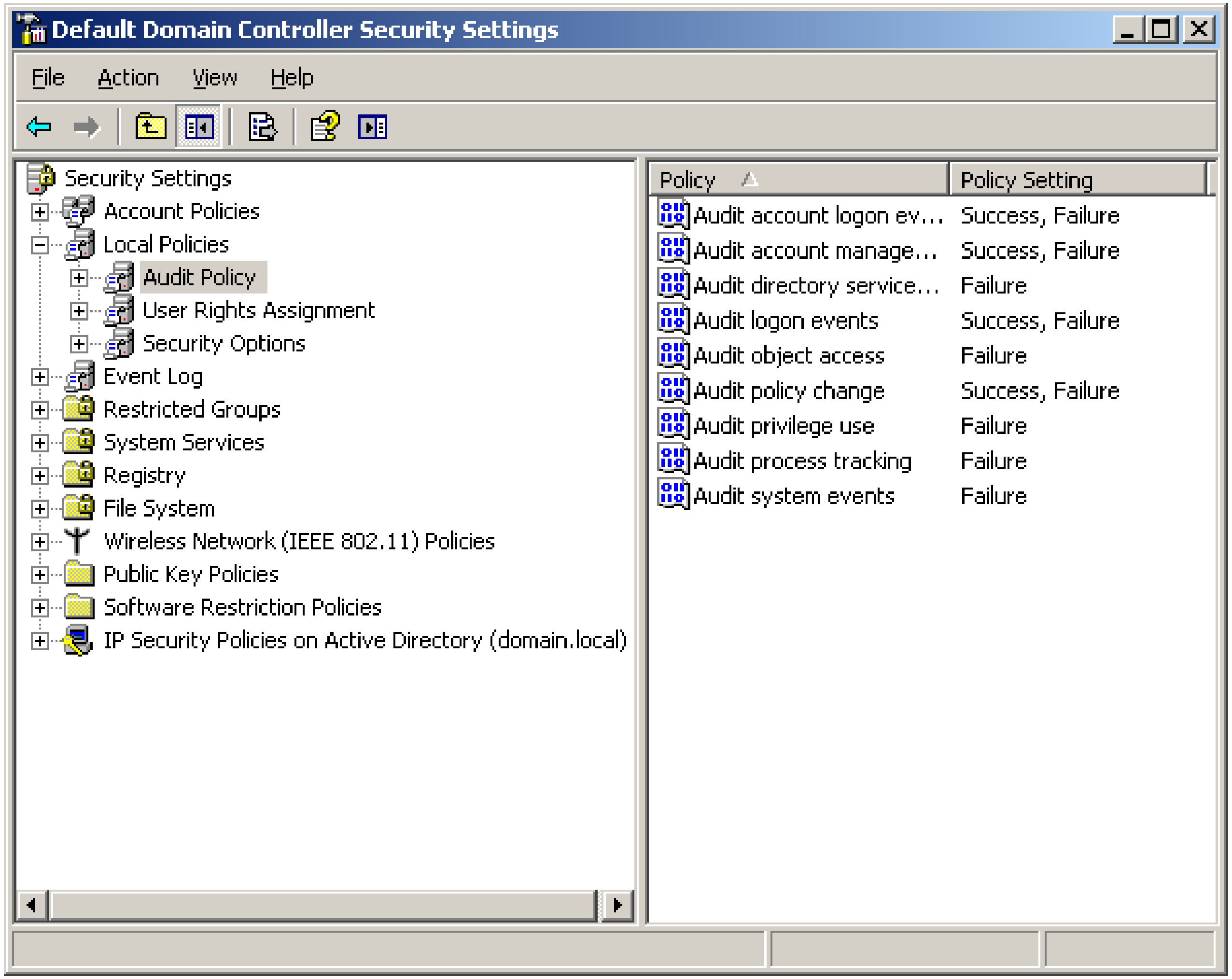
Audit Policies on a Windows Server

July 27, 2010

Domain Controller Security Settings

We open Domain Controller Security Settings window by selecting it on the Administrative Tools menu.

To view the individual polices, we highlight Audit Policies under Local Policies.

