CHECKLIST

# Windows 11 Hardening Checklist for Secure Enterprise Deployment

A practical, verifiable Windows 11 hardening checklist for secure enterprise deployment. Use it to validate baseline settings, controls, evidence, owners, and production readiness before rollout.

**Operating Systems - July 04, 2026**

## Purpose

Windows 11 deployment can fail operationally when security settings are assumed rather than verified: device encryption is inconsistent, local admin rights remain broad, attack surface reduction is incomplete, update controls are unclear, or logging is not available when an incident occurs. This checklist is designed to help technical teams harden Windows 11 in a repeatable way before production rollout.

Use this checklist to decide whether your Windows 11 baseline is ready for enterprise deployment, what evidence to capture, and what must be fixed before broad release. It is written for system engineers, DevOps engineers, and security professionals who need verifiable controls rather than general advice.

## How to use this checklist

Run the checklist by operational phase, not as a one-time audit. For each item, confirm the control, capture the evidence, and assign an owner who can fix gaps. Mark items as pass only when the acceptance criteria are demonstrably met on representative devices and, where relevant, in the management plane.

If a setting depends on edition, tenant policy, hardware capability, or licensing, verify that dependency first. For example, BitLocker behavior, virtualization-based security, or endpoint protection integrations may vary by device class and management model. If you need a reference workflow for safe, repeatable firewall validation, the same operational discipline used in How to Configure UFW Firewall Rules on Ubuntu Server applies here: define required access, test enforcement, then review exceptions before production use.

## 1) Scope and baseline definition

The purpose of this phase is to ensure the security baseline is explicit before any configuration is applied. A hardening effort that lacks a defined baseline usually produces drift, conflicting policies, and unowned exceptions.

## Checklist items

- ? Confirm the Windows 11 editions, device classes, and management methods in scope.
- ? Review which devices are corporate-owned, BYOD, kiosk, shared, or privileged admin workstations.
- ? Document the minimum supported hardware security features required for the baseline.
- ? Assign ownership for baseline policy, deployment, exception handling, and rollback.
- ? Validate which settings are controlled by local policy, domain policy, MDM, or security tooling.
- ? Define the configuration standard for new builds, in-place upgrades, and existing managed devices.
- ? Confirm whether pilot, production, and privileged endpoints require different profiles.

## Evidence to capture

- Approved baseline document or policy matrix.
- Device scope inventory with model, edition, and management channel.

- Ownership map with named approvers.
- Exception register and rollback contacts.

## Acceptance criteria

- Scope is documented and approved.
- Every hardening control has a named owner.
- The baseline can be applied consistently across the defined device groups.
- Exceptions are tracked and time-bound.

## Owner

Platform engineering or endpoint management lead, with security sign-off.

## Review cadence

Review before pilot deployment and again after any major policy or image change.

## Common mistakes

- Treating all Windows 11 devices as identical.
- Mixing pilot and production requirements.
- Applying settings without defining who can approve exceptions.

## 2) Identity, authentication, and local privilege control

The purpose of this phase is to reduce account takeover impact and limit what an attacker can do if a user context is compromised. Identity protection is only effective when privileged access is tightly controlled and local elevation paths are explicit.

## Checklist items

- ? Confirm that standard users do not have unnecessary local administrator rights.
- ? Review how privileged access is granted, time-limited, and revoked.
- ? Validate that separate admin accounts are used for administrative tasks.
- ? Document whether passwordless or MFA requirements apply to managed sign-in flows.
- ? Test that credential prompts do not silently bypass hardened authentication policies.
- ? Confirm that local administrator password management is in place where applicable.
- ? Validate that account lockout, sign-in restrictions, and recovery procedures are defined.
- ? Review the use of Microsoft Defender for Endpoint or equivalent controls for privileged identity telemetry if deployed; verify edition and licensing dependencies before relying on them.

## Evidence to capture

- Group membership exports showing local admin membership.
- Privileged access policy and approval workflow.
- MFA or passwordless enforcement records.
- Local admin password management reports, if used.

