Advanced Audit Policy Configuration

Goal: Configure advanced audit policies on a workstation GPO to monitor critical system events, logons, account management, privilege use, policy changes, and system integrity.

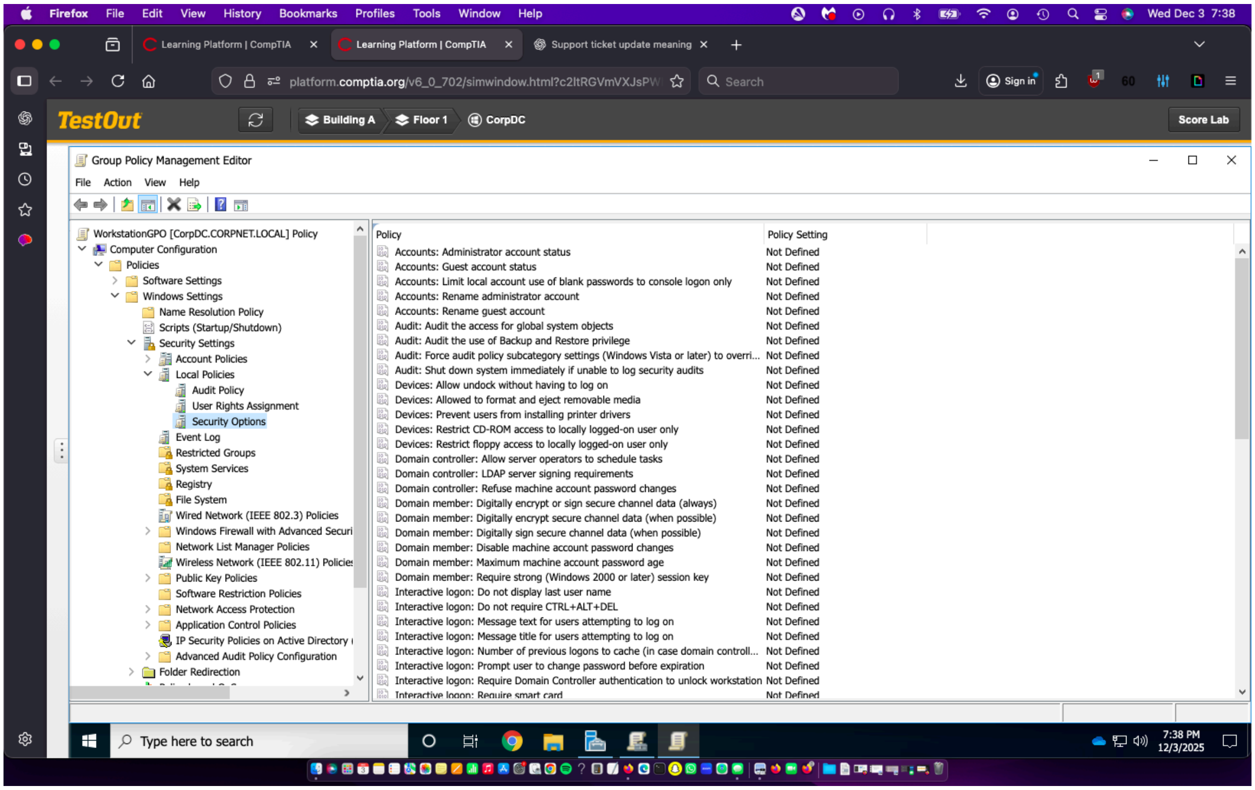
What This Lab Demonstrates

Shows the ability to implement granular auditing in a Windows environment, ensuring that security events are captured for monitoring, compliance, and forensic investigation.

Configuration Summary

1. Accessing Group Policy Management

Connected to **CorpNet.local** in the Group Policy Management Console and opened the **WorkstationGPO** for editing.