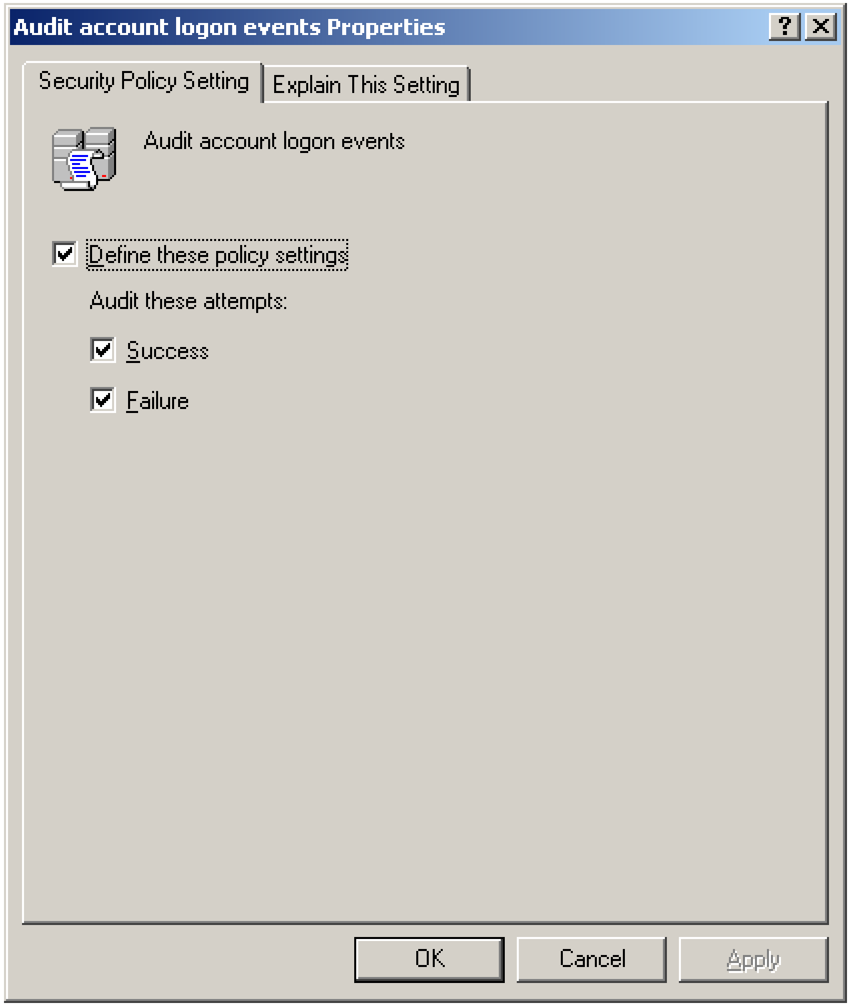


Policy	Policy Setting
Audit account logon ev...	Success, Failure
Audit account manage...	Success, Failure
Audit directory service...	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Failure
Audit system events	Failure

Audit Account Logon Events

This policy setting when made will audit each instance of a user logging on or off the domain from a client computer. The event is placed in the security log. We can choose to track both success and failure. If we check both, we will see an accounting of each attempt in the security log.

We opt to track both success and failure.



Audit account logon events Properties

Security Policy Setting | Explain This Setting

Audit account logon events

☑ Define these policy settings

Audit these attempts:

