SGBox Windows Auditing

Configuration Guide

SGBox

SecureGate S.r.l.
Via Melchiorre Gioia, 168 - 20125 Milano (Italy)
Tel: +39 02 60830172 - Fax: +39 02 60736014 - Email: info@sgbox.it
www.sgbox.it

Index

© Copyright SecureGate S.r.l. 2022 – All rights reserved

1 Introduction

To collect all the logs necessary to audit Windows Servers and Workstations, you need to configure the Group Policies enabling auditing for those objects you want to monitor and, if you want to Audit Files activity, the ACLs for the folders you want to check have to be configured as well.

You can control file activities on both shared folders and not shared local folders.

The first step is to configure group policies, or local policies if the Server or Workstation to be controlled is not part of an Active Directory domain.

You must also configure ACLs for the folders and/or disks that you want to monitor, bearing in mind that to obtain audit events, both configurations must be active on the folder or disk to be audited. If acLs are not applied, or if group policies are not configured, the events required for auditing will not be raised.

Be careful that if you want to check the events relating to an Active Directory Domain, you will need to configure the Object Level Auditing also at the Domain level.

© Copyright SecureGate S.r.l. 2022 – All rights reserved

2 Advanced Audit Policy Configuration

To have more detail and greater control over the auditing levels activated, it is preferable to configure and use advanced auditing policies.

2.1 Preliminary Activities

Before you switch to group policy configuration, you need to configure a couple of things that are essential for the solution to work properly:

- Security Options
- Security event log size and its retention methodology

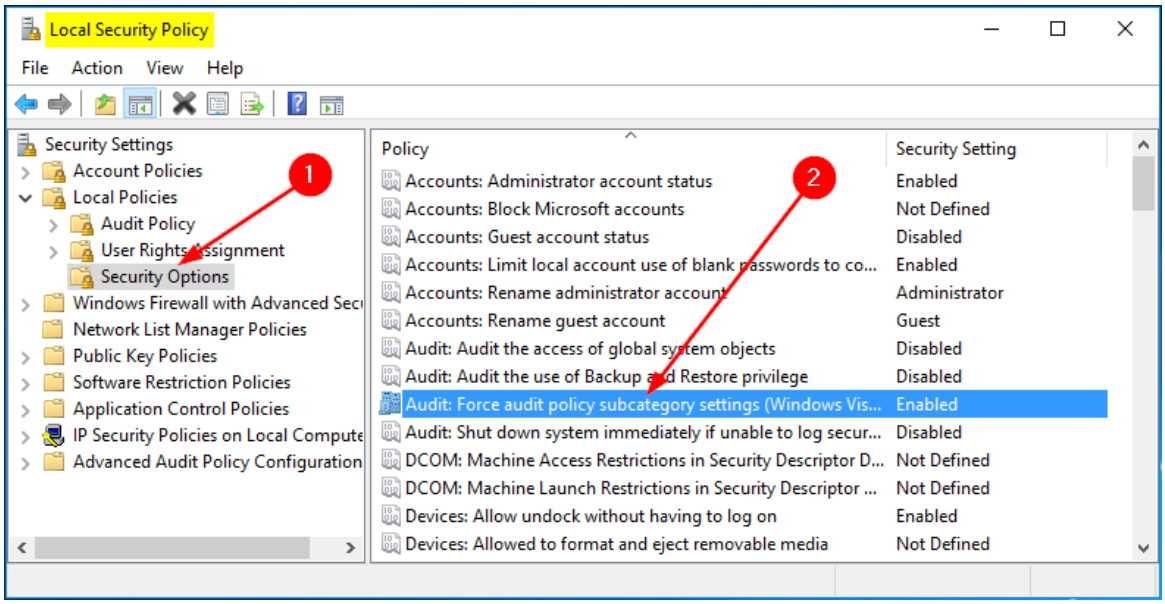
2.1.1 Security Options Configuration

If both basic and advanced audit policies are defined by chance, we would obtain incorrect audit values, to overcome this problem it is necessary to set up the Security Policy appropriately.

Verify that locally, on each Server/Workstation we are going to monitor, the Security Policy (1) **Audit: Force audit policy subcategory settings to override audit policy category settings** (2) is configured **on Enabled** (system default) so that basic audit policies are ignored in favor of advanced audit policies.

On the machines to be verified, open the Local Security Policy panel located in

Start -> Windows Administrative Tools -> Local Security Policy



© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.1.2 Event Log Configuration

The configuration of the security event log features can be performed both locally, for each machine, and centrally through Group Policy.

It is also very important to configure the size and operating mode of the Security Log appropriately so that no events are lost in case of temporary lack of connection with the Server or the SGBox Collector.

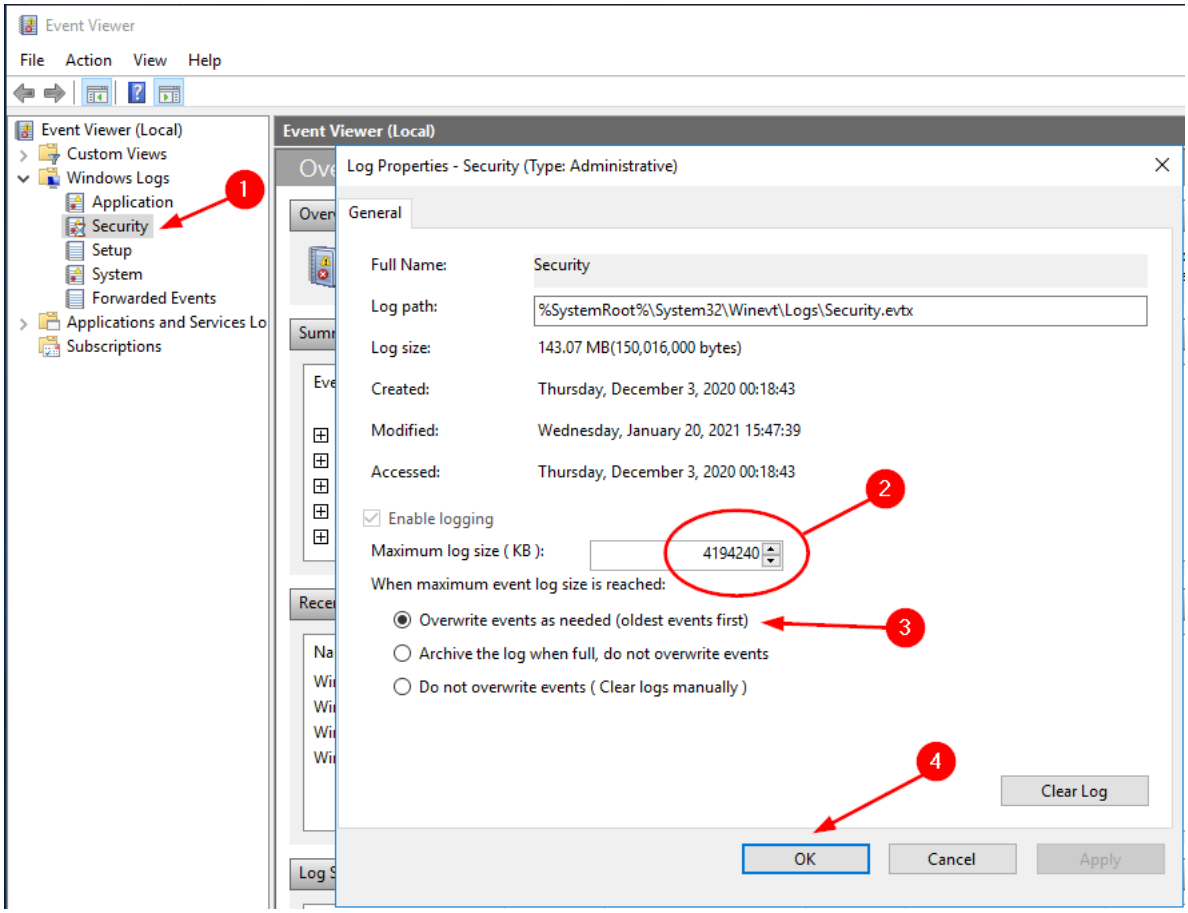
2.1.2.1 Local Configuration

On the machines to be monitored, open the Event Viewer csnap-in located in *Start -> Windows Administrative Tools -> Local Security Policy,* expand *Windows Logs* menu entry, right click on **Security** (1) and choose **Properties** from the pop-up menu.

Position yourself on **Security** (1) and set the values as follows:

- *Maximum log size (KB)*: **4194240** (2)
- *check* the radio button **Overwrite events as needed** (3)

and press **OK** (4) to save the configuration.



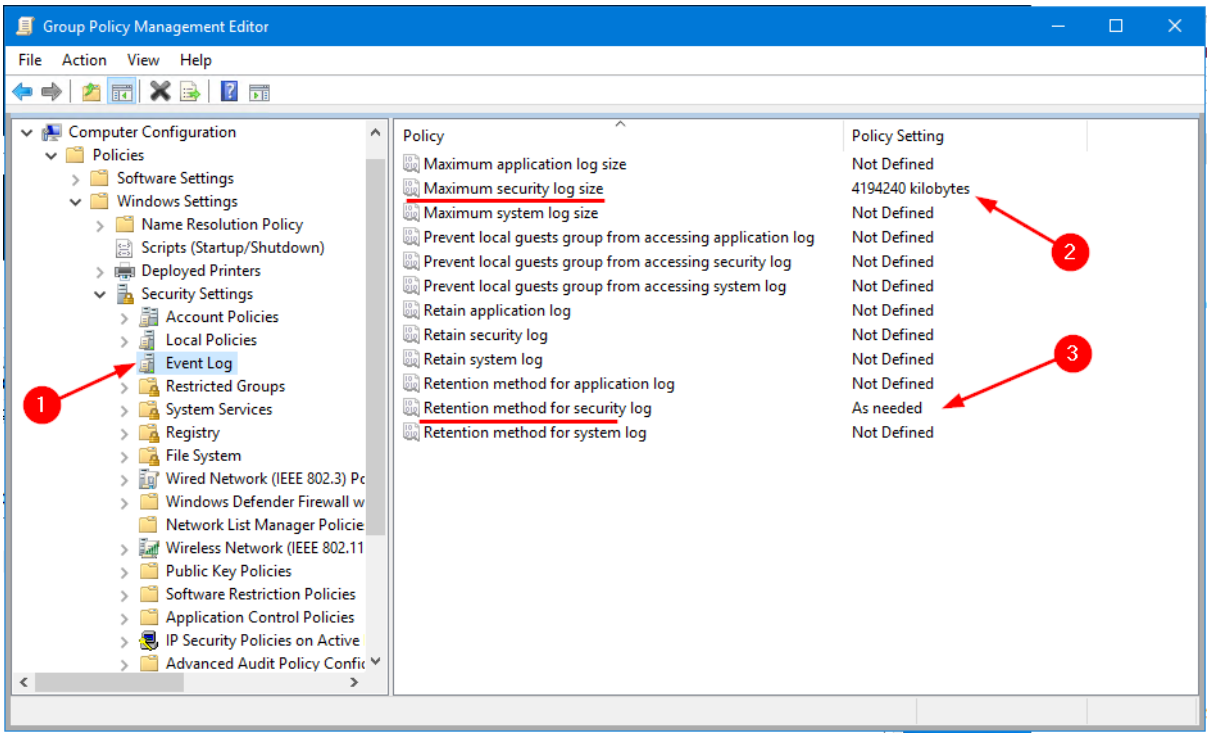
© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.1.2.2 GPO Configuration

On the Domain Controller, open the Group Policy Management snap-in located in *Start* → Windows Administrative *Tools* or *Start* -> *Administrative Tools*, depending on the Windows version.

Click on **Event Log** (1) and set policy values as follows:

- *Maximum security log size*: **4194240** kilobytes (2)
- *Retention method for security log*: **As Needed** (3)



Close the Snap-in and ensure that the policy is properly deployed.

© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.2 GPO Advanced Audit Policy Configuration

You can both enclose all settings in a single GPO or create specialized GPOs for each of the four categories shown below.

