that is using the ms-appinstallerprotocol. The ms-appinstallerprotocol allows users to install an application by clicking a link on a website. The recommended state for this setting is: Disabled.

Rationale :

Users should not have the ability to install an application by clicking a link on a website. If an unknown or malicious link is clicked, malicious software could be installed on the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop App Installer\Enable App Installer ms-appinstaller protocol.Note: This Group Policy path is provided by the Group Policy template DesktopAppInstaller.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Users will not have the ability to use the ms-appinstallerprotocol to install applications by clicking a link on a website.

18.10.17.2. L1 Ensure Enable App Installer Experimental Features is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether users can enable experimental features in the Windows Package Manager.The recommended state for this setting is Disabled.

Rationale :

Windows Package Manager is a command line tool can be used to discover, install, upgrade, remove and configure applications, and it can be used as a distribution channel for software packages containing tools and applications. Users should not have access to experimental features.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop App Installer\Enable App Installer Experimental Features.Note: This Group Policy path is provided by the Group Policy template DesktopAppInstaller.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Users will not have access to experimental features in the command line tool, winget to discover, install, upgrade, remove, configure, or distribute applications.

18.10.17.3. L1 Ensure Enable App Installer Hash Override is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether or not users can override the SHA256 security validation in the Windows Package Manager settings.The recommended state for this setting is: Disabled.

Rationale :

Users should not have the ability to override SHA256 security validation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop App Installer\Enable App Installer Hash Override.Note: This Group Policy path is provided by the Group Policy template DesktopAppInstaller.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Users will not have the ability to override the SHA256 security validation.

18.10.17.1. L1 Ensure Enable App Installer is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether standard users have access to the Windows Package Manager. Windows Package Manager is a package manager solution that consists of a command line tool and set of services for installing applications on Microsoft Windows 10 and 11.The recommended state for this setting is: Disabled.

Rationale :

Windows Package Manager is a command line tool can be used to discover, install, upgrade, remove and configure applications, and it can be used as a distribution channel for software packages containing tools and applications. Users should not have access to these types of development tools.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop App Installer\Enable App Installer.Note: This Group Policy path is provided by the Group Policy template DesktopAppInstaller.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Impact:Users will not have access to the command line tool, wingetto discover, install, upgrade, remove, configure, or distribute applications.

18.10.25.1.2. L1 Ensure Application Specify the maximum log file size KB is set to Enabled 32768 or greater

Rule Status :

Failed

Summary :

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale :

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 32,768 or greater.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB).Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Maximum Log Size (KB) , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker"s activities.

18.10.25.1.1. L1 Ensure Application Control Event Log behavior when the log file reaches its maximum size is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls Event Log behavior when the log file reaches its maximum size.The recommended state for this setting is: Disabled.
Note: Old events may or may not be retained according to the Backup log automatically when full policy setting.

Rationale :

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size.Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Retain old events , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.25.2.1. L1 Ensure Security Control Event Log behavior when the log file reaches its maximum size is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls Event Log behavior when the log file reaches its maximum size.The recommended state for this setting is: Disabled.
Note: Old events may or may not be retained according to the Backup log automatically when full policy setting.

Rationale :

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size.Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Retain old events , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.25.2.2. L1 Ensure Security Specify the maximum log file size KB is set to Enabled 196608 or greater

Rule Status :

Failed

Summary :

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.The recommended state for this setting is: Enabled: 196,608 or greater.

Rationale :

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 196,608 or greater.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB).Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Maximum Log Size (KB) , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker"s activities.

18.10.25.3.2. L1 Ensure Setup Specify the maximum log file size KB is set to Enabled 32768 or greater

Rule Status :

Failed

Summary :

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale :

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 32,768 or greater.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB).Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Maximum Log Size (KB) , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker"s activities.

18.10.25.3.1. L1 Ensure Setup Control Event Log behavior when the log file reaches its maximum size is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls Event Log behavior when the log file reaches its maximum size.The recommended state for this setting is: Disabled.
Note: Old events may or may not be retained according to the Backup log automatically when full policy setting.

Rationale :

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size.Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Retain old events , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.25.4.1. L1 Ensure System Control Event Log behavior when the log file reaches its maximum size is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls Event Log behavior when the log file reaches its maximum size.The recommended state for this setting is: Disabled.
Note: Old events may or may not be retained according to the Backup log automatically when full policy setting.

Rationale :

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size.Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Retain old events , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.25.4.2. L1 Ensure System Specify the maximum log file size KB is set to Enabled 32768 or greater

Rule Status :

Failed

Summary :

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale :

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 32,768 or greater.Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB).Note: This Group Policy path is provided by the Group Policy template EventLog.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Maximum Log Size (KB) , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker"s activities.

18.10.28.5. L1 Ensure Turn off shell protocol protected mode is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol, applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows.The recommended state for this setting is: Disabled.

Rationale :

Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode.Note: This Group Policy path is provided by the Group Policy template WindowsExplorer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates.
Impact:None - this is the default behavior.

18.10.28.3. L1 Ensure Turn off Data Execution Prevention for Explorer is set to Disabled

Rule Status :

Failed

Summary :

Disabling Data Execution Prevention can allow certain legacy plug-in applications to function without terminating Explorer.The recommended state for this setting is: Disabled. Note: Some legacy plug-in applications and other software may not function with Data Execution Prevention and will require an exception to be defined for that specific plug-in/software.

Rationale :

Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer.Note: This Group Policy path is provided by the Group Policy template Explorer.admx/admlthat is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.10.28.4. L1 Ensure Turn off heap termination on corruption is set to Disabled

Rule Status :

Failed

Summary :

Without heap termination on corruption, legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Ensuring that heap termination on corruption is active will prevent this.The recommended state for this setting is: Disabled.

Rationale :

Allowing an application to function after its session has become corrupt increases the risk posture to the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption.Note: This Group Policy path is provided by the Group Policy template Explorer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.3.2. L1 Ensure Prevent non-admin users from installing packaged Windows apps is set to Enabled

Rule Status :

Failed

Summary :

This setting manages non-Administrator users" ability to install Windows app packages.The recommended state for this setting is: Enabled.

Rationale :

In a corporate managed environment, application installations should be managed centrally by IT staff, not by end users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\App Package Deployment\Prevent non-admin users from installing packaged Windows apps.Note: This Group Policy path is provided by the Group Policy template AppxPackageManager.admx/admlthat is included with the Microsoft Windows 10 Release 2004 Administrative Templates (or newer). Impact:Non-Administrator users will not be able to install Microsoft Store app packages, unless they are explicitly permitted by other policies. If a Microsoft Store app is required for legitimate use, an Administrator will need to perform the installation from an Administrator context.This setting can prevent standard users (without Administrator access) from launching Office 365 (O365) applications, displaying the error: "Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."

18.10.41.1. L1 Ensure Block all consumer Microsoft account user authentication is set to Enabled

Rule Status :

Failed

Summary :

This setting determines whether applications and services on the device can utilize new consumer Microsoft account authentication via the Windows OnlineIDand WebAccountManagerAPIs. The recommended state for this setting is: Enabled.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft accounts\Block all consumer Microsoft account user authentication.Note: This Group Policy path is provided by the Group Policy template MSAPolicy.admx/admlthat is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Impact:All applications and services on the device will be prevented from new authentications using consumer Microsoft accounts via the Windows OnlineIDand WebAccountManagerAPIs. Authentications performed directly by the user in web browsers or in apps that use OAuthwill remain unaffected.

18.10.42.10.2. L1 Ensure Turn off real-time protection is set to Disabled

Rule Status :

Failed

Summary :

This policy setting configures real-time protection prompts for known malware detection.Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.The recommended state for this setting is: Disabled.

Rationale :

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-time protection.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.10.42.10.1. L1 Ensure Scan all downloaded files and attachments is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures scanning for all downloaded files and attachments.The recommended state for this setting is: Enabled.

Rationale :

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all downloaded files and attachments.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.10.42.10.4. L1 Ensure Turn on script scanning is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows script scanning to be turned on/off. Script scanning intercepts scripts then scans them before they are executed on the system.The recommended state for this setting is: Enabled.

Rationale :

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on script scanning.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Impact:None - this is the default behavior.

18.10.42.10.3. L1 Ensure Turn on behavior monitoring is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to configure behavior monitoring for Microsoft Defender Antivirus.The recommended state for this setting is: Enabled.

Rationale :

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on behavior monitoring.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.10.42.13.3. L1 Ensure Turn on e-mail scanning is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).The recommended state for this setting is: Enabled.

Rationale :

Incoming e-mails should be scanned by an antivirus solution such as Microsoft Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:E-mail scanning by Microsoft Defender Antivirus will be enabled.

18.10.42.13.1. L1 Ensure Scan packed executables is set to Enabled

Rule Status :

Failed

Summary :

This policy setting manages whether or not Microsoft Defender Antivirus scans packed executables. Packed executables are executable files that contain compressed code.The recommended state for this setting is: Enabled.

Rationale :

Packing executables is a way to compress and create smaller files and can make it difficult to access and analyze the code associated with the executable. This is a common method to obfuscate malicious executables by bad actors.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Scan packed executables.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer). Impact:None - This is the default behavior.

18.10.42.13.2. L1 Ensure Scan removable drives is set to Enabled

Rule Status :

Failed

Summary :

This policy setting manages whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.The recommended state for this setting is: Enabled.

Rationale :

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought in to the enterprise managed environment from an external, unmanaged computer.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Scan removable drives.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:Removable drives will be scanned during any type of scan by Microsoft Defender Antivirus.

18.10.42.5.1. L1 Ensure Configure local setting override for reporting to Microsoft MAPS is set to Disabled

Rule Status :

Failed

Summary :

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft renamed to Windows Defender Antivirus Cloud Protection Service and then Microsoft Defender Antivirus Cloud Protection Service . This setting can only be set by Group Policy. The recommended state for this setting is: Disabled.

Rationale :

The decision on whether or not to participate in Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS\Configure local setting override for reporting to Microsoft MAPS.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.10.42.6.1.1. L1 Ensure Configure Attack Surface Reduction rules is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.The recommended state for this setting is: Enabled.

Rationale :

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact:When a rule is triggered, a notification will be displayed from the Action Center.

18.10.42.6.1.2. L1 Ensure Configure Attack Surface Reduction rules Set the state for each ASR

Rule Status :

Failed

Summary :

This policy setting sets the Attack Surface Reduction rules.The recommended state for this setting is: 26190899-1602-49e8-8b27-eb1d0a1ce869 - 1(Block Office communication application from creating child processes) 3b576869-a4ec-4529-8536-b80a7769e899 - 1(Block Office applications from creating executable content) 56a863a9-875e-4185-98a7-b882c64b5ce5 - 1(Block abuse of exploited vulnerable signed drivers) 5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1(Block execution of potentially obfuscated scripts) 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1(Block Office applications from injecting code into other processes) 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1(Block Adobe Reader from creating child processes) 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1(Block Win32 API calls from Office macro) 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1(Block credential stealing from the Windows local security authority subsystem (lsass.exe)) b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1(Block untrusted and unsigned processes that run from USB) be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1(Block executable content from email client and webmail) d3e037e1-3eb8-44c8-a917-57927947596d - 1(Block JavaScript or VBScript from launching downloaded executable content) d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1(Block Office applications from creating child processes) e6db77e5-3df2-4cf1-b95a-636979351e5b - 1(Block persistence through WMI event subscription) Note: More information on ASR rules can be found at the following link: Use Attack surface reduction rules to prevent malware infection | Microsoft Docs.

Rationale :

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

How to fix :

To establish the recommended configuration via GP, set the following UI path so that 26190899-1602-49e8-8b27-eb1d0a1ce869, 3b576869-a4ec-4529-8536-b80a7769e899, 56a863a9-875e-4185-98a7-b882c64b5ce5, 5beb7efe-fd9a-4556-801d-275e5ffc04cc, 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84, 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c, 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b, 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2, b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4, be9ba2d9-53ea-4cdc-84e5-9b1eeee46550, d3e037e1-3eb8-44c8-a917-57927947596d, d4f940ab-401b-4efc-aadc-ad5f3c50688a, and e6db77e5-3df2-4cf1-b95a-636979351e5bare each set to a value of 1.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact:When a rule is triggered, a notification will be displayed from the Action Center.

18.10.42.6.3.1. L1 Ensure Prevent users and apps from accessing dangerous websites is set to Enabled Block

Rule Status :

Failed

Summary :

This policy setting controls Microsoft Defender Exploit Guard network protection.The recommended state for this setting is: Enabled: Block.

Rationale :

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Block.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Network Protection\Prevent users and apps from accessing dangerous websites.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact:Users and applications will not be able to access dangerous domains.

18.10.42.7.1. L1 Ensure Enable file hash computation feature is set to Enabled

Rule Status :

Failed

Summary :

This setting determines whether hash values are computed for files scanned by Microsoft Defender.The recommended state for this setting is: Enabled.

Rationale :

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor for suspicious and known malicious activity. File hashes are a reliable way of detecting changes to files, and can speed up the scan process by skipping files that have not changed since they were last scanned and determined to be safe. A changed file hash can also be cause for additional scrutiny.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact:This setting could cause performance degradation during initial deployment and for users where new executable content is frequently being created (such as software developers), or where applications are frequently installed or updated.For more information on this setting, please visit Security baseline (FINAL): Windows 10 and Windows Server, version 2004 - Microsoft Tech Community - 1543631. Note: The impact of this setting should be monitored closely during deployment to ensure user and system performance impact is within acceptable limits.

18.10.42.16. L1 Ensure Configure detection for potentially unwanted applications is set to Enabled Block

Rule Status :

Failed

Summary :

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.The recommended state for this setting is: Enabled: Block. For more information, see this link: Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs.

Rationale :

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Block.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Configure detection for potentially unwanted applications.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer). Impact:Applications that are identified by Microsoft as PUA will be blocked at download and install time.

18.10.42.17. L1 Ensure Turn off Microsoft Defender AntiVirus is set to Disabled

Rule Status :

Failed

Summary :

This policy setting turns off Microsoft Defender Antivirus. If the setting is configured to Disabled, Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.The recommended state for this setting is: Disabled.

Rationale :

It is important to ensure a current, updated antivirus product is scanning each computer for malicious file activity. Microsoft provides a competent solution out of the box in Microsoft Defender Antivirus.Organizations that choose to purchase a reputable third-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Turn off Microsoft Defender AntiVirus.Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Turn off Windows Defender , but it was renamed to Windows Defender Antivirus starting with the Windows 10 Release 1703 Administrative Templates. It was again renamed to Turn off Microsoft Defender Antivirus starting with the Windows 10 Release 2004 Administrative Templates. Impact:None - this is the default behavior.

18.10.43.5. L1 Ensure Configure Microsoft Defender Application Guard clipboard settings Clipboard behavior setting is set to Enabled Enable clipboard operation from an isolated session to the host

Rule Status :

Failed

Summary :

This policy setting allows you to decide how the clipboard behaves while in Microsoft Defender Application Guard.The recommended state for this setting is: Enabled: Enable clipboard operation from an isolated session to the host. Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container" for visiting untrusted websites. If the host clipboard is made available to Microsoft Defender Application Guard, a compromised Microsoft Defender Application Guard session will have access to its content, potentially exposing sensitive information to a malicious website or application. However, the risk is reduced if the Microsoft Defender Application Guard clipboard is made accessible to the host, and indeed that functionality may often be necessary from an operational standpoint.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Enable clipboard operation from an isolated session to the hostComputer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Configure Windows Defender Application Guard clipboard settings: Clipboard behavior setting , but it was renamed to Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting starting with the Windows 10 Release 2004 Administrative Templates. Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Microsoft Defender Application Guard sessions will not be able to access the host device"s clipboard, however the host device will be able to access the Microsoft Defender Application Guard session clipboard.