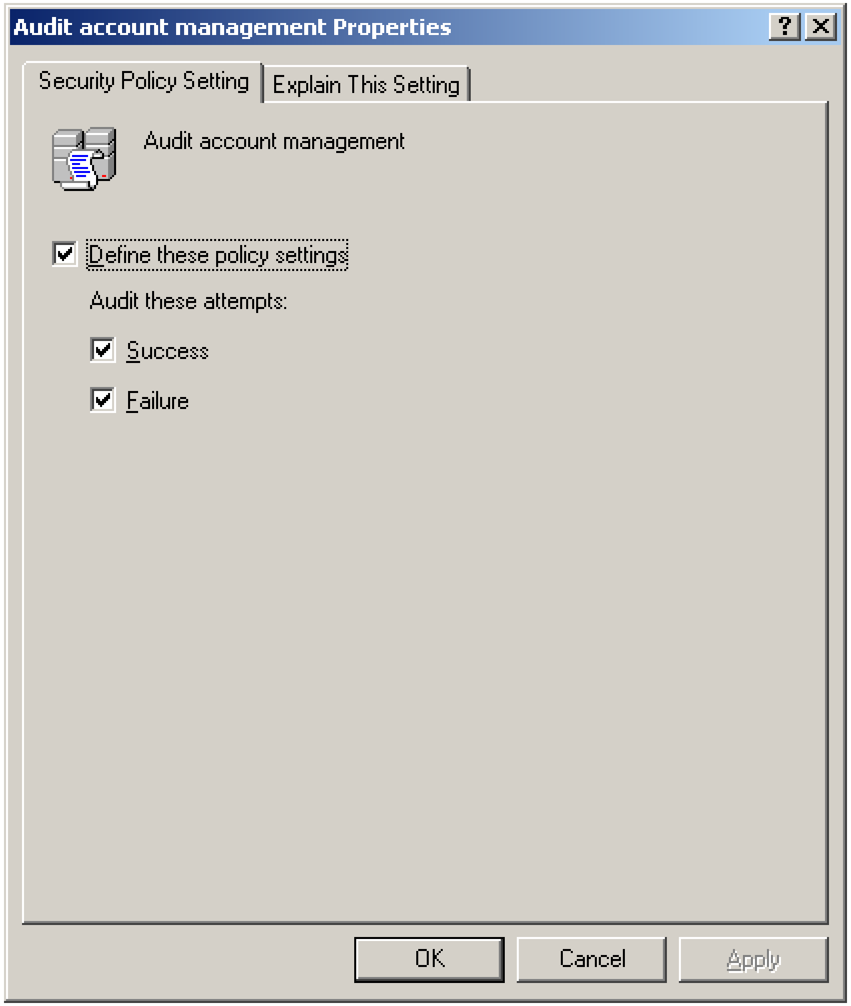
☑ Success

☑ Failure

Audit Account Management

This security setting when made will audit each event of account management on a computer, such as a user account or group is created, changed, or deleted, a user account is renamed, disabled, or enabled and a password is set or changed.

We opt to track both success and failure.



Audit account management Properties

Audit account management

☑ Define these policy settings

Audit these attempts:

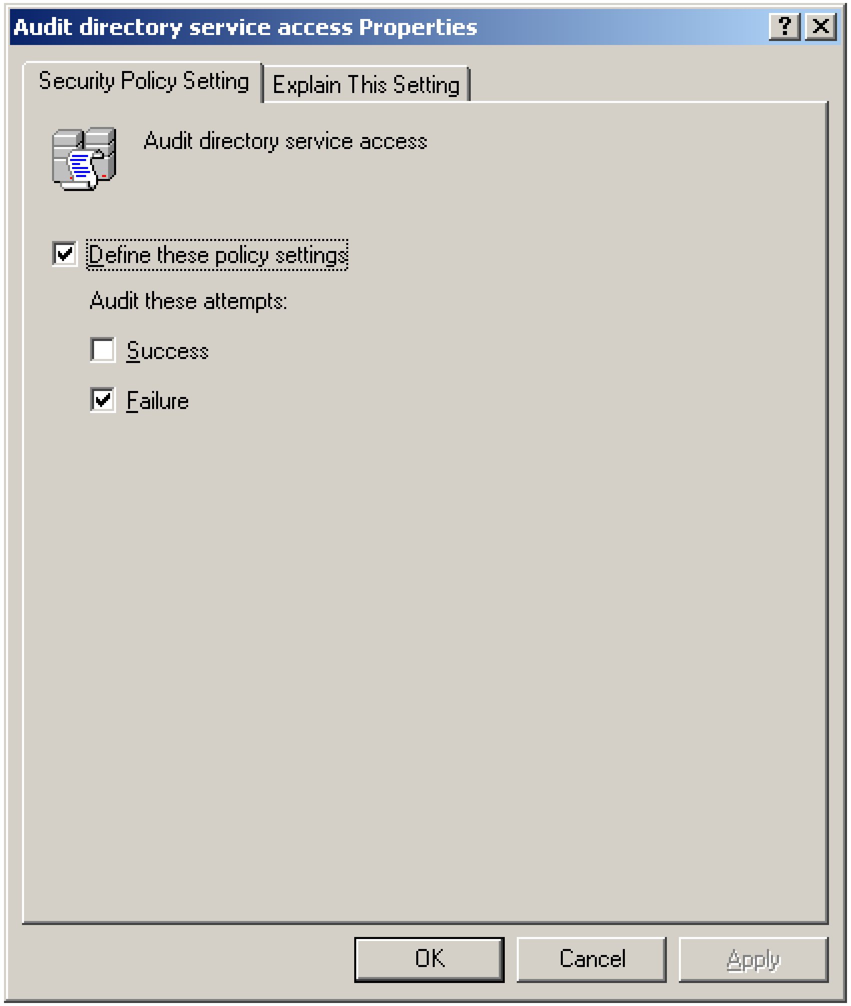
☑ Success

☑ Failure

Audit Directory Service Access

This security setting will audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified. Success audits produce an audit record when a user successfully accesses an Active Directory object that has a SACL specified. Failure audits create an audit record when a user unsuccessfully tries to access an Active Directory object that has a SACL specified.

We opt to track failures.



Audit directory service access Properties

Security Policy Setting | Explain This Setting

Audit directory service access

☑ Define these policy settings

Audit these attempts:

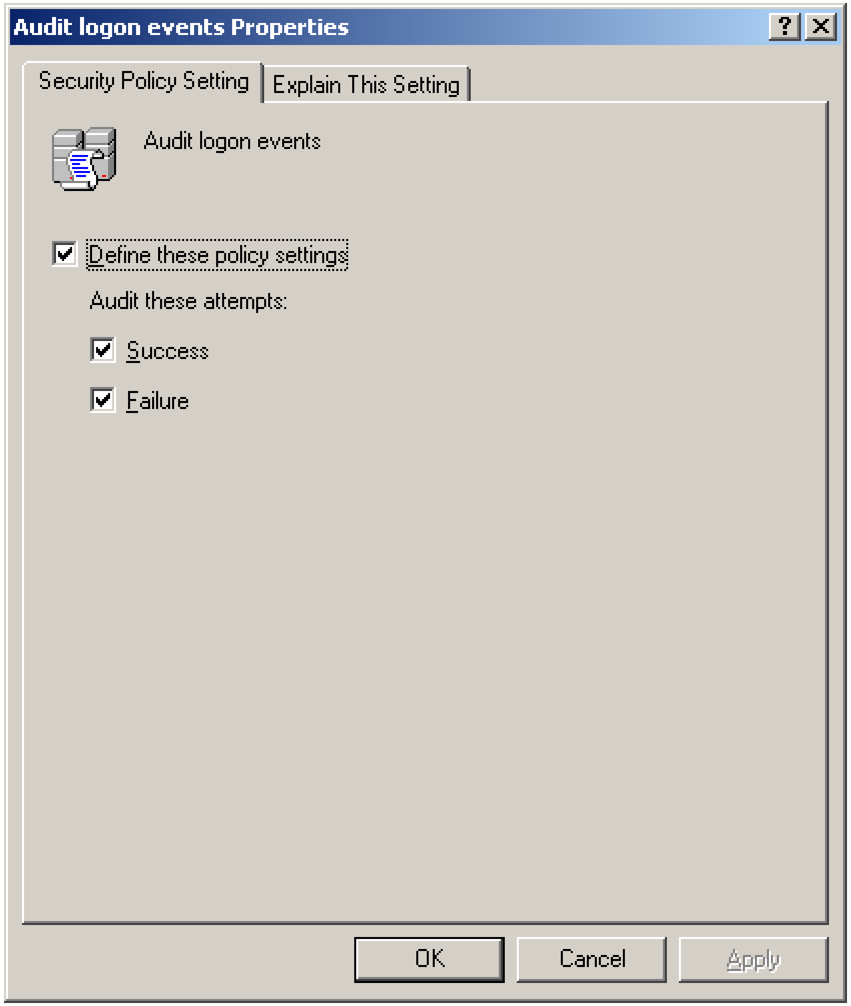
□ Success

☑ Failure

Audit Logon Events

This security setting will audit each time a user logs on to or off a computer. Account logon events are produced on domain controllers for domain account activity and on local computers for local account activity. If both account logon and logon audit policy categories are enabled, logons that use a domain account create a logon or logoff event on the workstation or server, and they generate an account logon event on the domain controller. Also, interactive logons to a member server or workstation that use a domain account produce a logon event on the domain controller as the logon scripts and policies are retrieved when a user logs on.

