

McAfee ePolicy Orchestrator 3.5

Centrally Manage Your System Security

Networked systems require constant vigilance against malicious threats and attacks—they're always out there, testing defenses, probing for weaknesses. Because of this, an administrator's job is a delicate balancing act. On one side are the demands of the business—managing a growing array of devices and responding to the needs of increasing numbers of mobile users. On the other side are the demands of security—keeping your systems compliant and managing the multiple layers of next-generation protection and tools required for today's evolving threats.

Complete visibility into your system security and enforcement of what is already in place is vital. Ultimately, each of these demands is constant and equal. Let one slip, and your universe can be thrown into a complete imbalance.

McAfee® ePolicy Orchestrator® 3.5 (ePO™) is the industry-leading, system security management solution—delivering a coordinated, proactive defense against malicious threats and attacks for the enterprise. As the central hub of McAfee System Protection Solutions, administrators can mitigate the risk of rogue, non-compliant systems, keep protection up-to-date, configure and enforce protection policies, and monitor security status, 24/7, from one centralized, truly enterprise-scalable console.

Mitigate the Risk of Rogue, Non-Compliant Systems

Mitigating attackable weaknesses should be a key priority for all security teams. A single, unknown system lacking appropriately managed protection represents a significant threat to the entire network—constant re-infection of known threats, the introduction of new vulnerabilities, potential threat targets, or propagation points all represent the symptoms and risks of these rogue systems. The knowledge of all systems connecting to the network is therefore critical to successfully protect the enterprise.

The problem of rogue systems is further compounded by the fact that in most networks, the only requirement to join is physical access. Contractors, outsourced employees, visitors to conference rooms, or just simply forgotten systems all have the same opportunity to connect to the corporate network and unintentionally represent a significant threat to network integrity and availability.

ePO 3.5 takes a unique approach to mitigating the risk of rogue, non-compliant systems. Using distributed sensors, ePO 3.5 passively monitors the network for any LAN-based connections, quickly establishing whether they are currently managed by ePO 3.5 and providing a range of policy-based responses to rogue systems that are not managed by

ePO 3.5. By rapidly identifying unmanaged systems, administrators are empowered to significantly improve system security compliance and mitigate the weakness of rogue, non-compliant systems.

Monitor System Security 24/7

ePO 3.5's integrated notification services and graphical reporting provide the 24/7 visibility required to effectively monitor system security, evaluate your policy's status, and find your network's weak points.

Instant, proactive information is critical for a security professional especially when monitoring compliance and threat activity. ePO 3.5 delivers integrated alerting and notification on compliance, threat activity, and rogue systems. Thresholds, defined by the administrator, will enable critical alerts to be sent to specified individuals via e-mail, SMS, text pager, or SNMP trap. Alerts cover threat activity, anti-virus compliance levels, and rogue system detections.

Furthermore, locating non-compliant systems, tracing an outbreak to its source, or determining effectiveness of security policies is effortless with ePO 3.5's wide array of over forty pre-defined reports. Ranging from one-page, executive security summaries to detailed information on virus policy and activity, desktop firewall policy, system vulnerabilities, anti-spam, and content filtering policies, all of the information is at your fingertips. Customizing reports to suit your specific needs is just as easy. Administrators may select from a variety of printable and exportable chart types including three-dimensional bar charts, pie charts, line graphs, and tables. ePO 3.5 is integrated with Business Objects® Crystal Reports technology and Microsoft® MSDE/SQL server for a balance of simplicity and power that suits every size of company.

Enforce Protection Compliance and Updates

One of the most difficult aspects of proactively managing a security policy is keeping all systems compliant with the latest protection. ePO 3.5 ensures enterprise-wide compliance with automatic policy enforcement, preventing systems from falling out of compliance and stopping end users from changing settings or disabling vital protection.

ePO 3.5 is central to effectively managing the update process. Updates can be scheduled at determined intervals by administrators and can be set per system or group or other method designated by the administrator. It uses an intelligent design of distributed repositories that puts none of the updating burden on the server, spreading the updating

throughout the network, keeping network traffic low and performance high. And it is comprehensive, with the ability to deploy updates for all McAfee DATs, engines, service packs, hotfixes, and patches.

