**Prep: Re-enable Hyper-V & create VMs**

1. Turn on **Hyper-V**  
   Control Panel → Turn Windows features on/off → ✅ Hyper-V (all) → Reboot.
2. Create a **Virtual Switch**  
   Hyper-V Manager → Virtual Switch Manager → **New External** (or Internal) → name LabSwitch.
3. Create VMs
   * **SCCM/AD Server**: Windows Server 2019/2022, 4 vCPU, 8–12 GB RAM, 150 GB disk, on LabSwitch.
   * **Client-PC**: Windows 10/11, 2 vCPU, 4 GB RAM, 60 GB disk, on LabSwitch.
4. (Optional) Static IPs  
   Example:
   * Server: 172.30.0.1/24, DNS: itself
   * Client: 172.30.0.50/24, DNS: 172.30.0.1

**1) Make the domain (on the Server VM)**

1. Rename server (e.g., WIN-URLAT89QEMJ) & restart.
2. **Add Roles & Features** → **AD DS** + **DNS** → Promote to **New Forest**: training.com.
3. Create OUs in **Active Directory Users & Computers**:
   * ITPEOPLE (for your lab devices & users).
4. Create a user sowmeeka (Password never expires for lab).

**2) Install SCCM prerequisites (on the Server)**

1. Roles/Features: **IIS**, **.NET 4.8**, **BITS**, **RDC**, **WSUS**.
2. Install **Windows ADK** + **WinPE add-on** (same OS generation as clients).
3. Install **SQL Server 2019** (default instance):
   * Collation: SQL\_Latin1\_General\_CP1\_CI\_AS
   * Give SQL service account local admin (lab-only) and set Max Server Memory (e.g., 4096–8192 MB).

**3) Install SCCM (MECM) Primary Site**

1. Run **SetupDL.exe** (optional) then **Splash.hta** → Install.
2. Choose **Primary Site** (standalone).
3. **Site code**: HVD (example) | **Site name**: Hydrate.
4. Install **Management Point (MP)** + **Distribution Point (DP)** on this server.
5. After setup, open **Console**.

**4) Boundaries, Discovery, Client Push**

1. **Administration → Hierarchy Configuration → Boundaries**
   * Add your **IP Subnet** (e.g., 172.30.0.0/24).
   * Add to a **Boundary Group** → associate with your **Site** and **DP**.
2. **Administration → Discovery Methods**
   * Enable **Active Directory System Discovery** (point to domain).
   * Run discovery now.
3. **Administration → Client Installation**
   * **Client Push Installation** → Enable → set an account with local admin on clients (or Domain Admin for lab).

**5) Join the client to the domain**

On **Client-PC**:  
This PC → Rename this PC (Advanced) → **Domain: training.com** → use Domain Admin → Restart.

**6) Make sure the SCCM client installs**

In **Assets & Compliance → Devices**, you should see the Client-PC. If **Client = No**:

**Option A: Push from Console**

* Right-click device → **Install Client** →  
  ✅ Always install client software  
  ✅ Install using site-assigned client settings  
  ✅ Allow installation on domain controller (if prompt)  
  → Site code: HVD → Next → Finish.

**Option B: Manual install (guaranteed)**

1. Share from server: \\172.30.0.1\SMS\_HVD\client (your path may be like \\<Server>\SMS\_<SiteCode>\client).
2. On Client-PC (as admin):
3. net use Z: \\172.30.0.1\SMS\_HVD
4. Z:
5. cd client
6. ccmsetup.exe /mp:WIN-URLAT89QEMJ SMSSITECODE=HVD /logon
   * /mp: = your server name (see **Administration → Site Configuration → Servers**).

**Verify** on client:

* Control Panel → Configuration Manager shows Site HVD.
* Logs: C:\Windows\ccmsetup\ccmsetup.log, C:\Windows\CCM\Logs\ClientIDManagerStartup.log.  
  **Goal**: In console, **Client = Yes**.