Firefox File Edit View History Bookmarks Profiles Tools Window Help
Wed Dec 3 7:38
Learning Platform | CompTIA
Learning Platform | CompTIA
Support ticket update meaning
platform.comptia.org/v6_0_702/simwindow.html?c2ltRGVmVXJsPW
Search
Sign in
TestOut
Building A
Floor 1
CorpDC
Score Lab
Group Policy Management Editor
File Action View Help
Type here to search
7:38 PM
12/3/2025

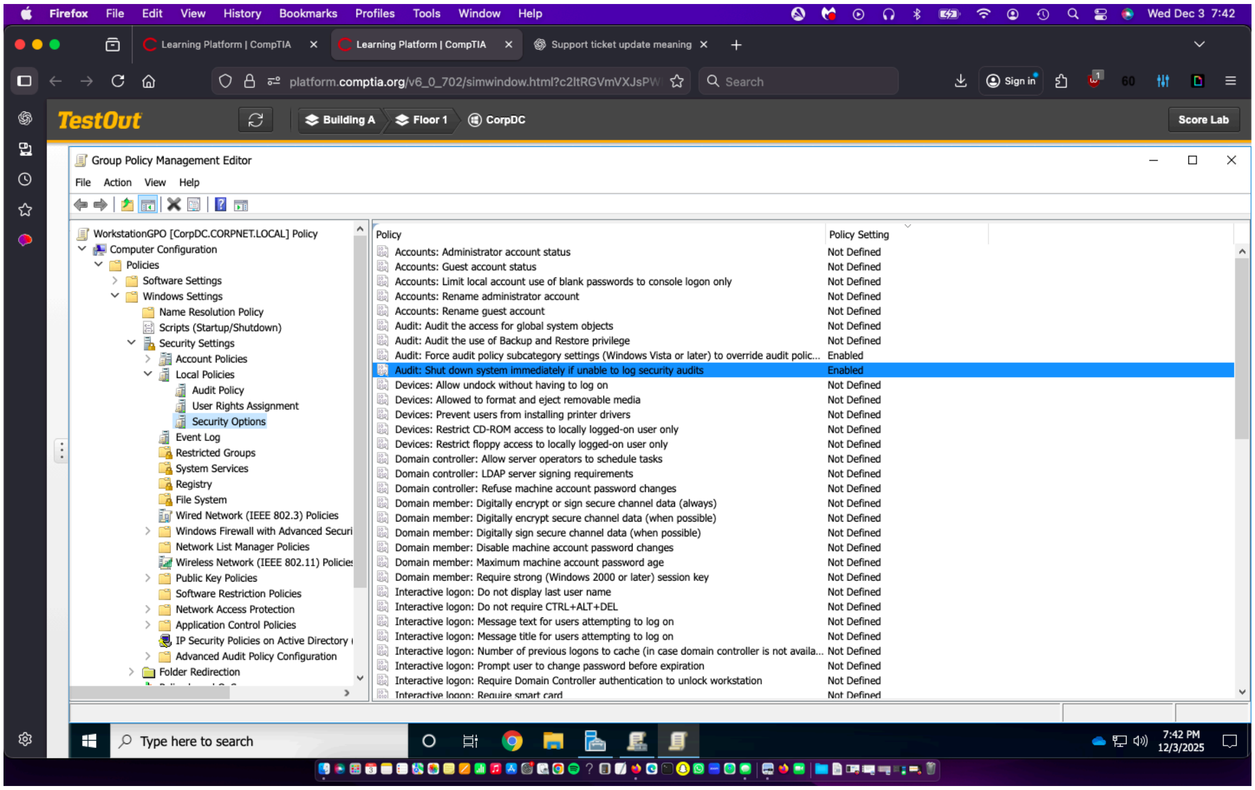
- WorkstationGPO [CorpDC.CORPNET.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Securi
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active Directory (
          - Advanced Audit Policy Configuration
        - Folder Redirection

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access for global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to overri...	Not Defined
Audit: Shut down system immediately if unable to log security audits	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controll...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined

2. Modifying Local Policies

Configured essential local security options, including:

- Force audit policy subcategory settings to override category settings
- Shut down system immediately if unable to log security audits