## Acceptance criteria

- Privileged access is limited, auditable, and revocable.
- Standard users cannot self-elevate through routine workflows.

- Recovery procedures are documented and tested.

## Owner

Identity engineering or security operations.

## Review cadence

Monthly, and immediately after user-role changes or service desk exceptions.

## Common mistakes

- Leaving vendor support accounts in local administrators.
- Using shared admin credentials for convenience.
- Assuming MFA is enforced without confirming the exact policy path.

## 3) Device security, boot integrity, and hardware-backed protections

The purpose of this phase is to ensure the device can trust its own boot and storage state before higher-layer controls are considered. Hardware-backed protection materially improves resilience against offline tampering and credential theft, but only when it is actually enabled and monitored.

## Checklist items

- ? Confirm Secure Boot is enabled on all supported devices.
- ? Validate that TPM 2.0 is present, active, and functioning.

- ? Test that BitLocker or equivalent full-disk encryption is enabled on system volumes.
- ? Review how recovery keys are escrowed, accessed, and audited.
- ? Confirm that virtualization-based security is enabled where supported by hardware and policy.
- ? Validate that memory integrity or equivalent protections are enabled on pilot systems where application compatibility allows.
- ? Review firmware settings for BIOS/UEFI password protection and removable boot control.
- ? Confirm that firmware updates are managed and monitored through an approved process.

## Evidence to capture

- Device compliance report with Secure Boot, TPM, and encryption status.
- BitLocker recovery key escrow record.
- Firmware and BIOS configuration baseline.
- Pilot compatibility exceptions for VBS-related protections.

## Acceptance criteria

- Hardware-backed protection requirements are met on in-scope devices.
- Recovery keys are escrowed in the approved system.
- Exceptions are documented for unsupported hardware only.

## Owner

Endpoint engineering with security architecture review.

## Review cadence

Per device model during pilot, then quarterly for the production fleet.

## Common mistakes

- Assuming TPM presence means the feature is operational.
- Enabling encryption without validating recovery-key escrow.
- Turning on memory integrity without testing application compatibility.

## 4) Attack surface reduction and application control

The purpose of this phase is to block common execution paths used by malware, living-off-the-land abuse, and unauthorized software installation. Hardening is strongest when policy is explicit, tested, and supported by exception handling for business-critical applications.

## Checklist items

- ? Confirm that application execution rules are defined for approved software paths.
- ? Review whether script execution, macro use, and unsigned code are restricted where feasible.
- ? Validate attack surface reduction rules on a pilot ring before broader rollout.
- ? Test that application allowlists or blocklists do not break required line-of-business software.
- ? Document exception handling for installers, scripts, and troubleshooting tools.
- ? Confirm that browser download and attachment handling policies align with the security baseline.
- ? Review whether removable media execution is blocked or constrained according to policy.
- ? Validate that NET Checklist: Operational Readiness Review for Production Use style evidence collection is used for software exceptions: owner, rationale, risk, and expiry.

## Evidence to capture

- Application control policy exports.
- Pilot failure logs for blocked applications.
- Approved exception list with expiry dates.
- Security event logs showing policy enforcement.

## Acceptance criteria

- Unapproved execution paths are blocked or tightly constrained.
- Approved business applications continue to function.
- Exceptions are documented, time-bound, and reviewed.

## Owner

Endpoint security engineering.

## Review cadence

Weekly during pilot; monthly after production release.

## Common mistakes

- Deploying block rules without application inventory.
- Allowing broad script exceptions to unblock one tool.
- Failing to set expiry dates on temporary exceptions.

## 5) Network exposure, firewalling, and remote access

The purpose of this phase is to minimize unnecessary inbound exposure while preserving required administrative and user connectivity. Windows 11 should not rely on implicit trust from the local network segment.

