# Windows Security Review: Workstation & Server configuration guide

**Description**: Hands-on lab that covers Windows server & workstation configuration best practices, registry configurations, useful group policies, and an event log overview.

### Learning Objectives:

* Windows server & workstation configuration best practices.
* Group Policy and registry overview.
* Event logging configuration and overview.

## CIS Hardened Images

<https://www.cisecurity.org/cis-hardened-image-list>

## Windows Workstations

***Secure Boot and TPMs***

To start, we want to focus on TPMs and secure Boot. Both of these are required by windows 11, and as we may know W10 is reaching the end of support on October 14, 2025.

**Secure Boot – What is it?**

Secure boot is a feature to help secure the windows boot process.

**Why do I need it?**

* Secure boot is the counter measure against:
  + *Firmware root kits: These kits overwrite the firmware of the PC's basic input/output system or other hardware so the rootkit can start before Windows.*
  + *Bootkits: These kits replace the OS's bootloader (the small piece of software that starts the OS) so that the PC loads the bootkit before the OS.*
  + *Kernel Rootkits: These kits replace a portion of the OS kernel so the rootkit can start automatically when the OS loads.*
  + *Driver Rootkits: These kits pretend to be one of the trusted drivers that Windows uses to communicate with the PC hardware.*

***Checking the status***

* *One way to check the compatibility of secureboot is to go to run > type msinfo32 and make sure BIOS is set to UEFI and Secure Boot state is ON.*

**How to configure it?**

**Through the registry**

* *Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\State*
* *Locate and double-click the DWORD UEFISecureBootEnabled > we want to set this value to “1”. Once set, restart the machine.*

***Through PowerShell (Run as administrator)***

* *Set-SecureBootUEFI –Enable*

***Can also do this through BIOS, and advanced startup.***

**TPMs – What are they?**

Trusted Platform Module is a specialized chip designed to securely store cryptographic keys used for encryption and decryption. Some of the Windows features that leverage the TPM are:

***Windows Hello –*** Uses the TPM to store biometric data and pins

***BitLocker –*** Uses the TPM to encrypt your hard drive by storing encryption keys.

**Why do I need it or what's the use case?**

* Microsoft recommends that you deploy phishing-resistant password-less authentication across your organization.
* BitLocker is also heavily utilized in most organizations.
* Required with windows 11.
* We want to use TPM version 2.0, and any machine shipped in the past 5 years likely has it.

***Checking the status***

* To see TPM status, Update and Security > Windows Security > Device Security. If it’s present, you’ll see a “Security Processor section”.
* check TPM.MSC (Deprecated)
* or the PowerShell command Get-TPM.

***Core Isolation – Memory Integrity***

[Device Security in the Windows Security App - Microsoft Support](https://support.microsoft.com/en-us/windows/device-security-in-the-windows-security-app-afa11526-de57-b1c5-599f-3a4c6a61c5e2)

***What does it do?***

Protects against attacks that try to exploit vulnerabilities in system memory, specifically guarding the kernel and core processes. It works by ensuring certain drivers and system processes load if they’ve passed a strict integrity check.

This setting might cause issues with hardware or drivers that are not fully compatible. Check for updates after enabling or disable it for troubleshooting.

***Patching and EOL***

* ***Vulnerabilities from 2018 were being exploited in 2023!***
  + CVE-2018-13379 (FortiGate SSL-VPN Path Traversal Vulnerability)
  + Exploit: This is a path traversal vulnerability in the FortiOS SSL VPN web portal that could potentially allow an unauthenticated attacker to download files through specially crafted HTTP resource requests.
  + Evidence: Exploit attempts were observed in the wild, particularly targeting unpatched FortiGate devices, leading to data breaches and ransomware attacks.
* ***Automatic patching***
  + Can be achieved through SCCM, WSUS, or RMM tools. Patch Tuesday is the second Tuesday of every month, but you likely want to wait to push out updates unless there is a critical vulnerability.
  + Good Idea to review patch notes, review patch status, have the ability to rollback and generally good practice to roll out patches in waves.
* ***Extended Security Updates*** 
  + Some may be eligible for extended security updates if licensing for the EOL product was purchased with Microsoft's volume licensing. The ESU program is a paid subscription, and is cumulative, meaning if you purchase the program in year 2, you’ll have to pay for year one as well. Security updates can occur for a maximum of 3 years.
  + Keep this in mind if you’re upgrading a lot of endpoints so your windows 10 machines can still receive necessary security updates.

***Privacy Settings***

* In short, some applications might be over permissioned, check Privacy settings in the “Settings” and review what may or may not be needed.