18.10.43.6. L1 Ensure Turn on Microsoft Defender Application Guard in Managed Mode is set to Enabled 1

Rule Status :

Failed

Summary :

This policy setting enables application isolation through Microsoft Defender Application Guard (Application Guard).There are 4 options available:Disable Microsoft Defender Application GuardEnable Microsoft Defender Application Guard for Microsoft Edge ONLYEnable Microsoft Defender Application Guard for Microsoft Office ONLYEnable Microsoft Defender Application Guard for Microsoft Edge AND Microsoft OfficeThe recommended state for this setting is: Enabled: 1Note #1: Microsoft Defender Application Guard requires hardware-assisted CPU virtualization (Intel VT-x or AMD- V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-
assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: At time of publication, Microsoft Defender Application Guard in all currently released versions of Windows 10 does not yet support protection for Microsoft Office, only for Microsoft Edge. Therefore the additional available options of 2and 3in this setting are not yet valid. Note #3: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

Microsoft Defender Application Guard uses Windows Hypervisor to create a virtualized environment for apps that are configured to use virtualization-based security isolation. While in isolation, improper user interactions and app vulnerabilities cant compromise the kernel or any other apps running outside of the virtualized environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 1.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Turn on Microsoft Defender Application Guard in Managed Mode.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Turn on Windows Defender Application Guard in Enterprise Mode , but it was renamed to Turn on Windows Defender Application Guard in Managed Mode starting with the Windows 10 Release 1903 Administrative Templates. It was again renamed to Turn on Microsoft Defender Application Guard in Managed Mode starting with the Windows 10 Release 2004 Administrative Templates. Impact:Microsoft Defender Application Guard will be turned on for Microsoft Edge.Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue.
Note #2: Microsoft Defender Application Guard requires the Internet Connection Sharing (ICS) (SharedAccess) service in order to operate, so an exception to disabling this service (see Section 5 in the CIS Microsoft Windows 10 benchmark only) will be required if choosing to enable Microsoft Defender Application Guard.

18.10.43.3. L1 Ensure Allow data persistence for Microsoft Defender Application Guard is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to decide whether data should persist across different sessions in Microsoft Defender Application Guard.The recommended state for this setting is: Disabled. Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container" for visiting untrusted websites. If data persistence is allowed, then it reduces the effectiveness of the sandboxing, and malicious content will be able to remain active in the Microsoft Defender Application Guard container between sessions.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow data persistence for Microsoft Defender Application Guard.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow data persistence for Windows Defender Application Guard , but it was renamed to Allow data persistence for Microsoft Defender Application Guard starting with the Windows 10 Release 2004 Administrative Templates. Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. None - this is the default behavior.

18.10.43.1. L1 Ensure Allow auditing events in Microsoft Defender Application Guard is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to decide whether auditing events can be collected from Microsoft Defender Application Guard.The recommended state for this setting is: Enabled. Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

Auditing of Microsoft Defender Application Guard events may be useful when investigating a security incident.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow auditing events in Microsoft Defender Application Guard.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow auditing events in Windows Defender Application Guard , but it was renamed to Allow auditing events in Microsoft Defender Application Guard starting with the Windows 10 Release 2004 Administrative Templates. Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Microsoft Defender Application Guard will inherit its auditing policies from Microsoft Edge and start to audit system events specifically for Microsoft Defender Application Guard. Collected logs are available for review on Microsoft Edge, outside of Application Guard.

18.10.43.2. L1 Ensure Allow camera and microphone access in Microsoft Defender Application Guard is set to Disabled

Rule Status :

Failed

Summary :

The policy allows you to determine whether applications inside Microsoft Defender Application Guard can access the devices camera and microphone.The recommended state for this setting is: Disabled. Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

In effort to stop sensitive information from being obtained for malicious use, untrusted sites within the Microsoft Defender Application Guard container should not be accessing the computers microphone or camera.

How to fix :

To establish the recommended configuration via GP, set the following UI path to DisabledComputer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow camera and microphone access in Microsoft Defender Application Guard.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow camera and microphone access in Windows Defender Application Guard , but it was renamed to Allow camera and microphone access in Microsoft Defender Application Guard starting with the Windows 10 Release 2004 Administrative Templates. Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. This is the default value so impact should be minimal to enforce this setting.

18.10.43.4. L1 Ensure Allow files to download and save to the host operating system from Microsoft Defender Application Guard is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether to save downloaded files to the host operating system from the Microsoft Defender Application Guard container.The recommended state for this setting is: Disabled. Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM. More information on system requirements for this feature can be found at System requirements for Microsoft Defender Application Guard (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container". Potentially malicious files should not be copied to the host OS from the sandboxed environment, which could put the host at risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow files to download and save to the host operating system from Microsoft Defender Application Guard.Note: This Group Policy path is provided by the Group Policy template AppHVSI.admx/admlthat is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow files to download and save to the host operating system from Windows Defender Application Guard , but it was renamed to Allow files to download and save to the host operating system from Microsoft Defender Application Guard starting with the Windows 10 Release 2004 Administrative Templates. Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. None - this is the default behavior.

18.10.4.1. L1 Ensure Let Windows apps activate with voice while the system is locked is set to Enabled Force Deny

Rule Status :

Failed

Summary :

This policy setting specifies whether Windows apps can be activated by voice (apps and Cortana) while the system is locked.The recommended state for this setting is: Enabled: Force Deny.

Rationale :

Access to any computer resource should not be allowed when the device is locked.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Force Deny.Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps activate with voice while the system is locked.Note: This Group Policy path is provided by the Group Policy template AppPrivacy.admx/admlthat is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer). Impact:Users will not be able to activate apps while the computer is locked.

18.10.50.1. L1 Ensure Prevent the usage of OneDrive for file storage is set to Enabled

Rule Status :

Failed

Summary :

This policy setting lets you prevent apps and features from working with files on OneDrive using the Next Generation Sync Client.The recommended state for this setting is: Enabled.

Rationale :

Enabling this setting prevents users from accidentally (or intentionally) uploading confidential or sensitive corporate information to the OneDrive cloud service using the Next Generation Sync Client.Note: This security concern applies to any cloud-based file storage application installed on a workstation, not just the one supplied with Windows.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage.Note: This Group Policy path is provided by the Group Policy template SkyDrive.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). However, we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version. Note #2: In older Microsoft Windows Administrative Templates, this setting was named Prevent the usage of SkyDrive for file storage , but it was renamed starting with the Windows 10 RTM (Release 1507) Administrative Templates. Impact:Users can"t access OneDrive from the OneDrive app and file picker. Windows Store apps can"t access OneDrive using the WinRTAPI. OneDrive doesn"t appear in the navigation pane in File Explorer. OneDrive files aren"t kept in sync with the cloud. Users can"t automatically upload photos and videos from the camera roll folder. Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive. Note #2: If your organization has decided to implement OneDrive for Business and therefore needs to except itself from this recommendation, we highly suggest that you also obtain and utilize the OneDrive.admx/admltemplate that is bundled with the latest OneDrive client, as noted at this link.this template is not included with the Windows Administrative Templates). Two alternative OneDrive settings in particular from that template are worth your consideration: Allow syncing OneDrive accounts for only specific organizations - a computer-based setting that restricts OneDrive client connections to only approved tenant IDs. Prevent users from synchronizing personal OneDrive accounts - a user-based setting that prevents use of consumer OneDrive (i.e. non-business).

18.10.56.2.3. L1 Ensure Do not allow passwords to be saved is set to Enabled

Rule Status :

Failed

Summary :

This policy setting helps prevent Remote Desktop clients from saving passwords on a computer.The recommended state for this setting is: Enabled. Note: If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.

Rationale :

An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user"s account and connects to their computer could use saved passwords to gain access to additional hosts.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

18.10.56.3.11.1. L1 Ensure Do not delete temp folders upon exit is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether Remote Desktop Services retains a user"s per-session temporary folders at logoff.The recommended state for this setting is: Disabled.

Rationale :

Sensitive information could be contained inside the temporary folders and visible to other administrators that log into the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not delete temp folders upon exit.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was named Do not delete temp folder upon exit , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.56.3.3.3. L1 Ensure Do not allow drive redirection is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevents users from sharing the local drives on their client computers to Remote Desktop Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient\<driveletter>$If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.The recommended state for this setting is: Enabled.

Rationale :

Data could be forwarded from the user"s Remote Desktop Services session to the user"s local computer without any direct user interaction. Malicious software already present on a compromised server would have direct and stealthy disk access to the user"s local computer during the Remote Desktop session.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Drive redirection will not be possible. In most situations, traditional network drive mapping to file shares (including administrative shares) performed manually by the connected user will serve as a capable substitute to still allow file transfers when needed.

18.10.56.3.9.5. L1 Ensure Set client connection encryption level is set to Enabled High Level

Rule Status :

Failed

Summary :

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.The recommended state for this setting is: Enabled: High Level.

Rationale :

If Remote Desktop client connections that use low level encryption are allowed, it is more likely that an attacker will be able to decrypt any captured Remote Desktop Services network traffic.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: High Level.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.56.3.9.2. L1 Ensure Require secure RPC communication is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication.You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.The recommended state for this setting is: Enabled.

Rationale :

Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

18.10.56.3.9.1. L1 Ensure Always prompt for password upon connection is set to Enabled

Rule Status :

Failed

Summary :

This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.The recommended state for this setting is: Enabled.

Rationale :

Users have the option to store both their username and password when they create a new Remote Desktop Connection shortcut. If the server that runs Remote Desktop Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user"s computer could connect to a Remote Desktop Server through the Remote Desktop Connection shortcut, even though they may not know the user"s password.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named Always prompt client for password upon connection , but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates. Impact:Users cannot automatically log on to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on.

18.10.56.3.9.4. L1 Ensure Require user authentication for remote connections by using Network Level Authentication is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.The recommended state for this setting is: Enabled.

Rationale :

Requiring that user authentication occur earlier in the remote connection process enhances security.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named Require user authentication using RDP 6.0 for remote connections , but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates. Impact:Only client computers that support Network Level Authentication can connect to the RD Session Host server.Note: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as Network Level Authentication will expect the user"s Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a double logon requirement for each and every new RDP session.

18.10.56.3.9.3. L1 Ensure Require use of specific security layer for remote RDP connections is set to Enabled SSL

Rule Status :

Failed

Summary :

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.The recommended state for this setting is: Enabled: SSL. Note: In spite of this setting being labeled SSL , it is actually enforcing Transport Layer Security (TLS) version 1.0, not the older (and less secure) SSL protocol.

Rationale :

The native Remote Desktop Protocol (RDP) encryption is now considered a weak protocol, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Host servers is preferred.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: SSL.Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP) connections.Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:TLS 1.0 will be required to authenticate to the RD Session Host server. If TLS is not supported, the connection fails.Note: By default, this setting will use a self-signed certificate for RDP connections. If your organization has established the use of a Public Key Infrastructure (PKI) for SSL/TLS encryption, then we recommend that you also configure the Server authentication certificate template setting to instruct RDP to use a certificate from your PKI instead of a self-signed one. Note that the certificate template used for this purpose must have Client Authentication configured as an Intended Purpose. Note also that a valid, non-expired certificate using the specified template must already be installed on the workstation for it to work. Note #2: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as the SSL/TLS security layer will expect the user"s Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a double logon requirement for each and every new RDP session.

18.10.57.1. L1 Ensure Prevent downloading of enclosures is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevents the user from having enclosures (file attachments) downloaded from an RSS feed to the user"s computer.The recommended state for this setting is: Enabled.

Rationale :

Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures.Note: This Group Policy path is provided by the Group Policy template InetRes.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was named Turn off downloading of enclosures , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:Users cannot set the Feed Sync Engine to download an enclosure through the Feed property page. Developers cannot change the download setting through feed APIs.

18.10.58.3. L1 Ensure Allow Cortana is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether Cortana is allowed on the device.The recommended state for this setting is: Disabled.

Rationale :

If Cortana is enabled, sensitive information could be contained in search history and sent out to Microsoft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana.Note: This Group Policy path is provided by the Group Policy template Search.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).
Impact:Cortana will be turned off. Users will still be able to use search to find things on the device and on the Internet.

18.10.58.5. L1 Ensure Allow indexing of encrypted files is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.The recommended state for this setting is: Disabled.

Rationale :

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files.Note: This Group Policy path is provided by the Group Policy template Search.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.58.6. L1 Ensure Allow search and Cortana to use location is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether search and Cortana can provide location aware search and Cortana results.The recommended state for this setting is: Disabled.

Rationale :

In an enterprise managed environment, allowing Cortana and Search to have access to location data is unnecessary. Organizations likely do not want this information shared out.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow search and Cortana to use location.Note: This Group Policy path is provided by the Group Policy template Search.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).
Impact:Search and Cortana will not have access to location information.

18.10.58.4. L1 Ensure Allow Cortana above lock screen is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether or not the user can interact with Cortana using speech while the system is locked.The recommended state for this setting is: Disabled.

Rationale :

Access to any computer resource should not be allowed when the device is locked.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana above lock screen.Note: This Group Policy path is provided by the Group Policy template Search.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).
Impact:The system will need to be unlocked for the user to interact with Cortana using speech.

18.10.5.1. L1 Ensure Allow Microsoft accounts to be optional is set to Enabled

Rule Status :

Failed

Summary :

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it.The recommended state for this setting is: Enabled.

Rationale :

Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional.Note: This Group Policy path is provided by the Group Policy template AppXRuntime.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

18.10.65.4. L1 Ensure Turn off the offer to update to the latest version of Windows is set to Enabled

Rule Status :

Failed

Summary :

Enables or disables the Microsoft Store offer to update to the latest version of Windows.The recommended state for this setting is: Enabled.

Rationale :

Unplanned OS upgrades can lead to more preventable support calls. The IT department should be managing and approving all upgrades and updates.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows.Note: This Group Policy path is provided by the Group Policy template WinStoreUI.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template WindowsStore.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Impact:The Microsoft Store application will not offer updates to the latest version of Windows.

18.10.65.3. L1 Ensure Turn off Automatic Download and Install of updates is set to Disabled

Rule Status :

Failed

Summary :

This setting enables or disables the automatic download and installation of Microsoft Store app updates.The recommended state for this setting is: Disabled.

Rationale :

Keeping your system properly patched can help protect against 0 day vulnerabilities.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off Automatic Download and Install of updates.Note: This Group Policy path is provided by the Group Policy template WinStoreUI.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template WindowsStore.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Impact:None - this is the default behavior.

18.10.65.2. L1 Ensure Only display the private store within the Microsoft Store is set to Enabled

Rule Status :

Failed

Summary :

This policy setting denies access to the retail catalog in the Microsoft Store, but displays the private store.The recommended state for this setting is: Enabled.

Rationale :

Allowing the private store will allow an organization to control the apps that users have access to add to a system. This will help ensure that unapproved malicious apps are not running on a system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Only display the private store within the Microsoft Store.Note: This Group Policy path is provided by the Group Policy template WindowsStore.admx/admlthat is included with the Microsoft Windows 10 Release 1607 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Only display the private store within the Windows Store app , but it was renamed starting with the Windows 10 Release 1803 Administrative Templates. Impact:Users will not be able to view the retail catalog in the Microsoft Store, but they will be able to view apps in the private store.

18.10.71.1. L1 Ensure Allow widgets is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether the Widgets feature is allowed on the device. The Widgets feature provides information such as, weather, news, sports, stocks, traffic, and entertainment (not an inclusive list).The recommended state for this setting is: Disabled.

Rationale :

Due to privacy concerns, apps and features such as Widgets on the Windows taskbar should be treated as a possible security risk due to the potential of data being sent back to third-parties, such as Microsoft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Widgets\Allow widgets.Note: This Group Policy path is provided by the Group Policy template NewsAndInterests.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).
Impact:The Widgets feature on the Windows taskbar will not be available on the device.

