

[illegible]

***akijgroup.co***

# Windows Server Hardening Checklist

---

## Introduction

Windows servers are a core part of any organization's IT infrastructure, and they often store and process critical business information. Securing these servers is crucial to prevent unauthorized access, data breaches, and downtime. Windows Server hardening involves configuring the server to reduce its attack surface and implementing best security practices to protect it from various cyber threats.

This document outlines a comprehensive checklist for hardening Windows servers, covering initial configurations, network security, user management, and more. It is designed to guide system administrators and security teams in implementing a robust security posture for their Windows Server environment.

## Table of Contents














1. Initial Configuration
2. Network Security
3. User Management
4. Audit and Monitoring
5. Patch Management
6. Secure Server Configuration
7. Advanced Security Configurations
8. Malware Protection
9. Backup and Recovery
10. Secure Application Configuration
11. Regular Security Audits

# Windows Server Hardening Checklist













---

## Checklist

### 1. Initial Configuration

-  **Install Latest Updates & Patches:**
  -  Ensure that Windows Server has all critical security updates and patches.
  -  Enable automatic updates for ongoing maintenance.
-  **Rename Default Administrator Account:**
  -  Rename the default "Administrator" account to a unique name.
-  **Set Strong Password Policies:**
  -  Implement complex passwords (minimum 12 characters).
  -  Enforce account lockout after 5 failed login attempts.
-  **Disable Unused Accounts:**
  -  Remove or disable guest and other unused accounts.
-  **Configure Local Security Policies:**
  -  Set account policies (e.g., password length, lockout duration).
  -  Configure audit policies to log security events.









### 2. Network Security

-  **Enable Windows Firewall:**
  -  Block all unnecessary inbound and outbound traffic.
  -  Implement rules based on specific application and service requirements.
-  **Disable Unnecessary Services & Protocols:**
  -  Disable legacy protocols (e.g., SMBv1, Telnet, FTP).
-  **Restrict Remote Access:**
  -  Disable RDP unless required, or limit access using firewalls or VPN.
  -  Enforce strong authentication for remote access (e.g., MFA).
-  **Implement IPsec for Encryption:**
  -  Use IPsec policies to encrypt sensitive network traffic.
-  **Restrict PowerShell Remoting:**
  -  Limit PowerShell remoting to trusted networks only.









# Windows Server Hardening Checklist

---







## 3. User Management

-  **Limit Administrative Privileges:**
  -  Ensure users only have permissions necessary for their roles.
-  **Implement Role-Based Access Control (RBAC):**
  -  Assign permissions based on roles to prevent privilege escalation.
-  **Separate Administrative & Standard Accounts:**
  -  Admins should have separate accounts for day-to-day operations.
-  **Regularly Review User Access:**
  -  Audit and remove stale or inactive user accounts.

## 4. Audit and Monitoring

-  **Enable Advanced Auditing:**
  -  Configure detailed logging for user activities, access attempts, and changes to critical files.
-  **Centralize Log Management:**
  -  Use a centralized logging solution like SIEM for log collection and analysis.
-  **Monitor Critical Changes:**
  -  Implement File Integrity Monitoring (FIM) for detecting unauthorized changes.
-  **Set Up Alerts for Suspicious Activity:**
  -  Configure alerts for failed login attempts, privilege escalations, and access to sensitive files.










## 5. Patch Management

-  **Deploy Windows Server Update Services (WSUS):**
  -  Use WSUS for centralized management of updates.
-  **Establish Patch Testing Procedures:**
  -  Test patches in a staging environment before deploying them to production servers.
-  **Automate Patch Deployment:**
  -  Schedule regular patching and maintenance windows to avoid disruptions.









# Windows Server Hardening Checklist

---








## 6. Secure Server Configuration

-  **Configure User Account Control (UAC):**
  -  Enable UAC to enforce approval for administrative changes.
-  **Enable BitLocker Disk Encryption:**
  -  Use BitLocker to encrypt sensitive data on the server.
-  **Disable Unnecessary Shares:**
  -  Remove or restrict network shares to prevent unauthorized access.
-  **Harden DNS Configuration:**
  -  Disable DNS recursion unless necessary.
  -  Enable DNSSEC to prevent spoofing and cache poisoning.

## 7. Advanced Security Configurations

-  **Apply Security Baselines:**
  -  Use CIS or Microsoft security baselines for hardening.
-  **Implement Least Privilege for Services:**
  -  Run services using least privilege accounts instead of SYSTEM.
-  **Disable Unused Network Protocols:**
  -  Turn off NetBIOS, LLMNR, and WPAD if not required.
-  **Enforce Group Policy Hardening:**
  -  Use GPOs to enforce security policies across the environment.

## 8. Malware Protection





-   **Install Reputable Anti-Malware Software:**
  - Deploy Windows Defender or third-party anti-malware solutions.
-  **Enable Exploit Guard Features:**
  -  Enable Attack Surface Reduction and Controlled Folder Access in Windows Defender.
-  **Schedule Regular Malware Scans:**
  -  Perform daily or weekly scans to detect potential threats.
-  **Use Application Whitelisting:**

# Windows Server Hardening Checklist





---

- ☒ Implement AppLocker or Windows Defender Application Control to restrict unauthorized applications.





## 9. Backup and Recovery

-  **Implement Automated Backups:**
  - ☒ Schedule regular backups of critical system and data files.
-  **Test Backup Restorations:**
  - ☒ Periodically test restoration procedures to verify the integrity of backups.
-  **Use Encryption for Backup Data:**
  - ☒ Ensure backup data is encrypted both in transit and at rest.
-  **Isolate Backups from Main Network:**
  - ☒ Use separate network segments for backup storage to prevent ransomware attacks.

## 10. Secure Application Configuration

-  **Remove Unnecessary Applications:**
  - ☒ Uninstall or disable unused applications and services.
-  **Harden Web Applications:**
  - ☒ Use a Web Application Firewall (WAF) to protect web-facing applications.
-  **Enforce Secure Coding Practices:**
  - ☒ Follow secure coding standards for custom-developed applications.
-  **Use Application Sandboxing:**
  - ☒ Run untrusted applications in a secure, isolated environment.

## 1. Regular Security Audits

-  **Perform Regular Vulnerability Scans:**
  - ☒ Use tools like Nessus or Qualys to identify and mitigate vulnerabilities.
-  **Conduct Penetration Testing:**
  - ☒ Periodically perform penetration tests to assess the effectiveness of security measures.
-  **Review Server Configurations:**
  - ☒ Regularly review server settings for compliance with security baselines.
-  **Document and Remediate Findings:**
  - ☒ Maintain documentation of all audit findings and apply necessary fixes.

# Windows Server Hardening Checklist

---

## Conclusion

This Windows Server Hardening Checklist provides a structured approach to securing Windows Servers, ensuring compliance with best practices and minimizing the risk of cyberattacks. Implementing these measures can significantly strengthen your server's security posture, helping safeguard sensitive data and critical systems. Regular reviews and updates of security configurations are recommended to keep the environment secure against evolving threats.