

McAfee Compatible Solution: AirPatrol WPM 1.0 and McAfee ePO 4.0

Use AirPatrol Wireless Policy Manager and McAfee® ePolicy Orchestrator® software to control wireless connectivity in your enterprise

AirPatrol's Wireless Policy Manager (WPM) is now integrated with McAfee ePolicy Orchestrator® (McAfee ePO™) software. WPM secures wireless interfaces on enterprise endpoints and empowers IT administrators to easily enforce common-sense rules on governing how employees use their wireless connectivity.

Today's wireless world is one in which ideas are exchanged faster, collaboration with colleagues is easier, and the traditional boundaries of an office environment have faded. With this new-found freedom comes a heightened requirement for wireless security. As companies embrace a wireless ecosystem, they realize the criticality of wireless security and the need to protect and manage the wireless assets they own. Making matters worse, the large majority of today's wireless users do not know how to securely use the wireless assets entrusted to them.

McAfee and AirPatrol solution and benefits

AirPatrol believes that wireless ubiquity and comprehensive security are not mutually exclusive. Armed with the proper tools, IT and security departments can effectively manage and mitigate wireless risks while supporting all the benefits that wireless networking offers. Using AirPatrol WPM, organizations of any size can strengthen their efforts to maintain a highly secure and compliant posture for regulations like NIST SP800-53, DoDD 8100.2, FISMA, PCI, SOX, HIPPA, and more.

WPM extends the capabilities of the McAfee ePO platform into the wireless domain, giving network administrators the ability to manage, distribute, and enforce wireless network policies from their central ePO management console. With WPM, organizations can secure their valuable laptops and PCs against today's wide range of mobile and wireless threats.

McAfee Compatible Solution
AirPatrol WPM 1.0 and McAfee
ePolicy Orchestrator 4.0



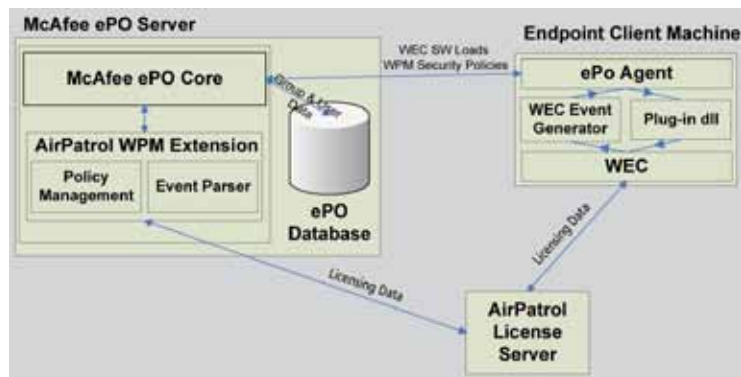
WPM is a centrally management application that an IT administrator uses to create group-, user-, or machine-specific policies that are “pushed” via the ePO infrastructure to an enforcement agent, known as the Wireless Endpoint Client (WEC), which resides on enterprise wireless endpoints.

About AirPatrol Wireless Policy Manager

AirPatrol's Wireless Policy Manager (WPM) is specifically designed to secure the wireless interfaces on endpoints and allow IT administrators to easily enforce common-sense rules that govern how employees use their wireless resources. With WPM, organizations can secure their valuable laptops and PCs against today's wide range of mobile and wireless threats.

About McAfee ePolicy Orchestrator (ePO) software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.



Overview of McAfee and AirPatrol integration.

Benefits

WPM works with ePO software to securely manage a large distributed deployment of WEC across the enterprise. ePO provides a secure infrastructure for:

- Distributing the WEC component to wireless endpoints across the enterprise
- Generating and managing subscriber list of users and endpoints
- Distributing wireless security policies to the distributed endpoints

In this way, the ePO platform provides a secure infrastructure for WPM, and WPM is used to generate and centrally manage tailored wireless endpoint security policies that include:

- AirSafe—Provides automatic, out-of-the-box protection against multihoming. Anytime a laptop's wireless interface (802.11 card or cellular broadband modem) is active and a wired Ethernet connection is attempted, WEC automatically disables the wireless connection.
- Infrastructure authentication policy enforcement for 802.11—Define minimum levels of security required when connecting to wireless networks.
- Ad-hoc authentication policy enforcement for 802.11 —Specify minimum levels of ad-hoc security required or completely disable the use of ad-hoc wireless networks.
- Virtual private network (VPN) policy enforcement—Auto-launch and enforce VPNs if certain wireless security parameters are not met.
- Connection exceptions—Create “whitelists” or “blacklists” of wireless access points to control which access points your users can associate with.
- Endpoint firewall—Enforce the use of host-based firewall prior to allowing wireless network connections
- Location aware—Predefined list of trusted, preferred wireless networks.
- USB device control—Control the types of USB devices that can connect to the WEC-enabled laptop.
- Secure passphrase distribution—Easily and securely distribute SSID passphrases to users.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