18.10.75.1.3. L1 Ensure Notify Password Reuse is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Enhanced Phishing Protection in Microsoft Defender SmartScreen warns users if they reuse their work or school password.The recommended state for this setting is: Enabled. Note: This setting only applies to Microsoft Accounts (computer or browser login) while using Microsoft Windows 11 and not on prem domain-joined accounts.

Rationale :

Users will be alerted if they try to use a password that has been exposed in a known data breach. This can help reduce the risk of password-related security incidents, such as unauthorized access to online accounts, and can encourage users to choose strong and unique passwords.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection\Notify Password Reuse.Note: This Group Policy path is provided by the Group Policy template WebThreatDefense.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Password reuse may be detected as a false positive by Microsoft.

18.10.75.1.2. L1 Ensure Notify Malicious is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Enhanced Phishing Protection in Microsoft Defender SmartScreen warns users if they type their work or school password into one of the following malicious scenarios: into a reported phishing site, into a Microsoft login URL with an invalid certificate, or into an application connecting to either a reported phishing site or a Microsoft login URL with an invalid certificate.The recommended state for this setting is: Enabled. Note: This setting only applies to Microsoft Accounts (computer or browser login) while using Microsoft Windows 11 and not on-prem domain-joined accounts.

Rationale :

Users will receive a pop-up notification if they try to access a website that is being blocked by Windows Defender SmartScreen. This assists users in making informed decisions about why the website is being blocked and whether to continue to it.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection\Notify Malicious.Note: This Group Policy path is provided by the Group Policy template WebThreatDefense.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:In some cases, Windows Defender SmartScreen may block legitimate websites, that have been incorrectly flagged by Microsoft.

18.10.75.1.5. L1 Ensure Service Enabled is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Enhanced Phishing Protection is in audit mode. This allows notifications to be sent to users regarding unsafe password events. Additionally, Enhanced Phishing Protection captures unsafe password entry events and sends diagnostic data through Microsoft Defender.The recommended state for this setting is: Enabled. Note: This setting only applies to Microsoft accounts (computer or browser login) while using Microsoft Windows 11 and not on-prem domain-joined accounts.

Rationale :

Allowing Enhanced Phishing Protection the ability to warn users about unsafe password use could prevent phishing attempts and (credential) data loss. In addition, the Microsoft 365 Defender Portal provides valuable phishing sensor data found in the environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection\Service Enabled.Note: This Group Policy path is provided by the Group Policy template WebThreatDefense.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:None - this is default behavior.

18.10.75.1.4. L1 Ensure Notify Unsafe App is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Enhanced Phishing Protection in Microsoft Defender SmartScreen warns users if they type their work or school passwords in Notepad, WordPad, or M365 Office apps like OneNote, Word, Excel, etc.The recommended state for this setting is: Enabled.

Note: This setting only applies to Microsoft Accounts (computer or browser login) while using Microsoft Windows 11 and not on prem domain-joined accounts.

Rationale :

Users will be warned if they store their password in Notepad or Microsoft 365 Office Apps. This can help reduce the risk of security incidents, such as data theft or data loss. Storing credentials in plain text allows for anyone who has authorized or unauthorized access to the system to obtain them.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection\Notify Unsafe App.Note: This Group Policy path is provided by the Group Policy template WebThreatDefense.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Saved passwords may be detected as false positives by Microsoft.

18.10.75.1.1. L1 Ensure Automatic Data Collection is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Enhanced Phishing Protection can collect additional information such as content displayed, sounds played, and application memory when users enter their work or school password into a suspicious website or app.The recommended state for this setting is: Enabled. Note: Per Microsoft, this information is used only for security purposes and helps SmartScreen determine whether the website or app is malicious.

Rationale :

Collection of this data assists Microsoft Defender SmartScreen in determining whether the user entered their work or school password into a suspicious website or app.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection\Automatic Data Collection.This Group Policy path may not exist by default. It is provided by the Group Policy template WebThreatDefense.admx/admlthat is included with the Microsoft Windows 11 Release 23H2 Administrative Templates (or newer). Impact:Enhanced Phishing Protection may automatically collect additional content for security analysis from a suspicious website or app when users enter their work or school password into a website or app.

18.10.75.2.1. L1 Ensure Configure Windows Defender SmartScreen is set to Enabled Warn and prevent bypass

Rule Status :

Failed

Summary :

This policy setting allows you to manage the behavior of Windows Defender SmartScreen. Windows Defender SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.The recommended state for this setting is: Enabled: Warn and prevent bypass.

Rationale :

Windows Defender SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Warn and prevent bypass.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender SmartScreen Note: This Group Policy path is provided by the Group Policy template WindowsExplorer.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Configure Windows SmartScreen , but it was renamed starting with the Windows 10 Release 1703 Administrative Templates. Impact:Users will be warned and prevented from running unrecognized programs downloaded from the Internet.

18.10.77.1. L1 Ensure Enables or disables Windows Game Recording and Broadcasting is set to Disabled

Rule Status :

Failed

Summary :

This setting enables or disables the Windows Game Recording and Broadcasting features.The recommended state for this setting is: Disabled.

Rationale :
If this setting is allowed, users could record and broadcast session info to external sites, which is both a risk of accidentally exposing sensitive company data (on-screen) outside the company as well as a privacy concern.

How to fix :
To establish the recommended configuration via GP, set the following UI path to Disabled:Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and Broadcasting\Enables or disables Windows Game Recording and Broadcasting.Note: This Group Policy path is provided by the Group Policy template GameDVR.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:Windows Game Recording will not be allowed.

18.10.78.1. L1 Ensure Enable ESS with Supported Peripherals is set to Enabled 1

Rule Status :

Failed

Summary :

Enhanced Sign-in Security isolates Windows Hello biometric (face and fingerprint) template data and matching operations to trusted hardware or specified memory regions.The recommended state for this setting is: Enabled: 1. (Enhanced Sign-in Security Enabled)

Rationale :

Because the channel of communication between the sensors and the algorithm is secured, it is impossible for malware to inject or replay data in order to simulate a user signing in or to lock a user out of their machine.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 1(Enhanced Sign-in Security Enabled):
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Hello for Business\Enable ESS with Supported Peripherals.Note: This Group Policy path is provided by the Group Policy template Passport.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:None - this is the default behavior.

18.10.79.2. L1 Ensure Allow Windows Ink Workspace is set to Enabled On but disallow access above lock OR Enabled Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether Windows Ink items are allowed above the lock screen.The recommended state for this setting is: Enabled: On, but disallow access above lockOR Enabled: Disabled.

Rationale :

Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: On, but disallow access above lockOR Enabled: Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow Windows Ink Workspace Note: This Group Policy path is provided by the Group Policy template WindowsInkWorkspace.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:Windows Ink Workspace will not be permitted above the lock screen.

18.10.7.2. L1 Ensure Set the default behavior for AutoRun is set to Enabled Do not execute any autorun commands

Rule Status :

Failed

Summary :

This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inffiles. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands.

Rationale :

Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user"s knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands.Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun.Note: This Group Policy path is provided by the Group Policy template AutoPlay.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:AutoRun commands will be completely disabled.

18.10.7.1. L1 Ensure Disallow Autoplay for non-volume devices is set to Enabled

Rule Status :

Failed

Summary :

This policy setting disallows AutoPlay for MTP devices like cameras or phones.The recommended state for this setting is: Enabled.

Rationale :

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices.Note: This Group Policy path is provided by the Group Policy template AutoPlay.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:AutoPlay will not be allowed for MTP devices like cameras or phones.

18.10.7.3. L1 Ensure Turn off Autoplay is set to Enabled All drives

Rule Status :

Failed

Summary :

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives.

Rationale :

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: All drives.Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay.Note: This Group Policy path is provided by the Group Policy template AutoPlay.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

18.10.8.1.1. L1 Ensure Configure enhanced anti-spoofing is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether enhanced anti-spoofing is configured for devices which support it.The recommended state for this setting is: Enabled.

Rationale :

Enterprise managed environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial Features\Configure enhanced anti-spoofing.Note: This Group Policy path is provided by the Group Policy template Biometrics.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Note #2: In the Windows 10 Release 1511 and Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was initially named Use enhanced anti-spoofing when available . It was renamed to Configure enhanced anti-spoofing starting with the Windows 10 Release 1703 Administrative Templates. Impact:Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

18.10.80.1. L1 Ensure Allow user control over installs is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether users are permitted to change installation options that typically are available only to system administrators. The security features of Windows Installer normally prevent users from changing installation options that are typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.The recommended state for this setting is: Disabled.

Rationale :

In an enterprise managed environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability to have any control over installs can risk unapproved software from being installed or removed from a system, which could cause the system to become vulnerable to compromise.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs.Note: This Group Policy path is provided by the Group Policy template MSI.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was named Enable user control over installs , but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates. Impact:None - this is the default behavior.

18.10.80.2. L1 Ensure Always install with elevated privileges is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled.

Rationale :

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges.Note: This Group Policy path is provided by the Group Policy template MSI.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.81.1. L1 Ensure Enable MPR notifications for the system is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether winlogonsends Multiple Provider Router (MPR) notifications. MPR handles communication between the Windows operating system and the installed network providers. MPR checks the registry to determine which providers are installed on the system and the order they are cycled through. The recommended state for this setting is: Disabled.

Rationale :

MPR is a legacy utility that provides notifications to registered credential managers or network providers when there is a logon event or a password change event. Although this functionality can be used by legitimate applications, it can also be abused by attackers to harvest logon information.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Enable MPR notifications for the system.Note: This Group Policy path is provided by the Group Policy template WinLogon.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact: Winlogonwill not send Multiple Provider Router (MPR) notifications on the system.

18.10.81.2. L1 Ensure Sign-in and lock last interactive user automatically after a restart is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.The recommended state for this setting is: Disabled.

Rationale :

Disabling this feature will prevent the caching of user"s credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Sign-in and lock last interactive user automatically after a restart.Note: This Group Policy path is provided by the Group Policy template WinLogon.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Sign-in last interactive user automatically after a system-initiated restart , but it was renamed starting with the Windows 10 Release 1903 Administrative Templates. Impact:The device does not store the user"s credentials for automatic sign-in after a Windows Update restart. The users" lock screen apps are not restarted after the system restarts. The user is required to present the logon credentials in order to proceed after restart.

18.10.88.1.2. L1 Ensure Allow unencrypted traffic is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.The recommended state for this setting is: Disabled.

Rationale :

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.88.1.3. L1 Ensure Disallow Digest authentication is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.The recommended state for this setting is: Enabled.

Rationale :

Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:The WinRM client will not use Digest authentication.

18.10.88.1.1. L1 Ensure Allow Basic authentication is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication.The recommended state for this setting is: Disabled.

Rationale :

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.88.2.1. L1 Ensure Allow Basic authentication is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.The recommended state for this setting is: Disabled.

Rationale :

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.88.2.3. L1 Ensure Allow unencrypted traffic is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.The recommended state for this setting is: Disabled.

Rationale :

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.10.88.2.4. L1 Ensure Disallow WinRM from storing RunAs credentials is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will allow RunAs credentials to be stored for any plug-ins.The recommended state for this setting is: Enabled. Note: If you enable and then disable this policy setting, any values that were previously configured for RunAsPasswordwill need to be reset.

Rationale :

Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials.Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:The WinRM service will not allow the RunAsUseror RunAsPasswordconfiguration values to be set for any plug-ins. If a plug-in has already set the RunAsUserand RunAsPasswordconfiguration values, the RunAsPasswordconfiguration value will be erased from the credential store on the computer.
If this setting is later Disabled again, any values that were previously configured for RunAsPasswordwill need to be reset.

18.10.90.2. L1 Ensure Allow networking in Windows Sandbox is set to Disabled

Rule Status :

Failed

Summary :

This policy setting enables or disables networking in the Windows Sandbox. Networking is achieved by creating a virtual switch on the host, and connecting the Windows Sandbox to it via a virtual Network Interface Card (NIC).The recommended state for this setting is: Disabled.
Note: The Windows Sandbox feature was first introduced in Windows 10 R1903, and allows a temporary "clean install" virtual instance of Windows to be run inside the host, for the ostensible purpose of testing applications without making changes to the host.

Rationale :

Disabling network access decreases the attack surface exposed by the Windows Sandbox and exposure of untrusted applications to the internal network.Note: Per Microsoft, enabling networking in the Windows Sandbox can expose untrusted applications to the internal network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Sandbox\Allow networking in Windows Sandbox.Note: This Group Policy path is provided by the Group Policy template WindowsSandbox.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:Network access to/from the Windows Sandbox will be disabled. Therefore, files will not be able to be moved to/from the Windows Sandbox via the network.

18.10.90.1. L1 Ensure Allow clipboard sharing with Windows Sandbox is set to Disabled

Rule Status :

Failed

Summary :

This policy setting enables or disables clipboard sharing with the Windows Sandbox.The recommended state for this setting is: Disabled.
Note: The Windows Sandbox feature was first introduced in Windows 10 R1903, and allows a temporary "clean install" virtual instance of Windows to be run inside the host, for the ostensible purpose of testing applications without making changes to the host.

Rationale :

Disabling copy and paste decreases the attack surface exposed by the Windows Sandbox and possible exposure of untrusted applications to the internal network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Sandbox\Allow clipboard sharing with Windows Sandbox.Note: This Group Policy path is provided by the Group Policy template WindowsSandbox.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:The copy and paste function to/from the Windows Sandbox will be disabled. Therefore, files will not be able to be moved to/from the Windows Sandbox via the clipboard.

18.10.91.2.1. L1 Ensure Prevent users from modifying settings is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Security settings.The recommended state for this setting is: Enabled.

Rationale :

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Security\App and browser protection\Prevent users from modifying settings.Note: This Group Policy path is provided by the Group Policy template WindowsDefenderSecurityCenter.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:Local users cannot make changes in the Exploit protection settings area.

18.10.92.1.1. L1 Ensure No auto-restart with logged on users for scheduled automatic updates installations is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation.The recommended state for this setting is: Disabled. Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.

Rationale :

Some security updates require that the computer be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted. Without the auto-restart functionality, users who are not security-conscious may choose to indefinitely delay the restart, therefore keeping the computer in a less secure state.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Legacy Policies\No auto-restart with logged on users for scheduled automatic updates installations.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named No auto-restart for scheduled Automatic Updates installations , but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates. Impact:None - this is the default behavior.

18.10.92.2.2. L1 Ensure Configure Automatic Updates Scheduled install day is set to 0 - Every day

Rule Status :

Failed

Summary :

This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS.The recommended state for this setting is: 0 - Every day. Note: This setting is only applicable if 4 - Auto download and schedule the installis selected in the recommendation "Configure Automatic Updates" . It will have no impact if any other option is selected.

Rationale :

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to 0 - Every day.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience\Configure Automatic Updates: Scheduled install day.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:If 4 - Auto download and schedule the installis selected in recommendation "Configure Automatic Updates" , critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

18.10.92.2.3. L1 Ensure Enable features introduced via servicing that are off by default is set to Disabled

Rule Status :

Failed

Summary :

This policy settings configures whether or not features and enhancements that are introduced through monthly cumulative updates (servicing), are enabled on the system.The recommended state for this setting is: Disabled.

Rationale :

Often, new features or enhancements that are enabled by default (before IT administrators are ready to manage them) can negatively impact the user experience or introduce bugs and security risks.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\\Windows Components\Windows Update\Manage end user experience\Enable features introduced via servicing that are off by default.This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:None - this is the default behavior.

18.10.92.2.4. L1 Ensure Remove access to Pause updates feature is set to Enabled

Rule Status :

Failed

Summary :

This policy removes access to "Pause updates" feature.The recommended state for this setting is: Enabled.

Rationale :

In order to ensure security and system updates are applied, system administrators should control when updates are applied to systems.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience\Remove access to Pause updates feature.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with the Microsoft Windows 10 Release 1809

& Server 2019 Administrative Templates (or newer). Impact:Users will not be able to select the "Pause updates" option in Windows Update to prevent updates from being installed on a system.