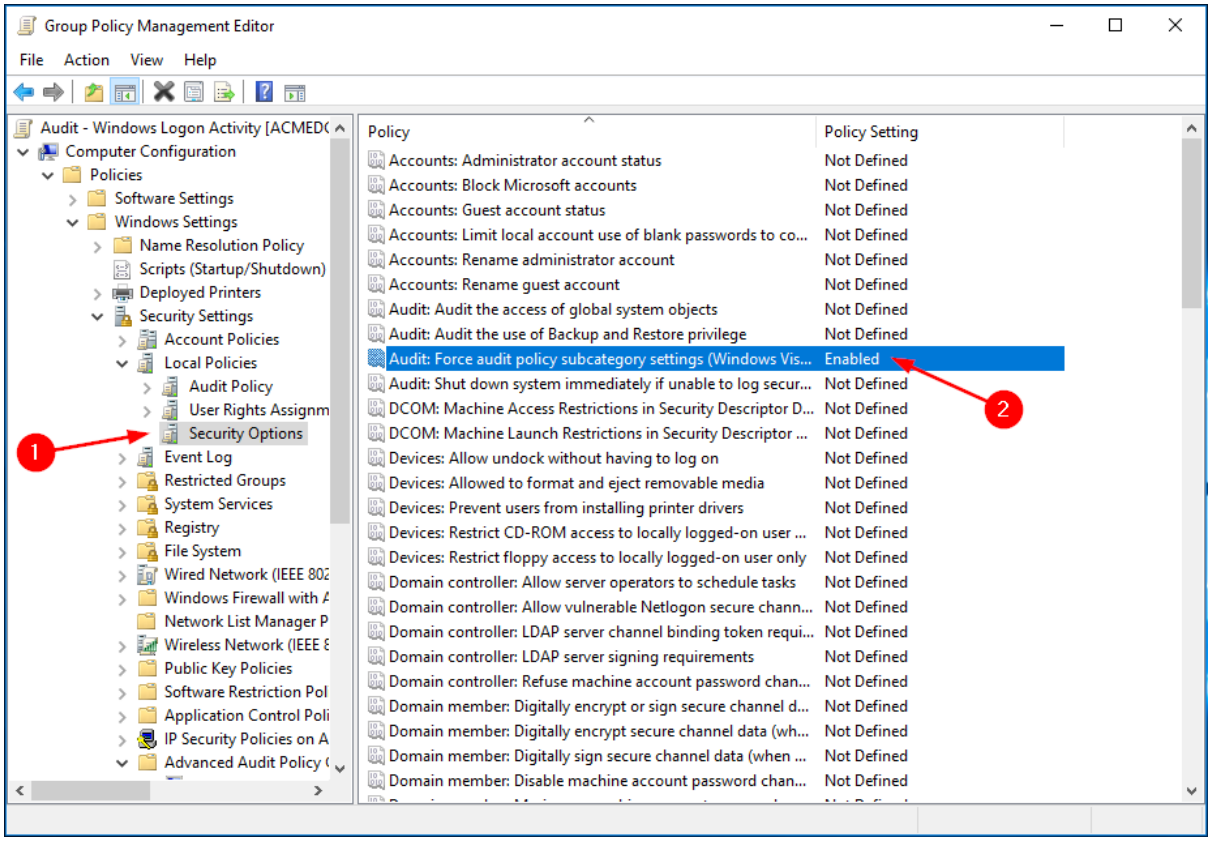
2.2.1 Logon Activity Auditing

On the Domain Controller, open the Group Policy Management snap-in located in *Start → Windows Administrative Tools* or *Start -> Administrative Tools*, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.1.1 Security Options

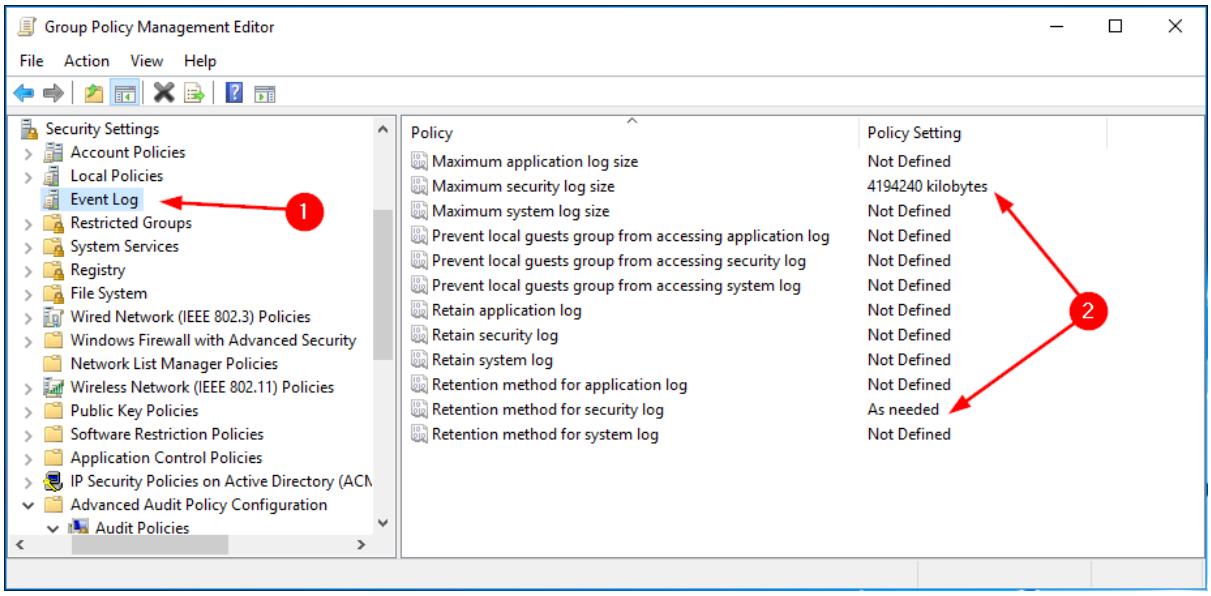
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy* click on **Security Options** (1) and set the parameters (2) as shown in the picture.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

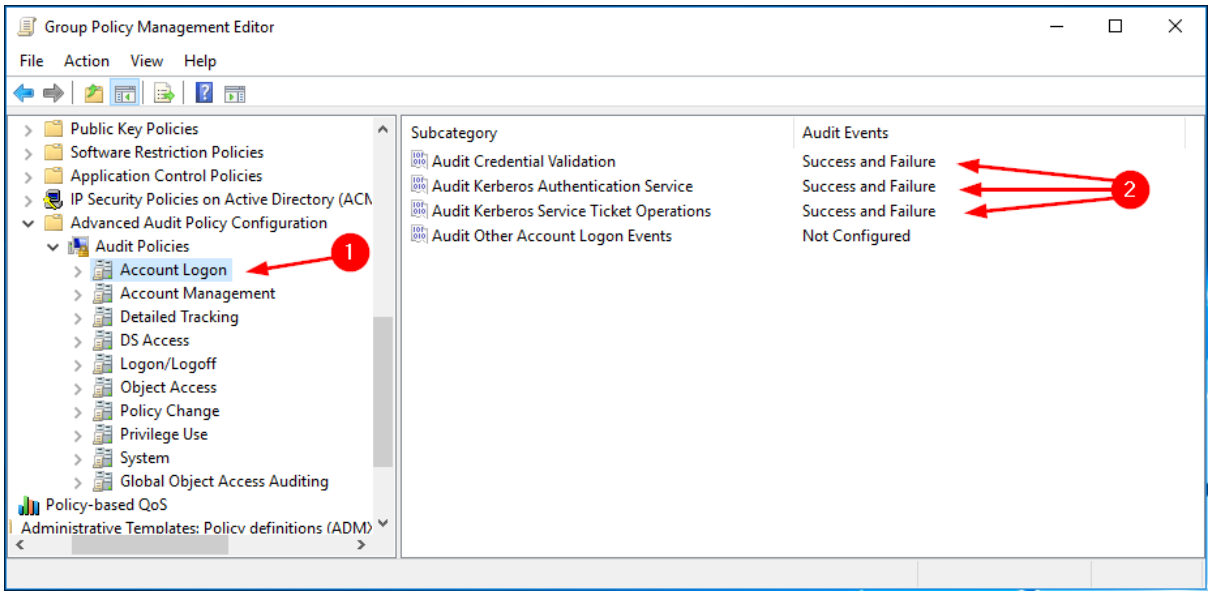
2.2.1.2 Event Log

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings*, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.1.3 Account Logon

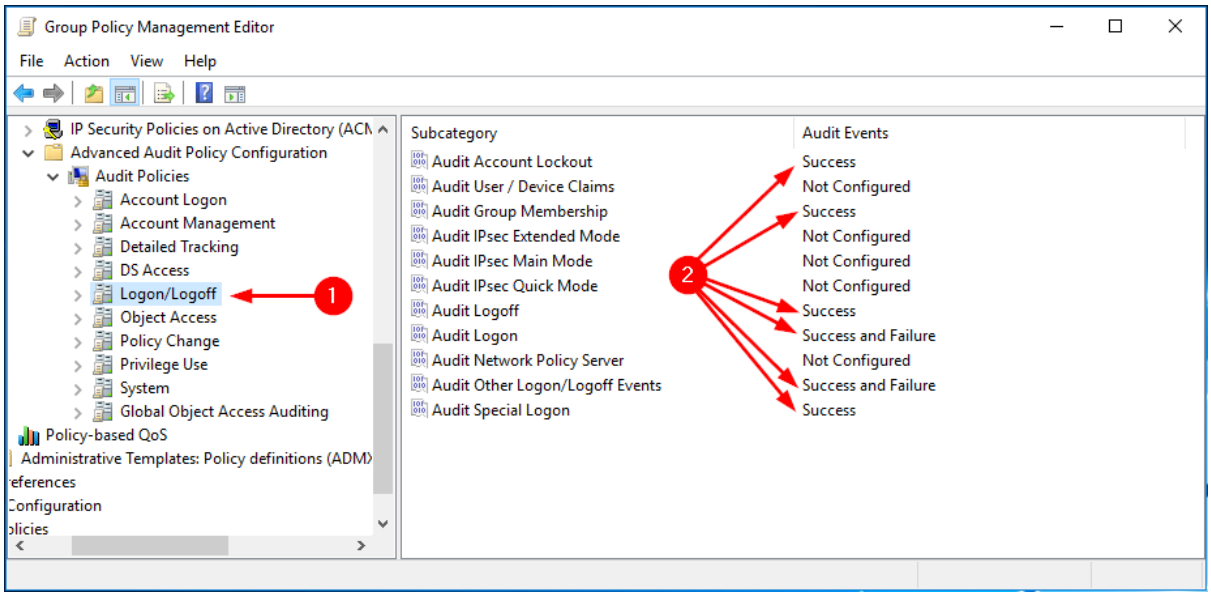
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **Account Logon** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

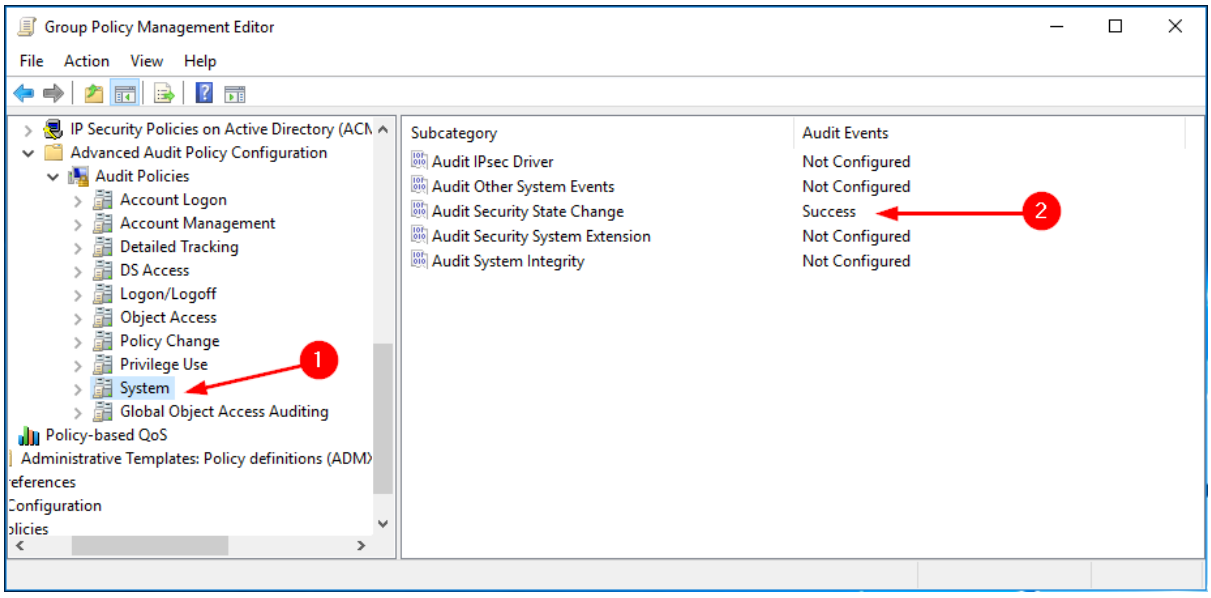
2.2.1.4 Logon/Logoff

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* click on **Logon/Logoff** (1) and configure parameters (2) as shown in the figure.