***Windows Defender SmartScreen***

[Microsoft Defender SmartScreen overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/)

* Windows Defender SmartScreen is native to windows and protects against phishing, malicious websites and downloading potentially malicious files.
* Analyzes web pages you visit and makes a determination if the page is suspicious. If it thinks the page is malicious, it will bring up a warning message to be cautious.
* You can usually expand the details and visit the site anyway as some may have seen.
* Also checks against a list of reported malicious software or phishing sites, and if it finds a match that same warning prompt will be listed.
* This extends to downloads as well, checking against a list of known malicious files.
* We’ve seen SmartScreen flag custom builds of ThreatLocker used for in-house troubleshooting.

***Biometric Authentication***

For Biometric Authentication, we really want to look into windows hello in this case.

***What is Windows Hello For business?***

[Windows Hello for Business overview | Microsoft Learn](https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/)

Windows Hello for Business is just an authentication technology that lets users sign into windows devices using biometric data, a pin as opposed to a password.

* It provides phishing resistant two-factor authentication for devices, and as mentioned Microsoft recommends that you deploy phishing-resistant password-less authentication across your organization.
* Specifically for the Biometric portion, it has facial recognition which utilizes your camera, Fingerprint recognition and Iris recognition.
* This Biometric data is stored locally, so there's no central data location where an attacker can steal this biometric data.
* GPO can be found at computer configuration > administrative Templates > Windows components > Windows Hello for Business

# Windows Server Security

**Roles and Features**

* Control Correlation Identifier (CCI) 000381 & WN19-00-000270 (STIG) Security Technical Implementation Guides
* Mentions to “The organization configures the information system to provide only mission essential capabilities”.
  + Map to NIST; 800-53 version 4 families specifically. Nist mappings are generally pretty broad so this one would fall under that.
  + Example: Telnet client is likely not needed on servers. Yes, there are ways to test ports that don't use an unencrypted protocol.
    - Use SSH, Personally I would avoid installing additional programs, but you can use NMAP as well from a secure workstation.
  + If we need to uninstall (or install) a role or a feature, we can use the server manager. We’ll leave this window open to bring us to our next point.

***Web Browsers on privileged machines***

[Securing Domain Controllers Against Attack | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack)

For this specific case, we’ll look at domain controllers. According to Microsoft, an analysis of thousands of domain controllers revealed numerous cases where users would use Internet explorer to browse the internet.

In their words, browsing the internet or an infected intranet from one of the most powerful computers in a windows infrastructure presents an extraordinary risk to an organization's security.

* We’re doing this because it’s susceptible to drive by downloads or installation of infected utilities.
* Another way to protect this is with firewall restrictions; you can block outbound connections from domain controllers to the internet and be more granular with communications used by your domain controller if it is communicating offsite.
* One thing to note though is organizations with regulatory requirements to keep an on-premises implementation of Active Directory, Microsoft recommends entirely restricting internet access to and from domain controllers.
  + Considering that we would in most cases want to block or restrict internet access, there’s a huge use case to limit ports used by your windows infrastructure and we’ll get to that in just a moment.

***PowerShell Execution Policies***

***What are they?***

Execution policies are a security feature that controls the conditions under which PowerShell loads configuration files and runs scripts. Ultimately to help prevent the execution of malicious scripts.

* Consider AllSigned
  + Scripts and config files must be signed by a trusted publisher, including scripts written on the local computer.
* or RemoteSigned execution policies.
  + Default execution policy for windows servers requires a signature from a trusted publisher on scripts and config files downloaded from the internet.
* Set to restricted if there's no need for it.
  + To set PowerShell execution policies, the command is: Set-ExecutionPolicy Restricted
    - Scope can be outlined for CurrentUser LocalMachine so on.

***Ports & Services***

***Why do we want to do this?***

Cis control 13, safeguard 13.4 suggests performing traffic filtering between network segments where appropriate.

* There are some mappings pertaining specifically to ports
  + Mapping of this would be from the Cybersecurity maturity model Certification, suggesting denying all, permitting by exception when it comes to network communication.
* In a way we’re following POLP or Principle of least privilege by using ports only necessary for the machine's role.
* An example of this is Active Directory only using a select number of ports.
  + 389 & 636 - LDAP and LDAPS
  + 88 - Kerberos
  + 53 - DNS
  + 445 – SMB
  + 135 - MS RPC
  + 123 – NTP
  + 464 - Kerberos Change/Set Password
  + 3268 & 3269 - Global Catalog (LDAP)

***Ways to limit ports***

* This can be achieved through firewall policies, by limiting inbound and outbound traffic in your network segments depending on the need.
* ThreatLocker Network control can also meet this need as well. With this you can implement a Zero-Trust approach to port limitations as it has the ability to ensure only secured and authorized ThreatLocker devices interact with network resources.

