

# Windows Vista ACL Class Exercise

## Goal

Use Windows Vista security subsystem to protect elements on a NTFS file system

## Scenario

You need to set up a file system for the Bob Co. This company has three sets of employees:

- Engineers
- Financial folks
- System Administrators

Each set of folks would like a place on the file system where in general they have full control and other folks have read-only access. But each group of folks would like to have the following subareas with different access:

- A public area that gives all users read and write access.
- A private area that blocks everyone except for folks of the same set.

The lab machines have been populated with the following users

- Ellen – Currently an engineer, but she used to be a financial person and she still sometimes fulfills that role.
- Bob – An engineer.
- Carol and Dave are both Financial folks
- Alice and Gus are both sys admins

Each user's password is their name plus "-test", e.g., alice's password is alice-test.

The following groups are also on these machines

- Engineering
- Financial
- Administrators

## Things you need to know

You will need to adjust the audit policies for the SACLs to have any effect. Go to Control Panel -> Administrative Tools -> Local Security Settings -> Local Policies -> Audit Policies. Be careful of enabling too many audit policies. They can get very verbose.

The event viewer is in Control Panel -> Administrative Tools -> Event Viewer

You can look at assigned privileges in Control Panel -> Administrative Tools -> Local Security Settings ->Local Policies ->User Rights Assignment.

You can manipulate the ACL's either graphically through the file explorer or textually through the icacls utility.

The vista image has a “tools” folder on the desktop. This includes some additional utilities like process explorer to examine the security setting on the running system.

## **Things to try**

In class attempt the following tasks.

1. Implement the directory structure that satisfies the security requirements described above.
2. Augment the scenario to block Alice from access to the financial private area (Alice is a member of the Financial group).
3. Cause audit messages to be sent to the event viewer when people without access attempt to access one of the private areas.
4. Is it feasible to block access from one of the administrative users? Why or why not?
5. Try viewing and setting integrity levels.
6. In the private directories, can you create directories or files that can be accessed by non-group users?