2.2.1.5 System

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **System** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

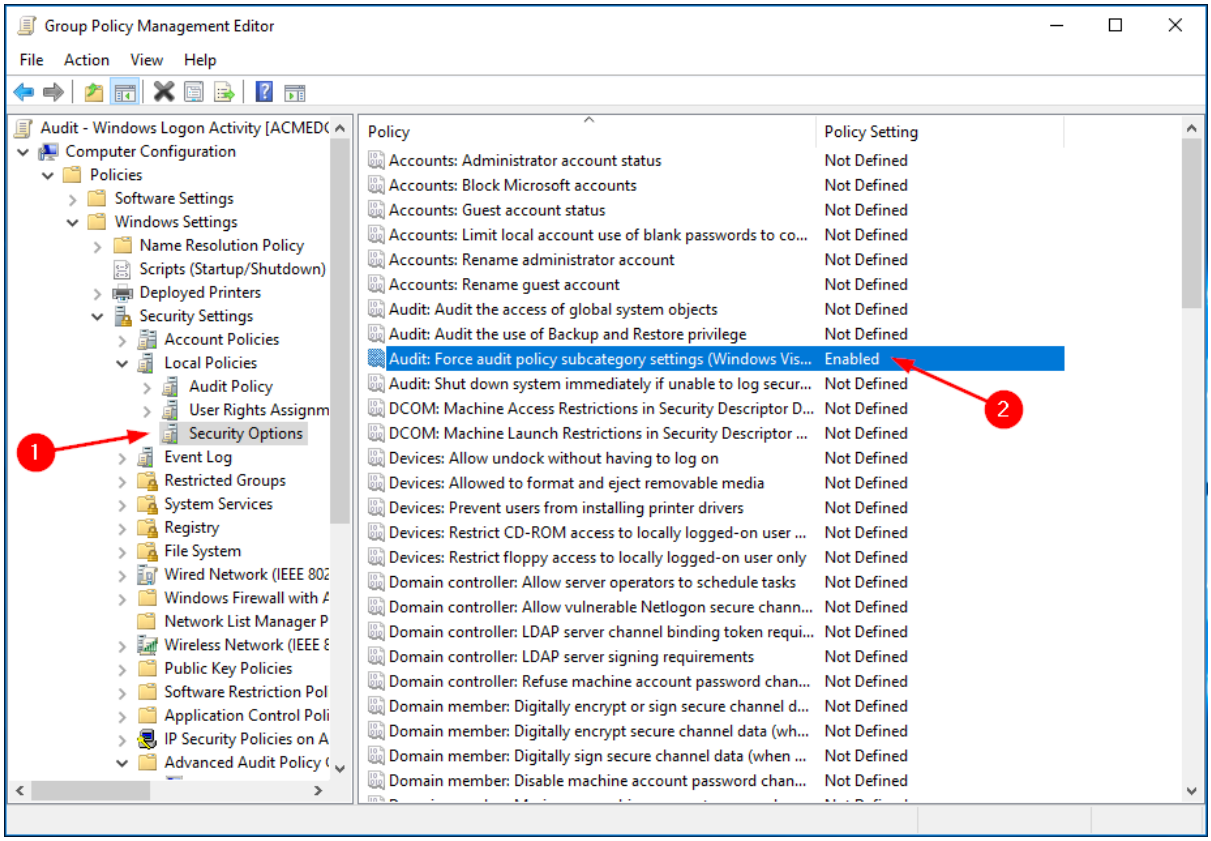
2.2.2 Domain Controller Auditing

On the Domain Controller, open the Group Policy Management snap-in located in *Start* → Windows Administrative *Tools* or *Start* -> *Administrative Tools*, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.2.1 Security Options

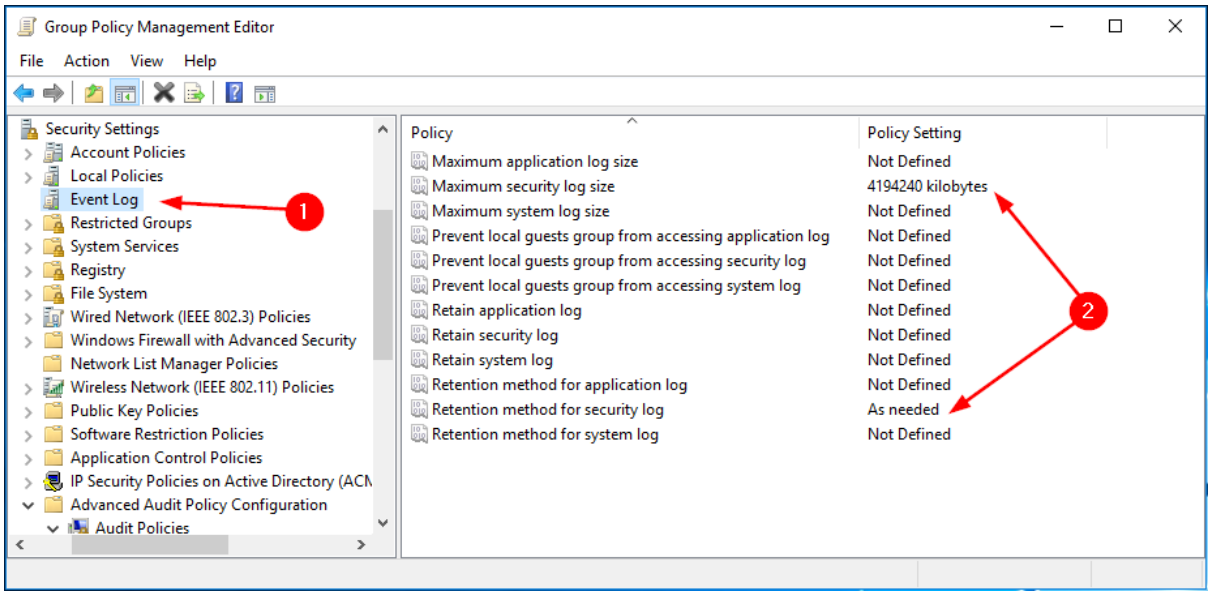
From *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Local Policy*, click on **Security Options** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

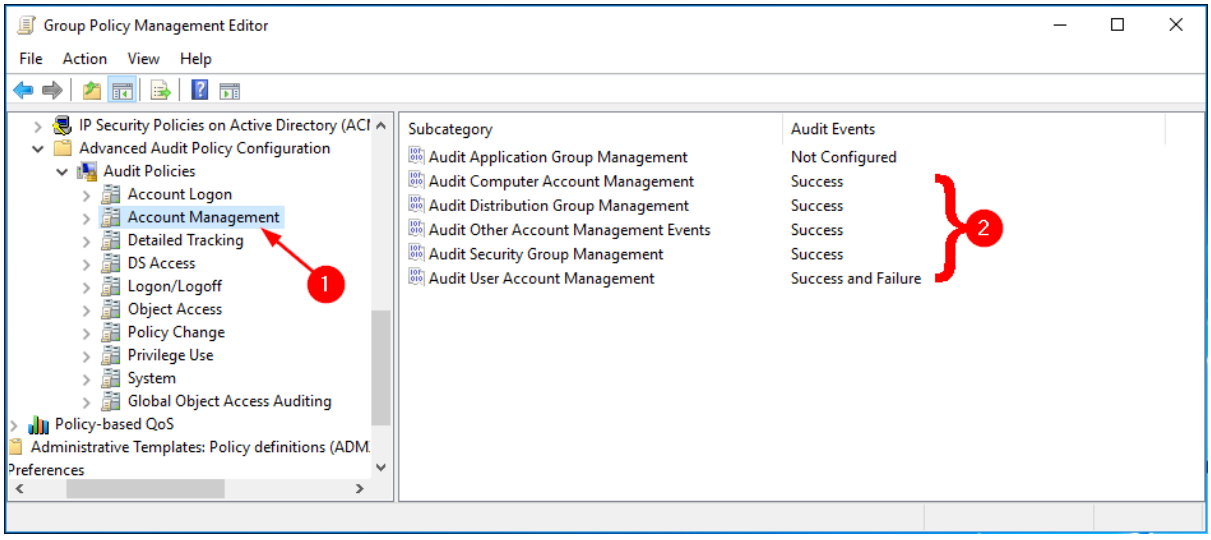
2.2.2.2 Event Log

From Computer Configuration -> Policies -> Windows Settings -> Security Settings, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.2.3 Account Management

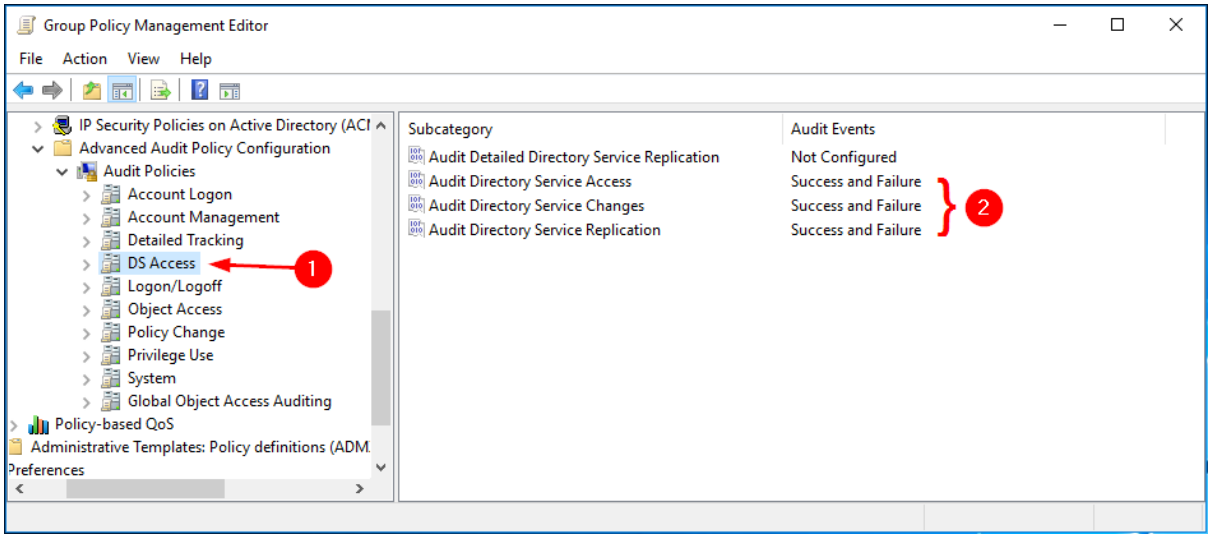
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **Account Management** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.2.2.4 DS Access

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **DS Access** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

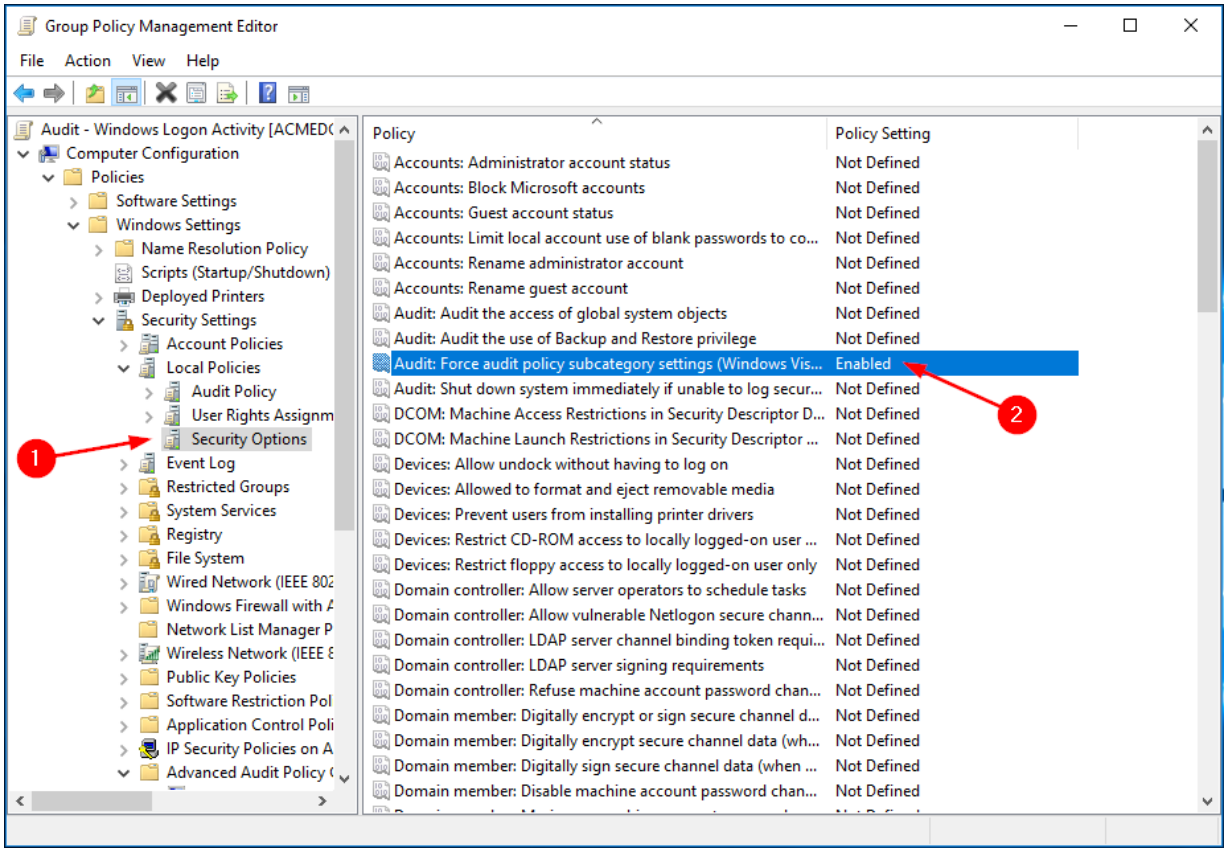
2.2.3 File Server Auditing

On the Domain Controller, open the Group Policy Management snap-in located in *Start → Windows Administrative Tools or Start -> Administrative Tools*, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.3.1 Security Options