Proactively Assess Microsoft Patch Compliance

Taking proactive measures to reduce system vulnerabilities and measuring the effectiveness of your patch deployments are simple and straightforward with ePO 3.5. The System Compliance Profiler (SCP) is an integral component of ePO 3.5, enabling security professionals to quickly assess enterprise-wide, system compliance, including the presence of vital Microsoft security patches. Profiling is based on rules, customized by the administrator or templates downloaded from McAfee, searching for a file, service, registry key, or specific Microsoft patch reference. Patch *fingerprinting* (utilizing MD5 hash codes) is also available to ensure absolute integrity of Microsoft security patches and prevent patch spoofing. Criticality of compliance is set by the administrator and easily monitored in the form of detailed, graphical compliance reports.

Respond Rapidly to Outbreaks

For effective outbreak response, ePO 3.5 is key in providing administrators with the means to tailor a response specifically to the threat. In emergencies where you need all machines to update immediately, the server can demand that all agents *update now* and effect that change across the network. Alternatively, the outbreak might require policy changes on the system firewall, or it might require just an update or policy change at the gateway. With ePO 3.5, your response will be immediate and laser-point-focused to the task at hand.

Express Global Updating ensures rapid enterprise updating—up to 50,000 systems in an hour or less—all verified within ePO 3.5's powerful reporting. Distribution across the global network ensures bandwidth efficiency and greatly increases the ability to respond to new and emerging threats.

Protect Mobile Users

With ePO 3.5, *mobile employee* doesn't have to be a scary phrase for the security team. By enforcing policy, even when the laptop is not connected to the network, and making updates happen whenever a connection to the Internet is sensed, ePO 3.5 effectively manages your unmanageable infrastructure. And since mobile and remote users demand more flexibility, ePO 3.5 automatically provides them with updates from the nearest, most bandwidth-efficient repository and allows postponeable and resumable updating. Ultimately, ePO 3.5 ensures that your remote and mobile

users are as well protected and easily managed as those connecting via LAN.

Enterprise-Wide Management Made Easy

ePO 3.5 is designed with enterprise scalability in mind, managing up to 250,000 users per server and easily operated from anywhere using a remote console, saving your company the costs of additional hardware and management. Policies covering every layer of malicious threat protection—from updating frequency, to personal firewall settings, to patch assessment, to file types to be scanned, to heuristic scanning settings—can be centrally set per machine or per group and are entirely customizable by the administrator. All are automatically enforced to ensure rock-solid protection.

Need to manage protection in more than one language? No problem. Want to manage legacy anti-virus products as well as the current security applications? Easy. Need to have different administrators manage different parts of your network? Done deal. Have Windows®, Linux, and NetWare file servers? No sweat. Want integration with Microsoft Active Directory? No problem. Want to add system firewalls and intrusion prevention? Simple. ePO 3.5 handles all this with ease.

Integrate with Key Infrastructure Investments

Designed with administrative efficiency in mind, ePO 3.5 focuses on leveraging key investments in Microsoft Active Directory (AD), ensuring simplified change control and directory consistency throughout the enterprise. Microsoft AD integration allows the scheduled importing of systems from AD into the ePO 3.5 directory and also, where appropriate, provides the capability to identically mirror AD groupings within the ePO 3.5 directory.

Lower Operational and Infrastructure Costs

ePO 3.5 will help you consolidate your security vendors, integrate with your network and security infrastructure, and reduce capital and operational costs with one centralized approach to managing system security.

Two Important Questions

In the fight against malicious code, there are a lot of questions you can ask, but there are really only two that matter. The first is, *Are we protected?* The second is, *Are we infected?* ePO 3.5 can answer both—ensuring your protection is in place with verification and a display of your hotspots.

System Requirements

For System Requirements information, see the System Requirements data sheet.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, ePolicy Orchestrator, ePO, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-e35-001-0704