BLUE LANCE

Microsoft Windows Advanced Audit Policy Configurations for LT Auditor+

Reference Guide

Contents

Table of Contents

Windows Audit Policies Required for LT Auditor+

Advanced Audit Policies need to be configured on specific Group Policy Objects (GPO) to ensure successful auditing with LT Auditor+.

These policies need to be set to successfully audit Active Directory changes, File System modifications and Login/Logout activities on the Microsoft Windows system.

The following sections detail the specific Advanced Audit Policies configuration requirements.

Active Directory

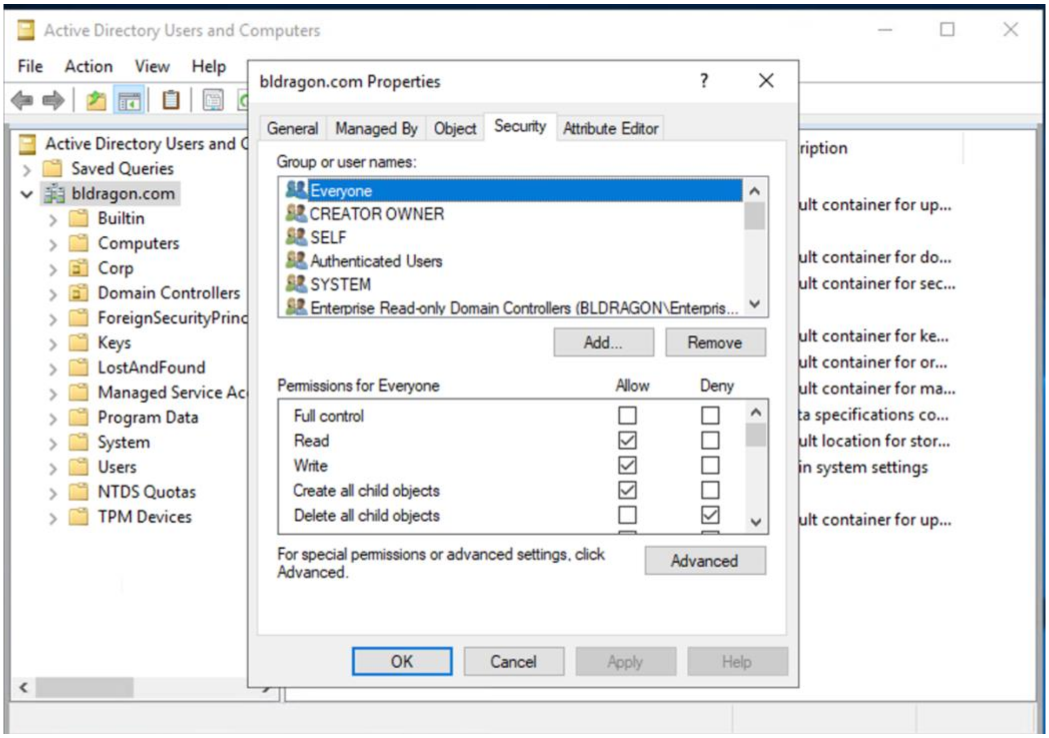
To successfully audit Active Directory events with LT Auditor+, the following settings need to be configured.

1. Security Access Control Lists (SACLs) on the Active Directory Domain object.
2. Advanced Audit Policies (DS Access and Account Management) on the Default Domain Controller Group Policy or any other GPO that covers all Domain Controllers.

Domain Object SACLs

This setting may be configured by default, but it is important to validate that the following SACL audit entries are defined on the domain object.

1. Launch Windows Active Directory and Users MMC.
2. Click on View → Advanced Features to enable.
3. Right-click on the root domain object and click on Properties to bring up the Properties Window as shown below:



Active Directory Users and Computers

bldragon.com Properties

General | Managed By | Object | Security | Attribute Editor

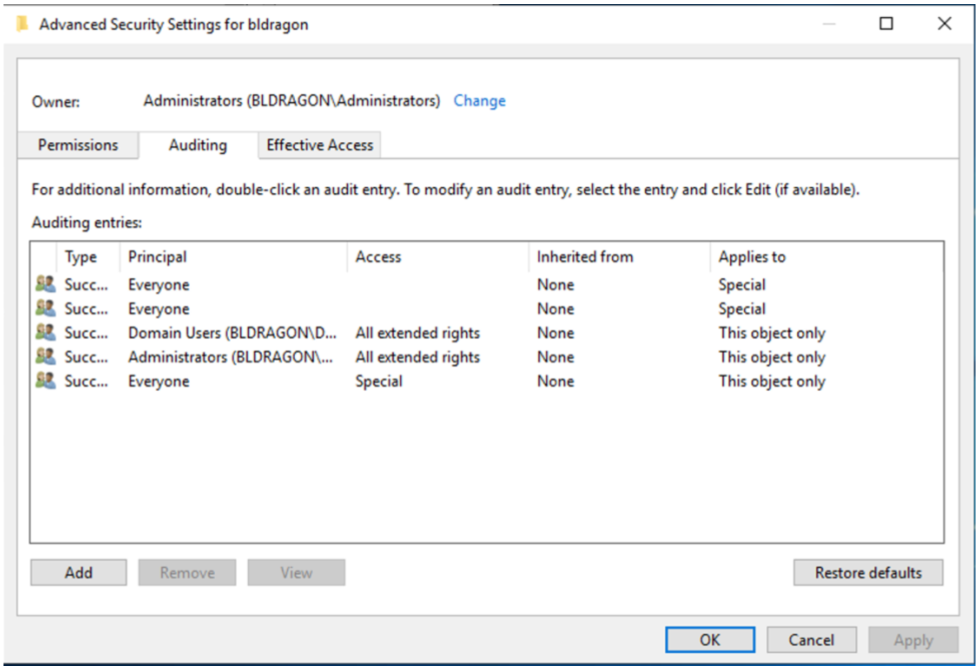
Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Enterprise Read-only Domain Controllers (BLDRAGON\Enterpris...