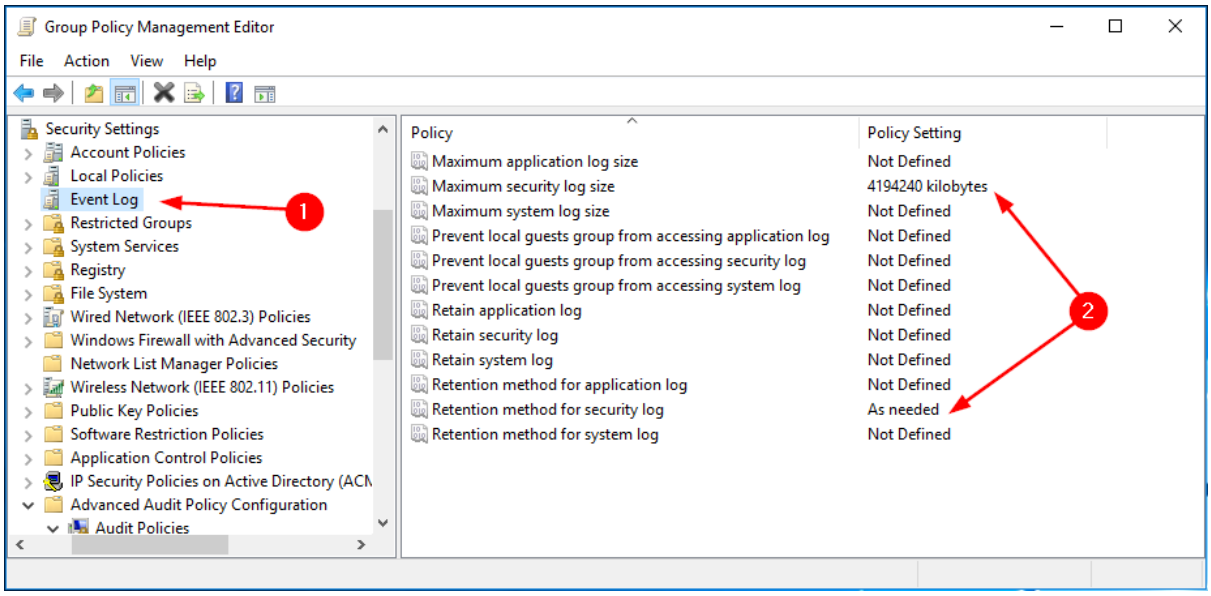
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy*, click on **Security Options** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

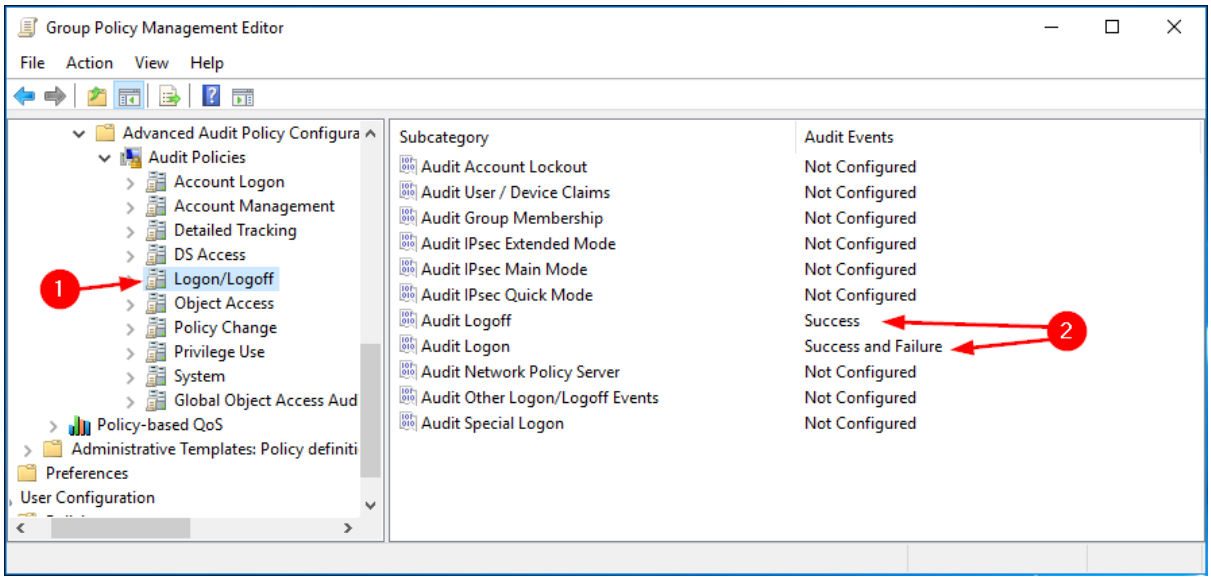
2.2.3.2 Event Log

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings*, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.3.3 Logon/Logoff

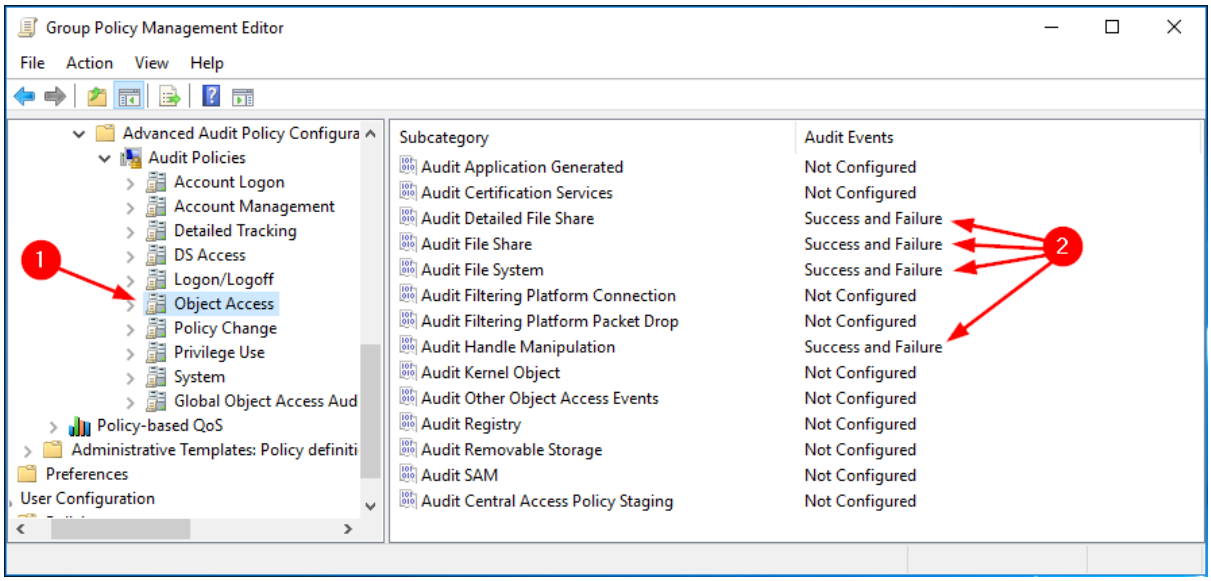
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* click on **Logon/Logoff** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

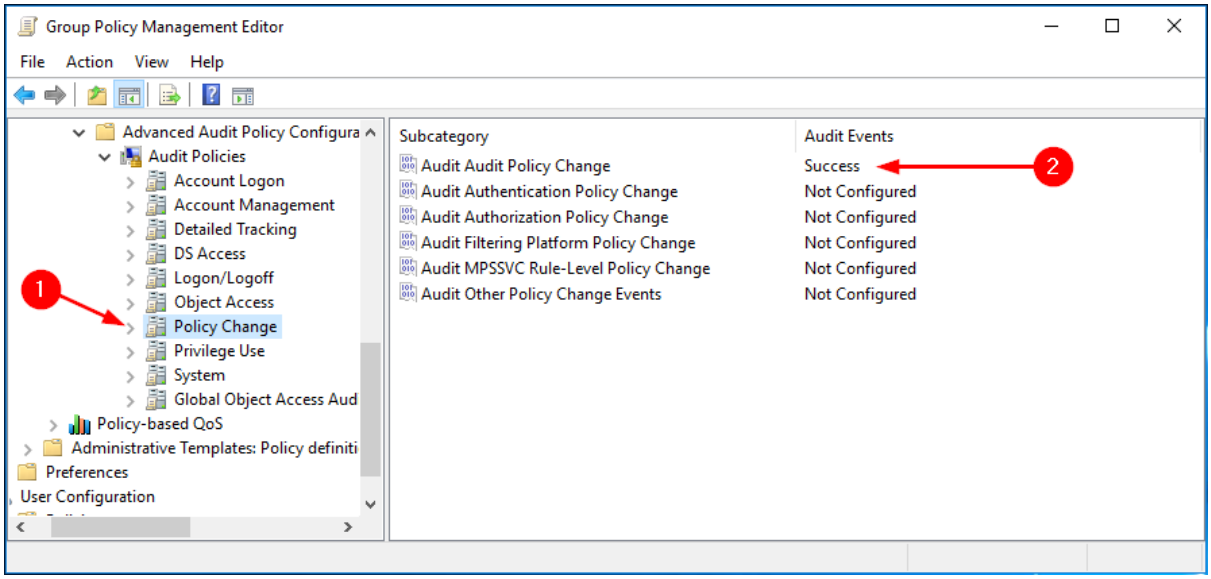
2.2.3.4 Object Access

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Object Access** (1) and configure parameters (2) as shown in the figure.



2.2.3.5 Policy Change

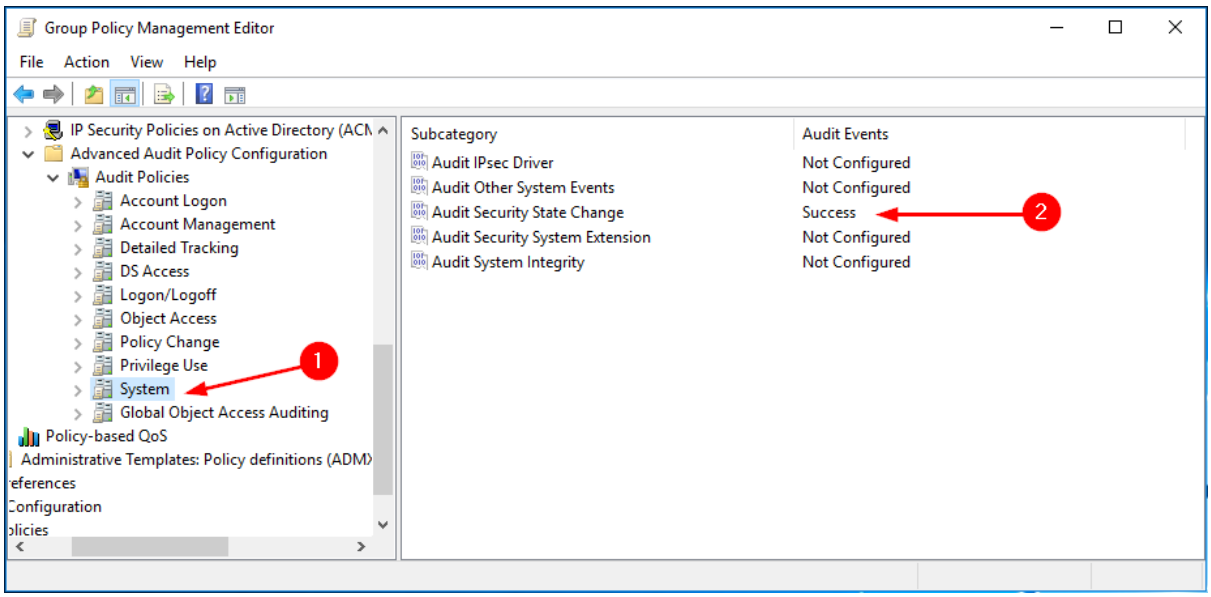
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Policy Change** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.2.3.6 System

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* click on **System** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

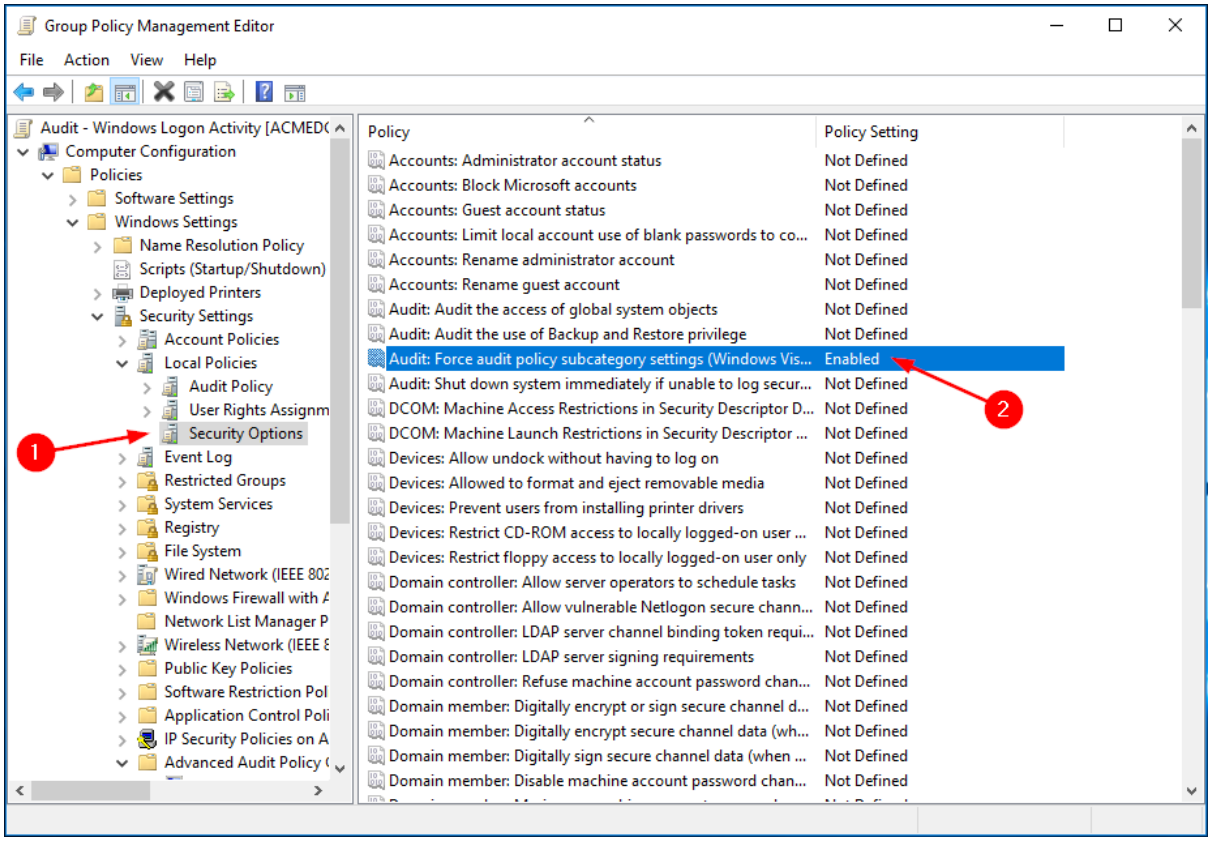
2.2.4 Windows Servers and Workstation Auditing

On the Domain Controller, open the Group Policy Management snap-in located in *Start → Windows Administrative Tools or Start -> Administrative Tools*, depending on the Windows version.

