# Tactical Guide:
## Turning on Auditpol for Log Monitoring

---

## 1 CardinalByte Expert Insight

Logging is like a security camera for your computer's operating system. By default, Windows doesn't record enough detail to help in a forensic investigation. Using `auditpol` ensures that events like account lockouts, privilege changes, and file access are documented.

## 2 Why It Is Required

The FTC Safeguards Rule requires "monitoring and logging the activity of authorized users and detecting unauthorized access." Without verbose logging, you cannot prove what a hacker did (or didn't) touch.

## 3 Regulatory Body

**FTC** and **NIST SP 800-171**.

## 4 How to Implement

Use the Command Prompt (Admin) to configure the Audit Policy (Auditpol) to track "Success" and "Failure" for critical categories.

## 5 Step by Step Instructions

1. **Admin Command:** Open CMD as Administrator.
2. **Logon Events:** Type `auditpol /set /subcategory:"Logon" /success:enable /failure:enable`.
3. **Account Mgmt:** Type `auditpol /set /subcategory:"User Account Management" /success:enable`.
4. **Policy Change:** Type `auditpol /set /subcategory:"Authentication Policy Change" /success:enab`
5. **Verify:** Type `auditpol /get /category:*` to see the active settings.

## 6 Tactical and Operational Checklist

- ☐ Auditpol settings deployed to all office computers.
- ☐ Event Log size increased (at least 1GB) to prevent overwriting.
- ☐ Weekly review of ”Failure” logon logs for brute-force patterns.

## 7 Expert Tip

*Check for ”Event ID 4625” (An account failed to log on). A high frequency of these is a sure sign of an automated attack.*