We will track both success and failure.



Audit logon events Properties

Audit logon events

☑ Define these policy settings

Audit these attempts:

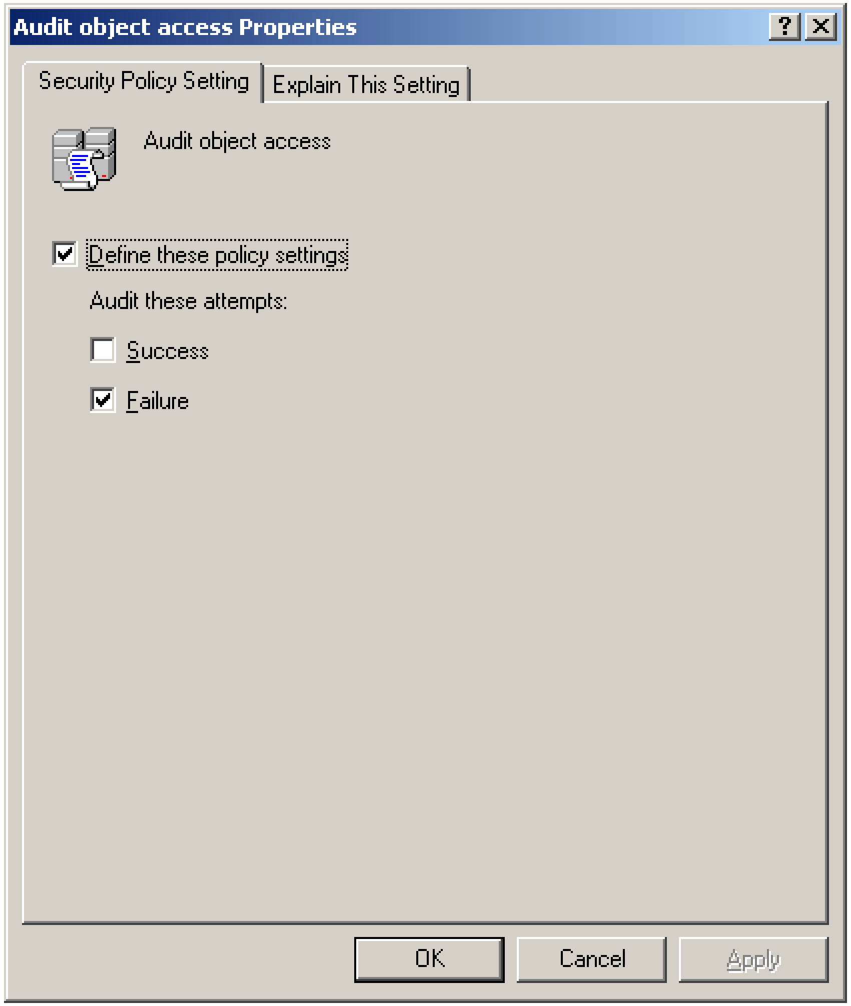
☑ Success

☑ Failure

Audit Object Access

This security setting will audit the event of a user accessing an object—for example, a file, folder, registry key, printer, and so forth—that has its own system access control list (SACL) specified.

If we define this policy setting, we will specify failure, so there will be a report generated when a user unsuccessfully attempts to access an object that has a SACL specified.



