CHECKLIST

Windows 10 Local Security Policy Hardening Checklist

A practical checklist for evaluating, applying, and validating Windows 10 Local Security Policy changes before production use.

Windows 10 Local Security Policy Hardening Checklist

Use this checklist to harden a Windows 10 endpoint with Local Security Policy while minimizing operational risk. It is designed for standalone, lab, recovery, kiosk, or otherwise locally managed systems. If the device is domain joined, confirm whether domain policy or a hardened baseline is the authoritative control before making changes locally.

---

1) Confirm the host context

- [ ] Identify the device role: standalone, domain-joined, lab, kiosk, recovery, or special-purpose.
- [ ] Confirm whether the system is managed by local policy only or by a central policy source.
- [ ] Document any business-critical functions that could be affected by security changes.
- [ ] Identify local accounts, service accounts, scheduled tasks, remote support tools, and admin workflows in use.
- [ ] Confirm whether the host requires offline access, temporary isolation, or emergency recovery capabilities.

2) Define the security goal

- [ ] State the risk you want to reduce: weak passwords, account abuse, limited logging, unauthorized access, or privilege misuse.
- [ ] Choose the smallest set of settings that address that risk.
- [ ] Avoid enabling settings just because they are available.
- [ ] Note any controls that should remain unchanged for compatibility reasons.
- [ ] Record the expected security outcome in plain language.

3) Review account policy settings

- [ ] Verify password complexity requirements.
- [ ] Verify minimum password length.
- [ ] Review password age and history settings.
- [ ] Review account lockout threshold, duration, and reset counter values.
- [ ] Confirm whether local account policies are actually authoritative on this host.
- [ ] Check whether the settings could affect local admin access, automation, or recovery workflows.
- [ ] If the system is domain-joined, confirm the domain policy source before changing local account policy.

4) Review audit policy settings

- [ ] Enable logging that supports later investigation and validation.
- [ ] Confirm visibility for logon and logoff activity.
- [ ] Confirm visibility for account management activity.
- [ ] Confirm visibility for privilege use or sensitive administrative actions.
- [ ] Confirm visibility for policy changes.
- [ ] Verify that auditing produces useful events without overwhelming the log.
- [ ] Ensure someone is responsible for reviewing the resulting logs.

5) Review user rights assignment

- [ ] Identify who can log on locally.
- [ ] Identify who can log on through Remote Desktop, if applicable.
- [ ] Identify who can access the system over the network.
- [ ] Identify who can shut down the system.
- [ ] Identify who can back up files and directories.
- [ ] Identify who can load and unload device drivers, if applicable.
- [ ] Identify service accounts and scheduled task identities that require elevated rights.
- [ ] Remove broad or unnecessary rights where safe to do so.
- [ ] Preserve documented administrative access paths.

6) Review security options

- [ ] Review anonymous access restrictions.
- [ ] Review guest account handling.
- [ ] Review local administrator and built-in account behavior.
- [ ] Review UAC-related settings that affect elevation and admin prompts.
- [ ] Review SMB and legacy protocol-related options where relevant.
- [ ] Review settings that influence cached credentials, sign-in behavior, or interactive logon.
- [ ] Avoid changes that could break required authentication, remote administration, or file access.
- [ ] Prefer settings that reduce exposure without changing core workflow behavior.

7) Stage the change safely

- [ ] Apply changes to a test machine or non-production copy first.
- [ ] Change one control group at a time.
- [ ] Document the exact setting names and values before modifying them.
- [ ] Keep a rollback plan for every change.
- [ ] Set a maintenance window if reboot, logoff, or service interruption may be required.
- [ ] Save screenshots or exported policy evidence where appropriate.

8) Validate the applied settings

- [ ] Confirm the setting appears in the expected local policy location.
- [ ] Confirm the effective behavior matches the intended control.
- [ ] Refresh policy or reboot if required by the setting.
- [ ] Verify authentication still works for approved users and admins.
- [ ] Verify remote administration still works if the host depends on it.
- [ ] Verify required services still start successfully.
- [ ] Verify file access, share access, and application startup still behave normally.
- [ ] Verify audit events are being generated as expected.

9) Test for side effects

- [ ] Test local logon.
- [ ] Test administrative logon.
- [ ] Test remote access, if used.
- [ ] Test service startup and scheduled tasks.
- [ ] Test access to required files, shares, or devices.
- [ ] Test any recovery or support process that may rely on the previous behavior.
- [ ] Confirm no unexpected lockouts or access denials occurred.
- [ ] Confirm no critical application regression was introduced.

10) Confirm logging and investigation readiness

- [ ] Check that relevant security events are present in the event log.
- [ ] Confirm log retention is sufficient for operational review.
- [ ] Confirm logs are accessible to the team responsible for monitoring.
- [ ] Correlate security policy changes with event log evidence when possible.
- [ ] If applicable, review firewall audit evidence alongside security logs.
- [ ] Keep a record of what changed, when it changed, and who approved it.

11) Document and approve

- [ ] Record the host name, role, and environment.
- [ ] Record the exact policy settings changed.
- [ ] Record the reason for each change.
- [ ] Record the validation steps performed.
- [ ] Record any known limitations or exceptions.
- [ ] Obtain approval before moving the change to production.
- [ ] Update baseline or support documentation if the change is now standard.

12) Rollback readiness

- [ ] Save the previous policy values before making changes.
- [ ] Confirm how to restore prior settings.
- [ ] Identify who can perform the rollback if needed.
- [ ] Verify the rollback process on a test system if the change is high risk.
- [ ] Keep rollback notes with the change record.

Quick decision check

Use this final check before production use:

- [ ] The device role is clearly understood.
- [ ] The authoritative policy source is known.
- [ ] Only necessary settings were changed.
- [ ] Authentication and admin access were tested.
- [ ] Logging was verified.
- [ ] Side effects were reviewed.
- [ ] Rollback steps are documented.
- [ ] The change is approved for the environment.

Operational reminder

Local Security Policy is most useful when it reduces risk on a specific endpoint without conflicting with how that host is actually used. Treat it as a targeted hardening tool, not a replacement for centralized policy management.

If the device is part of a managed environment, confirm whether a hardened baseline or domain policy should control the setting instead of the local host.