# Top 11 Windows Audit Policy Best Practices

Last Updated: March 17, 2023 by [Robert Allen](https://activedirectorypro.com/author/mug/)

This is the ultimate guide to Windows audit and security policy settings.

In this guide, I will share my tips for audit policy settings, password and account policy settings, monitoring events, benchmarks, and much more.

Table of contents:

* [What is Windowing Auditing](https://activedirectorypro.com/audit-policy-best-practices/#what-is-auditing)
* [Use The Advanced Audit Policy Configuration](https://activedirectorypro.com/audit-policy-best-practices/#use-advanced-audit-policy)
* [Configure Audit Policy for Active Directory](https://activedirectorypro.com/audit-policy-best-practices/#active-directory-audit-policy)
* [Configure Audit Policy for Workstations and Servers](https://activedirectorypro.com/audit-policy-best-practices/#server-audit-policy)
* [Configure Event Log Size and Retention Settings](https://activedirectorypro.com/audit-policy-best-practices/#event-log)
* [Recommended Password & Account Lockout Policy](https://activedirectorypro.com/audit-policy-best-practices/#password-policy)
* [Recommended Audit Policy Settings](https://activedirectorypro.com/audit-policy-best-practices/#audit-policy)
* [Monitor These Events for Compromise](https://activedirectorypro.com/audit-policy-best-practices/#monitor-events)
* [Centralize Event Logs](https://activedirectorypro.com/audit-policy-best-practices/#centralize-logs)
* [Audit Policy Benchmarks](https://activedirectorypro.com/audit-policy-best-practices/#audit-policy-benchmarks)
* [Planning Your Audit Policy](https://activedirectorypro.com/audit-policy-best-practices/#plan)

## What is Windows Auditing?

Windows auditing is an important component of [Active Directory security](https://activedirectorypro.com/active-directory-security-best-practices/) and helps to monitor network activity.

A Windows audit policy defines what type of events you want to keep track of in a Windows environment. For example, when a user account gets locked out or a user enters a bad password these events will generate a log entry when auditing is turned on.  An auditing policy is important for maintaining security, detecting security incidents, and meeting compliance requirements.

## Use the Advanced Audit Policy Configuration

When you look at the audit policies you will notice two sections, the basic audit policy, and the advanced audit policy. When possible you should only use the Advanced Audit Policy settings located under Security Settings\Advanced Audit Policy Configuration.

The advanced audit policy settings were introduced in Windows Server 2008, it expanded the audit policy settings from 9 to 53. The advanced policy settings allow you to define a more granular audit policy and log only the events you need. This is helpful because some auditing settings will generate a massive amount of logs.

**Important:** Don’t use both the basic audit policy settings and the advanced settings located under Security Settings\Advanced Audit Policy Configuration. Using both can cause issues and is not recommended.

Microsoft provides the following information.

![Graphical user interface, text, application, email

Description automatically generated]()

The advanced audit policy has the following categories. Each category contains a set of policies.

* Account Logon
* Account Management
* Detailed Tracking
* DS Access
* Logon/Logoff
* Object Access
* Policy Change
* Privilege Use
* System
* Global Object Access Auditing

Resources:

[Threats and Countermeasures Guide: Advanced Security Audit Policy](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125919(v=ws.10))

## Recommended Tool: Security Event Manager

[Security Event Manager](https://www.solarwinds.com/security-event-manager?CMP=BIZ-ADP-SW_WW_X_X_PPD_LD_EN_X_0-SEM-X_0_X_X_X_X-X) is an all-in-one SIEM solution for log collection, storage, analysis, and reporting designed to help IT pros identify and respond to cyber threats and demonstrate compliance

Collects consolidates, normalizes, and visualizes logs and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, OS, and other applications

[![Graphical user interface, chart, application, pie chart

Description automatically generated]()](https://www.solarwinds.com/security-event-manager?CMP=BIZ-ADP-SW_WW_X_X_PPD_LD_EN_X_0-SEM-X_0_X_X_X_X-X)

## Configure Audit Policy for Active Directory (For all Domain Controllers)

By default, there is a bare minimum audit policy configured for Active Directory. You will need to modify the default domain controller policy or create a new one.

Follow these steps to enable an audit policy for Active Directory.

### Step 1: Open the Group Policy Management Console

![Graphical user interface, application

Description automatically generated]()

### Step 2: Edit the Default Domain Controllers Policy

Right click the policy and select edit

![Graphical user interface, application

Description automatically generated]()

### Step 3: Browse to the Advanced Audit Policy Configuration

Now  browse to the Advanced Audit Policy Configuration

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration

![A picture containing graphical user interface

Description automatically generated]()

### Step 4: Define Audit Settings

Now you just need to go through each audit policy category and define the events you want to audit. See the recommended audit policy section for the recommended settings.

## Configure Audit Policy on Workstations and Servers

It is highly recommended that you enable an audit policy on all workstations and servers. Most incidents start at the client device, if you are not monitoring these systems you could be missing out on important information.