Create a category-specific GPO, or use a general gpo, and configure the various options as follows.

2.2.4.1 Security Options

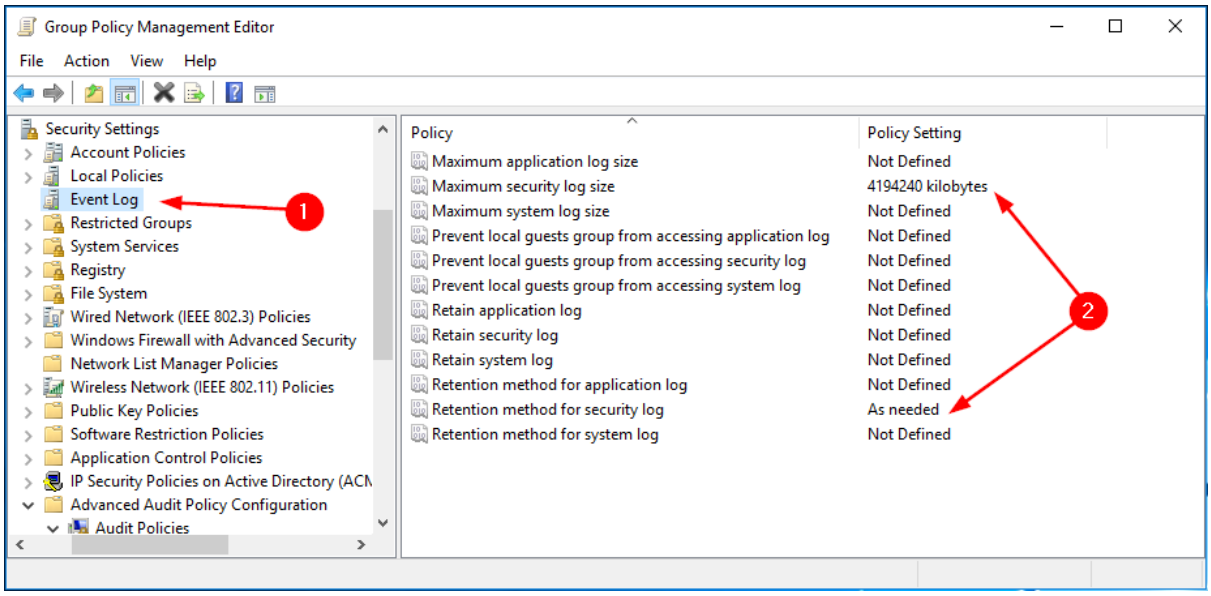
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy*, click on **Security Options** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

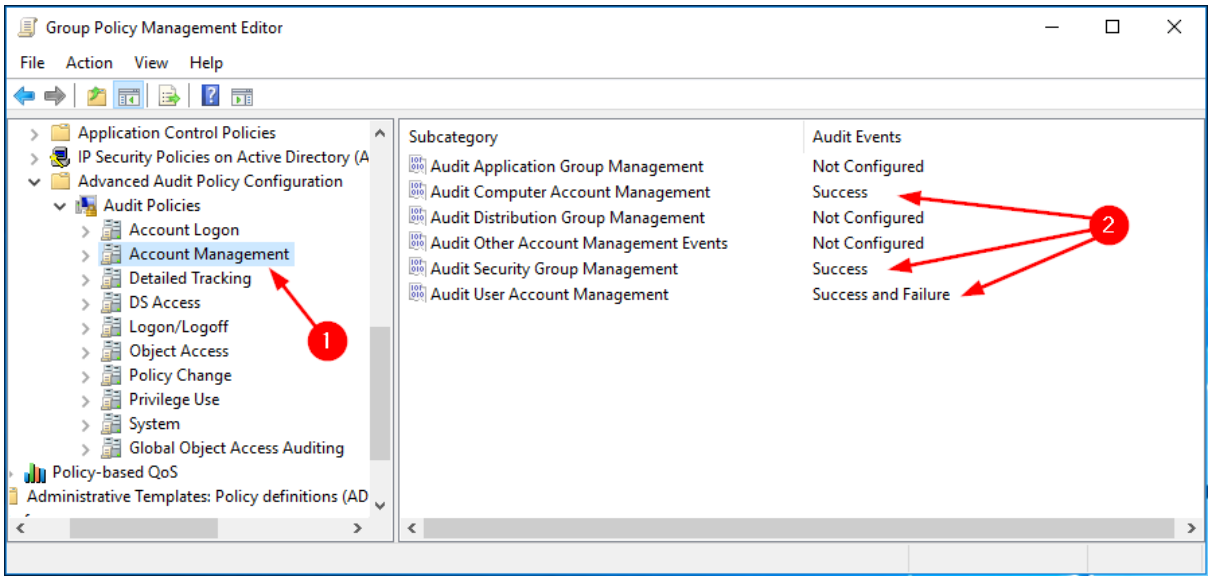
2.2.4.2 Event Log

From Computer Configuration -> Policies -> Windows Settings -> Security Settings, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.4.3 Account Management

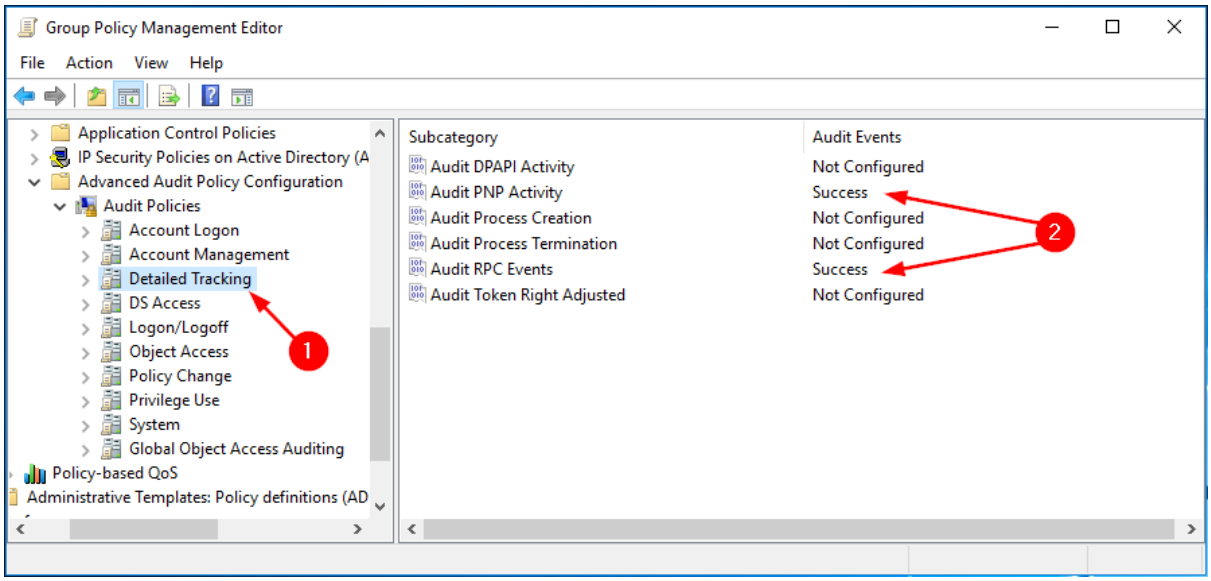
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* click on **Account Management** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

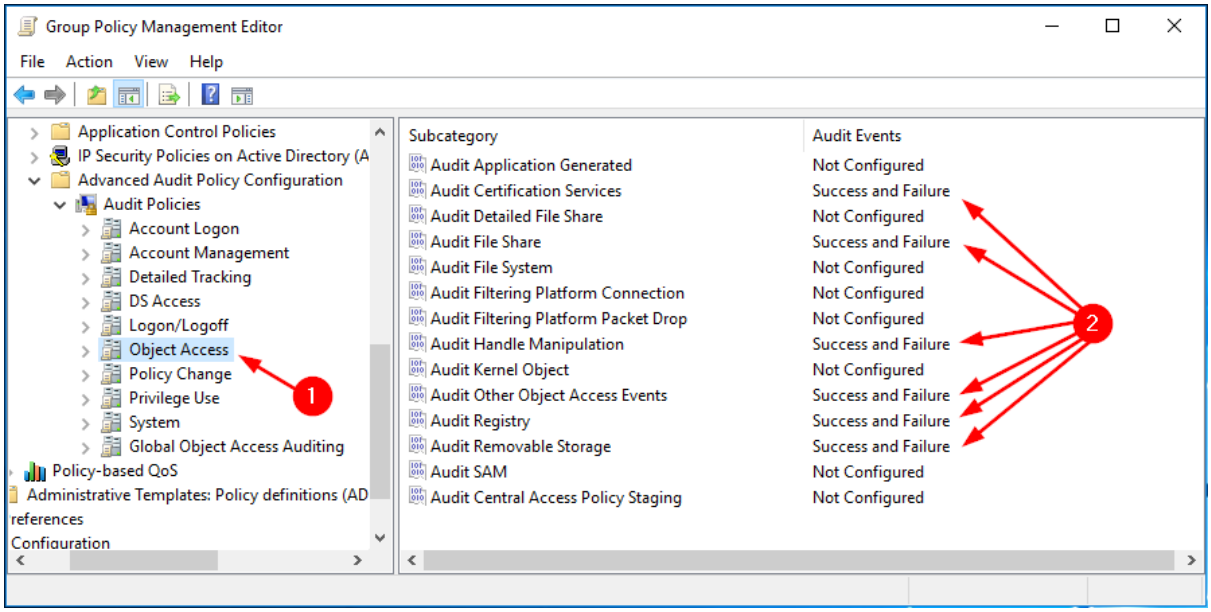
2.2.4.4 Detailed Tracking

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Detailed Tracking** (1) and configure parameters (2) as shown in the figure.



2.2.4.5 Object Access

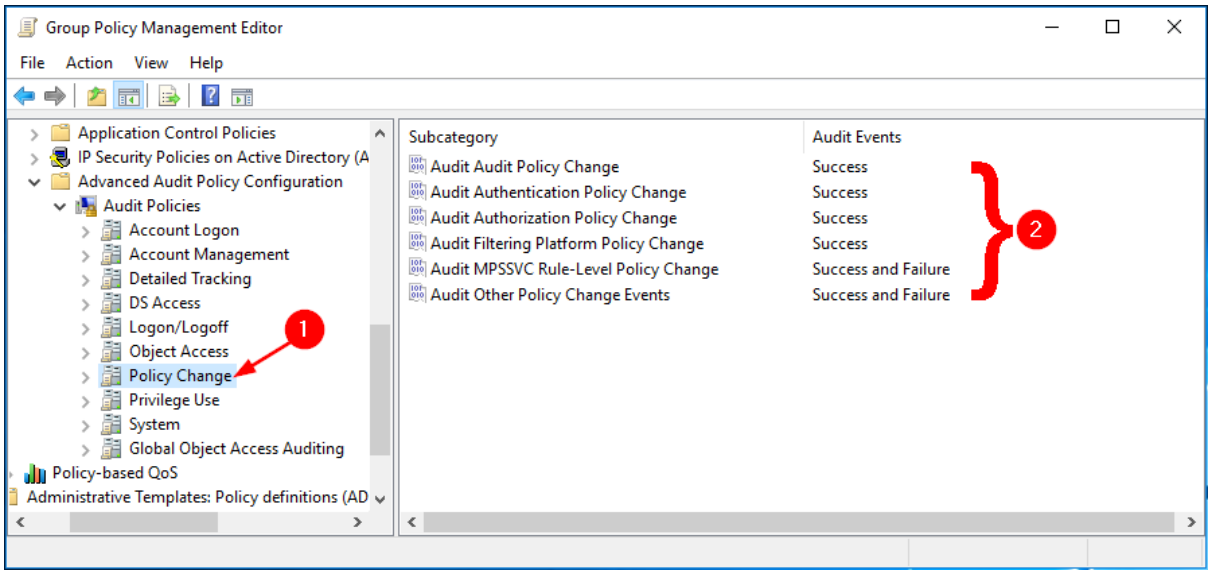
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Object Access** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