Permissions for Everyone	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	□	☑

For special permissions or advanced settings, click Advanced.

4. Select the Security Tab, click on Advanced and select the Auditing tab as shown below:



Advanced Security Settings for bldragon

Owner: Administrators (BLDRAGON\Administrators) Change

Permissions | Auditing | Effective Access

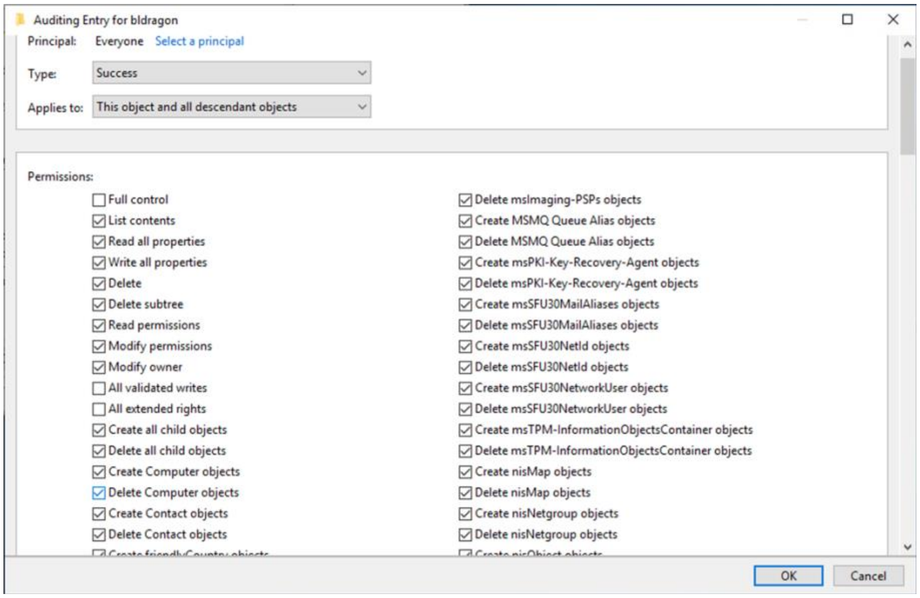
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone		None	Special
Succ...	Everyone		None	Special
Succ...	Domain Users (BLDRAGON\D...	All extended rights	None	This object only
Succ...	Administrators (BLDRAGON\...	All extended rights	None	This object only
Succ...	Everyone	Special	None	This object only

5. Click Add to create a new audit entry and select the Principal "Everyone." Make sure to check the following permissions as displayed below:
   - Write all properties.
   - Delete.
   - Delete subtree.
   - Modify permissions.
   - Modify owner.
   - Create all child objects.
   - Delete all child objects.

   Note: All "create" and "delete" entries will get checked automatically.



Auditing Entry for bldragon

Principal: Everyone Select a principal

Type: Success

Applies to: This object and all descendant objects

Permissions:

□ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☑ Delete
☑ Delete subtree
☑ Read permissions
☑ Modify permissions
☑ Modify owner
□ All validated writes
□ All extended rights
☑ Create all child objects
☑ Delete all child objects
☑ Create Computer objects
☑ Delete Computer objects
☑ Create Contact objects
☑ Delete Contact objects
☑ Create friendlyCountry objects

☑ Delete msImaging-PSPs objects
☑ Create MSMQ Queue Alias objects
☑ Delete MSMQ Queue Alias objects
☑ Create msPKI-Key-Recovery-Agent objects
☑ Delete msPKI-Key-Recovery-Agent objects
☑ Create msSFU30MailAliases objects
☑ Delete msSFU30MailAliases objects
☑ Create msSFU30NetId objects
☑ Delete msSFU30NetId objects
☑ Create msSFU30NetworkUser objects
☑ Delete msSFU30NetworkUser objects
☑ Create msTPM-InformationObjectsContainer objects
☑ Delete msTPM-InformationObjectsContainer objects
☑ Create nisMap objects
☑ Delete nisMap objects
☑ Create nisNetgroup objects
☑ Delete nisNetgroup objects
☑ Create nisObject objects

Note: You can also modify an existing audit entry instead of adding a new one.