18.10.92.2.1. L1 Ensure Configure Automatic Updates is set to Enabled

Rule Status :

Failed

Summary :

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:2 - Notify for download and auto install (Notify before downloading any updates)3 - Auto download and notify for install (Download the updates automatically and notify when they are ready to be installed.) (Default setting)4 - Auto download and schedule the install (Automatically download updates and install them on the schedule specified below.))5 - Allow local admin to choose setting (Leave decision on above choices up to the local Administrators (Not Recommended))The recommended state for this setting is: Enabled. Note: The sub-setting " Configure automatic updating: " has 4 possible values all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of 4 - Auto download and schedule the install. This suggestion is not a scored requirement. Note #2: Organizations that utilize a third--party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to Disabledso that the native Windows Update mechanism does not interfere with the third--party patching process.

Rationale :

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience\Configure Automatic Updates.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Critical operating system updates and service packs will be installed as necessary.

18.10.92.4.2. L1 Ensure Select when Preview Builds and Feature Updates are received is set to Enabled 180 or more days

Rule Status :

Failed

Summary :

This policy setting determines when Preview Build or Feature Updates are received.Defer Updates This enables devices to defer taking the next Feature Update available to your channel for up to 14 days for all the pre-release channels and up to 365 days for the Semi-Annual Channel. Or, if the device is updating from the Semi-Annual Channel, a version for the device to move to and/or stay on until the policy is updated or the device reaches end of service can be specified. Note: If you set both policies, the version specified will take precedence and the deferrals will not be in effect. Please see the Windows Release Information page for OS version information. Pause Updates To prevent Feature Updates from being received on their scheduled time, you can temporarily pause Feature Updates. The pause will remain in effect for 35 days from the specified start date or until the field is cleared (Quality Updates will still be offered). Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect. Note #2: Starting with Windows 10 R1607, Microsoft introduced a new Windows Update (WU) client behavior called Dual Scan , with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to Not Configured or configure the setting Do not allow update deferral policies to cause scans against Windows Update (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links: Demystifying Dual Scan WSUS Product Team Blog./xhtml:li> Improving Dual Scan on 1607 WSUS Product Team Blog./xhtml:li>Note #3: Prior to Windows 10 R1703, values above 180 days are not recognized by the OS. Starting with Windows 10 R1703, the maximum number of days you can defer is 365 days.

Rationale :

In a production environment, it is preferred to only use software and features that are publicly available, after they have gone through rigorous testing in beta.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 180 or more days.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Select when Preview Builds and Feature Updates are received.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Select when Feature Updates are received , but it was renamed to Select when Preview Builds and Feature Updates are received starting with the Windows 10 Release 1709 Administrative Templates. Impact:Feature Updates will be delayed until they are publicly released to general public by Microsoft.

18.10.92.4.4. L1 Ensure Enable optional updates is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether devices are able to receive optional updates (including Controlled Feature Rollout (CFRs)). These optional updates can include non-security updates, feature enhancements, and other improvements.The recommended state for this setting is: Disabled.

Rationale :

Often, new features or enhancements that are enabled by default (before IT administrators are ready to manage them) can negatively impact the user experience or introduce bugs and security risks.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Enable optional updates.This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with the Microsoft Windows 11 Release 23H2 Administrative Templates (or newer). Impact:New features will not be available on the system until the feature update that includes these features and enhancements is installed.

18.10.92.4.1. L1 Ensure Manage preview builds is set to Disabled

Rule Status :

Failed

Summary :

This policy setting manages which updates that are received prior to the update being released.Dev Channel: Ideal for highly technical users. Insiders in the Dev Channel will receive builds from our active development branch that is earliest in a development cycle. These builds are not matched to a specific Windows 10 release. Beta Channel: Ideal for feature explorers who want to see upcoming Windows 10 features. Your feedback will be especially important here as it will help our engineers ensure key issues are fixed before a major release. Release Preview Channel (default): Insiders in the Release Preview Channel will have access to the upcoming release of Windows 10 prior to it being released to the world. These builds are supported by Microsoft. The Release Preview Channel is where we recommend companies preview and validate upcoming Windows 10 releases before broad deployment within their organization. The recommended state for this setting is: Disabled. Note: Preview Build enrollment requires a telemetry level setting of 2 or higher and your domain registered on insider.windows.com. For additional information on Preview Builds, see: https://aka.ms/wipforbiz.

Rationale :

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready builds.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Manage preview builds.Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/admlthat is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact:Preview builds are prevented from installing on the device.

18.10.92.4.3. L1 Ensure Select when Quality Updates are received is set to Enabled 0 days

Rule Status :

Failed

Summary :

This settings controls when Quality Updates are received.The recommended state for this setting is: Enabled: 0 days. Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect. Note #2: Starting with Windows 10 R1607, Microsoft introduced a new Windows Update (WU) client behavior called Dual Scan , with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to Not Configured or configure the setting Do not allow update deferral policies to cause scans against Windows Update (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links: Demystifying Dual Scan WSUS Product Team Blog./xhtml:li> Improving Dual Scan on 1607 WSUS Product Team Blog./xhtml:li>

Rationale :

Quality Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:0 days.Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Select when Quality Updates are received.Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsUpdate.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.4.1. L1 Ensure Apply UAC restrictions to local accounts on network logons is set to Enabled

Rule Status :

Failed

Summary :

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the LocalAccountTokenFilterPolicyregistry value to 0. This is the default behavior for Windows. Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicyregistry value to 1. For more information about local accounts and credential theft, review the " Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques. documents. For more information about LocalAccountTokenFilterPolicy, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista. The recommended state for this setting is: Enabled.

Rationale :

Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\Apply UAC restrictions to local accounts on network logons.Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:None - this is the default behavior.

18.4.2. L1 Ensure Configure RPC packet level privacy setting for incoming connections is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls packet level privacy for Remote Procedure Call (RPC) incoming connections.The recommended state for this setting is: Enabled.

Rationale :

A security bypass vulnerability (CVE-2021-1678 | Windows Print Spooler Spoofing Vulnerability. exists in the way the Printer RPC binding handles authentication for the remote Winspool interface. Enabling the RPC packet level privacy setting for incoming connections enforces the server-side to increase the authentication level to minimize this vulnerability.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure RPC packet level privacy setting for incoming connections.Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:None - this is default behavior.

18.4.5. L1 Ensure Enable Certificate Padding is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures whether the WinVerifyTrust.unction performs strict Windows Authenticode signature verification for Portable Executable files (PE files). If enabled, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification. The recommended state for this setting is: Enabled.

Rationale :

A remote code execution vulnerability exists in the way that the WinVerifyTrust.unction handles Windows Authenticode signature verification for portable executable (PE) files. For more information on this vulnerability, visit CVE-2013-3900 - Security Update Guide - Microsoft - WinVerifyTrust Signature Validation Vulnerability.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Certificate Padding.Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:Microsoft recommends that installers are built to only extract content from validated portions of signed files. Some installers do not follow this guidance and therefore may be negatively impacted by this setting.

18.4.4. L1 Ensure Configure SMB v1 server is set to Disabled

Rule Status :

Failed

Summary :

This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol.The recommended state for this setting is: Disabled.

Rationale :

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.More information on this can be found at the following links: Stop using SMB1 | Storage at Microsoft. Disable SMB v1 in Managed Environments with Group Policy "Stay Safe" Cyber Security Blog. Disabling SMBv1 through Group Policy Microsoft Security Guidance blog.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 server.Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft.

18.4.6. L1 Ensure Enable Structured Exception Handling Overwrite Protection SEHOP is set to Enabled

Rule Status :

Failed

Summary :

Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). We recommend enabling this feature to improve the security profile of the computer.The recommended state for this setting is: Enabled.

Rationale :

This feature is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. This protection mechanism is provided at run-time. Therefore, it helps protect applications regardless of whether they have been compiled with the latest improvements, such as the /SAFESEH option.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP).Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. More information is available at MSKB 956607: How to enable Structured Exception Handling Overwrite Protection (SEHOP) in Windows operating systems.Impact:After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

18.4.3. L1 Ensure Configure SMB v1 client driver is set to Enabled Disable driver recommended

Rule Status :

Failed

Summary :

This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (MRxSmb10), which is recommended to be disabled. The recommended state for this setting is: Enabled: Disable driver (recommended). Note: Do not, under any circumstances , configure this overall setting as Disabled, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale :

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.More information on this can be found at the following links: Stop using SMB1 | Storage at Microsoft. Disable SMB v1 in Managed Environments with Group Policy "Stay Safe" Cyber Security Blog. Disabling SMBv1 through Group Policy Microsoft Security Guidance blog.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Disable driver (recommended).Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 client driver.Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft.

18.4.7. L1 Ensure NetBT NodeType configuration is set to Enabled P-node recommended

Rule Status :

Failed

Summary :

This setting determines which method NetBIOS over TCP/IP (NetBT) uses to register and resolve names. The available methods are:The B-node (broadcast) method only uses broadcasts.The P-node (point-to-point) method only uses name queries to a name server (WINS).The M-node (mixed) method broadcasts first, then queries a name server (WINS) if broadcast failed.The H-node (hybrid) method queries a name server (WINS) first, then broadcasts if the query failed.The recommended state for this setting is: Enabled: P-node (recommended)(point-to-point). Note: Resolution through LMHOSTS or DNS follows these methods. If the NodeTyperegistry value is present, it overrides any DhcpNodeTyperegistry value. If neither NodeTypenor DhcpNodeTypeis present, the computer uses B-node (broadcast) if there are no WINS servers configured for the network, or H-node (hybrid) if there is at least one WINS server configured.

Rationale :

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node (point-to-point) will prevent the system from sending out NetBIOS broadcasts.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: P-node (recommended).Computer Configuration\Policies\Administrative Templates\MS Security Guide\NetBT NodeType configuration.Note: This change does not take effect until the computer has been restarted. Note #2: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Please note that this setting is only available in the Windows 10 v1903 baseline (FINAL) for Windows 10 v1903 and Windows Server v1903 (or newer) release of SecGuide.admx/adml, so if you previously downloaded this template, you may need to update it from a newer Microsoft baseline to get this new NetBT NodeType configuration setting.
Impact:NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

18.4.8. L1 Ensure WDigest Authentication is set to Disabled

Rule Status :

Failed

Summary :

When WDigest authentication is enabled, Lsass.exe retains a copy of the user"s plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server.For more information about local accounts and credential theft, review the " Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques. documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is: Disabled.

Rationale :

Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication (disabling may require KB2871997).Note: This Group Policy path does not exist by default.

An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link. Impact:None - this is also the default configuration for Windows 8.1 or newer.

18.5.1. L1 Ensure MSS AutoAdminLogon Enable Automatic Logon is set to Disabled

Rule Status :

Failed

Summary :

This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group.For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:None - this is the default behavior.

18.5.13. L1 Ensure MSS WarningLevel Percentage threshold for the security event log at which the system will generate a warning is set to Enabled 90 or less

Rule Status :

Failed

Summary :

This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold.The recommended state for this setting is: Enabled: 90% or less. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated.

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

How to fix :
To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:An audit event will be generated when the Security log reaches the 90% percent full threshold (or whatever lower value may be set) unless the log is configured to overwrite events as needed.

18.5.7. L1 Ensure MSS NoNameReleaseOnDemand Allow the computer to ignore NetBIOS name release requests except from WINS servers is set to Enabled

Rule Status :

Failed

Summary :

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request.The recommended state for this setting is: Enabled.

Rationale :

The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries.An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:None - this is the default behavior.

18.5.10. L1 Ensure MSS ScreenSaverGracePeriod The time in seconds before the screen saver grace period expires is set to Enabled 5 or fewer seconds

Rule Status :

Failed

Summary :

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

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

18.5.5. L1 Ensure MSS EnableICMPRedirect Allow ICMP redirects to override OSPF generated routes is set to Disabled

Rule Status :

Failed

Summary :

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes.The recommended state for this setting is: Disabled.

Rationale :

This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system"s exposure to attacks that will impact its ability to participate on the network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

18.5.9. L1 Ensure MSS SafeDllSearchMode Enable Safe DLL search mode is set to Enabled

Rule Status :

Failed

Summary :

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:Search folders specified in the system path first, and then search the current working folder.Search current working folder first, and then search the folders specified in the system path.When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.The recommended state for this setting is: Enabled. Note: More information on how Safe DLL search mode works is available at this link: Dynamic-Link Library Search Order - Windows applications | Microsoft Docs.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:None - this is the default behavior.

18.5.3. L1 Ensure MSS DisableIPSourceRouting IP source routing protection level is set to Enabled Highest protection source routing is completely disabled

Rule Status :

Failed

Summary :

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing.The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale :

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:All incoming source routed packets will be dropped.

18.5.2. L1 Ensure MSS DisableIPSourceRouting IPv6 IP source routing protection level is set to Enabled Highest protection source routing is completely disabled

Rule Status :

Failed

Summary :

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network.The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale :

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled.Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level.Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings Microsoft Security Guidance blog.Impact:All incoming source routed packets will be dropped.

18.6.11.2. L1 Ensure Prohibit installation and configuration of Network Bridge on your DNS domain network is set to Enabled

Rule Status :

Failed

Summary :

You can use this procedure to control a user"s ability to install and configure a Network Bridge.The recommended state for this setting is: Enabled.

Rationale :

The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A Network Bridge thus allows a computer that has connections to two different networks to share data between those networks.In an enterprise managed environment, where there is a need to control network traffic to only authorized paths, allowing users to create a Network Bridge increases the risk and attack surface from the bridged network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network.Note: This Group Policy path is provided by the Group Policy template NetworkConnections.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Users cannot create or configure a Network Bridge.

18.6.11.4. L1 Ensure Require domain users to elevate when setting a networks location is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether to require domain users to elevate when setting a network"s location.The recommended state for this setting is: Enabled.

Rationale :
Allowing regular users to set a network location increases the risk and attack surface.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Require domain users to elevate when setting a network"s location.Note: This Group Policy path is provided by the Group Policy template NetworkConnections.admx/admlthat is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer). Impact:Domain users must elevate when setting a network"s location.

18.6.11.3. L1 Ensure Prohibit use of Internet Connection Sharing on your DNS domain network is set to Enabled

Rule Status :

Failed

Summary :

Although this "legacy" setting traditionally applied to the use of Internet Connection Sharing (ICS) in Windows 2000, Windows XP & Server 2003, this setting now freshly applies to the Mobile Hotspot feature in Windows 10 & Server 2016.The recommended state for this setting is: Enabled.

Rationale :

Non-administrators should not be able to turn on the Mobile Hotspot feature and open their Internet connectivity up to nearby mobile devices.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Sharing on your DNS domain network.Note: This Group Policy path is provided by the Group Policy template NetworkConnections.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

18.6.14.1. L1 Ensure Hardened UNC Paths is set to Enabled with Require Mutual Authentication Require Integrity and Require Privacy set for all NETLOGON and SYSVOL shares

Rule Status :

Failed

Summary :

This policy setting configures secure access to UNC paths.The recommended state for this setting is: Enabled, with "Require Mutual Authentication", "Require Integrity", and Require Privacy set for all NETLOGON and SYSVOL shares.

Rationale :

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the MS15-011. MSKB 3000483.ecurity update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update.
Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk: *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabledwith the following paths configured, at a minimum: *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths.Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with the MS15-011. MSKB 3000483.ecurity update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

18.6.21.2. L1 Ensure Prohibit connection to non-domain networks when connected to domain authenticated network is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time.The recommended state for this setting is: Enabled.

