# Autopilot Azure AD Join via Intune

|  |  |  |  |
| --- | --- | --- | --- |
| Step No. | Description | Assigned to | Status |
| Step 1: | Determine a process to import the Device hash from remote devices (both managed by SCCM and Unmanaged) into ACG Autopilot service via Powershell and GraphAPI |  |  |
| Step 2: | Create the “ACGAPAADJ” GroupTag and Assign it to your resources. |  |  |
| Step 3: | Create the Dynamic Membership AAD Group off of the “ACGAPAADJ” GroupTag |  |  |
| Step 4: | Create/Validate the AADJ Autopilot Deployment Profile & Assign it to your target AAD Group |  |  |
| Step 5: | Create/Validate the ESP Profile & Assign it to your target AAD Group |  |  |
| Step 6: | Create/Validate the below Required ACG Default Security Stack Win32 App Objects in Intune and Assign it to your target AAD Group |  |  |
| Step 7: | Create/Validate the Compliance Policy and assign it to your target AAD Group |  |  |
| Step 8: | Create Endpoint Security Baseline off of ACG Default Domain Policy and assign it to your target AAD Group |  |  |
| Step 9: | Create Bitlocker Policy via Endpoint Security and assign it to your target AAD Group |  |  |
| Step 10: | Create these below configuration Profiles and assign it to your target AAD Group:   * OneDrive KFM * Microsoft Edge * Store Unpin from Taskbar * Disable User ESP * ACG Trusted Root Certificate * Etc etc |  |  |
| Step 11: | Test and troubleshoot the APAADJ provisioning policy on both Physical and Virtual Machines |  |  |
| Step 12: | Monitor and maintain the APAADJ process by leveraging Powershell, GraphAPI & Log Analytics workbooks |  |  |
| Step 13: | Send out Comms |  |  |
| Step 14: | Documentation and sign-off |  |  |