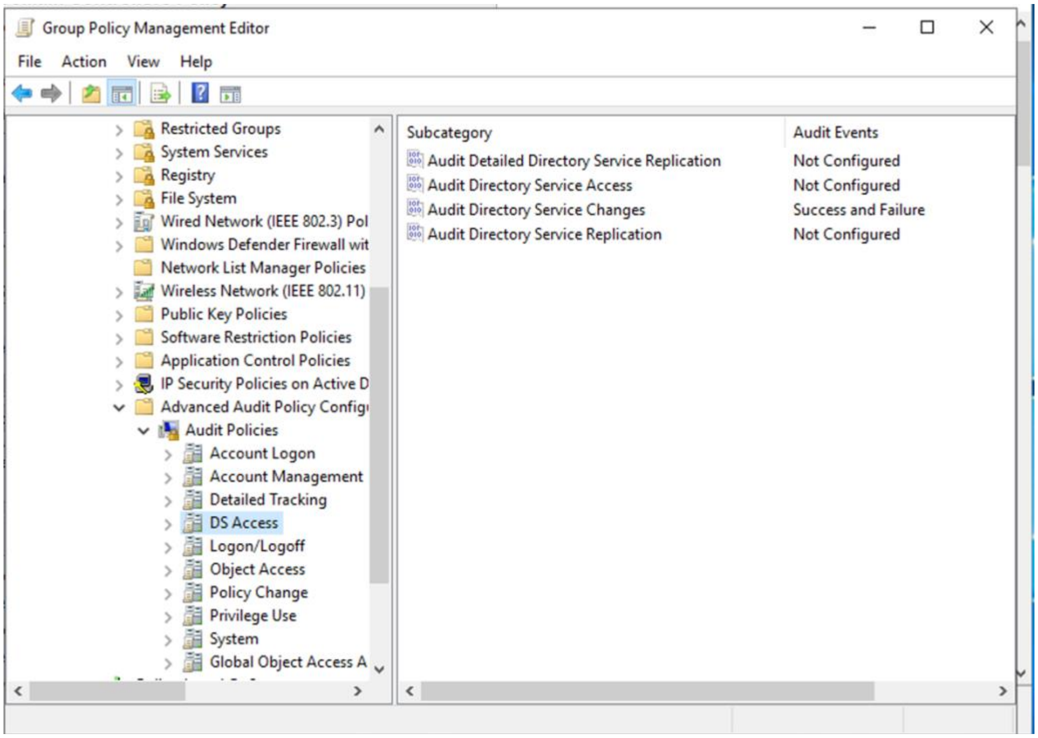
6. Click OK to save setting.

Note: If your Active Directory environment contains multiple OUs that do not inherit from the parent domain object, you may need to create similar audit entries for those OU objects.

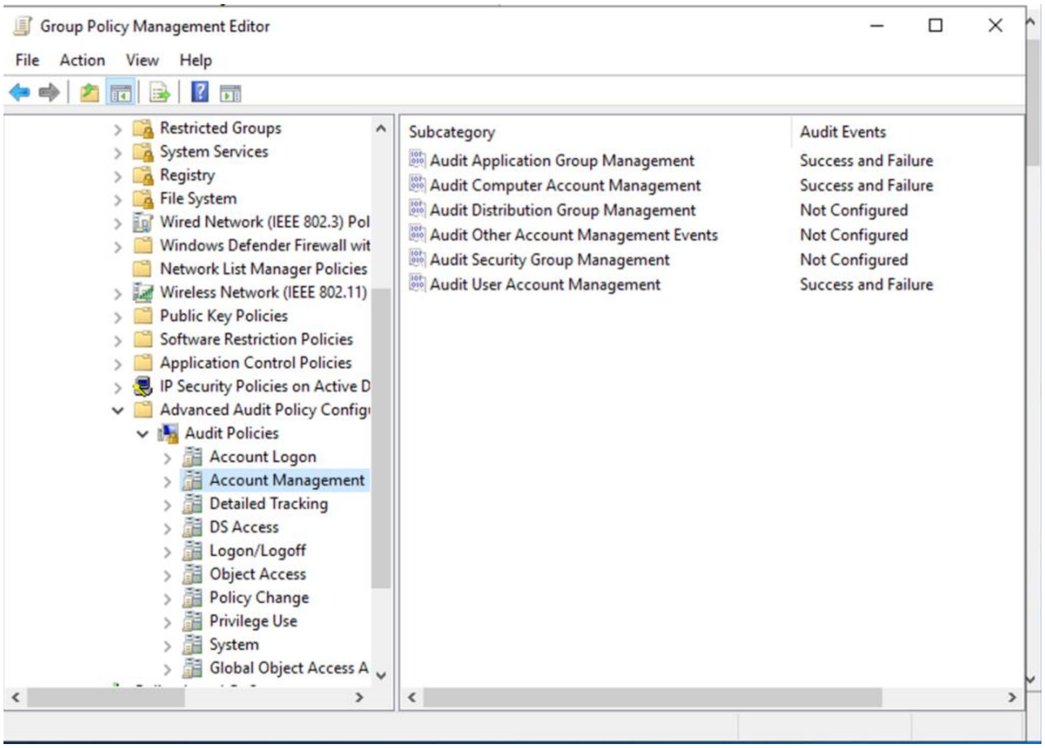
Advanced Auditing Policies for the Default Domain Controller Group Policy
The second step requires audit entries to be defined on the default group policy for Domain Controllers. Use the Group Policy Management MMC to access Advanced Audit Policies and configure the following audit entries:

