How to Configure an Audit Policy

Task. Configure an audit policy.

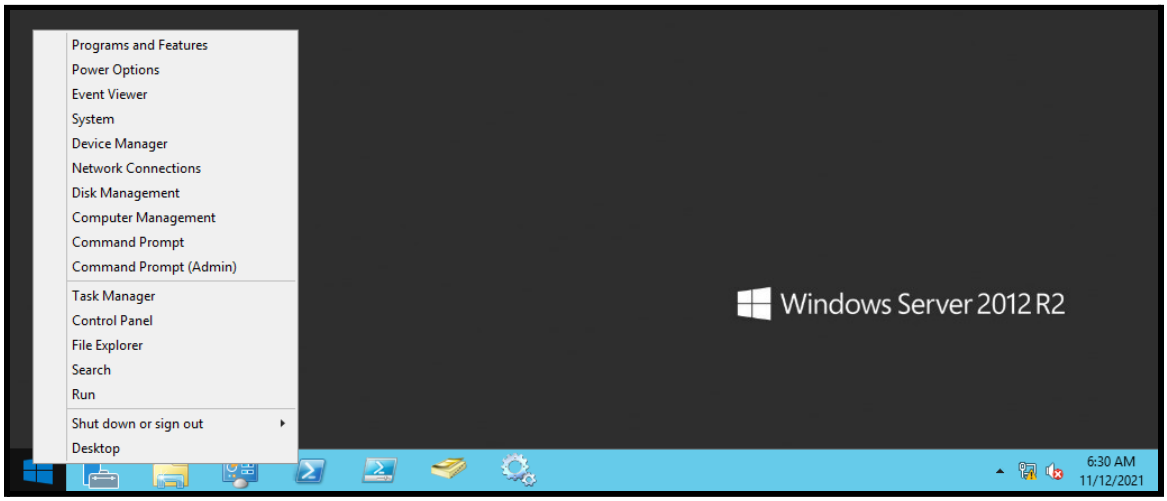
Purpose. An audit policy specifies categories of security-related events you want to audit. In layman's terms, your audit policy determines what gets logged (i.e., logon attempts, USB connections, etc.).

Conditions. You have domain administrator privileges and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

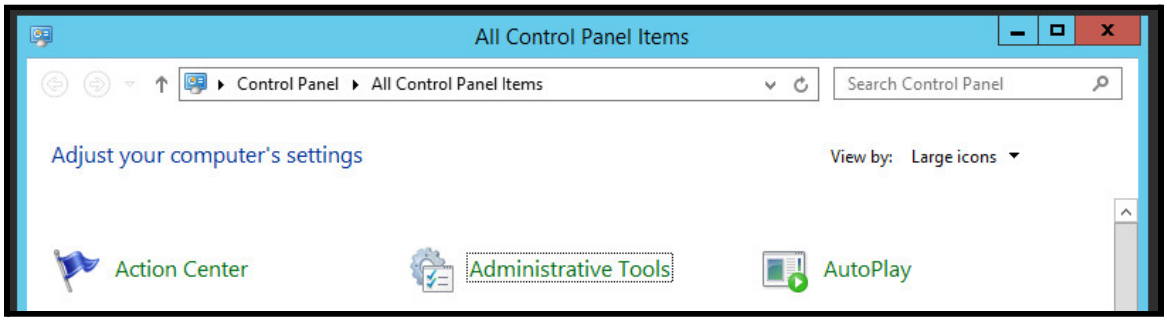
Standard. You were able to create an audit policy using Group Policy.

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

Step 2. Right-click on the Windows icon in the bottom-left corner and select "Control Panel."

