

McAfee Compatible Solution: AirPatrol WPM 2.0 and McAfee ePO 4.5 and 4.6

Use AirPatrol Wireless Policy Manager and McAfee® ePolicy Orchestrator® software to easily secure wireless connectivity within your enterprise.

McAfee Compatible Solution

AirPatrol WPM 2.0 and McAfee ePolicy Orchestrator 4.5 and 4.6

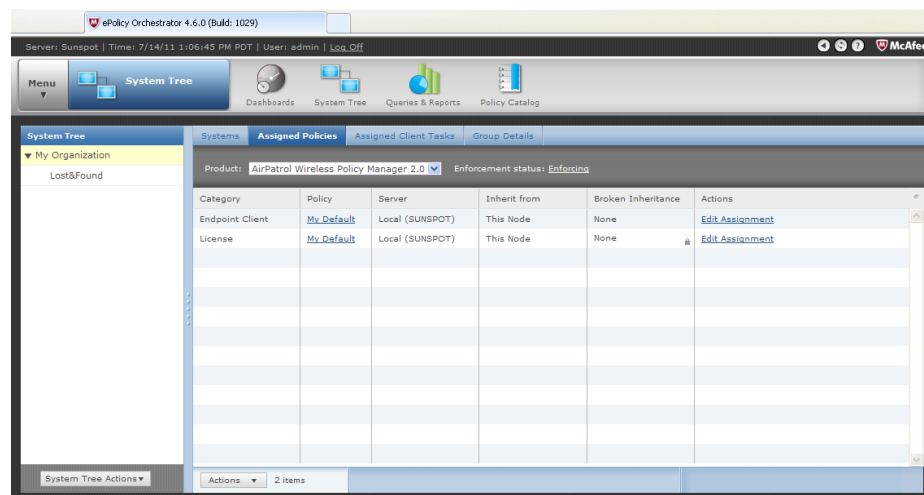
AirPatrol's Wireless Policy Manager (WPM) is now integrated with McAfee ePolicy Orchestrator (ePO) software. WPM secures wireless interfaces on enterprise endpoints and empowers IT administrators to easily enforce common-sense rules on governing how employees use their wireless connectivity.

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 recognize the criticality of wireless security and the need to protect and manage the wireless assets they own.

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.

AirPatrol WPM extends the capabilities of McAfee's 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.



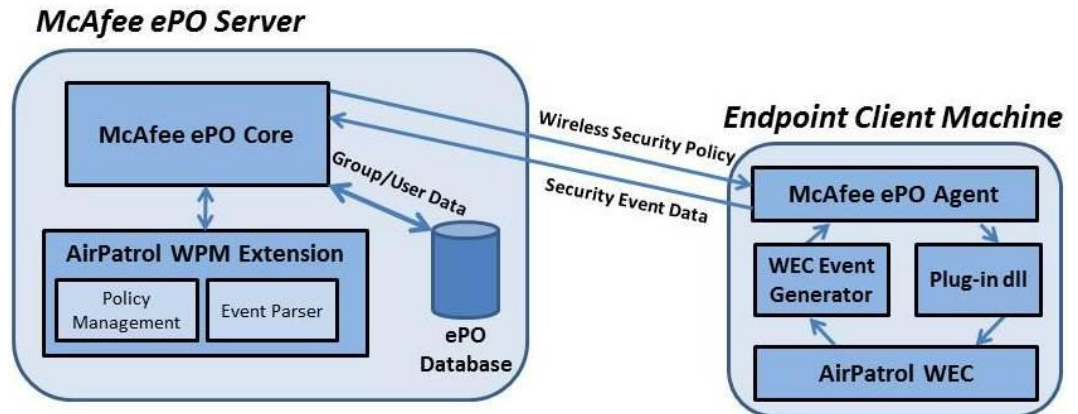
AirPatrol WPM is a centralized management application which an IT administrator uses to create group, user, or machine specific policies which are 'pushed' via the ePO infrastructure to an enforcement agent, known as the AirPatrol Wireless Endpoint Client (WEC), which resides on enterprise wireless endpoints.

McAfee and the McAfee logo [Insert <Relevant McAfee marks>] are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2010 McAfee, Inc..



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.



Benefits

AirPatrol WPM works with ePO software to easily and securely manage a large distributed deployment across the enterprise. EPO provides a secure infrastructure for:

- Distributing the AirPatrol 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 AirPatrol 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 AirPatrol Wireless Policy Manager

AirPatrol's Wireless Policy Manager (WPM) is specifically designed to secure the wireless interfaces on endpoints and allows 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.

