iSSC – Default Intune Policy Settings Breakdown

The below is a non-exhaustive list of the Intune policies applies by default as part of Security Hardening Measures for endpoints.

Items not included on this list are considered to be of no consequence to end users, and affect things like allowed NTLM encryption types, or policies which complement the settings listed below, but do not form a policy directive in their own right.

1. Configuration Profiles
   1. iSSC – Account Protection Policy
      1. Scope: All Devices
      2. Enable Credential Guard with UEFI Lock
   2. iSSC – Application Control Policy
      1. Scope: All Devices
      2. User built-in controls
         1. Audit Only Mode
         2. Trust Apps with good reputation, and apps from managed installers
   3. iSSC – ASR Exclusions
      1. Scope: All Devices
      2. Allow WhatsApp Windows Store App
   4. iSSC – Bitlocker Policy
      1. Scope: All Devices
      2. Encrypt System Drive
      3. Encrypt All Fixed Drives
      4. Do Not Encrypt removable drives
      5. Store Bitlocker recovery info in Azure AD
      6. Use 48-character recovery passwords only
      7. Require TPM
      8. Used-Space only encryption
      9. Use XTS-AES 128-bit encryption
      10. Automatically configure without user interaction
   5. iSSC – Block Store Policy
      1. Scope: All Devices
      2. Block Software installation from Windows Store
   6. iSSC – Configure OneDrive Folder Redirection
      1. Scope: All Users
      2. Automatically backup Desktop, Pictures and Documents folders to OneDrive
      3. Automatically sign into OneDrive as the current signed-in user
   7. iSSC – Defender for Endpoint Security Baseline
      1. Scope: All Devices
      2. Enable SmartScreen
         1. Warn users and prevent SmartScreen Bypass
      3. Enable Archive Scanning
      4. Enable Behavior Monitoring
      5. Enable Cloud Protection
      6. Enable Email Scanning
      7. Enable Removable Drive Scanning
      8. Enable Access Protection
      9. Enable Realtime Monitoring
      10. Enable Network File Scans
      11. Enable Downloaded File Scanes
      12. Allow UI Access
      13. Block obfuscated scripts
      14. Block Office applications from creating child processes
      15. Block Win32 API Calls from Office Macros
      16. Block Executable files from running unless they meet trusted, prevalence or age criteria
      17. Block JavaScript or VBScript from launching downloaded executable content
      18. Block untrusted and unsigned processes that run from USB
      19. Block Adobe Reader from creating child processes
      20. Block Credential Stealing
      21. Block Webshell creation for servers
      22. Block abuse of vulnerable drivers
      23. Audit persistence through WMI
      24. Block use of copied or impersonated system tools
      25. Block Office applications from injecting code into other processes
      26. Use advanced protection against ransomware
      27. Audit process creation originating from PSExec and WMI commands
      28. Block Office Apps from creating executable content
      29. Audit reboots in Safe Mode
      30. Block Executable content from email and webmail
      31. Prevent users from overriding Defender rules
      32. Enable Network Protection in Block Mode
      33. Enable PUA protection
      34. Run quick scans on schedule at 2am
      35. Update definitions every 4 hours
      36. Automatically submit samples
      37. Credential Guard Enabled
          1. Also in Account Protection Policy
      38. DMA Guard – Block All
      39. Firewall Settings
          1. Disable Stateful FTP
          2. Enable Stealth Mode
          3. Overlap with Firewall Policies
   8. iSSC – Exploit Protection Policy
      1. Scope: All Devices
      2. Disallow Exploit Protection Override (local users cannot make changes in the exploit protection settings area)
   9. iSSC – M365 Apps Security Baseline
      1. Scope: All Devices
      2. Block Flash activation in Office Documents
      3. Restrict Legacy JScript execution
      4. Block Macros from Running
      5. Disable Trust Bar Notifications for Unsigned app add-ins and block them
      6. Require that app add-ins are signed by a trusted publisher
      7. Disallow trusted locations on the network
      8. Legacy File Types: Open / Save options blocked
         1. Exception to Excel 97 – 2003 Workbooks, these are allowed in protected view
      9. Disable UI Extending from documents and Templates
      10. Various related complimentary settings
   10. iSSC – Microsoft Edge Security Baseline
       1. Scope: All Devices
       2. Disallow unconfigured sites from being reloaded in IE Mode
       3. Disallow users from proceeding from HTTPS warning pahe
       4. Enable Site isolation for every site
       5. Disallow automatic opening of MHT and MHTML files from the web in IE mode
       6. Prevent the following extensions from being installed:
          1. McAfee WebAdvisor
       7. Enable Smart Screen
       8. Block potentially unwanted apps
       9. Prevent bypassing Defender SmartScreen Prompts
       10. Enable Website Typo protection
       11. Various minor complimentary settings
   11. iSSC – Outlook Automatic Configuration
       1. Scope: All Users
       2. Automatically Configure First Outlook profile based on Primary SMTP Address
   12. iSSC – Screen Lock Policy
       1. Scope: All Devices
       2. Require Password
          1. Lock Device after 30 Minutes
   13. iSSC – Windows 10 / 11 Security Baseline
       1. Scope: All Devices
       2. Disable Lock Screen Camera
       3. Disable Lock Screen Slideshow
       4. Apply UAC to local accounts
       5. Disable SMB v1
       6. Turn off Multicast DNS resolution
       7. Harden UNC Paths
       8. Prohibit connection to non-domain networks when connected to a domain-authenticated network