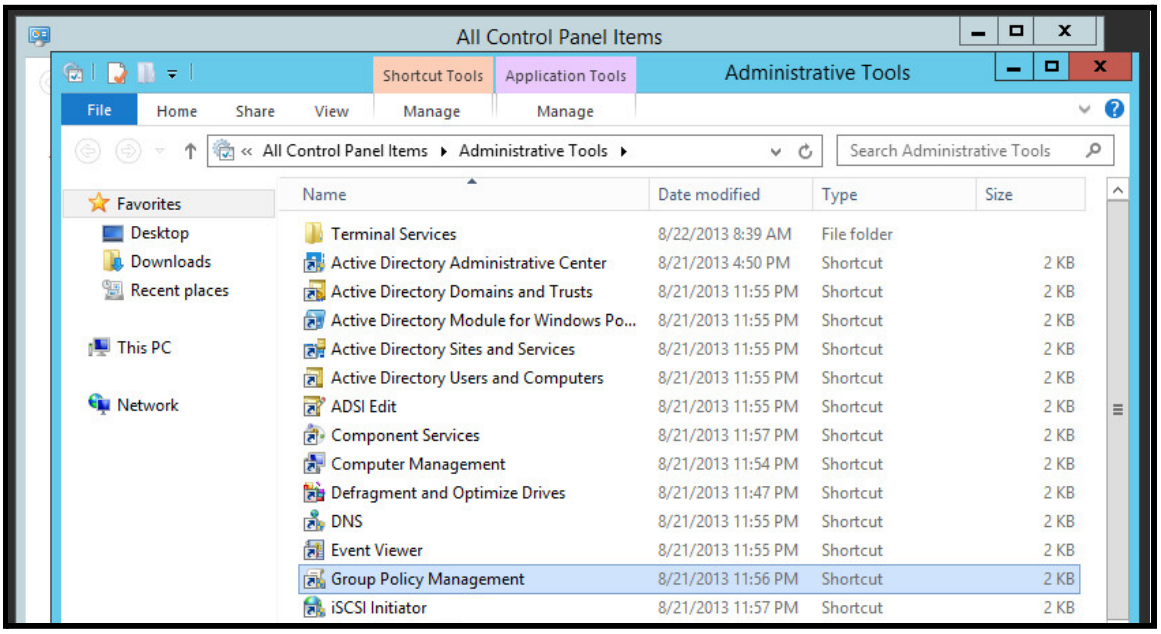


Step 3. Click-on "Administrative Tools."

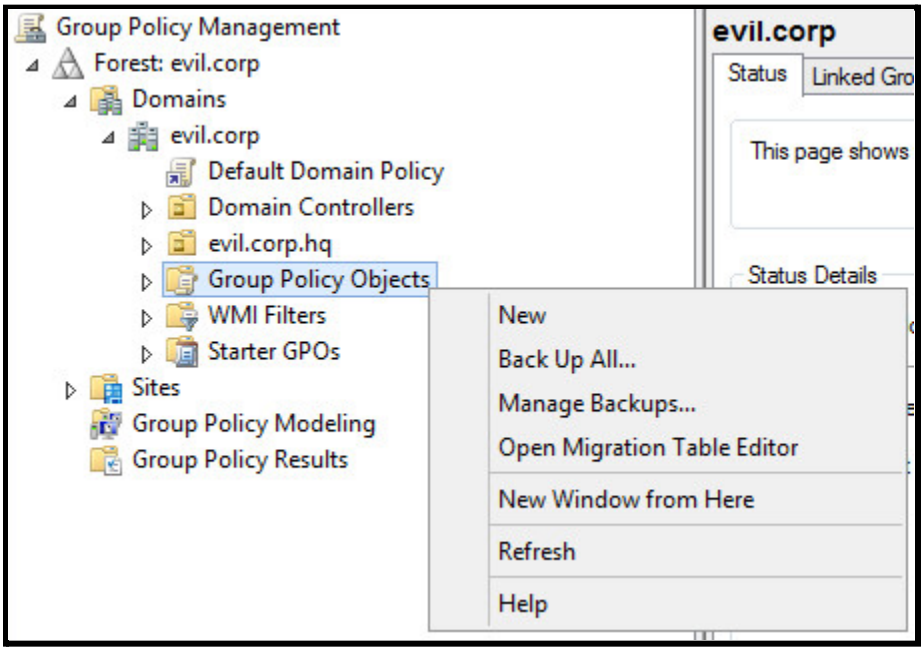


How to Configure an Audit Policy

Step 4. Double-click “Group Policy Management.”