To configure an audit policy for workstations and servers you will need to create a new audit policy. This will be a separate audit policy from your domain controllers. I would not apply this policy to the root of the domain, it is best to have all your workstations and servers in a separate organization unit and apply the audit policy to this OU.

You can see below I have an organizational unit called ADPRO computers. This organizational unit contains sub OUs for department workstations and a server OU for all the servers. I will create a new audit policy on the ADPRO computers OU, this policy will target all devices in this folder.

![Graphical user interface, text, application

Description automatically generated]()

## Configure Event Log Size and Retention Settings

It is important to define the security event log size and retention settings. If these settings are not defined you may overwrite and lose important audit data.

**Important:** The logs generated on servers and workstations from the audit policy are intended for short term retention. To keep historical audit logs for weeks, months or years you will need to set up a centralized logging system. See the section below for recommendations.

In your audit policy, you can define the event log settings at Computer Configuration -> Policies -> Security Settings -> Event Log

![Graphical user interface, text, application

Description automatically generated]()

Here are the recommended settings

* Maximum application log size
  + 4,194,240 (kilobytes)
* Maximum Security log size
  + 4,194,240 (kilobytes)
* Maximum system log size
  + 4,194,240 (kilobytes)

Even with the log settings configured you could still overwrite events in a short period of time. It all depends on your audit policy and how many users you have. If you are tracking bad password attempts for 2000 users that will generate way more events than 20 users.

Resource:

[Recommended settings for event log sizes in Windows](https://support.microsoft.com/en-us/help/957662/recommended-settings-for-event-log-sizes-in-windows)

## Recommended Password and Account Lockout Policy

To successfully audit user accounts you need to ensure you have the password and account lockout policy configured. If you are auditing for account lockouts but don’t have a lockout threshold set you will never see those events.

These settings are from the MS Security baseline Windows 10 and Server 2016 document.

### Password Policy

GPO location:  Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

* Enforce password history
  + 24
* Maximum password age
  + 60
* Minimum password age
  + 1
* Minimum password length
  + 14
* Password must meet complexity requirements
  + Enabled
* Store passwords using reversible encryption
  + disabled

### Account Lockout Policy

GPO  location: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

* Account lockout duration
  + 15
* Account lockout threshold
  + 10
* Reset lockout counter after
  + 15

Resource:

[Microsoft Security compliance toolkit](https://www.microsoft.com/en-us/download/details.aspx?id=55319)

## Recommended Audit Policy Settings

These settings are from the MS Security baseline Windows 10 and Server 2016 document.

Recommended domain controller security and audit policy settings.

GPO Policy location: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration

#### Account Logon

* Audit Credential Validation
  + Success and Failure
* Audit Kerberos Authentication Services
  + Not configured
* Audit Kerberos Service Ticket Operations
  + Not configured
* Audit Other Account Logon Events
  + Not configured

#### Account Management

* Audit Application Group Management
  + Not configured
* Audit Computer Account Management
  + Success
* Audit Distribution Group Management
  + Not configured
* Audit Other Account Management Events
  + Success and Failure
* Audit Security Group Management
  + Success and Failure
* Audit User Account Management
  + Success and Failure

#### Detailed Tracking

* Audit DPAPI Activity
  + Not configured
* Audit Plug and Play Events
  + Success
* Audit Process Creation
  + Success
* Audit Process Termination
  + Not Configured
* Audit RPC Events
  + Not Configured
* Audit Token Right Adjected
  + Not Configured

#### DS Access

* Audit Detailed Directory Service Replication
  + Not configured
* Audit Directory Service Access
  + Success and Failure
* Audit Directory Service Changes
  + Success and Failure
* Audit Directory Service Replication
  + Not Configured

#### Logon/Logoff

* Audit Account Lockout
  + Success and Failure
* Audit User / Device Claims
  + Not configured
* Audit Group Membership
  + Success
* Audit IPsec Extended Mode
  + Not configured
* Audit IPsec Main Mode
  + Not configured
* Audit Logoff
  + Success
* Audit Logon
  + Success and Failure
* Audit Network Policy Server
  + Not configured
* Audit Other Logon/Logoff Events
  + Not configured
* Audit Special Logon
  + Success

#### Object Access

* Audit Application Generated
  + Not configured
* Audit Certification Services
  + Not configured
* Audit Detailed File Share
  + Not configured
* Audit File Share
  + Not configured
* Audit File System
  + Not configured
* Audit Filtering Platform Connection
  + Not configured
* Audit Filtering Platform Packet Drop
  + Not configured
* Audit Handle Manipulation
  + Not configured
* Audit Kernal Object
  + Not configured
* Audit Other Object Access Events
  + Not configured
* Audit Registry
  + Not configured
* Audit Removable Storage
  + Success and Failure
* Audit SAM
  + Not configured
* Audit Central Access Policy Staging
  + Not configured

### Policy Change

* Audit Audit Policy Change
  + Success and Failure
* Audit Authentication Policy Change
  + Success
* Audit Authorization Policy Change
  + Success
* Audit Filtering Platform Policy Change
  + Not configured
* Audit MPSSVC Rule-Level Policy Change
  + Not Configured
* Audit Other Policy Change Events
  + Not configured

