

Windows 11 Enterprise PXE Deployment Guide

Standard Operating Procedure: Network Boot, Automated WinPE & Zero-Touch Domain Staging



Automated Zero-Touch Deployment Architecture

This deployment pipeline enables end-to-end bare-metal installation of Windows 11 Pro across CHCFC workstations and laptops. From power-on (F12) to ready-to-use domain join, the system dynamically configures chassis naming, auto-partitions drives, bypasses TPM/CPU limits on legacy hardware, joins Active Directory, and deploys Bitdefender & NinjaOne agents automatically.

1. Physical Machine Boot & BIOS Selection (Press F12)

One-Time Boot Menu Execution: Connect the target workstation to the staging network (LAN 10.77.1.0/24) via Ethernet. Power on the machine and immediately tap **F12** continuously until the One-Time Boot Menu appears.

Boot Mode Matrix & Firmware Constraints:

- Modern Hardware (OptiPlex 7040+, Micro PCs, All Laptops):** Select **UEFI Boot** → **ONBOARD NIC (IPv4)**. Ensure Secure Boot is enabled or disabled as needed; TPM 2.0 bypass is applied automatically if missing.
- Legacy Hardware (Dell OptiPlex 790):** In BIOS (F2) → *Boot Sequence*, ensure *Boot List Option* is set to **Legacy**. Under Legacy Boot, select **Onboard NIC**. (OptiPlex 790 has incomplete UEFI 2.0 and hangs on UEFI PXE).
- SATA Controller Mode:** Ensure SATA operation in BIOS is set to **AHCI**. Windows 11 native inbox storahci.sys recognizes internal drives out of the box with zero third-party storage drivers required.

DHCP & TFTP Handshake: The client DHCP request receives Option 66 (Next Server: 10.77.1.220) and Option 67 (Boot File). Legacy BIOS loads undionly.kpxe; UEFI loads ipxe.efi, which chains directly to http://10.77.1.220:8089/boot.ipxe.

2. iPXE Menu Selection & Pre-Boot Streaming

Interactive Boot Menu: iPXE presents the *Enterprise Network Boot & Installation* menu with a 5-minute fallback to local drive:

- Option 1 (Automated):** Install Windows 11 Pro - Automated Unattended (Domain Join) ← *Recommended default for staging.*
- Option 2 (Manual):** Install Windows 11 Pro - Interactive Setup (via Media Share) ← *For custom disk or edition selection.*

High-Speed HTTP Asset Streaming via wimboot:

When selected, iPXE streams the Windows boot environment over high-speed HTTP (TCP port 8089) instead of slow TFTP. wimboot packages the following core files into system memory in ~15-20 seconds:

```
kernel http://10.77.1.220:8089/wimboot
initrd http://10.77.1.220:8089/win11/bootmgr bootmgr (or bootmgr.efi)
initrd http://10.77.1.220:8089/win11/BCD BCD (Pre-configured BCD store)
initrd http://10.77.1.220:8089/win11/boot.sdi boot.sdi (System deployment image RAM container)
initrd http://10.77.1.220:8089/win11/boot.wim boot.wim (WinPE OS image with injected network drivers)
initrd http://10.77.1.220:8089/win11/autounattend.xml autounattend.xml (Base unattended answer file)
```

Deployment Monitor Live Tracking: NGINX logs every downloaded block. Technicians can view active downloads live at http://10.77.1.220:8087/monitor or by typing pxe-monitor -w in terminal.

3. WinPE RAM Disk Architecture (X:\ vs Y:\) & Automated Startup

Filesystem	Physical Location	Contents & Operational Role
X:\ Drive (WinPE RAM Disk)	Volatile System RAM (Expanded boot.wim)	Minimal Windows Preinstallation OS kernel, core diagnostic utilities (diskpart, drvload, curl, findstr), injected drivers staged in X:\Drivers, and staging scripts. Size: ~900 MB.
Y:\ Drive (Media Network Share)	Local High-Speed Samba \\10.77.1.220\win11	Full Windows 11 installation media (Y:\sources\install.wim, setup.exe, \$OEM\$ scripts). Mounted anonymously (guest). Windows Setup streams the multi-gigabyte OS image directly over Gigabit LAN without consuming local RAM.

Automated Startup Pipeline (winpeshl.ini → startnet.cmd):

- Dynamic Driver Loading:** Ingests all .inf drivers staged in X:\Drivers via drvload (specifically official SHA-256 WHQL driver e1c65x64.inf for Intel 82579LM NICs).
- Network Initialization:** Executes wpeinit and wpeutil initializenetwork; pings 10.77.1.220 until the network link negotiates.
- Hardware Compatibility Bypasses:** Injects registry DWORDs into HKLM\SYSTEM\Setup\LabConfig (BypassTPMCheck, BypassSecureBootCheck, BypassCPUCheck, BypassRAMCheck, BypassStorageCheck).
- Local Share Mount:** Mounts \\10.77.1.220\win11 to drive letter Y: with automatic retries.
- Monitor Telemetry:** Fires beacons to http://10.77.1.220:8087/api/beacon (WinPE_Network_Ready and Media_Share_Mounted).