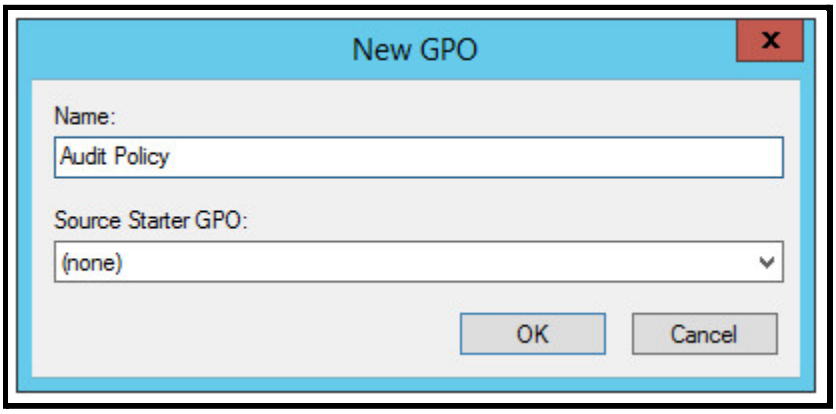


Step 5. Right-click the “Group Policy Objects” container and select “New.”

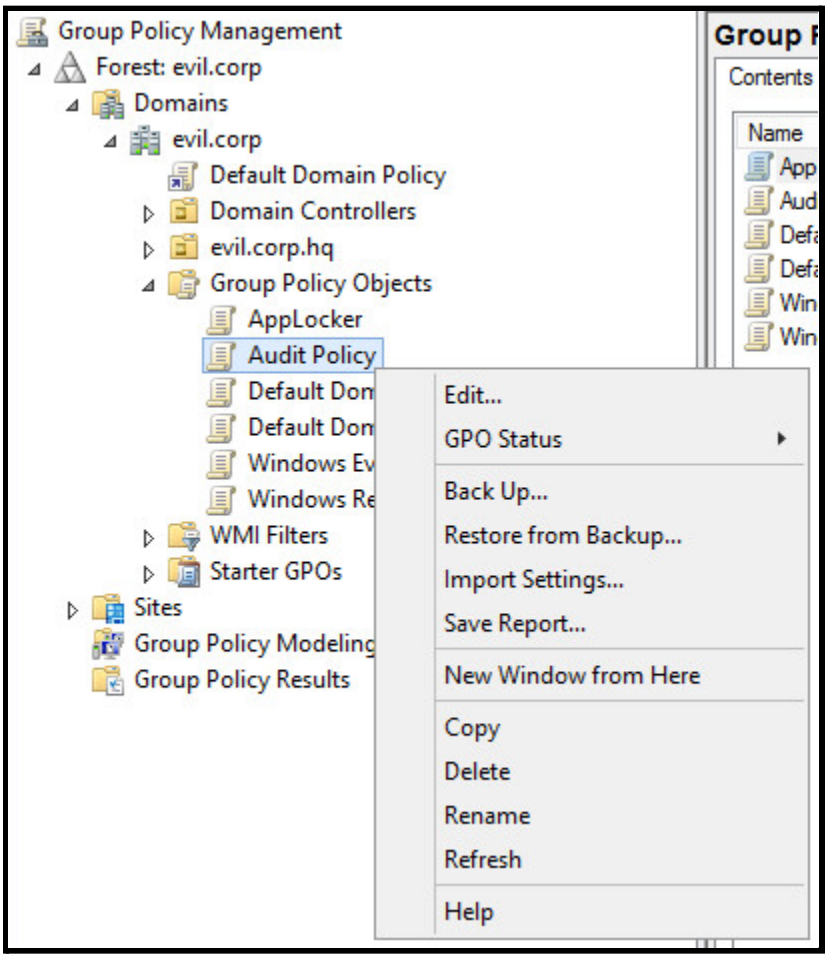


How to Configure an Audit Policy

Step 6. Type “Audit Policy” in the “Name” field.

