# Zero-Touch Pre-Delivery Deployment Checklist

## Step 1: MDM Platform Configuration

### Security & Compliance Policies

- [ ] **Disk Encryption:** Enforce BitLocker (Windows) or FileVault (macOS) with escrowed keys
- [ ] **Passcode Standards:** Define complexity, length, and rotation requirements
- [ ] **OS Update Cadence:** Set mandatory update windows and "N-1" versioning
- [ ] **EDR/Antivirus:** Pre-configure silent install for security stack (e.g., CrowdStrike)
- [ ] **Firewall Settings:** Enable system firewalls and block unauthorized incoming ports

### Application Management

- [ ] **Core App Bundle:** Set "Required" apps (Slack, Zoom, Outlook) for automatic, silent installation
- [ ] **VPP/Store Integration:** Link Apple Volume Purchase Program or Microsoft Store for Business
- [ ] **Self-Service Portal:** Populate an "On-Demand" app store (e.g., Company Portal or Jamf Self Service)
- [ ] **App Configuration:** Pre-populate server URLs or license keys so users don't have to type them
- [ ] **Browser Management:** Force managed profiles, bookmarks, and security extension

### Baseline Configurations

- [ ] **Connectivity:** Pre-load corporate Wi-Fi certificates and Always-On VPN configs
- [ ] **Core Productivity:** Set "Required" apps (Slack, Outlook, Teams) for auto-install
- [ ] **Browser Management:** Force managed profiles and security extensions for Chrome/Edge

---

## Step 2: User Profiles & Identity

- [ ] **IdP Integration:** Link MDM to Identity Provider (Okta, Entra ID, Google)
- [ ] **Dynamic Groups:** Create role-based groups based on department attributes to trigger specific settings and app bundles
- [ ] **Privilege Management:** Define Standard vs Admin user roles for local accounts
- [ ] **SSO Extension:** Configure single sign-on for platform-specific system prompts
- [ ] **Conditional Access:** Block access to SaaS apps if the device is not MDM-enrolled

---

## Step 3: Enrollment Platform Setup

### Apple Business Manager (ABM)

- [ ] **MDM Server Token:** Upload public key to ABM to authorize MDM connection
- [ ] **ADE Profile:** Create automated enrollment profile to skip setup screens
- [ ] **Supervision:** Ensure all devices are flagged as "Supervised" for total control

### Windows Autopilot

- [ ] **Tenant Mapping:** Verify Microsoft Entra ID Tenant is mapped to Intune
- [ ] **Enrollment Status Page (ESP):** Enable visual progress bar for end-user setup
- [ ] **Hardware Hash Sync:** Confirm automatic registration for vendor purchases

### Android Zero-Touch (ZTE)

- [ ] **ZTE Portal Access:** Authorize corporate Google account for the ZTE portal
- [ ] **DPC Extras:** Define JSON configuration data for the Device Policy Controller

### Other Specialized Platforms

- [ ] **API/Token Handshake:** Establish a secure link between the manufacturer’s portal and your MDM
- [ ] **Skip Setup Logic:** Configure flags to bypass manufacturer-specific registration and privacy screens
- [ ] **Default Assignment:** Set a "Default MDM Server" so all new hardware is automatically funneled to your MDM

- [ ] **Hardware ID Mapping:** Establish a method (CSV or Reseller API) to associate unique serials with your account

---

## Step 4: Vendor & OEM Collaboration

- [ ] **Org ID Sharing:** Provide Apple Org ID / Microsoft Tenant ID to the vendor
- [ ] **Vendor Portal:** Gain admin access to the reseller's device enrollment dashboard
- [ ] **Serial Audit:** Establish a workflow for receiving serial/hash CSVs via API or email