**7) Put devices/users in the right OU (matches your sir’s steps)**

* Move **Client-PC** to **ITPEOPLE** OU.
* Move **user sowmeeka** to **ITPEOPLE** OU.  
  *(Helps GPO for the MSIX certificate in a later step.)*

**8) Create a clean device collection for Hyper-V VMs**

**Assets & Compliance → Device Collections** → Create:

* Name: HyperV-Clients → Add **Client-PC** as a direct member.

**9) Prepare the content source share**

On the server create: D:\Sources\Apps\ and share as \\172.30.0.1\Sources (Read for Domain Computers).

Folders:

\\172.30.0.1\Sources\7zip\

7zip\_23.01.msi

7zip\_23.01\_to\_25.01.msp

\\172.30.0.1\Sources\NotepadMSIX\

Notepad.msix

Notepad\_SigningCert.cer (or .pfx if you have private key)

**10) Deploy 7-Zip (MSI + MSP) via SCCM**

**A) Create the Application**

1. **Software Library → Applications → Create Application** → **Manually specify**.
2. Name: 7-Zip 25.01 (MSI+MSP) → Next.

**B) Add Deployment Type (use Script Installer so we can use PATCH property)**

1. **Add** → **Manually specify deployment type**.
2. **Content location**: \\172.30.0.1\Sources\7zip\.
3. **Installation program** (one atomic transaction with PATCH):
4. msiexec /i "7zip\_23.01.msi" PATCH="%~dp0\7zip\_23.01\_to\_25.01.msp" /qn /norestart /l\*v "%WinDir%\Temp\7zip\_install.log"

(Using %~dp0 ensures it finds the MSP in the same folder.)

1. **Uninstall program** (choose one that fits your MSI):
   * If you know the ProductCode:
   * msiexec /x {PRODUCT-CODE-GUID} /qn /norestart
   * Or:
   * "C:\Program Files\7-Zip\Uninstall.exe" /S
2. **Detection Method** (recommended—post-patch version):
   * **Registry**:  
     Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip  
     Value: DisplayVersion  
     Data: 25.01  
     *(If your repack uses another key, open the client after manual install once and confirm exact key/value.)*
3. **User Experience**: Install for **System**, whether or not user is logged on.

**C) Distribute & Deploy**

1. Right-click the app → **Distribute Content** → select your **DP**.
2. After content is **Success**, right-click app → **Deploy** → Collection: HyperV-Clients.
3. **Purpose**: Required (auto), or Available (Software Center).
4. Schedule → Asap → Next → Close.

**Verify on client**

* Software Center → 7-Zip installs.
* Check C:\Windows\Temp\7zip\_install.log (if needed).
* Programs & Features shows **7-Zip 25.01**.
* SCCM logs: C:\Windows\CCM\Logs\AppDiscovery.log, AppEnforce.log.

**11) Prepare MSIX certificate trust (via GPO)**

MSIX needs its **signing certificate** trusted on clients.

**A) Create/Use a GPO to deploy the cert**

1. On the server: **Group Policy Management**.
2. Right-click **ITPEOPLE** OU → **Create a GPO** → MSIX Trusted Cert → **Edit**.
3. Go to:  
   Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies → Trusted People
   * Right-click **Certificates** → **All Tasks → Import** → select Notepad\_SigningCert.cer.
   * Finish.

*(If you have* ***.pfx*** *with private key, import to* ***Trusted Publishers*** *instead. For most sideloaded MSIX,* ***Trusted People*** *with public .cer is fine.)*

**B) (Optional) Enable Appx/MSIX policies**

Same GPO (helps on older builds):

* Computer Configuration → Administrative Templates → Windows Components → App Package Deployment
  + **Allow all trusted apps to install** → Enabled
  + **Allow deployment operations in special profiles** → Enabled
  + **Allow deployment of Windows Store apps** → Enabled

**C) Apply the GPO on clients**

On **Client-PC** (as admin):

gpupdate /force

Reboot once.  
Check cert presence: **certlm.msc** → **Trusted People → Certificates** (should show your publisher).

**12) Deploy Notepad (MSIX) via SCCM**

**A) Create the Application (MSIX type)**

1. **Software Library → Applications → Create Application**.
2. Choose **Windows app package (\*.appx, \*.msix)**.
3. Select \\172.30.0.1\Sources\NotepadMSIX\Notepad.msix.
4. Wizard populates **Name**, **Publisher**, **Package Family Name**.

