

# McAfee Policy Auditor

Integration + Innovation = Compliance Efficiency

Efficiently automate manual audit processes with advanced, purpose-built IT auditing.

## Key Advantages

### Improve operations

Unify management of policy audits and endpoint security

### Reduce time to compliance

Run consolidated audits across both managed (agent-based) and unmanaged (agentless) systems

### Prove compliance consistently

Report against key industry mandates, internal policies and file integrity monitoring

### Automate manual audits

Up-to-date data, powerful dashboards and reports, and built-in waiver management simplify every step

### Enforce compliance

Remediate non-compliant systems with McAfee Remediation Manager

### SCAP-FDCC validated

Validated by NIST as conforming to the SCAP standard

## Raise productivity, lower audit costs

If compliance mandates are intended to improve security, why do audits and endpoint policy management take so much time away from managing IT risk? Because myriad point processes and products result in ad hoc efforts and error.

McAfee offers an optimized approach. Integration and innovation produce real return on investment (ROI) and significant productivity gains, while lowering fear of audits.

## Prove compliance with key industry mandates

By mapping IT controls against pre-defined policy content, Policy Auditor automates manual audit processes and helps you report consistently and accurately against internal and external policies. Policy Auditor ships with benchmark templates for a variety of compliance mandates: the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and the best-practice frameworks ISO 27001 and Control Objectives for Information and Related Technology (COBIT). Templates cover Windows, Solaris, Linux Red Hat, HP/UX, and Mac OS-X platforms.

## Cut management effort with unprecedented ePO integration

Seamless integration with McAfee ePolicy Orchestrator® (ePO™) eases agent deployment, management, and reporting. The single ePO console lowers cost of ownership by consolidating

endpoint security management and compliance management. You save hardware, training, and operational costs, and get unified control over the policies and protections on each host.

## Optimized file integrity monitoring

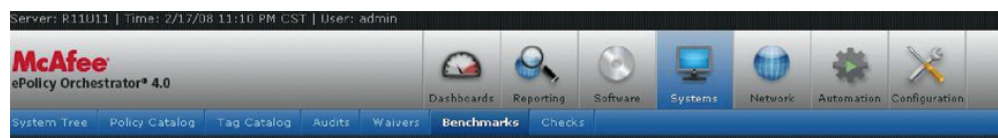
McAfee Policy Auditor has been extended with file integrity monitoring capabilities, including the ability to detect changes to file and directory permissions and content through scheduled scans. It also includes powerful reporting, the ability to measure against baseline configurations, and a single interface, McAfee ePolicy Orchestrator, to monitor and approve policy changes.

## Unified policy audits to reduce time to compliance

Organizations can run consolidated audits across both managed (agent-based) and unmanaged (agentless) systems. From ePO they can define and select a unified policy benchmark once and have the assessment performed across many different asset types. This reduces the effort needed to run audits and, for the first time, provides organizations with a single unified report across all assets.

## Use scripting to further extend Policy Auditor agent check capabilities

Create rules from any scripting language supported by the system being audited to extend the check capabilities of Policy Agents further. Sample languages include VBScript, Batch files, Perl and Python.



Four Policy Auditor tabs in the ePO console make it easy to deploy policies and manage audit processes.

**Specifications**

**Server and console**

- Free disk space: 1 GB minimum (first-time installation); 1.5 GB minimum (upgrade); 2 GB recommended
- Memory: 1 GB RAM minimum (2–4 GB recommended)
- CPU: Pentium III-class 1.0 GHz or better (1.5 GHz or better, multi-processor or dual-core recommended)
- Operating system: Microsoft Windows 2000 SP4/Windows Server 2003 SP1/2 R2 (32-bit) only

**McAfee agents**

- CPU: Pentium-class, Celeron, or compatible processor
- Memory: 512 MB RAM minimum (1 GB recommended)
- Free disk space: 100 MB
- Operating system: Windows 2000, XP, 2003, Vista; Linux Red Hat; Solaris; Macintosh OS-X; HP/UX

**Database software**

- Microsoft SQL Server 2005, MSDE 2000, or SQL 2000

**Remote console**

- New web-based console only requires a web browser

**Web browser**

- Microsoft Internet Explorer 6.0 SP1 or later

**Meet the new standard in compliance validation: SCAP**

Policy Auditor sets a new standard with its aggressive implementation of the Secure Content Automation Protocol (SCAP) family. This open standard enables interoperability between products and services, helping reduce audit time, expense, and effort. Supported protocols include:

- eXtensible Checklist Configuration Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)
- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)

**Import and adapt industry benchmarks in minutes**

Through SCAP support and its own innovative engineering, McAfee helps you validate compliance easily, even when benchmarks and policies change. Download benchmarks from authoritative sites, such as the Federal Desktop Core Configuration (FDCC) benchmark on the National Institute of Standards and Technology (NIST) web site, and, within minutes, view detailed security guidance to benchmarks. Uniform benchmarks limit misinterpretations between security teams and external auditors.

**Ensure up-to-date data and reduce disruptions**

An innovative continuous audit model helps security and audit teams ensure data is current and accurate. It eliminates manual data generation for internal and external audits. To prevent disruption to critical business applications,

a blackout window lets IT operations specify times when audits may not be conducted.

**Align business and audit processes**

Audits are never convenient, but they can now be less disruptive. You can document and grant three types of waivers to justify deviations from policy, and set expiration dates to limit exposure.

- Exemption—Excuses a system from all audits
- Exemption—Excuses a system from all audits
- Suppression—An exception that is suppressed from reports

**Simplify trouble ticketing**

When audits detect issues, ePO helps you create and track them easily. Optional integrations let you push tickets to third-party trouble ticketing systems like Remedy.

**Enforce compliance through McAfee Remediation Manager**

Go beyond identifying problems. Import Policy Auditor results into McAfee Remediation Manager for automated remediation of non-compliant systems.

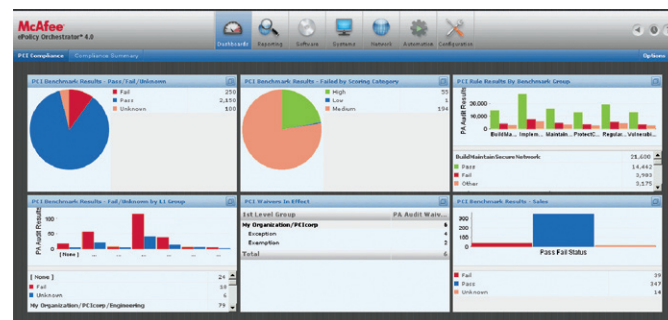
**McAfee solution services**

Along with our McAfee SecurityAlliance™ partners, McAfee offers a wide variety of services to help you assess, plan, deploy, tune, and manage your security and compliance efforts.

**Technical support**

McAfee Gold Technical Support is included with your purchase. Make sure everything runs smoothly during and after installation by upgrading support with flexible programs from McAfee Technical Support.

For more information about Policy Auditor, please visit [www.mcafee.com](http://www.mcafee.com).



Powerful, graphical dashboards help you measure, monitor, and report compliance.