4. Dynamic Machine Tailoring & Auto-Partitioning (configure.vbs)

Before launching Windows Setup, startnet.cmd executes cscript //nologo X:\Windows\System32\configure.vbs. This script inspects the bare-metal hardware and adapts the installation dynamically:

1. Chassis Detection & Standardized Computer Naming:
Queries Win32_SystemEnclosure.ChassisTypes and Win32_BIOS.SerialNumber to generate the official NetBIOS hostname:

- **Laptops / Portables (Chassis Types 8, 9, 10, 14, 30, 31, 32):** Assigned CHC-LP-<SERVICE TAG> (e.g. CHC-LP-7K2X9Q1).
- **Desktops / Workstations (Chassis Types 3, 4, 6, 7, etc.):** Assigned CHC-PC-<SERVICE TAG> (e.g. CHC-PC-4M8P2W1).
- Enforces the strict 15-character Windows NetBIOS naming limitation.

2. Firmware Detection & Automated Zero-Touch Diskpart:
Inspects HKLM\System\CurrentControlSet\Control\PEFirmwareType to dynamically create X:\diskpart.txt and execute diskpart /s X:\diskpart.txt to clean Disk 0:

- **UEFI Mode (PEFirmwareType = 2):** clean → convert gpt → create efi 100MB FAT32 (System) → create msr 16MB → create primary NTFS (Windows, letter=W)
- **Legacy BIOS Mode (PEFirmwareType = 1):** clean → convert mbr → create primary 100MB NTFS Active (System) → create primary NTFS (Windows, letter=W)

3. Dynamic Answer File Generation: Injects the calculated ComputerName into X:\autounattend.xml and exports COMP_NAME, MODEL, MAC, and FIRMWARE to X:\env.cmd.

5. Unattended Configuration Engine: autounattend.xml Settings

Configuration Pass	XML Component	Settings Applied & Automation Details
1. windowsPE (Pre-Install)	Microsoft-Windows-Setup International-Core-WinPE	<ul style="list-style-type: none">• Sets InputLocale, SystemLocale, and UILanguage to en-US (0409).• Bypasses Setup UI prompts: WillShowUI = Never.• Automatically accepts Microsoft EULA: AcceptEula = true.• Installs Windows 11 Pro from Y:\sources\install.wim.• Targets formatted storage: InstallToAvailablePartition = true.• Applies default Pro product key: VK7JG-NPHTM-C97JM-9MPGT-3V66T.
2. specialize (Hardware Config)	Microsoft-Windows-Shell-Setup UnattendedJoin	<ul style="list-style-type: none">• Sets ComputerName dynamically from configure.vbs (CHC-PC-* / CHC-LP-*).• Sets TimeZone to Eastern Standard Time.• Sets Organization to CHCFC and RegisteredOwner to CHCFC IT.• Automated Active Directory Domain Join:<ul style="list-style-type: none">- Domain: inside.chcfc.org- Target OU: OU=Staging,DC=inside,DC=chcfc,DC=org- Service Account: svc-domainjoin (Delegated machine join).
3. oobeSystem (First User Boot)	Microsoft-Windows-Shell-Setup (OOBE & Accounts)	<ul style="list-style-type: none">• Completely Hides All Out-of-Box Experience (OOBE) Screens: HideEULAPage, HideLocalAccountScreen, HideOEMRegistrationScreen, HideOnlineAccountScreens, HideWirelessSetupInOOBE, ProtectYourPC=1.• Sets NetworkLocation to Work.• Local Administrator Account Provisioning:<ul style="list-style-type: none">- Sets Built-in Administrator password to standard enterprise IT secret.- Provisions local IT admin account: chcfcadmin in Administrators group.

6. First-Boot Software Pipeline (SetupComplete.cmd) & Quick Reference

Post-Install Automation (C:\Windows\Setup\Scripts\SetupComplete.cmd):
Upon initial Windows 11 boot, Windows executes SetupComplete.cmd under NT AUTHORITY\SYSTEM before user login:

1. Mounts software distribution repository \\g22.inside.chcfc.org\SoftwareDeploy.
2. Deploys **Bitdefender Endpoint Security** silently (/bdparams /silent).
3. Deploys **NinjaOne Greenfield 1 RMM Agent** silently (msiexec /i ninja-gf1-auto.msi /qn /norestart).
4. Posts completion beacon to Deployment Monitor (marking node **100% Completed**) and notifies Zulip **#SoftwareInstall**.
5. Disconnects software deploy share and unregisters temporary deployment staging files.

PXE Service / URL	Address / Location	Credentials / Access Role
Deployment Monitor Web	http://10.77.1.220:8087/monitor	Auto-refreshing dashboard; CLI: pxe-monitor -w
Win11 Samba Image Share	\\10.77.1.220\win11	Anonymous / Guest access, No password
Software Deployment Share	\\g22.inside.chcfc.org\SoftwareDeploy	Active Directory Domain Authenticated
Local Admin Fallback	User: chcfcadmin	Standard Enterprise IT Secret (IT password vault)