Rationale :

The potential concern is that a user would unknowingly allow network traffic to flow between the insecure public network and the enterprise managed network.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected to domain authenticated network.Note: This Group Policy path is provided by the Group Policy template WCM.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:The computer responds to automatic and manual network connection attempts based on the following circumstances: Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked. Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

18.6.21.1. L1 Ensure Minimize the number of simultaneous connections to the Internet or a Windows Domain is set to Enabled 3 Prevent Wi-Fi when on Ethernet

Rule Status :

Failed

Summary :

This policy setting prevents computers from establishing multiple simultaneous connections to either the Internet or to a Windows domain.The recommended state for this setting is: Enabled: 3 = Prevent Wi-Fi when on Ethernet.

Rationale :

Preventing bridged network connections can help prevent a user unknowingly allowing traffic to route between internal and external networks, which risks exposure to sensitive internal data.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 3 = Prevent Wi-Fi when on Ethernet.Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain.Note: This Group Policy path is provided by the Group Policy template WCM.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates. It was updated with a new Minimize Policy Options sub-setting starting with the Windows 10 Release 1903 Administrative Templates. Impact:While connected to an Ethernet connection, Windows won"t allow use of a WLAN (automatically or manually) until Ethernet is disconnected. However, if a cellular data connection is available, it will always stay connected for services that require it, but no Internet traffic will be routed over cellular if an Ethernet or WLAN connection is present.

18.6.23.2.1. L1 Ensure Allow Windows to automatically connect to suggested open hotspots to networks shared by contacts and to hotspots offering paid services is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether users can enable the following WLAN settings: "Connect to suggested open hotspots," "Connect to networks shared by my contacts," and "Enable paid services"."Connect to suggested open hotspots" enables Windows to automatically connect users to open hotspots it knows about by crowdsourcing networks that other people using Windows have connected to."Connect to networks shared by my contacts" enables Windows to automatically connect to networks that the user"s contacts have shared with them, and enables users on this device to share networks with their contacts."Enable paid services" enables Windows to temporarily connect to open hotspots to determine if paid services are available.The recommended state for this setting is: Disabled. Note: These features are also known by the name " Wi-Fi Sense ".

Rationale :

Automatically connecting to an open hotspot or network can introduce the system to a rogue network with malicious intent.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings\Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services.Note: This Group Policy path is provided by the Group Policy template wlansvc.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Impact: Connect to suggested open hotspots , Connect to networks shared by my contacts , and Enable paid services will each be turned off and users on the device will be prevented from enabling them.

18.6.4.3. L1 Ensure Turn off multicast name resolution is set to Enabled

Rule Status :

Failed

Summary :

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.The recommended state for this setting is: Enabled.

Rationale :

An attacker can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, tricking the host into thinking that it knows the location of the requested system.Note: To completely mitigate local name resolution poisoning, in addition to this setting, the properties of each installed NIC should also be set to Disable NetBIOS over TCP/IP(on the WINS tab in the NIC properties). Unfortunately, there is no global setting to achieve this that automatically applies to all NICs - it is a per-NIC setting that varies with different NIC hardware installations.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off multicast name resolution.Note: This Group Policy path is provided by the Group Policy template DnsClient.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).
Impact:In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

18.6.4.1. L1 Ensure Configure DNS over HTTPS DoH name resolution is set to Enabled Allow DoH or higher

Rule Status :

Failed

Summary :

This setting determines if DNS over HTTPS (DoH) is used by the system. DNS over HTTPS (DoH) is a protocol for performing remote Domain Name System (DNS) resolution over the Hypertext Transfer Protocol Secure (HTTPS). For additional information on DNS over HTTPS (DoH), visit: Secure DNS Client over HTTPS (DoH) on Windows Server 2022 | Microsoft Docs. The recommended state for this setting is: Enabled: Allow DoH. Configuring this setting to Enabled: Require DoHalso conforms to the benchmark.

Rationale :

DNS over HTTPS (DoH) helps protect against DNS spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. It can also help prevent man-in-the-middle (MitM) attacks because the session in-between is encrypted.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Allow DoH(configuring to Enabled: Require DoHalso conforms to the benchmark): Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Configure DNS over HTTPS (DoH) name resolution.Note: This Group Policy path is provided by the Group Policy template DnsClient.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer). Impact:If the option Enabled: Require DoHis chosen, this could limit third-party products from logging DNS traffic (in transit) as the traffic would be encrypted while in transit. The Require DoH option could also lead to domain-joined systems not functioning properly within the environment. The option Enabled: Allow DoHwill perform DoH queries if the configured DNS servers support it. If they dont support it, classic name resolution will be used. This is the safest option. Note: Per Microsoft, don"t enable the Enabled: Require DoHoption for domain-joined computers as Active Directory Domain Services is heavily reliant on DNS because the Windows Server DNS Server service does not support DoH queries.

18.6.4.2. L1 Ensure Configure NetBIOS settings is set to Enabled Disable NetBIOS name resolution on public networks

Rule Status :

Failed

Summary :

This policy setting specifies if the Domain Name System (DNS) client will perform name resolution over Network Basic Input/Output System (NetBIOS). NetBIOS is a legacy name resolution method for internal Microsoft networking that predates the use of DNS for that purpose (preActive Directory). Some legacy applications still require the use of NetBIOS for full functionality.The recommended state for this setting is: Enabled: Disable NetBIOS name resolution on public networks. Configuring this setting to Enabled: Disable NetBIOS name resolutionalso conforms to the benchmark.

Rationale :

NetBIOS does not perform authentication and can allow remote attackers to cause a denial of service by sending spoofed Name Conflicts or Name Release datagrams. This is also known as "NetBIOS Name Server Protocol Spoofing". Preventing the use of NetBIOS on public networks reduces the attack surface.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Disable NetBIOS name resolution on public networks.Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Configure NetBIOS settings.Note: This Group Policy path is provided by the Group Policy template DnsClient.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:None - this is the default behavior.

18.6.8.1. L1 Ensure Enable insecure guest logons is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.The recommended state for this setting is: Disabled.

Rationale :

Insecure guest logons are used by file servers to allow unauthenticated access to shared folders.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled:Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons.Note: This Group Policy path is provided by the Group Policy template LanmanWorkstation.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).
Impact:The SMB client will reject insecure guest logons. This was not originally the default behavior in older versions of Windows, but Microsoft changed the default behavior starting with Windows 10 R1709: Guest access in SMB2 disabled by default in Windows 10 and Windows Server 2016.

18.7.10. L1 Ensure Point and Print Restrictions When installing drivers for a new connection is set to Enabled Show warning and elevation prompt

Rule Status :

Failed

Summary :

This policy setting controls whether computers will show a warning and a security elevation prompt when users create a new printer connection using Point and Print.The recommended state for this setting is: Enabled: Show warning and elevation prompt. Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change.hich modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652Manage new Point and Print default driver installation behavior (CVE-2021-34481). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale :

Enabling Windows User Account Control (UAC) for the installation of new print drivers can help mitigate the PrintNightmare vulnerability (CVE-2021-34527. and other Print Spooler attacks. Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Show warning and elevation prompt.Computer Configuration\Policies\Administrative Templates\Printers\Point and Print Restrictions: When installing drivers for a new connection.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.7.11. L1 Ensure Point and Print Restrictions When updating drivers for an existing connection is set to Enabled Show warning and elevation prompt

Rule Status :

Failed

Summary :

This policy setting controls whether computers will show a warning and a security elevation prompt when users are updating drivers for an existing connection using Point and Print.The recommended state for this setting is: Enabled: Show warning and elevation prompt. Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change.hich modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652Manage new Point and Print default driver installation behavior (CVE-2021-34481). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale :

Enabling Windows User Account Control (UAC) for updating existing print drivers can help mitigate the PrintNightmare vulnerability (CVE-2021-34527. and other Print Spooler attacks. Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Show warning and elevation prompt.Computer Configuration\Policies\Administrative Templates\Printers\Point and Print Restrictions: When updating drivers for an existing connection.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.7.8. L1 Ensure Limits print driver installation to Administrators is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether users who aren"t Administrators can install print drivers on the system.The recommended state for this setting is: Enabled. Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change.hich modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652Manage new Point and Print default driver installation behavior (CVE-2021-34481).

Rationale :

Restricting the installation of print drives to Administrators can help mitigate the PrintNightmare vulnerability (CVE-2021-34527. and other Print Spooler attacks.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled. Computer Configuration\Policies\Administrative Templates\Printers\Limits print driver installation to Administrators.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer). Impact:None - this is the default behavior.

18.7.9. L1 Ensure Manage processing of Queue-specific files is set to Enabled Limit Queue-specific files to Color profiles

Rule Status :

Failed

Summary :

This policy setting manages how queue-specific files are processed during printer installation. At printer installation time, a vendor-supplied installation application can specify a set of files, of any type, to be associated with a particular print queue. The files are downloaded to each client that connects to the print server.The recommended state for this setting is: Enabled: Limit Queue-specific files to Color profiles.

Rationale :

A Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-36958. exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges and then install programs; view, change, or delete data; or create new accounts with full user rights.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Limit Queue-specific files to Color profiles.Computer Configuration\Policies\Administrative Templates\Printers\Manage processing of Queue-specific files.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:None - this is default behavior.

18.7.6. L1 Ensure Configure RPC listener settings Authentication protocol to use for incoming RPC connections is set to Enabled Negotiate or higher

Rule Status :

Failed

Summary :

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.The recommended state for this setting is: Enabled: Negotiateor higher.

Rationale :

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Negotiateor higher: Computer Configuration\Policies\Administrative Templates\Printers\Configure RPC listener settings: Configure protocol options for incoming RPC connections.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

18.7.7. L1 Ensure Configure RPC over TCP port is set to Enabled 0

Rule Status :

Failed

Summary :

This policy setting controls which port is used for RPC over TCP for incoming connections to the print spooler and outgoing connections to remote print spoolers.The recommended state for this setting is: Enabled: 0.

Rationale :

Using dynamic ports for printing makes it more difficult for an attacker to know which port is being used and therefore which port to attack.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 0.Computer Configuration\Policies\Administrative Templates\Printers\Configure RPC over TCP port.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:If your current print environment is configured for a specific TCP port, this setting may require a firewall change (if applicable) for continued printing.

18.7.5. L1 Ensure Configure RPC listener settings Protocols to allow for incoming RPC connections is set to Enabled RPC over TCP

Rule Status :

Failed

Summary :

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.The recommended state for this setting is: Enabled: RPC over TCP.

Rationale :

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: RCP over TCP.Computer Configuration\Policies\Administrative Templates\Printers\Configure RPC listener settings: Configure protocol options for incoming RPC connections Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

18.7.3. L1 Ensure Configure RPC connection settings Protocol to use for outgoing RPC connections is set to Enabled RPC over TCP

Rule Status :

Failed

Summary :

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.The recommended state for this setting is: Enabled: RPC over TCP

Rationale :

This setting prevents the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: RPC over TCP.Computer Configuration\Policies\Administrative Templates\Printers\Configure RPC connection settings: Protocol to use for outgoing RPC connections.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

18.7.4. L1 Ensure Configure RPC connection settings Use authentication for outgoing RPC connections is set to Enabled Default

Rule Status :

Failed

Summary :

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.The recommended state for this setting is: Enabled: Default

Rationale :

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Default.Computer Configuration\Policies\Administrative Templates\Printers\Configure RPC connection settings: Use authentication for outgoing RPC connections.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

18.7.1. L1 Ensure Allow Print Spooler to accept client connections is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls whether the Print Spooler service will accept client connections.The recommended state for this setting is: Disabled. Note: The Print Spooler service must be restarted for changes to this policy to take effect.

Rationale :

Disabling the ability for the Print Spooler service to accept client connections mitigates remote attacks against the PrintNightmare vulnerability (CVE-2021-34527. and other remote Print Spooler attacks. However, this recommendation does not mitigate against local attacks on the Print Spooler service.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\Printers\Allow Print Spooler to accept client connections.Note: This Group Policy path is provided by the Group Policy template printing2.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Provided that the Print Spooler service is not disabled, users will continue to be able to print from their workstation . However, the workstation"s Print Spooler service will not accept client connections or allow users to share printers. Note that all printers that were already shared will continue to be shared.

18.7.2. L1 Ensure Configure Redirection Guard is set to Enabled Redirection Guard Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Redirection Guard is enabled for the print spooler. Redirection Guard can prevent file redirections from being used within the print spooler.The recommended state for this setting is: Enabled: Redirection Guard Enabled.

Rationale :
This setting prevents non-administrators from redirecting files within the print spooler process.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Redirection Guard Enabled.Computer Configuration\Policies\Administrative Templates\Printers\Configure Redirection Guard.Note: This Group Policy path is provided by the Group Policy template Printing.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).
Impact:None - this is default behavior.

18.9.13.1. L1 Ensure Boot-Start Driver Initialization Policy is set to Enabled Good unknown and bad but critical

Rule Status :

Failed

Summary :

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver: Good: The driver has been signed and has not been tampered with. Bad: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized. Bad, but required for boot: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver. Unknown: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver. If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.The recommended state for this setting is: Enabled: Good, unknown and bad but critical.

Rationale :

This policy setting helps reduce the impact of malware that has already infected your system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Good, unknown and bad but critical:Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy.Note: This Group Policy path is provided by the Group Policy template EarlyLaunchAM.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:None - this is the default behavior.

18.9.19.6. L1 Ensure Continue experiences on this device is set to Disabled

Rule Status :

Failed

Summary :

This policy setting determines whether the Windows device is allowed to participate in cross-device experiences (continue experiences).The recommended state for this setting is: Disabled.

Rationale :

A cross-device experience is when a system can access app and send messages to other devices. In an enterprise managed environment only trusted systems should be communicating within the network. Access to any other system should be prohibited.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Group Policy\Continue experiences on this device.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.'

18.9.19.4. L1 Ensure Configure security policy processing Do not apply during periodic background processing is set to Enabled FALSE

Rule Status :

Failed

Summary :

The "Do not apply during periodic background processing" option prevents the system from updating affected security policies in the background while the computer is in use. When background updates are disabled, updates to security policies will not take effect until the next user logon or system restart.This setting affects all policy settings that use the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).The recommended state for this setting is: Enabled: FALSE(unchecked).

Rationale :

Setting this option to false (unchecked) will ensure that domain security policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processingoption to FALSE(unchecked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Built-in security template settings will be reapplied by Group Policy even when the system is in use, which may have a slight impact on performance.

18.9.19.7. L1 Ensure Turn off background refresh of Group Policy is set to Disabled

Rule Status :

Passed

Summary :

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers.The recommended state for this setting is: Disabled.

Rationale :

This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.9.19.2. L1 Ensure Configure registry policy processing Do not apply during periodic background processing is set to Enabled FALSE

Rule Status :

Failed

Summary :

The "Do not apply during periodic background processing" option prevents the system from updating affected registry policies in the background while the computer is in use. When background updates are disabled, registry policy changes will not take effect until the next user logon or system restart.This setting affects all policy settings within the Administrative Templates folder and any other policies that store values in the registry.The recommended state for this setting is: Enabled: FALSE(unchecked).

Rationale :

Setting this option to false (unchecked) will ensure that domain registry policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processingoption to FALSE(unchecked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even when the system is in use, which may have a slight impact on performance.

18.9.19.3. L1 Ensure Configure registry policy processing Process even if the Group Policy objects have not changed is set to Enabled TRUE

Rule Status :

Failed

Summary :

The "Process even if the Group Policy objects have not changed" option updates and reapplies registry policies even if the registry policies have not changed.This setting affects all registry policy settings within the Administrative Templates folder and any other policies that store values in the registry.The recommended state for this setting is: Enabled: TRUE(checked).

Rationale :

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changedoption to TRUE(checked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

18.9.19.5. L1 Ensure Configure security policy processing Process even if the Group Policy objects have not changed is set to Enabled TRUE

Rule Status :

Failed

Summary :

The "Process even if the Group Policy objects have not changed" option updates and reapplies security policies even if the security policies have not changed.This setting affects all policy settings within the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).The recommended state for this setting is: Enabled: TRUE(checked).