***Some small reasons why we take this approach***

* SonicWall's 2021 Cyber Threat Report mentions there was a 9% increase in port scanning since the previous year.
* Commonly exploited ports include SMB, RDP, Telnet, FTP, ETC

***Network infrastructure Roles***

***DHCP***

* Consider using DHCP on your firewall or other networking equipment.
  + In a scenario where responsibilities are split, you wouldn’t want network administrators to have excess roles to your server to manage DHCP when it can be done with layer 3 switches or a firewall.
  + Separating out your roles
  + Run DHCP Best Practice Analyzer Tool. If DHCP role is installed:
    - Open server manager > DHCP tab > Under tasks, Start BPA Scan. Once complete it will list any basic misconfigurations.

***DNSSEC***

[Overview of DNSSEC - Azure Public DNS | Microsoft Learn](https://learn.microsoft.com/en-us/azure/dns/dnssec)

***What is it?***

DNSSEC adds cryptographic signatures to existing DNS records, which are stored in name servers. These signatures are then checked which verifies that the requested DNS record comes from its authoritative name server and wasn’t altered in transit.

* Adding this mitigates spoofing and cache poisoning attacks.
* Required for some compliance, SC-20: Secure Name/Address Resolution service namely.
* If you want to send your Network Admins for a spin, ask them to implement DNSSEC.

***Microsegmentation***

[Secure networks with Zero Trust | Microsoft Learn](https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks)

Microsegmentation is a Zero Trust strategy for network segmentation, calling for networks to be segmented into smaller networks to contain specific workloads. Microsegmentation focuses on east-west traffic, mitigating lateral movement through your network in the event of unauthorized access.

* Can achieve something akin to Microsegmentation with ThreatLocker Network control as well.

***Guest, Anonymous, and Everyone Access***

* Local Security policies can restrict everyone and anonymous access.
  + Permissions are Overly broad.
  + Some group policies pertain to Everyone, Guest and Anonymous access.

***Secure Admin workstation***

[Implementing Secure Administrative Hosts | Microsoft Learn](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts)

* The concept of Secure admin workstations is that they are servers or workstations used specifically performing administrative tasks on privileged accounts from. Using one of these, you want to keep in mind a “productivity system” and an “administrative workstation system”.

***Directory Security***

Some things you can do are utilize an auditing tool, ManageEngine has one SolarWinds permissions analyzer and so on.

* Enable Auditing for user account changes, we’ll go into some of the audit policies you can implement a bit later.
* View Effective permissions in the advanced security window.
  + Step 1 – Locate the document, user, object, for which you want to view the permissions.
  + Step 2 – Right-click the object and click “Properties” in the context menu.
  + Step 3 – Switch to “Security” tab and click “Advanced”.
  + Step 4 – In the “Permissions” tab, you can see the permissions held
  + Step 5. Click “Effective Access”
  + Step 6. Click “select a user”, choose group if desired, select a device if desired, click “view effective access”

CISA recommends deleting/disabling accounts after 45 days of inactivity.

# THE OBVIOUS

**Physical Security**

* Lock your computer when walking away. Dynamic lock can lock your computer when pairing is broken from a BT device.
* Secure servers with badge access.

***Password/Passphrase Policies***

* [Free Password Generator | Create Strong Passwords and Passphrases | Bitwarden](https://bitwarden.com/password-generator/)
* G2aB3QgxDSobqv VS Chewy-Snooze-Preset

***MFA***

* Implement and enforce MFA, MS authenticator and DUO can be tied to domain account logins.
* Additionally, to touch on it again it’s recommended that you roll out phish-resistant MFA methods across your organization ASAP!

# Group Policy & Windows Registry

***Registry Hardening Techniques***

One of the hardening techniques we can do is to control registry access, and we’ll achieve that using Group Policy.

* ***Prevent Registry editing tools***
  + Does exactly as the name suggests, the policy will prevent or disable the use of Regedit.exe
  + User Configuration > Administrative Templates > System > Root folder of system
  + Pair this with “Run only Specified windows applications” to outline which windows applications your users can run.
* ***Run only specified Windows Applications*** 
  + User configuration > Administrative Templates > System > Root Folder of system.
* ***Enable registry auditing policies***
  + This policy is to audit each time an account accesses a registry object. As a result, an audit event is generated.
  + To get there, we’ll go to Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object access then “Audit Registry”
  + Some of the events it will produce are:
    - Event ID 4663 will indicate the specific registry key that was accessed, the type of access (e.g., read or write), and the user who performed the action.
    - 4670: Permissions for an object were changed (e.g., registry key permissions).