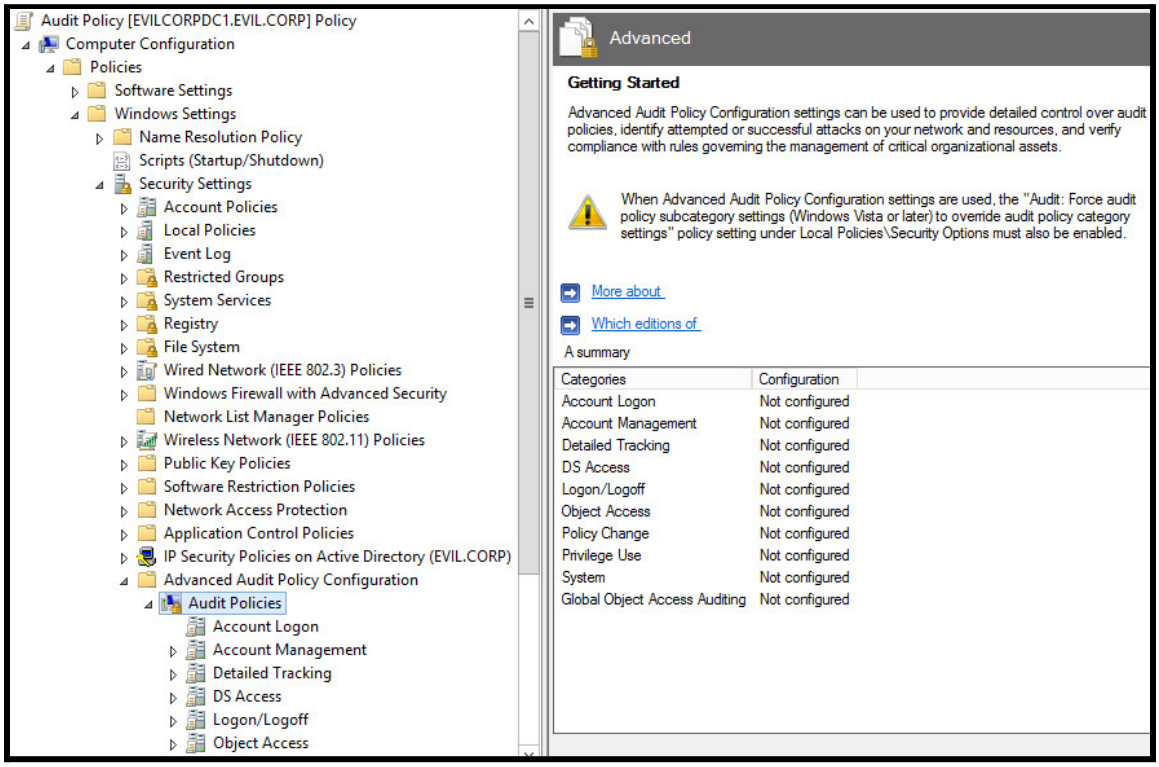


Step 7. Right-click the GPO you created and select “Edit.”



How to Configure an Audit Policy

Step 8. With the GPO open, navigate to the following path: “Computer Configuration” > “Policies” > “Windows Settings” > “Security Settings” > “Advanced Audit Policy Configuration” > “Audit Policies.”



