**Manual Steps Required to Comply with Windows 10 CIS Level 1**

Manual steps are required due to differing SID’s within different Windows 10 versions thus unable to automate the process for setting user specific settings.

|  |  |
| --- | --- |
| **Password Policies** | |
| 1 | Open Local Security Policy > Action > Import Policy |
| 2 | Select Password Policy.inf file and open |
| 3 | If modification required open the file with notepad and adjust values as per organization policy. |

|  |  |
| --- | --- |
| **2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Access this computer from the network” > Remove all accounts **EXCEPT** “administrators” and “remote desktop users” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.5 Ensure 'Allow log on locally' is set to 'Administrators, Users'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Allow log on locally” > Remove all accounts **EXCEPT** “administrators” and “users” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.7 Ensure 'Back up files and directories' is set to 'Administrators'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Back up files and directories” > Remove all accounts **EXCEPT** “administrators” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.16 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Deny access to this computer from the network” > Remove all accounts **EXCEPT** “Local account” and “Guest” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.17 Ensure 'Deny log on as a batch job' to include 'Guests'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Deny log on as a batch job” > Remove all accounts **EXCEPT** “Guest” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.18 Ensure 'Deny log on as a service' to include 'Guests'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Deny log on as a service” > Remove all accounts **EXCEPT** “Guest” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.20 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Deny log on through Remote Desktop Services” > Remove all accounts **EXCEPT** “Guest” and “Local Account” |
| 2 | Warning: 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. |

|  |  |
| --- | --- |
| **2.2.37 Ensure 'Restore files and directories' is set to 'Administrators'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Restore Files and Directories” > Remove all accounts **EXCEPT** “administrators” |
| 2 | Warning: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs. |

|  |  |
| --- | --- |
| **2.2.38 Ensure 'Shut down the system' is set to 'Administrators, Users'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “User Rights Assignment” > “Shutdown the system” > Remove all accounts **EXCEPT** “administrators” and “users” |
| 2 | Warning:  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. |

|  |  |
| --- | --- |
| **2.3.1.5 Configure 'Accounts: Rename administrator account'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “Security Options” > “Accounts: Rename administrator account” |
| 2 | Set a new administrator account name instead of the default value |
| **2.3.1.6 Configure 'Accounts: Rename guest account'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “Security Options” > “Accounts: Rename guest account” |
| 2 | Set a new guest account name instead of the default value |
| **2.3.7.5 Configure 'Interactive logon: Message text for users attempting to log on'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “Security Options” > “Interactive Logon: Message text for users attempting to log on” |
| 2 | Key in your message for the user when trying to logon. |

|  |  |
| --- | --- |
| **2.3.7.6 Configure 'Interactive logon: Message title for users attempting to log on'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “Security Options” > “Interactive Logon: Message title for users attempting to log on” |
| 2 | Key in your title of the message for the user when trying to logon. |

|  |  |
| --- | --- |
| **2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'** | |
| 1 | Open Local Security Policy > Proceed to “Local Policies” > “Security Options” > “Network Security: Force logoff when logon hours expire” |
| 2 | Change the setting to **“Enabled”**  **Warning: To affect domain account setting must be push through GPO** |
| **17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure'** | |
| 1 | Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Account Logon” > Select “Audit Credential Validation” |
| 2 | Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |
| **17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure'** | |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Account Management” > Select “Audit Application Group Management” | |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” | |
| **17.2.3 Ensure 'Audit User Account Management' is set to 'Success and Failure'** | |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Account Management” > Select “Audit User Account Management” | |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” | |
| **17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success'** | |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Detailed Tracking” > Select “Audit PNP Activity” | |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” | |

|  |
| --- |
| **17.3.2 Ensure 'Audit Process Creation' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Detailed Tracking” > Select “Audit Process Creation” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Account Lockout” |
| Change the setting > Tick Configure the following audit events: > Tick “Failure” |