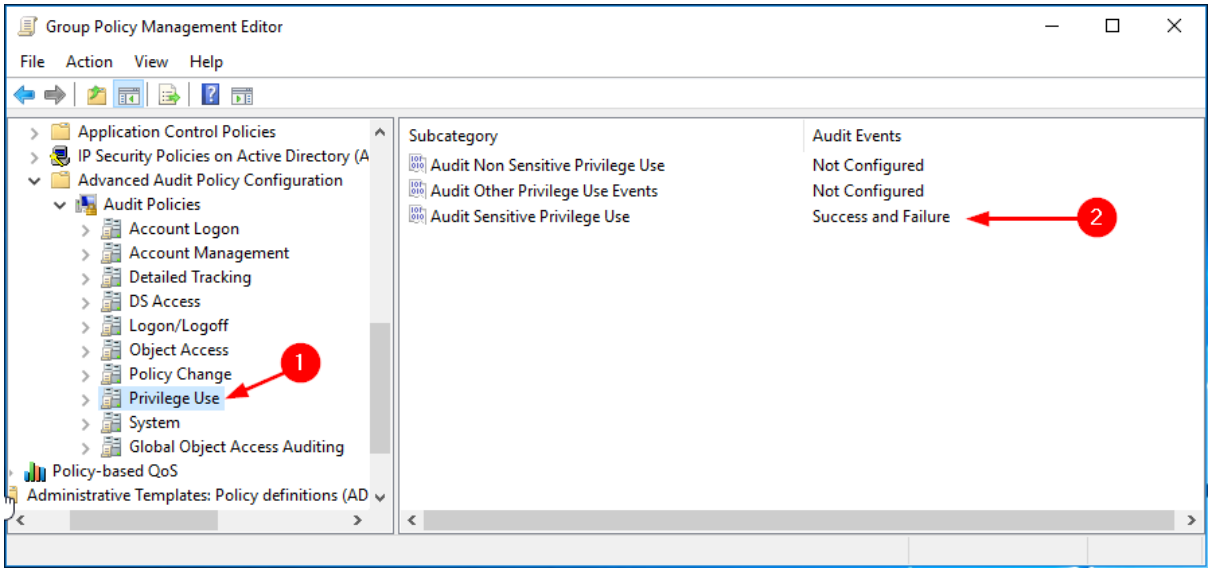
2.2.4.6 Policy Change

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Policy Change** (1) and configure parameters (2) as shown in the figure.



2.2.4.7 Privileged Use

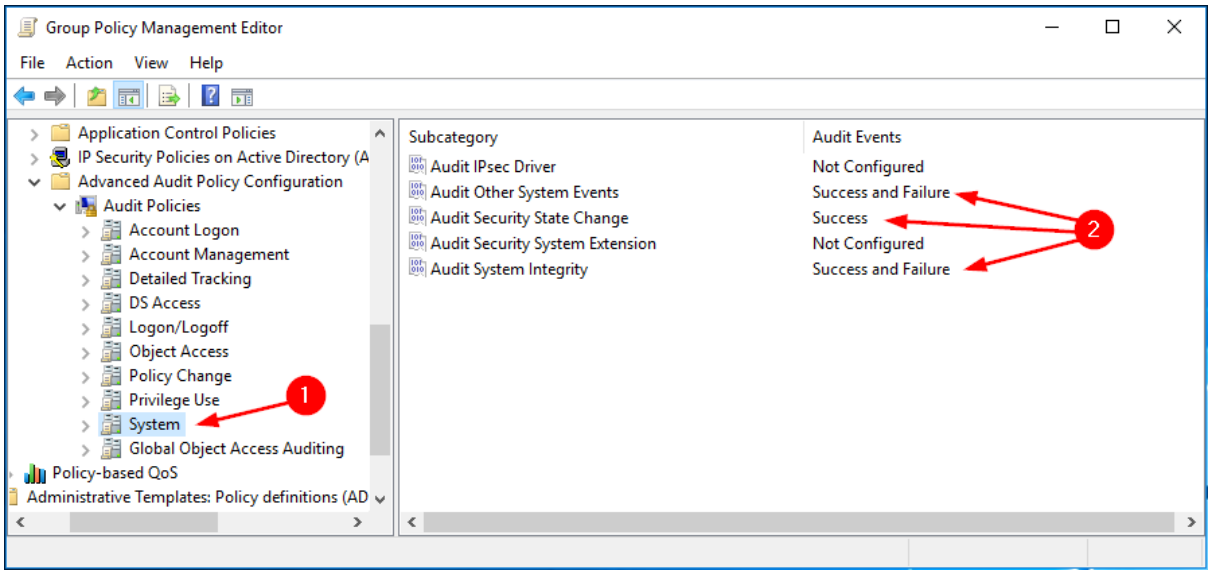
From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Privileged Use** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

2.2.4.8 System

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **System** (1) and configure parameters (2) as shown in the figure.



© Copyright SecureGate S.r.l. 2022 – All rights reserved

3 Object-level access auditing configuration

3.1 Active Directory Windows Server 2012 and higher

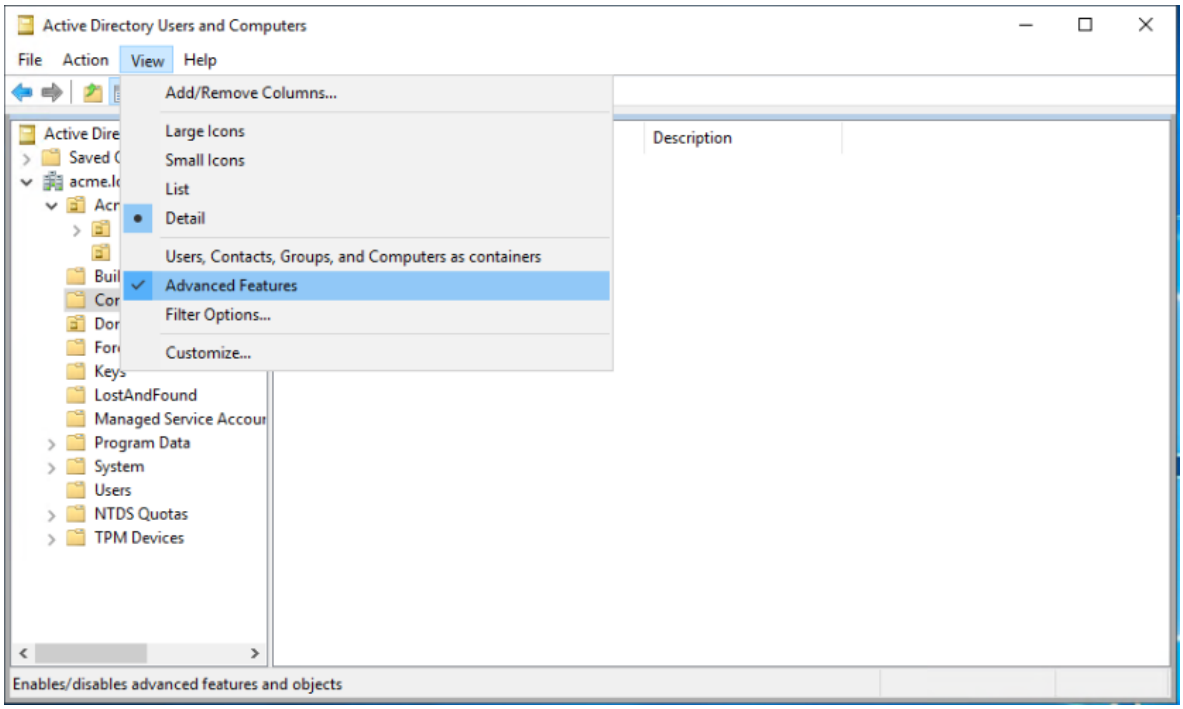
If you want to collect information on user activity in the domain, it is necessary to configure Object-level auditing for the Domain partition also.

If you also want to check for changes to the AD Configuration and Schema, you must also enable Object-level auditing for Configuration and Schema partitions.

Please follow the procedure below for each Domain or Organizational Unit you wish to control.

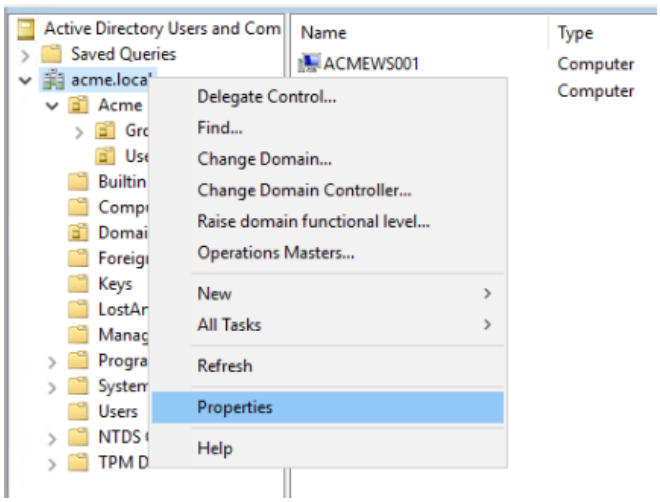
1) From any Domain Controller belonging to the Domain you want to control, open the **Active Directory Users and Computers** snap-in located in *Start → Windows Administrative Tools* or in *Start -> Administrative Tools*, depending on the Windows version.

   Click on the **View** tab and verify that **Advanced Features** is selected.



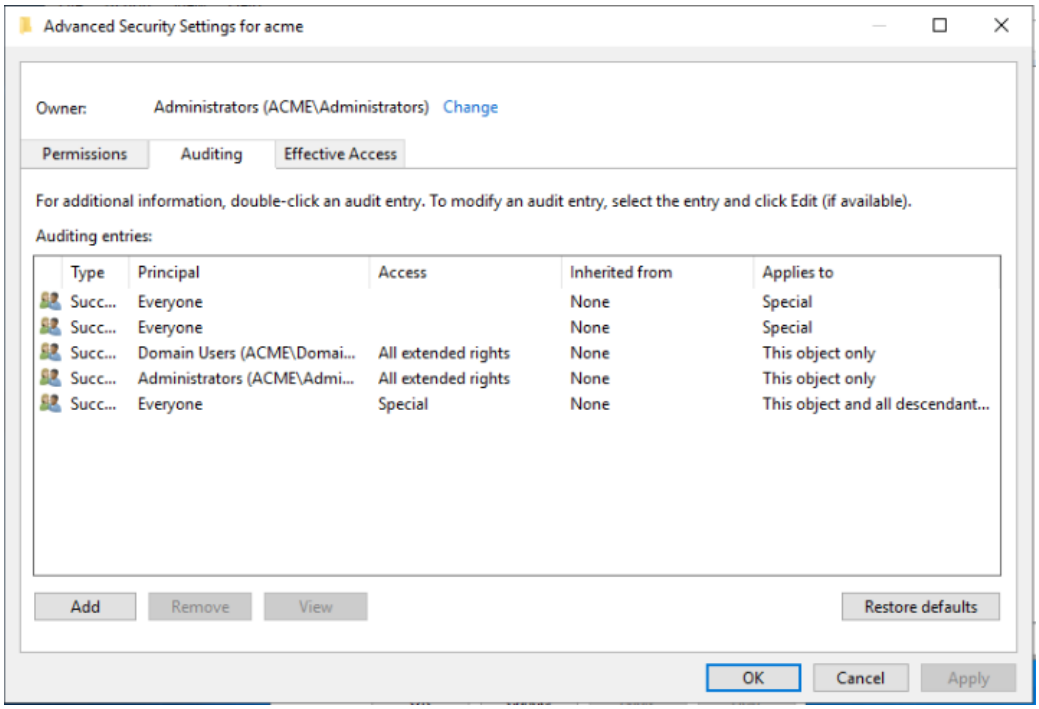
© Copyright SecureGate S.r.l. 2022 – All rights reserved

2) Right click on the Domain node you want to control and select **Properties**.



