# Configuring Audit Policies

Planning is an important step in the auditing process. Administrators should be selective in determining the objects to audit. Auditing creates system overhead, therefore auditing too many objects will cause the security log to become large and difficult to manage.

Before audit records are logged, an auditing policy must be established. The policy defines the types of events that will be audited for a specific user or group of users. However, enabling the auditing policy is only part of the work associated with setting up auditing. Auditing implementation has several steps:

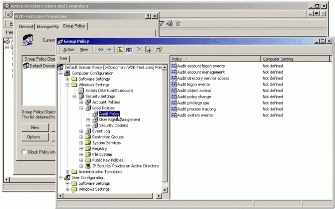
1. Enable auditing on the domain controller.
2. Select objects to audit, and set the system access control lists (SACL) for the objects.
3. Configure the event log.
4. Protect the audit data from unauthorized access or modification.
5. Review and maintain the audit logs.

This subsection deals only with steps one and two; all other aspects of audit management are addressed in the Audit Management subsection of this document.

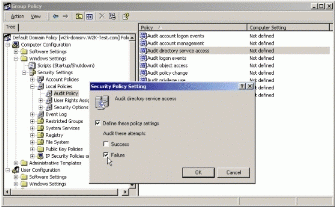
An auditing policy specifies categories of security-related events that must be audited. When Windows 2000 is first installed, all auditing categories are turned off. By turning on various auditing event categories, the administrator can implement an auditing policy that suits the security needs of the organization.

Auditing can be enabled on the Domain Controller as follows:

1. Log on using an administrator account.
2. Open the **Active Directory Users and Computers** tool.
3. Right-click the container holding the domain controller and click **Properties**.
4. Click the **Group Policy** tab, and then click **Edit** to edit the **Default Domain Policy**.
5. In the **Group Policy** window, expand **Computer Configuration**, navigate to **Windows Settings**, to **Security Settings**, and then to **Local Policies**.
6. Select **Audit Policy**.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab028_big(l=en-us).gif)

1. As an example, double-click **Audit Directory Service Access** policy and choose to enable or disable successful or failed access attempts.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab029_big(l=en-us).gif)

1. Click **OK**. It will take a few minutes for the change to take effect, and other domain controllers will receive the change at the next regular replication interval.

Best Practices for Auditing

To minimize the risk of several specific security threats, the administrator can take various auditing steps. The administrator should select the events to be audited considering the set of threats specific to the environment. The following table provides an example of various events that could be audited, as well as the specific security threat that the audit event monitors.

|  |  |
| --- | --- |
| **Audit Event** | **Potential Threat** |
| Failure audit for logon/logoff | Random password hack |
| Success audit for logon/logoff | Stolen password break-in |
| Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events | Misuse of privileges |
| Success and failure audit for file-access and object-access events. File Manager success and failure audit of Read/Write access by suspect users or groups for the sensitive files. | Improper access to sensitive files |
| Success and failure audit for file-access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers. | Improper access to printers |
| Success and failure write access auditing for program files (.EXE and .DLL extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log. | Virus outbreak |

Appendix B – Audit Categories and Events, of the Windows 2000 Security Configuration Guide, contains a table that provides a cross reference of audit categories and audit events to the auditable events required in the Windows 2000 ST requirements. This can be used as a reference when implementing an audit policy that must address specific ST requirements.

[Top Of Page](https://technet.microsoft.com/en-us/library/dd277403.aspx#mainSection)

Enabling Object Auditing

If audit access to objects is chosen as part of the audit policy, either the audit directory service access category (for auditing objects on a domain controller), or the audit object access category (for auditing objects on a member server) must be also turned on. Once the correct object access category has been turned on, each individual object's **Properties** can be used to specify whether to audit successes or failures for the specific access request to each group or user.

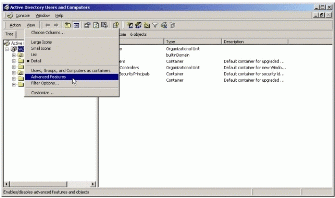
[Top Of Page](https://technet.microsoft.com/en-us/library/dd277403.aspx#mainSection)

Enabling Auditing on Directory Objects

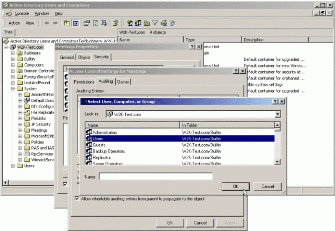
The administrator can set an auditing SACL for a directory object using the following procedure:

**Warning:** The SeSecurityPrivilege allows a user to set SACLs on objects. Administrators must ensure that this privilege is not assigned to non-administrative users.

