McAfee Enterprise Log Manager

Cut compliance costs with log collection, storage, and management

By properly collecting and storing logs, you will reduce the cost of compliance with a clear audit trail of activity that can't be repudiated. McAfee® Enterprise Log Manager efficiently collects, compresses, and stores all log files. Integration with McAfee Enterprise Security Manager provides advanced searching, analytics, correlation, alerting, and reporting. All events and alerts provide easy, one-click access to the original source log record, so your forensics efforts will benefit too.

Key Advantages

- Universal log collection and retention to meet compliance requirements
- Flexible storage and retention appropriate to each log source
- Supports chain of custody and forensics
- Log analysis and search
- Stores logs locally or via a managed storage area network
- Fully integrated with McAfee Enterprise Security Manager
- Flexible, hybrid delivery options include physical and virtual appliances

If it is a log file, McAfee Enterprise Log Manager collects, signs, and stores it. McAfee automates log management and analysis for all log types, including Microsoft Windows event logs, database logs, application logs, and syslogs. Logs are signed and validated, ensuring authenticity and integrity—a necessity for regulatory compliance. Out-of-the-box, compliance rule sets and reports make it simple to prove that your organization is in compliance and policies are being enforced.

Using this tightly integrated log collection, management, and analysis environment will both strengthen your security profile and dramatically improve your ability to comply with standards such as PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, and SOX.

Intelligent Log Management

McAfee Enterprise Log Manager collects logs intelligently, storing the right logs for compliance, and parsing and analyzing the right logs for security. You can retain logs in their original format for as long as you need to support your specific compliance needs. Since we do not alter the original log files, McAfee supports chain of custody and non-repudiation efforts.

Information retention needs differ depending upon the log source and the varying compliance requirements that you must satisfy. McAfee Enterprise Log Manager uses easily customizable storage pools to ensure that your logs are stored correctly and for the right amount of time. Choose the best storage option for your needs: up to 7.5 TB of usable hard drive disk storage on the appliances and optional fiber channel cards for high-speed storage area network.

Log files alone don't tell us everything that we need. They contain important pieces of evidence and are a critical link in establishing chain of custody, but they also raise important new questions. For example, we might see a username in an access log, but there is no information about that user's role or privileges. We also might know which system was accessed, but we may know nothing about what types of information are used by that system or who should be accessing it.

Integrated with McAfee Enterprise Security Manager

McAfee Enterprise Log Manager is an optional, integrated part of McAfee Enterprise Security Manager. While McAfee Enterprise Log Manager stores the logs, McAfee Enterprise Security Manager can deeply parse, normalize, and analyze log information, making it immediately available for real-time security investigations and incident response.

When a security event is generated, the parsed event files are linked directly to the source log file and even to the specific log record—enabling one-click access during the event management and forensic processes. There's no extra step, extra application to launch, or extra time wasted searching through logs manually.

Rich Context for Analysis

McAfee Enterprise Security Manager and McAfee Enterprise Log Manager together provide context about each and every log—making every parsed log record more valuable. Information can include:

- The source or destination IP address
- Identity context

Use Cases

McAfee Enterprise Log Manager provides log management and retention capabilities to support advanced use cases, including:

- Establish and automate compliant data/log retention
- Establish non-repudiation of evidence
- Establish an audit trail for administrator activity
- Establish an audit trail for user account activity and changes
- Establish automated reporting

- The hostname or service being used
- Vulnerability information from a vulnerability assessment scanner
- Network topological information
- Policy and privacy information

Flexible Storage Pools

McAfee Enterprise Log Manager storage pools add flexibility to how logs are kept long term. Storage pools are virtual groups of usable storage that can be distributed across various groups of physical storage devices (local storage, NFS, SAN, FTP, SCP, CIF, and others) to accommodate different log management needs.

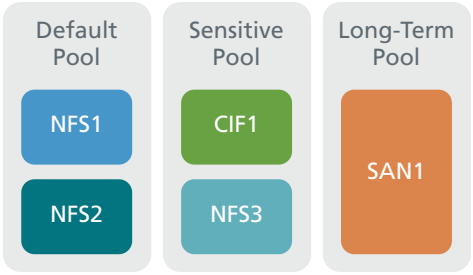

Figure 1. Flexible storage pools support custom log retention.

A storage pool can consist of multiple devices, and data can be assigned to a particular pool based on the source device, so that logs can be stored in separate locations based on their relevance to security, compliance, confidentiality, or other criteria. For example, logs that are critical to compliance might be stored to a pool consisting of multiple, redundant network storage devices. Less critical logs might be stored to less redundant systems; and logs that are most useful for forensics might be stored locally for more rapid analytics.

Fast Deployment

McAfee Enterprise Log Manager and McAfee Enterprise Security Manager can be deployed together using a single combination appliance or can be distributed both horizontally and hierarchically to support even the largest enterprise networks. In either case, McAfee Enterprise Log Manager is easy to deploy. Just select "enable logging" on any configured data source, and those logs will be digitally signed and stored.

Integrated with Your Infrastructure

While most log management solutions operate in isolation, McAfee Enterprise Log Manager works in concert with other information security systems. Through McAfee Enterprise Security Manager, it connects to the rest of your security infrastructure to simplify security operations, improve overall efficiency, and lower costs. You can integrate intelligent log management with powerful analytics, network inspection, database event monitoring, and more.

Full Text Search

The enhanced search view is available when there is a McAfee Enterprise Log Manager device on the system. It provides you with real-time tracking of search progress and results when you are performing a search of logs on the McAfee Enterprise Log Manager. It uses an internal full-text indexing engine to limit the number of files searched, reducing search time. Additionally, the enhanced graphical user interface takes advantage of both the indexing engine and the McAfee Enterprise Log Manager archive's statistical reporting capabilities to provide you with real-time information about the amount of data that must be searched, allowing you to further constrain the query to minimize the number of files to be searched.

System Specifications

Hardware Specifications	ELM-6000	ELM-5600	ELM-4600
Collection Rates	75,000 events per second	50,000 events per second	40,000 events per second
Analytical Performance	14 TB	8 TB	1.8 TB

For more information, visit mcafee.com/ELM.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

47200ds_elm_0612_fnl_ETMG