Rationale :

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changedoption to TRUE(checked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing.Note: This Group Policy path is provided by the Group Policy template GroupPolicy.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Built-in security template settings will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

18.9.20.1.6. L1 Ensure Turn off Internet download for Web publishing and online ordering wizards is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards.The recommended state for this setting is: Enabled.

Rationale :

Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards.Note: This Group Policy path is provided by the Group Policy template ICM.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

18.9.20.1.2. L1 Ensure Turn off downloading of print drivers over HTTP is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.The recommended state for this setting is: Enabled.

Rationale :

Users might download drivers that include malicious code.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP.Note: This Group Policy path is provided by the Group Policy template ICM.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Print drivers cannot be downloaded over HTTP.Note: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

18.9.25.4. L1 Ensure Password Settings Password Complexity is set to Enabled Large letters small letters numbers special characters

Rule Status :

Failed

Summary :

This policy setting configures the Windows LAPS Password Settings policy for password complexity.Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexityoption to Large letters + small letters + numbers + special characters.Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:None - this is the default behavior.

18.9.25.7. L1 Ensure Post-authentication actions Grace period hours is set to Enabled 8 or fewer hours but not 0

Rule Status :

Failed

Summary :

This policy settings configures post-authentication actions which will be executed after detecting an authentication by the Windows LAPS managed account. The Grace periodrefers to the amount of time (hours) to wait after an authentication before executing the specified post-authentication actions. The recommended state for this setting is: Enabled: 8 or fewer hours, but not 0. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory). Note #3: If this policy is set to 0it prevents all post-authentication actions from occurring.

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: 8 or fewer hours, but not 0.Computer Configuration\Policies\Administrative Templates\System\LAPS\Post-authentication actions: Grace period (hours).Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:After 8 hours, the Windows LAPS managed account password will be reset and log off the system.

18.9.25.5. L1 Ensure Password Settings Password Length is set to Enabled 15 or more

Rule Status :

Failed

Summary :

This policy setting configures the Windows LAPS Password Settings policy for password length.Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.The recommended state for this setting is: Enabled: 15 or more. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Lengthoption to 15 or more.Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:Windows LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

18.9.25.6. L1 Ensure Password Settings Password Age Days is set to Enabled 30 or fewer

Rule Status :

Failed

Summary :

This policy setting configures the Windows LAPS Password Settings policy for password length.Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.The recommended state for this setting is: Enabled: 30 or fewer. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Age (Days)option to 30 or fewer.Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:None - this is the default behavior, unless set to fewer than 30 days.

18.9.25.1. L1 Ensure Configure password backup directory is set to Enabled Active Directory or Enabled Azure Active Directory

Rule Status :

Failed

Summary :

This policy setting configures which directory Windows LAPS will use to back up the local admin account password.The recommended state for this setting is: Enabled: Active Directoryor Enabled: Azure Active Directory. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.
Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory). Note #3: Windows LAPS does not support simultaneous storage of the local admin password in both directory types.
Note #4: If the setting is configured and the managed device is not joined to the configured directory type, the local administrator password will not be managed by Windows LAPS.

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Active Directoryor Enabled: Azure Active Directory.Computer Configuration\Policies\Administrative Templates\System\LAPS\Configure password backup directory.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:The passwords managed by Windows LAPS will only be retrievable from the configured directory type.

18.9.25.8. L1 Ensure Post-authentication actions Actions is set to Enabled Reset the password and logoff the managed account or higher

Rule Status :

Failed

Summary :

This policy settings configures post-authentication actions which will be executed after detecting an authentication by the LAPS managed account. The Actionrefers to actions to take upon expiry of the grace period before executing the specified post-authentication actions. Post-authentication actions: Reset password: upon expiry of the grace period, the managed account password will be reset. Reset the password and logoff the managed account: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminated. Reset the password and reboot the device: upon expiry of the grace period, the managed account password will be reset and the managed device will be immediately rebooted. Warning: After an interactive logon session is terminated, other authenticated sessions using the Windows LAPS managed account may still be active. The only way to ensure that the previous password is no longer in use is to reboot the OS. The recommended state for this setting is: Enabled: Reset the password and logoff the managed accountor higher. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Reset the password and logoff the managed accountor higher: Computer Configuration\Policies\Administrative Templates\System\LAPS\Post-authentication actions: Actions.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:After the grace period expires, the Windows LAPS managed account password will be reset and logged off the system or the OS will be restarted.

18.9.25.3. L1 Ensure Enable password encryption is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether the Windows LAPS managed password is encrypted before being sent to Active Directory.The recommended state for this setting is: Enabled. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory). Note #3: This setting has no effect unless the password has been configured to be backed up to Active Directory, and the Active Directory domain functional level is at Windows Server 2016 or above. Note #4: This setting has no relevance (but is harmless) when storing Windows LAPS passwords to Entra ID (formerly Azure Active Directory) as it automatically encrypts all Windows LAPS passwords.

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\LAPS\Enable password encryption.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).
Impact:None - this is the default behavior.If the domain functional level is set at or above Windows Server 2016, the Windows LAPS managed account password is encrypted automatically, if it is set at a lower domain functional level, the Windows LAPS managed account password will not be backed up to the directory.

18.9.25.2. L1 Ensure Do not allow password expiration time longer than required by policy is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures whether the password age dictated by the Windows LAPS "Password Settings" policy is enforced and cannot be extended manually (only shortened) by an authorized technician.If an expiration is detected, the password is changed immediately, and password expiration is set according to policy.The recommended state for this setting is: Enabled. Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations. Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale :

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\LAPS\Do not allow password expiration time longer than required by policy.Note: This Group Policy path may not exist by default. It is provided by the Group Policy template LAPS.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer). Impact:None - this is the default behavior.Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

18.9.26.2. L1 Ensure Configures LSASS to run as a protected process is set to Enabled Enabled with UEFI Lock

Rule Status :

Failed

Summary :

This policy setting controls whether the Local Security Authority Subservice Service (LSASS) runs in protected mode and also has the option to lock in protected mode with Unified Extensible Firmware Interface (UEFI). The Local Security Authority (LSA), which includes the LSASS process, validates users for local and remote sign-ins and enforces local security policies.The recommended state for this setting is: Enabled: Enabled with UEFI Lock. Note: This additional protection to prevent reading memory and code injection by non-protected processes is supported by Windows 8.1 (or newer).

Rationale :

Provides added security for the credentials that LSA stores and manages. Enabling this setting with UEFI Lockprevents the setting from being changed remotely.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Enabled with UEFI Lock.Computer Configuration\Policies\Administrative Templates\System\Local Security Authority\Configures LSASS to run as a protected process.Impact:Once this setting has been applied (Enabled), removing the group policy setting (set to Not Configured) will not reverse the impact. In order to reverse the impact, you must explicitly configure this setting to Disabled and follow Microsoft"s documentation on disabling the UEFI Lock.

18.9.26.1. L1 Ensure Allow Custom SSPs and APs to be loaded into LSASS is set to Disabled

Rule Status :

Failed

Summary :

This policy setting controls the configuration under which the Local Security Authority Subsystem Service (LSASS) will load custom Security Support Provider/Authentication Package (SSP/AP).The recommended state for this setting is: Disabled.

Rationale :

Vulnerabilities exist where attackers are able to intercept logon credentials via SSP/AP. Disabling Custom SSPs and APs to be loaded into LSASS minimizes this vulnerability.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Local Security Authority\Allow Custom SSPs and APs to be loaded into LSASS.Impact:Custom Security Support Provider/Authentication Packages will not be permitted to load this may impact some legitimate third-party packages.

18.9.28.2. L1 Ensure Do not display network selection UI is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.The recommended state for this setting is: Enabled.

Rationale :

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI.Note: This Group Policy path is provided by the Group Policy template Logon.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:The PC"s network connectivity state cannot be changed without signing into Windows.

18.9.28.6. L1 Ensure Turn off picture password sign-in is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to control whether a domain user can sign in using a picture password.The recommended state for this setting is: Enabled. Note: If the picture password feature is permitted, the user"s domain password is cached in the system vault when using it.

Rationale :

Picture passwords bypass the requirement for a typed complex password. In a shared work environment, a simple shoulder surf where someone observed the on-screen gestures would allow that person to gain access to the system without the need to know the complex password. Vertical monitor screens with an image are much more visible at a distance than horizontal key strokes, increasing the likelihood of a successful observation of the mouse gestures.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in.Note: This Group Policy path is provided by the Group Policy template CredentialProviders.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Users will not be able to set up or sign in with a picture password.

18.9.28.7. L1 Ensure Turn on convenience PIN sign-in is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer Configuration\Administrative Templates\Windows Components\Microsoft Passport for Work.Note: The user"s domain password will be cached in the system vault when using this feature. Note #2: If this setting is Disabled, Windows Hello will not allow Windows Hello Face or Fingerprint to be configured. An exception to this recommendation might be needed if these features are used in the environment. The recommended state for this setting is: Disabled.

Rationale :

A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in.Note: This Group Policy path is provided by the Group Policy template CredentialProviders.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Turn on PIN sign-in , but it was renamed starting with the Windows 10 Release 1511 Administrative Templates. Impact:None - this is the default behavior.

18.9.28.1. L1 Ensure Block user from showing account details on sign-in is set to Enabled

Rule Status :

Failed

Summary :

This policy prevents the user from showing account details (email address or user name) on the sign-in screen.The recommended state for this setting is: Enabled.

Rationale :

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the workstation 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.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in.Note: This Group Policy path is provided by the Group Policy template Logon.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:Users cannot choose to show account details on the sign-in screen.

18.9.28.3. L1 Ensure Do not enumerate connected users on domain-joined computers is set to Enabled

Rule Status :

Failed

Summary :

This policy setting prevents connected users from being enumerated on domain-joined computers.The recommended state for this setting is: Enabled.

Rationale :

A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers.Note: This Group Policy path is provided by the Group Policy template Logon.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:The Logon UI will not enumerate any connected users on domain-joined computers.

18.9.28.4. L1 Ensure Enumerate local users on domain-joined computers is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows local users to be enumerated on domain-joined computers.The recommended state for this setting is: Disabled.

Rationale :

A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers.Note: This Group Policy path is provided by the Group Policy template Logon.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:None - this is the default behavior.

18.9.28.5. L1 Ensure Turn off app notifications on the lock screen is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to prevent app notifications from appearing on the lock screen.The recommended state for this setting is: Enabled.

Rationale :
App notifications might display sensitive business or personal data.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen.Note: This Group Policy path is provided by the Group Policy template Logon.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).
Impact:No app notifications are displayed on the lock screen.

18.9.33.6.2. L1 Ensure Allow network connectivity during connected-standby plugged in is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.The recommended state for this setting is: Disabled.

Rationale :

Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, plugged in and in a sleep state.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in).Note: This Group Policy path is provided by the Group Policy template Power.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:Network connectivity in standby (while plugged in) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

18.9.33.6.6. L1 Ensure Require a password when a computer wakes plugged in is set to Enabled

Rule Status :

Failed

Summary :

Specifies whether or not the user is prompted for a password when the system resumes from sleep.The recommended state for this setting is: Enabled.

Rationale :

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in).Note: This Group Policy path is provided by the Group Policy template Power.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:None - this is the default behavior.

18.9.33.6.5. L1 Ensure Require a password when a computer wakes on battery is set to Enabled

Rule Status :

Failed

Summary :

Specifies whether or not the user is prompted for a password when the system resumes from sleep.The recommended state for this setting is: Enabled.

Rationale :

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery).Note: This Group Policy path is provided by the Group Policy template Power.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:None - this is the default behavior.

18.9.33.6.1. L1 Ensure Allow network connectivity during connected-standby on battery is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.The recommended state for this setting is: Disabled.

Rationale :

Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, on battery and in a sleep state.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (on battery).Note: This Group Policy path is provided by the Group Policy template Power.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:Network connectivity in standby (while on battery) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

18.9.35.2. L1 Ensure Configure Solicited Remote Assistance is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.The recommended state for this setting is: Disabled.

Rationale :

There is slight risk that a rogue administrator will gain access to another user"s desktop session, however, they cannot connect to a user"s computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance.Note: This Group Policy path is provided by the Group Policy template RemoteAssistance.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

18.9.35.1. L1 Ensure Configure Offer Remote Assistance is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer.Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.The recommended state for this setting is: Disabled.

Rationale :

A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance.Note: This Group Policy path is provided by the Group Policy template RemoteAssistance.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:None - this is the default behavior.

18.9.36.1. L1 Ensure Enable RPC Endpoint Mapper Client Authentication is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the trusting domain DCs (see Microsoft KB3073942., so we do not recommend applying it to Domain Controllers. Note: This policy will not in effect until the system is rebooted. The recommended state for this setting is: Enabled.

Rationale :

Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication.Note: This Group Policy path is provided by the Group Policy template RPC.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

18.9.36.2. L1 Ensure Restrict Unauthenticated RPC clients is set to Enabled Authenticated

Rule Status :

Failed

Summary :

This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers.This policy setting impacts all RPC applications. In a domain environment this policy setting should be used with caution as it can impact a wide range of functionality including group policy processing itself. Reverting a change to this policy setting can require manual intervention on each affected machine. This policy setting should never be applied to a Domain Controller.A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically requested to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy setting.Note: This policy setting will not be applied until the system is rebooted. The recommended state for this setting is: Enabled: Authenticated.

Rationale :

Unauthenticated RPC communication can create a security vulnerability.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Authenticated.Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict Unauthenticated RPC clients.Note: This Group Policy path is provided by the Group Policy template RPC.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:None - this is the default behavior.

18.9.3.1. L1 Ensure Include command line in process creation events is set to Enabled

Rule Status :

Failed

Summary :

This policy setting controls whether the process creation command line text is logged in security audit events when a new process has been created.The recommended state for this setting is: Enabled. Note: This feature that this setting controls was not originally supported in workstation OSes older than Windows 8.1. However, in February 2015 Microsoft added support for the feature to Windows 7 and Windows 8.0 via an update - KB3004375. Therefore, this setting is also important to set on those older OSes.

Rationale :

Capturing process command line information in event logs can be very valuable when performing forensic investigations of attack incidents.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events.Note: This Group Policy path is provided by the Group Policy template AuditSettings.admx/admlthat is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact:Process command line information will be included in the event logs, which can contain sensitive or private information such as passwords or user data.Warning: There are potential risks of capturing credentials and sensitive information which could be exposed to users who have read-access to event logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: About Logging Windows - PowerShell | Microsoft Docs.

18.9.4.1. L1 Ensure Encryption Oracle Remediation is set to Enabled Force Updated Clients

Rule Status :

Failed

Summary :

Some versions of the CredSSP protocol that is used by some applications (such as Remote Desktop Connection) are vulnerable to an encryption oracle attack against the client. This policy controls compatibility with vulnerable clients and servers and allows you to set the level of protection desired for the encryption oracle vulnerability.The recommended state for this setting is: Enabled: Force Updated Clients.

Rationale :

This setting is important to mitigate the CredSSP encryption oracle vulnerability, for which information was published by Microsoft on 03/13/2018 in CVE-2018-0886 | CredSSP Remote Code Execution Vulnerability. All versions of Windows from Windows Vista onwards are affected by this vulnerability, and will be compatible with this recommendation provided that they have been patched at least through May 2018 (or later).

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Force Updated Clients.Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Encryption Oracle Remediation.Note: This Group Policy path is provided by the Group Policy template CredSsp.admx/admlthat is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).Impact:Client applications which use CredSSP will not be able to fall back to the insecure versions and services using CredSSP will not accept unpatched clients. This setting should not be deployed until all remote hosts support the newest version, which is achieved by ensuring that all Microsoft security updates at least through May 2018 are installed.