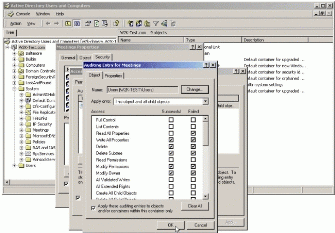
1. Log on using an administrator account.
2. Open the Active Directory Users and Computers tool.
3. On the **View** menu, select **Advanced Features**.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab030_big(l=en-us).gif)

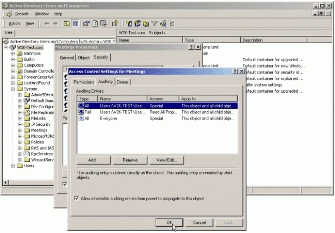
1. Locate the container for the object, right-click it, and then click **Properties**.
2. Click the **Security** tab.
3. Click **Advanced**, and click the **Auditing** tab.
4. Click the **Add**button.
5. Select a security principle name and click **OK**.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab031_big(l=en-us).gif)

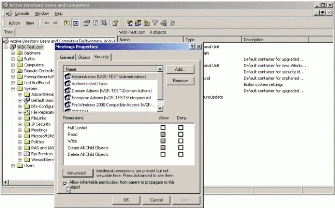
1. A dialog box will appear with two tabs—**Object** and **Properties**.
2. The **Object** tab allows the selection of generic and control rights to audit.
3. The **Properties** tab allows selection of property accesses to audit.
4. Use the pull-down lists to make selections.
5. Click each tab that needs to be modified, and select the check boxes for the accesses or properties to be audited.
6. Check the **Apply . . .** box and then click **OK**.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab032_big(l=en-us).gif)

1. In the **Access Control Settings** window, choose whether the choices will be inherited from the parent container to this object. If yes, then select the **Allow inheritable auditing entries from parent to propagate to this object** check box.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab033_big(l=en-us).gif)

1. Click **Apply**, and then click **OK**.
2. In the **Properties** window, decide whether auditing permissions must be inherited from the parent container to propagate this object. If yes, then check the appropriate box.

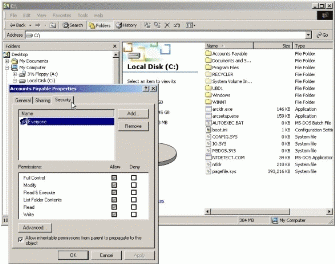
[](https://technet.microsoft.com/en-us/library/dd277403.w2kab034_big(l=en-us).gif)

1. Click **Apply** and then click **OK**.

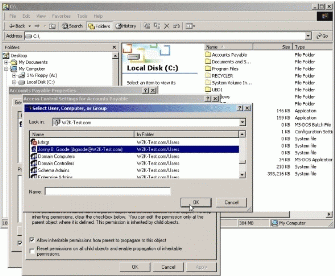
Enabling and editing Audit on Files and Folders

**To set, view, change, or remove auditing for a file or folder:**

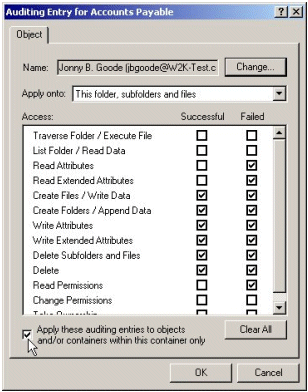
1. Open **Windows Explorer**, and then locate the file or folder to audit.
2. Right-click the file or folder, select **Properties**, and then click the **Security** tab.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab035_big(l=en-us).gif)

1. Click **Advanced**, and then click the **Auditing** tab.
2. To set up auditing for a new group or user, click **Add**.
3. In **Name**, type the user name, or select a user from the list and then click **OK** to automatically open the **Auditing Entry** dialog box.

[](https://technet.microsoft.com/en-us/library/dd277403.w2kab036_big(l=en-us).gif)

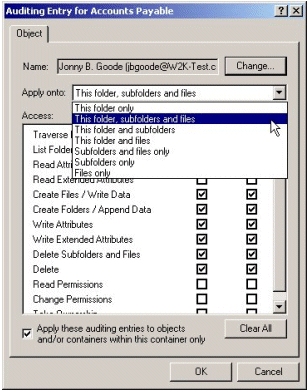
1. In the **Auditing Entry** dialog box, under **Access** click **Successful**, **Failed**, or both to select the events to be audited for this user and then check the **Apply these auditing entries to objects and/or containers within this container** selection box if it is necessary to propagate the changes to sub-containers. Click **OK** to close the **Auditing Entry** dialog box.



1. To view or change auditing for an existing group or user, simply click on the name, and then click **View/Edit**.
2. To remove auditing for an existing group or user, click the name, and then click **Remove**.

**Note:**

* If necessary, in the Auditing Entry dialog box, select where auditing is to take place in the Apply onto list. The Apply onto list is available only for folders.



* Before Windows 2000 will audit access to files and folders, the Audit Object Access setting in the Audit Policy must be enabled. If not, an error message will appear when auditing is set up for files and folders, and no files or folders will be audited. Once auditing is enabled, view the security log in Event Viewer to review successful or failed attempts to access the audited files and folders.