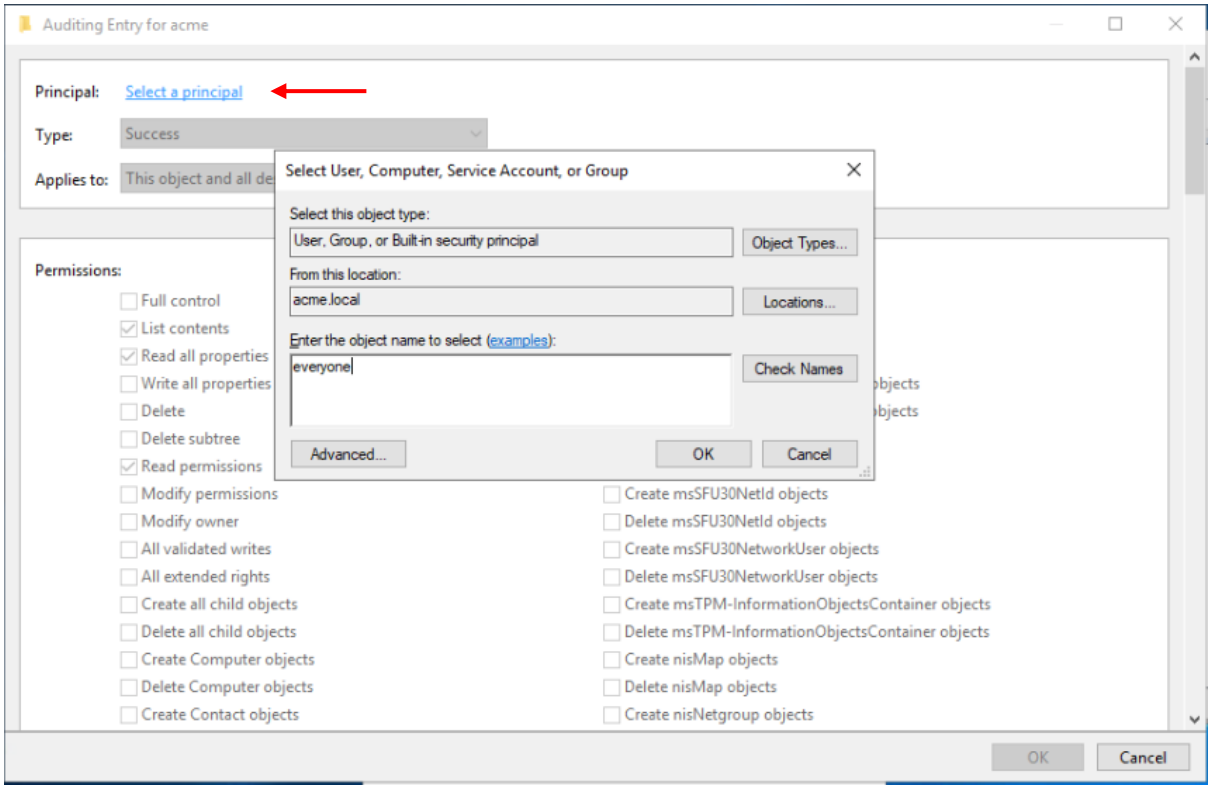
3) Within the Propertis panel select the **Security** tab then click on the button **Advanced** in the lower right corner.

4) In the "Advanced Security Settings" panel select the **Auditing** tab.



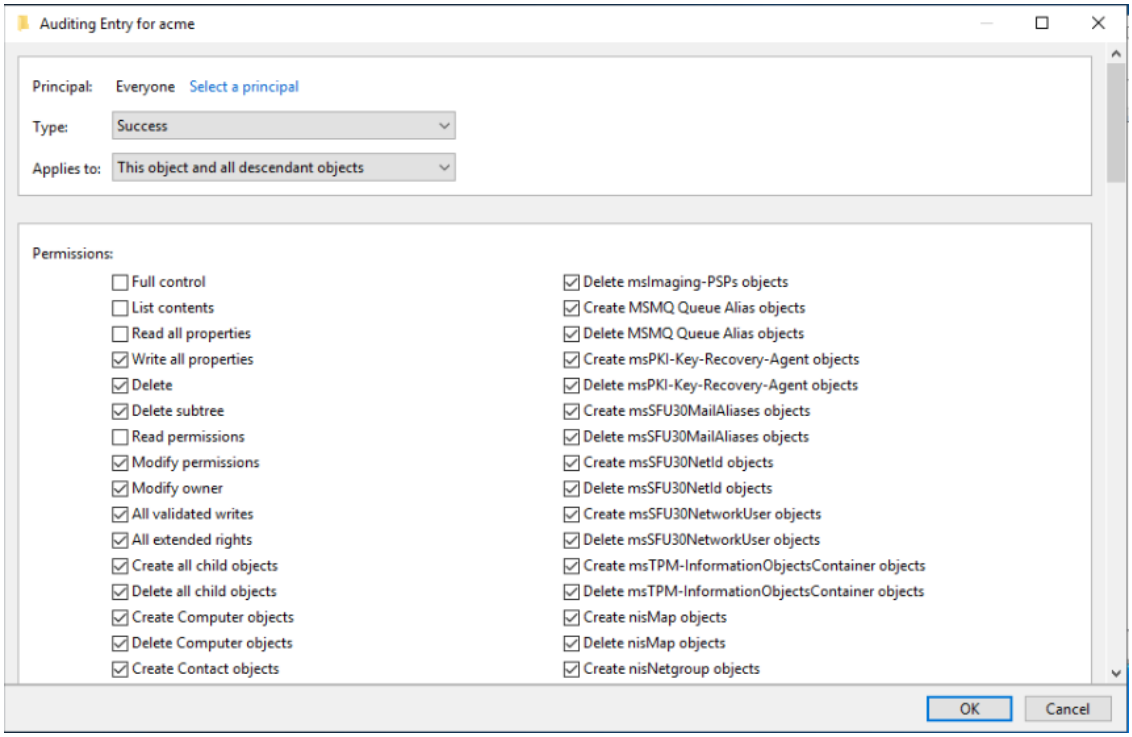
Click on the **Add** button and then, within the "Auditing Entry" panel, select the **Select a principal** link.

© Copyright SecureGate S.r.l. 2022 – All rights reserved



5) In the "Select User, Computer, Service Account, or Group" panel type **everyone** in the **Enter the object name to select** field, then confirm clicking the **OK** button.

Back in the "Auditing Entry" panel, set the **Type:** field to "*Success*" and the **Applies to:** field on "*This object and all descendant objects*".



© Copyright SecureGate S.r.l. 2022 – All rights reserved

6) In the **Permissions** box, select all the checkboxes but the following:

   - Full Control
   - List Contents
   - Read All Properties
   - Read Permissions

7) Check that at the end of the Permission box, the checkbox **Only apply these auditing settings to objects and/or containers within this container** is not selected and click the **OK** button to confirm changes.

© Copyright SecureGate S.r.l. 2022 – All rights reserved

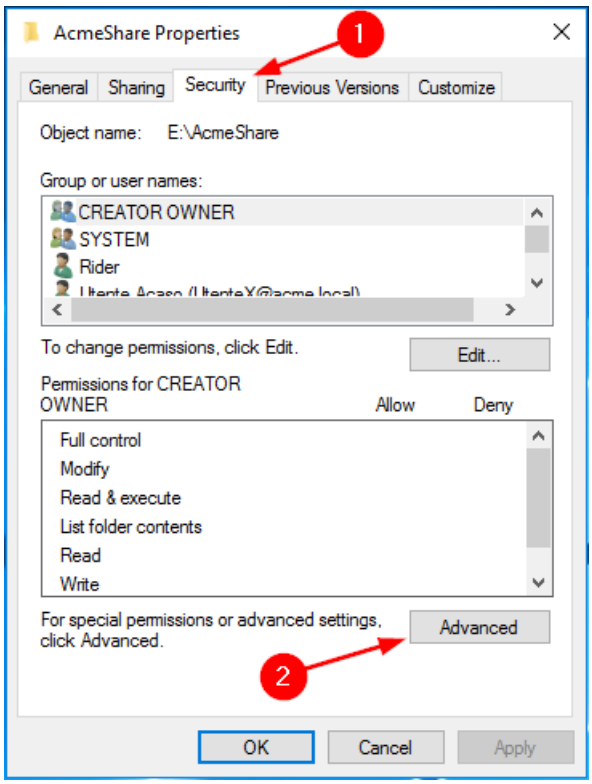
3.2 Windows File Server 2012 and higher

Object-level access auditing configuration is essential to be able to collect audit events generated by the Advanced Audit Policy specified above.

By configuring Object-level access auditing we will specify which event classes to collect and which users to monitor.

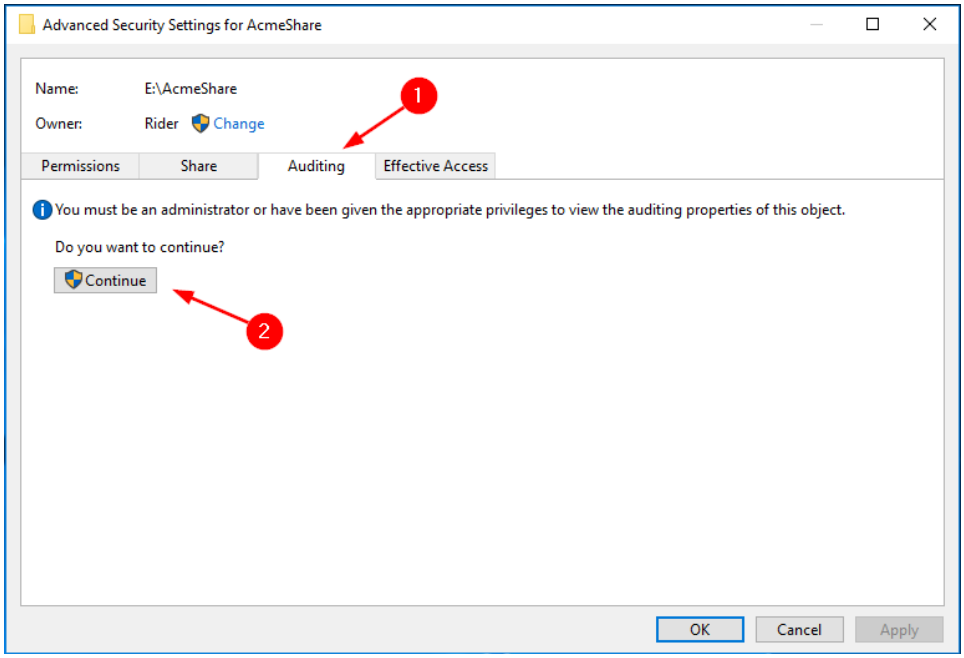
Follow these steps for each folder or disk that you want to monitor.

1) Right-click the folder you want to monitor and select **Properties** from the pop-up menu. Select the **Security** tab (1) and then click **Advanced** (2).

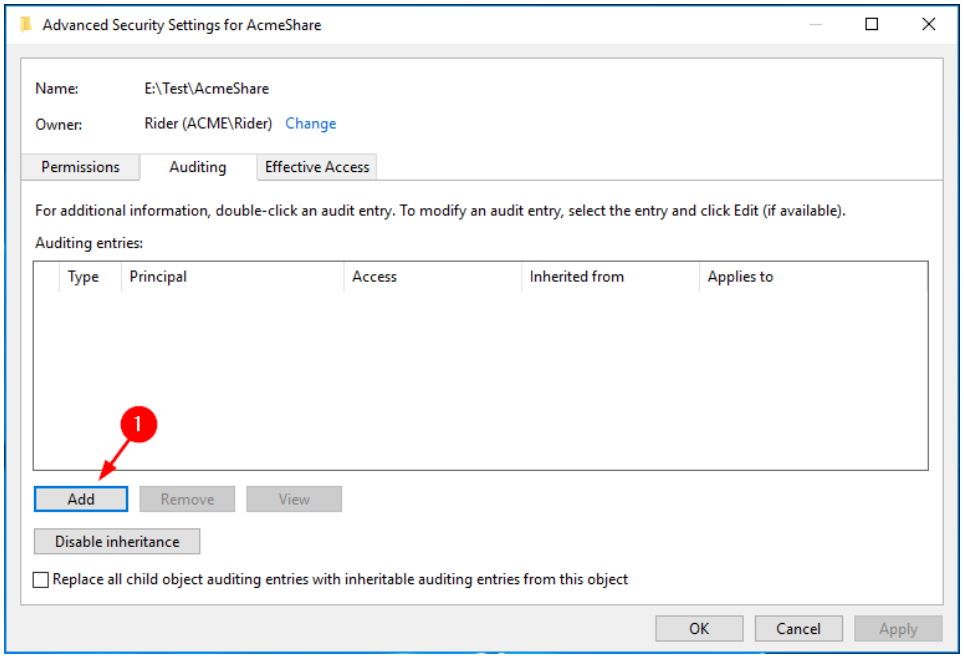


© Copyright SecureGate S.r.l. 2022 – All rights reserved

2) Select the **Auditing** tab and click **Continue** (2)

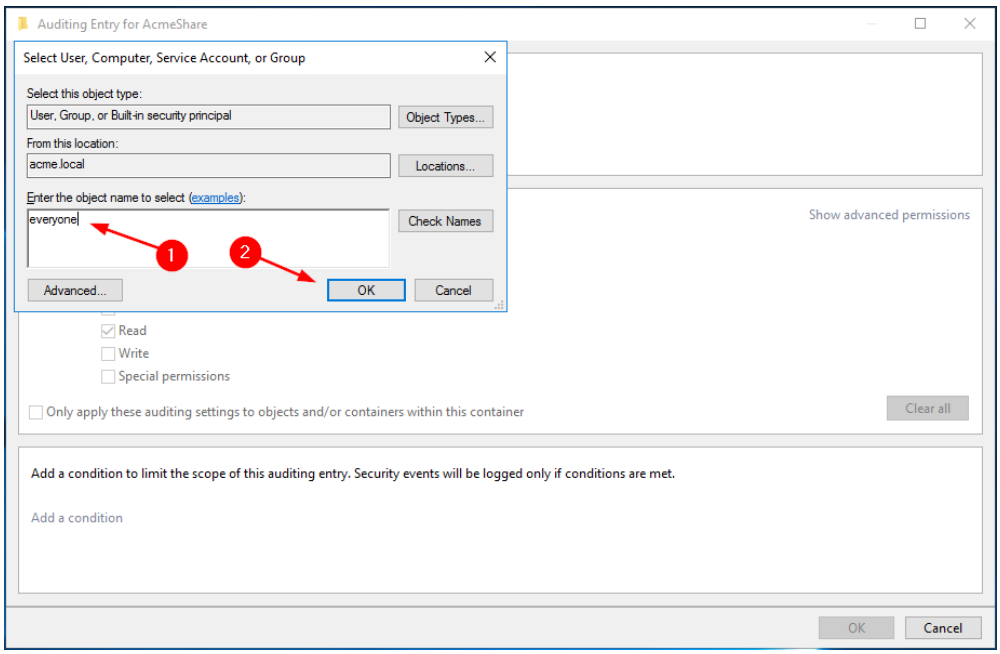


3) click the **Add** button (1) to add a new auditing permission configuration.