18.9.4.2. L1 Ensure Remote host allows delegation of non-exportable credentials is set to Enabled

Rule Status :

Failed

Summary :

Remote host allows delegation of non-exportable credentials. When using credential delegation, devices provide an exportable version of credentials to the remote host. This exposes users to the risk of credential theft from attackers on the remote host. The Restricted Admin Mode and Windows Defender Remote Credential Guard features are two options to help protect against this risk.The recommended state for this setting is: Enabled. Note: More detailed information on Windows Defender Remote Credential Guard and how it compares to Restricted Admin Mode can be found at this link: Protect Remote Desktop credentials with Windows Defender Remote Credential Guard (Windows 10) | Microsoft Docs.

Rationale :

Restricted Admin Mode was designed to help protect administrator accounts by ensuring that reusable credentials are not stored in memory on remote devices that could potentially be compromised. Windows Defender Remote Credential Guard helps you protect your credentials over a Remote Desktop connection by redirecting Kerberos requests back to the device that is requesting the connection.Both features should be enabled and supported, as they reduce the chance of credential theft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Remote host allows delegation of non-exportable credentials.Note: This Group Policy path is provided by the Group Policy template CredSsp.admx/admlthat is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Impact:The host will support the Restricted Admin Mode and Windows Defender Remote Credential Guard features.

18.9.51.1.2. L1 Ensure Enable Windows NTP Server is set to Disabled

Rule Status :

Failed

Summary :

This policy setting specifies whether the Windows NTP Server is enabled. Disabling this setting prevents the system from acting as a NTP Server (time source) to service NTP requests from other systems (NTP Clients).The recommended state for this setting is: Disabled.

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. This should be done through a known NTP server. Member servers and workstations should not typically be time sources for other clients.

How to fix :

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/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

18.9.51.1.1. L1 Ensure Enable Windows NTP Client is set to Enabled

Rule Status :

Failed

Summary :

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows synchronization from a systems computer clock to NTP server(s).The recommended state for this setting is: Enabled. Note: If a third-party time provider is used in the environment, an exception to this recommendation will be needed.

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.

How to fix :

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/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:System time will be synced to the configured NTP server(s).

18.9.5.7. L1 Ensure Turn On Virtualization Based Security Kernel-mode Hardware-enforced Stack Protection is set to Enabled Enabled in enforcement mode

Rule Status :

Failed

Summary :

This policy setting enables Hardware-enforced Stack Protection for kernel-mode code. Kernel-mode data stacks are hardened with hardware-based shadow stacks, which store intended return address targets to ensure that program control flow is not tampered.The recommended state for this setting is: Enabled: Enabled in enforcement mode. Note: Virtualization Based Security (VBS) requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: This specific security feature of VBS is only compatible with Windows 11 Release 22H2 (or newer). Note #3: Only Intel CPUs from Tiger Lake and beyond or AMD CPUs Zen3 and beyond (both were release in fall 2020) are compatible with this security feature. Note #4: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

This setting stores a copy of the apps shadow stack (intended code execution flow) in the hardware-based (CPU) security feature VBS. This can prevent malware from hijacking an apps code by exploiting memory bugs such as stack buffer overflows, dangling pointers, or uninitialized variables. This allows VBS to shut down any exploit attempts via the modification of the intended code execution flow.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled: Enabled in enforcement modeComputer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Kernel-mode Hardware-enforced Stack Protection.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer). Impact:This setting is dependent upon Virtualization Based Protection of Code Integrity (aka HVCI) first being enabled, in addition to CPU hardware support for shadow stacks. If either HVCI is not enabled or hardware-based shadow stacks are not supported, this setting will have no effect.If this setting is successfully enabled, shadow stack violations will be fatal.Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue.

18.9.5.1. L1 Ensure Turn On Virtualization Based Security is set to Enabled

Rule Status :

Failed

Summary :

This policy setting specifies whether Virtualization Based Security is enabled. Virtualization Based Security uses the Windows Hypervisor to provide support for security services.The recommended state for this setting is: Enabled. Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs. Note #3: If the Level 2 recommendation to configure Log on as a service (from Section 2.2) is implemented, the additional security principal WDAGUtilityAccountmust also be granted that User Right Assignment in order for Virtualization Based Security (in Microsoft Defender Application Guard) with the Next Generation Windows Security (NGWS) profile to function.

Rationale :

Kerberos, NTLM, and Credential manager isolate secrets by using virtualization-based security. Previous versions of Windows stored secrets in the Local Security Authority (LSA). Prior to Windows 10, the LSA stored secrets used by the operating system in its process memory. With Windows Defender Credential Guard enabled, the LSA process in the operating system talks to a new component called the isolated LSA process that stores and protects those secrets. Data stored by the isolated LSA process is protected using virtualization-based security and is not accessible to the rest of the operating system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).
Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

18.9.5.4. L1 Ensure Turn On Virtualization Based Security Require UEFI Memory Attributes Table is set to True checked

Rule Status :

Failed

Summary :

This option will only enable Virtualization Based Protection of Code Integrity on devices with UEFI firmware support for the Memory Attributes Table. Devices without the UEFI Memory Attributes Table may have firmware that is incompatible with Virtualization Based Protection of Code Integrity which in some cases can lead to crashes or data loss or incompatibility with certain plug-in cards. If not setting this option the targeted devices should be tested to ensure compatibility.The recommended state for this setting is: True (checked). Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

This setting will help protect this control from being enabled on a system that is not compatible which could lead to a crash or data loss.

How to fix :

To establish the recommended configuration via GP, set the following UI path to TRUE.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes Table.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

18.9.5.5. L1 Ensure Turn On Virtualization Based Security Credential Guard Configuration is set to Enabled with UEFI lock

Rule Status :

Failed

Summary :

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials. The "Enabled with UEFI lock" option ensures that Credential Guard cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI.The recommended state for this setting is: Enabled with UEFI lock. Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

The Enabled with UEFI lockoption ensures that Credential Guard cannot be disabled remotely.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled with UEFI lock.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Credential Guard Configuration.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible. Warning #2: Once this setting is turned on and active, Credential Guard cannot be disabled solely via GPO or any other remote method. After removing the setting from GPO, the features must also be manually disabled locally at the machine using the steps provided at this link: Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs.

18.9.5.2. L1 Ensure Turn On Virtualization Based Security Select Platform Security Level is set to Secure Boot or higher

Rule Status :

Failed

Summary :

This policy setting specifies whether Virtualization Based Security (VBS) is enabled. VBS uses the Windows Hypervisor to provide support for security services.The recommended state for this setting is: Secure Bootor Secure Boot and DMA Protection. Note: VBS requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

Secure Boot can help reduce the risk of bootloader attacks and in conjunction with DMA protections to help protect data from being scraped from memory.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Secure Bootor Secure Boot and DMA Protection.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Select Platform Security Level.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:Choosing the Secure Bootoption provides the system with as much protection as is supported by the computers hardware. A system with input/output memory management units (IOMMUs) will have Secure Boot with DMA protection. A system without IOMMUs will simply have Secure Boot enabled without DMA protection. Choosing the Secure Boot with DMA protectionoption requires the system to have IOMMUs in order to enable VBS. Without IOMMU hardware support, VBS will be disabled. Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

18.9.5.3. L1 Ensure Turn On Virtualization Based Security Virtualization Based Protection of Code Integrity is set to Enabled with UEFI lock

Rule Status :

Failed

Summary :

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.The recommended state for this setting is: Enabled with UEFI lock. Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM. More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs.Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

The Enabled with UEFI lockoption ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled with UEFI lock.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue. Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible. Warning #2: Once this setting is turned on and active, Virtualization Based Security cannot be disabled solely via GPO or any other remote method. After removing the setting from GPO, the features must also be manually disabled locally at the machine using the steps provided at this link: Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs.

18.9.5.6. L1 Ensure Turn On Virtualization Based Security Secure Launch Configuration is set to Enabled

Rule Status :

Failed

Summary :

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.The recommended state for this setting is: Enabled. Note: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale :

Secure Launch changes the way Windows boots to use Intel Trusted Execution Technology (TXT) and Runtime BIOS Resilience features to prevent firmware exploits from being able to impact the security of the Windows Virtualization Based Security environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Secure Launch Configuration.Note: This Group Policy path is provided by the Group Policy template DeviceGuard.admx/admlthat is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer). Impact:Note: This setting was moved from the Next Generation (NG) profile to the Level 1 (L1) profile for the Windows 11 Operating System only . NG profile settings were isolated from the L1 profile due to potential hardware compatibility issues. The Windows 11 Operating System is dependent on the same hardware as the NG settings, so hardware compatibility is no longer an issue.
Warning : All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

18.9.7.2. L1 Ensure Prevent device metadata retrieval from the Internet is set to Enabled

Rule Status :

Failed

Summary :

This policy setting allows you to prevent Windows from retrieving device metadata from the Internet.The recommended state for this setting is: Enabled. Note: This will not prevent the installation of basic hardware drivers, but does prevent associated third-party utility software from automatically being installed under the context of the SYSTEMaccount.

Rationale :

Installation of software should be conducted by an authorized system administrator and not a standard user. Allowing automatic third-party software installations under the context of the SYSTEMaccount has potential for allowing unauthorized access via backdoors or installation software bugs.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Administrative Templates\System\Device Installation\Prevent device metadata retrieval from the Internet.Note: This Group Policy path is provided by the Group Policy template DeviceInstallation.admx/admlthat is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates, or with the Group Policy template DeviceSetup.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Standard users without administrator privileges will not be able to install associated third-party utility software for peripheral devices. This may limit the use of advanced features of those devices unless/until an administrator installs the associated utility software for the device.

19.5.1.1. L1 Ensure Turn off toast notifications on the lock screen is set to Enabled

Rule Status :

Failed

Summary :

This policy setting turns off toast notifications on the lock screen.The recommended state for this setting is Enabled.

Rationale :

While this feature can be handy for users, applications that provide toast notifications might display sensitive personal or business data while the device is left unattended.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen.Note: This Group Policy path is provided by the Group Policy template WPN.admx/admlthat is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact:Applications will not be able to raise toast notifications on the lock screen.

19.7.26.1. L1 Ensure Prevent users from sharing files within their profile. is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether users can share files within their profile. By default, users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile.The recommended state for this setting is: Enabled.

Rationale :

If not properly configured, a user could accidentally share sensitive data with unauthorized users. In an enterprise managed environment, the company should provide a managed location for file sharing, such as a file server or SharePoint, instead of the user sharing files directly from their own user profile.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled:User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile..Note: This Group Policy path is provided by the Group Policy template Sharing.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates.
Impact:Users cannot share files within their profile using the sharing wizard. Also, the sharing wizard cannot create a share at %root%\Usersand can only be used to create SMB shares on folders.

19.7.38.1. L1 Ensure Turn off Windows Copilot is set to Enabled

Rule Status :

Failed

Summary :

This policy setting configures the use of Windows Copilot. Windows Copilot is an artificial intelligence (AI) assistant that"s integrated in Microsoft Windows workstation OSes, beginning with Windows 11 Release 23H2.The recommended state for this setting is: Enabled.

Rationale :

While AI can be an exciting new technology, it also carries its own risks, including the possibility of users accidentally uploading or typing personal or organization-sensitive data into it, with no real way to undo or get that data back.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Policies\Administrative Templates\Windows Components\Windows Copilot\Turn off Windows Copilot.This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsCopilot.admx/admlthat is included with the Microsoft Windows 11 Release 23H2 Administrative Templates (or newer). Impact:Users will not be able to use Windows Copilot and its icon will not appear on the taskbar.

19.7.42.1. L1 Ensure Always install with elevated privileges is set to Disabled

Rule Status :

Failed

Summary :

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled.

Rationale :

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges.Note: This Group Policy path is provided by the Group Policy template MSI.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

19.7.5.1. L1 Ensure Do not preserve zone information in file attachments is set to Disabled

Rule Status :

Failed

Summary :

This policy setting allows you to manage whether Windows marks file attachments with information about their zone of origin (such as restricted, Internet, intranet, local). This requires NTFS in order to function correctly, and will fail without notice on FAT32. By not preserving the zone information, Windows cannot make proper risk assessments.The recommended state for this setting is: Disabled. Note: The Attachment Manager feature warns users when opening or executing files which are marked as being from an untrusted source, unless/until the file"s zone information has been removed via the "Unblock" button on the file"s properties or via a separate tool such as Microsoft Sysinternals Streams.

Rationale :

A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user. The Attachment Manager feature will warn users when opening or executing files which are marked as being from an untrusted source, unless/until the file"s zone information has been removed.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments.Note: This Group Policy path is provided by the Group Policy template AttachmentManager.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:None - this is the default behavior.

19.7.5.2. L1 Ensure Notify antivirus programs when opening attachments is set to Enabled

Rule Status :

Failed

Summary :

This policy setting manages the behavior for notifying registered antivirus programs. If multiple programs are registered, they will all be notified.The recommended state for this setting is: Enabled. Note: An updated antivirus program must be installed for this policy setting to function properly.

Rationale :

Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments.Note: This Group Policy path is provided by the Group Policy template AttachmentManager.admx/admlthat is included with all versions of the Microsoft Windows Administrative Templates. Impact:Windows tells the registered antivirus program(s) to scan the file when a user opens a file attachment. If the antivirus program fails, the attachment is blocked from being opened.

19.7.8.2. L1 Ensure Do not suggest third-party content in Windows spotlight is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Windows will suggest apps and content from third-party software publishers.The recommended state for this setting is: Enabled.

Rationale :
Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

How to fix :
To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not suggest third-party content in Windows spotlight.Note: This Group Policy path is provided by the Group Policy template CloudContent.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will no longer suggest apps and content from third-party software publishers. Users may still see suggestions and tips to make them more productive with Microsoft features and apps.

19.7.8.5. L1 Ensure Turn off Spotlight collection on Desktop is set to Enabled

Rule Status :

Failed

Summary :

This policy setting removes the Spotlight collection setting in Personalization, rendering the user unable to select and subsequently download daily images from Microsoft to the system desktop.The recommended state for this setting is: Enabled.

Rationale :

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display images from Microsoft.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Spotlight collection on Desktop.Note: This Group Policy path is provided by the Group Policy template CloudContent.admx/admlthat is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).
Impact:The Spotlight collectionfeature will not be available as an option in Personalization settings, so users will not be able to download daily images from Microsoft.

19.7.8.1. L1 Ensure Configure Windows spotlight on lock screen is set to Disabled

Rule Status :

Failed

Summary :

This policy setting lets you configure Windows Spotlight on the lock screen.The recommended state for this setting is: Disabled. Note: Per Microsoft TechNet. this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale :

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Configure Windows spotlight on lock screen.Note: This Group Policy path is provided by the Group Policy template CloudContent.admx/admlthat is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact:Windows Spotlight will be turned off and users will no longer be able to select it as their lock screen.

2.2.19. L1 Ensure Deny log on locally to include Guests

Rule Status :

Failed

Summary :

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests. Important: If you apply this security policy to the Everyonegroup, no one will be able to log on locally.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Guests.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally.Impact:If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNETaccount on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

2.2.34. L1 Ensure Profile single process is set to Administrators

Rule Status :

Passed

Summary :

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

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process.Impact:None - this is the default behavior.