Audit Policy	Subcategory	Audit Events
DS Access	Audit Directory Service Changes	Success and Failure
Account Management	Audit User Account Management	Success and Failure
Account Management	Audit Computer Account Management	Success and Failure
Account Management	Audit Group Account Management	Success and Failure

Example of a Default Domain Controller GPO configured to audit Active Directory events for LT Auditor+:


Group Policy Management Editor
File
Action
View
Help
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Defender Firewall wit
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access A

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured


Group Policy Management Editor
File
Action
View
Help
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Defender Firewall wit
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access A

Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Not Configured
Audit User Account Management	Success and Failure

File System

To audit file modifications, the following settings need to be applied:

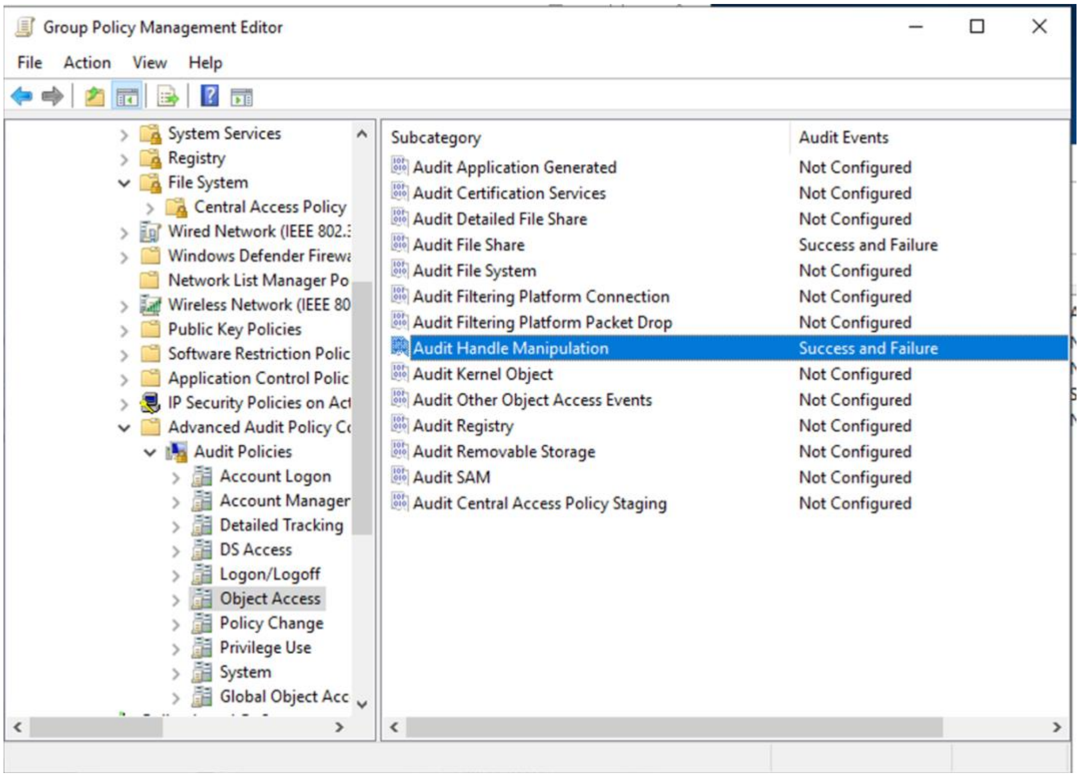
1. Advanced Audit Policy (Object Access) settings on a GPO linked to OUs associated with file servers to be audited.
2. SACL entries on all audited folders.

Advanced Audit Policy on File Server GPO

To audit files and folders, the following settings to be configured on Object Access policy for the GPO associated with the OUs that contain the file servers.

Audit Policy	Subcategory	Audit Events
Object Access	Audit File System	Success and Failure
Object Access	Audit Handle Manipulation	Success and Failure

Example of a GPO configured to audit File System activity for LT Auditor+.

