auditpol.exe | Audit Policy Program

Archived: 2026-04-05 23:09:51 UTC

auditpol.exePermalink

- File Path: `C:\Windows\SysWOW64\auditpol.exe`
- Description: Audit Policy Program

HashesPermalink

Type	Hash
MD5	`214E0EA1F7F7C27C82D23F183F9D23F1`
SHA1	`D19837AFE4A9F8631E6F68D1A354E072AEA89388`
SHA256	`7F5B9DCC8F4825D19D9C7B6A82A149DB624E39E0E2B8819317332FA7713C58C5`
SHA384	`C763941493B9D86F2A3647B580FFF282ED7F700B5110488CB80EB0BE07DBE0E422F0F22403CADDFEE0847BC547A2E9CA`
SHA512	`7B067F00510F830872655244D454B26987D118017E7A447ECA77CCD1221814C08753E96066D05818416AE44E65E9B7CBF22DD03BD574FB64388835B328C`
SSDEEP	`768:Aay2Mii5gL4cu7yp+RKSCIbEIbMhfdy3vf7aG:HdfTLg++RxCubady3vf7`

Runtime DataPermalink

Usage (stdout):Permalink

```
 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
```

Usage (stderr):Permalink

```
 Error 0x00000057 occurred:
The parameter is incorrect.
```

SignaturePermalink

- Status: Signature verified.
- Serial: `33000000BCE120FDD27CC8EE930000000000BC`
- Thumbprint: `E85459B23C232DB3CB94C7A56D47678F58E8E51E`
- Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
- Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

- Original Filename: AUDITPOL.EXE.MUI
- Product Name: Microsoft Windows Operating System
- Company Name: Microsoft Corporation

- File Version: 10.0.14393.0 (rs1_release.160715-1616)
- Product Version: 10.0.14393.0
- Language: English (United States)
- Legal Copyright: Microsoft Corporation. All rights reserved.

Possible MisusePermalink

The following table contains possible examples of `auditpol.exe` *being misused. While* `auditpol.exe` *is* ***not*** *inherently malicious, its legitimate functionality can be abused for malicious purposes.*

Source	Source File	Example
sigma	proc_creation_win_susp_nt_resource_kit_auditpol_usage.yml	`title: Suspicious NT Resource Kit Auditpol Usage`
sigma	proc_creation_win_susp_nt_resource_kit_auditpol_usage.yml	`description: Threat actors can use an older version of the auditp available inside the NT resource kit to change audit policy config to impair detection capability. This can be carried out by selecti disabling/removing certain audit policies as well as restoring a c policy owned by the threat actor.`
sigma	proc_creation_win_susp_nt_resource_kit_auditpol_usage.yml	`- https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Windows%202000%20Resource%20Kit%20Tools`
sigma	proc_creation_win_sus_auditpol_usage.yml	`title: Suspicious Auditpol Usage`
sigma	proc_creation_win_sus_auditpol_usage.yml	`description: Threat actors can use auditpol binary to change audi configuration to impair detection capability. This can be carried selectively disabling/removing certain audit policies as well as r a custom policy owned by the threat actor.`
sigma	proc_creation_win_sus_auditpol_usage.yml	`Image|endswith: '\auditpol.exe'`
atomic-red-team	T1562.002.md	Use the cleanup commands to restore some default auditpol settings (your settings will be lost)
atomic-red-team	T1562.002.md	auditpol /set /category:”Account Logon” /success:disable /failure:disable
atomic-red-team	T1562.002.md	auditpol /set /category:”Logon/Logoff” /success:disable /failure:disable
atomic-red-team	T1562.002.md	auditpol /set /category:”Detailed Tracking” /success:disable
atomic-red-team	T1562.002.md	auditpol /set /category:”Account Logon” /success:enable /failure:enable
atomic-red-team	T1562.002.md	auditpol /set /category:”Detailed Tracking” /success:enable

Source	Source File	Example
atomic-red-team	T1562.002.md	auditpol /set /category:”Logon/Logoff” /success:enable /failure:enable
atomic-red-team	T1562.002.md	Clear the Windows audit policy using auditpol utility. This action would st audit events from being recorded in the security log.
atomic-red-team	T1562.002.md	auditpol /clear /y
atomic-red-team	T1562.002.md	auditpol /remove /allusers

Additional Info*Permalink

**The information below is copied from MicrosoftDocs, which is maintained by Microsoft. Available under CC BY 4.0 license.*

---

auditpolPermalink

Displays information about and performs functions to manipulate audit policies, including:

- Setting and querying a system audit policy.
- Setting and querying a per-user audit policy.
- Setting and querying auditing options.
- Setting and querying the security descriptor used to delegate access to an audit policy.
- Reporting or backing up an audit policy to a comma-separated value (CSV) text file.
- Loading an audit policy from a CSV text file.
- Configuring global resource SACLs.

SyntaxPermalink

```
auditpol command [<sub-command><options>]
```

ParametersPermalink

Sub-command	Description
/get	Displays the current audit policy. For more information, see auditpol get for syntax and options.
/set	Sets the audit policy. For more information, see auditpol set for syntax and options.
/list	Displays selectable policy elements. For more information, see auditpol list for syntax and options.
/backup	Saves the audit policy to a file. For more information, see auditpol backup for syntax and options.

Sub-command	Description
/restore	Restores the audit policy from a file that was previously created by using auditpol /backup. For more information, see auditpol restore for syntax and options.
/clear	Clears the audit policy. For more information, see auditpol clear for syntax and options.
/remove	Removes all per-user audit policy settings and disables all system audit policy settings. For more information, see auditpol remove for syntax and options.
/resourceSACL	Configures global resource system access control lists (SACLs). **Note:** Applies only to Windows 7 and Windows Server 2008 R2. For more information, see auditpol resourceSACL.
/?	Displays help at the command prompt.

Additional ReferencesPermalink

- Command-Line Syntax Key