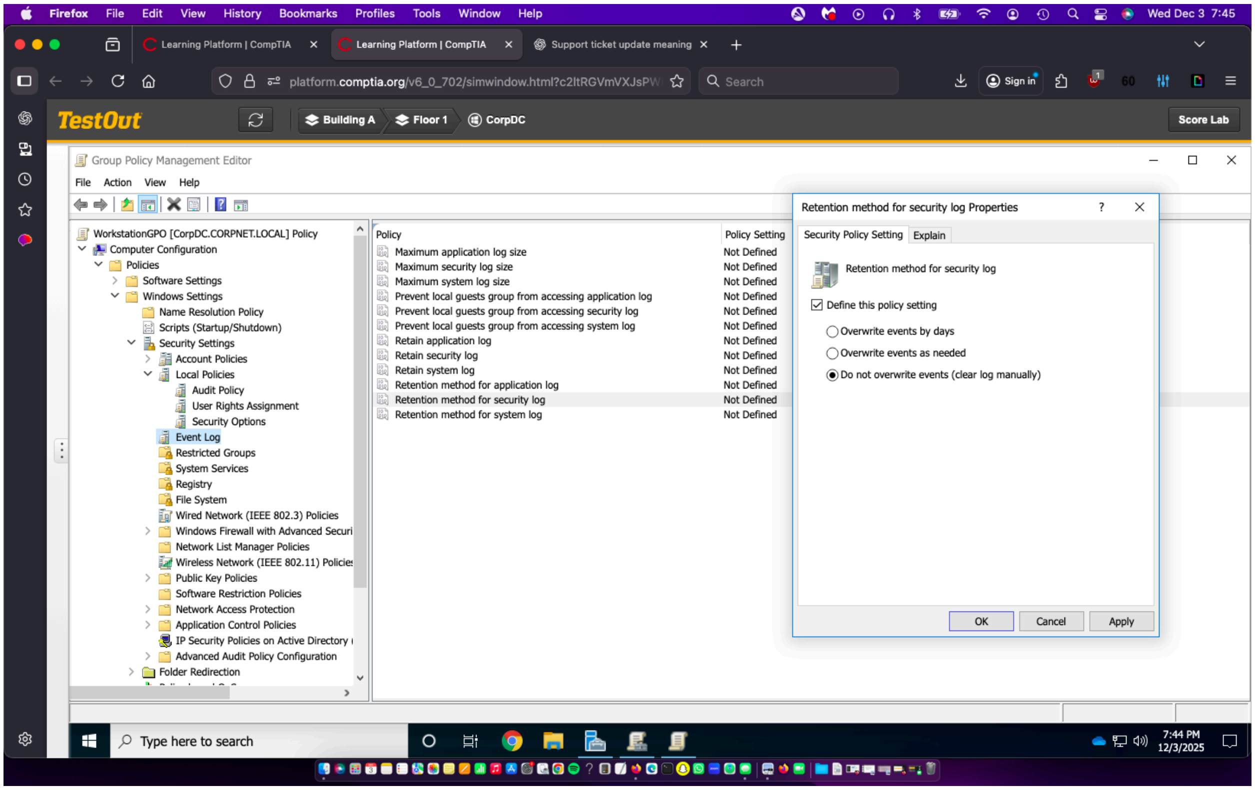

Group Policy Management Editor
File Action View Help
WorkstationGPO [CorpDC.CORPNET.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Securi
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (
Advanced Audit Policy Configuration
Folder Redirection
TestOut
Building A
Floor 1
CorpDC
Score Lab
Type here to search
7:42 PM
12/3/2025

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access for global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit polic...	Enabled
Audit: Shut down system immediately if unable to log security audits	Enabled
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not availa...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined

---

3. Configuring Event Log Policies

Updated Event Log settings to define retention for security logs (do not overwrite events).
This ensures that critical audit data is preserved for compliance and incident investigation.


Group Policy Management Editor
File Action View Help
WorkstationGPO [CorpDC.CORPNET.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Securi
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Folder Redirection
TestOut
Building A
Floor 1
CorpDC
Score Lab
Type here to search
7:44 PM
12/3/2025

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Retention method for security log Properties

Security Policy Setting | Explain

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

○ Overwrite events as needed

● Do not overwrite events (clear log manually)