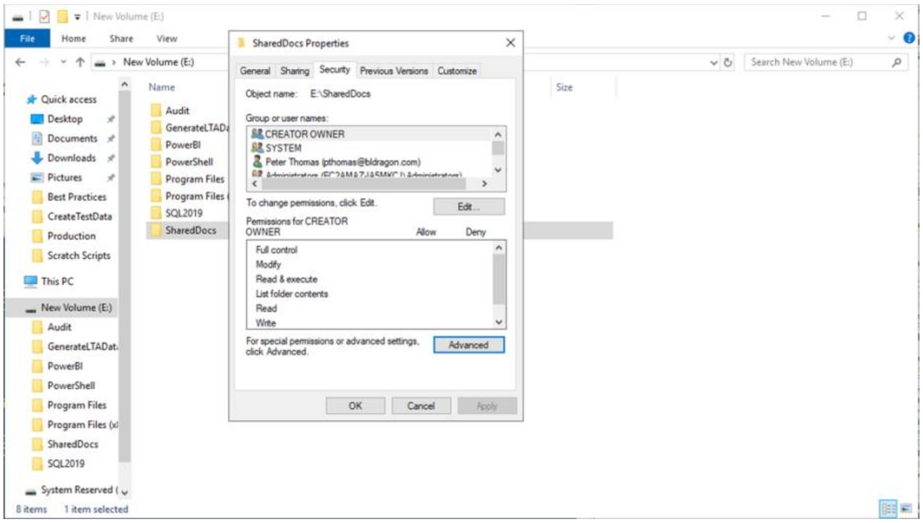


Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Not Configured
Audit File Share	Success and Failure
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Success and Failure
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

SACL Entries on Audited Folders

The following steps outline how to configure SACLs on Windows shares or folders that need to be audited:

1. Right-click on shared or root folder and click Properties.



Object name: E:\SharedDocs

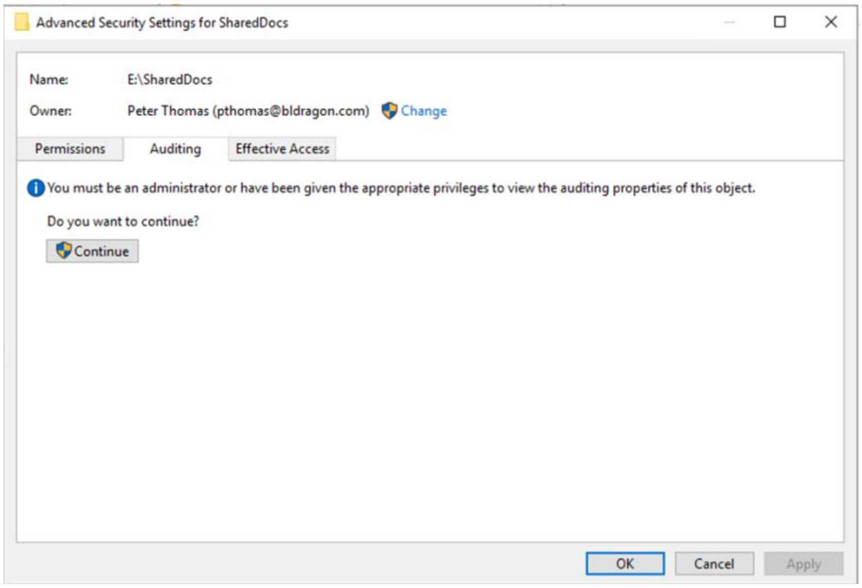
Group or user names:
CREATOR OWNER
SYSTEM
Peter Thomas (pthomas@bldragon.com)
Administrators (EC2AMAZ-JA5MKC\Administrators)

To change permissions, click Edit.

Permissions for CREATOR OWNER — Allow — Deny
Full control
Modify
Read & execute
List folder contents
Read
Write

For special permissions or advanced settings, click Advanced.

2. Select the Security Tab and click Advanced.



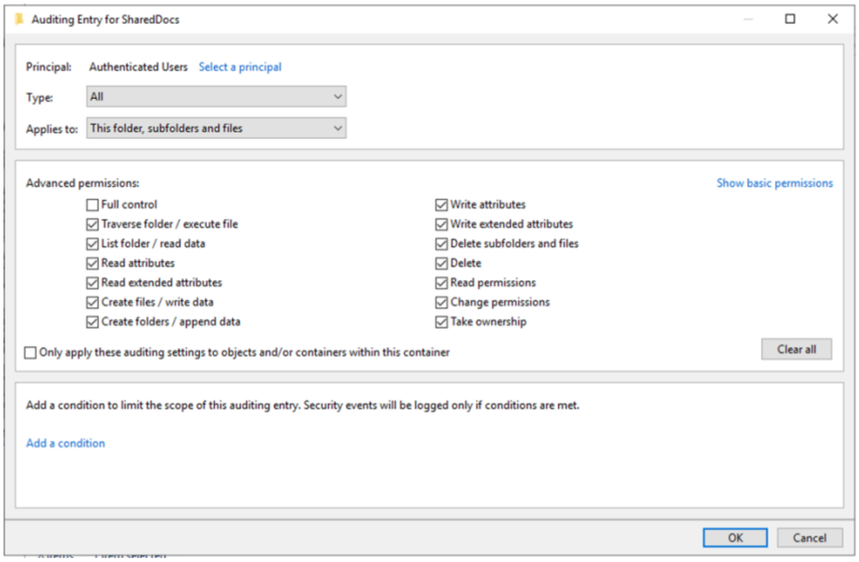
Name: E:\SharedDocs

Owner: Peter Thomas (pthomas@bldragon.com) Change

You must be an administrator or have been given the appropriate privileges to view the auditing properties of this object.