# Group Policies

***Best Practices***

* + Do not modify the default domain or domain controller policy.
    - Default domain policies are linked to the root of the domain and will apply to all users and computers within the domain. Stick with simple account policies, account lockout policies and things of that nature.
    - Domain controller policies should have their own separate GPO, and limit what is applied to this GPO as well.
  + Simplify administration and be mindful of startup and logon times.
    - Some settings that can cause slow startup times are startup scripts or login scripts downloading large files
    - Can also split up GPOs into smaller policies, so it makes management a bit easier.
  + Disable unused computer and user configurations
    - An example of this would be to disable a user configuration portion of a GPO if I have a computer config GPO labeled browser settings for example.
  + Backup your GPOs!
    - Browse to the GPO you want to backup, there should be a backup or a backup all option.
      * Can also be done via PowerShell.

***Useful Group Policies***

* Prevent Access to registry editing tools
  + Gone over already
* Interactive logon: Require Windows Hello for Business or smart card
  + Mentioned so it enforces phishing resistant MFA, great if you have a full windows environment.
* Disable LLMNR
  + LLMNR is vulnerable and is prone to man-in-the-middle attacks and spoofing. Disabling it ultimately reduces your attack surface.
  + May need ADMX file templates for these.
  + Computer Configuration\Administrative Templates\Network\DNS Client\Multicast Name Resolution
* Disable NTLM
  + Namely NTLMv1, which is also susceptible to man-in-the-middle attacks and relay attacks.
  + Before disabling it, you may want to verify in event viewer on domain controllers if there are connection attempts with NTLMv1.
  + This is under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: LAN Manager authentication level. We want it to be set to Send NTLMv2 response only. Refuse LM & NTLM
* Remove Anonymous Users from Everyone Permissions
  + Computer Configuration\Windows Settings\Security Settings\Security options\Network Access: Let everyone permissions apply to anonymous users
    - This should be disabled by default
    - Having it enabled poses a risk of non-authenticated users accessing shared network resources.
* Monitor Changes to GPO settings
  + Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies then at the root of Audit policies you’ll see DS Access, then select Audit Directory Service Changes
* Block Microsoft Store
  + Might be necessary if you want one method to block progressive web app installations (PWAs)
  + Can be found at Computer Configuration\Administrative Templates\Windows Components\Turn off the Store Application
* Prohibit access to the control panel
  + User Configuration\Administrative Templates\Control Panel\Prohibit access to Control Panel and PC settings.
* Enable Audit Logging
  + This brings us to the event viewer and last section of our Windows Security Review Lab

# Event Logging

***Basic Audit Policies***

* Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy.
* Basic Audit Policies are broader, less granular settings, and typically cover major event categories like logons, account management, and system events.

***Event ID 4624 (Successful Logon): Basic Audit Policy***

* This event is generated by the "Logon/Logoff" category in basic audit policies, which tracks user logon and logoff events.
* Event ID 4625 (Failed Logon): Basic Audit Policy
* This event is also part of the "Logon/Logoff" category and is logged for failed login attempts.

***Event ID 4720 (A User Account Was Created): Basic Audit Policy***

* This event is part of "Account Management," which tracks changes like user account creation.

***Event ID 4740 (A User Account Was Locked Out): Basic Audit Policy***

* This event falls under "Account Logon" events and is tracked when an account lockout occurs due to failed login attempts.

***Advanced Audit Policies:***

* Advanced Audit Policies offer more granular control over specific events, allowing detailed logging and reporting for particular user actions and system changes.
* Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.

***Event ID 4648 (Logon Attempt Using Explicit Credentials): Advanced Audit Policy***

* This event is part of the "Logon/Logoff" category in advanced auditing. It tracks when a user attempts to log on using explicit credentials (e.g., run as or other credential elevation).

***Event ID 4670 (Permissions on an Object Were Changed): Advanced Audit Policy***

* This event falls under "Object Access," which is an advanced audit policy category. It tracks changes to the permissions on files or objects (e.g., files, directories, registry keys).

***Event ID 4672 (Special Privileges Assigned to New Logon): Advanced Audit Policy***

* This event is part of "Logon/Logoff" under advanced auditing. It tracks when a user logs on with special privileges, such as administrative privileges.

***Event ID 4688 (A New Process Has Been Created): Advanced Audit Policy***

* This event falls under "Detailed Tracking" in advanced audit policies, which logs the creation of new processes on the system.

***Event ID 4719 (System Audit Policy Change): Advanced Audit Policy***

* This event is part of "Policy Change" in advanced audit policies. It tracks changes to the system audit policy settings themselves.