

Get commands

Auditpol /?

```
C:\Windows\system32>auditpol/?
Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?          Help (context-sensitive)
/get        Displays the current audit policy.
/set        Sets the audit policy.
/list       Displays selectable policy elements.
/backup     Saves the audit policy to a file.
/restore    Restores the audit policy from a file.
/clear      Clears the audit policy.
/remove     Removes the per-user audit policy for a user account.
/resourceSACL  Configure global resource SACLs

Use AuditPol <command> /? for details on each command

C:\Windows\system32>Auditpol/?
Usage: AuditPol command [<sub-command><options>]
```

Get audit status of categories

Auditpol /get /category:\*

```
Use AuditPol <command> /? for details on each command

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             Success and Failure
  IPsec Driver                 No Auditing
  Other System Events          Success and Failure
  Security State Change        Success
Logon/Logoff
  Logon                        Success
  Logoff                       Success
Account Lockout
  Account Lockout              Success
IPsec Main Mode
  IPsec Main Mode              No Auditing
IPsec Quick Mode
  IPsec Quick Mode             No Auditing
IPsec Extended Mode
  IPsec Extended Mode          No Auditing
Special Logon
  Special Logon                Success
```

Enable audit to success

Audit /set /subcategory:"Process Creation" /success:enable

```
Non-sensitive Privilege Use    No Auditing
Other Privilege Use Events     No Auditing
Detailed Tracking
  Process Termination          No Auditing
  DPAPI Activity               No Auditing
  RPC Events                   No Auditing
  Process Creation             No Auditing
Policy Change
  Audit Policy Change          Success
```

verify

```
C:\Windows\system32>auditpol /get /subcategory:"Process Creation"
System audit policy
Category/Subcategory          Setting
Detailed Tracking
  Process Creation             Success
```

To get the logs  
Open notepad  
Get systemname  
Open eventveiwier

```
C:\Windows\system32>notepad.exe  
C:\Windows\system32>whoami.exe  
qwerty-pc\qwerty  
C:\Windows\system32>eventvwr.msc  
C:\Windows\system32>notepad.exe
```