Do you want to continue?

3. Click Auditing tab and select Authenticated Users as the Principal with the following permissions to audit for: "All" types that apply to "all subfolders."



Principal: Authenticated Users Select a principal

Type: All

Applies to: This folder, subfolders and files

Advanced permissions:

☐ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☑ Read permissions
☑ Change permissions
☑ Take ownership

☐ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

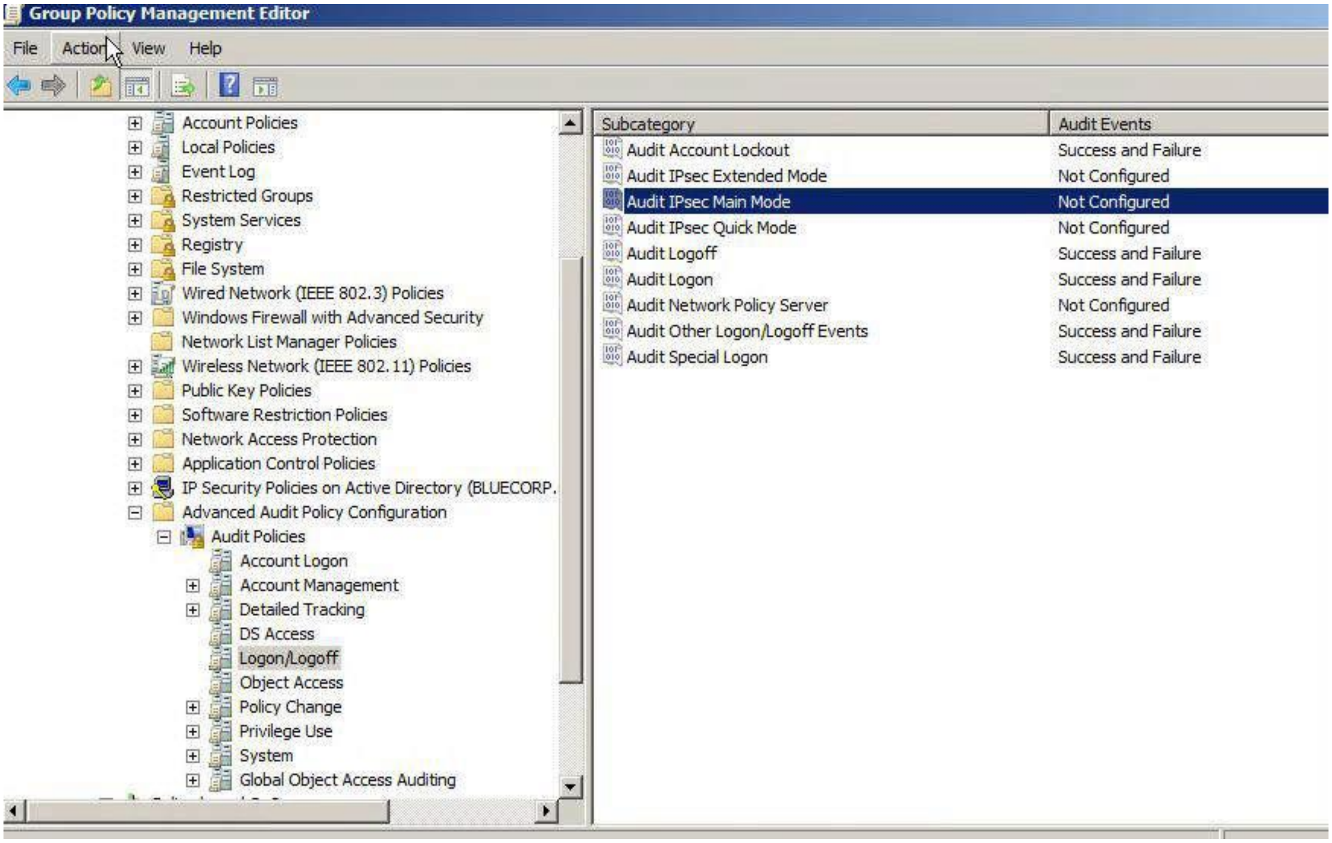
4. Conditions can be set to restrict the scope of auditing.

Login/Logout

To audit login and logout activity for the domain, the following audit entries need to be configured on the GPO associated with the domain. Blue Lance recommends that these settings are defined for the Default Domain Group Policy.