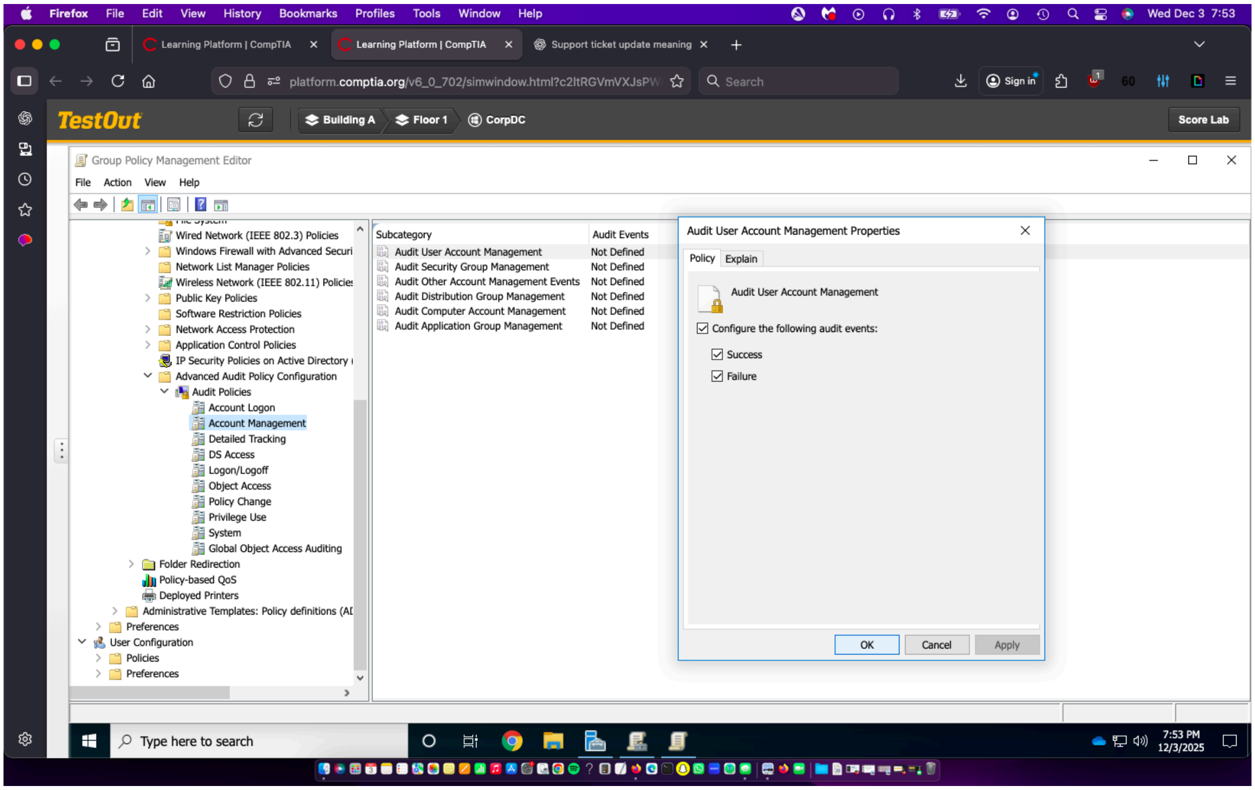
OK | Cancel | Apply

---

4. Setting Advanced Audit Policy Categories

Enabled subcategory-level auditing for critical areas, including:

- **Account Logon & Management** (success/failure)
- **Detailed Tracking** (process creation)
- **Logon/Logoff** (success/failure)
- **Policy Change** (success/failure)
- **Privilege Use** (success/failure)
- **System Integrity & Security Extensions**


Firefox File Edit View History Bookmarks Profiles Tools Window Help
Wed Dec 3 7:53
Learning Platform | CompTIA
Learning Platform | CompTIA
Support ticket update meaning
platform.comptia.org/v6_0_702/simwindow.html?c2ltRGVmVXJsPW
Search
Sign in
TestOut
Building A
Floor 1
CorpDC
Score Lab
Group Policy Management Editor
File Action View Help
Type here to search
7:53 PM
12/3/2025

- Wired Network (IEEE 802.3) Policies
- Windows Firewall with Advanced Securi
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Network Access Protection
- Application Control Policies
- IP Security Policies on Active Directory (
- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing
- Folder Redirection
- Policy-based QoS
- Deployed Printers
- Administrative Templates: Policy definitions (AI
- Preferences
- User Configuration
  - Policies
  - Preferences

Subcategory	Audit Events
Audit User Account Management	Not Defined
Audit Security Group Management	Not Defined
Audit Other Account Management Events	Not Defined
Audit Distribution Group Management	Not Defined
Audit Computer Account Management	Not Defined
Audit Application Group Management	Not Defined

Audit User Account Management Properties

Policy | Explain

Audit User Account Management

☑ Configure the following audit events:

☑ Success

☑ Failure

Security Value

This configuration ensures that all relevant security events are tracked at a granular level, preserving logs for auditing, compliance, and forensic analysis while supporting proactive security monitoring and incident response.