## Checklist items

- ? Confirm that the Windows Defender Firewall profile is enabled for domain, private, and public networks.
- ? Review inbound rule exceptions and remove legacy or unused allowances.
- ? Validate that required management ports are restricted to trusted sources.
- ? Test that remote desktop or remote assistance access is explicitly approved and logged.
- ? Document whether VPN, ZTNA, or network access control is required for internal-only services.
- ? Confirm that SMB, WinRM, WMI, and other administrative channels are constrained to approved admin paths.
- ? Validate that local firewall policy is not silently overridden by conflicting rules.
- ? Review network discovery and file sharing settings for shared or sensitive endpoints.

## Evidence to capture

- Firewall policy export and effective-rule report.
- Approved remote access matrix.
- Connectivity test results from allowed and blocked sources.
- Administrative channel restriction documentation.

## Acceptance criteria

- Firewall profiles are enabled and enforced.
- Only required inbound access is allowed.
- Remote administration paths are documented and limited.

## Owner

Network security or endpoint management.

## Review cadence

Per policy change and after any new remote access requirement.

## Common mistakes

- Leaving broad inbound rules from legacy imaging.
- Allowing administrative protocols from all internal subnets.
- Forgetting to validate firewall behavior after policy merge.

## 6) Update, patch, and rollback readiness

The purpose of this phase is to keep devices current without making updates an uncontrolled production risk. Secure deployment depends on predictable update rings, clear deferral rules, and a proven rollback path for problematic patches.

## Checklist items

- ? Confirm that quality updates, feature updates, and driver updates follow an approved cadence.

- ? Review update rings or deployment groups for pilot, broad, and high-risk devices.
- ? Validate pause, deferral, and deadline settings against operational requirements.
- ? Test that reboot behavior is acceptable for user productivity and admin endpoints.
- ? Document rollback options for failed updates or broken drivers.
- ? Confirm that update compliance reporting is available to operations and security.
- ? Validate that out-of-band update handling is defined for critical fixes.
- ? Review whether third-party patching is governed separately from operating system updates.

## Evidence to capture

- Update policy configuration and ring definitions.
- Compliance dashboard snapshots.
- Pilot update outcome reports.
- Rollback procedure with support contacts.

## Acceptance criteria

- Update timing is predictable and auditable.
- Pilot devices validate changes before production devices receive them.
- Rollback steps are documented and feasible.

## Owner

Endpoint operations.

## Review cadence

Weekly during update cycles; monthly for policy review.

## Common mistakes

- Pushing feature updates to all devices at once.
- Mixing driver remediation with OS patching without a test ring.
- Having no documented recovery path when an update breaks a critical app.

## 7) Logging, monitoring, and incident response readiness

The purpose of this phase is to make sure security events can be detected, investigated, and correlated before an incident occurs. If logs are incomplete or not retained, a hardened endpoint may still be operationally blind.

## Checklist items

- ? Confirm that security auditing is enabled for logon, privilege use, policy changes, and process creation where required.
- ? Review event forwarding or endpoint telemetry routing to the central monitoring platform.
- ? Validate that endpoint alerts are actionable and mapped to an owner.
- ? Test that clock synchronization is working so event timelines are reliable.
- ? Document log retention periods and storage capacity assumptions.
- ? Confirm that incident responders can isolate, collect, and preserve evidence from a device.
- ? Validate that tamper protection or equivalent safeguards are enabled where available.
- ? Review whether removable media, suspicious PowerShell activity, and privilege escalation events are visible to monitoring.

## Evidence to capture

- Audit policy export.
- Sample forwarded events or telemetry records.
- Incident response runbook for Windows 11 endpoints.
- Retention and capacity calculations.

## Acceptance criteria

- Required events are generated and centralized.
- Incident responders can act on endpoint telemetry.
- Log retention supports investigation and compliance needs.

## Owner

Security operations and incident response.

## Review cadence

Monthly, and after any SIEM or telemetry change.

## Common mistakes

- Enabling audit settings without confirming event collection.
- Keeping logs too briefly to support investigations.
- Ignoring time drift, which can make correlation unreliable.

# 8) Data protection, privacy, and removable media control

The purpose of this phase is to limit data loss from endpoint compromise, lost devices, and accidental transfer to untrusted storage. Data controls are only meaningful when classification, encryption, and media rules are aligned.