Audit object access Properties

Security Policy Setting | Explain This Setting

Audit object access

☑ Define these policy settings

Audit these attempts:

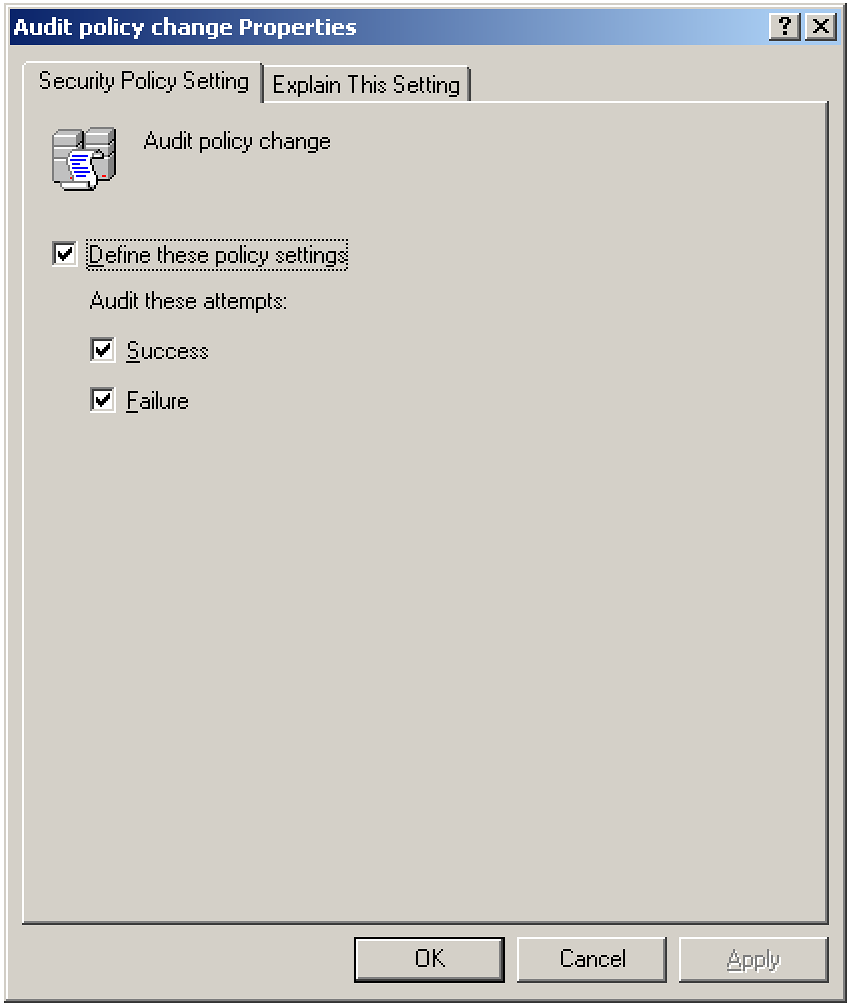
☐ Success

☑ Failure

Audit Policy Change

This security setting will audit every incident of a change to user rights assignment policies, audit policies, or trust policies.

We will define the policy with success and failure. Success audits make a record entry when a change to user rights assignment policies, audit policies, or trust policies is successful. Failure audits create a record entry when a modification to user rights assignment policies, audit policies, or trust policies fails.



Audit policy change Properties

Audit policy change

☑ Define these policy settings

Audit these attempts:

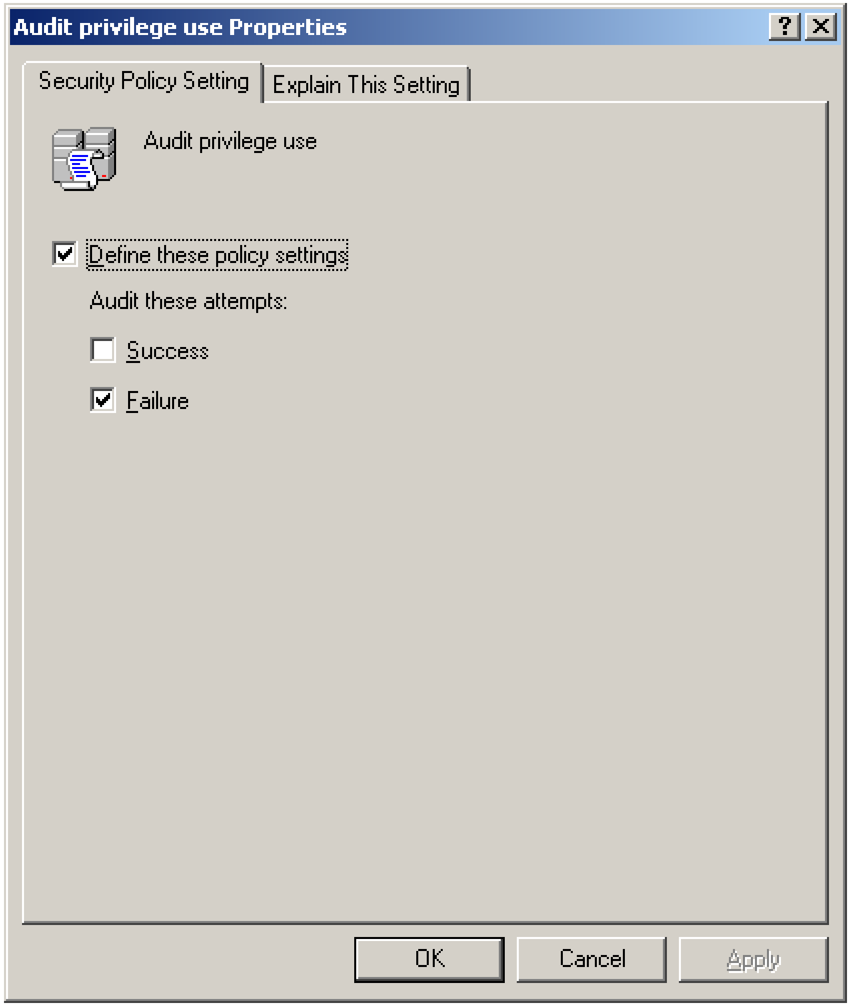
☑ Success

☑ Failure

Audit Privilege Use

This security setting will audit whether each instance of a user exercising a user right is granted or denied.

We choose to track the failures so a report will be generated when the exercise of a user right fails.



Audit privilege use Properties

Security Policy Setting | Explain This Setting

Audit privilege use

☑ Define these policy settings

Audit these attempts:

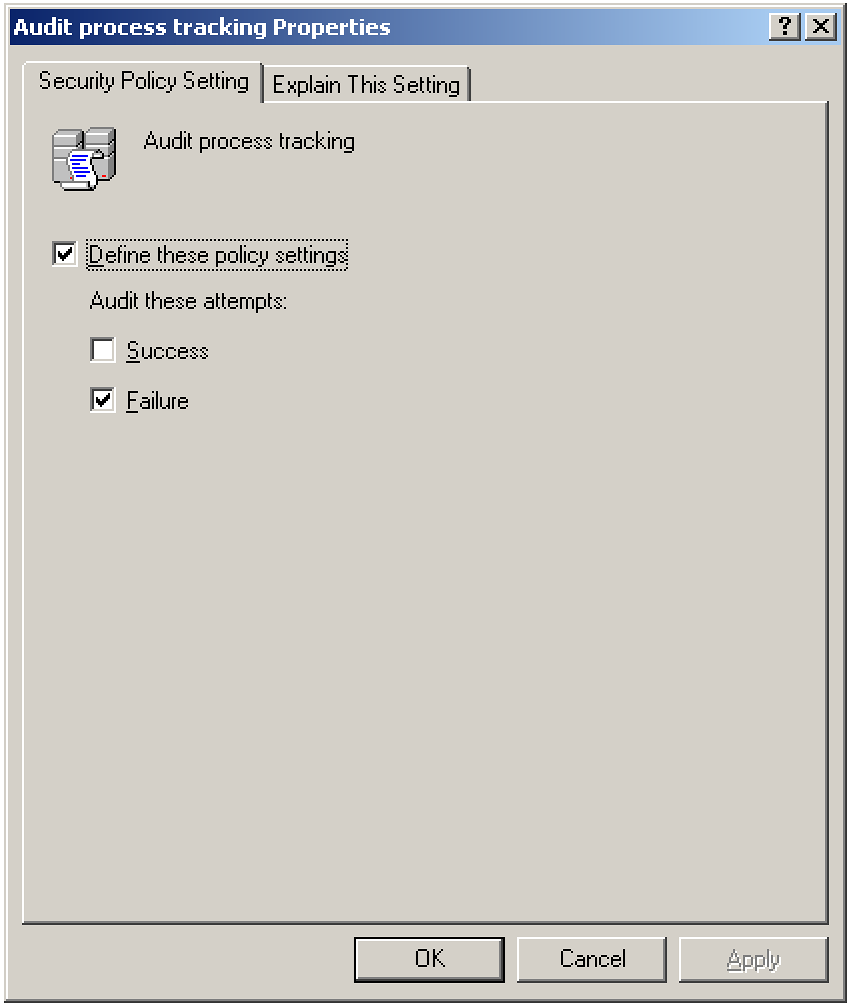
□ Success

☑ Failure

Audit Process Tracking

This security setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

We opt to track failures.



Audit process tracking Properties

Security Policy Setting | Explain This Setting

Audit process tracking

☑ Define these policy settings

Audit these attempts:

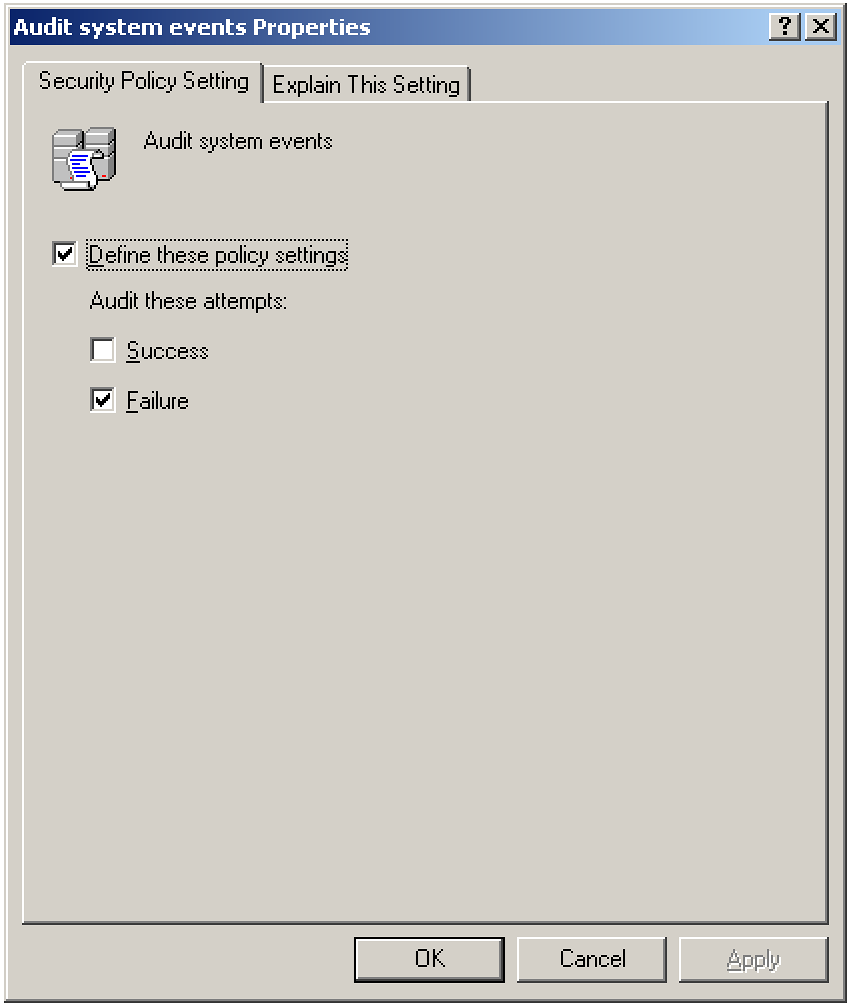
☐ Success

☑ Failure

Audit System Events

This security setting determines whether to audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.

We opt to track failures.



Audit system events Properties

Security Policy Setting | Explain This Setting

Audit system events

☑ Define these policy settings

Audit these attempts:

□ Success

☑ Failure

Audit Policies Completed

Audit policies can be changed anytime by the Network Administrator to help track the functionality of the domain.