**B) Deployment Type defaults**

* Installation cmd will be handled by SCCM (uses DISM/Add-AppxPackage).
* **Detection** uses the **Package Family Name** (good).

**C) Distribute & Deploy**

1. **Distribute Content** to your **DP**.
2. **Deploy** to HyperV-Clients (Available or Required).

**Verify on client**

* Software Center → Notepad installs.
* If it fails with certificate errors, re-check Step 11 (cert in Trusted People) and rerun:
  + Logs: **Event Viewer → Microsoft-Windows-AppxDeploymentServer/Operational**
  + SCCM logs: AppEnforce.log, AppDiscovery.log.

**13) (Optional) Assign Primary Users (like your sir’s note)**

**Assets & Compliance → Devices → your device → Edit Primary User** → add TRAINING\administrator or training\sowmeeka.  
*(Only for user-centric deployments; not required for device-required installs.)*

**14) Quick Troubleshooting checklist**

* **Client = No** in console → check ccmsetup.log and **Boundaries**/**Boundary Groups**.
* **Content not found** → confirm **Distribute Content** finished & client can reach \\172.30.0.1\SMSPKGx$ shares.
* **7-Zip not at 25.01** → verify Detection Rule points to final version; use PATCH= install.
* **MSIX fails** → certificate not in **Local Computer → Trusted People**; apply GPO and reboot; check AppxDeploymentServer log.
* **Software Center empty** → client policy refresh may be pending; on client run:
* Machine Policy Retrieval & Evaluation Cycle (from Control Panel → Configuration Manager → Actions)

**Exactly what to run (copy-paste friendly)**

**Client manual install (if push fails):**

net use Z: \\172.30.0.1\SMS\_HVD

Z:

cd client

ccmsetup.exe /mp:WIN-URLAT89QEMJ SMSSITECODE=HVD /logon

**7-Zip MSI+MSP install command (inside SCCM Deployment Type):**

msiexec /i "7zip\_23.01.msi" PATCH="%~dp0\7zip\_23.01\_to\_25.01.msp" /qn /norestart /l\*v "%WinDir%\Temp\7zip\_install.log"

**Force GPO on client:**

gpupdate /force

**Step 1: Create a folder for packages**

1. On your **SCCM Server machine** (or a file server in the same domain), go to C:\ drive.
2. Create a new folder, e.g.
3. C:\SCCM\_Sources
4. Inside it, make subfolders for each app, for example:
5. C:\SCCM\_Sources\7Zip
6. C:\SCCM\_Sources\NotepadMSIX

**🔹 Step 2: Share the folder**

1. Right-click the SCCM\_Sources folder → **Properties**.
2. Go to **Sharing** tab → click **Advanced Sharing…**.
3. Tick **Share this folder**.
4. Give a Share Name (example: SCCM\_Sources).  
   The UNC path will look like:
5. \\YourServerName\SCCM\_Sources

**🔹 Step 3: Set permissions**

1. In **Permissions**, add **Everyone** (for lab) → allow **Read**.  
   👉 (In production, you’d give **Read** rights only to the SCCM server’s computer account and SCCM admins).
2. Click **OK** → **Apply**.

**🔹 Step 4: Copy your installer files**

1. Copy your **MSI + MSP** for 7-Zip into:
2. C:\SCCM\_Sources\7Zip

Example:

* + 7zip.msi
  + 7zip\_update.msp

1. Copy your **MSIX + Certificate** for Notepad into:
2. C:\SCCM\_Sources\NotepadMSIX

Example:

* + Notepad.msix
  + NotepadCert.cer

**🔹 Step 5: Test access from client VM**

1. Log in to your **Hyper-V Client VM** (already joined to domain).
2. Press Win + R → type the share path, e.g.:
3. \\YourServerName\SCCM\_Sources
4. You should see 7Zip and NotepadMSIX folders.  
   If yes → your share is ready ✅.  
   If not → check Firewall and permissions.