Auditing Policy Settings

This reference describes how to determine audit settings by checking the registry.

For troubleshooting purposes, it may be useful to be able to determine the audit policy on a computer without using User Manager. This information is stored in the registry under:

HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv

NOTE: Administrators do not have access to this information by default. You must change the permissions on the registry keys.

This location contains a string of numbers, with the following format:

0Z2114000A0000000B0000000C0000000D0000000E0000000F0000000G00000007000000

Value	Meaning
A	**Restart, Shutdown, System**
B	**Logons and Logoffs**
C	**File and Object Access**
D	**Use of User Rights**
E	**Process Tracking**
F	**Security Policy Management**
G	**User and Group Management**
Z	**Determines if the policy is enabled or disabled.**

If any of the values (A,B,C,D,E,F,G) are set to 1, success auditing is enabled on those areas.

If any of the values (A,B,C,D,E,F,G) are set to 2, failure auditing is enabled on those areas.

If any of the values (A,B,C,D,E,F,G) are set to 3, both success and failures are audited on those areas.

If the value of Z is 1, the policy is enabled; if it is 0, auditing is disabled.

NOTE: You can have an audit policy (such as Audit Successful and Failed Logon Attempts), but have it disabled. You may also have an enabled audit policy that audits nothing.

Examples:

Everything is Audited:

012114000300000003000000030000000300000003000000030000000300000007000000

Nothing is audited (but auditing is enabled):

012114000000000000000000000000000000000000000000000000000000000007000000

Recommended Internet Sites

- How To Determine Audit Policies from the Registry: https://web.archive.org/web/20160306051121/https://www.kazamiya.net/files/PolAdtEv_Structure_en_rev2.pdf

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.