Audit Policy	**Subcategory**	**Audit Events**
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Login/Logoff	Audit Account Lockout	Success and Failure
Login/Logoff	Audit Logoff	Success and Failure
Login/Logoff	Audit Logon	Success and Failure
Login/Logoff	Audit Other Logon/Logoff Events	Success and Failure
Login/Logoff	Audit Special Logon	Success and Failure

Example of Default Domain Controller GPO configured to Login/Logout activity:


Group Policy Management Editor
File
Action
View
Help
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
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 (BLUECORP.
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

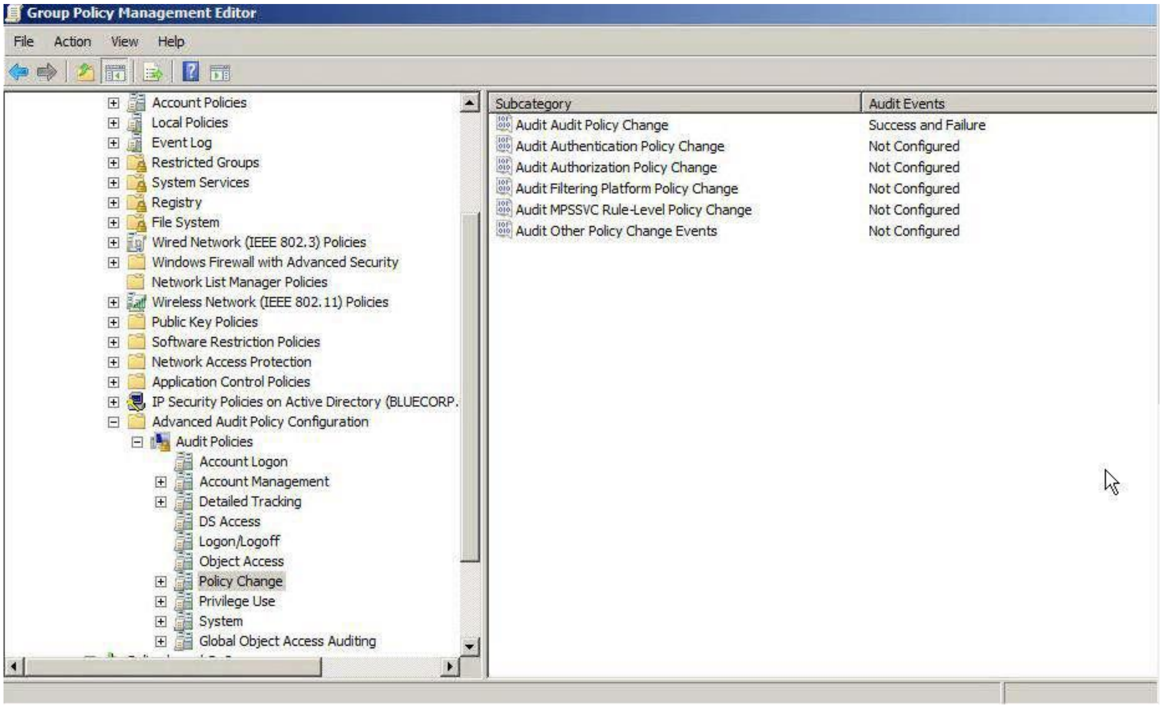
Subcategory	Audit Events
Audit Account Lockout	Success and Failure
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Audit Policy Changes

To audit changes to audit policies, the following audit entries are required:

Audit Policy	Subcategory	Audit Events
Policy Change	Audit Policy Change	Success and Failure

Example of GPO configured to audit policy changes:



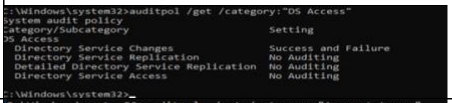
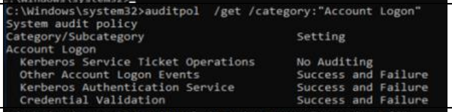
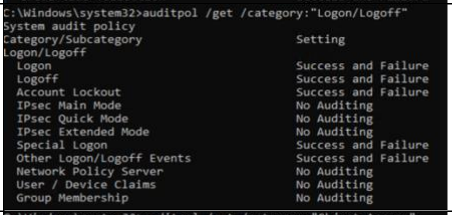
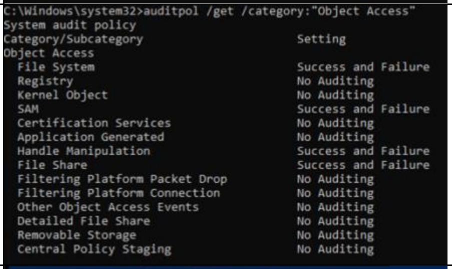
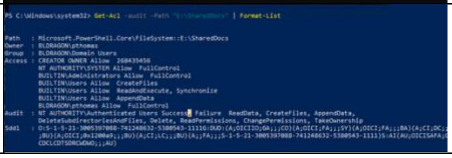
- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System
- Wired Network (IEEE 802.3) Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Network Access Protection
- Application Control Policies
- IP Security Policies on Active Directory (BLUECORP.
- 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

Subcategory	Audit Events
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Not Configured
Audit Authorization Policy Change	Not Configured
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Not Configured
Audit Other Policy Change Events	Not Configured

APPENDIX A — Checking Assigned Permissions

The following commands can be used to check and ensure audit policies have been configured correctly.