#### Privilege Use

* Audit Non Sensitive Privilege Use
  + Not configured
* Audit Other Privilege Use Events
  + Not configured
* Audit Sensitive Privilege Use
  + Success and Failure

#### System

* Audit IPsec Driver
  + Success and Failure
* Audit Other System Events
  + Success and Failure
* Audit Security State Change
  + Success
* Audit Security System Extension
  + Success and Failure
* Audit System Integrity
  + Success and Failure

#### Global Object Access Auditing

* File System
  + Not configured
* Registry
  + Not configured

I recommend you download the [Microsoft Security compliance toolkit](https://www.microsoft.com/en-us/download/details.aspx?id=55319). It has an excel document with recommended security and audit settings for windows 10, member servers, and domain controllers. In addition, the toolkit has additional documents and files to help you apply security and audit settings.

## Centralize Windows Event Logs

When you enable a security and audit policy on all systems those event logs are stored locally on each system. When you need to investigate an incident or run audit reports you will need to go through each log individually on each computer. Another concern is what if a system crashes and you are unable to access the logs?

and… don’t forget those local logs are intended for short term storage. In large environments, those local logs will be overwritten by new events in a short period of time.

Centralizing your logs will save you time, ensure logs are available, and make it easier to report and troubleshoot security incidents. There are many tools out there that can centralize Windows event logs.

Below is a list of free and premium tools that will centralize Windows event logs. Some of the free tools require a bit of work and may require additional software to visualize and report on the logs. If you have the budget I recommend a premium tool, they are much easier to setup and saves you a ton of time.

1. [SolarWinds Log Analyzer](https://www.solarwinds.com/log-analyzer?CMP=BIZ-ADP-SW_WW_X_X_PPD_LD_EN_X_0-LAZ-X_0_X_X_X_X-X) (Premium tool, 30-day FREE trial)
2. [Windows Event Collector](https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/) (Free, requires additional tools to visualize and report on data)
3. [ManageEngine Audit Plus](https://www.manageengine.com/products/active-directory-audit/) – (Premium tool)
4. [Splunk](https://www.splunk.com/) – (Premuim tool, a popular tool for analyzing various log files)
5. [Elastic Stack](https://www.elastic.co/elk-stack) – (Free download)

## Monitor These Events for Compromise

Here is a list of events you should be monitoring and reporting on.

* Logon Failures – Event ID 4624, 4771
* Successful logons – Event ID 4624
* Failures due to bad passwords – Event ID 4625
* User Account Locked out – Event ID 4740
* User Account Unlocked – Event ID 4767
* User changed password – Event ID 4723
* User Added to Privileged Group – Event ID 4728, 4732, 4756
* Member added to a group – Event ID 4728, 4732, 4756 , 4761, 4746, 4751
* Member removed from group – Event ID 4729, 4733, 4757, 4762, 4747, 4752
* Security log cleared – Event ID 1102
* Computed Deleted – Event ID 4743

## Audit Policy Benchmarks

How do you know for sure if your audit policy is getting applied to your systems? How does your audit policy compare to industry best practices? In this section, I’ll show you a few ways you can audit your own systems.

### Using auditpol

auditpol is a built-in command that can set and get the audit policy on a system. To view the current audit run this command on your local computer

auditpol /get /category:\*

![A picture containing text

Description automatically generated]()

You can check these settings against what is set in your group policy to verify everything is working.

### Microsoft Security Toolkit

I mention this toolkit in the recommended settings section but it is worth mentioning again. It contains a spreadsheet with the Microsoft recommended audit and security policy settings. It also includes GPO settings, a script to install, and GPO reports. It is a great reference for comparing how your audit policy stacks up against Microsoft’s recommendations.

### CIS Benchmarks

CIS benchmarks have configuration guidelines for 140+ systems, including browser, operating systems, and applications.

[CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/)

### CIS CAT Pro

CIS provides a tool that can automatically check your systems settings and how it compares to its benchmarks. This is by far the best method for testing your audit policy against industry benchmarks. The pro version does require a membership, there is a free version with limited features.

[CIS-CAT Pro](https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/)

## Planning Your Audit Policy

Here are some tips for an effective audit policy deployment.

### Identify your Windows audit goals

Don’t just go and enable all the auditing settings, understand your organization’s overall security goals. Enabling all the auditing rules can generate lots of noise and could make your security efforts more difficult than it should be.

### Know your Network Environment

Knowing your network, Active Directory architecture, OU design and security groups are fundamental to a good audit policy. Deploying an audit policy to specific users or assets will be challenging if you do not understand your environment or have a poor logical grouping of your resources.

### Group Policy

It is best to deploy your audit policy with group policy. Group policy gives you a centralized location to manage and deploy your audit settings to users and assets within the domain.

### How will you obtain event data

You will need to decide how will event data be reviewed.

* Will the data be kept on local computers
* Will the logs be collected on each system and put into a centralized logging system?

From Article

[Top 11 Windows Audit Policy Best Practices - Active Directory Pro](https://activedirectorypro.com/audit-policy-best-practices/#what-is-auditing)