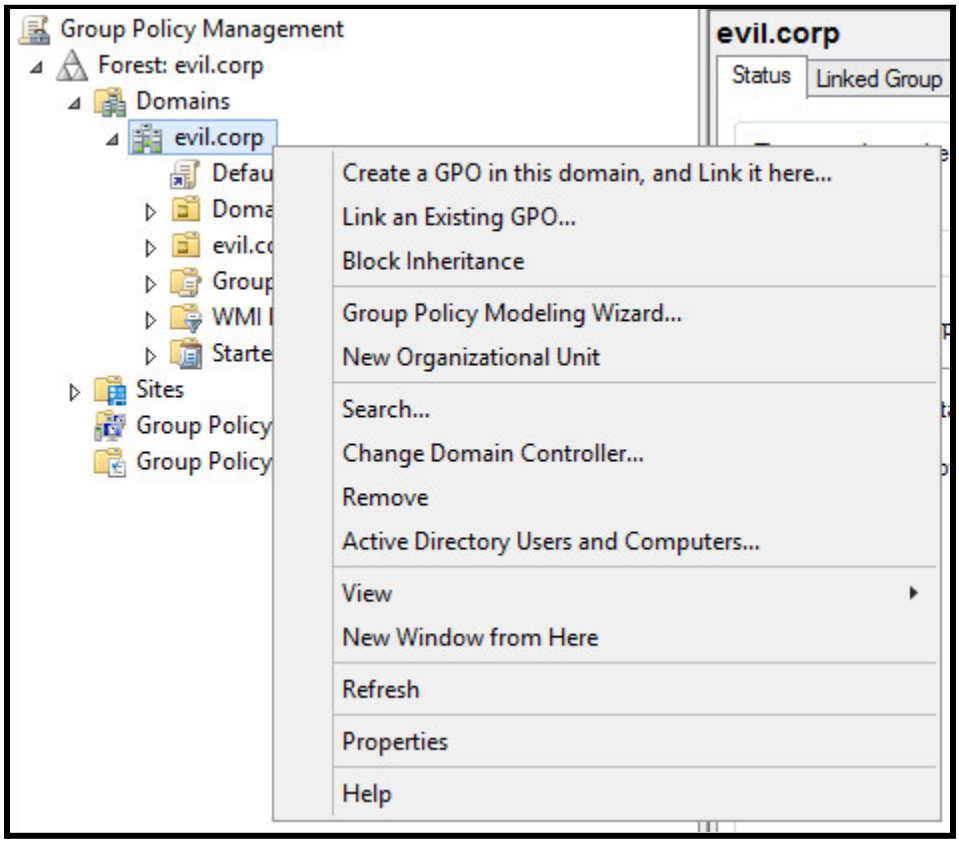
Step 9. Browse the available “Categories.” Configure each “Subcategory” as specified below.

- Account Management
    - Audit User Account Management: Success
    - Audit Security Group Management: Success
- Detailed Tracking
    - Audit Process Creation: Success
- Logon/Logoff
    - Audit Logon: Success, Failure
    - Audit Special Logon: Success
- Object Access
    - Audit File Share: Success
    - Audit File System: Success
    - Audit Filtering Platform Connection: Success, Failure
    - Audit Other Object Access Events: Success
    - Audit Registry: Success
    - Audit Removable Storage: Success
- Policy Change
    - Audit Audit Policy Change: Success
- System
    - Audit Security System Extension: Success, Failure

The table below identifies the Event IDs generated by the Subcategories listed above.

Audit Policy Subcategory	Audit	Event ID	Event
User Account Management	Success	4720	A user account was created
	Success	4722	A user account was enabled
	Success	4723	Password change attempt
	Success	4724	New password failed
Security Group Management	Success	4728	Global group addition
	Success	4732	Local group addition
	Success	4756	Universal group addition
Process Creation	Success	4688	A new process was created
Logon	Success	4624	An account successfully logged on
	Failure	4625	An account failed to log on
Special Logon	Success	4672	Special privileges assigned
File Share	Success	5140	A network share was accessed
	Both	5145	A network share was enumerated
File System	Success	4663	Object access attempt
Filtering Platform Connection (a.k.a. Windows Firewall)	Success	5156	A connection was allowed
	Failure	5157	A connection was blocked
Other Object Access	Success	4698	A scheduled task was created
Registry	Success	4663	Object access attempt
Removable Storage	Success	6416	External device recognized
Policy Change	Success	4719	System audit policy was changed
Security System Extension	Success	4697	A service was installed

Step 10. Close the GPO. Right-click on your domain and select “Link an Existing GPO…”



Step 11. Select the GPO you created and click-on “OK.”