Note: commands are run from command prompt or PowerShell, and user should have administrative rights to run the command.

Category	Host to run command	Command/PowerShell Window (run as Administrator)	Command
Active Directory Changes	On any Domain Controller	 C:\Windows\system32>auditpol /get /category:"DS Access" System audit policy Category/Subcategory Setting DS Access Directory Service Changes Success and Failure Directory Service Replication No Auditing Detailed Directory Service Replication No Auditing Directory Service Access No Auditing C:\Windows\system32>_	Auditpol /get /category: “DS Access”
Account Logon	On any Domain Controller	 C:\Windows\system32>auditpol /get /category:"Account Logon" System audit policy Category/Subcategory Setting Account Logon Kerberos Service Ticket Operations No Auditing Other Account Logon Events Success and Failure Kerberos Authentication Service Success and Failure Credential Validation Success and Failure	Auditpol /get /category: “Account Logon”
Logon/Logoff	On any Windows machine	 C:\Windows\system32>auditpol /get /category:"Logon/Logoff" System audit policy Category/Subcategory Setting Logon/Logoff Logon Success and Failure Logoff Success and Failure Account Lockout Success and Failure IPsec Main Mode No Auditing IPsec Quick Mode No Auditing IPsec Extended Mode No Auditing Special Logon Success and Failure Other Logon/Logoff Events Success and Failure Network Policy Server No Auditing User / Device Claims No Auditing Group Membership No Auditing	Auditpol /get /Category: “Logon/Logoff”
Object Access	On File Servers	 C:\Windows\system32>auditpol /get /category:"Object Access" System audit policy Category/Subcategory Setting Object Access File System Success and Failure Registry No Auditing Kernel Object No Auditing SAM Success and Failure Certification Services No Auditing Application Generated No Auditing Handle Manipulation Success and Failure File Share Success and Failure Filtering Platform Packet Drop No Auditing Filtering Platform Connection No Auditing Other Object Access Events No Auditing Detailed File Share No Auditing Removable Storage No Auditing Central Policy Staging No Auditing	Auditpol /get /Category: “Object Access”
SACL entries on Audited Folder	PowerShell command on File Server	 PS C:\Windows\system32> Get-Acl -audit -Path "E:\SharedDocs" | Format-List Path : Microsoft.PowerShell.Core\FileSystem::E:\SharedDocs Owner : BLDRAGON\pthomas Group : BLDRAGON\Domain Users Access : CREATOR OWNER Allow 268435456 NT AUTHORITY\SYSTEM Allow FullControl BUILTIN\Administrators Allow FullControl BUILTIN\Users Allow CreateFiles BUILTIN\Users Allow ReadAndExecute, Synchronize BUILTIN\Users Allow AppendData BLDRAGON\pthomas Allow FullControl Audit : NT AUTHORITY\Authenticated Users Success, Failure ReadData, CreateFiles, AppendData, DeleteSubdirectoriesAndFiles, Delete, ReadPermissions, ChangePermissions, TakeOwnership Sddl : O:S-1-5-21-3005397088-741248632-5300543-1111G:DUD:(A;OICIIO;GA;;;CO)(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;CI;DC;; ;BU)(A;OICI;0x1200a9;;;BU)(A;CI;LC;;;BU)(A;;FA;;;S-1-5-21-3005397088-741248632-5300543-1111)S:AI(AU;OICISAFA; CDCLCDTSDRCWDWO;;;AU)	Get-Acl -audit -Path "<Audited Folder>" | Format-List

APPENDIX B — Windows Event IDs Used by LT Auditor+

ACTIVE DIRECTORY

Category	LT Auditor+ Event	Object	Windows Event ID
Object			
	Create Object		5137
		User	
		Global Security Group	
		Domain Local Security Group	
		Computer	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
		Other	
	Delete Object		5141
		User	
		Global Security Group	
		Domain Local Security Group	
		Computer	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
		Other	
	Modify Security DACL		5136
	Rename Object		4781
	Move Object		5139
	Add Attribute		5136
	Delete Attribute		5136
Account Modification			
	Enable Account		4722
	Disable Account		4725
	Set Password		4724
	Change Password		4723
	Account Locked		4740

	Account Unlocked		4767
Group Membership			
	Add Member to group		5136
		Global Security Group	
		Domain Local Security Group	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
	Remove Member from group		5136
		Global Security Group	
		Domain Local Security Group	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
	Trusted domain added		4706
	Audit policy changed		4719

Windows File System

Category	LT Auditor+ Event	Windows Event ID
File		4656
	Create File	
	Write File	
	Rename File	
	Delete File	
	Access File	
Directory		4656
	Make Directory	
	Remove Directory	
	Rename Directory	
	Access Directory	
File Directory		4656
	Write Security DACL	

	Write Attribute	
	Take Ownership	