|  |
| --- |
| **17.2.2 Ensure 'Audit Security Group Management' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Account Management” > Select “Audit Security Group Management” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |
| **17.5.3 Ensure 'Audit Logoff' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Logoff” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” |

|  |
| --- |
| **17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Logon” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” and “Failure” |

|  |
| --- |
| **17.5.6 Ensure 'Audit Special Logon' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Special Logon” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” and “Failure” |

|  |
| --- |
| **17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Policy Change” > Select “Audit Audit Policy Change” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” |

|  |
| --- |
| **17.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Policy Change” > Select “Audit Authentication Policy Change” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” |

|  |
| --- |
| **17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “System” > Select “Audit Other System Events” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” and “Failure” |

|  |
| --- |
| **17.9.3 Ensure 'Audit Security State Change' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “System” > Select “Audit Security State Change” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” |

|  |
| --- |
| **17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “System” > Select “Audit System Integrity” |
| Change the setting > Tick Configure the following audit events: > Tick “Success” and “Failure” |

|  |
| --- |
| **17.5.2 Ensure 'Audit Group Membership' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Group Membership” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Logon/Logoff” > Select “Audit Other Logon/Logoff Events” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Object Access” > Select “Audit Detailed File Share” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Object Access” > Select “Audit File Share” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Object Access” > Select “Audit Other Object Access Events” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Object Access” > Select “Audit Removable Storage” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Policy Change” > Select “Audit Authorization Policy Change” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Policy Change” > Select “Audit MPSSVC Rule-Level Policy Change” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Policy Change” > Select “Audit Other Policy Change Events” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “Privilege Use” > Select “Audit Sensitive Privilege Use” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “System” > Select “Audit IPsec Driver” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success'** |
| Open Local Security Policy > Proceed to “Advanced Audit Policy Configurations” > “System Audit Policies – Local Group Policy Object” > “System” > Select “Audit Security System Extension” |
| Change the setting > Tick Configure the following audit events: > Tick both “Success” and “Failure” |

|  |
| --- |
| **18.9.77.3.1 Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'** |
| Open “Local Group Policy Editor”, “Computer Configuration” > “Administrative Templates” > “Windows Components” > “Microsoft Defender Antivirus” > “MAPS” > Select “Configure local setting override for reporting to Microsoft MAPS” |
| Change the setting to **“DISABLED”** and apply the setting |

|  |
| --- |
| **2.3.10.10 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow’** |
| Open “Local Security Policy” > “Local Policies” > “Security Options” > “Network Access: Restrict clients allowed to make remote calls to SAM’ |
| Select “Edit Security” > Only Administrator group is allowed remote access |

|  |
| --- |
| **9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'** |
| Open “Local Security Policy” > “Windows Defender Firewall With Advanced Security > Expand fully and right click “Windows Defender Firewall with Advanced Security – Local Group Policy Object” > Select properties |
| Change Firewall State to “On” for Domain Profile tab |

|  |
| --- |
| **9.1.5 Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'** |
| Open “Local Security Policy” > “Windows Defender Firewall With Advanced Security > Expand fully and right click “Windows Defender Firewall with Advanced Security – Local Group Policy Object” > Select properties |
| Under Domain tab > Select Customize under Logging section > Change the Name field to “%systemroot%\system32\logfiles\firewall\domainfw.log” |

|  |
| --- |
| **9.2.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'** |
| Open “Local Security Policy” > “Windows Defender Firewall With Advanced Security > Expand fully and right click “Windows Defender Firewall with Advanced Security – Local Group Policy Object” > Select properties |
| Under Private tab > Select Customize under Logging section > Change the Name field to “%systemroot%\system32\logfiles\firewall\privatefw.log” |

|  |
| --- |
| **9.3.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'** |
| Open “Local Security Policy” > “Windows Defender Firewall With Advanced Security > Expand fully and right click “Windows Defender Firewall with Advanced Security – Local Group Policy Object” > Select properties |
| Under Public Profile tab > Select Customize under Logging section > Change the Name field to “%systemroot%\system32\logfiles\firewall\publicfw.log” |