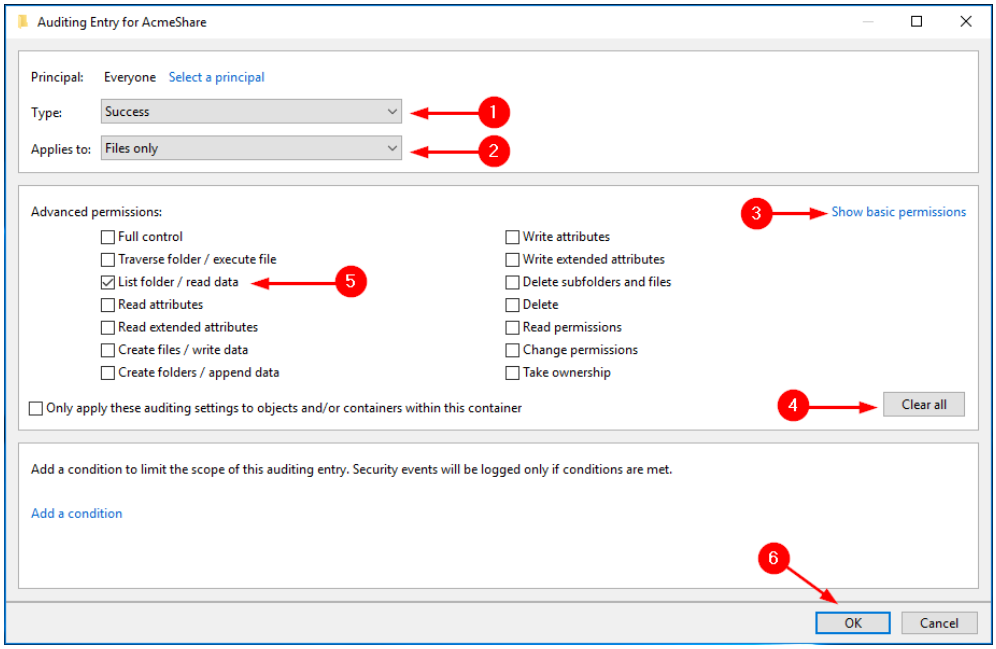
© Copyright SecureGate S.r.l. 2022 – All rights reserved

4) Click the **Select a principal** link in the top-left corner to add a new principal. Then select **Everyone** (1), or any custom group that contains the users for whom you want to monitor access.



You can now set the audit entries for the access types you want to control. The configurations needed are shown below:

5) Read access succeeded



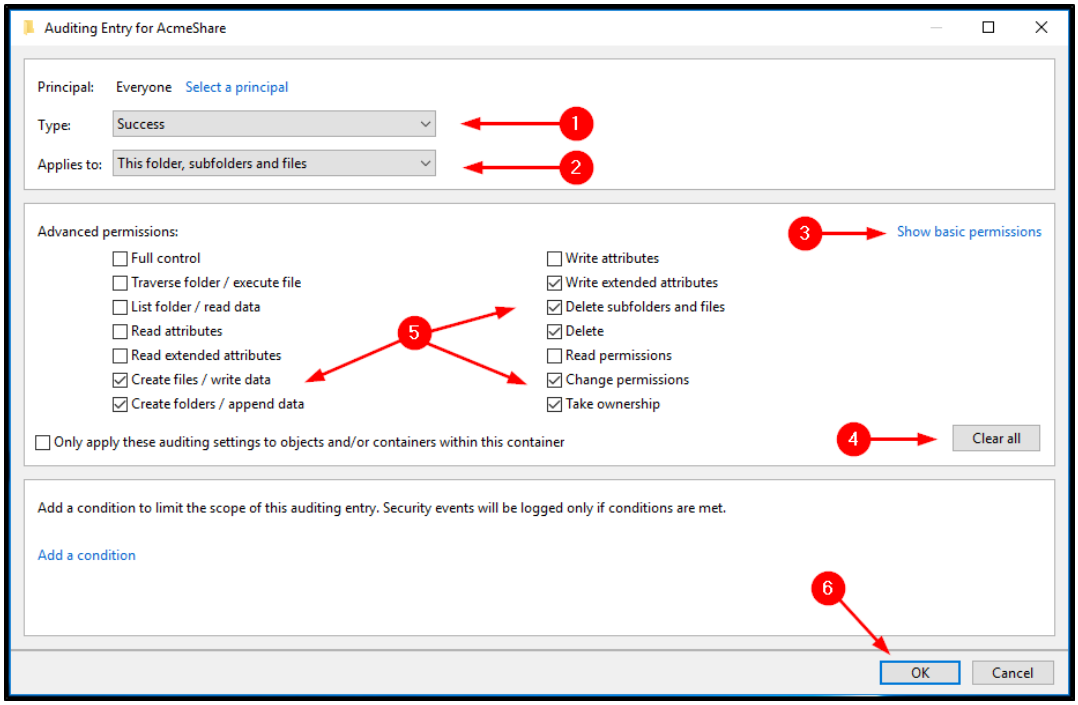
- Set **Type:** -> Success (1)
- Set **Applies to:** -> File Only (2)
- Click the link **Show Advanced Permissions** (3)

© Copyright SecureGate S.r.l. 2022 – All rights reserved

- Click the **Clear All** button (4) to clear all preset permissions
- Select the following permissions (5)
    - List folder / read data
- Press the **OK** button (6) to save the configuration

6) Successful edit access

Repeat steps 3 and 4 to create a new permission set and set it as follows:

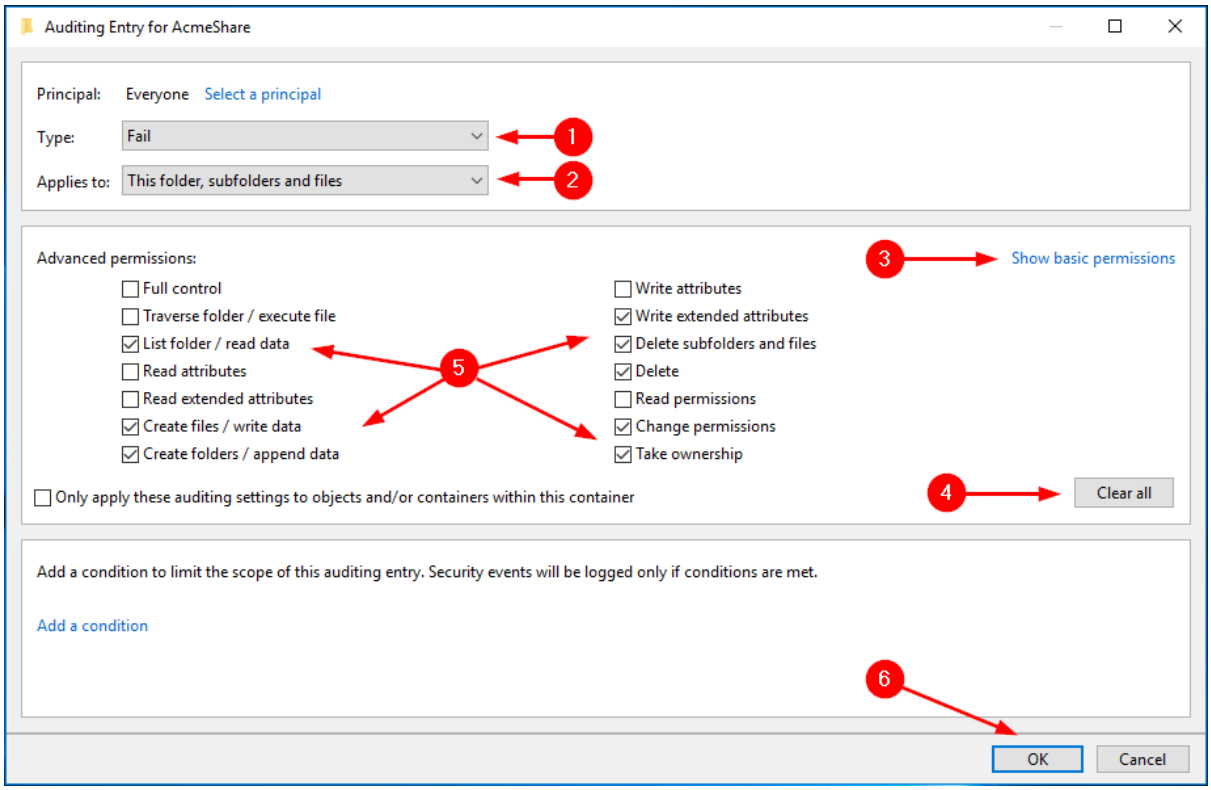


- Set **Type:** -> Success (1)
- Set **Applies to:** -> This folder, subfolders, and files (2)
- Click the link **Show Advanced Permissions** (3)
- Click the **Clear All** button (4) to clear all preset permissions
- Select the following permissions (5)
    - Create files / write data
    - Create folders / append data
    - Write extended attributes
    - Delete subfolders and files
    - Delete
    - Change permissions
    - Take ownership
- Press the **OK** button (6) to save the configuration

© Copyright SecureGate S.r.l. 2022 – All rights reserved

7) Read or Edit access failed

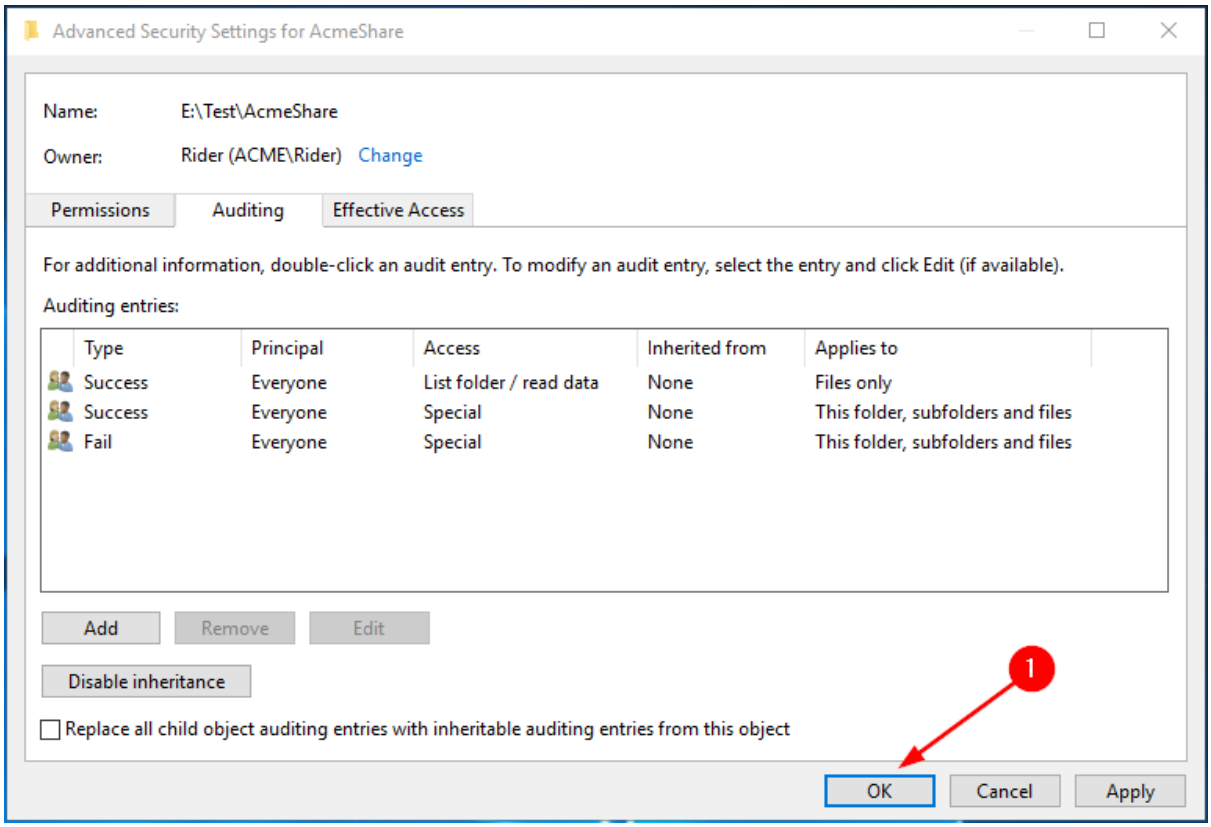
Repeat steps 3 and 4 to create a new permission set and set as follows:



- Set **Type**: -> Fail (1)
- Set **Applies to:** -> This folder, subfolders, and files (2)
- Click the link **Show Advanced Permissions** (3)
- Click the **Clear All** button (4) to clear all preset permissions
- Select the following permissions (5)
    - List folder / read data
    - Create files / write data
    - Create folders / append data
    - Write extended attributes
    - Delete subfolders and files
    - Delete
    - Change permissions
    - Take ownership
- Press the **OK** button (6) to save the configuration

© Copyright SecureGate S.r.l. 2022 – All rights reserved

8) After the configurations, click the **OK** button (1) to save and apply the set permissions.



© Copyright SecureGate S.r.l. 2022 – All rights reserved