2.2.20. L1 Ensure Deny log on through Remote Desktop Services to include Guests Local account

Rule Status :

Failed

Summary :

This policy setting determines whether users can log on as Remote Desktop clients. After the baseline workstation is joined to a domain environment, there is no need to use local accounts to access the workstation from the network. Domain accounts can access the workstation for administration and end-user processing. This user right supersedes the Allow log on through Remote Desktop Services user right if an account is subject to both policies. The recommended state for this setting is to include: Guests, 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 accountis not available in Windows 7 and Windows 8.0 unless MSKB 2871997.as been installed. Note #2: In all versions of Windows prior to Windows 7, Remote Desktop Services was known as Terminal Services , so you should substitute the older term if comparing against an older OS.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services.Impact:If you assign the Deny log on through Remote Desktop Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

2.2.4. L1 Ensure Adjust memory quotas for a process is set to Administrators LOCAL SERVICE NETWORK SERVICE

Rule Status :

Failed

Summary :

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

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process.Impact:Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

2.2.18. L1 Ensure Deny log on as a service to include Guests

Rule Status :

Failed

Summary :

This security setting determines which service accounts are prevented from registering a process as a service. This user right supersedes the Log on as a service user right if an account is subject to both policies. The recommended state for this setting is to include: Guests. Note: This security setting does not apply to the System, Local Service, or Network Serviceaccounts.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Guests.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service.Impact:If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

2.2.17. L1 Ensure Deny log on as a batch job to include Guests

Rule Status :

Failed

Summary :

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right.This user right supersedes the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Guests.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job.Impact:If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely. For example, if you assign this user right to the IWAM_ (ComputerName) account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guestsgroup, but on a computer that was upgraded from Windows 2000 this account is a member of the Guestsgroup. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

2.2.9. L1 Ensure Change the time zone is set to Administrators LOCAL SERVICE Users

Rule Status :

Passed

Summary :

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers.The recommended state for this setting is: Administrators, LOCAL SERVICE, Users.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, Users.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone.Impact:None - this is the default behavior.

2.2.10. L1 Ensure Create a pagefile is set to Administrators

Rule Status :

Passed

Summary :

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer.The recommended state for this setting is: Administrators.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile.Impact:None - this is the default behavior.

2.2.11. L1 Ensure Create a token object is set to No One

Rule Status :

Passed

Summary :

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.

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object.Impact:None - this is the default behavior.

2.2.12. L1 Ensure Create global objects is set to Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

Rule Status :

Passed

Summary :

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right.Users who can create global objects could affect processes that run under other users" sessions. This capability could lead to a variety of problems, such as application failure or data corruption.The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects.Impact:None - this is the default behavior.

2.2.5. L1 Ensure Allow log on locally is set to Administrators Users

Rule Status :

Failed

Summary :

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, Users. Note: The Guestaccount is also assigned this user right by default. Although this account is disabled by default, it"s recommended that you configure this setting through Group Policy. However, this user right should generally be restricted to the Administratorsand Usersgroups. Assign this user right to the Backup Operatorsgroup 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.

How to fix :

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

2.2.6. L1 Ensure Allow log on through Remote Desktop Services is set to Administrators Remote Desktop Users

Rule Status :

Passed

Summary :

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 Administratorsgroup or use the Restricted Groups feature to ensure that no user accounts are part of the Remote Desktop Usersgroup. Restrict this user right to the Administratorsgroup, and possibly the Remote Desktop Usersgroup, 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: The above list is to be treated as a whitelist, which implies that the above principals need not be present for assessment of this recommendation to pass. Note #2: In all versions of Windows prior to Windows 7, 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.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, Remote Desktop Users.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.

2.2.7. L1 Ensure Back up files and directories is set to Administrators

Rule Status :

Failed

Summary :

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories.Impact:Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

2.2.8. L1 Ensure Change the system time is set to Administrators LOCAL SERVICE

Rule Status :

Passed

Summary :

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer"s time setting is changed, logged events reflect the new time, not the actual time that the events occurred.The recommended state for this setting is: Administrators, LOCAL SERVICE. Note: Discrepancies between the time on the local computer and on the Domain Controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the Domain Controllers.

Rationale :

Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer"s time may cause that computer to be unable to obtain or grant Kerberos tickets.The risk from these types of events is mitigated on most Domain Controllers, Member Servers, and end-user computers because the Windows Time service automatically synchronizes time with Domain Controllers in the following ways:All client desktop computers and Member Servers use the authenticating Domain Controller as their inbound time partner.All Domain Controllers in a domain nominate the Primary Domain Controller (PDC) Emulator operations master as their inbound time partner.All PDC Emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner.The PDC Emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server.This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time.Impact:There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

2.2.15. L1 Ensure Debug programs is set to Administrators

Rule Status :

Passed

Summary :

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it.The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs.Impact:If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the Debug programs user right to a separate Group Policy for that OU. The service account that is used for the cluster service needs the Debug programs user right; if it does not have it, Windows Clustering will fail. Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool Kill.exerequires this user right for administrators to terminate processes that they did not start.

2.2.14. L1 Configure Create symbolic links

Rule Status :

Passed

Summary :

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only Administratorscan create symbolic links. The recommended state for this setting is: Administratorsand (when the Hyper-V feature is installed) NT VIRTUAL MACHINE\Virtual Machines.

Rationale :

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

How to fix :

To implement the recommended configuration state, configure the following UI path:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links.Impact:In most cases there will be no impact because this is the default configuration. However, on Windows Workstations with the Hyper-V feature installed, this user right should also be granted to the special group NT VIRTUAL MACHINE\Virtual Machines- otherwise you will not be able to create new virtual machines.

2.2.13. L1 Ensure Create permanent shared objects is set to No One

Rule Status :

Passed

Summary :

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right.The recommended state for this setting is: No One.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects.Impact:None - this is the default behavior.

2.2.16. L1 Ensure Deny access to this computer from the network to include Guests Local account

Rule Status :

Failed

Summary :

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 accountis not available in Windows 7 and Windows 8.0 unless MSKB 2871997.as 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.

How to fix :

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network.Impact:If you configure the Deny access to this computer from the network user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

2.2.22. L1 Ensure Force shutdown from a remote system is set to Administrators

Rule Status :

Passed

Summary :

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

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system.Impact:If you remove the shutdown from a remote system user right from the Server Operators group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Force

2.2.1. L1 Ensure Access Credential Manager as a trusted caller is set to No One

Rule Status :

Passed

Summary :

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

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

How to fix :
To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller.Impact:None - this is the default behavior.

2.2.21. L1 Ensure Enable computer and user accounts to be trusted for delegation is set to No One

Rule Status :

Passed

Summary :

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.The recommended state for this setting is: No One. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation.Impact:None - this is the default behavior.

2.2.30. L1 Ensure Manage auditing and security log is set to Administrators

Rule Status :

Passed

Summary :

This policy setting determines which users can change the auditing options for files and directories and clear the Security log.The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log.Impact:None - this is the default behavior.

2.2.3. L1 Ensure Act as part of the operating system is set to No One

Rule Status :

Passed

Summary :

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access.The recommended state for this setting is: No One. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system.Impact:There should be little or no impact because the Act as part of the operating system user right is rarely needed by any accounts other than the Local Systemaccount, which implicitly has this right.

2.2.2. L1 Ensure Access this computer from the network is set to Administrators Remote Desktop Users

Rule Status :

Failed

Summary :

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).The recommended state for this setting is: Administrators, Remote Desktop Users. Note: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same Access this computer from the networkUser Right Assignment. For more information on adding the service account please see Make sure the DSA is allowed to access computers from the network in Microsoft Defender for Identity | Microsoft Docs.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, Remote Desktop Users.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network.Impact:If you remove the Access this computer from the network user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it be assigned to the Authenticated Usersgroup. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

2.2.27. L1 Ensure Lock pages in memory is set to No One

Rule Status :

Passed

Summary :

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur.The recommended state for this setting is: No One.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory.Impact:None - this is the default behavior.

2.2.32. L1 Ensure Modify firmware environment values is set to Administrators

Rule Status :

Passed

Summary :

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would result in a denial of service condition.The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values.Impact:None - this is the default behavior.

2.2.31. L1 Ensure Modify an object label is set to No One

Rule Status :

Passed

Summary :

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege.The recommended state for this setting is: No One.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to No One.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label.Impact:None - this is the default behavior.

2.2.26. L1 Ensure Load and unload device drivers is set to Administrators

Rule Status :

Passed

Summary :

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista.The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers.Impact:If you remove the Load and unload device drivers user right from the Print Operatorsgroup or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

2.2.25. L1 Ensure Increase scheduling priority is set to Administrators Window ManagerWindow Manager Group

Rule Status :

Passed

Summary :

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools.The recommended state for this setting is: Administrators, Window Manager\Window Manager Group.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, Window Manager\Window Manager Group.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority.Impact:None - this is the default behavior.

2.2.24. L1 Ensure Impersonate a client after authentication is set to Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

Rule Status :

Failed

Summary :

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connectfor example, by remote procedure call (RPC) or named pipesto a service that they have created to impersonate that client, which could elevate the unauthorized user"s permissions to administrative or system levels.Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.Also, a user can impersonate an access token if any of the following conditions exist:The access token that is being impersonated is for this user.The user, in this logon session, logged on to the network with explicit credentials to create the access token.The requested level is less than Impersonate, such as Anonymous or Identify.An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker"s level of access to that of the client. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication.Impact:In most cases this configuration will have no impact. If you have installed Web Server (IIS) , you will need to also assign the user right to IIS_IUSRS.

2.2.23. L1 Ensure Generate security audits is set to LOCAL SERVICE NETWORK SERVICE

Rule Status :

Failed

Summary :

This policy setting determines which users or processes can generate audit records in the Security log.The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits.Impact:On most computers, this is the default configuration and there will be no negative impact. However, if you have installed Web Server (IIS) , you will need to allow the IIS application pool(s) to be granted this user right.

2.2.39. L1 Ensure Take ownership of files or other objects is set to Administrators

Rule Status :

Passed

Summary :

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects.Impact:None - this is the default behavior.

2.2.38. L1 Ensure Shut down the system is set to Administrators Users

Rule Status :

Failed

Summary :

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

Rationale :

The ability to shut down a workstation should be available generally to Administrators and authorized users of that workstation, but not permitted for guests or unauthorized users - in order to prevent a Denial of Service attack.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, Users.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system.Impact:The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

2.2.33. L1 Ensure Perform volume maintenance tasks is set to Administrators

Rule Status :

Passed

Summary :

This policy setting allows users to manage the system"s volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition.The recommended state for this setting is: Administrators. Note: A workstation with Microsoft SQL Server installed will require a special exception to this recommendation for the account that runs the SQL Server service to be granted this user right.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks.Impact:None - this is the default behavior.

2.2.37. L1 Ensure Restore files and directories is set to Administrators

Rule Status :

Failed

Summary :

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista (or newer) in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that is used to back up data.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories.Impact:If you remove the Restore files and directories user right from the Backup Operatorsgroup and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won"t negatively affect the ability of your organization"s personnel to do their jobs.

2.2.36. L1 Ensure Replace a process level token is set to LOCAL SERVICE NETWORK SERVICE

Rule Status :

Failed

Summary :

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges.The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token.Impact:On most computers, this is the default configuration and there will be no negative impact. However, if you have installed Web Server (IIS) , you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

2.2.35. L1 Ensure Profile system performance is set to Administrators NT SERVICEWdiServiceHost

Rule Status :

Passed

Summary :

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system"s active processes and provide insight into the potential attack surface of the computer.The recommended state for this setting is: Administrators, NT SERVICE\WdiServiceHost.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators, NT SERVICE\WdiServiceHost.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance.Impact:None - this is the default behavior.

2.3.10.7. L1 Ensure Network access Remotely accessible registry paths is configured

Rule Status :

Passed

Summary :

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winregregistry key. Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2). Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor"s display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

Rationale :

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

How to fix :

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications SOFTWARE\Microsoft\Windows NT\CurrentVersionComputer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths.Impact:None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.Note: If you want to allow remote access, you must also enable the Remote Registry service.

2.3.10.8. L1 Ensure Network access Remotely accessible registry paths and sub-paths is configured

Rule Status :

Passed

Summary :

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winregregistry key. Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008 (non-R2), and Windows Server 2003 does not exist in Windows XP. Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor"s display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog

Rationale :

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

How to fix :

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog SOFTWARE\Microsoft\OLAP Server SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLogComputer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths.Impact:None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.Note: If you want to allow remote access, you must also enable the Remote Registry service.

2.3.10.12. L1 Ensure Network access Sharing and security model for local accounts is set to Classic - local users authenticate as themselves

Rule Status :

Passed

Summary :

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource.The recommended state for this setting is: Classic - local users authenticate as themselves. Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale :

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Classic - local users authenticate as themselves.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts.Impact:None - this is the default configuration for domain-joined computers.

2.3.10.2. L1 Ensure Network access Do not allow anonymous enumeration of SAM accounts is set to Enabled

Rule Status :

Passed

Summary :

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections.The recommended state for this setting is: Enabled. Note: This policy has no effect on Domain Controllers.

Rationale :

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

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts.Impact:None - this is the default behavior. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

2.3.10.6. L1 Ensure Network access Named Pipes that can be accessed anonymously is set to None

Rule Status :

Passed

Summary :

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.The recommended state for this setting is: <blank>(i.e. None).

Rationale :

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

How to fix :

To establish the recommended configuration via GP, set the following UI path to <blank>(i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously.Impact:This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function.

2.3.10.9. L1 Ensure Network access Restrict anonymous access to Named Pipes and Shares is set to Enabled

Rule Status :

Passed

Summary :

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymouslyand Network access: Shares that can be accessed anonymouslysettings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccesswith the value 1in the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parametersregistry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients" access to named resources.The recommended state for this setting is: Enabled.

Rationale :

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares.Impact:None - this is the default behavior. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the Network access: Named pipes that can be accessed anonymously list: COMNAP: SNA session accessCOMNODE: SNA session accessSQL\QUERY: SQL instance accessSPOOLSS: Spooler serviceLLSRPC: License Logging serviceNETLOGON: Net Logon serviceLSARPC: LSA accessSAMR: Remote access to SAM objectsBROWSER: Computer Browser servicePrevious to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

2.3.10.5. L1 Ensure Network access Let Everyone permissions apply to anonymous users is set to Disabled

Rule Status :

Passed

Summary :

This policy setting determines what additional permissions are assigned for anonymous connections to the computer.The recommended state for this setting is: Disabled.

Rationale :
An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

How to fix :
To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users.Impact:None - this is the default behavior.

2.3.10.11. L1 Ensure Network access Shares that can be accessed anonymously is set to None

Rule Status :

Passed

Summary :

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.The recommended state for this setting is: <blank>(i.e. None).

Rationale :
It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

How to fix :
To establish the recommended configuration via GP, set the following UI path to <blank>(i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously.Impact:None - this is the default behavior.

2.3.10.4. L1 Ensure Network access Do not allow storage of passwords and credentials for network authentication is set to Enabled

Rule Status :

Failed

Summary :

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication.The recommended state for this setting is: Enabled. Note: Changes to this setting will not take effect until Windows is restarted.

Rationale :

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication.Impact:Credential Manager will not store passwords and credentials on the computer. Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren"t accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third-party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

2.3.10.1. L1 Ensure Network access Allow anonymous SIDName translation is set to Disabled

Rule Status :

Passed

Summary :

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name.The recommended state for this setting is: Disabled.

Rationale :

If this policy setting is enabled, a user with local access could use the well-known Administrator"s SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

How to fix :

To establish the recommended configuration via GP, set the following UI path to Disabled.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation.Impact:None - this is the default behavior.

2.3.10.10. L1 Ensure Network access Restrict clients allowed to make remote calls to SAM is set to Administrators Remote Access Allow

Rule Status :

Failed

Summary :

This policy setting allows you to restrict remote RPC connections to SAM.The recommended state for this setting is: Administrators: Remote Access: Allow. Note: A Windows 10 R1607, Server 2016 or newer OS is required to access and set this value in Group Policy. Note #2: This setting was originally only supported on Windows 10 R1607 or newer, then support for it was added to Windows 7 or newer via the March 2017 security patches. Note #3: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same Remote Access: Allowpermission. For more information on adding the service account please see Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity | Microsoft Docs.

Rationale :

To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

How to fix :

To establish the recommended configuration via GP, set the following UI path to Administrators: Remote Access: Allow.Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict clients allowed to make remote calls to SAM.Impact:None - this is the default behavior.