       9. Printers
          1. Enable Printer Redirection guard
          2. Require Authentication for outgoing RCP connections
          3. Enable RCP Listener
             1. Only allow RPC over TCP
             2. Negotiate Authentication
          4. Only allow admins to install print drivers
       10. Turn off toast notifications on lock screen
       11. Disallow custom SSPs and APs to be loaded into LSASS
       12. Power Management
           1. Disallow standby states when sleeping
           2. Require password when computer wakes up
       13. Disable built-in remote assistance feature
       14. Disable autorun
       15. Disable enumeration of admin accounts on UAC prompt / elevation
       16. Enable Smart Screen
           1. Overlap with Defender Policy
       17. Various Internet Explorer settings
           1. Deprecated, but still forms part of the Microsoft-published baseline
       18. Defender
           1. Enable Process Scanning
           2. Enable routine remediation
       19. Remote Desktop
           1. Prevent local drive redirection
           2. Do not allow passwords to be saved
           3. Always prompt for password upon connection
           4. Set encryption level: High
       20. Prevent automatic sign in on restart
       21. Turn on PowerShell script block logging
       22. WinRM
           1. Disable basic authentication
           2. Disable unencrypted traffic
           3. Disallow digest authentication
           4. Prevent WinRM from storing RunAs credentials
       23. Browser
           1. Block Password Manager
           2. Prevent Certificate overrides
       24. Prevent direct memory access
       25. Defender
           1. Settings mirrored in Defender policy
       26. Device Guard
           1. Enable Secure Launch, if supported
           2. Enable Virtualization based security
           3. Platform Security: Turn on VBS with Secure Boot
       27. Device Lock
           1. Min Password / PIN Length: 6
           2. Password History: 24
       28. Allow Windows Spotlight
       29. Block Windows Consumer Features
       30. Block 3rd Party suggestions in Spotlight
       31. Firewall
           1. Mirrors settings in Firewall Policy
       32. Disable insecure guest logins
       33. Prevent indexing of encrypted items
       34. Prevent voice activation of apps while screen is locked
       35. Prevent various classes of users from accessing device from network, prevent guest from logging in at all.
       36. Wi-Fi Settings
           1. Disable Internet Sharing
           2. Disallow auto connection to Wi-Fi Sense Hotspots
   14. iSSC – Windows Device Restriction Policy
       1. Scope: All Devices
       2. Block Mobile App Store
       3. Block Cortana
       4. Max minutes of inactivity until screen locks: 30 mins
       5. Windows Spotlight: Block
       6. Defender AV
          1. Overlaps with Defender Policies
   15. iSSC – Windows Firewall Settings
       1. Scope: All Devices
       2. Enable Firewall
       3. Enable Logging of Successful Connections
       4. Enable Logging of Ignored Rules
       5. Enable Logging of Dropped Packets
       6. Disable Local Policy Merge
       7. Default Outbound Action: Allow
       8. Default Inbound Action: Deny
       9. Disable Inbound Notifications
       10. Object Access Audit Logging: Enabled for Success and Failures
   16. iSSC – Windows Health Monitoring
       1. Scope: All Devices
       2. Enable Health Monitoring
          1. Scope: Endpoint Analytics
   17. iSSC – Windows LAPS
       1. Scope: All Devices
       2. User Built-in administrator account
       3. Backup LAPS password to Azure AD
          1. Password Age: 365 Days
       4. Post Authentication Actions: Reset Password and Logoff managed account
          1. With 8-hour Delay
2. Compliance Policies
   1. iSSC – Windows Compliance Policy
      1. Scope: All Devices
      2. Require Bitlocker
      3. Require Secure Boot
      4. Require Code Integrity
      5. Require Device to be at or Below Threat Level: Medium
      6. Require Firewall
      7. Require TPM
      8. Require Antivirus
      9. Require Antispyware
      10. Require Defender Antimalware
      11. Require Defender Antimalware being up to date
      12. Require Real-Time Protection
      13. Mark Device as Non-Compliant after 14 Days
   2. iSSC – Android Compliance Policies
      1. Scope: All Devices
      2. Require Device to be at or Below Risk Score: Medium
      3. Block Rooted Devices
      4. Mark Device as Non-Compliant after 7 Days
   3. iSSC – iOS Compliance Policy
      1. Scope: All Devices
      2. Require Device to be at or Below Threat Level: Medium
      3. Require Device to be at or Below Risk Score: Medium
      4. Block Rooted Devices
      5. Mark Device as Non-Compliant after 7 Days
3. Applications
   1. Microsoft 365 Apps for Business / Enterprise (Current Channel)
      1. Scope: All Devices
   2. Microsoft Company Portal
      1. Scope: All Devices
   3. Microsoft Edge
      1. Scope: All Devices
4. Windows Updates
   1. iSSC – Windows Update Ring Settings
      1. Scope: All Devices
      2. Quality Update Deferral: 7 Days
      3. Feature Update Deferral: 7 Days
      4. Update Deadline: 7 Days from Approval
      5. Auto Reboot: No
      6. Auto Install During Maintenance Windows (6pm to 4am)
   2. iSSC – Windows 10 22h2 Upgrade
      1. Scope: All Devices
      2. Deploy Latest Windows 10 Upgrade to devices not eligible to upgrade to Windows 11
   3. iSSC – Windows 11 24h2 Upgrade
      1. Scope: All Devices
      2. Deploy Latest Windows 11 Upgrade to eligible Windows 10 and 11 devices
5. Windows Defender
   1. iSSC – Defender EDR Deployment Profile
      1. Scope: All Devices
      2. Deploy Defender for Endpoint Automatically