## Checklist items

- ? Confirm that sensitive data categories are defined for endpoint handling.
- ? Review whether removable storage is blocked, read-only, or allowlisted by policy.
- ? Validate that copy, paste, sync, and cloud upload controls match data handling requirements.
- ? Test that encryption is enforced for local data stores and external media where required.
- ? Document whether DLP or equivalent controls are operating on managed devices.
- ? Confirm that screenshots, print, or shared clipboard restrictions are applied where mandated.
- ? Review privacy-impacting telemetry settings to ensure they align with organizational policy and legal requirements.
- ? Validate that browser and sync client behavior do not bypass approved data controls.

## Evidence to capture

- Data classification and handling policy.
- Removable media control policy.
- Encryption compliance report for endpoints and external media.
- DLP or data control test results.

## Acceptance criteria

- Data handling rules are implemented consistently.
- High-risk transfer paths are restricted or monitored.
- Exceptions are approved and audited.

## Owner

Security governance with endpoint engineering support.

## Review cadence

Quarterly, or after any data policy change.

## Common mistakes

- Applying data controls only to file shares and not endpoint storage.
- Allowing unrestricted USB use for convenience.
- Forgetting that browser sync can move data outside the intended boundary.

## 9) Readiness scoring and pass/fail decision rule

The purpose of this phase is to turn the checklist into a deployment decision rather than a documentation exercise. Use a simple maturity score to compare device groups and make release decisions consistently.

## Scoring method

- Assign 2 points for each item that is fully implemented and evidenced.
- Assign 1 point for each item that is partially implemented but has an approved, time-bound exception.
- Assign 0 points for each item that is missing, unverified, or outside policy.

Score each operational phase separately, then total the result.

## Decision rule

- Deploy: all critical items in phases 2 through 7 score 2, and no phase has unresolved 0-point items.
- Pilot only: there are documented exceptions, but every exception has an owner, risk acceptance, and expiry date.
- Hold: any critical control is missing, unverified, or cannot be monitored.

## Maturity bands

- 0-40%: high risk; baseline not ready.
- 41-70%: partial readiness; limited pilot only.
- 71-90%: deployable with exceptions under active control.
- 91-100%: strong readiness; maintain monitoring and drift control.

## Pass/fail criteria

Pass only when evidence exists for each critical item, the control owner has signed off, and the device group can be monitored after deployment. Fail when a control depends on assumptions, a manual process without auditability, or a setting that cannot be validated on representative devices.

## 10) Common deployment mistakes to avoid

The purpose of this phase is to prevent avoidable hardening failures that typically show up after rollout, not during the pilot.

## Checklist items

- ? Review whether any policy relies on default settings instead of explicit enforcement.
- ? Confirm that pilot results were validated on multiple hardware models, not just one build.
- ? Document whether security exceptions have expiration dates and owners.
- ? Validate that rollback steps were tested before production approval.
- ? Review whether monitoring, logging, and help desk procedures were updated with the new baseline.
- ? Confirm that user-impacting controls were communicated to support teams before rollout.
- ? Test that devices rejoin management and compliance reporting after reset or reimage events.

## Evidence to capture

- Pilot summary and defect log.
- Exception register with expiry dates.
- Rollback test evidence.
- Support readiness notes.

## Acceptance criteria

- Known pitfalls have explicit mitigations.
- Operations, support, and security share the same rollout criteria.
- The deployment process is repeatable on new devices.

## Owner

Program lead or endpoint release manager.

## Review cadence

Before each production wave and after any major incident.

## Final deployment verdict

A Windows 11 hardening program is production-ready only when the baseline is explicit, identity and privilege are constrained, device protections are verified, network exposure is reduced, updates are controlled, logging is centralised, and exceptions are operationally owned. If any of those areas depend on assumptions, the rollout is not yet ready for secure enterprise use.

Use this checklist as a gate, not a guidepost: capture evidence, score each phase, close the gaps, and only then approve wider deployment. That discipline is what keeps hardening from becoming a paper exercise.

Use this guidance together with algorithms implementation roadmap to connect the workflow with related operational context already available on the site.